Vulnerability Assessment and Penetration Testing: A proactive approach towards Network and Information Security

Muhammad Zeeshan[1], Shams Un Nisa[2], Tazeen Majeed[3], Nayab Nasir[4], Saadia Anayat[5].
Department of Computer Science and Information Technology
Virtual University of Pakistan, Lahore Pakistan.
Peshawar Campus[1], Islamabad Campus[2], Faisalabad Campus[3, 4], Talagang Campus[5].
ms150400558[1], ms140400309[2], ms160400234[3], ms150400522[4], ms150401012[5]@vu.edu.pk

ABSTRACT

With increasing dependency on IT infrastructure, the main objective of a system administrator is to maintain a stable and secure network, to identify common network threats and define countermeasures to prevent these threats. The information which is stored in computer's repository may be less compromised than the information travelling over the network. Network is an untrusted environment as compared to computer's repository, so information needed to kept secret and must not be stolen. In this paper, we perform an empirical study on how to do vulnerability assessment with the aim of search for any potential loopholes or vulnerability contain in a system. And also briefly described the existing tools of the Pen- testing, no one of the tools have capabilities to find out all the vulnerabilities. We will perform different phases of the penetration testing for proactively to protect from any possible treats towards our network. Hence penetration testers are hoped to be ethical which conducting tests.
.

KEYWORDS

Vulnerability, DDoS, DNS, Spoofing, Asset, Capabilities, Privilege Escalation.

1.INTRODUCTION

Vulnerability assessment is the process of digging out these black holes and then reporting along with necessary measures to overcome these black holes to avoid any mishap. In this paper we will through light on basic IT security concepts along with common network attacks and vulnerabilities form where attacks exploit. [1] 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 term that refers to flaw or weakness in the network or system from where any attacker can get into our network or system to exploit. The network or system having these vulnerabilities is called vulnerable network or vulnerable system. More the network system is vulnerable; more is the threat to exploit. Millions of systems exploit every year due to vulnerabilities. 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 usually result from 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 Scanning is the process of defining, identifying and classifying vulnerabilities in a network or communication system. 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 assists businesses in the determination of security posture of the environment and the level of exposure to threats.

Figure1: Vulnerability Assessment [2]

Vulnerability Assessment has a superior role in every type of computer applications, system and infrastructure. Any system providing any kind of computing service may have vulnerabilities so VA test is very much important 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. Vulnerability Assessment can be more effective and valuable if performed in following order. [2]

- 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 repeated after fixed prescribed time intervals (in general quartile basis). This will help the team to cover any vulnerability timely that may occur in a 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 purpose of any organization to make profits towards its vision and goals. So organizations have opportunity to deploy Information Technology Infrastructures. So securing the network and communication system is the core objective after deployment to prevent an attacker to get into network that can be set a very large potential risk for the system.

Therefore vulnerability assessment performs to check out black holes in a system. Objective of Vulnerability Assessment may include System Accreditation, Risk Assessment, Network Auditing, Compliance Checking and Continuous Monitoring. These vulnerabilities may occur from 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 infrastructures are deployed for information sharing 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 [3] . Data may travel on 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.

5.1 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.

5.2 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 guessed and probed. This scheme must be changed to keep default password intact. 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 to customize and must be kept complex to guess by any attacker.

5.3 Miss-configured firewall rules

Use of firewall in to prevent unauthorized access is pretty good practice but most of the times miss-configuration of rules on firewalls is a vulnerability. These rules may contain serious weaknesses that allow unauthorized access in network systems. So firewalls should be ruled according to standards. OWASP has defined wonderful policies for firewall configuration as well.

5.4 Mobile devices

Uses of wireless mobile devices like laptops, tablets, smart phones pose a greatest risk in our network system 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.

5.5 USB flash drives

Use of USB devices are a pattern. These devices may contain passwords and other sensitive information; if stolen or misplaced can be a cookbook for an evildoer. These portable devices may contain malware and viruses which can harm our system inside the firewall.

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

Presence of vulnerabilities may welcome a vast 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 [4]. 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 is a continuous rotating process to Discover, Prioritize Assets, Assessment, Reporting, Remediating, and to verification that vulnerabilities have been eliminated.

