Lab2: Assignment + Tool

William Fan, Danielle Santos Almeida, Jose Marvin Garcia

Montgomery College

NWIT 246 - Simulated Network Scanning.

Prof. Vargas

9/13/25

**Part 1: Reading & Written Report**

**Task A:** Scanning and Initial Access

1. What is network scanning, and why do attackers like Salt Typhoon use it?

Network scanning is basically a way to explore what is running on a network. Attackers send probes to computers and devices to see which ones respond, what ports are open, and what services are active. In other words, it is like shaking all the doors in a building to see which ones are unlocked.  
 Groups like Salt Typhoon use scanning because it helps them prepare their attacks. Instead of blindly guessing, scanning gives them a map of the network so they can decide where to focus. If they find a server running old software or a system exposed to the internet, they know they might be able to use it as their way in. This makes their attacks faster, more targeted, and more likely to succeed. According to the August 2025 advisory on Salt Typhoon, “the group relies on scanning exposed services as the foundation of its operations” (Medium). This shows that reconnaissance is not just a preparation step but a deliberate strategy attackers use to minimize risk and increase their success rate.

2. What kinds of devices or systems do they look for when scanning?

Salt Typhoon doesn't just look for any machine—they go after systems that can give them access or control. Examples include:

* Servers such as email, web, and file servers, because these are critical and often face the internet.
* Network devices like routers, firewalls, and VPN gateways, which can open the door to internal systems if they are misconfigured.
* Windows domain controllers, since taking control of Active Directory usually means controlling the whole network.
* IoT or industrial devices, which often run outdated software and are harder for defenders to secure.

In short, attackers are not only interested in what exists but also in what is weak and valuable. The advisory specifically pointed out that Salt Typhoon often searches for “unpatched VPN appliances and vulnerable Microsoft Exchange servers” (*Medium*). These systems are attractive because they sit at the edge of networks and, once compromised, provide attackers with a direct path into sensitive internal resources.

3. What tools do they likely use to scan networks?

Attackers have plenty of tools available, and many of them are free to download. The most common one is Nmap, which is used by both security professionals and hackers to find open ports and running services. Another tool, Masscan, is known for its speed and can scan very large networks quickly. There are also simpler tools like Angry IP Scanner, and even search engines like Shodan, which lets attackers look up devices already exposed to the internet. Researchers have even shown that Masscan can “scan the entire Internet in under six minutes,” which explains why state-sponsored groups value it for large-scale reconnaissance. Combined with Nmap’s detail-oriented scans, this pairing gives attackers both speed and precision.

**Task B: What Happens After Scanning?**

1. List 2–3 other actions Salt Typhoon takes after scanning.

After completing network scans, Salt Typhoon typically performs follow-up actions that help them gain persistence and access to sensitive data. Some of the most common actions include:

* Credential theft, such as stealing usernames, passwords, or authentication tokens.
* Lateral movement, which means using stolen credentials or network trust relationships to move into more important systems.
* Data exfiltration, where they transfer valuable information out of the victim’s network to attacker-controlled servers.

These steps are critical because scanning alone does not give them control. The real damage happens in the stages that follow, when the attackers start exploiting what they discovered.

2. Pick two and explain how it helps them stay hidden or steal information.

* Credential theft: If attackers steal usernames and passwords, they can log in like a normal user. This means they don’t always need malware to stay inside the system, which makes them harder to notice. It also gives them long-term access because stolen accounts can be reused later.
* Lateral movement: With those stolen credentials, attackers move to more important systems. For example, they might start on a small server and then use remote tools like RDP to jump to a domain controller. Since admins also use these same tools, the attacker’s activity blends in with daily operations, which keeps them hidden.

3. Why is it harder to detect attackers who 'live off the land'?

When attackers 'live off the land,' they don’t bring in obvious malware. Instead, they use tools already built into the system, like PowerShell or Windows Command Prompt. Security programs see these tools running all the time, so the attacker’s activity doesn’t immediately stand out.

The problem for defenders is that the logs look normal, and it’s difficult to tell the difference between a real admin doing work and an attacker misusing the same commands. This method is one of the reasons state-sponsored groups like Salt Typhoon are so dangerous—they can quietly sit inside networks for months without anyone realizing it.

