PENETRATION TESTING AND VULNERABILITY ASSESSMENT: INTRODUCTION, PHASES, TOOLS AND METHODS

Kristina Božić,
Nikola Penevski,
Saša Adamović*

Singidunum University,
Belgrade, Serbia

Abstract:
Penetration testing is the practice of testing a computer system, network or web application to find security vulnerabilities by using a diverse variety of tools and methods. This work is a brief overview of the phases, including reconnaissance or information gathering, scanning, vulnerability analysis, exploitation, and reporting, along with some of the basic tools and methods of penetration testing. It's fundamental, for every penetration tester, to be familiar with these concepts in order to successfully execute a full testing process and forge good reports.

Keywords:
Penetration Testing, Vulnerabilities, Security Testing, Vulnerability Assessment, Exploits.

1. INTRODUCTION

With the ever growing connectivity of things through the internet, security is becoming one of the most important parts of information systems. Businesses tend to protect their information assets by complying with the mandated security regulations and following best practices in order to reduce the risks that they might face. In an attempt to solve the security problem and comply with the mandated security regulations, security experts have developed various security assurance methods including proof of correctness, layered design, software engineering environments and penetration testing.

Penetration testing is a comprehensive method to test the complete, integrated, operational, and trusted computing base that consists of hardware, software and people. The objective is to test real-time systems, find any potential vulnerabilities, and take measures to improve the overall security of the system.

Penetration testing differs from security testing. The latter demonstrates the correct behavior of the system's security controls while penetration testing determines the difficulty for someone to evade an organization's security controls and gain unauthorized access to its information and information systems.

Correspondence:
Saša Adamović

e-mail:
sadamovic@singidunum.ac.rs

DOI: 10.15308/Sinteza-2019-229-234

Experts have developed various tools and methods with the aim to provide a better, more efficient and dynamic examination. This paper provides an overview by going through phases, tools and methods used in penetration testing.

2. BACKGROUND

Penetration Testing

Penetration Testing can be defined as "is an authorized simulated cyber attack on a computer system, performed to evaluate the security of the system".[1] Process of penetration testing, or for short pen testing, is performed by trained security experts called ethical hackers. The purpose of these tests is to find the security vulnerabilities that the software may contain.

The Nation Institute of Standards and Technology (NIST) defines penetration testing as: "a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries".[2]

Some of the best Penetration Testing Companies in recent years are Security Assessment, Security Audit Systems and Hacklabs.[3]

Phases of Penetration Testing

The process of penetration testing is consisted of five phases:

1. Reconnaissance – in the first step, a tester must gather basic information of a targeted system, such as the correct domain of web server, are there any sub-domains connected to this domain, is there any firewall, relevant IP addresses and so on. The information gathered here is used later on in the testing, which makes this step very important.
2. Scanning – in this step the use of technical tools is needed to further the attacker's knowledge of the system. By doing that we can gain information about what type of services are running on the server and what is the version of the given server. Additional information can be identification of the port that this service is running, and which Operating System is used on the system.
3. Gaining Access/Discover Vulnerability – in this step a tester must use the information gathered from the previous two phases in order to successfully penetrate the targeted system.
4. Maintaining Access/Exploitation – after successfully compromising a system, tester's goal is to breach all types of securities and gain remote access to the system. If the rules of engagement permit this, a tester ensures that he will be able to maintain access for further examination or penetration of the targeted system.
5. Covering Tracks/Report Generation – the attacker must not leave any trace of compromising the system. This includes returning the system to a state that it was in before the attack by clearing logs and resetting security parameters. In the case of report generation, a tester would write a full report of the Penetration test and give insight on how to increase the overall security of the system.[4]

Penetration Testing methods and benefits

Methods used in penetration testing are:

1. External testing which targets the assets of a company that are available on the internet
2. Internal testing allows a tester to access an application behind the firewall to simulate an attack by a malicious insider
3. Blind testing where a tester only knows the name of the target
4. Double Blind testing means that the security personnel of a targeted company has no knowledge about the arranged simulated attack
5. Targeted testing where both the tester and security personnel of the targeted company work together to provide a security team with real-time feedback from a hacker's perspective.

