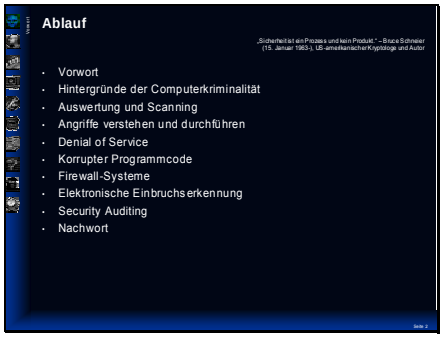
1



Diese Präsentation wurde von Marc Ruef für die Universität Luzern entwickelt. Der Fokus dieser richtet sich auf das Thema Computersicherheit, das in erster Linie für Einsteiger mit soliden Computerkenntnissen verständlich gemacht werden soll. Alle Rechte sind vorbehalten. Das Kopieren der Informationen ist unverfälscht und mit Quellenangabe jedoch erlaubt.

Die Präsentation selbst, Details zu dieser, ein aktuelles Literaturverzeichnis, die Übungen sowie die dazu erforderliche Software finden sich auf der Workshop-Webseite unter http://www.computec.ch/mruef/publikationen/lehrgang_computersicherheit/ - Der Autor steht Ihnen gerne bei Fragen zur Verfügung. Weitere Informationen zum Thema Computersicherheit finden sich auf http://www.computec.ch

2



Es werden zahlreiche Themen aus dem Bereich der Computersicherheit behandelt. Dabei wird sich darum bemüht, die Grundlagen praxisnah zu vermitteln, um das Verständnis für die einzelnen Bereiche zu manifestieren. Nach einer grundlegenden Einführung ins Genre durch Betrachtungen historischer und kultureller Hintergründe wird das technische Vorgehen eines Angreifers besprochen. Dabei werden verschiedene Technologien diskutiert. Im letzten Teil der Vorlesung werden auf spezifische Schutzmassnahmen und –vorgehensweisen eingegangen.

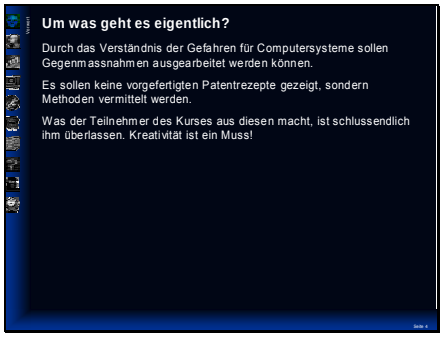
3



Der Autor und Dozent des Lehrgangs Computersicherheit ist Marc Ruef. Er arbeitet als Security Consultant (Leiter Security Auditing) bei der Schweizer Firma scip AG in Zürich (http://www.scip.ch/). Dieses Unternehmen hat sich auf die Beratung im Bereich der Computersicherheit spezialisiert. Einen Grossteil des Kundenstammes machen dabei Finanzinstitute aus.

Marc Ruef betreut seit 1997 die Webseite www.computec.ch, die als das umfassendste Archiv freier deutschsprachiger Publikationen zum Thema Computersicherheit gilt. Er ist Autor verschiedenster Bücher, zeichnet sich für diverse Übersetzungen und einer Vielzahl an Fachartikeln verantwortlich. Zudem ist er Dozent an verschiedenen Universitäten und Fachhochschulen. Desweiteren betreut und unterstützt er diverse internationale Projekte. Zu seinen Hobbies zählen die Musik, Literatur und Informatik im allgemeinen. Weitere Informationen zur Person finden sich auf der privaten Webseite unter http://www.computec.ch/mruef/

4



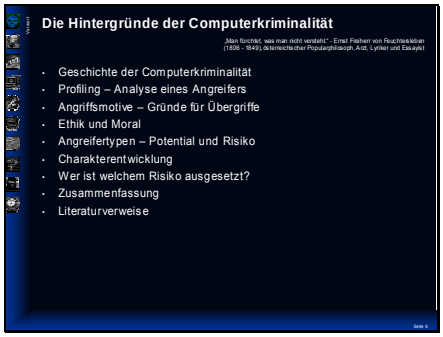
Die Ziele der Vorlesung haben einen primär akademischen und wissenschaftlichen Charakter. Das grundlegende Wissen des Bereichs soll praxisnah vermittelt und so das Interesse des Studenten geweckt werden. Vor allem die Eigeninitiative der Teilnehmer soll angeregt werden. Es werden deshalb keine Patentrezepte für Probleme postuliert, sondern mögliche Herangehensweisen zur Problemlösung besprochen. Was der Teilnehmer des Kurses aus diesen macht, ist schlussendlich ihm überlassen. Kreativität ist ein Muss!

5



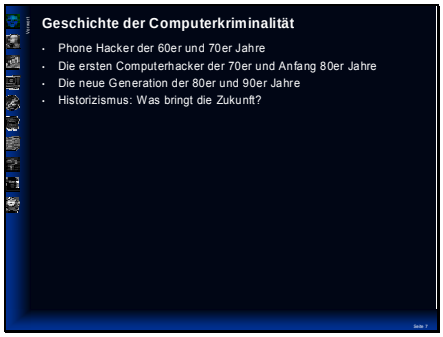
Eine Vielzahl der Folien ist animiert, was natürlich bei ausgedruckten oder konvertierten Exemplaren (PDF) leider nicht zum Zug kommt. Aus diesem Grund wird auf die offizielle PowerPoint-Präsentation verwiesen, die sich auf der offiziellen Workshop-Webseite unter http://www.computec.ch/mruef/publikationen/lehrgang_computersicherheit/ findet. Dort sind ebenfalls weitere Informationen zur Vorlesung, ein aktuelles Literaturverzeichnis, die Übungen sowie die für diese erforderliche Software bereitgestellt. Die Webseite ist für jedermann zu erreichen.

6



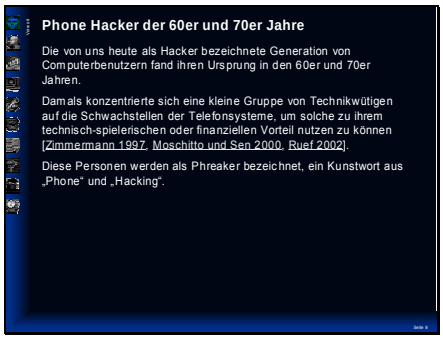
Als Einführung ins Genre wollen wir uns mit den Hintergründen der Computerkriminalität befassen. Dazu werden wir einen historischen Abriss der Entwicklungen betrachten, um uns dann mit der Analyse der Motive zu beschäftigen. Moralische und ethische Aspekte spielen dabei eine zentrale Rolle. Später wollen wir die Angreifertypen klassifizieren, uns mit deren Entwicklung, Potential und Risiko auseinandersetzen. Nur so können wir abstecken, was ein adäquates Mass an Sicherheit überhaupt bedeutet. Denn man fürchtet primär, was man nicht versteht. Zum Schluss wird es wie immer eine Zusammenfassung des Teilkapitels sowie Literaturverweise geben.

7



Die Betrachtungen der Geschichte der Computersicherheit hilft uns zu verstehen, wie das Genre und die Subkultur gewachsen ist. Wir wollen ihre Entstehungsphase mit den Phone Hackern (Phreaker) in den 60er Jahren diskutieren, um danach die Etablierung der Personal Computer (PC) und dem Wandel zum Computer-Hacker Ende der 70er Jahre zu analysieren. Die rasante Entwicklung des Computerbereichs in den 90er Jahren hat auch dazu beigetragen, dass sich im Bereich der Computersicherheit die Dinge überschlagen haben. Auf die interessantesten und wichtigsten Ereignisse dieser Dekade wollen wir ebenfalls eingehen. Zum Schluss werden wir Historizismus betreiben und diskutieren, welche Entwicklungen uns in absehbarer Zukunft erreichen werden.

8



Der Ursprung des Themas Computersicherheit, so sagt man, findet sich in den 60er Jahren. Damals waren Computersysteme noch nicht für jedermann zugänglich und die schwindende Anzahl der an Technik interessierter Personen fokussierte sich auf Telefonsysteme. Durch die Manipulation dieser und dem Umgehen von Sicherheitsmassnahmen entstand der Bereich des Phreakings. Dies ist ein Kunstwort, das aus den beiden englischen Wörtern „Phone" (dt. Telefon) und „Hacking" (dt. Hacken) besteht. In der modernen Literatur populistischer Couleur wird wehmütig auf diese Zeit zurückgeblickt [Zimmermann 1997, Moschitto und Sen 2000, Ruef 2002].

9



Das Buch „Der Hacker" von Christian Zimmermann [1997] bespricht sehr schön die technischen Aspekte damaliger Techniken. Allen voran das populäre Blueboxing. Bei diesem wird mittels einem speziellen Ton, der durch ein Telefon geschickt wird, Einfluss auf das Steuerungssystem genommen. Dadurch liess sich beispielsweise der Gebührenzähler deaktivieren oder Umleitungen speichern. In „Hackertyles" von Denis Moschitto und Evrim Sen [2000] wird die Geschichte der Entwicklung dieser Möglichkeit durch John T. Draper (aka. Captain Crunch) erzählt.

10



Zur damaligen Zeit entwickelte sich das Phreaking schon fast ein bisschen zu einem Volkssport. Vor allem Studenten mit Interesse für Elektronik und Elektrotechnik erachteten das staatliche Telefonnetz als Spielwiese. Immerwieder wurden neue Techniken entwickelt, mit denen gebührenfrei telefoniert oder andere Spielereien umgesetzt werden konnten. So entwickelten sich auch Untergrund-Gruppierungen und –Magazine (z.B 2600, siehe http://www.2600.com/). Damit war der Informationsaustausch der Phreaker gewährleistet, was den Telefongesellschaften natürlich gar nicht behagte, denn diese mussten sich von nun an mit immer raffinierterer Telefon-Piraterie herumärgern. Ursprünglich als kleines Übel abgetan realisierten die Betreiber das Problem und versuchten sich in der Umsetzung effektiver Gegenmassnahmen.

11

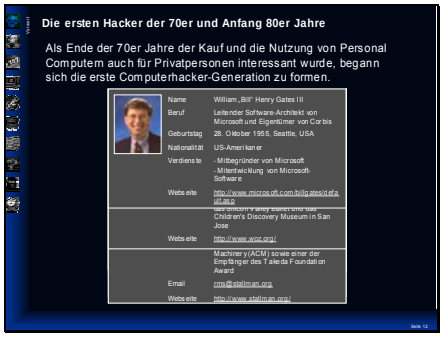


Das Thema Phone-Hacking verlor in den 90er Jahren fortwährend an Reiz. Die Telefongesellschaften hatten mittlerweile ausgeklügelte Systeme etabliert, so dass das Umsetzen klassischer Boxing-Techniken nicht mehr ohne weiteres möglich war. Aber auch mit dem Fall der Telefon-Preise war das Interesse am freien Telefongespräch nicht mehr wirklich gegeben.

Dennoch gab und gibt es weiterhin Techniken, die vereinzelt angewendet werden. Das Thema Beigeboxing, bei dem sich in eine bestehende Telefonleitung eingeklinkt wurde, ist vor allem in Bezug auf öffentliche Telefone interessant geblieben [Phake 1998]. Durch das Wardialing werden Nummernbereiche nach verwertbaren Systemen (z.B. Voicemail-System oder Remote-Modem) abgesucht [McClure et al. 2003]. Das Thema Chipkarten-Hacking ist nach wie vor interessant, erfordert aber ein sehr hohes Mass an technischem Verständnis und oftmals das Vorhandensein teurer Hardware [Ruef 2000a, 2000b, Rankl und Effing 2002]. Mit der ISDN-Technologie wurden neue Möglichkeiten für Angriffe gewährt, die vor allem die 90er Jahre dominiert haben, aber nicht mehr zu einer sehr hohen Verbreitung des Phreakings beitragen konnten [Ferreau 1997]. Das Thema GSM wurde bisher eher stiefmütterlich behandelt, obschon es in diesem Belang einige wichtige Durchbrüche gab.

Gegenwärtig ist der Bereich von Voice-over-IP (VoiP) in aller Munde. Durch die Telefonnutzung über bestehende IP-Kanäle wird einmal mehr die Zusammenführung klassischer Phreaking-Technik und modernem Netzwerk-Hacking gegeben sein [Davidson und Fox 2001, Maguire 2004, Tanase 2004].

12



Als Ur-Hacker werden jene Persönlichkeiten bezeichnet, die sehr früh zur Entwicklung und Mitgestaltung der Computer-Technologien beigetragen haben. Der Begriff „Hacker" wurde dabei mehr als Titel für eine Person verliehen, die ein komplexes Problem sehr effizient adressieren und lösen konnte. Neben den Entwicklern traditioneller Betriebssysteme sind auch die Autoren von Programmiersprachen typische Hacker der alten Generation.

13



Spieltrieb und kriminelle Interessen haben dazu geführt, dass das Thema Computerkriminalität schon sehr früh gegeben war. Interessant dabei ist, dass schon zu Beginn der 70er Jahre computergestützte Betrugsfälle dokumentiert sind.

Eine Auflistung zu wichtigen historischen Ereignissen im Bereich der Computersicherheit wird auf http://www.computec.ch/history.php zur Verfügung gestellt.

14



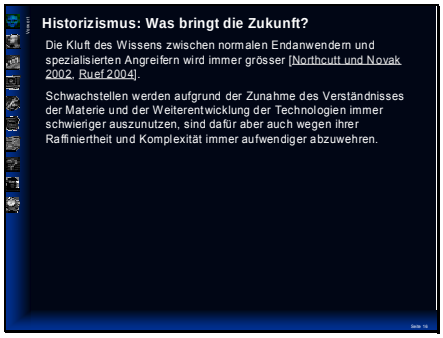
Mit der Popularisierung des Internets entwickelt sich das Thema Computersicherheit mit einer ebenso rasanten Geschwindigkeit. Errungenschaften auf der Seite von Sicherheitsspezialisten gehen mit neuen Angriffsvarianten der Hacker-Community einher. Neue Technologien, Techniken und Methoden werden am laufenden Band vorgestellt und übertrumpfen sich immerwieder mit einer neuen Qualität und Raffinesse. Es bilden sich eine Vielzahl an Hacker-Vereinigungen, die sich entweder für das Aufdecken neuer Schwachstellen stark machen und die Internet-Gemeinschaft vor korrupten Übergriffen warnen wollen [Wieckmann 1998, Rogge 2001]. Eine schöne Illustration der damaligen Entwicklungen ist im Artikel „Die Entwicklung der (deutschsprachigen) Hacker-Szene" von Marc Ruef [2005] festgehalten.

15



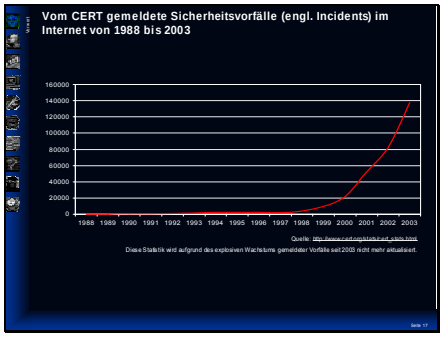
Der Spieltrieb und Neugierde der Angreifer hat Kosten für Industrie und Wirtschaft verursacht. Fortwährend werden neue Fällen von umfangreichen Einbrüchen oder Sabotage-Akten bekannt. Mitte der 90er Jahre spitzt sich der Fall um den US-Amerikaner Kevin Mitnick zu. Nach zweijähriger Fahndung wird er vom FBI verhaftet. Eine etwas einseitige literarische Erzählung der damaligen Ereignisse ist im Buch „Data Zone“ von Tsutsomu Shimomura und John Markoff [1996] festgehalten. Ersterer war massgeblich an der Fassung von Mitnick beteiligt. Die mit dem Titel „Takedown“ (2000, http://www.imdb.com/title/tt0159784/) erschienene Verfilmung des Buches erschien ebenso voreingenommen und wurde durch eine Gegendarstellung der schönen Dokumentation „Freedom Downtime“ von Emmanuel Goldstein (2001, http://www.imdb.com/title/tt0309614/), einem engen Freund Kevin Mitnicks, relativiert.

16



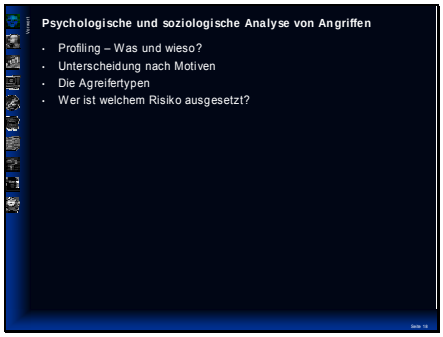
Die Entwicklung im Computerbereich zeigt, dass eine immer grössere Abstraktion gegeben ist. Wobei früher noch mittels Assembler auf einzelne Register des Speichers zugegriffen wird, erfordern moderne Programmiersprachen wie Microsoft Visual Basic .NET nur noch das Ansteuern symbolischer Objekte. Das Verständnis für die innere Funktionsweise der Systeme schwindet aufgrund dieser Meta-Schichten zunehmends. Davon ist ebenfall der Bereich der Computersicherheit betroffen, in dem Transparenz und Verständnis für einzelne Abläufe unabdingbar bleibt. So gibt es immer mehr eine Kluft zwischen normalen Endanwendern ohne tiefschürfende technische Kenntnisse und semi-professionellen Angreifern mit solidem technischem Verständnis. Letztere sehen sich aber zunehmends mit einer Professionalisierung im Bereich der Computersicherheit konfrontiert, so dass moderne Schutzsysteme es überhaupt immer schwieriger machen, ein System erfolgreich anzugreifen. Dies ist mit einem militärischen Wettrüsten vergleichbar, bei dem Angreifer neue Angriffstechniken entwickeln und die Industrie neue Gegenmassnahmen dagegen verkaufen will.

17



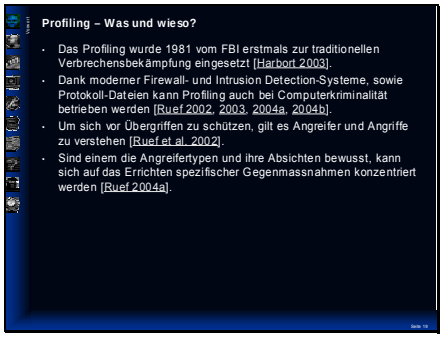
Die Anzahl der vom CERT (http://www.cert.org/) gemeldeten Sicherheitsvorfälle (engl. Incidents) im Internet hat sich ins Unermessliche gesteigert. Seit 2003 wird die Grafik, die auf der Webseite zur Verfügung gestellt wird, auch nicht mehr nachgetragen. Durch die Automatisierung von Angriffen ist es nicht verwunderlich, dass die Anzahl der Übergriffe weiter steigen oder mindestens anhalten wird.

18



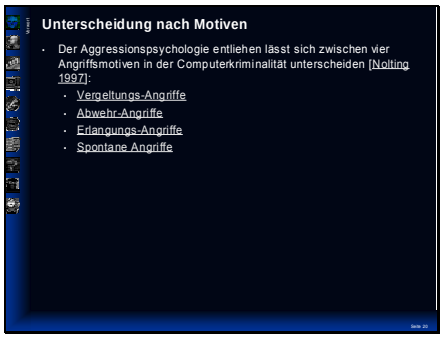
Dem Informatik- und Computerbereich wird gerne vorgeworfen, den Mensch aus den Augen zu verlieren. Wir wollen diesen Fehler nicht begehen und uns deshalb mit den Charakteren beschäftigen, die sich für das Genre begeistern können. Durch Profiling-Techniken, wie ursprünglich vom FBI entwickelt und mittlerweile weltweit von den Polizei-Verbänden eingesetzt werden, wollen wir uns ein klares Bild darüber machen, mit wem wir es überhaupt zu tun haben. Dabei unterscheiden wir nach Motiven, wobei wir uns dabei der aus der Aggressionspsychologie entliehene Klassifizierung und Terminologie bedienen wollen. Desweiteren unterteilen wir die verschiedenen Angreifertypen je nach Motivation, sozialem sowie technischem Hintergrund. Anhand dieser Analysen wird es uns möglich sein zu determinieren, wer überhaupt welchem Risiko ausgesetzt ist. Dies ermöglicht es uns, ein adäquates Mass an Sicherheit anzustreben.

19



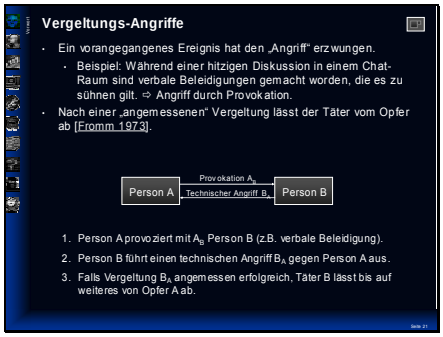
Die Technik des Profilings wurde Anfang der 80er Jahre erstmals vom FBI zur traditionellen Verbrechensbekämpfung eingesetzt. Die Bücher von Stephan Harbort illustrieren dem Laien anhand zahlreicher Beispiele von Serien-Verbrechern sehr schön, weshalb und wie dies umgesetzt wird [Harbort 2003]. Wir wollen uns die dadurch gewonnenen Erkenntnisse zunutze machen, um eine derartige Analyse ebenfalls im Bereich der Computerkriminalität anzuwenden. Moderne Sicherheitssysteme (Firewalls und Intrusion Detection-Systeme) unterstützen uns dabei. So können wir lernen Angreifer zu verstehen und entsprechend ihren Übergriffen entgegenwirken. Wie dies konkret umgesetzt werden kann, ist in zahlreichen Fachartikeln von Marc Ruef in den Jahren 2002 bis 2005 veröffentlicht worden [Ruef 2002, 2003, 2004a, 2004b]. Eine umfassende Darlegung psychologischer Hintergründe steht noch aus, wird aber voraussichtlich 2006/2007 publiziert werden.

20



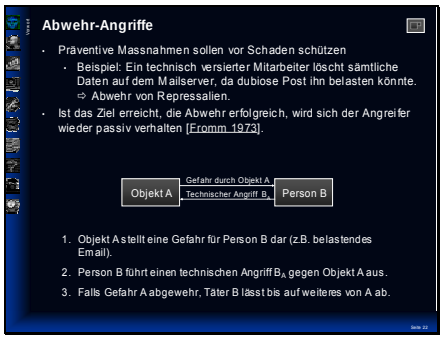
Wir bedienen uns einer klassischen Kategorisierung aus dem Bereich der Aggressionspsychologie, um die Motive im Bereich der Computerkriminalität einteilen zu können. Dabei unterscheiden wir nach Hans-Peter Nolting vier Angriffsvarianten - Vergeltungs-Angriff, Abwehr-Angriff, Erlangungs-Angriff und spontaner Angriff -, die wir im Folgenden genauer betrachten wollen [Nolting 1997].

21



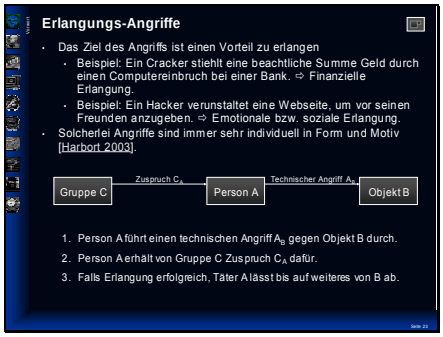
Bei einem Vergeltungs-Angriff hat ein vorangehendes Ereignis den Angriff quasi erzwungen. Beispielsweise hat jemand während einem Gespräch das Gegenüber provoziert (z.B. blossgestellt). Das vorige Opfer wird nun zum Täter und übt Vergeltung durch einen technischen Übergriff [Nolting 1997]. Der Täter lässt in der Regel erst dann vom Opfer ab, wenn er in seinen Augen Gerechtigkeit erfahren hat [Fromm 1973]. Oftmals ist aber eine derartige Motivation der Antrieb für langwierige Fehden.

22



Abwehr-Angriffe weisen die Eigenschaft der Prävention auf. Durch den Angriff soll möglicher Schaden abgewendet werden [Nolting 1997]. Zum Beispiel dann, wenn ein Mitarbeiter eine Email, die er zuvor aus einer hitzigen Entscheidung heraus verschickt hat, unerlaubt aus dem Postfach des Empfängers löscht. Ist das Ziel, also die Abwehr möglicher Repressalien, erreicht, lässt das Täter jeweils wieder ab [Fromm 1973]. Derartige Angriffsmuster werden gerne zur Legitimierung von Delikten herangezogen.

23



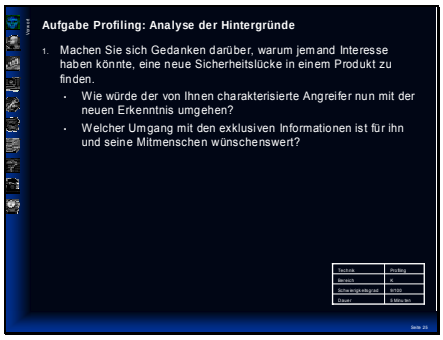
Erlangungs-Angriffe gelten als die populärsten Intentionen. Sie haben ein einziges Ziel, dem Angreifer einen Vorteil zu verschaffen [Nolting 1997]. Dies kann durch das Einholen von Informationen, den Missbrauch von Ressourcen oder das Abzweigen von Geld gegeben sein. Es gilt zu bemerken, dass direkte finanzielle Erlangung gerne als erstes genannt wird, sie aber nur einen verhältnismässig geringen Teil der Motive ausmacht. Emotionale sowie soziale Erlangung (Anerkennung) und mit ihnen Gruppendynamik spielen viel mehr eine Rolle. Entsprechend weist diese Angriffsform ein Höchstmass an Vielschichtigkeit und Komplexität auf. Sie sind in ihrer Form deshalb oftmals sehr verschieden [Harbort 2003].

24



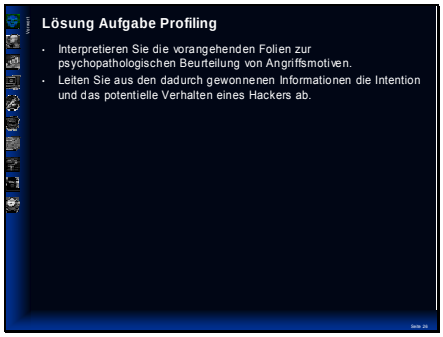
Die letzte Form der Angriffe wird als spontant [Nolting 1997, Harbort 2003] bezeichnet. Die Spontanität ist, meines Erachtens, jedoch eher auf das vermeintliche Fehlen von Gründen für einen Übergriff gekennzeichnet. Ein Beispiel wäre, wenn jemand ohne ersichtlichen Grund eine Webseite verunstaltet.

25



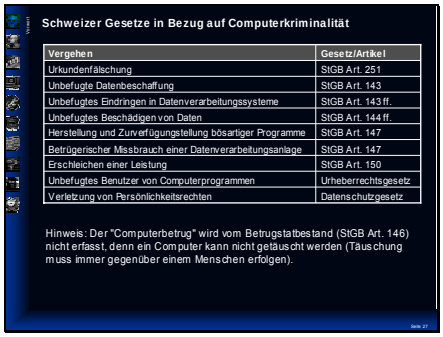
Machen Sie sich Gedanken darüber, warum jemand Interesse haben könnte, eine neue Sicherheitslücke in einem Produkt zu finden. Beantworten Sie danach die folgenden Fragen: Wie würde der von Ihnen charakterisierte Angreifer nun mit der neuen Erkenntnis umgehen? Welcher Umgang mit den exklusiven Informationen ist für ihn und seine Mitmenschen wünschenswert? Die Antwort finden Sie auf der folgenden Folie.

26



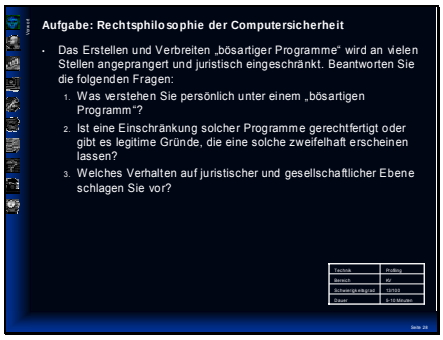
Die Gründe, warum jemand eine Schwachstelle in einem Produkt finden könnte sind vielfältig. Das Heranziehen der psychopathologischen Betrachtungen dieses Kapitels zeigen, dass die Antworten sehr unterschiedlich ausfallen können. Das Finden einer Schwachstelle, um den Hersteller und die Nutzer auf diese hinzuweisen, damit entsprechenden Gegenmassnahmen eingeleitet werden können, ist mit Sicherheit die edelste Vorgehensweise. Warum jemand soetwas macht, ist sehr unterschiedlich. Entweder möchte er sich Anerkennung in gewissen Kreisen einholen: Seine Freunde sollen ihn für sein Engagement bewundern oder er möchte seine Funde in einer Bewerbung erwähnen können.

27



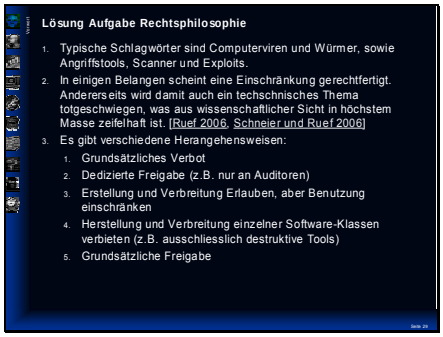
Die Schweizer Gesetzgebung deckt mit dem StGB (Strafgesetzbuch) eine Vielzahl der Computerdelikte ab. In einigen Punkten kommt ebenfalls das Urheber- und das Datenschutzgesetz zum Tragen. Dabei sei der Hinweis angebracht, dass „Computerbetrug“ vom Betrugstatbestand (StGB Art. 146) nicht erfasst wird, denn ein Computer kann nicht getäuscht werden – Eine Täuschung muss immer gegenüber einem Menschen erfolgen.

28



Wie erwähnt, wird das Erstellen und Verbreiten „bösartiger Programme“ wird an vielen Stellen angeprangert und juristisch mit StGB Art. 147 eingeschränkt. Doch was verstehen Sie unter einem „bösartigen Programm“? Ist eine Einschränkung solcher Programme gerechtfertigt oder gibt es legitime Gründe, die eine solche zweifelhaft erscheinen lassen? Welches Verhalten auf juristischer und gesellschaftlicher Ebene schlagen Sie vor?

29

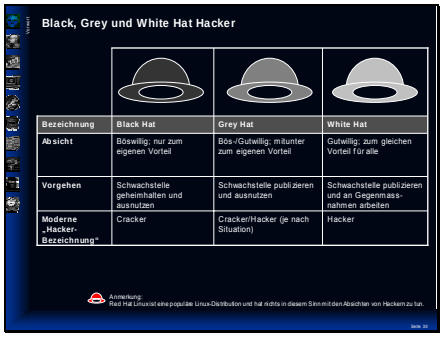


Die Beantwortung der Frage, was denn nun ein bösartiges Programm überhaupt sei, ist sehr schwierig. Unter bösartigen Programmen können in erster Linie Software-Routinen verstanden werden, die einer Sache oder eine Person direkt oder indirekt Schaden zuführen. Ein Computervirus oder –wurm mit offensichtlicher und durschlagender Schadensroutine wäre dem eindeutig zuzuteilen. Gehört aber nun ein Virus, der entwickelt wurde, um einen anderen Virus zu entfernen, ebenfalls zur Klasse der bösartigen Software?

Wie sieht es mit Tools aus, mit denen sich Schwachstellen auffinden und ausnutzen lassen (Securityscanner oder Exploits)? Diese können sowohl für den unerlaubten Einbruch in Systeme genutzt werden – Oder sie lassen sich von Administratoren einsetzen, um schnell und komfortabel etwaige Schwächen ausfindig zu machen und zu beheben. Sie sehen also, dass die „Bösartigkeit“ eines Produkts in erster Linie von seiner Nutzung und dem Anwender abhängt. Der bekannte US-amerikanische Kryptologe und Buchautor Bruce Schneier hat dies ebenfalls in einem Briefwechsel mit Marc Ruef anhand der Beispiele von Telefonen und Autos geäussert [2006]. Es bleibt somit fragwürdig, eine schwer definierbare Gattung von Software pauschal zu verbieten, denn damit entstehen unter Umständen für eine Vielzahl gutartiger Benutzer entscheidende Nachteile.

Es gibt verschiedene alternative Herangehensweisen, wobei sämtliche mit Vor- und Nachteilen behaftet sind. Es scheint, als seien grundsätzlich destruktive Mittel, die sich in keinster Weise für andere Zwecke einsetzen lassen, in der Tat juristisch einzuschränken. Für alle Lösungen im Bereich der Grauzone ist meines Erachtens – und diese Meinung teilen viele Experten - eine liberale Freigabe beizubehalten. Denn wie Schneier sehr schön schreibt, ist eine derartige Limitierung nur sehr selten zum Wohl einer Gemeinschaft.

30

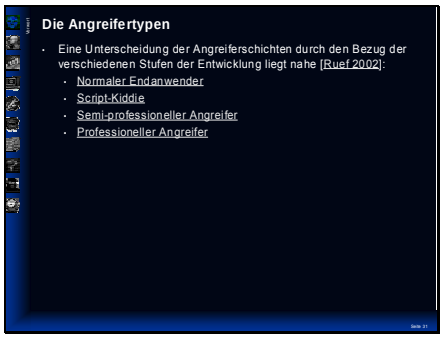


In der Hacker-Szene hat sich über die Jahre eine eigene Klassifizierung für die Vorgehensweise und Absichten eines Hackers entwickelt. So wird in erster Linie zwischen einem Black Hat und einem White Hat unterschieden. Ersterer sucht und missbraucht Schwachstellen zu seinem eigenen Vorteil. Diesen will er so lange wie möglich sein Eigen nennen und hält brisantes Wissen längstmöglich geheim. Gutartige Hacker bezeichnen solche Personen oftmals abschätzig als Cracker.

Mit reiner Weste agieren White Hat Hacker. Diese arbeiten gutwillig und versuchen zum Vorteil für jedermann Probleme offenzulegen. Das Informieren eines Hersteller oder Benutzers über den Sachverhalt ist ihnen mindestens so wichtig wie die Bekanntmachung an der breiten Öffentlichkeit (z.B. durch Advisories oder Fachartikel). Nur so kann gewährleistet werden, dass Schwachstellen schnell gefunden und behoben werden, damit bösartige Cracker (Black Hats) keinen Vorteil erlangen können.

Da die Abgrenzung zwischen Black und White Hat oftmals schwierig ausfällt und nicht immer jeder seiner Linie treu bleibt, gibt es ebenfalls sogenannte Grey Hats. Diese arbeiten manchmal gut-, manchmal böswillig. So kann es sein, dass er eine Schwachstelle findet und zu seinen Gunsten ausnutzt, sofern der Schaden nicht willkürlich und übertrieben ausfällt. Das Bekanntmachen des Problems wird kurze Zeit verzögert, um mit den neuen Möglichkeiten wenigstens ein bisschen „Spass" zu haben. Im Übrigen ist Red Hat Linux (http://www.redhat.com/) eine populäre Linux-Distribution, die nichts in diesem Sinn mit den Absichten von Hackern zu tun hat.

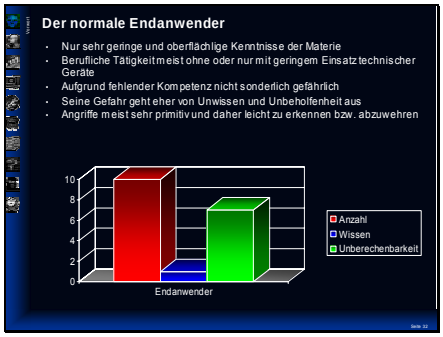
31



Ein Angreifer entwickelt sich im Laufe seiner Karriere. In der Fachliteratur wurden verschiedene Modelle zur Unterteilung der Angreifertypen auf dieser Ebene vorgeschlagen. Sehr umfassend ist da beispielsweise der Vorschlag von Ryan Russell und Stace Cunningham im Buch „Maximum Protection" [2001]. Dort werden in Kapitel 3.1 (deutsche Auflage, 2001, Seiten 31 bis 38) fünf verschiedene Typen unterschieden, die sich jedoch nicht primär anhand ihres Wissens sondern anhand ihrer Intention einteilen lassen.

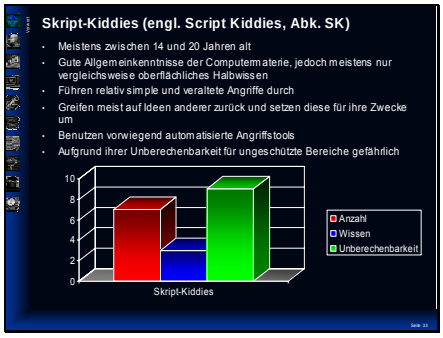
Wir wollen nach [Ruef 2002] eine Unterteilung in vier Typen unternehmen, die sich jeweils nach Wissen, Ausrichtung und Gefahrenpotential voneinander unterscheiden. Im Folgenden werden wir die jeweiligen Typen von Normaler Endanweder, Skript-Kiddie, semi-professioneller und professioneller Angreifer diskutieren. Die Reihenfolge dessen ist im Normalfall die Entwicklung eines einfachen zu einem hochspezialisierten Angreifer. Dieser Ansatz erhebt keinerlei Anspruch auf Vollständigkeit oder absolute Richtigkeit. Er erscheint für unser Vorgehen, der Ermittlung des Risikos und der Ableitung angemessener Gegenmassnahmen, als am sinnvollsten.

32



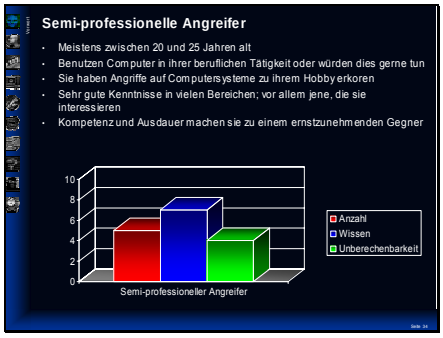
Der am meisten verbreitete Typ ist der normale Endanwender. Er wird von erfahrenen Hackern gerne als DAU (Dümmster Anzunehmender User) abgestempelt. Er weist nur sehr geringe und oberflächige Kenntnisse zu Computern und Sicherheit auf. Das hat oftmals damit zu tun, weil er sich noch nicht intensiv mit der Materie auseinandergesetzt hat. Aus diesem Grund geht er oftmals einer Tätigkeit nach, die nicht oder nur wenig den Einsatz von Computersystemen erfordert. Aufgrund seiner fehlenden technischen Kompetenz geht keine allzu grosse Gefahr von ihm aus. Schäden entstehen höchstens durch dumme Zufälle oder schlicht fehlerhaftes Verhalten des Benutzers. Das Umgehen einfacher Schutzmassnahmen ist ihm nicht möglich, weshalb er auf absolut primitive Angriffstechniken zurückgreifen wird.

33



Entscheidet sich ein normaler Endanwender dazu, sich intensiver für das Thema Computersicherheit zu begeistern, greift er in erster Linie auf altbekannte Techniken zurück, die er möglichst einfach mit dem Heranziehen vorgefertigter Tools umsetzen möchte. Aus diesem Grund werden derartige Angreifer, deren Wissen über allgemeine Kenntnisse noch nicht hinausgeht, als Skript-Kiddies bezeichnet. Ein Titel, der von erfahrenen Hackern und Crackern sehr abschätzig und unter ihresgleichen gar als Beleidigung verwendet wird. Skript-Kiddies sind meistens männlich und zwischen 14 und 20 Jahren alt. Entsprechend gehen Sie oftmals noch zur Schule oder befinden sich in einer Ausbildung. Sie investieren oftmals ein Grossteil ihrer Freizeit für ihren Computer, wobei sie ihn jedoch eher zum Spielen denn für effektives Arbeiten nutzen. Aufgrund ihrer Unberechenbarkeit und den oftmals fehlenden ethischen Grundsätzen sind sie besonders für ungeschützte oder schlecht geschützte Bereiche gefährlich.

34



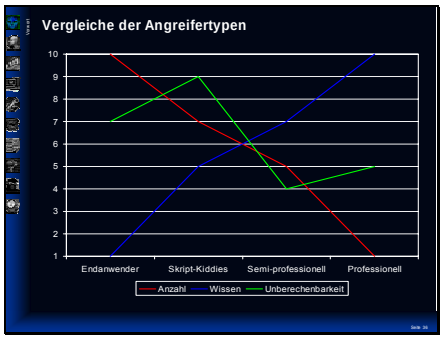
Die Weiterentwicklung eines Skript-Kiddies ist im semi-professionellen Angreifer gegeben. Dieser interessiert sich meistens schon länger und intensiver für den Computer, weshalb er wenigstens auf gewissen Bereichen ein solides Wissen zusammentragen konnte. Die meist zwischen 20 und 25 Jahren alten männlichen Personen sind vorwiegend im universitären Umfeld zu finden. Sie haben das Programmieren und Angreifen von Computersystemen zu ihrem Hobby gemacht und verfolgen dies mit entsprechender Leidenschaft. Ihre Kompetenz und Ausdauer machen sie zu einem ernstzunehmenden Gegner, der durch sein partielles Fachwissen durchaus grössere Schutzvorkehrungen umgehen kann.

35



Die Perfektion von Angriffen auf Computersystemen ist nur einer sehr kleinen Elite überlassen. Das Zusammentragen des Wissens erfordert sehr viel Zeit, weshalb die meisten von ihnen aus beruflichen Gründen mit der Materie zu tun haben. Viele ehemalige Hacker werden von Sicherheitsfirmen angestellt und arbeiten dort als Security Consultants oder Penetration Tester. Sie sind in der Lage spezialisierte und optimierte Angriffe umzusetzen, deren Techniken sie in manchen Fällen gar selber entwickelt oder wenigstens verbessert haben. Ihr zielsicheres und souveränes Vorgehen ermöglicht ihnen durchschlagskräftige, schwer erkennbare und abwehrbare Attacken. Deshalb ist ein sehr hohes Mass an Sicherheit erforderlich, um den Erfolg von Übergriffen dieses Angreifertyps möglichst (lange) zu verhindern.

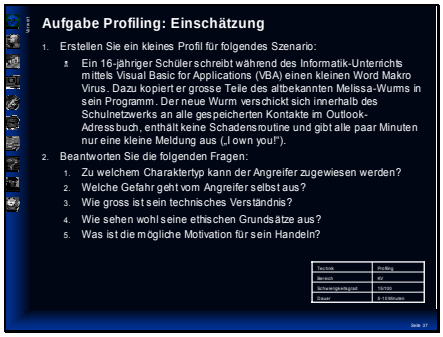
36



Der Vergleich der Attribute der diskutierten Angreifertypen zeigt sehr schön die jeweilige Entwicklung des Einzelnen auf. So offenbart sich, dass spezialisiertes Wissen erst in einer späten Phase angehäuft werden kann. Nur die wenigsten Angreifer weisen ein solch festes Interesse auf, dass sie sich bis zum professionellen Angreifer entwickeln können. Ein mehrjähriges Studium der Materie ist erforderlich, um vom herkömmlichen Endanwender zum professionellen Angreifer zu werden. Die Vielzahl der Angreifer kommt eben nicht über das Stadium eines Skript-Kiddies heraus.

Interessant zu sehen ist ebenfalls, dass die Unberechenbarkeit die einzige Eigenschaft ist, die sich nicht konstant entwickelt. Skript-Kiddies mit ihrem Halbwissen gelten als viel unberechenbarer weder normale Endanwender. Wiederum gelten professionelle Angreifer aufgrund der Vielzahl der durch sie verfolgbaren Techniken als unberechenbarer weder semi-professionelle Angreifer.

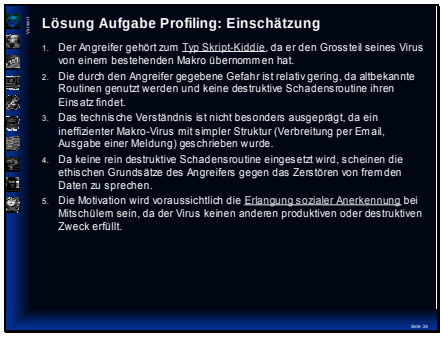
37



Befassen Sie sich nun mit dieser Aufgabe, in der eine kleine Fallstudie eines Profilings vorgetragen wird: Ein 16-jähriger Schüler schreibt während des Informatik-Unterrichts mittels Visual Basic for Applications (VBA) einen kleinen Word Makro Virus. Dazu kopiert er grosse Teile des altbekannten Melissa-Wurms in sein Programm. Der neue Wurm verschickt sich innerhalb des Schulnetzwerks an alle gespeicherten Kontakte im Outlook-Adressbuch, enthält keine Schadensroutine und gibt alle paar Minuten nur eine kleine Meldung aus („I own you!").

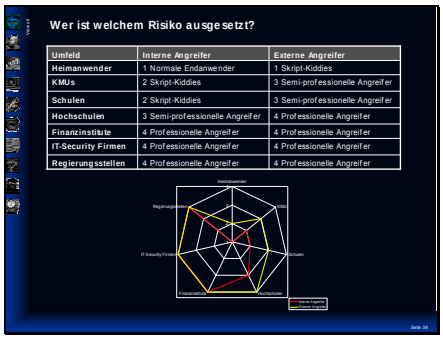
Beantworten Sie die folgenden Fragen: Zu welchem Charaktertyp kann der Angreifer zugewiesen werden? Welche Gefahr geht vom Angreifer selbst aus? Wie gross ist sein technisches Verständnis? Wie sehen wohl seine ethischen Grundsätze aus? Was ist die mögliche Motivation für sein Handeln?

