Hacker Highschool
SECURITY AWARENESS FOR TEENS

LEKTION 2
GRUNDLEGENDE BEFEHLE IN LINUX UND WINDOWS

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

Daniel Fernández Bleda, Internet Security Auditors

Jairo Hernández, La Salle URL Barcelona

Jaume Abella, La Salle URL Barcelona - ISECOM

Kim Truett, ISECOM

Pete Herzog, ISECOM

Marta Barceló, ISECOM

ÜBERSETZUNG

Georg Berky

Karl Pausch

2.1.Einführung und Ziele dieser Lektion

Diese Lektion macht dich mit den wichtigsten Tools für der Betriebssysteme Windows und Linux vertraut, um später damit die Übungen lösen zu können.

Am Ende diese Lektion solltest du die folgenden Windows- und Linuxbefehle beherrschen:

- grundlegende Windows- und Linuxbefehle
- die wichtigsten Netzwerktools:
  - ping
  - tracert
  - netstat
  - ipconfig
  - route

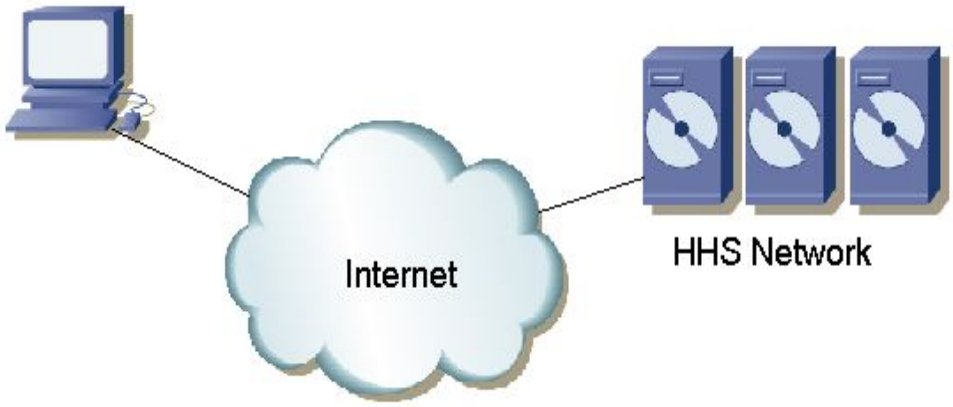
2.2. Anforderungen und Aufbau

2.2.1 Anforderungen

Für diese Lektion wirdst du folgendes benötigen:

- einen PC mit Windows 98/ME/2000/NT/XP/2003
- einen PC mit SuSE/Debian/Knoppix Linux
- Zugriff auf das Internet

2.2.2 Deine Arbeitsumgebung



So sieht die Umgebung aus, in der du arbeiten wirst. Auf der einen Seite steht dein Computer mit Zugriff auf das Internet, auf der anderen befindet sich das ISECOM Hackerhighschool Netzwerk, auf das du über das Internet zugreifen kannst. Mit dem HHS Netzwerk wirst du die meisten deiner Tests durchführen.

Der Zugriff auf das ISECOM Netzwerk ist beschränkt. Dein Lehrer muss erst unseren Netzwerkadministrator Kontaktieren, um den Zugriff freizuschalten. Details finden sich auf http://www.hackerhighschool.org.

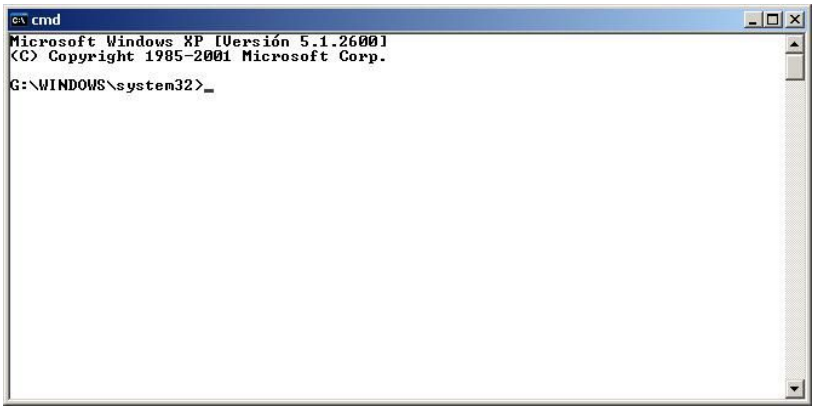
2.3.Systemoperationen unter Windows

Die meisten Tools, die wir für die Erforschung von Netzwerken brauchen, sind Teil des Windows Betriebssystems. Deswegen zeigen wir dir zuerst, wie du die Eingabeaufforderung ("shell", "DOS Fenster") in Windows öffnest.

