Der Penetration Test

Der Penetration Test ist ein Mittel, um mögliche Fehler zu erkennen und damit die IT-Sicherheit zu erhöhen. Der richtige Partner und ein strukturiertes Vorgehen sind dabei sehr wichtig, um eine qualifizierte Aussage über den Stand der IT-Mittel zu erhalten und diese in Vergleich setzen zu können. Dieser Beitrag zeigt ein mögliches Vorgehen für ein optimales Ergebnis.

Inhaltsverzeichnis

1	**PROBLEMSTELLEN**	**2**
2	**STANDARDS**	**2**
3	**SCHRITTE EINES PENETRATION TESTS**	**3**
4	**WERKZEUGE**	**3**
5	**DER PENETRATION TEST**	**3**
5.1	Schwachstellen in Windowssystemen	6
5.2	Schwachstellen in Unixsystemen	8
5.3	Schwachstellen in Web-Anwendungen	9
6	**FAZIT**	**11**

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

GO OUT
IT-SECURITY HOSTING

1 Problemstellen

Der IT Alltag ist oft von Hektik und Stress begleitet. Sehr schnell kann es geschehen, meist unabsichtlich, dass eine Härtungsmassnahme oder eine Testregel in der Firewall vergessen geht. Ebenfalls gehören ständige Änderungen und Erweiterungen am Netzwerk zum täglichen Business. Sollte dann ein Mitarbeiter zusätzlich 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“.

2 Standards

Im Gegensatz zu IT-Revisionen gibt es im Bereich der 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.

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 Grundschutzhandbuch, SOX und Basel II. Aufgrund der Praxisorientierung und der Standardkonformität erfreut es sich international wachsender Beliebtheit.

Das BSI (Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.de) hat in Zusammenarbeit mit BDO 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.

Bundesamt für Sicherheit in der Informationstechnik

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. Vom EC-Council steht zudem die Möglichkeit zur Verfügung, sich als Ethical Hacker zertifizieren zu lassen.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

3 Schritte eines Penetration Tests

Der Ablauf eines Penetration Tests sieht in etwa immer gleich 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 interne Infrastruktur (White- oder Grey-Hacking) und können durch netzwerkinterne Tests inkl. Social Engineering erweitert werden. Wichtig hier sind die rechtlichen Spielregeln und die Vertraulichkeitsvereinbarung
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 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.

4 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 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 erwähnenswert sind sicherlich die sogenannten Exploit Frameworks. Sie beinhalten eine Sammlung von diversen Werkzeugen unter einer einheitlichen Oberfläche, meistens direkt bootbar von einer Standalone CD-ROM.

5 Der Penetration Test

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. Auch Seiten 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

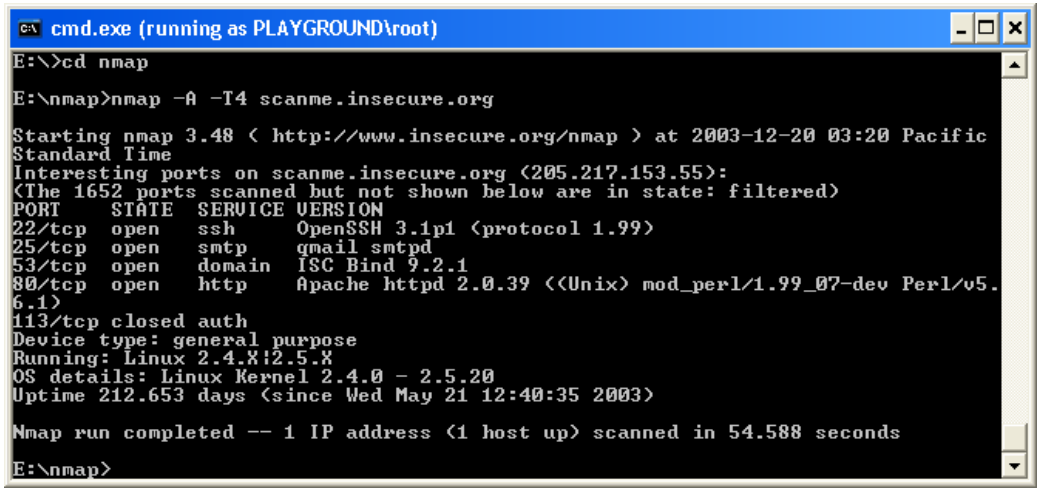
GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Jahren noch abgerufen werden. Ebenfalls sind Namen von Personen, ev. sogar mit einer Emailadresse versehen, ideal für die weiteren Angriffe.

