Hacker Highschool
SECURITY AWARENESS FOR TEENS

LES 5
SYSTEEM IDENTIFICATIE

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.

All works copyright ISECOM, 2004.

Informatie over de “Gebruiksvoorwaarden”

De lessen en werkboeken van het Hacker Highschool (HHS) project zijn beschikbaar onder de volgende door ISECOM gestelde voorwaarden:

Alle informatie uit het HHS-project mag, niet-commercieel, gebruikt worden voor en door basisschool-leerlingen en studenten van middelbaar en hoger onderwijs. Dit materiaal mag niet worden gereproduceerd voor (door-)verkoop in welke vorm dan ook. Gebruik van dit materiaal in een klas, cursus, training, kamp of andere georganiseerde vorm van kennisoverdracht waarvoor geld wordt gevraagd is expliciet verboden zonder een licentie. Om een licentie te regelen kunt u het onderdeel LICENSE bezoeken op de website van de Hacker Highschool, www.hackerhighschool.org/license.

Het HHS-project is een leermiddel en, zoals met elk leermiddel, de docent/trainer bepaalt in grote mate het effect van het leermiddel. ISECOM kan geen aansprakelijkheid aanvaarden voor de positieve of negatieve gevolgen van het gebruik van dit materiaal en de daarin opgenomen informatie.

Het HHS-project is een initiatief van de open community, en wanneer u de resultaten van onze inspanning waardevol genoeg vindt om het te gebruiken, vragen we u uw steun te betuigen door:

- de aankoop van een licentie;
- een donatie
- ons te sponsoren.

Op al het werk berust copyright van ISECOM, 2004.

Inhoudsopgave

Contributors

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

Vertaald door:

Raoul Teeuwen

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

LA SALLE
Enginyeria
Arquitectura

Universitat Ramon Llull

5.0 Introductie

Het is logisch dat iemand die achter het toetsenbord van je computer plaatsneemt, informatie van die computer kan achterhalen, zoals het besturingssysteem dat in gebruik is en welke programma's er op draaien, maar het is ook mogelijk om een netwerkverbinding te gebruiken en veel van zulke informatie te verzamelen over een computer op afstand (remote computer). In deze les vertellen we je over manieren om zulke informatie te verzamelen. Als je weet hoe zulke informatie verzameld kan worden, kan je zorgen dat jouw systeem zulke gegevens niet prijsgeeft.

5.1 Een server identificeren

Er is een aantal handige bronnen op internet waarmee je informatie over domeinnamen en IP-adressen kunt achterhalen.

5.1.1 De eigenaar van een domein vaststellen

De eerste stap om een computer op afstand te identificeren is te kijken naar de domein-naam of het IP-adres. Door een Whois lookup te doen kom je achter waardevolle informatie, zoals de eigenaar van de domeinnaam en zijn contactgegevens, mogelijk inclusief adressen en telefoonnummers. Merk op dat er tegenwoordig een aantal domein-registrars zijn, en dat niet in alle whois databases informatie staat over alle domeinen. Wellicht moet je dus meerdere whois databases doorzoeken om informatie te vinden over de domeinnaam die je onderzoekt.

5.1.2 Het IP-adres van een domein vaststellen

Er is een aantal manieren om het IP-adres te achterhalen dat bij een domein hoort. Het adres zit mogelijk bij de whois informatie, of je zult een DNS of Domain Name Service lookup moeten gebruiken. (Een web zoekmachine zal een aantal bronnen ophoesten om IP-adressen te achterhalen via domeinnamen.)
Als je het IP-adres hebt kun je de gegevens van de verschilende leden van de Number Resource Organization (http://www.arin.net/ of http://www.ripe.net/) gebruiken om informatie te achterhalen over hoe IP-adressen zijn verdeeld. IP-nummers worden in grote groepen toegekend aan service providers en netwerken, en weten in welke groep een IP-adres valt en wie rechten heeft tot die groep, kan zeer waardevol zijn. Het kan helpen achter informatie te komen over de server of de service provider waar een website gebruik van maakt.

Oefeningen:
Neem een geldige domeinnaam and gebruik een Whois lookup om er achter te komen van die dat domein is.
dominio (http://www.whois.com -> “isecom.org”+Go -> Whois Lookup) Welke andere informatie is beschikbaar? Wanneer is het domein aangemaakt (created)? Wanneer vervalt (expired) het? Wanneer zijn de gegevens voor het laatst bijgewerkt (updated)?
Vind het ip-adres van deze domeinnaam. Gebruik de whois lookups van de verschillende leden van de Number Resource Organization om te achterhalen aan wie het IP-adres is toegekend. (Begin op de www.arin.net, pagina. Daar tref je ook links naar andere leden van de NRO.) Welke andere reeksen/blokken/groepen van IP-nummers zijn aan deze organisatie toegekend?

