Mittels Profiling Angreifern auf die Spur kommen

Marc Ruef, scip AG, maru-at-scip.ch

Die elektronische Einbruchserkennung ist für viele noch immer ein Mythos. Die Leute, die sich an diesen herangewagt haben, wissen die Möglichkeiten jedoch zu schätzen. Doch oft wird dabei lediglich der technische Aspekt der Lösung Beachtung geschenkt. Dass die soziologische Analyse ebenso zur Bekämpfung von Attacken und Einbrüchen beitragen kann, wird gerne übersehen. An dieser Stelle kommt jedoch das Profiling ins Spiel, bei dem ein Übergriff analysiert wird, um die Hintergründe dessen zu erfahren.

Sie sind Firewall-Administrator eines grösseren Unternehmens und finden sich aufgrund eines anstehenden Software-Updates in der unangenehmen Situation wieder, am Samstag Morgen die erforderlichen Wartungen vorzunehmen. Beim Routine-Check der Rechner stellen Sie fest, dass die Log-Datei Ihrer Security-Systeme mit Daten überfüllt sind. Zwar sind die Server Ihrer Organisation stark frequentiert, jedoch protokolliert die Firewall und das Intrusion Detection-System nur verdächtige oder unerlaubte Aktivitäten. Nach kurzer Einsicht der Protokoll-Informationen stellen Sie fest, dass eine Vielzahl an unerwünschten Zugriffsversuchen stattgefunden haben.

Die erste Analyse

Nach einer etwas genaueren Analyse können Sie eine erste Aussage darüber machen, dass es sich dabei in erster Linie um einen harmlosen Portscan gehandelt hat. Dieser wurde von einer einzigen IP-Adresse aus Deutschland ausgeführt. Es ist früher Samstag Morgen und die meisten Leute - vor allem wenn sie erwerbstätig sind - werden diese frühen Stunden ihres freien Tages im Bett verbringen. Handelt es sich beim Angreifer um einen Jugendlichen, der aus Langeweile oder Neugierde mal eben unsere Hosts überprüfen will?

Glücklicherweise werden sämtliche Kommunikationen mit den wichtigen Systemen im Netzwerk durch einen Protokoll-Analyzer aufgezeichnet. Durch das Einsehen der verdächtigen IP-Pakete ist ersichtlich, dass der Angriff von einem Unix-System - wahrscheinlich ein Linux-Rechner mit einem Kernel der 2.4-Reihe - umgesetzt wurde. Diese Eingränzung haben zum Beispiel die Verteilung der TCP-Sequenznummern und einige sporadisch genutzte IP-Optionen ermöglicht.

Obschon die Handhabung von Linux in den letzten Jahren stark vereinfacht wurde, gilt dieses Unix-Derivat noch immer als „freakiges“ System, von dem der Normalanwender lieber seine Finger lässt. Der Angreifer wird also ein Faible für Computer haben und sich selbst wohl kaum als herkömmlichen Endanwender sehen.

Von der Software zum Charakter

Weiterhin kann aus den Paketen des Portscan-Vorgangs eine ebenfalls besondere Charakteristik erkennt werden. Die Reihenfolge der überprüften Ports, die generierten Pakete sowie die Durchführung des Verbindungsabbaus sind typisch für das Auswertungs-Tool nmap. Nmap ist seit Jahren sehr beliebt bei Administratoren und Angreifern. Dies vor allem aufgrund dessen, da es sehr effizient und zuverlässig arbeitet.

„Exotische und optimierte Scan-Techniken deuten auf einen erfahrenen und zielstrebigen Angreifer hin.“

Der Portscan basiert auf der sogenannten half-open SYN-Methode. Im Unterschied zur klassischen full-connect TCP-Portscan Variante werden nicht alle Schritte des Drei-Wege-Handschlags von TCP beim Verbindungsaufbau durchlaufen. Dies schafft ein Mehr an Effizienz, da nur ein Bruchteil der für einen full-connect TCP-Portscan erforderlichen Pakete versandt werden. Die SYN-Methode muss explizit beim Aufrufen von nmap durch den Schalter –sS aktiviert werden. Der Angreifer ist also mit den Möglichkeiten von nmap und den Vorteilen exotischer Scan-Techniken vertraut. Es handelt sich also kaum um einen blutigen Anfänger.

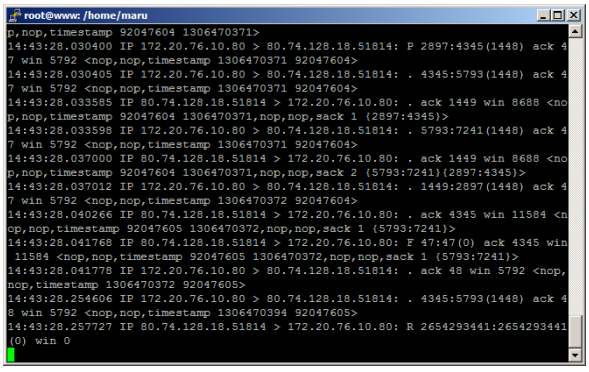


Abbildung 1: Mit Protokoll-Analyzern wie TCPdump (Screenshot) oder Ethereal lassen sich die Pakete eines Angriffs aufzeichnen und auswerten.

