Lab 3 Automation Breakdown  
CIS 450  
Krutarth Panchal

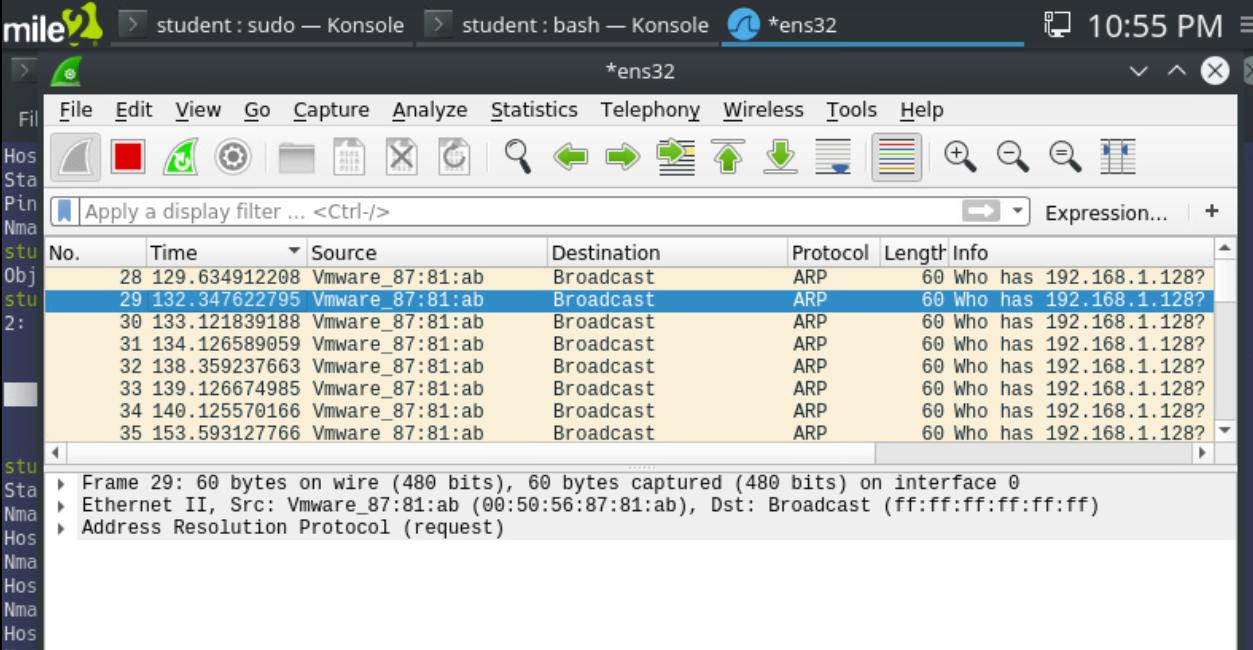
Section 1- Analyze the calls.

