Project-03 Enumeration and Scanning  
Working on Stapler: 1

Jose Ramirez

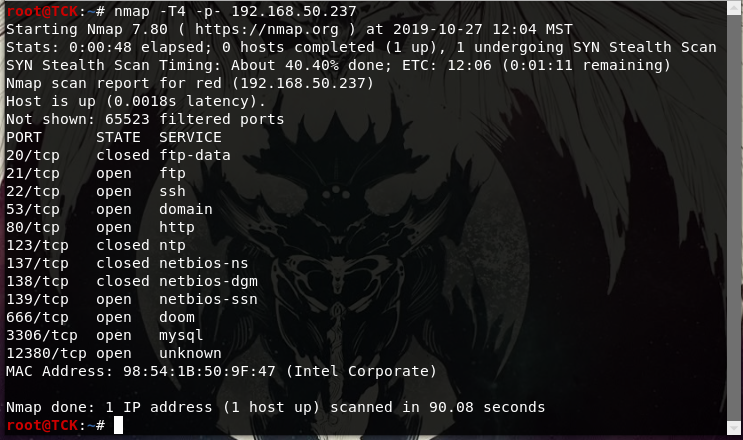
University of Advancing Technology

Project-03 Enumeration and Scanning  
Working on Stapler: 1

# Part 1:

1. **Port scan the hosts in scope with Nmap.**
   1. **If you have more than 10 hosts, only provide the results of the 10 with the most ports open.**

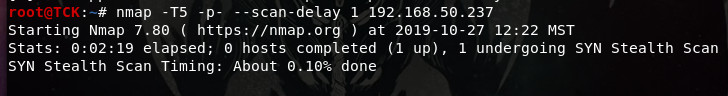
I was able to find 12 open ports on the machine.



1. **Scan a host adjusting the timing of requests with Nmap.**

I usually already do this, so I will increase my timing to 5 and see if there is anything different. I am also adding the scan delay option.

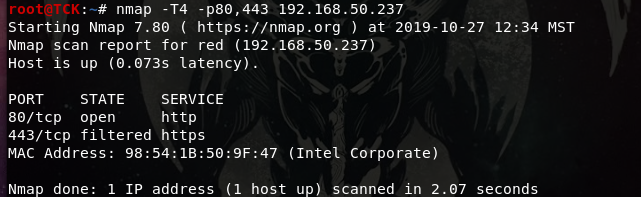
I had to cancel the scan because the delay really slows things down. I can see how this can be useful when you are trying to avoid detection.



1. **Use Nmap to sweep the scope for systems running web servers on port 80 and port 443.**

Tool: nmap  
Command: nmap -T4 -p80,443 192.168.50.237  
Intended result: Find services on port 80  
  
Result:

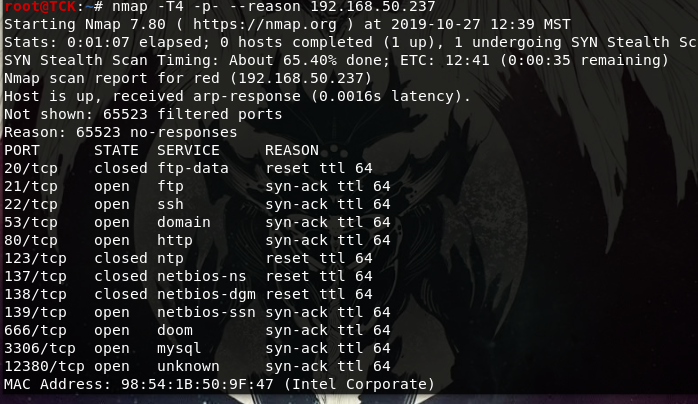
Port 80 is open and port 443 is filtered



1. **Run a scan on a host and tell Nmap to display the reason it finds the port in the state it does.**

Tool: nmap  
Command: nmap -T4 -p- --reason 192.168.50.237  
Intended result: Explanations on port states.  
  
Result:

This is an interesting option to add to the command, the 4 closed ports gave a reset flag and the open ports managed to complete the three-way handshake.

