Research Report 1: ***Report on Network Mapping and Analysis Using NMAP***

By: Farzaneh Noroozi

Date: 7/18/2023

what did you do?

Introduction:

The purpose of this report is to outline the methodology and process used to map and analyze the network of our organization. The objective was to identify network components and protocols, assess the attack surface, and uncover potential vulnerabilities. This report provides a detailed account of the steps taken, including the use of Nmap and Zenmap for scanning and analysis.

Mapping the Network:

1. Obtaining Permission:

Initially, an attempt was made to gain permission from the manager to use the work computer's IP address for the mapping process. Unfortunately, permission was denied. Consequently, the decision was made to utilize the personal computer's IP address.

2. Downloading Nmap:

To begin the process, Nmap was downloaded following these steps:

a. Visit the official Nmap website (https://nmap.org) and navigate to the "Download" section.
b. Choose the appropriate version for the personal computer's operating system.
c. Download the installer package.
d. Run the installer and follow the on-screen instructions to complete the installation.

3. Finding the IP addresses:

To locate our device's IP address, we can navigate to the "Shields UP" section on the website https://www.grc.com/, which I found **73.37.102.78** for my laptop. Also, we can find it through "ipconfig" command on CMD which my laptop IPv4 was **192.168.0.15** there. I also omit the last digit of an IP address and replace it with "/24" in Nmap scanning (In my case use 192.168.0.15 instead of **192.168.0.10/24**. This allows us to efficiently scan multiple hosts within that specific subnet. I decided to scan all these three IP addresses.

Analyzing the Network:

1. Launching Zenmap:

After Nmap was successfully installed, Zenmap was launched to provide a graphical interface for interacting with Nmap.

2. Target Selection:

In Zenmap, locate the "Target" field where the IP address of the organization's network needs to be entered. The specific IP address to be scanned was 192.168.0.15.

3. Selecting Scan Profiles:

Different scan profiles were tested within Nmap. Initially, an Intense scan profile was used. However, after analyzing the output data obtained from different profiles, it was determined that a slow comprehensive scan would provide more accurate results for analysis.

4. Initiating the Scan:
To start the scanning process, Zenmap was instructed to utilize Nmap's scanning techniques. The software began gathering information about the network components and protocols. The scan was performed on two IP addresses: 192.168.0.15 and 192.168.0.10/24.

5. Monitoring the Scan:
During the scan, Zenmap displayed real-time information about the ongoing process. This included details such as scanned ports and discovered hosts.

6. Scan Completion and Results:
Upon completion of the scan, Zenmap presented the results in a tabular format. The report included information about open ports, services running on those ports, and other relevant details about the network.

Analysis and Vulnerability Assessment:

1. Interpretation of Results:
Following the scan, the Nmap report was thoroughly analyzed. Each line of the report was cross-referenced with external sources to understand its meaning and significance.

2. Identifying Network Components and Protocols:
The scan results were carefully examined to identify the network components and protocols used within the network. Special attention was given to open ports and associated services, enabling a comprehensive understanding of the network's structure.