5.2 Services vaststellen

Zodra je de eigenaar en het IP-adres van een domein hebt vastgesteld kun je gaan kijken naar informatie over de server waar het domein naar verwijst.

5.2.1 Ping en TraceRoute

Nu je weet wie de eigenaar is van het domein en aan wie het IP-nummer is toegekend, kun je gaan kijken of de server waarop de website draait actief is. Het ping commando vertelt je of er daadwerkelijk een computer is verbonden met het domein of IP. Het commando

ping domein of
ping ipadres
ESSON 5 – SYSTEM IDENTIFICATION
vertelt je of er een actieve computer is op dat adres.
Als de output van het ping commando aangeeft dat de pakketjes die zijn verstuurd ook werden ontvangen, dan kun je er van uitgaan dat de server actief is.
Een ander commando, tracert (in Windows) of traceroute (in Linux) laat je de route zien die pakketjes afleggen als het van jouw computer naar de computer op afstand probeert te komen. Het bekijken van de route die pakkets afleggen levert soms informatie op over computers die in hetzelfde netwerk zitten als de computer waar je onderzoek naar doet. Zo zijn computers met een sterk gelijkend IP-adres vaak verbonden in hetzelfde netwerk.
Oefeningen:
Ping een geldige website of IP-adres (ping www.isecom.org of ping 216.92.116.13). Als je een succesvolle reactie krijgt, ping dan het volgende IP-adres. Kreeg je daar ook een succesvolle reactie?
Gebruik tracert of traceroute om de route te bekijken vanaf je eigen computer naar het IP-adres dat je in de vorige oefening hebt gebruikt. Langs hoeveel computers komen de pakketjes? Zijn er computers met een gelijksoortig IP-adres?

5.2.2 Banner Grabbing

De volgende stap in het identificeren van een computer op afstand is proberen een verbinding te maken via telnet en FTP. De server-programma's voor die services tonen tekst-berichten die men banners noemt. Een banner toont soms duidelijk en precies welk server-programma aan het werk is. Wanneer je bijvoorbeeld verbinding maakt met een anonieme FTP-server krijg je wellicht het volgende bericht te zien:

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

Terwijl het nummer 220 een FTP-code is waarmee wordt gecommuniceerd dat de server klaar is voor een nieuwe gebruiker, zien we aan de tekst-boodschap ProFTPD Server welk FTP server-programma draait op de computer op afstand. Door vervolgens een internet zoekmachine te gebruiken kun je achterhalen welk besturingssysteem in gebruik is, inclusief andere details zoals minimum systeemvereisten, mogelijkheden, beperkingen en bekende problemen/gaten. Het grootste probleem als je banner-informatie gebruikt om een beeld te krijgen van het systeem op afstand, is dat slimme systeembeheerders valse informatie in die

banners kunnen opnemen. Een banner met de tekst GaatJeNiksAanServer is duidelijk vals, maar een Unix system met een banner met de tekst WS_FTP Server (een Windows-gebaseerde FTP server) maakt een onderzoek lastig.

5.2.3 Services van poorten en protocollen identificeren

Je kunt ook bepalen welke programma's actief zijn op een systeem door te kijken welke poorten open staan en welke protocollen in gebruik zijn.
Start maar eens door te kijken naar je eigen lokale computer. Gaan naar een commando-prompt of shell prompt en voer het netstat programma uit met de -a (of all) parameter:
netstat -a
De computer zal een lijst met open poorten tonen, inclusief enkele van de services die gebruik maken van die poorten:

Active Connections
LESSON 5 – SYSTEM IDENTIFICATION
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 *:*
Hiermee krijg je zicht op vele van de op je lokale computer actieve programma's en services – velen waarvan je vast geen idee had dat ze actief waren/zijn.
Een ander programma, fport, levert informatie die sterk lijkt op die van netstat, maar het geeft ook gedetailleerde informatie over welke programma's gebruik maken van de open poorten en protocollen. (Fport is gratis te downloaden van www.foundstone.com.)
Een ander programma, nmap (voor network mapper) doet nog grondiger onderzoek naar de open poorten op je computer. Als nmap wordt uitgevoerd toont het een lijst van open poorten en de services of protocollen die gebruik maken van de open poorten. Het is wellicht ook in staat te bepalen welk besturingssysteem je computer gebruikt. Als je bijvoorbeeld nmap op je lokale computer loslaat kun je iets zien als het volgende:
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 is beschikbaar bij je Hacker Highschool of de L. A. S.-cd. Je kunt het ook downloaden van www.insecure.org.

