Hacker Highschool
SECURITY AWARENESS FOR TEENS

LES 8
DIGITAAL FORENSISCH ONDERZOEK

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

"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.

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

Table of Contents

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

Auteurs

Simon Biles, Computer Security Online Ltd.
Pete Herzog, ISECOM
Chuck Truett, ISECOM
Marta Barceló, ISECOM
Kim Truett, ISECOM

Vertaald door:

Raoul Teeuwen

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

8.0 Introductie

Forensisch onderzoek gaat over het toepassen van een gestructureerde onderzoekstechniek om een serie gebeurtenissen te reconstrueren. De meeste mensen zijn tegenwoordig bekend met forensisch onderzoek via film en TV, ondermeer door het populaire "CSI (Crime Scene Investigation)". Forensische wetenschap was lange tijd – en eigenlijk nog steeds – sterk verbonden met Forensische Pathology – achterhalen hoe mensen zijn overleden. De vroegste optekening op gebied van forensisch onderzoek is ook op dat gebied.
In 1248 werd een Chinees boek, *Hsi DuanYu* (het wegspoelen van verkeerde zaken), gepubliceerd. Het boek beschrijft hoe je kunt bepalen of iemand is verdronken of gewurgd.[1]
Digitaal forensisch onderzoek is wat minder rommelig en wat minder bekend. Het is de kunst van het reconstrueren wat er in een digitaal apparaat is gebeurd. Vroeger was het beperkt tot computers, tegenwoordig omvat het alle digitale apparaten zoals mobiele telefoons, digitale camera's en GPS[2]-apparaten. Het is gebruikt om moordenaars, kidnappers, fraudeurs, mafia-bazen en anderen met slechte bedoelingen te pakken.

In deze les gaan we twee aspecten van forensisch onderzoek behandelen (allemaal computer gebaseerd helaas – hier geen mobiele telefoon-zaakjes).
1. Wat mensen zoal doen met hun eigen computer.
Dit omvat ...
- ... het herstellen van verwijderde bestanden.
- ... elementaraire decryptie.
- ... zoeken van bepaalde bestandstypes.
- ... zoeken van bepaalde zinnen.
- ... het bekijken van interessante gebieden op de computer.

2. Wat gebruikers op afstand (remote user) zoal doen op de computer van een ander.
Dit omvat ...
- ... het lezen van logbestanden.
- ... acties reconstrueren.
- ... de bron achtrhalen.

Deze les gaat zich concentreren op tools zoals die beschikbaar zijn voor Linux. Er zijn ook tools beschikbaar voor het Windows-platform, evenals gespecialiseerde forensische hard- en software, maar omdat Linux in staat is vele bestands en besturings-systemen te benaderen en begrijpen, is het de ideale omgeving voor de meeste forensische acties.
1 Kennelijk heeft het iets te maken met de afdrukken die rond de keel achterblijven, en de mate waarin het water is doorgedrongen in de longen.
2 Global Positioning System – een ding dat je vertelt waar je je op aarde bevindt aan de hand van een aantal satelietten.

8.1 Forensische principes

8.1.0 Introductie

Er is een aantal basis principes die je in acht moet nemen, of je nu een computer onderzoekt, of een lijk. In dit deel lees je een korte samenvatting van die principes.

8.1.1 Voorkom besmetting

Op TV zie je forensische onderzoekers in witte jassen en met handschoenen bewijsmateriaal verzamelen met een pincet en het in afsluitbare plastic zakken stoppen. Dit doen ze om

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

"besmetting" te voorkomen. Dan gaat het er bijvoorbeeld om dat er vingerafdrukken worden toegevoegd aan het handvat van een mes door iemand die het oppakt (denk aan de *Fugutive* als je die gezien hebt ... Kijk welke problemen hij er door kreeg!)

8.1.2 Ga methodisch te werk

Wat je ook doet, als (wanneer?) je terecht komt in een rechtbank moet je in staat zijn alles wat je gedaan hebt te rechtvaardigen. Wanneer je op een wetenschappelijke en methodische manier te werk gaat, nauwgezet aantekeningen maakt over wat je doet en hoe je dat doet, dan wordt verantwoording afleggen een stuk eenvoudiger. Het zorgt er ook voor dat iemand anders je stappen kan nagaan en controleren of je geen fouten hebt gemaakt waardoor je bewijs in twijfel kan worden getrokken.

