INFONEWS

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

www.goSecurity.ch
Mit Sicherheit an der richtigen Adresse.

Penetration Test

Die Angriffe gegen Unternehmen über das Internet haben massiv zugenommen. Der Penetration Test ist ein geeignetes Mittel, Schwachstellen frühzeitig zu erkennen und Massnahmen dagegen zu ergreifen.

Dieser INFONEWS geht auf folgende Themen ein:
- Wie ist ein typisches Vorgehen?
- Welche Hilfsmittel werden eingesetzt?
- Wie sehen mögliche Schwachstellen aus?

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1 Der Penetration Test

Praktisch jeden Tag werden neue Gefahren und Sicherheitslücken in Applikationen und Betriebssystemen entdeckt. Nur wenige Augenblicke später sind bereits Tools verfügbar, die diese Lücken ausnützen. Alle Lücken zu kennen und entsprechend zeitgerecht zu schliessen, ist bei den täglichen Arbeiten eines Administrators praktisch nicht mehr möglich. Zudem müssen viele Zugänge geöffnet sein, da ansonsten beispielsweise kein Zugriff auf die Webseite möglich ist oder die Emails nicht empfangen werden können. Der Penetration Test ist ein Mittel, um mögliche Fehler frühzeitig zu erkennen und damit die IT-Sicherheit zu erhöhen. Dieser Beitrag zeigt ein mögliches Vorgehen und erwähnt Mittel, die eingesetzt werden können, damit ein optimales Ergebnis erzielt werden kann. Dier INFONEWS kann aber nicht auf alle Möglichkeiten und Tools eingehen, sondern soll einen Überblick zum besseren Verständnis eines Penetration Tests geben.

2 Problemstellen

Der IT Alltag ist oft von Hektik und Stress begleitet. Sehr schnell kann es geschehen, meist unabsichtlich, dass eine Härtungsmassnahme nicht oder eine Testregel in der Firewall vergessen geht. Ebenfalls gehören ständige Änderungen und Erweiterungen am Netzwerk zum täglichen IT-Business. Sollte dann zusätzlich ein Mitarbeiter die Firma verlassen, geschieht die Übergabe aus unserer Erfahrung oft nicht optimal. Dass dabei die Dokumentation gerne vernachlässigt wird, zeigen diverse Studien. Nicht vergessen werden dürfen die regelmässigen Änderungen an Systemen und Software durch Patches und Updates. Aus diesen Gründen lautete bereits 1993 der Usenet-Ausspruch von Dan Farmer und Wietse Venema „Improving the Security of your Site by Breaking Into it“.

3 Informationen

Im Gegensatz zu IT-Revisionen gibt es zur Durchführung von Penetration Tests weder gesetzliche Vorgaben noch Richtlinien. Somit sind der Ablauf, die Methodik und die Art der Dokumentation offen. Seit einigen Jahren gibt es Versuche, diesen Missstand zu beheben.

3.1 OSSTMM

Zu den bekanntesten Verfahren gehört sicherlich das Open Source Security Testing Methodology Manual OSSTMM (http://www.osstmm.org). Das OSSTMM ist bezüglich technischen Security Audits kompatibel zu gängigen Standards und Weisungen wie ISO/IEC 27001/27002, IT Grundschutzkatalogen des BSI, SOX und Basel II / III. Auf Grund der Praxisorientierung und der

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Standardkonformität erfreut es sich international wachsender Beliebtheit.

3.2 BSI Leitfaden

Das BSI (Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.de) hat in Zusammenarbeit mit der BDO Visura und Ernst & Young einen Leitfaden zur Organisation und Durchführung von Penetration Tests mit dem Titel „Durchführungskonzept für Penetrationstests“ erstellt. Zusätzlich werden die rechtlichen Rahmenbedingungen dargestellt, die im Umfeld von Penetrationstests zu beachten sind. Die Studie stellt keine Anleitung zum "Hacken" von Netzen und Systemen dar, daher wurde bewusst auf detaillierte technische Anleitungen und Beschreibung von Werkzeugen, die in Penetrationstests verwendet werden, verzichtet. (Donwload unter https://www.bsi.bund.de/ContentBSI/Publikationen/Studien/pentest/index_htm.html)

3.3 Technical Guide to Information Security Testing

Vom US-amerikanischen National Institute of Standards and Technology (NIST) wurden die „Technical Guide to Information Security Testing“ erstellt und befindet sich seit November 2007 im Draft-Status (Download unter http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf).