38



Der Angreifer gehört zum Typ Skript-Kiddie, da er den Grossteil seines Virus von einem bestehenden Makro übernommen hat. Die durch den Angreifer gegebene Gefahr ist relativ gering, da altbekannte Routinen genutzt werden und keine destruktive Schadensroutine ihren Einsatz findet. Das technische Verständnis ist nicht besonders ausgeprägt, da ein ineffizienter Makro-Virus mit simpler Struktur (Verbreitung per Email, Ausgabe einer Meldung) geschrieben wurde. Da keine rein destruktive Schadensroutine eingesetzt wird, scheinen die ethischen Grundsätze des Angreifers gegen das Zerstören von fremden Daten zu stehen. Die Motivation wird voraussichtlich die Erlangung sozialer Anerkennung bei Mitschülern sein (emotionaler/sozialer Erlangungs-Angriff), da der Virus keinen anderen produktiven oder destruktiven Zweck erfüllt.

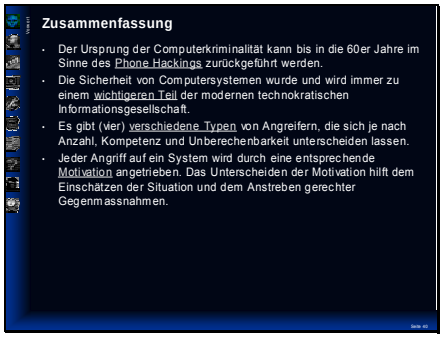
39



Anhand der vorher determinierten Kompetenz und Verbreitung der jeweiligen Angreifertypen können wir nun verschiedene Risikokategorien darlegen. Dabei unterscheiden wir grob zwischen internen und externen Angreifern. Erstere befinden sich in der Regel im internen Netzwerk. Sie geniessen erweitertes Wissen über die Umgebung und ein Mehr an Privilegien. Damit gelten sie als authentisierte oder wenigstens legitime Benutzer. Externe Angreifer sind Personen, die sich ausserhalb des Perimeters befinden. Meistens sind dies Leute aus dem Internet, ohne irgendwelche zusätzlichen Zugangsberechtigungen.

Wie wir sehen können, unterscheidet sich das Sicherheitsrisiko eines Heimanwenders erheblich von dem eines Finanzinstituts. Es ist deshalb nicht verwunderlich, dass schon von diesem Gesichtspunkt aus die jeweiligen Stellen das Thema Computersicherheit ganz anders adressieren. Es macht eben wenig Sinn, dass ein Privatwender genauso sFr. 100'000 für eine hochleistungsfähige Firewall-Lösung wie eine Grossbank investiert. Das Erreichen eines annehmbaren Stands an Sicherheit ist für beide Parteien mit ganz anderen Voraussetzungen zu versuchen.

40



Der Ursprung der Computerkriminalität kann bis in die 60er Jahre im Sinne des Phone Hackings zurückgeführt werden. Die Sicherheit von Computersystemen wurde und wird immer zu einem wichtigeren Teil der modernen technokratischen Informationsgesellschaft. Man kann dabei zwischen (vier) verschiedenen Typen von Angreifern, die sich je nach Anzahl, Kompetenz und Unberechenbarkeit unterscheiden, differenzieren. Jeder Angriff auf ein System wird durch eine entsprechende Motivation angetrieben. Das Unterscheiden der Motivation hilft dabei dem Einschätzen der Situation und dem Anstreben gerechter Gegenmassnahmen.

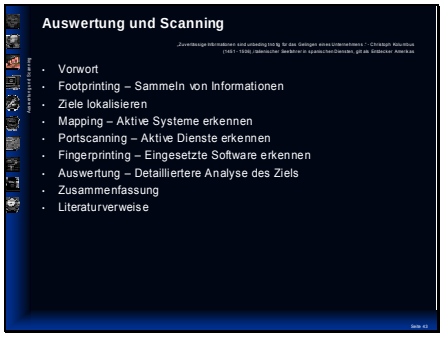
41



42

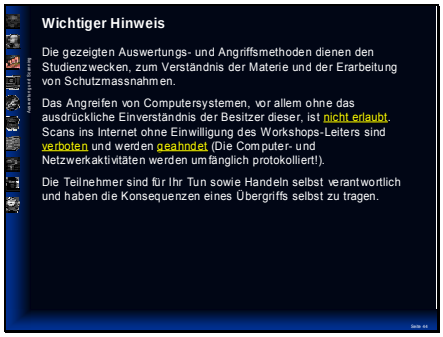


43



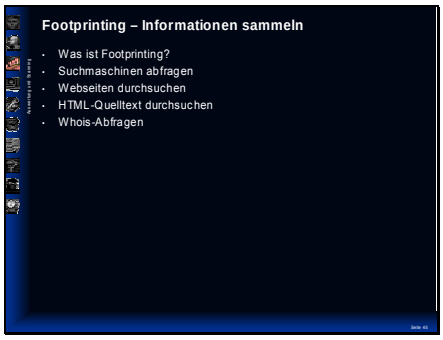
Mit dem Kapitel Auswertung und Scanning wollen wir erste technische Gehversuche unternehmen. Dabei wollen wir das typische Vorgehen eines Angreifers nachahmen. Durch das Footprinting sammeln wir erste Informationen über eine Zielumgebung. Haben wir ein Objekt technisch lokalisiert, werden wir versuchen anhand des Mappings dessen effektive Existenz und Erreichbarkeit zu determinieren. Danach wenden wir die traditionelle Technik des Portscannings an, um die aktiven Dienste des Zielsystems und damit seine potentielle Angriffsfläche ausmachen zu können. Mit verschiedenen Fingerprinting-Techniken versuchen wir sodann herauszufinden, welche Software auf dem Zielsystem eingesetzt wird. Nur mit dem Wissen um das genutzte Betriebssystem und die eingesetzten Software-Komponenten können wir effiziente Angriffe initiieren. Durch die erweiterte Auswertung werden wir weitere Details zusammentragen, die uns das Umsetzen der Attacken vereinfachen können.

44



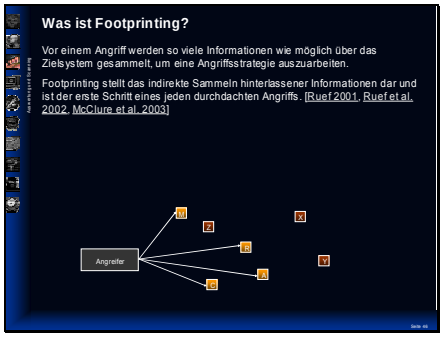
Hierbei handelt es sich um die mitunter wichtigste Folie der gesamten Vorlesung. Bitte halten Sie sich an die Vorgaben des Dozenten. Probleme jeglicher Art, die durch die missbräuchliche Nutzung des Wissens und der Ressourcen resultieren, sind nicht auf den Lehrgang oder den Dozenten zurückzuführen. Jeder Student ist für sein Tun selber verantwortlich, hat sich den Konsequenzen seines Handelns selber zu stellen. Die für die Recherchen und die Übungen bereitgestellte Infrastruktur wird technisch Überwacht, weshalb ohne Probleme Rückschlüsse auf Missbrauch und dessen Verursacher gemacht werden können.

45



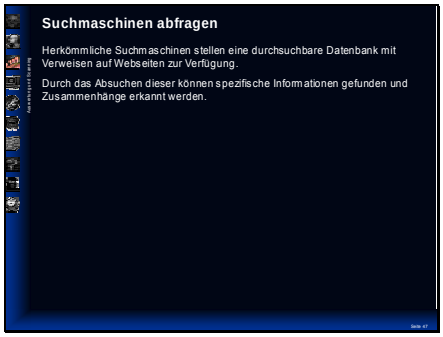
Durch das Footprinting wird ein erstes Zusammentragen von Informationen zu einem Ziel getätigt. Der Name ist dem Jäger-Jargon entliehen, bei welchem durch das Auslesen der Fussspuren das Wild aufgestöbert wird. Wir werden einige der einfacheren und populären Footprinting-Techniken diskutieren und für das bessere Verständnis dieser sie durchspielen. Dazu zählt vor allem das Durchsuchen von Suchmaschinen und Webseiten zum Auffinden von möglichst vielen sensitiven Informationen. Einen Blick in den HTML-Quelltext einer Webseite verrät dabei oftmals noch viel mehr. Und zum Schluss wollen wir uns mit dem whois-Dienst auseinandersetzen, der wiederum ein Mehr an Informationen zu einem Ziel bereitstellen kann.

46



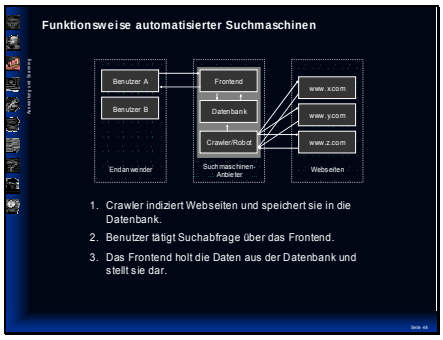
Vor einem Angriff werden so viele Informationen wie möglich über das Zielsystem gesammelt, um eine Angriffsstrategie auszuarbeiten. Footprinting stellt das indirekte Sammeln hinterlassener Informationen dar und ist der erste Schritt eines jeden durchdachten Angriffs. Der Begriff ist dem Jäger-Jargon entliehen, bei welchem durch das Auslesen der Fussspuren das Wild aufgestöbert wird. Eine umfassende Erläuterung zur strategischen Vorgehensweise wurde erstmals umfassend in den Büchern „Hackers Guide“, „Das Anti-Hacker Buch“ [McClure et al. 2003], „Die Sicherheit von Windows“ [Ruef 2001] und „Hacking Intern“ [Ruef et al. 2002] vorgetragen.

47



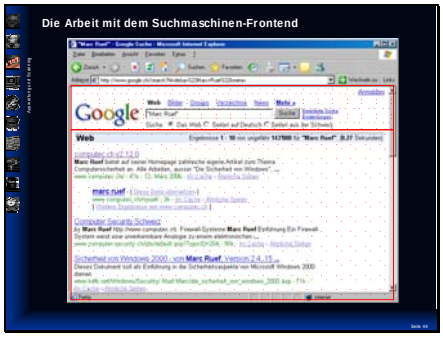
Eine der klassischen Methoden des Footprintings zieht Suchmaschinen heran. Traditionelle Index-Suchmaschinen durchsuchen eine Webseite und speichern die Daten dieser in eine Datenbank. Durch Suchabfragen lässt sich der Datenraum dieser Seiten durchsuchen und so effizient die gewünschte Information finden. Angreifer benutzen diese Technik ebenso, um sensitive und für Angriffe verwertbare Informationen zu finden.

48



Automatisierte Index-Suchmaschinen benutzen sogenannte Crawler, Robots oder Spider. Das sind Agenten, die wie Clients funktionieren und auf einzelne Webseiten zugreifen. Die vom Webserver zurückgeschickten Informationen werden sodann durch den Crawler in die Datenbank gespeichert und damit indiziert. Ein Benutzer kann nun durch ein Frontend diese Datenbank nach bestimmten Mustern durchsuchen. In der Regel findet eine Volltext-Suche auf den Inhalt der indizierten Daten (z.B. Datei-Inhalt, Seiten-Titel, URL, Meta-Informationen) statt. Wird eine Übereinstimmung gefunden (engl. Match), wird das Resultat ausgegeben. Bei populären Suchmaschinen wird dabei der Seitentitel, eine kurze Beschreibung oder der Auszug des Dateiinhalts sowie ein Link auf die Ressource dargeboten. Der Benutzer weiss so, wo sich die von ihm gesuchten Informationen befinden und kann anhand der Sichtung der Links die eigentlichen Daten zusammentragen.

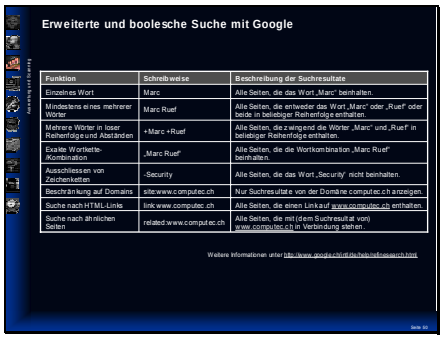
49



Es gibt eine Vielzahl an verschiedenen Suchmaschinen. Ursprünglich galt Altavista (http://www.altavista.com/) als die umfassendste Index-Suchmaschine. Dieser Titel wurde im jüngsten Millenium durch das Angebot von Google (http://www.google.com/) übernommen - die Firma wurde am 7. September 1998 von Larry Page und Sergey Brin gegründet -, dessen Index-Suchmaschine einen Grossteil des öffentlichen World Wide Webs abdeckt. Durch ein einfaches und schlichtes Frontend lassen sich intuitive und komplexe Abfragen erstellen, dessen Resultate als Links samt kurzer Übersicht dargestellt werden.

In diesem Beispiel wird eine einfache Suchabfrage für den String „Marc Ruef“ umgesetzt. Wie zu sehen ist, sind innert 0,27 Sekunden ungefähr 143‘000 Resultate für die besagte Eingabe zusammengetragen worden. Die Sortierung der Resultate erfolgt dabei der Wichtigkeit der einzelnen Treffer (engl. Hits). Dabei kommt der sogenannte PageRank-Algorithmus zum Einsatz, der nach seinem Erfinder Lawrence Page benannt wurde. Je mehr Links auf eine Seite verweisen, umso wichtiger ist sie. Je wichtiger wiederum die verweisenden Seiten sind, desto grösser ist der Effekt. Die Bewertung einer Ressource reicht dabei von 0 bis 10, wobei der Wert 10 für besonders populäre Angebote steht. Der PageRank-Algorithmus versucht dabei einen zufällig durch das Netz surfenden Benutzer, der auf der Suche nach möglichst soliden Quellen ist, nachzubilden.

50



Viele moderne Suchmaschinen unterstützen erweiterte Suchabfragen, bei denen vorzugsweise boolesche Logik zum Einsatz kommt. So ist wohl jedem Benutzer die einfache Suche mit einem einzelnen Wort wie „Marc“ bekannt. Werden die beiden Worte „Marc“ und „Ruef“ lose eingegeben, werden in erster Linie Webseiten angezeigt, die beide Worte in beliebiger Reihenfolge enthalten. Aber auch Ressourcen werden vorgetragen, die nur einen der Begriffe aufweisen.

Will man nun nur Treffer anzeigen lassen, die beide Worte enthalten, muss man sich des speziellen Operators + (Additions-Zeichen) bedienen. Wird dieses einem Wort vorangestellt, lässt sich eine logische Und-Verknüpfung erstellen. Die Eingabe von „+Marc +Ruef“ führt nun dazu, dass nur Seiten angezeigt werden, die beide Worte ausweisen können. Die Reihenfolge der Treffer der einzelnen mit Und verknüpften Zeichenketten im Dokument ist dabei irrelevant. Eine weitere Verknüpfung der Begriffe lässt sich mit dem doppelten Anführungszeichen umsetzen. Werden mehrere Worte in solche eingeschlossen, gilt die Eingabe als autonome Zeichenkette. Es werden sodann nur Treffer angezeigt, die genau diesen String enthalten.

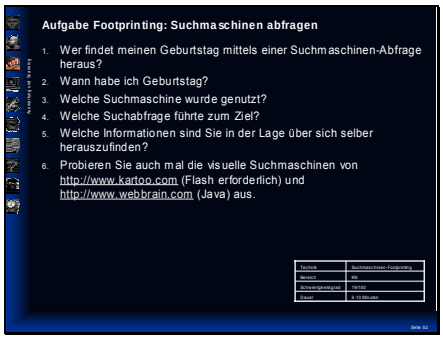
Es gibt noch eine Vielzahl anderer Operatoren und Features, die sich je nach Suchmaschine unterscheiden können. Google weist hierbei einige wirklich nützliche Funktionen auf, mit denen sich äusserst effizient das World Wide Web durchsuchen lässt. Mehr Informationen finden sich auf den Hilfe-Seiten von Google selbst.

51



Es gibt eine Vielzahl an verschiedenen Suchmaschinen, die komplett anders funktionieren, different strukturiert sind und die Resultate unterschiedlich darstellen. Eine Index-Suchmaschine wie die populäre von Google kommt relativ schlicht daher und zeigt eine sequentielle Auflistung der Suchtreffer. Anders arbeitet hier kartoo.com, eine erweiterte Index-Suchmaschine, die die Daten in Form einer Karte illustriert. Damit werden Verknüpfungen der Resultate visuell sichtbar und können damit auf einen Blick besser verarbeitet werden.

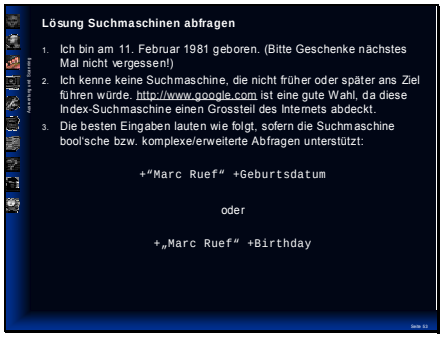
52



Gehen wir nun ungezwungen an eine erste Übung im Umgang mit Suchmaschinen heran. Da ich davon ausgehe, dass Sie schon einmal auf den Dienst einer Suchmaschine wie Google zurückgegriffen haben, werden Sie die folgenden Fragen sicher ohne grössere Mühe beantworten können. Es steht Ihnen dabei frei, welche Suchmaschine Sie in welcher Form benutzen wollen. Nennen Sie mir mit der Hilfe einer Suchabfrage mein Geburtsdatum. Welche Suchmaschine haben Sie für das Erfüllen dieser Aufgabe herangezogen und welche Eingabe führte Sie zu Ihrem Ziel?

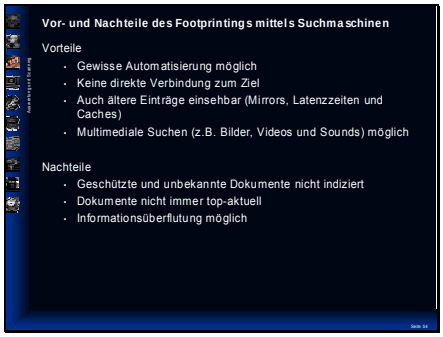
Solange Ihre Mitstudenten mit der Umsetzung dieser Aufgabe noch nicht fertig sind, können Sie mal schauen, welche Informationen Sie über sich mit der Hilfe einer Suchmaschine zusammentragen können. Der Eingabe Ihres Namens oder Ihrer Mailadresse wird vielleicht die eine oder andere Überraschung zu Tage fördern. Vor allem wenn Sie sich schon längere Zeit aktiv im Internet bewegen, ist die Chance besonders gross, dass Sie in einer populären Suchmaschine gelistet sind. Versuchen Sie auch mal die visuellen Suchmaschinen unter http://www.kartoo.com/ und http://www.webbrain.com/ zu bedienen.

53



Wie Sie sicher herausgefunden haben, bin ich am 11. Februar 1981 (Wassermann) geboren. Es gibt wohl keine etablierte Suchmaschine, die nicht früher oder später diese Information bereitstellen kann. Allen voran Google (http://www.google.com/), das alleine bei der Eingabe meines Namens rund 171‘000 Resultate zu liefern in der Lage ist. Typische Eingaben zur Bewältigung der Aufgabe sind „+Marc +Ruef +Geburtsdatum“ oder „+Marc +Ruef +Birthday“. Aber auch durch das einfache Heranziehen meines Vor- und Nachnamens lässt sich über kleinere Umwege auf meine private Webseite (http://www.computec.ch/mruef/), damit auf meinen Lebenslauf und entsprechend das Geburtsdatum schliessen.

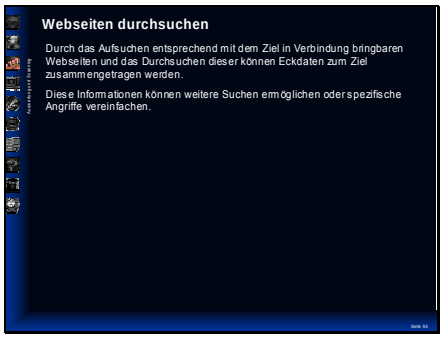
54



Das Footprinting mittels Suchmaschinen hat entscheidende Vorteile. So geschehen derartige Suchabfragen in der Regel ohne direkten Zugriff auf Systeme der Zielumgebung. Dem eigentlichen Ziel ist es entsprechend praktisch nicht möglich, während einer solch frühen Auswertungsphase das Voranschreiten eines Angriffs überhaupt auch nur ansatzweise zu erkennen. Desweiteren können derartige Footprinting-Zugriffe sehr gut automatisiert werden. Mittels simplen Skripten lassen sich so innert Minuten Namen, Mailadressen und Telefonnummern von Zielumgebungen zusammentragen. Dank Mirror- und Cache-Funktionen einiger Suchmaschinen (auch Google) können teilweise auch schon wieder vom Netz genommene Informationen durchsucht werden. Mittels multimedialen Suchen lassen sich teilweise gar Portrait-Fotos von Zielpersonen oder Videos auftreiben. Eine hervorragende Voraussetzung für Angriffe auf psychologischer Ebene (z.B. Social Engineering mittels Phishing).

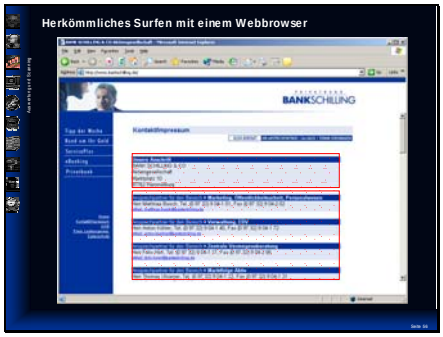
Die Nachteile von Suchmaschinen sind grundsätzlich in ihren technischen Limitierungen gegeben. So kann eine Suchmaschine nur jene Dokumente indizieren, auf die sie auch Lesezugriff ausüben kann. Geschützte und unbekannte Dokumente finden sich also nicht in den Datenbanken der Suchmaschinen-Betreiber. Da der Prozess des Crawlings sehr zeit- und ressourcen-intensiv ist, wird er zyklisch wiederholt. So kann es vorkommen, dass die von einer Suchmaschine bereitgestellten Daten nicht immer auf dem neuesten Stand sind. Desweiteren ist die Überflutung durch eine Vielzahl an Informationen denkbar. Für einen Angreifer kann es bei im Internet besonders aktiven Zielen sehr schwierig sein, die wichtigsten Informationen aus der hohen Anzahl der Daten zu extrahieren. Viel Zeit und Erfahrung sind dafür oftmals von Nöten.

55



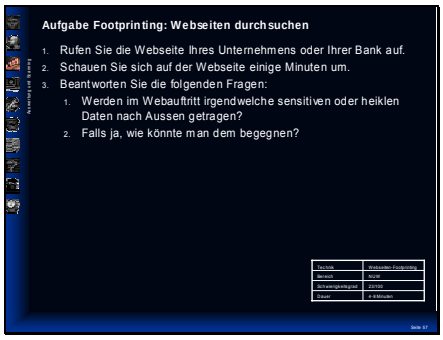
Ist der Name einer Webseite zur Zielumgebung bekannt (z.B. aufgrund der Suche mittels einer Suchmaschine) kann ein erster Zugriff auf diese umgesetzt werden. So lässt sich mit einem unauffälligen Zugriff, der sich nicht von demjenigen eines normalen Benutzers unterscheiden lässt, eine direkte Informationssammlung weiterführen. Während des Durchstöberns des Webangebots kann man als Angreifer versuchen ein Gefühl für die Zielumgebung sowie die Philosophie der Mitarbeiter zu bekommen. Diese Information kann für weitere Auswertungen und Angriffe, diese nicht nur psychologischer Natur, sehr nützlich sein.

56



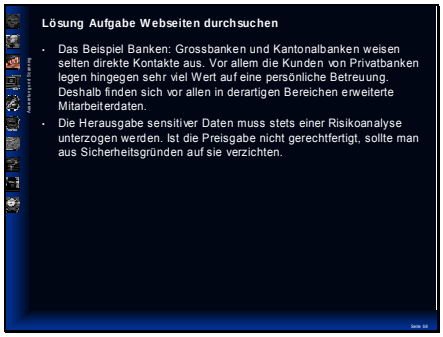
Dieses Beispiel einer ausländischen Privatbank zeigt, dass sich auf Webseiten oftmals Adressen, Namen, Mailadressen und Telefonnummern von Angestellten bereitgestellt werden. Diese lassen sich für weitere Auswertungen (z.B. zusätzliche Suchmaschinen-Abfragen oder Wardialing) oder direkte Angriffe (z.B. Social Engineering mittels Phishing) einsetzen.

57



Schauen Sie sich als Übung die Webseite Ihrer Bank oder Ihres Arbeitgebers an. Nehmen Sie sich ruhig Zeit, sich durch die einzelnen Bereiche der Webseite zu klicken. Beantworten Sie daraufhin die Frage, ob im besagten Web-Angebot ebenfalls irgendwelche sensitiven Informationen zusammengetragen werden. Machen Sie sich desweiteren Gedanken darüber, wie man diesem Problem der freizügigen Informationspreisgabe entgegnen könnte, ohne irgendwelche anderen Nachteile in Kauf nehmen zu müssen.

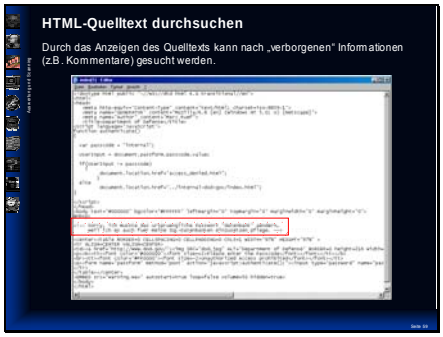
58



Das Beispiel Banken: Grossbanken und Kantonalbanken weisen selten direkte Kontakte aus. Vor allem die Kunden von Privatbanken legen hingegen sehr viel Wert auf eine persönliche Betreuung. Deshalb finden sich vor allen in derartigen Bereichen erweiterte Mitarbeiterdaten.

Die Herausgabe sensitiver Daten muss stets einer Risikoanalyse unterzogen werden. Ist die Preisgabe nicht gerechtfertigt, sollte man aus Sicherheitsgründen auf sie verzichten.

59

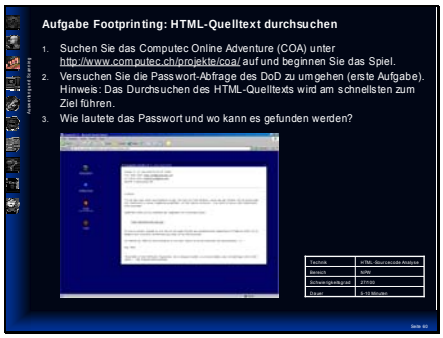


Beim Betreten einer Webseite mit einem Webbrowser wird eine interpretierte Fassung des Web-Dokuments, in der Regel ist dies HTML, dargestellt. Der Webbrowser parst dabei die durch die Seitenbeschreibungssprache bereitgestellten Anweisungen, weshalb eine erweiterte Formatierung erst möglich wird (z.B. fette Schrift oder das Einbinden von Bildern). Ein Benutzer sieht somit nur das, was für ihn wichtig ist.

Die Struktur von HTML lässt jedoch oftmals weitere Rückschlüsse auf eine Zielumgebung zu. So können Kommentare beispielsweise zusätzliche Hintergrundinformationen zu einem Webauftritt bereithalten. Der Vermerk von Passwörtern oder anderweitigen Zugriffsinformationen ist nicht selten gesehen. Im obigen Beispiel wird ein solcher Kommentar, der sich auf die Vergabe des Passworts einer SQL-Datenbank bezieht, dargestellt.

Die Anzeige des Quelltexts kann in den meisten Webbrowsern umgesetzt werden. Der Microsoft Internet Explorer stellt dieses Feature mit der Hilfe von notepad.exe zur Verfügung. Die Anzeige des Quelltexts kann dabei durch den Menü-Punkt „View" und den Eintrag „Source" umgesetzt werden. Bei Mozilla Firefox ist dies ähnlich über den Menü-Punkt „View" und danach den Eintrag „Page Source" möglich.

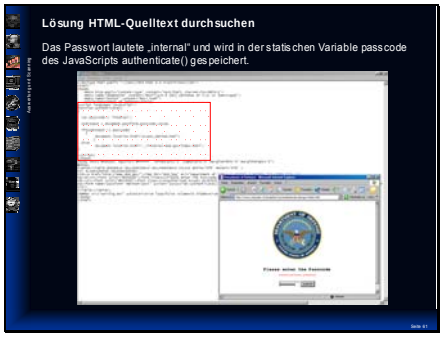
60



Wir wollen nun innerhalb eines praktischen Beispiels illustrieren, wie mächtig diese simple Analysemöglichkeit moderner Webbrowser sein kann. Gehen Sie dazu auf die URL http://www.computec.ch/projekte/coa/ . Dort finden Sie das Online-Spiel Computec Online Adventure (COA). Starten Sie das Spiel und schlüpfen Sie in die Rolle des Hackers Ethan Hunt, der in fiktive Computersysteme eindringen will.

Eine der ersten Aufgaben besteht darin, in ein System des Department of Defense (DoD) einzubrechen. Nach dem Klicken des Links im Email wird die Authentisierungs-Seite der Regierungsbehörde angezeigt. Versuchen Sie mit der Hilfe der Analyse des HTML-Quelltexts das Passwort herauszufinden und dank diesem die Authentisierung erfolgreich umzusetzen. Lassen Sie beispielsweise im Microsoft Internet Explorer durch View/Source die entsprechende Datei laden. Wie lautet das Passwort für den Zugriff und wo kann es genau gefunden werden?

61



Die Authentisierung der Webseite des Department of Defense ist client-seitig umgesetzt und JavaScript-basierend. Dies bedeutet, dass man mit der Einsicht des HTML-Quelltexts die Funktionsweise des Authentisierungs-Mechanismus‘ analysieren kann. Der Quelltext lässt sich in den meisten Browsern durch eine Funktion im Sinne von View/Sourcecode anzeigen.

Wie sodann im entsprechenden JavaScript nachzusehen ist, wird dabei ein statisches Passwort in der Variable passcode definiert. Diess lautet „internal“ und wird beim Versuch einer Authentisierung innerhalb der Funktion authenticate() durch die Eingabe des Benutzers verglichen. Lautet die in der Variable userinput abgelegte Eingabe des Benutzers gleich wie der Inhalt der Variable passcode (also die Zeichenkette „internal“), wird der Zugang gewährt. Andernfalls wird eine Seite samt Fehlermeldung geladen.

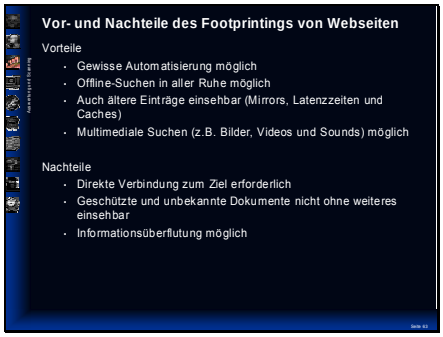
62



Einige der Index-Suchmaschinen stellen Cache-Versionen ihrer Datenbank-Einträge zur Verfügung. Dies macht es möglich, dass man auch auf frühere Versionen eines Web-Dokuments zugreifen kann.

Unter http://web.archive.org wird ein Projekt bereitgestellt, das sich auf das Archivieren von Web-Dokumenten spezialisiert hat. So wird es möglich, dass man auf alte Versionen von Webseiten zugreifen kann. In einzelnen Fällen lassen sich so historische Deltas der Informationsfreigabe eruieren, was wiederum für weitere Auswertungen und Angriffe nützlich sein kann.

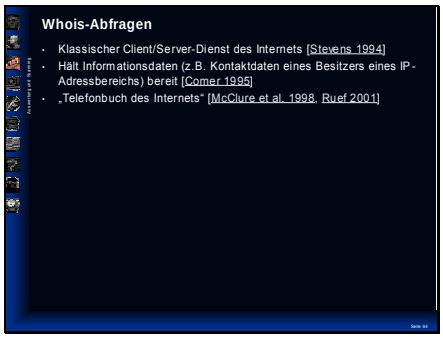
63



Das Footprinting von Webseiten weist wiederum angenehme Vorteile auf. So lassen sich mittels Offline-Browsern lokale Kopien von Webseiten erstellen. Die akribische Suche kann so dann in aller Ruhe und ohne die Möglichkeit einer Entdeckung umgesetzt werden. Automatisierung mittels Skripten und regulären Ausdrücken lässt sich ebenso effizient inszenieren. Durch die Cache- und Mirroring-Funktionen verschiedener Suchmaschinen und Projekte lassen sich auch Suchen „in der Vergangenheit“ anstellen. Ebenso wird durch das Medium Internet eine multimediale Suche möglich, die wiederum vor allem in Bezug auf psychologische Übergriffe von Nutzen sein kann.

Ein entscheidender Nachteil des Footprintings einer Webseite ist, dass der Angreifer eine direkte Verbindung mit dem Zielsystem herstellen muss. Dies eröffnet theoretisch das Risiko, dass der Angreifer und sein Vorgehen identifiziert werden kann. Sollte sich der Angreifer jedoch ganz normal auf der Webseite bewegen, ist sein Verhalten nur sehr schwer von dem eines herkömmlichen Besuchers zu unterscheiden. Zudem lassen sich mittels Zweitanschlüssen, Proxies und WLAN-Hijacking die Herkunft verschleiern. Wiederum wird der Angreifer jedoch nur auf öffentlich zugängliche Informationen zugreifen können. Nicht bekannte und geschützte Bereiche bleiben einer Einsicht vorbehalten. Desweiteren kann auch hier der Fall eintreten, dass sich der Angreifer mit einer wahren Informationsflut herumschlagen muss. Dies ist besonders bei umfassenden Web-Auftritten der Fall.

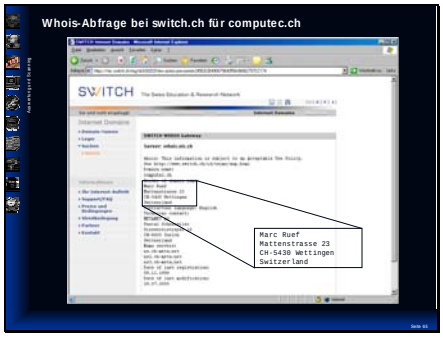
64



Whois ist ein klassischer Dienst des Internets. Er hält Informationen zu Besitzern und Verwaltern von Internet-Ressourcen (IP-Adressen und Domains) bereit und gilt somit als das Telefonbuch des Internets. Viele Registratoren und Verwalter stellen einen Zugriff auf diesen Dienst bereit, um entsprechende Nachforschungen anstellen zu können. Beispielsweise dann, wenn eine Fehlfunktion in einem System ausgemacht werden konnte (z.B. Wiederholter Versand von Emails) und der Betreuer dessen über das Problem informiert werden will. [Stevens 1994, Comer 1995]

Wie auch schon in den anderen Diskussionen zum Thema Footprinting können derartige Informationen für eine weitere Auswertung oder einen Angriff relevant sein. Wir wollen deshalb im folgenden diskutieren, welches Gefahrenpotential von whois ausgeht und wie sich ein Angreifer durch einen derartigen Dienst einen Vorteil verschaffen will.

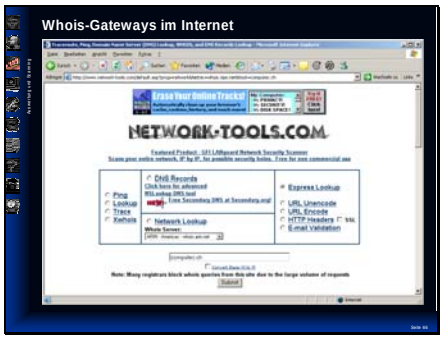
65



Für die Registration von Domains mit der Top-Level-Domain .ch (Schweiz) und .li (Liechtenstein) zeichnet sich SWITCH (The Swiss Education & Research Network) verantwortlich. Auf der Webseite http://www.switch.ch/ lassen sich auch entsprechende whois-Abfragen mittels komfortablem Web-Frontend umsetzen.

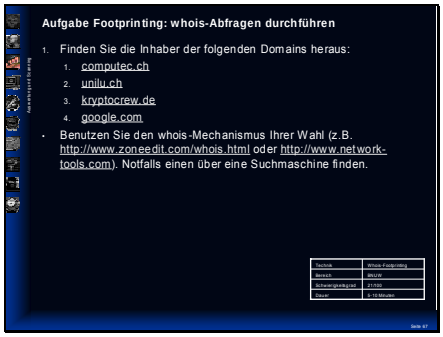
In diesem Beispiel wurde eine Abfrage für die Domain computec.ch initiiert. Der Besitzer dieser wird samt Name und Anschrift ausgewiesen. Desweiteren finden sich Kontaktdetails zur technischen Wartung zuständigen Person. Ebenfalls ist hierbei die Anschrift des Technical Contact abgedruckt. Desweiteren finden sich Hinweise auf die Nameserver sowie Daten zur Registration und Anpassung des Datensatzes.

66



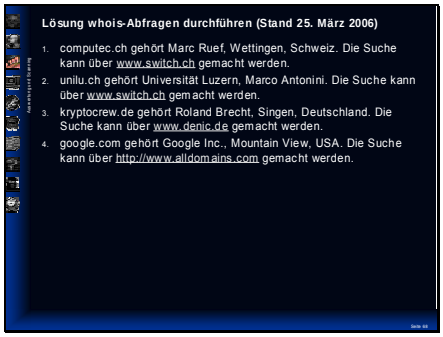
Im Internet finden sich eine Vielzahl an Gateways, mit denen sich derartige Abfragen sehr einfach und effizient umsetzen lassen. Die Anbieter dieser freien Angebote sind dabei oftmals darum bemüht, dass durch gewisse Logiken automatisch die richtigen Informationen zusammengetragen werden.

67



Versuchen Sie nun ein Footprinting mittels whois-Abfragen für die oben genannten Domains umzusetzen. Identifizieren Sie dabei die Besitzer der besagten Ressourcen. Benutzen Sie den whois-Mechanismus Ihrer Wahl (z.B. http://www.zoneedit.com/whois.html oder http://www.network-tools.com/). Versuchen Sie notfalls einen über eine Suchmaschine zu finden.

68



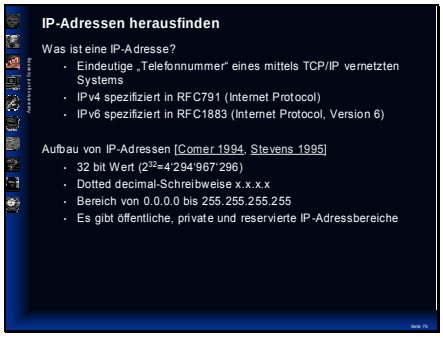
Die jeweiligen Lösungen sind in der Folie selbst ersichtlich. Ebenso die Nennung des Dienstes, mit dem das Resultat umgesetzt werden kann. Alternative Lösungswege über andere Dienste sind natürlich ebenso denkbar. Sämtliche Herangehensweisen in dieser Aufgabe zu besprechen würde aber den Rahmen der Vorlesung bei weitem sprengen.

69



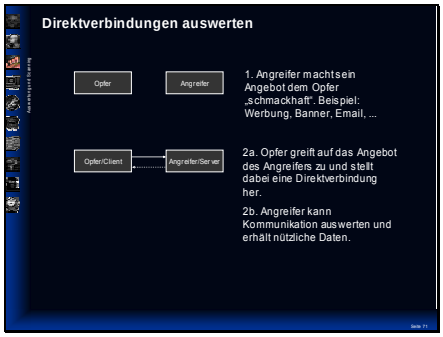
In diesem kleinen Kapitel wollen wir sehen, wie ein Zielsystem nun überhaupt lokalisiert werden kann. Wir werden als Einführung die Nutzung und Funktionsweise von IP-Adressen besprechen. Anhand von Direktverbindungen zu einer IP-Adresse wollen wir das Zielsystem lokalisieren. Als Alternative der Identifikation einer IP-Adresse eines Zielsystems soll die Auswertung von Mail-Headern diskutiert werden.

70



Um in TCP/IP-Netzen, wie das Internet auch eines ist, eine Verbindung herzustellen, wird mitunter auf IP-Adressen zurückgegriffen. Dies sind eindeutige Nummern, mit dem sich ein netzwerkfähiger Rechner adressieren lässt. Die gegenwärtig am meisten verbreitete Version ist mit IPv4 gegeben, die in RFC 791 (Internet Protocol) spezifiziert ist. IP-Adressen sind dabei durch einen 32 bit Wert repräsentiert, was wiederum insgesamt 2^32 IP-Adressen (4'294'967'296) möglich macht. Vorwiegend wird die Dotted decimal-Schreibweise genutzt, wobei sich der mögliche IP-Adressbereich von 0.0.0.0 bis 255.255.255.255 erstreckt. IP-Adressen werden in öffentliche, private und reservierte Bereiche unterteilt. Eine gültige private IP-Adresse nach RFC 1918 (Address Allocation for Private Internets) lautet beispielsweise 192.168.0.1. [Comer 1994, Stevens 1995]

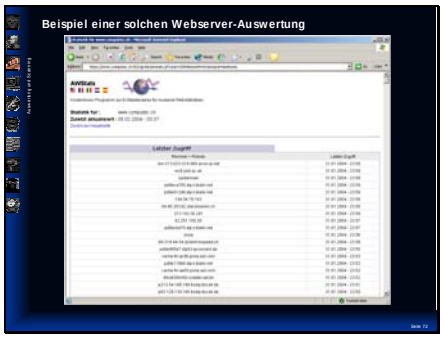
71



Eine klassische Technik, um die IP-Adresse eines Zielsystems identifizieren zu können, ist das direkte Herstellen einer Verbindung zu diesem. Dies kann beispielsweise durch die Eingabe einer URL in einem Webbrowser erfolgen. Das Betriebssystem wird sodann im Rahmen von TCP/IP die IP-Adresse des Zielsystems ermitteln und einen Datenaustausch mit diesem anstreben. Sobald diese Verbindung etabliert ist, kann anhand der Socket-Informationen die Quell- und Ziel-Adresse ausgemacht werden. Beide Parteien sind somit in der Lage, das Gegenüber anhand der eindeutigen IP-Adresse zu identifizieren.

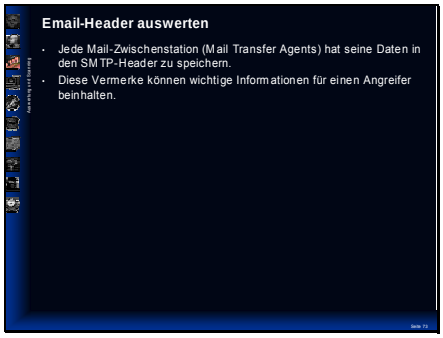
Ein solcher Verbindungsaufbau kann mittels Social Engineering provoziert werden, indem der Angreifer beispielsweise ein Email mit einer vermeintlich interessanten URL an sein Opfer schickt. Sobald dieses den Link in der Nachricht öffnet und damit eine Verbindung zu einem System herstellt, das unter der Kontrolle des Angreifers steht, findet er sich im Besitz der Information zur IP-Adresse des Gegenübers.

72



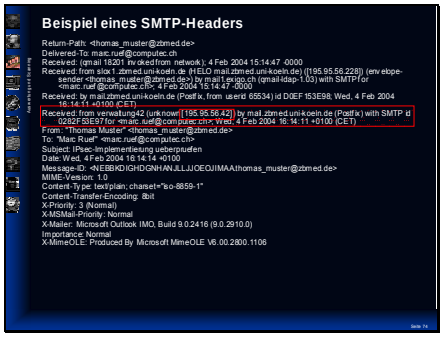
Dieser Screenshot soll verdeutlichen, wie einfach eine derartige Auswertung umgesetzt werden kann. Die meisten professionellen Server-Implementierungen weisen umfassende Protokollierungs-Möglichkeiten auf. In diesem Beispiel wird das open-source Tool AWStats genutzt, um die Logs eines Apache Webservers grafisch aufzubereiten. Anhand dieser Liste lassen sich sodann die letzten Zugriffe anzeigen. Sehr schön kann man so die IP-Adressen und Hostnamen der Benutzer erkennen. Kann man den Zugriff seines Opfers zeitlich eingrenzen, lässt sich dessen Zugriffsversuch einfach isolieren.

73



Eine ebenfalls gern genutzte Möglichkeit des Identifizierens der IP-Adresse einer Person ist in der Auswertung des Mailverkehrs gegeben. Dabei wird der Mail-Header eines empfangenen Emails analysiert, um Rückschlüsse auf die Herkunft und den Pfad des Schreibens schliessen zu können. Neben der Identifikation des Zielsystems lassen sich so auch architektonische und netzwerk-topologische Eigenschaften der Zielumgebung ausmachen (z.B. Firewall-Elemente und Antiviren-Gateways).

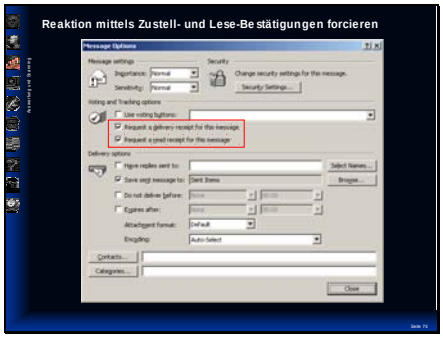
74



Ein jedes Email besteht aus einem Header und aus einem Body. Im Body ist der eigentliche Inhalt des Schreibens festgehalten. Ebenso kann ein Anhang (engl. Attachment) Teil des Bodies sein. Im Mail-Header sind Steuerungsinformationen der Nachricht festgehalten. So wird dort beispielsweise der Absender in der From-Zeile und der Empfänger in der To-Zeile vermerkt.

