Fortsetzung von Seite 13

tels eines Passwortcrackers oder durch Abhören des Netzwerkverkehrs (Sniffing) an das Passwort eines gültigen Accounts und kann sich auf dem entsprechenden System einloggen.

In der Folge kann er mittels der kopierten digitalen Identität des rechtmässigen und ahnungslosen Benutzeraccount-Besitzers quasi in dessen Namen agieren um beispielsweise via diverse Brückenköpfe Scheinangriffe auszuführen. In der Praxis werden oft ganze Ketten von Brückenköpfen quer über alle möglichen Länder und Kontinente eingesetzt, damit das so genannte Tracing des echten Ursprungs der Hackerattacke erschwert wird und der Hacker besser getarnt ist. Scheinangriffe sind vom Opfer von echten Angriffen nicht zu unterscheiden.

Spuren verwischen

Nachdem alle benötigten Vorarbeiten vom Hacker erledigt wurden, kann die eigentliche Attacke beginnen. Als erstes wird versucht, das Anfallen und die Aufzeichnung jeglicher echter Spuren zu verhindern. Dies geschieht einerseits mittels des Einsatzes von Brückenköpfen und andererseits durch systematisches Umleiten oder Deaktivieren der Logging-Funktion der Zielsysteme. Anschliessend kann der Hacker seinen eigentlichen Auftrag erledigen und beispielsweise Daten und Programme manipulieren. Nach getaner Arbeit installieren Hacker oft noch Hintertürchen wie beispielsweise Trojaner (siehe auch nachfolgende Artikel) auf den kompromittierten Systemen, die es dem Hacker in Zukunft vereinfachen, erneut Zugriff auf das System zu bekommen. Sollte es dem Hacker nicht gelingen, die Kontrolle über das Zielsystem zu erlangen, führt er oftmals als Frustreaktion eine Denial-of-Service-Attacke aus, welche bei Erfolg die Verfügbarkeit des angegriffenen Systems negativ beeinträchtigt. Nachdem der Angriff abgeschlossen ist, werden möglichst alle Spuren verwischt und die Logging-Funktion des Zielsystems wieder hergestellt. Allfällig eingesetzte Brückenköpfe werden ebenfalls von Spuren gesäubert.

Gegenmassnahmen

Obwohl während einer relativ langen Zeitspanne Informationen über das Zielobjekt gesammelt werden, findet der eigentliche Angriff innerhalb eines eng bemessenen Zeitfensters statt (siehe Grafik). Es ist also von entscheidender Bedeutung, einen geplanten Hackerangriff möglichst früh zu erkennen und abzuwehren. Die wohl wirkungsvollste Massnahme ist die Steigerung der Security Awareness der Mitarbeiter. Denn wer sich bewusst ist, dass sämtliche Informationen einen Wert haben, welche im Web, im Gespräch oder auf dem Schreibtisch liegend aktiv oder passiv an andere weitergegeben werden, der überlegt sich, ob, wem und vor allem was er an andere kommuniziert. Dieses gesteigerte Sicherheitsbewusstsein der Mitarbeiter erschwert Unberechtigten die Informationsgewinnung massgeblich und vereitelt manche geplante Hackerattacke bereits in einer frühen Phase.

Weitere präventive Massnahmen sind regelmässige Sicherheitsüberprüfungen und Vulnerability Management-Systeme. Falls der Hackerangriff dennoch in die heisse Phase der laufenden Attacke geht, so soll die Attacke raschestmöglich erkannt und der Hacker in die Irre geleitet werden, um wertvolle Zeit für Gegenmassnahmen zu gewinnen. Um Attacken zu erkennen, haben sich in der Praxis Intrusion-Detection und Prevention-Systeme bewährt, welche Alarm schlagen und allenfalls selbständig Gegenmassnahmen wie das Kappen einer bestimmten Verbindung einleiten können.