2.3.1 Wie man ein DOS Fenster öffnet

Um die folgenden Befehle ausführen zu können, musst du zuallererst ein DOS-Fenster (auch Eingabeaufforderung genannt) öffnen. Das funktioniert bei allen Windowsversionen folgendermaßen:

1. Klicke auf Start
2. Klicke auf "Ausführen"
3. Unter Windows 95/98/ME: gib **"command"** ein
   Bei allen anderen Windowsversionen: gib **"cmd"** ein.
   Klicke anschliessend auf OK oder drücke Enter.
4. Ein Fenster, das etwa so aussieht erscheint auf deinem Bildschirm:



5. Jetzt kannst du die Befehle aus der Liste unten eingeben und ausführen

2.3.2 Befehle und Tools (Windows)

Befehle

date	Anzeigen und Ändern der Datums
time	Anzeigen und Ändern der Uhrzeit
ver	Zeigt dir die MS-DOS Version an, die dein System verwendet
dir	Zeigt dir den Inhalt eines Verzeichnisses (Ordner, directory) an
cls	Löscht alles was in dem Fenster angezeigt worden ist
mkdir / md *verzeichnis*	Erstellt ein neues Verzeichnis mit dem angegebenen Namen, z. B. md tools

chdir, cd *verzeichnis*	Wechsle in das angegebene Verzeichnis, z.B. cd tools
rmdir, rd *verzeichnis*	Löscht das Verzeichnis mit dem angegebenen Namen, z.B. rd tools
tree *verzeichnis*	Zeigt die Verzeichnisstruktur eines Ordners an, z.B. tree c:\tools
chkdisk	Überprüft deine Festplatte und zeigt die Ergebnisse der Prüfung an
mem	Zeigt dir an, wieviel Speicher vom System gerade verwendet wird, und wieviel noch frei ist
rename, ren *quelle ziel*	Benennt Dateien um, z.B. ren referat.txt tagebuch.txt
copy *quelle ziel*	Erstellt eine Kopie der Datei *quelle*. Die neue Datei heisst *ziel*. Beispiel: copy tagebuch.txt tagebuch_sicherung.txt
move *quelle ziel*	Verschiebt eine Date oder ändere den Namen von Dateien und Verzeichnissen, z.B. move c:\tools c:\tmp
type *datei*	Zeigt dir den Inhalt der Datei im DOS-Fenster an, z.B. type tagebuch.txt
more *datei*	Zeigt dir den Inahlt der Datei Bildschirm für Bildschirm an, z.B. more tagebuch.txt
delete, del *datei*	Löscht eine oder mehrere Dateien, z.B. del tagebuch.txt

Die kursiv gedruckten Worte musst du nicht wörtlich eingeben, sie dienen als Platzhalter für einen Datei- oder Verzeichnisnamen. Sind mehrere Befehle aufgezählt, z.B. **delete** und **del**, dann bedeutet dies, dass es sich um zwei identische Kommandos handelt.

Tools

ping *host*	Stellt fest, ob die Maschine namens host erreichbar ist. Dieser Befehl schickt über das ICMP Protokoll "Paktete" an einen anderen Computer, um festzustellen, ob dieser über das Netzwerk erreichbar ist. Danach zeigt es eine Statistik der gesendeten und beantworteten Pakete an, sowie die Zeit, die der andere Rechner zum Antworten gebraucht hat. Den Namen des anderen Computers kannst du als URL oder IP-Adresse angeben, z.B. ping www.google.com ping 193.145.85.2 Einige Optionen von ping: /n zahl: Sendet nur zahl pakete /t : Sendet Pakte, bis du Strg-C drückst Mehr Optionen kannst du mit ping /h herausfinden.

