Hacker Highschool
SECURITY AWARENESS FOR TEENS

Lektion 8
Digitale Forensik

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.

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.

Für das gesamte Material: © 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.

Inhaltsverzeichnis

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.

Mitwirkende

Pete Herzog, ISECOM

Chuck Truett, ISECOM

Marta Barceló, ISECOM

Kim Truett, ISECOM

Übersetzung

Georg Berky

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.

8.0 Einführung

Bei der Forensik handelt es sich um die Anwendung einer methodischen Untersuchungstechnik um eine Abfolge von Geschehnissen zu rekonstruieren. Die meisten Menschen sind aus Film und Fernsehen schon vertraut mit dem Konzept der Forensik, CSI (Crime Scene Investigation) ist eine der bekanntesten Sendungen dazu. Forensik wurde eine lange Zeit, und wahrscheinlich immer noch, mit der forensischen Pathologie verknüpft, bei der man herauszufinden versucht wie Menschen gestorben sind. Das erste mal wurde die Forensik 1248 in dem chinesischen Buch Hsi Duan Yu (Das Ausschließen von Fehlern) schriftlich erwähnt. Dieses Buch beschreibt wie man herausfindet ob jemand ertrunken ist oder stranguliert wurde. Die Digitale Forensik ist ein bisschen weniger chaotisch und ein bisschen weniger bekannt. Es ist die Kunst etwas nachzustellen das in einem digitalen Gerät passiert ist. In der Vergangenheit hat sich die digitale Forensik auf die Computer beschränkt, aber inzwischen hat sie sich auf alle digitalen Geräte ausgedehnt wie Handys, Digitale Kameras und sogar GPS Geräte. Sie wird benutzt um Mörder, Entführer, Betrüger, Mafia Bosse und noch eine Menge anderer unfreundlicher Menschen zu schnappen.

In dieser Lektion werden wir uns mit zwei Aspekten der Forensik befassen (alles Computer basiert Ich habe Angst es ist kein Handy Material hier) ?????

1. Was der Benutzer selbst auf seinem Computer gemacht hat

Folgendes wird dabei behandelt:

- Die Wiederherstellung von gelöschten Dateien.
- Grundlegende Entschlüsselung.
- Die Suche nach bestimmten Dateiarten.
- Die Suche nach bestimmten Sätzen.
- Und das Ansehen von interessanten Bereichen auf dem Computer.

2. Was ein entfernter Benutzer auf dem Computer eines anderen getan hat.

Dabei wird folgendes behandelt:

- Das lesen der Logdateien.
- Das rekonstruieren von Aktivitäten.
- Das Nachverfolgen der Herkunft.

Diese Lektion legt den Fokus auf die Werkzeuge die unter Linux verfügbar sind. Es gibt auch Werkzeuge die unter Windows verfügbar sind, genauso wie es Hardware und Software gibt um forensische Analysen durchzuführen, aber mit den Möglichkeiten die Linux zum aufnehmen und nachvollziehen für eine große Zahl von wechselnden Betriebs- und Dateisystemen bietet, ist es die ideale Umgebung für die meisten forensischen Tätigkeiten.

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.

8.1 Forensische Prinzipien

8.1.0 Einführung

Es gibt ein Zahl von grundlegenden Prinzipien die unerlässlich sind egal ob man einen Computer oder einen Körper untersucht. Dieser Abschnitt ist eine kurze Zusammenfassung dieser Prinzipien.

8.1.1 Vermeide Verunreinigungen

Im Fernseher siehst Du das forensische Untersuchungspersonal in weißen Anzügen und mit Handschuhen bekleidet, wie sie alle Beweise nur mit Pinzetten anfassen und sie dann in versiegelte Plastikbeutel packen. Das passiert um „Verunreinigungen" zu vermeiden. Diese Verunreinigungen können einen Beweis verderben, zum Beispiel wenn sich auf dem Griff eines Messers Fingerabdrücke befinden und jemand hebt es auf und fasst es an (denke an die Krimis die gesehen hast, und in welche Schwierigkeiten die Unschuldigen kommen wenn deren Fingerabdrücke auf der Tatwaffe gefunden werden.).

