A Comparison and Categorization of Penetration Testing Tools

Dr. K B Priya Iyer[1], B.Loganayaki[2], P.Priyadharshini[2]
[1]Associate Professor, Department of Computer Science, [2]Student-M.Sc. IT
M.O.P. Vaishnav College for Women(Autonomous), Chennai, India
[1]Priya_balu_2002@yahoo.co.in, [2]bloganayaki30@gmail.com , [3]priyabooma96@gmail.com

Abstract: *Security is all about making a system behave properly during the presence of a malicious attack even though system failures happen in the real world. Penetration testing is an attack of a system for validating security by checking the vulnerabilities existing in the system. It is also known as pen test. The pen test provides an organized way to identify security shortcomings. This paper presents an overview of penetration testing, its phases, tools and techniques. The paper also gives the comparison of various tools used for penetration testing with respect to their features.*

Keywords: *Security, Penetration testing, vulnerability, Reconnaissance, cyber-attack.*

1. INTRODUCTION:

As the technology increases rapidly, there comes the challenge of providing a secure environment. So pen test is a tool that spots vulnerabilities and exploits them. This improves the security of the system. A pen tester is an ethical hacker who assesses information security of an organization. The difference of pen tester from hacker is permission. A pen tester will have permission from the head of an organization that is being tested. A pen test is a security audit finding the risk involved. The pen test report identifies the security flaws in the system and provides potential impacts of the organization.

Phases of Penetration Testing

Phase 1 – Reconnaissance

A survey of information or knowledge about the target system or network. The tester in this phase acquires more knowledge about the target business, the objective system and its operation. It includes distinguishing the target, discovering the target system's IP address range, domain name, network, mail server and DNS information. [1]

Phase 2 – Scanning

Scanning the target system looking for weaknesses. Requires the utilization of special tools to gather information on target, about the systems that are setup. It incorporates scanning the target for network services, open ports, identifying firewall, detecting vulnerabilities, operating system identification, etc.

Phase3 – Gaining Access

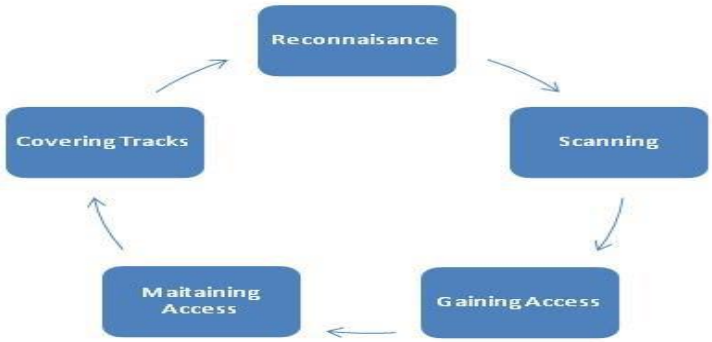
This phase takes control of one or more target system in order to either extract information of value. It also utilizes the network as a dispatch site for attacks against a target. It includes exploiting of vulnerabilities, social engineering, etc.

Phase 4 – Maintaining Access

After gaining access of the target network, the tester must develop steps involved in maintaining access so as to gather as much data as possible. In this phase the tester should remain stealthy in order to not get caught while using the host environment. It includes back door installation on the target network in maintaining the access gain and connect to target anytime.

Phase 5 – Covering Tracks

In this phase tester involves in hiding the intrusion and possible controls abandoned for future references. The tester removes all kinds of logs, identified back doors and anything relating the attack.



Importance and need for using Penetration Testing

- Describing the possibility of a actual set of attack paths
- Recognizing higher-risk vulnerabilities that effect from a combination of lower-risk vulnerabilities broken in a particular categorization
- Classifying vulnerabilities that may be hard or difficult to identify with automated network or application vulnerability scanning software
- Evaluating the scale of possible business and operational effects of popular attacks
- Testing the capability of network protectors to effectively identify and respond to the attacks
- Providing proof to support increased investments in security workforces and knowledge to C-level management, investors, and customers
- Gathering compliance needs both annual and ongoing penetration testing (after any system changes)
- Post security incident, an organization needs to regulate the vectors that were used to increase access to a cooperated system (or entire network). Joint with scientific analysis, a penetration test is often used to reproduce the attack chain, or else to authorize that new security controls put in place will spoil a similar attack in the future.

