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

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

A screenshot of a computer

Description automatically generated

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.

1. **Submit your table for enumerating ports, services, and operating systems**(10points) A white grid with black text

   Description automatically generated A screenshot of a computer

   Description automatically generated A white grid with black text

   Description automatically generated A white grid with black text

   Description automatically generated A white grid with black text

   Description automatically generated

**A screenshot of a computer

Description automatically generated**

**A white table with black text

Description automatically generated**

A table with text on it

Description automatically generated

**A white table with black text

Description automatically generated**

**A white sheet with black text

Description automatically generated**

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

1. 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.

1. 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.

1. **List three ways and/or options you might use nmap such that alarms are less likely to be raised**(10 points)
   1. 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.
   2. 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.
   3. 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.
2. **Take a screenshot of the vulnerability output from scanning X.X.X.100** (10 points)

A screenshot of a computer

Description automatically generated

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

**A screenshot of a computer

Description automatically generated**

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.

1. **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.

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

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

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.

1. **List 2-3 additional vulnerabilities that interest you and make a note of their CVE and which hosts they were found on**(10 points)
   1. 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.

* 1. 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.

* 1. 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.