Penetration Testing In System Administration

Muhammad Zunnurain Hussain, Muhammad Zulkifl Hasan, Muhammad Taimoor Aamer Chughtai

ABSTRACT: In this paper, Authors will be discussing the penetration testing in system administration and challenges faced by the industry in securing the data and information using different techniques. Penetration Testing is modern technique of assessing the vulnerabilities in the system. It has been performed to explore all the loop holes in the system and the tester behave like an attacker. All the potential weaknesses, access to data manually or automatically being checked and verifies by the tester. The purpose of this activity is to gather all the required information to secure the data before real attack effects the system, during the process port scanning and other activities were performed and finally as report will be made to suggest improvement in the system to secure it. It is very challenging these days to secure the communication between two users although people use different encryption techniques [1].

Keywords: OS Operating System, Dos Denial of Service.

1. INTRODUCTION

Security of the Network and the systems are the main concerns these days. This is because of the increase in connected devices with internet. The application security has also affected due to this fact now days as compared to the past. For every company, group or educational institute it is essential now to secure the classified information, records from unauthorised access, they have to implement structured approach in order to secure it from attacker. Some of the designed security methods are proof of correctness, layered design, and software engineering environments and finally penetration testing. Penetration testing is an emerging method to test the vulnerabilities in the system, identification of poor and improper system configuration, hardware & software flaws and operational weaknesses in the process or technical countermeasures. The tests can be performed manually or automatically depending on the requirements.

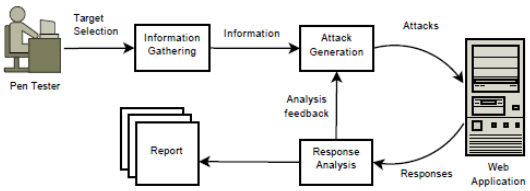

FIGURE 1 : *PHASES OF PENETRATION TESTING*

This paper will provide an overview of penetration testing, why we conduct this? What are the steps involved in performing pen testing, steps in accomplishing network penetration testing? Motivation to perform this test, various tools used for penetration testing [2]. The authors will also be considering the facts that affects the consumption of resources (time and finances) as they cannot be replenished.

- *Muhammad Zunnurain Hussain, Muhammad Zulkifl Hasan, Muhammad Taimoor Aamer Chughtai*
- *Sr Lecturer CS& IT Deptt, BULC, Lecturer CS Deptt, NUST, Sr Lecturer CS& IT Deptt, BULC*
- *engrrhusain@gmail.com, engrrhasan@gmail.com, mtaimoor.aamer@gmail.com*

If we consider time as an example of resources, it cannot be reset[3], [4]. The organiser has to take care of the limited resources before accomplishing the goal, several solutions are available to plan and execute with limited resources it is the researcher who has to decide among all[5]. Automated penetration testing is an emerging area these days. Security is a big concern for everybody these days and it cannot be checked by hand on large scale network to identify it. Instead of getting the identifying it by hand, large scale organization are using automated or semi-automated techniques to identify the loop holes in their system and network[6]. Semi-automated systems are using various tools that are built in to provide support to small industries or even large scale network so that they can easily identify the security concerns and possible entry points for the hackers. Configuration of the system need to be updated and revised in order to provide secure network and system administration to the organization. Standard operating procedures need to be predefined and compliance has to be double checked by the concerned authority on regular basis, the attacks occurs due to individual mistake and negligence in order to follow the procedure on regular basis. Training should be provided to the individual who is looking after the system[7]. Expectation level from the system engineer should be raised after providing him sufficient training and information on security of the system as well as network. Semi-automated penetration test was conducted on small scale where there is limitation of hosts computers, it was not a success in reality as it can't be scaled to large one. Hoffman's had figured out the feasibility of the models with respect to penetration testing, he concluded with very low remarks in achieving his set goals [8], [9]. Even the medical records are being stored electronically on any of the cloud facility with added security and confidentiality protocols in order to cure it from hacking and attacks. Information technology is facing diversified issues and challenges these days as the system and network increasing periodically. Periodic test is the requirement of todays every system so that entry points and loop holes should be known to all the system engineers and network experts.

