Network Scanning and Enumeration

MODULE 2

Agenda

1.Scanning Networks

2.Network Scanning Concepts

3.Scanning Tools and Techniques

4.Scanning Beyond IDS and Firewall

5.Banner Grabbing

6.Draw Network Diagrams 7.Scanning Pen Testing

8.Enumeration Concepts 9.NetBIOS, SNMP, LDAP, NTP, SMTP, and DNS Enumeration 10.Enumeration Countermeasures 11.Other Enumeration Techniques 13.Enumeration Pen Testing

Scanning Network

Network scanning is a method used to identify active hosts, open ports, and available services on a network. It provides insights into the network's structure, aiding in the identification of potential entry points and security vulnerabilities.

WHY IS NETWORK SCANNING NECESSARY

- **Identify Live Hosts**: Determine which devices or hosts are active on a network.
- **Find Open Ports**: Discover accessible services by identifying open ports on each device.
- **Analyze Services**: Assess the type and version of services running on each open port, helping to evaluate the network's security posture.

TYPES OF SCANS

- **Ping Sweep**: Determines which hosts are online by sending ICMP echo requests.
- **Port Scan**: Scans each host for open ports to identify accessible services.
- **Service and Version Detection**: Probes open ports to identify the specific software and version running.

Practical Time

A common network scanning activity is a **ping sweep**. This scan sends an ICMP (Internet Control Message Protocol) request to each IP address in a subnet to check if a device is responding, helping to locate active devices.

```
$ nmap -sn 192.168.1.0/24
```

- This command targets the entire subnet 192.168.1.0/24 and checks for active hosts by performing a ping sweep.
- The output will list all active devices (hosts) that responded to the scan. For each active device, Nmap will display the IP address, and potentially the hostname, helping to build a basic network map.

Network Scanning Concepts

Network scanning is a crucial activity in cybersecurity that involves identifying devices, services, and vulnerabilities within a network. Understanding the fundamental concepts of network scanning helps professionals effectively assess and secure their environments.

TYPES OF SCANS

- **Active Scanning**: This method involves actively sending requests to devices on a network and analyzing their responses. Active scans can reveal open ports, services running, and potentially identify vulnerabilities. However, they can be noisy and might trigger alarms on intrusion detection systems (IDS).

- **Passive Scanning**: In contrast, passive scanning involves monitoring network traffic without sending any requests. It analyzes data packets to gather information about devices and services. This method is stealthier and less likely to alert security systems, but it may not provide as comprehensive a view as active scanning.

Active Scanning

```
$ nmap -sS -p 1-1000 192.168.1.10
```

Explanation:

- **-sS**: This flag specifies a SYN scan, which is a stealthy way to determine open ports.
- **-p 1-1000**: This option tells Nmap to scan the first 1,000 ports.
- **192.168.1.10**: The target IP address of the web server.

This example illustrates how active scanning actively interacts with the target to gather information about open ports and services.

Scanning Tools and Techniques

Network scanning tools and techniques are essential for identifying devices, services, and vulnerabilities within a network. Here are some popular tools and techniques commonly used in network scanning:

POPULAR SCANNING TOOLS

- **Nmap**: A widely-used network scanning tool that allows users to discover hosts and services on a network. It supports various scanning techniques and provides detailed information about the detected services and their versions.
- **Nessus**: A comprehensive vulnerability scanner that not only detects open ports and services but also assesses vulnerabilities in those services. It is often used for conducting thorough security assessments.
- **Angry IP Scanner**: A fast and lightweight tool that scans IP addresses in a given range and provides information about active hosts and their open ports.
- **OpenVAS**: An open-source vulnerability scanning tool that offers extensive scanning capabilities and is designed to identify security issues in systems.

COMMON SCANNING TECHNIQUES

- **TCP/IP Scanning**: This technique involves sending TCP packets to target ports to determine their status (open, closed, or filtered). It’s effective for discovering services running on a network.
- **Ping Sweeps**: A method used to identify live hosts on a network by sending ICMP echo requests (ping) to multiple IP addresses. This helps in quickly determining which devices are active.
- **Service Version Detection**: Some tools (like Nmap) can query open ports to determine the version of the service running, providing insight into potential vulnerabilities.

Using Nmap to Perform a TCP Scan

Scenario: A network administrator wants to discover open ports on a specific server to assess its security.

```
$ nmap -sT -p 1-65535 192.168.1.10
```

Explanation:

- **-sT**: This flag specifies a TCP connect scan. It completes the TCP handshake to check for open ports.
- **-p 1-65535**: This option tells Nmap to scan all 65,535 TCP ports on the target.
- **192.168.1.10**: The target IP address of the server.

