



#### What Are the Penetration Testing Steps?

1. Information Gathering (Reconnaissance)
2. Discovery and Scanning
3. Vulnerability Assessment
4. Exploitation
5. Final Analysis and Review
6. Utilize The testing Results

Ananlysis

Step:-1

## 1. Information Gathering (Reconnaissance)

In this step, the organization being tested provides the pentester with basic details about the systems or assets within the test's scope. Additionally, the pentester uses open-source intelligence (OSINT) to gather more information from publicly available sources about the target environment.

इस चरण में, परीक्षण किया जा रहा संगठन, परीक्षण के दायरे में आने वाले सिस्टम या परिसंपत्तियों के बारे में बुनियादी विवरण पेन्टेस्टर को प्रदान करता है। इसके अतिरिक्त, पेन्टेस्टर लक्ष्य वातावरण के बारे में सार्वजनिक रूप से उपलब्ध स्रोतों से अधिक जानकारी एकत्र करने के लिए ओपन-सोर्स इंटेलिजेंस (OSINT) का उपयोग करता है।

Reconnaissance is a critical step in security testing, as it allows pentesters to uncover additional details that may have been overlooked, unknown, or not shared by the organization. This step is especially valuable in internal or external network penetration testing. However, it is less common to perform extensive reconnaissance during web application, mobile application, or API penetration testing.

सुरक्षा परीक्षण में Reconnaissance एक महत्वपूर्ण कदम है, क्योंकि यह Pentesters को अतिरिक्त विवरण उजागर करने की अनुमति देता है जिन्हें अनदेखा किया जा सकता है, अज्ञात हो सकता है, या संगठन द्वारा साझा नहीं किया जा सकता है। यह कदम विशेष रूप से अंतरिक्ष या बाहरी नेटवर्क पैठ परीक्षण में मूल्यवान है। हालाँकि, वेब एप्लिकेशन, मोबाइल एप्लिकेशन या API पैठ परीक्षण के दौरान व्यापक Reconnaissance करना कम आम है।

👉 There are two methods of Reconnaissance.

1. Passive Reconnaissance
2. Active Reconnaissance

1. **Passive Reconnaissance:** Gathering information from publicly available sources (WHOIS records, social media, public websites)

👉 Passive Reconnaissance: सार्वजनिक रूप से उपलब्ध स्रोतों (WHOIS रिकॉर्ड, सोशल मीडिया, सार्वजनिक वेबसाइट) से जानकारी एकत्र करना।

1. **Active Reconnaissance:** Interacting with the target to gather more detailed information, such as using network tools to identify systems and services.

👉 Active Reconnaissance: अधिक जानकारी एकत्र करने के लिए लक्ष्य के साथ बातचीत करना, जैसे कि प्रणालियों और सेवाओं की पहचान करने के लिए नेटवर्क उपकरणों का उपयोग करना।

## Step:-2

### 2. Discovery and Scanning

Discovery scanning is a method used to identify perimeter vulnerabilities. The data collected during this process helps uncover information such as open ports, available services on targeted hosts, or subdomains for web applications. After gathering this information, the pentesters analyze the scan results and develop a strategy to exploit potential weaknesses.

*Discovery and Scanning* एक ऐसी विधि है जिसका उपयोग परिधि कमज़ोरियों की पहचान करने के लिए किया जाता है। इस प्रक्रिया के दौरान एकत्र किया गया डेटा खुले पोर्ट, लक्षित होस्ट पर उपलब्ध सेवाओं या वेब अनुप्रयोगों के लिए उपडोमेन जैसी जानकारी को उजागर करने में मदद करता है। यह जानकारी एकत्र करने के बाद, *pentester scan* परिणामों का विश्लेषण करते हैं और संभावित कमज़ोरियों का फायदा उठाने के लिए एक रणनीति विकसित करते हैं।

*While some organizations end their penetration tests after obtaining the discovery scan results, relying solely on these scans without manual analysis and exploitation means you won't fully understand the extent of your attack surface. Manual testing is essential to uncover deeper vulnerabilities that automated scans might miss.*