Benefits of Penetration Testing are:

1. Discovery of publicly available information that has vulnerabilities which can harm the system
2. Managing the unnecessary ports and services open to external access despite the fact that they are not being used
3. Identifying poorly configured systems that allow easy exploitation by a malicious attacker, or poor patch management processes.
4. Finding weak passwords on the system
5. Inadequate or a complete lack of antivirus software
6. Penetration Testing gives company clear recommendations on how to improve their security and maintain their system.

Vulnerability Assessment

Vulnerability Assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, application and network infrastructures and providing the organization doing the assessment with the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately.[5] Vulnerability Assessment is important because it provides a company with information on the security risks and weaknesses in their systems, and helps them to better understand their security flaws and overall risk of a faulty system.

A vulnerability assessment includes penetration testing components used to identify vulnerabilities in the company's personnel, and discover processes that might not be detectable with network or system scans. Some types of vulnerability assessment scans are listed below:

1. Network-based scans, used to identify network security attacks
2. Host-based scans, used to discover vulnerabilities in servers or other network hosts.
3. Wireless network scans usually used to identify rogue access points, or just validate that the company's network is securely configured
4. Application scans, used in website testing to discover potential software vulnerabilities
5. Database scans, used to determine weak points in a database in order to prevent malicious attacks

Figure 1. Phases of Penetration Testing

3. PENETRATION TESTING AND VULNERABILITY ASSESSMENT MOST USED TOOLS

Penetration testing is method used to find the vulnerabilities that exist in the system. These tests simulate various types of attacks on the targeted system using variety of tools. Some of those tools and basics of their usage will be reviewed in this work.

Nmap

Network mapper, or for short Nmap, is a free and open source tool which can be used for initial scanning of systems or networks. This tool is always used in the first phase of penetration testing because of its utilities. Most useful Nmap utilities are gaining insight of a targeted network, including the discovery of hosts available on that network, operating systems running on them and port discovery. Nmap is also suitable for scanning both large and small networks.

Some basic Nmap scanning examples which can be used in enumeration are listed below:

nmap -sP 10.0.0.0/24 – this ping scans the network and makes a list of machines that respond to it

nmap -p 1-65535 -sV -sS target – this is a full TCP port scan along with service version detection

nmap -v -sS -A target – this command prints verbose output, runs stealth tcp syn scan with OS and version detection

nmap -v -p 1-65535 -sV -O -sS target – this prints verbose output, runs a stealthy syn scan, OS and version detection with a full port range scan

Shodan

Shodan represents a search engine and can be used for finding specific devices and their types. Most common searches are for webcams, cisco and netgear devices.

Shodan search engine works by scanning the entire Internet and then parse the banners returned by scanned devices. When the search is over, the information received by shodan search will be most likely about web servers and their versions, as well as anonymous FTP servers if they exist in a particular location, and the information about the model of the device.