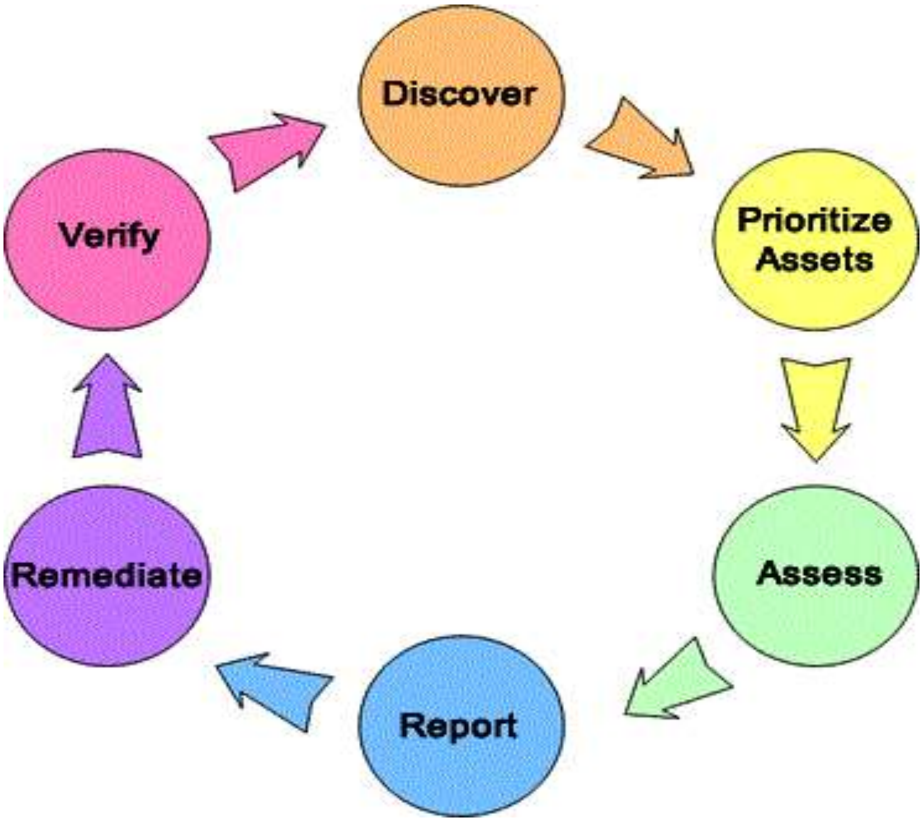

Figure 2: Vulnerabilities Management Life Cycle [4]

These steps have been further elaborated given as under.

7.1 Discover

To record all assets of the network, operating systems and other devices, list all vulnerabilities on a regular schedule.

7.2 Prioritize

Categorize assets and assign values to those assets groups based on their importance in business operation.

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

7.3 Report

Measure the assets according to security policy of business organization. Document assessment based on security risks, threats and known vulnerabilities.

7.4 Remediate

Fix vulnerabilities according to business risks. Enable access controls and cover loop holes in network systems.

7.5 Verify

Verify that 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 is the technique refers to the attempt 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

People often consider as Penetration Testing and Vulnerabilities Assessment are two names of same term but in actual these two terminologies have difference upto some extent. Vulnerabilities Assessment mainly covers the scoping of different areas that are vulnerable to network attacks whereas Penetration testing mainly refers to gaining most possible access inside the 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.

Testing a new system before its online launching is a good practice. 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

Table 1: Comparison of Vulnerability Assessment and Penetration Testing [5]

10. WHY PENETRATION TESTING?

Penetration testing is an essential practice to ensure that organization’s network is secure and upto 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.

10.1 Business Perspective of Penetration Testing

Penetration testing safeguards IT systems 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 helps in identification and nominates the risks before a security breach can occur which to prevent financial losses due to security is valuable in breaches to overcome a huge cost for recovery. 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.

Single incident of security breach may lead organization to loss of customers’ confidence, challenges in marketing strategies, dishonor of other stockholders and even failure of entire business. The study of CSI has estimated that the recovery may costs approximates upto $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.

10.2 Operation Perspective of Penetration Testing

Penetration testing helps shape up security procedures through appropriate vulnerabilities identification and assessment procedures. This help out proactive elimination of threats and risks, corrective and preventive measures, quickly real potential vulnerabilities. Penetration testing can help to 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.

- Mysterious understanding with Operating systems.
- Expert 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.
- Deep understanding with scripting, BAT or VB Scripting.
- Low lever programming techniques including assembly languages, system programming and network level programming.
- Deep understanding 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.
- Vast working with IPS and IDS. How to use these devices to prevent 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

Two main types of Pen-Testing are 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. No unauthorized personals have access to these gadgets like Data Centers, Equipment and infrastructure. So a comprehensive policy is needed 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.