Weitere Informationen liefern 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 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 Informationssuche bildet SamSpade, welches Funktionen zu WHOIS, Ping, Traceroute und DNS in einer grafischen Oberfläche bietet. Alles ist zwar auch von der Kommandozeile möglich, aber mit diesem Tool geht es doch etwas einfacher.

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 antworten 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 ausgelesen 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 (genannt 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 –O –p1-65535 <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



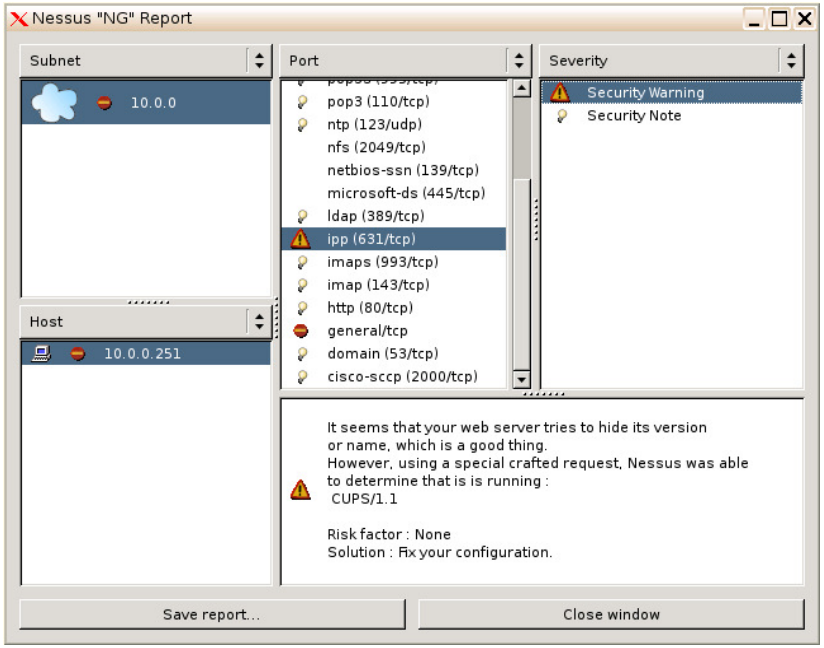
goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

letzte Parameter sagt aus, dass alle 65'535 Ports durchgescannt werden.

Als weitere Möglichkeit stehen Vulnerability Scanner auf der Liste. Diese verursachen jedoch einen grossen „Lärm". 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, 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 diesen 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.



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.

5.1 Schwachstellen in Windows-systemen

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 oder der GFI Languard Network Security Scanner. Sind Lücken in den eingesetzten Versionen bekannt, geben dies die beiden 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 erfolgt

