Hacker Highschool
SECURITY AWARENESS FOR TEENS

LEKTION 5
IDENTIFIKATION VON SYSTEMEN

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

"License for Use" Information

The following lessons and workbooks are open and publicly available under the following terms and conditions of ISECOM:

All works in the Hacker Highschool project are provided for non-commercial use with elementary school students, junior high school students, and high school students whether in a public institution, private institution, or a part of home-schooling. These materials may not be reproduced for sale in any form. The provision of any class, course, training, or camp with these materials for which a fee is charged is expressly forbidden without a license including college classes, university classes, trade-school classes, summer or computer camps, and similar. To purchase a license, visit the LICENSE section of the Hacker Highschool web page at www.hackerhighschool.org/license.

The HHS Project is a learning tool and as with any learning tool, the instruction is the influence of the instructor and not the tool. ISECOM cannot accept responsibility for how any information herein is applied or abused.

The HHS Project is an open community effort and if you find value in this project, we do ask you support us through the purchase of a license, a donation, or sponsorship.

Informationen zur Nutzungslizenz

Die folgenden Lektionen und Arbeitsmaterialien sind öffentlich verfügbar unter den folgenden Bedingungen seitens ISECOM:

Alle Materialien der Hacker Highschool werden für den nicht-kommerziellen Einsatz in Grund-, Haupt-, Realschulen und Gymnasien zur Verfügung gestellt, sowohl für öffentliche und private Bildungseinrichtungen, als auch für Privatunterricht zu Hause. Die Materialien dürfen in keiner Form für den Wiederverkauf reproduziert werden. Der kommerzielle Einsatz der Materialien, welche käuflich erworben werden können, in jeglicher Form von Schulstunde, Unterricht, Training, Meeting, Kongress, Vorlesung, Fortbildung, Sommer- oder Abendschulen ist ohne vorigen Erwerb einer Lizenz explizit untersagt. Um eine Lizenz zu erwerben, besuchen Sie bitte http://www.hackerhighschool.org/license.

Das Hacker Highschool (HHS) Projekt ist ein Unterrichtswerkzeug. Der Einfluss auf die Lernenden liegt beim Lehrer, nicht jedoch beim Werkzeug. Aus diesem Grund erkärt sich ISECOM nicht für Schäden verantwortlich, welche aus einem eventuellen Missbrauch der hier publizierten Informationen hervorgehen.

Das HHS Projekt ist die Arbeit einer offenen Gemeinschaft. Wir hoffen, dass die Lesenden Nutzen in unsem Projekt finden werden und bitten um Unterstützung unserer Arbeit, sei es durch den Erwerb einer Lizenz, durch eine Spende, Sponsoring oder in anderer Form.

Inhalt

Mitwirkende

Chuck Truett, ISECOM
Marta Barceló, ISECOM
Kim Truett, ISECOM
Pete Herzog, ISECOM

ÜBERSETZUNG

Georg Berky

Karl Pausch

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

LA SALLE
Enginyeria
Arquitectura

Universitat Ramon Llull

5.0 Einleitung

Für jemanden, der an Deinem Computer sitzt, ist es nicht allzu schwer, Informationen über Dein System zu sammeln, weder über Dein Betriebssystem, noch über die Programme, die auf Deinem Computer laufen. Es ist aber auch möglich, über das Netzwerk Informationen über einen entfernten (remote) Computer zu sammeln. In dieser Lektion lernen wir einige Techniken, wie man derartige Informationen sammeln kann. Wenn wir wissen, wie solche Informationen gesammelt werden, ist es leichter für uns, unsere eigenen Rechner vor solchen Aktivitäten zu schützen.

5.1 Identifikation von Servern

Es gibt im Web eine Menge nützlicher Ressourcen, die es Dir erlauben, Informationen über Domänen- (Domain) Namen und IP-Adressen zu sammeln.

