Hacker Highschool
SECURITY AWARENESS FOR TEENS

LEZIONE 2
COMANDI BASE DI WINDOWS E LINUX

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.

Informazioni sulla licenza d’uso

Le seguenti lezioni ed il materiale per gli esercizi (workbook) sono materiale di tipo "open" e pubblicamente disponibili, secondo i seguenti termini e condizioni di ISECOM:

Tutto il materiale inerente il progetto Hacker Highschool è fornito esclusivamente per utilizzo formativo di tipo “non-commerciale” verso gli studenti delle scuole elementari, medie e superiori ed in contesti quali istituzioni pubbliche, private e/o facenti parte di attività del tipo “doposcuola”.

Il materiale non può essere riprodotto ai fini di vendita, sotto nessuna forma ed in nessun modo.

L’erogazione di qualunque tipologia di classe, corso, formazione (anche remota) o stage tramite questo materiale a fronte del corrispondimento di tariffe o denaro è espressamente proibito, se sprovvisti di regolare licenza, ivi incluse classi di studenti appartenenti a college, università, trade-schools, campi estivi, invernali o informatici e similari.

Per comprendere le nostre condizioni di utilizzo ed acquistare una licenza per utilizzi di tipo commerciale, vi invitiamo a visitare la sezione LICENSE del sito web Hacker Highschool all’indirizzo http://www.hackerhighschool.org/license.

Il Progetto HHS è uno strumento per apprendere e, come ogni strumento di questo tipo, la chiave formativa consiste nella capacità e nell'influenza dell'istruttore, e non nello strumento formativo. ISECOM non può accettare e/o farsi carico di responsabilità per il modo in cui le informazioni qui contenute possono essere utilizzate, applicate o abusate.

Il Progetto HHS rappresenta uno sforzo di una comunità aperta: se ritenete il nostro lavoro valido ed utile, vi chiediamo di supportarci attraverso l'acquisto di una licenza, una donazione o una sponsorizzazione al progetto.

Tutto il materiale e' sotto copyright ISECOM, 2004

Indice

Hanno contribuito

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

Per la versione in lingua italiana:

Raoul Chiesa, ISECOM

Doriano Azzena, centro CSAS del progetto Dschola IPSIA Castigliano - Asti

Sophia Danesino, centro CSAS del progetto Dschola ITIS Peano – Torino

Nadia Carpi, centro CSAS del progetto Dschola ITIS Peano – Torino

Fabrizio Sensibile, OPST&OPSA Trainer, @ Mediaservice.net Srl, Torino - ISECOM Authorized Training Partner

Claudio Prono, @ Mediaservice.net Srl, Torino – ISECOM Authorized Training Partner

2.1 Obiettivi

In questa lezione intendiamo presentarti i comandi e gli strumenti (tool) base di Windows e di Linux; avrai bisogno di familiarizzare con il loro uso per risolvere gli esercizi proposti nel seguito del corso. Al termine della lezione avrai appreso i comandi:

- generali di Windows e Linux.
- base sulla rete:
  - ping
  - tracert, traceroute
  - netstat
  - ipconfig, ifconfig
  - route

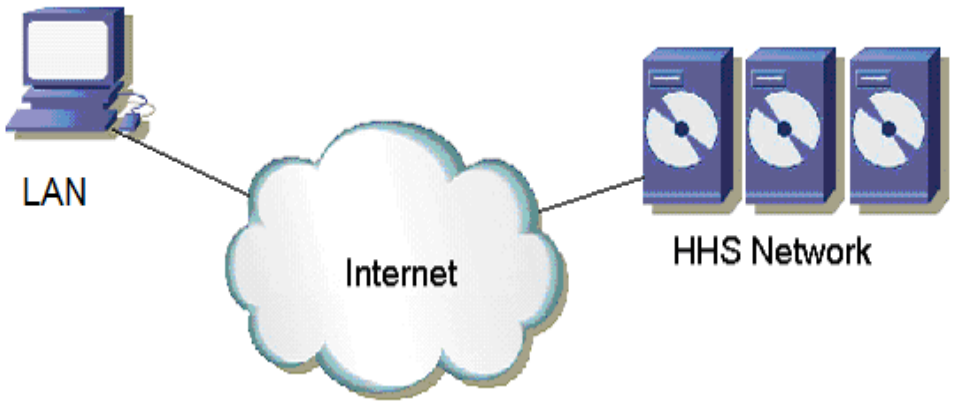
2.2 Requisiti e ambiente

2.2.1 Requisiti

Per questa lezione sono necessari:

- Un PC con Windows 98/Me/2000/NT/XP/2003.
- Un PC con Linux Suse/Debian/Knoppix…
- Accesso a Internet.