Sogenannte Honeypots sind echt aussehende, aber mit falschen Daten gefütterte Systeme, welche dem Hacker ein interessantes System vortäuschen, in dem er sich dann bewegt und damit schliesslich Zeit vergeudet. Es gibt also durchaus Mittel, Hackerangriffe mittels Prävention zu verhindern oder zumindest deren Erfolg zu vereiteln. Dank richtigen Aktionen des vermeintlichen Opfers resigniert am Schluss nur einer – der Hacker. ■

Workshop – Hack yourself

Ethical Hacking Gewiefte Hacker platzieren Trojaner, um Computersysteme über das Internet fernzusteuern. Diese Systeme dienen meist als so genannter «Brückenkopf» für weitere Angriffe. Lesen Sie, wie Hacker dabei vorgehen und testen Sie mit einem Trojaner, ob Ihr Netzwerk vor derartigen Angriffen gefeit ist.

Simon Wepfer*

Sicherheitskonzepte, die sich auf eine harte Schale verlassen, dabei allerdings die Sicherheit der inneren Systeme vernachlässigen, werden im Fachjargon mit dem Begriff «Candy-Sicherheit» umschrieben. Mit den Süssigkeiten sind konkret die M&M's Bonbons gemeint, deren weicher Kern sich dann offenbart, sobald die Glasur mit einem kräftigen Biss oder geduldigem Lutschen durchdrungen ist. Tatsächlich ist einem Hacker die Firewall an sich egal. Verschiedene Dienste wie Mail-, DNS- oder Webserver müssen vom Internet her erreichbar sein. Ein Hacker wird denn auch versuchen, den Hebel eher dort anzusetzen, als sich an einer Firewall die Finger zu verbrennen.

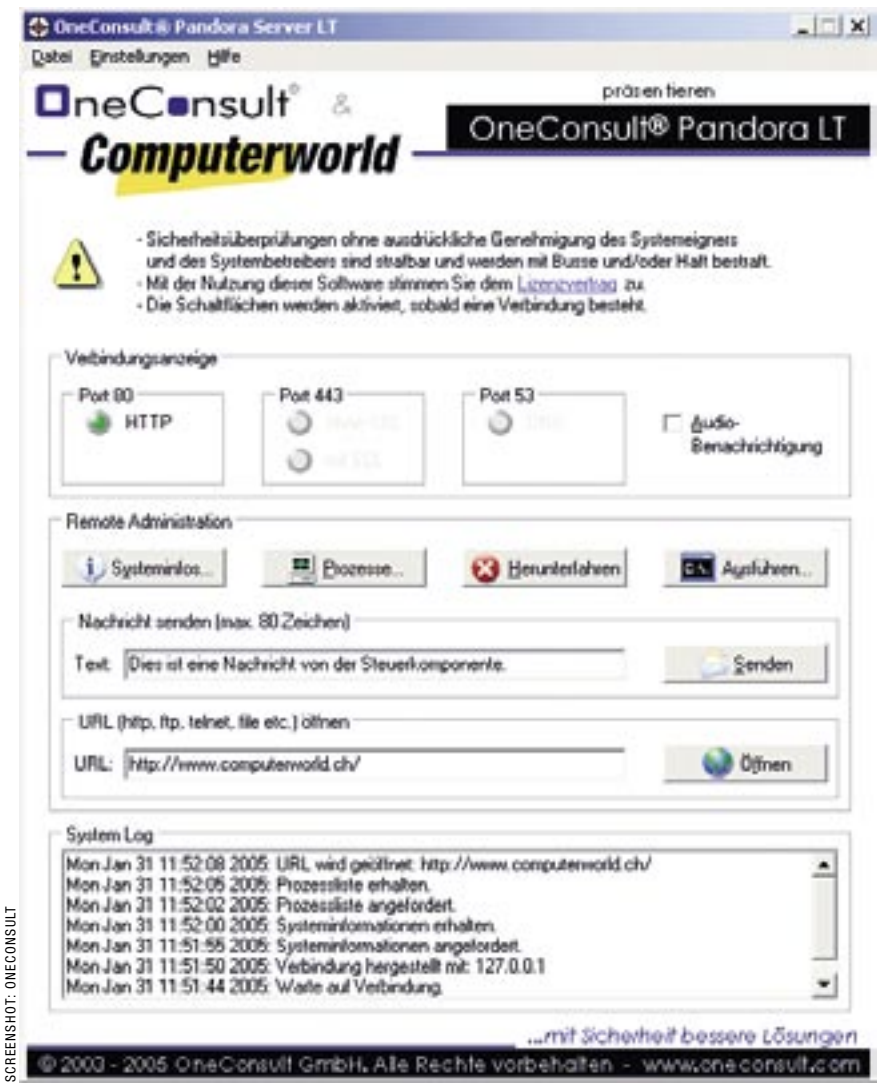
Die zur Verfügung stehenden Dienste nutzen auch Trojaner aus: Die Programme verbinden sich durch die Firewall hindurch mit einer Steuerkomponente oder loggen sich auf einem IRC-Kanal (Internet Relay Chat) ein, um von dort Steuerbefehle zu erhalten. Auf diese Weise lässt sich ein Rechner in einem geschützten Netzwerk fernsteuern – trotz Firewall. Der Datentransfer sieht dann etwa wie eine herkömmliche Verb indung mit einem Webserver aus, doch statt Webseiten werden Steuerbefehle, Finanzdaten oder Passwörter übertragen.