8.1.3 De keten van bewijs

Je moet bewaken dat je de zogenaamde "Keten van bewijs" in tact houdt. Dit betekent dat je van elk moment in de tijd, vanaf het moment dat iets als bewijsmateriaal werd geidentificeerd tot het moment waarop het in de rechtbank wordt getoond, je moet kunnen vertellen waar het bewijsstuk was en wie er toegang toe had. Hiermee moet duidelijk worden gemaakt dat er in die tijd op geen enkele manier met het bewijs kon worden geknoeid.

8.1.4 Conclusie

Onthoudt deze dingen goed, en je zult, ook als je je werk nooit mee hoeft te nemen naar een rechtbank, je vaardigheden als forensisch onderzoeker kunnen maximaliseren.

8.2 Stand-alone forensisch onderzoek

8.2.0 Introductie

Dit deel gaat over het forensisch onderzoek van een individuele machine. Bij gebrek aan een betere term noemen we het "stand-alone forensisch onderzoek". Dit is waarschijnlijk de meest voorkomende vorm van computer forensisch onderzoek – het belangrijkste doel is uitvinden wat er is gebeurd met gebruikmaking van een bepaalde computer. De forensisch onderzoeker zou kunnen zoeken naar bewijs van fraude, zoals financiele
spreadsheets, bewijs van communicatie met iemand anders, e-mails of een adressenlijst, of bewijs van een bepaalde aard, zoals pornografische afbeeldingen.

8.2.1 Hard disk en opslagmedia basics

Er zijn verschillende onderdelen waaruit een gemiddelde computer bestaat. Je hebt de processor,
geheugen, grafisch kaarten, DVD/CD-spelers en nog veel meer. Eén van de meest cruciale onderdelen is de harddisk (harde schijf, hard drive). Hier is het merendeel van de informatie opgeslagen die een computer nodig heeft om te kunnen werken. Ze bevatten het besturingssysteem (Operating System (OS)) zoals Windows of Linux, evenals

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

gebruikersapplicaties zoals tekstverwerkers en spelletjes. En het is ook de plaats waar een enorme hoeveelheid data is opgeslagen, bewust, doordat de gebruiker een bestand heeft opgeslagen, of onbewust, door het gebruik van tijdelijke bestanden en cache-bestanden. Hiermee kan een forensisch onderzoeker reconstrueren welke acties een gebruiker op een computer heeft uitgevoerd, welke bestanden zijn benaderd en nog veel, veel meer.
Je kunt op meerdere nivo's een harde schijf onderzoeken. Voor deze oefening zullen we alleen kijken naar het nivo van het bestandssysteem. Het is echter goed te beseffen dat professionals in staat zijn harde schijven tot in groot detail te bekijken en de inhoud te bepalen – zelfs als hij meerdere malen overschreven is.
Het bestandssysteem van een computer is te vergelijken met een archiefkast. Het bevat laden/planken
(partities), mappen (directories) en individuele documenten (bestanden/files). Bestanden en directories kunnen onzichtbaar zijn, alhoewel dit oppervlakkig is en makkelijk ongedaan gemaakt kan worden.
Door de volgende oefeningen uit te voeren krijg je een veel beter begrip van de basisbegrippen van disk opslag.