8.1.2 Handle methodisch

Was immer Du auch tust, wenn Du einmal vor Gericht stehst, musst Du Dich für alle Aktivitäten die Du getan hast verantworten. Wenn Du in einer wissenschaftlichen und methodischen Art und Weise wirkst, und Dir dabei sorgfältige Notizen über das was Du tust und wie Du es tust machst, wird die Rechtfertigung um einiges leichter werden. Zudem erlaubt es jemand anderem Deine Schritte nachzuvollziehen und zu überprüfen das Du keinen Fehler gemacht hast, was den Wert Deiner Beweise nicht in Zweifel zieht.

8.1.3 Beweiskette

Du musst in der Forensik eine Struktur einhalten die sich „Beweiskette" nennt. Das heißt das Du zu jedem Zeitpunkt von der Aufnahme der Beweise bis zu deren letztendlichen Präsentation vor Gericht, nachweisen kannst wer darauf Zugriff hatte und wo es war. Das schließt aus das sich jemand daran zu schaffen gemacht, oder sie in irgendeiner Art verfälscht hat.

8.1.4 Schlussfolgerung

Behalte diese Dinge gut in Erinnerung, und selbst wenn Du Deine Arbeit nicht vor Gericht bringen musst, wirst Du doch Deine Fähigkeiten als forensischer Untersucher steigern können.

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 Alleinstehende Forensik

8.2.0 Einführung

Dieser Abschnitt behandelt die forensische Untersuchung einer einzelnen Maschine. Aus Mangel an einem besseren Begriff nennen wir es „Alleinstehende Forensik". Das ist vermutlich der bekannteste Teil der Computer Forensik, dessen Hauptaufgabe darin besteht herauszufinden was geschehen ist mit Hilfe eines speziellen Computers. Der forensische Untersucher könnte nach Beweisen für Betrug suchen, wie Finanztabellen, Beweise über Kommunikation mit jemand anderes, E-Mails oder ein Adressbuch oder Beweise von spezieller Natur wie Pornografische Bilder.

8.2.1 Grundlagen zu Festplatten und Speichermedien

Es sind mehrere Komponenten die einen durchschnittlichen Computer ausmachen. Da ist der Prozessor, Speicher, Grafikkarte, CD Laufwerk und noch einiges mehr. Eine der wichtigsten Komponenten ist die Festplatte. Dort ist die Mehrheit der Informationen die ein Computer zum Funktionieren benötigt gespeichert. Das Betriebssystem wie Windows oder Linux sind hier abgelegt zusammen mit Benutzeranwendungen wie Textverarbeitung und Spielen. Dort sind auch eine erhebliche Menge an Daten gespeichert, entweder absichtlich durch das abspeichern einer Datei oder zufällig durch die Nutzung von temporären Dateien und Cache Speicher. Das erlaubt einem forensischen Untersucher Aktivitäten zu rekonstruieren die ein Computerbenutzer auf seinem Computer durchgeführt hat, auf welche Dateien zugegriffen wurde und noch viel, viel mehr.

Es gibt mehrere Ebenen auf denen Du eine Festplatte untersuchen kannst. Für den Zweck dieser Übung, schauen wir uns nur die Dateisystemebene an. Man sollte aber anmerken das Profis sehr wohl in der Lage sind Festplatten in einem höherem Detaillierungsgrad zu untersuchen um nachzuweisen was auf Ihnen abgelegt wurde, sogar wenn dies mehrere Male überschrieben wurde.

Das Dateisystem ist die Computer Umsetzung eines Aktenschranks. Es beinhaltet Schubladen (Partitionen), Akten (Verzeichnisse) und einzelne Papierstücke (Dateien). Dateien und Verzeichnisse können versteckt sein, wenngleich dies auch nur oberflächlich ist und leicht überwunden werden kann.

Indem Du Dich durch die folgenden Übungen arbeitest, solltest Du ein weit besseres Verständnis für die Grundlagen von Plattenspeicher bekommen.

Übungen:
Suche nach Informationen für jeden der folgenden Begriffe zu Speichermedien und bringe in Erfahrung wie Sie funktionieren. Das Verstehen der grundsätzlichen Funktionsweise von Geräten ist Dein erster Schritt in Richtung Forensik.

1. Magnetische-/Fest-/Physikalische Platte: Das ist dort wo Dein Computer Dateien speichert. Erkläre wie Magnetismus auf einer Festplatte genutzt wird.
2. Spur: Was wird „Spuren auf einer Festplatte" genannt?
3. Sektoren: Das ist ein feststehender Platz in den Daten passen. Erkläre wie.

