What If you are thinking that I am not connected to Internet Is my System Secure ? I am using IDPS and Firewall while connected to Internet.

Then You are Wrong Still amazed How let’s see still Hackers can Hack into Your System/Server/Network Lets Read this Whitepaper to know more about Penetration Testing How You can Secure Your Network/Server/System or How Any Intruder can Hack into your System to steal your confidential or privates files.

**Vulnerability Assessment, Penetration testing or Ethical Hacking?  
- What's the difference?**

In general, the above terms are used interchangeably within the industry, although it is always a good idea to clarify the supplier's perception of the term used to ensure you are comparing like for like offerings. Although they are generally interchangeable, there are semantically some differences between the vulnerability assessment and penetration testing/ethical hacking: Vulnerability assessments tend to be performed using automated scanning tools. These tools when used in isolation however have a number of limitations, not least of which is the inability to exploit the potential vulnerability to confirm its presence and demonstrate the real-world risk associated with its exploitation.

Penetration testing and ethical hacking will normally provide a number of important additions: Firstly, a range of tools and technologies will be used. Secondly, potential vulnerabilities will normally be exploited to confirm their existence, and simulate a real attacker more closely. Not all issues can be exploited (for example, some require very specific scenarios or actions by third parties to be exploitable) but the vulnerabilities existence will be proved/disproved as far as reasonably possible.

**What is Penetration Testing?**

Penetration testing is the process of attempting to gain access to resources without knowledge of user-names,passwords and other normal means of access.

The penetration tester will have permission from the owner of the computing resources that are being tested and will be responsible to provide a report. The goal of a penetration test is to increase the security of the computing resources being tested.

In many cases, a penetration tester will be given user-level access and in those cases, the goal would be to elevate the status of the account or user other means to gain access to additional information that a user of that level should not have access to.

It’s important to understand that it is very unlikely that a pen-tester will find all the security issues. As an example, if a penetration test was done yesterday, the organization may pass the test. However, today is Microsoft’s “patch Tuesday” and now there’s a brand new vulnerability in some Exchange mail servers that were previously considered secure, and next month it will be something else. Even ZERO Day Attacks can create a Headache after completing Penetration Test as You have to Maintaining secure network requires constant vigilance.

**Penetration - Testing vs. Vulnerability Assessment**

The main focus of this paper is penetration testing but there is often some confusion between penetration testing and vulnerability assessment. The two terms are related but penetration testing has more of an emphasis on gaining as much access as possible while vulnerability Assessment places the emphasis on identifying areas that are vulnerable to a computer attack. An automated vulnerability scanner will often identify possible vulnerabilities based on service banners or other network responses that are not in fact what they seem.

A penetration test is like any other test in the sense that it is a sampling of all possible systems and configurations. Unless the contractor is hired to test only a single system, they will be unable to identify and penetrate all possible systems using all possible vulnerabilities. As such, any Penetration Test is a sampling of the environment. Furthermore, most testers will go after the easiest targets first then he can deal with Hard System Configuration for better Conclusion to find vulnerability and penetrate into it deeper.

**How Vulnerabilities Are Identified**

Vulnerabilities need to be identified by both the penetration tester and the vulnerability scanner. The steps are similar for the security tester and an unauthorized attacker. The attacker may choose to proceed more slowly to avoid detection, but some penetration testers will also start slowly so that the target company can learn where their detection threshold is and make improvements.

Once the tester has an idea what software might be running on the target computers, that information needs to be verified. The tester really does not know what is running but he may have a pretty good idea. The information that the tester has can be combined and then compared with known vulnerabilities, and then those vulnerabilities can be tested to see if the results support or contradict the prior information.

In a stealthy penetration test, these first steps may be repeated for some time before the tester decides to launch a specific attack. In the case of a strict vulnerability assessment, the attack may never be launched so the owners of the target computer would never really know if this was an exploitable vulnerability or not.