© scip AG

Interessant ist, dass als Quellport stets der TCP-Port 80 verwendet wird. Standardmässig nutzt nmap jedoch irgendeinen zufällig gewählten kurzlebigen Quell-Port für Scan-Zugriffe. Die Wahl des Ports 80 ist sinnvoll, weil darauf spekuliert wird, dass eine Fehlkonfiguration der Firewall Zugriffe mit diesem Port nicht protokolliert oder limitiert. Die explizite Wahl eines Quellports lässt vermuten, dass der Angreifer weiss, was und wie er es am besten tut. Ein unerfahrener Angreifer würde auf die Angabe eines ausserodentlichen Quellports verzichten, da ihm die Option nicht bekannt ist oder sie für ihn keinen Zweck erfüllt.

Ein plötzlicher Einbruch

Wir werden aus unseren Untersuchungen gerissen, als eines der Intrusion Detection-Systeme einen vermeintlichen Einbruch in einen unserer Webserver meldet. Sie lassen unverzüglich von ihrer Analyse ab und gehen der Sache auf den Grund.

Durch die Situation ein bisschen nervös loggen Sie sich auf dem Server-System - es handelt sich um ein OpenBSD - ein, um die Aktivitäten des Benutzers in Augenschein zu nehmen. Sie sind natürlich in erster Linie daran interessiert, wer der Angreifer ist. Aber ebenso wichtig erscheint es Ihnen zu wissen, was er vor hat. Durch einige speziell installierte Überwachungs-Tools sind Sie in der Lage jeden Schritt des Angreifers zu protokollieren, ohne dabei durch Ihre virtuelle Anwesenheit aufzufallen und ihn gar zu verschrecken.

Sie können sehen, dass der Benutzer eine Reihe der üblichen Unix-Kommandos eingibt, um sich auf dem Host umzusehen. Ihnen fällt dabei auf, dass der Eindringling dabei manchmal versehentlich die Kommandos anderer Systeme nutzt: Um den Inhalt eines Verzeichnisses anzuzeigen greift der Angreifer die ersten paar Mal fälschlicherweise auf das Windows-Kommando „dir“ anstatt auf die Unix-Form „ls“ zurück. Und die Netzwerk-Einstellungen überprüft er mittels dem unter Windows gebräuchlichen „ipconfig“ anstatt mit dem Unix-typischen „ifconfig“.

Sie vermuten also, dass der Angreifer mindestens ebenso auf Windows-Systemen zu Hause ist, da er in seiner Hektik versehentlich eben diese Kommandos heranzieht.

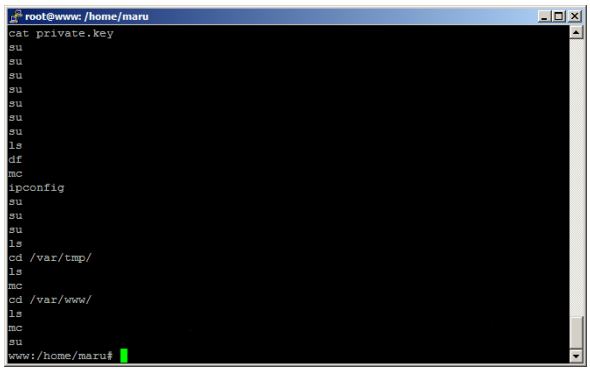


Abbildung 2: Die Shell-History auf einem Unix/Linux-System kann Aufschlüsse über das Verhalten, die Kenntnisse und Hintergründe eines Angreifers geben.

Die Motivation

Wir haben bisher eine Determinierung vornehmen können, aus welchem Umfeld der Angreifer stammt und welches technische Know-How er für sein Vorhaben mitbringt. Bisher ist es uns jedoch noch immer ein Rätsel, was das Motiv für seinen Angriff ist.

Während wir das Treiben des Eindringlings beobachten wird uns dies jedoch plötzlich klar. Er beginnt die Web-Dokumente auf dem Webserver zu löschen. Wir beobachten dieses Tun relativ gelassen, da wir wissen, dass wir natürlich ein Backup des Web-Auftritts zur Hand haben. Danach beginnt der Angreifer ein eigenes index.html zu erstellen. In diesem vermerkt er die Botschaft: „Dieser Rechner wurde von N30 gehackt!“ Danach loggt sich unser unfreiwilliger Gast aus. Und der Spuk kommt zu seinem Ende.

„Das Verständnis für die Motivation eines Angriffs lässt adäquate Gegenmassnahmen erarbeiten.“

Während Sie das Backup der Firmen-Webseite einspielen wird klar, was die Motivation für den Einbruch war: Der Angreifer wollte der Organisation eins auswischen und seine Überlegenheit demonstrieren. In der Aggressions-Psychologie spricht man dabei von einem „Erlangungs-Angriff mit narzisstischem Charakter“. Der Angreifer will seinen Erfolg mit anderen Teilen, um dadurch Anerkennung für sein Können zu erhalten.

