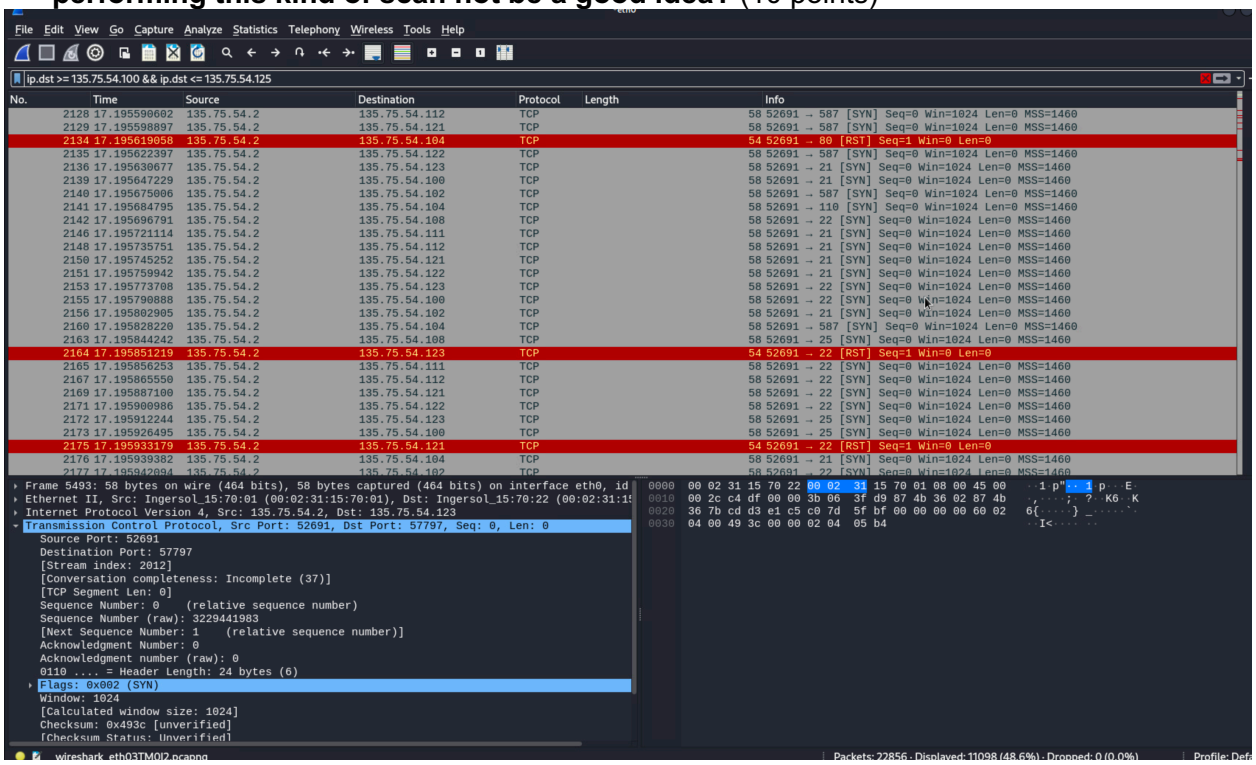
Lab 02 Template – Ethan Roepke

1) **Read the man pages of nmap. What nmap flag run a scan without performing a ping scan first?** (10 points)
   -Pn

2) **Examine the Wireshark output. How many packets were generated? Why might performing this kind of scan not be a good idea?** (10 points)



This is the filter I used since I did not know of a better filter to use. I scrolled through all the packets after filtering which was roughly 11000 packets when doing Nmap scan. Performing this kind of scan is not a good idea because it scanning a wide range of IP addresses can cause large amounts of network traffic which can disrupt normal operations and trigger alarms. As well as scanning a large range at a time can give inaccurate results. Some devices may not respond while others may respond with inconsistent responses.

3) **Submit your table for enumerating ports, services, and operating systems**(10points)

HOST	OPEN PORTS	Services	OS Guess(1)	OS Guess (1) Reason	OS Guess(2)	OS GUESS(2) Reason	OS by nmap
135.75.54.100	135	msrpc	Windows OS networking	These ports are used for SMB protocol whcih is used with file sharing	Windows XP	Port 445 tells us the version is windows XP	Windows XP
	139	netbios-ssn					
	445	microsoft-ds					