5.1.1. Identifikation des Inhabers einer Domain

Der erste Schritt bei der Identifikation eines Systems ist es, sich die IP-Adresse oder den Domänennamen anzusehen. Mittels eines whois lookup können wir wertvolle Informationen sammeln - sowohl den Namen des Besitzers der Domain, als auch Kontaktinformationen, sogar Telefonnummern. Du solltest beachten, dass es mittlerweile mehrere „domain registrars“ (Organisationen, die Domainnamen vergeben) gibt und nicht alle dieser whois Datenbanken enthalten Informationen für alle Domains. Es könnte also nötig sein, dass Du Dir mehr als eine ansehen musst, um Informationen über die Domäne herauszufinden, für die Du Dich interessierst.

5.1.2. Identifikation der IP-Adresse zu einer Domäne

Es gibt mehrere Möglichkeiten, die IP-Adresse einer Domäne herauszufinden. Die Adresse könnte einerseits in den whois Informationen stehen, andererseits könnte man sie mit Hilfe eines DNS- („domain name service“) Lookup herausfinden. Mittels einer Suchmaschine findest Du sicher nützliche Ressourcen, um die IP-Adresse einer Domain herauszufinden.

Hast Du die Adresse herausgefunden, kannst Du in den records (Datensätzen) der Number Ressource Organisation (http://www.arin.net oder http://www.ripe.net) nach Informationen suchen, wie die IP-Adressen in dieser Domäne verteilt sind. Die IP-Adressen sind auf Netzwerke und ISPs („internet service providers“) verteilt. Es kann sich als sehr hilfreich herausstellen, zu wissen, zu welcher Gruppe eine einzelne IP-Adresse gehört und wer diese Gruppe kontrolliert, wenn Du beispielsweise Informationen über einen Server oder den Service Provider einer Webseite herausfinden willst.

Übungen:
Suche Dir eine existierende Website, etwa isecom.org und führe einen whois Lookup durch, um herauszufinden, wem diese Webseite gehört. Den whois Lookup kannst du etwa bei

http://www.whois.com durchführen. Bei den meisten Linux Distributionen ist whois bereits als Programm installiert, das du aus der Shell heraus ausführen kannst. Welche anderen Informationen erhältst du durch den Lookup? Wann wurde die Domäne erstellt, wann hört sie auf zu existieren? Wann wurde das letzte Update der Informationen durchgeführt?

Finde die IP-Adresse für diesen Domänennamen heraus. Führe einen whois Lookup nach den verschiedenen Mitgliedern der Number Ressource Organisation durch, um herauszufinden, wem diese Adresse zugewiesen worden ist. (Beginne bei www.arin.net wo Du auch Links zu den anderen Mitgliedern der NRO findest.) Wie ist die IP-Range (die Menge von IP-Adressen), zu der auch der gesuchten Domäne gehört?

5.2 Identifikation von Services

Hast Du den Besitzer und die IP-Adresse einer Domäne herausgefunden, kannst Du anfangen, nach Informationen über den Server, auf den sich diese Domäne bezieht, zu suchen.

5.2.1. Ping und Traceroute

Da Du jetzt weißt, wem die Domäne gehört und wem die IP-Adresse zugewiesen worden ist. Nun kannst Du überprüfen, ob der Server, auf dem sich die Webseite befindet, auch aktiv ist. Der Ping-Befehlt wird Dir sagen, ob überhaupt ein Server mit dieser IP-Adresse oder Domäne verbunden ist.

ping Domäne ODER
ping IP-Adresse

wird Dir sagen, ob es einen aktiven Computer an dieser Stelle gibt.

Ein weiterer Befehl tracert (unter Windows) oder traceroute (unter Linux) zeigt Dir die Route an, welche die Pakete von Deinem zum entfernten Computer nehmen. Mit diesem Befehl erhältst du auch zusätzliche Informationen über die anderen Computer im Netzwerk deines Zielcomputers. Computer mit gleichen IP-Adressen sind meistens Teil des selben Netzwerkes.