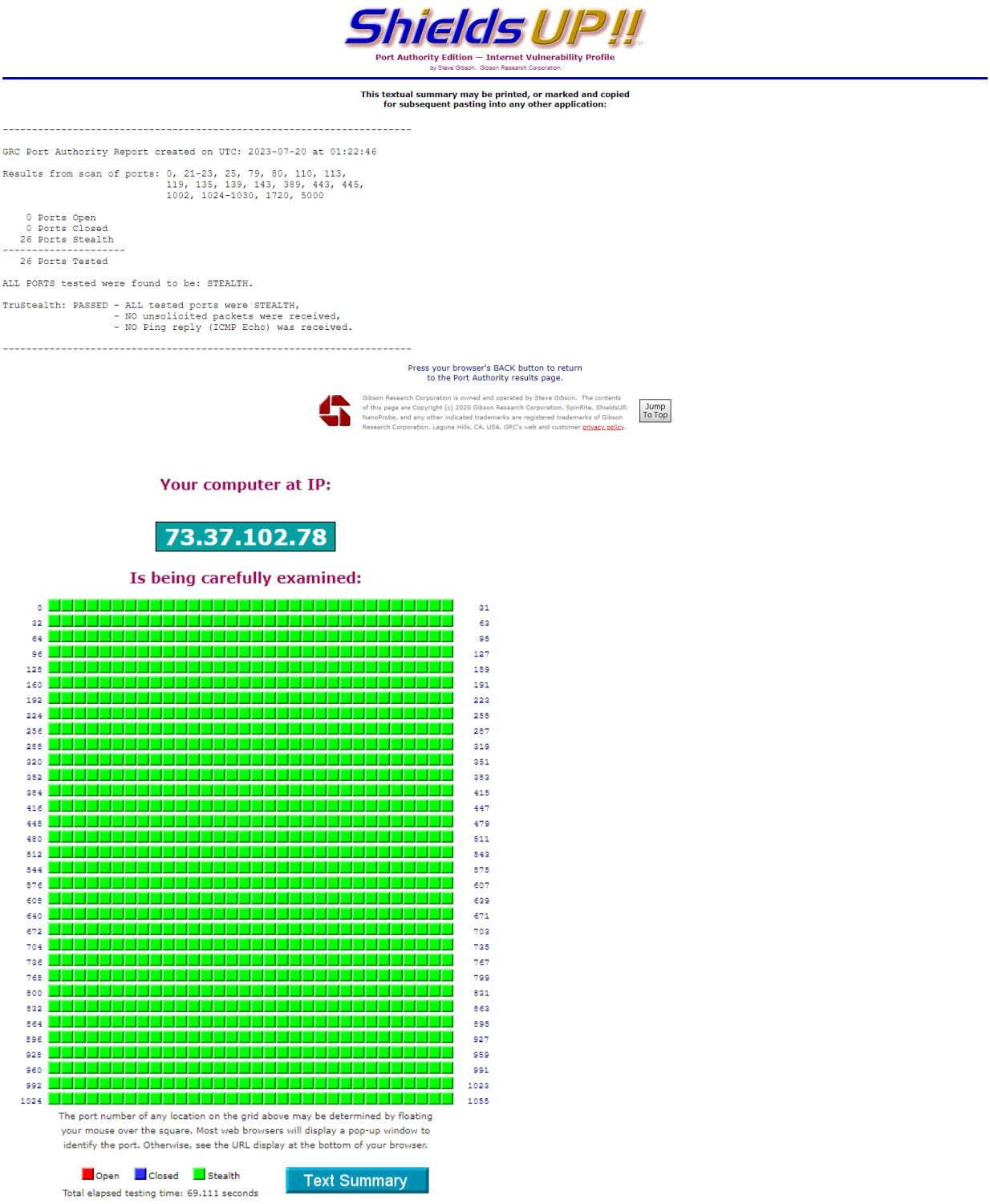
3. Vulnerability Identification:
The scan results were reviewed to identify potential vulnerabilities or areas that could be targeted in a cybersecurity attack. This involved identifying open ports, outdated services, and any misconfigurations that could pose a risk to the network's security.

Expanding Analysis to Other Network Components and Protocols:

While Zenmap primarily focuses on scanning IP networks, it is important to extend the analysis to other components and protocols within the organization's infrastructure. Consideration should be given to performing separate scans or employing tools specifically designed for assessing the security posture of mobile, Bluetooth, IoT, wireless, and cloud networks.

what were the results?

7. I received the following reports for my computer from navigating to the "Shields UP" section on the website https://www.grc.com/.



Shields UP!!
Port Authority Edition — Internet Vulnerability Profile
by Steve Gibson, Gibson Research Corporation.

This textual summary may be printed, or marked and copied for subsequent pasting into any other application:

```
-------------------------------------------------------------------------

GRC Port Authority Report created on UTC: 2023-07-20 at 01:22:46

Results from scan of ports: 0, 21-23, 25, 79, 80, 110, 113,
                            119, 135, 139, 143, 389, 443, 445,
                            1002, 1024-1030, 1720, 5000

    0 Ports Open
    0 Ports Closed
   26 Ports Stealth
--------------------
   26 Ports Tested

ALL PORTS tested were found to be: STEALTH.

TruStealth: PASSED - ALL tested ports were STEALTH,
                   - NO unsolicited packets were received,
                   - NO Ping reply (ICMP Echo) was received.

-------------------------------------------------------------------------
```

Press your browser's BACK button to return to the Port Authority results page.

Jump To Top

Your computer at IP:

73.37.102.78

Is being carefully examined:

0 31
32 63
64 95
96 127
128 159
160 191
192 223
224 255
256 287
288 319
320 351
352 383
384 415
416 447
448 479
480 511
512 543
544 575
576 607
608 639
640 671
672 703
704 735
736 767
768 799
800 831
832 863
864 895
896 927
928 959
960 991
992 1023
1024 1055

The port number of any location on the grid above may be determined by floating your mouse over the square. Most web browsers will display a pop-up window to identify the port. Otherwise, see the URL display at the bottom of your browser.

