Penetration testing Plan for “Spice” an E-commerce Startup for selling spices

What Is Penetration Testing?

We can figure out the vulnerabilities of a computer system, a web application or a network through penetration testing.

A penetration test tells whether the existing defensive measures employed on the system are strong enough to prevent any security breaches. Penetration test reports also suggest the countermeasures that can be taken to reduce the risk of the system being hacked.

➢ Phases of Penetration Testing

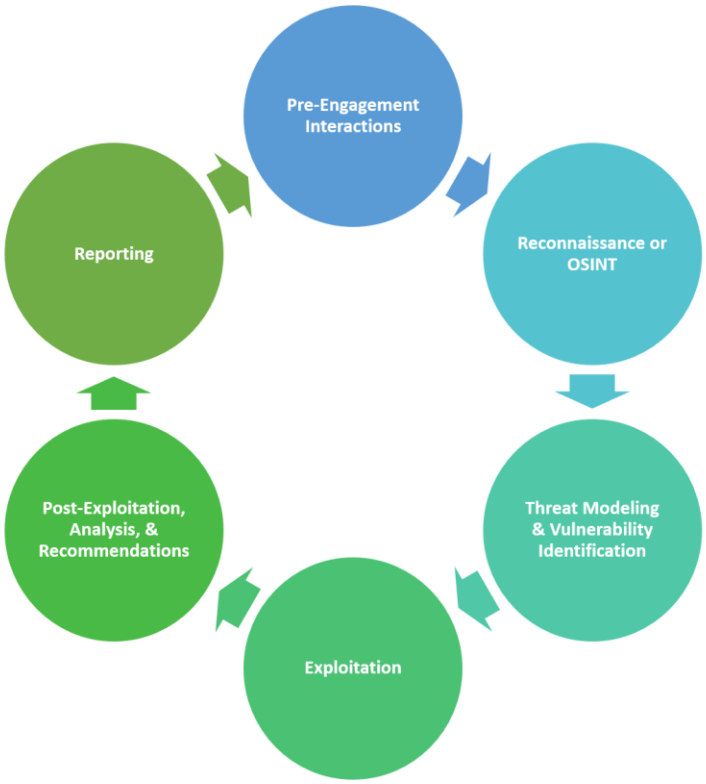


Fig-1: Phases of penetration testing

1. Pre-Engagement Interactions

One over-looked step to penetration testing is pre-engagement interactions or scoping. 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.

During the Pre-Engagement phase, the penetration testers should work with your company to fully understand any risks, your organizational culture, and the best pentesting strategy for your organization. You may want to perform a white box, black box, or gray box penetration test. It's at this stage when the planning occurs along with aligning your goals to specific pentesting outcomes.

2. Reconnaissance or Open Source Intelligence (OSINT) Gathering

Reconnaissance or Open Source Intelligence (OSINT) gathering is an important first step in penetration testing. A pentester works on gathering as much intelligence on your organization and the potential targets for exploit.

Depending on which type of pentest you agree upon, your penetration tester may have varying degrees of information about your organization or may need to identify critical information on their own to uncover vulnerabilities and entry points in your environment.

3. Threat Modeling & Vulnerability Identification

During the threat modeling and vulnerability identification phase, 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 will often use a vulnerability scanner to complete a discovery and inventory on the security risks posed by identified vulnerabilities. Then the pentester will validate if the vulnerability is exploitable. The list of vulnerabilities is shared at the end of the pentest exercise during the reporting phase.

4. Exploitation

With a map of all possible vulnerabilities and entry points, 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.

If you established a scope initially, then the pentester will only go as far as determined by the guidelines you agreed upon during the initial scoping. For example, you may define in your scope to not pentest cloud services or avoid a zero-day attack simulation.

Some of the standard exploit tactics include:

- Web Application Attacks
- Network Attacks
- Memory-based attacks
- Wi-Fi attacks
- Zero-Day Angle
- Physical Attacks
- Social engineering

The ethical hacker will also review and document how vulnerabilities are exploited as well as explain the techniques and tactics used to obtain access to high-value targets. Lastly, during the exploitation phase, the ethical hacker should explain with clarity what the results were from the exploit on high-value targets.

