Penetration Testing and Vulnerability Assessment

Irfan Yaqoob [1], Syed Adil Hussain [2], Saqib Mamoon [3], Nouman Naseer [4], Jazeb Akram [5], Anees ur Rehman [6]
[1, 2, 3, 4, 5] University of the Punjab, Jhelum Campus, Pakistan
[6] University of Engineering and Technology, Lahore, Pakistan

Abstract – The main objective of this research paper is to identify common network threats and define countermeasures to prevent these threats. In this modern era, all of the persons are using the facility of internet. SECURITY is one of the major issue faced by everyone. Everyday professional hackers crack the security and take the advantage of vulnerabilities to access the top secret and confidential data. To avoid these threats we proposed a solution named vulnerability assessment and penetration testing (VAPT). In this technique CIA principal are achieved, CIA is abbreviated Confidentiality, Integrity and Availability. All three goals refer your data to keep secure and not to go in wrong hands. Confidentiality refers to the concept of keeping data out of reach of unauthorized persons, integrity refers the data must not be alters in case on unauthorized access and availability refers to the concept of high availability i.e. data is available to all the users when needed. So in vulnerability assessment we find week point of the system and in penetration testing we proposed how to keep our system secure from hackers and stop possible attacks. This paper gives the best overview of VAPT and describes the different process and methodology of Vulnerability Assessment and Penetration Testing.

Index Terms – Vulnerability assessment, DDoS, ARP, SQL, DNS, Spoofing, Asset, Capabilities, Penetration Testing, Web Server, DHCP Server, Mailing Server, External Penetration Testing, Internal Penetration Testing, Black Box Testing, White Box Testing, Gray Box Testing, Virus, Trojan Horse, Worm, Privilege Escalation Network Security.

1. INTRODUCTION

Vulnerability assessment, also known as vulnerability analysis is a process that defines, identifies, and classifies the security holes (vulnerabilities) in a communication infrastructure, network, or a computer. In this paper we will discuss different and important concept of information technology along with common network attacks and vulnerabilities form where attacks exploit. This repot also covers penetration testing. What procedures penetration testing undergo. Scope of Pen-Test, Pen-Test Approaches, Models, Techniques etc. Pen-Test formal and standard report formats, case study and countermeasures to cover vulnerabilities in Pen-Test report are parts of this report.

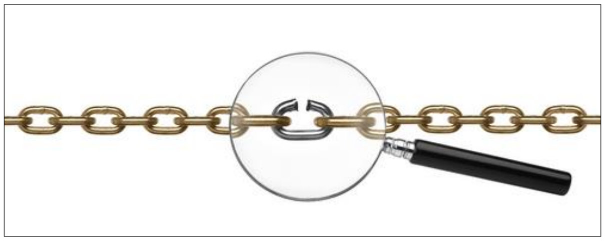
This paper is divided into various sections. In section ii, iii and IV the author will describes what is vulnerabilities and why vulnerabilities Assessment, in section V and VI the network vulnerabilities and threat to network vulnerabilities is described. The section IX to XVII details the different texts of vulnerabilities like PEN-Testing, Black Box Testing, White Box Testing and Gray Box Testing, XIX is last section where author conclude this paper with the complete details of the work of vulnerabilities Assessment and Penetration Testing.

2. VULNERABILITY

Vulnerability in network security is defined as flaw or weakness in the network or system from where any attacker can possess into our network or system to exploit. The network or system containing these vulnerabilities is called vulnerable network or vulnerable system. More the network system is vulnerable; more is the threat to exploit. Because of these vulnerabilities numbers of systems are exploit each year. Vulnerable network or system may be compromised by different attacks like, DDoS, DNS Spoofing, DHCP Snooping, ARP Poisoning, Man-in-the-Middle, Smurf attacks, Buffer overflow, SQL injection attack and other many cyber-attacks along with a number of malicious attacks including Viruses, Trojan horse, Worms, Malwares and root kits etc. These vulnerabilities are due to week passwords, software bugs, non-patching of software's and operating systems. Script code injection spaces etc.

3. VULNERABILITY ASSESSMENT

Vulnerability Assessment (VA) or Vulnerability Analysis (VA) or Vulnerabilities the process of scanning the system or software or a network to find out the flaws and weakness in that. This also includes series of systematic measures used to review and prioritize security vulnerabilities in a network or communication system/ or any application service. Vulnerability Assessment helps businesses in the determination of security posture of the environment and the level of exposure to threats.