**Why We need Penetration Testing**

There are a variety of reasons for performing a penetration test. One of the main reasons is to find vulnerabilities and fix them before an attacker does. Sometimes, the IT department is aware of reported vulnerabilities but they need an outside expert to officially report them so that management will approve the resources necessary to fix them. Testing a new system before it goes on-line is also a good idea. Another reason for a penetration test is to give the IT department at the target company a chance to respond to an attack. ISO 27000 , The Payment Card Industry (PCI) Data Security Standard, and other recent security recommendations and regulations, require external security testing.

Over the past few years We have seen Hackers performing Denial of Service attacks on very critical Infrastructures like GOVT Operations, Nuclear Operations, Banks and Corporate. Even Hacking into Different Websites and Server using vulnerabilities in Software and web based application. As some of the Server and Websites stores very Confidential like Passwords, Credit Card/Debit Card Information, Information the following Industries given below should conduct PT on regular basis.

* Banking, Finance, Insurance
* Online retail & Ecommerce
* Manufacturing
* Telecommunications
* Research Development
* Government
* Television Media
* Education Sectors

Most of websites have vulnerabilities that could lead to the theft of sensitive corporate data such as credit card information and customer lists. Hackers are concentrating their efforts on web-based applications - shopping carts, forms, login pages, dynamic content, etc. Accessible 24/7 from anywhere in the world, insecure web applications provide easy access to backend corporate databases. If web applications are not secure, then your entire database of sensitive information is at serious risk.

**Find Holes Now Before Somebody Else Does**

At any given time, attackers are employing any number of automated tools and network attacks looking for ways to penetrate systems. Only a handful of those people will have access to Zero - day exploits, most will be using well known (and hence preventable) attacks and exploits.

In a sense, think of a Penetration Test as an annual medical physical. Even if you believe you are healthy, your physician will run a series of tests (some old and some new) to detect dangers that have not yet developed symptoms.

***Penetration Testing Framework***

This Famework draws your attention to the main phases of the test that should be perfomed while Vulnerability Assessment and Penetration Testing for the beginners, Some security testers believe that a security test is simply a “point in time” view of a defensive posture and present the output from their tests as a “security snapshot”. They call it a snapshot because at that time the known vulnerabilities, the known weaknesses, and the known configurations have not changed.

Many variables affect the outcome of a test, including the personal style and bias of a tester. Precisely because of all these variables, it is important to define the right way to test based on best practices and a worldwide consensus. If you can reduce the amount of bias in testing, you will reduce many false assumptions and you will avoid mediocre results. You’ll have the correct balanced judgment of risk, value, and the business justification of the target being tested. By limiting and guiding our biases, it makes good security testers great and provides novices with the proper methodology to conduct the right tests in the right areas.

Following are the main phases that should be covered:

Vulnerability Assessment and Penetration Testing (VAPT) should be proceed into following stages:

**1.1 )** Acquisition and Information gathering on Network/System along with detailed description of important issues that needs to be clarified in a contract before carrying out VAPT.

**1.2)** Risk analysis for identifying and assessing risks associated with VAPT.

**1.2.3)** Following testing activities need to be completed in VAPT:

1. Information Gathering Scanning:
   1. Intelligence gathering and information assessment are the foundations of a good penetration test.
   2. The more informed the tester is about the environment, the better the results of the test will be.

In this section, a number of items should be written up to show the CLIENT the extent of public and private information available through the execution of the Intelligence gathering phase of PTES. At a minimum, the results identified will be presented in 4 basic categories:

1. **Passive Intelligence:**

Intelligence gathered from indirect analysis such as DNS,Google dorking for IP/infrastructure related information. This section will focus on the techniques used to profile the technology in the CLIENT environment WITHOUT sending any traffic directly to the assets.

1. **Active Intelligence:**

This section will show the methods and results of tasks such as infrastructure mapping, port scanning, and architecture assessment and other foot printing activities. This section will focus on the techniques used to profile the technology in the CLIENT environment by sending traffic DIRECTLY to the assets.

1. **Corporate Intelligence:**

Information about the structure of the organization, business units, market share, vertical, and other corporate functions should be mapped to both business process and the previously identified physical assets being tested.

1. **Personnel Intelligence:**

Any and all information found during the intelligence collection phase which maps users to the CLIENT organization. This section should show the techniques used to harvest intelligence such as public/private employee depots, mail repositories, org charts and other items leading to the connection of employee/company.