Emails werden in der Regel über SMTP-Relays verschickt. Diese Mailserver sind dafür zuständig, die Nachricht an den endgültigen Zielort zu transferieren. Laut den Spezifikationen des Simple Mail Transfer Protocols (SMTP, RFC 821) hat jedes Relay mitunter seine IP-Adresse im Header zu speichern. Dabei geben die jeweiligen Relays ebenfalls die IP-Adresse des letzten Hops innerhalb ihres Received-Vermeks an. So kann es also sein, dass das erste SMTP-Relay, das die Email-Nachricht vom Rechner des Senders entgegennimmt, dessen IP-Adresse im SMTP-Header festhält. Vor allem offene Relays und jene von Freemailern (z.B. Hotmail und GMX) tun dies, um Missbräuchen (z.B. Spam) entgegenzuwirken.

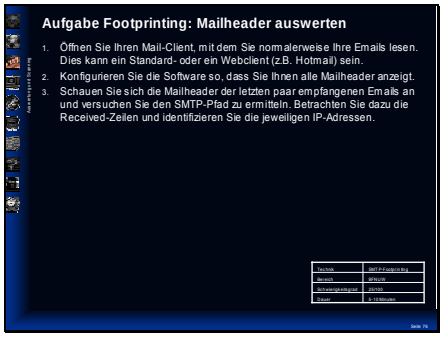
75



In der Regel wird ein Angreifer versuchen, eine Email-Antwort seines Opfers zu provozieren, um die Auswertung des Mail-Headers umsetzen zu können. Es kann jedoch sein, dass das Opfer nicht auf diesen Trick reinfällt und von der Beantwortung absieht. In diesem Fall kann man versuchen erweiterte Funktionen von SMTP ins Spiel zu bringen. So bieten die meisten modernen Mail-Clients die Möglichkeit, dass der finale Mailserver eine automatische Zustellbestätigung nach Empfang der Nachricht verschickt. So lässt sich wenigstens der erfolgreiche Versand und die IP-Adresse des finalen Mailservers identifizieren. Desweiteren kann auf die Funktion zurückgegriffen werden, die ein automatisches Beantworten bei der erstmaligen Ansicht des Emails durch das Opfer initiiert. Damit wird eine manuelle Beantwortung des Schreibens hinfällig.

Es ist zu beachten, dass diese Funktionen zwar allesamt in den Standards dokumentiert sind, jedoch nicht jeder Hersteller von Mail-Software diese auch umfassend implementiert. Hinzu kommt, dass diese Features eben genau aus Sicherheitsgründen oftmals standardmässig deaktiviert sind oder durch sicherheitsbewusste Benutzer manuell abgeschaltet werden.

76

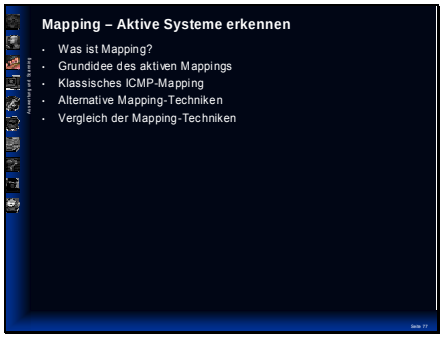


Führen Sie nun alleine oder in Zweiergruppen eine solche Auswertung des Mail-Headers einer Emails durch. Verschicken Sie als erstes ein reguläres Email an eine Zieladresse, auf dessen Postfach Sie zugriff haben. Um die Technik realitätsnah illustrieren zu können, sollte das nicht unbedingt die eigene Mailadresse sein, weil sonst in den meisten Fällen lediglich eine lokale Mailzustellung (LMTP, Local Mail Transfer Protocol) umgesetzt werden könnte, was die Auswertung des Mailheaders verhindern könnte.

Haben Sie das Email an die Zieladresse geschickt, sollte es dort mit einem regulären Mailprogramm eingesehen werden. Bei Freemailer-Diensten wie Hotmail oder GMX kann dies auch über die Web-Oberfläche geschehen. Suchen Sie nun in Ihrem Mailprogramm eine Funktion, die das Anzeigen sämtlicher Header-Daten ermöglicht. Bei Microsoft Outlook müssen Sie dazu mit der rechten Maustaste auf das Email klicken und dann im Kontextmenü den Punkt „Optionen“ auswählen. In der Textbox werden sodann die SMTP-Header angezeigt.

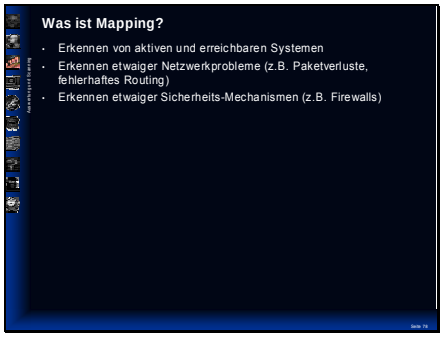
Sobald Sie diese einsehen können, machen Sie sich an die Analyse der jeweiligen Zeilen. Vor allem die Received-Zeilen sind interessant, beinhalten sie doch die Daten der jeweiligen SMTP-Relays. In manchen Fällen wird jedoch auch die IP-Adresse des Absenders in einer Zeile wie X-IP-Adress oder X-Origin festgehalten.

77



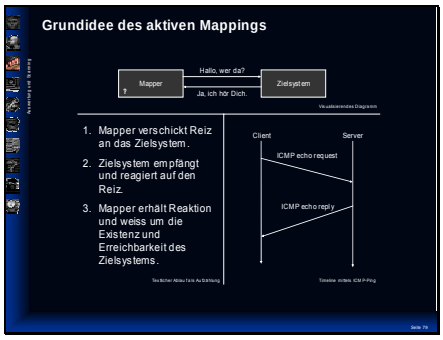
Hat ein Angreifer erste Informationen zu einer Zielumgebung innerhalb des Footprinting-Prozesses sammeln können, wird er die wahre Existenz und technische Erreichbarkeit potentieller Angriffsziele ausmachen wollen. Dazu werden unterschiedliche Methoden des Mappings verwendet, die wir im Folgenden genauer betrachten wollen. Als erstes diskutieren wir, was überhaupt die Idee des Mappings ist, um danach die klassische Mapping-Technik mit Ping (ICMP echo request) zu illustrieren. Einige Übungen werden die Idee dessen näherbringen können. Desweiteren schauen wir uns kurz alternative Mapping-Techniken samt ihren Vor- und Nachteilen an.

78



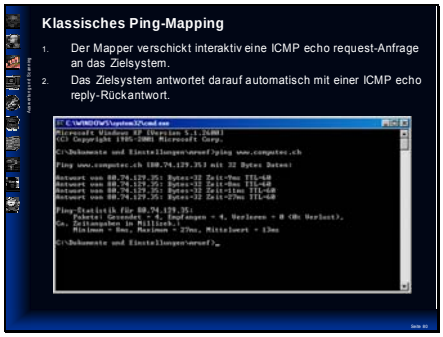
Die Technik des Mappings wird eingesetzt, um die Existenz und Erreichbarkeit eines Systems zu determinieren. Dies wird in einer frühen Phase eines Angriffs umgesetzt, um weitere Zugriffe nicht unnötig oder in unauffälliger Weise anzustreben. Mitunter lassen sich mittels Mapping-Techniken ebenfalls Sicherheits-Systeme wie Firewall-Elemente ausmachen, die in jeglicher Phase eines Angriffs von Interesse sind. Wir wollen uns in diesem Kapitel aber vorwiegend auf die grundsätzliche Idee des Mappings, des Erkennens der Erreichbarkeit eines Hosts, fokussieren.

79



Die Grundidee des aktiven Mappings greift auf das Reiz/Reaktions-Schema zurück. Der Mapper schickt einen Reiz an das Zielsystem. Dieses wird jenachdem auf diesen reagieren und antworten. Anhand des Verhaltens des Zielsystems kann der Mapper die Existenz und Erreichbarkeit dessen identifizieren.

80

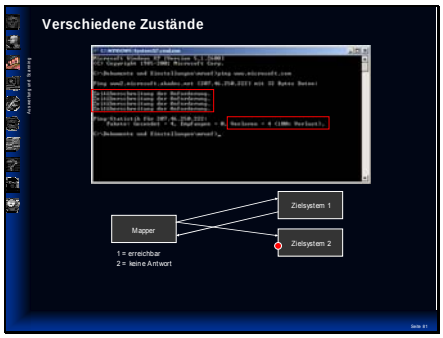


Die klassische Mapping-Technik setzt eine ICMP echo request-Anfrage ein, die durch das Zielsystem bei erfolgreichem Erhalt und Verarbeitung durch eine ICMP echo reply-Rückantwort bestätigt werden sollte. Bleibt in diesem Fall die Reaktion aus, trat ein Problem bei der ICMP-Kommunikation mit dem Zielsystem auf.

Ein einfaches Ping-Mapping kann mit einem simplen Aufruf des Ping-Kommandos umgesetzt werden. Dieses ist Teil vieler modernen Betriebssysteme (sowohl Unix/Linux als auch Windows). Der Syntax hat die Form „ping <zielsystem>“, wobei das Attribut <zielsystem> den Hostnamen oder die IP-Adresse des zu überprüfenden Systems definiert. Jenachdem wie die Implementierung umgesetzt wird, verhält sich der Ping-Zugriff geringfügig anders. Bei Microsoft Windows werden standardmässig 4 ICMP echo request-Pakete verschickt und ausgewertet. Danach wird eine Statistik des Suchlaufs ausgegeben und Ping kehrt wieder zur Kommandozeile zurück.

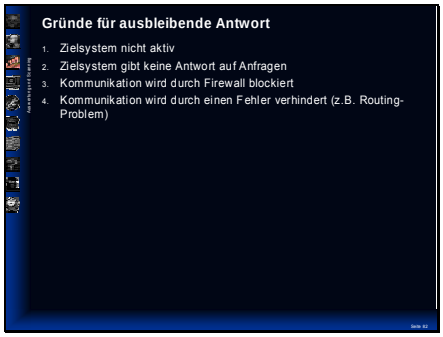
In obigem Beispiel wird ein normaler Ping-Zugriff unter Microsoft Windows XP umgesetzt. Als Zielsystem wird der Host mit dem Namen www.computec.ch angegeben. Die Ping-Implementierung unter Windows führt eine IP-Adressauflösung durch (80.74.129.35) und schickt jeweils 4 ICMP echo request-Datenpaket à 32 Bytes an das Zielsystem. Nach dem Absetzen der Anfrage wird eine Statistik des Zugriffs ausgegeben, die in diesem Fall den Versand von 4 Anfragen und den Empfang von wiederum 4 Antworten kennzeichnet. Ganz am Schluss findet sich eine Übersicht der Zeitwerte dieser Zugriffe.

81



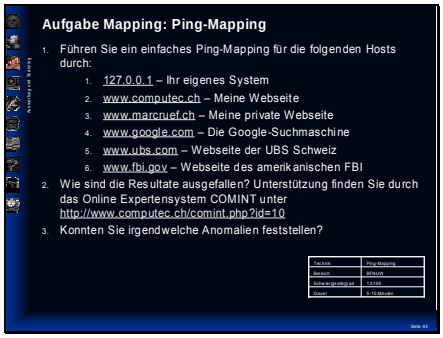
Ein Mapping-Zugriff mittels Ping kann verschiedene Resultate offenlegen. In obigem Beispiel wird ein Ping für den Host mit dem Namen www.microsoft.com ausgeführt. Die Namensauflösung ist erfolgreich und die 4 ICMP echo request-Anfragen werden verschickt. Jedoch wird auf einer jeden Zeile der Hinweis „Zeitüberschreitung der Anforderung“ ausgegeben. Dies ist das Resultat, wenn die Anfrage nicht innerhalb der vorgegebenen Zeit durch eine reguläre ICMP echo reply-Rückantwort bestätigt wurde. Wie auch in der abschliessenden Ping-Statistik vermerkt ist, sind 100 % der Anfragen verloren gegangen. Der Ping-Zugriff war also hier nicht erfolgreich. Die möglichen Gründe dafür wollen wir auf der nächsten Folie diskutieren.

82



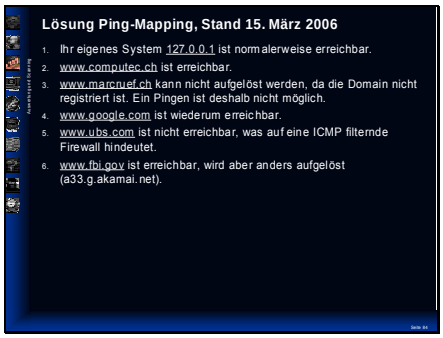
Es gibt verschiedene Gründe, warum innerhalb eines Ping-Zugriffs eine Antwort ausbleiben kann. Der häufigste Grund ist mit Sicherheit, dass das Zielsystem nicht aktiv ist. Das Erreichen dessen wird aufgrund fehlender Konnektivität nicht möglich bleiben. Sicherheitsbewusste Administratoren pflegen ihre Systemen jedoch so, dass sie auf Mapping-Anfragen keine Antworten verschicken. Im Falle von Ping werden eingehende ICMP echo request-Pakete (Typ 8) verworfen. Ebenfalls kann es aber auch sein, dass ein Firewall-Element den Zugriff verhindert. Dies ist meistens dann der Fall, wenn die Firewall eingehenden ICMP-Datenverkehr nicht zulässt. So mancher Administrator setzt auch auf der Firewall die Regel um, dass eingehende ICMP echo request-Pakete verworfen werden. In manchen Fällen werden gar ebenfalls die ausgehenden ICMP echo reply-Rückantworten (Typ 0) unterbunden. Und zu guter letzt kann es auch sein, dass ein Fehler den erfolgreichen Mapping-Zugriff verhindert. Dazu zählen traditionelle Netzwerk- oder Software-Fehler, bei denen Pakete an falsche Destinationen geschickt (Probleme beim Routing) oder anderweitig falsch verarbeitet werden.

83



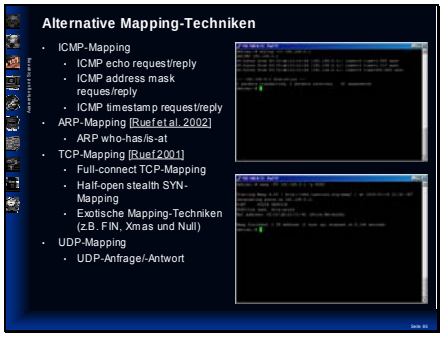
Führen Sie nun innerhalb einer Übung die Ping-Zugriffe auf die oben genannten Systeme durch. Benutzen Sie dazu den regulären Ping-Befehl Ihres Betriebssystems. Bei Microsoft Windows ist dieser innerhalb des MS DOS-Eingabeaufforderung erreichbar. Diese erreichen Sie bei neueren Windows-Systemen über die Schaltfläche Start, die Auswahl des Eintrags „Ausführen“ und die Eingabe des Befehls „cmd“. Danach können Sie einen herkömmlichen Aufruf in der Form von „ping <zielsystem>“ umsetzen. Eine Hilfestellung zur Bewältigung dieser Aufgabe finden Sie im freien Online Expertensystem COMINT unter http://www.computec.ch/comint.php?id=10 – Dieses Produkt begleitet Sie Schritt für Schritt durch ein erfolgreiches Mapping. Notieren Sie sich, wie die Resultate der Ping-Zugriffe der jeweiligen Zielsysteme ausgefallen sind. Etwaige Anomalien sind ebenfalls festzuhalten.

84



Die Lösungen entnehmen Sie dieser Folie. Es ist zu beachten, dass die Resultate jenachdem von den hier dokumentierten abweichen können. Migrationen in den Zielumgebungen können zu anderem Verhalten führen.

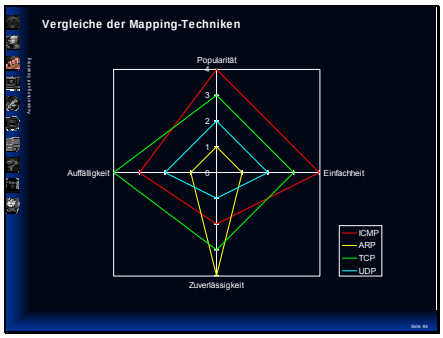
85



Es gibt eine Vielzahl an verschiedenen Mapping-Techniken. Wir haben bisher lediglich das traditionelle Ping-Mapping mittels ICMP echo diskutiert. Alternative Mapping-Techniken kommen dann zum Einsatz, wenn ein Zugriff nicht erfolgreich verlaufen ist. Unter gewissen Umständen lassen sich nämlich mit anderen Protokollen und Methoden die etablierten Sicherheitsmechanismen (z.B. Firewalls und ACLs) umgehen.

Das ICMP-Protokoll stell noch einige andere Typen zur Verfügung, mit denen sich vergleichbare Zugriffe wie mit Ping umsetzen lassen. In lokalen Netzen wird gerne auf das sehr zuverlässige und schwer zu entdeckende ARP-Mapping zurückgegriffen, das wiederum das Address Resolution Protocol (ARP) zur Identifikation eines Zielsystems heranzieht (siehe Screenshot 1) [Ruef et al. 2002]. Etwas populärer und vor allem bei Mapping-Zugriffen im Internet sehr hilfreich ist das sogenannte TCP-Mapping, bei dem klassische Portscan-Technologien zur Determinierung der Erreichbarkeit eines Hosts eingesetzt wird (siehe Screenshot 2) [Ruef 2001]. Das UDP-Mapping verfährt da in ähnlichem Rahmen, ist aber aufgrund des Einsatzes des User Datagram Protocols eher weniger zuverlässig. Eine Auflistung und Begleitung aktiver Mapping-Methoden finden sich weiterhin im Expertensystem COMINT unter http://www.computec.ch/comint.php?id=8

86



Die jeweiligen Methoden des Mappings weisen gewisse Vor- und Nachteile auf, die in diesem Diagramm visualisiert werden. Die Popularität des ICMP-Mappings ist unbestritten. Diese kommt vor allem daher, weil es sehr einfach und zuverlässig mit der jeweiligen Ping-Implementierung des Betriebssystems umgesetzt werden kann. Aber entsprechend ist auch die Auffälligkeit besonders hoch, denn viele Sicherheits-Systeme (Firewalls und Intrusion Detection-Systeme) richten ihr Augenmerk auf solcherlei ICMP-Kommunikationen.

Von den alternativen Mapping-Techniken ist vor allem das ARP-Mapping besonders interessant [Ruef et al. 2002]. Dieses lässt sich jedoch nur in lokalen Netzen bzw. einem gleichen Subnetz umsetzen. Da Zugriffe über das Internet aufgrund den Limitierungen des eingesetzten Address Resolution Protocols nicht möglich sind, ist diese Technik entsprechend unpopulär. In lokalen Netzen bleibt es aber die erste Wahl, da es in Punkto Effizienz, Zuverlässigkeit und Unauffälligkeit nicht übertroffen werden kann.

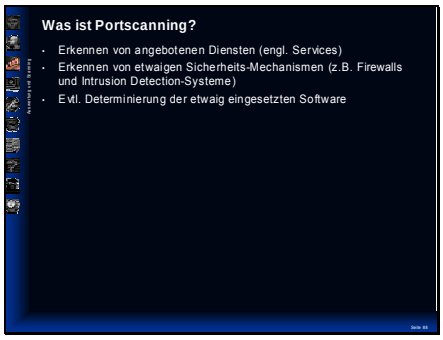
Die alternativen Methoden mittels TCP und UDP sind in allen Bereichen einsetzbar und eignen sich hervorragend zum Ausweichen, falls ICMP versagt. Die Zuverlässigkeit ist in gewissen Situationen gar höher weder beim traditionellen Ping-Mapping [Ruef 2001]. Jedoch ist die Auffälligkeit entsprechender Zugriffe relativ gross, da viele Sicherheits-Lösungen die jeweiligen Anfragen als Portscan verstehen könnten.

87



Nachdem wir die Existenz und Erreichbarkeit eines Hosts mittels Mapping identifizirt haben, wollen wir uns über die durch ihn bereitgestellten Dienste informieren. Dies tun wir mit der traditionellen Portscanning-Technik, die die Port-Stati auf dem Zielsystem über ein Netzwerk feststellen kann. Je mehr Dienste ein System anbietet, desto mehr Angriffsfläche gewährt es. Nach einer Einführung in das Thema Portscan wollen wir uns den full-connect TCP-Scan anschauen, der gemeinhin als der Klassiker der Portscanning-Techniken gilt. Desweiteren wollen wir sehen, wie sich ein half-open SYN-Scan verhält, der einiges schwieriger zu entdecken ist. Und zum Schluss werden wir einen kurzen Blick auf einige der exotischen Scan-Techniken werfen, die zwar in den meisten Fällen nicht besonders zuverlässig aber dafür umso schwerer zu entdecken sind.

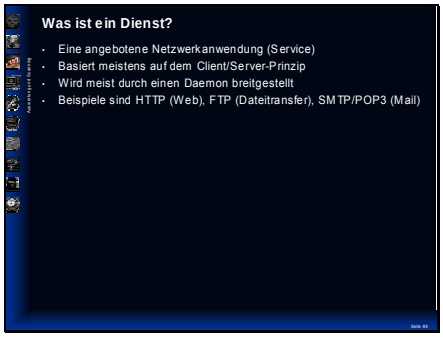
88



Die Technik des Portscannings hat grundsätzlich zum Ziel, die Stati eines Ports an einem Zielsystem zu determinieren. Anhand dieser Informationen können die Dienste (engl. Services), die von einem Server angeboten werden, identifiziert werden [McClure 1998, Ruef 2001, Ruef et al. 2002]. Im weiteren Verlauf wird der Angreifer seine Auswertungen und Angriffe auf diese Dienste fokussieren.

Desweiteren lässt sich innerhalb des Portscannings ebenfalls Sicherheitssysteme eruieren. Ein bestimmtes Verhalten der Ports lässt in manchen Fällen Rückschlüsse auf den Einsatz von Firewall-Systemen und ACLs zu. Ebenfalls kann die Charakteristika eines Ports Ableitungen auf die eingesetzte Software und das genutzte Betriebssystem zulassen.

89



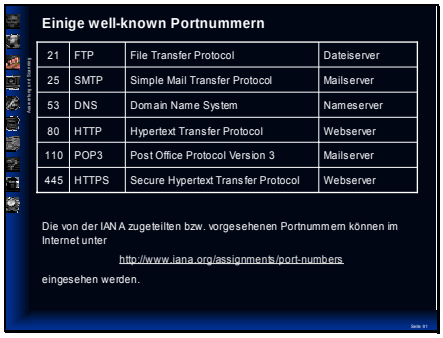
Unter dem Begriff Dienst (engl. Service) wird eine angebotene Netzwerkanwendung verstanden. Diese basieren meist auf dem Client/Server-Prinzip. Dies bedeutet, dass der Dienst als Server eine bestimmte Netzwerkanwendung bereitstellt. Der Benutzer kann von diesem Dienst mit der Hilfe des entsprechenden Clients Gebrauch machen. Sehr bekannte Dienste werden durch Web- und Mailserver bereitgestellt. Diese können durch einen Benutzer mittels Webbrowser und Mailclient genutzt werden. Netzwerkdienste werden dabei in der Regel an bestimmte Ports gebunden, zu denen ein Client eine Verbindung herstellen muss. [Stevens 1994, Comer 1995]

90



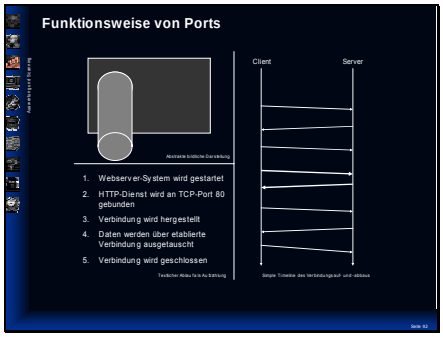
Unter Port wird eine Adresskomponente von Netzwerkprotokollen verstanden. Im Rahmen der Transportprotokolle UDP und TCP wird er für die Zuweisung und das Anbieten von Diensten genutzt. Ein Port innerhalb von IPv4 weist einen nummerischen 16 bit Wert auf, was die Umsetzung von 2^16 Ports (65'535) ermöglicht. Dabei ist der Bereich von 0 bis 65535 zugelassen. Die Ports 1 bis 1023 gelten als well-known Ports, da auf diesen die bekanntesten Dienste (z.B. HTTP für Web und SMTP für Email) genutzt werden. In der Regel benötigt ein Benutzer administrative Privilegien, um einen Dienst innerhalb dieses Bereichs an einen Port zu binden. Die Ports über 1023 gelten als kurzlebige Ports, werden sie doch oftmals innerhalb zeitlich begrenzter Kommunikationen von Sockets genutzt. [Stevens 1994, Comer 1995]

91



Die IANA publiziert regelmässig eine Liste von Empfehlungen, welche Dienste an welchen Port gebunden werden sollten. Diese ist online unter http://www.iana.org/assignments/port-numbers zu finden. Vor allem im Bereich der well-known Ports (1 bis 1023) gibt es typische Vergaben, wie zum Beispiel Port 25 für SMTP (Simple Mail Transfer Protocol, Mailserver) und Port 80 für HTTP (Hypertext Transfer Protocol, Webserver). Es gilt dabei zu beachten, dass dies lediglich eine Empfehlung ist. Administratoren und Nutzer können theoretisch Dienste an beliebige Ports binden.

92



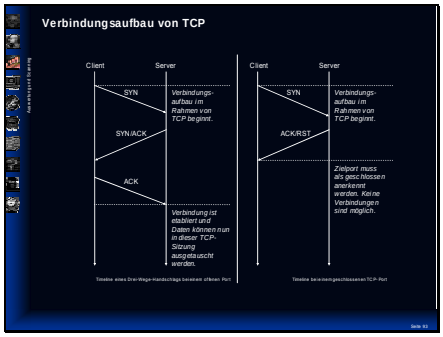
Diskutieren wir nun die Funktionsweise eines Ports. Nehmen wir als Beispiel einen Webserver, der auf einem Host installiert, konfiguriert und gestartet wird (1). Dieser bindet sich standardmässig an den TCP-Port 80 (2). Dabei wird der besagte Port in den LISTENING-Modus (dt. Abhörend) geschaltet. Der Server „lauscht“ nun auf diesem Port nach ankommenden Anfragen.

Wird nun ein Client – in diesem Beispiel ein Webbrowser - gestartet und damit eine Verbindung zum Zielsystem hergestellt, verbindet sich der Client auf den Zielport. Der Server ist gewillt Anfragen auf dem genutzten Port entgegenzunehmen und lässt entsprechend die Verbindung zu (3). Im Rahmen von TCP wird die Verbindung sodann als etabliert (engl. Established) bezeichnet. Client und Server haben nun die Möglichkeit, über diesen Kanal Daten auszutauschen.

Der Datenaustausch findet dabei im Rahmen des entsprechenden Anwendungsprotokolls statt (4). Im Beispiel des Webserver und Webbrowsers ist dies im Normalfall HTTP (Hypertext Transfer Protocol), das für die Datenübertragung im World Wide Web (WWW) genutzt wird. Ist der Datenaustausch beendet, kann die Verbindung wieder abgebaut werden (5).

Die meisten Server-Implementierungen arbeiten Multithreading. Das bedeutet, dass sie sich an ein und denselben Port binden und dort mehrere Verbindungen zeitgleich bearbeiten können. Mit Multithreading wird das quasi simultane Abarbeiten mehrerer Threads (das sind Ausführungsstränge innerhalb eines einzelnen Prozesses oder eines Tasks) bezeichnet. Es ist also nicht so, dass wenn sich ein Client auf den Port des Servers verbunden hat, letzterer von nun an keine neuen Verbindungen mehr annehmen kann. Die Identifikation der jeweiligen Clients findet dabei auf dem Netzwerk durch die eindeutigen Socket-Informationen statt. [Stevens 1994]

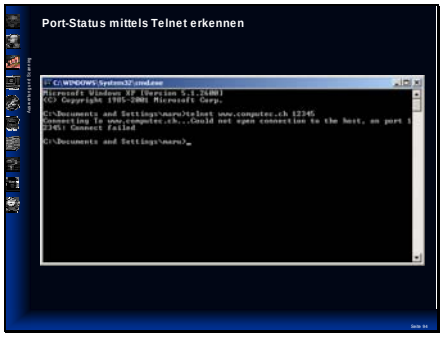
93



Betrachten wir nun den Verbindungsaufbau ihm Rahmen von TCP etwas genauer. Bedienen wir uns der Timeline-Darstellung, wie sie mitunter auch von W. Richard Stevens in seinem Standardwerk „TCP/IP Illustrated, Volume 1: The Protocols“ genutzt werden [Stevens 1994]. Dort ist die hier diskutierte Funktionsweise sehr schön und umfassend besprochen: (1) Möchte ein Client eine TCP-Verbindung zu einem Server herstellen, schickt er als erstes ein TCP-Paket mit gesetzter SYN-Flagge an den Zielport des Zielsystems. SYN steht dabei für Synchronisation. (2) Ist der Server gewillt, diese Verbindung aufzubauen, weil zum Beispiel ein Server an den anvisierten Port gebunden wurde, wird er die Anfrage quittieren. Dies macht er, indem er ein TCP-Paket mit gesetzter SYN- und ACK-Flagge zurückschickt. ACK steht dabei für Acknowledge und ist als Bestätigung der vorangehenden SYN-Anfrage zu verstehen. Die SYN-Flagge zeigt, dass auch der Server eine Synchronisation mit dem Client herstellen möchte. (3) Hat der Client die Bestätigung des Servers erhalten, wird er die SYN-Anfrage ebenfalls mit einem ACK-Segment bestätigen wollen. Da hierbei insgesamt drei Schritte durchlaufen werden, wird dies auch als Drei-Wege-Handschlag von TCP (engl. Three-way-handshake) bezeichnet.

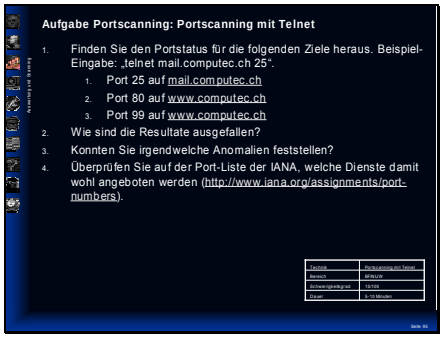
Das Verhalten bei einem Zugriff auf einen „geschlossenen“ Port, der sich nicht im LISTENING-Modus befindet und auf dem entsprechend kein Dienst bereitgestellt wird, sieht leicht anders aus. (1) Wiederum schickt der Client seine initiale Anfrage in der Form eines TCP-Pakets mit gesetzter SYN-Flagge an den Zielport des Zielsystems. (2) Da diese nun aber auf dem angefragten Port keinen Dienst anbietet, wird der weitere Verbindungsaufbau abgebrochen. Das Server-System schickt dazu ein Paket mit gesetzten ACK- und RST-Flaggen. Die ACK-Flagge bestätigt wiederum den Erhalt des vorangehenden SYN-Pakets. Die RST-Flagge weist jedoch auf den Umstand hin, dass keine Verbindung erlaubt wird. RST steht dabei für Reset, also das Zurücksetzen des Verbindungsaufbaus. Der Client weiss in diesem Fall nach Erhalt des RST-Pakets, dass auf dem Zielport kein Dienst bereitgestellt wird.

94



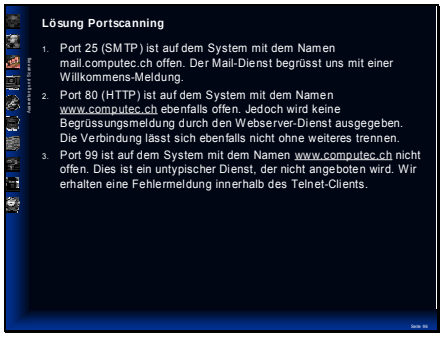
Eine sehr einfache Möglichkeit, den Port-Status auf einem Zielsystem zu bestimmen, ist im Heranziehen einer herkömmlichen Netzwerk-Anwendung gegeben. So manche von diesen lässt nämlich die Angabe eines Zielports, auf den sich verbunden werden soll, zu. Bestes Beispiel ist die Terminal-Emulation TELNET, dessen Client Bestandteil vieler moderner Betriebssysteme ist. Durch den einfachen Syntax „telnet <zielsystem> <zielport>“ lässt sich eine Verbindung zum Zielport auf dem Zielsystem herstellen [Stevens 1994, Ruef et al 2002]. Ist der Port offen, kann die Verbindung etabliert werden. Ist dem nicht so, wird ein Verbindungsfehler ausgegeben. In obigem Beispiel wird unter Microsoft Windows XP mit der Eingabe von „telnet www.computec.ch 12345“ eine Verbindung auf den TCP-Port 12345 auf dem Zielsystem mit dem Hostnamen www.computec.ch umgesetzt. Da sich auf dem Zielport am Zielsystem kein angebotener Dienst findet, ist eine Verbindung nicht möglich. Der Telnet-Client gibt nach wenigen Sekunden eine Fehlermeldung aus, dass kein Zugriff möglich war. Der Port muss als geschlossen betrachtet werden.

95



Führen Sie nun innerhalb dieser Übung selber ein manuelles Portscanning mittels Telnet durch. Öffnen Sie dazu bei Windows die MS DOS-Eingabeaufforderung durch das Klicken auf den Start-Knopf und das Auswählen des Eintrags „Ausführen“. Geben Sie dort „cmd“ ein und starten Sie. Auf der Kommandozeile kann der Telnet-Client mit der Eingabe von „telnet“ aufgerufen werden. Ein Zugriff auf den TCP-Port 25 des Systems mit dem Namen mail.computec.ch setzen Sie beispielsweise mit der Eingabe von „telnet mail.computec.ch 25“ um. Führen Sie die Scanning-Zugriffe der Übung durch und notieren Sie sich die Resultate. Welche Ports konnten als offen und welche als geschlossen identifiziert werden? Sind ansonsten irgendwelche Anomalien festzustellen? Überprüfen Sie zudem auf der offiziellen Port-Liste der IANA, die Sie unter http://www.iana.org/assignments/port-numbers erreichen können, welche Dienste auf diesen Ports wohl angeboten werden.

96

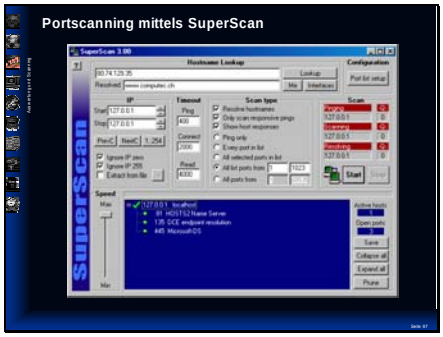


Einige der Zugriffe sollten erfolgreich verlaufen sein. Einfachstes Beispiel ist die Telnet-Verbindung auf den TCP-Port 25 des Zielsystems mail.computec.ch. Dabei handelt es sich um den SMTP-Dienst, der für das Annehmen und Verschicken von Emails verantwortlich ist. Sobald Telnet eine Verbindung zum Zielport etablieren konnte, begrüsst uns der Mailserver mit einer kleinen Meldung. Diese weist uns an, dass der Server zur Eingabe bereit ist.

Der Zugriff auf den TCP-Port 80 des Zielsystems www.computec.ch sollte ebenfalls erfolgreich verlaufen. Hierbei wird sich auf den Webserver verbunden, der nach etablierter Sitzung auf die Eingabe durch den Client wartet. Dieses Vorgehen unterscheidet sich von jenem vieler anderer Server-Implementierungen. Webserver geben also von sich aus keine Willkommens-Meldungen aus, sondern verharren nach etablierter Verbindung in einem wartenden Schweigen.

Der letzte Zugriff auf den TCP-Port 99 sollte nicht erfolgreich verlaufen sein. Der Telnet-Client weist in diesem Fall die Fehlermeldung aus. Grund dafür ist, dass auf diesem Port am Zielsystem kein Dienst angeboten wird. Der Port befindet sich also nicht im LISTENING-Modus und entsprechende Verbindungsanfragen werden vom Betriebssystem zurückgesetzt.

97

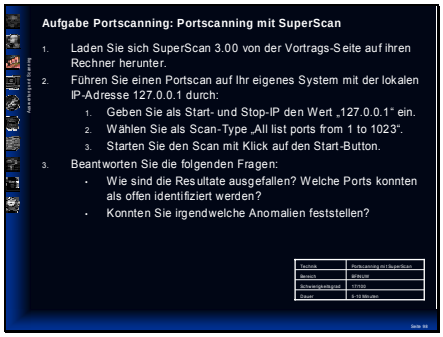


Das manuelle Absuchen offener Ports mittels Netzwerkanwendungen wie einem Telnet-Client gestalten sich schwierig, mühsam und langwierig. So kann lediglich immer nur ein Zielport anvisiert werden. Möchte man Ausschau nach den möglichen angebotenen Diensten halten, eignet sich ein automatisiertes Portscanning besser. Es gibt eine Vielzahl an Portscanning-Utilities, die das Determinieren der Portstati eines Zielsystems komfortabel umsetzen können.

Die mitunter populärste Lösung nennt sich nmap (Network Mapper) und wurde von einem Hacker namens Fyodor ursprünglich für Linux entwickelt (http://www.insecure.org/). Das zeilenbasierte Tool gibt es jedoch mittlerweile für die meisten populären Betriebssysteme [McClure et al. 1998, Ruef 2001, Ruef et al 2002]. Dennoch wollen wir in Windows-Umgebungen auf die Freeware-Lösung SuperScan der amerikanischen Firma Foundstone (http://www.foundstone.com/) zurückgreifen [Ruef et al. 2002].

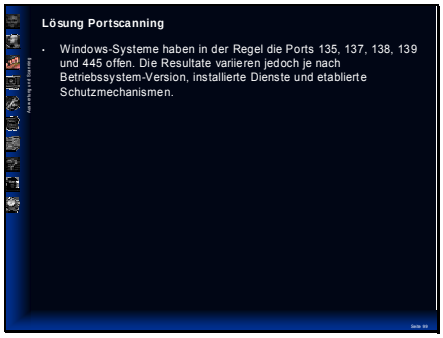
Wie in der Video-Aufzeichnung zu sehen ist, wird ein Scan auf die lokale IP-Adresse 127.0.0.1 umgesetzt. Hier lassen sich ebenfalls ganze IP-Adressbereiche in den Feldern Start und Stop definieren. Um ein ganzes Klasse C-Netzwerk zu scannen, kann als Start 192.168.0.1 und als Ziel 192.168.0.254 eingegeben werden. Danach werden die Scan-Typen definiert. Die Auflösung von Hostnamen und das Umsetzen eines Mapping-Zugriffs vor dem eigentlichen Portscan sind anzuraten, um möglichst viele und zuverlässige Informationen zusammentragen zu können. Ebenfalls lässt sich automatisiertes Banner-Grabbing mit der Anzeige der automatisierten Rückantworten eines Dienstes umsetzen. Danach wird der Port-Bereich angegeben, der überprüft werden soll. Wir greifen auf eine interne Liste zurück, die die wichtigsten Ports scannen lässt. Als Nummernbereich definieren wir 1 bis 1023, was den well-known Ports gleichkommt. Dadurch können wir sicherstellen, dass schnell und effizient die wichtigsten Dienste ermittelt werden können. Durch das Klicken auf den Start-Button kann der Scan gestartet werden. Nach wenigen Sekunden ist der Portscan auf das lokale System beendet und die angebotenen Dienste werden in der Übersicht dargestellt. In diesem Beispiel sind dies die TCP-Port 81, 135 und 445.

98



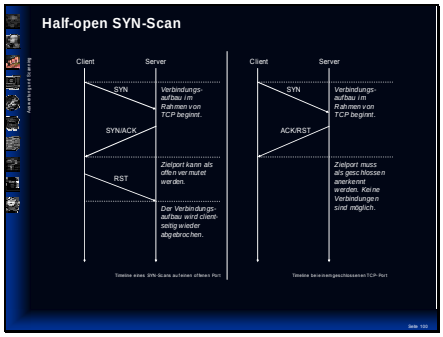
Setzen Sie nun selber den zuvor gezeigten Portscan auf Ihrem System um. Laden Sie dazu als erstes den freien Portscanner SuperScan 3.00 von der Workshop-Webseite herunter. Nachdem Sie die Software installiert haben, führen Sie sie aus. Geben Sie nun als Start- und End-IP Ihre lokale IP-Adresse 127.0.0.1 ein. Damit gewährleisten Sie, dass nur dieses eine System gescannt wird. Wählen Sie als Scan-Type „All list ports" und geben Sie dort den Bereich 1 bis 1023 ein. Damit beschränken wir uns auf den Zugriff der well-known Ports, die besonders erfolgsversprechend sind. Danach klicken Sie auf den Start-Button und gewähren der Software einige Minuten Zeit, um den Scan-Durchlauf abzuschliessen. Betrachten Sie nun die Resultate in der Übersicht. Wie sind diese ausgefallen? Welche Ports konnten auf Ihrem System als offen identifiziert werden? Konnten Sie irgendwelche Anomalien feststellen?

99



Windows-Systeme haben in der Regel die NetBIOS-Ports 135, 137, 138, 139 und 445 offen. Die Resultate variieren jedoch je nach Betriebssystem-Version, installierte Dienste und etablierte Schutzmechanismen.

100

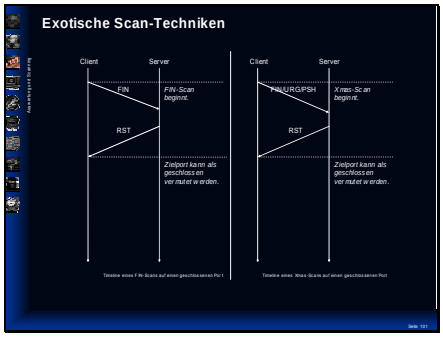


Die zuvor illustrierte TCP-Portscan Technik wird gerne als full-connect bezeichnet. Dies rührt daher, weil im Rahmen von TCP der gesamte Drei-Wege-Handschlag durchlaufen und eine komplette Verbindung hergestellt wird. Dies ist unter Umständen besonders auffällig, weil die jeweiligen Server-Implementierungen oftmals erfolgreiche Sitzungen in den Protokollen speichern. Der Scan-Zugriff könnte so schnell entdeckt werden.

Aus diesem Grund wird auf die half-open Methode ausgewichen. Hierbei initiiert der Client einen herkömmlichen Verbindungsaufbau im Rahmen von TCP. (1) Dazu schickt er ein TCP-Segment mit gesetzter SYN-Flagge an den Port des Zielsystems. (2) Bietet dieses auf dem angesprochenen Port einen Dienst an und ist es gewillt eine Verbindung zuzulassen, wird ganz regulär die Anfrage mit einem SYN/ACK-Paket quittiert. Die ersten beiden Schritte des üblichen Drei-Wege-Handschlags von TCP sind damit durchlaufen. (3) Nun verschickt aber der Client anstatt einer finalen ACK-Bestätigung ein TCP-Segment mit gesetzter RST-Flagge. Mit diesem Reset verhindert er, dass eine Etablierung der Sitzung zustande kommt und der Zugriff in den Protokolldateien der Netzwerkanwendung vermerkt werden könnten.

Das Verhalten bei geschlossenem Zielport ist hingegen identisch mit dem eines full-connect TCP-Portscans. Auch hier wird auf die initiale SYN-Anfrage (1) mit einem ACK/RST-Segment (2) der Zugriff grundsätzlich verweigert.

101

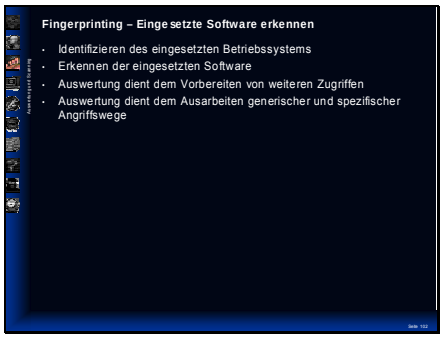


Viele Sicherheitssysteme sind in der Lage full-connect und half-open TCP-Portscans zu erkennen. Das Muster dieser ist einfach zu identifizieren. Aus diesem Grund wurden weitere exotische Scan-Techniken entwickelt. Eine davon wird FIN-Scan genannt. (1) Dabei schickt der Client ein TCP-Segment mit gesetzter FIN-Flagge an den Zielport des Zielsystems. (2) Entgegnet dieses mit einem TCP-Segment mit gesetzter RST-Flagge, muss der Port als geschlossen angesehen werden. Jegliche andere Antwort (auch das Ausbleiben einer solchen) kann als offener Port identifiziert werden.

Ähnlich verhält sich auch die Xmas-Scan Technik. (1) Bei dieser wird jedoch ein initiales TCP-Segment mit den drei gesetzten Flaggen FIN (Final), URG (Urgent) und PSH (Push) verschickt. (2) Wiederum deutet eine Rückantwort in der Form eines TCP-Segments mit gesetzter RST-Flagge auf einen geschlossenen Port hin.

