Securium fox Technologies Pvt Ltd

Internship Day-14

NAME: Teja Vardhan Madamanchi

DATE : 11 June 2021

THE HACKER METHODOLOGY

The Process that pentesters follow is summarized in the following steps:

1. **Reconnaissance**
2. **Enumeration/Scanning**
3. **Gaining Access**
4. **Privilege Escalation**
5. **Covering Tracks**
6. **Reporting**

1. Reconnaissance

--The first phase of the Ethical Hacker Methodology is **Reconnaissance.**
--Reconnaissance is all about collecting information about your target.

Reconnaissance usually involves using *publicly available* tools like Google to conduct research about your target.

2. Enumeration and Scanning Overview

The second phase of the Hacker Methodology is **Scanning and Enumeration.**
This is where a hacker will start interacting with (scanning and enumerating) the target to attempt to find vulnerabilities related to the target.

In the scanning and enumeration phase, the attacker is interacting with the target to determine its overall **attack surface.**

The attack surface determines what the target might be vulnerable to in the Exploitation phase.

Nmap is a tool which can scan a target and tell us a wide variety of things:

- What ports are open

- The operating system of the target(Windows, Linux, MacOS, etc. including what version of the Operating System)
- What services are running and what version of the service(for example, just saying FTP (File Transfer Protocol) isn't enough - nmap can attempt to fingerprint and determine the exact VERSION of FTP which may enable us to find a specific vulnerability in the target)

3. Exploitation

The exploitation phase can only be as good as the recon and enumeration phases before it, if you did not enumerate all vulnerabilities you may miss an opportunity, or if you did not look hard enough at the target - the exploit you have chosen may fail entirely!

One common tool used for exploitation is called **Metasploit** which has many built-in scripts to try to keep life simple.

4. Privilege Escalation

After we have gained access to a victim machine via the exploitation phase, the next step is to **escalate privileges** to a higher user account. The following accounts are what we try to reach as a pentester:

- **In the Windows world, the target account is usually: Administrator or System.**
- **In the Linux world, the target account is usually: root**

5. Covering Tracks

Since the rules of engagement for a penetration test should be agreed to before the test occurs, the penetration tester should stop IMMEDIATELY when they have achieved privilege escalation and report the finding to the client.

6. Reporting

The final phase of the pentest methodology is the reporting phase.
The reporting phase often includes the following things:

- **The Finding(s) or Vulnerabilities**
- **The CRITICALITY of the Finding**
- **A description or brief overview of how the finding was discovered**
- **Remediation recommendations to resolve the finding**

A findings summary is usually something like this:

- **Finding:** SQL Injection in ID Parameter of Cats Page
- **Criticality:**Critical

- **Description:** Placing a payload of 1' OR '1'='1 into the ID parameter of the website allowed the viewing of all cat names in the cat Table of the database. Furthermore, a UNION SELECT SQL statement allowed the attacker to view all usernames and passwords stored in the Accounts table.
- **Remediation Recommendation:** Utilize a Prepared SQL statement to prevent SQL injection attacks

COMMON TERMINOLOGIES

Vulnerability

A vulnerability is a weakness in design, implementation, operation, or internal control. Vulnerability refers to the inability (of a system or a unit) to withstand the effects of a hostile environment.

Attack

An Attack is any attempt to expose, alter, disable, destroy, steal or gain information through unauthorized access to or make unauthorized use of an asset. A cyberattack is any offensive maneuver that targets computer information systems, infrastructures, computer networks, or personal computer devices.

Threat

In computer security, a threat is a potential negative action or event facilitated by a vulnerability that results in an unwanted impact to a computer system or application.

Exploit

It is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic.

Common Vulnerabilities and Exposures

The **Common Vulnerabilities and Exposures** (**CVE**) system provides a reference-method for publicly known information-security vulnerabilities and exposures.

Social engineering

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information.
An example of social engineering is the use of the "forgot password" function on most websites which require login.

Phishing

It is the attempt of acquiring sensitive information such as usernames, passwords, and credit card details directly from users by deceiving the users.

Digital signature

A Digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature, where the prerequisites are satisfied, gives a recipient very strong reason to believe that the message was created by a known sender (authentication), and that the message was not altered in transit(integrity).

Hash Function and Hashing

A **hash function** is any function that can be used to map data of arbitrary size to fixed-size values. The values returned by a hash function are called *hash values*, *hash codes*, *digests*, or simply *hashes*. The values are usually used to index a fixed-size table called a *hash table*. Use of a hash function to index a hash table is called ***hashing* or *scatter storage addressing***.