Ein Rootkit ist eine Weiterentwicklung der Trojaner: Es versteckt sich und seine Aktivitäten durch Modifikationen am Betriebssystem. Besonders perfid gehen dabei die so genannten «Kernel Rootkits» vor. Sie werden beispielsweise in Form eines Gerätetreibers geladen und nisten sich tief im Betriebssystem ein. Das Kernel Rootkit setzt Filterfunktionen (Dateien/Verzeichnisse, Prozessl iste, Netzwerkverbindungen) direkt bei den entsprechenden Systemfunktionen ein, um sich zu verbergen. So kann auch eine Desktop-Firewall nicht erkennen, dass soeben eine vom Anwender unerwünschte Netzwerkverbindung hergestellt worden ist.

Kombinierte Sicherheits-Systeme auf Sicherheitslücken zu überprüfen gehört ebenfalls zu den Aufgaben eines ethischen Hackers. Beim Ethical Hacking wird mit der Erlaubnis des Systemeigners versucht, in ein Computersystem einzudringen. Der Hacker belegt die erfolgreiche Penetration, indem er zum Beispiel eine Datei auf dem Zielsystem platziert. Dabei können zwei verschiedene Ansätze verfolgt werden: Beim direkten Ansatz wird nach ausnutzbaren Sicherheitslücken gesucht, um das Ziel zu erreichen (siehe Praxisbericht).

Beim indirekten Ansatz übernimmt hingegen ein Mitarbeiter bewusst die Rolle des Opfers, indem er beispielsweise einen E-Mail-Anhang doppelklickt oder sich über eine speziell für diesen Test bereit gestellte Internetseite infiziert. Dieser Ansatz bringt den Vorteil mit sich, dass mit weniger Aufwand mehrere sicherheitsrelevante Komponenten wie etwa Antiviren-Schutz, E-Mail-Filter, Proxy-Server und Firewalls in Kombination getestet werden können.

*Simon Wepfer ist Consultant bei der auf Informationssicherheit (IT Security) und strategische Beratung spezialisierten OneConsult GmbH.



SCREENSHOT: ONECONSULT

Mit der von Oneconsult entwickelten Client-/Server-Anwendung Pandora LT lässt sich überprüfen, ob das eigene Netzwerk anfällig auf Hackerattacken ist. .

Hack yourself

Wir möchten Sie einladen, Ihre eigene Netzwerkinfrastruktur mittels indirektem Ansatz zu überprüfen. Es handelt sich hierbei um einen von vielen Sicherheitstests, die bei einer technischen Sicherheitsüberprüfung vorgenommen werden: Es wird versucht, einen PC im LAN (Local Area Network) durch die Firewall hindurch remote zu administrieren. Hierfür stellen wir unter http://www.oneconsult.com/downloads/downloads.html die Software «OneConsult Pandora LT» zur Verfügung. Pandora ist eine Client-/Server-Anwendung und besteht aus dem Trojaner (Clientkomponente) und der Steuerkomponente.

