ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 12, December 2022

An Approach towards Scanning Information Assets Using Penetration Testing As a Security Measure

[1] DR.Umesh Kumar Sing, [2] Shabana

[1] Director, ICS Vikram University Ujjian, Madhya Pradesh, India.
[2] ICS Vikram University Ujjian, Madhya Pradesh, India.
Corresponding Author Email: [1] umeshsingh@rediffmail.com, [2] Shabanasheikh09@gmail.com

***Abstract*— Computer specialists conduct security audits to defend computer networks and system against cyber-attacks and prevent unauthorized access to sensitive information and data breaches. Attacks on the system are being used in the penetration testing or intrusion process to investigate for system weaknesses, flaws and vulnerabilities. Internet and information security is crucial in the modern digital age considering the increase of cyberattacks in the fifth-generation warfare. The term "fifth-generation warfare," or simply "5GW," refers to a systematic of waging war involving non-kinetic military operations, such as social manipulation attacks, online propaganda campaigns, cyberattacks, data theft as well as cutting-edge technologies like artificial intelligence and machine learning or cognitive computing.**

There is a lot of misconception regarding the differences between vulnerability analysis, risk assessments, and penetration testing, however pen testing is the key to maintaining things secure. For penetration testing, we leverage the power of the findings from vulnerability assessments. Nowadays, every firm pays more attention to protecting its resources and data to safeguard themselves from future cyber-attacks.

Keywords: Internet Security, Penetration Testing, Vulnerability Analysis, Risk Assessments, Corporate and Education Assets, Data security.

I. INTRODUCTION

Almost all contemporary enterprises and educational institutions rely on information technology (IT) solutions to enhance operational procedures and organizational security.

In addition to facilitating seamless operation, a well-implemented solution can significantly improve management procedures. Unfortunately, despite the obvious advantages these modern systems provide, if a technology is infiltrated by cybercriminals, businesses may incur devastating consequences and losses. As a necessity, robust defenses against hackers are required.

Penetration testing is a security-focused systematic study conducted from both the inside and the outside world to search for technology flaws that an intruder might exploit. Any configuration of an application, host, or network can be referred to as a system that is being target using cyber-attack. The penetration test provides a intense viewpoint on the organizations and information technology of the organization's existing security postures. To evaluate the viability of an exploitation and the implications of a successful exploit, penetration testing is performed.

The penetration test's basic operation is a crucial factor in its success. To properly assess the condition and generate reports aimed at various points of view inside a company, a technological and effective approach should be applied. To allow the tester to completely explore, their instincts shouldn't be restrictive. A penetration test typically starts with a vulnerability assessment. The exploit of any known flaws, to verify their presence, and the detection of the harm that the exposure would cause and the consequent impact on the organization are additional steps in a penetration test.

II. VULNERABILITY ASSESSMENT VS. PENETRATION TESTING

Vulnerability analyses includes information technology audits and security audits. where a cyber assault could flourish therefore infrastructure underlying information technology is examined. In terms of exploitation, frequently in terms of compliance, effectiveness, and efficiency, whereas penetration testing typically goes further with a priority on detecting vulnerabilities and obtaining as much access to the system as possible and then exploiting them. The major step in safeguarding the infrastructure is penetration testing, which is a crucial tool for identifying system weaknesses. When a computer is assessed for vulnerabilities, an attack on the system is prevented before it can be compromised, whereas a penetration test is used to determine how serious and deep an assault can go before it can penetrate a computer system.

Computer risks are looked for during vulnerability assessments, and false positives are removed from the result by mapping them to real entry-level vulnerabilities in a penetration testing. The penetration test's goal is to determine whether or not the security measures currently in place are adequate.

Vulnerability assessment is similar to judging whether a door is open or closed by simply looking at it. While a penetration test is actively trying to unlock the gate, see how far it is heading, and uncovers the possibility after accessing the gate, this may allow someone to get unauthorized entry. A penetration test is a better indicator of a system, software or network's vulnerability. Although vulnerability assessment is somewhat less aggressive and should not potentially impair systems or network functions, penetration testing is much more aggressive by nature. As a result, the penetration test causes more disruption to network or system services.