* Network Scanning
* Port Scanning
* System Identification and Trusted System Scanning\
* Service Identification Scanning
* Vulnerability Scanning
* Malware Scanning
* Spoofing
* Scenario Analysis

1. Vulnerability Assessment:

Vulnerability assessment is the act of identifying the POTENTIAL vulnerabilities which exist in a TEST and the threat classification of each threat. In this section, a definition of the methods used to identify the vulnerability as well as the evidence/classification of the vulnerability should be present. In addition this section will include:

* 1. Network Architecture Review
  2. Server Assessment (OS, Security Configuration etc.)
  3. Security Devices Assessment (IOS, Security Configuration etc.)
  4. Network Devices Assessment (Security Configuration etc.)
  5. Website Assessment (Security Configuration, Security Certificates, Services etc.)
  6. Vulnerability Research & Verification

1. Penetration Testing:
   1. Application Security Testing and Code Review
   2. OS Fingerprinting
   3. Service Fingerprinting
   4. Access Control Mapping
   5. Denial of Service (DoS)
   6. Distributed DoS
   7. Authorization Testing
   8. Lockout Testing
   9. Password Cracking
   10. Cookie Security
   11. Functionality Testing (Input validation of login fields, Transaction Testing etc.)
   12. Containment Measures Testing
   13. War Dailing
2. Website/Web Application Assessment

Check various web attacks and web applications for web attacks. The various checks/attacks/vulnerabilities should cover the following or any type of attacks, which are vulnerable to the website/web application.

* 1. Vulnerabilities to SQL injections
  2. CRLF injections
  3. Directory Traversal
  4. Authentication hacking/attacks
  5. Password strength on authentication pages
  6. Scan java-script for security vulnerabilities
  7. File inclusion attacks
  8. Exploitable hacking vulnerable
  9. Web server information security
  10. PHP remote scripts vulnerability
  11. HTTP injection
  12. Phishing a website
  13. Buffer overflows, Invalid inputs, Insure storages etc
  14. Any other attacks, which are vulnerability to the website and web applications.

Web assessment should be done by using industry standards and also as per the Open Web Application Security Project (OWASP) methodology to identify the security vulnerabilities including top web application vulnerabilities viz. Cross site scripting (XSS), Injection Flaws, Malicious File Execution, Insecure Direct Object Reference, Cross Site Request Forgery (CSRF), Information Leakage and Improper Error Handling, Broken Authentication and Session Management, Insecure Cryptographic Storage, Insecure Communications, Failure to Restrict URL Access etc. and also to identify remedial solutions and recommendations for making the web application secure.

**1.2.4) Post Testing Actions and Reports:** Summary comparisons of Network Testing Techniques used for VAPT along with Reports and Recommendations along with solution as per the industry standard and best practices.

**1.3) Approach to be followed in Penetration Testing is given here below:**

a) Information base (Grey Box Testing)

b) Aggressiveness (Passive Scanning)

c) Scope (Focused)

d) Approach (Overt)

e) Technique (Network-based)

f) Starting Point (from the outside and the inside)

**1.4) Method of VAPT to be followed:**

The vendor has to undertake the VAPT in a phased manner as described below:

PHASE 1 – Conduct of VAPT as per Scope, Evaluation & Submission of Preliminary Reports of Finding and Discussion on the Findings.

PHASE 2 – Submission of Reports

**1.5) VAPT Core Team**

1.5.1) The Core team assigned for VAPT activity should have minimum 2 professionals in each of the following category with valid certification mentioned thereon.

a) Information Security (CISA/CISM/CISSP)

b) Network (CCNA/CCNP or equivalent)

c) Operating Systems (Certification from Microsoft/Linux/Solaris/AIX)

d) Databases (Oracle/MySQL/MS SQL/Sybase/etc)

e) Ethical Hacking (CEH)

Who have associated/conducted at least one VAPT for Clients IT Infrastructure and should be on permanent roll of the Organization.