Oefening:
Voer netstat uit op je lokale computer, en gebruik de -a parameter.
netstat -a
LESSON 5 – SYSTEM IDENTIFICATION
Welke poorten zijn open? Kun je, met een internet zoekmachine, uitvinden welke services van die poorten gebruik maken? (Dit is ook een prima oefening om thuis uit te proberen, om te zien of je computer overbodige – en potentieel gevaarlijke – services zoals FTP en telnet draait.)
Voer nmap, uit en gebruik de -sS (voor SYN Stealth scan) en -O (voor ' raad het besturingssysteem) parameters
en het IP-adres 127.0.0.1 als doelwit.
nmap -sS -O 127.0.0.1
IP-adres 127.0.0.1 is de local host, oftewel je lokale computer. (Let op: dit is een ander IP-adres dan wat computers op het internet gebruiken om met je systeem te communiceren; op elke computer verwijst IP-adres 127.0.0.1 naar de lokale computer) Welke open poorten vindt nmap? Welke services en programma's maken gebruik van die poorten? Probeer nmap eens uit te voeren terwijl je een webbrowser of de telnet client open hebt staan. Zie je verschil in de resultaten van nmap?

5.3 System Fingerprinting

Nu je weet hoe je de identiteit van een server moet vaststellen en hoe je een scan doet van de open poorten en met deze informatie bepaalt welke services er actief zijn, kun je die informatie gebruiken om een systeem op afstand te fingerprinten, waarbij je bepaalt wat waarschijnlijk het besturingssysteem is en welke services er op het systeem actief zijn.

5.3.1 Computer op afstand onderzoeken

Als je een IP-adres of een domeinnaam anders dan 127.0.0.1 als parameter van nmap gebruikt kun je open poorten op computers op afstand onderzoeken. Het betekent niet dat er open poorten zullen zijn of dat je ze zult vinden, maar je weet nu hoe je het kunt proberen.
Stel dat je bijvoorbeeld grote hoeveelheden spam mails ontvangt en je wil informatie achterhalen over de persoon die je de e-mails stuurt. Je bekijkt de headers van enkele van de e-mails en ziet dat de meeste e-mails afkomstig zijn van hetzelfde IP-adres: 256.92.116.13 (zie Les 9: E-mail Beveiliging voor meer details over het bekijken van email headers).
Via een whois lookup zie je dat het adres onderdeel uitmaakt van een blok adressen dat is toegewezen aan een grote ISP, maar je ziet geen informatie over het specifieke IP-adres.
Als je vervolgens nmap gebruik om de computer op dat adres te scannen, krijg je de volgende resultaten:
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%C=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

De poorten die gemarkeerd zijn als filtered staan bekend als kwetsbaar voor aanvallen, dus het is niet vreemd dat die worden getoond als gefiltered. Wat zeer interessant is, is dat poorten 21, 22 en 23 – voor
ftp, ssh en telnet – allemaal als open worden gerapporteerd.

Het laatste wat nmap probeert te doen is bepalen welk besturingssysteem draait op de gescande computer. In dit geval zijn de resultaten van de tests die nmap uitvoert onvoldoende om dat te bepalen, maar omdat nmap laat zien dat ftp- en telnet-services beiden draaien, kan je nog proberen daar verbinding mee te maken om te zien of de banners nog informatie prijsgeven.

Wanneer je een FTP-verbinding maakt zie je de volgende banner:
LESSON 5 – SYSTEM IDENTIFICATION
220 ftp316.pair.com NcFTPd Server (licensed copy) ready.

Wanneer je vervolgens via telnet verbinding probeert te maken, toont de computer de volgende banner
FreeBSD/i386 (ttyp7)

Via een snelle zoektocht op het internet kom je er achter dat NcFTPd een Unix programma is en dat FreeBSD een Unix-achtig besturingssysteem is, dus is het waarschijnlijk dat de server een versie van FreeBSD gebruikt als zijn besturingssysteem. Je kunt er niet zeker van zijn dat dit klopt (de informatie van banners kan vals zijn), maar de informatie is bruikbaar voor een redelijke gok.

Gebruikmakend van nmap, aangevuld met FTP en telnet, heb je vastgesteld dat de server vanwaar spam naar jou is verstuurd, draait op een Unix-achtig besturingssysteem– waarschijnlijk FreeBSD – en dat die machine is geconfigureerd om een grote verscheidenheid aan informatie te ontvangen en versturen, via een aantal services waaronder FTP,telnet, http, smtp en pop3.

Verder lezen

Nmap: http://www.insecure.org/nmap/
Meer over 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
Een aantal websites met informatie over poorten en de services die er gebruik van maken:
http://www.chebucto.ns.ca/~rakerman/port-table.html
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
Verschillnde mogelijkheden voor DNS lookups: http://www.dnsstuff.com/
Ping:http://www.freesoft.org/CIE/Topics/53.htm