UNIT – III

Preparing for a Hack: Technical Preparation, Managing the Engagement Reconnaissance: Social Engineering, Physical Security, Internet Reconnaissance

Preparing for a Hack:

1) **Technical Preparation**

Technical Preparation is the process of gathering information, configuring tools, understanding the target environment, and planning testing activities before conducting an authorized ethical hacking or penetration testing exercise.

Objectives

- Understand the target environment.
- Identify potential vulnerabilities.
- Prepare tools and resources.
- Ensure efficient and safe testing.
- Minimize risks to business operations.

Steps in Technical Preparation

1. Understand the Scope

- Review the systems, networks, and applications to be tested.
- Identify testing boundaries and restrictions.
- Verify authorization and permissions.

2. Gather Target Information

Collect information about:

- IP addresses
- Domain names
- Network architecture
- Operating systems
- Applications and services

Techniques

- Open-Source Intelligence (OSINT)
- DNS lookups
- WHOIS information
- Public website analysis

3. Prepare the Testing Environment

- Configure testing systems.
- Update operating systems and security tools.
- Verify network connectivity.
- Create backups if necessary.

4. Select Appropriate Tools

Common tools used during ethical hacking:

Category	Examples
Network Scanning	Nmap
Packet Analysis	Wireshark
Vulnerability Assessment	Nessus
Web Security Testing	Burp Suite

Penetration Testing	Metasploit Framework

5. Verify Access Requirements

- Obtain necessary credentials.
- Ensure access to testing environments.
- Confirm communication channels with stakeholders.

6. Review Previous Test Results

- Analyze past vulnerabilities.
- Verify remediation status.
- Identify recurring security issues.

7. Establish Documentation

Prepare:

- Testing plan
- Scope document
- Rules of engagement
- Incident response procedures
- Reporting templates

8. Assess Potential Risks

- Identify systems sensitive to testing.
- Determine possible service impacts.
- Define emergency stop procedures.

Technical Preparation Checklist

Activity	Status
Authorization Obtained	✓
Scope Defined	✓
Information Gathered	✓
Tools Prepared	✓
Access Verified	✓
Previous Results Reviewed	✓
Documentation Ready	✓
Risk Assessment Completed	✓

Importance of Technical Preparation

- Improves testing efficiency.
- Reduces operational risks.
- Enhances vulnerability detection.
- Ensures compliance with organizational policies.
- Produces more accurate assessment results.

Managing the Engagement Reconnaissance:

Managing the Engagement: **The process of planning, coordinating, monitoring, and controlling a security assessment or penetration test to ensure it is completed safely, effectively, and within the agreed scope.**

Reconnaissance

Reconnaissance is the first phase of ethical hacking and penetration testing in which information about the target is collected. It is also known as **information gathering** or **footprinting**.

Objectives

- Understand the target environment.
- Identify potential attack surfaces.
- Gather information useful for later testing phases.

Types of Reconnaissance

1. Passive Reconnaissance

Information is collected without directly interacting with the target.

Examples:

- Search engine research
- Social media analysis
- Public records review
- WHOIS lookups

2. Active Reconnaissance

Information is collected through direct interaction with the target.

Examples:

- Network scanning
- Port scanning
- Service enumeration
- Banner grabbing

Information Gathered During Reconnaissance

Information Type	Examples
Network Information	IP addresses, network ranges
Domain Information	Domain names, DNS records
System Information	Operating systems, services
Employee Information	Email addresses, job roles
Web Information	Websites, technologies used

Reconnaissance Process

```
Target Identification
         ↓
Information Gathering
         ↓
Network Discovery
         ↓
Service Identification
         ↓
Vulnerability Identification
```

1) Social Engineering:

Social Engineering is the practice of manipulating, deceiving, or influencing people into revealing confidential information or performing actions that compromise security. Instead of attacking technical systems directly, social engineering exploits **human behavior and trust**.

Objectives

- Obtain sensitive information.
- Gain unauthorized access to systems.
- Bypass security controls.
- Trick users into performing actions beneficial to the attacker.

Common Social Engineering Techniques

1. Phishing

- Fraudulent emails or messages designed to steal usernames, passwords, or financial information.

2. Spear Phishing

- Targeted phishing attacks directed at specific individuals or organizations.

3. Vishing (Voice Phishing)

- Attackers use phone calls to deceive victims into revealing confidential information.

4. Smishing (SMS Phishing)

- Fraudulent text messages used to obtain sensitive information.

5. Pretexting

- Creating a fabricated scenario or identity to gain a victim's trust.

6. Baiting

- Offering something attractive (such as free software or a USB drive) to entice victims into compromising security.

7. Tailgating (Piggybacking)

- Gaining physical access to restricted areas by following an authorized person.