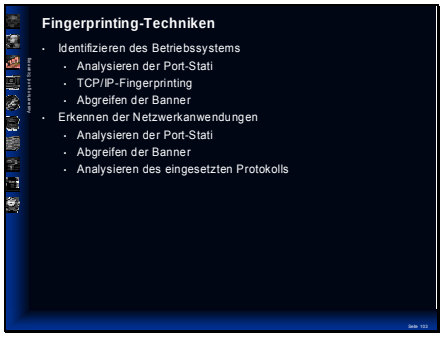
Das Problem dieser exotischen Techniken ist, dass sie nicht besonders zuverlässig sind. Der Grund ist jener, dass nicht alle Betriebssysteme bei einem geschlossenen Port mit dem erwarteten RST-Paket reagieren. So bleiben oftmals die Antworten aus, auch wenn der Zielport geschlossen ist. Im Rahmen des FIN- und Xmas-Scans wäre dies jedoch das Indiz für einen offenen Port. Der gleiche Effekt kann auch bei Netzwerkproblemen gegeben sein, wenn die initialen Anfragen oder die Rückantworten verloren gehen. So wird der Scanner auch in dieser Situation die Zielports fälschlicherweise als offen deklarieren. Das bekannte Scanning- und Auswertungs-Utility nmap versucht jedoch anhand einer statistischen Analyse derartige Fehlinterpretationen zu vermeiden.

102



Fingerprinting ist eine wichtige Technik, mit der sich auf einem Zielsystem eingesetzte Software erkennen lässt. So kann mit dem OS-Fingerprinting das eingesetzte Betriebssystem und mittels Application-Fingerprinting die genutzten Applikationen ermittelt werden. Diese Informationen sind sehr wichtig, um zielgerechte Attacken fahren zu können. Es macht nämlich sehr wenig Sinn, einen für Microsoft Windows XP entwickelten Angriff auf auf Red Hat Linux anzuwenden. Die Architekturen sind oftmals zu unterschiedlich, alsdass sich der gleiche Erfolg einstellen würde.

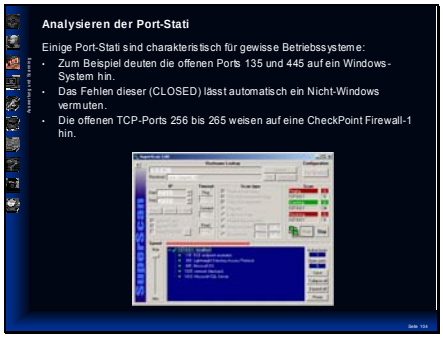
103



Wir wollen im Folgenden einige traditionelle Fingerprinting-Techniken diskutieren. Zur Identifikation eines Betriebssystems wollen wir die Port-Stati dessen studieren. Durch TCP/IP-Fingerprinting ermitteln wir anhand der Analyse des TCP/IP-Stacks das genutzte Betriebssystem sehr genau. Und ebenfalls die Angaben innerhalb von Anwendungen selbst lassen Rückschlüsse auf das genutzte Betriebssystem zu.

Desweiteren sollen die angebotenen Netzwerkanwendungen bestimmt werden. Dazu analysieren wir einmal mehr die Port-Stati und nehmen die Vorgaben der IANA zu Rate. Durch das aktive Abgreifen von Willkommens-Bannern versuchen wir den Namen und die Versionsnummer einer eingesetzten Netzwerkapplikation zu erkennen. Desweiteren verwenden wir unsere Zeit, um mittels Application Mapping das eingesetzte Protokoll der Anwendungsschicht zu erfassen.

104



Durch die zuvor besprochenen Portscanning-Techniken können wir die Port-Stati an einem Zielsystem identifizieren. Dabei gibt es typische Portbelegungen, die charakteristisch für einzelne Betriebssysteme und Installationen sein können. Bestes Beispiel ist die Windows-Betriebssystemreihe von Microsoft, die seit Microsoft Windows 95 auf offene NetBIOS-Ports (135 bis 139 sowie 445) setzt. Werden diese Ports als offen vorgefunden, handelt es sich beim Zielsystem mit grösster Wahrscheinlichkeit um ein modernes Windows. Jenachdem welcher dieser NetBIOS-Dienste wie implementiert ist, ist gar ein Rückschluss auf die jeweilige Windows-Version möglich. Wiederum kann man beim Fehlen dieser Ports das Zielsystem als Nicht-Windows einstufen. Es gibt noch eine Reihe anderer Charakteristika, die auf jeweilige Betriebssysteme und Installationen hindeuten können.

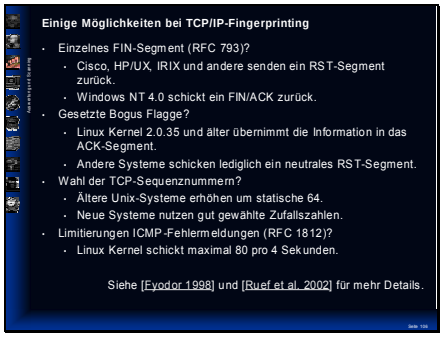
105



Betriebssysteme verwenden zur TCP/IP-Kommunikation einen sogenannten TCP/IP-Stack (dt. TCP/IP-Stapel). Dieser deckt die Palette der genutzten Protokolle ab, ist für die Verkapselung (engl. Encapsulation) und Codierung (engl. Encoding) dieser zuständig. Das Verhalten des Protokoll-Stapels unterscheidet sich dabei je nach Implementierung und Betriebssystem. Durch das TCP/IP-Fingerprinting (manchmal auch nur OS- oder Stack-Fingerprinting genannt) wird eine Analyse dieses Verhaltens umgesetzt, um das genutzte Betriebssystem zu ermitteln [McClure et al. 1998, Ruef et al. 2002]

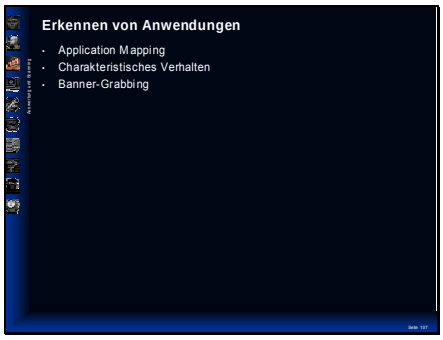
Eine der populärsten Lösungen zu diesem Zweck ist nmap (Network Mapper) von Fyodor, das ursprünglich für Linux entwickelt wurde, mittlerweile aber auch auf anderen Plattformen zur Verfügung steht. Dort kann mit dem Schalter –O das OS-Fingerprinting aktiviert werden. Verschiedene Tests werden sodann durchlaufen und das Betriebssystem mehr oder weniger präzise bestimmt [Fyodor 1997, 1998, Ruef 2000]. In obigem Beispiel wurde das OS-Fingerprinting auf ein aktuelles Microsoft Windows XP mit Service Pack 2 und (teilweise) aktivierter Internetverbindungsfirewall angesetzt.

106



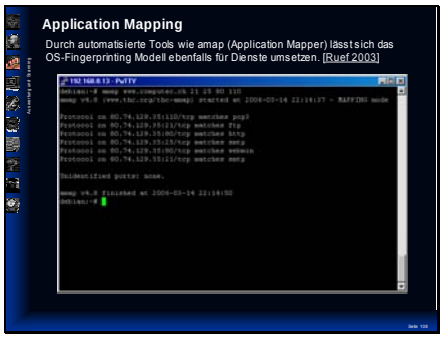
TCP/IP-Fingerprinting analysiert die Charakteristika des Verhaltens einer TCP/IP-Implementierung. Dazu werden teilweise fehlerhafte und fehlende Optionen eingesetzt, die je nach Produkt anders gehandhabt werden. Im Buch „Hacking Intern“ von Marc Ruef et al. [2002] werden die Analysetechniken von nmap im Detail besprochen.

107



Das Erkennen des Betriebssystems mittels OS-Fingerprinting kann ebenfalls auf (Netzwerk-)Anwendungen übertragen werden. Innerhalb des Application Mappings wird als erstes versucht zu erkennen, um was für eine Netzwerkapplikation es sich handelt, die an einen Port gebunden worde. So lässt sich meistens ermitteln, ob es sich beim Zielport um einen Web- oder einen Mailserver handelt. Das genutzte Protokoll (HTTP oder SMTP) kann so ebenfalls eruiert werden. Desweiteren kann anhand des chrakteristischen Verhaltens ein Applikations-Fingerprinting umgesetzt werden. Das Verfahren ist in seinen Grundzügen ähnlich wie jenes des OS-Fingerprintings. Zudem werden wir uns mit aktivem Banner-Grabbing auseinandersetzen, bei dem der Willkommens-Banner einer Netzwerkanwendung ausgewertet und damit Rückschlüsse auf die eingesetzte Software gemacht werden.

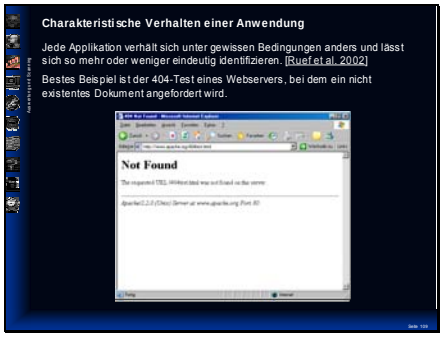
108



Unter Application Mapping wird gemeinhin die Technik verstanden, anhand des Verhaltens einer Netzwerkapplikation dessen Protokoll zu ermitteln. Die populärste Implementierung eines Tools, das diese Auswertung automatisiert, ist amap (Application Mapper) von THC (The Hackers Choice, http://www.thc.org/). Diese Software arbeitet, wie dies auch bei aktivem OS-Fingerprinting der Fall ist, mit dem Reiz/Reaktions-Schema. Hierbei baut die Anwendung eine Verbindung zum Zielport auf. Durch den Versand bestimmter Reize werden Reaktionen generiert, die wiederum ausgewertet werden. Jenachdem wie das Verhalten des Servers ausfällt, kann auf eine andere Netzwerkanwendung geschlossen werden. [Ruef 2003]

In obigem Beispiel wird ein amap-Zugriff auf den Host mit dem namen www.computec.ch umgesetzt. Als Zielports werden 21, 25, 80 und 110 definiert. Die Ausgabe zeigt deutlich, dass die Software in der Lage war, die Dienste zu erkennen (wenn auch nicht immer ganz exakt; Beispiel von Port 21 als ftp und smtp). In besagtem Mitschnitt ist zu sehen, dass jeweils die Empfehlungen der IANA befolgt wurde und die Dienste auf ihren well-known Ports angeboten wird.

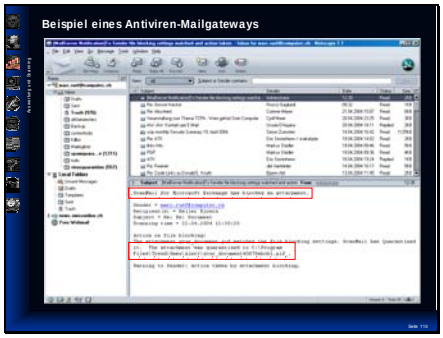
109



Das charakteristische Verhalten einer (Netzwerk-)Anwendung kann grundsätzlich herhalten, um das eingesetzte Produkt zu identifizieren. Jede Applikation verhält sich unter gewissen Bedingungen anders und lässt sich so mehr oder weniger eindeutig identifizieren. [Ruef et al. 2002]

Ein einfaches Beispiel ist im Web-Umfeld gegeben. Wird innerhalb einer Webseite auf ein nicht existentes Dokument zugegriffen, wird im Rahmen von HTTP eine 404 Not Found-Fehlermeldung ausgegeben. Diese weist den Benutzer darauf hin, dass die aufgesuchte Ressource nicht existiert. Viele Webserver-Implementierungen kommen mit Standard-Fehlermeldungen daher. Durch den bewussten Aufruf eines nicht existenten Dokuments kann nun die besagte Fehlermeldung provoziert werden. Die populäre Webserver-Implementierung von Apache pflegt Standard-Fehlermeldungen zu nutzen, in denen im Footer der Namen und die Versionsnummer des HTTP-Daemons angezeigt wird. Ideal, um weitere Nachforschungen zum am Zielsystem eingesetzten Produkt anzustellen.

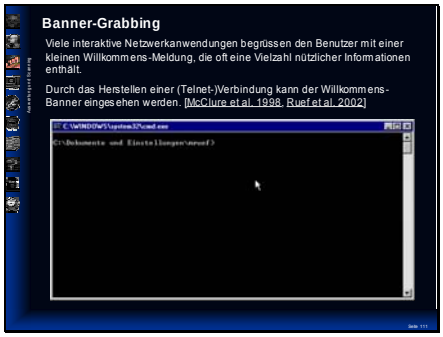
110



Ein anderes exemplarisches Verhalten ist im Mail-Bereich zu suchen. In diesem Beispiel wurde ein Email an einen Empfänger geschickt. Die Antiviren-Lösung des Empfängers hat im Anhang der Nachricht bösartigen Programmcode entdeckt, diesen in die Quarantäne verschoben und dem Absender eine Benachrichtigung zukommen lassen. Diese wird im Screenshot dargestellt. Wie zu sehen ist, kann im besagten Schreiben erkannt werde, um was für ein Produkt es sich dabei handelt. Hierbei wird scheinbar die kommerzielle Antiviren-Lösung ScanMail der Firma TrendMicro (http://www.trendmicro.com/) eingesetzt. Dies wird auf einem Microsoft Exchange Server genutzt. Einen Hinweis auf die Verzeichnis-Struktur des Exchange-Systems wird ebenfalls gegeben. Wie in der Pfad-Angabe zu sehen ist, wurde die Datei in einen Unterordner des Verzeichnisses „C:\Program Files\“ verschoben. Daran lässt sich zusätzlich erkennen, dass wohl die englische Version von Windows zum Einsatz kommt. Anhand der ausgewiesenen Scanning Time kann ebenfalls die Zeiteinstellungen auf dem Zielsystem erkannt und eventuell Rückschlüsse auf die geographische Positionierung des Hosts gemacht werden.

Dies alles sind Informationen, die für weitere Angriffe sehr nützlich sein könnten. Selbst die Sprachwahl auf dem Zielsystem kann von Nutzen sein. So ist es nämlich in seltenen Fällen gegeben, dass nur gewisse Sprachversionen eines Produkts von einem Fehler betroffen sind. Oder der Hinweis, dass ein Zielsystem in einem anderen Land mit einer anderen Zeitzone steht. Dies kann Social Engineering-Angriffe stützen und Attacken dann umsetzen lassen, wenn möglichst niemand in der Zielumgebung zugegen ist. Jede Information für einen Angreifer ist zu seinem Vorteil.

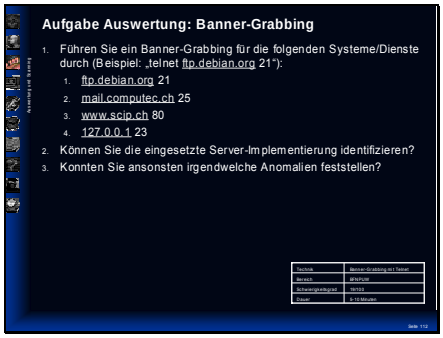
111



Viele interaktive Netzwerkanwendungen begrüssen den Benutzer mit einer kleinen Willkommens-Meldung, die oft eine Vielzahl nützlicher Informationen enthält. Durch das Herstellen einer (Telnet-)Verbindung kann der Willkommens-Banner eingesehen werden. [McClure et al. 1998, Ruef et al. 2002]

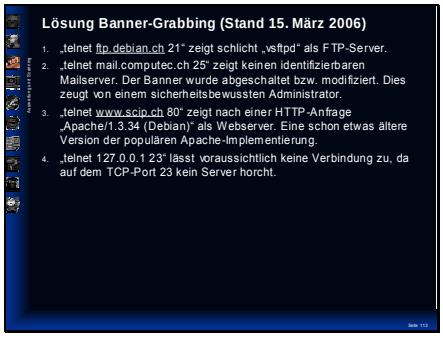
In diesem Beispiel wird mit der Terminal-Emulation Telnet eine Verbindung zum TCP-Port 25 des Zielsystems mit dem Hostnamen smtp.swissonline.ch hergestellt. Dies ist der SMTP-Port des Mailservers von Swissonline. Der Syntax von Telnet ist dabei einfach gehalten und setzt sich aus Programmaufruf, Zielsystem und Zielport zusammen: „telnet smtp.swissonline.ch 25“. Nach der Etablierung der Sitzung begrüsst uns der Mailserver mit dem Willkommens-Banner, in dem er den Namen und die Versionsnummer der eingesetzten Software propagiert. In diesem Beispiel handelt es sich um die populäre und für ihre Komplexität bekannte Sendmail-Implementierung.

112



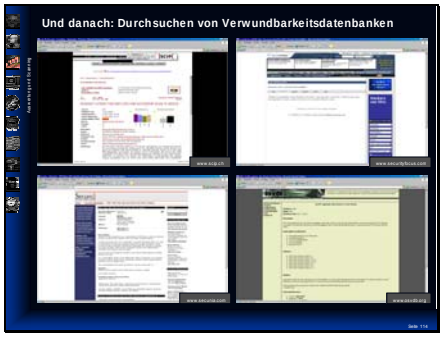
Beginnen Sie nun selber mit dem Umsetzen von aktivem Banner-Grabbing. Benutzen Sie dazu wie im vorangehenden Beispiel den Telnet-Client Ihres Betriebssystems. Auf diesen können Sie komfortabel in der MS DOS-Eingabeaufforderung zugreifen. Diese Öffnen Sie mit einem Klick auf den Start-Button der Startleiste, das Auswählen des Eintrags „Ausführen“ und der Eingabe von „cmd“. In der Kommandozeile können Sie sodann durch einen Aufruf in der Form von „telnet ftp.debian.org 21“ eine Telnet-Verbindung zu einem beliebigen TCP-Port umsetzen. Die Nummern in den Aufgaben geben an, auf welchen Zielport Sie sich verbinden sollen. Schauen Sie sich ansonsten nocheinmal das vorangehende Beispiel an, falls Ihnen das genaue Vorgehen nicht klar sein sollte.

113



Das Verhalten einer Netzwerkapplikation in Bezug auf ihren Banner ist stets unterschiedlich. Sowohl in den jeweiligen Implementierungen als auch nach entsprechenden Konfigurations-Eingriffen kann der Umfang und die Art der Meldungen ganz anders ausfallen. „telnet ftp.debian.ch 21“ zeigt schlicht „vsftpd“ als FTP-Server an. „telnet mail.computec.ch 25“ zeigt keinen identifizierbaren Mailserver. Der Banner wurde abgeschaltet bzw. modifiziert. Dies zeugt von einem sicherheitsbewussten Administrator. „telnet www.scip.ch 80“ zeigt nach einer HTTP-Anfrage „Apache/1.3.34 (Debian)“ als Webserver. Eine schon etwas ältere Version der populären Apache-Implementierung. „telnet 127.0.0.1 23“ lässt voraussichtlich keine Verbindung zu, da auf dem TCP-Port 23 kein Server horcht.

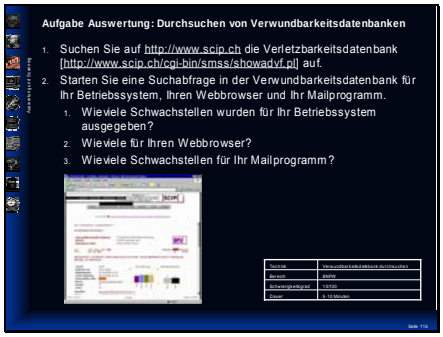
114



Konnte die auf dem Zielsystem eingesetzte Software erkannt werden, können Verwundbarkeitsdatenbanken durchsucht werden. In diesen werden bekannte Schwachstellen dokumentiert. Neben einer allgemeinen Beschreibung finden sich meistens auch weitere Hinweise dazu, wie die Schwachstelle ausgenutzt oder behoben werden kann. Angreifer können so schnell und komfortabel eine effektive Angriffsstrategie entwickeln, ohne selber weitläufige Analysen (z.B. Reverse Engineering) anstellen zu müssen.

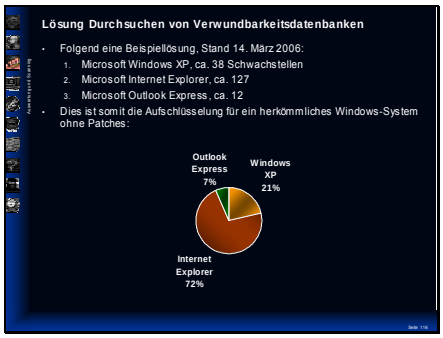
Die wohl bekannteste Verwundbarkeitsdatenbank wird unter http://www.securityfocus.com/bid/ bereitgestellt. Diese war eine der ersten Datenbanken, die vorwiegend die Meldungen aus der englischsprachigen Bugtraq-Mailingliste dokumentiert hat. Mit OSVDB (Open-source Vulnerability Database) wird unter http://www.osvdb.org/ eine quelloffene Datenbank für Verwundbarkeiten angeboten. In deutscher Sprache gehalten ist hingegen die scip_Verwundbarkeitsdatenbank der Schweizer Firma scip AG. Unter http://www.scip.ch/ werden umfassende Informationen zu alten und neuen Sicherheitslücken bereitgestellt.

115



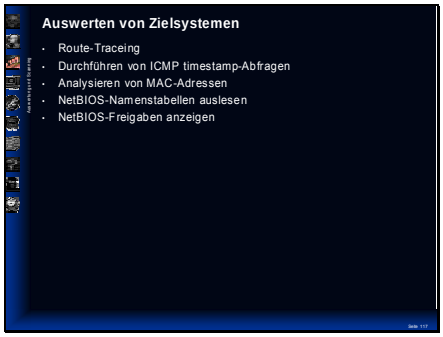
Sehen wir uns nun in dieser Übung den Umgang mit Verwundbarkeitsdatenbanken an. Als Beispiel nehmen wir die deutschsprachige Datenbank der scip AG, die über ein Web-Frontend verfügt. Auf der Webseite http://www.scip.ch/ finden Sie einen Link, der zu den Verwundbarkeiten führt. Sodann erhalten Sie eine Übersicht der aktuellen Schwachstellen des laufenden Monats. Oben links können Sie manuell das Jahr und den Monat wechseln. Seit Februar 2003 werden die Einträge täglich aktualisiert. Rechts oben finden Sie neben statistischen Auswertungen ebenfalls einen Link zur Such-Maske. Sobald sich diese geöffnet hat, können Sie anhand von Comboboxen und Textfeldern nach Schwachstellen suchen. Führen Sie nun dank den jeweiligen Suchabfragen die Aufgabe durch und ermitteln Sie die dokumentierten Schwachstellen zu der von Ihnen eingesetzten Software. Wieviele Sicherheitslücken sind für diese festgehalten?

116



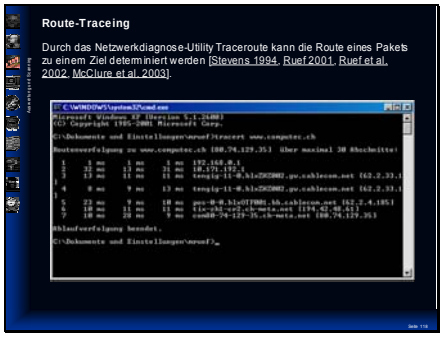
Die Lösung der Übung zu Verwundbarkeitsdatenbanken ist sowohl vom aktuellen Stand der Forschung als auch von der jeweiligen Suche abhängig. Es ist zu beobachten, dass Schwachstellen in den Windows-Betriebssystemen, im Linux Kernel, im Microsoft Internet Explorer und in Mozilla Firefox am meisten vorhanden sind.

117



Es gibt eine Vielzahl weiterer Möglichkeiten, wie ein Zielsystem samt seiner Umgebung ausgewertet werden kann. Wir werden uns nachfolgend die populärsten Techniken anschauen. Durch das Route-Traceing werden wir ein Zugriffspfaddiagramm erstellen, mit dessen Hilfe wir die Route zum Ziel und etwaige Sicherheitselemente (z.B. Firewall) erkennen können. Mit dem Durchführen von ICMP timestamp-Anfragen werden wir mit der Hilfe des ICMP-Protokolls die Uhrzeit am Zielsystem ablesen. Mit der Analyse von MAC-Adressen können wir den Hersteller einer Netzwerkkarte ermitteln und damit die Architektur des Zielsystems ableiten. Und zum Schluss wollen wir uns noch das in Windows-Umgebungen gern eingesetzte Auswerten von NetBIOS diskutieren. Durch das Auslesen von Namenstabellen versuchen wir erweiterte Informationen über ein Windows-System zu erlangen und mit dem Scannen von NetBIOS-Freigaben lassen sich freigegebene Ressourcen entdecken.

118

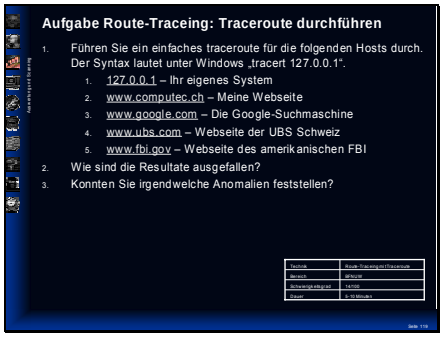


Traceroute ist der Name eines populären Netzwerkdiagnoseutilities, das Teil vieler moderner Betriebssysteme mit Netzwerkunterstützung ist. Durch diese Software kann die Route zu einem Ziel ermittelt und damit ein Zugriffspfaddiagramm erstellt werden. Traceroute schickt dazu jeweils ein Paket mit einem sehr niedrigen TTL-Wert (Time-to-Live) an das Zielsystem. Ein jedes Zwischensystem, auch Hop genannt, muss nach der Weitergabe des Pakets den TTL-Wert mindestens um 1 dekrementieren. Erreicht die TTL eines IP-Pakets den Wert 1, sollte der aktuelle Hop das Paket verwerfen und eine ICMP exceeded-Fehlermeldung (Typ 11) an das Quell-System zurückschicken. So kann theoretisch von jedem Hop eine Meldung provoziert und damit die Route des Pakets bestimmt werden. Bei einem Traceroute verschickt sodann der finale Zielhost hingegen eine ICMP Destination unreachable Port unreachable-Fehlermeldung (Typ 3, Code 3). Das Traceroute-Utility weiss nun, dass das Ziel erreicht wurde. [Stevens 1994, Ruef 2001, Ruef et al. 2002, McClure et al. 2003]

Unter UNIX/Linux kann Traceroute normalerweise mit der Eingabe von „traceroute“ genutzt werden. Bei Windows-Systemen ist das zeilenorientierte Utility über „tracert.exe“ zu erreichen. In diesem Beispiel wird mit der Eingabe von „tracert www.computec.ch“ ein Route-Traceing für das System mit dem Hostnamen www.computec.ch umgesetzt. Nach einer IP-Adressauflösung wird das eigentliche Zugriffspfaddiagramm erstellt. Auf einer jeden Zeile wird der Name bzw. die IP-Adresse des Hops angegeben. Im Beispiel mit erfolgreichem Ablauf sind insgesamt 7 Systeme vermerkt.

Kann die Ablaufverfolgung nicht erfolgreich umgesetzt werden, weil ein Hop zum Beispiel vom Absetzen der ICMP-Fehlermeldungen absieht (z.B. eine Firewall ohne ICMP-Unterstützung), wird dies durch Sterne angezeigt. Der TTL-Wert wird sodann um 1 erhöht und das Paket erneut verschickt. Dies wird solange wiederholt, bis der Zugriff entweder erfolgreich verlaufen ist oder die maximale Anzahl von 30 erreicht wurde. Ein Traceroute-Zugriff kann sowohl unter Linux als auch Windows mit der Escape-Sequenz Ctrl+C abgebrochen werden.

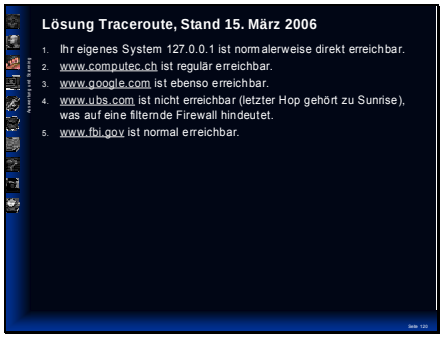
119



Führen Sie nun selber Route-Traceings mit der Hilfe des Traceroute-Utilities durch. Das zeilenbasierte Netzwerkdiagnoseutility kann unter Windows einmal mehr am besten in der MS DOS-Eingabeaufforderung genutzt werden. Klicken Sie dazu auf den Start-Button der Startleiste, wählen Sie dort den Menü-Punkt Ausführen und geben Sie in das Textfeld „cmd" ein. Sodann öffnet sich ein Fenster, in dem Sie beispielsweise durch die Eingabe von „tracert www.computec.ch" einen Traceroute-Zugriff auf das System mit dem Hostnamen www.computec.ch umsetzen können.

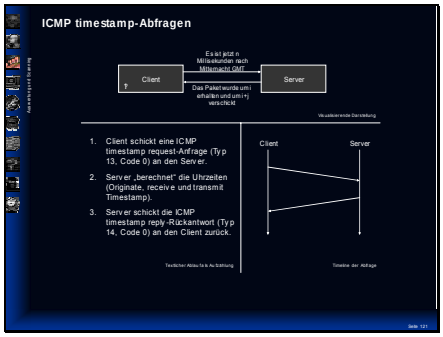
Als Ziel der Übung ist die Loopback-Adresse 127.0.0.1 Ihres lokalen Systems, meine Webseite www.computec.ch, die Suchmaschine www.google.com, mit www.ubs.com die Webseite der UBS Schweiz und mit www.fbi.gov der Webauftritt der amerikanischen Bundespolizei FBI vorgegeben. Notieren Sie sich die Resultate und etwaige Anomalien.

120



Bei den gegebenen Traceroute-Aufgaben ist wiederum das Resultat von der jeweiligen Implementierung abhängig. Migrationen in der Zielumgebung (z.B. Anpassungen des Routings oder der Firewall-Regeln) können zu komplett anderem Verhalten führen. Der Effekt eines Traceroute-Zugriffs auf die Loopback-Adresse 127.0.0.1 verhält sich jedoch immer gleich. Der Erfolg ist stets gegeben, da ein lokaler Zugriff umgesetzt wird. Erreichbare Systeme werden in der Regel nach einigen Hops (ca. 10 im Schnitt im Internet) identifiziert. Verschickt ein Hop oder das Endsystem keine ICMP-Fehlermeldungen, wird dies durch Sterne gekennzeichnet. Dabei kann es durchaus sein, dass nur einzelne Hops, oftmals Firewall-Elemente, so ausgewiesen werden.

121

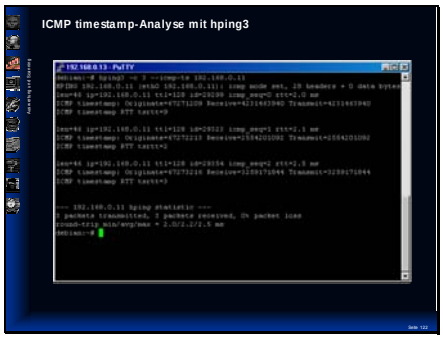


Für einen Angreifer kann das Wissen um die Zeiteinstellungen auf dem Zielsystem sehr nützlich sein. So kann daraus zum Beispiel geschlossen werden, in welcher Zeitzone und damit in welcher geographischen Region sich der Host befindet. Damit können Angriffe besser koordiniert werden. Wobei bei Social Engineering-Attacken der Zugriff möglichst dann erfolgen sollte, wenn jemand in der Zielumgebung zugegen ist, kann genau der umgekehrte Effekt bei rein technischen Angriffen erwünscht sein. Nämlich den Zugriff genau dann durchzuführen, wenn mit grösster Wahrscheinlichkeit keiner der Administratoren Zugriff auf die Log-Dateien hat und die Attacke erkennen könnte.

Die klassische Methode zur Determinierung der Zeit eines netzwerkfähigen Systems ist mit ICMP timestamp gegeben. Das ICMP-Protokoll bietet auf der Basis des Client/Server-Prinzips die Möglichkeit, dass eine ICMP timestamp request-Anfrage (Typ 13, Code 0) an das Zielsystem geschickt wird. Dieses vergleicht die eigene Uhrzeit mit derjenigen der Anfrage (originate), analysiert den Zeitpunkt des Erhalts der Nachricht (receive) und generiert seinen eigenen Zeitstempel (transmit). Sodann wird eine ICMP timestamp reply-Rückantwort (Typ 14, Code 0) an das Quellsystem zurückgeschickt. [Comer 1995]

Wie bei vielen ICMP-Auswertungstechniken ist auch hier die grösste Gefahr, dass derartiger Netzwerkverkehr durch ein Firewall-System limitiert wird. Vor allem ICMP timestamp wird gerne abgeschaltet, da es eigentlich keinem produktiven Einsatz dienlich ist. So ist es auch oftmals gegeben, dass die jeweiligen Endsysteme die Verarbeitung dieses ICMP-Typs gar nicht unterstützen. Eine Auswertung ist in diesem Fall nicht möglich.

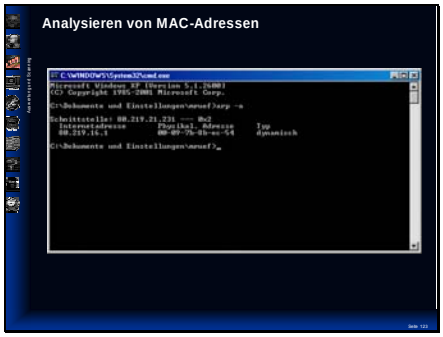
122



Wir wollen hier exemplarisch das Durchführen von ICMP timestamp-Auswertungen mit dem open-source Utility hping3 illustrieren. Dieses zeilenbasierte Tool verhält sich in diesem Zusammenhang sehr ähnlich wie die gängigen Implementierungen des Ping-Kommandos. Durch den Schalter –c kann die Anzahl der zu verschickenden ICMP timestamp request-Anfragen definiert werden. In diesem Beispiel haben wir 3 eingesetzt. Durch das Argument --icmp-ts definiert sich der Typ der Anfragen (ICMP TimeStamp). Und zum Schluss folgt die IP-Adresse des Zielsystems, an das die Pakete geschickt werden soll.

Das gänzliche Verhalten des Zugriffs unterscheidet sich nur in gewissen Punkten von demjenigen eines herkömmlichen Ping-Zugriffs. So werden die statistischen Anzeigen eines jeden erfolgreichen ICMP timestamp-Zugriffs ausgewiesen. In den jeweiligen Zeilen findet sich die Originate, Receive und Transmit-Zeitstempel der jeweiligen Pakete. Diese Werte zeigen stets die Millisekunden seit Mitternacht GMT an.

123

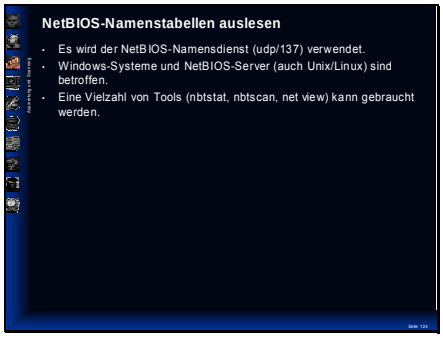


Eine MAC-Adresse (Media Access Control, auch LAN-Adresse, Ethernet-ID oder bei Apple Airport-ID genannt) ist eine weltweit eindeutige Hardware-Adresse einer Netzwerkschnittstelle. Anhand dieser, bestehend aus 48 bit, kann eine Identifikation des jeweiligen Geräts in einem Netzwerk umgesetzt werden. Die Auflösung von MAC-Adressen und IP-Adressen findet dabei durch das Address Resolution Protocol (ARP) statt. [Stevens 1994, Comer 1995]

Durch das Kommando arp, das Teil eines jeden netzwerkfähigen Betriebssystems ist, kann Zugriff auf den lokalen ARP-Cache ausgeübt werden. In diesem werden temporär sämtliche MAC-Adressen mit dazugehöriger IP-Adresse gespeichert. Damit will ein mehrmaliges Auflösen einer Adresse in kurzer Zeit und damit die erweiterte Belastung des Netzwerks verhindert werden. Mit dem Schalter –a kann der Inhalt der aktuellen ARP-Tabelle ausgegeben werden. Sodann finden sich sämtliche Hosts (mit IP- und MAC-Adresse), zu denen in letzter Zeit eine Verbindung hergestellt wurde. Diese Vorgehensweise kann auch bei einer erweiterten Mapping-Analyse hilfreich sein.

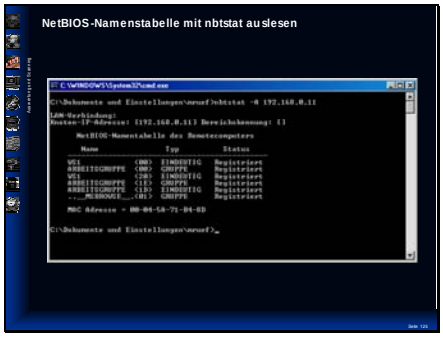
Das erste Bit einer MAC-Adresse gibt an, ob es sich um eine Einzeladresse oder Gruppenadresse handelt. Das folgende Bit 46 zeigt an, dass die MAC-Adresse global eindeutig ist oder lokal administriert wird und nur dort eindeutig ist. Die folgenden 22 Bits (Bits 45 bis 24) beschreiben eine von der IEEE vergebene Herstellerkennung (auch OUI - Organisation Unique Identifier genannt). Unter http://anonsvn.ethereal.com/ethereal/trunk/manuf wird eine Liste der vordefinierten MAC-Adressbereiche publiziert. Darin ist sehr schön zu erkennen, welche Hersteller welche Adressen zugeteilt bekommen haben. Anhand dieser Information lässt sich unter Umständen die Architektur des Zielsystems identifizieren und auf typische Installationen schliessen (z.B. wird eine Intel-Karte wohl eher weniger in einer SPARC-Umgebung von Sun Microsystems Ihren Einsatz finden).

124



NetBIOS wurde 1983 bei der Firma Sytec, Inc. im Auftrag von IBM für das IBM PC Network, einer proprietären Hardwarelösung zur Vernetzung kleiner Arbeitsgruppen, entwickelt. NetBIOS erlaubt einer Applikation, einen 16 Zeichen langen Namen netzwerkweit zu registrieren. Diese Technologie wurde vor allem durch Microsoft in Windows vorangetrieben. Durch verschiedene Tools ist es möglich, Informationen zu einem Host über NetBIOS auszulesen. Dabei wird auf den NetBIOS-namensdienst, der auf UDP-Port 137 angeboten wird, zurückgegriffen.

125



In diesem Beispiel wird mit dem Diagnoseutility nbtstat eine entsprechende Auswertung vorgenommen. Die besagte Software ist Teil moderner Windows-Systeme (seit Windows 95) und wird in der Kommandozeile ausgeführt. Hierbei wird durch das Nutzen des Schalters –A ein Zugriff über die IP-Adresse auf ein Remote-System angesetzt. Als Zieladresse wird im Beispiel 192.168.0.11 eingegeben. [Ruef et al. 2002]

In der Ausgabe ist sehr schön zu sehen, wie der NetBIOS-Hostname, der Name der Arbeitsgruppe und die MAC-Adresse ausgelesen werden können. Die ersten beiden Informationen sind oftmals ein wichtiger Teil von expliziten NetBIOS-Attacken. Angreifer sind deshalb gerne darum bemüht, diese Informationen vor dem effektiven Angriff (z.B. SMBdie) in Erfahrung zu bringen. Die MAC-Adresse kann wiederum für Auswertungen herhalten. Bei einem solchen Zugriff bleibt jedoch interessant, dass nun eben halt die MAC-Adresse auch über verschiedene Netzwerke hinweg in Erfahrung gebracht werden kann, was ansonsten nur in lokalen Netzen vorbehalten bleibt.

Eine Information, die in diesem Beispiel nicht auftaucht, ist der Benutzername jenes Anwenders, der gerade auf dem Zielsystem eingeloggt ist. Diese wäre von erhöhter Wichtigkeit, kann sie doch für weitere technische (z.B. Bruteforce-Attacke auf ein Netzwerk-Konto) und psychologische Angriffe (z.B. Phishing) herangezogen werden.

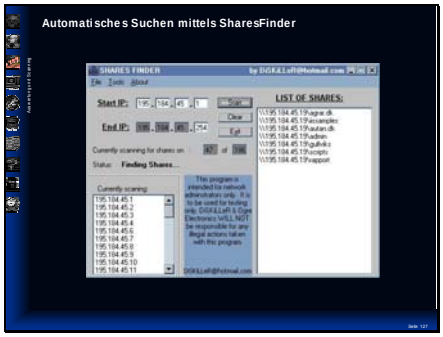
126



In Windows-Umgebungen bleibt das Auswerten von NetBIOS-Freigaben ebenfalls wichtig. Mit solchen können Ressourcen eines Systems über das Netzwerk angeboten werden. Neben Drucken lassen sich so auch Verzeichnisse und Datenträger freigeben. Sehr einfach können die Freigaben eines Systems innerhalb des Explorers von Windows identifiziert werden. Dabei steuert man lediglich eine Adresse in der Form von \\127.0.0.1 an, wobei ebenfalls mit (NetBIOS-)Hostnamen gearbeitet werden kann.

Sind Freigaben vorhanden, werden diese entsprechend im Browser angezeigt, so als seien diese Teil eines lokalen Datenträgers. Ist der NetBIOS/SMB-Dienst am Zielsystem angeboten aber keine Freigaben getätigt worden, wird der Inhalt des Browsers einfach leer dargestellt. Ist der Dienst hingegen gar nicht vorhanden, wird der Browser eine Fehlermeldung ausgeben.

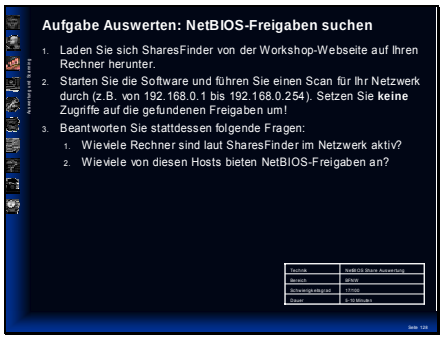
127



Es gibt eine Vielzahl an Tools, mit denen ganze IP-Adressbereiche nach NetBIOS-Freigaben abgesucht werden können. Ein kleines und handliches Utility wird mit der Freeware SharesFinder angeboten. Diese Software für Microsoft Windows lässt in der letzten Version das Absuchen eines ganzen Klasse C-Netzwerks (also 256 IP-Adressen) zu.

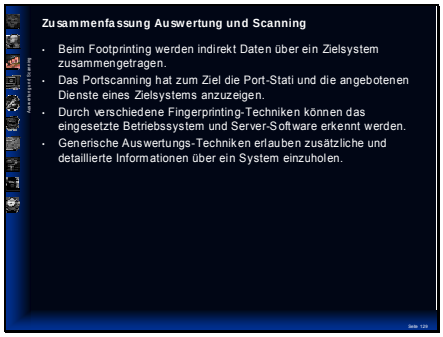
In diesem Beispiel wird der öffentliche Bereich 195.184.45.1 bis 195.184.45.254 überprüft. Als erstes sucht das Programm mittels Mapping nach erreichbaren Systemen im Zielbereich. Danach wird Versucht im Rahmen von NetBIOS eine Verbindung aufzubauen und die Freigaben (engl. Shares) auszulesen. Diese werden sodann in der rechten Textbox aufgelistet und können nun komfortabel angesteuert werden.

128



Wir wollen uns in dieser Aufgabe mit der Handhabung von SharesFinder vertraut machen. Laden Sie dazu die Software von der Workshop-Webseite auf Ihren Rechner herunter. Die ZIP-Datei entpacken Sie in ein Verzeichnis Ihrer Wahl. Danach öffnen Sie das Verzeichnis und starten die EXE-Datei. Das grafische Utility wird sodann gestartet. Geben Sie nun den Zielbereich ein, den sie nach Freigaben absuchen wollen. Sollte die IP-Adresse Ihres Rechners beispielsweise 192.168.0.23 lauten, dann führen Sie doch einen Scan auf das ganze Klasse C-Netzwerk 192.168.0.1 bis 192.168.0.254 durch. Setzen Sie danach keine Zugriffe auf die gefundenen Ressourcen um. Beantworten Sie stattdessen die Fragen, wieviele Rechner laut SharesFinder als aktiv identifiziert wurden und welche von Ihnen NetBIOS-Freigaben anbieten.

129

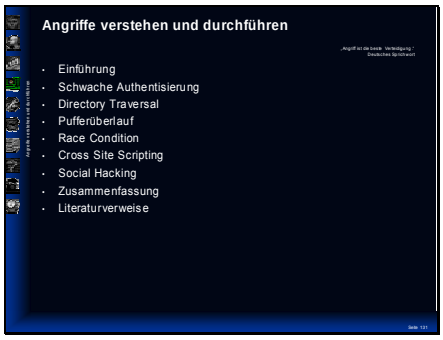


Zu Beginn eines professionellen Angriffs wird ein Angreifer stets möglichst viele Informationen über die Zielumgebung in Erfahrung bringen. Dadurch sollen weitere Auswertungen und Attacken möglichst effizient vorbereitet und durchgeführt werden. Durch das indirekte Sammeln von Daten, dies wird als Footprinting bezeichnet, können oftmals sehr viele Details zusammengetragen werden. Internet-Suchmaschinen spielen dabei eine wichtige Rollen. Durch das Portscanning werden die Port-Stati und damit die von einem Zielsystem angebotenen Dienste identifiziert. Es gibt verschiedene Techniken, wie derartige Scan-Zugriffe ausgeführt werden können. Die jeweiligen Fingerprinting-Zugriffe erlauben es einem Angreifer, das auf dem Zielsystem eingesetzte Betriebssystem sowie die genutzte Software (z.B. Server-Versionen) zu identifizieren. Dies ist sehr wertvoll, um zielgerichtet vorzugehen. Und generische Auswertungs-Techniken wie ICMP timestamp-Abfragen oder NetBIOS-Auswertungen können weitere Angriffspunkte identifizieren.