5. Post-Exploitation, Risk Analysis & Recommendations

After the exploitation phase is complete, 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 are unable to provide recommendations on how to remediate the vulnerabilities within the environment. Make sure you ask to see 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, and prevent future unauthorized access into the system through whatever means necessary.

Typical cleanup activities include:

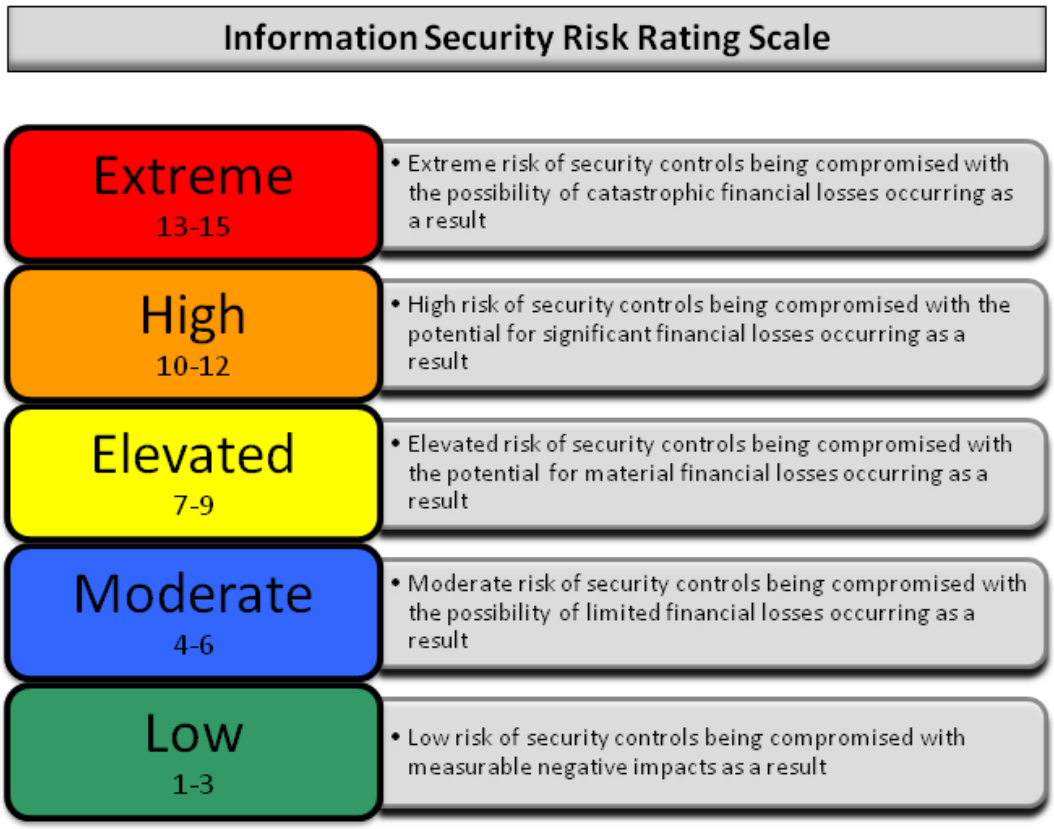
- Removing any executables, scripts, and temporary files from compromised systems
- Reconfiguring settings back to the original parameters prior to the pentest
- Eliminating any rootkits installed in the environment
- Removing any user accounts created to connect to the compromised system

6. Reporting

Reporting is often regarded as the most critical aspect of a pentest. It's where you will 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 significantly 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.

Your penetration report will also include a helpful overall security risk score. It may be inspired by ITIL, FAIR, or DREAD methods and look something like this:



Following is the typical content of a penetration testing report –

- Executive Summary
- Scope of work

- Project objectives
- Assumption
- Timeline
- Summary of findings
- Summary of recommendation Methodology
- Planning
- Exploitation
- Reporting Detail Findings
- Detailed systems information
- Windows server information