Open Closed Stealth

Text Summary

Total elapsed testing time: 69.111 seconds

information we can get from analyzing the Nmap report for IP address **192.168.0.15**:

Components and Protocols Used:

- The report shows the scan was performed on a single host with the IP address 192.168.0.15.
- The scan identified several open ports on the host, including:
- TCP ports: 135 (msrpc), 139 (netbios-ssn), 445 (microsoft-ds?), 3580 (http), 5357 (http)
- UDP ports: 123 (ntp), 137 (netbios-ns), 138 (netbios-dgm), 500 (isakmp), 1900 (upnp), 2343 (nati-logos) 3702 (ws-discovery), 4500 (nat-t-ike), 5000 (upnp), 5001 (commplex-link), 5050 (mmcc), 5353 (mdns), 5355 (llmnr), 6000 (X11), 6001 (X11:1)
- The protocols observed include TCP, UDP, and DNS.

Attack Surface Analysis:

Based on the open ports and protocols found, we can analyze the attack surface presented by the network:

1. TCP Ports:
   - Port 135: This is the Microsoft Windows RPC (Remote Procedure Call) service, which could be targeted for remote code execution vulnerabilities.
   - Port 139: This is the NetBIOS Session Service, commonly used for file and printer sharing. It could be exploited for unauthorized access or information disclosure.
   - Port 445: This port is typically associated with the SMB (Server Message Block) protocol and could be targeted for various SMB-related attacks, including file sharing and remote code execution.
   - Port 3580: This port is running the National Instruments LabVIEW service locator HTTPD. It may have its own set of vulnerabilities that could be exploited.
   - Port 5357: This port is associated with the Microsoft HTTPAPI HTTPD and could be targeted for HTTP-related attacks.

2. UDP Ports:
   - Port 123: This is the NTP (Network Time Protocol) service, which could be targeted for time-related attacks.
   - Port 5353: This is the mDNS (Multicast DNS) service, which could be targeted for DNS-based attacks or service discovery exploits.

3. Other Ports:
   - The remaining open ports on various UDP ports indicate potential services or protocols running, such as UPnP, NAT-T IKE (IPsec Key Exchange), X11 (X Window System), etc. Each of these services may have their own set of vulnerabilities.

information we can get from the Nmap report for IP address **192.168.0.10/24**:

Components and Protocols Used:

1. IP Addresses: The scan identified a range of IP addresses in the network, starting from 192.168.0.0 to 192.168.0.255.

2. Hosts: Several hosts were scanned, but most of them were reported as "host down" (unreachable or not responding).

3. Ports: The scan targeted a total of 10,000 ports on the remaining live hosts.

Attack Surface Analysis:

1. Open Ports: The scan found open ports on some of the live hosts. Notable open ports include:

- 192.168.0.10: 445/tcp, 139/tcp, 80/tcp, 443/tcp, 8200/tcp, 20005/tcp (These ports could indicate potential services or applications running on the host.)
- 192.168.0.11: 139/tcp, 80/tcp (Similar to above, these ports might reveal the presence of specific services.)
- 192.168.0.13: 3000/tcp, 3001/tcp, 7000/tcp, 49152/tcp, 1055/tcp (Open ports may correspond to various applications or services.)

2. Potential Services: The open ports hint at potential services running on the live hosts. Ports such as 80 (HTTP), 443 (HTTPS), 445 (SMB), 3389 (Remote Desktop), and 139 (NetBIOS) are commonly used for web servers, file sharing, and remote access services.

3. Vulnerabilities: Open ports represent potential attack vectors and could expose the network to various vulnerabilities if the services running on these ports are not adequately secured and patched.

4. Network Reachability: Many hosts were reported as "host down," indicating they were either unreachable or not responding. However, this doesn't necessarily mean they are entirely secure, as attackers might still attempt to target them if they become reachable in the future.

5. Unresponsive Hosts: Unresponsive hosts could indicate network segmentation or potential filtering mechanisms in place. However, this doesn't guarantee complete protection, as attackers might still find other entry points.

6. SYN Stealth Scan: The SYN stealth scan identifies open ports using a more covert approach to avoid detection by intrusion detection systems (IDS) or firewalls. This suggests a higher level of reconnaissance and potential attack intent by the scanner.

