Homework 2
Network Monitoring

1. Nmap 20%

Install Nmap in your machine:
https://nmap.org/book/install.html

Use the Nmap tutorial as a reference:
https://nmap.org/book/man.html

a) A very common way to scan a large list of IP addresses to see if they are "up" is to send ICMP pings to the hosts. Q: According to the tutorial, what happens when a host does not reply to an ICMP ping scan (i.e., what will Nmap try next?)

Now let us run some experiments.

Disclaimer: Scanning computers or IP addresses that are not owned by you can fire Intrusion Detection Alerts by the network monitoring those systems and can get you in trouble. You need to get permission to scan a computer that you do not own.

For this homework we will scan **scanme.nmap.org** (this server is managed by the Nmap project and allows users to scan it as long as the scans are not too intrusive) and your own computer.

Type the command:
```
nmap --help
```

b) Find the Nmap commands for:
- OS detection
- Service Detection
- Increased verbosity

and briefly explain what these commands do (in your own words).

c) Perform a scan with "Increased verbosity", "Service Detection", and "OS detection" to the host **scanme.nmap.org**. Screenshot the result of the scan and answer the following questions:

- What OS is the machine running (the best guess of Nmap)?
- Which ports does the machine have open?
- Which services (and their versions) is this machine providing?

d) Perform the same scan with the "**`localhost`**" domain (i.e., your machine). Screenshot the result of the scan and answer the following questions:
- What OS is your computer is running (according to Nmap)?
- Which ports do you have open?
- Which services (and their versions) is your machine running?

In your home network find the (private network) IP address of your router. (*If you do not have a home network then ignore this point and answer the last question of this homework instead*).

Now, assume the address of your router is **`192.168.0.1`** (if it is not, replace the following commands with the IP address of your router).

e) Perform the scan looking for computers active in the range **`192.168.0.1`** to **`192.168.0.5`** for example: "**`nmap -sP 192.168.0.1-5`**". What does this scan do? How many machines did Nmap find? (show a screenshot of the results).

2. Wireshark 20%

Wireshark can be downloaded from the following link:
https://www.wireshark.org

Documentation can be found in the following link:
https://www.wireshark.org/docs/wsug_html_chunked/

Most of the questions here can be answered by looking at the statistics menu of Wireshark.

Download the "**`swat_00027_20151126002110.pcap`**" file from eLearning.

a) Look at the Ethernet layer. What are the MAC addresses of all the communicating parties?

b) Look at the IPv4 addresses involved in the communications. Draw a network diagram showing which IP addresses are communicating with each other. (Hint: communications are happening via TCP and/or UDP).

c) List all the application-layer protocols that Wireshark identifies (the protocols on top of TCP and UDP), and give their frequency (% of packets of any protocol on top of TCP or UDP).

3. Capturing Packets 20%

Start Wireshark to capture packets in your own computer (and remember to stop capturing packets at the end of your homework!)

a) What is the IP address of your computer? Print a packet and show your IP address. (To print packets in Wireshark go to the "File" command menu option, and then select "Print..." and "Selected packet only". You can then save as a .pdf and import to your report).

b) Now in your favorite web browser go to **galaxy.utdallas.edu** and enter your username and password.
- Print the packets (and include a sample of the packets as part of your report) where you think your username and password are being sent.
- Can you see your username? Can you see your password? Explain why you can see your password or why you cannot see it.

c) Now download the syllabus for this course on my website while running Wireshark:
http://www.utdallas.edu/~jdv052000/cs6324/cs-6324-s19-syllabus_v2.pdf

- Find the packets where you see the **http** request. Right click the packet, and click "follow" and select "TCP stream". What do you see? Include sample of the packets in your report.

Clear "display filters" on Wireshark. Access the syllabus again using **https** (instead of **http**).

- Explain what happens.
- By the way, what was the IP address your computer accessed to download the syllabus? And what ports were used? (Answer for both the **http** and the **https** requests).