130

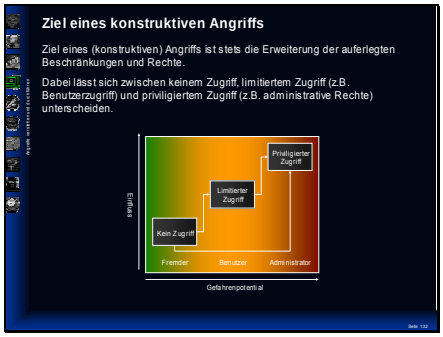


131



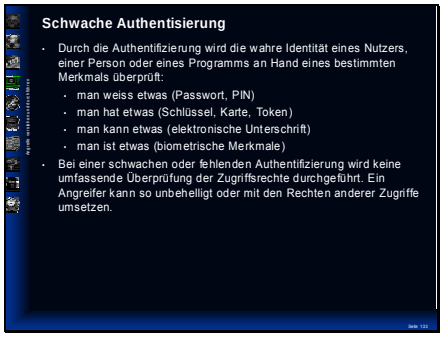
Nachdem wir uns nun primär mit der Vorbereitung eines Angriffs - der Auswertung der Zielumgebung - beschäftigt haben, wollen wir nun Attacken im Detail diskutieren. Dabei werden wir uns auf populäre Techniken, die wir ohne exotische Methoden und Besonderheiten illustrieren wollen, beschränken. Schwache Authentisierungen, Directory Traversal, Pufferüberlauf-Attacken, Race Conditions und Cross Site Scripting sind Angriffstechniken, die auf technischer Ebene realisiert werden. Zum Schluss wollen wir aber nocheinmal die psychologischen Aspekte von Attacken in der Form von Social Hacking besprechen.

132



Ziel eines (konstruktiven) Angriffs ist stets die Erweiterung der auferlegten Beschränkungen und Rechte. Dabei lässt sich zwischen keinem Zugriff, limitiertem Zugriff (z.B. Benutzerzugriff) und priviligiertem Zugriff (z.B. administrative Rechte) unterscheiden.

133



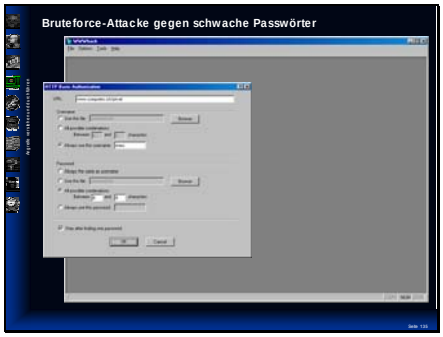
Schwache Authentisierungen sind die wohl bekannteste Schwachstelle von IT-Systemen. Durch die Authentifizierung wird die wahre Identität eines Nutzers, einer Person oder eines Programms an Hand eines bestimmten Merkmals überprüft (z.B. Passwort). Bei einer schwachen oder fehlenden Authentifizierung wird keine umfassende Überprüfung der Zugriffsrechte durchgeführt. Ein Angreifer kann so unbehelligt oder mit den Rechten anderer Zugriffe umsetzen.

134



Zu Beginn des neuen Milleniums war besonders das Fehlen von Passwort-Schutz bei NetBIOS-Freigaben innerhalb von Windows ein grosses Problem. Durch das Scannen von NetBIOS-Freigaben im Internet konnte innert Minuten Zugriff auf eine Vielzahl an ungeschützten Systemen erlangt werden [Ruef 2001]. Teilweise waren ganze Festplatten ohne Passwort-Schutz freigegeben und über das Internet zugreifbar. Eine Manipulation der Daten (z.B. Löschen) oder das Auslesen dieser (z.B. Lebenslauf oder weitere Passwörter) sind sodann im Rahmen der NetBIOS-Kommunikation nur einige Klicks zusätzlicher Aufwand. Durch ein angepasstes Freigabe-System seit Microsoft Windows XP und Server 2003 wurde dieses Problem weitestgehend eingeschränkt. Freigaben ohne Passwort sind nicht mehr ohne weiteres möglich.

135

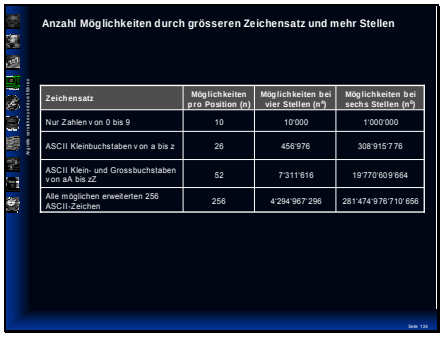


Im Internet sind eine Vielzahl an Tools erhältlich, die automatisiert einen Angriff auf Passwort-Authentisierungen umsetzen können. Sogenannte Bruteforce-Tools probieren nacheinander sämtliche möglichen Zeichenkombinationen aus, bis sie das richtige Passwort gefunden haben. Ein solcher Angriff ist zeitaufwendig aber dafür primitiv. Dies bedeutet, dass ein jeder, der die Software bedienen kann, die Attacke zu starten in der Lage ist.

Gerade weil eine Bruteforce-Attacke so zeitaufwendig ist und sowie die meisten Benutzer schwache Passwörter einsetzen, wird auf Wörterbuch-Attacken (engl. Dictionary Attacks) ausgewichen. Anstatt wie bei einer Bruteforce ein Passwort auf sämtliche Zeichenkombinationen hin zu überprüfen, wird mit Wortlisten gearbeitet. In diesen finden sich die bekanntesten Wörter einer natürlichen Sprache (z.B. Deutsch oder Englisch). Benutzt nun ein Anwender ein Wort, das im alltäglichen Sprachgebrauch vorkommt (z.B. der Name der Freundin), dürfte das Passwort sehr schnell gefunden werden.

In diesem Beispiel wird eines der bekanntesten Bruteforce-Utilities abgebildet. Die Windows-Software WWWhack (http://www.computec.ch/download.php?view.459) ist darauf ausgelegt, Passwörter im World Wide Web zu knacken. Vor allem der Angriff auf htaccess-Passwortabfragen war damit sehr beliebt. Aber auch Formular-Authentisierungen innerhalb von HTML, wie sie beispielsweise auch bei vielen Web-Freemailern (Hotmail und GMX) angeboten werden, sind damit möglich. Die Software wurde aber seit vielen Jahren nicht mehr weiterentwickelt. Sie kränkelt zudem an einer schlechten Performance und Instabilität während der Ausführung. Aus diesem Grund werden heutzutage Attacken gerne mit anderen Tools initiiert.

136

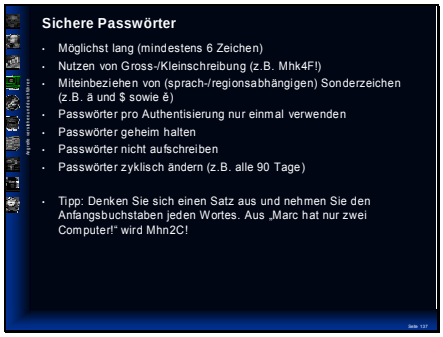


Die Zeitdauer, die eine erfolgreiche Bruteforce-Attacke benötigt, ist von der Stärke des eingesetzten Passworts abhängig. Die Stärke eines Passworts definiert sich durch seine Komplexität. Die Länge, die Anzahl der verschiedenen Zeichen sowie eine möglichst hohe Entropie bei der Wahl dieser machen die Komplexität eines Passworts aus [Müller 2004]. In dieser Tabelle wird aufgezeigt, wie sich die Komplexität eines Passworts berechnen lässt und wie ein exponentieller Wachstum in der Stärke umgesetzt werden kann.

Die Berechnung ist sehr einfach. Nehmen wir ein Beispiel einen PIN, der lediglich aus nummerischen ganzen Zahlen bestehen kann. Ein einstelliger PIN kann entsprechend 10 Zustände einnehmen, wobei die Ziffern 0, 1, …, 9 eingesetzt werden können. Erweitern wir die Länge des PINs auf vier Stellen, dann haben wir 10^4 Möglichkeiten für ein Passwort. Dies macht schon 10‘000 mögliche Passwörter aus. Bei sechs Stellen sind dies gar eine Million möglicher Passwörter (10^6).

Durch das Einbringen von Buchstaben lässt sich die Möglichkeiten pro Position steigern. Werden lediglich Kleinbuchstaben des englischen Alphabets [a-z] eingesetzt, sind 26 unterschiedliche Zustände pro Position möglich. Bei vier Stellen haben wir somit die Anzahl von 456‘976 möglichen Passwörtern. Das sind 45,69 mal mehr mögliche Passwörter, weder wenn wir lediglich Zahlen von 0 bis 9 einsetzen würden. Erweitern wir den Zeichensatz noch um die Grossschreibung [aA-zZ], haben wir bei vier Stellen sogar 7‘311‘616 mögliche Passwörter. Dies sind wiederum 16 Mal mehr weder zuvor.

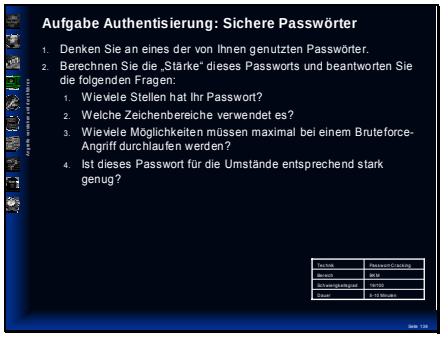
137



Wir können also zusammenfassen, dass sichere Passwörter möglichst lang sind. Vier Stellen sind dabei eindeutig zu wenig. Sechs oder gar acht Stellen sind wünschenswert. Es sollen nicht nur Ziffern sonder auch alphanummerische Zeichen samt Gross-/Kleinschreibung zum Einsatz kommen. Dies erweitert den Schlüsselraum enorm. Durch das Miteinbeziehen von sprach- und regionsabhängigen Sonderzeichen – sofern vom Produkt unterstützt – erweitert ebenfalls die Anzahl für mögliche Sonderzeichen. Zudem werden aber auch viele Cracking-Utilities unnütz gemacht. Denn diese können oftmals nur mit einem englischen Zeichensatz umgehen. Umlaute oder das scharfe S sind sodann unknackbar für derartige Tools. Die Wahl eines komplexen Passworts, das sich zudem einfach merken lässt, ist nicht immer einfach. Denken Sie sich am besten einen Satz aus und nehmen Sie den Anfangsbuchstaben jeden Wortes. Aus „Marc hat nur zwei Computer!“ wird Mhn2C! [Müller 2003]

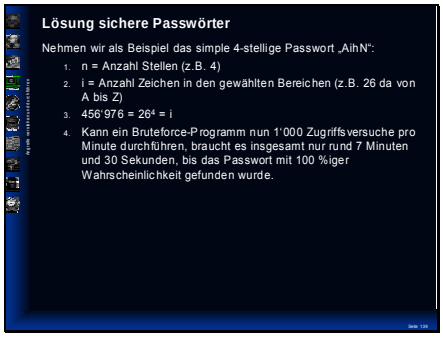
Durch das Verwenden verschiedener Passwörter kann verhindert werden, dass nach dem erfolgreichen Herausfinden oder Brechen eines solchen ebenfalls andere Authentisierungs-Mechanismen überlistet werden können. Das Geheimhalten eines Passworts ist natürlich Pflicht, damit Dritte nicht unerlaubten Zugang erlangen können. Indem man Passwörter nicht aufschreibt, kann man den Verlust oder die Einsicht dieser durch andere verhindern. Durch das zyklische Ändern der Passwörter können gebrochene wieder hergestellt werden. Die Lebenszeit eines Passworts ist je nach Einsatzgebiet abhängig. Eine Anpassung alle 90 Tage ist im alltäglichen Einsatz jedoch ein guter Mittelwert.

138



Denken Sie nun an eines der von Ihnen im täglichen Einsatz genutzten Passworts. Zum Beispiel an jenes Ihres Windows- oder Mail-Kontos (z.B. Hotmail oder GMX). Berechnen Sie nun die Stärke dieses Passworts und beantworten Sie die Fragen der Aufgabe. Anhand dieser sollten Sie überschlagen können, ob das von Ihnen eingesetzte Passwort als stark gilt und somit als sicher klassifiziert werden kann.

139



Nehmen wir als Beispiel das relativ simple Passwort „AihN“. Dieses besteht nur aus 4 Stellen. Als Zeichensatz kommen Buchstaben mit Gross-/Kleinschreibung des englischen Alphabets zum Einsatz. Die Anzahl der möglichen Passwörter mit diesem Zeichensatz ist 26^4, was insgesamt 456‘976 verschiedene Passwörter ausmacht. Kann man nun mit einem Bruteforce-Programm 1‘000 Zugriffsversuche pro Minute durchführen, braucht man nur rund 7 Minuten und 30 Sekunden, bis das Passwort mit 100 %iger Sicherheit gefunden wurde. Statistisch kann man aber sagen, dass das Bruteforce-Cracking nur die Hälfte der Zeit benötigt, da die Analyse des 50 % des Schlüsselraums ausreichen, um das Passwort zu identifizieren.

Der Test auf 1‘000 Passwörter pro Minute ist hierbei lediglich ein Beispiel. Bei Angriffsversuchen über ein Netzwerk ist die Anzahl der Zugriffe von der Auslastung der Ressourcen und der Latenzzeit der Kommunikation abhängig. Mindestens 2 Zugriffe pro Sekunde – also 120 pro Minute - sollten aber möglich sein. Bei lokalen Attacken sind aber weitaus mehr als 1‘000 Zugriffe pro Minute denkbar. Da muss sogar mit mehreren 10‘000 gerechnet werden. Ein schwaches Passwort kann also beim Offline-Cracking meist noch viel schneller herausgefunden werden.

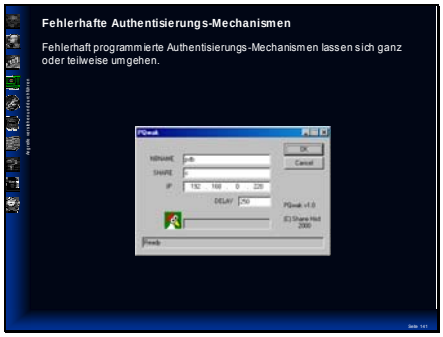
140



Die Wahl schwacher Passwörter ist aber nicht die eigentliche Todsünde, die im Rahmen von Authentisierungen zum Tragen kommen kann. Viel schlimmer sind sogenannte Standardkonten oder Standardpasswörter. Viele Hersteller geben ihre Produkte, egal ob nun Software oder Hardware, mit Standardkonten heraus. Diese sind stets gleich und erlauben es bei der Inbetriebnahme, schnell und unkompliziert das Produkt einsetzen zu können. [McClure et al. 1998]

Viele Anwender und Administratoren vergessen oder übersehen jedoch, dass das Bestehenbleiben derartiger Standardeinstellungen ein enormes Sicherheitsrisiko darstellt. Angreifer sind sich dessen bewusst, dass vielerlei Produkte mit Standardkonten ausgeliefert werden. Durch umfassende und aktuelle Listen, die im Internet verfügbar sind, können so Attacken auf derartige Fehlkonfigurationen eingeleitet werden. Die Tabelle zeigt einen kleinen Auszug derartiger Standardeinstellungen. Besonders beliebt sind identische Benutzernamen und Passwörter. Eine akkurate und aktuelle Liste wird unter http://www.phenoelit.de/dpl/dpl.html bereitgestellt.

141



Ein weiteres Problem von Authentisierungs-Mechanismen ist in einer fehlerhaften Implementierung gegeben. In solchen Fällen ist es dann plötzlich unwichtig, ob ein Benutzer nun Standardkonten angepasst und möglichst starke Passwörter eingesetzt hat. Ein gutes Beispiel war bei Microsoft Windows 98 und NT 4.0 gegeben. Dort konnte wegen einer fehlerhaften Implementierung in der Passwort-Authentisierung von NetBIOS-Freigaben besonders effektiv eine Bruteforce-Attacke umgesetzt werden. Das Problem bestand darin, dass jeder Buchstabe des Passworts einzeln auf seine Richtigkeit hin überprüft werden konnte. Dies versprach dem Angreifer einen enormen Geschwindigkeitsvorteil. Innert weniger Minuten war so ein jedes Passwort geknackt. [Ruef 2001]

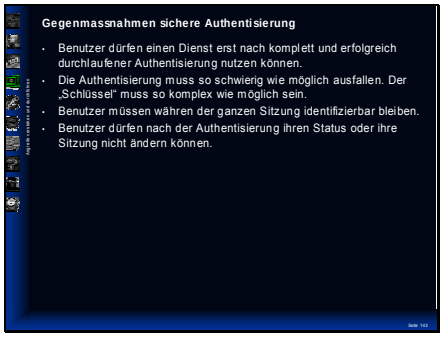
142



Die Authentisierung mittels Benutzername und Passwort gilt als relativ schwach. Aus diesem Grund wurden eine Vielzahl alternativer Authentisierungs-Mechanismen entwickelt. Im Online-Banking wird zunehmends der Einsatz eines Tokens populärer. Dabei wird mit einer Lösung wie RSA SecurID auf einer kleinen Karte eine Zufallszahl generiert, die neben dem Benutzernamen und Passwort als dritte Komponente ihren Einsatz findet. Ein Angreifer kann ohne den Besitz des Tokens und damit das Wissen der Geheimzahl keine erfolgreiche Authentisierung umsetzen.

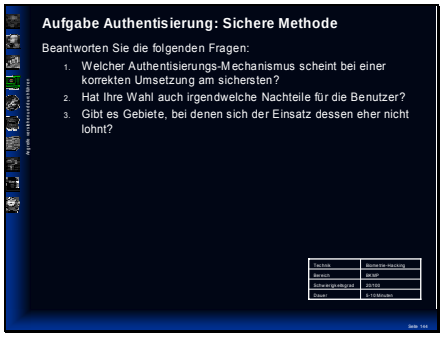
Eine preisgünstige und umfangreicher einsetzbare Technologie ist in den Chipkarten gegeben. Durch intelligente Prozessorkarten (engl. Smartcards) kann ebenfalls auf der Basis eines Tokens eine strenge Authentisierung umgesetzt werden. Der Angreifer muss sich wiederum im Besitz eines besonderen Geräts befinden. Da diese aber verloren gehen oder gestohlen werden können, sind biometrische Merkmale zunehmends im Gespräch für den breitflächigen Einsatz. Durch Fingerabdruck oder Gesichtserkennung soll eine Person eindeutig identifiziert und damit eine strenge Authentisierung realisierbar sein. Datenschützer fürchten in diesem Zusammenhang aber den Verlust der Privatsphäre [Ruef 2005].

143



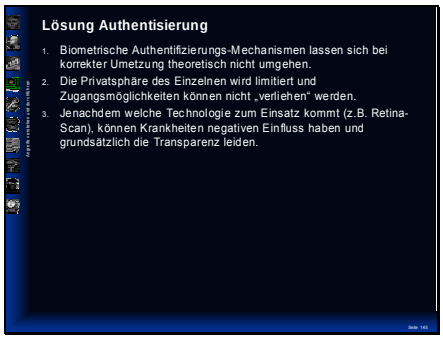
In Bezug auf Authentisierungs-Mechanismen gilt es einige grundsätzliche Dinge zu beachten. So darf ein Benutzer technisch erst dann als legitim klassifiziert werden, wenn er die Authentisierung komplett erfolgreich durchlaufen kann. Die Authentisierung muss dabei für einen Angreifer so schwierig wie möglich zu meistern sein. Der Schlüssel also so komplex wie möglich, damit eine Imitation nicht oder nur mit erheblichem Aufwand möglich ist. Der authentisierte Benutzer muss danach innert der ganzen Sitzung eindeutig identifizierbar und verfolgbar sein. Ein Ändern des Status oder ein Übertreten der Sitzung darf nicht möglich sein.

144



Machen Sie sich nun Gedanken über sichere Authentisierungen. Welcher Authentisierungs-Mechanismus scheint Ihrer Meinung nach bei einer kompetenten und umfassenden Implementierung das höchste Mass an Sicherheit gewährleisten zu können? Geht Ihre Wahl auch mit einem gewissen Nachteil für den Endbenutzer einher? Muss er zum Beispiel Einbussen in Punkto Handhabung oder Privatsphäre auf sich nehmen? Gibt es zudem Gebiete, bei denen sich der Einsatz der von Ihnen vorgeschlagenen Technologie gar nicht lohnt?

145

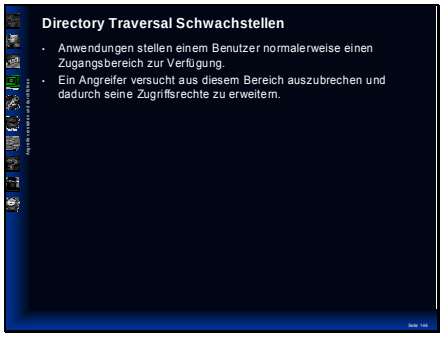


Grundsätzlich kann man sagen, dass bei einer richtigen Implementierung die Technologien aus dem biometrischen Bereich das höchste Mass an Sicherheit versprechen. Vor allem Iris-/Retina-Scans sind sehr schwer zu überlisten. Bei derartigen Methoden kann jedoch die Privatsphäre eines jeden Bürgers enorm leiden. Die eindeutige Identifikation liesse sich auch für ein Profiling im grösseren Stil einsetzen.

Desweiteren können Zugangsmöglichkeiten nicht „verliehen" werden. Wäre beispielsweise eine Fingerabdruck-Authentifizierung erforderlich, um Zugang zu Ihrer Wohnung zu erlangen, können Sie bei einem längeren Urlaub Ihren Nachbarn nicht spontan einen „Schlüssel" ausleihen.

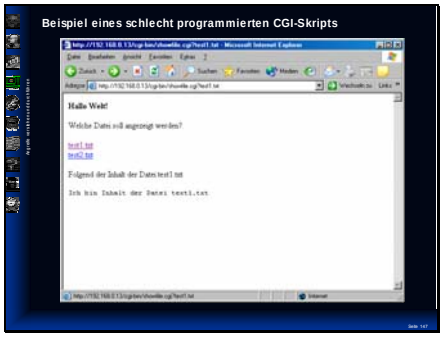
Zudem können biometrische Mechanismen zu Komplikationen führen. Augenkrankheiten bei Iris-Scan oder Schnittwunden bei Fingerprint-Analysen führen zu fehlerhaften Resultaten und können einer legitimen Person den Zutritt verweigern. Ebenso wären Rückschlüsse auf Krankheiten denkbar, was zu Diskriminierungen im Alltag führen könnte. Ein solches Szenario wurde sehr eindrücklich im Film „Gattaca" (1997, http://www.imdb.com/title/tt0119177/) von Andrew Niccol aufgezeigt.

146



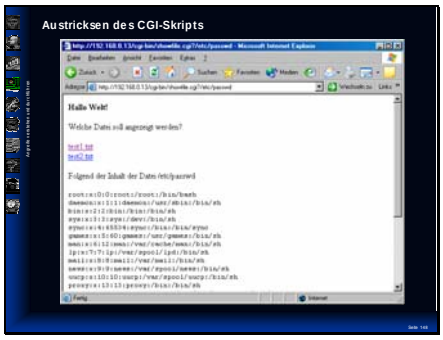
Eine Schwachstelle, die vor allem bei Web-Applikationen gegeben ist, nennt sich Directory Traversal. Anwendungen stellen Benutzern in der Regel einen gewissen Kontext zur Verfügung. Dabei werden Zugriffe auf bestimmte Dateien gewährt. Im Falle von Web-Servern sind dies die Web-Dateien, die sich im entsprechenden Web-Verzeichnis (wwwroot) befinden. Bei Directory Traversal versucht der Angreifer nun, aus diesem Verzeichnis-Kontext auszubrechen und damit Zugriff auf andere Daten zu erhalten.

147



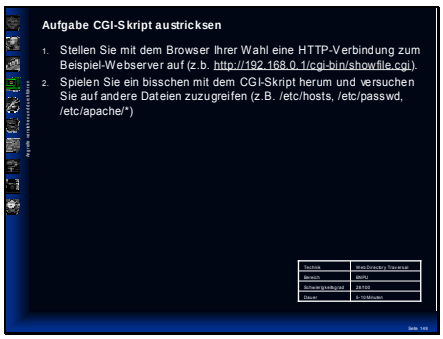
Directory Traversal-Schwachstellen lassen sich am einfachsten anhand eines fehlerhaften umgesetzten CGI-Skripts auf einem Webserver illustrieren. In diesem Beispiel wird die URL http://192.168.0.13/cgi-bin/showfile.cgi?test1.txt aufgerufen. Dabei ist die Datei showfile.cgi für die Anzeige des Inhalts einer Datei zuständig. Beim Zugriff wird als $QUERY_STRING der Name der anzuzeigenden Datei, in diesem Beispiel test1.txt, mitgegeben.

148



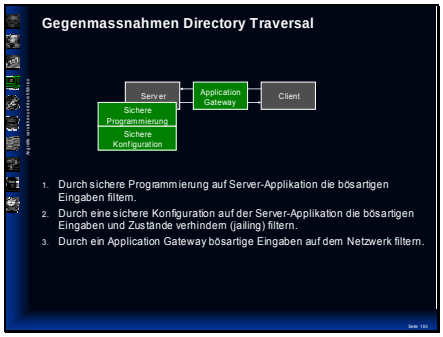
Ein Angreifer hat dabei die Möglichkeit, den Namen der anzuzeigenden Datei selber zu bestimmen. Anstatt nun an der vordefinierten Auswahl der Namen test1.txt und test2.txt festzuhalten, kann auf einen beliebigen Dateinamen zugegriffen werden. Dabei lassen sich im Rahmen der Directory Traversal-Schwachstelle ebenfalls Verzeichnisse angeben. In diesem Beispiel wird als $QUERY_STRING der Absolute Pfad /etc/passwd angegeben. Der Aufruf erfolgt direkt in der Adresszeile des Webbrowsers. Sodann wird der Inhalt der Linux-Passwortdatei des Webservers ausgegeben. Der Angreifer ist damit aus dem Web-Verzeichnis ausgebrochen und konnte auf sensitive Systemdateien zugreifen. Neben absoluten Pfaden werden bei derartigen Attacken ebenfalls relative Pfade mit der Hilfe der Zeichenkette ../ eingesetzt. So hätte diese Attacke auch mit dem Zugriff ../../../../etc/passwd umgesetzt werden können. Dabei wird vier Stufen höher in der Verzeichnishierarchie des Zielsystems gesprungen, um sodann ins Verzeichnis /etc abzutauchen und auf die Datei passwd zuzugreifen. [McClure et al. 1998, Hoglund und McGraw 2004]

149



Führen Sie nun selbst einen solchen Directory Traversal-Zugriff zu. Stellen Sie eine Verbindung zum Test-Server her. Die IP-Adresse dessen wird Ihnen im Rahmen des Kurses bekanntgegeben. Lautet diese beispielsweise 192.168.0.1, starten Sie sodann den Webbrowser (z.B. Microsoft Internet Explorer) und geben Sie die Adresse http://192.168.0.1/cgi-bin/showfile.cgi ein. Spielen Sie nun ein bisschen mit dem Skript herum, um ein Gefühl für seine Verhaltensweise zu bekommen. Setzen Sie nun eine Directory Traversal-Attacke um, indem Sie nun manuell den Namen der Datei auf /etc/hosts oder /etc/apacke/* ändern.

150

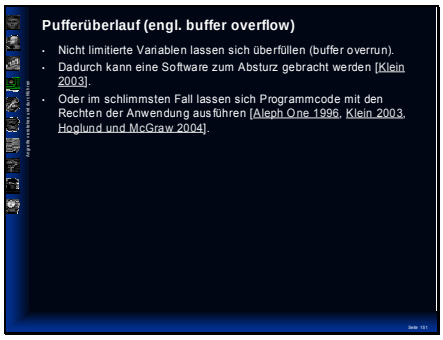


Die Gegenmassnahmen bei Directory Traversal-Attacken können auf verschiedenen Ebenen umgesetzt werden. Die sicherste und effizienteste Methode ist, Applikationen vor unerwünschten Zugriffen abzusichern. Eingaben durch Benutzer sollten auf ihre Richtigkeit hin untersucht und fehlerhafte oder verdächtige Zugriffe verworfen werden.

Zudem kann eine sichere Konfiguration auf einem Webserver helfen, wenigstens sensitive Systembereiche vor unerwünschten Zugriffen zu schützen. Webserver sowie PHP bieten derartige Funktionen an.

Desweiteren können ebenfalls Application Gateways bösartige Zugriffe frühzeitig erkennen und verhindern. Vor allem Zeichenketten wie ../ und ..\ deuten auf einen Directory Traversal-Versuch hin.

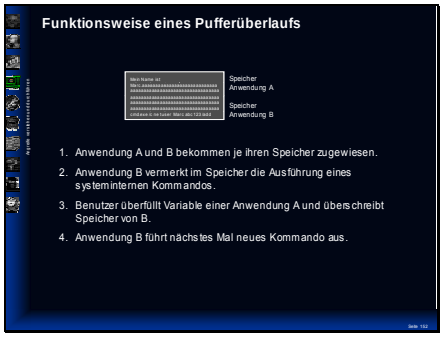
151



Es gibt keine andere Angriffstechnik, die den Bereich der Computersicherheit so geprägt hat, wie Pufferüberlauf-Attacken (engl. Buffer overflow). Dabei werden durch eine fehlerhafte Variablen-Behandlung Speicher überschrieben, um damit erweiterten Einfluss auf die Funktionsweise eines Programms bzw. des Systems zu erlangen. Neben Denial of Service durch Speicherschutzverletzungen lassen sich so auch im schlimmsten Fall beliebiger Programmcode ausführen. Das erfolgreiche Ausnutzen einer Pufferüberlauf-Schwachstelle ist jedoch sehr schwierig und erfordert ein enormes Verständnis für Betriebssysteme und ihr Speichermanagement. Aus diesem Grund gelten Pufferüberlauf-Attacken seit jeher als die Königsdisziplin des Exploitings.

Ursprünglich wurde das Thema Pufferüberlauf durch Aleph One im Jahr 1996 publik gemacht. Sein Artikel „Smashing the Stack for Fun an Profit“ im populären Phrack-Magazin inspirierte Tausende Hacker und Cracker zum Finden und Ausnutzen von Pufferüberlauf-Schwachstellen [Aleph One 1996]. Sehr schön und umfangreich geht Tobias Klein in seinem Buch „Buffer Overflows und Format-String-Schwachstellen“ [2003] auf das Thema ein. Exotische und erweiterte Techniken werden ebenfalls in „Exploiting Software“ von Hoglund und McGraw [2004] diskutiert.

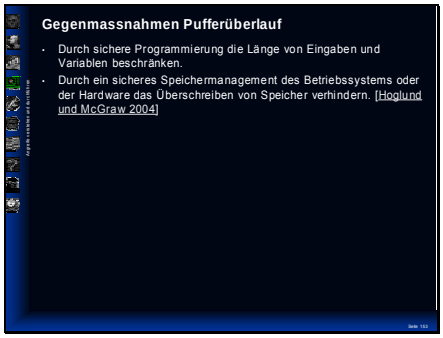
152



Das erfolgreiche Umsetzen eines konstruktiven Pufferüberlauf-Angriffs zum Ausführen beliebigen Programmcodes ist sehr kompliziert. Aus diesem Grund wollen wir die Funktionsweise dessen hier nur ganz rudimentär betrachten. Detaillierte Informationen finden sich in [Aleph One 1996], [Klein 2003] sowie [Hoglund und McGraw 2004].

Gehen wir davon aus, dass die Anwendungen A und B ihren Speicher zugeteilt bekommen. In diesem können Sie Informationen abspeichern und abrufen. Der Zugriff bleibt dabei ihnen (und dem Betriebssystem) vorbehalten. Nun vermerkt Anwendung B in ihrem Speicherbereich, dass ein systeminternes Kommando ausgeführt werden soll. Der Benutzer überfüllt nun eine Variable der Anwendung A und kann damit den Speicher der Anwendung B überschreiben. Damit kann er direkten Einfluss auf Anwendung B ausüben und dadurch dessen Verhalten manipulieren. Das auszuführende Kommando wurde angepasst und wird nun beim nächsten Aufruf durch die Anwendung B ausgeführt. Somit konnte durch Anwendung A erweiterte Rechte erlangt werden.

153



Pufferüberlauf-Schwachstellen gelten in erster Linie als Programmierfehler. Entsprechend sind Entwickler angehalten, bei der Programmierung gewisse Grundregeln zu beachten. Setzt man eine Sprache ein, die gegen Pufferüberlauf-Schwachstellen verwundbar ist (z.B. C), dann muss man auf die korrekte Behandlung von Variablen achten. Eingaben von Benutzern sollten stets auf ihre Länge hin untersucht und überlange Eingaben verhindert werden. In sicherheitskritischen Umgebungen und bei besonders komplexen Projekten, bei denen Performance keine allzu grosse Rolle spielen, sollte man auf eine alternative Sprache ausweichen, die weniger bzw. gar nicht Anfällig gegen Pufferüberlauf-Angriffe ist.

Desweiteren bieten einige Betriebssysteme (und Prozessoren) zusätzliche Features an, wie das Überschreiben von Speicher und das Ausführen beliebigen Programmcodes verhindert werden können. In sicherheitsrelevanten Bereichen sollte man derartige Funktionen einsetzen. Es gilt jedoch zu bedenken, dass es auch hier erweiterte Techniken gibt, wie derartige Schutzmassnahmen umgangen werden können. Im Buch „Exploiting Software“ von Greg Hoglund und Gary McGraw [2004] werden einige dieser vorgestellt.

154



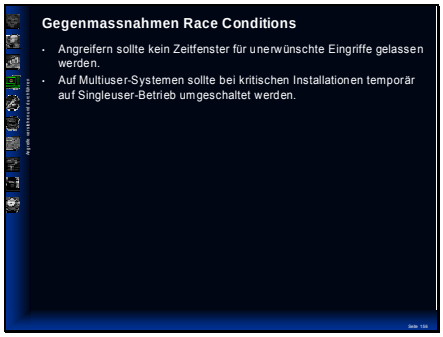
Computersysteme und Anwendungen pflegen sequentiell zu arbeiten. Dabei wird Schritt für Schritt vorgegangen, bis das Ziel erreicht ist. Bei einer solchen Abarbeitung kann es jedoch zu Fehlern kommen bzw. ein Zeitfenster für einen Race Condition-Angriff entstehen.

155



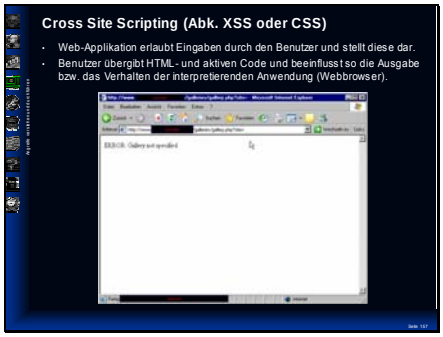
(1) Gehen wir davon aus, dass auf einem System eine Datenbank installiert werden soll. (2) Während der Installation werden die Daten in ein allgemein zugängliches Verzeichnis kopiert. (3) Nun wird erst nach dem Kopieren der Dateien werden die Zugriffsrechte für die neuen Dateien limitiert. In der Zwischenzeit hätte eine entsprechende Manipulation stattfinden können.

156



Um Race Conditions zu begegnen, sollten Zeitfenster für Angriffe verhindert werden. Dateien sollten stets sofort mit den richtigen Rechten geschrieben werden, so dass unerlaubte Zugriffe gar nicht erst stattfinden können. Auf Multiuser-Systemen sollte bei kritischen Installationen temporär auf Singleuser-Betrieb umgeschaltet werden.

157

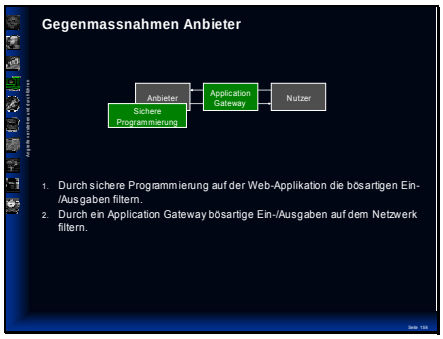


In den letzten Jahren grösster Beliebtheit erfreuten sich Cross Site Scripting-Attacken (Abk. CSS oder XSS). Diese gehören zur Klasse der Injection-Schwachstellen im Web-Bereich. Eine Vielzahl der Web-Anwendungen nimmt Eingaben des Benutzers entgegen, verarbeitet sie und geben das Resultat wieder aus. Bei einem Injection-Angriff wird die Eingabe so umgesetzt, dass sie erweiterten Einfluss auf die Ausgabe ausüben kann. Die primitivste Form ist dann gegeben, wenn sich eigener HTML-Code einbringen lässt. Sodann kann mit dem Einfluss der Ausgabe diese so angepasst werden, dass ein Opfer in die Irre geleitet werden kann. Zum Beispiel mit einem Hinweis, dass die Eingabe nicht verarbeitet werden kann und man das Passwort an eine bestimmte Mailadresse schicken soll.

In diesem Beispiel wird eine HTML-Injection in einem Live-Webserver im Internet umgesetzt. Dabei wird die GET-Variabe site manipuliert. Diese gibt an, auf welche Foto-Gallerie zugegriffen werden soll. Ist die Gallerie nicht vorhanden, wird eine Fehlermeldung ausgegeben. Nun wird aber anstatt eines normalen Namens HTML-Code eingesetzt, der ebenfalls ausgegeben wird. Dies ist ein eindeutiges Indiz dafür, dass sich technisch gestützte Social Engineering-Attacken oder gar aktives Cross Site Scripting umsetzen lässt.

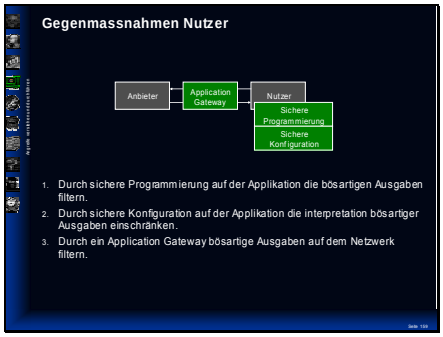
Bei Cross Site Scripting wird dieses Szenario noch weitergeführt, indem aktive Inhalte injiziert werden. Dieser Code wird dann im Kontext des Webbrowsers des Besuchers ausgeführt. Am einfachsten lässt sich dies oftmals mit JavaScript umsetzen. Anstatt nun statischen HTML-Code einzusetzen, wird mittels JavaScript ein erweiterter Angriff ausgeführt. Sodann lassen sich Cookies auslesen und an andere Seiten schicken [McClure et al. 1998]. Oder browserspezifische Attacken (z.B. das Ausnutzen einer Pufferüberlauf-Schwachstelle) lässt sich initiieren.

158



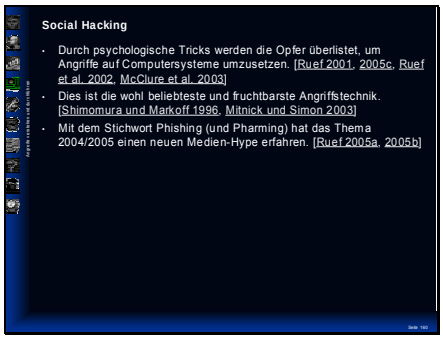
Cross Site Scripting-Attacken lassen sich auf verschiedenen Ebenen verhindern. Als erstes sei gesagt, dass dies ein grundsätzliches Problem ist, das dem Entwickler und Anbieter zugeschrieben werden muss. Dieser sollte durch eine sichere Programmierung gewährleisten, dass unerwünschte und erweiterte Eingaben durch einen Benutzer gar nicht getätigt werden können. Gerade Sonderzeichen, wie sie im Web- und Entwicklungsbereich gängig sind, haben nur selten etwas in einer Eingabe verloren. Sonderzeichen wie <, >, ; oder „ sollten gefiltert werden. Dies kann ebenfalls auf einem Application Gateway mit HTTP-Proxy stattfinden, ist aber bestmöglich direkt in der Web-Anwendung umzusetzen. Web-Sprachen wie PHP bieten dafür gar eigene Codierungs- bzw. Filterungs-Mechanismen an.

159



Der Benutzer kann ebenfalls ein Firewall-Element mit Proxy einsetzen, um etwaige Übergriffe zu verhindern. Auch dort hat ein Filtern auf Sonderzeichen stattzufinden. Desweiteren kann er aber durch eine sichere Konfiguration seines Browsers verhindern, dass aktive Inhalte ohne weiteres ausgeführt werden. Die Unterstützung von JavaScript und dergleichen sollte in sicherheitsbewussten Umgebungen lediglich für Ressourcen zugelassen sein, die als vertrauenswürdig und sicher eingestuft werden können.

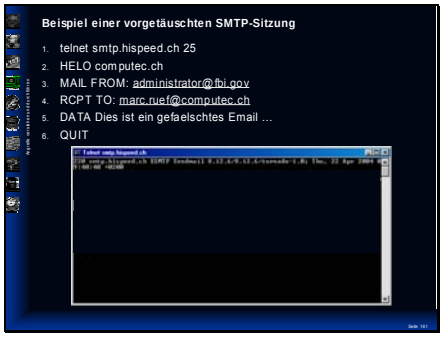
160



Wir haben bisher einige technische Angriffsvarianten gesehen. Die erfolgsversprechendste ist aber seit jeher der Angriff auf psychologischer Ebene. Durch raffinierte Tricks versuchen Betrüger ihre Opfer so zu manipulieren, dass sie einen Vorteil für sich erlangen können. Das Abschwatzen von Passwörtern über Telefon ist dabei besonders klassisch, wird jedoch zunehmends durch das Phishing per Email ersetzt.

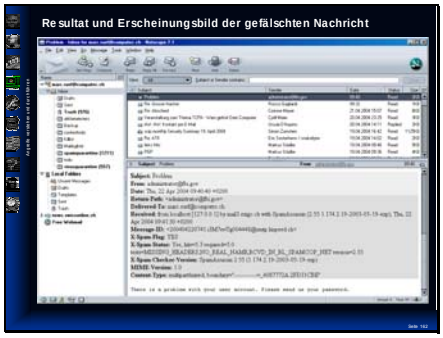
Kevin Mitnick galt jahrelang als einer der Supercracker weltweit. Nach seiner Entlassung aus der Haft, das FBI hatte Ihn 1995 endlich festnehmen können, publizierte er sein Wissen im Buch „The Art of Deception – Controlling the Human Element of Security" [Mitnick und Simon 2003]. Dies gilt als das Kompendium zum Thema Social Engineering.

161



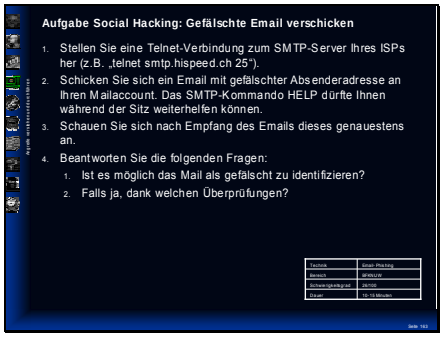
Wir wollen nun sehen, wie sich ein Phishing-Zugriff mittels technischen Hilfsmitteln aufwerten lässt. Dazu werden wir ein Email mit falschem Absender verfassen. Hierzu stellen wir mittels Telnet eine Verbindung zu einem offenen SMTP-Relay her. (1) In diesem Beispiel geschieht dies mit der Eingabe von „telnet smtp.hispeed.ch 25“, um mittels Telnet eine Verbindung zum Port tcp/25 des Hosts mit dem Namen smtp.hispeed.ch herzustellen. (2) Nachdem uns der Mailserver mit seinem Willkommens-Banner begrüsst hat, melden wir uns mit dem SMTP-Kommando HELO an. Dabei geben wir eine gültige Domain an, die wir als unsere Herkunft deklarieren wollen. In diesem Beispiel computec.ch; sie ist jedoch in der Regel frei wählbar. (3) Sobald der Server diese Information angenommen hat, beginnen wir mit dem eigentlichen Erstellen des Emails. Durch das Kommando „MAIL FROM“ können wir den Absender bestimmen. Hierbei benutzen wir „MAIL FROM: administrator@gov.fbi“, um die vermeintliche Administrativadresse von fbi.gov zu nutzen. (4) Wird der Absender akzeptiert, können wir mit dem Kommando „RCPT TO“ den Empfänger definieren. In diesem Beispiel die Mailadresse marc.ruef@computec.ch. (5) Wenn auch diese angenommen wurde, geben wir das SMTP-Kommando DATA ein. Sodann können wir den Inhalt des Emails (engl. Body) angeben. Benutzen wir „Subject“ auf der ersten Zeile, lässt sich ebenfalls der Betreff des Emails bestimmen. Möchten wir die Eingabe abschliessen, benutzen wir einen einzelnen Punkt auf einer separaten Zeile. Sodann wird das Email für den Versand in die Queue geschrieben. (6) Die Arbeit ist getan und wir können mit dem Kommando QUIT die Verbindung zum SMTP-Server wieder beenden.

162



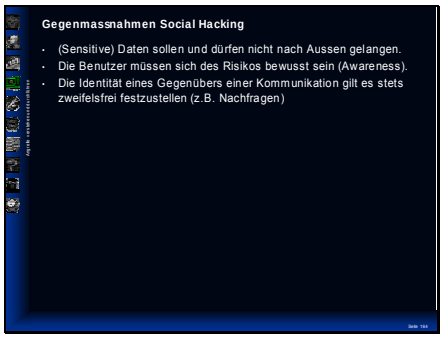
Wechseln wir nun in die Inbox von marc.ruef@computec.ch, um den Erhalt des vorgetäuschten Emails zu verifizieren. Wir können sehr schön sehen, dass der Absender administrator@fbi.gov angenommen und das Schreiben mit diesem ausgestattet wurde. Der Versand des Phishing-Mails war erfolgreich.