Virtual penetration testing refers to testing virtual assets or intangible assets include Operating Systems, Software’s, Web Servers, IOS, Firewalls, Databases and other intangible assets in a business organization. Most of network attacks take place 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. penetration testing and vulnerabilities assessment in virtual assets is more challenging that for physical assets. More than 80% energies are expended in protecting these virtual assets as compared protecting physical assets.

Besides these penetration testing types it is pertinent to closely classify penetration testing in another manner. Penetration testing i.e. Physical PT, Network PT and Social Engineering PT. Network Penetration testing is an ethical way of the identification of security flaws of networks. Test is 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 scans an application’s security controls by highlighting risks posed from potential vulnerabilities in applications. Many organizations use firewalls and other traffic monitoring systems 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 is another very important field that imposes 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 observes that upto what extent an organization’s workers can exploit organization’s secrets that are harmful for existing 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.

13.1 Black Box Testing

In Black Box Testing, the testers do not have any knowledge about target. They have to dig out vulnerabilities and loopholes on the basis of their own scuff. 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.

13.2 White Box Testing

In white box penetration testing approach, testers are equipped with all necessary information about the target. Generally test team and organization's team 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.

13.3 Gray Box Testing

Gray box testing falls between black and white box testing in which partial disclosure of information about test targets are provided to test teams. 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.

13.4 External penetration testing

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

13.5 Internal penetration testing

Is performed from inside the organization's network that own test target. This strategy is useful to check out upto 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 can be performed 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 a critical 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.

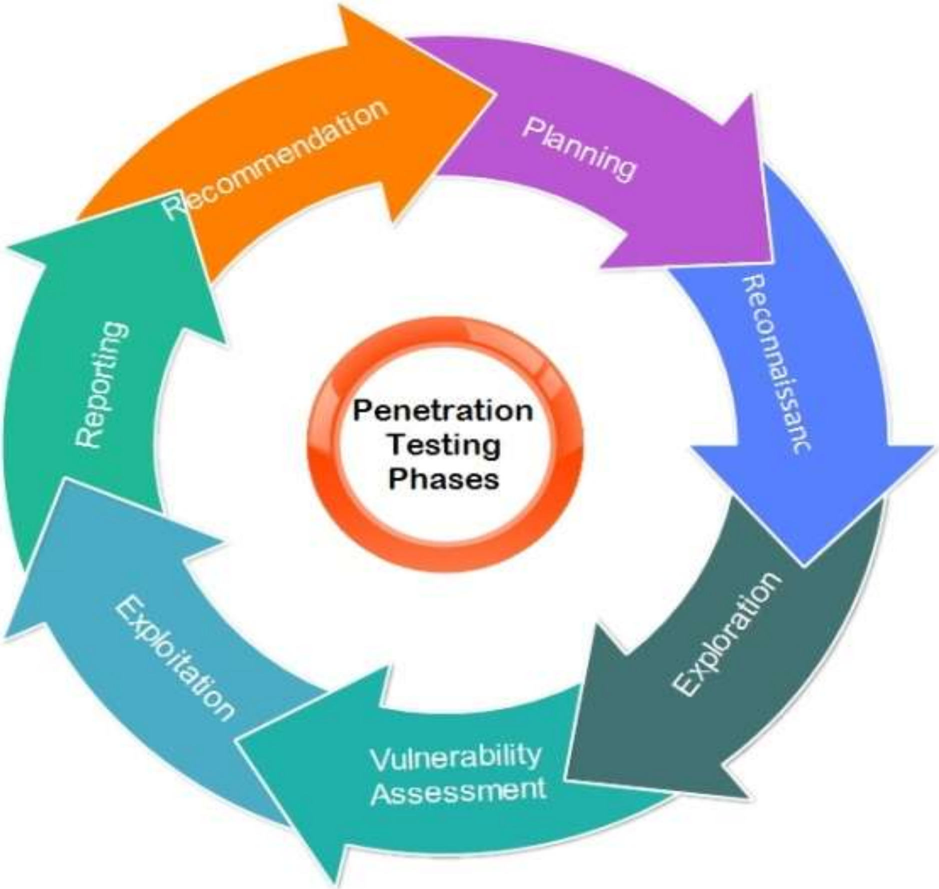

Figure 3: Phases of Penetration Testing [6]

15.1 Planning

Planning phase encircles to scope of the test. What are the business objectives that will be achieved after testing, What to test, how to test, what conditions will be applied, the time frame for test execution and usually cost of the test are considered in planning phase of penetration test.