Open-source intelligence

Open-source intelligence(**OSINT**) is a multi-factor (qualitative, quantitative) methodology for collecting, analyzing and making decisions about data accessible in publicly available sources to be used in an intelligence context.

Buffer Overflow

A Buffer overflow, or buffer overrun, is an anomaly where a program while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations.

Reverse Shell

A reverse shell is a shell session established on a connection that is initiated from a remote machine, not from the local host. Attackers who successfully exploit a remote command execution vulnerability can use a reverse shell to obtain an interactive shell session on the target machine and continue their attack.

Bind Shell

Bind shell is a type of shell in which the target machine opens up a communication port or a listener on the victim machine and waits for an incoming connection. The attacker then connects to the victim machine's listener which then leads to code or command execution on the server.

Network socket

A Network socket is a software structure within a network node of a computer network that serves as an endpoint for sending and receiving data across the network. The structure and properties of a socket are defined by an application programming interface (API) for the networking architecture. Sockets are created only during the lifetime of a process of an application running in the node.

Bug

A software bug is an error, flaw or fault in a computer program or system that causes it to produce an incorrect or unexpected result, or to behave in unintended ways

XML

Extensible Markup Language (**XML**) is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

API

An **Application programming interface** (**API**) is an interface that defines interactions between multiple software applications or mixed hardware software intermediaries. API is a software intermediary that allows two applications to talk to each other. Each time you use an app like Facebook, send an instant message, or check the weather on your phone, you're using an API.

Metasploit Framework

The Metasploit Framework is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. The Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. At its core, the Metasploit Framework is a collection of commonly used tools that provide a complete environment for penetration testing and exploit development.

Malware

Malicious software (malware) installed on a computer can leak personal information, can give control of the system to the attacker and can delete data permanently. Malware is usually introduced into a network through phishing malicious attachments, or malicious downloads, but it may gain access through social engineering or flash drives as well.

Types of Malware

1. Virus

Viruses are designed to damage the target computer or device by corrupting data, reformatting your hard disk, or completely shutting down your system. They can also be used to steal information, harm computers and networks, create botnets, steal money, render advertisements, and more.

2. Worm

Worms spread over computer networks by exploiting operating system vulnerabilities. A worm is a standalone program that replicates itself to infect other computers, without requiring action from anyone.Since they can spread fast, worms are often used to execute a payload—a piece of code created to damage a system. Payloads can delete files on a host system, encrypt data for a ransomware attack, steal information, delete files, and create botnets.

3. Trojan Horse

A Trojan horse, or "Trojan", enters your system disguised as a normal, harmless file or program designed to trick you into downloading and installing malware. As soon as you install a Trojan, you are giving cyber criminals access to your system. Through the Trojan horse, the cyber criminal can steal data, install more malware, modify files, monitor user activity, destroy data, steal financial information, conduct denial of service (DoS) attacks on targeted web addresses, and more.

4. Spyware

Installed on your computer without your knowledge, spyware is designed to track your browsing habits and internet activity. Spying capabilities can include activity monitoring, collecting keystrokes, and harvesting of account information, logins, financial data, and more. Spyware can spread by exploiting software vulnerabilities, bundling with legitimate software, or in Trojans.

5. Adware

Adware is often known for being an aggressive advertising software that puts unwanted advertising on your computer screen. Malicious adware can collect data on you, redirect you to advertising sites, and change your internet browser settings, your default browser and search settings, and your homepage.

6. Ransomware

Ransomware is a type of malware that holds your data captive and demands payment to release the data back to you. It restricts user access to the computer by either encrypting files on the hard drive or locking down the system and displaying messages that are intended to force the user to pay the attacker to release the

restrictions and regain access to the computer. Once the attacker is paid, your system and data will usually go back to its original state.

Nmap

Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.

Password cracking

In cryptanalysis and computer security, password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system in scrambled form.

Client OS & Server OS

A client operating system is an operating system that operates within desktops and other various portable devices, whereas a server operating system is an operating system that is designed to be installed and used on a server.

Packet

A packet is a small segment of a larger message. Data sent over computer networks, such as the Internet is divided into packets. These packets are then recombined by the computer or device that receives them.

