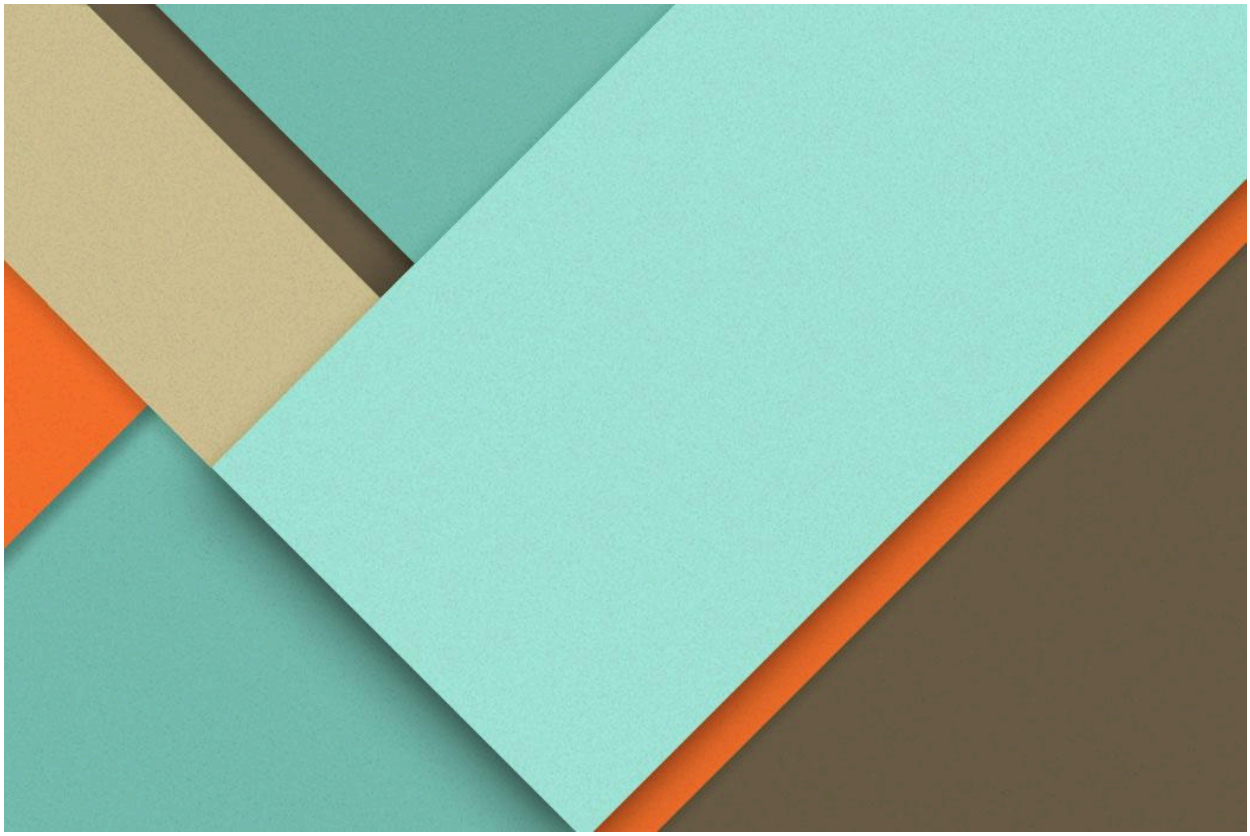

SCANNING NETWORK

19.01.2025

MUAHAMMED SAFAYATH T
STUDENT @INTELLIPAT
KERALA
suhailariyallur1@gmail.com

Overview

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper.

Goals

1. Lorem ipsum dolor sit amet, consectetuer adipiscing elit
2. Sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat.

TASKS:-

1. Host Discovery Using the 'ping' Command: Your first task is to perform host discovery on the client's network using the 'ping' command. Provide a detailed explanation of the data you can extract from the results and how this helps in the assessment.

2. Comprehensive Port Scan: Now, you need to conduct a comprehensive and non-intrusive port scan on the specified target IP address. Outline the steps you would take, including the choice of tools and software. Explain the reasons for using non-intrusive methods.

3. OS Discovery and Ethical/Legal Considerations: Perform OS discovery on the network you do not own or manage. Discuss the ethical and legal considerations that security professionals should be aware of and adhere to during this process.