15.2 Reconnaissance

Once the scope of the test has been defined, the next step is reconnaissance phase. Information gathering about target network deals with this phase. Information as much as possible are gathered in this phase. This is a comprehensive phase that may include indentifying 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.

15.3 Exploration

This phase deals with exploring the entire network based on necessary information gathered in reconnaissance phase. More specific 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.

15.4 Vulnerability Assessment

Finding the existing vulnerabilities by using both manual and automated techniques, vulnerability management, vulnerabilities discovery, threat classification and values of active and passive threats to a vulnerable system are discovered in this phase [7]. Penetration testers may use automated tools for known vulnerabilities. These tools are helpful by having updated databases for latest vulnerabilities and their details.

15.5 Exploitation

This is more challenging 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.

15.6 Reporting and Recommendation

This almost last phase in which testing team document all of its observations. This is final document on which all the phases based. The true and final purpose of a penetration test is to point out all vulnerabilities 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 performed with highly qualified professionals 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

Although there are a vast number of tools that are used in penetration testing, however a few most widely using tools are being discussed in brief. Different tools are popular to perform different kind of tasks in different domains. No single tool is capable to do all tasks in penetration testing. A combination among these tools leads to a 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.

17.1 Nmap

Nmap (Network Mapper) is known as the World's best port scanner. It is free tool available in both Back Track and Kali Linux. It enables testers to perform network discovery, port scanning, host discovery, version detection, OS detection etc. Nmap is usually deployed in security audit of a device or a firewall, identification of open ports in target system, network mapping, network inventory, asset management and maintenance, gathering traffic in the network, finding and exploiting vulnerabilities in the network. 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 is capable to run on all major 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.

17.2 Nessus

Nessus is top rated network vulnerability scanner. It was initially 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 scanner as its developers conducted a survey in 2006 of used by almost 75000 organizations. It is web tool that can scan vulnerabilities like, vulnerabilities that allow remote hacker to access sensitive data, miss configured system like missing patches, default passwords, common password configured, missed passwords etc. Nessus also powerful in determining DoS attacks and conducting of PC-DSS audits etc.

17.3 Metasploit Framework

Metasploit Framework is a power exploitation tool which enables penetration tester to develop and execute exploit code against target network. It can also be employed to test vulnerabilities in network system. It is open source and available free of cost for 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.

17.4 Wireshark

Wireshark is another excellent and unique tool based on its specific use and nature. This is another multi platform, open source network platform analyzer which scans live data travelling in network. Wireshark has a number of dominant features including viewing of TCP streams in the network. Wireshark supports a vast variety of protocols and media types.

17.5 Aircrack

Aircrack is a tool for wireless cracking. 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.

17.6 Cain & Abel

It is well know UNIX based free network sniffing tool. This is known windows only password recovery tool. It recovers password by 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.

I thing 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 is the process of exploring vulnerabilities in a network in order to find out all possibilities and loopholes from where attackers get 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. 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 [8].

18.1 Written Permission

Pen-Testers must have sign legal written document duly signed by both parties prior of conducting s penetration test. Testers should have to document all of the processes of penetration test. This will protect testers from any legal issue in future.

18.2 Damage Control

In some live environments the pen-test may set a potential harm to 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.

18.3 Scope of Work

Pen-Testers must have to define scope of work defining external and/or internal vulnerabilities assessment. Scope also includes which networks, what systems, what devices will be performed test on.

18.4 Professional Approach

The pen-testers must have to define that they will follow well know professional standard to perform the test even any vulnerability could not be found. [9] 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.

18.5 Premises and Jurisdiction

Jurisdiction of the test should be defined which clearly depicts the venue where test is going to be performed. Different countries may have different Cyber Laws so performing test in America may be a legal issue that in Germany.

18.6 Privacy Issue

A successful pen-test can be performed by getting into one's computer or network system. So sensitive data or databases may be accessed during test process. So clause of data privacy must be included in the agreement.

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

Penetration testing and vulnerabilities assessment is a very growing field in IT security. We perform penetration testing for proactively protect from any possible treats towards our network. 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] P. Engebretson, The Basics of Hacking and Penetration Testing, 225 Wyman Street, Waltham, MA 02451, USA: Elsevier Inc, 2011.