III. PROBLEM STATEMENT

Finding controllable security flaws is the fundamental objective of vulnerability assessments. and to find events in order to prevent them from being exploited by unauthorized users. Penetration testing is a technique used by information technology specialists to address issues with vulnerabilities assessment, with an emphasis on high severity vulnerabilities. An useful assurance evaluation tool that aids the company and its functioning is the penetration testing technique**.**

Penetration testing assists companies in protecting themselves from breakdown in terms of business perspective by preventing monetary damage, demonstrating diligence and compliance for industry regulators, clients, and stockholders, maintaining corporate reputation, and rationalizing information security investment.

Businesses spend thousands of dollars to resolve data breaches and losses caused by them. Recovery costs alone are estimated by a CSI study to cost $ 167,713 per event. In order to prevent economic loss due to security threats, penetration tests can discover and uncover risk before security flaws happen.

The industry has established regulatory standards for computing systems, and noncompliance with those standards may result in severe fines, incarceration, or even the organization's demise. As a proactive service, penetration testing fills in the gaps that enterprises need for auditing or compliance tasks.

A single instance of client data being compromised can be terrible. Loss of customer trust and brand recognition can put the entire company at risk. Penetration tests were required to enhance cybersecurity throughout the enterprise.

This aids the company in avoiding security issues that could damage consumer loyalty, expose its corporate image, and jeopardize its brand.

Penetration testing assesses the effectiveness of current security solutions and offers a solid foundation for upcoming security technology investments or upgrades. It gives senior management an "Issue of evidence" and a strong argument in support of the investment proposal.

Penetration testing, from a tactical perspective helps in moulding the information security policy by quickly and precisely identifying weak points, actively removing and identifying risk, putting remedial measures in place, and expanding IT awareness.

If an organization's security principles and procedures include penetration testing, it can offer thorough details about actual permeable security dangers. It will enable organizations to recognize both current and future problems with speed and precision.

Penetration testing can assist organizations in fine-tuning and validating adjustments or fixes to continually minimize identified risks by effectively and efficiently segregating and prioritizing essential information vulnerabilities. The consequences and possibility of organizational vulnerabilities can be identified with the aid of penetration testing. This will enable the company to set priorities for identified vulnerabilities and put those fixes into place. Penetration testing consumes a lot of patience, research, and expertise. with test site problems. In light of this, conducting a penetration test will help everyone engaged learn more and be more skilled.

IV. THE PENETRATION TESTING METHODOLOGY

A penetration test's objectives include assessing the system under test's level of risk and identifying any potential breakdown techniques. It is necessary in some situations to carry out a reliable test that is valid. In addition to the testing step itself, which is covered in this section. Initiation, planning, execution, and report are the four main stages of a successful penetration test.

Initiation

The project initiation phase comprises a first discussion with the client (founder) of the system being tested in order to develop an understanding with the examiner. Both parties establish the parameters of the test, the area of scope, the individuals in charge of certain duties, the activities that testers are permitted to perform, and the testing schedule at this phase. Besides this, it also includes the forming of a team and the sharing of critical personal details.

Preparation:

The contract created during the early phase is taken into consideration before the real penetration test begins. When a penetration test involves more than one penetration tester, the work is organized and distributed among the team members. Tools are chosen and set up in accordance with the tasks which need to be completed. Penetration testers must consider the durability and integrity of the system being tested at this step.

Testing:

This step resembles the breaking process and incorporates actual hacking. hacking. To be able to review the unexpected events happen, every action made during the system testing should be recorded. Communication with the client is also crucial in circumstances where the entry tester needs the system owner's consent before acting. The test procedure entails a number of distinct steps, which are described in the sections below. When fresh data is gathered, some of these stages are repeated. This enables the examiner to track or fill in prior gaps in new sections of the system being tested.