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

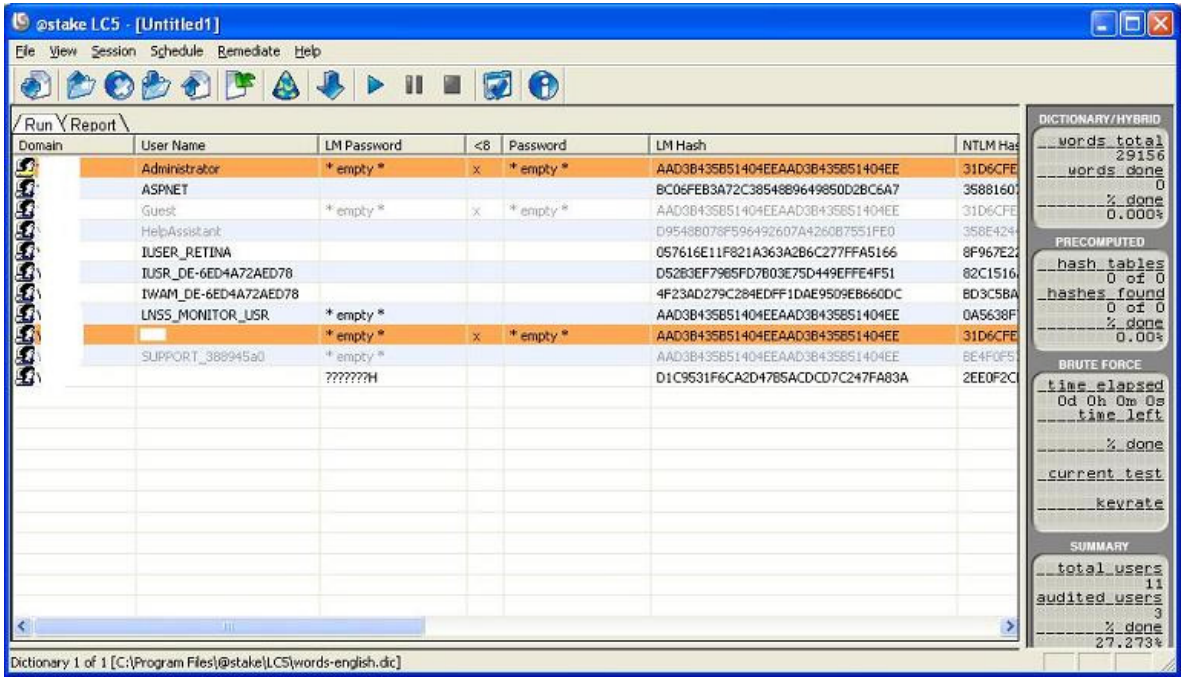
goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

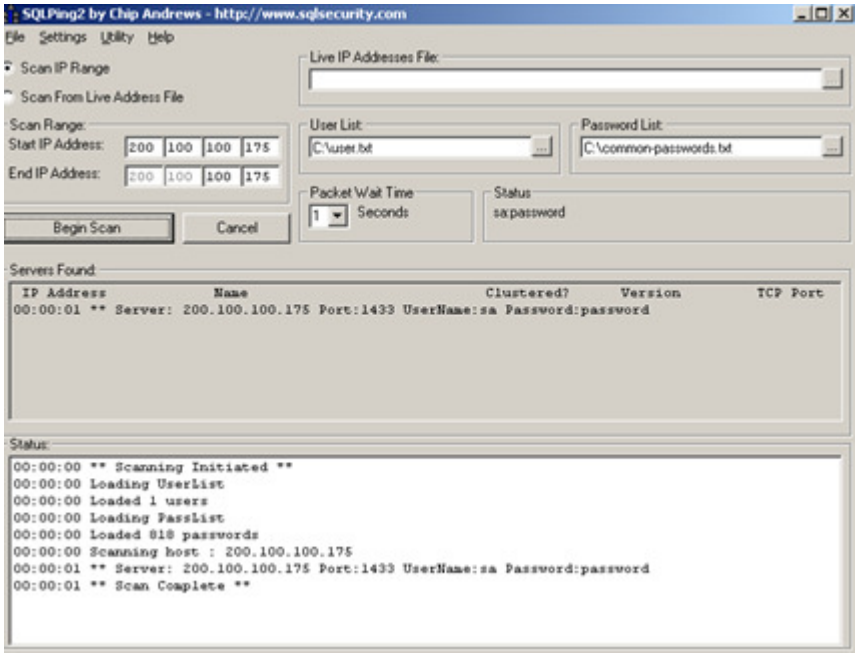
Telefon 052 320 91 20
Fax 052 320 91 21

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 grobfahrlässige 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. 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 forceSQL: forceSQL.exe <IP> SA –b 5. Damit wird eine Brute-Force Attacke auf den Benutzer SA (System Administrator) mit einer maximalen Passwortlänge von fünf Zeichen ausgeführt. Grafisch kann diese Arbeit auch an SQLPing delegiert werden.



5.2 Schwachstellen in Unixsystemen

Auch unter Unix sind Schwachstellen offen. Typische Ports, die als Angriffsziel interessant sein können, sind: ssh (22), telnet (23), finger (79), exec (512), login (513) und shell (514).