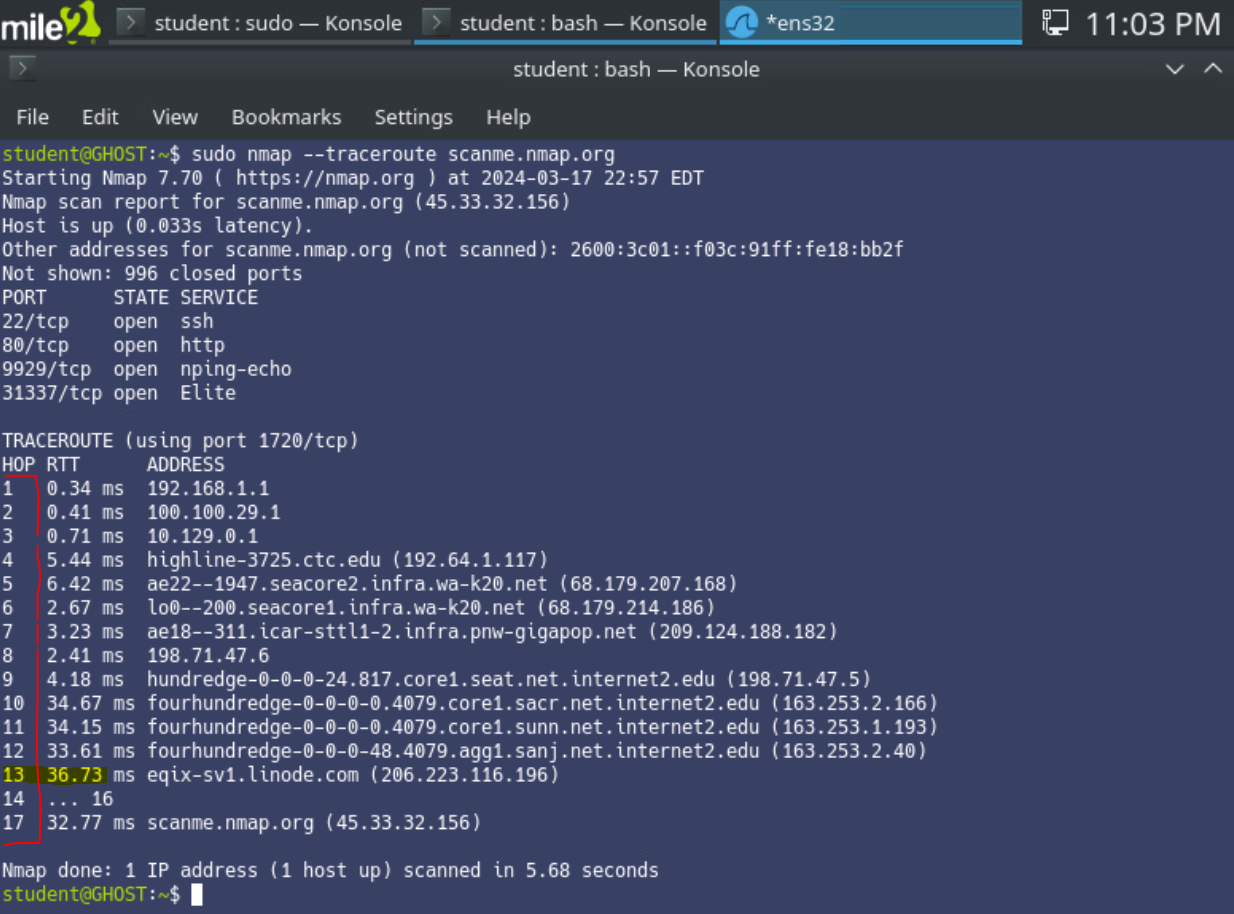
1. What is the ip address for your GHOST machine?  
   a. 192.168.1.121 (Fig 1.1)  
   command: ip addr show dev ens32  
   A screenshot of a computer

   Description automatically generated  
   (Fig 1.1)
2. What is the current MAC address for your GHOST machine?  
   - 00:50:56:87:1d:7b (Fig 1.1)  
   command: ip addr show dev ens32
3. What is the current subnet range that your GHOST machine is in?  
   a. Network IP: 192.168.1.0/24 (Fig 1.1)  
   b. Assignable range: 192.168.1.1 - 192.168.1.254 (Fig 1.1)  
   c. Broadcast IP:192.168.1.255 (Fig 1.1)  
   command: ip addr show dev ens32
4. What NMAP scan can you utilize to ping scan for your subnet?  
   A computer screen shot of a computer

   Description automatically generated  
   (Fig 1.2)  
   command: nmap -sn 192.168.1.0/24
5. Based on the results from NMAP scan you ran in step 4, what other network queries were performed?  
   A computer screen shot of a computer

   Description automatically generated  
   (Fig 1.3)  
   command: nmap -sn 192.168.1-51.0-255
6. How could you disable the additional network querries that were performed?  
   A screenshot of a computer

   Description automatically generated  
   (Fig 1.4)  
   by using the argument -n as shown in the Fig 1.4  
   command: nmap -sn -n 192.168.1.0/24
7. What are the IP addresses for the devices in your subnet?  
   a. Win7x86: 192.168.1.123  
   b. Ubuntu16: 192.168.1.122  
   c. Ubuntu14: 192.168.1.133
8. Using Wireshark in Ghost and capturing on any interface, re-run the command you ran in Question 3. Are the Ips scanned sequentially or at random?  
     
