# STRENGTHENING INFOMATION SECURITY WITH VAPT

Sherin S Panikar
Institute of Management and Computer Studies
Thane (West), India.
University of Mumbai

***Abstract—***
***Vulnerability Assessment and Penetration Testing (VAPT) provides enterprises with a more comprehensive application evaluation than any single test alone. Using the Vulnerability Assessment and Penetration Testing (VAPT) approach gives an organization a more detailed view of the threats facing its applications, enabling the business to better protect its systems and data from malicious attacks. Vulnerabilities can be found in Network or Applications from third-party vendors and internally made software, but most of these flaws aren't easily found and fixed. Using VAPT enables to focus on mitigating critical vulnerabilities while the VAPT continues to discover vulnerabilities. VAPT involves compromising the system, and during the process, some of the files may be altered. This process ensures that the system is brought back to the original state, before the testing, by cleaning & restoring the data and files used in the target machines. Certain measures and methods are been suggested in this study to determine and prevent exploitation (Attacks) with Manual Pentesting.***

***Keywords—***
***Information Security, Cyber Security, InfoSec, CyberSec, VAPT, Metasploit Penetration Testing, Vulnerability Assessment, Hacking, Ethical Hacking, Metasploit Framework, Computer Hacking and Forensics.***

## I. INTRODUCTION

IT environment systems such as computers and networks are scanned in order to identify the presence of vulnerabilities associated with them. As per the information provided by the latest survey more than 80% of websites are vulnerable, especially those which are created by using any

engine such as WordPress, BlogSpot etc. leading to the leak of sensitive corporate information and data such as passwords, credit card info etc. Basically, Black hats 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 back-end corporate databases. As per Network based a potential flaws could be determined by an Attacker which may be allowing him to infiltrate in to a particular network and could inject malicious files that can be used to gain access over the system or server. Depending on his intentions an attacker may lead to further procedure of exploitation. Once the network components have been identified, they can be assessed for vulnerabilities.
These vulnerabilities could be Technology weaknesses, Configuration weaknesses, Security policy weaknesses.
Any vulnerability that is discovered will need to be addressed to mitigate any threat that could take advantage of the vulnerability.

## II. AN OVERVIEW OF VA-&-PT

Vulnerability Assessment is the process of systematically scanning an organization's servers, workstations, devices, operating systems, and other application software to detect and identify vulnerabilities. Identified vulnerabilities could include missing patches, gaps or loopholes in system design, misconfigurations etc. Any exposure of these gaps might result in unauthorized



ISSN: 2278 – 1323 

access to confidential data and information and pose a threat to the organization. Vulnerability Assessment utilizes specific tools to identify vulnerabilities and provide remedial measures.

Penetration Testing which is also known as Ethical Hacking, Penetration Testing is the process of launching real world, secure attacks on IT infrastructure and systems to help identify the extent of exposures without causing any harm to existing data and systems. Penetration Testing helps detect possible threats by conducting mock attacks within the enterprise IT framework and helps IT managers identify threats before actual occurrence.

Although used synonymously, there is a subtle difference between Vulnerability Assessment and Penetration Testing. While Vulnerability Assessment helps identify vulnerabilities, Penetration Testing attempts to validate these vulnerabilities by deploying scenarios that mimic possible malicious attacks. Most Vulnerability Assessment tools test for known system vulnerabilities and chances of producing false positives are high in this case. Penetration Testing addresses the issue of false positives by miming typical attack scenarios and studying system response to them. Vulnerability Assessment and Penetration Testing tools when deployed together can substantially eliminate the risk of false positives and provide organization specific actionable events without unnecessarily overloading the organization's human resources.

VAPT is most often overlooked as an integral part of IT security best practices. However, given today's volatile environment of cyber scams and online security threats, it is important for organizations to deploy strong and foolproof VAPT solutions. Enterprise IT needs to be aware of known and unknown vulnerabilities and their impact on IT infrastructure and business processes. VAPT solutions not only detect threats, but also offer dynamic remedial measures to mitigate the risks arising out of these threats.