Frame

A frame is a digital data transmission unit in computer networking and telecommunication. A frame works to help identify data packets used in networking and telecommunications structures.In packet switched systems, a frame is a simple container for a single network packet. In other telecommunications systems, a frame is a repeating structure supporting time-division multiplexing.

Well known ports

PORT NUMBER	TRANSPORT PROTOCOL	SERVICE NAME	RFC
20, 21	TCP	File Transfer Protocol (FTP)	RFC 959
22	TCP and UDP	Secure Shell (SSH)	RFC 4250-4256
23	TCP	Telnet	RFC 854
25	TCP	Simple Mail Transfer Protocol (SMTP)	RFC 5321
53	TCP and UDP	Domain Name Server (DNS)	RFC 1034-1035
67, 68	UDP	Dynamic Host Configuration Protocol (DHCP)	RFC 2131
69	UDP	Trivial File Transfer Protocol (TFTP)	RFC 1350
80	TCP	HyperText Transfer Protocol (HTTP)	RFC 2616
110	TCP	Post Office Protocol (POP3)	RFC 1939
119	TCP	Network News Transport Protocol (NNTP)	RFC 8977
123	UDP	Network Time Protocol (NTP)	RFC 5905
135-139	TCP and UDP	NetBIOS	RFC 1001-1002
143	TCP and UDP	Internet Message Access Protocol (IMAP4)	RFC 3501
161, 162	TCP and UDP	Simple Network Management Protocol (SNMP)	RFC 1901-1908, 3411-3418
179	TCP	Border Gateway Protocol (BGP)	RFC 4271
389	TCP and UDP	Lightweight Directory Access Protocol	RFC 4510
443	TCP and UDP	HTTP with Secure Sockets Layer (SSL)	RFC 2818
500	UDP	Internet Security Association and Key Management Protocol (ISAKMP) / Internet Key Exchange (IKE)	RFC 2408 - 2409
636	TCP and UDP	Lightweight Directory Access Protocol over TLS/SSL (LDAPS	RFC 4513
989/990	TCP	FTP over TLS/SSL	RFC 4217
			https://ipwithease.com

802.3(Ethernet)

Ethernet is a family of wired computer networking technologies commonly used in local area networks, metropolitan area networks and wide area networks. It was commercially introduced in 1980 and first standardized in 1983 as IEEE 802.3.

802.11(wifi)

IEEE 802.11 is used in most home and office networks to allow laptops, printers and smartphones, and other devices to communicate with each other and access the Internet without connecting wires.

802.11a (OFDM waveform)

It uses the same data link layer protocol and frame format as the original standard, but an OFDM based air interface (physical layer) was added.
It operates in the 5 GHz band with a maximum net data rate of 54 Mbit/s, plus error correction code, which yields realistic net achievable throughput in the mid-20 Mbit/s.

802.11b

The 802.11b standard has a maximum raw data rate of 11 Mbit/s (Megabits per second) and uses the same media access method defined in the original standard.

802.11g

It operates at a maximum physical layer bit rate of 54 Mbit/s exclusive of forward error correction codes, or about 22 Mbit/s average throughput.

802.11n

802.11n operates on both the 2.4 GHz and the 5 GHz bands. Support for 5 GHz bands is optional. Its net data rate ranges from 54 Mbit/s to 600 Mbit/s.

CPU core

A CPU core is a CPU's processor. A core can work on one task, while another core works a different task, so the more cores a CPU has, the more efficient it is.
A core, or CPU core, is the "brain" of a CPU. It receives instructions, and performs calculations, or operations, to satisfy those instructions. A CPU can have multiple cores.
A processor with two cores is called a dual-core processor; with four cores, a quad-core; six cores, hexa-core; eight cores, octa-core.

Privilege Escalation

Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system, or software application to gain elevated access to resources that are normally protected from an application or user.
There are two main types of privilege escalation: horizontal and vertical.

Vertical Privilege Escalation

Vertical privilege escalation occurs when an attacker gains access directly to an account with the intent to perform actions as that person. This type of attack is easier to pull off since there is no desire to elevate permissions. The goal here is to access an account to further spread an attack or access data the user has permissions to.

Horizontal Privilege Escalation

Horizontal privilege escalation is a bit tricky to pull off as it requires the attacker to gain access to the account credentials as well as elevating the permissions. This type of attack tends to require a deep understanding of the vulnerabilities that affect certain operating systems or the use of hacking tools.

Thread

A Thread of execution is the smallest sequence of programmed instructions that can be managed independently by a scheduler, which is typically a part of the operating system.