163



Setzen Sie nun ebenfalls den Versand eines Emails mit gefälschter Absenderadresse um. Stellen Sie dazu mit der Hilfe eines Telnet-Clients die Verbindung zum SMTP-Server Ihres Prodivers her. Dieser ist normalerweise mit dem Hostnamen smtp.provider.ch oder mail.provider.ch erreichbar. Befinden Sie sich zum Beispiel im Netzwerk der Hispeed Cablecom (Swissonline), können Sie mit dem Kommando „telnet smtp.hispeed.ch 25" eine Verbindung zum TCP-Port 25 des Mailservers mit dem Hostnamen smtp.hispeed.ch herstellen. Nachdem die Verbindung etabliert wurde, können Sie das Email umsetzen. Benutzen Sie dazu die zuvor gezeigten SMTP-Kommandos HELO, MAIL FROM, RCPT TO, DATA und QUIT. Der Befehl HELP dürfte Ihnen bei Problemen weiterhelfen. Verschicken Sie das Email an eine Adresse, auf die Sie Zugriff haben. Schauen Sie sich nach erfolgreichem Versand die Nachricht an und untersuchen Sie sie (z.B. die erweiterten SMTP-Header anzeigen lassen). Beantworten Sie nun die Frage, ob und wie ein Email mit gefälschter Absenderadresse identifiziert werden kann.

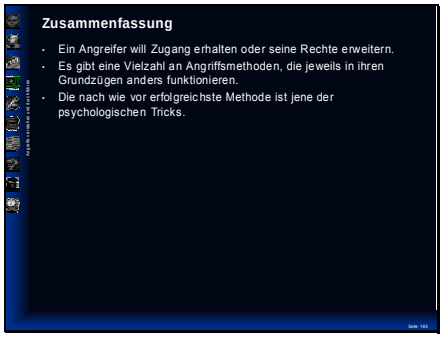
164



Angriffe auf psychologischer Ebene können nicht oder nur sehr schwer mit technischen Hilfsmitteln verhindert werden [Ruef 2005]. Ein annehmbares Mass an Kritizismus im Rahmen des gesunden Menscheverstandes sollte jedoch eine Vielzahl der populären Angriffe verhindern. Dazu zählt beispielsweise ein plumpes Phishing per Email, bei dem sich der Angreifer als Mitarbeiter einer Bank ausgibt und nach den Authentisierungs-Informationen des E-Bankings nachfragt.

In grösseren Unternehmungen werden die Anwender durch Awareness-Schulungen mit dem Thema Information Security konfrontiert und entsprechende Abwehrstrategien diskutiert. So gilt es die Identität des Gegenübers – vor allem wenn es um den Austausch sensibler Daten geht – ausnahmslos zu überprüfen. Ein Rückruf per Telefon zur Verifizierung eines internen Anschlusses oder das Nachfragen bei Vorgesetzten kann vor dreisten Attacken schützen.

165

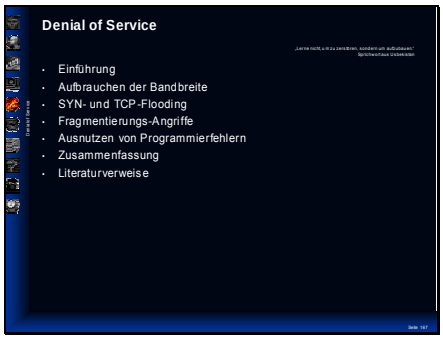


Grundsätzlich will ein Angreifer erweiterte Rechte in einer Umgebung erhalten. Dazu versucht er die Limitierungen, die ihm auferlegt wurden, zu umgehen und bestmöglich administrative Privilegien zu erhalten. Dabei gibt es eine Vielzahl an Angriffstechniken und –methoden, die ein derartiges Vorgehen ausmachen können. Pufferüberlauf-Attacken, Directory Traversal-Schwachstellen und Race Conditions sind nur einige davon. In den meisten Fällen erfolgreich ist jedoch das Social Hacking, bei dem durch psychologische Tricks ein Opfer manipuliert und so die Herausgabe sensitiver Informationen forciert werden kann. Dagegen helfen nur selten technische Schutzmassnahmen. Gesunder Menschenverstand und eine gewisse Portion Misstrauen sind leider die Grundpfeiler einer funktionierenden Informationsgesellschaft.

166

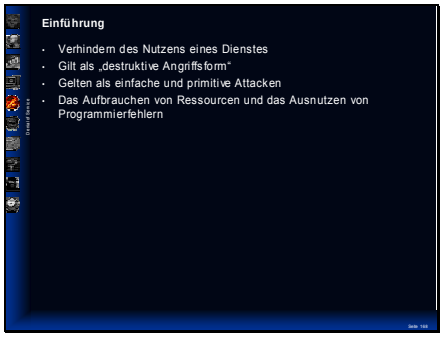


167



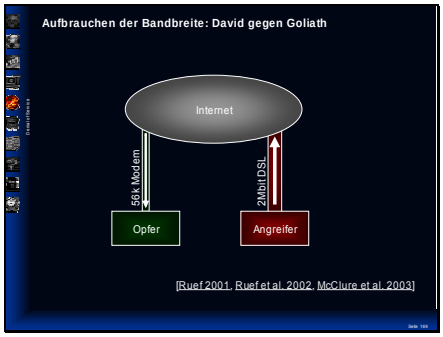
Nachdem wir vorwiegend konstruktive Vorgehensweisen des Auswertens und Angreiferns kennengelernt haben, wollen wir uns mit destruktiven Attacken auseinandersetzen. Dabei werden wir einige Konzepte von Denial of Service kennenlernen. Dies reicht vom klassischen Aufbrauchen der Bandbreite über Schwächen in der TCP/IP-Protokollfamilie bis hin zu Fehlern von Netzwerkapplikationen.

168



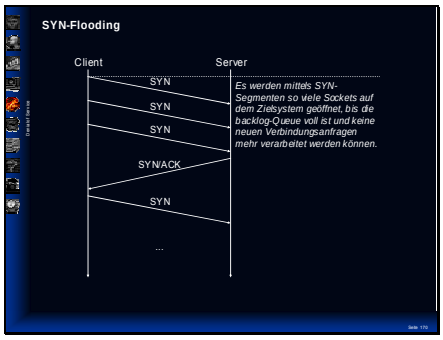
Destruktive Attacken zielen darauf ab, den legitimen Benutzern eines Dienstes den Zugriff auf diesen zu verwehren. Dies wird als Denial of Service (Abk. DoS) bezeichnet und gilt aufgrund der einfachen Umsetzungsweise als primitive Angriffsart. Denial of Service-Attacken setzen auf zwei verschiedene Konzepte. Zum einen können Ressourcen aufgebraucht und zum anderen Programmierfehler ausgenutzt werden.

169



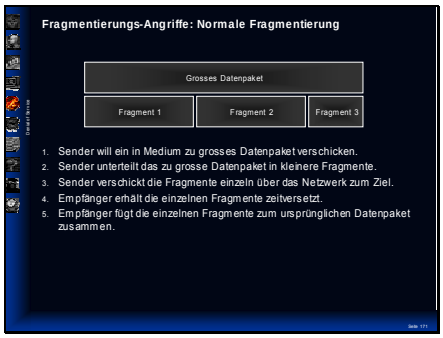
Die klassische und am einfachsten zu verstehende Denial of Service-Attacke ist im Aufbrauchen der Bandbreite gegeben. Gehen wir davon aus, dass ein nichts ahnendes Opfer im World Wide Web surft. Es greift dabei auf ein älteres Modem mit 56 Kbit zurück. Nun will ein Angreifer mit seinem neuen 2 Mbit Kabelmodem einen Angriff umsetzen. Er überlastet dabei die Anbindung des Gegenübers, indem er möglichst viele Daten überträgt. Da er mit einem Mehr an Bandbreite auftrumpfen kann, ist bei diesem Zugriff der Flaschenhals eindeutig beim älteren Modem gegeben. [Ruef 2001, Ruef et al. 2002, McClure et al. 2003]

170



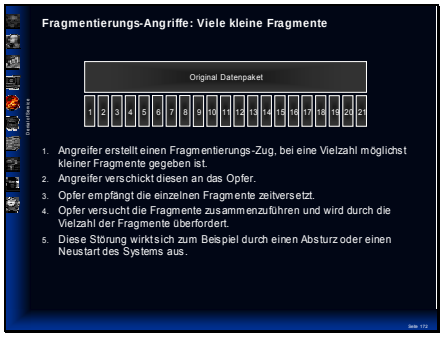
Eine klassische Denial of Service-Angriffsart nennt sich SYN-Flooding. Dabei verschickt der Angreifer eine Vielzahl an TCP-Paketen mit gesetzter SYN-Flagge an einen offenen Port des Zielsystems. Da dies der normale Verbindungsaufbau im Rahmen des Drei-Wege-Handschlags von TCP ist, wird der Server die Anfrage mit einem SYN/ACK-Segment bestätigen. Danach wird auf eine finale Bestätigung mittels SYN-Paket gewartet. Dieses letzte Paket trifft jedoch nie ein, weshalb auf dem Server eine Vielzahl an halboffenen Verbindungen gegeben ist. Diese werden erst nach einem gewissen Timeout von mehreren Sekunden wieder geschlossen. Damit kann die Backlog-Queue von TCP-Aufgebraucht werden. Das Zielsystem ist danach nicht mehr in der Lage, weitere SYN-Anfragen anzunehmen und damit legitime TCP-Verbindungen aufzubauen. [Stevens 1994, Ruef 2001, Ruef et al. 2002, McClure et al. 2003]

171



Fragmentierungs-Angriffe gehören ebenso zu den klassischen Denial of Service-Attacken. Um diese besser verstehen zu können, wollen wir die normale IP-Fragmentierung innerhalb von TCP/IP besprechen. (1) Gehen wir davon aus, dass ein Host ein grosses Datenpaket übertragen will. (2) Dieses ist für das gegebene Medium (z.B. Ethernet) zu gross, weshalb es vor dem Versand in kleinere Fragmente unterteilt wird. (3) Die einzelnen Fragmente werden nun einzeln über das Netzwerk geschickt. (4) Es kann nun gegeben sein, dass der Empfänger diese einzelnen Fragmente zeitversetzt und in unvorhergesehener Reihenfolge erhält. (5) Er wartet sodann, bis sämtliche Fragmente des Fragmentierungs-Zuges angekommen sind, um diese wieder in der richtigen Reihenfolge zusammenzusetzen. Sodann erhält er Zugriff auf das ursprünglich vorgesehene Datenpaket.

172



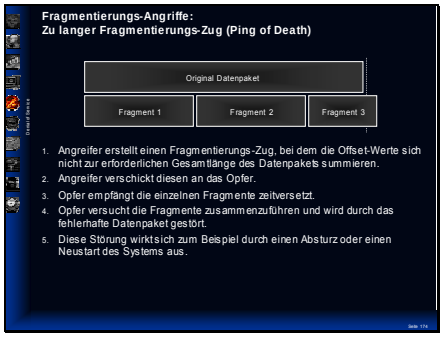
Ein möglicher Angriff über Fragmentierung ist durch eine erhöhte Fragmentierung gegeben. (1) Dabei wird das ursprüngliche Datenpaket in eine Vielzahl kleinere Datenpakete zerteilt. (2) Der Angreifer verschickt diesen umfassenden Fragmentierungs-Zug an das Zielsystem, (3) das diese auch - eventuell gar wiederum in einer fehlerhaften Reihenfolge - empfangen wird. (4) Das Opfer will nun eine Reassemblierung der vielen Fragmente umsetzen, was zu einer erhöhten Auslastung des Systems (CPU) führen wird. (5) Eine derartige Störung kann sich bei einigen Systemen mit einem Absturz oder Neustart auswirken. Die Denial of Service-Attacke ist sodann erfolgreich.

173



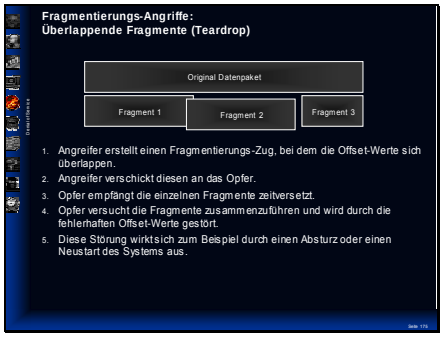
Ein Fragmentierungs-Angriff, der von der Idee her dem SYN-Flooding ähnlich ist, ist der nicht abgeschlossene Fragmentierungs-Zug. (1) Dabei erstellt der Angreifer einen normalen Fragmentierungszug, in diesem Beispiel bestehend aus 3 Fragmenten. (2) Nun verschickt er die ersten beiden Teile an das Zielsystem, (3) welches diese zeitversetzt erhält. (4) Es kann noch keine Reassemblierung der Fragmente umsetzen, da das letzte Fragment noch nicht eingetroffen ist. Auf den Erhalt dessen wird gewartet, wobei der Angreifer es einfach nicht losschickten will. Wiederum wird eine halbfertige Fragmentierung erst nach einiger Zeit verworfen. (5) Eine Vielzahl nicht abgeschlossener Fragmentierungs-Züge kann dazu führen, dass keine weiteren IP-Pakete oder Fragmente mehr eingehen können.

174



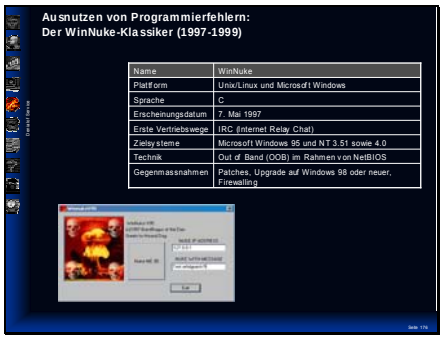
Eine andere Variante eines Angriffs über IP-Fragmentierung ist bei einem zu langen Fragmentierungs-Zug gegeben. Diese Technik wird auch als Ping of Death bezeichnet. (1) Dazu erstellt der Angreifer einen Fragmentierungs-Zug, die sich nicht zur eigentlichen Gesamtlänge des ursprünglichen Datenpakets summieren. (2) Er verschickt nun diesen korrupten Fragmentierungs-Zug an das Zielsystem, (3) welches die Fragmente zeitversetzt erhält. (4) Das Zielsystem versucht sich nun an der Reassemblierung des Fragmentierungs-Zugs und wird dabei durch die fehlerhaften Offset-Werte aus dem Tritt gebracht. Dieser Angriff hat bei älteren Windows-Systemen zu einem Bluescreen, bei anderen Systemen zu einem Absturz oder einem Neustart geführt.

175



Wiederum eine sehr populäre Denial of Service-Attacke, die sich IP-Fragmentierung zunutze macht, trägt den Namen Teardrop. (1) Hierbei werden ebenfalls korrupte Offset-Werte bei den Fragmenten genutzt und damit eine Überlappung dieser provoziert. (2) Der Angreifer verschickt diesen korrupten Fragmentierungs-Zug (3) und das Opfer erhält diese zeitversetzt. (4) Das Opfer versucht diese zusammenzuführen und wird durch die fehlerhaften Offset-Werte gestört. (5) Diese Störung kann sich wiederum in einem Absturz des Zielsystems oder in einem Neustart dessen auswirken.

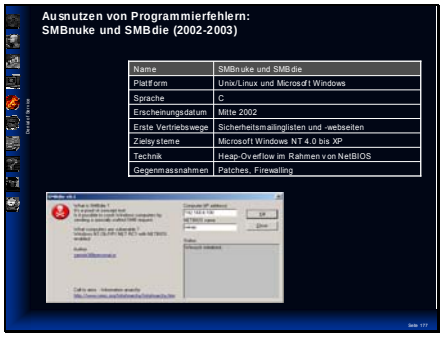
176



Das populärste Tool für Denial of Service ist mit WinNuke gegeben, welches erstmal am 7. Mai 1997 publiziert wurde. Dieses, welches ursprünglich in C für Unix/Linux geschrieben wurde, nutzt einen Fehler in der NetBIOS-Implementierung von Microsoft Windows aus. Der Angriff mit dem namen Out of Band (OOB) betrifft die älteren Windows-Versionen 95, NT 3.51 sowie 4.0. Besonders populär wurde der Angriff aber erst, als ein handliches Tool für Windows entwickelt wurde, das mit dem Namen WinNuke95 herausgegeben wurde. In den Jahren 1997 bis 1999 war es ein beliebtes Spielchen im Internet, sein Gegenüber mal eben schnell einen Bluescreen of Death generieren zu lassen.

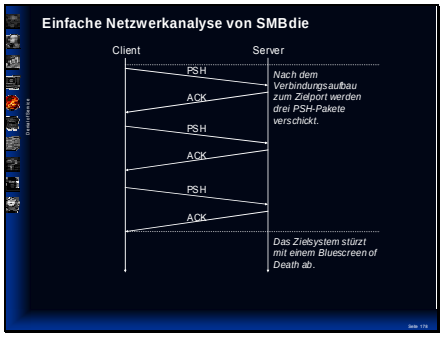
Die betroffenen Nutzer waren angehalten, auf eine neuere Windows-Version zu aktualisieren. So war beispielsweise Windows 98 nicht betroffen. Es wurden jedoch ebenfalls Patches zum Problem herausgegeben. Mittels Firewalling kann der Zugriff von WinNuke verhindert und damit die Attacke unterbunden werden.

177



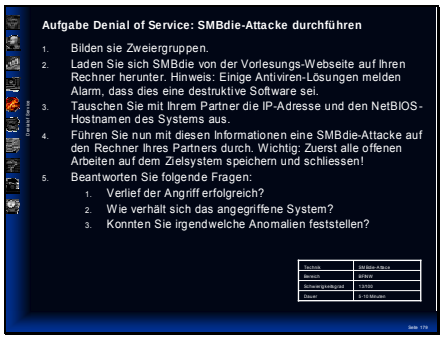
Als Nachfolger von WinNuke kann SMBdie verstanden werden. Dies stellt die Windows-Portierung von SMBnuke dar, einem wiederum ursprünglich für Unix/Linux entwickelten Denial of Service-Tool. Die in C geschriebene Applikation nützt Mitte 2002 einen Heap-Overflow im Rahmen von NetBIOS aus und weist damit auffällige Ähnlichkeiten mit WinNuke auf. Betroffen sind dieses Mal aber auch neuere Versionen von Windows wie NT 4.0 und XP. Microsoft hat mit Patches für die betroffenen Systeme reagiert und empfahl den Einsatz von Firewalling, um direkte Zugriffe von SMBnuke und SMBdie zu verhindern.

178



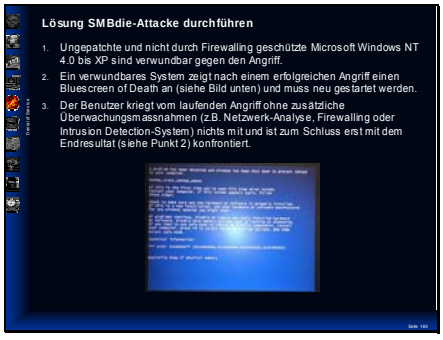
Eine einfache Netzwerkanalyse von SMBdie zeigt, dass nur insgesamt 6 Pakete im Rahmen eines Angriffs übertragen werden müssen, bis ein Bluescreen provoziert und damit die Denial of Service-Attacke erfolgreich umgesetzt wird. Auffällig dabei ist, dass sämtliche Pakete des Angreifers mit einer gesetzten PSH-Flagge (Push) verschickt werden. Eine der vielen Charakteristika dieses Angriffs.

179



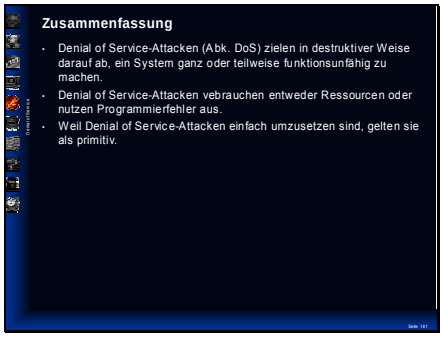
Um das Verständnis für die Einfachheit eines Denial of Service-Angriffs mit vorgefertigtem Tool zu erhalten, wollen wir nun selber einen Angriff ausprobieren. Bilden Sie nun Zweiergruppen und laden Sie jeweils von der Vorlesungswebseite das Tool SMBdie auf Ihren Rechner herunter. Entpacken Sie das Archiv und starten Sie die darin enthaltene EXE-Datei. Es kann durchaus sein, dass die gegenwärtige Antiviren-Lösung korrupten Programmcode darin vorfindet. Diese Meldung können Sie weitestgehend ignorieren. Wir werden im Kapitel über Computerviren genauer erläutern, wieso. Führen Sie nun eine SMBdie-Attacke auf den Rechner Ihres Partners durch. Geben Sie dazu die IP-Adresse sowie den NetBIOS-Namen des Hosts ein. Letzteren können Sie theoretisch mit dem Kommando „nbtstat –A <ziel-ip>“ herausfinden. Lesen Sie dazu das entsprechende Kapitel über NetBIOS-Auswertungen nach. Beantworten Sie nach dem Angriff nun die Frage, ob und inwiefern die Attacke erfolgreich verlaufen ist. Wie hat sich das angegriffene System verhalten und/oder konnten Sie irgendwelche Anomalien feststellen?

180



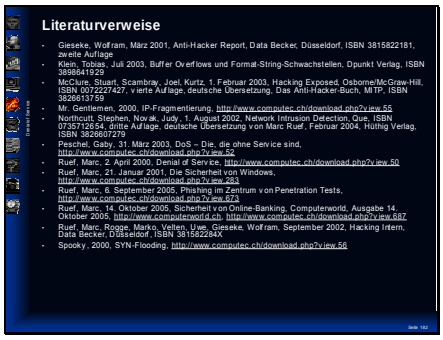
Der Angriff mit SMBdie verläuft nur auf den Systemen Microsoft Windows NT 4.0 und XP erfolgreich, sofern diese nicht mittels Patches und Firewalling vor dem Angriff geschützt sind. Ein verwundbares System zeigt nach einem erfolgreichen Angriff einen Bluescreen of Death an (siehe Bild unten) und muss neu gestartet werden. Der Benutzer kriegt vom laufenden Angriff ohne zusätzliche Überwachungsmassnahmen (z.B. Netzwerk-Analyse, Firewalling oder Intrusion Detection-System) nichts mit und ist zum Schluss erst mit dem Endresultat konfrontiert.

181

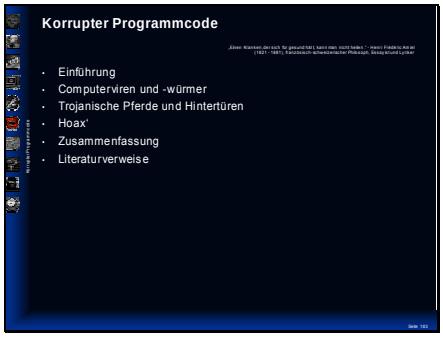


Denial of Service-Attacken (Abk. DoS) zielen in destruktiver Weise darauf ab, ein System ganz oder teilweise funktionsunfähig zu machen. Dabei werden entweder Ressourcen verbraucht oder Programmierfehler ausgenutzt. Wir haben einige dieser Techniken exemplarisch diskutiert, wobei vor allem WinNuke als die unbestritten populärste Angriffstechnik gilt. Weil Denial of Service-Attacken einfach umzusetzen sind, gelten sie als primitiv und werden von vielen Hackern verachtet.

182



183



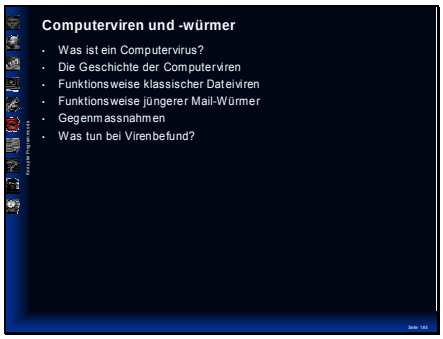
In diesem Kapitel werden wir uns mit korruptem Programmcode (engl. malicous code) beschäftigen. Nach einer allgemeinen Einführung in die Funktionsweise und Absichten derartiger Programme werden wir im Detail Computerviren und –würmer behandeln. Desweiteren schauen wir uns an, wie Trojanische Pferde aussehen und wozu Hintertüren (engl. backdoors) dienen. Zum Schluss werden wir sogenannte Hoax besprechen, die einen ähnlichen Effekt wie Computerwürmer haben können, aber auf einer ganz anderen Ebene ansetzen.

184



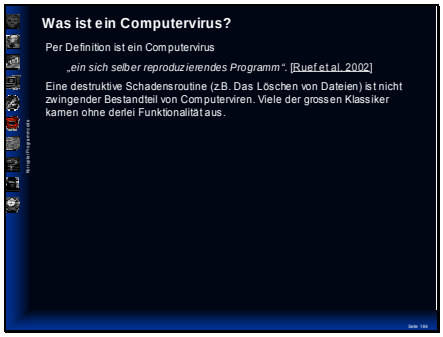
Unter korruptem oder schädlichen Programmcode (engl. malicous code) wird ein Stück Software verstanden, das sich unerwünschten oder unbefugten Zugriff auf einen Computer bzw. dessen Komponenten verschafft. Die populärster Vertreter dieser Gattung sind Computerviren und –würmer. Aber auch Trojanische Pferde, Hintertüren, Angriffstools und Exploits können in diese Kategorie fallen.

185



Computerviren und –würmer machen sicher einen Hauptteil des korrupten Programmcodes aus. Aus diesem Grund wollen wir uns als erstes ausführlich mit der Funktionsweise dieser beschäftigen. Nach einer kurzen Definition der Begrifflichkeiten werden wir die historischen Aspekte der Computerviren diskutieren, um danach die Funktionsweise verschiedener Viren und Würmer zu illustrieren. Als Beispiele werden dabei ein klassischer Dateivirus und ein moderner Mail-Wurm herhalten. Zum Schluss werden wir die Gegenmassnahmen und der Ablauf bei einem vermeintlichen Virenbefund abhandeln.

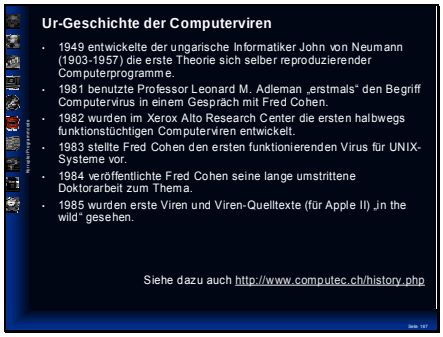
186



Die Definition eines Computervirus ist schwer und wird in der verschiedenen Literatur immerwieder anders vorgetragen. Im Rahmen dieser Vorlesung werden wir die Terminologie des Buches „Hacking Intern“ (2002) benutzen, bei dem ein Computervirus schlicht als „ein sich selber reproduzierendes Programm“ bezeichnet wird. Damit ist die Grundlage eines biologischen Virus, seine eigene Verbreitung, erfüllt.

Das Unterbringen etwaiger Schadensroutinen oder Zusatzfunktionen (z.B. polymorphes Verhalten) ist Optional und nicht zwingend ein Teil eines Computervirus. Dies ist ein sehr wichtiger Aspekt, um den wissenschaftlichen Nutzen derartiger Entwicklungen besser verstehen und Computerviren nicht pauschal als Übel abstempeln zu können.

187



Die Ur-Geschichte der Computerviren kann bis in die Mitte des Neuzehnten Jahrhunderts zurückverfolgt werden. Der ungarische Informatiker John von Neumann stellte im Jahre 1949 erstmals eine Theorie von sich selber reproduzierenden Computerprogrammen vor. Dies wird als die intellektuelle Geburtsstunde heutiger Computerviren verstanden. Der Begriff ansich wurde aber erst 1981 von Professor Leonard M. Adleman in einem Gespräch mit Fred Cohen genutzt. Beide gälten als die Ur-Väter späterer Entwicklungen. Ein erster funktionstüchtiger Computervirus wurde im Jahre 1982 im Xerox Alto Research Center entwickelt und ein Jahr später stellte Fred Cohen einen ersten funktionstüchtigen Virus für UNIX-Systeme vor. Daraufhin veröffentlichte Cohen 1984 seine Doktorarbeit, die sich intensiv mit dem Thema auseinandersetzte. Diese war lange Zeit umstritten, sahen viele darin eine Anleitung für eine destruktive Vorgehensweise, die die Entwicklung des Informatik-Bereichs nachträglich in negativer Hinsicht beeinträchtigen könnte. Derlei Kritiker sollten nicht vollkommen im Unrecht sein, denn so wurden nur Monate später erste Computerviren samt Quelltexte für Apple II „in the wild“ gesehen.

Betrachtet man die ersten Jahre der Viren-Entwicklung auf Computersystemen, so bemerkt man, dass bis zu Fred Cohens Doktorarbeit 1984 ein sehr wissenschaftliches Interesse dem Genre entgegengebracht wurden. Die Entwicklungen konzentrierten sich in erster Linie darauf, sich selber reproduzierende Programme zu erschaffen und damit ein Abbild biologischer Viren umsetzen zu können. Dies, so war man der Ansicht, sei ein wichtiger Schritt im Verständnis für die Funktionsweise biologischen Lebens.

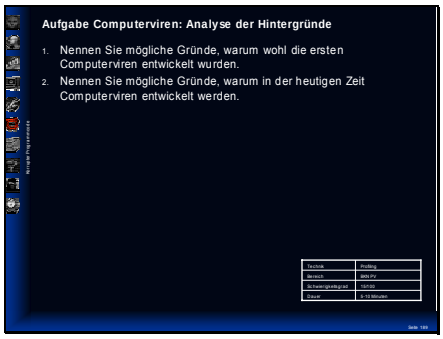
188



Die Anzahl der Computerviren ist seit den 90er Jahren jedoch explodiert. So gab es eine Vielzahl an Schädlingen für populäre Systeme wie diejenigen von Apple, Amiga oder MS DOS. Zu einem Problem neuer Dimensionalität wurde das Ganze jedoch mit der Popularisierung des Internets. Dank der globalen Vernetzung war es nun möglich, Computerviren über Netzwerke verbreiten zu können. Innert Sekunden wurde so die Infektion hunderter Hosts möglich.

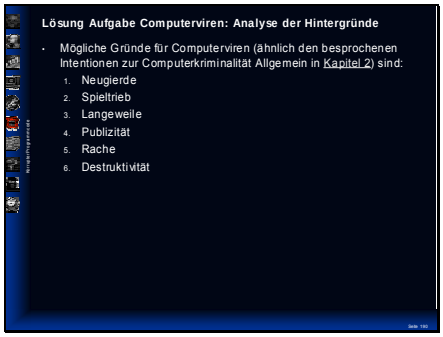
Ein erster populistischer Höhepunkt der Computerviren und –würmer war am 29. März 1999 durch Melissa gegeben. Dieser Word-Makrovirus befiel eine noch nie dagewesene Anzahl an Systemen im Internet. Die Tages- und Massenmedien verhalfen Melissa damit zu einer weltweiten Popularität, die noch nie zuvor ein Virus erlangen konnte. Zwei Jahre später wurde mit dem VBS-Virus ILOVEYOU ein ähnliches Szenario gegenwärtig. Praktisch niemand, der regelmässig über Email kommunizierte, hat nicht früher oder später mit eine viren-verseuchten Nachricht erhalten. 2001 war mit einigen anderen effektiven und populären Würmern wie CodeRed oder Nimda das Viren-Jahr schlechthin. Alle paar Wochen las man in den Zeitungen vor neuen Schädlingen, wobei diese – obschon technisch in mancherlei Hinsicht raffiniert umgesetzt – nicht mehr die gleiche Aufmerksamkeit erhielten. Der bisher verheehrendste Wurm war W32.Blaster.Worm, der sich einen seit mehreren Monaten im Windows-Betriebssystem bekannt gewordenen Fehler zunutze macht, um Systeme zu infizieren. Die Neuerung dabei war, dass ein jeder verwundbarer Host, der mit dem Internet verbunden war, sofort und ohne Wissen des Nutzers kompromittiert werden konnte. Dies zeigte sehr deutlich, wie ein falsches Patch-Management in einer Monokultur zu Horror-Szenarien führen kann.

189



Wir haben im ersten Kapitel die psychologischen und soziologischen Hintergründe der Computerkriminalität besprochen. Auf dieser Ebene wollen wir uns nun ebenfalls mit Computerviren beschäftigen. Denken Sie also darüber nach, warum wohl die ersten Computerviren entwickelt wurden. Welche Absichten verfolgten die Ur-Väter von Melissa und ILOVEYOU? Nennen Sie desweiteren Gründe, warum in der heutigen Zeit Viren und Würmer geschrieben werden. Inwiefern unterscheiden sich die Absichten im Jahr 2000 von denen im Jahr 1950?

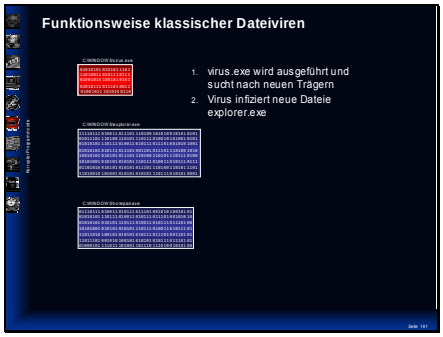
190



Die Gründe für Angriffe und die Entwicklung von Computerviren können unterschiedlicher Natur sein. Die ersten Gehversuche in diesem Bereich wurden sicher aufgrund von Neugierde und Spieltrieb gemacht. Die Frage, inwiefern auf einem Computer das Verhalten eines biologischen Virus nachgebildet werden konnte, war Kern vieler Bestrebungen.

In der heutigen Zeit werden Computerviren jedoch nicht mehr auf solch edler Ebene entwickelt. Publizität, die ein Flächenbrand wie Melissa eingebracht hat, ist für so manchen Entwickler verlocken. Ebenso können Langeweile und Rache eine wichtige Rolle spielen. Seit den 90er Jahren sind politisch motivierte Viren und Würmer immerwieder gesehen.

191

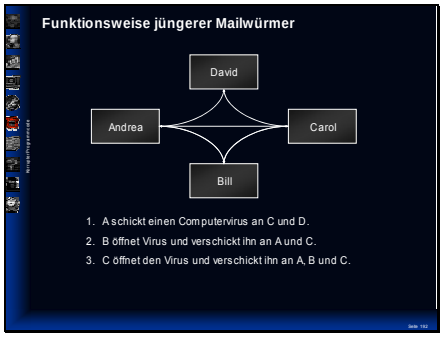


Das Verständnis für die grundlegende Funktionsweise von Computerviren kann durch einen klassischen Dateivirus am einfachen illustriert werden. Ein Viren-Entwickler stellt einen eigenen Computervirus her, den wir in unserem Beispiel virus.exe nennen wollen. Diesen speichert er in das Verzeichnis C:\WINDOWS, das das Systemverzeichnis von Windows-Umgebungen darstellt. Wird dieser Virus nun ausgeführt, sucht er im gleichen Verzeichnis nach weiteren Dateien, die er infizieren kann. Der Virus ist dabei so geschrieben, dass er als Wirt EXE-Dateien nutzt, da diese ebenfalls ausgeführt werden können. virus.exe infiziert nun die Datei explorer.exe. Dabei überschreibt er den ersten Teil der Wirtsdatei mit seinem eigenen Programmcode. Wird die infizierte Datei explorer.exe nun wiederum ausgeführt, wird statt der ursprünglichen Funktion die Funktion des Computervirus aufgerufen, was wiederum zu einer Infektion einer neuen Datei führen kann.

Diese Funktionsweise ist sehr primitiv. Zum einen handelt es sich hier um einen überschreibenden Dateivirus. Dabei wird der Original-Code des Wirts durch den Viren-Code überschrieben. Die ursprüngliche Datei ist damit zerstört und kann nicht mehr im eigentlichen Rahmen genutzt werden. Es gibt deshalb alternative Infektionsmöglichkeiten, wie diejenige der anhängenden Dateiviren. Dabei wird der Virus-Code an den Original-Code der Wirtsdatei angehängt. Wird nun die infizierte Datei ausgeführt, startet sie als erstes den Viren-Code und danach den Original-Code. Damit wird die Zerstörung der Original-Datei verhindert. Ein neues Problem eröffnet sich aber sodann, denn sämtliche Infizierten Dateien wachsen dabei um die Länge des Computervirus an.

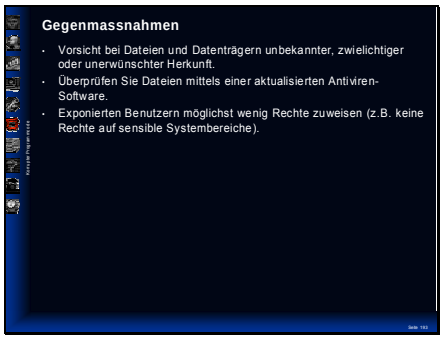
Desweiteren wurde in diesem Beispiel auf eine Routine verzichtet die überprüft, ob eine potentielle Wirtsdatei schon infiziert wurde. Effiziente Computerviren pflegen eine solche Funktion einzusetzen, um Doppel-Infektionen, die zu sonderbaren Effekten führen können, zu vermeiden. Viele andere Funktionen können ebenfalls Teil solcher Viren sein. Polymorphe Viren verändern zum Beispiel von Infektion zu Infektion ihr Auftreten, weshalb sie durch Pattern Matching nur sehr schwer zu erkennen sind.

192



Moderne Mailwürmer funktionieren vom Prinzip her ähnlich wie klassische Dateiviren. Der Unterschied liegt jedoch im Übertragungsmedium und der Infektions-Art. Dateiviren bewegen sich auf einem lokalen Dateisystem und infizieren logische Dateien auf diesem. Mailwürmer hingegen verschicken sich selber via Email und infizieren meistens mehrere Komponenten eines Systems. Dabei kann ein gewisser Lawineneffekt (oder Vireneffekt) festgestellt werden, bei dem sich die Infektion wellenartig ausbreitet.

193



Der wichtigste Schutz vor einer Infektion durch einen Computervirus ist der kritische Umgang mit Dateien und Datenträgern. Solche unbekannter, zwielichtiger oder unerwünschter Herkunft sollten nicht benutzt werden. Ein Email, das von einer unbekannten Person verschickt wurde und einen dubiosen Anhang enthält, sollte gar nicht erst geöffnet werden. Grundsätzlich gilt, dass jede Datei vor dem Öffnen und in regelmässigen Abständen mit einer aktualisierten Antivirus-Software auf schädlichen Programmcode hin untersucht werden sollte. Damit kann das Einschleppen bösartigen Codes verhindert werden. Der Schaden, der mit einer Viren-Infektion einhergeht, kann durch ein striktes Benutzermanagement eingedämmt werden. Exponierten Benutzern sollten deshalb möglichst wenige Rechte zugeteilt werden, so dass im Falle einer Infektion das Ausarten auf sensible Systemteile gar nicht möglich ist.

194

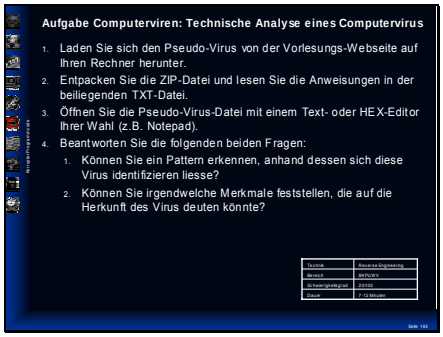


Zum Schutz vor korruptem Programmcode wurden Antiviren-Lösungen entwickelt. Diese überprüfen Dateien vor und während einer Nutzung auf schädliche Routinen, so dass eine Infektion verhindert werden kann. Dabei kommen zwei Techniken zum Einsatz.

Die klassische Technik ist im Pattern-Matching gegeben. Dabei wird in einer Datenbank typische Muster für eine Erkennung gespeichert. Eine Datei wird sodann auf eine typische Zeichenkette, die auf korrupten Programmcode hindeutet, untersucht. Ist eine Übereinstimmung gegeben, ist eine Infektion absehbar. Ein einfaches Beispiel dieser Technologie lässt sich mit W32.Blaster.Worm vortragen. Dabei fand sich im kompilierten Wurm die Zeichenkette „I just want to say LOVE YOU SAN!! billy gates why do you make this possible? Stop making money and fix your software!!“. Eine Antiviren-Lösung musste eine Datei lediglich auf diesen Inhalt hin untersuchen, um die Existenz des Blaster-Wurms verifizieren zu können. Grundlegende Einschränkung des Pattern-Matchings ist, dass ein Virus und seine Struktur zuerst bekannt sein müssen. Eine Antiviren-Lösung kann eine Infektion nur dann feststellen, wenn das entsprechende Muster in der Datenbank gespeichert wurde.

Aufgrund der Limitierungen des starren Pattern-Matchings wurde die sogenannte heuristische Suche als Alternative entwickelt. Hierbei untersucht die Antiviren-Lösung das Verhalten einer Software, um typische Vorgehensweisen von korruptem Programmcode zu identifizieren. Beispielsweise deutet das Überschreiben einer ausführbaren Datei auf einen Dateivirus hin. Oder das Formatieren eines Datenträgers auf die Schadroutine eines besonders heimtückischen Schädlings. Aber auch bei der heuristischen Suche kann es zu Problemen kommen. Und zwar lassen sich nicht sämtliche Vorgehensweisen von Viren-Entwicklern abbilden. Das Übersehen von Schadroutinen oder die fehlerhafte Identifikation einer solcher (z.B. bei einem Partitionierungs-Programm) sind durchaus möglich.

195



Um ein besseres Verständnis für Computerviren, Antiviren-Lösungen und deren Hintergründe zu erlangen, wird diese Übung herangezogen. hierbei geht es um die Analyse eines Pseudo-Virus. Diesen können Sie von der Workshop-Webseite auf Ihren Rechner herunterladen. Entpacken Sie das ZIP-Archiv mit einem Packer Ihrer Wahl (z.B. WinZip). Lesen Sie danach die Anweisungen in der Text-Datei durch, die in eben diesem Archiv enthalten war. Öffnen Sie nun die Pseudo-Virus-Datei mit einem Text- oder HEX-Editor. Sie können dazu das Notepad von Windows gebrauchen. Dieses öffnen Sie über den Button Start, die Auswahl von Programs, das Selektieren von Accessories und das Anwählen von Notepad. Gehen Sie nun auf File/Open, um die besagte Datei zu öffnen. Hierbei handelt es sich um einen Pseudo-Virus, der weder lauffähig noch von destruktiver Natur ist. Führen Sie nun eine Analyse dieser Datei durch und beantworten Sie die Fragen. Ob und inwiefern können Sie ein Pattern ausmachen, mit dem sich dieser Virus eindeutig identifizieren liesse? Können Sie zudem irgendwelche Merkmale ausmachen, die Rückschlüsse auf den Entwickler bzw. dessen Herkunft zulassen?

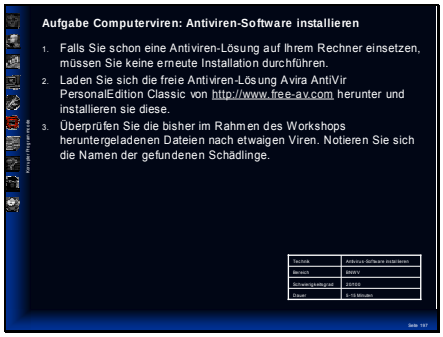
196



Die Analyse des Pseudo-Virus erfolgt hierbei durch ein simples Reverse Engineering, bei dem die kompilierte Fassung dessen betrachtet wird. Als eindeutige Identifikation der Datei lässt sich die Zeichenkette „Tröööt, MARC wants a CAKE!" identifizieren. Dieses Pattern liesse sich innerhalb einer Antiviren-Lösung einfach implementieren, um den Schädling ausmachen zu können.

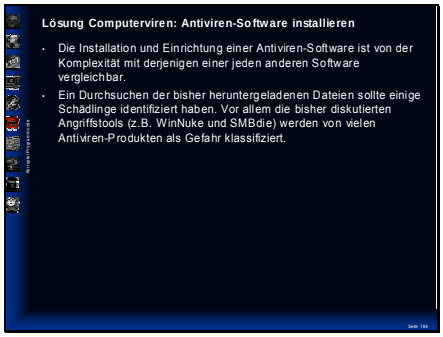
Desweiteren deutet der Einsatz von Umlauten innerhalb dieser Zeichenkette darauf hin, dass der Entwickler aus einem Land kommt, das ein derartiges Charset einsetzt. Länder mit englischen Wurzeln können damit theoretisch ausgeschlossen werden. Viel eher kommen Staaten wie die Schweiz, Deutschland, Österreich oder Liechtenstein in Frage. Dies ist eine gute Grundlage für ein soziodemographisches Profiling des Viren-Entwicklers.