Scanning beyond IDS and Firewall

When conducting network scans, it's essential to consider the presence of Intrusion Detection Systems (IDS) and firewalls, which are designed to monitor and restrict unauthorized access to networks. To effectively gather information without triggering alarms, various stealth techniques can be employed. Here are some strategies for scanning that can help bypass these security measures:

STEALTH SCANNING TECHNIQUES:

- **SYN Scanning**: This method involves sending SYN packets to the target ports to initiate a TCP handshake. If a port is open, the target responds with a SYN-ACK, while closed ports respond with a RST. This technique is less likely to be logged by IDS compared to a full TCP connect scan.
- **Fragmentation**: By breaking up the scanning packets into smaller fragments, it can be challenging for firewalls and IDS to reconstruct and analyze them, potentially allowing some packets to bypass detection.
- **Idle Scanning**: This technique uses a third-party host (an idle machine) to send packets to the target, making it appear that the idle host is performing the scan. This can be effective in remaining under the radar of IDS and firewalls.

TIMING AND PERFORMANCE:

- **Slow Scans**: Slowing down the scan speed can reduce the likelihood of detection. Tools like Nmap allow users to adjust timing templates, which can help avoid triggering security alerts.
- **Randomized Targeting**: Scanning targets in a non-sequential order can help evade detection and reduce the chances of being flagged by monitoring systems.

USE OF DECOY SCANS:

Sending scans from multiple IP addresses can obscure the source of the scan. By using decoy options in tools like Nmap, it becomes harder for IDS to identify the actual scanning IP.

Utilizing SYN Scanning in Nmap

Scenario: A penetration tester wants to check for open ports on a server while minimizing the risk of detection by an IDS.

```
$ nmap -sT -p 1-65535 192.168.1.10
```

Explanation:

- **-sT**: This flag specifies a TCP connect scan. It completes the TCP handshake to check for open ports.
- **-p 1-65535**: This option tells Nmap to scan all 65,535 TCP ports on the target.
- **192.168.1.10**: The target IP address of the server.

This example illustrates how SYN scanning with Nmap can effectively gather information about open ports while minimizing the risk of detection by IDS and firewalls, making it a valuable technique in network assessments.

Banner Grabbing

Banner grabbing is a technique used in network security to collect information about the services and applications running on a server. By connecting to specific ports and querying for information, attackers and security professionals can identify the software versions and configurations of services. This information is valuable for:

- **Identifying Services**: Banner grabbing helps determine which services are running on a particular host. For example, connecting to a web server can reveal whether it is running Apache, Nginx, or another service.
- **Version Detection**: By analyzing the banner information, one can identify the specific version of the software in use. This is crucial because certain versions may have known vulnerabilities.
- **Vulnerability Assessment**: Knowing the software and version allows security professionals to cross-reference this information with vulnerability databases (like CVE) to identify potential security issues that need addressing.
- **Network Mapping**: Banner grabbing can be part of a larger reconnaissance effort, helping to map out services and systems within a network.

Using cURL for Banner Grabbing

Scenario: A security analyst wants to gather information about a web server to identify its software version.

```
$ curl -I http://evil.com
```

Explanation:

- **curl: This command invokes cURL.**
- **-I: This option tells cURL to fetch only the HTTP headers, which typically include the server banner.**
- **http://evil.com This is the target URL of the web server.**

This example shows how cURL can be effectively utilized for banner grabbing, providing valuable insights into the software running on a web server, which is crucial for assessing security and identifying potential vulnerabilities.

Scanning in Penetration Testing

Scanning is a fundamental phase in penetration testing (pen testing), where security professionals simulate attacks to identify vulnerabilities in systems and networks. The integration of scanning into pen testing is crucial for several reasons:

- **Vulnerability Identification**: Scanning helps uncover vulnerabilities that could be exploited by attackers. This includes identifying open ports, services running, and software versions that may be outdated or misconfigured.

- **Comprehensive Assessment**: By employing various scanning techniques (e.g., active and passive scanning), pen testers can gain a thorough understanding of the target environment, allowing for a more effective assessment of security posture.

- **Prioritization**: Scanning results help pen testers prioritize vulnerabilities based on severity, potential impact, and exploitability. This allows them to focus on the most critical issues first.

- **Planning Exploits**: Understanding the vulnerabilities and the network layout informs the planning of specific attack vectors during the exploitation phase of the pen test.

Enumeration Concepts

Enumeration is a critical phase in the information-gathering process of network security assessments. It involves extracting detailed information from a network or system to identify resources, configurations, and potential vulnerabilities. The key aspects of enumeration include:

- The primary goal of enumeration is to gather specific details about users, groups, services, shares, and network resources. This information can be vital for planning attacks or improving security.

- Enumeration techniques can vary based on the target system and protocol. Common methods include:
  - Querying services for user accounts.
  - Retrieving network shares and their permissions.
  - Gathering information about running services and applications.

- Successful enumeration can reveal critical information that attackers could leverage for further exploitation, making it an essential step in both offensive and defensive security practices.