tracert host	Zeigt dir die Route an, die Pakete nehmen, wenn sie an den Rechner *host* geschickt werden. tracert ist eine Abkürzung für "trace route" ("verfolge die Route"). Mit diesem Tool kannst du die Route, die deine Pakete von deinem Rechner zur Zielmaschine nehme, verfolgen. Das Programm zeigt dir auch die Zeit für jeden einzelnen Schritt an. Die maximale Anzahl an Schritten ("hops", "jumps"), die tracert dir anzeigt, ist 30. Beispiele: tracert www.google.com tracert 193.145.85.2 Optionen: /h zahl : überprüfe maximal *zahl* jumps /d : zeige nur die IP-Adressen der Rechner Mehr Optionen erfährst du, wenn du nur tracert eingibst
ipconfig	Zeigt dir Informationen über aktive Netzwerkinterfaces (Ethernet, PPP usw.) an Optionen: /all : Zeige mehr Details /renew *name* : Startet die automatische Konfiguration von *name*, wenn DHCP verwendet wird. /release *name* : Deaktiviert alle bestehenden Verbindungen von *name*, wenn DHCP verwendet wird. Mehr Optionen erfährst du, wenn du ipconfig /? eingibst.
route print	Zeigt dir die routing table ("Routingtabelle") an. Das Kommando route dient dazu, der Routingtabelle statische Einträge hinzuzufügen, diese zu löschen, oder einfach nur dazu, Informationen über die Einträge anzuzeigen. Einige Optionen: print : zeigt dir die Einträge an delete : löscht einen Eintrag add : fügt einen Eintrag hinzu Mehr Optionen findest du mit route /?

netstat	Zeigt dir Informationen über den Netzwerkstatus und bestehende Verbindungen mit anderen Computern an. Einige Optionen: /a : Zeigt alle Verbindungen und offene Ports an /n : Zeigt die Informationen in numerischer Form an (z.B. IP-Adressen anstelle von URLS) /e zeigt Informationen über das Ethernet an Beispiel: netstat /a /n Mehr Optionen findest du mit netstat /?

Wenn du mehr über einen Befehl herausfinden willst, kannst du ***befehl* /h**, befehl **/?** oder **help *befehl*** im DOS-Fenster eingeben. Bei netstat kannst du **netstat /h, netstat /?** und **help netstat.**

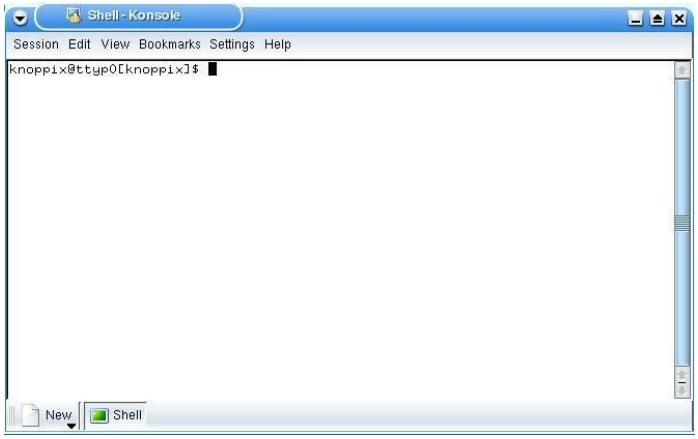
2.4. Systemoperationen (Linux)

Genauso wie in Windows wirst du unter Linux den Großteil der Befehle, die du hier lernst, von einem Fenster mit einem Konsolenemulator aus aufrufen. Als nächstes zeigen wir dir, wie du ein solches Fenster startest.