Falls keine entsprechenden Schutzmechanismen installiert wurden, sollte es möglich sein, das mit der Clientkomponente «infizierte» System über die Serverkomponente remote zu steuern. Dies funktioniert oft auch durch eine Hardware-Firewall hindurch. Das Tunneling findet bei Pandora LT über das http-Protokoll statt. Schlägt eine direkte Verbindung fehl, versucht der Trojaner diese über einen Proxy Server aufzubauen.

Pandora wird voraussichtlich von Ihrem Anti-Virenprogramm nicht erkannt. Dies bedeutet aber nicht, dass Ihr Anti-Virenprogramm versagt hat. Anti-Virenprogramme erkennen bekannte Viren an Hand von Signaturen (Bit-Mustern). Da es sich bei Pandora LT nicht um ein schon länger im Umlauf befindliches, potenziell gefährliches Tool handelt, wird dessen Bit-Muster (noch) nicht erkannt.

1. Notieren Sie sich die Firewall-Konfiguration auf den Systemen, auf welchen Sie OneConsult® Pandora LT verwenden möchten.
2. Stellen Sie sicher, dass die auf dem zu steuernden System installierte Software-Firewall ausgehende Verbindungen auf TCP Port 80 (http) zulässt.
3. Stellen Sie sicher, dass auf dem System, auf dem die Steuerkomponente gestartet werden soll, eingehende und ausgehende Verbindungen auf TCP Port 80 (http) erlaubt sind.
4. Starten Sie das Programm OneConsult-Pandora-Server.exe. Die Steuerkomponente ist nun bereit und wartet auf eine Verbindung.
5. Starten Sie auf dem zu steuernden System das Programm OneConsult-Pandora-Client.exe: Es öffnet sich ein DOS-Fenster, in welchem Sie den Systemnamen oder die IP-Adresse der Steuerkomponente eingeben müssen.
6. Sobald die Verbindung mit der Steuerkomponente aufgebaut wurde, können Sie auf der Steuerkomponente die vom Frontend unterstützten Befehle ausführen.
7. Sie können die Programme der Client- und Serverkomponente jederzeit durch das Schliessen der zugehörigen Fenster beenden.

Eine ausführlichere Bedienungsanleitung wird mit der Software mitgeliefert. Falls die Desktop-Firewall auf dem zu steuernden Rechner den Verbindungsaufbau nicht gestattet, ist der Rechner vor herkömmlichen Trojanern (ohne Rootkit-Funktionalitäten) ge-schützt. In diesem Fall sollten Sie den Zugriff trotzdem gewähren, um zu testen, ob weitere Komponenten im Netzwerk die Verbindung verhindern können.

Fazit

Sicherheitsrichtlinien und Mitarbeiter mit gesteigerter Security-Awareness in Kombination mit einem mehrschichtigen, technischen Schutzkonzept (Zwiebelschalen-Modell) bieten einen guten Schutz vor derartigen Angriffen. So wird aus einem knackigen M&M eine harte Zwiebel, wo keiner zweimal hineinbeissen möchte. ■

Info/http://www.oneconsult.com

Praxisbericht: Ethical Hacking

Hacking Der direkte Ansatz im Ethical Hacking verfolgt das Ziel, ein System ohne aktive Mithilfe des Besitzers zu manipulieren. Im Gegensatz zum indirekten Ansatz ist der Aufwand schwerer abzuschätzen. Dieser Bericht zeigt aus der Angreifer-Perspe k-tive den praktischen Ablauf eines ethischen Hackings.

Simon Wepfer

Ich schreibe meinem Freund J. eine E-Mail und frage ihn, ob er sich für einen Hackversuch an seinem Heimnetz begeistern könne. Eine halbe Stunde später trifft seine Erlaubnis ein. Genau genommen hat der Angriff bereits mit meiner Anfrage begonnen: Ich schaue mir die Header-Informationen der E-Mail an und erfahre so die IP-Adresse des Zielsystems.