## III.ROLE & COMPARISION:

### *Penetration Testing & Vulnerability Assessment*

Vulnerability Analysis is the process of identifying vulnerabilities on a network, whereas a Penetration Testing is focused on actually gaining unauthorized access to the tested systems and using that access to the network or data, as directed by the client.

A Vulnerability Analysis provides an overview of the flaws that exist on the system while a Penetration Testing goes on to provide an impact analysis of the flaws identifies the possible impact of the flaw on the underlying network, operating system, database etc.

Vulnerability assessment use scanners to identify vulnerabilities that throws lot of false positives. In Penetration testing as there is human intervention to exploit vulnerabilities false positives does not exist.

Vulnerability Analysis is more of a passive process. In Vulnerability Analysis you use software tools that analyze both network traffic and systems to identify any exposures that increase vulnerability to attacks. Penetration Testing is an active practice wherein ethical hackers are employed to simulate an attack and test the network and systems' resistance.

Vulnerability Analysis deals with potential risks, whereas Penetration Testing is actual proof of concept. Vulnerability Analysis is just a process of identifying and quantifying the security Vulnerabilities in a system. Vulnerability Analysis doesn't provide validation of Security Vulnerabilities. Validation can be only done by Penetration testing.

The scope of a Penetration Testing can vary from a Vulnerability Analysis to fully exploiting the targets to destructive testing. Penetration Testing consists of a Vulnerability Analysis, but it goes one step ahead where in you will be evaluating the



ISSN: 2278 – 1323 

security of the system by simulating an attack usually done by a Malicious Hacker.

For instance a Vulnerability Analysis exercise might identify absence of anti-virus software on the system or open ports as a vulnerability. The Penetration Testing will determine the level to which existing vulnerabilities can be exploited and the damage that can be inflicted due to this.

A Vulnerability Analysis answers the question: "What are the present Vulnerabilities and how do we fix them?" A Penetration Testing simply answers the questions: "Can any External Attacker or Internal Intruder break-in and what can they attain?"

A Vulnerability Analysis works to improve security posture and develop a more mature, integrated security program, where as a Penetration Testing is only a snapshot of your security program's effectiveness.

Commonly Vulnerability Assessment goes through the following phases: Information Gathering, Port Scanning, Enumeration, Threat Profiling & Risk Identification, Network Level Vulnerability Scanning, Application Level Vulnerability Scanning, Mitigation Strategies Creation, Report Generation, and Support. Where as a Penetration Testing Service however have following phases: Information Gathering, Port Scanning, Enumeration, Social Engineering, Threat Profiling & Risk Identification, Network Level Vulnerability Assessment, Application Level Vulnerability Assessment, Exploit Research & Development, Exploitation, Privilege Escalation, Engagement Analysis, Mitigation Strategies, Report Generation, and Support.

## IV. VAPT REQUIREMENTS

Adaptation of Manual Process which needs to be followed accordingly.

### *a) Information Gathering*

Information Gathering is a method of collecting information about the network or the system you are testing. Such as IP address, OS Version etc. Basically this is applicable to all the modes of testing as mentioned above.

### *b) Vulnerability Detection*

In this phenomena many tools such as vulnerability scanners, network scanners etc. are used to find the associated vulnerability in that particular network mode,

### *c) Information Analysis And Penetration Testing*

This process is used to analyze the identified vulnerabilities, associated with the information gathered about the IT environment systems and networks to apply a plan for penetrating into the network and system by the process of Penetration Testing. In penetration testing process, the target systems are attacked and penetrated using the plan applied in the earlier process.

### *d) Privilege Escalation*

After the successful penetration into the system, privilege escalation technique is used to identify and escalate access to gain higher privileges, such as registry/root access or administrative privileges to that particular it environment system or network.

### *e) Result Analysis And Cleanup*

At last in this process the root cause analysis is performed as a result of a successful compromise to the system leading to penetration testing and providing suitable recommendations in order to make the system secure by plugging the holes in the system. Vulnerability assessment and penetration testing involves compromising the system, and as the result of this process some of the files may be altered. This process ensures that the system is brought back to the original state, before



ISSN: 2278 – 1323 

the testing, by cleaning up or restoring the data and files used in the target machines.