Target identification:

Acquiring data about the target system, such as available domains and sub-domains, IP addresses, Email accounts, interests of the target, internal resources, security protocols, technologies being used, etc. is known as target identification. The quantity of information accessible to the penetration testing team at the onset determines how important the goal assessment step will be. Particularly in the context of external penetration testing, which occurs when the tester does not have preliminary access to the internal resources, the victim must be identified. There are numerous ways to find useful information, including website checks, information gathering through search engines, and social engineering activities.

Port scanning:

An open port is searched by the Transmission Control Protocol (TCP) or Universal Datagram Protocol (UDP) port at this step of the penetration process. In addition to this, services and software running on those open ports along with their versions are explored in Port scanning process. This methodology is also known as Network scanning. Outdated services running on ports are used to target and exploit in this scenario.

The practice of finding weaknesses in a network beforehand they may be exploited by someone else with malicious intent to harm the network is known as vulnerability analysis. With this proactive approach, vulnerability is identified and addressed before anyone is aware of it.

Exploiting vulnerabilities entails using specialized methods and skills to execute an attack against the target system. Penetration testers with experience can exploit the system using their skill.

In most cases, computers run many services that communicate with one another via TCP or UDP ports and are linked to a network. There are 65535 defined ports on the computer. Three broad categories can be used to group them:

(i) Popular ports (0–1023)
(ii) Licensed ports (1024–49151)
(iii) Dynamic and/or private ports (49152–65535)

A port scan does not directly impair the host, but it may aid the attacker in discovering the ports that are open for attack launch. A port scan basically entails transmitting a message to every port, answering it, and listening to it one at a time. Such a response can indicate whether the port is in operation, enabling further research into the port's susceptibility to prospective assault launchers in the future. Six categories are typically used to standardize the scan findings on the port:

Open Ports- An application that is open on this port is one that is actively accepting TCP connections and UDP datagram associations. Often, the main objective of port scanning is to find these. Security-conscious individuals are aware that any open port is a potential attack vector. While network administrators attempt to block or secure open ports without harming legitimate users, attackers and pen-testers are interested in exploiting them.

Closed - A closed port is reachable (it receives NMAP probe packets and responds to them), but it serves no purpose. They can be used for OS detection and for proving that a server is up or not (host discovery, or ping scanning). It would be worthwhile to search in case something opens later, because closed ports can be recovered. Supervisors can research using a firewall to block certain ports. They then show in a filtered state, which will be covered later.

Filtered- Due to packet filtering, the Nmap is unable to verify whether the port is open because its probe cannot access the port. Filtering might come via host-based firewall software, router rules, or a dedicated firewall device. Because they offer so little information, these ports annoy attackers. The ICMP error signals,which can sometimes be returned by filters, are less prevalent than filters that simply ignore the probe. In the event that the probe is dropped due to network congestion, this compels the Nmap to retry numerous times. The scan is severely slowed down as a result.

Unfiltered - When a port is in the unfiltered state, it is reachable but the Nmap cannot tell whether it has been open or closed. Ports in this state are only classified by ACK scans, which are used to map firewall rule sets. Other scan kinds, such as window, SYN, or fin scans, can help open the port by scanning infiltrating ports.

Open filtered- When Nmap is unable to detect whether a port is open or filtered, it holds it in the state of "Open Filtered." This happens with scan types where open ports are unresponsive. A probe might have been dropped by a packet filter or removed if there was no response, depending on the circumstances. Nmap therefore cannot determine whether the port is active or not.

Closed filtered- When the Nmap is unable to detect whether the port is closed or filtered, this condition is applied. It is only employed for passively IP scanning.

Enumeration:

After the access checker has compiled a list of the hosts and services that make up the system being tested, it is time to pinpoint those that have the greatest chance of compromising. Along with the outcomes of port scans, enumeration involves gathering data on the system's services. Examples of this data include the current service version, any known vulnerabilities, the password lockout policy, etc. for a particular service. Pen tester is able to locate the weak spots with the help of this expertise. At this point, tester expertise is quite helpful, but the tool can also be utilized to aid the tester in their scanning.