**Task C: MITRE ATT&CK Mapping**

1. Choose 2 attacker techniques used by Salt Typhoon: We chose 1) Initial Access 2) Credential Access/Persistence

2. Write an explanation of how each technique was used based on the article and fill in this table:

| **Tactic** | **Technique Name** | **Technique ID** | **Explanation** |
| --- | --- | --- | --- |
| Initial Access | Exploit Public-Facing Application | T1190 | P1 |
| Credential Access / Persistence | Network Sniffing | T1040 | P2 |

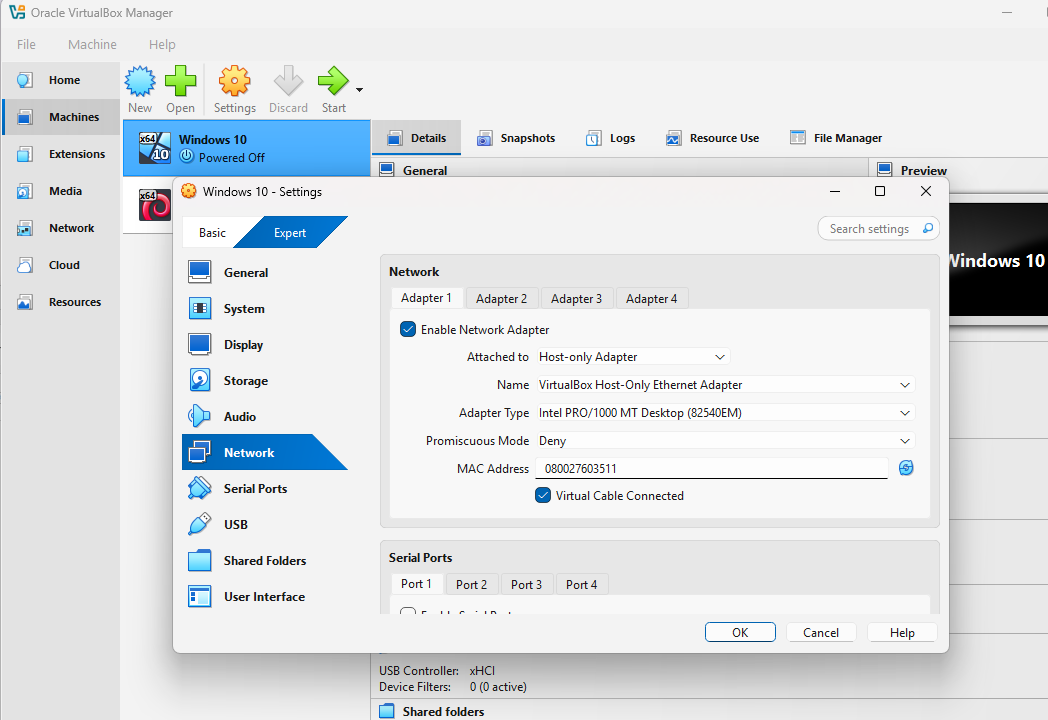
P1: Exploit Public-Facing Application tactic is a type of attack under Initial Access. It involves opponents exploiting vulnerabilities in web servers, databases, VPN appliances, or any other device that provides entry into the targeted network. To put it simply, tools such as Burp Suite, Metasploit Framework and SQL map can be used to do such an attack. All these facilities are called internet-facing systems. The weaknesses can be zero-day vulnerabilities, known bugs, misconfigurations, or outdated drivers. Once breached/exploited, attackers can use this as a foot in the door to move deeper into the environment. This could potentially cause greater damage and allow access to more sensitive information. This technique has been observed in real-world groups like APT28, APT29, and HAFNIUM (MITRE ATT&CK). This illustrates its continued relevance as a common method of gaining unauthorized access.

P2: Network Sniffing falls under the Credential Access tactic category. Adversaries may employ network sniffing tools to capture packets transmitted across a local network. For example, using monitor mode in Wireshark, as demonstrated in NWIT 245, is one method of performing network sniffing. This technique enables adversaries to collect sensitive information during transmission, including usernames, passwords, cookies, or configuration details. In certain cases, attackers can also capture encrypted traffic for later offline decryption. The credentials obtained through network sniffing may then be used to escalate privileges, maintain persistence, and evade detection during routine security scans.