Das Profil des Eindringlings

Der Zeitpunkt des Angriffs lässt vermuten, dass der Angreifer wohl kaum seinen Samstag morgen zur Erholung vorgesehen hat. Arbeitslosigkeit oder einen verschobenen Schlafrythmus können der Grund dafür sein.
Das vom Angreifer eingesetzte Betriebssystem,

© scip AG

wahrscheinlich Linux, gilt bei normalen Anwendern als „Spezialisten-System“. Dieser Hinweis auf einen spezialisierten Angreifer wird zudem durch die relativ effiziente Einsetzung des Portscanning-Tools nmap bekräftigt. Der Angreifer weiss also voraussichtlich, was er will und wie er es verhältnismässig optimal erreicht.

Nach erfolgreichem Einbruch auf dem Webserver deuten fehlerhafte Kommando-Eingaben durch den Eindringling darauf hin, dass er sich auch in der Windows-Welt zuhause fühlt. Vielleicht ist dies gar sein bevorzugtes Betriebssystem und Unix/Linux lediglich ein willkommenes Mittel für seine Angriffs-Zwecke.

Das Löschen des Webauftritts und das Einspielen einer eigenen Meldung mit dem Erfolg deuten auf einen Drang nach Anerkennung – der vorwiegend im jugendlichen Alter stark und in dieser Form ausgeprägt ist - hin.

Obschon der Angreifer durch das Verlangen der eigenen Bestätigung, durch die kindliche Neugierde getrieben und mit einem soliden Computerwissen bewaffnet eine ernstzunehmende Gefahr darstellt, ist die Motivation ansich eher harmlos. Der Angreifer lässt vom Objekt ab, sobald er sein Ziel erreicht hat.

Eine wirkliche Gefahr wäre bestehend, wenn der Angreifer in der vermeintlichen Heimlichkeit Hintertüren eingerichtet und sein destruktives Treiben sehr diszipliniert und erst zu einem späteren Zeitpunkt umgesetzt hätte.

Fazit

Wir haben gesehen, wie elektronische Einbruchserkennung in ihrer schönsten und aufregendsten Form stattfinden kann. Es geht dabei in erster Linie darum, Angriffe und Einbrüche zu erkennen.
Aber damit ist es noch nicht getan, denn mindestens so wichtig ist zu erfahren, wieso der Angriff erfolgreich ausfallen konnte, was der Angreifer vor hat und wer er überhaupt ist. Nur wenn wir diese Fragen klären können, können wir uns erfolgreich vor vergleichbaren und weiteren Übergriffen schützen.
Die in diesem Artikel vorgetragene Fallstudie ist nicht zwingend an Realtime-Betrachtungen gebunden. Ebenso können auch im Nachhinein entsprechend Analysen und Ableitungen durchgeführt werden. Wichtig dabei ist jedoch immer, dass die Protokolle der Anwendungen und Kommunikationen zur Einsicht zur Verfügung stehen. Eine gut eingerichtete Umgebung, die Möglichkeiten für die Auswertung der Protokolle gibt sowie ein Log-Management sind dazu unabdingbar.

Der Autor

Marc Ruef arbeitet als Security Consultant bei der schweizer Firma scip AG (http://www.scip.ch), welche sich auf Sicherheitsberatungen im Bankenumfeld spezialisiert hat. Er hat eine Vielzahl an Artikeln, Büchern und Übersetzungen im Bereich Computersicherheit publiziert, betreut einige namhafte internationale Projekte auf diesem Gebiet und unterrichtet an diversen Fachhochschulen sowie Universitäten.

Impressum

scip AG
Technoparkstrasse 1
CH-8005 Zürich
T +41 44 445 1818
mailto:info-at-scip.ch
http://www.scip.ch

scip AG ist eine unabhängige Aktiengesellschaft mit Sitz in Zürich. Seit der Gründung im September 2002 fokussiert sich die scip AG auf Dienstleistungen im Bereich IT-Security. Unsere Kernkompetenz liegt dabei in der Überprüfung der implementierten Sicherheitsmassnahmen mittels **Penetration Tests** und **Security Audits** und der Sicherstellung zur Nachvollziehbarkeit möglicher Eingriffsversuche und Attacken (**Log-Management** und **forensische Analysen**). Vor dem Zusammenschluss unseres spezialisierten Teams im Jahre 2002 waren die meisten Mitarbeiter mit der Implementierung von Sicherheitsinfrastrukturen beschäftigen. So verfügen wir über eine Reihe von Zertifizierungen (Solaris, Linux, Checkpoint, ISS, Okena, Finjan, TrendMicro, Symantec etc.), welche den Grundstein für unsere Projekte bilden. Den kleinsten Teil des Wissens über Penetration Test und Log-Management lernt man jedoch an Schulen – nur jahrelange Erfahrung kann ein lückenloses Aufdecken von Schwachstellen und die Nachvollziehbarkeit von Angriffsversuchen garantieren.