4. Video from NSA 10%

Please watch the video: https://www.youtube.com/watch?v=bDJb8WOJYdA

a) What are the six stage process for a successful attack? Provide a short one sentence description for each of these stages.

b) What are the three most popular tools for the initial exploitation phase?

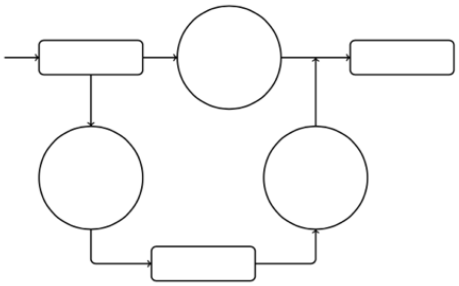
c) The speaker says the zero-day attacks NSA has are the main way to get into systems. True or False?

d) What is "Pass the Hash" vulnerability?

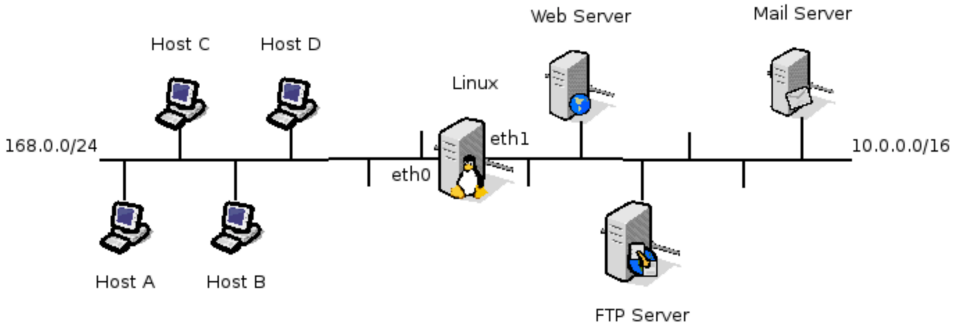
5. Firewalls: IPTables 20%

Use the Packet Filtering HOWTO as reference:
https://netfilter.org/documentation/HOWTO/packet-filtering-HOWTO.html

a) As explained in the HOWTO, fill the following figure and briefly explain each component:



Suppose you have the following network:



The IP addresses of the hosts and servers are the following:

- Host A: 192.168.0.10
- Host B: 192.168.0.11
- Host C: 192.168.0.20
- Host D: 192.168.0.21
- Linux eth0: 192.168.0.1
- Linux eth1: 10.0.0.1
- Web server: 10.0.0.10
- FTP server: 10.0.0.50
- Mail server: 10.0.0.180

Assume that, by default, all traffic is forbidden in the Linux router. Write the necessary **`iptables`** rules to allow the following:

a) Allow all the hosts in the 192.168.0.0/24 subnet to access the standard HTTP (80/tcp) and HTTPS (443/tcp) ports in the web server.

b) Allow host D to connect to the SSH (22/tcp) port of the Linux.

c) Allow the Linux router to connect to every server on every port within the entire subnet.

d) Allow hosts A and C to connect to the FTP server (21/tcp).

e) Allow hosts B and D to check their emails in the mail server (993/tcp, 995/tcp).

6. Snort 10%

Snort is an Intrusion Detection System (IDS) that uses signatures to identify malicious activity. Go to the Snort official documentation and take a look at chapter 3 (Writing snort rules).
https://snort.org/documents/snort-users-manual

a) Enumerate all the possible actions.

b) Write a Snort rule to look for SSH (port 22) login attempts for user **`root`**.

c) Given the following "ETERNALBLUE SMB installation return signal" payload (ff 53 4d 42 32 02 00 00 c0), write a Snort rule to detect this attack.

7. Snort (Do this point only if you do not have a home network to test the Nmap command from Question 1)

Go to the search rules website of snort:
http://www.snort.org/search

a) Search for: backdoor, icmp, finger and ms-sql. For each of these 4 keywords, describe two of the rules you found in the Snort website (i.e., 8 descriptions overall). In your explanation be sure to explain what exactly each rule is looking for.