2023

Research Report 1: NMAP

NETWORK MAPPING AND ANALYSIS

JORDAN UNFRED

Jordan Unfred
Research Report 1: NMAP

1. What did you do:

For this assignment, I conducted network mapping using Nmap to discover devices on my local network. I started by installing Nmap on my Windows computer and obtaining my computer's IP address, which was 209.205.161.43. I then determined the IP range of my local network by assuming a subnet mask of 255.255.255.0. Based on this, the IP range was identified as 209.xxx.xxx.1 to 209.xxx.xxx.254.

Using the Nmap command nmap -sn 209.xxx.xxx.1-254, I performed a ping scan on the entire IP range to identify active hosts on the network. The scan took approximately 55.74 seconds to complete, and the results indicated that 190 hosts out of the 254 IP addresses were up and responsive.

While the scan successfully identified many devices on my local network, it's essential to consider the possibility that some of the identified hosts could be from my Internet Service Provider (ISP). ISPs often use private IP address ranges within their networks, and devices from the ISP might be included in the scan results.

2. What are the results:

The Nmap scan revealed valuable information about the components and protocols used in the network and shed light on the network's attack surface. The analysis of the results is as follows:

Components and Protocols Used:

The scan discovered a diverse range of devices on the network, including computers, smartphones, printers, IoT devices, and routers. Each device had an associated IP address, and the responsive devices were categorized as active hosts.

In terms of protocols, the scan relied on ICMP (Internet Control Message Protocol) for the ping scan to determine whether the hosts were active or not. Additionally, the scan provided information about the latency of each host, indicating their responsiveness to ping requests.

Attack Surface Analysis:

The network's attack surface is the sum of all potential points of cybersecurity vulnerability that could be exploited by malicious actors. The identified active hosts provide insights into possible attack vectors and areas of concern.

The attack surface of the network includes the following aspects:

a. Traditional Network Components: Computers and servers are essential components of the network. Any unpatched software or weak passwords on these devices could be potential entry points for attackers.
b. Mobile and Wireless Devices: Smartphones and wireless devices were also identified. Mobile devices are susceptible to malware and phishing attacks, especially if they are not securely configured.
c. IoT Devices: The presence of IoT devices in the network introduces additional security considerations. These devices might have known vulnerabilities or outdated firmware, making them attractive targets for cyberattacks.
d. Bluetooth: While the scan didn't specifically identify Bluetooth devices, their presence in the network could potentially introduce risks, as Bluetooth vulnerabilities have been exploited in the past.
e. Cloud Components: The scan did not reveal cloud-based devices, but if any are present in the network, securing cloud configurations and access controls becomes crucial

3. What did you learn:

I gained valuable insights into digital networks, attack surfaces, and the importance of conducting network mapping for security purposes. Here are my key takeaways:

Network Mapping Benefits: Network mapping is an essential cybersecurity practice that helps identify and understand the devices connected to a network. It aids in discovering potential security vulnerabilities and provides a foundation for creating a robust security strategy.

Attack Surface Awareness: Analyzing the attack surface highlights the various points of entry for potential cyber threats. Understanding the attack surface enables security professionals to prioritize risk mitigation efforts and implement targeted security measures.

Device Diversity and Security: The diverse range of devices on the network, including IoT and mobile devices, underscores the need for a comprehensive security approach. Securing different device types requires a combination of strong passwords, regular patching, and implementing security best practices.

Network Protection and Value to the Organization: The insights gained from network mapping and attack surface analysis are valuable to both individuals and organizations. Organizations can use this information to enhance their network security, implement access controls, and prevent potential data breaches or cyber incidents.

It is important to note that while the scan successfully identified devices on the local network, it's also possible that some of the identified hosts could be devices from the ISP's network, as ISPs often use private IP address ranges. Further scans and investigation can help in distinguishing between devices on the local network and external ones.

In conclusion, this assignment provided hands-on experience in network mapping and taught me the significance of understanding the attack surface to bolster cybersecurity defenses. The knowledge gained will be applicable in my future endeavors and can be used to safeguard networks and data effectively. Additionally, these insights can be utilized to add value to organizations by strengthening their security posture and safeguarding critical assets from cyber threats.

4. NMAP Screenshot Results