UNIT - IV

Enumeration: Enumeration Techniques, Soft Objective, Looking Around or Attack, Elements of Enumeration, Preparing for the Next Phase.

Exploitation: Intuitive Testing, Evasion, Threads and Groups, Operating Systems, Password Crackers, Root Kits, applications, War dialing, Network, Services and Areas of Concern.

Enumeration and Exploitation

1. Enumeration

Definition

Enumeration is the process of gathering detailed information about a target system after initial scanning.
It helps attackers or security testers identify:

- User accounts
- Shared resources
- Network services
- Operating systems
- Applications
- System information

Enumeration is commonly used in:

- Ethical hacking
- Penetration testing
- Cybersecurity assessments

1.1 Enumeration Techniques

Enumeration techniques are methods used to extract information from a target system.

Common Techniques

1. NetBIOS Enumeration

Used to gather:

- Computer names
- Shared folders
- User accounts

Example

Command:

```
nbtstat -A 192.168.1.10
```

This displays NetBIOS information of the target.

2. SNMP Enumeration

Uses the Simple Network Management Protocol to collect device information.

Information Collected

- Routing tables
- Network devices
- System names

Example

```
snmpwalk -v1 -c public 192.168.1.1
```

3. LDAP Enumeration

Used in directory services like Microsoft Active Directory.

Information Collected

- User accounts
- Groups
- Organizational units

4. DNS Enumeration

Used to gather DNS records.

Example

```
nslookup
dig example.com
```

5. SMTP Enumeration

Used to verify valid email users on mail servers.

Example

```
VRFY admin
```

1.2 Soft Objective

Definition

Soft objectives are indirect goals achieved during enumeration without directly attacking the target.

Purpose

- Understand the environment
- Identify weaknesses
- Collect useful information

Examples

- Identifying employee names
- Finding email formats
- Discovering server versions

Example

An attacker gathers employee emails from company websites before phishing attacks.

1.3 Looking Around or Attack

Looking Around

This means passive observation without damaging the system.

Activities

- Browsing open shares
- Reading banners
- Identifying services

Example

Checking open ports using:

```
nmap 192.168.1.5
```

Attack

After gathering information, attackers may exploit vulnerabilities.

Example

Using weak credentials found during enumeration to access a server.

1.4 Elements of Enumeration

Enumeration contains several important elements.

1. User Enumeration

Finding usernames on a system.

Example

```
enum4linux -U 192.168.1.20
```

2. Group Enumeration

Finding user groups and permissions.

Example

Administrators group in Windows.

3. Network Resource Enumeration

Identifying:

- Shared folders
- Printers
- Services

4. Service Enumeration

Discovering running services.

Example

FTP, SSH, HTTP services.

5. System Enumeration

Gathering:

- OS details

- Hostnames
- Device types

1.5 Preparing for the Next Phase

After enumeration, attackers or testers prepare for exploitation.

Activities

- Analyzing collected data
- Identifying vulnerabilities
- Selecting attack methods
- Prioritizing targets

Example

If enumeration reveals:

- Open SSH port
- Weak password policy

Then password attacks may be planned.

2. Exploitation

Definition

Exploitation is the process of taking advantage of vulnerabilities to gain unauthorized access or control.

It is performed after scanning and enumeration.

2.1 Intuitive Testing

Definition

Testing based on logical thinking and experience rather than automated tools alone.

Purpose

- Identify hidden weaknesses
- Test unusual attack paths

Example

Trying default credentials:

```
admin/admin
```

2.2 Evasion

Definition

Methods used to avoid detection by security systems.

Techniques

- Packet fragmentation
- Encryption
- Spoofing IP addresses

Example

Using stealth scanning in Nmap:

```
nmap -sS 192.168.1.1
```

2.3 Threads and Groups

Threads

Definition

Threads are lightweight processes executed simultaneously.

Purpose in Exploitation

- Faster attacks
- Parallel scanning

Example

Password crackers using multiple threads.

Groups

Definition

Collections of users with similar privileges.

Importance

Attackers target privileged groups like:

- Administrators
- Root users

2.4 Operating Systems

Purpose

Attackers identify operating systems to choose suitable exploits.

Common OS Targets

- Windows
- Linux
- macOS

Example

OS detection using:

```
nmap -O 192.168.1.5
```

2.5 Password Crackers

Definition

Tools used to recover passwords.

Types

- Dictionary attacks
- Brute-force attacks
- Rainbow table attacks

Examples

- John the Ripper
- Hashcat

Example

Trying multiple passwords automatically.

2.6 Root Kits

Definition

Malicious software that hides attacker activities and provides privileged access.

Purpose

- Maintain persistence
- Hide files/processes

Types

- Kernel rootkits
- User-mode rootkits

Example

A rootkit hides malware from antivirus programs.

2.7 Applications

Definition

Software applications can contain vulnerabilities.

Common Targets

- Web browsers
- Email clients
- Database applications

Example

SQL Injection attack on a web application.

2.8 War Dialing

Definition

Technique used to scan telephone numbers for modems.

Purpose

- Find remote access systems

Example

Automated dialing software tests phone numbers for modem responses.

2.9 Network

Network Exploitation Areas

Attackers may target:

- Routers
- Switches
- Firewalls
- Wireless networks

Example Attacks

- ARP spoofing
- Packet sniffing
- Denial of Service (DoS)

2.10 Services and Areas of Concern

Services

Network services often targeted include:

- FTP
- SSH

- HTTP
- DNS
- SMTP

Areas of Concern

1. Weak Passwords

Easy-to-guess passwords.

2. Unpatched Systems

Old software vulnerabilities.

3. Misconfigurations

Incorrect security settings.

4. Open Ports

Unnecessary services exposed.

5. Lack of Encryption

Sensitive data transmitted openly.

Overall Flow of Enumeration and Exploitation

1. Scanning
2. Enumeration
3. Vulnerability Identification
4. Exploitation
5. Privilege Escalation
6. Maintaining Access

Short Summary Table

Topic	Description
Enumeration	Collecting detailed system information
Enumeration Techniques	Methods like SNMP, DNS, LDAP
Soft Objective	Indirect information gathering
Looking Around	Passive observation
Exploitation	Using vulnerabilities to gain access
Evasion	Avoiding detection
Password Crackers	Recovering passwords

Root Kits	Hiding attacker presence
War Dialing	Searching for modem systems
Services & Concerns	Weaknesses in services and configurations