Now as you got aware about the basics of processes involved in vulnerability assessment and penetration testing let's move on some VAPT tools which are required at every steps to perform VAPT successfully: –

***Web Application Attack and Audit Framework***

W3af is an extremely powerful and flexible framework for finding and exploiting web application vulnerabilities. It is easy to use and features a lot of web assessment and exploitation plugins.

***Induction of Metasploit :***

The **MetasploitProject** is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

Its best-known sub-project is the open source. **Metasploit Framework**, a tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shellcode archive and related research.

The Metasploit Project is well known for its anti-forensic and evasion tools, some of which are built into the Metasploit Framework.

## V. METHODOLOGY

During Information gathering should be to gain accurate information about your targets without revealing your presence or your intentions, to learn how the organization operates, and to determine the best route. Metasploit is the best console for information gathering, as it is a very comprehensive penetration testing tool. This covers whole information gathering of a network using Metasploit.

Information gathering requires careful planning, research, and most importantly, the ability to think like an attacker. At this step, you will attempt to collect as much information about the target environment as possible.
There are two types of information gathering: passive and active.

***1) Passive Information Gathering***
Using passive information gathering, you can discover information about targets without touching their systems. For example, you can identify network boundaries, operating systems, open ports, and web server software in use on the target without touching their system.

***2) Active Information Gathering***
In active information gathering, we interact directly with a system to learn more about it. We might conduct port scans for open ports on the target or conduct scans to determine what services are running. Each system or running service that we discover gives us another opportunity for exploitation.
But beware If you get careless while active information gathering, you might be nabbed by an IDS or intrusion prevention system (IPS).



ISSN: 2278 – 1323 


**Importing Nmap Results into Metasploit**

When you are working with other team members, with various individuals scanning at different times and from different locations, it helps to know how to import a basic nmap generated XML export file into the Framework.

First, we scan the Windows virtual machine using the -oX option to generate a Target.xml file.

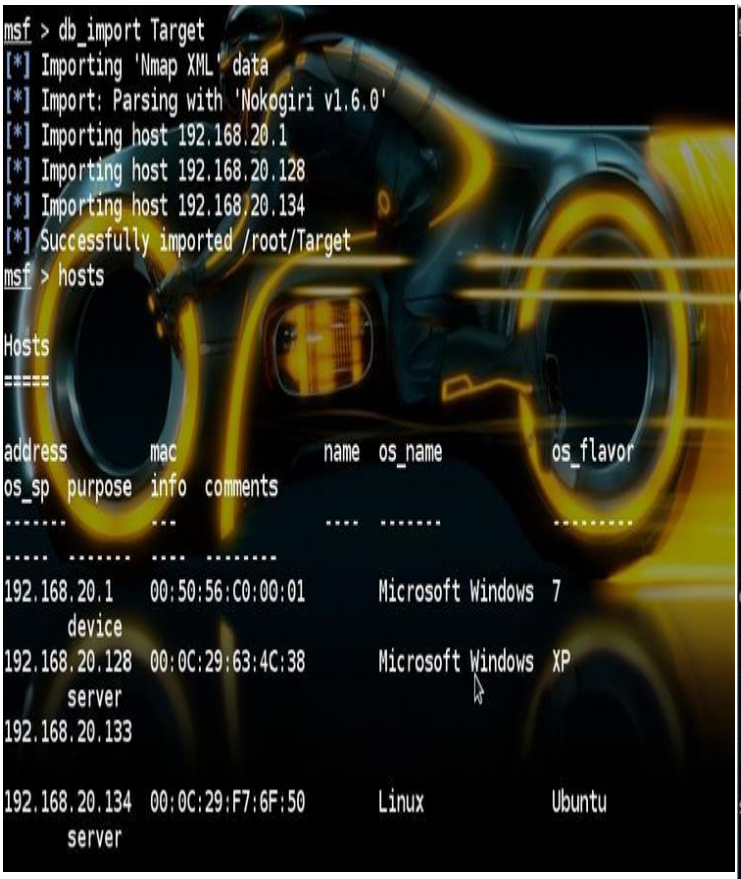
#nmap -Pn -sS -A -oX Target 192.168.20.0/24


After generating the XML file, we use the **db_import** command to import it into our database. We can then verify that the import worked by using the **"hosts"**command, which lists the systems entries that have been created, as shown here:

msf > db_import Subnet1.xml
msf> hosts



ISSN: 2278 – 1323 





**Running Nmap from MSFconsole**

We've performed advanced enumeration on our target, now let's connect Nmap with Metasploit. First, we should be able to enter the db_nmap command from within msfconsole to run Nmap and have its results automatically stored in our new database.