2.2.2 Ambiente



Questo è l'ambiente in cui lavoreremo; esso è costituito dalla rete, con accesso a internet, da cui lavorerai e dalla rete di server di ISECOM destinata al programma Hacker Highschool (HHS), alla quale si accede attraverso Internet. Quella di ISECOM è la rete sulla quale realizzerai la maggior parte dei test.

Devi tenere presente che l'accesso alla rete di prova ISECOM è limitato a coloro che partecipano al programma HHS. Il tuo istruttore dovrà contattare l'amministratore del sistema come descritto sul sito www.hackerhighschool.org per farti ottenere il diritto di accesso.

2.3 Sistema Operativo: WINDOWS

La maggior parte degli strumenti utilizzati per studiare le reti sono comandi interni del sistema operativo Windows. Per questo motivo esaminiamo come aprire una finestra di comando quando utilizzi Windows come sistema operativo.

2.3.1 Come aprire una finestra MS-Dos?

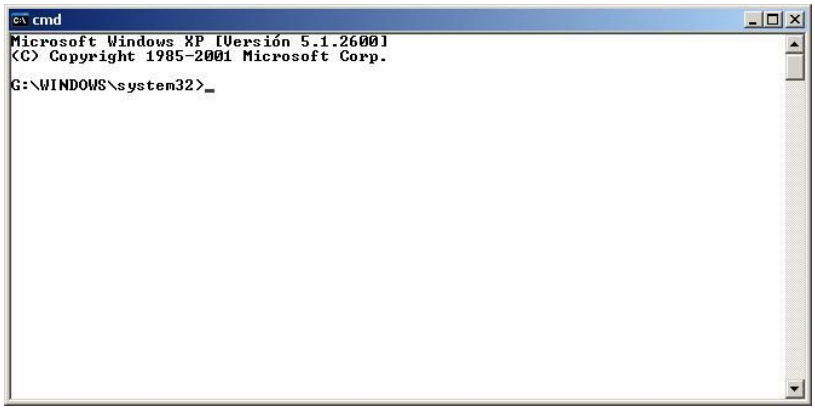
Per poter utilizzare i comandi devi aprire una finestra di comando (finestra MS-DOS). Il procedimento è lo stesso per qualsiasi verisone di Windows:

1.- Clicca il bottone START o AVVIO

2.- Scegli l'opzione Esegui.

3.- Scrivi "**command**" se utilizzi Windows 95/98 o "**cmd**" per il resto di Windows, clicca poi su OK.

4.- Apparirà una finestra simile alla seguente:



5.- Ora puoi provare i comandi e gli strumenti (tool) sotto indicati.

2.3.2 Comandi base

date	Mostra o imposta la data del sistema
time	Mostra o imposta l'ora del sistema
ver	Motra la versione di MS-DOS che si sta utilizzando
dir	Mostra la lista delle sottocartelle e file di una cartella o directory
cls	Pulisce (cancella) lo schermo
mkdir <directory> **md** <directory>	Crea una directory o cartella. Per esempio: `md tools`

chdir <directory> **cd** <directory>	Mostra il nome o cambia la directory corrente. Per esempio: `cd tools`
rmdir <directory> **rd** <directory>	Elimina una directory o cartella. Per esempio: `rd tools`
tree <directory>	Mostra in forma grafica-testo la struttura di cartelle. Per esempio: `tree c:\tools`
chkdsk	Controlla un disco e mostra informazioni sul suo stato
mem	Mostra la quantità di memoria utilizzata e libera nel sistema
rename <origine> destinazione> **ren** <origine> <destinazione>	Cambia il nome di uno o più file. Per esempio: `ren vecchionome nuovonome`
copy <origine> <destinazione>	Copia uno o più file in un altro posto. Per esempio: `copy c:\util\nomefile.txt c:\temp`
move <origine> <destinazione>	Cambia il nome di file e directory. Per esempio: `move c:\tools c:\strumenti`
type <file>	Mostra il contenuto di un file di testo. Per esempio: `type c:\tools\nomefile.txt`
more <file>	Mostra il contenuto di un file di testo una videata alla volta. Per esempio: `More c:\toole\nomefile.txt`
delete <file> **del** <file>	Elimina uno o più file. Per esempio: `del c:\tools\nomefile.txt`

Nota: le parole tra i simboli < > non sono comandi, devono essere sostituite dai valori desiderati. Ci sono comandi che si possono attivare utilizzando le forme estese o brevi, per esempio "delete " e "del" sono lo stesso comando.

