Ethical Hacking and its Methodology

DianApps

Ethical Hacking is an act of penetrating systems and networks to find out the threats in those systems. It is also a process to crack the vulnerabilities in the network which a malicious attacker may exploit, causing loss of data, financial loss, and other significant damages.

Coming to its methodology, ethical hackers use the same methods and tools as used by malicious (black hat) hackers, after the permission of an authorized person. Whereas on the other hand, evil hackers use the methods in disgracing and illegal ways.

What is an Ethical Hacker?

Mostly an Ethical Hacker is coined as ‘White Hat Hacker.’ An ethical hacker is information security, computer, and networking expert who systematically attempts to infiltrate computer systems, applications, networks, and other computer resources with the permission of its owners.

The purpose of an ethical hacker is to evaluate the security and identify the vulnerabilities in the system which are exploitable, in systems infrastructure and networks. It is to determine whether unauthorized access or other malicious activities are possible.

Hacking Methodology

Following Methodology is adapted by White Hat hackers for Ethical Hacking:

Phase 1 — Reconnaissance

This is a set of techniques like footprinting, scanning, and enumeration along with processes used to discover and find information about the target system. An ethical hacker during reconnaissance attempts to gather as much information about a target system as possible. They follow a seven-step process as listed below:

1. **Information Gathering** — The idea over here is to collect as much information as possible about the target which is interesting, new and of utmost importance. And to achieve this many tools are available which are used by hackers so as to stop any real planned attacks.

2. **Determining the network range** — After finding out the target IP address, it is time to determine the network range. It is important to determine the maximum number of networks that will give a clear plan and matrix of hacking.
3. **Identifying the active machine** — We need to find the active machines that are on the target network range. It is a simple way by performing a ping on the target network. In order to avoid it being caught by the host or rejected, we need to follow a proper suit so as to complete the process successfully.
4. **Finding open ports and access points** — After determining the network range and active machine, an ethical hacker proceeds with the port scanning process to retrieve the open TCP and UDP access port points.
5. **OS fingerprinting** — It is the process of learning whether the operating system is running on the target device. So, OS Fingerprinting is the process in which we compute and determine the identity of a remote host's operating system.
6. **Fingerprinting Services** — This is accomplished by sending specially crafted packets to a target machine and then noting down their response. It is analysed by gathering the information to determine the target OS.
7. **Mapping the Network** — It is the study of the physical connectivity of networks. In-network mapping, an ethical hacker discovers the devices on

the network and their connectivity which is not to be confused with the network discovery or network enumerating that leads to discovery of their characteristics.

Types of Reconnaissance

It takes place in two parts which are described below:

Active Reconnaissance Passive Reconnaissance Directly connected to computer system to gain information Cannot directly connect to target system for gaining the information Port scanning to find weaknesses in target system DNS Lookup to check all the records of DNS of a given domain name Mirroring Website Google Search Email tracking Whois Queries SNMP Sweeps Social Networking Sites It is done by tools like Nmap, HT track, Ping It is done by using tools like GHDB, Whois, NSlookup

Nmap Tool for Active Reconnaissance

Network Mapper is a free, open-source utility for network discovery and security auditing. It is useful for tasks such as network inventory, managing service upgrade schedules and monitoring host or service uptime. It is designed rapidly to scan large networks but works fine against single hosts. Network mapper runs on all major computer operating systems and official binary packages are available for Linux, Windows and Mac OSX.

Following are the examples of Nmap:

- Scan a single IP / Range of IP’s nmap 192.168.1.1/nmap 192.168.1.1–20
- Scan a Host nmap www.testhostname.com
- Scan a single Port / Range of Port nmap -p 22 192.168.1.1 / nmap -p 1–100 192.168.1.1
- Scan using TCP connect / SYN scan nmap-sT 192.168.1.1/nmap-sS 192.168.1.1
- Scan UDP ports nmap -sU -p 123,161,162 192.168.1.1
- Detect OS and Services nmap -A 192.168.1.1
- Save default output to file nmap -oN outputfile.txt 192.168.1.1
- Scan using default safe scripts nmap -sV -sC 192.168.1.1
- Heartbleed Testing nmap — script=asn-query, whois, ip-geolocation-maxmind192.168.1.0/24

GHDB — Google Hacking Database

The Google Hacking Database was originally developed by Johnny Long, which uses Googledorks which are google operators used in search strings such as in URL, filetype, allintext, site, cache and also operators such as +, -, * and more. Googledorks when used correctly, can sometimes reveal interesting and even sensitive information such as error messages, vulnerable servers and websites, login pages, sensitive files and more.