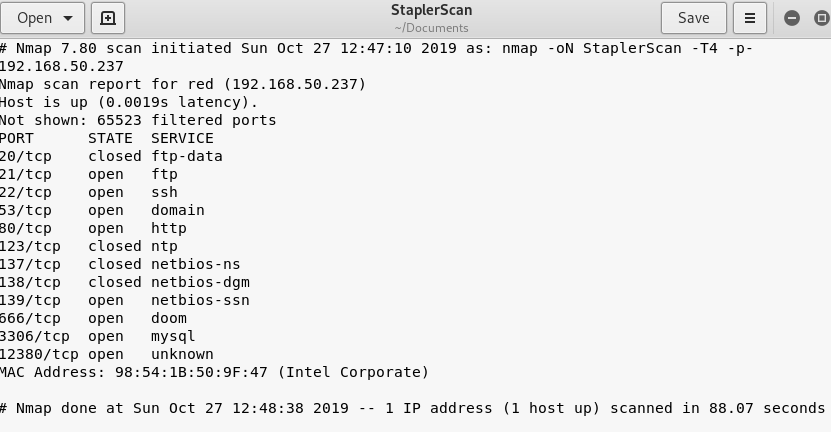


1. **Scan a system with Nmap and output the results to a Normal File.**
   1. **Just provide the command you would use, you do not have to append the results or the file.**

Tool: nmap  
Command: nmap -oN StaplerScan -T4 -p- 192.168.50.237  
Intended result: Outputting results in normal text file format

Result:

The file was created and placed in the pwd.

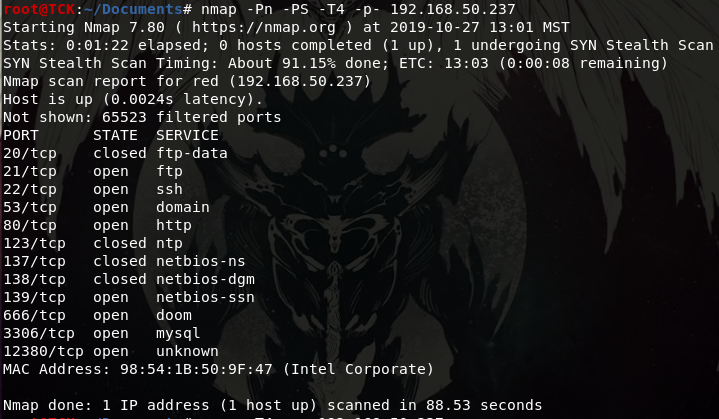


1. **Scan a host as if it where denying ICMP (ping).**

Tool: nmap  
Command: nmap -Pn -PS -T4 -p- 192.168.50.237  
Intended result: Go past the ICMP requests and go straight to the Syn/Ack scan

Result:

I got the same results as the scans before.

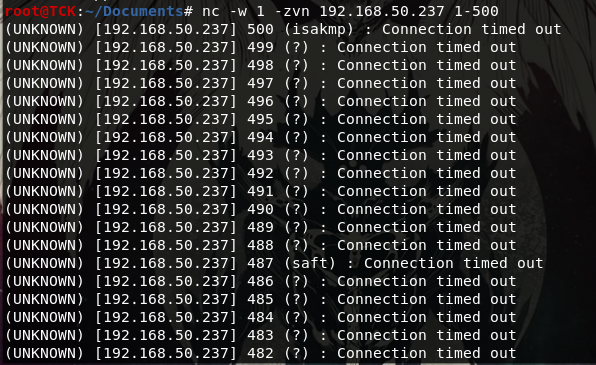


1. **Port scan on a host for open ports 1 through 500 with Ncat. Yes, Ncat.**
   1. **When do you think you might use Ncat vs Nmap?**

Tool: netcat  
Command: nc -w 1 -zvn 192.168.50.237  
Intended result: Port scan the host with ncat

Result:

A slow port scan that is connecting and leaving each port specified. I had to look this one up, I managed to get the -w and -z part before, but I was missing the verbose option. I believe you would use this if nmap was not available. I feel like you would be generating a lot more traffic with ncat. You would also use netcat if you are trying to establish connections to the target.

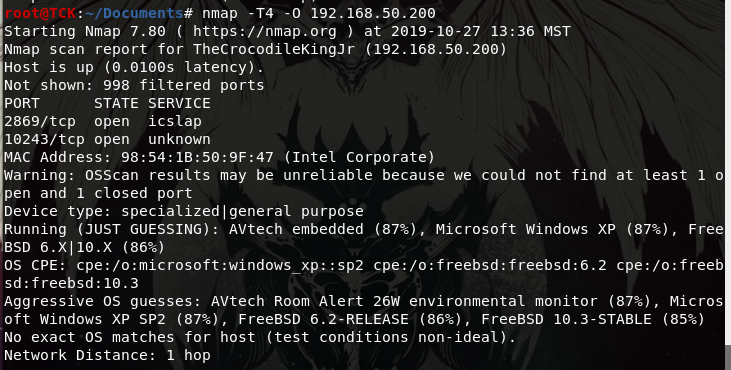


1. **Perform Operating System identification on one of the hosts on your network.**
   1. **You can use either Nmap or Xprobe2.**
   2. **How accurate was the guess by the tool?**

Tool: nmap  
Command: nmap -T4 -O 192.168.50.200  
Intended result: Identify my laptops OS as Windows 10

Result:

The OS scan was way off, it detected AVtech embedded, Windows XP, and FreeBSD.



