***CFSS INTERNSHIP***

1. **What is the difference between White-Box, Black-Box and Gray-Box Penetration Testing?**

* Explanation: Describe the key differences in the level of access and knowledge provided to the penetration tester in each approach, and explain when each is used in real-world scenarios.

**Ans:** White-Box,Black-Box and Grey-Box penetration testing are different approaches to assessing the security of a system, primarily based on the level of information the tester has about the target system.

Here’s how they differ:-

**White-Box Penetration Testing**

* **Description:** The tester has full knowledge of the target system, including access to source code, architecture diagrams, credentials, and configuration details.
* **Purpose:** It is designed to simulate an insider threat or well-informed attacker.
* **Advantages:**

1. Comprehensive and in-depth analysis.
2. Faster identification of vulnerabilities since testers know where to focus.
3. Allows for through code-level security assessments.

* **Disadvantages:**

1. Unrealistic in terms of simulating external attacks.
2. Requires more resources and expertise to analyze the system fully.

* **Access and Knowledge:** The tester is given full access to the system, including source code, network architecture, configurations, and credentials.
* **When Used:**

1. To conduct a thorough and detailed security assessment.
2. To simulate an insider threat or a highly knowledgeable attacker.
3. During software development to identify vulnerabilities in the code and design.

* **Example Scenario:** A company wants to ensure that their application is secure before release by examining the source code and infrastructure.

*Used during software development to identify deep vulnerabilities.*

**Black-Box Penetration Testing**

* **Description:** The tester has no prior knowledge of the system. They approach it like an external attacker with no insider information.
* **Purpose:** It simulates a real-world external attack scenario.
* **Advantages:**

1. Provides insight into vulnerabilities visible to external attackers.
2. Can uncover isssues related to poorly protected public-facing systems.

* **Disadvantages:**

1. Time-consuming due to lack of prior knowledge.
2. May miss vulnerabilities that an insider might exploit.
3. Limited depth compared to white-box testing.

* **Access and Knowledge:** The tester has no prior knowledge of the system They approach it as an external attacker with no insider information.
* **When Used:**

1. To simulate a real-world external attack scenario.
2. To test the security of public-facing systems(websites, APIs).
3. For compliance with security regulations requiring external attack simulation.

* **Example Scenario:** An organization wants to evaluate how exposed their web application is to an attacker who has no internal access.

*Testing the security of public-facing systems like websites or APIs*

**Grey-Box Penetration Testing**

* **Description:** The tester has partial knowledge of the system, such as user-level access, network diagrams, or limited system details.
* **Purpose:** It strikes a balance between white-box and black-box testing, simulating an attacker who has some insider knowledge to access.
* **Advantages:**

1. More realistic scenario for organizations(simulating a disgruntled employee or a partially successful attacker)
2. Balances efficiency and comprehensiveness.
3. Faster than black-box testing and more focused than white-box testing.

* **Disadvantages:**

1. May still miss some vulnerabilities due to limited knowledge.
2. Depends heavily on the accuracy and relevance of the information provided.

* **Access and Knowledge:** The tester has partial knowledge of the system, such as user-level access, network diagrams, or limited system details.
* **When Used:**

1. To simulate an attacker with limited insider access, such as a disgruntled employee or a hacker who has breached low-level defenses.
2. To balance throughness with time and cost efficiency.
3. In hybrid environments where both external and internal risks are considered.

* **Example Scenario:** A company wants to test the impact of a compromised employee account or partially leaked internal information.

*Evaluating risks from compromise employee accounts.*

**Here is the summarization of the above:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Aspect** | **White-Box Testing** | **Black-Box Testing** | **Grey-Box Testing** |
| **Knowledge Level** | Full Knowledge(source code, network, architecture) | No Prior Knowledge of the system | Partial Knowledge(user credentials, network diagrams) |
| **Access Provided** | Complete Access to Internal Systems. | No Access, simulates an outsider. | Limited Access, such as User-level access. |
| **Purpose** | Simulates an insider or well-informed attacker. | Simulates a real-world external attack. | Simulates a partially informed attacker. |
| **Depth of Testing** | Highly comprehensive and detailed. | Limited to what is externally visible. | Balanced between depth and realism. |
| **Example Scenario** | Code review during Software Development. | Testing public-facing systems like websites or APIs. | Evaluating risks from compromised user accounts. |

1. **What are the main phases of a Penetration Test, and what activities are performed in each phase?**

* Explanation: List and explain the key phases of a penetration test, including planning, reconnaissance, vulnerability assessment, exploitation, post exploitation, and reporting.

**Ans:** A Penetration Test (PenTest) is typically conducted in several phases to identify and exploit vulnerabilities systematically. Below are the key phases and the activities performed in each:

1. **Planning**

*Purpose:* Define the scope, objectives, and rules of engagement.

*Activities:* We have to perform the below mentioned activities-

1. Identify the target systems, testing methods, and timeline.
2. Obtain authorization to perform the test.
3. Define success criteria(specific vulnerabilities to uncover).
4. Agree on legal and ethical considerations with stakeholders.
5. **Reconnaissance**

*Purpose:* Gather information about the target to identify potential entry points.