Following are the examples of GHDB:

- [cache:] cache:www.xyz.com
- [info:] info:www.xyz.com
- [related:] related:www.xyz.com
- [inurl:] inurl:query
- [allinurl:] allinurl:faq contact
- [intittle:] Movie comedy intittle:top ten
- [allintittle:] allintittle:top ten

- [intext:] Shubham intext:samuel
- [allintext:] allintext:recipes lime coriander

Phase 2 — Scanning

Collecting more information using complex and aggressive reconnaissance techniques is termed as Scanning

Scanning is a set of steps and methods that are for identifying live hosts, ports, services and discovering operating systems and architecture of the target system. Identifying vulnerabilities, threats in the network by scanning which is used to create a profile of the target organization.

Following procedure is to be followed while performing the process of Scanning:

1. Which Servers are alive
2. Specific IP address
3. Operating System
4. System Architecture
5. Services running on each System

Types of Scanning in Detail

1.Port Scanning

Port Scanning is a series of messages sent by someone who is attempting to break into a computer system to learn which computer network services, each associated with a renowned port number, the computer provides. It is a favourite approach of computer crackers which gives the attacker an idea of where to probe for weaknesses. Fundamentally, this method consists of sending a message to each port, one by one. The responses received indicates whether the port is used and can, therefore, be probed for weakness.

Different Types of port scans involve:

- Vanilla — It is an attempt to connect to all ports. In all, there are 65,536 vanilla ports.
- Strobe — The attempt to connect to only some of the selected ports. There are under 20 strobe ports.
- Stealth scan — Numerous techniques for stealth scanning that attempts to prevent the request for the connection being logged.
- FTP Bounce Scan — There are attempts that are directed through a File Transfer Protocol (FTP) server to disguise the cracker's location.
- Fragmented Packets — This scanning is done by sending packet fragments that can get through simple packet filters in a firewall.
- UDP — In this Scan, the User looks for open User Datagram Protocol ports.
- Sweep — Here the hacker scans the same port using a number of computer machines.

2.Network Scanning

A network scanner is an important element in the collection of the network administrator and penetration tester. This allows the user to map the network as well as to find the devices that would be hard to find manually. It also allows a security analyst or pen-tester to locate the devices on the network that could be likely to use to begin a breach into the network.

Ethical Hackers need to follow these easy steps to get it into successful working:

1. Identify the Active Hosts.
2. Gathering Information on the live target IP address of the vulnerable hosts in order to launch the attack.
3. Operating System detection using TCP/IP fingerprinting where they send packets to the remote host and examines practically every bit in the responses.
4. System Architecture is a method where specific weak spots are detected in the application software or the operating system which can be used to crush the system or compromise it for undesired purposes.
5. Enables version detection of a particular Service.

3.Vulnerability Scanning

This method is an inspection of the potential points of exploits on a system or network to identify the security holes. In the vulnerability scan, it detects and classifies the system’s weaknesses in computers, networks and communication equipment. It then predicts the effectiveness of countermeasures.

A vulnerability scanner attempts to log into the systems using default or other credentials which build a more detailed picture of the system. After it has built up an inventory, it checks each item in the inventory against one or more databases of known vulnerabilities. This is to see if any items are subject to any of these vulnerabilities.

The outcome of a vulnerability scan is a list of all the systems that are found and identifies on the network. In turn, highlighting any known weaknesses that need hacker’s whole attention.

Vulnerabilities Scanning results into:

- Finding weaknesses in the system.
- And reports any false positive.