8. Impersonation

- Pretending to be a trusted employee, vendor, or authority figure.

Social Engineering Attack Process

```
Information Gathering
         ↓
Target Selection
         ↓
Building Trust
         ↓
Exploitation
         ↓
Obtaining Information or Access
```

Human Factors Exploited

Factor	Description
Trust	Believing someone is legitimate
Fear	Responding to threats or urgency
Curiosity	Desire to know or obtain something
Greed	Attraction to rewards or benefits
Authority	Obedience to perceived authority figures

Helpfulness	Willingness to assist others

Prevention Measures

- Security awareness training.
- Verification of identities and requests.
- Strong authentication mechanisms.
- Careful handling of emails, links, and attachments.
- Regular security policies and procedures.
- Reporting suspicious activities promptly.

Advantages for Attackers

- Often easier than technical attacks.
- Can bypass sophisticated security technologies.
- Exploits natural human behavior.

2) Physical Security:

Physical Security refers to the protection of people, hardware, facilities, equipment, and other physical assets from unauthorized access, theft, damage, sabotage, or natural disasters.

Objectives

- Prevent unauthorized physical access.
- Protect information systems and equipment.
- Safeguard employees and visitors.
- Ensure business continuity.
- Reduce risks from theft, vandalism, and disasters.

Importance of Physical Security

Even the strongest cybersecurity measures can be bypassed if an attacker gains physical access to systems, servers, or network devices. Physical security is therefore a critical component of overall information security.

Physical Security Controls

1. Perimeter Security

Protects the outer boundary of a facility.

Examples:

- Fences
- Gates
- Security guards
- Surveillance cameras (CCTV)

2. Access Control Systems

Restricts entry to authorized personnel only.

Examples:

- ID cards
- Smart cards
- Biometric authentication
- Keypad locks

3. Environmental Controls

Protects equipment from environmental threats.

Examples:

- Fire suppression systems
- Smoke detectors

- Air conditioning systems
- Water leak detection

4. Monitoring and Surveillance

Monitors activities within facilities.

Examples:

- CCTV cameras
- Alarm systems
- Motion detectors
- Security monitoring centers

5. Equipment Protection

Protects hardware and network devices.

Examples:

- Locked server rooms
- Cable locks
- Equipment cabinets
- Asset tracking systems

Physical Security Threats

Threat	Description
Theft	Unauthorized removal of equipment or data
Vandalism	Intentional damage to property
Unauthorized Access	Entry by unauthorized individuals
Fire	Damage caused by fire incidents
Natural Disasters	Floods, earthquakes, storms, etc.
Power Failure	Loss of electrical power affecting operations
Tailgating	Following authorized personnel into secure areas

Layers of Physical Security

```
Perimeter Security
        ↓
Building Security
        ↓
Floor Security
        ↓
Room Security
        ↓
Device Security
```

3) Internet Reconnaissance

Internet Reconnaissance is the process of collecting information about a target organization, system, or individual from publicly available Internet sources. It is usually the first phase of ethical hacking and penetration testing and is also known as **Internet Footprinting**.

Objectives

- Gather information about the target.
- Identify potential attack surfaces.
- Discover network and system details.
- Support vulnerability assessment and security testing.

Types of Internet Reconnaissance

1. Passive Reconnaissance

Information is collected without directly interacting with the target.

Examples:

- Search engine research
- Social media analysis
- Public websites
- WHOIS records
- Job postings

2. Active Reconnaissance

Information is collected through direct interaction with the target systems.

Examples:

- DNS queries
- Network scanning
- Port scanning
- Service enumeration

Information Gathered During Internet Reconnaissance

Information Type	Examples
Domain Information	Domain names, subdomains
Network Information	IP addresses, network ranges
DNS Information	DNS records, mail servers
Employee Information	Names, email addresses, job roles
Technology Information	Operating systems, web servers, software versions
Organizational Information	Business locations, partners, suppliers

Common Internet Reconnaissance Techniques

Search Engine Analysis

- Collect information from public search engines.
- Identify exposed documents and web pages.

WHOIS Lookup

- Obtain domain registration details.
- Identify domain owners and contact information.

DNS Enumeration

- Discover DNS records and network infrastructure.

Website Analysis

- Examine websites for technologies and exposed information.

Social Media Research

- Gather information about employees and organizational activities.

Reconnaissance Process

```
Target Identification
        ↓
Information Gathering
        ↓
Domain and DNS Analysis
        ↓
Network Discovery
        ↓
Technology Identification
        ↓
Security Assessment Planning
```

Benefits

- Provides valuable intelligence about the target.
- Helps identify potential vulnerabilities.
- Supports effective penetration testing.
- Reduces testing time and effort.