2.4.1 Wie man ein Konsolenfenster aufruft

Um die Befehle unten auszuführen, benötigen wir zuerst ein Konsolenfenster:

1. Klicke auf den "Programm starten" (oder "start application") Button
2. Klicke auf "Programm ausführen" (oder "run command")
3. Gib **konsole** ein
4. Ein Fenster, das etwa so wie dieses aussieht öffnet sich



5. - Jetzt kannst du die Befehle und Tools unten eingeben und verwenden

2.4.2 Befehle und Tools (Linux)

Befehle

pwd	Zeigt dir den Namen des aktuellen Verzeichnisses an
hostname	Zeigt dir den Namen des Computers an, auf dem du gerade arbeitest
finger *benutzer*	Zeigt dir Informationen über den Benutzer *benutzer* an
ls	Zeigt dir den Inhalt des aktuellen Verzeichnisses an
cd *verzeichnis*	Wechselt in das angegebene Verzeichnis *verzeichnis*. Wird kein Verzeichnis angegeben, wechselt man damit ins home Verzeichnis (das persönliche Verzeichnis eines Benutzers) Beispiele: $> cd Wechselt nach /home/*benutzername*, wobei benutzername der Name ist, unter dem du dich angemeldet hast (probiere einmal den Befehl **whoami** aus) $> cd - Wechselt ins das Verzeichnis, das du zuletzt besucht hast. $> cd /tmp Wechselt ins Verzeichnis tmp
cp *quelle ziel*	Erstellt eine Kopie der Datei *quelle* mit dem Namen *ziel,* z.B. cp / etc/passwd /tmp
rm *datei*	Löscht die Datei *datei*, z.B. rm meinedatei.txt
mv *quelle ziel*	Verschiebt die Datei *quelle* nach *ziel* oder bennennt sie um, z.B. mv altedatei neuedatei
mkdir *verzeichnis*	Erstellt ein neues Verzeichnis namens *verzeichnis*.
rmdir *verzeichnis*	Löscht das Verzeichnis *verzeichnis*, z.B. rmdir meinordner
find / -name *dateiname*	Durchsucht / und alle Unterordner nach Dateien mit dem namen *dateiname*, z.B. find / -name meinedatei
echo *string*	Schreibt *string* (Strings sind Zeichenketten) auf das Standardausgabegerät ("stdout"), also auf deinen Bildschirm.
kommando > *dateiname*	Führt *kommando* aus und leitet die normale Ausgabe auf den Bildschirm in die Datei *dateiname* um, z.B. ls > verzeichnisinhalt.txt
kommando >> *dateiname*	Führt *kommando* aus und leitet die normale Ausgabe auf den Bildschirm ans Ende der Datei *dateiname* um, z.B. ls >> verzeichnisinhalt.txt
man *kommando*	Zeigt dir die Anleitung zum Befehl *kommando* an. Dies ist einer der wichtigsten und wertvollsten Linuxbefehle. Beispiel: man ls

Die kursivgedruckten Worte sind wie oben nur als Platzhalter gedacht. Ersetze sie durch passende Werte.

Benötigst du weitere Hilfe zu einem Befehl, gib ***befehl* --help** ein oder verwnde **man *befehl***. Willst du etwa mehr über den Befehl ls wissen, dann kannst du **ls --help** oder **man ls** eingeben.

Tools
(Details finden sich im Abschnitt über Windows. Optionen werden unter Linux mit - statt / angegeben)

ping *host*	Verify the contact with the machine "host" Example: ping www.google.com
traceroute *host*	Show the route that the packets follow to reach the machine "host". Example: tracert www.google.com
ifconfig	Display information on the active interfaces (ethernet, ppp, etc.)
route	Display the routing table
netstat	Display information on the status of the network Example: netstat -an

Grundlegende Befehlsentsprechungen für Windows/Linux

In der nachfolgenden Tabelle findet Ihr eine Aufstellung der grundlegenden Befehlsentsprechungen zwischen Linux und Windows. Die Befehle werden entweder in einer Shell (unter Linux) oder in einem MS-DOS Fenster (unter Windows) ausgeführt.

Linux	Windows
command --help	command /h, command /?
man command	help command
cp	copy
rm	del
mv	move
mv	ren
more, less, cat	type
lpr	print
rm -R	deltree
ls	dir
cd	cd
mkdir	md
rmdir	rd
route	route print
traceroute –I	tracert
ping	ping
ifconfig	ipconfig

2.5. Übungen

2.5.1 Übungen unter Windows

1. Öffne ein DOS-Fenster

2. Identifiziere die MS-DOS Version mit der du arbeitest. Welche verwendest du? Welches Kommando hast du verwendet, um das herauszufinden?