Tools Used for Scanning

Various tools and techniques are used by hackers under the scanning process, which are as follows:

- **Superscan:** Powerful Tool from Mcafee: TCP port scanner, pinger, hostname
- **Zen Map:** Powerful Tool to detect OS, Version, Ping Sweep, Port Scanning and more
- **wups:** A Powerful UDP port scanner (works only in

32-bit system)
- **Net Scan Tool suite pack:** A collection of Tools- Port Scanners, Flooders, Web Rippers, Mass Emailers

Hping3 Tool for Scanning

It is a network tool that enables to send custom TCP/IP packet and display target replies like ping program does with ICMP replies. Hping3 handles fragmentation, arbitrary packets body and size. It can be used on order to transfer files compressed under supported protocols.

Following are the examples of Hping3:

- **ICMP Ping-** hping3 -1/ — icmp 192.168.1.1
- **ACK / UDP Scan on port 80-** hping3 –A 192.168.1.1 –p 80 / hping3 -2 192.168.1.1 –p 80
- **Collecting initial sequence number-** hping3 192.168.1.1 –q –p 139 –S
- **Firewall and timestamp-** hping3 –S 192.168.1.1 –p 80 —-tcp-timestamp
- **SYN scan on the port range-** hping3 -8/ — scan 1–100 –S 192.168.1.1 -V
- **Intercept all traffic containing HTTP signature-** hping3 -9 HTTP –I eth0
- **Flooding the victim-** hping3 192.168.1.1 –flood

Enumeration

Enumeration makes a fixed active connection to the system and is the first attack on the target system. It is defined as the process of extracting user names, network resources, machines names, shares and services from the system. Under this phase, the attacker creates an active connection to the system and performs directed queries in order to gain more information about the target IP address and port.

The gathered info is then used to identify the vulnerabilities or weak points in the system security and tries to exploit the system gaining phase.

Tools for Enumeration

FTP Enumeration

It is a tool that is used for enumerating OS-level user accounts via the FTP service. It is fairly simple to modify to script to work against other vulnerable FTP servers such as BlackMoon FTP Server.

Superscan

It is a free port scanning networking tool that has the primary purpose of scanning an IP range. This tool supports extremely fast host discovery lookups as well as TCP and UDP port scans. Its multi-threaded and asynchronous techniques allow users to enter a hostname, IP or IP range and start the scan.

IP Tools

Internet Protocol address is a number assigned to a machine that has a computer network and uses the IP for communicating.

Netstat

This displays an active connection for the Transmission Control Protocol (TCP) and lists the ports on which the computer is listening. It is useful for displaying statistics and enumerating open ports across multiple platforms.

What is NetBios Enumeration?

It stands for 'Network Basic Input Output System.' This system allows the computer to communicate over a LAN and to share the files and printers.

NetBIOS is used to identify network devices over TCP/IP Windows. NetBios must be unique on a network that is limited to 16 characters. The 15 characters are used for the device name and the 16th character is reserved for identifying the type of service running or name record type.

Attackers/hackers use this enumeration to obtain:

- List of computers that belong to a domain
- List of shares on the individual hosts on the network
- Policies and passwords

Counter Measures

1.Close Ports 135–139

2.Disable NetBIOS over TCP/IP

Phase 3

Gaining Access

1. System Hacking

2. Acquire Passwords

3. Password Cracking Techniques

4. Generate Rainbow Tables

Password Cracking

Now that the attacker has acquired the required information, He now tries to hack into the system.

Non-Electronic Attack Attacker need not to possess technical knowledge to crack password. Active Online Attack Attacker performs password cracking by directly communicating with the victim machine. Passive Online Attack Attacker performs password cracking without communicating with the victim machine. Offline Attack Attacker copies target's password file and then tries to crack password in his own machine at different location.

Active Online Attack

Dictionary Attack A Dictionary file is loaded into the cracking application that runs against user accounts. Brute Force Attack The program tries every combination of characters until the password is broken. Rule Based Attack The attack is used when the attacker gets some information about the password.

Password Cracking Tools

Rtgen WinRtgen Pwdump7 Fgdump LOphtcrack Ophcrack Cain & Abel

— — -x — — -