|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name: | : | Bocobo, Adolf Vincent Padua, Jaymar | Lab No. | : | 3 |
| Topic | : | Port Scanning Using Nmap | Group No. | : | 20 |
| Subject | : | Cyber Security | Score | : |  |

In this lab, we are going to use Nmap to perform network discovery and port scans including

scanning a range of IPs, specific ports, fingerprinting Operating Systems and discovering IPs.

**Procedure/ Algorithm**

**Step 1:** installation of Linux on hyper v  
  
A screenshot of a computer

AI-generated content may be incorrect.

**Step 2:** Scan 1000 common ports for a single IP (nmap <IP\_Address>)

A screenshot of a computer

AI-generated content may be incorrect.

**Step 3:** Scan only port 22 specifically

A screenshot of a computer

AI-generated content may be incorrect.

**Step 4:** Fingerprint the OS and find the Linux kernel version

A screenshot of a computer

AI-generated content may be incorrect.

**Step 5:** There is a secret service running on an uncommon port, you must find which port, but the challenge

is that you cannot scan ALL ports, but you are allowed to scan the port range between 40,000 –

60,000, so issue one command which scans that range.

A screenshot of a computer

AI-generated content may be incorrect.

**Result and Discussion**

**Step 1:**After installation of Linux of I created a file on desktop I named it Lab with a ./main\_script.sh file inside, because the default has no Labs folder on desktop.

**Step 2:**nmap 192.168.56.1 This command tells **Nmap** (a network scanner) to scan the IP address 192.168.56.1 and check the **1000 most common ports** to see which ones are open.

**Step 3:**sudo nmap -p 22 127.0.0.1 This scan checks if port 22, which is used for remote access (SSH), is open on the local machine (127.0.0.1). The result shows that the port is open, meaning the computer is allowing secure remote connections. This is normal if you're using tools to control the computer from another device.

**Step 4:**This scan checks what operating system and kernel version the local machine is running. The result shows that it's using a Linux system with a kernel version between 2.6.32 and 6.2. This helps identify the type of system and its version, which can be useful for troubleshooting or security testing.

**Step 5:**This command tells nmap to scan only the ports between **40000 and 60000** on your own machine (127.0.0.1) to check which one is open and might be running a hidden service.

**Conclusion**

Through this lab, we successfully used Nmap to explore and analyze network services by scanning common and specific ports, identifying open services, and fingerprinting the operating system. We also learned how to search for hidden services within a restricted port range, enhancing our understanding of basic network reconnaissance techniques essential in cybersecurity.