Vulnerability Assessment play a vital role in every type of computer applications, system and infrastructure. Any system which is providing any kind of computing services may contain vulnerabilities so VA test plays a vital for every kind of computer application. In computer networks and communications, our information use to travel out of computers so presence of vulnerabilities may compromise our whole networks to exploited. If we perform following step then vulnerability assessment will be more effective

- Classification of Assets, Capabilities, and Resources.
- Assigning values and significance of these resources.
- Identifying vulnerabilities and potential threats to each resource.
- Mitigating and eliminating most somber vulnerabilities for the most important assets, resources and capabilities.
- Repeating steps from 1 to 4 in the same order after prescribed time frame.

The process of vulnerability assess should be performed in a fixed time intervals (in general quartile basis). In this way project team easily and timely detect any vulnerability that may occurs in network system. VA can be as single or the combination on both automated and manual scan of IT/ network infrastructure and without VA there is a risk that the network is not secured which may result serious exploits.

4. WHY VULNERABILITY ASSESSMENT?

The main objective of any organization to make profits towards its vision and goals. So organizations have opportunity to deploy Information Technology Infrastructures. After deployment of the information technology infrastructure, the main aim of any organization is to prevent their communication network and secure their confidential information from unauthorized access.

Therefore vulnerability assessment performs to check out weakness and flaws in a system. Objective of Vulnerability Assessment may include System Accreditation, Risk Assessment, Network Auditing, Compliance Checking and Continuous Monitoring. Major cause of vulnerabilities are due to weak passwords, flaws in systems, faulty and inappropriate configuration and human errors like, inappropriate permissions assigned to users, inappropriate network design and devices and like this etc. Some business standards institutions like PCI-DSS require organizations to perform vulnerability assessment on their network or systems.

5. COMMON NETWORK VULNERABILITIES

Networks and communication setup are designed to convey our information and data between devices. So our data or information has to travel out of devices like computers, tabs and mobile phones etc. Data and information have more threat of get compromised when out of our computers. Data and information may passed from wired or wireless medium. Vulnerabilities in our networks welcome attackers to get in communication systems to exploit. Here major network vulnerabilities are being listed from typical reviews.

- Missing patches

  Security patches are the software that system developers provide time to time after their continuous research on operating systems or software they provide to end users. These patches must be installed on operating systems. These patches cover any vulnerability in the system. Not needed all patches but recommended patches must be installed on core operating systems like servers cover related vulnerabilities. For example installation of security updates provided by Microsoft may cover possible vulnerability present in web server.

- Weak or default passwords

  Many systems like Domain Systems, Database Systems, Routers, Switches, Firewalls, IDS/IPS, Web Applications along with web servers and other systems like these are configured with week or default password. These passwords can easily be judge and hacked. For this strong passwords and recommended and also avoid from keeping default passwords. For example if we purchase a D-Link Wireless Access Point for our home usage. It has configured with default username “admin” and default password “admin”. Any attacker has easy access to our wireless network by these password schemes. So passwords must be changed and it should be complex so that hacker cannot access our system.

- Miss-configured firewall rules

  Firewall is the best thing which is used to prevent unauthorized access, malicious activities are not easily performed, but some time miss-configuration of firewall leads to vulnerabilities. These rules may contain serious weaknesses that allow unauthorized access in network systems. So firewalls should be configured according to proper standards. OWASP has defined wonderful policies for firewall configuration as well.

- Mobile devices

  Uses of remote cell phones like portable PCs, tablets, PDAs represent a most serious hazard in our system framework to get hacked. Almost all mobile devices can store cookies, web passwords, cache passwords; emails containing sensitive data in have a big vulnerability when connecting these devices with corporate networks.

- USB flash drives

  Use of USB devices are a pattern. These devices may contain passwords and other sensitive information; if stolen or misplaced can bring us to serious danger, because it contain our confidential data. And there is greater chance that these devices contain virus and worms, which affect our security walls.

Other vulnerabilities include authentication bypassing, plaintext passwords, wireless key enumeration, privilege escalation, gaining access, buffer overflow, remote command execution, cryptographic vulnerabilities like weak encryption algorithms and keys etc. These loopholes must be covered to ensure security.

6. THREATS TO VULNERABLE NETWORKS

Network system having vulnerabilities may bring a great number of network threats. These threats include Malware, Viruses, Worms, Payloads, Trojan Horses, Spywares, Root kits, Port Scanning, Social Engineering, MAC Address Spoofing, DoS and DDoS attacks, ARP Poisoning Attacks. These threats can also be categorizes as Untrusted Threats, Structured Threats, External Threats and Internal Threats and a vast number of cyber-attacks other than these. Every attack has its own potential towards networks. These attacks can takes place due to presence of vulnerabilities in network of telecommunication systems.

