

Advanced data Security

Part II: Communication Security

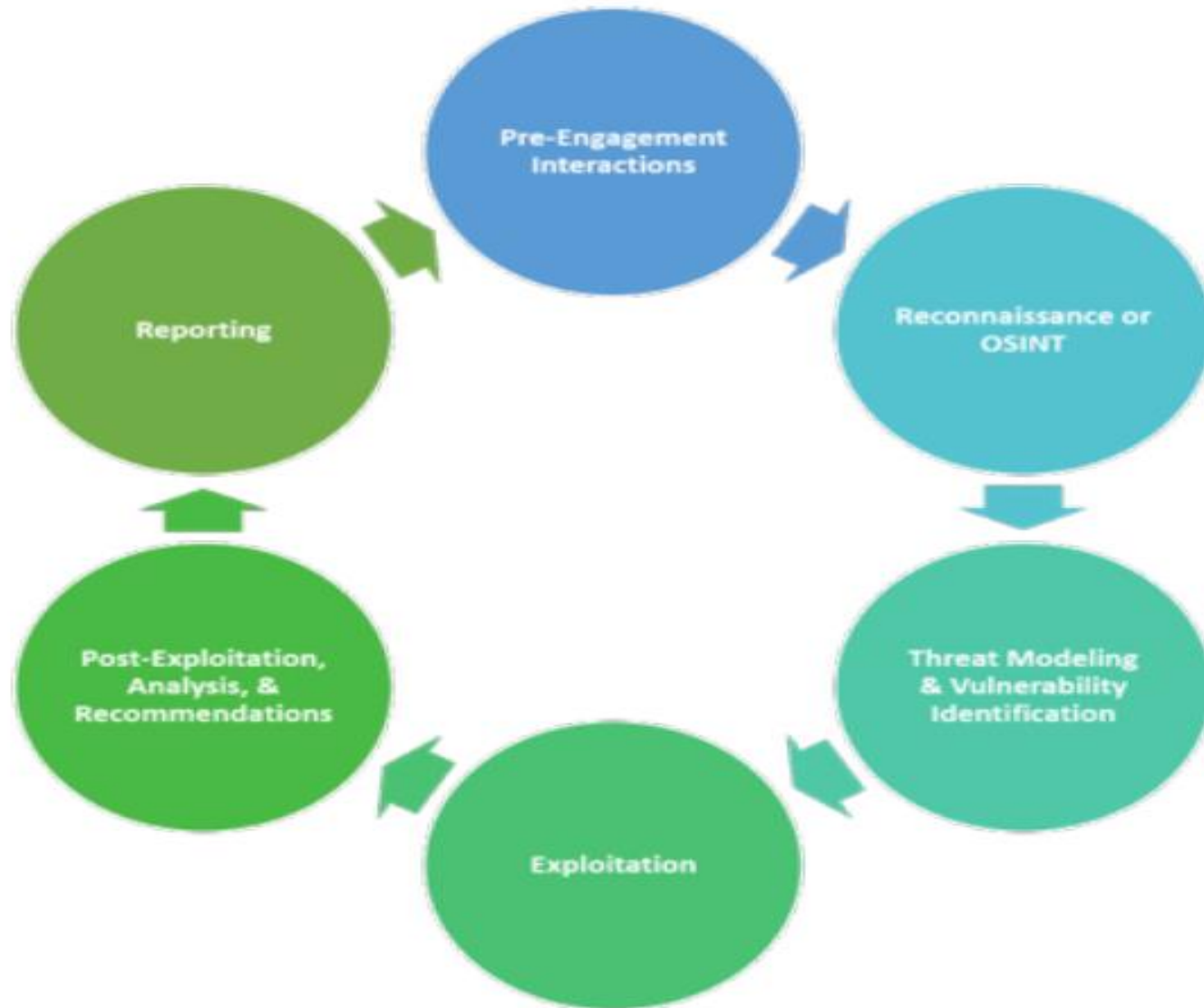
Chapter 9: Penetration Testing

Prepared by:
Dr. Hamssa Hasrouny

Penetration testing

- Penetration test or [security testing](#).
- Conducting a [regular penetration test](#) is a helpful way to identify serious vulnerabilities within your IT environment.
- A [trusted ethical hacker](#) performs the penetration test using a [methodical](#) and thorough approach.
- **Why** does your technology and environment need penetration testing?
 - Because every business has something to lose- and data is [one of the most valuable assets](#) that a hacker can gain. Whether through an [application, device, or network](#).
 - the data you are responsible for, is at risk when you don't verify the security measures protecting it.
- Whose job is on the line if your clients' data (or your organization's other assets) are compromised?
 - Investing in penetration testing is one way to [show clients](#), prospects, and competitors that you are willing to take every step necessary to [safeguard the data](#) that has been entrusted to you.