Pen test is used to detect and measure possible vulnerabilities and to guarantee the security of data. It is based on testing process that is used to recognize risks. It effectively point out the areas from where unauthorized or illegal access can be obtained that could destroy the trustworthiness and reputation of a business environment.
The risk assessment is the main objective of the penetration testing which is used to determine the security system flaws of a computer network in several ways.

2. REVIEW OF LITERATURE

- Used Vulnerability Assessment and Penetration Testing (VAPT) for cyber defense. This research analyzed the performance of VAPT for cyber defense technology to give the proactive cyber defense as to find the vulnerabilities in advance before the attacker could attack the system. The study discussed the prevalent Vulnerability assessment techniques and some VAPT tools. VAPT is a step by step process, and its life cycle includes 9 steps in the process. The results of the study shown that VAPT is an effective technique for Cyber defense technology. The administer can save his resources and sensitive information using VAPT technique and achieve proactive cyber defense.
- presented an introduction of Penetration testing to address the vulnerability of computer systems. This paper included a literature survey of Penetration testing performed by security experts to find the vulnerabilities of the system. The study describes two main types of penetration testing white box and black box testing. The study also analyzed different tools of penetration testing specifically vulnerability scanners included amore explained review of tools such as Nessus.
- Investigated different Penetration testing tools using Kali Linux. This research helped to understand how to perform different penetration tests with virtualized tools, systems, and private networks. The test was performed to detect attacks such as Man-in-the-Middle attack and traffic sniffing. The technique used Ettercap and Driftnet for security auditing and computer network analysis. The implementation also used the Wireshark for traffic sniffing. The results showed that proposed technique for penetration testing could be used successfully in real time environment.
- Proposed a context to calculate vulnerabilities of SCADA systems at three levels: structure, circumstances, and access points. The proposed technique was based on cyber systems combined with the password models and firewall, the primary mode of defense in the electricity industry today. The effect of a possible electronic intrusion was assessed by its potential loss of load in the Grid. This method was supported by a combination of a logic-based simulation technique and a unit for the power flow calculation.
- Proposed an approach that analyses the output, including error messages, of both legal and malicious test cases to learn more about the type and structure of the back-end database. This information is then used to craft attack in-
- puts that are more likely to be successful at revealing vulnerabilities.
- Presented a survey of vulnerabilities and mitigations related to cyber security. The paper focused on the vulnerabilities in multiple industrial radio technologies such as IEEE 802.15.4, IEEE 802.11, WirelessHART, Bluetooth, and ZigBee. The paper discussed how vulnerabilities on industrial radio technologies could be used as vectors for attacks on control systems in complex infrastructures

3. PENETRATION TESTING TOOLS:

This section provides a general idea of various testing tools and their usage, how they exploit vulnerability. The most popular penetration testing tool.

Kali Linux

Kali Linux is a Debian-based Linux distribution aimed at advanced penetration testing, security auditing and a member of UNIX OS family. Maintained and funded by offensive security Limited.kali Linux is primarily designed for pen Testing and Digital Forensics which means the branch of forensic science encompassing the recovery and investigation of material found in digital services. Kali Linux has more than 300 tools which automatically works within its environment. It offers vast plug and play wireless support. The chief attraction was the ARM support provided by Kali Linux. It is an Open source and has Monolithic type kernel. Available in 32-bit and 64-bit images for use on hosts based on the x-36 instruction set.

Features:

- It has more than 300 pen testing tools.
- Multilingual support.
- Completely customizable.
- Huge wireless device support and compatible with USB.
- Advanced RISC Machine support -Kali Linux has ARM repositories integrated with mainline distribution.