7. VULNERABILITY MANAGEMENT LIFE CYCLE

Vulnerability management consists of process named as Discover, Prioritize Assets, Assessment, Reporting, Remediating, and to verification that vulnerabilities have been eliminated.

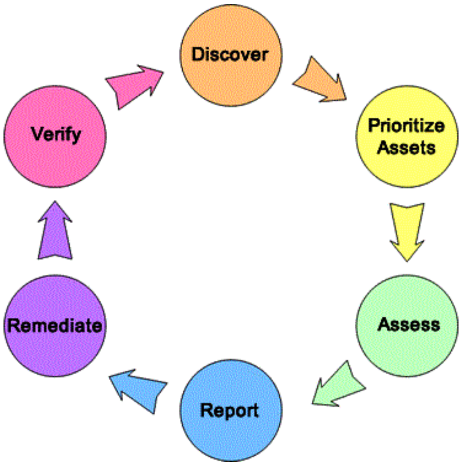


Fig: Vulnerabilities Management Life Cycle [5]

These steps have been further elaborated given as under.

Discover: -Discover means having proper record network assets, operating systems and other devices, list all vulnerabilities on a regular schedule.

Prioritize: - Categorize and assign values to those assets according to their importance and need in business operation.

Assess: - To determine a major and basic risk profile based on assets priority, risk and vulnerabilities.

Report:- Measure the level of business hazard related with your benefits as per your security strategies. Archive a security arrange, screen suspicious action, and depict known vulnerabilities..

Remediate:- fix vulnerabilities according to business risks. Enable access controls and cover weakness and flaw in network systems.

Verify: - Checking whether vulnerabilities that were discovered have eliminated. These may be carried out by security audits.

8. PENETRATION TESTING (PEN-TESTING)

Penetration Testing or simply Pen-Testing or Security Testing also known as ethical hacking the technique used to discover vulnerabilities in network system before an attacker exploits. This is the act of gaining access to networks or systems resources without the knowledge of user credentials like usernames and passwords. Penetration testing report visualize the evidence that vulnerabilities are present in your network or system from there penetration is possible in. moreover a penetration test report is capable to visualize the proactive and remedial measures to protect your network and enhance comprehensive defensive strategy. The penetration test report also depicts the satisfactory security approaches adopted by our security responsible professionals. These test report are also often required by security agencies, law-and-order agencies, information systems auditors and other stockholders.

It is significant to discuss that it is unlike that a pen-tester will uncover all vulnerabilities in one pen-test report. For example if a pen-tester has generated a report today it is obvious that it may no longer be valid after one month. It is because after the approval of pen-test report by owner, system may have get patched with new updates which may last a vulnerability in some web server which may considered secure in last pen-test report. So maintain a secure infrastructure, constant vigilance is considered necessary.

9. PEN-TESTING VS VA

In general people believe that Penetration Testing and Vulnerabilities Assessment are two same term but in actual these two terminologies have difference up to some extent. Vulnerabilities Assessment is defined as automatically identify weakness of the system via a software rather manually whereas Penetration testing mainly refers to a form of stress testing which exposes weakness in a vulnerable networks and sets standards to cover these vulnerabilities in the network. Vulnerabilities assessment process stops just before the system is compromised whereas break in as far as the scope of the agreement.

Penetration tests are important for a number of reasons like:-

- Determining the possibility of particular attacks to take place.
- Discover high risk vulnerabilities resulting from low risk vulnerabilities.
- Identifying vulnerabilities that may be difficult or impossible to detect with general scanning software.
- Identifying magnitude of a successful attack to a vulnerable network.
- Testing capabilities of network defenders to detect and response to network attacks.
- Provide evidence to increase allocations in security budgets.

Before launching a new system it is highly recommended that it should be tested first so that to check any vulnerability in the system. By this practice lots of vulnerabilities are identified before the system launching to avoid serious exploits. The Payment Card Industry (PCI) Data Security Standard (DSS) define Penetration Testing Standards. At least these standards are required to get meet for satisfactory pen-testing approach.

Let us consider comparison from another aspect as in tabular description.