3.4 OWASP

Das Open Web Application Security Project (OWASP) ist eine offene Community mit dem Ziel, Unternehmen und Organisationen zu unterstützen, sichere Anwendung zu entwickeln, zu kaufen und zu warten. Bei OWASP sind folgende Dienstleistungen frei zugänglich:

- Werkzeuge und Standards für Anwendungssicherheit
- Bücher über das Testen von Anwendungssicherheit,
- Entwicklung und Review von sicherem Quellcode
- Grundlegende Sicherheitsmassnahmen und –bibliotheken

Alle Werkzeuge, Dokumente und Foren sind für jeden, der an der Verbesserung von Anwendungssicherheit interessiert ist, frei zugänglich. OWASP sieht die Anwendungssi-

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

cherheit als eine Herausforderung für Menschen, Prozesse und Technologien. Die effektivsten Ansätze zur Verbesserung der Anwendungssicherheit müssen alle diese Bereiche berücksichtigen.

Die OWASP Foundation ist eine gemeinnützige Organisation, die den langfristigen Erfolg des Projekts sicherstellt. Fast jeder, der zu OWASP gehört, ist ehrenamtlich engagiert – einschliesslich OWASP Board, Global Committees, Chapter Leaders, Project Leaders und Project Members. Wir unterstützen innovative Sicherheitsforschung durch Zuschüsse und Infrastruktur.
Weitere Informationen sind unter http://www.owasp.org abrufbar. Unter anderem die OWASP Top 10! eine Liste der 10 kritischsten Sicherheitsrisiken für Webanwendungen.

3.5 Zertifizierungen

3.5.1 Ethical Hacker

Das Certified Ethical Hacker (CEH) Programm zertifiziert Personen in der spezifischen Netzwerk-Sicherheits-Disziplin des Ethical Hacking von einer herstellerneutralen Perspektive. Eine CEH-Zertifizierung bescheinigt Sicherheitsbeauftragten, Revisoren, Sicherheitsexperten, Website-Administratoren, und jedem, der mit der Integrität der Netzwerk-Infrastruktur betraut ist, tiefgehendes Wissen über die Anwendung und Umsetzung von IT-Sicherheit. Ein CEH ist ein erfahrener Profi, der es versteht, wie man die Schwächen und Angriffspunkte in Zielsystemen aufspürt und verwendet die gleichen Kenntnisse, Methoden und Instrumente wie böswillige Hacker.

Informationen zu den Ausbildungen sind unter http://www.eccouncil.org/ zu finden.

3.5.2 Offensive Security Certified Professional

Die Zertifizierung Offensive Security Certified Professional (OSCP) basiert auf dem Ethical Hacking. Entwickelt wurde diese von Offensive Security, die aus dem Trainingsprogramm für BackTrack entstanden ist. Um die Zertifizierung OSCP zu erhalten, muss in einer Laborumgebung eine existierende IT-Umgebung erfolgreich und dokumentiert gehackt werden. Dazu stehen dem Prüfling 24 Stunden zur Verfügung.

Weitere Informationen sind unter http://www.offensive-security.com/ abrufbar.

3.5.3 Weitere IT-Security Zertifizierungen

Es gibt zahlreiche weitere Zertifizierungen. Im Wikipedia sind viele davon aufgelistet:
http://de.wikipedia.org/wiki/Liste_der_IT-Zertifikate
(2. Abschnitt).

4 Schritte eines Penetration Tests

Der Ablauf eines Penetration Tests sieht in etwa wie folgt aus: Workshop – Testphase – Bericht – Präsentation.

In einem ersten Workshop werden die Ziele der Tests definiert. Hier muss auch klar die Motivation festgehalten werden, die ein potentieller Hacker aufwenden kann. Zudem wird festgehalten, wie weit die beauftragten „Hacker" gehen dürfen. Die Möglichkeiten eines gezielten Angriffs umfassen ein Blackbox-Hacking von Aussen, ein Hacking mit teilweisem oder komplettem Wissen über die

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

interne Infrastruktur (White- oder Grey-Hacking) und können durch netzwerkinterne Tests inkl. Social Engineering erweitert werden (Social Engineering: „Angriff" auf den Personen, z.B. Ausgabe als befugter Techniker oder externer Dienstleister mit dem Ziel in ein Gebäude einzudringen oder an Informationen zu gelangen). Wichtig hier sind die rechtlichen Spielregeln und die Vertraulichkeitsvereinbarung. Ebenfalls gilt es den richtigen Zeitpunkt zu definieren. Dabei wird auf die Umgebung des Kunden Rücksicht genommen, z.B. Tests zu Zeiten mit niedriger Last.

Blackbox: es stehen nur minimale Informationen über die Testumgebung zur Verfügung Whitebox: umfangreiche Informationen stehen zur Verfügung Graybox: es stehen die für die effiziente Durchführung notwendigen Informationen zur Verfügung.