Übungen:

Pinge eine existierende Webseite oder IP-Adresse (etwa isecom.org oder 216.92.116.13). Wenn Du eine positive Antwort erhältst (wenn der gepingte host also auf deine Anfrage reagiert), probiere es mit dem nächsten. Erhältst Du hier auch eine positive Antwort?

Verwende traceroute (oder tracert unter Windows), um die Route von Deinem Rechner zum entfernten Rechner der vorigen Übung herauszufinden. Wie viele Sprünge (sogenannte „hops“) brauchen die Pakete? Sind die IP-Adressen von einigen Hops ähnlich?

5.2.2. Banner grabbing

Der nächste Schritt zur Identifizierung eines entfernten Computers ist, sich mittels telnet oder

FTP dorthin zu verbinden. Die Serverprogramme dieser Dienste zeigen bei der Verbindung meistens ein sogenanntes Banner an. Bei einem FTP Server sieht das beispielsweise so aus:

```
 Connected to anon.server.
220 ProFTPD Server (Welcome . . . )
User (anon.server:(none)):
```

220 ist ein Code des FTP-Protokolls, der angibt, dass der Server für einen neuen Benutzer bereit ist. „ProFTPD Server“ ist der Name des Serverprogramms, welches auf dem entfernten Computer läuft. Mit einer Suchmaschine kannst Du herausfinden, auf welchem Betriebssystem das Programm läuft, was es kann, was es nicht kann und welche bekannten Fehler es in diesem Programm gibt.

Das größte Problem bei der banner grabbing Methode ist die Tatsache, dass der Administrator das Banner fälschen und durch ein anderes, plausibel aussehendes ersetzen kann, was sich „banner spoofing“ nennt. Bei einem Banner mit „Was geht dich mein Server eigentlich an?“ ist es Dir sicher klar, dass es sich um eine Fälschung handelt, aber „WS_FTP Server“ (ein Server für Windows) auf einer Unix Maschine ist nicht so leicht als Fälschung zu identifizieren und könnte sogar Deine ganze Informationssuche in die falsche Richtung leiten.

5.2.3. Identifikation von Services durch Ports und Protokolle

Wir können auch feststellen, welche Dienste auf einem Rechner laufen, wenn wir uns die offenen Ports und die verwendeten Protokolle ansehen.

Sieh Dir zunächst Deinen eigenen Computer an. Öffne ein DOS-Fenster oder eine Shell und starte das netstat Programm:

```
netstat -a
```

Der Computer wird Dir alle offenen Ports anzeigen und einige der Dienste, die diesen Port verwenden:

```
Active Connections:
Proto Local Address              Foreign Address      State
TCP   YourComputer:microsoft-ds YourComputer:0       LISTENING
TCP   YourComputer:1025          YourComputer:0       LISTENING
TCP   YourComputer:1030          YourComputer:0       LISTENING
TCP   YourComputer:5000          YourComputer:0       LISTENING
TCP   YourComputer:netbios-ssn   YourComputer:0       LISTENING
TCP   YourComputer:1110          216.239.57.147:http TIME_WAIT
UDP   YourComputer:microsoft-ds *:*
UDP   YourComputer:isakmp        *:*
UDP   YourComputer:1027          *:*
UDP   YourComputer:1034          *:*
UDP   YourComputer:1036          *:*
UDP   YourComputer:ntp           *:*
UDP   YourComputer:netbios-ns    *:*
UDP   YourComputer:netbios-dgm   *:*
```

Hier kannst Du viele der aktiven Dienste auf deinem Computer sehen, von denen Du vielleicht noch nicht einmal wusstest, dass sie laufen.

Ein anderes Programm namens fport gibt Dir ähnliche Informationen wie netstat, zeigt aber zusätzlich noch das Programm an, das den Port verwendet. Du kannst es kostenlos unter http://www.foundstone.com herunterladen. Unter Linux kannst Du auch die -p Option für netstat verwenden, um die Programme zu den Verbindungen anzuzeigen.