Flexibility: Kali Linux can run natively when fixed on computers hard disk or can be booted from a live CD or a live USB or it can run on a virtual machine.KALI LINUX can be installed within a chroot environment on an android device.

METASPLOIT

In this software, security and IT team detect security problems, verify vulnerability modifications and manage expert-driven security valuation, providing security risk intelligence. Some amenities are smart exploitation, key auditing, web application scanning and social engineering. Teams can collaborate in Metasploit and present their findings in consolidated reports. Metasploit consist of different editions starts from free edition to professional enterprise edition based on the Metasploit structure, which is an open source software development kit. Metasploit is a hacking outline transcribed in Ruby. It is designed to help make writing and implementing exploits as simple as possible. Open source tools used for Pen testing, IDS Signature Development and Exploit research. Runs on any operating system such as source code for Linux/Unix/MacOSX and portable to windows via CYGWIN.

Nmap

Nmap –Network Mapper. Nmap is an open source tool which can rapidly scan wide range of network devices and delivers valuable information about those devices. It can be used for IT reviewing and determining as well as for security reporting of the network. This tool uses Internet Protocol packets to decide what hosts are available on the network, the services enabled, versions of the host, what type of firewall or packet filters present and other features of the network. The information can be used to recognize and spot-on security holes and by attackers to perform investigation about the types and quantities of targets available and what weakness exist. Nmap is obtainable for a wide-ranging of operating system platforms. The standard download is a compressed file containing the UNIX version(which runs on Linux, Solaris Free/Net/and Mac OS X) and the windows version as well as NmapFE, the Xwindows front end for UNIX, and NmapWIN, the recommended Windows GUI for Nmap. Nmap can perform a wide range of scans. Some are more aggressive and transparent, while some are designed to be cautious and scan unobserved. Some of the scan types are UDP scan, ACK scan, RPC Scan, FIP Bounce, List scan, Window Scan, IP Protocol scanning etc. Nmap capability to be run from both the command line and from a GUI support most people to get the tool up and running very fast. Advanced features require more command line and technical expertise to use the tool effectively.

Advantages: Host Discovery, Port Scanning, Version detection, OS Detection and Scriptable interaction with the target.

Disadvantage: Even though the server is sheltered by a firewall, Nmap could not recognize the host operating system properly.

SQLmap

It is an open source tool to use SQL injection in better and simpler way.SQLmap developed in python.SQLmap automates the process of spotting and exploiting SQL injection faults and taking over of database servers.

It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the databases, to retrieving the essential file system and executing commands on the operating system via out-of-band connections. It supports various type of database like MySQL, Oracle, Microsoft SQL Server, Microsoft Access, Sybase, SAP MaxDB, Informix database management systems etc.SQL injection techniques are

- Boolean-based blind: Based on page changes, data inferred, char by char.
- Time-based blind: Based blind: Based on time, data is inferred, char by char.
- Error-based: Uses the error that is displayed to extract data.
- UNION query: changes the SQL queries to extract data.
- Stacked queries: Semi-colon is used to inject multiple statements into the SQL query.

Features:

- Support to dump database table entirely; i.e.) Search for specific database names, specific tables across all databases or specific columns across all database tables.
- Support to directly connect to the database without passing Vis SQL injection DBM Credentials, IP address ,port, and database name.

WIFIPHISHER

Wifiphisher is a security based tool that supports automated attacks against Wi-Fi networks in order to acquire secret passphrases and other credentials.

Features: All it takes is one person to fall for the attack and the entire network becomes compromises, Encryption type doesn't matter such as WEP/WPA/WPA2, open source (Python, HTML, CSS, JS).

WIRESHARK

Wireshark is an Open Source .It is a network packet analyzer. A network packet analyzer will attempt to detention network packets and tries to show that packet data in detail. It is used to troubleshoot network difficulties, inspect security difficulties, debug protocol execution and also people use it to learn network protocol.