**1.6) Completion of VAPT activity**

1.6.1) The Vulnerability Assessment should be carried out at on-site for the devices/servers etc. and Penetration Testing should be carried out from the Our site. The VAPT may also be carried out simultaneously in all the locations after obtaining written permission from the Client.

1.6.2) The Company will complete the VAPT activity and submit the reports within two months from the date of acceptance of Purchase Order.

**1.7) Deliverables**

The deliverables for VAPT activity are as follows:

**1.7.1)** Execution of Vulnerability Assessment and Penetration Testing for the identified network devices, security devices, servers, applications, websites etc. as per the scope mentioned in Approach & analysis of the findings and guidance for resolution of the same. (Type – service & documentation).

**1.7.2)** VAPT Report (Type – Documentation)

The VAPT report should contain the followings:

1. Identification of auditee (Address & Contact information)
2. Dates & Locations of VAPT
3. Terms of reference
4. Standards followed
5. Summary of audit findings including identification tests, tools used and results of test performed (like vulnerability assessment, penetration testing, application security assessment, website assessment,etc.)
6. Tools used and methodology employed
7. Positive security aspects identified
8. List of vulnerabilities identified
9. Description of vulnerabilities
10. Risk rating or severity of vulnerability
11. Category of risk: Very High/High/Medium/Low
12. Test cases used for assessing the vulnerabilities
13. Illustration of test cases
14. Applicable screenshots
15. Analysis of vulnerabilities & issues of concern
16. Recommendations for corrective action
17. Personnel involved in the audit

The Company conducting Test may further provide any other required information as per the approach adopted by them and which they feel is relevant to the audit process. All the gaps, deficiencies, vulnerabilities observed shall be thoroughly discussed with respective Client officials before finalization of the report.

**1.7.3)** The VAPT report should comprise the following sub reports:

a) **VAPT Report – Executive Summary**: The vendor should submit a report to summarize the Scope, Approach, Findings, and recommendations, in a manner suitable for senior management.

b) **VAPT Report – Core Findings along with Risk Analysis**: The vendor should submit a report bringing out the core findings of the VAPT conducted for network devices, security devices, servers and websites.

c) **VAPT Report – Detailed Findings/Checklists**: The detailed findings of the VAPT would be brought out in this report which will cover in detail all aspects viz. Identification of vulnerabilities/ threats in the systems (specific to equipment’s/resources – indicating the name and IP address of the equipment with office and department name), Identification of threat sources, Identification of risk, Identification of inherent weakness, Servers/Resources affected with IP address etc. Report should classify the observations into Critical/Non Critical category and assess the category of Risk Implication as Very High/High/Medium/Low risk based on the impact. The various checklist formats, designed and used for conducting the VAPT activity as per the scope, should also be included in the report separately for servers (different for different OS), Application, Network equipments, Security equipments etc, so that they provide minimum domain wise baseline security standard/practices to achieve a reasonably secure IT environment for technologies deployed by the Client. The reports should be substantiated with the help of snap shots/evidences/documents etc. from where the observations were made.

d) **VAPT Report – In depth analysis of findings/ Corrective Measures & Recommendations along with Risk Analysis**: The findings of the entire VAPT process should be critically analyzed and controls should be suggested as corrective/preventive measures for strengthening/safeguarding the IT assets of the Client against existing and future threats in the short/long term. Report should contain suggestions/recommendations for improvement in the systems wherever required. If recommendations for Risk Mitigation/Removal could not be implemented as suggested, alternative solutions to be provided. Also, if the formal procedures are not in place for any activity, evaluate the process & the associated risks and give recommendations for improvement as per the best practices.

e) **VAPT Report – Suggestion for Industry Best Practices**: The vendor has to provide hardening parameters for OS, websites, web-based applications, databases, servers, network and security devices as per the industry best practices standard.

**1.7.4)** **Documentation Format:**

a) All documents will be handed over in three copies, signed, legible, neatly and robustly bound on A4 size, good quality paper. The place of submission of reports shall be informed to select.

b) Soft copies of all the documents properly encrypted in MS Word/MS Excel/PDF format also to be submitted in CDs/DVDs along with the hard copies.

c) All documents shall be in plain English.