Hacker Highschool
SECURITY AWARENESS FOR TEENS

LESSON 2
BASIC COMMANDS IN LINUX AND 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.

All works copyright ISECOM, 2004.

Table of Contents

Contributors

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

2.1. Introduction and Objectives

This lesson introduces commands and basic tools for both Windows and Linux operating systems so that you can become familiar with them. These commands will be used to complete the exercises in the following lessons

At the end of this lesson, you should know the following commands:

> General Windows and Linux commands

> Basic network commands and tools

    - ping

    - tracert

    - netstat

    - ipconfig

    - route

2.2. Requirements and Setup

2.2.1 Requirements

For the lesson, the following are needed:

- a PC with Windows 98/Me/2000/NT/XP/2003

- a PC with Linux Suse/Debian/Knoppix

- access to the Internet.

2.2.2 Setup
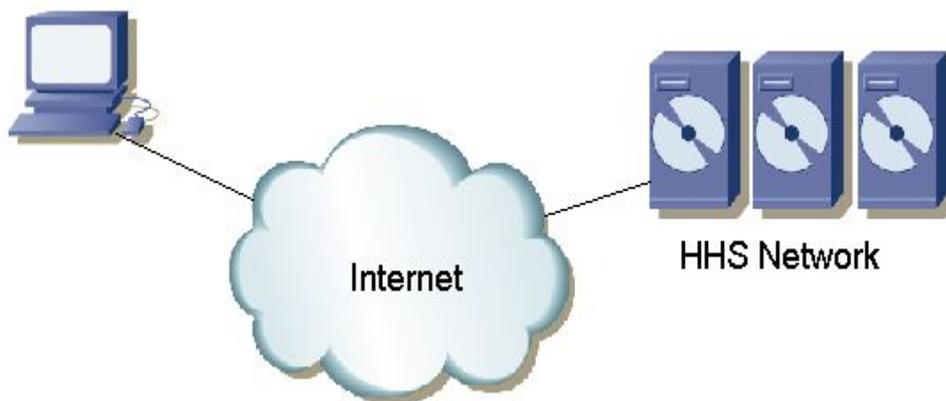
This is the setup in which you are going to work. It consists of your PC, with access to the Internet, and the ISECOM Hacker Highschool network, which you will access through the Internet. This is the network against which you will make most of the tests.

Note that access to the ISECOM test network is restricted. In order to gain access to it, your instructor must contact the sytem administrator, as detailed on the www.hackerhighschool.org web site.

2.3. System Operation: WINDOWS

Most of the tools used for the study of networks are internal commands in the Windows operating system. Therefore, we are going to explain how to open a command window when the Windows operating system is being used.

2.3.1 How to open an MS-DOS window

To issue the following commands, it is necessary to open a command prompt (an MS-DOS window). The procedure for this is the same for all versions of Windows.

1.- Click the START button

2.- Choose the RUN option

3.- Type "**command**" if you are using Windows 95/98 or "**cmd**" for all other versions of Windows and press Enter or click OK.

4.- A window similar to the following one will appear:
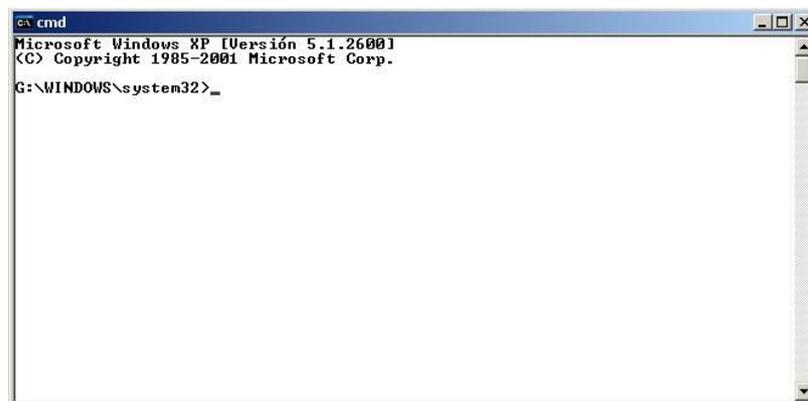
5.- Now the commands and tools listed below can be entered.