2.3.3 Strumenti (tool) di rete

ping <host>	Il comando ping permette di inviare "pacchetti" ICMP (Internet Control Message Protocol) a un altro computer, per verificare se è raggingbile attraverso la rete (internet o locale). Inoltre mostra un riassunto statistico sulla percentuale di pacchetti che non hanno ottenuto risposta e il tempo di risposta. Al posto del parametro host Si puo' utilizzare il nome o il numero (indirizo IP) del computer da testare.
	Per esempio:
	`ping www.google.com`
	`ping 193.145.85.2`
	Alcune opzioni sono:
	-h <N> : per specificare N salti come massimo
	-n <N> : invia N pacchetti
	-t : invia un numero infinito di pacchetti, Per interrompere premere: CTRL+C.
	Per visualizzare altre opzioni: `ping /h`

tracert <host>	Il comando tracert è l'abbreviatura di **trace route**, che ci permette di conoscere il percorso che seguono i pacchetti a partire dall'origine, ovvero il tuo computer, fino al computer destinazione. Inoltre ci indica il tempo di ciascun salto. Come massimo, saranno visualizzati 30 salti. E' interessante osservare che si ottengono i nomi dei computer attraverso i quali viaggiano i pacchetti.
	Per esempio:
	`tracert www.google.com`
	`tracert 193.145.85.2`
	Alcune opzioni:
	-h <N> : per specificare al massimo N salti.
	-d : non mostra il nome dei computer.
	Per visualizzare più opzioni: `tracert`

ipconfig	Il comando ipconfig mostra informazioni sulle interfacce di rete attive nel computer. Per esempio: `ipconfig` Alcune opzioni: **/all** : motra il maggior numero di dettagli **/renew** nome : rinnova la connessione con "nome" quando si usa la configurazione automatica con DHCP. **/release** nome : disattiva tutte le connessioni con "nome" quando si usa la configurazione automatica con DHCP. Per visualizzare più opzioni: **`ipconfig /?`**
route	Il comando route serve per definire i percorsi (route) statici , cancellare i percorsi o semplicemente per visualizzare lo stato dei percorsi. Alcune opzioni: **Print** : mostra la lista dei percorsi (route). **Delete** : cancella un percorso. **Add** : aggiunge un percorso. Per esempio: `route print` Per visualizzare più opzioni: **`route /?`**
netstat	Mostra informazioni sullo stato della rete e delle connesioni di rete stabilite con computer remoti. Alcune opzioni: **-a** testa tutte le connessioni e le porte di ascolto. **-n** mostra gli indirizzi e le porte in forma numerica. **-e** mostra statistiche Ethernet. Per esempio: **`netstat`** **`netstat –an`** Per visualizzare più opzioni: **`netstat /?`**

2.4 Sistema operativo: LINUX

Proprio come con Windows. Se utilizzi Linux, la maggior parte dei comandi che userai sarà eseguita da una console o da una finestra emulazione di console. Per questo motivo ora ti spiegheremo come aprire una finestra di console in Linux.

2.4.1 Come aprire una finestra di console?

Per eseguire i comandi seguenti devi aprire una finestra di console:

1. – Clicca il bottone di AVVIO o di START
2. – Scegli l'opzione Esegui Comando o Run Command :
3. – Scrivi "konsole".
4. – Dovrebbe aprirsi una finestra come la seguente:

5. – Ora puoi utilizzare i comandi e gli strumenti (tool) sotto indicati.

