Scanning and Identifying Network Nodes

CompTIA Security + (SY-601)

Objectives:

- Identifying the Kali and Windows Servers
- Performing basic scans of the network
- Identifying hosts and Services
- Using banner grabbing to identify services

Materials:

To conveniently manouevre via the lab activities, the following materials (tools) were fully utilized:

- *Networking tools:* Ifconfig, ipconfig, arp, pathping, netdiscover, nmap
- *Banner Grabbing Tools:* Curl, Firefox
- *Virtual Machines:* Domain Controller 1, Microsoft Installer and Kali Linux

Procedure:

Identifying local Network Configurations

- The Kali Virtual Machine (Kali VM) was logged into.
- In the Terminal Emulator, the following commands were run: Ifconfig, ip a, ip.route.show, arp -a, ip neighbor, netdiscover -i eth0 -r 10.1.0.0/24
- The Domain Controller 1 (DC1) was logged into to access the User Control Access (UAC) via the Command Prompt (Admin)
- In the Windows Command Processor, the following commands were run: ipconfig, pathping

Using nmap to discover hosts

- The Kali VM was switched back, to run the following commands: nmap10.1.0.0/24, nmap -sS 10.1.0.254, nmap -A 10.1.0.254, nmap -p 20-200 10.1.0.0/24, nmap –top-ports 20 10.1.0.0/24

Banner Grabbing with curl & Firefox

- In the Kali VM Terminal, the following commands were run: firefox http://10.1.0.1, dig -x 10.1.0.254, dig soa corp.515support.com

Observations:

- Running the command, Ifconfig and ip a in the Kali VM, the IP address for the eth0 adapter displayed an IP address of 10.1.0.192
- The command ip route show and arp -a, in the Kali VM, respectively displayed the IP addresses of their router 10.1.0.254 and 10.1.0.1 (DC1.corp.515support.com)
- Running the command, ip neighbor; displayed a replica of the above findings
- The command -i.eth0 -r 10.1.0.0/24, showed a very slow response. However, it displayed 5 hosts on the netdiscover.
- The Domain Controller, User Account Control (UAC); accessed via Command Prompt (Admin), displayed an IP address of 10.1.0.1 upon running the command, ipconfig.
- The command, pathping 10.1.0.192 on UAC, Command Prompt (Admin), showed 0% packets lost; for a correct presentation, the percentage symbol was supposed to be included.
- In the Kali VM, the command, nmap localhost was run to discover open ports
- The command, nmap 10.1.0.0/24 was run on the Kali VM terminal to perform a basic network scan. It displayed all the open ports (i.e. /tcp ports)
- A stealthy scan was conducted on the Kali VM via running the command, nmap -sS 10.1.0.254. It displayed the SSH and DNS services which were running
- The Operating System (0S) Linux, which was being utilized to achieve the above findings was identified by the command, nmap -A 10.1.0.254
- In the Kali VM, to scan for open ports in the range of 20-200 on the network was achieved by running the command, nmap -p 20-200 10.1.0.0/24. Port 80 was seen to be open on MS1
- Referring to the above procedure & findings, the command, nmap –top-ports 20 10.1.0.0/24 displayed the open ports in a customized format; 'The twenty most common ports'
- The network for hosts that were up and down were conveniently observed by running the command, nmap -sn 10.1.0.0/24
- In the Kali VM's terminal, the command, curl -s -I 10.1.0.0/24 was successfully run to connect to the 10.1.0.1 server and the IIS 10 web server service and version was displayed

- Internet Information Service (IIS), web server service was observed in Kali VM, by running the command, firefox http://10.1.0.1
- The Command, dig -x 10.1.0.254, displayed the IP address of the Domain Name Service (DNS) server that answers the query

Results:

- In summary, the lab exercise successfully achieved its objectives which included:
- **Identifying the Kali and Windows Server:** through commands like Ifconfig, ipconfig, and arp, the lab identified network configurations and server IP addresses.
- **Performing basics of a network scan:** Tools like netdiscover and nmap were used to scan the network and identify hosts and services.
- **Identifying Hosts and Services:** Various commands and tools were utilized to identify hosts, open ports, and running services on the network.
- **Using Banner Grabbing to Identify Services:** Banner grabbing techniques were employed using tools like curl and Firefox to gather information about services running on specific IP addresses.

Conclusion:

In conclusion, this lab exercise on scanning and identifying network nodes has been instrumental in deepening my understanding of network security concepts covered in the CompTIA Security+ course. By employing tools like netdiscover, nmap, and banner grabbing techniques, I gained practical experience in mapping network topology, identifying active hosts, and discovering running services.

The significance of this lab exercise lies in its direct application to real-world scenarios in cybersecurity. Understanding how to scan and identify network nodes is crucial for assessing network vulnerabilities, detecting potential security threats, and implementing effective defense mechanisms.

Through hands-on experimentation with Kali Linux and Windows environments, I acquired valuable skills in network reconnaissance, which are essential for security professionals tasked with securing organizational networks and mitigating cybersecurity risks. This lab exercise reinforced the importance of thorough network scanning and vigilant monitoring as fundamental components of a robust cybersecurity strategy.

Overall, the knowledge and skills gained from this lab exercise will serve as a solid foundation for further exploration and application of advanced security concepts in the CompTIA Security+ course and beyond. It underscores the practical relevance of network scanning techniques in safeguarding sensitive information and maintaining the integrity of enterprise networks in today's dynamic threat landscape

Challenges:

- There was a system freeze leading to the inability of navigating Virtual Machines conveniently
- It several attempts to discover that the packets that were lost during the were to be presented with a percentage symbol
- There was a misunderstanding in typing the command, firefox https://10.1.0.1 in the Kali VM, specifically: spacing errors.

Future Work:

Explore advanced scanning, vulnerability assessment, IDS/IPS, network forensics, and threat intelligence.