Summary and Findings:

We can understand that there are several live hosts on the network with open ports, implying the presence of various services or applications. Commonly used ports like 80 (HTTP) and 443 (HTTPS) suggest web servers or applications with a web interface, while ports like 445 (SMB) and 139 (NetBIOS) indicate possible file sharing or Windows network services.
The attack surface of the network appears significant due to the presence of multiple live hosts with open ports, especially if those services are not adequately protected or updated with the latest patches. The existence of unresponsive hosts may indicate some level of network segmentation, but it doesn't guarantee immunity against potential attacks. Attackers may continue their reconnaissance and exploitation attempts on these hosts in the future if they become reachable.

To improve the security posture of the network, it is essential to:

1. Regularly patch and update all software and applications running on the live hosts to address known vulnerabilities.

2. Configure firewalls and access controls properly to restrict unnecessary exposure of services to the internet or other untrusted networks.

3. Implement strong authentication mechanisms, especially for remote access services like RDP (3389), to prevent unauthorized access.

4. Continuously monitor the network for unusual activity or intrusion attempts using intrusion detection systems and security event monitoring.

5. Conduct periodic security assessments, including penetration testing, to identify and fix potential security weaknesses.

Additionally, since the report does not include information about mobile, Bluetooth, IoT, wireless, or cloud components and protocols, it is essential to ensure these areas are also covered in a comprehensive cybersecurity assessment. Each of these components introduces its own set of unique risks and security considerations, and they should not be overlooked in a thorough analysis of the attack surface.

information we can get from the Nmap report for IP address **73.37.102.78**:

Components and Protocols Used:
1. Nmap Scripting Engine (NSE): Explanation: Nmap Scripting Engine is a powerful feature of Nmap that allows the execution of scripts for various purposes during the scan. NSE scripts are used to extend Nmap's capabilities, perform specific tasks, and gather additional information about the target.

2. Ping Scan: Explanation: Ping Scan is used to determine the online status of hosts. It sends ICMP echo requests to potential target hosts and checks for responses to identify live hosts on the network.

3. SYN Stealth Scan: Explanation: SYN Stealth Scan is a type of port scanning technique used by Nmap to determine open ports on the target host. It works by sending SYN packets to the target ports and analyzing the responses to identify open ports.

4. UDP Scan: Explanation: UDP Scan is used to identify open User Datagram Protocol (UDP) ports on the target. Unlike TCP, UDP is a connectionless protocol, making its scanning more challenging.

5. Service Scan: Explanation: Service Scan aims to identify the services running on the open ports of the target host. It analyzes the responses received from open ports to determine the specific services running on those ports.

6. OS Detection: Explanation: OS Detection is an attempt to identify the operating system running on the target host. Nmap uses various techniques, such as analyzing network responses and fingerprinting, to make an educated guess about the operating system.
Attack Surface Analysis:

The Nmap scan for IP address 73.37.102.78 revealed the following information:

1. Error in "mtrace" NSE script: The "mtrace" NSE script requires the "fromip" argument to be provided, but it was not supplied during the scan. This could result in incomplete or inaccurate results from the "mtrace" script.

2. Error in "shodan-api" NSE script: The "shodan-api" NSE script requires the ShodanAPI key to be specified using the "shodan-api.apikey" argument. As the key was not provided, the script was unable to use Shodan's capabilities to enhance the scan results.

3. Open Port 53/TCP: Port 53 with TCP protocol was found to be open on the target host (73.37.102.78). Port 53 is commonly associated with DNS (Domain Name System) services.

4. Open Port 53/UDP: Port 53 with UDP protocol was also found to be open on the target host (73.37.102.78). This is the standard port for DNS using UDP.

5. Open Port 47808/UDP: Port 47808 with UDP protocol was identified as open on the target host (73.37.102.78). Without additional information, the purpose of this port remains unknown.

Overall, the Nmap scan provided valuable insights into the target host's open ports and services, as well as attempted OS detection. However, the presence of errors during the execution of certain NSE scripts may have limited the completeness of the results. It is advisable to troubleshoot and fix these errors to obtain more comprehensive and accurate information about the target system's attack surface.

what did you learn?

Insights and Takeaways:

Throughout the process of mapping and analyzing the network using Nmap and Zenmap, I gained valuable insights into the world of cybersecurity and network vulnerability assessment. As someone new to this field, it was a fascinating experience to delve into the intricacies of analyzing open ports, identifying potential vulnerabilities, and understanding the overall attack surface of a network.