जबकि कुछ संगठन *Discovery Scan* के परिणाम प्राप्त करने के बाद अपने प्रवेश परीक्षण समाप्त कर देते हैं, *Manual analysis and exploitation* के बिना केवल इन स्कैन पर निर्भर रहने का मतलब है कि आप अपने हमले की सतह की सीमा को पूरी तरह से नहीं समझ पाएंगे। मैन्युअल परीक्षण गहरी कमज़ोरियों को उजागर करने के लिए आवश्यक है जो स्वचालित स्कैन से छूट सकती हैं।

#### 👉 There are different methods of Discovery scanning

1. Network Scanning
2. Port scanning
3. Service Enumeration

1. **Network Scanning :** *Mapping the network to discover live hosts and devices.*

👉 *Network Scanning :* लाइव होस्ट और डिवाइस की खोज के लिए नेटवर्क का मानचित्रण करना।

2. **Port Scanning :** *Identifying open ports and services running on them.*

👉 *Port Scanning :* खुले पोर्ट और उन पर चल रही सेवाओं की पहचान करना।

3. **Service Enumeration :** *Gathering information on versions of services, operating systems, etc.*

👉 *Service Enumeration :* सेवाओं के संस्करणों, ऑपरेटिंग सिस्टम आदि के बारे में जानकारी एकत्र करना।

**Required Tools :-** *Nmap (Network Mapper), Nessus, OpenVAS, Nikto, Masscan* and other network scanning tools.

**Step :-3**

#### 3. Vulnerability Assessment

A vulnerability assessment is conducted in order to gain initial knowledge and identify any potential security weaknesses that could allow an outside attacker to gain access to the environment or technology being tested. A vulnerability assessment is never a replacement for a penetration test, though.

*Vulnerability Assessment* प्रारंभिक जानकारी प्राप्त करने और किसी भी संभावित सुरक्षा कमज़ोरी की पहचान करने के लिए किया जाता है जो किसी बाहरी हमलावर को परीक्षण किए जा रहे वातावरण या तकनीक तक पहुँच प्राप्त करने की अनुमति दे सकता है। हालाँकि, भेद्यता मूल्यांकन कभी भी प्रवेश परीक्षण का विकल्प नहीं होता है।

#### 👉 These methods Vulnerability Assessment

- Use automated vulnerability scanning tools to detect known weaknesses.
- 👉 ज्ञात कमज़ोरियों का पता लगाने के लिए स्वचालित vulnerability scanning टूल का उपयोग करें।
- Manual vulnerability analysis by identifying misconfigurations or insecure coding practices.
- 👉 गलत कॉन्फ़िगरेशन या असुरक्षित कोडिंग प्रथाओं की पहचान करके मैन्युअल भेद्यता विश्लेषण।

**Required Tools :-** Burp Suite , Nessus , OpenVAS, etc.

#### Step:-4

#### 4. Exploitation

*This is where the action happens!*

*After interpreting the results from the vulnerability assessment, our expert penetration testers will use manual techniques, human intuition, and their backgrounds to validate, attack, and exploit those vulnerabilities. Automation and machine learning can't do what an expert pen tester can. An expert penetration tester is able to exploit vulnerabilities that automation could easily miss.*

👉 यहाँ से असली कार्यवाई शुरू होती है।

एक बार जब Vulnerability Assessment परिणामों का विश्लेषण किया जाता है, तो हमारे कुशल प्रवेश परीक्षक मैन्युअल तकनीकों, मानवीय अंतर्ज्ञान और अपनी विशेषज्ञता का उपयोग करके उन कमज़ोरियों को सत्यापित करने, उन पर हमला करने और उनका फायदा उठाने के लिए आगे आते हैं। जबकि स्वचालन और मशीन लर्निंग का अपना स्थान है, वे एक पेशेवर पेन परीक्षक की अंतर्दृष्टि और अनुकूलनशीलता की नकल नहीं कर सकते हैं, जो उन कमज़ोरियों को उजागर और उनका फायदा उठा सकते हैं जिन्हें स्वचालित उपकरण आसानी से अनदेखा कर सकते हैं।

#### These methods of Exploitation

- Use exploits to breach system security.
- 👉 सिस्टम सुरक्षा भंग करने के लिए शोषण का उपयोग करें।
- Techniques may include buffer overflows, injection attacks, or credential-based attacks.
- 👉 तकनीकों में बफर ओवरफ्लो, इंजेक्शन हमले या क्रेडेंशियल-आधारित हमले शामिल हो सकते हैं।