2. WHY WE CONDUCT PENETRATION TEST

We do these tests to prevent our information from breach. To identify all the entry points of an attacker and set the controls on each point, to ensure overall security of the system. Get a proper baseline for the test and finally to compliance with security policies of the information in the

industry. We have to set a scope of the test, either the attacker or the ethical hacker is sitting inside or accessing the information externally. The tester has been hired by the company itself or somebody wants to gain access of the critical data of the company externally. An ethical hacker is white hat hacker who has been hired by the company to specify the entire weakness of the security policies and practice in the system.

3. Steps of Penetration Test

First of all, we have set a goal, after that we will be gathering the information on the system on which we are going to perform test. We will be running the discovery by scanning the port and vulnerability assessment, analysis will be performed on the basis of gathered information. Control on the system will be taken over after the exploitation, brute forcing or social engineering. A report will be complied finally as evidence which includes risk analysis and remedies on all the collected vulnerabilities [10].

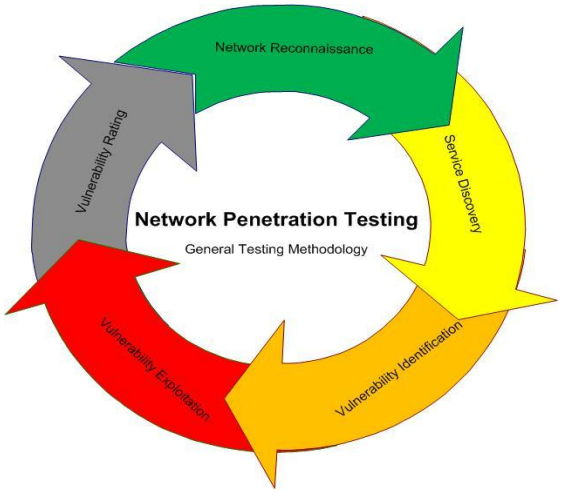

Figure 2 : *Steps of Network Penetration*

a. Network Reconnaissance

It refers to collect as much information as we can about target in prior to perform an attack. This can be further divided into Active and Passive. Former involves information collection with direct dealings like social engineering and the later without any direct dealings by investigating press release or public records.

b. Service Discovery

It refers to identification of all the open as well as close ports and even for the known vulnerabilities on the target machine.

c. Vulnerability Identification

It can be identified and gained at OS level, system level or even network level. From normal access hacker can even proceed with privilege escalation. It often includes password cracking, buffer overflows, DoS attack etc.

d. Vulnerability Exploitation

It is where hacker strives to retain its control over target with backdoors, rootkits or Trojans. Compromised machines can even be used as Bots and Zombies for further attacks.

e. Vulnerability Rating

To avoid being exposed or caught, a good hacker will leave no impressions of his presence. So he attempts to overwrite the system and application logs [11].

4. Motivation to Get a Penetration Test

a. Provide a professional kick-start

Numerous associations misjudge how wide open their security experience is, and miscalculates the capacity and resources their internal IT staff can utilize to address it. A penetration test provides a professional kick start to understanding current security posture specifically because it recognizes gaps in security, and outlines where to apply security technologies and services so that the organization can develop an action plan to reduce the threat of attack or misuse.

b. Creates a Compelling Event:

How can network administrators and security managers give explanation for a needed increase in the security budget or make the security message heard at the executive level? Well-document results from a penetration test that expose the vulnerability of customer data, human resources records or even executive e-mail accounts create compelling events that any executive concerned with company finances, liability or reputation needs to know.

c. Performs Due meticulousness and Independent Audits:

Security posture needs to be examined on a regular basis to account for the development of new Internet threats. An unbiased security analysis and penetration test can focus internal security resources where they are needed most. In addition, an independent security audit provides facts of due meticulousness in a legal Context for protecting online assets, limiting C-level liability and/or minimizing potential loss of shareholder value. These independent audits are rapidly becoming a requirement for obtaining cyber-security insurance.

d. Meets Regulatory Requirements:

Regulatory and legislative requirements are making penetration tests required as a necessity of doing business. Regulations such as HIPAA (Health Insurance Portability and Accountability Act), OCC Bulletin 2014, and Graham Leach Bliley all include security compliance codes

e. Protects Against Inter-Connected Partner Risk

Online commerce initiatives require organizations to grant partners, suppliers, B2B exchanges, customers and other trusted connections into their networks. The entire structure is only as strong as its weakest link. Any poorly secured system, left unchecked, poses dangerous security risks for everyone else. Many organizations are now requiring that their security vendor provide security audits of partners to ensure that all connected entities have a standard baseline for security.