1. **Perform application fingerprinting on a host with Nmap.**
   1. **In your estimation did Nmap properly identify the services running on the machine?**
   2. **Where there unknown application fingerprints?**
   3. **If Nmap doesn’t know what a service is, what steps could you take to determine what the service is?**

Tool: nmap  
Command: nmap -sV -T4 -p- 192.168.50.237  
Intended result: Determine the services on the open ports

Result:

Service disclosure was successful. I think so, looking at the port numbers and the services found, everything seems to add up correctly, except for the service on 12380, might just be a hidden HTTP server. Yea there was a service that was not identified, it gave me an unknown fingerprint. You can try to connect to it and see if it has a banner, you could also try probe it more with the -A option.

1. **You are on a penetration test. Your customer asks you to identify all of the hosts in a given network range. You notice that they are filtering ICMP so you can’t ping hosts to determine if they are alive. How would you determine which hosts in the network range are actually up?**

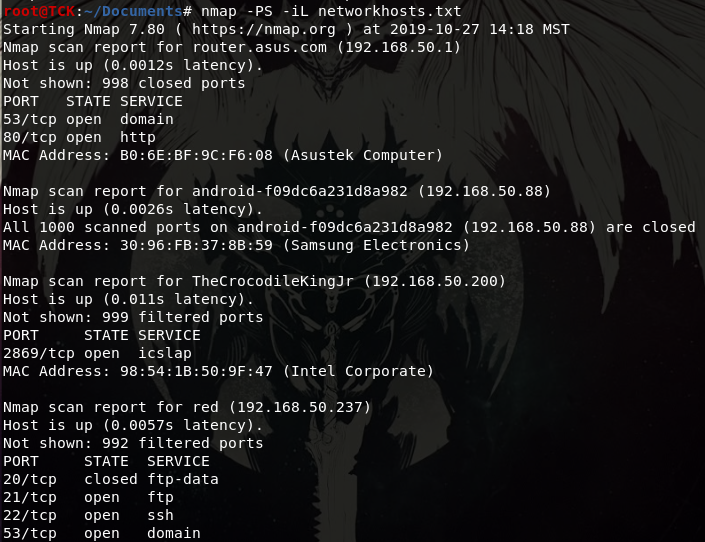
While testing this I found that the -PS and -Pn options work on more than one target, so if you used the command on the network, it would find the hosts on it. I was able to find most of the devices in my network with the command **nmap -PS -Pn 192.168.50.0/24**. This did not seem to find all the targets, so I tried the -PO option, **nmap -PO 192.168.50.0/24**, which gave me all 5 hosts on my network.

1. **Take a couple of the hosts from your network and put them in a plain text file. Put the IP addresses in the file so there is only one per line. Name this file “networkhosts.txt” Use Nmap with the appropriate command line argument to import this file and scan the contents.**

Tool: nmap  
Command: nmap -PS -iL networkhosts.txt  
Intended result: Scan the IP addresses in the file

Result

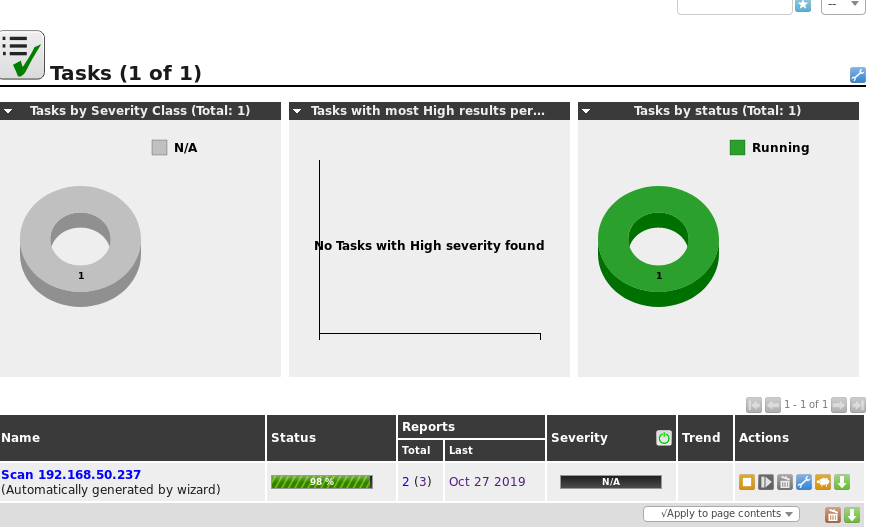
The scan went through, and I got the intended results.