	Vulnerability Assessment	Penetration Testing
Attributes	List-oriented	Goal-oriented
Type of Reports	Prioritized list of vulnerabi-lities categorized by critica-lly for remediation	Specific information of what data was compromised and vulnerabilities exploited
Purpose	Identify security vulnerab- ilities in system that may be exploited	Determine whether an application can withstand an intrus- ion attempt

10. WHY PENETRATION TESTING?

Once I wrote a blog on the topic of penetration testing; almost all the reader asked me this question *“Why Penetration Testing is so important”?* The answer can be given in a number of ways however the precise answer that I love is *“the process of finding vulnerabilities in networks and fix then before an attacker attacks”.* Penetration testing is very much important and it ensures that organization’s network is safe and up to date in meeting security standards. So by escaping to perform penetration test in systems is attempting to leverage the vulnerabilities discovered hence there is no way of knowing the risks that are presented to network system based on those vulnerabilities. We may divide why to perform penetration testing from different perspectives i.e. Business Perspective and Operational Perspective.

a) Business Perspective of Penetration Testing

Penetration testing secure IT infrastructure against failure by preventing financial losses. Organizations do spend millions of dollars from information security breaches on notification costs, remedial measures after system compromises for security which further lead to deceased productivity and lost revenue. So penetration testing is used to identify and nominates the possible risks of the organization and in this way organization secure his assets and confidential data from unauthorized access and secure his information . Authenticated industry standards have mandated as regulatory requirements for computing security systems, in case noncompliance heavy fines or other penalties may be imposed on those organizations during IT security audit processes.

If an organization compromise on security, it will bring them to a serious trouble some time it may leads to loss of customers’ confidence, challenges in marketing strategies, and dishonor of other stockholders and even failure of entire business. The study of CSI has estimated that the recovery may costs approximates up to $167700.00 per incident which is very huge amount. Penetration Testing assesses value of existing security products and provides the supporting opinion of future investment in information technology security mechanisms. PT can provide an evidence of issue and solid proposal of investment in IT security.

b) Operation Perspective of Penetration Testing

Penetration testing guides us to determine security procedures through appropriate vulnerabilities identification and assessment procedures. This will help us for the elimination of threats and risks, corrective and preventive measures, quickly real potential vulnerabilities. Through Penetration testing we can fine tune or patch to proactively eradicate the risks that have been identified during the process of vulnerabilities assessment.

11. WHO TO PERFORM PENETRATION TEST?

PCI DSS does not entail that QSA or ASV to execute a penetration test. PCI DSS requires performing this test by either expert internal resource or expert third party. If internal resources are to perform this test then these professionals must be well equipped and well qualified. Usually these professional are separate from the system for which penetration testing is being performed. For example a network administrator should not be engaged to perform penetration test of his own domain. Same case for other network domains like firewall, domain services or web services. Beside of these, at least following capabilities make comparatively good penetration testing professional.

- Complete knowledge of Operating systems.
- Professional in networking technologies including OSI, TCP/IP, DHCP, DNS, Routing, Switching, Snooping, ARP/RARP, STP/RSTP, all network security threats and attacks and all other areas which are not discussable here.
- Vast knowledge of scripting, BAT or VB Scripting.
- Must know about system programming, network programming and low level programming like assembly language.
- Deep knowledge with cores or network firewalls and proxy servers. Access control using these resources. After mastering these basics, one can move to PIX or ASA firewalls.
- Deep understanding with IPS and IDS. How to use these devices to secure our networks and what are dimensions of these devices.
- Knowledge of computer forensic domain.
- Must be database expert and at home in handling all complex level problems in Database Management Systems and System Analysis.

12. PENETRATION TESTING TYPES

Mainly there is two type of Pen-Testing, Physical Penetration Testing and Virtual Penetration testing. Physical includes tangible assets like Data Centers, Servers, Routers, Switches, CCTV Systems, Security Barriers and Security Guards etc. in this type penetration testers use to assess security loop holes that may exists in accessing IT gadgets physically. Illegal or unauthorized people have no access to these gadgets like Data Centers, Equipment and infrastructure. So a proper policy and standers are required to be defined regarding physical assets. Other natural disaster proofing falls also in physical penetration testing. It is needed to outcome that our building where core network infrastructure exists must be proofed in case flood, earthquake, heavy rain, storm, fire and even Cooling of Data Centers Equipment, Humidity etc.

In Virtual penetration testing we are testing intangible assets which may be Operating Systems, Software's, Web Servers, IOS, Firewalls, Databases and other virtual assets in a business organization. Mostly cause of network attacks are due to vulnerabilities in virtual infrastructures. These attacks are often software lever attacks which include, DoS/DDoS, Spoofing, DHCP Snooping, ARP Poisoning, Database Injection, phishing, overflows, exploit, password and hijack attacks etc. To secure virtual assets is more challenging for vulnerability assessment and penetration testing than physical assets. So virtual assets is more challenging than physical assets. More than 80% energies are expended in protecting these virtual assets as compared protecting physical assets.