Um warm zu werden beginne ich mit einem Traceroute und einigen DNS- und Whois-Abfragen. Dann starte ich einen Portscan auf die TCP Ports 1-80. Hierfür verwende ich das Open-Source-Tool nmap. Der Syn-Scan (-sS) sendet Kommunikationsanfragen an Zielports, ohne eine Protokoll-konforme Verbindung herzustellen:

- nmap -sS -O -T Polite -P0 -vvv -p 1-80 ziel-ip

Die Option -O versucht das Betriebssystem am Verhalten zu erkennen (OS Fingerprinting). Der Scan selbst benötigt einige Minuten. An Hand des Outputs ist erkennbar, dass es sich vermutlich um ein Zyxel Produkt handelt und der FTP- und Telnet-Dienst aktiv sind. Nebenbei betrachte ich natürlich ständig den Netzwerkverkehr mit ethereal oder tcpdump.

Standard-Passworte

Ich versuche zunächst mit dem Standard-Passwort der Zyxel-Produkte die Herrschaft über den Router zu erlangen. Ich rufe eine Telnet-Session auf und gebe das Passwort «1234» ein. Leider schlägt der Versuch fehl. Ich versuche das Passwort noch mit einigen Schüssen ins Blaue zu erraten – ohne Erfolg. Scheint doch nicht ganz so einfach zu sein.

Verwundbarkeiten

Nachdem die aktiven Dienste bekannt sind, starte ich den Security-Scanner «Nessus», um das Zielsystem nach Sicherheitslücken zu untersuchen.

- nessus-update-plugins
- nessusd -D
- nessus

Zuerst aktualisiere ich die Test-Plugins. Anschliessend starte ich den Nessus Daemon. Dabei handelt es sich um den Dienst, welcher die Tests ausführt. Mit dem dritten Befehl starte ich schliesslich das GUI. Ich wähle sämtliche passenden Plugins aus (ausser den DoS-Tests) und definiere die bekannten Zielports sowie die Ziel-Adresse. Nur wenige Minuten später ist der Test bereits beendet, der Report zeigt jedoch leider keine ausnutzbaren Verwundbarkeiten.

Dictionary Attacke

Ich entscheide mich, eine so genannte Dictionary Attacke auf den FTP-Dienst zu starten. FTP eignet sich für solche Fälle besonders gut. Hat das Opfer ein simples Passwort gewählt, verspricht dieser Angriffstyp nämlich hohe Erfolgschancen. Hierfür wird ein Tool benötigt, das selbständig Benutzernamen- und Passwort-Kombinationen ausprobieren kann. Gängige Tools sind beispielsweise Hydra, TeeNet oder Brutus.

Die zahlreichen Passwortlisten sind im Internet schnell gefunden. Nach lediglich 330 Versuchen ist das Passwort geknackt: homer. Darauf hätte ich

Weitere Links:

Nmap Portscanner: **http://www.insecure.org/**
Nessus Vulnerabiliy Scanner: **http://www.nessus.org/**
OneConsult Pandora LT: **http://www.oneconsult.com/downloads/downloads.html**

auch kommen sollen, schliesslich ist das Opfer ein treuer Simpsons-Fan.

Besuch von aussen

Der Router ist erobert. Ich könnte ein Remote Sniffing einrichten, so dass der gesamte Internetverkehr über meinen Rechner läuft. Mit dieser Technik lassen sich Passworte und E-Mail-Verkehr mitlesen. Ich aktiviere via Telnet das Webinterface auf der WAN-Seite und sehe mir die Tabelle mit den vergebenen Adressen an: Dabei erfahre ich Name und IP-Adressen von zwei PCs und zwei weitere Adressen.

Ich beschliesse, einen dieser Hosts genauer unter die Lupe zu nehmen. Damit dieser vom Internet her erreichbar ist, konfiguriere ich den Router entsprechend. Einen Portscan später stelle ich fest, dass es sich beim internen Ziel um einen Multifunktionsdrucker handelt. Drucker werden oft als sicherheitsrelevante Komponente ignoriert. Ich konsultiere eine entsprechende Default-Passwortliste und versuche, mit «access» Telnet-Zugang zu erlangen: Mit Erfolg. Solche Drucker lassen sich auch dazu nutzen, um Dateien zu verstecken oder Portscans zu fahren. Zum Spass printe ich eine Testseite aus – dabei frage ich mich, ob mein Drucker auch schon scheinbar grundlos Seiten ausgespuckt hat.