1. Importance of Permission and Authorization: One crucial lesson I learned is the significance of obtaining proper permission and authorization before conducting network scanning and analysis. The denial of permission, in this case, led me to use an alternative IP address, which highlighted the importance of compliance with organizational policies and legal requirements. Conducting network scanning and vulnerability assessments require ethical considerations, ensuring that the analysis is done within legal and ethical boundaries and respecting the privacy and security of the network's owners.

2. Selection of Scan Profiles: I discovered the critical role that scan profiles play in shaping the accuracy and depth of the analysis. By experimenting with different profiles and comparing the results, I realized that a slow comprehensive scan offers a more detailed and reliable understanding of the network's security posture compared to an initial Intense scan.

3. Continuous Monitoring of Scan: Real-time monitoring of the scan process taught me the importance of closely tracking its progress. This allowed me to identify any issues or discrepancies that arose and address them promptly, ensuring the scan proceeded smoothly and effectively.

4. Interpretation and External Validation: Thoroughly analyzing the scan results and seeking external validation proved to be an invaluable step. By cross-referencing the findings with external sources, I was able to interpret the significance of each line in the report and grasp the potential risks associated with identified components, protocols, and vulnerabilities.

5. Expansion to Other Network Components and Protocols: Although my focus was primarily on IP networks during this analysis, I realized the importance of extending the assessment to other network components and protocols. This insight highlighted the need to consider mobile, Bluetooth, IoT, wireless, and cloud networks as they introduce additional attack vectors and vulnerabilities. Employing specialized tools and conducting separate scans for these components would provide a more comprehensive understanding of the network's security landscape.

6. When we omit the last digit of an IP address and replace it with "/24" in Nmap scanning (In my case use 192.168.0.15 instead of 192.168.0.10/24), we are performing a subnet scan using CIDR notation. For example, if we use 192.168.0.10/24, it means scanning all IP addresses in the 192.168.0.0/24 subnet, ranging from 192.168.0.0 to 192.168.0.255. This allows us to efficiently scan multiple hosts within that specific subnet.

Value to the Organization:

The knowledge and skills gained from this exercise can be of immense value to organizations in several ways:

1. Enhanced Security Posture: By conducting network mapping and analyzing the attack surface, organizations can proactively identify potential vulnerabilities and take appropriate measures to mitigate risks. This approach helps enhance the overall security posture of the organization and bolsters its defense against cyber threats.

2. Prioritization of Vulnerabilities: Through the identification and assessment of vulnerabilities, organizations can prioritize their remediation efforts. This allows for resource allocation to address critical vulnerabilities that pose the most significant risks to the network and its assets.

3. Compliance and Regulatory Requirements: Analyzing the network and identifying vulnerabilities aids organizations in meeting compliance and regulatory requirements. By addressing security gaps and maintaining necessary standards, organizations can protect sensitive data and fulfill their legal obligations.

4. Incident Response Preparedness: A comprehensive understanding of the attack surface and potential vulnerabilities equips organizations with the necessary insights to prepare and improve their incident response plans. This preparedness ensures swift and effective responses to security incidents, minimizing their impact.

5. Continuous Improvement: Regular network mapping and analysis enable organizations to stay abreast of the ever-evolving security landscape. By identifying emerging threats, implementing the latest security measures, and adapting to evolving attack vectors, organizations can continuously improve their security practices.

6. External Validation and Collaboration: Seeking external validation and collaborating with other security experts or organizations can improve the accuracy and credibility of the analysis. External validation helps ensure that the identified vulnerabilities are legitimate and increases confidence in the assessment results.

7. Incident Response Planning: Understanding the network's attack surface and potential vulnerabilities aids in incident response planning. Organizations can use this knowledge to develop effective response strategies and improve their ability to detect and mitigate security incidents.

8. Continuous Learning and Adaptation: The cybersecurity landscape is ever-changing, and continuous learning is crucial to stay updated with emerging threats and new attack techniques. Regular network scanning and analysis enable organizations to adapt their security practices and maintain robust defenses.

In conclusion, as a newcomer to the field of cybersecurity, the process of mapping and analyzing the network using Nmap and Zenmap has been an enlightening and educational experience. It has provided me with a deeper understanding of network vulnerability assessment and the significance of analyzing open ports and potential vulnerabilities. I am excited to further develop my skills and knowledge in this field and contribute to the security of organizations in the future.