2.4.2 Comandi base

Pwd	Mostra il nome della directory corrente.
Hostname	Mostra il nome del computer locale (quello su cui stai lavorando)
finger <utente>	Mostra informazioni sull'utente Per esempio: `finger root`

ls	Lista il contenuto delle directory Per esempio: `ls -la`

cd <directory>	Cambia dalla directory corrente a <directory>. Se non si specifica <directory> il cambio avviene nella home dell'utente.
	Eempio 1:
	Se il tuo login è "miologin", il comando
	`$cd`
	Cambia alla directory /home/miologin
	Esempio 2:
	`$cd -`
	Cambia all'ultima directory visitata.
	Esempio 3:
	`$cd /tmp`
	Cambia alla directory "tmp"

cp <origine> <destinazione>	Copia file. Copia il file "origine" in "destinazione". Per esempio: `Cp /etc/passwd /tmp`
rm <file>	Elimina file. Solo il propietario dei file (oppure root) puo' eliminare. Per esempio: `Rm nomefile`
mv <origine> <destinazione>	Muove o rinomina file e directory. Per esempio: `Mv nomeantico nomenuovo`
mkdir <directory>	Crea una directory di nome "directory" Per esempio: `mkdir miadirectory`
rmdir <directory>	Elimina la directory <directory> se è vuota. Per esempio: `rmdir miadirectory`
man <comando>	Mostra le pagine del manuale on-line Per esempio: `man ls`

Nota: Le parole comprese tra i simboli < > non sono comandi, devono essere sostituite dai valori desiderati.

2.4.3 Strumenti (Tool) di rete

ping <host>	Il comando ping permette di inviare "pacchetti" ICMP (Internet Control Message Protocol) a un altro computer, per verificare se è raggingbile attraverso la rete (internet o locale). Inoltre mostra un riassunto statistico sulla percentuale di pacchetti che non hanno ottenuto risposta e il tempo di risposta. Al posto del parametro host Si puo' utilizzare il nome o il numero (indirizo IP) del computer da testare.
	Per esempio:
	`ping www.google.com`
	`ping 193.145.85.2`
	Per visualizzare più opzioni: `man ping`

traceroute <host>	Il comando traceroute indica il percorso (route) che seguono i pacchetti dall'origine, il tuo computer, al computer destinazione chiamato <host>. Per esempio: `traceroute www.google.com` Per visualizzare più opzioni: `man traceroute`
Ifconfig	Il comando ifconfig mostra informazioni sulle interfacce attive (ethernet, ppp, etc.). Per esempio: `ifconfig` Per visulaizzare più opzioni: `man ifconfig`

route	Il comando route serve per definire i percorsi (route) statici, eliminare i percorsi o semplicemente visualizzare lo stato dei percorsi
	Alcune opzioni:
	print: mostra la lista dei percorsi.
	delete: elimina un percorso.
	add: aggiunge un percorso.
	Per esempio:
	`route`
	`route del default`
	`route add default gw 192.168.1.1`
	Per visualizzare più opzioni: `man route`

Netstat	Mostra informazioni sullo stato della retee delle connessioni TCP/IP stabilite.
	Per esempio:
	`netstat`
	`netstat –an`
	Per avere più opzioni: `man netstat`

Nota: nel digitare i comandi tieni conto del fatto che linux è "case sensitive", ovvero distingue tra maiuscolo e minuscolo.

Per esempio:
Pwd non è un comando valido (compare la P maiuscola)
pwd è un comando valido

2.5 Esercizi

Esercizio 1:

Approfondimento di Windows.

a. Accedi a una finestra MS_DOS

b. Identifica la versione di MS-DOS che stai utilizzando. Cosa hai trovato? Che comando hai utilizzato?.

c. Identifica la data e l'ora del sistema. Se non sono esatte modificale. Che comando hai utilizzato?

d. Identifica tutte le directory e file che si trovano in "c:\". Che comando hai utilizzato?

e. Crea la directory "c:\hhs\lezione0". Copia in questa directory tutti i file con l'estensione ".sys" que trovi in "c:\". Quali file hai trovato? Quale comando hai utilizzato?

f. Identifica l'indirizzo IP del tuo computer. Che comando hai utilizzato? Che indirizzo hai?

g. Traccia il percorso dal tuo computer a "www.google.com". Identifica gli indirizzi IP dei router intermedi.

Esercizio 2:

Approfondimento di Linux.

a. Identifica il propietario del file "/etc/passwd". Che comando hai utilizzato?

b. Crea la directory "lavoro" nella tua home direcory (per esempio, se il tuo login è "miologin", crea la directory in "/home/miologin"), e copia il file "passwd" nella directory "lavoro" che hai appena creato. Identifica il propietario del file "passwd" che hai copiato.

c. Crea la directory ".nascosto" nella directory "lavoro". Lista il contenuto di questa directory. Cosa devi fare per poter visuaizzare il contenuto della directory ".nascosto"?

d. Crea il file "test1" con il contenuto "Questo è il contenuto del file test1" nella directory "lavoro". Crea il file "test2" con il contenuto "Questo è il contenuto del file test2" nella directory "lavoro". Copia in un file di nome "test" il contenuto dei precedenti file. Quali comandi hai utilizzato?

e. Identifica il nome e l'indirizzo IP del tuo computer. Che comando hai utilizzato? Che indirizzo IP ha?

f. Traccia il percorso dal tuo computer a "www.apache.org". Identifica gli indirizzi IP dei router intermedi.