   (Fig 1.5)  
   Nmap is random while selected the Ips
9. Who is the primary DNS server in your subnet?  
   Primary DNS server doesn’t seem to show up on my wireshark instance.
10. What is the IP for scanme.nmap.org?  
    IP: 45.33.32.156  
    A screenshot of a computer program

    Description automatically generated  
    (Fig 1.6)  
    command: sudo nmap –traceroute scanme.nmap.org
11. Perform traceroute with Nmapto scanme.nmap.org. How many hops are there to the host? What’s the maxinmum latency for the route?  
       
    (Fig 1.7)  
    a. 17 hops  
    b. 36.73ms is maximum latency at hop 13.

Section 2 – Protocol Discovery and Enumeration

1. Windows has an inherit rule to block ICMP traffic. What switch option can be used so that Nmap will continue scanning without sending an ICMP ping to the host?  
   -command: sudo nmap -Pn 192.168.1.124  
   -“-Pn” tells nmap to treat all host as online and instructs to skip discovery. (refer “a” in Fig 2.1 in the screenshot below)  
   A screenshot of a computer

   Description automatically generated  
   (Fig 2.1)
2. After performing a TCP SYN scan on the Windows device in the network, what ports responded and what is their status?  
   -Refer to “b” in Fig 2.1 above it shows all the services that responded.  
   Port 135(mrpsc), Port 139(NetBIOS) and port 445(Domain services/SMB service) are some of the ports that are open.
3. After performing a TCP SYN scan on the Ubuntu 14 device in the network, what ports responded and what is their status?  
   -command: sudo nmap -Pn -sS 192.168.1.133  
   A computer screen shot of a computer program

   Description automatically generated  
   (Fig 2.2)  
   -Port 631 Internet Printing Protocol responded but it is in closed status as per as Fig 2.2.
4. After performing a TCP SYN scan on the Ubuntu 16 device in the network, what ports responded and what is their status?  
   command: sudo nmap -Pn -sS 192.168.1.122  
   A computer screen with text and numbers

   Description automatically generated

(Fig 2.3)  
- Mail service(smtp port 25), Web service(http port 80), RDBMS service(MySQL port 3306) are among few that responded and they are running in open status as per as Fig 2.3.