Features: Offered for UNIX and Windows operating system, It captures alive packets data from a network boundary, Packets are shown with very comprehensive protocol information, It opens and save packet data captured, It will Import and export packet information from and to portion of other capture programs, screen packets and examine for packets on various criteria.

Disadvantage:

Wireshark isn't an disturbance recognition structure. It will not report when somebody does eccentric things on target network.

Wireshark will not operate things on network, it will only measure things from it. Wireshark doesn't send packets on the network or do other active things.

4. COMPARISION OF VARIOUS PENETRATION TESTING TOOLS

Features Tools	Open Source	Multi-Lingual	Scanning	OS Compatibility	Expose Vulnerability	Display actual Threats
Kali Linux	yes	yes	Uses one of the tool to access vulnerability	Unix type	Yes	yes
Metasploit	yes	yes	Uses Built in plugins such as Nessus, Nexpose, OpenVAS & WMAP.	Platform independent	Yes	yes
Nmap	yes	No [c,c++,python,Lua]	Host discovery& port scanning & OS detection	Platform independent	Yes	yes
SQLmap	yes	no	SQL injection	Platform dependent [Linux,windows,Macos]	Yes	yes
WifiPhisher	yes	no	No		Yes	yes
Wireshark	yes	No[c,c++]	types of networks, including Ethernet, IEEE 802.11, and loopback.	Platform independent	Yes	yes

The Metasploit Framework can be extended to use add-ons in multilingual feature. Metasploit Pro makes the reliable Metasploit Framework reachable to all network with an easy-to-use interface, as well as wizards to get launching and reporting on full pen tests in short period. It is well known for its anti-forensic and elusion tools, some are built into the Metasploit Framework. After comparison of important penetration testing tools with their features, Metasploit satisfies all the features and also user-friendly.

5. CONCLUSION:

A Penetration testing is implemented to determine how well an organization's assets are protected from a direct internet attack. This paper describes the approach used previously for the network penetration test and the best

suitable tool is also discussed. The aim of this paper was to provide a general overview of the penetration testing, phases, tools and techniques employed earlier in previous studies and in network security.

REFERENCES:

1. Harsh deep Singh, Dr. Jaswinder Singh May – June 2017 Penetration Testing in Wireless Networks - International Journal of Advanced Research in Computer Science.
2. Goel, J. N., & Mehtre, B. (2015). Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. Procedia Computer Science, 57, 710-715.
3. Fiocca, M. (2009). Literature Study of Penetration Testing.
4. B L V Vinay Kumar, K Raja Kumar, & V Santhi. (2016). Penetration Testing using Linux Tools: Attacks and Defense Strategies. International Journal of Engineering Research andTechnology,V5(12), 153-158.
5. Ten, C., Liu, C., & Manimaran, G. (2008). Vulnerability Assessment of Cybersecurity for SCADA Systems. IEEE Transactions on Power Systems, 23(4), 1836-1846.
6. A, Ciampa, C. A. Visaggio, and M. Di Penta. Aheuristic-based approach for detecting SQL-injectionvulnerabilities in web applications. In Proceedings of theICSE Workshop on Software Engineering for Secure Systems (SESS '10)
7. Reaves, B., & Morris, T. (2012). Analysis and mitigation of vulnerabilities in short-range wireless communications for industrial control systems. International Journal of Critical Infrastructure Protection, 5(3-4), 154-174. [9]He, L., & Bode, N. (n.d.). Network Penetration Testing
8. chiem Trieu Phong “A study of penetration Testing Tools and Approaches” Eds. Auckland :Academic, 2014

WEB REFERENCES:

- https://msdn.microsoft.com/en-us/library/cc875806.aspx
- https://www.linux.com/news/interview-fyodor-nmap
- https://threatpost.com/wifiphisher-wi-fi-hacking-tool-automates-phishing-attacks/110201/]
- https://informationtreasure.wordpress.com/2014/07/24/hacking-website-with-sqlmap-in-kali-linux/