Oefeningen:
Zoek voor alle volgende kreten op gebied van opslagmeda informatie over wat ze betekenen en hoe ze werken. Begrip van hoe dingen werken is normaal gesproken de eerste stap op gebied van forensische studie.
1. Magnetische/Harde/Fysieke schijf: dit is waar je computer bestanden opslaat. Leg uit hoe magnetisme wordt gebruikt in/op een harde schijf.
2. Tracks: waar heeft men het over als men praat over "tracks op een harddisk"?
3. Sectors: Dit is een vast gebiedje waar data in past. Leg uit hoe.
4. Cluster/Allocation unit: leg uit waarom een bestand als hij naar schijf wordt geschreven meer plaats kan innemen dan hij eigenlijk nodig heeft. Wat gebeurt er met die lege ruimte? Zoeken op de kreet "file slack" kan je helpen.
5. Free/"Unallocated" Space: Dit heb je over nadat er bestanden zijn gewist. Of zijn die bestanden echt weg? Leg uit hoe een bestand wordt verwijderd op een computer. Zoeken naar hulpmiddelen voor "secure delete" kan je helpen. Weten hoe je kunt zorgen dat een bestand echt gewist wordt is een prima manier om te leren waarom zulke hulpmiddelen nodig zijn.
6. Hash, ook bekend als een MD5 hash: leg uit wat deze hash is en waar hij voor wordt gebruikt.
7. BIOS: Dit staat voor "Basic Input/Output System". Wat is dit en waar op de computer is het opgeslagen?
8. Boot Sector: Dit werkt met partitie tabellen om je PC te helpen het te starten besturingssysteem te vinden.
Er zijn vele tools om te werken met partities, waarbij de meest bekende fdisk is.
Weten hoe die tools werken is je eerste stap in begrijpen van partities en de boot sector.
9. Cyclical Redundancy Check (CRC): Als je een "read error" boodschap krijgt van je harde schijf, betekent dat dat de CRC-controle op de data is mislukt. Zoek uit wat de CRC-controle is en wat hij doet.
10. File Signature: Vaak heeft een bestand een kleine handtekening (signature) van 6 bytes aan het begin van het bestand wat aangeeft om welk soort bestand het gaat. Door een bestand in een teksteditor zoals Notepad te openen is de makkelijkste manier om dit te zien. Open 3 bestanden van elke soort van de volgende type bestanden in een teksteditor: .jpg, . gif, .exe, .mp3. Wat was het eerste woord aan het begin van elk bestand?
11. RAM (Random-Access Memory): Dit is ook bekend als "geheugen" ("memory") en het is een tijdelijke plaats om informatie weg te schrijven en te lezen. Het is veel, veel sneller dan schrijven naar een harde schijf. De informatie in dit geheugen gaat verloren als de stroom

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

naar de computer uitvalt. Leg uit hoe RAM werkt. Er van uitgaande dat je computer 512 Mb RAM heeft, zoek informatie over een computer die meer RAM heeft.
12. Zoek uit hoe groot de grootste RAM-disk (een supersnelle harde schijf, geemuleerd in RAM) is. Hoeveel maal groter is die harde schijf dan de harde schijf in jouw computer?

8.2.2 Encryptie, decryptie en bestandsformaten

Veel bestanden die je zult tegenkomen zullen niet gelijk leesbaar zijn. Veel programma's hebben hun eigen bestandsindeling, terwijl anderen standaard formaten gebruiken – bijvoorbeeld een standaard formaat voor plaatjes - gif, jpeg, etc. Linux bevat een perfect hulpmiddel om te bepalen van welk type een bestand is. Het heeft de naam **file.**

Parameter voor het commando	Effect
-k	Stop niet bij het eerste resultaat, ga door.
-L	Volg symbolische links
-z	Probeer in gecomprimeerde bestanden te kijken.

Een voorbeeld van het gebruik van het file commando staat hieronder:

```
[simon@frodo file_example]$ ls
arp.c nwrap.pl
isestorm_DivX.avi oprp_may11_2004.txt
krb5-1.3.3 VisioEval.exe
krb5-1.3.3.tar Windows2003.vmx
krb5-1.3.3.tar.gz.asc
[simon@frodo file_example]$ file *
arp.c: ASCII C program text

isestorm_DivX.avi: RIFF (little-endian) data, AVI
krb5-1.3.3: directory
krb5-1.3.3.tar: POSIX tar archive
krb5-1.3.3.tar.gz.asc: PGP armored data
nwrap.pl: Paul Falstad's zsh script text
executable
oprp_may11_2004.txt: ASCII English text, with very long
lines, with CRLF line terminators
VisioEval.exe: MS-DOS executable (EXE), OS/2 or MS
Windows
Windows2003.vmx: a /usr/bin/vmware script text
executable
[simon@frodo file_example]$
```