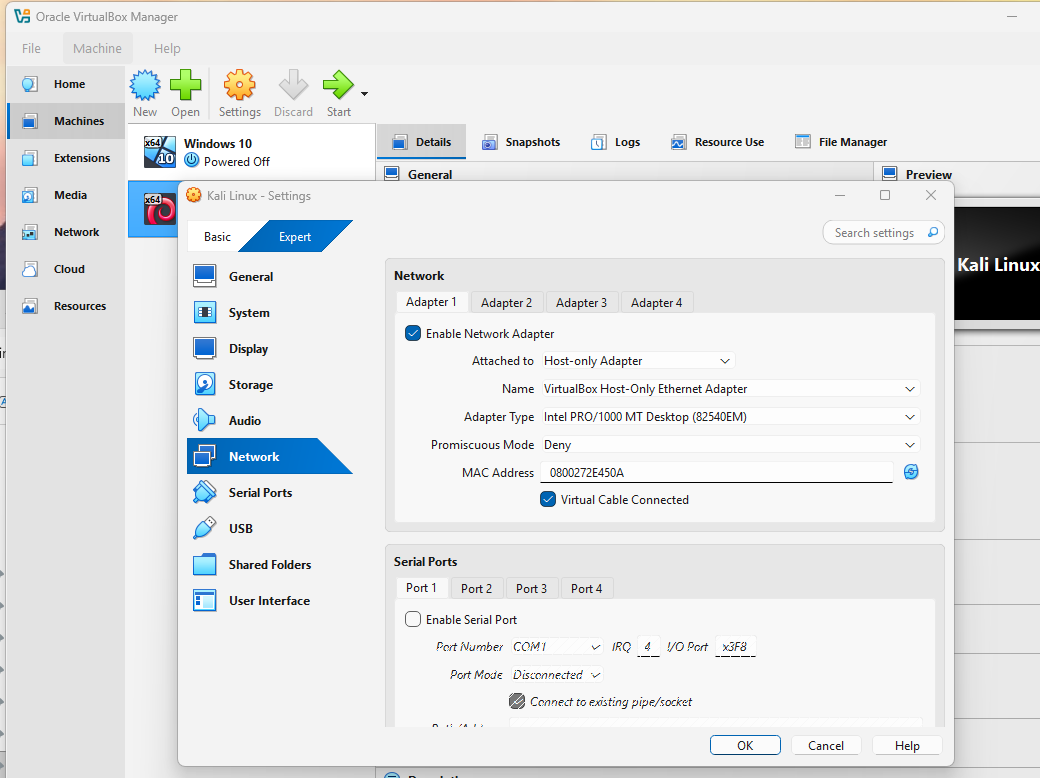
**Part 2: Hands-On Lab – Simulated Network Scanning**

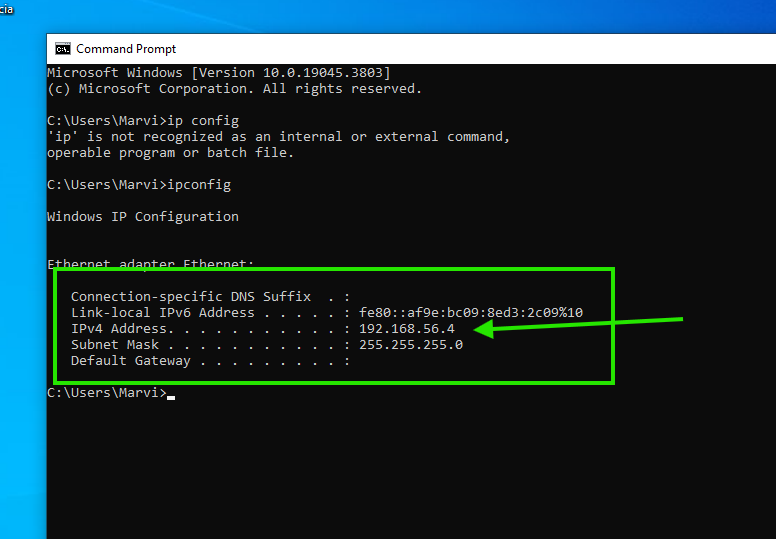
In this lab, we simulated an attack using scanning tools such as Nmap to demonstrate how attackers use this method. To do this, we used VirtualBox with two virtual machines: one running Windows 10 and the other running Kali Linux. Windows 10 served as the target machine, whereas Kali Linux acted as the attacker. So the first step is to network configuration. We want both machines in the same network so Nmap can work.