Die Testphase wird anschliessend ausführlich beschrieben. Daher hier nur zwei Bemerkungen. Wichtig ist es, nie das Ziel der Tests aus den Augen zu verlieren. Schnell kann es in der Flut von Informationen geschehen, dass ein falscher Weg eingeschlagen wird. Im Gegensatz steht dazu, dass die Kreativität der Angriffe nicht ausser Acht gelassen werden darf. Ein stures Vorgehen nach Checklisten zeigt oft nicht das ganze Bild.

Der anschliessende Bericht zeigt das Vorgehen, die eingesetzten Tools sowie die Erkenntnisse aus den Ergebnissen. Sollten Schwachstellen ersichtlich sein, sind diese mit Massnahmen zu versehen und in einer Prioritätenliste festzuhalten. Soweit möglich sind Zusammenhänge aufzuzeigen und in einem gesamtheitlichen Bild darzustellen.

Die Präsentation ist analog aufgebaut. Da Penetration Tests oft auch von der Geschäftsleitung in Auftrag gegeben werden, sollte dies für die Präsentation beachtet und entsprechend umgesetzt werden. Es hilft nicht, Ergebnisse schön zu malen, sondern nüchtern und ohne Bewertung wiederzugeben. Es liegt im Ermessen und dem notwendigen Fingerspitzengefühl des Prüfers, mit dieser Situation umzugehen. Schlussendlich geht es immer darum, die Verbesserung der IT-Sicherheit voranzutreiben.

5 Vorgehen

5.1 Werkzeuge

An dieser Stelle ist es nicht möglich, auf alle zur Verfügung stehenden Werkzeuge einzugehen. Praktisch für jeden möglichen und unmöglichen Zweck steht ein Programm oder ein Tool bereit. Täglich stossen neue dazu. Bei der Beschreibung des Vorgehens wird jeweils auf ein Programm hingewiesen, viele davon stammen aus der Open Source Szene. An dieser Stelle nur ein Hinweis auf eine Tool Sammlung.

5.1.1 BackTrack

BackTrack ist ein auf Ubuntu GNU/Linux basierendes Betriebssystem mit dem Fokus auf Penetration Testing und Forensik. BackTrack bietet ein breites Spektrum an Tools, Port Scannern und Passwort Knack-Programmen. Es ist als Live CD oder Live USB verfügbar, kann aber auch auf eine Festplatte installiert werden. Unter anderem sind die folgenden Tools integriert:

- Metasploit (http://www.metasploit.com/)
- RFMON (Wireless Treiber) mit Aircrack-NG und Kismet

- Nmap
- Ophcrack
- Ettercap
- Wireshark
- BeEF (Browser Exploitation Framework)
- Hydra
- OWASP Security Framework
- und viele weitere

BackTrack ist in 12 Bereiche unterteilt:

- Information Gathering
- Vulnerability Assessment
- Exploitation Tools
- Privilege Escalation
- Maintaining Access
- Reverse Engineering
- RFID Tools
- Stress testing
- Forensics
- Reporting Tools
- Services
- Miscellaneous

Weitere Informationen und Download unter: http://www.backtrack-linux.org

5.2 Informationssuche

Der erste Schritt des Penetration Tests umfasst die Informationssuche. Welche Informationen sind im Internet verfügbar, sei dies auf der Homepage des Unternehmens oder via einer Suchmaschine wie zum Beispiel von Google oder Social Networking Plattformen. Auch Webseiten zur Stellensuche sind eine gute Quelle. Sucht die Firma zum Beispiel nach Oracle Spezialisten, wird vermutlich auch Oracle als Datenbanklösung eingesetzt. Das Internet vergisst dabei nichts. Wurde in einem Forum eine Frage platziert, kann diese auch nach Jahren noch abgerufen werden. Ebenfalls sind Namen von Personen, ev. sogar mit einer Emailadresse versehen, ideal für die weiteren Angriffe. Gute Hilfeleistung bietet hier http://www.yasni.ch, eine Personensuchmaschine.

Erste Informationen liefern auch WHOIS und DNS. Was sind für Angaben zu den IP-Adressen festgehalten? Verfügt das Unternehmen über weitere IP-Adressen? Welche Informationen stehen in den DNS-Einträgen? Kann gar ein kompletter Zonentransfer ausgeführt werden? Ist dies der Fall, sind auf einen Blick alle Anlaufstellen der Firma bekannt. Interessant sind sicherlich A Einträge zu Web- und Mailserver. Der MX Eintrag zeigt, welchen Weg die Emails ins Unternehmen nehmen. Ein SPF (Sender Policy Framework) zeigt zusätzlich, ob Mails via andere Wege ins Internet gelangen (zum Beispiel im Falle eines Backup-Mailservers). Ein Tool zur einfachen bilden die Funktionen WHOIS, Ping, Traceroute und DNS. Eine Onlinelösung ist hier http://www.dnsstuff.com.