# Part 2:

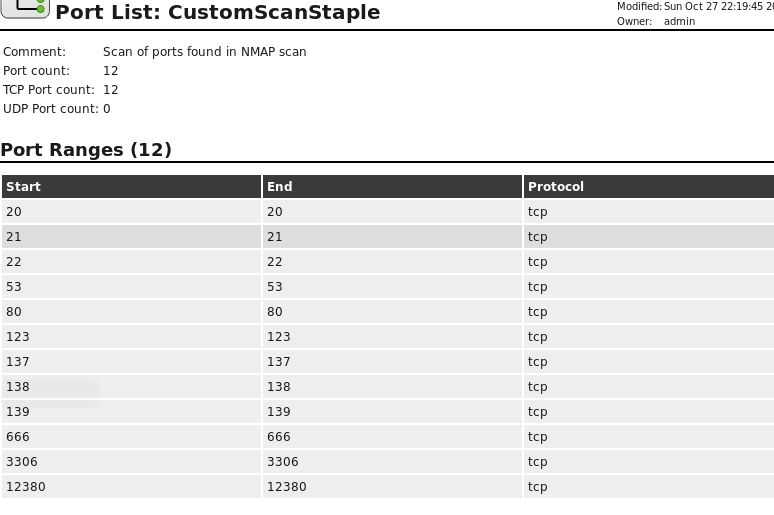
1. **Enter the IP address of the target system into OpenVAS and Scan it.**

You need to go to Scans/Tasks and create a new scan with the wizard or manually. If you wanted the scan to run later you can modify the start time, if not, the scan will begin immediately. It took me while to execute the correct scan, most of the time I was getting errors and my reports were empty. Seems like some of the filters were wrong? I managed to fix it though.



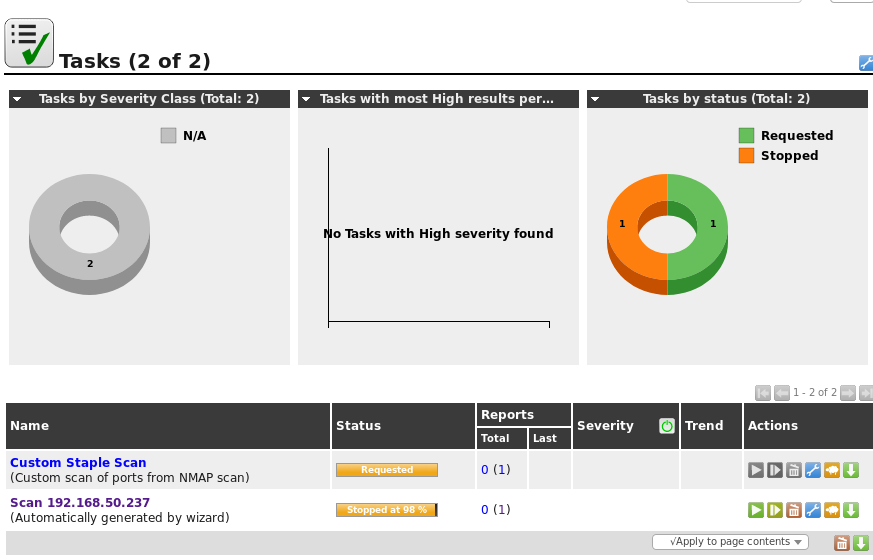
1. **Create a new custom scan policy in OpenVAS, this link may help**
   1. **In this new policy trim down the vulnerability checks so that they are more relevant to the operating system you are scanning. Give a few examples of checks that you removed. Give a few examples of checks that you kept.**

I created a custom scan list from the results I got from the NMAP scan done on the target earlier. If I focus on just those ports we might be able to find more things about them. I included all the ports found in the nmap scan



1. **Scan the IP address of the target system again using the new setup that you created.**

I succsefully created a new task with the new scan policy. I also lowered the QoD to 30% just to see how much of a difference there is between results.



1. **Do you see any items you suspect as false positives? Why do you believe them to be false?**

No it all seems pretty accurate compared to my Nmap results, the target is also old so the vulnerabilities being displayed have a high chance of being exploitable. All of the vulnerabilities listed correspond to the services detected.



1. **Do you believe that there are vulnerabilities on the system that the vulnerability scanner didn’t find? Why do you believe so?**

I believe there are some it missed. Especially the port 666 one, it is supposed to be used by the game DOOM, but there are reports stating it is used by malware as a backdoor. It could just be the game running, but I believe there is some backdoor involved.

1. **Export the data from the scan in a format you can read later. (PDF is fine)**
   1. **include a copy with your report.**

Exported to PDF

References

Last Name, F. M. (Year). Article Title. *Journal Title*, Pages From - To.

Last Name, F. M. (Year). *Book Title.* City Name: Publisher Name.