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.

4. Cluster/Speicherverteilungseinheit: Erkläre warum eine Datei, wenn sie auf die Festplatte geschrieben wird, mehr Platz einnimmt als sie eigentlich benötigt. Was passiert mit dem freien Platz? Der Begriff „file slack“ sollte Dir dabei helfen.
5. Freier/nicht verteilter Platz: Das ist das was Du zurückgelassen hast wenn Dateien gelöscht wurden. Sind die gelöschten Dateien wirklich weg? Erkläre wie eine Datei auf dem Computer gelöscht wird. Die Suche nach Werkzeugen zum sicheren Löschen könnten Dir dabei helfen. Zu wissen wie man sicher eine Datei löscht, so das sie wirklich weg ist, ist ein guter Weg zu lernen warum man solche Werkzeuge benötigt.
6. Prüfsumme (Hash), auch bekannt als MD5 Prüfsumme: Erkläre was eine Prüfsumme ist und für was man sie benötigt.
7. BIOS: Steht für „Basic Input/Output System“. Was ist das und wo ist es gespeichert auf einem PC?
8. Boot Sektor: Er arbeitet mit Partitionstabellen welche Deinem PC helfen das Betriebssystem zu finden und zu starten. Es gibt viele Werkzeuge um Partitionen zu erstellen, wie das Standardwerkzeug welches fdisk genannt wird. Zu wissen wie diese Werkzeuge arbeiten ist der erste Schlüssel zum Verständnis von Partitionen und boot Sektoren.
9. Cyclical Redundancy Check (CRC): Wenn Du eine Lesefehler-Nachricht von Deiner Festplatte bekommst, dann heißt das Deine Daten haben den CRC Check nicht bestanden. Finde heraus was ein CRC Check ist und was er tut.
10. Datei Signatur: Häufig haben Dateien eine kleine 6-byte Signatur am Anfang welche identifiziert um welche Art von Datei es sich handelt. Die Datei mit einem Texteditor zu öffnen ist der einfachste Weg um dies herauszufinden. Öffne drei Dateien der folgenden Dateitypen in einem Texteditor: .jpg, .gif, .exe, .mp3. Welches Wort siehst Du als erstes am Anfang jeder Datei?
11. RAM (Random Access Memory): Der RAM ist auch als Hauptspeicher bekannt und ist ein temporärer Speicher zum Lesen und Schreiben von Informationen. Das schreiben in den RAM ist sehr viel schneller als das schreiben auf die Festplatte. Aber die Informationen im RAM sind verloren sobald die Stromzufuhr zum Computer unterbrochen ist. Erläutere wie der RAM funktioniert. Dein Computer wird irgendetwas zwischen 64 und 512 MB an RAM haben. Suche nach Informationen zu Computern die mehr an RAM haben als oben genannt.
12. Zur Zeit hat die größte RAM Disk (eine superschnelle Festplatte die im RAM emuliert wird) eine Kapazität von 2.5 TB (Terrabyte). Um wie viel größer als Dein PC ist das?

8.2.2 Entschlüsselung, Verschlüsselung und Dateiformate

Eine Menge Dateien mit denen Du zu tun hast werden nicht sofort lesbar sein. Eine Menge Programme haben Ihr eigenes proprietäres Dateiformat, während andere ein Standardformat benutzen, zum Beispiel die Standard Formate für Bilder wie gif, jpeg, etc. Linux bietet dazu ein hervorragendes Werkzeug welches Dir hilft herauszufinden um welchen Typ Datei es sich handelt. Das Werkzeug nennt sich file.

Befehlszeilenschalter	Effekt
-k	Bleibt nicht bei der ersten Übereinstimmung stehen, sondern sucht weiter.
-L	Folgt den symbolischen Links.
-z	Versucht in die gepackte Datei zu sehen.

Nachfolgend findest Du ein Beispiel für den Befehl file.

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.

```
[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]$
```

Von hier aus kannst Du nun einige Versuche machen bestimmte Arten von Dateien zu lesen. Es gibt eine Anzahl an Dateikonvertierungswerkzeugen welche standardmäßig unter Linux verfügbar sind, und sogar noch mehr die über das Internet verfügbar sind, dazu gibt es noch eine Menge an Dateibetrachtern für unterschiedlichste Formate. Manchmal benötigt man mehr als einen Schritt um einen Punkt zu kommen an dem man wirklich mit den Daten arbeiten kann, versuche nach allen Seiten zu denken!