#msf > db_nmap -sS -A 172.16.32.131

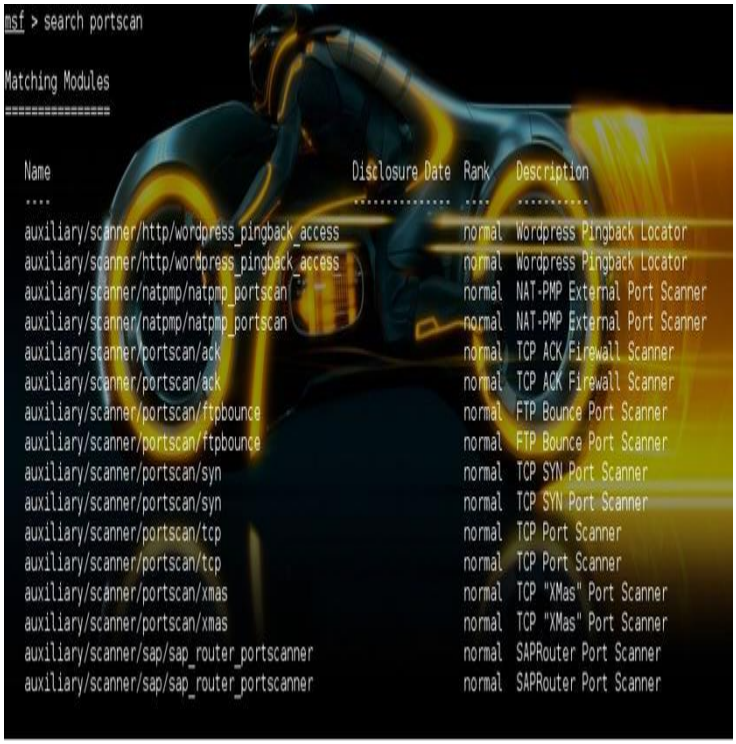
Metasploit has several port scanners built into its auxiliary modules that directly integrate with most aspects of the Framework. We'll use these port scanners to leverage compromised systems to access and attack.

To see the list of port scanning tools that the Framework offers, enter the following.