Phases of Penetration Testing



Phases of Penetration Testing(1)

The phases are critical to the successful planning and execution of a penetration test.

1. Pre-Engagement Interactions or Information gathering:

- During this pre-phase, a penetration testing company will outline the logistics of the test, expectations, legal implications, objectives and goals the customer would like to achieve.
- the penetration testers should work with company to fully understand any risks, the organizational culture, and the best pentesting strategy for the organization.
- You may want to perform a white box, black box, or gray box penetration test.
- The planning occurs along with aligning your goals to specific pentesting outcomes.

Phases of Penetration Testing(2)

2. Reconnaissance or Open Source Intelligence (OSINT) Gathering:

- The whole point of this phase is **getting to know the target**.
- A pentester works on gathering as much intelligence on your organization and **the potential targets for exploit**.
- Who are **the important people** in the company?
 - This can be answered by looking at the company web site or LinkedIn.
- Who do they **do business with**?
 - they may be able to use social engineering, by make a few “sales calls” to the company.
- What **public data is available** about the company?
 - Hackers collect IP address information and run scans to determine what hardware and software they are using.
- A pentester uses an exhaustive checklist for finding open entry points and vulnerabilities within the organization.

Phases of Penetration Testing(2)

2. Reconnaissance or Open Source Intelligence (OSINT) Gathering:

- Common intelligence gathering techniques include:
 - **Search engine queries:** a request for information that is made using a search engine.
 - **Domain name searches/WHOIS lookups:** WHOIS Tool To See Who Owns a Domain and Access Registration Data.
 - **Social Engineering**
 - **Internet Footprinting** – email addresses, usernames, social networks,
 - **Internal Footprinting** –Ping sweeps, port scanning, reverse DNS, packet sniffing:
 - **Ping sweeps:** a network scanning technique used to determine which of a range of IP addresses map to live hosts (computers).
 - **reverse DNS:** If you type in an IP address, we will attempt to locate a dns PTR record for that IP address.

Phases of Penetration Testing(3)

3. Threat Modeling and Vulnerability Identification: (Discovery and Scanning – Vulnerability assessment)

- the tester identifies targets and maps the attack vectors. Any information gathered during the Reconnaissance phase is used to inform the method of attack during the penetration test.
- The most common areas a pentester will map and identify include:
 - Business assets – identify and categorize high-value assets
 - Employee data
 - Customer data
 - Technical data
 - Threats – identify and categorize internal and external threats
 - Internal threats – Management, employees, vendors, etc.
 - External threats – Ports, Network Protocols, Web Applications, Network Traffic, etc..
- A pentester uses a **vulnerability scanner** to complete a **discovery and inventory** on the security risks posed by identified vulnerabilities.
- Then validates if the vulnerability is exploitable.

Phases of Penetration Testing(4)

4. Exploitation:

- the pentester begins to test the exploits found within your network, applications, and data.
- The goal is for the ethical hacker is to **see exactly how far they can get into** your environment, identify high-value targets, and avoid any detection.
- Some of the standard exploit tactics include:
 - **Web Application Attacks:** attempt by a malicious actor to compromise the security of a Web-based application.
 - target either the application itself to gain access to sensitive data,
 - or use the application to launch attacks against users of the application.
 - **Network Attacks:** attempt to gain unauthorized access to an organization's network, with the objective of stealing data or perform other malicious activity.
 - **Memory-based attacks:** exploit the most common vulnerability in applications (buffer overflows)
 - **Zero-Day Angle:** an attack that exploits a potentially serious software security weakness that the vendor or developer may be **unaware of**.
 - **Wi-Fi attacks, Physical Attacks, Social engineering**