HOST	OPEN PORTS	Services	OS Guess(1)	OS Guess (1) Reason	OS Guess(2)	OS GUESS(2) Reason	OS by nmap
135.75.54.102	7	echo	Windows 9	port 445/139 gives us a hint that its a microsoft version	Windows 9	Port 445 lets us know that its a version between 7 and 10	Windows 10
	9	discard					
	13	daytime					
	17	qotd					
	19	chargen					
	80	http					
	135	msrpc					
	139	netbios-ssn					
	445	microsoft-dns					
	515	printer					
	2179	vmrdp					
	8088	randan-http					

HOST	OPEN PORTS	Services	OS Guess(1)	OS Guess (1) Reason	OS Guess(2)	OS GUESS(2) Reason	OS by nmap
135.75.54.104	22	ssh	Linux	Because port 22 is open and port 80/443 not associated to OS systems	Linux	Port 22/80/443 lets us know its Ubuntu and Ubuntu is in Linux	Linux 2.6.x|3.x
	80	http					
	443	https					

HOST	OPEN PORTS	Services	OS Guess(1)	OS Guess (1) Reason	OS Guess(2)	OS GUESS(2) Reason	OS by nmap
135.75.54.106	80	http	Windows 8	Ports 135/139/445 so associated with a windows OS system	FreeBSD	Both ports let us know the version is FreeBSD	FreeB 6.x
	135	msrpc					
	139	netbios-ssn					
	445	microsoft-ds					

HOST	OPEN PORTS	Services	OS Guess(1)	OS Guess (1) Reason	OS Guess(2)	OS GUESS(2) Reason	OS by nmap
135.75.54.108	135	msrpc	Windows microsoft OS	ports 135/139/445 all associated with microsoft and could be a variety of windows versions	Windows 8	Port 445 gives us a version range from 7-10	Windo 10
	139	netbios-ssn					
	445	microsoft-ds					

HOST	OPEN PORTS	Services	OS Guess(1)	OS Guess (1) Reason	OS Guess(2)	OS GUESS(2) Reason	OS by nmap
135.75.54.111	135	msrpc	Windows 10	All ports associate to windows and guessing widows 10 becasue port 3389 is remote access	Windows 10	More ports used from .111 and knows its a windows version 7-10 given from port 445	Windows 10
	139	netbios-ssn					
	445	microsoft-ds					
	3389	ms-wbt-server					
	5357	wsdapi					

HOST	OPEN PORTS	Services	OS Guess(1)	OS Guess (1) Reason	OS Guess(2)	OS GUESS(2) Reason	OS by nmap
135.75.54.112	22	ssh	macOS	Port 80 doesnt matter and port 22 is open and associated with a unix like system	Linux	port 22 lets us know its Ubuntu therefore is is a version of linux	Linux 4.x|5.x
	80	http					

HOST	OPEN PORTS	Services	OS Guess(1)	OS Guess (1) Reason	OS Guess(2)	OS GUESS(2) Reason	OS by nmap
135.75.54.121	22	ssh	macOS	has same ports as .112 and not sure what else it could be besides macOS or linux	Linux	port 22 lets us know its Ubuntu therefore is is a version of linux	Linux 4.x|5.x
	80	http					

HOST	OPEN PORTS	Services	OS Guess(1)	OS Guess (1) Reason	OS Guess(2)	OS GUESS(2) Reason	OS by nmap
135.75.54.122	22	ssh	BSD	port 22 gives me hint its some Unix-like system and port 8089 is used to allow outbound network connections to specified IP subnets	Linux	port 22 lets us know its Ubuntu therefore is is a version of linux	Linux 4.x|5.x
	8089	unknown					

HOST	OPEN PORTS	Services	OS Guess(1)	OS Guess (1) Reason	OS Guess(2)	OS GUESS(2) Reason	OS by nmap
135.75.54.123	22	ssh	FreeBSD	Its a unix-like OS system but port 10000 gives me a hint that it might be FreeBSD because it is used for web based tools	Linux	port 22 lets us know its Ubuntu therefore is is a version of linux	Linux 4.x|5.x
	10000	snet-sensor-mgmt					

4) **For each host answer the following:** (10 points)

a) Were either of your guesses accurate in guessing the OS?

The two guesses I got right came from .104 and .111
I was able to figure out if they were associated with Microsoft so most of those were close but I didn't have enough information to decide with version it was at first.

b) Why might it be valuable to determine operating systems without performing an nmap scan?