Ein anderes Programm namens nmap (für „network mapper“) überprüft Computer um einiges gründlicher auf offene Ports. Wenn Du es startest, wird es alle offenen Ports und Dienste oder Protokolle die diese Ports nutzen anzeigen. Es kann auch erraten, welches Betriebssystem der entfernte (remote) Computer verwendet. Wenn Du nmap auf Deinen Computer einsetzt (das Beispiel unten zeigt einen Linux Rechner), wirst Du etwa folgendes Ergebnis erhalten:

```
Port    State Service
22/tcp        open  ssh
68/tcp        open  dhcpclient
139/tcp       open  netbios-ssn
445/tcp       open  microsoft-ds
Device type: general purpose
Running: Linux 2.4X|2.5.X
OS details: Linux Kernel 2.4.0  2.5.20
Uptime 1.024 days (since Sat Jul 4 12:15:48 2004)
```

Nmap findest Du auf der Hackerhighschool- oder L.A.S.-CD. Du kannst es auch von http://www.insecure.org herunterladen.

Übungen:

Verwende netstat mit der -a Option auf Deinem eigenen Computer:

```
netstat -a
```

Welche offenen Ports werden angezeigt? Suche mit einer Suchmaschine, um die Services, die diesen Port verwenden, herauszufinden. Das kannst du auch auf Deinem Computer zuhause machen, um herauszufinden, ob dort Dienste laufen, die womöglich gefährlich sind, etwa telnet oder ftp.

Starte nmap und lass nmap Deinen Computer scannen. Verwende die -sS Option für Syn-Scan und -O (großes O), um Dein Betriebssystem erraten zu lassen.

```
nmap -sS -O 127.0.0.1
```

Die IP-Adresse 127.0.0.1 gibt immer Deinen lokalen Computer an. Jeder Computer hat die IP-Adresse 127.0.0.1, die immer auf ihn selbst zeigt. Diese spezielle IP-Adresse unterscheidet sich von den anderen IP-Adressen, die alle verschieden sein müssen, um Verbindungen mit anderen Computer zu ermöglichen.

Welche offenen Ports findet nmap? Welche Services und Programme verwenden diese Ports? Ändert sich das Ergebnis von nmap, während du beispielsweise mit deinem Browser eine Webseite ansiehst. Ändert sich dabei das Ergebnis von netstat?

5.3 Der Fingerabdruck eines Systems: Fingerprinting

Da wir jetzt wissen, wie wir einen Server identifizieren und nach offenen Ports scannen, um die laufenden Dienste auf dem Rechner zu erfahren, können wir diese Informationen zusammen verwenden, um einen fingerprint („Fingerabdruck") des entfernten Computers zu erstellen. Dieser fingerprint sagt uns etwas über das wahrscheinlich laufende Betriebssystem und die Dienste auf diesem Rechner.

5.3.1. Scannen des Computers

Wenn Du dem Programm nmap eine andere Adresse oder einen anderen host als z.B. 127.0.0.1 oder localhost zum scannen angibst, kannst Du damit auch auf entfernten Computern nach offenen Ports suchen. Natürlich gibt es dort nicht notwendigerweise offene Ports, aber mit nmap kannst Du das wenigstens überprüfen.

Stelle Dir beispielsweise vor, dass Du eine große Menge Spam Mails empfängst. Du wirst wahrscheinlich herausfinden wollen, wer Dir diese Spam-Mails sendet. Wenn wir uns die Header der Mails ansehen, stellen wir fest, dass die meisten von der gleichen IP-Adresse kommen, zum Beispiel von 256.92.116.13 (in Lektion 9 findest Du mehr über Mail-Header).

Ein whois Lookup sagt Dir, dass die IP-Adresse aus einer großen IP-Range eines großen ISPs kommt, gibt Dir allerdings keine weiteren Informationen über diese spezielle IP-Adresse.