4. Scanning Beyond IDS and Firewall: Conduct a scan beyond the

Intrusion Detection System (IDS) and Firewall. Provide a report of all the outcomes, including vulnerabilities and potential risks that may have been missed by these security measures.

5. Network Scan Using Wireshark: Create a step-by-step tutorial on how to use Wireshark to carry out a basic network scan. Demonstrate how to locate open ports on a target machine as an example.

6. Generating a Comprehensive Report: After completing the tasks mentioned above, generate a comprehensive report summarizing your findings, including vulnerabilities, risks, and recommendations for improving the network's security.

NOTE:-

Ensure that you have proper authorization to perform network scanning on the chosen target. Always follow ethical and legal guidelines when conducting security assessments. The target could be any authorized domain or any of the domains from the below list:

1. www.certifiedhacker.com
2. www.moviescope.com
3. www.goodshopping.com
4. T estphp.vulnweb.com
5. Machine IP from your Lab Setup

SOLUTIONS :--

1 :- HOST DISCOVERY USING PING COMMAND ➖

ping 192.168.0.110

-If the host is reachable or alive we will get icmp echo replay starting with 64 bytes

-if host is not alive we will get replay mentioning that host is unreachable

Included Bash Shell command for Aotomatic full network scanning to get alive hos t with is few seconds using ping:- (ip_ping.sh) command— bash /path/to/ip_ping.sh

Analysis of Ping Results:

- **Active Hosts Identification**: If a host replies with an Echo Reply, it indicates that the host is active and reachable on the network. You can identify which systems are available for further analysis or penetration testing.
- **Network Latency Assessment**: The `time` value tells you how fast the network is between you and the target. A high response time could indicate network congestion, longer distances, or suboptimal routing.
- **Host Location Estimation**: By checking the TTL value, you can estimate how far away a target is from your location. A TTL value of 64, for instance, typically indicates a host on the local network or a nearby device, while a TTL of 128 or higher could indicate a system further away.
- **Firewalls and ICMP Blocking**: If the ping results show a timeout or no response, the host might be actively blocking ICMP traffic. This could be a sign of a firewall or security system designed to prevent ICMP-based scanning. In such cases, alternative methods of host discovery, such as port scanning or using other protocols (e.g., TCP/UDP), may be required.
- **Network Configuration Issues**: If no responses are received from multiple IP addresses on the same subnet, it could indicate misconfigurations in network settings, a failure in the network infrastructure (e.g., routers), or a network-wide issue.

2:-

nmap -sS -sV -T3 -p- 192.168.1.x

``` - `-sS`: SYN Scan for stealth. -

`-sV`: Version detection to get service info. -

`-T3`: Timing template set to a moderate scan speed to reduce the chances of detection (T0 to T5 range for timing; T3 is a good balance between speed and stealth). -

`-p-`: Scan all 65535 ports.

SYN Scan (`-sS`): Also known as a "half-open" scan, it sends a SYN packet and waits for a response. This method does not complete the TCP handshake, making it less likely to be detected than a full connection scan.

Stealth Scan (`-sF`, `-sX`, `-sN`): These scans manipulate the flags in the TCP packet to avoid detection by firewalls or intrusion detection systems. These types of scans may be useful if the network employs an IDS/IPS.
```

Also can add -Pn if you are sure that host is alive and there is firewall which is blocking Icmp echo request . why -Pn is important in such a case:-

> The target is behind a firewall or network device that blocks ping requests (ICMP).

- You are certain the target is online, and you don't want to waste time on host discovery.
- You want to avoid triggering intrusion detection systems (IDS) or firewalls that might block or log ping requests.

When you use `-Pn`, Nmap assumes that the target is up and directly proceeds with port scanning, even if it hasn't received any response to the host discovery phase.

Mitigating Risks and Avoiding Detection:

- **Use Timing Adjustments**: Use slower scan times and timing templates to avoid tripping alarms.
- **Avoid Aggressive Scanning**: Don't use overly intrusive scan types, like `-sX` (Xmas scan), unless absolutely necessary.
- **Perform Limited Scans**: Conduct limited scans in stages, rather than all ports at once, to avoid suspicious activity spikes.