Phases of Penetration Testing(5)

5. Post-Exploitation, Risk Analysis and Recommendations:

- After the exploitation, the goal is to document the methods used to gain access to your organization's valuable information.
- The penetration tester should be able to determine the value of the compromised systems and any value associated with the sensitive data captured.
- Some pentesters are unable to quantify the impact of accessing data or to provide recommendations on how to remediate the vulnerabilities within the environment.
- Make sure you ask a sanitized penetration testing report that clearly shows recommendations for fixing security holes and vulnerabilities.
- Once the penetration testing recommendations are complete, the tester should:
 - clean up the environment,
 - reconfigure any access he/she obtained to penetrate the environment,
 - prevent future unauthorized access into the system.

Phases of Penetration Testing(5cont)

5. Post-Exploitation, Risk Analysis & Recommendations:

- Typical cleanup activities include:
 - **Removing** any executables, scripts, and temporary files from compromised systems
 - Reconfiguring settings **back to the original** parameters prior to the pentest
 - Eliminating any rootkits installed in the environment
 - Removing any user accounts created to connect to the compromised system

Phases of Penetration Testing(6)

6. Reporting:

- obtain **written recommendations** from the penetration testing company and have an opportunity **to review the findings** from the report with the ethical hacker(s).
- The findings and detailed explanations from the report will offer you **insights and opportunities** to improve your security posture.
- The report should show you exactly **how entry points** were **discovered** from the OSINT and Threat Modeling phase as well as **how you can remediate the security issues** found during the Exploitation phase.
- include a helpful **overall security risk score**.
- quality penetration testing report will also provide you with a **roadmap of recommendations, mapping the major vulnerabilities** to a defined timeline.

Phases of Penetration Testing(6)

6. Reporting:

One (1) to Three (3) Months	
Tasks	
Create Remediation Strategy	
• Leverage results found within the Penetration Test to create a full remediation strategy • This assessment report will provide the basis for this action. It must now be formalized and approved by the CLIENT Security Team.	
Create Information Security Council/Task Force	
• To gain better traction in the remediation and security onboarding process, CLIENT should create a specific ISEC council to aid in remediation and adequately involve each individual team. • The council should consist of Management of each individual business unit •	
Begin Security Project planning	
• Assign Executive owners of security for CLIENT • ...	
Prioritize Remediation Events	
• Leverage results found within Penetration Test to gain understanding of the tasks needed to be performed in order to resolve the risks identified. • Assign priority listing to remediation tasks that will provide the highest level of impact and largest reduction of identified risk. • Start process with server patching to gain quick increases in environment security.	
Patch Services	
• Specific things to be fixed/how... • ...	
Harden Servers	

Types of Penetration Testing

1. Internal and External Network Penetration Testing
2. Web Application Penetration Testing
3. Mobile Application (iOS or Android) Penetration Testing
4. Wireless Penetration Testing
5. API (REST or SOAP) Penetration Testing
6. Continuous Penetration Testing

Types of Penetration Testing(1)

Network Penetration Testing:

External threats to your network may seem more obvious than internal threats.

If an external host is compromised, it can lead to an attacker digging deeper into your internal environment.

- Port scans and other network service interaction and queries
- Network sniffing, traffic monitoring, traffic analysis, and host discovery
- Password cracking via capture and scanning of authentication databases
- Buffer overruns
- Spoofing or deceiving servers regarding network traffic

Types of Penetration Testing(2)

Web Application Penetration Testing:

- Application Logic Flaw
- Session Management
- Cookie Manipulation
- Brute-Force Attacks
- Poor Server Configuration
- File Upload/Download attack
- Manipulation Injection Attacks for HTML,SQL
- Manual Testing

Types of Penetration Testing(3)

Mobile Application (iOS or Android) Penetration Testing:

- Identify and Protect Sensitive Data on Mobile Devices
- Handle Password Credentials Securely on Mobile Devices
- Ensure Sensitive Data is Protected in Transit
- Implement User Authentication, Authorization, and Session Management
- Correctly Keep the Backend APIs (Services) and the Platform (Server) Secure
- Secure Data Integration with Third-Party Services and Applications
- Pay Specific Attention to the Collection and Storage of Consent for the Collection and Use of the User's Data
- Implement Controls to Prevent Unauthorized Access to Paid-For Resources
- Ensure Secure Distribution/Provisioning of Mobile Applications