Wenn du dann nmap verwendest um diesen Computer zu scannen, bekommst Du in etwa solche Informationen:

```
nmap -sS -O 256.92.116.13
Starting nmap 3.50 ( http://www.insecure.org/nmap ) at 2004-07-03 20:13
Eastern Daylight Time
Interesting ports on 256.92.116.13:
(The 1632 ports scanned but not shown below are in state: closed)
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
23/tcp    open     telnet
25/tcp    open     smtp
80/tcp    open     http
110/tcp    open     pop3
113/tcp    open     auth
135/tcp    filtered msrpc
136/tcp    filtered profile
137/tcp    filtered netbios-ns
138/tcp    filtered netbios-dgm
139/tcp    filtered netbios-ssn
143/tcp    open     imap
144/tcp    open     news
161/tcp    filtered snmp
306/tcp    open     unknown
443/tcp    open     https
445/tcp    filtered microsoft-ds
513/tcp    open     login
514/tcp    open     shell
```

```
No exact OS matches for host (If you know what OS is running on it, see
http://www.insecure.org/cgi-bin/nmap-submit.cgi).
TCP/IP fingerprint:
SInfo(V=3.50%P=i686-pc-windows-windows%D=7/3%Time=40E74EC0%O=21%=1)
TSeq(Class=TR%IPID=RD%TS=1000HZ)
T1(Resp=Y%DF=Y%W=FFFF%ACK=S++%Flags=AS%Ops=MNWNNT)
T2(Resp=N)
T3(Resp=N)
T4(Resp=N)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=N)
T7(Resp=N)

Uptime 1.877 days (since Thu Jul 01 23:23:56 2004)
Nmap run completed -- 1 IP address (1 host up) scanned in 775.578 seconds
```

Die Ports, die als filtered erkannt worden sind, sind sehr bekannt dafür potentiell angreifbar zu sein. Es ist, also kein Wunder, dass sie gefiltert werden. Was für uns am interessantest ist, sind die Ports 21, 22 und 23 für FTP, SSH und Telnet.

Als letztes versucht nmap noch, das Betriebssystem des Zielrechners festzustellen. In unserem Fall führten die Tests von nmap zu keinem aufschlussreichen Ergebnis. Da wir aber auf Port 21, 22 und 23 Dienste entdeckt haben, können wir versuchen, uns dorthin zu verbinden, um über eventuell vorhandene Banner etwas über das Zielsystem herauszufinden. Wenn wir uns mit FTP mit dem remote Rechner verbinden, erhalten wir folgendes Ergebnis:

220 ftp316.pair.com NcFTPd Server (licensed copy) ready.

Verbinden wir uns mittels Telnet, bekommen wir folgendes Ergebnis:

FreeBSD/i386 (ttyp7)

Eine kurze Suche im Web sagt uns, dass FreeBSD ein Unix-ähnliches Betriebssystem und NcFTPd ein FTP-Server für Unix ist. Wir können uns zwar nicht ganz sicher sein (Banner können gefälscht werden), aber diese zwei Indizien deuten auf die Richtigkeit unserer Vermutung hin.

Mit nmap, telnet und ftp haben wir jetzt also herausgefunden, dass der Server, der uns Spam geschickt hat, wohl ein Unix-ähnliches Betriebssystem verwendet – wahrscheinlich FreeBSD – und dazu benutzt (verwendet) wird, mit Hilfe einer Menge von Diensten (ftp, telnet, http, smtp, pop3) eine große Menge von Informationen zu verschicken.

Weitere Informationen

Nmap: http://www.insecure.org/nmap/

Mehr über Nmap:
http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=8702942&classroom=

Fport:http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/proddesc/fport.htm

Ein paar Seiten über Ports und Dienste, die diese verwenden:
http://www.chebucto.ns.ca/~rakerman/port-table.htm
http://www.chebucto.ns.ca/~rakerman/port-table.html#IANA
http://www.iana.org/assignments/port-numbers
http://www.networksorcery.com/enp/protocol/ip/ports00000.htm

DNS lookups: http://www.dnsstuff.com/

Ping: http://www.freesoft.org/CIE/Topics/53.htm