Why Non-Intrusive Methods:

Non-intrusive methods help to:

- Avoid detection by IDS/IPS systems.
- Prevent triggering alerts from firewalls, which might block subsequent scanning attempts.
- Minimize disruption to services or systems.
- Ensure that the target does not experience slowdowns, crashes, or other negative impacts during the scan.

Practicals included in nmap_stealthscan.txt

3:-

FOR OS DISCOVERY ➖

Nmap -O 192.168.0.X

Key Takeaways for Network Scanning And Awareness :

1. **Obtain Permission**: Always get explicit, written permission from the network or system owner before performing OS discovery or penetration testing.
2. **Avoid Disruption**: Use non-intrusive and minimally disruptive techniques for OS discovery to prevent system downtime or disruption.
3. **Follow the IT Act**: Ensure compliance with the **IT Act, 2000** and its sections on unauthorized access, hacking, and data theft.
4. **Report Findings Responsibly**: In case of vulnerabilities, follow responsible disclosure practices to notify the affected organization or entity.
5. **Understand the Law**: Be aware of the **Personal Data Protection Bill** and the implications it may have on handling personal data during testing.

Practicals included in nmap_stealthscan.txt

4:-

Sending fragmented packets may not be monitored by the firewall.

>Nmap -f <target>

>Nmap -mtu 8 <IP> :- evade detection of the firewalls which focus on large packets

>Nmap -g <source port> <target> :- specify a source port like 53 for dns to deceive target as it is legitimate .

>Nmap —scan-delay 500ms <target> :- it scan with delay which look more legitimate for firewall

>Nmap -D RND:10 <ip> :- decoy scanning with random 10 ip address as source.

Practical included on nmap_scanningBeyondFirewall.txt

5):-

Wireshark for LAN Network scanning

First scan Windows machine with nmap from kali

Nmap 192.168.0.112

Go to wireshark in windows vm which is nmap target and packets are sent from kali to look for open ports in windows vm

If you see SYN-ACK packets from the target in response to your SYN packets, this indicates that the port is open.

Screenshots are provided for wireshark open port monitoring

6:-

1. Methodology

Describe the methods and tools used during the assessment.

- **Host Discovery**: Used the `ping` command to identify live hosts.
- **Port Scanning**: Conducted a non-intrusive scan using tools like `nmap`.
- **OS Discovery**: Identified operating systems using fingerprinting techniques.
- **Scanning Beyond IDS/Firewall**: Tested the network's defense mechanisms.
- **Network Analysis**: Monitored network traffic using Wireshark.

2. Findings

Host Discovery

- **Tools Used**: `ping`
- **Results**: Number of live hosts identified, IP addresses, and response times.
- **Insights**: Stability and availability of the hosts.

Port Scanning

- **Tools Used**: `nmap`
- **Results**: List of open ports, services running on those ports.

- **Insights**: Potential entry points and exposure of critical services.

OS Discovery

- **Tools Used**: `nmap -O`
- **Results**: OS types and versions.
- **Insights**: Vulnerability to specific OS-related exploits.

Scanning Beyond IDS/Firewall

- **Tools Used**: `nmap`, `metasploit` (optional)
- **Results**: Bypassed defense mechanisms, identified hidden vulnerabilities.
- **Insights**: Effectiveness of IDS/Firewall configurations.

Network Analysis Using Wireshark

- **Tools Used**: Wireshark
- **Results**: Captured network traffic, identified open ports and services.
- **Insights**: Unencrypted sensitive data, anomalous traffic patterns.

3. Vulnerabilities and Risks

Detail each vulnerability discovered, its risk level, potential impact, and how it could be exploited.

- **Example**: Open SSH Port
  - **Risk Level**: High
  - **Impact**: Unauthorized access to server
  - **Exploitation**: Brute-force attacks, weak password exploits

4. Recommendations

Provide actionable steps to mitigate each identified vulnerability.

- **Secure Open Ports**: Close unnecessary ports, implement port filtering.
- **OS Updates**: Patch outdated operating systems.
- **IDS/Firewall Enhancements**: Update rules, implement deep packet inspection.
- **Encrypt Traffic**: Use TLS/SSL for sensitive data transmission.
- **Regular Audits**: Conduct periodic security assessments.