Hiermee kun je een start maken met pogingen om het bestand te lezen. Linux bevat een aantal bestandconversie hulpmiddelen en je treft er nog meer op het internet, evenals bestandsviewers voor uiteenlopende formaten. Soms is er meer dan 1 stap nodig om in een positie te komen waarin je met de data aan de slag kunt – denk creatief!
Zo nu en dan zul je encrypted bestanden tegenkomen of bestanden die beschermd zijn met een wachtwoord.
De mate waarin je hier last van hebt verschilt, van encryptie die eenvoudig te kraken is tot spul waar de slimste geheime dienst hoofdpijn van zou krijgen. Er zijn diverse tools te vinden op internet die je kunt proberen om de encryptie op een bepaald bestand te breken. Het is

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

waardevol de omgeving van de computer die je onderzoekt te bestuderen. Mensen zijn niet erg goed in het onthouden van wachtwoorden, wellicht dat het ergens in de buurt is opgeschreven. Bekende keuzes voor een wachtwoord zijn ondermeer: huisdieren, familieleden, datums (trouwdag, geboortedatum), telefoonnummers, kentekenbewijzen en andere simpele combinaties (123456, abcdef, qwerty etc.). Mensen gebruiken vaak hetzelfde wachtwoord voor verschillende dingen, dus als het je lukt 1 wachtwoord te achterhalen, kun je dat mogelijk op meerdere omgevingen gebruiken.

Oefeningen:
Voor deze oefeningen leren we hoe we wachtwoorden moeten kraken. Alhowel het legaal is om je eigen wachtwoorden te kraken mocht je die vergeten zijn, is het in sommige landen niet legaal om te achterhalen hoe iets anders encrypted is, om te voorkomen dat dat andere materiaal gekraakt wordt.
DVD-films zijn encrypted om te voorkomen dat de film illegaal wordt gekopieerd. Dit is een prima voorbeeld van hoe je encryptie kunt gebruiken. Het is verboden om te bestuderen hoe die encryptie werkt. Dit brengt ons bij je eerste oefening:
1. Wat is "DeCSS" en welke relatie heeft het met DVD encryptie? Zoek naar "decss" om meer te leren.
2. Als je weet dat iets beveiligd is met een wachtwoord en je wilt toch bij de data van dat bestand, dan zul je dat wachtwoord moeten "kraken". Zoek informatie over het kraken van verschillende soorten wachtwoorden. Zoek daarbij naar het "kraken van XYZ-wachtwoorden" waarbij XYZ de volgende waardes heeft:
a. MD5
b. Adobe PDF
c. Excel
3. Als de encryptie te sterk is om gekraakt te worden, dan is het wellicht nodig een “dictionary attack” te doen (ook wel bekend als “brute force”). Zoek uit wat een dictionary attack is.

8.2.3 Een speld in een hooiberg vinden

Commercieel forensische software bevat krachtige zoekhulpmiddelen die je in staat stellen te zoeken naar vele combinaties en permutaties daarvan. Als je niet over die dure commerciele software kunt beschikken, zul je slimmer te werk moeten gaan. Linux bevat voldoende mogelijkheden om soortgelijke hulpmiddelen samen te stellen uit standaard utilities. De volgende tekst legt uit hoe je find, grep en strings, gebruikt en laat vervolgens zien hoe je met pipe de kracht van die commando's combineert.

8.2.3.1 find

```
find [path...][expression]
```

find wordt gebruikt om binnen het besturingsysteem bestanden te vinden die aan bepaalde criteria voldoen. Het is niet ontworpen om naar de inhoud van bestanden te kijken. Er moet een miljoen permutaties van zoekmogelijkheden zijn om naar een bestand te zoeken.

Oefening:
1. Lees de handleiding voor find. Zorg dat je een resultaat krijgt voor elk van de volgende uitdrukkingen in de tabel hieronder. (Hint: waar een getal is vermeld als argument, dan is dat als volgt te lezen: +n – voor
groter dan n; -n – voor minder dan n; n – voor precies n.)