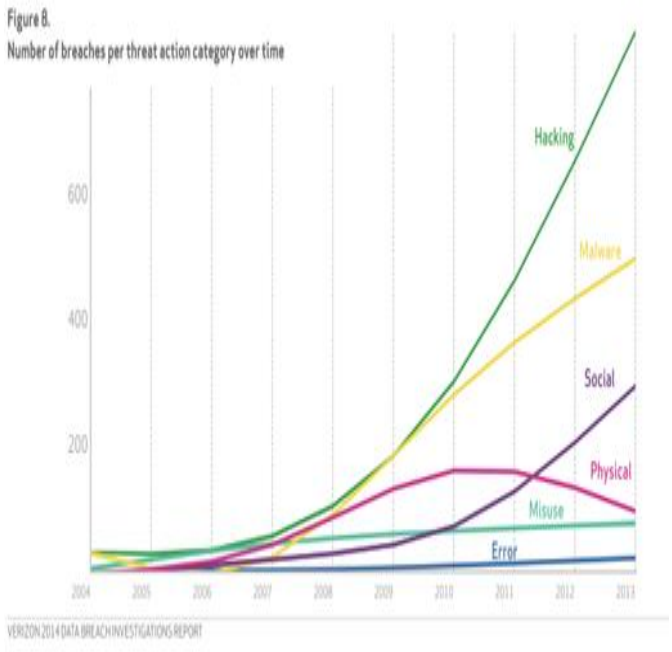
#msf > search portscan



ISSN: 2278 – 1323 

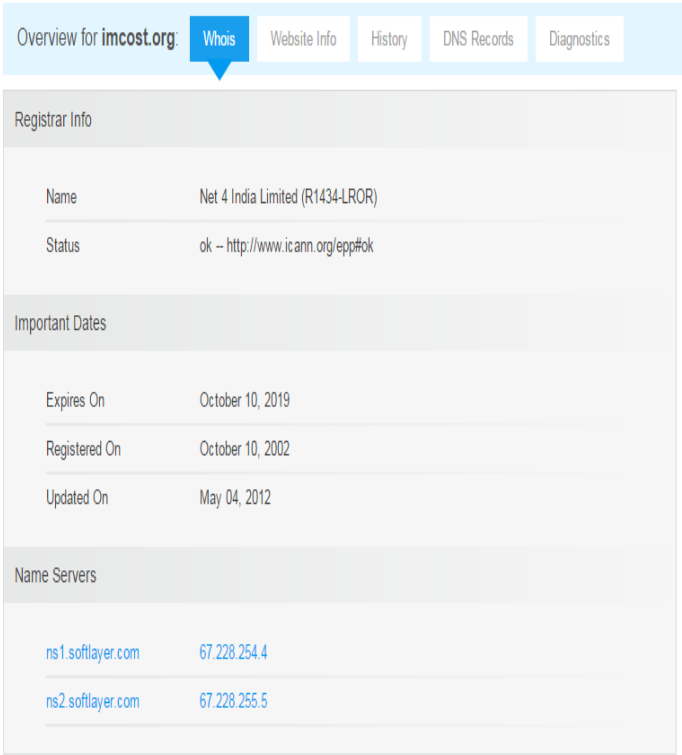



## DATA BREACH INVESTIGATION REPORT



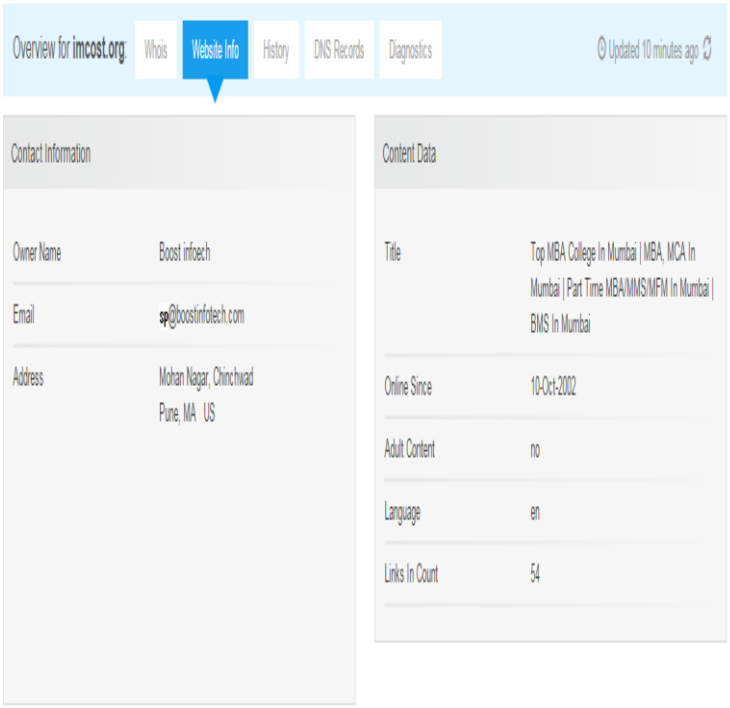

## VI. CONDUCTING PETEST ON WEBSITE

***Reports after Scanning:*** www.imcost.org



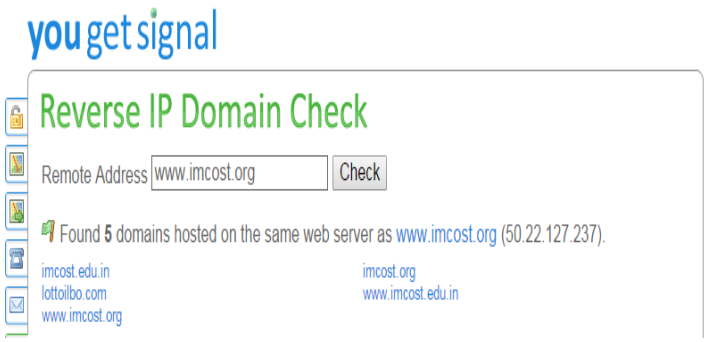



ISSN: 2278 – 1323 





Registration Details




Domains Hosted On Same Web Server



ISSN: 2278 – 1323 

**Information Gathering**

Domain Name:IMCOST.ORG

Domain ID: D91080579-LROR

Creation Date: 2002-10-10T09:34:32Z

Updated Date: 2012-05-04T12:21:06Z

Registry Expiry Date: 2019-10-10T09:34:32Z

Sponsoring Registrar:Net 4 India Limited (R1434-LROR)

Sponsoring Registrar IANA ID: 1007

WHOIS Server:

Referral URL:

Domain Status: ok -- http://www.icann.org/epp#ok

Registrant ID:10686475097360

Registrant Name:Boost infoech

Registrant Organization:

Registrant Street: mohan nagar, chinchwad

Registrant City:pune

Registrant State/Province:MA

Registrant Postal Code:411019

Registrant Country:IN

Registrant Phone:+99.999999999999

Admin ID:10686475101040

Admin Name:sandeep p pachpande

Admin Organization:

Admin Street: mohan nagar , chinchwad

Admin City:pune

Admin State/Province:MA

Admin Postal Code:411019

Admin Country:IN

Admin Phone:+91.0207464400

Admin Phone Ext:

Admin Fax: +91.0207471753

Tech ID:10686475110780

Tech Name:sandeep p pachpande

Tech Street: mohan nagar , chinchwad

Tech City:pune

Tech State/Province:MA

Tech Postal Code:411019

Tech Country:IN

Tech Phone:+91.0207464400

Tech Fax: +91.0207471753

Name Server:NS1.SOFTLAYER.COM

Name Server:NS2.SOFTLAYER.COM

DNSSEC:Unsigned

## VII. PROPOSED SOLUTION

***"Manual Pentesting"***

A Penetration tester's job is to demonstrate and document a flaw in security. In a normal situation, a pen tester will perform reconnaissance to find some vulnerabilities, exploit those vulnerabilities to gain access, then possibly extract some small piece of data of value to prove that the system is not secure. Note that this doesn't say which vulnerability the tester will exploit, and the tester might be free to try anything from a social engineering attack to a WiFi sniffer to a physical break-in. However, pen testers generally must work within limits or boundaries. Often this is at the



ISSN: 2278 – 1323 