197



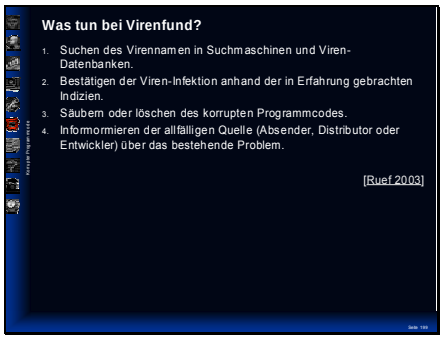
Wir wollen uns nun mit der Handhabung einer Antiviren-Lösung vertraut machen. Dazu wollen wir die freie Software Avira AntiVir installieren. Sollten Sie auf Ihrem Rechner schon ein Antiviren-Produkt im Einsatz haben, können Sie von einer erneuten Installation einer solchen absehen. Falls dem nicht so ist, gehen Sie auf die Webseite des Herstellers unter http://www.free-av.com und laden Sie sich die PersonalEdition Classic herunter. Installieren Sie nach dem Download die Software und starten Sie sie auf. Überprüfen Sie nun im Rahmen des Workshops sämtliche bisher heruntergeladenen Dateien auf schädlichen Programmcode. Notieren bzw. speichern Sie die Namen der gefundenen Schädlinge.

198



Die Installation und Einrichtung einer Antiviren-Software ist von der Komplexität mit derjenigen einer jeden anderen Software vergleichbar. Ein Durchsuchen der bisher heruntergeladenen Dateien sollte einige Schädlinge identifiziert haben. Vor allem die bisher diskutierten Angriffstools (z.B. WinNuke und SMBdie) werden von vielen Antiviren-Produkten als Gefahr klassifiziert.

199



Für viele Endanwender stellt sich irgendwann einmal die Frage, was bei einem Virenbefund überhaupt zu tun ist. Meldet eine der genutzten Antiviren-Lösungen korrupten Programmcode, sollte man sich als erstes über den vermeintlichen Schädling informieren. Viele moderne Antiviren-Produkte bieten dazu eine Offline-Datenbank an, in der man knappe Informationen zur Situation findet. Viel besser ist man aber mit den Online-Datenbanken bedient, durch die sehr aktuelle und zuverlässige Details zu den jeweiligen Viren und ihren Abkömmlingen bereitgestellt werden. Eine Abfrage mit dem Namen des gefundenen Schädlings über eine Suchmaschine dürfte schnell Informationen zusammentragen lassen. Dabei wird oftmals erläutert, anhand welcher Indizien sich die Infektion durch den Virus ausmachen lässt. Überprüfen Sie diese Hinweise, um ganz sicher zu sein, dass es sich auch wirklich um den ganz bestimmten Virus handelt.

Antiviren-Produkte erlauben sodann das säubern, löschen oder verschieben der infizierten Dateien. Bevorzugen Sie das säubern, um den Original-Zustand einer Datei wieder herzustellen und diese auch weiterhin nutzen zu können. Falls das nicht möglich ist – weil es sich zum Beispiel um einen überschreibenden Dateivirus handelt – sollten Sie die Datei löschen. Damit geht natürlich ein Datenverlust einher. Sollten Sie durch ein Backup den betriebsbereiten Zustand wiederherstellen wollen, überprüfen Sie sicherheitshalber auch die älteren Versionen auf allfällige Infektionen.

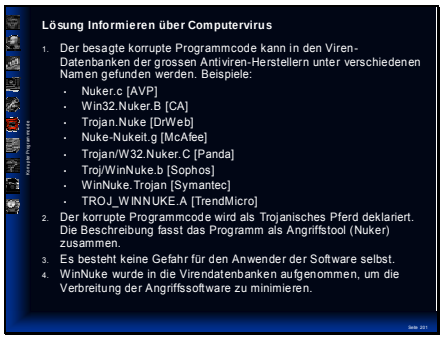
Sollte es sich um das erstmalige Auftreten eines Schädlings handeln oder das Verhalten von dem der öffentlichen Viren-Datenbanken abweichen, informieren Sie den Hersteller und Ihr CERT (Computer Emergency Response Team) über den Sachverhalt. Diese werden sich sodann der Sache annehmen und weitere Schritte einleiten.

200



Gehen wir nun davon aus, dass Ihre Antiviren-Lösung in einem der von Ihnen heruntergeladenen Dateien einen Virus mit dem Namen „WinNuke" findet. Informieren Sie sich nun mit Hilfe von Suchmaschinen und Viren-Datenbanken (z.B. http://www.symantec.com/avcenter/vinfodb.html) über diesen Schädling. Handelt es sich dabei wirklich um destruktive Software? Und welches Vorgehen schlagen Sie vor?

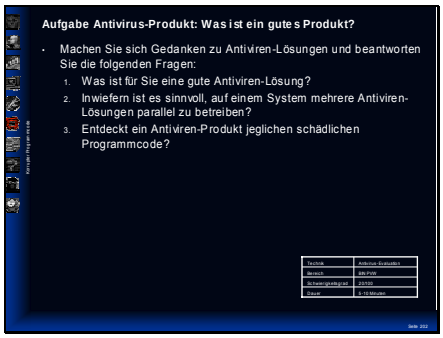
201



Der besagte korrupte Programmcode kann in den Viren-Datenbanken der grossen Antiviren-Herstellern unter verschiedenen Namen gefunden werden (siehe dazu http://www.symantec.com/avcenter/venc/data/winnuke.trojan.html). Dies ist ein grundlegendes Problem der Antiviren-Hersteller, da sich diese nur selten auf einen einheitlichen Namen, der eine Recherche vereinfachen würde, einigen können. Ein wildes Durcheinander ist vor allem dann gegeben, wenn verschiedene Versionen eines Schädlings auftauchen. Einige Hersteller nummerieren diese anders weder andere und komplettieren damit das Terminologie-Chaos.

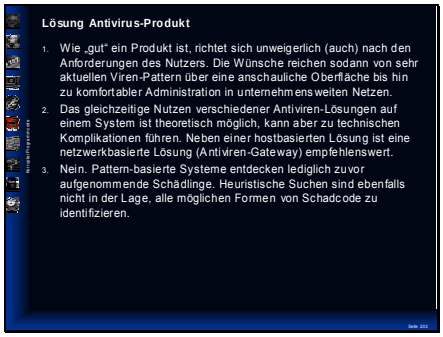
Der korrupte Programmcode wird oftmals als Trojanisches Pferd deklariert, wobei die Beschreibung das Programm als Angriffstool (Nuker) zusammenfasst. Es besteht keine Gefahr für den Anwender der Software selbst, denn diese wird lediglich für das Umsetzen einer klassischen Denial of Service-Attacke gegen ältere Windows-Systeme eingesetzt. WinNuke wurde in die Virendatenbanken aufgenommen, um die Verbreitung der Angriffssoftware zu minimieren, so dass nicht versehentlich oder absichtlich mit dieser Angriffe umgesetzt werden.

202



Als Übung wollen wir nun darüber diskutieren, was eine gute Antiviren-Lösung ausmacht. Was ist denn für Sie eine gute Antiviren-Lösung? Welche Funktionen und Prioritäten sollte diese aufweisen? Inwiefern ist es sinnvoll, auf einem System mehrere Antiviren-Lösungen parallel zu betreiben? Beantworten Sie zum Schluss die Frage, ob denn nun ein Antiviren-Produkt jeglichen schädlichen Programmcode rechtzeitig zu entdecken in der Lage ist.

203

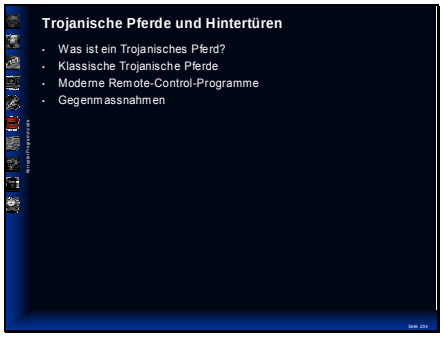


Wie „gut“ ein Produkt ist, richtet sich unweigerlich (auch) nach den Anforderungen des Nutzers. Die Wünsche reichen sodann vom kleinen Preis über sehr aktuellen Viren-Pattern oder eine anschauliche Oberfläche bis hin zu komfortabler Administration in unternehmensweiten Netzen. Wie bei jeder Produkte-Evaluation gilt es einen Anforderungskatalog zu erstellen, in dem die Bedürfnisse adressiert werden. Nur so lässt sich das passende Produkt ausmachen.

Das gleichzeitige Nutzen verschiedener Antiviren-Lösungen auf einem System ist theoretisch möglich, kann aber zu technischen Komplikationen führen. Neben einer hostbasierten Lösung ist eine netzwerkbasierte Lösung (Antiviren-Gateway) empfehlenswert.

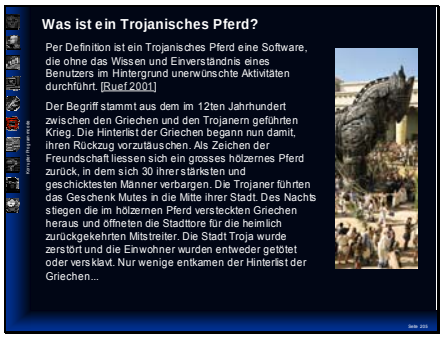
Pattern-basierte Systeme entdecken zudem lediglich zuvor aufgenommene Schädlinge. Heuristische Suchen sind ebenfalls nicht in der Lage, alle möglichen Formen von Schadcode zu identifizieren. Eine Kombination dieser Techniken ist empfehlenswert, um eine möglichst umfassende Abdeckung der Entdeckung gewährleisten zu können.

204



Wenden wir uns nun von den Computerviren und –würmern ab, um uns mit Trojanischen Pferden und Hintertüren zu beschäftigen. Nach einer Einführung ins Thema werden wir uns mit der Funktionsweise klassischer Trojanischer Pferde auseinandersetzen. Danach fokussieren wir uns auf eine praxisnahe Analyse des Umgangs von modernen Remote-Control-Programmen, mit dessen Hilfe sich komfortable Hintertüren umsetzen lassen. Zum Schluss wollen wir besprechen, wie moderne Trojanische Pferde erkannt und dessen Einsatz verhindert werden kann.

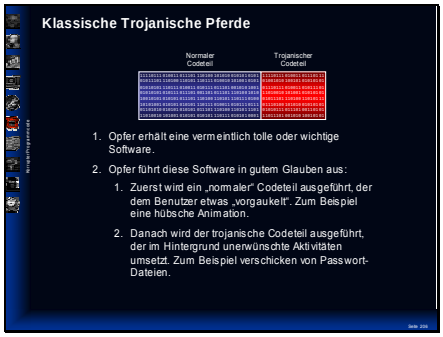
205



Per Definition ist ein Trojanisches Pferd eine Software, die ohne das Wissen und Einverständnis eines Benutzers im Hintergrund unerwünschte Aktivitäten durchführt.

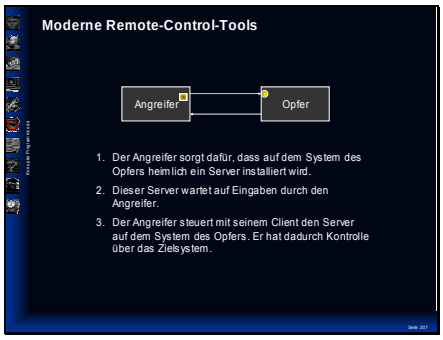
Der Begriff stammt aus dem im 12ten Jahrhundert zwischen den Griechen und den Trojanern geführten Krieg. Die Hinterlist der Griechen begann nun damit, ihren Rückzug vorzutäuschen. Als Zeichen der Freundschaft liessen sich ein grosses hölzernes Pferd zurück, in dem sich 30 ihrer stärksten und geschicktesten Männer verbargen. Die Trojaner führten das Geschenk Mutes in die Mitte ihrer Stadt. Des Nachts stiegen die im hölzernen Pferd versteckten Griechen heraus und öffneten die Stadttore für die heimlich zurückgekehrten Mitstreiter. Die Stadt Troja wurde zerstört und die Einwohner wurden entweder getötet oder versklavt. Nur wenige entkamen der Hinterlist der Griechen...

206



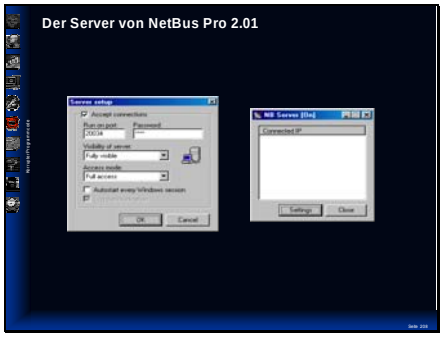
Klassische Trojanische Pferde setzten erstmals das Konzept des hölzernen Pferdes mit hohlem Bauch auch auf dem Computer um. (1) Dabei erhält ein Opfer eine vermeintlich wichtige oder interessante Software, welche natürlich unbedingt und sofort ausgeführt werden will. (2.1) Neben einem normalen Codeteil, der ausgeführt wird, (2.2) wird im Hintergrund ebenfalls eine unerwünschte Prozedur durchlaufen, die die Umgebung zu kompromittieren in der Lage ist. Dies reicht vom Einrichten eines neuen Benutzers über das Deaktivieren von Antiviren-Software bis hin zum Verschicken von Passwörtern.

207



Moderne Remote-Control-Tools (auch Remote-Access-Tools oder RAS genannt), sind eine spezielle Form der Trojanischen Pferde. (1) Dabei generiert ein Angreifer einen Server, den er dem Opfer zukommen lässt. Dies ist ebenfalls ein Stück Software, das aus irgendeinem Grund gestartet werden will. (2) Nachdem der Server als trojanischer Teil des Pakets gestartet wurde, bindet er sich an einen Port und wartet auf Eingaben durch den Angreifer. (3) Sodann kann der Angreifer durch eine etablierte Verbindung zum Server das Zielsystem fernsteuern, als sässe er direkt davor.

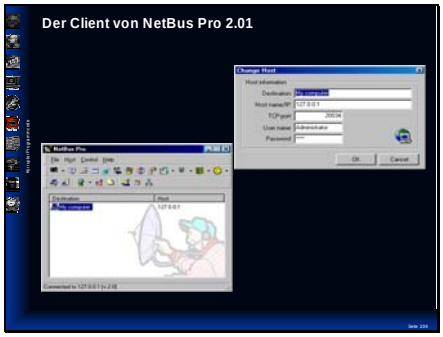
208



Neben SubSeven und BackOrifice (Abk. BO) ist vor allem NetBus ein sehr populäres Trojanisches Pferd mit Remote-Control-Funktionalität. Die Abbildungen Zeigen den Server-Teil. Links sehen wir die Konfigurations-Einstellungen des Servers. In diesem lässt sich der Zugriff pauschal aktivieren und deaktivieren („Accept connections"). Ist ein Zugriff erlaubt, kann der Port, an den sich der Server bindet, eingestellt werden. Standardmässig wird dieser an tcp/20034 gebunden. Ebenfalls lässt sich ein Passwort für den Zugriff einstellen. Angreifer verhindern so, dass auch andere Leute von einer Infektion einen Vorteil erlangen können. Mit der „Visibility of server" wird die Sichtbarkeit des Servers und mit „Access mode" die Zugriffsberechtigung eingestellt.

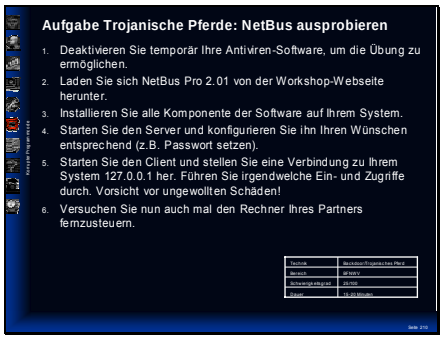
Rechts sehen wir nun den angezeigten Server, wie er auf einem infizierten System untergebracht wäre. Durch das Anzeigen dessen lassen sich etablierte Verbindungen identifizieren. Ein Angreifer ist natürlich darauf aus, dass diese Information, die auf eine Infektion durch NetBus hinweisen würde, für das Opfer nicht ersichtlich ist. Aus diesem Grund kann der Server ebenfalls unsichtbar konfiguriert werden.

209



Der Client von NetBus überzeugt durch seine Übersichtlichkeit. In der Liste lassen sich verschiedene Systeme, die einen NetBus-Server bereitstellen, definieren. Diese können mit einem Namen, ihrer IP-Adresse, dem zugewiesenen Zielport und den Anmeldeinformationen (Benutzername und Passwort) abgespeichert werden. Durch einen Doppelklick auf einen Eintrag lässt sich die Verbindung herstellen. Sodann ist eine Fernsteuerung möglich. Diese kann wahlweise durch die Icons in der Toolbar oder durch die Einträge des Frame-Menüs umgesetzt werden. Vom Auslesen und Kopieren von Dateien bis hin zur Fernsteuerung der Maus und Tastatur ist alles möglich. Selbst Dinge, die ein Administrator in einem herkömmlichen Windows-Umfeld zu machen nicht in der Lage ist.

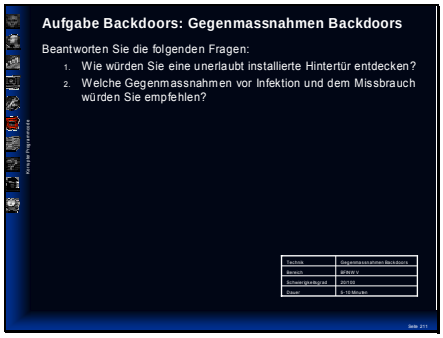
210



Probieren Sie nun NetBus selber aus. Deaktivieren Sie dazu temporär die Antiviren-Software auf Ihrem System. Dadurch soll eine Intervention dieser verhindert werden, so dass wir eine kontrollierte Infektion des Hosts zulassen können. Laden Sie nun NetBus von der Workshop-Webseite auf Ihren Rechner herunter und installieren Sie sowohl den Client als auch den Server. Starten Sie nun den Server auf und konfigurieren Sie diesen Ihren Wünschen entsprechend. Anpassungen an den Einstellungen sind für die Testzwecke eigentlich nicht erforderlich.

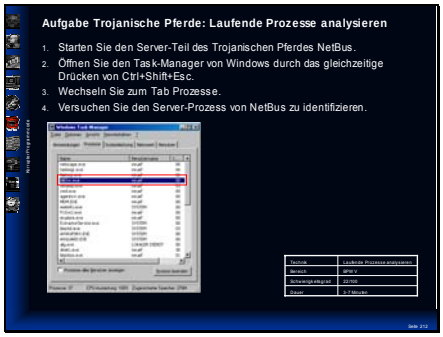
Starten Sie nun den Client und stellen Sie eine Verbindung zu Ihrem eigenen System her. Eröffnen Sie dazu eine neue Verbindung, bei der Sie als IP-Adresse ihre Loopback-Adresse (127.0.0.1) und als Zielport den vordefinierten Port angeben. Speichern Sie den Eintrag und doppelklicken Sie ihn, um eine Verbindung herzustellen. Den Status einer solchen Erkennen Sie unten in der Statusbar des Clients. Sobald eine Verbindung erfolgreich hergestellt werden konnte, können Sie die jeweiligen Funktionen von NetBus ausprobieren. Seien Sie jedoch vorsichtig, löschen Sie nicht ungewollt Dateien oder fahren den Rechner herunter.

211



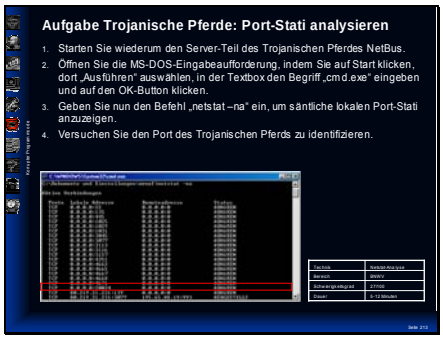
Nachdem Sie nun die Funktionsweise von Remote-Control-Utilities und im Spezifischen von NetBus kennengelernt haben, beantworten Sie einige Fragen. Wie würden Sie eine unerlaubt installierte Hintertür entdecken? Und welche Gegenmassnahmen würden Sie empfehlen, damit eine Infektion durch eine solche und die Nutzung dieser verhindert werden kann?

212



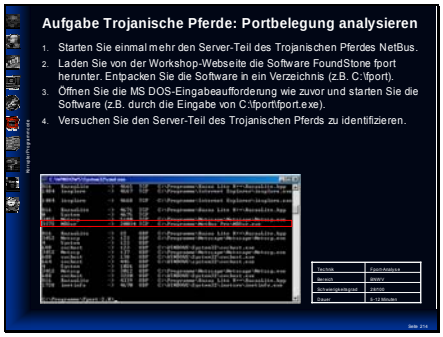
Die Beantwortung der zuvor gestellten Fragen wollen wir gleich mit einer neuen Übung umsetzen. Als erstes wollen wir mit der Hilfe des Taskmanagers die laufenden Prozesse analysieren. Starten Sie dazu erst den Server-Teil von NetBus, um eine ungewollte Einbringung einer Hintertür zu simulieren. Öffnen Sie nun den Taskmanager von Windows durch das Drücken der Tastenkombination Ctrl+Shift+Esc. Nach wenigen Augenblicken sollte sich dieser öffnen und sofort die gegenwärtigen Prozesse des Systems anzeigen. Falls zuerst andere Daten eingeblendet werden sollten, wechseln Sie zum Tab „Prozesse“. Versuchen Sie nun den Server-Prozess von NetBus zu identifizieren. Sie sollten nämlich hierbei den Namen der gestarteten EXE-Datei (namentlich NBSvr.exe) finden, sofern diese zuvor nicht umbenannt wurde.

213



Neben der Prozess-Analyse kann auch die Port-Analyse eine Netzwerk-Hintertür identifizieren lassen. Sorgen Sie dafür, dass der Server-Teil von NetBus noch immer gestartet ist, um die Hintertür zu simulieren. Öffnen Sie nun die MS DOS-Eingabeaufforderung, indem Sie auf Start klicken, dort „Ausführen“ auswählen, in der Textbox den Begriff „cmd.exe“ eingeben und den OK-Button drücken. Sodann sollte sich die schwarze Eingabezeile öffnen. In dieser können Sie nun mit der Eingabe von „netstat –na“ die aktuellen Port-Stati des eigenen Hosts anzeigen lassen. Dort sollte beim Protokoll TCP (Proto) die lokale Adresse 0.0.0.0:20034 im Status ABHÖREN gegeben sein. Dies bedeutet, dass auf Ihrer Netzwerkschnitsttelle für den Port 20034 für sämtliche Quelladressen nach Anfragen gehorcht wird. Der Server hat sich also an diesen Port gebunden. Der Port kann variieren, jenachdem wie der NetBus-Server konfiguriert wurde.

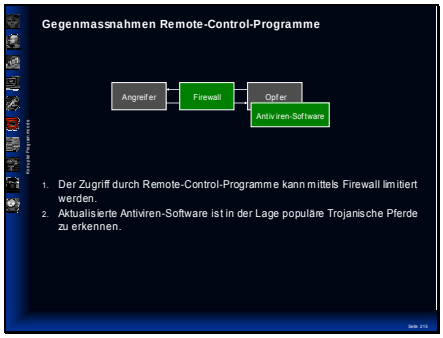
214



Mit der lokalen Port-Analyse von netstat lassen sich unerwünschte Server-Elemente sehr gut ausmachen. Doch leider zeigt uns das besagte Netzwerkdiagnoseutility nicht an, welcher Prozess sich da an den Port gebunden hat. Zu diesem Zweck hat das US-Amerikanische Unternehmen Foundstone (http://www.foundstone.com/) ein freies Tool mit dem Namen fport entwickelt [McClure et al. 2003]. Dieses funktioniert ähnlich wie netstat, ist aber in der Lage dide Prozess-ID, den Prozessnamen und den Pfad des assoziierten Programms auszugeben.

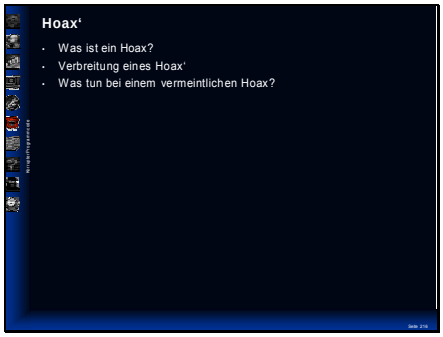
Starten Sie einmal mehr den Server-Teil von NetBus, um die Hintertür zu aktivieren. Laden Sie nun das Tool fport von der Workshop-Webseite auf Ihren Rechner herunter. Das ZIP-Archiv entpacken Sie mit einem Tool wie WinZip. Öffnen Sie nun die MS DOS-Eingabeaufforderung wie zuvor und starten Sie fport. Haben Sie das Tool beispielsweise in das Verzeichnis C:\fport\ entpackt, können Sie dies innerhalb der Kommandozeile mit der Eingabe von C:\fport\fport.exe tun. Sodann wird Ihnen ähnlich wie bei netstat die jeweiligen Portbelegungen mit erweiterten Details angezeigt. Versuchen Sie nun anhand des Prozessnamens, der Portnummer oder der Pfadangabe den laufenden Prozess des NetBus-Servers zu identifizieren.

215



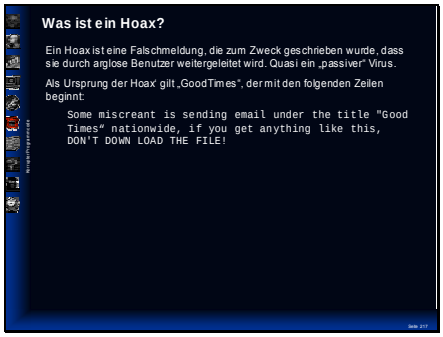
Hintertüren in Form von netzwerkbasierten Remote-Control-Programmen können auf verschiedenen Ebenen entgegnet werden. Einmal sind aktualisierte Antiviren-Lösungen in der Regel in der Lage, eine drohende Infektion durch einen Server abzuwenden. Dabei ist aber zu beachten, dass dies bei individuellen Anfertigungen von Remote-Control-Software nur selten der Fall ist. Hierbei kommt einmal mehr der Nachteil des Pattern-Matchings zum Tragen. Zudem kann aber mit einer Firewall verhindert werden, dass der Angreifer über das Netzwerk eine Verbindung zum Opfer herstellen kann. Dabei bleibt zwar die Infektion und damit der Server auf dem Host des Opfers bestehen, aber es kann kein Missbrauch umgesetzt werden.

216



Hoax‘ können ebenfalls zu schädlichem Programmcode zugeteilt werden. Wir wollen uns deshalb anschauen, was ein Hoax genau ist und wie eine Verbreitung eines solchen aussieht. Ebenso wollen wir besprechen, wie man sich am besten bei einem vermeintlichen Hoax verhalten soll.

217



Ein Hoax ist eine Falschmeldung, die zum Zweck geschrieben wurde, dass sie durch arglose Benutzer weitergeleitet wird. Quasi ein „passiver" Virus. Als Ursprung der Hoax' gilt „GoodTimes", der mit den folgenden Zeilen beginnt: „Some miscreant is sending email under the title "Good Times" nationwide, if you get anything like this, DON'T DOWN LOAD THE FILE! "

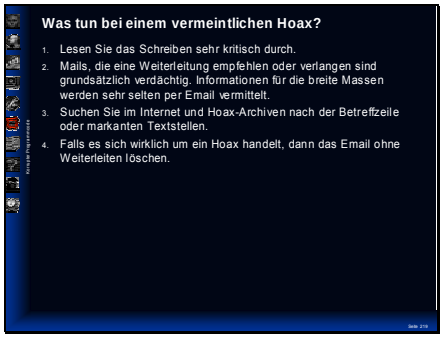
218



Die Verbreitungsstruktur eines Hoax ist derjenigen eines Computervirus oder –wurms sehr ähnlich. Auch hier kommt ein viraler Effekt zum Tragen, wobei die Falschmeldung jedoch manuell durch die Benutzer weitergeschickt wird. Es findet also keine automatisierte Infektion und Weiterverbreitung statt. Der Angriff setzt viel mehr auf psychologischer Ebene an.

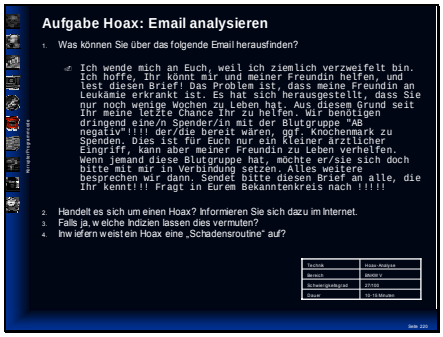
Oftmals wird bei derartigen Kettenbriefen damit gelockt, dass ein Weitersenden an 5 seiner Freunde einen Gewinn mit sich bringen würde. Ein beliebter Hoax des Chat-Systems ICQ ist, dass wenn man die Nachricht an seine Freunde weiterleitet, man ein spezielles Icon zugeteilt bekommt. Oder im Netzwerk der Swisscom werden immerwieder Hoax-SMS verschickt, bei denen damit gelockt wird, dass ein Weiterleiten eine Gratisnutzung des Dienstes mit sich führen würde. Dies ist natürlich alles Unsinn.

219



Um die Verbreitung von Hoax zu verhindern, sollten Sie stets jeglicher Information, die Ihnen zugekommen lassen wird, kritisch begutachten. Mails, die eine Weiterleitung empfehlen oder verlangen sind grundsätzlich verdächtig. Informationen für die breiten Massen werden sehr selten per Email vermittelt. Dazu zählen sowohl Patches durch grosse Software-Konzerne wie Microsoft oder ein Spendenaufruf für krebskranke Kinder. Sollten Sie der Meinung sein, dass Ihnen ein Hoax geschickt wurde, informieren Sie sich mittels Suchmaschinen und Hoax-Archiven über das Schreiben. Durch die Betreffzeile oder markante Textstellen lassen sich die Echtheit eines Schreibens oftmals gut falsifizieren. Falls es sich wirklich um ein Hoax handelt, dann das Email ohne Weiterleiten löschen. In einzelnen Fällen kann es sich lohnen, den Absender über den Hoax zu informieren und ihn darum zu bitten, derartige Schreiben in Zukunft nicht mehr zu verschicken.

220



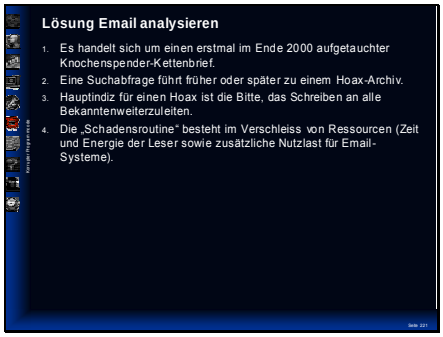
Was können Sie nun über folgenden Text, der per Email eingetroffen ist, herausfinden:

Was können Sie über das folgende Email herausfinden?

„Ich wende mich an Euch, weil ich ziemlich verzweifelt bin. Ich hoffe, Ihr könnt mir und meiner Freundin helfen, und lest diesen Brief! Das Problem ist, dass meine Freundin an Leukämie erkrankt ist. Es hat sich herausgestellt, dass Sie nur noch wenige Wochen zu Leben hat. Aus diesem Grund seit Ihr meine letzte Chance Ihr zu helfen. Wir benötigen dringend eine/n Spender/in mit der Blutgruppe "AB negativ"!!!! der/die bereit wären, ggf. Knochenmark zu Spenden. Dies ist für Euch nur ein kleiner ärztlicher Eingriff, kann aber meiner Freundin zu Leben verhelfen. Wenn jemand diese Blutgruppe hat, möchte er/sie sich doch bitte mit mir in Verbindung setzen. Alles weitere besprechen wir dann. Sendet bitte diesen Brief an alle, die Ihr kennt!!! Fragt in Eurem Bekanntenkreis nach !!!!!“

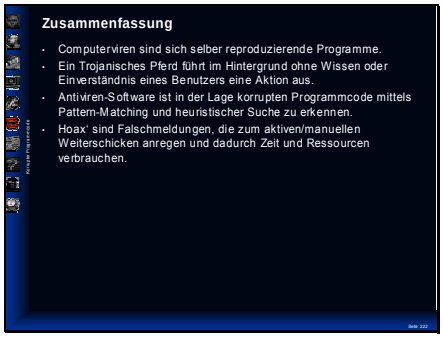
Handelt es sich um einen Hoax? Informieren Sie sich dazu im Internet. Falls ja, welche Indizien lassen dies vermuten? Und inwiefern weist ein Hoax eine „Schadensroutine“ auf?

221



Eine Recherche zum besagten Text sollte ergeben haben, dass es sich hier um einen Hoax handelt. Dieser, der auch mit dem Namen „Knochenspender-Kettenbrief“ in diversen Hoax-Archiven geführt ist, tauchte erstmals Ende 2000 auf. Hauptindiz für einen Hoax ist die Bitte, das Schreiben an alle Bekanntenweiterzuleiten. Die „Schadensroutine“ eines Hoax besteht grundsätzlich im Verschleiss von Ressourcen (Zeit und Energie der Leser sowie zusätzliche Nutzlast für Email-Systeme). Im Gegensatz zu Computerviren und –würmern setzt er jedoch auf psychologischer Ebene an.

222

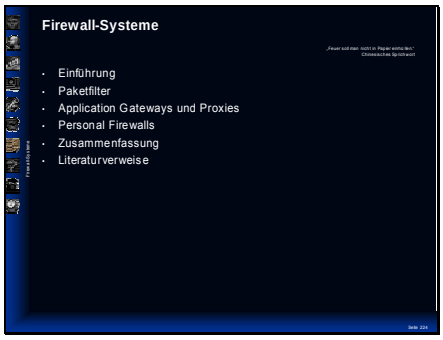


Als Definition von Computerviren können wir sagen, dass es sich dabei um sich selber reproduzierende Programme handelt. Andere Funktionen wie Schadensroutinen sind nicht zwingend Teil eines Computervirus. Ein Trojanisches Pferd hingegen, führt im Hintergrund und ohne das Wissen des Anwenders andere Tätigkeiten weder die vorgegebenen durch. Moderne Trojanische Pferde etablieren nach dem traditionellen Client/Server-Prinzip Hintertüren (engl. Backdoors), die das netzwerkgestützte Fernsteuern von Hosts erlauben. Mit der Hilfe von Antiviren-Software lässt sich korrupter Programmcode begegnen. Zur Identifikation dessen wird sowohl Pattern-Matching als als heuristische Suchen herangezogen. Und bei einem Hoax handelt es sich um eine Falschmeldung, die als Kettenbrief getarnt weitergeschickt werden soll und damit nur unnötig Ressourcen verbraucht.

223



224



Firewall-Systeme galten lange Zeit als das Herzstück eines modernen Netzwerks. Nach einer Einführung in die Grundlagen dieser wollen wir uns mit den beiden Technologien der Paketfilter und Application Gateway auseinandersetzen. Dabei werden wir ebenfalls auf die Vor- und Nachteile der beiden Ansätze eingehen. Desweiteren besprechen wir die Funktionsweise von Personal Firewalls, die hostbasiert die Sicherheit eines Systems erweitern sollen. Im letzten Schritt besprechen wir die Konzeption einer Firewall-Lösung, was als Grundpfeiler des Einsatzes einer solchen gilt.

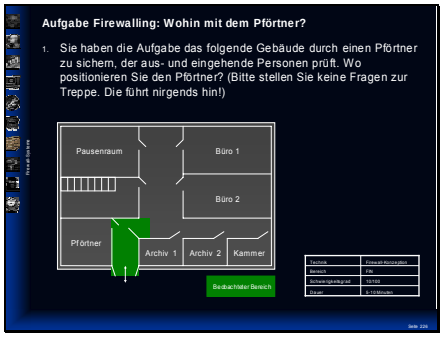
225



Dr. Norbert Pohlmann schreibt in seinem Buch „Firewall-Systeme", dass unter einer Firewall eine Kombination aus elektronischer Brandschutzmauer und Pförtner verstanden werden kann. Die Brandschutzmauer sorgt dafür, dass sich ein Brand innerhalb eines Gebäudes nicht ausweitet und die Flammen nicht auf andere Teile übergreifen kann. Genauso ist es bei einer Firewall, die Angriffe einschränken und die Ausbreitung von Viren sowie Würmern verhindern soll.

Der Pförtner hingegen ist für die Überprüfung und Protokollierung des Durchgangs zuständig. Er schaut, welche Personen und Objekte das Gebäude betreten und verlassen. Diese Ein- und Austritte werden Protokolliert, um Anomalien festzustellen und nachträglich Rückschlüsse bei fehlerhaftem Verhalten machen zu können. Genauso ist auch eine Firewall dafür zuständig, dass die die passierenden Datenpakete und Kommunikationen überprüft und protokolliert. Letzteres ist sowohl bei einer Fehlersuche als auch in Bezug auf die elektronische Einbruchserkennung eine wichtige Sache.

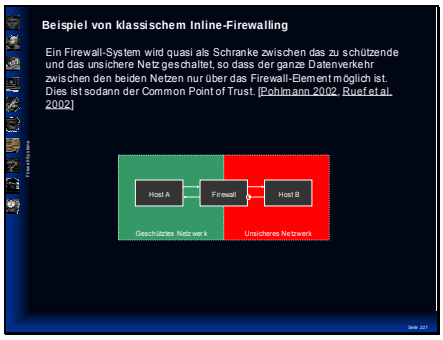
226



Um die grundlegende Funktion eines Firewall-Elements verstehen zu können, wollen wir uns mit einer speziellen Übung beschäftigen. Sie sehen hier den Grundrissplan eines Gebäudes. Darin sehen Sie im Süden den Haupteingang. Desweiteren finden sich diverse Räume und Durchgänge im Gebäude. Wo würden Sie nun den Pförtner positionieren, um ein Höchstmass an Effektivität durch diesen gewährleisten zu können?

Da der Pförter die Ein- und Ausgänge überwachen und protokollieren muss, sollte er entsprechend in der Nähe des Haupteingangs platziert werden. Mit der Bildung eines solchen Foyers kann er den Überblick wahren und seiner Aufgabe nachkommen.

227



Klassisches Firewalling versteht sich als Inline-Element. Dabei wird, wie im Beispiel des Pförtners, der Ein- und Ausgang eines zu schützenden Netzwerks überwacht. Die Firewall wird dabei zwischen das geschützte und das unsichere Netzwerk gestellt. Möchte nun ein System aus dem geschützten Netzwerk auf ein System im unsicheren Netzwerk zugreifen, muss es in jedem Fall die Firewall am Perimeter passieren. Diese überprüft, protokolliert und limitiert die Verbindung entsprechend Ihrer Konfiguration. Selbiges gilt natürlich, und dies ganz besonders, in umgekehrter Richtung, wenn Host B aus dem unsicheren Netzwerk auf Host A im geschützten Netzwerk zugreifen möchte. Da eine Kommunikation dieser zwei Netze nur über die eine Verbindung durch die Firewall möglich ist, spricht man von einem Common Point of Trust – Also ein zentraler Punkt, der das Vertrauen einer Verbindung zu gewährleisten versucht.

228

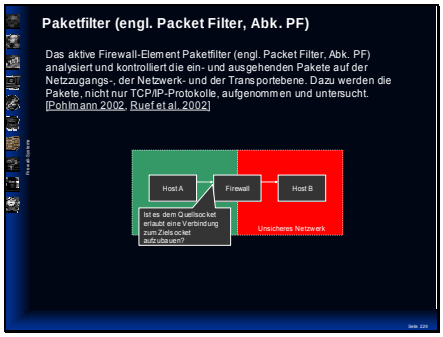


Firewalls werden in verschiedenen Formen angeboten. Grundsätzlich können moderne Betriebssysteme mit Netzwerkunterstützung zu Firewalls umfunktioniert werden. Dazu lässt sich eine entsprechende Software nachrüsten, die sodann ein Routing, Limitieren und Protokollieren von Netzwerkverbindungen zulässt. Mit einer Linux-Distribution, einige von ihnen sind gar extra dafür entwickelt worden, kann eine solche Lösung kostengünstig und effizient umgesetzt werden. In Windows-Umgebungen kann eine ähnliche Funktionalität ebenfalls mittels kostengünstigen Personal Firewalls eingebracht werden.

Im privaten Bereich und bei KMUs haben sich in den letzten fünf Jahren Appliances eingebürgert. Dabei handelt es sich um kleine Kästchen, die die Grösse und Funktionsweise eines simplen Routers samt ACL (Access Control List) mit sich bringen. Diese Geräte können meist dank verschiedener Interfaces wie ein Hub betrieben werden. Sie sind mit einem eigenen Betriebssystem ausgestattet, dass die entsprechende Firewall-Funktionalität gewährleistet. Populäre Lösungen sind jene von SonicWall, ZyWALL und NetGear. Aber auch viele andere Hersteller von Netzwerkelementen sind auf den Trend einfacher Firewall-Appliances aufgesprungen.

In hochkomplexen Umgebungen, in denen aufgrund einer erhöhten Datenverarbeitung besondere Anforderungen an die Performance eines Firewall-Systems gestellt werden, bieten professionelle Anbieter oftmals erweiterter Router-Elemente, Rack-Systeme oder Thin-PCs an. Diese sind quasi eine professionelle Ausgabe der kleineren Appliance-Boxen. Bessere Hardware und umfassendere Software-Komponenten machen derlei Lösungen vor allem für Grossfirmen interessant. Zum Einsatz kommen in diesen Bereichen mitunter die Lösungen von CheckPoint, Cisco und SideWinder.

229

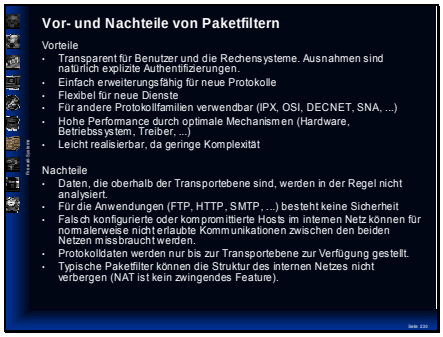


Es gibt verschiedene Firewall-Technologien. Wir wollen in dieser Vorlesung zwischen Paketfilter und Application Gateways unterscheiden. Das aktive Firewall-Element Paketfilter (engl. Packet Filter, Abk. PF) analysiert und kontrolliert die ein- und ausgehenden Pakete auf der Netzzugangs-, der Netzwerk- und der Transportebene. Dazu werden die Pakete, nicht nur TCP/IP-Protokolle, aufgenommen und untersucht.

Möchte ein Host A an der Schnittstelle 1 eine Verbindung zum Host B an der Schnittstelle 2 aufbauen, wird der Paketfilter als erstes die Socket-Informationen der gewünschten Kommunikation begutachten. Dabei wird die Quell-IP-Adresse, der Quell-Port, die Ziel-IP-Adresse und der Zielport mit den Regeln im Firewall-Regelwerk verglichen. Ist eine solche Regel vorhanden, wird entsprechend nach ihr reagiert. Eine erlaubte Verbindung wird zugelassen und transparent weitergeleitet. Der Paketfilter fungiert dann quasi als transparenter Router zwischen den Netzen.

Ist die Verbindung hingegen nicht zugelassen, wird sie unterbunden. Dabei kann zwischen einem Verbieten (endl. deny) und eine Verwerfen (engl. drop) unterschieden werden. Bei einem Deny schickt die Firewall eine ICMP- oder TCP-Fehlermeldung an das Quellsystem, um die unerlaubte Verbindung angemessen zu quittieren und wieder abzubauen. Diese höfliche Methode kann jedoch durch Angreifer genutzt werden, um eine Auswertung der Firewall-Konfiguration vorzunehmen. Entsprechend weichen viele sicherheitsbewusste Administratoren auf Drop-Regeln aus, bei denen im Fall einer unerwünschten Verbindung die Anfragen einfach verworfen werden. Durch das Ausbleiben der ICMP- oder TCP-Fehlermeldungen gestaltet sich ein Auswerten der Firewall schon schwieriger.

230

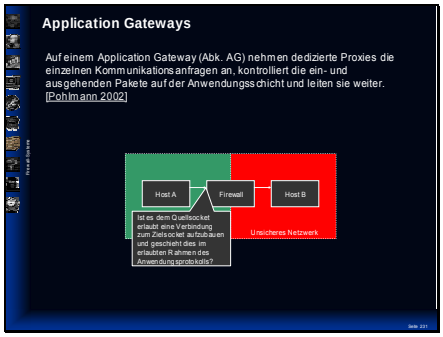


Wie jede Technologie weisen Paketfilter eine Vielzahl an Vor- und Nachteilen auf. Ein wichtiger Vorteil ist, dass sie für die Benutzer komplett transparent betrieben werden können. Sofern keine expliziten Authentisierungen bei einem Verbindungsaufbau vorgeschrieben wird, bekommt der Benutzer gar nichts von der Schutzmassnahme mit. Dies ist besonders in grossen Umgebungen von Vorteil, um den administrativen Aufwand und den Support so gering wie möglich zu halten.

Ein weiterer grosser Vorteil dieser Technologie ist, dass sie relativ simpel ist. Grob gesagt handelt es sich bei einem Paketfilter lediglich um einen Router mit einigen zusätzlichen Funktionen. ACL (Access Control List) und NAT (Network Address Translation) sind die herausragenden Unterschiede zu einem solchen. Diese Einfachheit sorgt dafür, dass sich ein solches System einfach warten lässt. Neue Protokollfamilien und Protokolle sind einfach implementiert. Das Fehlen von Komplexität sorgt ebenfalls dafür, dass die Fehleranfälligkeit bei der Entwicklung und Wartung sehr gering ist.

Der grösste Nachteil von Paketfiltern ist jedoch, dass die Daten und Kommunikationen normalerweise nicht oberhalb der Transportebene angeschaut werden. So lassen sich also nur IP- und TCP-/UDP-Informationen auswerten. IP-Adressen, Portnummern, gesetzte Flaggen und genutzte Optionen sind das einzige, was analysiert werden kann. Dies macht Paketfilter für eine Reihe von komplexen Angriffen verwundbar. So lassen sich diese sehr oft mittels Tunneling und simplem Port-Wechsel austricksen.