Uitdrukking	Effect
-amin n	Bestand benaderd in de laatste n minuten

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

-anewer
-atime
-cnewer
-iname
-inum
-name
-regex
-size

8.2.3.2 grep

grep is een ongelooflijk krachtig hulpmiddel. Het wordt gebruikt om bepaalde regels te vinden binnen een bestand. Hiermee ben je in staat snel bestanden binnen een directory of bestandssysteem te vinden die bepaalde waardes bevatten. Het biedt ook de mogelijkheid te zoeken op normale uitdrukkingen. Er zijn zoekpatronen waarmee je kunt aangeven aan welke voorwaarden de zoekopdracht moet voldoen. Een voorbeeld: voor een kruiswoordpuzzel zoek je alle lettercombinaties in een woordenboek die starten met een "s" en eindigen op een "t".

```
grep ^s.*t$ /usr/share/dict/words
```

Oefening:
1. Lees de handleiding (man) voor grep.
2. Zoek bekende uitdrukkingen voor grep op op het Internet. Probeer een uitdrukking samen te stellen waarmee je zoekt op alle woorden met een lengte van vier letters en die een "a" bevatten.

8.2.3.3 strings

strings is nog een bruikbaar hulpmiddel. Dit commando doorzoekt elk willekeurig bestand op zoek naar voor mensen leesbare tekenreeksen (strings). Dit kan een grote hoeveelheid informatie opleveren over een bepaald bestand, vaak met informatie over de applicatie waarmee het bestand werd gemaakt, de auteur, de datum en tijd waarop het werd gemaakt en dergelijke.

Oefening:
1. Lees de handleiding (man) voor strings.

8.2.3.4 awk

awk is een programmeertaal die ontworpen is om te werken met strings. Het wordt gebruikt om informatie vanuit het ene commando te voeren aan een ander commando. Om bijvoorbeeld alleen de lopende programma's te zien bij uitvoering van het ps commando zou je het volgende commando gebruiken:

```
ps | awk '{print $4}'
```

Oefening:
1. Lees de handleiding (man) voor awk.

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

8.2.3.5 The Pipe "|"

Alle hiervoor genoemde hulpmiddelen zijn makkelijk te combineren met het Unix-commando "pipe". Hiervoor gebruiken we het "|" symbool. Hiermee kun je de uitkomst (output) van het ene commando via een pijp voeren aan een ander commando. Om alle bestanden van het mpg-type in de huidige directory te vinden, gebruiken we de volgende commando-combinatie:

```
ls | grep mpg
```

Oefening:

1. Vind, door gebruik te maken van de pipe, het ls commando en grep, alle bestanden in de huidige directory die deze maand zijn gemaakt.
2. Print, door gebruik te maken van het ps commando en awk, een lijst met alle lopende proces-namen.

8.2.4 Andere bronnen gebruiken

Er zijn vele andere interessante manieren om te onderzoeken hoe een computer is gebruikt. Bijna elke applicatie die wordt uitgevoerd laat op een of andere manier sporen na, naast de bestanden die het direct gebruikt of aanmaakt. Hieronder kunnen zich tijdelijke bestanden (temporary files) bevinden om bewerkingen uit te voeren, lijsten van recent gebruikte bestanden of de geschiedenis (history) van de webbrowser.

Oefening:

1. Wat is een browser cache? Vind de plek waar je browser zijn cache bewaart.
2. Wat zijn browser cookies? Vind de plek waar je webbrowser zijn cookies opslaat.
3. Zoek informatie over webbrowser cookies. Welke soorten cookies bestaan er en welke informatie bevatten ze?
4. Je computer gebruikt tijdelijke directories waar het standaard gebruikersbestanden opslaat. Die plek is vaak bekend onder de naam Application Data. Zoek de tijdelijke (temporary) directories die zich op je computer bevinden. Hoewel ze vaak de naam tmp of temp hebben zijn er meestal nog veel meer waar je geen weet van hebt. Een goede manier om zulke plaatsen te vinden is door het commando FIND uit te voeren en te zoeken naar bestanden die vandaag zijn aangemaakt. Verdwijnen die bestanden wanneer de computer herstart wordt?