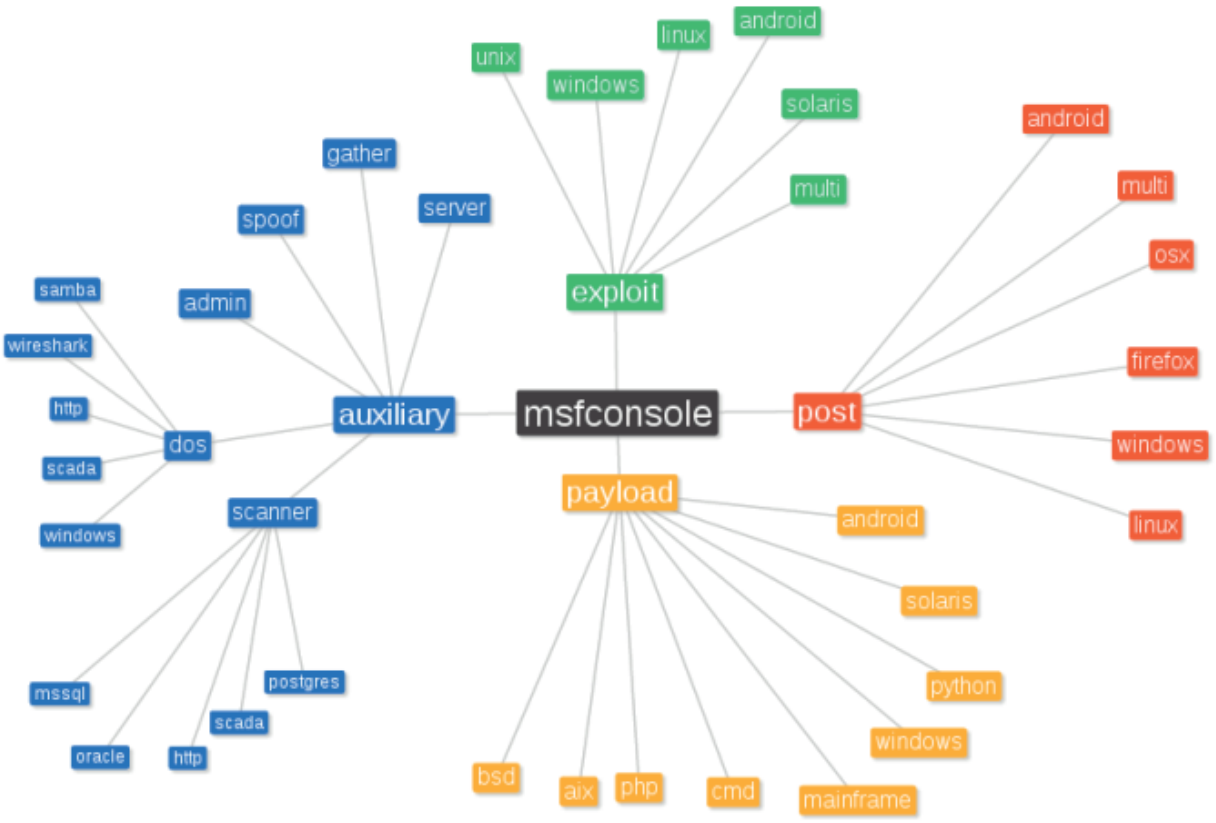

Figure 2. Metasploit Framework Modules

The use of Shodan search engine will most likely increase even more for security research around the Internet of things.

Burp Suite

Burp Suite is a platform for performing security testing of web applications. It's a tool that supports the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.[6]

Some of the essential manual tools that are provided by Burp Suite are listed down below:

1. It allows a manual tester to intercept all requests and responses between the browser and the target application, even with HTTPS in use.
2. It allows the following commands: view, edit or drop individual messages in order to manipulate components of the application.
3. The fine-grained interception rules can be configured in order to control precisely which messages are going to be intercepted
4. The Repeater tool allows to manually edit and reissue individual requests
5. It captures detailed attack results, with all relevant information about each request and response presented in table form. Information obtained with Burp Suite are most likely to be the payload values, HTTP status code, response timers or cookies.[7]

Metasploit

Metasploit is a platform which includes Metasploit Framework and some of the commercial counterparts, and it allows finding, exploiting and validating vulnerabilities.

Metasploit Framework is an open source project which provides the infrastructure, content and tools for performing penetration tests. Anti-forensics andadvanced evasion tools are also offered, and some of them are built into the Metasploit Framework.