Penetration: The act of exploiting a system under test's known vulnerabilities is known as penetration. A system weakness that was never anticipated by the system's developers is exploited by the penetration tester (or an attacker). Exploitation aims to get access to a resource, such as one remote shell that can be used to command a system on a network. Buffer overflows, SQL injection, setup mistakes, and other attacks.

Because exploits may cause either temporary or lasting damage. The penetration tester must evaluate the system being tested to decide whether using a fixed exploit is appropriate. The examination is typically assisted in making these conclusions by maintaining proper interaction with clients.

Privilege Escalation: When a vulnerability is compromised, availability to the resource is frequently restricted. For instance, the penetration tester could be able to access a user account with minimal credentials, yet some performance tasks demand high privileges. Escalation phase entails increased resource exploitation and an increase in the tester's influence over the target machine or network.

Maintaining access: A host being hacked does not automatically mean that it is simple to govern. To control the compounding machine in the same manner as the administrator, the penetration tester needs an interaction system. Sometimes exploits give the tester a direct interactive interface (like a shell to control remote resources), but other times it requires an extra step to get this interactive and long-term access.

Clean up and clear logs: Nothing deployed during the test should be left on the network by a qualified penetration tester. Every modified configuration must be reset to its initial state as well. The cleanup phase's goal is to stop the system being tested from developing any new flaws. According to a hacker, this phase's purpose is different. In order to prevent being discovered and recognized, a hacker must have all traces of his presence removed from the target system. A hacker might be more interested in leaving a backdoor, or a way to acquire the same amount of access without having to attack a different system again.

Reporting: The reporting of test results is the last step in the entrance exam process. The paper includes information about the flaws discovered during testing, including how they could be exploited and what to do to find them. Just receiving a list of issues is not particularly valuable in the eyes of the customer. Therefore, it is frequently preferred to hold a workshop so that the report's contents may be addressed, and the penetration tester can precisely explain what occurred to the client. Another advantage of a follow-up session is that the extent of vulnerability discovered can be reviewed and specified during the penetration test. Along with the customer, severity denotes a level of danger and susceptibility that is dependent.

Penetration testing Tools used in

S.No.	Name of Tool	Specific Purpose	Cost	Portability
1	Nmap	Find and mapping web server along with discovering open ports and running services and their versions	**Free**	Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga
2	Amass Scanner	Mapping hosts on a network	**Free**	Linux, MacOS, Microsoft Windows
3	Nikto	Identifies the kind, version, add-on, as well as other vital files of the web application or server and quickly analyses it, and reports and applications common software and server configuration errors, outdated servers and programs, insecure files, default files.	Open source	Windows, Mac OSX, Linux and Unix (including RedHat, Solaris, Debian, Knoppix, etc)
4	Dirb, Dirbuster	Detects new URLs on the test target, and fuzzes to find web pages	**Free**	Linux
5	Wireshark	Network monitoring	Open source	Linux
6	Wayback Machine	Grab older versions of website and webpages	**Free**	Any Web-Browser
7	OpenVAS	Vulnerability Scanner	Commercial	Linux, Windows
8	Acunetix Scanner	Web vulnerability scanner	Commercial	Linux, Microsoft Windows

9	Firefox Extension-Wappalyzer and Netcraft	Web technologies and server information	**Free**	Any platforms that supports Firefox
10	Nessus	Detect vulnerabilities that allow remote cracker to control or access sensitive data, misconfiguration, default password, and denial of service	Commercial	Mac OS X, Linux, FreeBSD, Oracle Solaris, Windows, Apple
11	Metasploit Framework	Develop and execute exploit code against a remote target machine, test vulnerability of computer systems	**Free**	All versions of Unix and Windows
12	Burpsuite Professional	Intercepts requests and responses, manipulating and crawling.	Commercial	Linux, Windows

Tools Description- The methodology for this study and penetration testing has used a wide variety of tools and software. These tools were a tremendous assistance during tests, assisting with everything from information collecting to exploitation.

