**Penetration Testing**

## 

**Penetration Testing** or Pen Testing is a type of Security Testing used to uncover vulnerabilities, threats and risks that an attacker could exploit in software applications, networks or web applications. The purpose of penetration testing is to identify and test all possible security vulnerabilities that are present in the software application. Penetration testing is also called Pen Test.

**Vulnerability** is the risk that an attacker can disrupt or gain authorized access to the system or any data contained within it. Vulnerabilities are usually introduced by accident during the software development and implementation phase. Common vulnerabilities include design errors, configuration errors, improper authentication, business logic errors, web application bugs etc.

**Why Penetration Testing?**

* If a company wants their data to be secured, penetration testing is essential to ensure security.
* In case if the web application or server was already hacked or compromised and the organization wants to determine whether any threats are still present in the system to avoid future hacks.
* Proactive Penetration Testing is the best safeguard against hackers.
* Getting an idea of the total number of threats which may compromise your web application or server in future.

**Types of Penetration Testing:**

The type of penetration test selected usually depends on the scope and whether the organization wants to simulate an attack by an employee, Network Admin (Internal Sources) or by External Sources. There are three types of Penetration testing and they are:

* Black Box Penetration Testing
* White Box Penetration testing
* Grey Box Penetration Testing

**Black Box Penetration Testing:** In this approach, a tester has no knowledge about the systems to be tested. He is responsible to collect information about the target network or system.

**White Box Penetration Testing:** In this approach, the tester is usually provided with complete information about the network or systems to be tested including the IP address schema, source code, OS details, etc. This can be considered as a simulation of an attack by any Internal sources (Employees of an Organization).

**Grey Box Penetration Testing**: in grey box pen test a tester is provided with partial knowledge of the system. It can be considered as an attack by an external hacker who has gained illegitimate access to an organization's network infrastructure documents.

**What types Penetration Testing / Security Services do We provide?**

* **Web Application Penetration Testing:**

Penetration testing aka Pen Test is the most commonly used security testing technique forweb applications. Web Application Penetration Testing is done by simulating unauthorized attacks internally or externally to get access to sensitive data or server by abusing the different functionalities the web application is providing us. OWASP top 10 is our priority in the list provided below.

**Vulnerabilities we check in Web App testing:**

1. Contact Form Testing
2. Proxy Server(s) Testing
3. Spam Email Filter Testing
4. Network Firewall Testing
5. Security Vulnerability Testing
6. Credential Encryption Testing
7. Cookie Testing
8. Testing For Open Ports
9. Application Login Page Testing
10. Error Message Testing
11. HTTP Method(s) Testing
12. Username and Password Testing
13. File Scanning
14. SQL Injection Testing
15. XSS Testing
16. Access Permission Testing
17. User Session Testing
18. Brute Force Attack Testing
19. DoS (Denial of Service) Attack Testing
20. Directory Browsing
21. Improper access control
22. Secrets publically available in javascript chunks
23. Business logic errors
24. Insecure Direct object references (IDOR)
25. Unauthorize access
26. Directory Traversal
27. Directory and file bruteforce
28. Allocation of resources without throttling
29. CRLF injection
30. Command injection
31. Cleartext submission of sensitive information
32. Cross Site Request Forgery
33. HTTP request smuggling
34. Improper access control
35. Input Validation
36. Missing authorization
37. Information Disclosure
38. Open Redirect
39. Path traversal
40. Server side request forgery (SSRF)
41. Unrestricted file upload with dangerous extension
42. ClickJacking
43. XML external entity (XXE)
44. Local file inclusion (LFI)
45. Remote file inclusion (RFI)
46. Insecure storage of sensitive information
47. OS command injection
48. Password or secrets in configuration files
49. Server side template injection (SSTI)
50. Security through obscurity
51. Source Code and company secrets disclosure.
52. Broken Access Control
53. Security misconfigurations
54. Privilege escalation

* **Cloud Security Assessment:**

A cloud security assessment (CSA) can help you identify and mitigate security risks in cloud computing.

In this section we cover misconfigurations of security policies in AWS and Azure including s3 bucket policies and security of the whole admin panel.

**S3:** For testing s3 buckets we just need the names of the buckets.

**Admin level security policies:** For overall assessment you have to give us read access to the panel to determine the total risk and for making your cloud panel more secure.

### **API Pen Testing:**

We also perform penetration testing on API server and its endpoints. And here is the list of things we check on API penetration testing:

1. Missing Object Level Access Control
2. Broken Authentication
3. Excessive Data Exposure
4. Lack of Resources and Rate Limiting
5. Missing Function/Resource Level Access Control
6. Mass Assignment
7. Security Misconfiguration
8. Injection
9. Improper Assets Management

### **Network Pen Testing:**

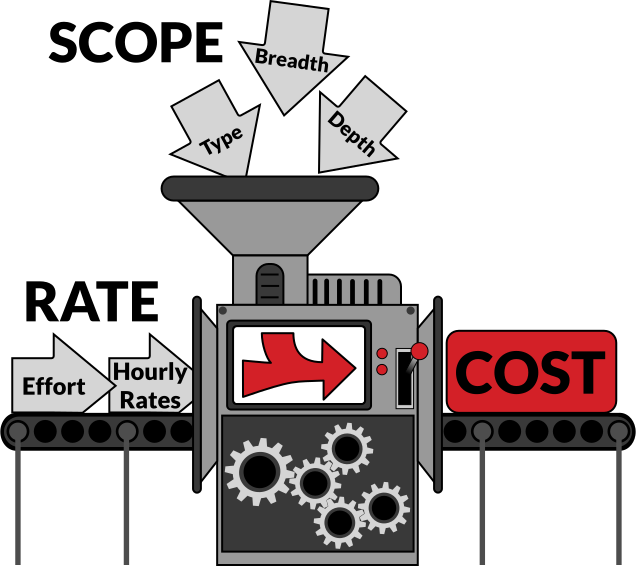
### This is one of the most commonly performed penetration tests where the openings in the network are identified by which entry is being made in the systems on the network to check what kind of vulnerabilities are there.