Gelegentlich wirst Du mit Dateien in Berührung kommen die verschlüsselt oder Passwort geschützt sind. Die dahinterliegende Schwierigkeit variiert dabei von Verschlüsselung die einfach geknackt werden kann bis zu Verschlüsselung die selbst der NSA Kopfschmerzen bereiten würde. Hier gibt es wieder eine Anzahl an Werkzeugen im Internet welche Du nutzen kannst um die Verschlüsselung einer Datei zu knacken. Es macht sich auch bezahlt wenn man die Umgebung des Computers mit an dem man arbeitet untersucht. Einige geläufige Wahlen für Passwörter enthalten auch: Haustiere, Verwandte, Datumsangaben (Hochzeit, Geburtsdatum etc.), Telefonnummern, Autokennzeichen und andere leicht zu merkende Kombinationen (123456, abcdef, qwertz etc.). Personen streuben sich auch mehr als ein, zwei Passwörter zu benutzen, wenn Du also ein Passwort für eine bestimmte Datei oder Anwendung rückkonstruiert hast, dann versuche das Passwort auch bei anderen Dateien und Anwendungen zu nutzen. Die Wahrscheinlichkeit ist hoch das es das gleiche ist.

Übungen:

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.

In dieser Übung werden wir etwas über das cracken von Passwörtern lernen. Während es legal ist Dein eigenes Passwort zu cracken falls Du es einmal vergessen hast, ist es in manchen Ländern nicht legal herauszufinden wie ein Passwort von jemand anderem verschlüsselt ist.....

Filme auf DVD sind verschlüsselt um Sie vor Raubkopierern zu schützen welche Sie dann illegal verkaufen. Und weil es eine hervorragende methode zum verschlüsseln ist, ist es illegal nach der Wirkungsweise der Verschlüsselung zu forschen. Das führt uns zur ersten

Übungen:

1. Was ist „DeCSS“ und welche Verbindung gibt es zur DVD Verschlüsselung? Suche nach „decss“ um mehr darüber herauszufinden.
2. Zu wissen das etwas passwortgeschützt ist heißt das man lernen muss wie man die Datei öffnen kann. Dies ist bekannt als „cracken“ des Passworts. Finde Information wie man unterschiedliche Arten von Passwörtern crackt. Um Informationen zu finden, suche nach „cracking XYZ passwords“ wobei XYZ für die Art Passwort steht nach der Du suchen möchtest. Tu das für die folgenden Arten von Passwörter.
    a. MD5
    b. Adobe PDF
    c. Excel
3. Ist die Verschlüsselungsmethode zu stark um gebrochen zu werden, kann es nötig sein eine sogenannte „Wörterbuch Attacke“ (manchmal auch als „brute force“ bezeichnet) durchzuführen. Finde heraus was eine Wörterbuch Attacke ist.

8.2.3 Finde die Nadel im Heuhaufen

Kommerzielle forensische Software beinhaltet eine Menge mächtiger Suchwerkzeuge die Dir erlauben mit Kombinationen und Permutationen von Faktoren zu suchen. Ohne diese teuren kommerziellen Werkzeuge musst Du ein wenig mehr kreativ sein. Linux erlaubt Dir dabei mit einer vorhandenen Anzahl an Werkzeugen Dir selbst die Dinge zusammenzustellen die Du benötigst. Der nachfolgende Text beschreibt den Gebrauch der Befehle find, grep und strings sowie auch die Kombination der Befehle durch die pipe Funktion.

8.2.3.1 Find

Find [pfad....][Entsprechung]

Find wird dazu benutzt Dateien zu finden welche innerhalb des Betriebssystems bestimmten Kriterien entsprechen. File ist nicht dazu bestimmt innerhalb der Datei zu suchen. Es gibt wahrscheinlich eine Million Permutationen von Entsprechungen die kombiniert werden können um nach einer Datei zu suchen.

Übung:

1. Lese die Manual Seite für find. Ergänze den Effekt für jede Entsprechung in der nachfolgenden Tabelle. (Tip: Dort wo eine Zahl als Argument angegeben ist, kann das ganze in folgender Weise spezifiziert werden: +n heißt größer als n; -n heißt kleiner als n; n heißt genau n.)