Screenshot 1 - Windows 10 network:

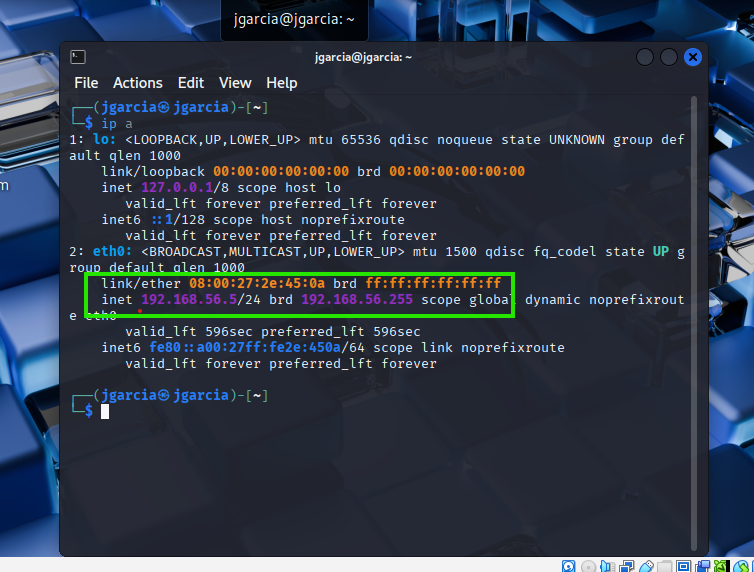


Screenshot 2 - Kali Linux network:



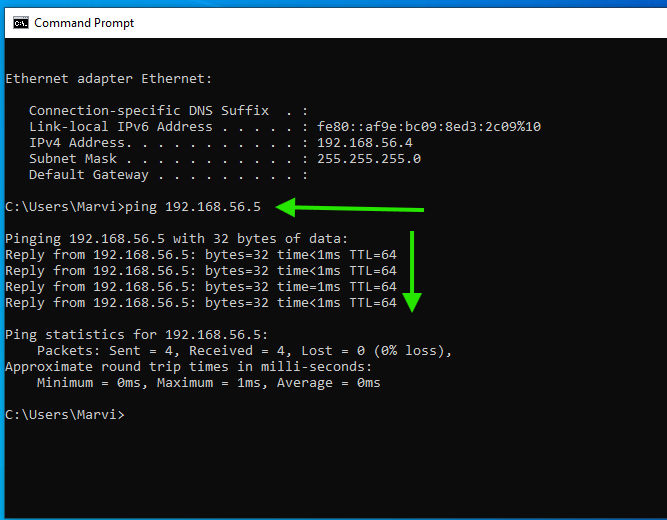
Screenshot 3 - After configuring both machines to the same network, we run the Windows 10 machine first and open the command prompt. Then we type ipconfig to find our IPV4 address: our windows 10 machine IPv4 address is: 192.168.56.4:

Screenshot 4 - Next, we run the Kali Linux machine and follow the same steps to find the IPv4 address. We open terminal and type “ifconfig” or “*ip a”*:

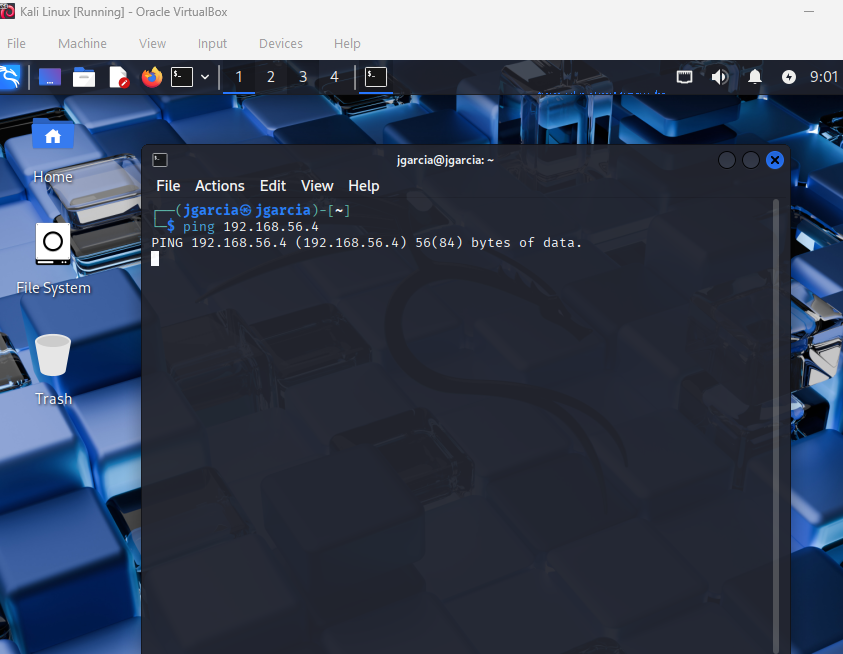


To verify that our PC and Kali Linux were correctly configured on the same network, I pinged the IPv4 address in each machine to show that they can communicate. Successful replies confirmed that the machines were able to communicate at the network level..

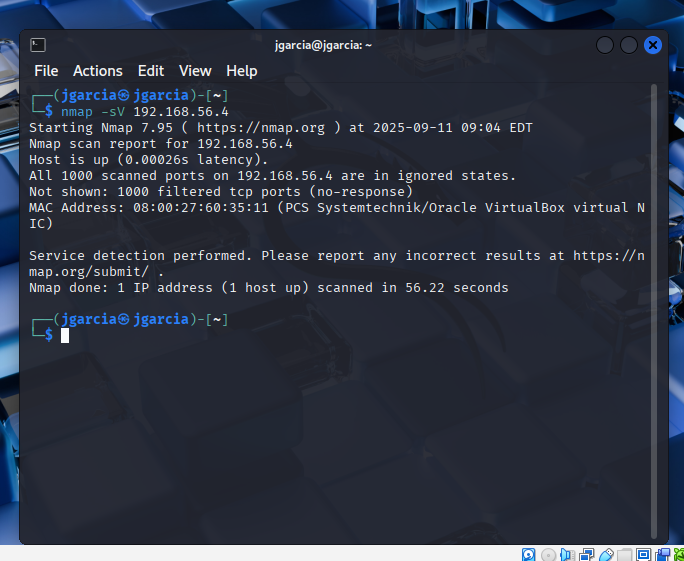
Screenshot 5 - Windows 10 is able to ping Kali Linux:



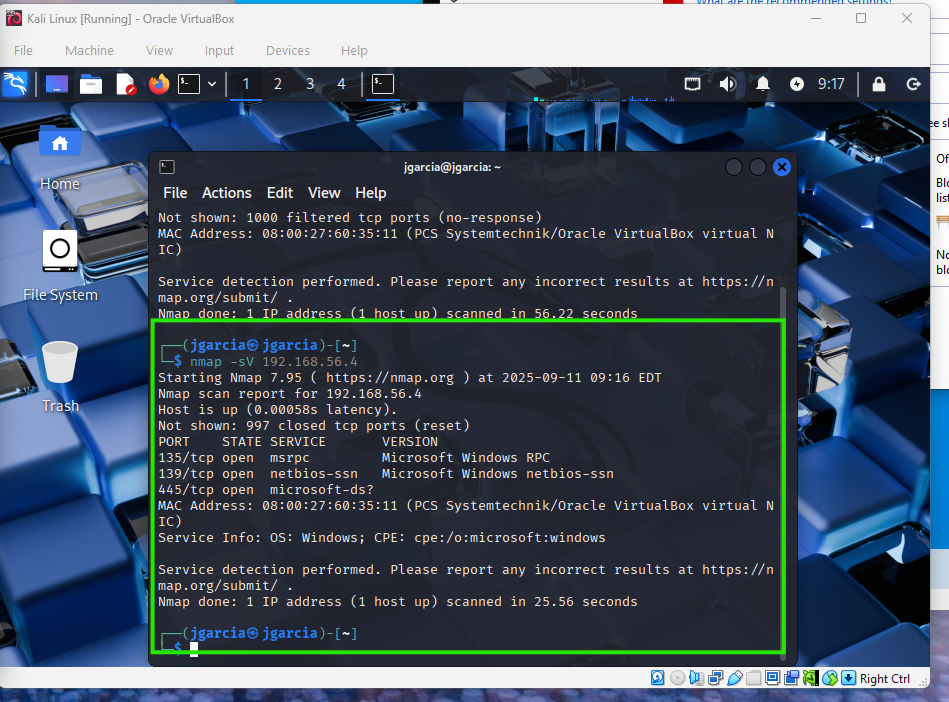
Screenshot 6 - Kali Linux is able to ping Windows 10:



Screenshot 7 - After making sure both machines are on the same network, we run the basic scan using nmap on Kali. We open the“terminal” to scan our target machine (Windows 10) and run the command “nmap -sV 192.168.56.4”: The -sV flag is used to identify the versions of services running on open ports, which helps determine whether the target is running outdated or vulnerable software. For example, if the output indicates an Apache HTTP server version that is known to have vulnerabilities, it can be cross-checked for potential exploitation.



As seen on the screen above, we found no open ports and all scanned ports are filtered. This is due to the firewall blocking.

Screenshot 8 - However, we disabled the firewall on the windows 10 machine by Control Panel → System and Security → Windows Defender Firewall and compared the results. We did the command again (nmap -sv 192.168.56.4) and was able to have results.

Observations:

After turning off the firewall on Windows 10, these open ports were found:

| **Port** | **State** | **Service** | **Version/Info** |
| --- | --- | --- | --- |
| 135 | open | msrpc | Microsoft Windows RPC |
| 139 | open | netbios-ssn | Microsoft Windows netbios-ssn |
| 445 | open | microsoft-ds | Microsoft Windows |

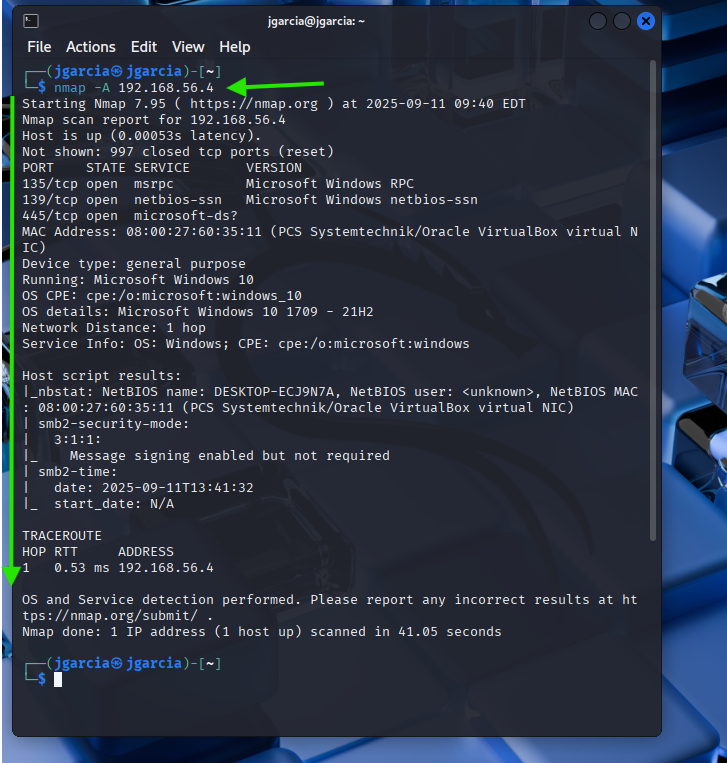
**What MITRE ATT&CK technique does this scanning activity map to?**

MITRE ATT&CK mapping for this scan:

* **Tactic:** Reconnaissance
* **Technique Name:** Network Scanning
* **Technique ID:** T1046

Performed an Nmap scan to identify open ports and running services on the Windows 10 host, discovering potential attack surfaces.

Screenshot 9 - Went back to do a deep scan using the command (on Kali Linux) “nmap -A 192.168.56.4”. The -A option enables aggressive scanning, which not only detects open ports and service versions but also attempts OS detection, script scanning, and traceroute. This provides more detailed information about the target system. Specifically, it identified the operating system, the device type, the NetBIOS name of the host, SMB protocol information and a traceroute showing the network path.