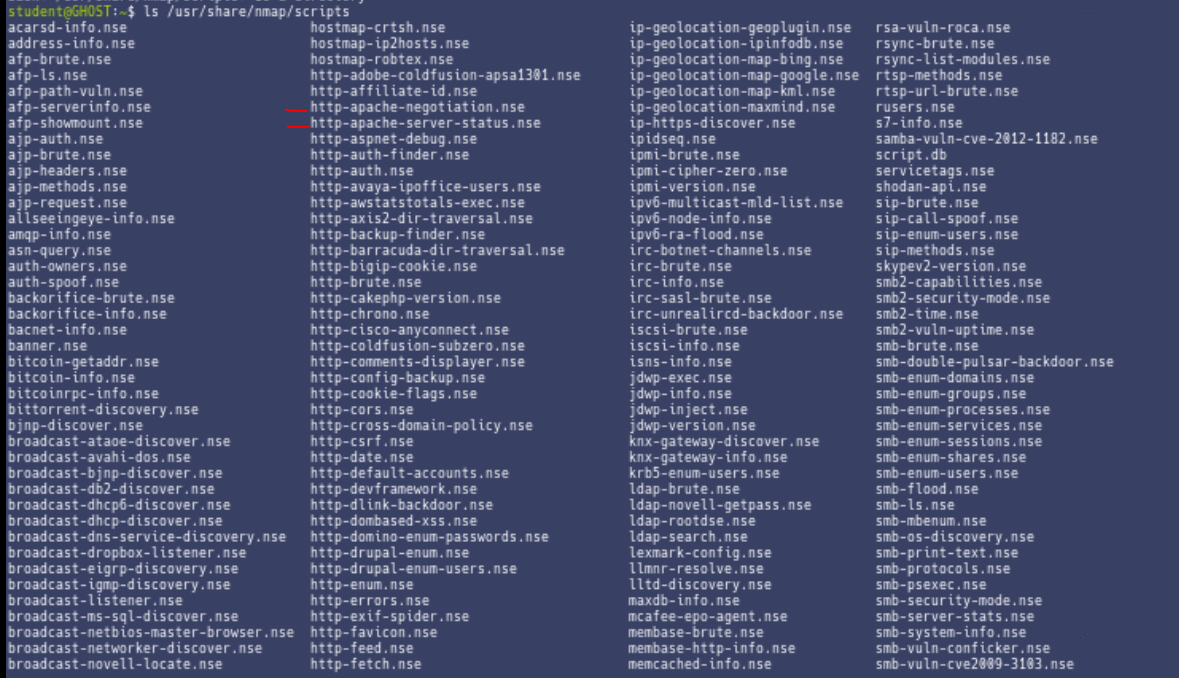
1. Perform an OS Detection Scan on the three host machines with a TCP SYN scan. What does Nmap say they are and what are they really?  
   command: sudo nmap -Pn -sS -O 92.168.1.124  
   A computer screen shot of a blue screen

   Description automatically generated  
   (Fig 2.4)  
   The above screenshot shows the OS detection scan of Windows machine, Nmap wasn’t able to identify the host as a Windows machine but there is Microsoft service port 445/tcp shows as open.
2. Using the Service Detection, what are the outputs for each port on Ubuntu 14?  
   command: sudo nmap -Pn -sS -O 192.168.1.133 -p 631  
   A screen shot of a computer screen

   Description automatically generated  
   (Fig2.5)  
   Fig 2.5 shows the result of nmap scanning on Ubuntu 14 (a) but nmap wasn’t able to identify service running on port 631(b) nor was it able to identify the OS version (c)
3. Using the Service Detection, what are the outputs for each port on Ubuntu 16?  
   command: sudo nmap -Pn -sS -O 192.168.1.122 -p 25,80,139,445,3306  
   A computer screen with red text

   Description automatically generated  
   (Fig 2.6)  
   Fig 2.6 shows the nmap scanning result for Ubuntu 16 where it was told to “-p) scan specific ports (a), this time nmap was able to identify services specifically MySQL service (b). Nmap wasn’t able to identify OS version but was able to suggest it is Linux based OS (c and d) in the screenshot.
4. Using the Service Detection, what are the outputs for each port on Windows 10?  
   command: sudo nmap-Pn -sS -O 192.168.1.124 -p 135,139,445,8000,8089  
   A computer screen shot of a computer

   Description automatically generated  
   (Fig 2.7)  
   Fig 2.7 shows the nmap scanning of Win10 machine where it was told to scan “-p” specific ports. It was able to identify services like msrcp for Windows remote procedure call, however it failed to identify exact OS version and it instead gave guesses that it could more than likely be a Windows OS host.
5. Based on the services found on Ubuntu 16, what NSE scripts could you run on each service?  
   command: locate \*.nse  
    ls /usr/share/nmap/scripts  
   A screenshot of a computer program

   Description automatically generated  
   (Fig 2.8)   
   Fig 2.8 shows the possible scripts that you can deploy against the Ubuntu 16 machine. I found various MySQL service related scripts that could be deployed against the victim’s machine.
6. Based on the services found on Ubuntu 14, what NSE scripts could you run on each service?  
   command: locate \*.nse   
    ls /usr/share/nmap/scripts  
     