5.3 Angriffsziel

Nachdem bereits viele Informationen zur Verfügung stehen, gilt es das Angriffsziel einzuschränken. Ein IP- und Portscan liefert die dazu notwendigen Informationen. Es soll geklärt werden, welche IP-Adressen auf Anfragen reagieren und welche offenen Ports im Internet ersichtlich sind. Daraus leiten sich die „interessanten" Ziele ab. In der Regel antworten die „Standardports" (d.h. Ports, die bekannt sind, oft unter 1024). Die Erfahrung zeigt, dass sich viele spannende Ports auch oberhalb der 50'000-Grenze befinden. Es lohnt sich, trotz grossem Zeitbedarf, alle 65'535 möglichen Ports durchzusehen. Gleichzeitig mit dem offenen Port sollte die Header-Information aus-

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

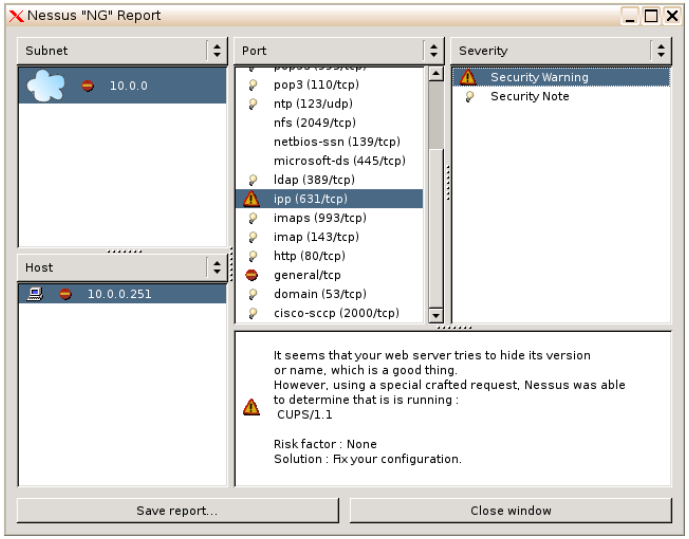
Telefon 052 320 91 20
Fax 052 320 91 21

gelesen werden. Viele Systeme sind sehr auskunftsfreudig und teilen mit, wer sie sind und vor allem in welcher Version sie vorliegen. Eine erneute Suche im Internet zeigt, ob sich das antwortende Programm auf dem aktuellsten Softwarestand befindet oder nicht. Falls nicht, sind vermutlich bereits Tools im Internet verfügbar, die gegen diese Schwachstelle eingesetzt werden können (so genannte Exploits). Zu den gängigsten Scan-Programmen gehört sicherlich NMap (http://www.nmap.org), welches auch unbemerkt IP- und Portscans durchführen kann. Ein Aufruf könnte zum Beispiel „nmap –sS –sV –O –p- <IP>“ lauten. Damit wird der Test im Stealth Scan Modus durchgeführt (d.h. der TCP Verbindungsaufbau wird nicht komplett durchgeführt und somit ev. auf der angegriffenen Seite auch nicht geloggt), mit –O wird zusätzlich versucht, das Betriebssystem herauszufinden. Der letzte Parameter sagt aus, dass alle 65'535 Ports durchgescannt werden.

```
Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp          Serv-U ftpd 4.0
25/tcp   open  smtp         IMail NT-ESMTP 7.15 2015-2
80/tcp   open  http         Microsoft IIS webserver 5.0
110/tcp  open  pop3         IMail pop3d 7.15 931-1
135/tcp  open  mstask       Microsoft mstask (task server - c:\winnt\system32\
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
5800/tcp open  vnc-http     Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows
```