*Activities:* We have to perform the below mentioned activities-

1. Perform passive reconnaissance (searching publicly available data, WHOIS, DNS records).
2. Conduct active reconnaissance (port scanning, ping sweeps).
3. Identify target assets, technologis, IP ranges, and domains.
4. **Vulnerability Assessment**

*Purpose: Identify security weaknesses in the target systems.*

*Activities:* We have to perform the below mentioned activities-

1. Use automated tools (Nessus, OpenVAS) to scan for known vulnerabilities.
2. Analyze misconfigurations, outdated software, and weak passwords.
3. Map vulnerabilities to potential exploits.
4. **Exploitation**

*Purpose: Test the identified vulnerabilities by attempting to exploit them.*

*Activities:* We have to perform the below mentioned activities-

1. Exploit vulnerabilities to gain unauthorized access, escalate privileges, or extract data.
2. Use tools like Metasploit, SQLMap, or custom scripts
3. Simulate real-world attack scenario while minimizing impact.
4. **Post-Exploitation**

*Purpose: assess the impact of the exploitation and gather additional information.*

*Activities:* We have to perform the below mentioned activities-

1. Analyze compromised systems to understand the potential for lateral movement.
2. Extract sensitive data (credentials, confidentisl files) for demonstration purposes.
3. Ensure no harmful changes or backdoors are left behind.
4. Evaluate the extent of system control and data exfiltration.
5. **Reporting**

*Purpose: Communicate findings, impact, and recommendations to stakeholders.*

*Activities:* We have to perform the below mentioned activities-

1. *Document vulnerabilities, exploited systems, and attack paths.*
2. *Provide risk ratings (critical, high, medium, low).*
3. *Offer remediation guidance and preventive measures.*
4. *Deliver a final report and decrief to stakeholders.*
5. **Explain the concept of “pivoting” in Penetration Testing. How is it used to move within a compromised network?**

* Explanation: Design pivoting, describe how it is performed in a penetration testing scenario, and explain how a tester can use it to escalate access within a network after compromising a single system.

**Ans: Pivoting-** Pivoting refers to a technique used in penetration testing where an attacker, after compromising one system in a network, uses that system as a foothold to access other systems or parts of the network that were otherwise inaccessible. Pivoting allows attackers to escalate access and move laterally within the network.

Pivoting is a critical step in penetration testing that demonstrates the potential consequences of an attacker gaining even limited access. By using pivoting, testers simulate real-world scenarios of lateral movement, privilege escalation, and internal exploitation to evaluate and improve network security.

**How Pivoting is Performed:**

1. **Initial Compromise:**

* The tester gains access to a single machine(through exploiting vulnerabilities, phishing, or brute force).
* This machine becomes the “pivot point” or staging area for further attacks.

1. **Discovery from the Compromised System:**

* The tester gathers information about the network’s internal structure, including-

1. Subnets
2. Internal IP address
3. Connected devices and services

* Tools like NMap, Netstat, or internal scripts are used for reconnaissance.

1. **Tunneling Traffic:**

* The tester sets up pivoting tunnels to reroute traffic through the compromised system.
* This can bypass network segmentation or firewalls that limit direct access to internal systems.
* Technical include-

1. SSH Tunneling: Forwarding traffic via SSH from the pivot point.
2. Proxy Chains: Rerouting traffic through proxies established on the compromised system.
3. SOCKS Proxies: Setting up a proxy on the pivot system to access internal resources.
4. **Lateral Movement:**

* The tester uses the pivot point to explore and attack other systems within the internal network.
* This involves-

1. Exploiting additional vulnerabilities on neighboring machines.
2. Credential harvesting and reusing for privileged access.
3. Escalating privileges on secondary targets.

**How Pivoting is Used:**

1. **Access Internal Resources:**

* Internal networks often have sensitive resources not exposed to the internet, such as databases, file shares, or management systems.
* Pivoting allows testers to probe and exploit these internal resources.

1. **Move Laterally:**

* Once inside, the tester uses the pivot point to jump from one machine to another, exploiting trust relationships and shared credentials.

1. **Privilege Escalation:**

* By accessing more critical systems(domain controllers, admin servers), the tester can escalate privileges and gain control over the entire network.

1. **Data Exfiltration and Demonstration:**

* With access to multiple systems, the tester can demonstrate the impact of a breach by extracting sensitive data or simulating real-world attacks.

**Example Scenario:**

1. A tester compromises a user workstation in an nterprise network through phishing.
2. They discover the workstation is part of an internal subnet that includes a database server.
3. The tester sets up an SSH tunnel from their machine through the compromised workstation to the internal database server.
4. Using the tunnel, they exploit a SQL vulnerability on the database server to extract sensitive data.
5. They escalate access by finding admin credentials on the database server to attack a domain controller.

**Key Tools for Pivoting:**

* **Metasploit Framework** – includes tools for pivoting and lateral movement.
* **SSH (Secure Shell) –** used for creating tunnels and forwarding traffic**.**
* **Proxy Chains –** reroutes connections through the compromised host.
* **Power Shell –** allows command execution and reconnaissance on Windows systems.