8.3 Netwerk forensisch onderzoek

8.3.0 Introductie

Netwerk forensisch onderzoek wordt gebruikt om uit te vinden waar een computer zich bevindt en om te bewijzen of een bepaald bestand vanaf een bepaalde computer is verzonden. Alhoewel netwerk forensisch onderzoek erg ingewikkeld kan zijn, willen we hier toch wat basisprincipes behandelen die dagelijks bruikbaar zijn.

8.3.1 Firewall logbestanden

Wie maakt verbinding met me? De firewall is een hulpmiddel die de verbinding tussen twee punten in het netwerk kan versperren. Er bestaan verschillende soorten firewalls. Los van het type of taak van de firewall, het gaat vooral om de details in de logbestanden van de

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.

firewall. Alleen met die logbestanden kun je aanvalspatronen of misbruik van de firewall opmerken.

Oefeningen:
1. Bezoek de website http://www.dshield.org. Deze website gebruikt logbestanden van firewalls van over de hele wereld om patronen van aanvalspogingen te ontdekken. Dit helpt beveiligingsprofessionals vast te stellen of de netwerken die ze beveiligen kwetsbaar zijn voor zulke aanvalstechnieken voordat ze daadwerkelijk aangevallen worden. Lees de informatie op de website en leg uit hoe het taartdiagram van de wereld tot stand komt en wat hij betekent.
2. Lees op dezelfde website de informatie onder "Fight back" en de e-mails die ze ontvangen. Leg uit wat het doel hiervan is.

8.3.2 Mailheaders

E-mails bereiken je met informatie over alle computers die ze op de weg naar je inbox hebben gepasseerd. Die informatie wordt in de headers opgeslagen. Soms bevatten de headers nog meer informatie. Het is echter niet altijd even makkelijk om de headers te bekijken. De diverse email-programma's hebben allemaal hun eigen manier waarop je bij de headers komt.
De echte truc in het lezen van de headers is overigens weten dat je ze van achter naar voor moet lezen. Bovenaan de lijst sta jij. De reis gaat daarna via elke regel totdat je in de laatste regel de computer vindt vanwaar de mail naar jou is gestuurd.

Oefeningen:
1. Een goede bron die zich focussed op netwerk forensisch onderzoek gericht tegen SPAM is http://www.samspade.org. Bezoek SamSpade.org en ga naar het onderdeel met de naam "The Library".
Als je dat deel leest zou je moeten kunnen uitleggen hoe je e-mail headers moet lezen/intepreteren. Je moet ook het stuk even lezen over nagemaakte (“forged”) e-mail headers en misbruik van e-mail. Leg de verschillende manieren uit waarop je e-mail kunt gebruiken om kwaad te doen.
2. Bepaal hoe je de e-mail headers kunt bekijken in de e-mails die jij ontvangt. Zijn er bepaalde velden in die headers die je vreemd voorkomen? Zoek ze op. Je moet in staat zijn om uit te leggen wat elk veld in die header betekent.

Verder lezen

De volgende links zijn in het Engels.
http://www.honeynet.org/papers/forensics/
http://www.honeynet.org/misc/chall.html - Wat forensische oefeningen.
http://www.porcupine.org/forensics/ - De klassieken
http://www.computerforensics.net/
http://www.guidancesoftware.com/corporate/whitepapers/index.shtm#EFE
http://www.forensicfocus.com/
http://www.securityfocus.com/infocus/1679
http://www.linuxsecurity.com/feature_stories/feature_

WWW.ISECOM.ORG / WWW.OSSTMM.ORG / WWW.ISESTORM.ORG / WWW.HACKERHIGHSCHOOL.ORG
ALL CONTENTS COPYRIGHT 2000 - 2004, THE INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES (ISECOM).ALL RIGHTS RESERVED.
ANY INFORMATION CONTAINED WITHIN THIS DOCUMENT MAY NOT BE MODIFIED OR SOLD WITHOUT THE EXPRESS CONSENT OF THE AUTHOR.