5.4 Vulnerability Scanner

Als weitere Möglichkeit stehen Vulnerability Scanner auf der Liste. Diese eigenen sich aber nur dann, wenn ein mögliches Angriffsziel festgestellt wurde, da diese einen grossen „Lärm“ verursachen. Je nachdem ob alle Personen der zu untersuchenden Firma Bescheid wissen, können diese bereits zu einem frühen Zeitpunkt eingesetzt werden. Sie dienen dazu, nebst den bereits erwähnten Ports auch Informationen zum Betriebssystem, Banner (Antworten auf Anfragen), Kontrolle von bekannten Sicherheitslücken, Verbesserungsvorschlägen und automatisch generierten Berichten zu erstellen. Eines dieser Programme ist Nessus (oder als Alternative OpenVAS), welches im Client-/Server-Prinzip funktioniert. Dabei wird der Server auf einem Unix-System installiert. Der Client kann via SSL eine Verbindung darauf aufbauen und die entsprechenden Routinen starten. Mit zusätzlichen Plug-Ins lassen sich diverse Sicherheitslücken des Betriebssystems bzw. der Dienste, die auf dem zu scannenden Host laufen, finden. Wichtig: bei allen Programmen kann es zu Fehlalarmen kommen. Eine manuelle Nachkontrolle ist daher zwingend notwendig.



GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Sind nun mögliche Angriffspunkte erkannt worden, gilt es, diese genauer zu untersuchen.

Nachfolgend wollen wir dies für die beiden Betriebssysteme Windows und Unix etwas genauer beschreiben. Abgerundet wird unser „Angriffsversuch" auf Web-Applikationen.

6 Schwachstellen in Windowssystemen

Obwohl dem Betriebssystem von Microsoft oft schlechtes nachgesagt wird, kann es doch sehr sicher betrieben werden. Die Erfahrung zeigt, dass die meisten Schwachstellen durch installierte Dienste verursacht werden. Jeder Dienst, vor allem die nicht benötigten, erhöhen die Angriffsfläche eines Systems. Zudem gilt, dass das Patchen oft vernachlässigt und dadurch einem potentiellen Angreifer die Arbeit unnötig erleichtert wird. Wenn dann in einer Firewall zu viele Ports geöffnet sind, wird die Gefahr einer erfolgreichen Attacke erhöht.

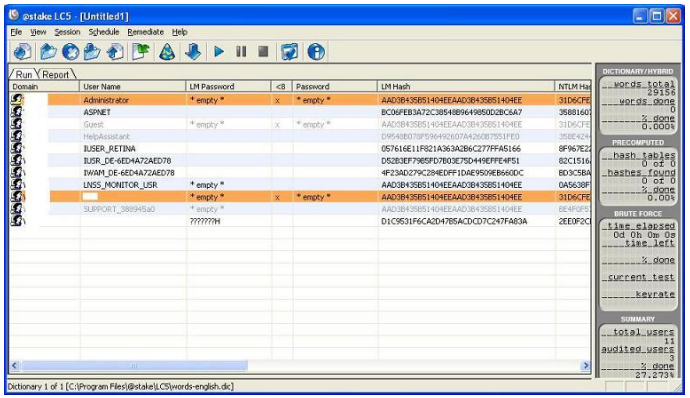
Wie bereits erwähnt, gibt der Portscan die ersten Informationen auf mögliche Schwachstellen bekannt. Sind typische Windows-Ports offen, wie Kerberos (88), RPC und Netbios (135-139), LDAP (389), SMB/CIFS (445), SQL Server (1433), AD Global Catalog (3268) und Terminal Services (3389) kann eine genauere Analyse weitere Informationen liefern. Hier lohnt sich der Einsatz eines umfassenden Scanners wie Nessus/OpenVAS oder der GFI Languard Network Security Scanner (http://www.gfisoftware.de/lannetscan). Sind Lücken in den eingesetzten Versionen bekannt, geben dies die Programme an. Nun muss nur noch im Internet das entsprechende Angriffstool gefunden werden. Google hilft hier sicherlich am schnellsten weiter, jedoch auch spezialisierte Seiten wie PacketStorm liefern oft ein passendes Programm.

Kann ein Zugriff auf die Anmeldeseite aufgebaut werden, sollten zuerst die möglichen Ziele identifiziert werden. In der Regel werden Accounts nach einer gewissen Anzahl Fehlversuchen gesperrt. Davon ausgenommen ist jedoch immer der Administrator. Der Administrator ist aber kein ideales Angriffsziel, da er (hoffentlich) gut überwacht wird. Ein Tool, das bei der Suche nach einem geeigneten Angriffsziel weiterhelfen kann, ist enum. Es nützt die Möglichkeit von Windows aus, sich mittels einer NULL Session auf einen Server zu verbinden. Damit ist es möglich, ohne Benutzernamen und Passwort einige Details abzufragen. Die Abfrage enum –P <IP> liefert als erstes die Passwortpolicy. Sind keine Einschränkungen vorhanden, d.h. kein Sperren bei einer gewissen Anzahl fehlerhaften Passworten, kann jeder beliebige Account verwendet werden. Mit enum –U <IP> werden die vorhandenen Benutzer-Accounts angezeigt. Mit –G werden auch die Gruppenzugehörigkeiten aufgeschlüsselt. Der Angriff er-