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.

Entsprechung	Effekt
-amin n	Auf die Datei wurde n Minuten zuvor zugegriffen
-anewer	
-atime	
-cnewer	
-iname	
-inum	
-name	
-regex	
-size	
-type	
-user	

8.2.3.2 Grep

Grep ist immens mächtiges Werkzeug. Es wird dazu benutzt bestimmte Zeilen innerhalb einer Datei zu finden. Es erlaubt Dir Dateien zu finden welche bestimmte Dinge beinhalten innerhalb eines Verzeichnisses oder innerhalb des Dateisystems. Es erlaubt Dir ebenfalls mit regulären Entsprechungen zu arbeiten. Dazu gibt es Suchmuster die Dir erlauben Kriterien festzulegen welche Deiner Suche entsprechen müssen. Zum Beispiel: finde alle Zeichenketten im Wörterbuch die mit „s“ beginnen und mit „t“ enden als Hilfe für ein Kreuzworträtsel.

Grep ^s.*t$ /usr/share/dict/words

Übungen:

1. lese die Manual Seite für grep.
2. Schaue nach regulären Entsprechungen für grep im Internet. Versuche eine regüläre Entsprechung zusammenstellen welche nach allen Wörtern schaut die vier Buchstaben lang ist und ein „a“ beinhaltet.

8.2.3.3 Strings

Strings ist ein weiteres gebräuchliches Werkzeug. Strings durchsucht eine Datei nach jeder Art Zeichenkette welche für Menschen lesbar ist. Dabei kann es eine Menge an Informationen über eine bestimmte Datei zurückgeben, wie Informationen über die Anwendung welche die Datei erzeugt hat, den Autor, die wirkliche Zeit der Erstellung und vieles mehr.

Übung:

1. Lese die Manual Seite für strings.

8.2.3.4 Awk

Awk ist eine Programmiersprache welche für die Arbeit mit Zeichenketten konstruiert wurde. Es wird benutzt um Informationen aus einem Befehl zu extrahieren und diese

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.

einem anderen zu übergeben. Um zum Beispiel nur die laufenden Programme aus dem ps Befehl zu bekommen, kannst Du die folgende Befehlskette benutzen:

ps | awk '{print $4}'

Übung:

1. Lese die Manual Seite für awk.

8.2.3.5 The Pipe „|"

Alle der oben genannten Werkzeuge können ganz einfach mit dem UNIX „pipe" Befehl miteinander kombiniert werden. Dies wird mit dem „|" Symbol angezeigt. Es erlaubt Dir die Ausgabe eines Befehls zu nehmen und über eine pipe in einen anderen Befehl zu geben. Um alle mpg Dateien im gegenwärtigen Verzeichnis zu finden kannst Du die folgende Befehlskette benutzen:

ls | grep mpg

Übungen:

1. Benutze die pipe, den ls Befehl und grep, um alle Dateien zu finden welche dieses Monat erstellt wurden.
2. Benutze den ps Befehl und awk um eine Liste aller laufenden Prozessnamen auszugeben.

8.2.4 Die Benutzung von anderen Quellen

Es gibt noch viele andere interessante Wege wie man einen Computer hinsichtlich seiner Nutzung untersuchen kann. Nahezu jede Anwendung die auf einem Computer läuft zeichnet, neben den Dateien in die direkt geschrieben wird und den Dateien die sie ausgibt, weitere Daten auf. Das können temporäre Dateien zur Verarbeitung, Listen von zuletzt aufgerufenen Dateien oder die Historie eines Web-browsers sein.

Übungen:

1. Was ist ein browser cache? Finde den Ort an dem Dein web-browser seinen cache ablegt.
2. Was sind browser cookies? Finde den Ort an dem Dein web-browser seine cookies ablegt.
3. Suche nach Informationen über web-browser cookies. Welche Art von cookies sind möglich, und welche Art von Informationen sind darin abgespeichert?
4. Dein Computer nutzt temporäre Verzeichnisse in die er per Vorgabe Dateien für den Benutzer schreibt. Dies sind als Anwendungsdaten bekannt. Finde die temporären Verzeichnisse die Du auf Deinem Computer zur Verfügung hast. Während sie meistens tmp oder temp genannt werden, gibt es sehr oft um einige mehr von denen Du nichts weißt. Versuche dazu den Befehl FIND zu benutzen um Dateien mit dem aktuellen Datum zu finden und Du wirst eine Menge temporärer Dateien entdecken. Verschwinden diese Dateien wenn Du Deinen Computer neu startest?