3. Auf welche Zeit und welches Datum ist deine Systemuhr eingestellt? Wenn eines der beiden nicht stimmt, stelle es auf den korrekten Wert.

4. Welche Verzeichnisse und Dateien befinden sich in c:\ ? Welche Kommandos hast du verwendet, um das herauszufinden?

5. Erstelle eine Verzeichnis c:\hhs\lesson0. Kopiere alle Dateien mit der Endung .sys im Verzeichnis c:\. Welche Dateien hast du dort gefunden? Welche Kommandos hast du verwendet?

6. Welche IP-Adresse hat dein Host? Welches Kommando hast du verwendet, um das herauszufinden?

7. Welche Route nehmen Pakete auf dem Weg von deinem Rechner zu www.google.com? Welche IP-Adressen liegen auf dieser Route?

2.5.2 Übungen unter Linux

1. Suche eine Datei namens passwd und finde heraus, welchem Benutzer sie gehört. Welche Kommandos hast du verwendet?

2. Erstelle ein Verzeichnis namens work in deinem Home-Verzeichnis (/home/*deinbenutzername*) und kopiere die Datei passwd in dieses Verzeichnis. Welchem Benutzer gehört die Kopie?

3. Erstelle ein Verzeichnis namens .hide in deinem Home-Verzeichnis. Gib den Inhalt dieses Verzeichnisses aus. Was musstest du tun, damit das funktioniert hat?

4. Erstelle eine Datei namens test1 mit dem Inhalt "Dies ist der Inhalt der Datei test1" im Verzeichnis work, das du vorhin erstellt hast. Erstelle eine Datei namens test2 mit dem Inhalt "Dies ist der Inhalt der Datei test2" im selben Verzeichnis. Kopiere den Inhalt der beiden vorigen Dateien in eine neue Datei namens test. Welche Kommandos hast du verwendet?

5. Welche IP-Adresse hat deine Maschine? Welche Kommandos hast du verwendet, um das herauszufinden?

6. Welche Route nehmen Pakete auf dem Weg von deinem Rechner zu www.google.com? Welche IP-Adressen liegen auf dieser Route?

2.5.3 Übung 3

Vervollständige die folgende Tabelle. Welche Befehle unter Windows entsprechen denen unter Linux? Beispielsweise ist ***befehl* --help** unter Linux das gleiche wie ***befehl* /?** unter Windows und **cp** entspricht **copy**.

	Microsoft Windows
command --help	command /h
cp	copy
	del
mv	
more	
	print
	deltree
ls	
cd	
	md
	rd
route	
	tracert
Ping	
	ipconfig

Weitere Informationen

Wenn du ausführliche Informationen zum Stoff dieser Lektion willst, besuche doch die folgenen URLs:

http://www.matisse.net/files/glossary.html
http://www.uic.edu/depts/accc/inform/v106.html
http://www.catb.org/~esr/jargon/

unter Windows: ***befehl /?***
unter Linux: man *befehl* **oder *befehl* –help**

Glossar

IP-Adresse ("IP-address")

Eine eindeutige Nummer, um einen Computer im Internet zu identifizieren. IP-Adressen sind 32bit lange Zahlen, die dezimal als vier Nummern geschrieben werden und jeweils einen Punkt zwischen den einzelnen Nummern, die von 0 bis 255 reichen, haben, z.B. 61.160.10.240

Domainname ("domain name")

Ein Name, der eine oder mehrere IP-Adressen identifiziert. Der Domainname www.microsoft.com repräsentiert etwa ein Dutzend IP-Adressen. Domannamen werden in URLs verwendet, um beispielsweise eine bestimmte Webseite zu identifizieren. In der URL http://www.pcwebopedia.com/index.html ist der Domainname pcwebopedia.com.

Jeder Domainname hat ein Suffix (eine Endung), die die Top Level Domain (TLD), zu der der Domainname gehört angibt. Es gibt nur eine begrenzte Anzahl von TLDs:

.gov für Institutionen der (amerikanischen) Regierung
.edu für Universitäten und andere Bildungseinrichtungen (in den USA)
.org für gemeinnützige ("nonprofit") Organisationen
.com für kommerzielle Firmen
.net für Netzwerk-organisationen
.de für Firmen, Organisationen und Einrichtungen in Deutschland