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

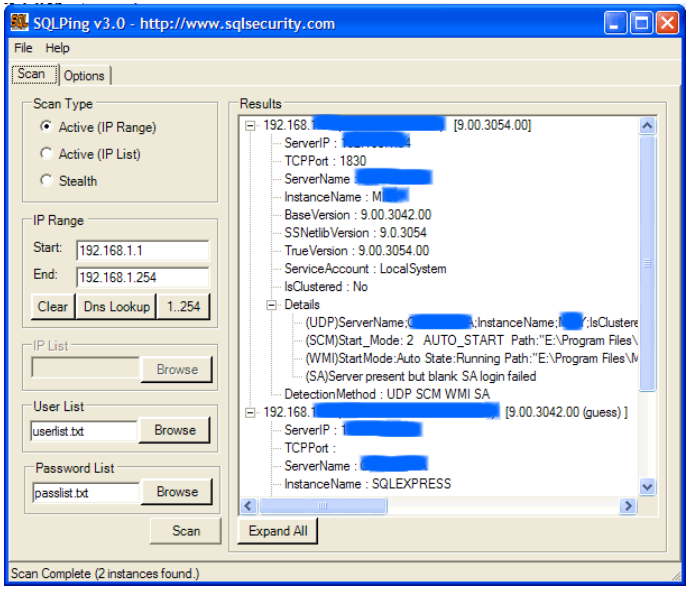
Telefon 052 320 91 20
Fax 052 320 91 21

folgt schlussendlich mit enum –D –u <Account> -f pwd.txt <IP>. pwd.txt enthält eine Liste von Passworten. Eine Brute-Force Attacke ist mit enum nicht möglich. Hier hilft aber das grafische Tool LC5 (L0phtCrack) weiter.



Immer wieder geschieht es, dass für die Serveradministration der Port 3389 (Terminal Services) auch durch die Firewall hindurch geöffnet wird. So kann der externe Support jederzeit auf den Server zugreifen. Dieses (grob-) fahrlässige Vorgehen öffnet einem Hacker einen optimalen Zugang zum System. Im Internet sind Tools verfügbar, die Brute Force Attacken auf diesen Port durchführen können. TSGrinder ist ein solches Tool, welches Terminal Server Verbindungen öffnet und ein Passwort nach dem anderen aus einer Textdatei an die Gegenseite schickt (http://www.hammerofgod.com/download.aspx). Die Empfehlung ist daher eindeutig: Terminal Services dürfen nur via VPN erreichbar sein.

Eine weitere „Sünde“ ist der direkte Zugriff auf den SQL Server. Sobald der Port 1433 offen ist, kann eine Attacke gefahren werden. Als ideal erweist sich das Tool SQLPing. Damit wird eine Brute-Force Attacke auf den Benutzer SA (System Administrator) ausgeführt (http://www.sqlsecurity.com/downloads).



7 Schwachstellen in Unixsystemen

Auch unter Unix sind Schwachstellen vorhanden. Typische Unix-Ports, die als Angriffsziel interessant sein können, sind: ssh (22), telnet (23) und finger (79).

Ist finger geöffnet, kann als erstes abgefragt werden, welche Benutzer gerade am System angemeldet sind: finger @<IP> liefert diese Antwort. Das Tool hydra kann an-

schliessend einen Angriff auf das Passwort starten. Dazu wird zum Beispiel eine Verbindung auf den Telnetserver gestartet: hydra –l <Benutzer> -P <Passwortliste> <IP> <Dienst>. Als Dienst können auch weitere eingesetzt werden.

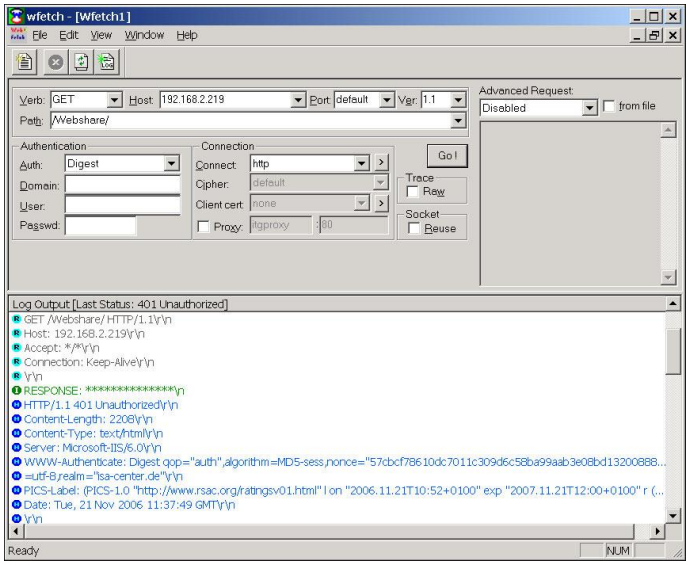
Sind Freigaben auf dieses System vorhanden, können diese mit showmount –e <IP> angezeigt werden. Ein „Anziehen" dieser Freigaben kann dann anschliessend mit mount geschehen.