   (Fig 2.9)  
   Fig 2.9 shows the various scripts that one can deploy against the Ubuntu 14 machine such as http Apache service related scripts that could be deployed against the victim’s machine.
7. Based on the services found on Windows 10, what NSE scripts could you run on each service?  
   command: locate \*.nse  
    ls /usr/share/nmap/scripts  
   A screenshot of a computer program

   Description automatically generated  
   (Fig 2.10)  
   Fig 2.10 shows the multiple scripts that one can deploy against the Windows 10 machine. I would use “win32” service related scripts such that could be deployed against the victim’s machine.
8. What Nmap switch option could you use to perform OS Detection, version scans and all of the scripts you’ve annotated in previous questions?  
   command: nmap –script “safe and default” 192.168.1.122  
   A computer screen shot of a blue screen

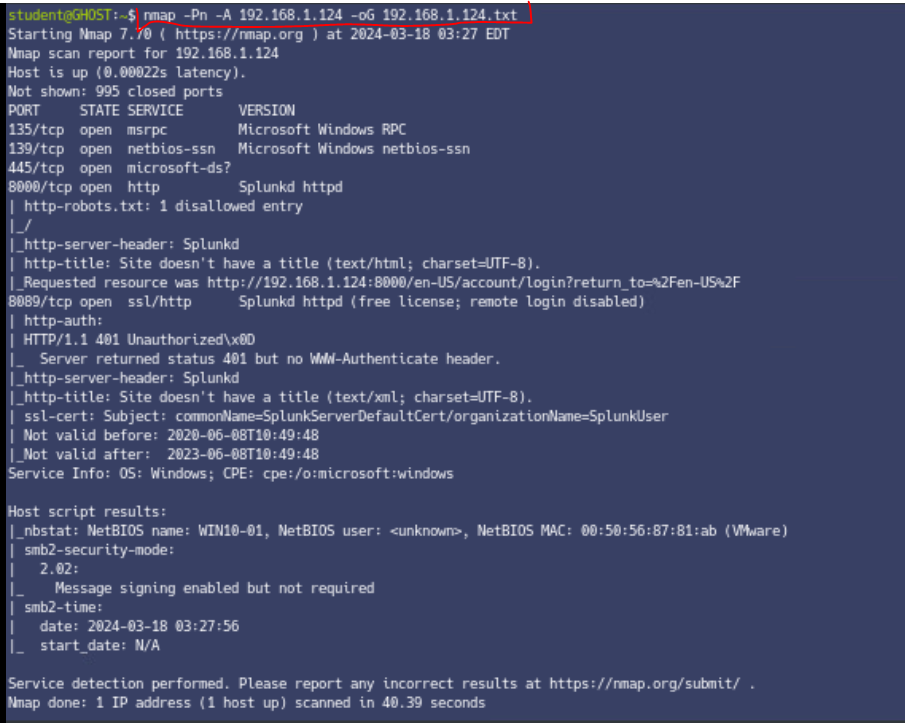
   Description automatically generated  
   (Fig 2.11)  
   Fig 2.11 indicates result of using script against one of the machines Ubuntu 16(a), where open ports smtp and http services are detected (b and c) and host script results are displayed OS detection, host name, account information and various other info(d).
9. Using the answer from Question 12, use it to scan “scanme.nmap.org”. Identify the Operating System, the services hosted, and any information that may seem important.  
   command: sudo nmap -A -Pn scanme.nmap.org  
   A screenshot of a computer program

   Description automatically generated  
   (Fig 2.12)  
   Fig 2.12 illustrates result of above command where following things were identified:  
   a. IP address: 45.33.32.156  
   b. Open ports with services open: Port 22 ssh and 80 http.  
   c. OS guesses: nmap believes that victim’s machine is Linux based OS.  
   d. Hops: The victim’s machine is 17 hops from offensive machine.