2.3.2 Commands and tools (Windows)

Commands

date	Display or set the date of the system
time	Display or set the time of the system
ver	Display the MS-DOS version that is being used
dir	Display the list of subdirectories and files of a directory
cls	Clear the screen
mkdir, **md** *directory*	Make a directory with the name "directory" Example: md tools
chdir, cd *directory*	Display the name or change the current directory to "directory" Example: cd tools
rmdir, rd *directory*	Delete the directory with the name "directory" Example: rd tools

tree *directory*	Display the structure of folders of a path in text-graphic format Example: tree c:\tools
chkdsk	Check a disk and show a status report
mem	Show the amount of memory used and free in the system
rename, **ren** *source dest*	Change the name of files Example: ren oldname newname
copy *source dest*	Copy one or more files to another location Example: copy c:\tools\myfile.txt c:\tmp
move *source dest*	Move files and change the name of files and directories Example: move c:\tools c:\tmp
type *file*	Type the content of one or more text files Example: type c:\tools\myfile.txt
more *file*	Display the information screen by screen Example: more c:\tools\myfile.txt
delete, del *file*	Delete one or more files Example: del c:\tools\myfile.txt

Note: The words in italics are not commands, and must be replaced by the desired values. Some of the commands can be used by typing either their long version or short version; for example, "delete" and "del," are the same command.

Tools

ping *host*	Verify contact with the machine "host" The command ping sends "packets" using ICMP (Internet Control Message Protocol) to another computer, to learn whether it is accessible through the network. In addition, it shows a statistical summary about the percentage of packets that have not been answered and the response time. The name of the machine can be used directly or its IP address. Examples: ping www.google.com ping 193.145.85.2 Some options are: - n N: send N packets - t: ping the specified host until stopped (press CTRL+C to end) To see more options: ping /h

tracert *host*	Show the route that packets follow to reach the machine "host" The command tracert is the abbreviation of trace route, which allows you to learn the route that a packet follows from the origin, (your machine) to the destination machine. It can also tell you the time it takes to make each jump. At the most, 30 jumps will be listed. It is sometimes interesting to observe the names of the machines through which the packets travel. Examples: tracert www.google.com tracert 193.145.85.2 Some options are: - h N: to specify N, at the most, jumps. - d: to not show the names of the machines. To see more options: tracert
ipconfig	Display information on the active interfaces (ethernet, ppp, etc.) in the computer. Some options: /all: to show more details /renew *name*: renews connection with "name" when automatic configuration with DHCP is used. /release *name*: deactivates all matching connections when automatic configuration with DHCP is used. To see more options: ipconfig /?
route print	Display the routing table The command route serves to define static routes, to erase routes or simply to see the state of the routes. Some options: print: to show the list of routes. delete: to delete a route. add: to add a route. To see more options: route/?
netstat	Displays information on the status of the network and established connections with remote machines. Some options: -a: To sample all the connections and listening ports -n: to display addresses and port numbers in numeric form -e: to sample Ethernet statistics For example: netstat - an To see more options: netstat/?

9

For additional information on these commands and tools type "command /h" or "command /?," or "help command" from a MS-DOS window.

For example, for additional information on the tool netstat, we have three possibilities:

1) netstat /h

2) netstat /?

3) help netstat

2.4. System Operations: Linux

Just as in Windows, if you are using Linux, a great majority of the commands that you will use are executed from a console emulation window. Therefore, we will next learn how to open a console window in Linux.

2.4.1 How to open a console window

To issue the following commands, it is necessary to open a console window:

1. - To go to the START APPLICATION button

2. - Select "Run Command"

3. - Enter "konsole"

4. - A window similar to the following one will appear:
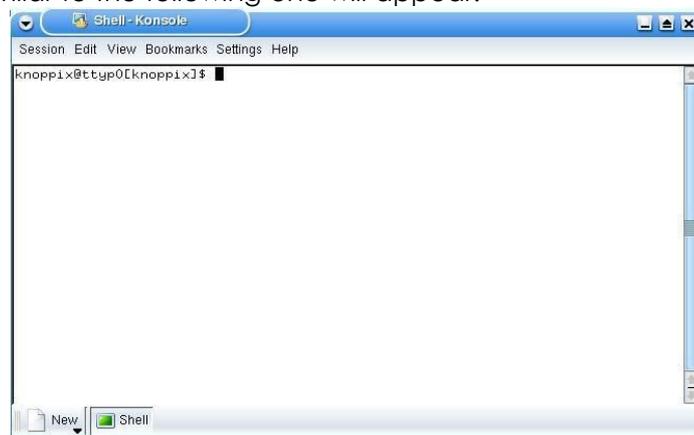
5. - Now the commands and tools listed below can be entered.