f. Offers validation:

As groups adapt to new business models and technologies, penetration test provides validation between business initiatives and a security framework that allows for

successful implementation at minimal risk. Basically, after an organization establishes its security practices and believes that its infrastructure is secure, a penetration test provides critical validation feedback.[12]

5. TOOLS USED FOR PENETRATION TESTING

Mostly the tools are open source will be discussing each step by step.

a. KaliLinux

Linux based open source debian designed and used for digital forensics and penetration testing. It is preinstalled with frequent penetration testing programs. It can be compiled using hard disk, Live CD or USB. It is a supported platform of the Metasploit projects fame work, it is a tool for developing and executing security exploits. Kali Linux has been created by the back track developers and is the most advanced and updated tool for penetration testing.

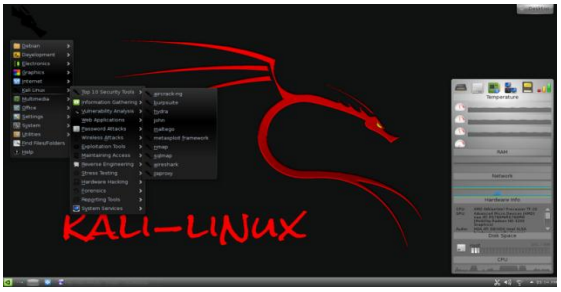

FIGURE 3: *KALI LINUX*

b. Commands used

In Kali Linux ◊Terminal
Basic Nmap command ◊ nmap [IP address of target]
Scanning specific port
◊ nmap [IP address of target] -p [specific port number]
Scanning version of service
◊ nmap -sV [IP address of target]
Scanning Operating System of target
◊ nmap -O [IP address of target]
OS fingerprinting, service enumerating, trace routing and running scripts at one go
◊ nmap -A [IP address of target]
Stealth scan
◊ nmap -sS [IP address of target]
Connect scan
◊ nmap -sT [IP address of target]
UDP scan
◊ nmap -sU [IP address of target]
To use more than one switches simultaneously
Ex. ◊nmap –sS -sV [IP address of target]
Running scripts using nmap
◊ nmap -scripts "[name of the script]" [IP address of target] -p [specific port number]

c. Maltego

It is an open source intelligence & forensics application. We can gather and represent information in easy and understandable way. The relevant information will be gathered and displayed in presentable way using this application.

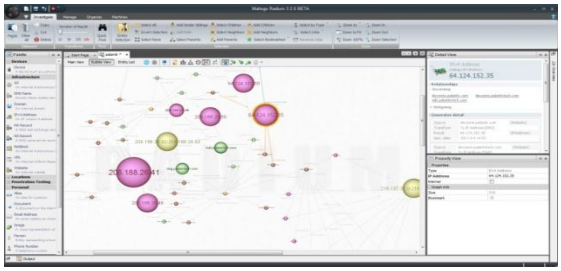

Figure 4 : *Maletgo Open source intelligence & forensics application layout*

d. WHOIS SERVICE

It is a query and response protocol & is widely used for querying database that stores the registered users of an internet resource, like domain name, IP Address block and autonomous system. The protocol stores & delivers database content in a human readable format.

FIGURE 5: *WHOIS*

e. Vega

Open source free testing platform to test the security of web applications. It can help you in finding and validating the SQL injection, cross site scripting (XSS), unintentionally disclosed sensitive information, & other vulnerabilities. Mainly its written in java and is GUI based which runs on Linux, OS X and windows [13].