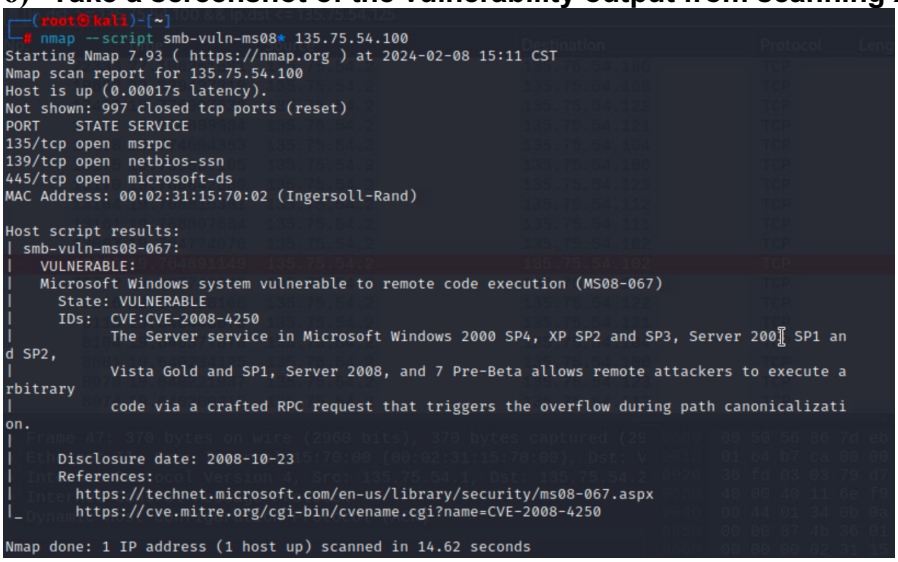
To determine OS systems without using an Nmap is valuable for many reasons and the biggest reason is avoiding a Nmap Detection/IDS if the network administrative and monitor it regularly. As well as running Nmap scans, it consumes CPU and memory both on scanning machines and the target network does not keep the attacker stealth.

5) **List three ways and/or options you might use nmap such that alarms are less likely to be raised** (10 points)

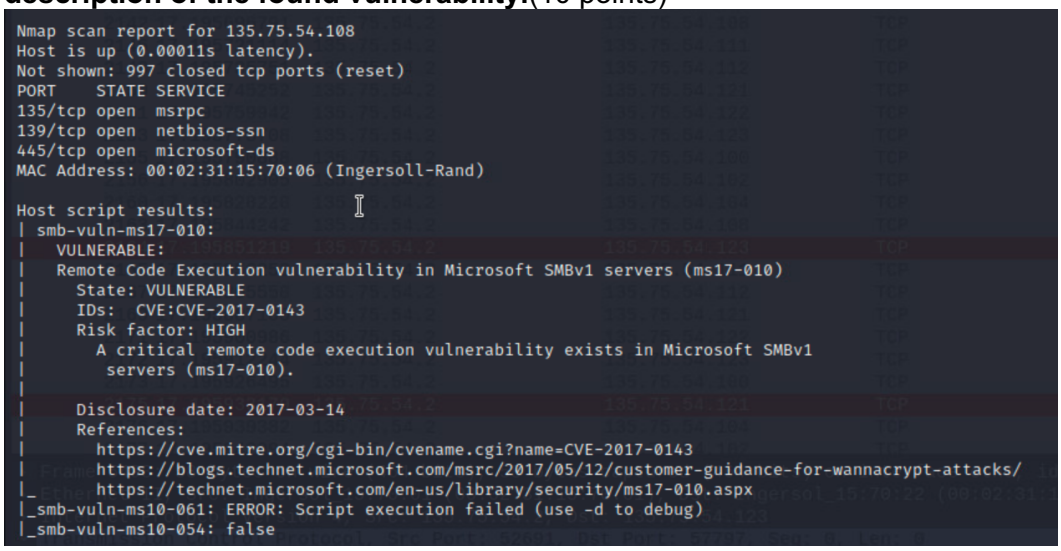
a. Using "- -scan-delay" will increase the time between scans. As well as using the "- -max-retries" which will reduce the amount of times it attempts a scan again. This will make the scans less noticeable and mitigate the risk of detection.
b. Nmap offers many options for stealthy scanning, including '-sS' (TCP SYN) , '-sA' (TCP ACK), '-sF' (TCP FIN). Using these three techniques send TCP packets that will be less likely detected by security measures compared to other methods.

c. Instead of using default scan options that are in Nmap, we could use '-p' which will specify specific ports. This will make the scans more focused and will not as likely alert the detection system.