Esercizio 3:

Completa la seguente tabella con i parallelismi tra Windows e Linux. Per esempio:

In Linux: il comando "comando –help" è lo stesso che il comando "comando /h" in Windows.

In linux: cp (copiare) è lo stesso che copy in Windows .

	Microsoft Windows
comando –help	comando /h
cp	copy
	del
mv	
more	
	print
	deltree
ls	
cd	
	md
	rd
route	
	tracert
ping	
	ipconfig

2.6. Ulteriori approfondimenti

Per un glossario esteso consulta i seguenti URL:

http://www.matisse.net/files/glossary.html

http://www.uic.edu/depts/accc/inform/v106.html

http://www.catb.org/~esr/jargon/

http://web.tiscali.it/glossario/

Windows – per informazioni aggiuntive su comandi e strumenti (tool) digita "comando /h" or "comando /?," o "help comando" da una finestra MS-DOS.

Linux – per informazioni aggiuntive su comandi e strumenti digita: "comando --help" o "man comando" da una shell.

Glossario

Indirizzo IP (IP address):

E' l'identificativo di un computer su Internet. Il formato è costituito da quattro numeri, con valori compresi tra 0 e 255, separati da un punto. L'identificativo è univoco, ovvero in qualsiasi istante su Internet non ci possono essere due o più computer con lo stesso identificativo.

Per esempio, 10.160.10.240 (indirizzo IP di tipo privato).

Dominio (Domain):

E' un nome che identifica uno o più indirizzi IP. Per esempio, il dominio Microsoft.com rappresenta circa una dozzina di indirizzi IP. I nomi di dominio sono utilizzati negli URLs per identificare determinate pagine Web. Per esempio, nella URL http://www.pcwebopedia.com/index.html, il nome di dominio è pcwebopedia.com.

Ogni nome di dominio ha un suffisso che indica a che livello di dominio superiore (TLD, Top Level Domain) appartiene. Il numero dei suffissi è limitato. Per esempio:

- gov – Istituzioni governative
- edu – Istituzioni Educative
- org – Organizzazioni (senza fini di lucro)
- com – Organizzazioni commerciali
- net – Organizzazioni di Rete
- it – Italia
- … etc …

Poichè Internet è basato sugli indirizzi IP, e non sui nomi di dominio, ogni server Web necessita un sistema di nomi di dominio (DNS, Domain Name System) che traduca i nomi in indirizzi IP.

MS-DOS (Microsoft Disk Operating System):

MS-DOS è un sistema operativo. La sua funzione è facilitare la comunicazione tra l'utente e il computer e utilizzare efficientemente le risorse disponibili, per esempio l'uso della memoria e della CPU.

Router:

Dispositivo che distribuisce il traffico tra le reti. Un router è connesso come mínimo a due reti, generalmente due LAN (Local Area Network) o WAN (Wide Area Networks) o una LAN e la rete del fornitore di accesso internet (ISP - Internet Service Provider). I router si trovano nei "gateway", luogo in cui due o più reti si connettono.

I router utilizzano le tabelle di instradamento per determinare il miglior percorso in cui dirigere i pacchetti IP, inoltre utilizzano protocolli tra cui l'ICMP per comunicare tra loro e configurare il miglior percorso tra due host.

Sistema Operativo (Operating System – OS):

Un sistema operativo è un programma speciale il cui compito principale è gestire gli altri programmi applicativi, per esempio Microsoft Word, Outlook, navigare internet, stampare, etc.

Il sistema operativo è anche responsabile di rilevare la presenza dei vari dispositivi hardware e stabilire la comunicazione tra l'utente e l'hardware (tastiera, mouse, monitor, etc). Esempi di sistemi operativi sono: Windows, Linux, UNIX, Mac OS X, etc.

Appendice: equivalenza tra i comandi base di Windows e Linux

La tabella seguente mostra l'equivalenza tra i comandi base di Linux e Windows. I comandi devono essere eseguiti da una shell (in Linux) o da una finestra MS-DOS (in Windows).

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