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.

8.3 Netzwerk Forensik

8.3.0 Einführung

Netzwerk Forensik wird dazu benutzt um herauszufinden wo sich ein Computer befindet und ob eine bestimmte Datei von einem bestimmten Computer gesendet wurde. Obwohl Netzwerk Forensik sehr kompliziert sein kann, wollen wir doch einige Grundlagen besprechen welche für den täglichen Gebrauch nützlich sein können.

8.3.1 Firewall Logs

Wer verbindet sich zu mir? Die Firewall ist ein Dienstprogramm welches Verbindungen zwischen zwei Punkten in einem Netzwerk unterbinden kann. Es gibt mehrere Arten von Firewalls. Ohne Bezug auf die Art und die Arbeit der Firewall zu nehmen, sind es doch die Firewall Logs welche Dir Auskunft über die Details geben. Nur mit Benutzung der Logs kannst Du Angriffsmuster und Missbrauch Deiner Firewall erkennen.

Übungen:

1. Besuche die Webseite **http://www.dshield.org**. Diese Webseite verarbeitet Firewall Logs aus der ganzen Welt um Muster für Netzwerk Angriffe zu finden. Dies hilft Sicherheitsexperten das Netzwerk welches Sie beschützen auf Sicherheitslücken zu überprüfen und vor allem auf diese bestimmten Attacken bevor sie passieren. Lies Dich durch die Webseite und erläutere wie das Tortendiagramm der Welt zustande kommt und was es aussagt.
2. Auf der selben Webseite lies den „Fight back“ Abschnitt und die Resonanz Mails die sie bekommen. Erläutere den Zweck.

8.3.2 Mail Headers

E-mails kommen mit Informationen von jedem Computer, welcher durchlaufen wird bis die Mail bei dir angekommen ist, an. Diese Informationen befinden sich im Nachrichtenkopf. Und manchmal ist sogar noch mehr Information im Nachrichtenkopf. Das ansehen der Nachrichtenköpfe ist aber nicht immer so einfach. Verschiedenartige Mail Programme haben auch unterschiedliche Wege um die Nachrichtenköpfe anzusehen. Der wirkliche Trick Nachrichtenköpfe zu lesen ist zu wissen das der Verlauf immer rückwärts ist. Am Anfang der Liste bist immer Du selbst. Dann wird der Weg aufgezeigt bis in der letzten Zeile der Computer oder das Netzwerk aufgeführt ist von dem die E-mail verschickt wurde.

Übungen:

1. Ein guter Fundort welcher sich auf Netzwerk Forensik im Bereich SPAM Bekämfung fokussiert hat ist **http://www.samspade.org**. Besuche samspade.org und schau in den Abschnitt der „The Library“ genannt wird. Mithilfe dieses Abschnitts solltest Du in der Lage sein zu erklären wie man einen E-Mail Nachrichtenkopf liest. Du solltest ebenfalls etwas über das Thema gefälschte E-Mail Nachrichtenköpfe und E-Mail Missbrauch lesen. Erkläre die unterschiedlichen Wege wie man E-Mail nutzen kann um Schaden zu zufügen.
2. Stelle fest wie man in die E-Mail Nachrichtenköpfe, der E-Mails welche Du empfangen hast, sehen kann. Sind dort bestimmte Felder in den Nachrichtenköpfen die Dir fremd erscheinen? Schau nach ob Du etwas darüber findest. Du solltest in der Lage sein zu erklären was jedes Feld im Nachrichtenkopf bedeutet.

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.

Weitere Informationen:

http://www.honeynet.org/papers/forensics/
http://www.honeynet.org/misc/chall.html - Some forensic Exercises.
http://www.porcupine.org/forensics/ - The classics
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_story-139.html
http://www.linuxsecurity.com/feature_stories/feature_story-140.html
http://www.securityfocus.com/incidents
http://staff.washington.edu/dittrich/talks/blackhat/blackhat/forensics.html
http://www.openforensics.org/
http://fire.dmzs.com/
http://www.sleuthkit.org/
http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm

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.