[2] W. Link, "http://en.wikipedia.org/wiki/Vulnerability_assessment".

[3] W. Link, "https://www.offensive-security.com/".

[4] J. Benetti, Step By Step Kali Linux and Wireless Hacking Basics, 2015 Edition, 2015.

[5] N. F. A. A. M. S. Zainudin, "A Survey on Conducting Vulnerability Assessment in Web-Based Application," in *International Conference on Advanced Machine Learning Technologies and Applications*, Switzerland, 2014.

[6] W. Link, "http://www.rhinosecuritylabs.com".

[7] K. K. K. Ankita Gupta, "Vulnerability Assessment and Penetration Testing," *International Journal of Engineering Trends and Technology,* vol. 4, no. 3, pp. 328-333, 2013.

[8] H. T. Tavani, "Ethics And Technology: Ethical Issues In An Age Of Information And Communication Technology," *ACM SIGCAS Computers and Society,* vol. 33, no. 3, September 2003.

[9] C. N. Sushilkumar Yadav, "Survey: Secured Techniques for Vulnerability Assessment and Penetration Testing," *International Journal of Computer Science and Information Technologies,* vol. 5, no. 4, pp. 5132-5135 , 2014.

[10] T. G. Proffitt, [2] Creating a Comprehensive Vulnerability Assessment Program for a Large Company Using Qualys Guard, SANS Institute Info Sec Reading Room , 2008.

[11] G. Weidman, Penetration Testing: A Hands-On Introduction to Hacking, USA: William Pollock, 2014.

[12] P. Kim, The Hacker Playbook: Practical Guide To Penetration Testing, North Charleston, South Carolina: Secure Planet LLC, 2014.

[13] I. John Wiley & Sons, Certified Ethical Hacking Version 8, Indianapolis, Indiana: Sybax Publishers, 2014.

[14] S. Harris, CISSP All-in-One Exam Guide, Seventh Edition, McGraw-Hill Education, 2016.

[15] White Paper What is a vulnerability assessment?, Miami, Florida, USA: DEMYO INC, 2011.

[16] E. D. a. C. Easttom, CompTIA Security+ Study Guide: SY0-401, 6th Edition, Sybax Publishers, 2014.

[17] W. Link, "http://swtestingmatters.blogspot.com/2012/08/penetration-testing-breaking-in-before.html".

[18] w. Link, "http://nizarbekai.com/services/penetration-testing/".

[19] W. Link, "http://www.vulnerabilityassessment.co.uk".

[20] W. Link, "[18] http://www.accuvant.com/blog/strategy-and-tactics-penetration-testing-in-the-security-program".

[21] w. Link, "http://www.ibm.com/systems/data/flash/be/resources/Attachement_2_-_IBM-ISS-PenTest-WP060608-073108.pdf".

[22] C. J. N. G. Umesh Kumar Singh, "Measurement of Security Dangers in University Network," vol. 155, no. 1, 2016.

[23] C. J. N. G. Umesh Kumar Singh, "Information Security Assessment by Quantifying Risk Level of Network Vulnerabilities," vol. 156, no. 2, 2016.

[24] V. B. S. a. M. C. Nandi, "Robust and accurate feature selection for humanoid push recovery and classification: deep learning approach," 2015.

[25] V. B. S. a. S. K. S. C. Behera, "An optimized feature selection technique based on incremental feature analysis for bio-metric gait data classification," 2016.

Muhammad Zeeshan received the Master degree in Computer Science from Virtual University of Pakistan in 2015. He is currently working toward the MSCS degree in Computer Science at VUP. His research interests are Network Security in cloud Computing and Attribute Based Access Control. He is currently an employ of FCSC Peshawar, under Ministry of Defence Islamabad,Pakistan.

Shams Un Nisa is currently an Lecturer in the Department of Computer Science, FG Degree College Karachi, SHe received the MCS and MSCS degree in Computer Science From VUP. Her research interests are cloud and network security.

Tazeen Majeed is with Department of Computer Science & Information Technology as a student of MSCS at VU, Lahore, Pakistan. She is currently working as a Computer Science Teacher in Blessing Home High School, Faisalabad.

Nayab Nasir is with Department of Computer Science & Information Technology as a student of MSCS at VU, Lahore, Pakistan. Her research interests are data mining.

Saadia Anayat is with Department of Computer Science & Information Technology as a student of MSCS at VU, Lahore, Pakistan. Her research interests are data mining, data warehousing and cloud computing data storage.