SHELT
YOUR CYBERSECURITY AS-A-SERVICE PARTNER

PENTEST METHODOLOGY

SHELT is committed to helping you strengthen your cybersecurity defenses.
Our comprehensive VAPT (Vulnerability Assessment and Penetration Testing) services are designed to uncover potential weaknesses and provide actionable insights to enhance your security posture.

We follow best practices and standards such as:

- MITRE ATT&CK Framework: PRE-ATT&CK, ATT&CK for Enterprise
- OWASP testing framework
- PCI DSS – Penetration Testing Guidance
- NIST 800-115 - Technical Guide to Information Security Testing

OUR VAPT & ISS SERVICES INCLUDE:

1 - Red Team Exercises
2 - Internal Penetration Testing
3 - Social Engineering Testing
4 - Black Box or Grey Box Web Application Penetration Testing
5 - Grey Box Mobile Application Penetration Testing
6 - Cybersecurity Maturity Assessment
7 - Infrastructure Security Assessment and Architecture
8 - Source code review

METHODOLOGY FOR PENTESTING

MITRE

The **MITRE** ATT&CK framework has become the industry standard for analyzing adversarial tactics and techniques. Organizations can improve their security posture by aligning penetration testing methodology with MITRE ATT&CK, which simulates real-world attacks and improves defensive capabilities.

MITRE ATT&CK in Penetration Testing

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a structured matrix that classifies attacker activities at different stages of the cyber kill chain. Using ATT&CK, penetration testers can:

- Identify real-world attack strategies and simulate adversary behavior to evaluate an organization's resistance.
- Enhance detection and response capabilities by integrating security controls with established methods.

Phases of MITRE-Aligned Penetration Testing

1. Reconnaissance & Initial Access: Use MITRE techniques to gather intelligence and exploit initial access points.
2. Execution & Persistence - Test malware execution, persistence mechanisms, and privilege escalation techniques.
3. Defense Evasion & Credential Access - Evaluate the effectiveness of security measures in preventing evasion methods and credential theft.
4. Lateral Movement & Impact - Assess the ability to detect adversary movement within the network and possible targets.

Benefits of MITRE-Based Penetration Testing

- Threat-Informed Testing
- Ensures simulations are consistent with real-world attack scenarios.
- Actionable Insights
- Offers a structured assessment for improving security controls and incident response.

OWASP

The **OWASP** (Open Web Application Security Project) methodology is commonly used to identify and mitigate web application security risks. Organizations can improve their security posture by aligning penetration testing procedures with OWASP, which addresses vulnerabilities that attackers typically exploit.

OWASP in Penetration Testing

OWASP offers a methodical approach to web application security, including the OWASP Top 10, which emphasizes the most serious security risks. OWASP helps penetration testers:

- Identify vulnerabilities that pose the most risk to web applications.

METHODOLOGY FOR PENTESTING

OWASP

- Use real-world attack scenarios to assess security measures.
- Enhance application security by using the best practice and mitigation measures.

Phases of OWASP-Aligned Penetration Testing

1. Information Gathering & Threat Modeling - Determine probable attack routes and understand the application's architecture.
2. Authentication and Session Management Testing: Assess the security of login procedures and session restrictions.
3. Input Validation & Injection Testing - Evaluate potential vulnerabilities such as SQL injection, XSS, and other input-based attacks.
4. Access Control & Business Logic Testing - Check for poor access controls and logical flaws that could be exploited.

Benefits of OWASP-Based Penetration Testing

- Risk-Based Prioritization
- Identifies the most common and significant security risks.
- Enhanced Application Security
- Increases protection against web-based attacks.
- Comprehensive Security Assessment
- Delivers practical information to improve security posture.

NIST

The **NIST** (National Institute of Standards and Technology) cybersecurity framework is well-known for developing guidelines to improve security and risk management. Organizations can improve their security posture by using NIST-compliant penetration testing procedures to systematically identify, protect, detect, respond to, and recover from cyber threats.

NIST in Penetration Testing

NIST delivers a structured approach to cybersecurity, including the NIST Cybersecurity Framework (CSF) and NIST Special Publication 800-115, which describes technical criteria for security testing.

Using NIST, penetration testers can identify vulnerabilities and assess security gaps according to industry standards:

- Use real-world attack scenarios to assess security measures.
- Strengthen cybersecurity resilience with best practices and mitigation methods.

Phases of NIST-Aligned Penetration Testing

1. Planning & Scoping - Using NIST standards, define the objectives, scope, and rules of engagement.

METHODOLOGY FOR PENTESTING

NIST

2. Information Gathering and Vulnerability Analysis: Identify assets, assess threats, and detect vulnerabilities.
3. Exploitation & Attack Simulation - Carry out controlled exploits to determine the impact of vulnerabilities.
4. Post-Exploitation and Reporting - Document discoveries, recommend mitigations, and enhance security procedures.

Benefits of NIST-Based Penetration Testing

- Standards-Based Security Assessment
- Aligns testing with commonly used cybersecurity frameworks.
- Enhanced Security Posture
- Offers structured information to help improve defenses and response plans.

