Network Scan and Traffic Analysis of a Metasploitable Machine

Introduction
The main purpose of this project is to understand how to scan and analyze a vulnerable machine (Metasploitable) in order to understand how network communication works.

Tools

- Vmware Workstation
- Kali Linux
- Metasploitable
- Nmap
- Wireshark

Procedure

First, I obtained the IP address of the Metasploitable machine by using the **ifconfig** command, which provides information on network interfaces. Then, within the Kali Linux bash, I used the command **ping 192.168.199.129** to confirm a connection. When you use the **ping** command and there is a connection, you will get a repeated response with ICMP packets, but if not, the bash will not give a response.

Next, using the Kali Linux bash, I used the command **nmap -sS -p- -sV -O 192.168.199.129** to scan each port.

- **Nmap:** This is the name of the tool.
- **-sS:** This is a SYN scan; it's an efficient and fast way for Nmap to send SYN packets to each port and wait for a response. If a SYN/ACK is received, the port is open, but if a RST is received, the port is closed.
- **-p-:** This flag scans all ports instead of the most common ones. It is a little slower but provides a complete search.
- **-sV:** This flag tells Nmap to find the exact version of the service running on each open port.
- **-O:** With this final flag, Nmap tries to determine the operating system of the target.

Port	State	Service	Version
21	open	ftp	vsftpd 2.3.4
22	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23	open	telnet	Linux telnetd
25	open	smtp	Postfix smtpd
53	open	domain	ISC BIND 9.4.2
80	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111	open	rpcbind	2 (RPC #100000)

139	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512	open	exec	netkit-rsh rexecd
513	open	login	OpenBSD or Solaris rlogind
514	open	tcpwrapped	
1099	open	java-rmi	GNU Classpath grmiregistry
1524	open	bindshell	Metasploitable root shell
2049	open	nfs	2-4 (RPC #100003)
2121	open	ftp	ProFTPD 1.3.1

With the Nmap scan, I found the data that is in the chart above, which shows the open ports, their service, and version. Nmap also determined that the OS of the machine is Linux 2.6.9 - 2.6.33.

Network Traffic Analysis

Within Wireshark, I started the packet capture. I then filtered it using **ip.addr == 192.168.199.129 and tcp.flags.syn == 1**. This filter allowed me to see the packets that Nmap sent to Metasploitable. After that, I used another filter: **ip.addr == 192.168.199.129 and tcp.flags.ack == 1**, which showed me the responses I got from the target for each port. Finally, the filter **ip.addr == 192.168.199.129 and tcp.flags.reset == 1** gave me the responses from the closed ports.

Conclusion

Through this project, I was able to download and install my own security lab using VMware, Kali Linux, and Metasploitable. I learned how to verify a connection between Linux and Metasploitable and acquired a series of commands that helped me check the version, ports, and services that are available, as well as which ones are closed. Additionally, with Wireshark, I was able to see the real communication within the network: the three-way handshake (SYN, SYN/ACK, ACK) and the responses captured when a service is closed (RST).