Besides above mention penetration testing types we classify penetration testing in some other way. Penetration testing i.e. Physical PT, Network PT and Social Engineering PT. Network Penetration testing is related to flaws or week point of networks, this testing helps to identify flaws of network. Series of test are applied on network devices like modems, switches, routers, remote access devices, IPS/IDS, Firewalls and other devices in network to scan the network.

On the other hand, application penetration testing is used to identify an application's security controls by highlighting risks posed from potential vulnerabilities in applications. Firewalls and other traffic monitoring systems are used by organization to protect information whereas security threats still exist due to a number of hidden vulnerabilities which is needed to be explored and system should be protected.

Social Engineering plays a vital role to identify security threats to organizations. Social Engineering involves human interaction to compromise information about computer system of an organization. So Social Engineering Penetration Testing process determines the level of security awareness among workers that directly and indirectly own IT systems of the organization. Social Engineering penetration test also check that at what extent an organization's workers can exploit organization's secrets that is dangerous for current system.

13. PEN-TESTING METHODOLOGIES

There are three known strategies of penetration testing that profession testers use to adopt. These methodologies include Black Box, White Box and Gray Box Penetration Testing.

a. Black Box Testing

A testing technique in which tester does not know the internal design or structure of the target. They have to check for incorrect or missing function or interface error. This strategy is similar to blind test and like procedures adopted by real attacker who has no idea and information regarding the organization's network.

b. White Box Testing

In white box penetration testing approach, testers has complete knowledge about the target. Tester has full knowledge of internal working of system Generally tester and developer work together to perform this kind of test where all information provided to the team prior of running test. This information may include paths, credentials, procedures, addresses and protocols etc. that are being used in organization's network.

c. Gray Box Testing

Gray box testing falls between black and white box testing in which somewhat knowledge of the internal working of target is known to tester. Usually testers does not provided all information for the target however they need to gather further information required by their own before conducting the test.

Where, there penetration testing strategies are being discussed, it is necessary not to ignore two important penetration testing strategies that are Internal and External Penetration Testing.

External penetration testing techniques involve tests on the target using procedures performed from outside of the organization. External Penetration testing is done to the possibilities of external hacker can get in and how far he can be able to gain access to organization's internal structure.

Internal penetration testing is performed from inside the organization's network that own test target. This strategy is used to find out up-to what extent a disgruntled employee can cause the damage to the organization. Internal penetration testing checks out the potential of harmfulness if organization's network successfully penetrated by an authorized inside user with assigned privileges.

14. AREAS OF PENETRATION TESTING

Penetration Testing is done in almost areas of information technology. As the whole IT revolves around data and information of the business. So data at every stage in every area is not perfectly safe. However major Penetration Test areas have discussed as under.

- Physical Penetration Testing
- Software Penetration Testing
- Database Penetration Testing
- Network Penetration Testing
- Web Penetration Testing
- Wireless Network Penetration Testing
- Social Engineering Penetration Testing
- Cloud Penetration Testing
- Operating Systems Penetration Testing
- Mobile Devices Penetration Testing

This research has scoped to Network Penetration Testing. Network Penetration Testing is consider to be a very important task and is very common among all areas of Information Technology.

15. PHASES OF PENETRATION TESTING

There is no hard and fast rule of conducting penetration testing with respect to phases of conducting penetration test however common phases that every tester must have to go through are 1. Reconnaissance, 2. Execution, 3. Discovery. These three steps are baseline of each penetration test however these phases are further divided into sub phases for convenience of penetration testers. I recommend seven phases of a professional penetration testing on a target network.

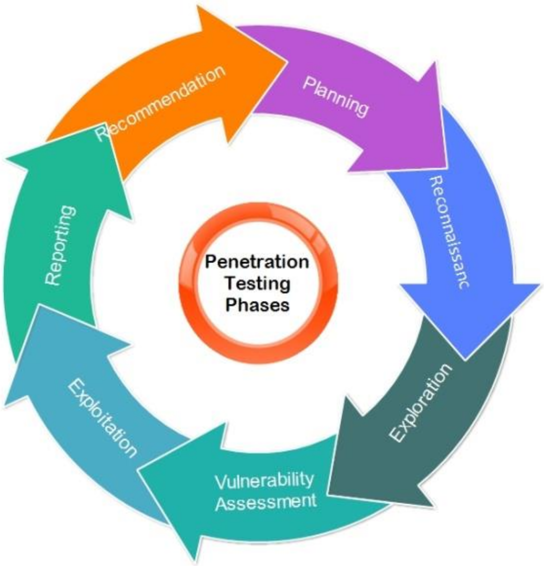


Fig: Phases of Penetration Testing [12]