RPC basierte Dienste sind ein beliebtes Angriffsziel. Daher liefert das Tool rpcinfo –p <IP> genauere Informationen. Alternativ kann dies auch mit nmap geschehen (nmap –sSRUV <IP>). Mit diesem Aufruf stehen alle notwendigen Informationen für einen weiteren Angriff zur Verfügung. Um welches System handelt es sich? Welche Applikationen sind installiert? Sind Schwachstellen dafür bekannt?

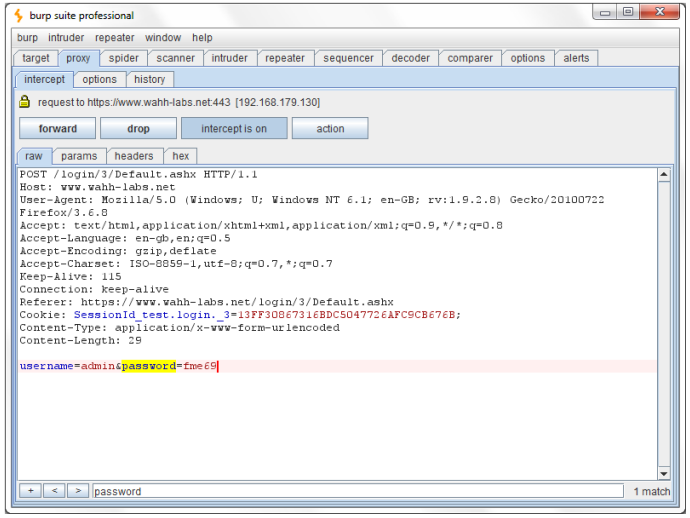
8 Schwachstellen in Web-Anwendungen

Die Betriebssysteme werden immer sicherer. Daher verlagern sich die Angriffe auf „leichtere" Ziele. Zu den beliebtesten gehören Web-Anwendungen. Immer mehr Applikationen bieten einen zusätzlichen Zugriff via HTTP (oder HTTPS). Aufgrund der Limitationen des zugrunde liegenden Protokolls ist es auch für erfahrende Programmierer nicht einfach, sichere Webanwendungen zu entwickeln.

Alle Daten werden als ASCII Text übermittelt (in beide Richtungen). Ein Abfangen und Senden ist daher nicht besonders schwer. Ein Tool, das dabei behilflich sein kann, ist WFetch. Damit lassen sich alle Parameter eines HTTP-Requests beeinflussen. Das Tool kann von der Microsoft Homepage heruntergeladen werden (http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=21625).



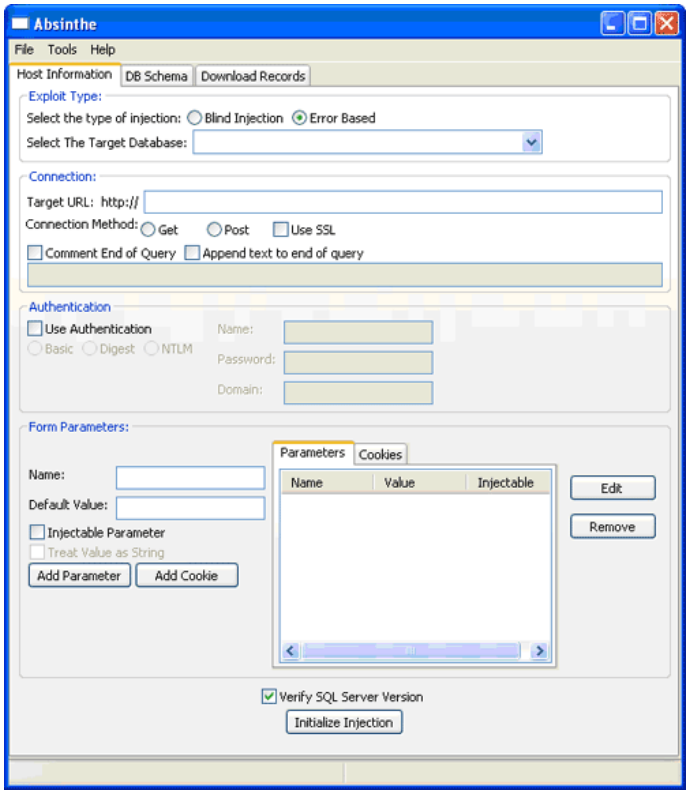
Damit eine Webseite und die übertragenen Daten einfach untersucht werden können, lohnt sich der Einsatz eines Proxys. Die BurpSuite ist ein sehr populärer Web-Proxy, der die Daten vor dem Versenden anzeigt und die Möglichkeit bietet, Modifikationen vorzunehmen (http://portswigger.net/burp/). Dies ist vor allem dann interessant, wenn in Formularen so genannte Hidden-Felder übertragen werden. Diese können so noch verändert werden, was oft die Möglichkeit bietet, auf fremde Daten zuzugreifen. Für schnelle Tests kann auch ein entsprechendes Plugin in Firefox verwendet werden.