NetBIOS, SNMP, LDAP, NTP, SMTP, and DNS Enumeration

- **NetBIOS (Network Basic Input/Output System)**:
  - **Purpose**: Used primarily in Windows networks for file sharing and communication.
  - **Significance**: Allows enumeration of users, groups, and shared resources on Windows machines. Tools like nbtscan can be used to gather this information.
- **SNMP (Simple Network Management Protocol)**:
  - **Purpose**: Used to manage and monitor network devices like routers, switches, and printers.
  - **Significance**: SNMP can provide extensive details about device configurations, performance metrics, and security vulnerabilities. Tools like snmpwalk are commonly used for enumeration.
- **LDAP (Lightweight Directory Access Protocol)**:
  - **Purpose**: Used for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.
  - **Significance**: Allows for the enumeration of user accounts, groups, and organizational units in an Active Directory environment. Tools like ldapsearch can be utilized for this purpose.

- **NTP (Network Time Protocol)**:
  - **Purpose**: Used to synchronize the clocks of computers over a network.
  - **Significance**: NTP can provide information about network devices' configurations and can potentially be exploited if not securely configured.
- **SMTP (Simple Mail Transfer Protocol)**:
  - **Purpose**: Used for sending emails.
  - **Significance**: Can be used for enumeration through commands like VRFY and EXPN, allowing testers to discover valid email addresses and potentially exploit weaknesses in the email server.
- **DNS (Domain Name System)**:
  - **Purpose**: Resolves domain names to IP addresses.
  - **Significance**: Enumeration can reveal information about domain structure, hostnames, and services. Tools like dig or nslookup can be used to gather this information.

Using SNMPwalk to Gather Device Information from a Network Printer

Scenario: A network administrator or penetration tester wants to gather information about a network printer to identify its configuration and potential vulnerabilities.

```
$ snmpwalk -v 2c -c public <printer_ip>
```

- **snmpwalk**: This command invokes the SNMPwalk tool, which retrieves information using SNMP.
- **-v 2c**: Specifies the SNMP version (in this case, version 2c).
- **-c public**: Specifies the community string used to access the SNMP data (commonly set to "public" for many devices).
- **<printer_ip>**: The IP address of the network printer.

How to Find printer ip ?

SHODAN DORKING ?

Printer Model: HP LaserJet Pro MFP

```
HP LaserJet Pro MFP "SNMP"
```

The above dorks helps in getting the Hp LaserJet Pro printer which are using SNMP

Enumeration Countermeasures

Enumeration poses significant risks to network security, as it enables attackers to gather sensitive information about systems, users, and configurations. To mitigate these risks, organizations can implement various countermeasures, including hardening techniques, security configurations, and ongoing monitoring.

STRATEGIES TO MITIGATE RISKS

1. **System Hardening**
2. **Security Configurations**
3. **Network Segmentation**
4. **Monitoring and Logging**
5. **User Education and Awareness**

Other Enumeration Techniques

In addition to the commonly discussed enumeration techniques, various other methods leverage network services and application-layer protocols to gather valuable information about systems, users, and network configurations. These techniques can be effective in identifying vulnerabilities but also pose significant risks if not properly managed. Below are several additional enumeration techniques, their effectiveness, and associated risks.

DIFFERENT TYPES OF ENUMERATION TECHNIQUES

FTP Enumeration:

- **Technique**: Use FTP commands to enumerate users and files on FTP servers. Commands like USER and PASS can be exploited to gather information about valid usernames.
- **Effectiveness**: Many FTP servers are misconfigured, allowing anonymous access or revealing user directories.
- **Risks**: Exposure of sensitive files and user credentials can lead to unauthorized access or data breaches.

HTTP Enumeration:

- **Technique**: Enumerate web applications by sending crafted HTTP requests to gather information about the application’s structure, such as valid endpoints, API methods, and hidden files.
- **Effectiveness**: Tools like Burp Suite and OWASP ZAP can automate this process, revealing configuration details or vulnerabilities like directory traversal.
- **Risks**: Excessive probing can lead to denial-of-service conditions, and misconfigured applications can leak sensitive data.

SMTP Enumeration:

- **Technique**: Use SMTP commands like VRFY and EXPN to enumerate valid email addresses and distribution lists on mail servers.
- **Effectiveness**: Effective against poorly secured mail servers that respond to these commands.
- **Risks**: Revealing valid email addresses can facilitate phishing attacks or social engineering.

Enumeration Pen Testing

Enumeration plays a critical role in the penetration testing (pen testing) lifecycle, serving as a vital step in the information-gathering phase. It involves extracting detailed information about systems, users, and configurations, which is essential for understanding the security posture of the target environment. The information gathered during enumeration helps pen testers identify vulnerabilities and plan their exploitation strategies effectively.

KEY CONTRIBUTIONS OF ENUMERATION IN PEN TESTING:

1. **Information Gathering**: Enumeration provides a comprehensive understanding of the target's architecture, including user accounts, group memberships, network resources, and services running on devices.
2. **Identifying Attack Vectors**: By enumerating systems and users, pen testers can pinpoint potential attack vectors, such as weak user accounts, misconfigured services, and exposed network resources.
3. **Prioritizing Risks**: The detailed information collected during enumeration allows testers to prioritize risks based on the criticality of the discovered accounts and services. This prioritization aids in focusing the testing efforts on the most vulnerable areas.

</>

Any Doubts ?

Hope you Enjoyed the Session

THANK YOU FOR JOINING