Planning: In Planning phase scope of the test is determined, Like in which system test is to be done , how it should be done and who will perform this test , what will be the time frame, what should be the benefit to the organization , all these things are checked in planning phase of Pen-testing

Reconnaissance: After the scope of the test is done, this is the second phase in which Information gathering about target network. Information as much as possible are gathered in this phase. This is a complete phase which may consist of identifying target network status, operating systems, IP addresses range, open ports, domain name, DNS, DHCP, Wifi Key, Mail Server Records etc. Host Finger Printing, Port Scanning, Network Mapping, Network Enumeration are usually considered in reconnaissance phase.

Exploration: This is the third phase that deals with exploring the entire network based on necessary information gathered in reconnaissance phase. More precise to the network services. Like checked opened ports in last step. Using opened ports, the tester enters the network and explore the network more deeply. Testers scans the network for discovering network devices, firewall rules, users accounts and access control etc.

Exploration include host exploration, services identification and platform identification etc.

Vulnerability Assessment: Vulnerability is a path through which threats are revealed. Vulnerabilities are actually weakness in the system. Vulnerability assessment is the process of computing, ranking and pinpointing the vulnerabilities in the system. Penetration testers may use automated tools for known vulnerabilities. These tools are helpful by having updated databases for latest vulnerabilities and their details.

Exploitation: This is most difficult phase in penetration testing which deals with attacks to the target network. The penetration tester tries to exploits for different vulnerabilities discovered in last phase. Privilege Escalation in considered sub part of exploitation phase in which usually attacker takes advantage of programming bugs or design loopholes to crawl to the privileged access that are usually protected general users and applications. The system having more privileged accounts can be exploits up to more extent.

Reporting and Recommendation: This last phase in which documentation is done by testing team. This is final document on which all the phases based. The main object of penetration test is to point out all flaws and weakness in a network or a system that have covered in last phases. Final report should cover all phases' activities including a cover sheet, executive summary of vulnerabilities found in the network, threats imposed from these vulnerabilities, list of tools used and most important final recommendation after overall examination of test report. Upon final recommendation covered in the report, values of threats and mitigation of threats are discussed. Final recommendation phase must be done with upper level management in which preventive proposals are provided against founded vulnerabilities.

16. PENETRATION TESTING STANDARDS

Following is the list of professional standards and certifications regarding penetration testing. These organizations are well known and are accredited throughout the Information Security World.

- EC-Council LPT (Licensed Penetration Tester)
- OSTTMM(Open Source Security Testing Methodology Manual)
- PTF (Penetration Testing Framework)
- OWASP(Open Web Application Security Project)
- ISSAF (Information Systems Security Assessment Framework)
- WASC-TC(Web Application Security Consortium Threat Classification)
- OISSG (Information Systems Security Assessment Framework)
- PCI DSS v3.1 (Payment Card Industry Data Security Standard)
- ISO/IEC27001:2005(Information Security Management Systems)
- ISO/IEC 27005:2008 (Information Security Risk Management)

17. PENETRATION TESTING TOOLS

However number of tools are used for penetration testing, but we discuss few of them in details. Different tools are popular to perform different kind of tasks in different domains. These tools are designed for specific purpose in used in specific domain. No single tool is capable to do all tasks in penetration testing. All these tools are used together which are then helpful for successful penetration testing report. Different flavors of Linux have designed specifically for Network / Information Security Assessment however Back Track 5.0 and Kali Linux have specifically designed and developed for this purpose. These are bootable operating systems that include lots of tools. Some tools are given as under.

- Nmap: Nmap (Network Mapper) is known as the World's best security scanner. It is used to determine hosts and services on a computer network. It is free tool available in both Back Track and Kali Linux. It is used to discover network discovery, port scanning, host discovery, version detection, OS detection etc. Typical Nmap is used for auditing the security of devices or firewall, network inventory, discover open ports on a target host, auditing the security of network, finding and exploiting vulnerabilities in the network. It is also used to find host discovery, post scanning and version detection. Nmap uses raw IP packets to find out what hosts are available, what kind of services are being offered by those hosts, what operating systems and their versions are running on hosts, what kind of firewalls are installed as well as a number of other parameters. It can work best in all operating systems in both GUI and Command Line utility. Nmap has a number of variations like Zenmap, Ncat, Ndiff and Nping for different tasks associated to each.
- Nessus: Nessus is top rated network vulnerability scanner developed by Tenable Network Security. Initially it was free and open source software designed to run only on Linux OS however, later on from 2008, it available with cost and can run on MAC OS, Windows OS, Free-BSD platforms. It is so powerful vulnerability scanner, and according to a survey in 2005 this tool was used by almost 75000 organizations. It is a web based tool used to scan DOS against TCP/Ip, default password, vulnerability that allow a remote hacker to control, preparation of PCI DSS audits and misconfiguration.