A module, which is a core component of the Metasploit Framework, is a piece of software that can perform

a specific action, for example scanning or exploiting. Every task done in Metasploit Framework is defined within a module. The following module types are the ones that are available on Metasploit Framework and contain a brief explanation of each:

1. Exploit - an exploit module executes a sequence of commands which then target a specific vulnerability found in a system or application.
2. Auxiliary - auxiliary modules include scanners, fuzzers, and denial of service attacks.
3. Post-Exploitation - a post-exploitation module allows additional information gathering, but it can be used to gain further access to an exploited target system.
4. Payload – an executable code that runs after an exploit successfully compromised a system and performs malicious actions written by the attacker.
5. NOP generator - NOP generator produces a series of random bytes that you can use to bypass standard IDS and IPS NOP sled signatures. [8]

Wireshark

Wireshark is a network packet analysis tool (also known as a network sniffer) which allows packets to be captured in real time while displaying them in a human readable format. Wireshark is a passive tool that only records network traffic without sending it. This means that if used on the network Wireshark cannot be detected by other parties. This tool is open source and is compatible with both UNIX and Windows and many other operating systems. It uses a graphical user interface which sets it apart from different packet analyzers such as tcpdump which with Wireshark shares many characteristics.

The information captured with Wireshark can be viewed through a GUI or the TTY mode TShark Utility. Wireshark is mostly used for troubleshooting network problems, for examining security problems, verifying network applications and debugging protocol implementations.

Wireshark allows for recording of network activity in different formats such as XML, PostScript, CSV or plain text so that the traffic can be analysed afterwards. It can record traffic directly from the internet via the network adapter, PPP/HDLC, ATM, Bluetooth, USB (natively supported on UNIX), Token Ring, etc. New protocols can be scrutinized within Wireshark by adding or creating plugin. Wireshark is capable of capturing compressed files and decompressing them on the fly further making it easier to analyse the data. It's also capable of capturing and playing VoIP in real time. Data can be collected from many protocols supported by Wireshark some of which include IPsec, ISAKMP, SSL/TLS, WEP, and WPA/WPA2. For an easier management of data and a more intuitive analysis Wireshark offers filters and coloring rules can be applied to different types of packets. Traffic recorded through Wireshark can be replayed to offer a repeatable controlled environment.

4. CONCLUSION

Penetration testing is a very effective method used to analyze security of a system. In testing, a variety of tools can be used to test different parts of a system and write a full report on one system's weaknesses. Some of the tools which are mostly used by pen testers are listed in this work, along with their basic usage and explanation. The most important thing for making a successful penetration test consists of following all the phases discussed above and keeping a clean record of all the information that were gathered during the process. The testers can choose from black box, white box and gray box types of testing, which depends on the amount of information available to testers. They can also choose which method to use, like from the internal or external testing among others, depending on the specific objectives that need to be achieved.

This paper describes and encloses all the basic knowledge needed for the beginning of penetration testing process, phases that the tester goes through with the goal of creating a detailed report that helps companies fix vulnerabilities, increase security and ensure safety of one company's data.

REFERENCES

[1] K. M. Henry, Penetration Testing: Protecting Networks and Systems. IT Governance, ITGP, 978-1-849-28371-7, 2012

[2] Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53 (Rev. 4), 2013

[3] Moseley (Raam), "Web Application Penetration Testing Checklist", 2019. [Online]. Available: https://cybersguards.com/web-application-penetration-testing-checklist-updated-2019/

[4] R. Corey, " Summarizing The Five Phases of Penetration Testing", 2015. [Online]. Available: https://www.cybrary.it/2015/05/summarizing-the-five-phases-of-penetration-testing/

[5] M. Rouse, L. Rosencrance, "Vulnerability Assessment (Vulnerability Analysis), 2018. [Online]. Available: https://searchsecurity.techtarget.com/definition/vulnerability-assessment-vulnerability-analysis

[6] D. Stuttard, "Burp Suite Package Description",2017. [Online]. Available: https://tools.kali.org/web-applications/burpsuite

[7] D. Stuttard, "Burp Suite", 2019. [Online]. Available: https://portswigger.net/burp/

[8] Rapid7, Metasploit Pro User Guide, retrieved from https://www.e-spincorp.com/pdf/product/Rapid7/Metasploit-Pro-user-guide.pdf