request of the clients: "Please demonstrate that you can or can't get inside our network, but we don't want you to send any phishing emails to our employees." And the security company may have a policy of never installing certain types of malware. (There's little reason for a pen-tester to install a botnet client or to hide his tracks behind a rootkit, for example, unless he's demonstrating the need to scan for botnets and rootkits.)Some clients will place many limits on the tests, such as "just test the security of my application server." These clients may be under the impression that a hacker will be thwarted by the magical firewalls they bought that will protect the app server from every conceivable form of external attack. Or it could be that they have a different team focused on firewall defenses, and a third team working on social engineering awareness campaigns. The client may also ask that the pen tester not exfiltrate the valuable data - knowledge of the holes themselves is enough for them. Either way, the pen tester must carefully stay within the limits given, even when the tester can identify a more effective avenue of exploitation. The pen tester is usually only reluctantly given a position of trust, because they're often viewed as "criminal hackers". By carefully documenting and exposing every flaw they exploited, they gain trust through professionalism. If a tester sees a flaw he is not authorized to explore, he should point it out, but not explore it unless he first obtains permission. Also note the goal of the pen tester is not to "install malicious software". The goal is to demonstrate the adequacy of the security guarding information of value (credit cards, trade secrets, marketing plans, server administration, etc.) Malware is just one technique used by hackers. For starters, I would recommend you read, practice, and learn what you can at home and on line. Check out the Certified Ethical Hacker books and training available. Try to attend local, regional, or national security conferences and events. You may have local "white-hat" groups like OWASP that have meetings you can attend and people you can meet. You may also have a more "gray-hat" DEFCON chapter nearby, again, these would be people you could learn from. It's worth noting that quite often, a client will impose limits on a pen-tester's scope of practice. They may hire someone to test their network, their physical security, or even just their reception staff's reaction to suspicious characters; so quite often the difference between two jobs is what the client wants doing.