- Metasploit Framework: Metasploit Framework is a open source tool that provide information about security flaws and vulnerabilities and help in penetration testing. It can also be employed to test vulnerabilities in network system. It is available free of cost and runs on almost all versions of UNIX and Windows. Metasploit Framework provides attack payloads, attack libraries that can be put jointly for modular approach. Main purpose of Metasploit Framework is to get access to command prompt of computer in targeted network. Once command prompt is accessed it is very easy for even hacker to have all controls over that target. Once; from hacker's point of view; the system is accessed, he can execute code for easier access to target next time.
- Wireshark: Wireshark originally named as ETHEREAL is another excellent and unique tool based on its specific use and nature. This is another multi-platform, open source network platform analyzer which is used for troubleshooting analysis of a network. Wireshark is used for viewing of TCP streams in the network. Wireshark supports a vast variety of protocols and media types.
- Aircrack:- Aircrack is a tool to access WIFI network secuity. It intelligently can crack 802.11 a/n/g wireless networks. It uses best wireless cracking algorithms to recover WiFi Keys by examining even encrypted packets. Aircrack has a number of tools like Airodump, Aireplay, Aircrack-ng and Airdecap for different assignments.
- Cain & Abel: - It a password recovery tool for Window. This is known windows only password recovery tool. It recovers password using technique like network sniffing, cracking encrypted password by dictionary attacks, bruit-f0rce attacks, sniffing VOIP communications, decoding scrambled passwords, uncovering cached passwords alongwith analysis of routing protocols being used in the network in well documented manner. It has some additional feature like WEP cracking calculating hashes.

I think pertinent to at least name other very important network penetration testing tools like Snort, NetCat, TCPDump, John the Ripper, Kismet, OpenSSH/PuTTY, Brup Suit, Nikto, Hping, Ettercap, Sysinternals, W3af, OpenVAS, Scapy, THC Hydra, Paros Proxy, NetStumbler, WinDump, Network Security Toolkit, OWASP Mantra etc. Each tool among these has specific usage in specific scenario and is being widely used in penetration testing and hacking procedures.

18. ETHICAL AND LEGAL ISSUES

However Penetration Testing also known as ethical hacking is the process of exploring weakness in a network in order to find out all possibilities and loopholes from where attackers penetrate into the network system and exploits. In actual Penetration Testing totally resembles the process of hacking into networks but only the difference is that hacking is a crime that is done illegally whereas penetration testing is conducted in a legal way, because it is done by hackers by the permission of that owner of the system. Different countries have settled codes of laws for hackers. The owner the network employee pen-testers to dig out all the possible holes in order to mitigate hacking attacks. It is very pertinent for both parties to sign mutual agreement before observing a penetration test. The agreement may have following clauses.

- Written Permission: Before conducting a pen test, both parties sign on written documents. Testers should have to document all of the processes of penetration test. This will protect testers from any legal issue in future.
- Damage Control: While performing pen testing, there should be the chance of damage in the network. So the testers must have to notify customer about potential harm or incidental damage that may occur during the test. Testers do not take liability in case incidental harm of record or deletion of data etc.
- Scope of Work: Pen-Testers must have to define scope of work defining external and/or internal vulnerabilities assessment. Scope also consists of networks, what systems, what devices will be performed test on, how much time is required etc.
- Professional Approach: Professional technique and approaches are performed by pen-tester to find the possible vulnerability in the network. Also priory defines what kind of service is needed by the owner like just port scanning or exploitation etc. It is not good to make promises of digging hills.
- Premises and Jurisdiction: In this section it is clearly defined that where is venue to perform the pen-test. Different countries may have different Cyber Laws so performing test in America may be a legal issue that in Germany.
- Privacy Issue: As the pen tester penetrate into the system or network, so they access confidential data and other database, so he should not compromise on privacy issue of that organization.

Besides all above cited clauses are in favor of penetration testers, pen-testers are also expected to be ethical during and after a successful pen-test. Usually, computer users are not technical and they rely on the technical professionals so penetration testers are also needed to act as doctor not a thief. Because of this, information and network security is being monitored and governed by authorized organizations that have provided licenses and certifications that guarantee technical competency along-with ethical considerations of licensees.