6) **Take a screenshot of the vulnerability output from scanning X.X.X.100** (10 points)



7) **Find at least one other vulnerability using NSE and include a screenshot and a short description of the found vulnerability.**(10 points)

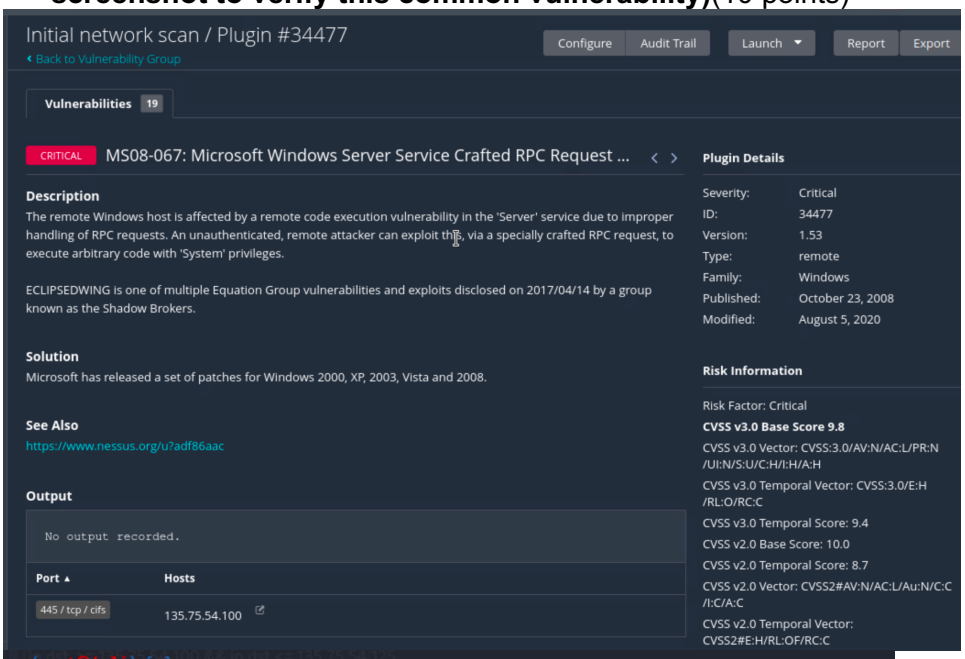


I ran nmap "--script smb-vuln-ms* 135.75.54.100-125" which will target vulnerabilities related to SMB protocols. I added '*' so "smb-vuln-ms" can execute multiple SMB detection scripts. I found a Vulnerability in 135.75.54.108 which is "smb-vuln-ms17-010". This detects if a Microsoft SMBv1 server is vulnerable to a remote code execution vulnerability.

8) **Look at the traffic captured in Wireshark and comment on what types of packets and different protocols are being used.** (10 points)

The type of packets we are receiving on wireshark is basically all of them. This is including TCP SYN/ACK Packets, UDP packets, ARP requests, ICMP requests, and many more that I could have missed. They send so many different protocols and packets because Nessus will port scan to identify what ports are open, packets to avoid IDS, send packets to discover live hosts. Nessus does this to gather as much information to identify vulnerabilities, information about security, and security posture of networks.

9) **Comment on a vulnerability that is common betwe ren NSE and Nessus (include screenshot to verify this common vulnerability)**(10 points)




```
┌──(root㉿kali)-[~]
└─# nmap --script smb-vuln-ms08* 135.75.54.100
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-08 15:11 CST
Nmap scan report for 135.75.54.100
Host is up (0.00017s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:02:31:15:70:02 (Ingersoll-Rand)

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 200[I] SP1 an
d SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute a
rbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalizati
on.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250

Nmap done: 1 IP address (1 host up) scanned in 14.62 seconds
```

This is a found vulnerability on .100 and I found this same vulnerability using NSE. This vulnerability allows remote attackers to execute arbitrary code by sending a specially crafted

RPC request that triggers a buffer overflow during path canonicalization. If the attacker is successful, they can gain unauthorized access to the system and execute malicious code.

10) **List 2-3 additional vulnerabilities that interest you and make a note of their CVE and which hosts they were found on**(10 points)
    a. Webmin 1.890 - 1.920 Remote Command Execution was found on .123
       CVE-2019-15107
       The Webmin install hosted on the remote host is affected by a remote command execution vulnerability.

    b. Apache < 2.4.49 Multiple Vulnerabilities was found on .106
       CVE-2021-40438
       The version of Apache httpd installed on the remote host is prior to 2.4.49.

    c. MS08-067: Microsoft Windows Server Service Crafted RPC Request found on .100
       CVE-2008-4250
       The remote Windows host is affected by a remote code execution vulnerability in the 'Server' service due to improper handling of RPC requests.