First Experiment

DOS Commands

(please hand in soft copy)

(You can select your own target websites, but avoid sensitive ones, such as FBI, CIA…)

Below are a few widely used DOS commands that are used by IT security professionals on a daily basis. Although DOS commands may seem archaic to those that grew up on Windows, many of the best security programs still use a command-line interface. Learning command-line will become easier with practice. Knowing how to use a command prompt will make the transition to the Linux operating system much easier. Many IT security tools are currently written exclusively for Linux and use only a command-line interface.

There are just a few of the most basic commands available to all users with a command prompt. A larger list is available by typing "help" at the DOS prompt. All versions of Windows have a command prompt for you to use. To pull up a command prompt you can go through the start menu. You can also click Start, Run, and then type Command.

IPCONFIG

The ipconfig command will give you a listing of the basic IP information for the computer you are using. You will get information about your IP address, subnet mask, and default gateway (the computer that connects you to the Internet). Write this information down because you will use it in later experiments involving port scanning, remote administration, penetration testing, etc. You will enter items 1 and 2 at the command prompt.

1. Type ipconfig
2. Type ipcofig /all
3. Take a screenshot

In the second command we wanted more information so we used the /all switch to give us more information. Now you know how to get the following information for any computer:

a. The IP address
b. The MAC address
c. The computer that connects to the Internet (default gateway)

Questions:

1. What is the practical difference between an IP address and a physical (MAC) address?
2. What is the "default gateway?"
3. What do DNS servers do?
4. What is subnet mask?

PING

Ping is a command that will tell you if a host is reachable and alive. It sends out a packet that asks the target computer to send back a message saying it is actually there. It also tells you how long it took to get back and if any of the packets were lost. This is useful should you need to determine whether a server/computer is running.

1. Type ping www. Utt.edu.ttt
2. Take a screenshot

Questions

1. Why does it send 4 packets?
2. What is TTL?
3. How do packets get lost?
4. Does each host name have an IP address assigned to it?

TRACERT

Trace route is a command that allows you to see every computer (including routers) between you and a target of your choosing. You can type in the name of the computer/web site (e.g. www. Utt.edu.tt) or the IP address of the computer (76.163.122.211)

1. Type tracert www.utt.edu.tt
2. Take a screenshot

If you type the same command on www.google.com, you might get a much longer list because it has to go through more computers to get to one of Google's servers.

Questions

1. How many computers do you go through each time you click on a website?
2. Why are some links slower than others?
3. Who owns all those computers routers that route the packets?
4. How does the tracert program actually work (hint: TTL)?

NETSTAT

Netstat is the command that lists all current network connections, connection statistics, the routing tables on your computer. The default netstat command will give you a listing of all the ports open on your computer as well as the foreign address of the computer to which you are connected.

Ports are like doors on your house. Information packets are addressed to a specific IP address (location) and port number (point of entry). Your house works the same way. It has an address (location) and door

(point of entry) where packages are delivered. Netstat can tell you which programs are sending or receiving information to/from your computer.

1. Type netstat
2. Take a screenshot

Note: You can use the –b switch to get information about which program is opening each port.

3. Type netstat –b
4. Take a screenshot

Note: to find out all the possible switches associated with the netstat command type the following

5. Type netstat ?
6. Take a screenshot

Questions

1. How can netstat help you track the information coming in and out of your computer?
2. How can netstat help you diagnose network problems?
3. How would the routing table (netstat –r) be useful?
4. Why would someone need different statistics for IP, IPv6, ICMP, TCP, UDP, etc.?

NSLOOKUP

Nslookup is a command that will give you all the IP addresses that are associated with a given domain name from the local DNS server. (it is like a Internet phone book.). for example, if you wanted to find out the IP address www.alexu.edu.eg you could use nslookup to identify them.

1. Type nslookup www.alexu.edu.eg
2. Take a screenshot

Questions

1. Why are there multiple IP addresses associated with a single domain name?
2. How could someone use nslookup in an unethical manner?
3. How do domain names and IP addresses get registered?

DIR & CD

For some of our experiments you will need to move between directories (folders) on you computer using DOS commands. The dir command gives you a listing of the files, programs, subdirectories in the current directory.