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

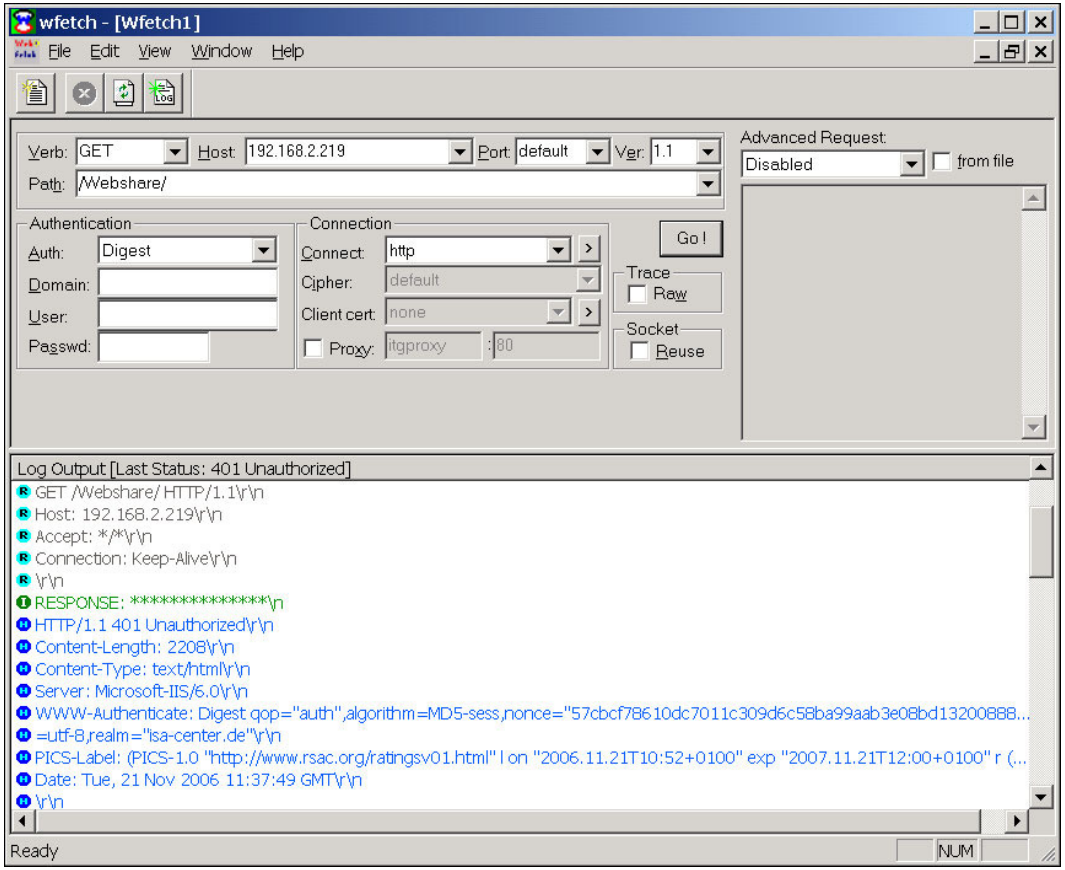
GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

5.3 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 Web-anwendungen 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.



GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

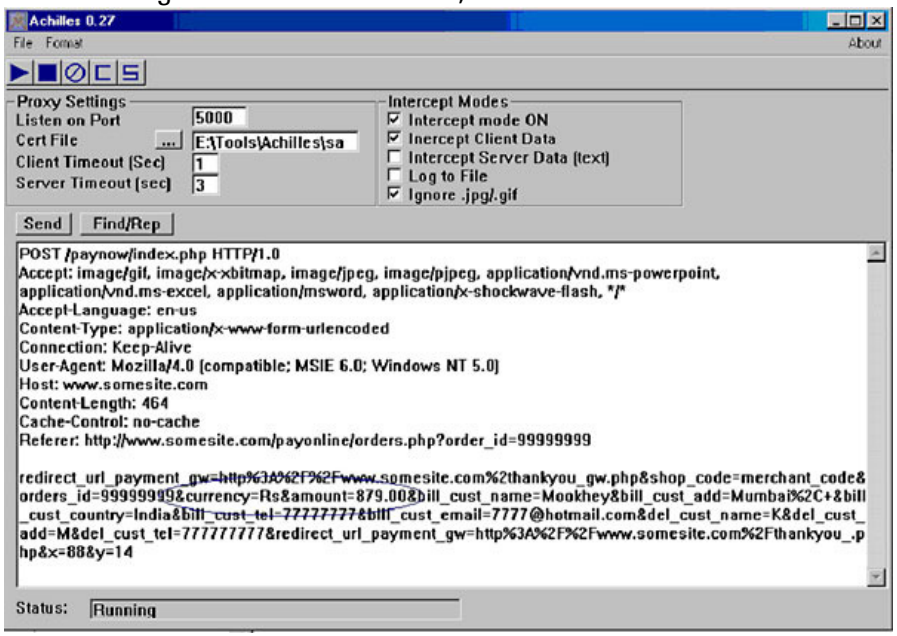
Telefon 052 320 91 20
Fax 052 320 91 21

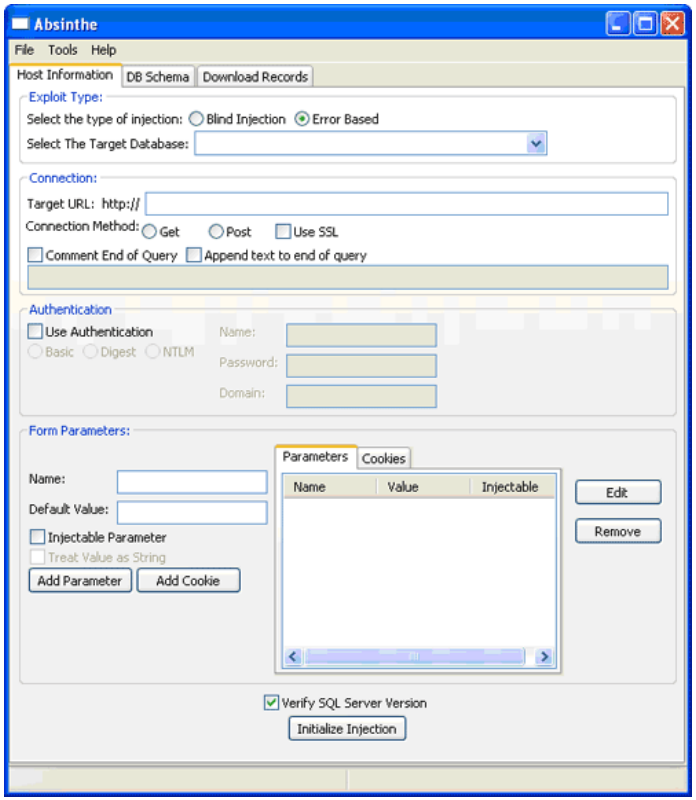
GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

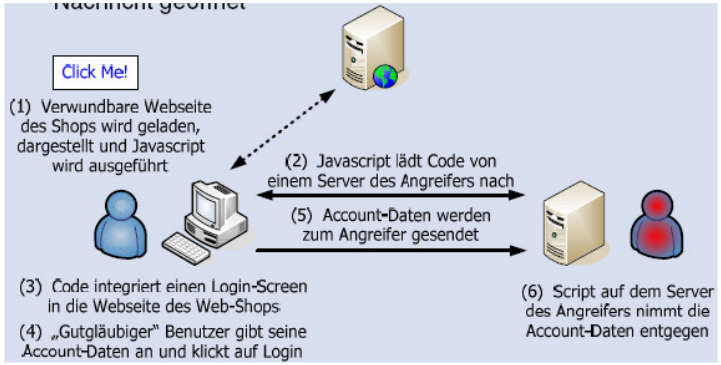
Damit eine Webseite und die übertragenen Daten einfach untersucht werden können, lohnt sich der Einsatz eines Proxys. Achilles Web-Proxy ist ein sehr populärer Web-Proxy, der die Daten vor dem Versenden anzeigt und die Möglichkeit bietet, Modifikationen vorzunehmen (http://www.mavensecurity.com/achilles). 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.

Der erste Angriffspunkt sind oft 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 dieses 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.





Eine neue Gefahr ist Cross Site Scripting. 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 <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.



Quelle: Marc Rennhard, ZHAW, goSecurity Forum #6

6 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.

Versuchen Sie sich als Hacker. Folgende Seiten fordern Sie heraus: http://isatcis.com/ oder das Sicherheitsportal http://www.astalavista.net (nur für Member, dafür mit sehr schweren Aufgaben).

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21