Ein weiterer Angriffspunkt sind Formulare. Handelt es sich um Loginfelder, hilft das Tool Brutus weiter, welches Benutzernamen und Passwort an die Webseite schickt. Leider gibt es aber für Formular-basierte Authentifizierung kein Universal-Tool, da die Web-Entwicklersprachen oft leicht voneinander abweichen.

Trotz vielen Fachberichten und Warnungen gibt es immer noch Formularfelder, welche den eingegebenen Inhalt ungeprüft an Datenbanken weiterreichen. SQL Injection heisst das entsprechende Angriffsszenario, welches versucht, diese Anfragen zu manipulieren. Ein Aufruf mit ´or 1=1 -- liefert ein Ergebnis, das immer wahr ist. Wird dies direkt weitergereicht, können alle Antworten, unabhängig des Suchbegriffs, ausgelesen werden. Klappt dies, kommen weitere Abfragen zum Zug, mit dem Ziel, herauszufinden, welche SQL Server Version eingesetzt wird, welche Datenbanken existieren sowie wie die genauen Inhalte anzuzeigen. Dies erfolgt in der Regel mit dem Aufruf von union.

Ein Tool, das hier grafisch weiterhilft, ist Absinthe (http://www.0x90.org/releases/absinthe/).



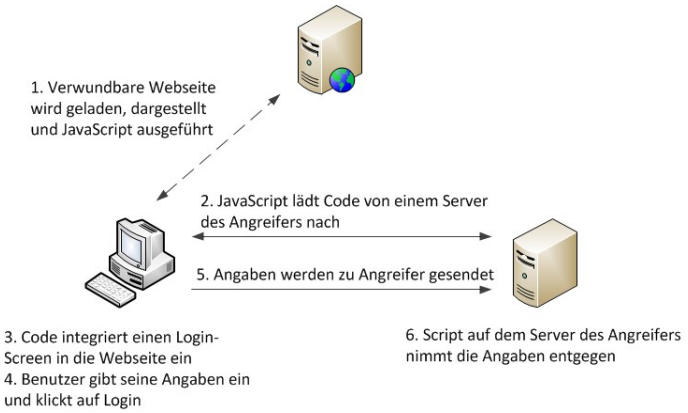
Eine weitere Gefahr ist Cross Site Scripting (XSS). Hier werden jedoch nicht Daten ausgelesen, sondern fremder Code in die echte Seite eingeschleust. Wiederum geschieht dies über schlecht ausgewertete Formularfelder. Ob die Seite dafür anfällig ist, lässt sich leicht mit

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

<script>Alert(´XSS Test´)</script> testen. Öffnet sich ein zusätzliches Fenster, ist die Seite anfällig auf Cross Site Scripting. Das gefährliche daran ist, dass sich ein Benutzer auf der richtigen Seite befindet, jedoch einen „falschen" Inhalt angezeigt bekommt. Werden so vertrauliche Informationen eingegeben, gelangen diese an den Angreifer und nicht an die Webseite.



9 Fazit

Diese Tests sind in der Regel nicht in einem Tag durchzuführen. Zu vielfältig sind die möglichen Angriffsflächen. Neben der Definition der eigenen Sicherheitsbedürfnissen gehört zu einem funktionierenden Sicherheits-Regelkreis das kritische Hinterfragen, ob die definierten Ziele mit den getroffenen Massnahmen erreicht wurden. Der Penetration Test liefert dabei eine unparteiische Drittmeinung. Das strukturiere Vorgehen hilft, mögliche Schwachstellen zu erkennen und geeignete Massnahmen zur Behebung zu treffen.

10 Quellen

Texte: Wikipedia, offizielle Homepages
Bilder: Offizielle Homepages, eigene Screenshots