Figure 6: *VEGA*

6. TCP/IP LAYER THEIR PROTOCOLS AND HACKING TOOLS ON EACH LAYER

TABLE 1: *HACKING TOOLS USED ON EACH LAYER*

TCP/IP Layer	Protocols	Hacking Tools
Application	HTTP,FTTP,SMTP, SNMP,NetBIOS	Nikto,BurpSuit, SQLmap ,Enum,CaimHavji, Netcat, Metasploit
Transport	TCP, UDP	Superscan,Nmap,Nessus,SNMPwalk,Cain,Netcat
Network	IP,ICMP,IGMP	Hping,Firewalk,Aircrack-ng,SamSpade,Wireshark
Host to Network	Ethernet, FDDI	Dsiff, Arpwatch

The above table shows the TCP/IP transmission control protocol / internet protocol layer along with their protocol list on each layer with relevant hacking tools that can be used to sniff the packet on each layer structure.

7. CONCLUSIONS

Penetration testing is a comprehensive methodology, which is used to identify the vulnerabilities in a system. The process offers benefits like deterrence of financial loss; industry rules and regulation compliance, Customers and stake holders, defending the corporate image, elimination of identified risk factors by pen tester. He should also identify the emerging technologies to the top management so that they can send their staff for those trainings. The Tester can use black box, white box or grey box depending on industry requirements and the access available to him. Also, tester can choose either he wishes to test the system sitting inside the network or by accessing the system externally, it all depends on the said goals set by him. Broadly used tests are network, application and social engineering. Sniffers collects all the desired information after trailing the network and looking the feeds of the system engineer on social networking sites. The kind of challenges he is facing in order to tackle the situation during system break down. The paper elaborates the phases, tools that can be used for penetration testing and in achieving the said goals. Mostly used steps are as under: information gathering, vulnerability assessment & analysis and exploitation. Various tools can be used on different services Web, database and forensics, there representation after sniffing the required information from the system or network. The report will be generated which will be put up to the top management so that they can have the complete picture of the weaknesses of the system. Instead of relying on system engineer expertize in order to handle difficult situation the companies should also encourage their staff for improving their skill set and knowledge up to the mark. So that they can handle any situation at any time and cost and will be held responsible for any company loss. The tester should submit a comprehensive report on his findings. He should also submit the remedies on each finding which includes counter measures for the identified vulnerabilities.

REFERENCES

[1]. A. G. Bacudio et al, "An overview of penetration testing," International Journal of Network Security & its Applications, vol. 3, pp. 19, 2011.

[2]. W. G. Halfond, S. R. Choudhary and A. Orso, "Penetration testing with improved input vector identification," in 2009 International Conference on Software Testing Verification and Validation, 2009, pp. 346-355.

[3]. J. Hoffmann et al, "SAT encodings of state-space reachability problems in numeric domains." in Ijcai, 2007, pp. 1918-1923.

[4]. H. Nakhost, J. Hoffmann and M. Müller, "Resource-constrained planning: A monte carlo random walk approach," in 22nd International Conference on Automated Planning and Scheduling (ICAPS), 2012, .

[5]. I. Arce and G. McGraw, "Guest editors' introduction: Why attacking systems is a good idea," IEEE Security & Privacy, vol. 2, pp. 17-19, 2004.

[6]. A. E. Gerevini, A. Saetti and I. Serina, "An approach to efficient planning with numerical fluents and multi-criteria plan quality," Artif. Intell., vol. 172, pp. 899-944, 2008.

[7]. P. Halsum and H. Geffner, "Heuristic planning with time and resource," in IJCAI Workshop on Planning with Resources, Seattle, USA, 2001, .

[8]. M. Steinmetz, "Critical constrained planning and an application to network penetration testing," in The 26th International Conference on Automated Planning and Scheduling, 2016, pp. 141.

[9]. J. Hoffmann and M. Fickert, Explicit Conjunctions W/O Compilation: Computing hFF (Πc) in Polynomial Time (Technical Report), 2015.

[10].P. P. Shimpi and M. S. Nagpure, "Decentralized Virtual VAPT Laboratory Model," Global Journal for Research Analysis, vol. 4, 2016.

[11].L. Vishnoi and V. Shrivastava, "Results of Penetration Testing on Various Operating Systems," .

[12]. (2001). Penetration Tests: The Baseline For Effective Information Protection Available: http://www.iss.net/documents/whitepapers/pentestwp.pdf. DOI: 14-12-2016.

[13].(2014). Penetration Testing. Available: https://www.depts.ttu.edu/cs/research/csecs/workshop/docs/.../Petetration-Testing.ppt. DOI: 14-12-2016.