19. CONCLUSION

In this article we mainly emphasized on and vulnerability and pen testing that provide security and ethical way to evaluate and determined the system and network weakness and flaws. Missing patched, weak or default passwords, opened unnecessary ports, miss configured firewalls and other networking devices, mobile and USB devices are common vulnerabilities, so penetration testing first points out these vulnerabilities then provides solutions to cover these vulnerabilities. Penetration testing can be performed externally and internally among three types as Black Box, White Box and Gray Box in a number of defined phases includes Planning, Reconnaissance, Exploration, Vulnerabilities Assessment, Exploitation, Reporting and Recommendation. There are several tools to conduct a penetration test like Nessus, Nmap, Metasploit and Cain & Abel etc. Each tool has expertise in specific area like Nmap is best in port scanning and Metasploit is best in exploitation etc. Penetration testing is similar in sense of hacking process hence penetration testing is legal while hacking is illegal. Penetration testing is observed upon the demand of owner whereas hacking is getting in networks illegally and is a crime. Hence penetration testers are hoped to be ethical which conducting tests.

REFERENCES

[1] Xynos, K., Sutherland, I., Read, H., Everitt, E., & Blyth, A. J. (2010). penetration testing and vulnerability assessments: A professional approach.

[2] Arkin, B., Stender, S., & McGraw, G. (2005). Software penetration testing. *IEEE Security & Privacy*, *3*(1), 84-87.

[3] Fonseca, J., Vieira, M., & Madeira, H. (2007, December). Testing and comparing web vulnerability scanning tools for SQL injection and XSS attacks. In *Dependable Computing, 2007. PRDC 2007. 13th Pacific Rim International Symposium on* (pp. 365-372). IEEE.

[4] Du, W., & Mathur, A. P. (2002). Testing for software vulnerability using environment perturbation. *Quality and Reliability Engineering International*, *18*(3), 261-272.

[5] Reddy, M. R., & Yalla, P. (2016, March). Mathematical analysis of Penetration Testing and vulnerability countermeasures. In *Engineering and Technology (ICETECH), 2016 IEEE International Conference on* (pp. 26-30). IEEE.

[6] Du, W., & Mathur, A. P. (1998). Vulnerability testing of software system using fault injection. *Purdue University, West Lafayette, Indiana, Technique Report COAST TR*, 98-02.

[7] Bacudio, A. G., Yuan, X., Chu, B. T. B., & Jones, M. (2011). An overview of penetration testing. *International Journal of Network Security & Its Applications*, *3*(6), 19.

[8] Bau, J., Bursztein, E., Gupta, D., & Mitchell, J. (2010, May). State of the art: Automated black-box web application vulnerability testing. In *Security and Privacy (SP), 2010 IEEE Symposium on* (pp. 332-345). IEEE.

[9] Goel, J. N., & Mehtre, B. M. (2015). Vulnerability assessment & penetration testing as a cyber defence technology. *Procedia Computer Science*, *57*, 710-715.

[10] Shah, S., & Mehtre, B. M. (2015). An overview of vulnerability assessment and penetration testing techniques. *Journal of Computer Virology and Hacking Techniques*, *11*(1), 27-49.

[11] Umrao, S. A. C. H. I. N., Kaur, M. A. N. D. E. E. P., & Gupta, G. K. (2012). Vulnerability assessment and penetration testing. *International Journal of Computer & Communication Technology*, *3*(6-8), 71-74.

[12] Knowles, W., Baron, A., & McGarr, T. (2015). Analysis and recommendations for standardisation in penetration testing and vulnerability assessment: penetration testing market survey.

[13] Fonseca, J., Vieira, M., & Madeira, H. (2008, December). Training security assurance teams using vulnerability injection. In *Dependable Computing, 2008. PRDC'08. 14th IEEE Pacific Rim International Symposium on* (pp. 297-304). IEEE.

[14] Austin, A., Holmgreen, C., & Williams, L. (2013). A comparison of the efficiency and effectiveness of vulnerability discovery techniques. *Information and Software Technology*, *55*(7), 1279-1288.

[15] Finifter, M., Akhawe, D., & Wagner, D. (2013, August). An Empirical Study of Vulnerability Rewards Programs. In *USENIX Security Symposium* (pp. 273-288).

Authors

Irfan yaqoob
Research Officer at Punjab Information Technology Board,
Field of Study: Software Quality Assurance, Soft. Engineering,
BS Computer Science

Saqib Mamoon
Research Scholar, Entrepreneur.
Field of Study:
Artificial Intelligence, Machine Learning and Deep Learning.
BS Computer Science