PTES

The **PTES** (Penetration Testing Execution Standard) defines an organized approach to penetration testing that ensures thorough and systematic security assessments. Organizations can improve their security posture by aligning penetration testing procedures with PTES. This allows them to effectively detect, exploit, and mitigate vulnerabilities.

PTES in Penetration Testing

PTES provides a comprehensive framework that addresses both technical and procedural aspects of penetration testing. Using PTES allows penetration testers to:

- Ensure a consistent and comprehensive testing approach.
- Use real-world attack scenarios to evaluate security defenses.
- Provide explicit guidelines for risk assessment and mitigation measures.

Phases of PTES-Aligned Penetration Testing

1. Pre-Engagement Interactions - Establish the objectives, scope, and rules of engagement.
2. Intelligence Gathering - Gather information about targets through open-source and technical reconnaissance approaches.
3. Threat Modeling - Using obtained intelligence, identify probable attack routes.
4. Exploitation - Simulate real-world attacks to evaluate system vulnerabilities.
5. Post-Exploitation: Assess the impact of an attack and its persistence mechanisms.
6. Reporting: Document findings, risk levels, and remediation recommendations.

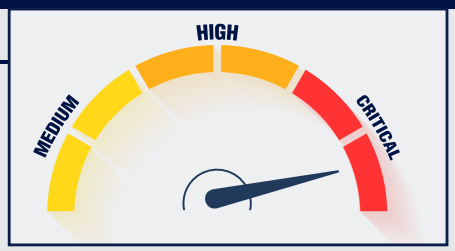
Benefits of PTES-Based Penetration Testing

- Comprehensive Security Assessment: Ensures that all essential security aspects are addressed.
- Standardized Testing Approach
- Follows best practices in penetration testing.
- Actionable Risk Insights
- Assists enterprises in prioritizing and addressing vulnerabilities efficiently.

CASE STUDY 1

PUBLICLY ACCESSIBLE .ENV FILE CONTAINING SENSITIVE INFORMATION

CRITICALITY



During a penetration test for our client, our team discovered that the .env directory of the web application is publicly accessible.

The .env file typically contains sensitive information such as database credentials, API keys, and configuration settings.

IMPACT
Unauthorized access to this file could lead to severe security risks, including unauthorized access to the database and other critical systems.

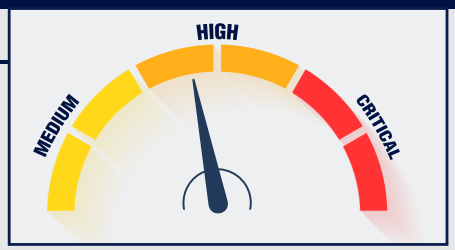
We recommended the following:

1. Configure the web server to deny access to the .env directory and ensure it is not publicly accessible.
2. Review the contents of the .env file and remove any sensitive information that should not be exposed.

CASE STUDY 2

UNAUTHORIZED ACCESS TO SWAGGER API DOCUMENTATION

CRITICALITY



During the penetration test, we discovered that the swagger.json documentation of the affected asset was publicly accessible.

This file could serve as a blueprint for the API, layering out critical details such as endpoints, request methods, parameters, response formats, and authentication methods.

IMPACT
An attacker could gain comprehensive knowledge of the API's structure, endpoints, methods, parameters, and response formats, which can aid them in crafting targeted attacks.

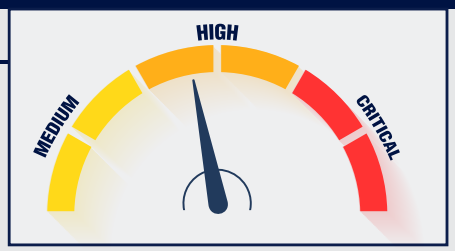
We recommended the following:

1. Ensure that the swagger.json file is not publicly accessible.
2. Implement proper access controls to restrict access to authenticated users only.

CASE STUDY 3

USE OF DEFAULT CREDENTIALS

CRITICALITY



During a penetration test, we discovered an application of which the default credentials had not been changed.

We were able to login and view the configuration settings and other information available on the affected asset.

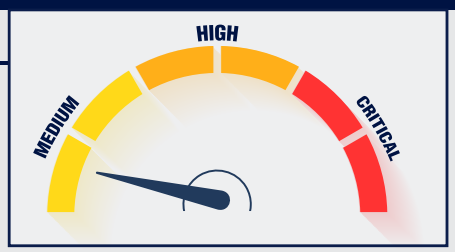
IMPACT
Unauthorized access could lead to data breaches and interception of communication.

We recommended that the default credentials be changed to a strong password which complies to the strong password policy.

CASE STUDY 4

CVE:CVE-2007-6750

CRITICALITY



This vulnerability in Microsoft Windows could allow remote code execution if a user is logged on and opens a specially crafted file.

The vulnerability is caused by the way that the Windows kernel handles objects in memory.

IMPACT
Successful exploitation could allow an attacker to take complete control of the affected system and utilize them for further attacks.

We recommended applying the security update provided by Microsoft to address the vulnerability.