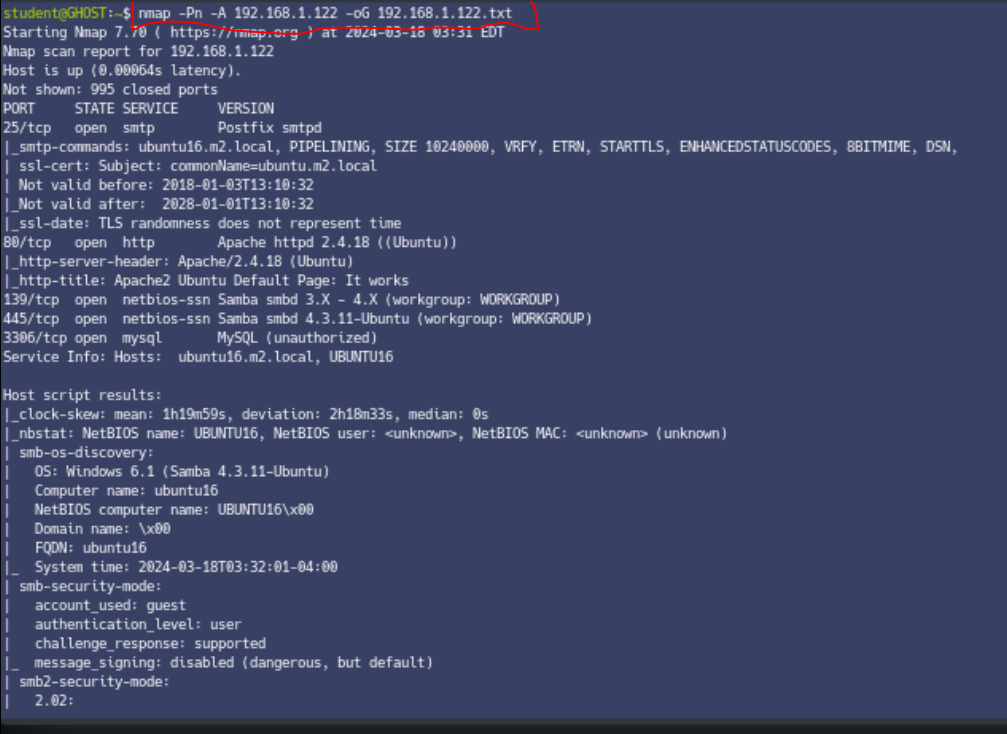
Section 3 and 4- Linux NMAP Automation.  
  
Nothing needed for Section 3 as per as instructions.

Section 4: Automation, Network Enumeration and Network Diagram

a. Automation script for Windows 10  
command: nmap -Pn -A 192.168.1.124 -oG 192.168.1.124.txt

(Fig 4.1)

b. Automation script for Ubuntu 16  
command: nmap -Pn -A 192.168.1.122 -oG 192.168.1.122.txt

  
(Fig 4.2)

c. Automation script for Ubuntu 14  
command: nmap -Pn -A 192.168.1.133 -oG 192.168.1.133.txt

A screenshot of a computer

Description automatically generated  
(Fig 4.3)

2. Enumeration/Table:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **MAC Address** | **IP Address** | **Hostname** | **OS** | **Open Ports** | **Closed Ports** | **Filtered Ports** | **Possible**  **Exploits** | **Notes** |
| 00:50:56:87:81:ab | 192.168.1.124/24 | WIN10-01 | Windows | 135,139,445,8000 | None identified by Nmap | None identified by Nmap | None identified by Nmap | Need to identify exploits |
| Not found by nmap | 192.168.1.122/24 | UBUNTU16 | Windows 6.1 (Samba 4.3.11-Ubuntu) | 25 | None identified by Nmap | None identified by Nmap | None identified by Nmap | Need to identify exploits |
| Not found by Nmap | 192.168.1.133/24 | Unidentified by Nmap | Unidentified by Nmap | None identified by Nmap | 631 | None identified by Nmap | None identified by Nmap | Need to identify exploits |

- Above is the Network table as detected by Nmap from Ghost security machine.

3. Network Diagram  
  
A diagram of a cloud router

Description automatically generated

(Fig 4.4)  
Above is the Network diagram as detected by GHOST Security system.

----------------------------------------------End of Lab---------------------------------------------------