## VIII. CONCLUSION

Penetration tests offer unparalleled insight into an organization's security effectiveness as well as a road map for enhancing security. By hiring experts to simulate a cyber attack, vulnerabilities can be identified and corrected before they are exploited by a hacker or malicious insider.

Penetration testing helps answer the question, "how effective are my computers, network, people, and physical security at deterring a highly motivated and skilled hacker?" A Pen Test is a simulated cyber attack that offers unparalleled insight into an organization's data security effectiveness. During the test, security vulnerabilities are identified and attempts are made to compromise systems and gain unauthorized access to data.

Manual Pentesting or Pentester or an Ethical Hacker are terms used to describe hacking performed by a company or individual to help identify potential threats on a computer or network. A Pentester attempts to bypass system security and search for any weak points that could be exploited by malicious hackers.

This information is then used by the organization to improve the system security, in an effort to minimize or eliminate any potential attacks.

Expressed (often written) permission to probe the network and attempt to identify potential security risks.

Respect the individual's or company's privacy.

Close out work, not leaving anything open for you or someone else to exploit at a later time.

Allow software developer or hardware manufacturer know of any security vulnerabilities



ISSN: 2278 – 1323 

you locate in their software or hardware, if not already known by the company.

At the conclusion of the penetration test, a detailed report summarizing the project is provided as the deliverable. The report contains several elements, including an executive summary, project methodology, systems tested, detailed summary of findings, risk overview, and recommendations. The end result of the test is either confirmation that systems are effectively secured or the identification of vulnerabilities that require remediation efforts.

## IX. ACKNOWLEDGEMENT

The Research Work was supported by OWASP members and KeralaCyberSquad Researchers & KeralaCyberArmy Researchers and Web Application Security Researchers. Comprehensive support from FireBleed Team, Hostmate.co,.

## X. REFERENCES

[1] James. S. Tiller, "CISO's guide to penetration testing", Taylor and Francis Group, CRC Press Publication, 2012.

[2] P. Xiong and L. Peyton, "A Model driven Penetration test framework for Web Applications", IEEE8th Annual International Conference on Privacy, Security & Trust, Aug 17-19, 2010, Ottawa, ON, Canada.

[3] B. Liu, L. Shi and Z. Cai, "Software Vulnerability Discovery Techniques: A Survey", IEEE 4th International Conference on Multimedia Information Networking and Security, Nov 2-4, 2012 Nanjing, China

[4] B. Duan, Y. Zhang and D. Gu, "An easy to deploy Penetration testing platform", IEEE 9th International Conference for young Computer Scientists, Nov 18-21, 2008, Hunan, China.

[5] Dr. D. Geer and J. Harthorne, "Penetration testing: A Duet", IEEE Proceedings of 18th Annual Computer Security Application Conference, ACSAC'02, 2002, Washington, DC, USA

[6] S. Sparks, S. Embleton, R. Cunningham and C. Zou, "Automated vulnerability analysis: Leveraging control flow for evolutionary", IEEE 23rd Annual Computer Security Applications Conference, Dec 10-14, 2007, Miami, Florida.

[7] Open Web Application Security Project, https://www.owasp.org/index.php/Category: Vulnerability

[8] Vulnerability Analysis, http://www.pentest-standard.org/index.php/ Vulnerability_Analysis

[9] Penetration Testing Limits http://www.praetorian.com/blog/penetration-testing/ limitations-of-penetration-testing/,2008

[10]EC-Council, (2010). Certified Ethical Hacking Training Course.

## XI. AUTHORS PROFILE

***Sherin S Panikar***, Master of Computer Application student from Institute of Management & Computer Studies, Thane. From University of Mumbai.
Certified Ethical Hacker v8 and Certified Security Expert from EC Council.
With 6 years of experience in Information Security & Cyber Security Domain. Well Versed with curcumventing Network Pentesting, Web Application Pentesting and Malware Analysis.
Blog: www.KeralaCyberSquad.blogspot.in



ISSN: 2278 – 1323 