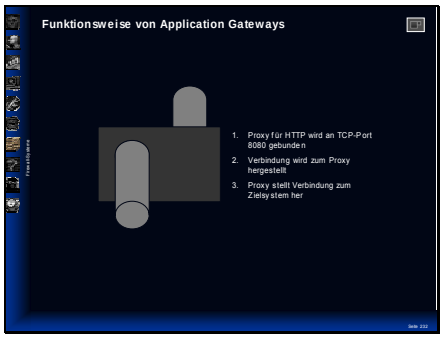
231



Um die Nachteile einer reinen Paketfilter-Umgebung aufzuheben, werden gerne Application Gateways zur Verfügung gestellt. Dies ist die zweite klassische Firewall-Technologie, bei der für einzelne Dienste dedizierte Proxies zur Verfügung gestellt werden. Ein Proxy ist quasi ein Dienst auf dem Firewall-Element, der sich weitestgehend wie ein herkömmlicher Server verhält. Möchte ein Client eine Verbindung über das Application Gateway hinweg aufbauen, muss er sich als erstes zum Proxy-Port verbinden. Auf diesem wird die eigentliche Verbindung hergestellt und auf Anfragen innerhalb der Netzwerkanwendung (z.B. HTTP oder SMTP) gewartet. Diese Anfragen werden sodann durch das Application Gateway verarbeitet und bei einer Erlaubnis an das eigentliche Ziel – den finalen Server – weitergeschickt. Dabei findet also eine Entkoppelung der Netze statt.

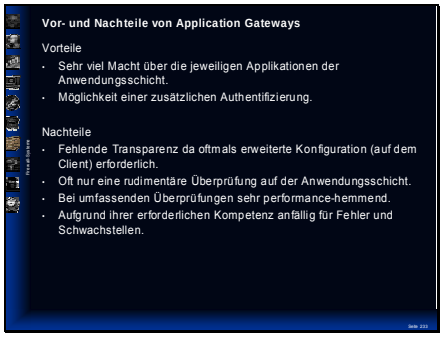
Neben den grundlegenden Informationen, die ein Paketfilter ebenfalls verarbeiten kann (IP-Adressen und Portnummern) lassen sich aber ebenfalls erweiterte Analysen auf der Applikationsschicht umsetzen. Der jeweilige Proxy weiss über jedes Kommando bescheid und kann gar ein solches auf seine Richtigkeit hin überprüfen. So ist es gar möglich, dass bestimmte Befehle, wie zum Beispiel die POST-Methode bei HTTP, verhindert wird. In einem solchem Fall generiert das Proxy-Element meistens eine reguläre Fehlermeldung im Rahmen der Dienst-Kommunikation. Dabei wird meist eine Meldung im Sinn von „nicht unterstützt“ (engl. not supported) oder „nicht zugelassen“ (engl. not allowed) an den Client gemeldet.

232



Die Funktionsweise eines Proxies auf einem Application Gateway ist in der ersten Phase derjenigen eines herkömmlichen Servers ähnlich. (1) Der Proxy-Dienst wird auf dem Application Gateway gestartet und bindet sich an einen Port. An diesem wartet er nun auf eingehende Verbindungen durch Clients, die über die Firewall hinweg eine Verbindung im Rahmen des angebotenen Dienstes nutzen wollen. (2) Nun baut ein Client eine Verbindung zu einem Zielsystem oder direkt zum Proxy auf. Die Verbindung zwischen dem Client und dem Application Gateway wird sodann etabliert und die beiden können miteinander kommunizieren. (3) Setzt nun der Client eine Anfrage um, wird diese durch den Proxy analysiert und protokolliert. Die zugelassene Anfrage wird an das eigentliche Zielsystem weitergeschickt, zu dem das Application Gateway zuerst eine Verbindung aufgebaut hat. Dabei findet also eine Entkoppelung der jeweiligen Parteien statt.

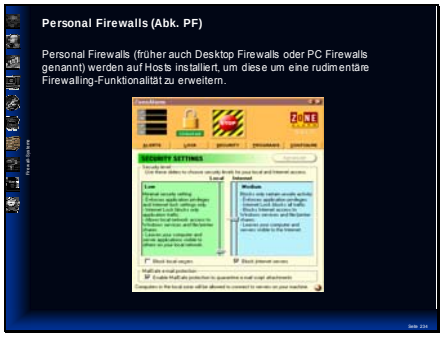
233



Application Gateways und ihre Proxies können sehr viel Macht über Netzwerkanwendungen ausüben. Durch das direkte Einsehen der Kommunikationen auf der Applikationsschicht lassen sich dediziertes Verhalten (z.B. einzelne Kommando-Folgen) unterbinden. Desweiteren erlauben Sie das Einbringen einer zusätzlichen Authentisierung. So wird in vielen Grossunternehmen vorgeschrieben, dass wer auf das World Wide Web (WWW) zugreifen möchte, sich zuerst mit Benutzername und Passwort ausweisen muss. Dadurch sollen Missbräuche (z.B. unerlaubtes Surfen oder Download illegaler Inhalte) verhindert werden.

Doch die Nachteile von Application Gateways gilt es nicht zu vergessen. Da eine Kommunikation mit spezifischen Proxies erforderlich ist, wird oftmals eine spezielle Konfiguration auf der Client-Seite vorausgesetzt. Die bedeutet ein Mehr an organisatorischem und technischem Aufwand. Nur wenige Dienste lassen sich dabei mit einem transparenten Proxy betreiben. Desweiteren versagen viele Application Gateways noch immer darin, eine wirklich umfassende Analyse der Kommunikationen zwischen den Netzwerkapplikationen durchzuführen. So werden oftmals nur rudimentäre Checks gemacht, so dass sich der Einsatz nicht gross von demjenigen eines simplen Paketfilters unterscheidet. Ein Application Gateway ist sehr komplex, da für einen jeden zu unterstützenden Dienst ein eigenen Proxy entwickelt werden muss. Diese Komplexität macht die Entwicklung und Nutzung von Application Gateways besonders Anfällig für Fehler.

234

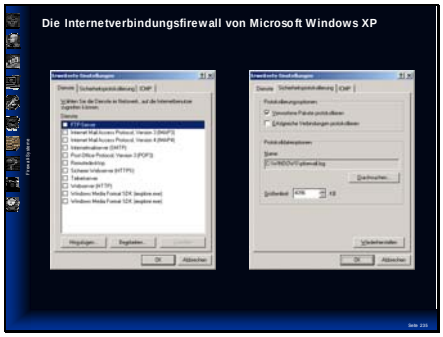


Durch sogenannte Personal Firewalls – diese wurden auch Desktop Firewalls und PC Firewalls genannt - lassen sich netzwerkfähige Systeme um rudimentäre Firewall-Funktionalitäten nachrüsten. Diese Technologie erfuhr besonders zwischen 1998 und 2001 einen grossen Boom. Die Entwickler solcher Lösungen versprachen damit, dass Hacker und andere Schädlinge vor unerwünschten Zugriffen abgehalten werden könnten.

Der Einsatz von Personal Firewalls ist unter Experten höchst umstritten. Einige von Ihnen behaupten, dass durch zusätzliche Software mangelnder Qualität neue Schwachstellen im System aufgetan werden könnten. Die Liste der Lücken populärer Personal Firewalls stützt diese These. Andere wiederum behaupten, dass die Hauptzielgruppe von Personal Firewalls – die Normalanwender – zu wenig technisches Verständnis für Firewalling aufbringen könnten, um diese Technologie sinnvoll einzusetzen. Frei nach der alten Firewall-Weisheit: Die Sicherheit eines Firewall-Schutzes ist von der Kompetenz des Administrators abhängig. Und in der Tat verstehen nur die wenigsten Endanwender, zu was für Konsequenzen das Zulassen von NetBIOS-Kommunikationen führt.

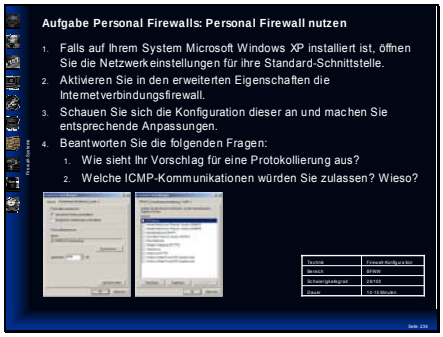
Trotzdem kann eine solide Personal Firewall durchaus ein Mehr an Schutz bedeuten. Bestes Beispiel war das Horror-Szenario um W32.Blaster.Worm, der eine schon über ein halbes Jahr bekannte Pufferüberlauf-Schwachstelle in der NetBIOS-Implementierung moderner Windows-Systeme ausnutzte. Durch den Einsatz einer restriktiv eingesetzten Personal Firewall konnte eine Infektion verhindert werden, da der Zugriff auf die entsprechenden NetBIOS-Ports geblockt war.

235



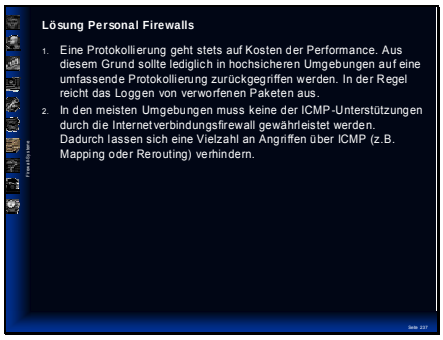
Microsoft Windows XP und Server 2003 bringen ihre eigenen Personal Firewalls mit (eigentlich unterstützte schon Microsoft WIndows NT 4.0 ganz rudimentäres Firewalling). Die Internetverbindungsfirewall erlaubt die Freigabe bestimmter Dienste. Werden diese auf dem lokalen System für jedermann angeboten, können Verbindungen zu ihnen erlaubt werden. Desweiteren wird eine Sicherheitsprotokollierung unterstützt, die die Aufzeichnung verworfener Pakete und erfolgreicher Verbindungen ermöglicht. Ebenfalls lassen sich dedizierte Einstellungen für die Unterstützung von ICMP vornehmen, so dass einige klassische Attacken über dieses Protokoll verhindert werden können (z.B. Ping-Mapping und Re-Routing).

236



Sollte auf Ihren System Microsoft Windows XP installiert sein, versuchen Sie sich an dieser Übung. Öffnen Sie die Einstellungen ihrer Netzwerkschnittstelle. Dies können Sie durch einen Klick auf den Start-Button, das Auswählen der Einstellungen und einen entsprechenden Klick auf die Netzwerkeinstellungen vornehmen. In den allgemeinen Einstellungen des neu geöffneten Fensters können Sie zum Reiter „Erweitert“ wechseln. Dort findet sich ein Button für das Öffnen der Einstellungen der Internetverbindungsfirewall des Betriebssystems. Schauen Sie sich dort ein bisschen um und führen Sie jene Anpassungen durch, die sie als sinnvoll erachten. In welcher Form haben Sie sich für eine Protokollierung entschieden? Und welche ICMP-Kommunikationen haben Sie in den Einstellungen zugelassen? Begründen Sie Ihre Antwort.

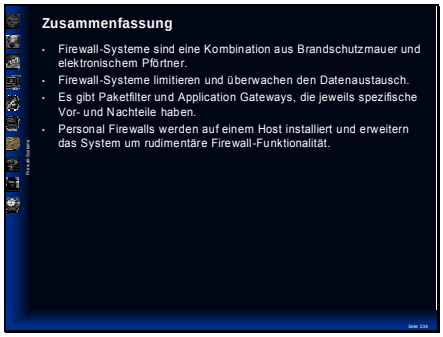
237



Eine Protokollierung geht stets auf Kosten der Performance. Aus diesem Grund sollte lediglich in hochsicheren Umgebungen auf eine umfassende Protokollierung zurückgegriffen werden. In der Regel reicht das Loggen von verworfenen Paketen aus.

In den meisten Umgebungen muss keine der ICMP-Unterstützungen durch die Internetverbindungsfirewall gewährleistet werden. Dadurch lassen sich eine Vielzahl an Angriffen über ICMP (z.B. Mapping oder Re-Routing) verhindern. Aus diesem Grund können Sie sämtliche ICMP-Kommunikationen deaktivieren. Sollten Probleme bei Netzwerkverbindungen auftreten, können Sie diese nach und nach wieder freischalten.

238

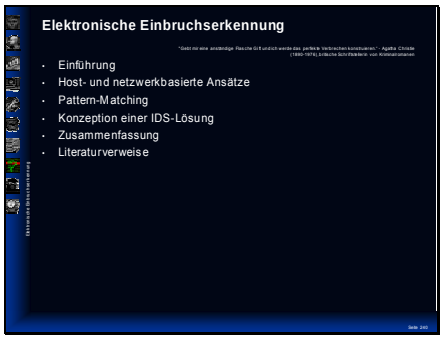


Wir haben in dieser Einführung gesehen, dass es sich bei Firewall-Systemen um eine Kombination aus einer Brandschutzmauer und elektronischem Pförtner handelt. Die Auswirkungen von Angriffen bzw. Einbrüchen werden limitiert (Brandschutzmauer), Kommunikationen überprüft und protokolliert (Pförtner). Dabei kommen zwei grundlegende Technologien zum Einsatz. Die einfachen Paketfilter überprüfen die Daten auf der Transportebene. Gilt es um die Analyse von Netzwerkanwendungen, kommen Application Gateways mit ihren dedizierten Proxies zum Einsatz. Personal Firewalls sind ein modernes Goodie, mit dem sich ein herkömmliches Betriebssystem um eine rudimentäre Firewall-Funktionalität erweitern lässt. In manchen Fällen lässt sich so die Netzwerksicherheit des Hosts erhöhen.

239

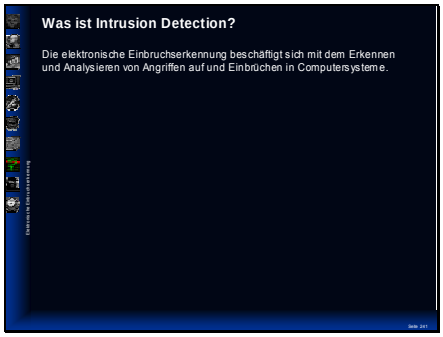


240



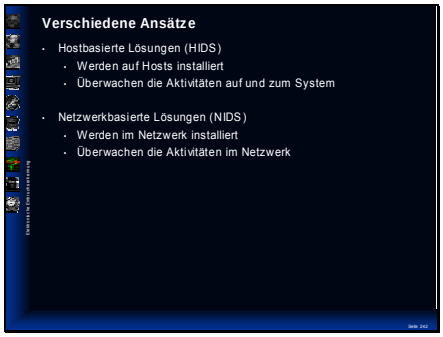
Die elektronische Einbruchserkennung versucht Attacken und Einbrüche zu erkennen, deren Hintergründe zu determinieren und damit adäquate Gegenmassnahmen anzustreben. Nach einer grundlegenden Einführung ins Thema wollen wir die host- und netzwerkbasierten Ansätze illustrieren. Dabei lernen wir ihre Vor- und Nachteile kennen. Danach besprechen wir die Technik des Pattern-Matchings bei der elektronischen Einbruchserkennung, um zum Schluss einige konzeptionelle Gedanken zur Umsetzung eines solchen Systems zu diskutieren.

241



Der englische Begriff „Intrusion Detection“ wird in der deutschen Literatur gerne als „elektronische Einbruchserkennung“ genutzt. Dabei geht es grundsätzlich um das Erkennen und Analysieren von Angriffen auf und Einbrüchen in Computersysteme. Mit der Hilfe spezieller Intrusion Detection-Systeme (IDS) und den Möglichkeiten des Protokollierens (z.B. Eventlog des Betriebssystems oder das Protokoll einer Firewall) können verdächtige Zugriffe inspiziert werden.

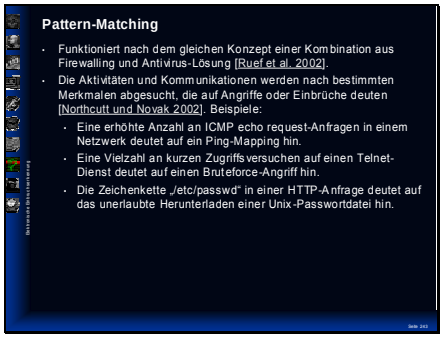
242



Intrusion Detection-Systeme (IDS) können dabei auf zwei verschiedenen Ebenen ansetzen. Da gibt es die hostbasierten Intrusion Detection-Systeme (HIDS), die auf einem System installiert werden. Durch verschiedene Techniken werden Netzwerkkommunikationen und das Verhalten auf dem Host selber überwacht. Bei verdächtigen oder unerwünschten Zugriffen wird Alarm geschlagen oder eine Gegenmassnahme eingeleitet (z.B. Benutzer aussperren).

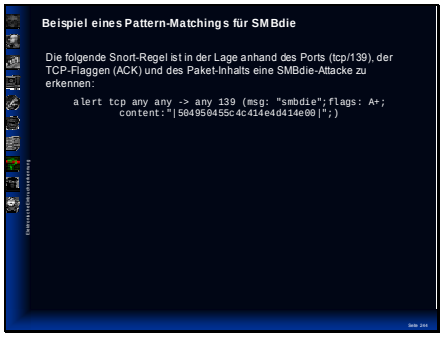
Bei hostbasierten Lösungen (NIDS) werden dedizierte Systeme in einem Netzwerk integriert. Diese überwachen möglichst unauffällig und passiv die Kommunikationen in diesem Netz. Verdächtige Zugriffe werden ebenfalls gemeldet oder gleich Gegenmassnahmen umgesetzt. Von den jeweiligen Herstellern wird gerne darauf verwiesen, dass sich um Falle eines Angriffs beispielsweise dynamisch die Regeln einer Perimeter-Firewall anpassen liessen.

243



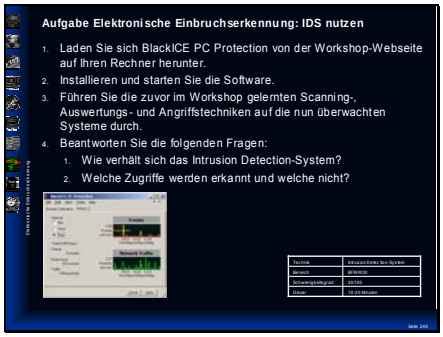
Viele Intrusion Detection-Systeme benutzen das aus dem Antiviren-Bereich bekannte Pattern-Matching, um Angriffe zu erkennen. Dabei werden die Kommunikationen nach bestimmten Merkmalen und Mustern untersucht, um etwaige Bestimmungen vornehmen zu können. So deutet beispielsweise eine erhöhte Anzahl an ICMP echo request-Anfragen in einem Netzwerk auf ein Ping-Mapping hin. Oder eine Vielzahl an Zugriffsversuchen auf einen Telnet-Dienst könnte das Resultat einer Bruteforce-Attacke auf deren Authentisierung sein. Ebenso könnte die Zeichenkette /etc/passwd in einer HTTP-Kommunikation darauf hindeuten, dass ein Angreifer durch irgendeine Web-Schwachstelle (z.B. Directory Traversal) die Passwortdatei von Unix herunterladen will.

244



Wir wollen das Pattern-Matching innerhalb der elektronischen Einbruchserkennung exemplarisch an einer Regel der populären Lösung Snort (http://www.snort.org/) illustrieren. Hierbei sehen wir, dass die Regel bei Zutreffen einen Alarm generiert (alert). Dabei wird nach einer TCP-Verbindung Ausschau gehalten, die auf den Port 139 abzielt. Weist ein solches Paket eine gesetzte ACK-Flagge sowie den Inhalt „504950455c4c414e4d414e00“ auf, muss es sich um einen Angriff mit SMBdie handeln.

245



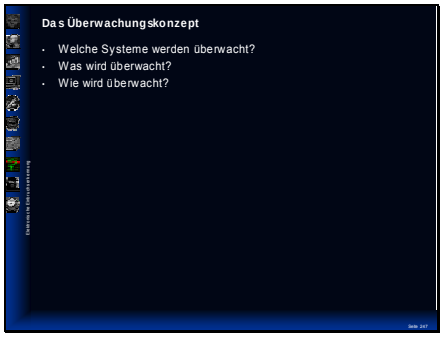
Gehen Sie nun auf die Workshop-Webseite und laden Sie sich die Software BlackICE PC Protection auf Ihren PC herunter. Dabei handelt es sich um die Trial-Version eines kommerziellen und hostbasierten Intrusion Detection-Systems. Installieren und starten Sie die Software. Führen Sie nun sämtliche im Rahmen des Workshops diskutierten Scanning-, Auswertung- und Angriffstechniken durch. Wie verhält sich nun das Intrusion Detection-System bei einem Angriff? Welche Zugriffe werden dabei erkannt und welche nicht? Können Sie weitere Anomalien feststellen?

246



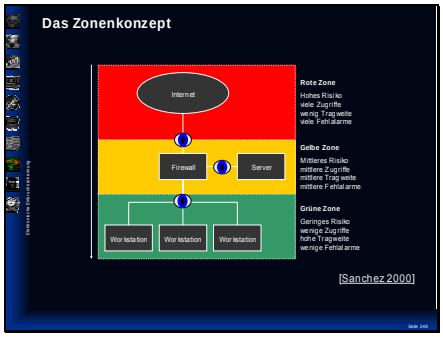
Das System verhält sich grundsätzlich ruhig, sofern keine Attacken umgesetzt werden. Wird ein Angriff erkannt, wird je nach Konfiguration eine Warnmeldung akustisch und visuell ausgegeben. Dabei werden eine Vielzahl der typischen Zugriffe eines Angreifers erkannt.

247



Wie bei jeder Lösung ist ein solides Konzept die Grundlage für den Erfolg dieser. Bei einer Überwachung mittels Intrusion Detection-Systemen sollte ein Assessment umgesetzt werden. In diesem wird festgehalten, welche Systeme und Daten überhaupt als besonders wertvoll und schützenswert klassifiziert werden können. Anhand dessen lässt sich definieren, welche Überwachungsmassnahmen überhaupt angemessen sind. So macht es nur wenig Sinn, dass man bei einem reinen Datenbankserver das IDS-System auf Angriffe per Email ansetzt. Dies wäre reine Ressourcen-Verschwendung.

248

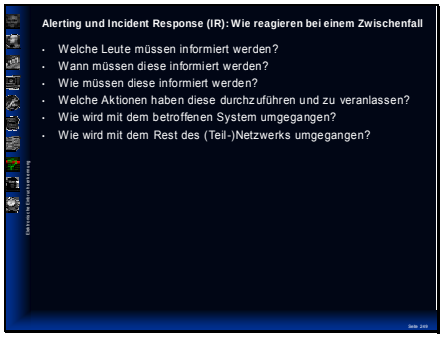


Die Definition des klassischen Zonenkonzepts von Intrusion Detection sieht insgesamt drei Zonen vor [Sanchez 2000]. In der roten Zone sind unsichere Systeme positioniert, zu denen keine oder nur eine geringe Vertrauensbeziehung herrscht. Dies ist in den meisten Fällen das Internet, das mit seiner Vielzahl an potentiellen Angreifern das grösste Risiko darstellt. Da durch viele „harmlosere“ Scan-Zugriffe ebenso viele Fehlalarme gegeben sein können, wird ein Intrusion Detection-System in einer solchen Zone oftmals nur als Angriffs-Erkennung eingesetzt. Dabei wird die statistische Auswertung herangezogen, um Trends bei Angriffen und das Interesse der Angreifer erkennen zu können.

In der gelben Zone finden sich Elemente, die einem mittleren Risiko ausgesetzt sind. Zum Beispiel Server-Systeme, die sich in einer DMZ befinden und durch nicht-vertrauenswürdige Benutzer bedient werden können. Die Überwachung sollte in diesem Fall schon umfassender Ausfallen, da eine direkte Interaktion mit potentiellen Angreifern immer ein gewisses Risiko in sich birgt.

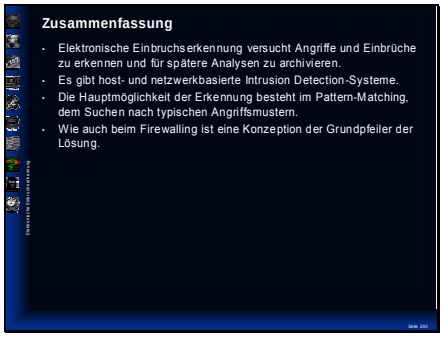
Die grüne Zone definiert das interne Netzwerk. Das Risiko in diesem ist im Gegensatz zum Internet gering. Es wird wenige Angriffe geben. Ist ein solcher jedoch erkannt, ist man mit einem grösseren Problem konfrontiert. Ein externer Angreifer aus der roten Zone könnte die Firewall umgangen haben oder ein interner Angreifer könnte eine kompromittierung des Netzwerks vorhaben. Entsprechend gilt es das Intrusion Detection-System sehr sensibel einzustellen und bei einem jeglichem Anzeichen eines Angriffs sofort Alarm zu schlagen.

249



Im Alerting und Incident Response (Abk. IR) wird das Verhalten bei einem Zwischenfall reagiert. Dies ist ein sehr wichtiger Prozess, ohne den die elektronische Einbruchserkennung nur wenig wert ist. So gilt es beispielsweise festzuhalten, welche Leute wann bei einem Zwischenfall informiert werden müssen. Ebenfalls der Weg der Informationsverteilung heisst es festzuhalten. Die Reaktionen bei einem Angriff oder Einbruch sind zu dokumentieren, um in der Hitze des Gefechts einen kühlen Kopf wahren zu können. Dabei ist es wichtig zu vermerken, wie mit den betroffenen Systemen umgegangen werden soll, ob und inwiefern eine forensische Analyse eingeleitet werden muss.

250

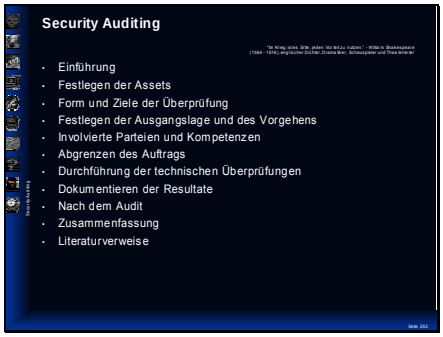


Wir haben gesehen, dass sich die elektronische Einbruchserkennung mit dem Entdecken und Analysieren von Angriffen und Einbrüchen beschäftigt. Dabei kommen host- und netzwerkbasierte Intrusion Detection-Systeme, aber auch die Protokoll-Mitschnitte anderer Lösungen (z.B. Firewalls), zum Einsatz. Die Hauptmöglichkeit der Erkennung besteht im Pattern-Matching, dem Suchen nach typischen Angriffsmustern. Dabei handelt es sich grundsätzlich um die gleiche Technologie, die auch bei Antiviren-Produkten zum Einsatz kommt. Zudem ist auch wie beim Firewalling eine Konzeption und saubere Umsetzung derer der wichtigste Grundpfeiler einer soliden Lösung.

251

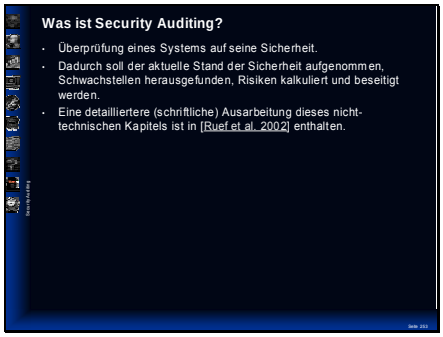


252



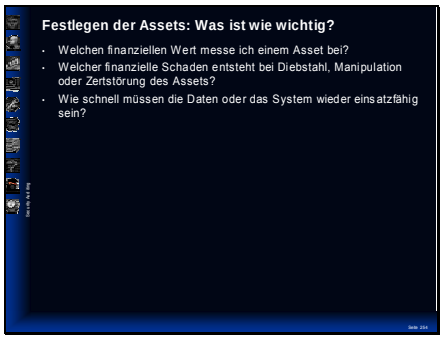
In diesem Kapitel wollen wir uns mit Security Auditing auseinandersetzen. Dabei wird diskutiert, wie eine technische oder konzeptionelle Überprüfung einer Computerumgebung vorgenommen werden kann. Der Ablauf des Kapitels ist dabei dem chronologischen Vorgehen eines Projekts sehr ähnlich. Als erstes werden die Assets, also die Ziele des Auftrags, definiert. Danach findet eine Definition der Form und Ziele des Audits statt. Daraus resultiert die Ausgangslage und das Vorgehen, das angestrebt werden will. Die involvierten Parteien und Kompetenzen gilt es abzustecken, um eine saubere Koordination gewährleisten zu können. Durch eine Abgrenzung innerhalb des Auftrags werden Missverständnisse verhindert. Sodann kann eine (technische) Überprüfung stattfinden. Daraus resultieren der Report, der die Schwachstellen sowie das Projekt ansich dokumentiert. Und nach einem jeden Audit gilt es das weitere Vorgehen zu definieren.

253



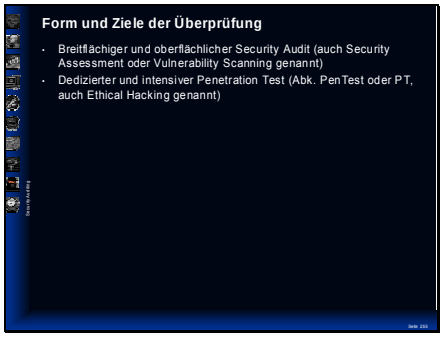
Bei einem Security Audit handelt es sich um die sicherheitsrelevante Überprüfung eines Systems. Dadurch soll der aktuelle Stand der Sicherheit aufgenommen, Schwachstellen herausgefunden, Risiken kalkuliert und beseitigt werden. Eine detailliertere (schriftliche) Ausarbeitung dieser nicht-technischen Betrachtungen ist im Buch „Hacking Intern“ ein ganzes Kapitel gewidmet.

254



In einer frühen Phase gilt es die Assets festzulegen. Unter Assets werden Objekte verstanden, die bei der sicherheitstechnischen Überprüfung eine Rolle spielen. Das können einzelne Systeme, ganze Netzwerke oder spezifische Informationen sein. Durch die Definition des Werts eines Assets lässt sich ableiten, wieviel Aufwand innerhalb des Testings eingebracht werden soll. Durch eine Risiko-Analyse, die beispielsweise den Diebstahl, die Manipulation oder Zerstörung des Objekts festhält, können entsprechende Ableitungen gemacht werden.

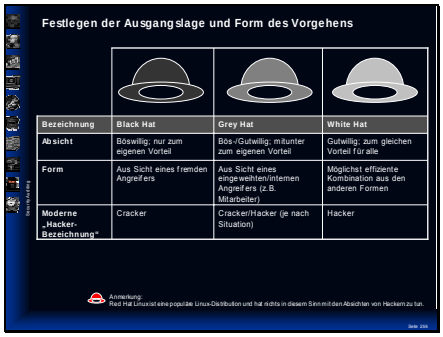
255



Die Terminologie bei Sicherheitsüberprüfungen ist nicht einheitlich gehalten. Wir wollen während dieser Vorlesung die Begriffe Security Audit, Security Assessment und Vulnerability Scanning synonym verwenden. Diese benutzen wir dann, wenn eine breitflächige Analyse der Sicherheit einer Umgebung umgesetzt werden soll. Anhand der Überprüfungen sollen potentielle Schwachstellen entdeckt und die gegenwärtige Sicherheit determiniert werden, so dass sich adäquate Gegenmassnahmen umsetzen lassen.

Dedizierter und zielgerichteter verhält sich ein Penetration Test, der gerne mit PenTest oder PT abgekürzt wird. Hierfür hat sich in den letzten Jahren ebenfalls der Begriff Ethical Hacking etabliert. Hierbei wird das möglichst realitätsnahe Vorgehen eines echten Angreifers nachgespielt, um Schwachstellen zu finden und ihr wahres Risiko zu erkennen. Sicherheitslücken werden dabei direkt ausgenutzt und damit die Echtheit der Vermutungen bestätigt.

256

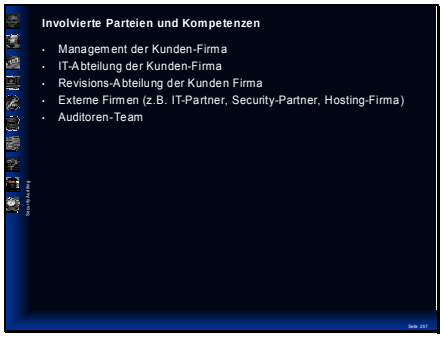


In der Hacker-Szene hat sich über die Jahre eine eigene Klassifizierung für die Vorgehensweise und Absichten eines Hackers entwickelt. So wird in erster Linie zwischen einem Black Hat und einem White Hat unterschieden. Ersterer sucht und missbraucht Schwachstellen in erster Linie zu seinem eigenen Vorteil. Diesen will er so lange wie möglich sein Eigen nennen und hält etwaiges Wissen längstmöglich geheim. Gutartige Hacker bezeichnen solche Personen oftmals abschätzig als Cracker.

Mit reiner Weste agieren White Hat Hacker. Diese arbeiten gutwillig und versuchen zum Vorteil für jedermann offenzulegen. Das Informieren eines Hersteller oder Benutzers über den Sachverhalt ist ihnen mindestens so wichtig wie die Bekanntmachung an der breiten Öffentlichkeit. Nur so kann gewährleistet werden, dass Schwachstellen schnell gefunden und behoben werden, damit bösartige Cracker (Black Hat) keinen Vorteil erlangen können.

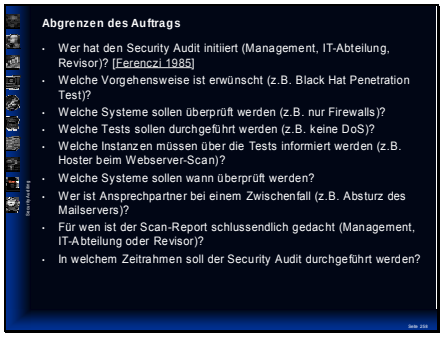
Da die Abgrenzung zwischen Black und White Hat oftmals schwierig ausfällt und nicht immer jeder seiner Linie treu bleibt, gibt es ebenfalls sogenannte Grey Hats. Diese arbeiten manchmal gut-, manchmal böswillig. So kann es sein, dass er eine Schwachstelle findet und zu seinen Gunsten ausnutzt, sofern der Schaden nicht willkürlich und übertrieben ausfällt. Das Bekanntmachen des Problems wird kurze Zeit verzögert, um mit den neuen Möglichkeiten wenigstens ein bisschen „Spass" zu haben. Im Übrigen ist Red Hat Linux (http://www.redhat.com/) eine populäre Linux-Distribution, die nichts in diesem Sinn mit den Absichten von Hackern zu tun hat.

257



Bei einem technischen Auditing sind oftmals verschiedene Parteien involviert. Diese gilt es zu identifizieren, ihre Position und Kompetenzen innerhalb des Projekts festzulegen. So können Partner frühzeitig über Scan-Zugriffe informiert und ein versehentliches Auslösen einer Incident Response verhindert werden.

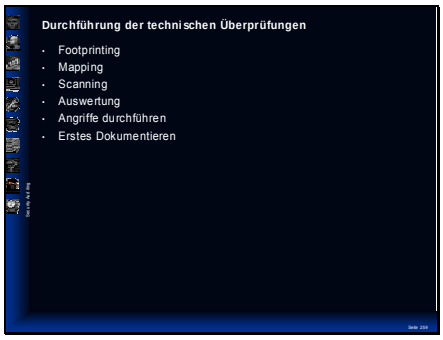
258



Durch verschiedene Fragen, die meistens schon während eines ersten Kickoff-Meetings gestellt werden, kann der Auftrag klar definiert und abgegrenzt werden. So ist es beispielsweise für das Reporting oftmals wichtig zu wissen, wer den Auftrag initiiert hat. Jenachdem ob dies ein Entscheid des oberen Managements oder der IT-Abteilung war, werden andere Anforderungen an Umfang, Detailtiefe und Ausrichtung gegeben sein.

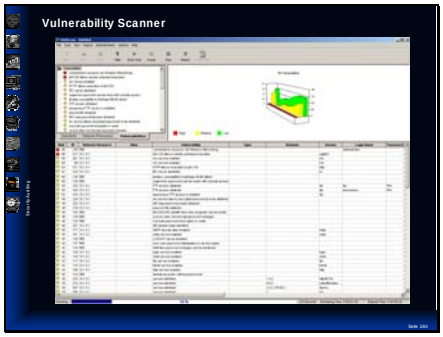
Von grösster Wichtigkeit bei der technischen Analyse ist die klare Definition der Assets. Anhand von IP-Adressen oder Hostnamen sollten sich die Zielsysteme eindeutig identifizieren lassen, so dass die Ressourcen auch für die richtigen Objekte investiert werden. Es gibt nichts Schlimmeres weder am Schluss eines Projekts zu merken, dass das falsche System untersucht hat.

259



Die technische Umsetzung der Überprüfungen wurde schon weitestgehend in den ersten Teilen dieser Vorlesung skizziert. Dabei wird grundsätzlich ähnlich wie ein richtiger Angreifer vorgegangen. Dieser wird sich als erstes mittels Footprinting über die Zielumgebung informieren, um danach mittels Mapping die Erreichbarkeit potentieller Ziele zu bestimmen. Sodann findet ein Scannen und Auswerten statt, durch das weitere Informationen zum Ziel zusammengetragen werden können. Erst dann finden die eigentlichen Angriffe, die das Ausnutzen von Schwachstellen zum Ziel haben, statt. Danach findet ein erstes Dokumentieren statt, mit dem der Grundbaustein für den finalen Report gelegt wird.

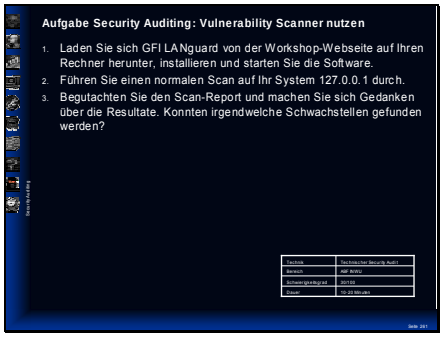
260



Durch sogenannte Vulnerability Scanner ist ein Auditor in der Lage, sehr einfach und unkompliziert ein technisches Vulnerability Assessment durchzuführen. Die Software trägt dabei über das Netzwerk Informationen zu den Zielsystemen zusammen. Dabei werden viele der Techniken, die wir in diesem Workshop kennengelernt haben, genutzt: Mapping, Portscanning, Auswertung und das Ausführen von Angriffen. Zum Schluss wird in der Regel eine Übersicht der vermuteten Schwachstellen sowie die Möglichkeit der Generierung eines Reports gegeben.

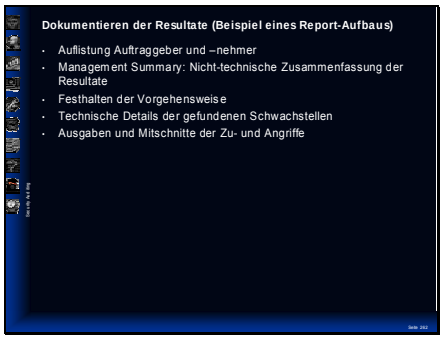
Die ursprünglich als open-source herausgegebene Software Nessus (http://www.nessus.org/) ist eine der bevorzugten Lösungen für derlei Analysen. Neben diesem Produkt werden unter Microsoft Windows vor allem kommerzielle Lösungen wie ISS Internet Scanner, Symantec NetRecon und GFI LANguard eingesetzt.

261



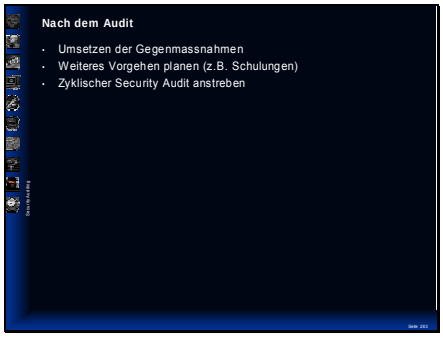
Benutzen Sie nun selber in unserem Test-Netzwerk einen Vulnerability Scanner. Gehen Sie dazu auf die Workshop-Webseite und laden Sie das Produkt GFI LANguard auf Ihren Rechner herunter. Installieren und starten Sie den Scanner. Führen Sie danach einen Scan auf ihren eigenen Rechner über die Loopback-Adresse 127.0.0.1 durch. Nach wenigen Minuten sollte die Analyse durchlaufen sein. Generieren Sie sich nun am besten einen Report und schauen Sie sich die Resultate an. Konnten irgendwelche Schwachstellen gefunden werden?

262



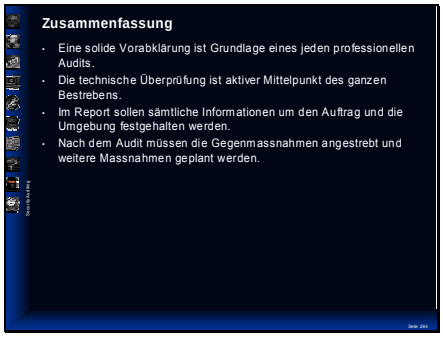
Obschon viele Scanning-Utilities die Generierung eines Reports ermöglichen, hat der Auditor die Resultate in ein einheitliches Format zu bringen. Das Dokumentieren eines Audits ist jenachdem sehr umfassend und kann einen Grossteil eines Projekts ausmachen. Der Umfang, die Detailtiefe und Struktur eines Reports richtet sich grundsätzlich nach den Anforderungen des Auftraggebers. Man kann jedoch sagen, dass in einem jeden Dokument ein Management Summary enthalten sein muss, dass auf ein oder zwei Seiten die Resultate zusammenfasst. In einem weiteren sollten sich eine detaillierte Auflistung der Schwachstellen sowie empfohlene Gegenmassnahmen finden. Falls möglich können die Scan-Mitschnitte und Original-Reports der jeweiligen Tools als Anhang mitgeliefert werden.

263



Mit der Durchführung eines Security Audits ist ein solcher noch lange nicht abgeschlossen. Es ist sehr wichtig, dass aus dem Report die empfohlenen Gegenmassnahmen ersichtlich sind. Diese müssen mit dem Kunden und etwaigen Partnerfirmen umgesetzt werden, um die Sicherheit der Umgebung noch zu erhöhen. Das weitere Vorgehen gilt es zu planen, wobei Awareness-Schulungen oder Hacker-Trainings der Administratoren ein guter Schritt sein können, um das Verständnis für die Problematik zu verbessern. Desweiteren sollten Security Audits zyklisch durchgeführt werden, um die Umsetzung der Massnahmen zu verifizieren und Trends identifizieren zu können.

264



Mit einem Security Audit kann die Sicherheit einer Umgebung bestimmt, auf Schwachstellen hingewiesen und diese ausgemerzt werden. Eine solide Vorabklärung ist dabei Grundlage eines jeden professionellen Audits. Nur so können Irrtümer und hektische Situationen während der eigentlichen Durchführung vermieden werden. Die technische Überprüfung ist dabei aktiver Mittelpunkt des ganzen Bestrebens. Im finalen Report sollen sämtliche Informationen um den Auftrag und die Umgebung festgehalten werden, so dass das Projekt nachvollzogen und weitere Schritte geplant werden können.

265



266



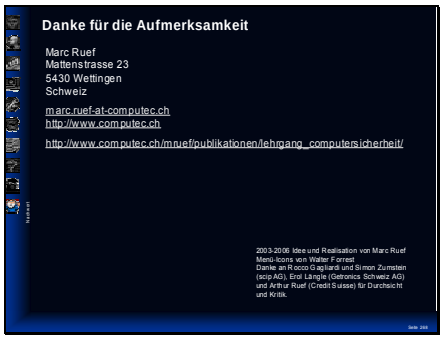
Sollten Sie Fragen zur Vorlesung, ihrem Inhalt, den Aufgaben oder Lösungen haben, zögern Sie nicht mich zu kontaktieren.

267



Ich möchte mich für die Aufmerksamkeit der Zuhörer und Leser bedanken. Ich hoffe, dass ich die Philosophie meines Genres und die Grundlagen dessen unterhaltsam und in nützlicher Weise vortragen konnte. Wir leben in einer technokratischen Gesellschaft, in der technische Hilfsmittel nicht mehr wegzudenken sind. Durch das Verständnis der Funktionsweise dieser können wir mithelfen, einen unkomplizierten Umgang zu pflegen. Lieber die Technik beherrschen, weder von ihr beherrscht zu werden.

268



Sie erreichen mich über meine Postadresse oder per Email auf marc.ruef-at-computec.ch. Aufgrund einer Vielzahl an Sendungen kann es sein, dass ich mehrere Monate brauche, um angemessen zu reagieren. Dies sei mir bitte verziehen. Auch weiterhin finden Sie überarbeitete Auflagen dieser Präsentation, Übungsaufgaben sowie ihre Lösungen, Software und Links auf der offiziellen Vorlesungs-Webseite unter http://www.computec.ch/mruef/publikationen/lehrgang_computersicherheit/

Danke an die vielen Lektoren und Studenten, die mir bei der Erarbeitung dieser Vorlesungsreihe geholfen haben. Im besonderen möchte ich mich bei Walter Forrest für die schönen Icons bedanken. Rocco Gagliardi und Simon Zumstein (scip AG), Erol Längle (Getronics Schweiz AG) sowie Arthur Ruef (Credit Suisse) gebührt mein Dank für ihre Durchsicht des ersten Manuskripts sowie die vielen Anregungen und Kritiken. Ohne Sie wäre diese Arbeit in der gegenwärtigen Form nicht möglich gewesen.