- **Tools used in Information Gathering and Footprinting**

Wappalyzer and Netcraft (Firefox extensions): Determining the web technologies involved in the development of the website has been made convenient thanks to Wappalyzer - an extension of Firefox browser. It gathered everything a researcher wanted to footprint a web application, including libraries and third-party modules.

Additionally, the Netcraft extension was useful for locating the target web application's DNS records and web server location. Furthermore, the Netcraft helped in obtaining the whois data, which holds very sensitive information.

Wayback machine: Wayback Machine is a repository of websites that were indexed by crawlers and offers snapshots of past editions of those websites. One can clearly uncover the website's older architectture and sensitive information that isn't currently visible.

- **Tools used in Network Scanning and Enumeration:**

Nmap: The network mapper, often known as Nmap, was useful in scanning hosts to determine whether they were up and whether ports are open. In addition, it was effective at detecting the services running on open ports and obtaining their versions.

Amass Scanner- It is a program similar to Nmap, provided some more information when the host application was network probed.

Dirb and Dirbuster: These tools made it possible to discover the target host's directories. Deep within the website, it exposes hidden links and directories that are not typically visible to users. These utilities use the fuzzing technique to extract the directories. The Dirbuster is a graphical user interface (GUI) version of the Dirb, a command line tool.

Wireshark: Wireshark was beneficial to track the data packets that were being sent between the client and the server, It was helpful to identify the unsecured connection used to transfer the plain-text data.

Tools used in Vulnerability Scanning:

Nikto, Acunetix, Nessus and OpenVAS vulnerability scanner: All these tools are all in the same class and help identify vulnerabilities and their intensity. Using these tools, a number of bugs in the web application were detected.

Tools used in Exploitation:

Metasploit framework : The Metasploit framework contains of the payloads, auxiliaries, and exploits needed to take exploit a host application. This was a crucial tool during the exploitation stage

Burpsuite Professional : Burpsuite Professional assisted in manipulating the request and intercepting it so that vulnerabilities could be verified.

V. CONCLUSION

A thorough way to find system weaknesses is penetration testing. Pen testing offers advantages like the protection of financial loss, adherence to industry regulators, clients, and shareholders, maintenance of business image, and active risk reduction. One of the most effective methods for evaluating security is penetration testing. In this paper, we examine how penetration testing can secure a network. This can be used to test the security measures put in place for the system under inspection. Professionals struggle to find the best means of care because of the large range of helpful gadgets that are on the market.

The goal of the study is to use penetration testing to give the society a more trustworthy benchmark for security. According to this study, benefits include reducing financial loss, monitoring industry regulators, users, and shareholders, protecting corporate image, and actively removing identified hazards. The complete penetration test process was given in this publication helps to counter fifth-generation warfare attacks.

REFERENCES

[1] Georgia Weidman, Penetration Testing - A Hands-On Introduction To hacking, No Starch Press, 2014, isbn: 978-1-59327-564-8.

[2] Rahmat Budiarto, Ramadass Sureswaran, Sureswaran Ramadass, Azman Samsudin, Salah Noor, Development of Penetration Ttesting Model for Increasing Network Security, Information and Communication Technologies: From Theory to Applications, 2004, isbn:0-7803-8482-2.

[3] Mohanty, D. “Demystifying Penetration Testing HackingSpirits,” http://www.infosecwriters.com/text_resources/pdf/pen_test2.pdf, accessed on Nov. 23, 2011.

[4] “Penetraion Testing Guide”, http://www.penetration-testing.com/

[5] iVolution Security Technologies, “Benefits of Penetration Testing,” http://www.ivolutionsecurity.com/pen_testing/benefits.php, accessed on Nov. 23, 2011.