**Required Tools :-** Metasploit framework , Burpsuite , Exploit-DB , SQL map and others exploitation tools.

#### Step:-5

#### 5. Final Analysis and Review

*When you work with KirkpatrickPrice on security testing, we deliver our findings in a report format.*

जब आप सुरक्षा परीक्षण पर किर्कप्राइटिकप्राइस के साथ काम करते हैं, तो हम अपने निष्कर्षों को एक रिपोर्ट प्रारूप में प्रस्तुत करते हैं।

*This comprehensive report includes narratives of where we started the testing, how we found vulnerabilities, and how we exploited them. It also includes the scope of the security testing, testing methodologies, findings, and recommendations for corrections.*

इस व्यापक रिपोर्ट में यह वर्णन शामिल है कि हमने परीक्षण कहाँ से शुरू किया, हमें कमज़ोरियाँ कैसे मिलीं और हमने उनका कैसे फ़ायदा उठाया। इसमें सुरक्षा परीक्षण का दायरा, परीक्षण पद्धतियाँ, निष्कर्ष और सुधार के लिए सिफारिशें भी शामिल हैं।

*Where applicable, it will also state the penetration tester's opinion of whether or not your penetration test adheres to applicable framework requirements.*

जहाँ लागू हो, यह पेनेट्रेशन परीक्षक की राय भी बताएगा कि आपका पेनेट्रेशन परीक्षण लागू ढांचे की आवश्यकताओं का पालन करता है या नहीं।

### Tasks

- *Review the findings, document what sensitive data was accessed, and evaluate the extent of access.*
- 👉 निष्कर्षों की समीक्षा करें, यह दस्तावेज करें कि किस संवेदनशील डेटा तक पहुंच बनाई गई, तथा पहुंच की सीमा का मूल्यांकन करें
  - *Determine the success of privilege escalation or lateral movement.*
- 👉 विशेषाधिकार वृद्धि या पार्श्व आंदोलन की सफलता का निर्धारण करें।

### Step:-6

#### 1. Utilize The testing Results

*The final stage of penetration testing is crucial. It involves using test results to prioritize vulnerabilities, assess their impact, develop remediation strategies, and guide future decisions.*

प्रवेश परीक्षण का अंतिम चरण महत्वपूर्ण है। इसमें कमज़ोरियों को प्राथमिकता देने, उनके प्रभाव का आकलन करने, उपचार की रणनीति विकसित करने और भविष्य के निष्यों को निर्देशित करने के लिए परीक्षण परिणामों का उपयोग करना शामिल है।

*Dharmendra kumar approach is unique because it customizes each test based on an organization's specific needs, following PTES guidelines but adapting to different threats. Our seven-stage process ensures thorough vulnerability identification and effective remediation guidance.*

धर्मेंद्र कुमार का दृष्टिकोण अद्वितीय है क्योंकि यह PTES दिशानिर्देशों का पालन करते हुए संगठन की विशिष्ट आवश्यकताओं के आधार पर प्रत्येक परीक्षण को अनुकूलित करता है, लेकिन विभिन्न खतरों के अनुकूल होता है। हमारी सात-चरणीय प्रक्रिया पूरी तरह से भेद्यता की पहचान और प्रभावी उपचार मार्गदर्शन सुनिश्चित करती है।

### Tasks

- *Compile a detailed report of the findings, including vulnerabilities, exploitation steps, and mitigation recommendations.*
- 👉 कमज़ोरियों, शोषण चरणों और शमन सिफारिशों सहित निष्कर्षों की एक विस्तृत रिपोर्ट संकलित करें।
- *Present the findings to the stakeholders for remediation and reinforce system defenses.*
- 👉 सुधार के लिए निष्कर्षों को हितधारकों के समक्ष प्रस्तुत करें तथा प्रणाली सुरक्षा को सुदृढ़ करें।
- *Retest after remediation to ensure vulnerabilities are fixed.*

👉 यह सुनिश्चित करने के लिए कि कमजोरियाँ ठीक हो गई हैं, सुधार के बाद पुनः परीक्षण करें।

### **Start Your Pen Testing Journey Today**

Thankyou for Visiting