Reconnaissance, Computer and Network Security, CSE 467
Department of Computer Science and Engineering, Miami University

Objectives

This lab provides hands-on experience using command-line utilities to perform tasks like port scanning, IP address discovery, and packet sniffing.

Background:

Command-line networking utilities such as **whois**, **nslookup**, **nmap**, and **tcpdump** are valuable assets in computer networking. These utilities can be used to monitor network traffic for malicious activity and for debugging communication in computer networks.

- nslookup: https://neverendingsecurity.wordpress.com/2015/04/13/nslookup-commands-cheatsheet/
- nmap : https://www.tutorialspoint.com/nmap-cheat-sheet
- tcpdump: https://gist.github.com/jforge/27962c52223ea9b8003b22b8189d93fb

You should never perform any of these attacks on any machines except for those specifically set up for you to practice.

Tasks:

1. Use **ifconfig** to find out the IP address of your VM. List the external IP address of your machine (ignore the 127.0.0.1 address).
    a. 172.17.13.47
2. Use **nslookup** to find out IP address associated with a domain name. Prepare a table with the domain name and the IP address for each of the following:
    a. harvard.edu
    b. miamioh.edu
    c. cnn.com
    d. sbhunia.me
    e. bhunias.sec.csi.miamioh.edu

Domains	IP Addresses
harvard.edu	151.101.194.133
miamioh.edu	10.5.32.12
cnn.com	151.101.193.67
sbhunia.me	185.199.108.153
bhunias.sec.csi.miamioh.edu	172.17.14.230

    f.
3. Use **whois** to find out information about a domain name. Prepare a table with address, phone number, and email addresses for each of the following (list all, in case of multiples):
    a. harvard.edu
    b. miamioh.edu
    c. cnn.com
    d. sbhunia.me
    e. bhunias.sec.csi.miamioh.edu

Reconnaissance, Computer and Network Security, CSE 467
Department of Computer Science and Engineering, Miami University

Domain	Address(es)	Phone number(s)	Email(s)
harvard.edu	Harvard University 784 Memorial Drive MA Cambridge, MA 02139 USA Benjamin Dash Harvard University 784 Memorial Drive Cambridge, MA 02138 USA +1.6174955708 Benjamin_Dash@harvard.edu Network Operations Harvard University HUIT Network Services 60 Oxford Street Cambridge, MA 02139 USA	+1.6174955708	Benjamin_Dash@harvard.edu netmanager@harvard.edu
miamioh.edu	Miami University Hoyt Hall Oxford, OH 45056 USA Domain Admin Miami University Hoyt Hall Oxford, OH 45056 USA	+1.5135291809	dnsadmin@listserv.miamioh.edu dnstech@miamioh.edu
cnn.com	Turner Broadcasting System, Inc. One CNN Center Atlanta, GA 30303 USA	+1.4048275000	tmgroup@turner.com hostmaster@turner.com
sbhunia.me	N/A	N/A	N/A

bhunias.sec.csi.miamioh.edu	No match		

4. Choose any 2 classmates. Use the **nmap** command to find the open ports in your friends' machines. List their IP address, the open port numbers, and the application running on that port. Please try nmap without any flag and then try with -sS, -sT, -sU flags.

IP	Open ports
172.17.13.184	22 (ssh), 80 (http), 443 (https), 68 (UDP)
172.17.13.54	22 (ssh), 80 (http), 443 (https), 68 (UDP)

5. Using **nmap**, find the list of active IPs in your subnet. Your subnet address would look like 172.17.38.0/24. Here, 172.17.38.0 is the subnet address. The 24 means the first 24 bits of the netmask is 1 and the rest 8 bits are zero.
    a. *hint:* use the -sP flag for **nmap** to do a Ping scan.
    b. 172.17.13.118
    c. 172.17.13.125
    d. 172.17.13.134 (3 out of 63)
6. Find out which machines have open port 80. Use the same subnet address as before.
    a. *hint:* use the -p flag with desired port number
    b. 172.17.13.118
    c. 172.17.13.125
    d. 172.17.13.134 (3 out of 63)
7. Use the **tcpdump** command to passively sniff traffic. To stop the sniffing, press CTRL+C. Identify which machines your VM is communicating to – provide port number and IP address.
    a. 172.17.13.54: 21923
    b. ceclnx01.csi.miamioh.edu.46642
    c. 172.17.13.184.57211
    d. 172.17.13.47.55947
    e. 172.17.13.47.5000
    f. 172.17.13.184.57212
8. Filter tcpdump for port 80. Do you see any traffic?
    a. *hint*: **sudo tcpdump port 80**
    b. No
9. Run the TCP dump on port 80 as in the previous task. Now ask your friend to access the website on your Kali machine. http://<UID>.sec.csi.miamioh.edu. Do you see any traffic? If so, from what IP? Which computer that IP belongs to?
10. **Yes from egb-10-33-10-225.muo.muohio.edu.53595, this belongs to Carson's Benton lab computer**

Submission:

- Submit on Canvas the required information in a Word Processor document (.doc, .docx)

Reconnaissance, Computer and Network Security, CSE 467
Department of Computer Science and Engineering, Miami University

- Please use the same numbering as in this document. If you include extra information, beyond what is required, please highlight your final answer.

Rubric

Description	Points
Question 1	**5**
Question 2 - 2 pts per entry	**10**
Question 3 - 2 pts per entry	**10**
Question 4 - 5 pts per classmate machine	**10**
Question 5	**10**
Question 6	**10**
Question 7	**10**
Question 8	**10**
Question 9 - 5 pts yes/no for seeing traffic, 10 pts explanation	**25**
Total	**100**

NMAP cheatsheet:

Nmap Target Selection

Scan a single IP	nmap 192.168.1.1
Scan a host	nmap www.testhostname.com
Scan a range of IPs	nmap 192.168.1.1-20
Scan a subnet	nmap 192.168.1.0/24
Scan targets from a text file	nmap -iL list-of-ips.txt

Nmap Port Selection

Scan a single Port	nmap -p 22 192.168.1.1
Scan a range of ports	nmap -p 1-100 192.168.1.1
Scan 100 most common ports (Fast)	nmap -F 192.168.1.1
Scan all 65535 ports	nmap -p- 192.168.1.1

Nmap Port Scan types

Scan using TCP connect	nmap -sT 192.168.1.1
Scan using TCP SYN scan (default)	nmap -sS 192.168.1.1
Scan UDP ports	nmap -sU -p 123,161,162 192.168.1.1
Scan selected ports - ignore discovery	nmap -Pn -F 192.168.1.1