Mittels nmap und der Option -b starte ich einen FTP bounce scan, indem ich das Multifunktionsgerät als Brückenkopf nutze. Hierbei wird das PORT-Kommando des FTP-Protokolls missbraucht, um die Verbindung auf wählbare IP-Adressen und Ports umzuleiten. Der FTP-Server zeigt dem Benutzer unterschiedliche Meldungen, wenn der Zielport offen oder geschlossen ist.

Ich sehe mich nicht weiter um und lasse die beiden PCs und die Spielkonsole in Frieden. Ich konfiguriere die Firewall wieder so, dass sie sich nicht mehr remote administrieren lässt. Die Verbindung wird getrennt und ein erneuter Portscan bestätigt mir, dass keine Dienste mehr verfügbar sind.

Social Engineering

Der Versuch ist gelungen. Wie würde ich aber vorgehen, wenn die Firewall korrekt konfiguriert wäre? Ich könnte mich am E-Mail- oder DNS-Server des Providers zu schaffen machen. Auch Web mail-Dienste bieten interessante Ziele für SQL Injection Angriffe. Hier wird wie bei so vielen technischen Angriffen eine Kreuzung zwischen Kontroll- und Datenströmen erzielt. So enthalten die Felder für Benutzernamen und Passwort plötzlich SQL-Befehle, welche die Authentifizierung umgehen. Da ich aber keine Erlaubnis des Providers habe, lasse ich das bleiben. Statt dessen beschliesse ich, J. ganz einfach einen Trojaner unterzujubeln. Sobald der Code ausgeführt wird, baut der Trojaner eine Verbindung zu meiner Steuerkomponente auf und wird mir die absolute Kontrolle über den Rechner verleihen. Die Weltherrschafft reisse ich dann vielleicht morgen an mich.

Es ist kein Kunststück, jemanden dazu zu bringen, ein bösartiges Programm auszuführen. Ein Social Engineer beeinflusst die Zielperson – meistens telefonisch – und erzeugt einen Bedarf. Kann er dann auch noch vortäuschen, dass die Software aus einer vertrauenswürdigen Quelle entstammt, ist der Trojaner schon so gut wie platziert. Wie bei herkömmlichen Authentifizierungsmechanismen (Benutzername und Passwort) genügen einem Social Engineer in den meisten Fällen lediglich zwei vertrauenswürdige Informationen, um Menschen erfolgreich zu manipulieren.

Ich denke kurz darüber nach, wie ich J. dazu bringen könnte, ein Programm auf seinem PC auszuführen. Dann packe ich sämtliche Logfiles der Penetration-Tests in ein ZIP-Archiv. Ich spekuliere auf die Bequemlichkeit des Menschen und packe zusätzlich den Trojaner mit dem vielversprechenden Namen «LogViewer.exe» ein. Mein Freund wird sich natürlich denken, dass er damit die hieroglyphischen Logdateien besser lesen kann – und das Programm starten. Im E-Mail-Text fasse ich mich kurz. Ich erzeuge nur ein wenig Druck, indem ich schreibe, dass ich die eine oder andere Lücke gefunden hätte. Alle weiteren Infos befänden sich im Dateianhang. Bevor ich das E-Mail absende, baue ich noch eine akustische Benachrichtigung in der Steuerkomponente ein, damit ich die nächsten Stunden nicht vor dem PC warten muss. Ich starte den Server und sende

Ethical Hacker erobern Computersysteme mit der Einwilligung des Eigners.

das E-Mail ab. Tatsächlich verwende ich für diesen Angriff genau drei Informationen: Zwei E-Mail-Adressen und die Kenntnis von der Sicherheitsüberprüfung. Ein Angreifer, der zum Beispiel die Mailbox von J. überwacht, hätte bereits durch das Abfangen einer einzigen E-Mail Kenntnis von diesen Informationen und könnte sie auf eine ähnliche Weise ausnutzen.

Am nächsten morgen klingelte mich nicht der Wecker, sondern die akustische Benachrichtigung der Steuerkomponente aus dem Bett. ■