[6] Shewmaker, J. (2008). “Introduction to Penetration Testing,” http://www.dts.ca.gov/pdf/news_events/SANS_Institute-Introduction_to_Network_Penetration_Testing.pdf, accessed on Nov. 23, 2011.

[7] “Application Penetration Testing,” https://www.trustwave.com/apppentest.php, accessed on Nov. 23, 2011.

[8] Mullins, M. (2005) “Choose the Best Penetration Testing Method for your Company,” http://www.techrepublic.com/article/choose-the-best-penetration-testing-method-for-yourcompany/5755555, accessed on Nov. 23, 2011.

[9] Saindane, M. “Penetration Testing – A Systematic Approach,” http://www.infosecwriters.com/text_resources/pdf/PenTest_MSaindane.pdf, accessed on Nov. 23,

[10] “Nmap – Free Security Scanner for Network Explorer, http://nmap.org/, accessed on Nov. 23, 2011.

[11] Filip Holik, Josef Horalek, Ondrej Marik, Sona Neradova, Stanislav Zitta, Effective penetration testing with Metasploit framework and methodologies ,15th ieee International Symposium on Computational Intelligence and Informatics,2014.

[12] Sheetal Bairwa, Bhawna Mewara and Jyoti Gajrani, Vulnerability Scanners: A Proactive Approach To Assess Web Application Security , International Journal on Computational Sciences & Applications, vol.4, no.1, 2014.

[13] Cynthia Bailey Lee, Chris Roedel and Elena Silenok, Detection and Characterization of Port Scan Attacks, univeristy of california, department of computer science and engineering (2003).

[14] P0f, http://www.net-security.org/software.php?id=164, accessed on Nov. 23, 2011.

[15] Httprint, http://net-square.com/httprint/, accessed on Nov. 23, 2011.

[16] Nessus, http://www.tenable.com/products/nessus, accessed on Nov. 23, 2011.

[17] Shadow Security Scanner, http://www.safety-lab.com/en/download.htm, accessed on Nov. 23, 2011.

[18] Iss Scanner, http://shareme.com/showtop/freeware/iss-scanner.html, accessed on Nov. 23, 2011.

[19] GFI LAN guard, http://www.gfi.com/network-security-vulnerability-scanner, accessed on Nov. 23, 2011.

[20] Brutus, http://download.cnet.com/Brutus/3000-2344_4-10455770.html, accessed on Nov. 23, 2011.

[21] MetaSploit, http://www.metasploit.com/, accessed on Nov. 23, 2011.

[22] Skoudis, E. “Powerful Payloads: The Evolution of Exploit Frameworks,” (2005). http://searchsecurity.techtarget.com/news/1135581/Powerful-payloads-The-evolution-of-exploitframeworks, accessed on Nov. 23, 2011.

[23] Andreu, A. (2006). Professional Pen Testing for Web Applications. Wrox publisher, 1st edition.

[24] OWASP. “Web Application Penetration Testing,” http://www.owasp.org/index.php/Web_Application_Penetration_Testing, accessed on Nov. 23, 2011.

[25] Fiddler, http://www.fiddler2.com/fiddler2, accessed on Nov. 23, 2011.

[26] Stuttard, D. and Pinto, M. (2008) The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws,, Wiley. 1st edition.

[27] “White Paper on Penetration Testing,” http://www.docstoc.com/docs/70280500/White-Paper-on-Penetration-Testing, accessed on Nov. 23, 2011.

[28] Neumann, P. (1977) “Computer System Security Evaluation,” Proceedings of AFIPS 1977 Natl. Computer Conf., Vol. 46, pp. 1087-1095.

[29] Pfleeger, C. P., Pfleeger, S. L., and Theofanos, M. F. (1989) “A Methodology for Penetration Testing,” Computers &Security, 8(1989) pp. 613-620.

[30] Bishop, M. (2007) “About Penetration Testing,” IEEE Security & Privacy, November/December 2007, pp. 84-87.