**Are any of them outdated or potentially vulnerable?**

Yes, based on the Nmap scan we can tell that port 445 (SMB) can be potentially vulnerable. In addition, the NetBios are services that attackers would get access to if they aren’t configured properly.  
 **If you were an attacker, which service might you explore first and further investigate?**

If we were an attacker, we would attack/explore port 445 (SMB), simply because this port is known for its vulnerabilities and the common attacks that it experiences.

**Analysis**:

In this lab, we performed network scanning on the Windows 10 Virtual Machine using Nmap. The basic scan (-SV) identified three open ports: 135 (MSRPC), 139 (NetBIOS-SSN), and 445 (SMB), showing that common Windows services were running. The detailed scan (-A) provided additional information, including the OS version (Windows 10 1709 – 21H2), device type, NetBIOS name, and SMB2 security settings. These results demonstrate how attackers can gather information about open ports, services, and host details to identify potential attack vectors. Port 445 (SMB) would likely be a primary target due to its common vulnerabilities. This scanning activity maps to the MITRE ATT&CK framework under Reconnaissance (T1046), as it involves identifying open ports and services. Overall, Nmap allowed me to see how reconnaissance helps attackers plan further actions and highlights why defending network services and monitoring scanning activity is important.

**Part 3: Reflection – Defending Against Scanning and Attacks**

**How could a company detect / block scanning activity?**  
 A company can detect scanning activity by monitoring for unusual traffic patterns with IDS tools such as Snort or Suricata. A modern Next Generation Firewall (NGFW) from vendors like Cisco, Dell, or SonicWall can provide similar functionality. For example, repeated connection attempts to many ports in a short time often indicate that an Nmap scan is in progress. Firewalls can also be configured to limit or block excessive requests from a single IP address—for instance, allowing a maximum of 60 scans per device per second. This reduces the chance of successful reconnaissance. Security teams can also enable logging on routers and switches to spot irregular behavior. In addition, tools such as honeypots can be deployed to attract attackers and detect scanning attempts early. By combining IDS, NGFWs, log analysis, and honeypots, a company can detect and block reconnaissance before it escalates into an attack.

**What steps could stop attackers like Salt Typhoon after they scan the network?**

First, companies should immediately limit exposed services. Unnecessary services or ports like Telnet and FTP should be blocked. Only necessary ports and critical services should be protected with authentication and encryption. Network segmentation can isolate sensitive systems so that even if one host is scanned or compromised, the rest of the network remains safe. Secondly, patching systems regularly ensures that vulnerabilities exposed during scanning are fixed. Endpoint Detection and Response (EDR) tools can also provide alerts when attackers attempt lateral movement. According to Heimdal Security, “Endpoint Detection and Response tools can support proactive threat hunting by providing real-time visibility, automated detection, and powerful analytics to uncover hidden threats.” This can act as a great method to stop the attackers.

**Works Cited:**

“Countering Chinese State-Sponsored Actors: Salt Typhoon.” *Medium*, 12 Aug. 2025, <https://medium.com/h7w/countering-chinese-state-sponsored-actors-af22ecb89371>.

Easton, Chuck. *Network Defense and Countermeasures: Principles and Practices.* 5th ed., Pearson, 2022.

ESET. “EDR Killers Get Popular. Here Is How to Stop Them.” *ESET Corporate Blog*, 27 Mar. 2025, <https://www.eset.com/us/about/newsroom/corporate-blog/edr-killers-get-popular-here-is-how-to-stop-them/>.

Heimdal Security. “How to Use EDR for Advanced Threat Hunting (With Real Examples).” *Heimdal Security*, 27 July 2025, <https://heimdalsecurity.com/blog/how-to-use-edr-for-advanced-threat-hunting/>.

*MITRE ATT&CK*. MITRE Corporation, <https://attack.mitre.org/>.

MITRE ATT&CK. “Exploit Public-Facing Application (T1190).” MITRE ATT&CK Enterprise [Matrix, MITRE, 15 Apr. 2025, attack.mitre.org/techniques/T1190/](http://attack.mitre.org/techniques/T1190/).