* **Internal Pen Testing:**

Internal penetration testing continues the assessment by helping to identify how far an attacker can laterally move through a network once an external breach has occurred.

An Internal Pentest could also be performed by giving access to the internal admin panels, CMS, HRMS by deploying it on testing environments just to determine the risk which a company may have from an employee or if an employee account gets compromised or hacked.

### 

**Penetration Testing Costing:**

Penetration testing services are usually quoted as a fixed price for the estimated effort to test the target. Without looking at scope and specifics, the average base cost of a penetration test is between $10,000 and $45,000. It is, of course, possible to receive more substantial or smaller quotes, depending on the details of the test. But most penetration tests fall somewhere in this territory. If you're new to penetration testing, it is unlikely that your first experience with a credible firm will extend too far outside this range.

**Let's take a look at the primary factors that are used to estimate effort, and will ultimately determine this base price: Scope and Rate.**

### **Scope:**

There's a substantial difference between the effort required to test a small web application versus the effort needed to test an extensive internal network. The scope can be expressed in part by the type of penetration test (e.g., a network, a building, an application, an organization, etc…), and then by the breadth and depth which may take on slightly different meanings depending on the type of test.

### **Type:**

Penetration testing is, in essence, an effort to breach the security controls of a system of assets. So what are the assets that need to be tested? For example, a network penetration test is a very common type, which is usually scoped as a test of network security controls plus all the devices connected to the network. A test of just an internal network will often carry a lower base price than a test of both the internal and external (i.e., the part available to the Internet) networks. The base price for testing a single web application is usually a bit less than the base price for testing a network.

Another aspect of type is if the test serves a specific purpose, such as PCI-DSS compliance. In these cases, a scope may be more than that of a non-PCI penetration test because of the additional effort required to meet the specific tasks required by the standard. Internally each penetration testing vendor will establish a base price for each type of test, which is used as a starting point.

### **Breadth:**

This dimension is more widely known as the potential attack surface that is in scope for a test. Its exact meaning depends on the type of penetration test. For example, if it is a network that is being tested, then the breadth is usually expressed as the network ranges and domains of the network that are in scope. For an application, you would express the breadth by defining boundaries such as APIs and microservices that are in or out of scope. For a test of physical locations, the breadth may be specified as a subset of available retail stores.

Some testing companies rely very heavily on automated scoping using statistics like the number of servers and workstations for a network test, or the number of dynamic pages in a web application. While these numbers may be useful in the scoping discussion, most professional firms will expect more context on the functionality and purpose of the system. For example, a chain of small locations with 100 identical sites may have more hosts, but less complexity than a single location site. If a pen testing company depends primarily on statistics for scoping and submits a quote significantly lower than others, it is likely that their testing methodology is based mostly on automated vulnerability scanning. See our article on how pen tests differ from vulnerability scans.

### **Depth:**

The depth of the test is a determination of how far the vendor should exploit vulnerabilities to assess the true risk to the organization. This can be a touchy subject with some penetration testing vendors because there are those in the industry who believe that your security assessment is not a penetration test unless it includes full exploitation of the organization. Unfortunately, the pendulum has also swung in the opposite direction, where some security assessments are dubbed as penetration tests when they are, in fact, just automated vulnerability assessments. No matter your definition of depth, it is vital to work with your vendor to determine it before the test starts. For example, for a web application, if the tester discovers XSS, is it in scope to leverage that flaw to hijack the browser session of your employee? If a command injection flaw is found, should the testers demonstrate the flaw and move on, or attempt to escalate privileges on the host machine and pivot onto other internal systems?

The depth of a penetration test depends on the specific objectives of the test. Though an automated vulnerability assessment is never an acceptable replacement for a penetration test, there are also many cases where granting free reign to exploit and pivot may not be necessary. For example, if your organization has an effective vulnerability remediation process, then a penetration test of an application may only require that vulnerabilities be identified with steps to reproduce. In this situation, spending additional effort to pivot from the application to unrelated systems inside an organization is frivolous and wastes time during the testing window.

### **Rate:**

The estimation process will usually start with an estimate of how much effort will be needed to perform the penetration testing plus some additional effort for generating the deliverables (i.e., the report) and project management. Once this can be expressed in hours, it is a simple exercise of multiplying the effort estimate by an hourly rate. The final number will be the unmodified fixed effort quote.

Hourly rates for security consulting services typically run anywhere from about $200 / hr to $500 / hr. (And to be transparent, Secure Ideas bills at $250 per hour.) Just like any experience-based trade, it may be worth paying a little more for top talent.