Types of Penetration Testing(4)

Wireless Penetration Testing:

- Rogue or Easily Accessible Access
- Vendor-Supplied Defaults
- Easy to Eavesdrop and/or Sniff
- No Wireless Network Monitoring
- Unauthorized, Slow Data Rates
- Misconfigured Firewalls
- WEP Weakness
- Man-in-the-Middle Attacks
- DoS Attacks

Types of Penetration Testing(5)

API (REST or SOAP) Penetration Testing:

APIs are the connective tissue responsible for transferring information between systems, both internally and externally.

- Excessive Data Exposure
- Lack of Resources and Rate Limiting
- Security Misconfiguration Injection
- Improper Assets Management
- Insufficient Logging and Monitoring

Types of Penetration Testing(6)

Continuous Penetration Testing:

- Applications change. Systems change. Networks change. Employees change. Hackers change.
- What happens when you connect a new API, add in a new server, or alter your environment in any way?
 - A web application that was stable yesterday may not be with the next update.
- So, why wouldn't you engage in continuous penetration testing?
 - A **standard penetration test** is a **snapshot of your security posture** at the specific time of testing,
 - whereas **continuous penetration testing** seeks to **fill in the gaps** between point-in-time penetration testing.
- Hacking attempts happen all the time, and so should penetration testing.

Action steps you should take when selecting a penetration testing vendor(1).

- ✓ **Determine Project Scope:** to determine a framework for the work to be done.
- ✓ **Determine Specializations Needed:** Every business and every industry is **unique**. Even **within industries**, businesses have **different configurations**. Multiple locations, open and closed systems, as well as customer, public-facing, and cloud-based applications can all play a role.
- ✓ **Perform Skills Evaluation:** make sure that your prospective vendor has the skills you need to assess your specific systems.
- ✓ **Check Credentials And Certifications:** Make sure that any company you are considering subscribes to the industry standard PTES (Penetration Testing Execution Standards).
 - You want a team of experienced professionals who hold one or more professional certifications considered industry standard,
 - as well as testing based on best practices, including OSSTM (Open Source Security Testing Methodology) and OWASP (Open Web Application Security Project).
 - you should also ask whether the vendor is certified or experienced with your specific situation.

Action steps you should take when selecting a penetration testing vendor(2).

- ✓ **Reputation And References:** You want [senior-level](#) assessments from a highly [professional company](#) that has done business with others in your industry.
 - It's important to check reputation and references.
 - Many companies will provide you a standard reference list, but make sure they can produce a list of actual clients.
- ✓ **Obtain Sample Reports:** Ask to see sample reports to assess what type of information is delivered.
 - ✓ Make sure it's not just full of industry jargon but provides easy-to-understand wording.
 - ✓ real value is [in the evaluation of the results](#) and the [action plan developed](#) to address problems.
- ✓ **Determine Data Security:** you will be opening up your systems to outsiders. you need to have a clear understanding of how data will be handled.
 - ✓ This should include how data is accessed, transmitted, stored, and disposed of when the job is finished.
 - ✓ During the penetration testing, you should know [who has access](#) to the data and [what records will be maintained](#).

Action steps you should take when selecting a penetration testing vendor(3).

- ✓ **Check For Liability Insurance:** If a problem does occur, you want a vendor that has liability insurance to remedy the situation and mitigate any losses that result from their testing.
 - ✓ The vendor you choose needs to be able to provide you with **proof of insurance** sufficient to cover potential losses that might occur if your **data or environment** is **compromised** as a result of the pen test.
- ✓ **Define The Rules Of Engagement:** clearly define the rules of engagement. A contract should detail the exact scope of the work and any limitations.
 - **Ex:** there may be times where certain systems will be unavailable for testing due to business concerns and production schedules. These rules should be spelled out in advance to avoid delays and misunderstandings.
- ✓ **Define Clear Expectations:** Both parties need to be clear about what deliverables are expected. There are options to determine the level and frequency of services provided, including one-time testing, follow-ups, ongoing testing, and on-demand services. Each option will deliver different solutions.
 - Be clear up front to avoid frustrations and misunderstandings later.