2.4.2 Commands and tools (Linux)

Commands

pwd	Display the name of the current directory.
hostname	Display the name of the local host (the computer which you are currently using)

finger *user*	Display information on the user "user" Example: finger root
ls	List the content of the directories Example: ls -la
cd *directory*	Change from current directory to "directory". If no directory name is specified it changes to the home directory, Example: For the login name "mylogin" the command $cd changes the directory to /home/mylogin Example: $cd - changes to the last visited directory Example: $cd /tmp changes to the "tmp" directory
cp *source dest*	Copy files. Copy the file "source" to the file "dest". Example: cp /etc/passwd /tmp
rm *file*	Delete files. Only the owner of the file (or root) can delete it. Example: rm myfile
mv *source dest*	Move or rename files and directories. Example: mv oldname newname
mkdir *directory*	Make a directory with the name "directory". Example: mkdir tools
rmdir *directory*	Delete the directory with the name "directory" if it is empty. Example: rmdir tools
find / -name *file*	Find a file with the name "file" beginning the search in the root directory Example: find / -name myfile
echo *string*	Write the string "string" in the standard output Example: echo hello
command > file	Redirect the normal screen output of the command "command" to the file "file" Example: ls > myls
command >> file	Redirect the normal screen output of the command "command" to the file "file". If the file already exists, it appends the output to the end of the file. Example: ls >> myls
man *command*	Show the pages of the online manual about "command" Example: man ls

Note: The words in italics are not commands and must be replaced by the desired values.

For additional information on the use of these commands and tools, type in "command -help" or "man command" in the console window.

For example, for additional information on the "ls" command, type in either of these two possibilities:
1) ls ––help
2) man ls

Tools (Please see the Windows section for details on these tools.)

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

Basic command equivalences for Windows/Linux

This is a table showing the basic command equivalences between Linux and Windows. Commands are executed from a shell (in Linux) or from a MS-DOS window (in Windows).

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. Exercises

2.5.1 Exercises in Windows

1. Go to a MS-DOS window.

2. Identify the version of MS-DOS that you are using. What version have you detected? What command have you used?.

3. Identify the date and time of the system. If they are incorrect, modify them so that they are correct. What command have you used?

4. Identify all the directories and files that are in "c:\". What command have you used?

5. Create the directory c:\hhs\lesson0. Copy in this directory all the files with the extension ".sys" that are in "c:\". What files have you found? What commands have you used?

6. Identify the IP address of your host. What command have you used? What IP address do you have?

7. Trace the route to "www.google.com". Identify IPs of the intermediate routers.

2.5.2 Exercises in Linux

1. Identify the owner of the file "passwd". (Note: first locate where this file is). What command have you used?

2. Create the directory "work" in your own home directory (for example, if your login is "mylogin", create the directory in "/home/mylogin"), and copy the file "passwd" in the directory "work" that you have just created. Identify the owner of the file "passwd" that has been copied.

3. Create the directory ".hide" in the "work" directory. List the contents of this directory. What did you have to do to see the contents of directory ".hide"?

4. Create the file "test1" with the content "This is the content of the file test1" in the "work" directory. Create the file "test2" with the content "This is the content of the file test2" in the "work" directory. Copy into a file with the name "test" the contents of previous files. What commands have you used?

5. Identify the name and the IP address of your machine. What commands have you used? What IP address do you have?

6. Trace the route to "www.google.com". Identify IPs of the intermediate routers.

2.5.3 Exercise 3

Complete the following table with parallelisms between Windows and Linux. For example: the Linux command "command -help" is equivalent to the Windows

command "command /h". As another example, in Linux: "cp" is just like the Windows command, "copy".

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

Further Reading

For an extensive glossary of terms visit the following URLs:

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

Windows – for additional information on commands and tools, type in "command /h" or "command /?," or "help command" from a MS-DOS window.

Linux – for additional information on commands and tools, type in "command --help" or "man command" from a shell.