ZROC102

Module 1 – Hacking Methodology

zumaroc

5 phases of Hacking

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Clearing Tracks

Phase1 - Reconnaissance

This is the first step in the ethical hacking methodology.

In this phase, an attacker gathers as much information as possible about the target prior to launching the attack.

Social engineering may be employed as part of this phase.

Another reconnaissance technique is "dumpster diving."

Types of Reconnaissance

Passive Reconnaissance

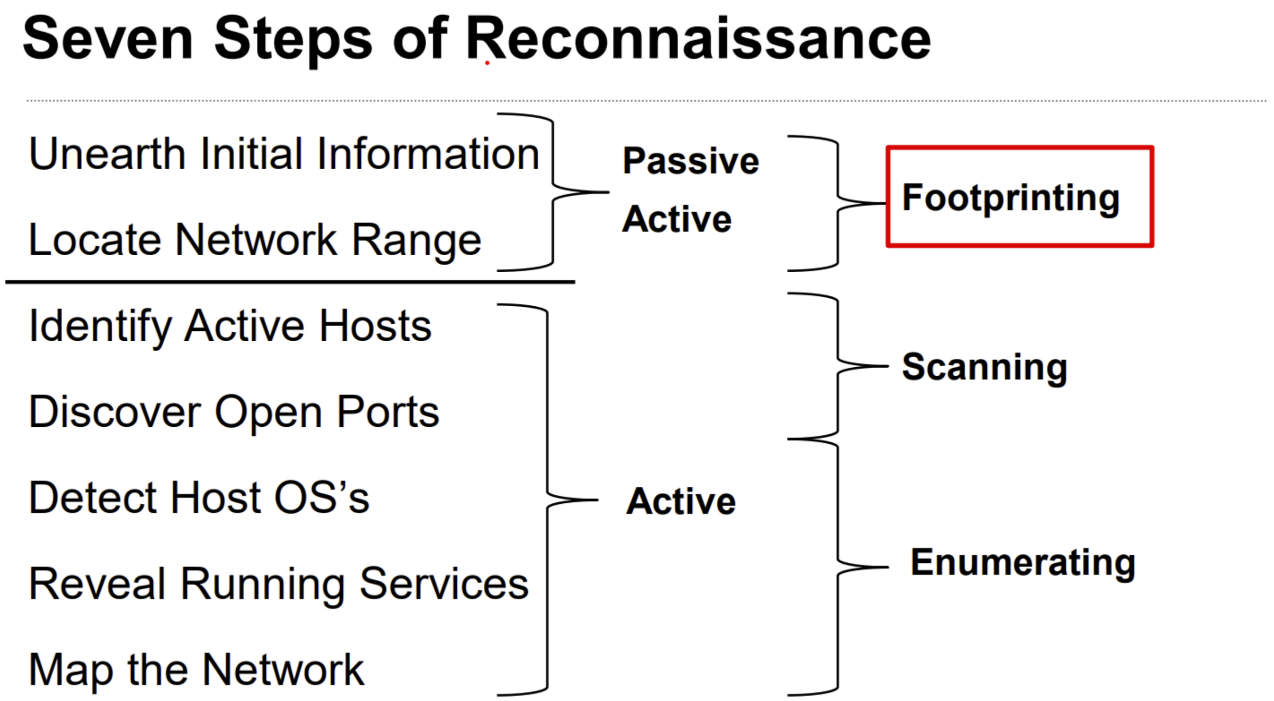
- Here, the attacker does not interact with the system directly. He uses publicly available information, social engineering, and dumpster diving as a means of gathering information. (google, mxtoolbox, shodan)

Active Reconnaissance

- Attacker tries to interact with the system by using tools to detect open ports, accessible hosts, router locations, network mapping, details of operating systems, and applications. (nmap)

Active reconnaissance is usually employed when the attacker discerns that there is a low probability that these reconnaissance activities will be detected.

Reconnaissance Diagram



Seven Steps of Reconnaissance

Unearth Initial Information

Locate Network Range

Passive

Active

Footprinting

Identify Active Hosts

Discover Open Ports

Detect Host OS's

Reveal Running Services

Map the Network

Active

Scanning

Enumerating

Information Gathering

OSINT

- is the action of searching for publicly available information via the internet, or “open-sources”, to get an understanding of the organization, its people/employees, and possible relationships to other organizations.

Tools:

- Search Engines e.g. google, bing
- DNS lookup tools e.g. mxtoolbox, whois

Footprinting

PART OF THE RECONNAISSANCE PHASE – OFTEN, THE TERMS FOOTPRINTING AND RECONNAISSANCE ARE USED INTERCHANGEABLY.

PROCESS OF GATHERING INFORMATION TO CREATE A BLUEPRINT OR MAP OF AN ORGANIZATION’S NETWORK AND SYSTEMS.

OBJECTIVE IS TO GAIN INSIGHT INTO THE TARGET – TO “KNOW YOUR ENEMY”

Reconnaissance Demo

- Company name: Megacorp One
- Now you must determine
- Do they have a presence on the internet? (www.domain.info)
- Can I find their IP space? (nslookup; set type=mx; domain.info)
- Can I find its employee’s email addresses/phone numbers?
- Can I build a hierarchy of the employees?

Active vs Passive

Passive	Active
Website Recon	DNS Enumeration
Whois Enumeration	Port Scanning
Google Hacking	Banner Grabbing
Shodan	Service Enumeration
OSINT Framework	
Security Headers scanner	

Phase2 - Scanning

Scanning is part of intelligence gathering, attackers gain information about:

- Services running on hosts
- Operating Systems
- System Architecture
- Specific IP addresses

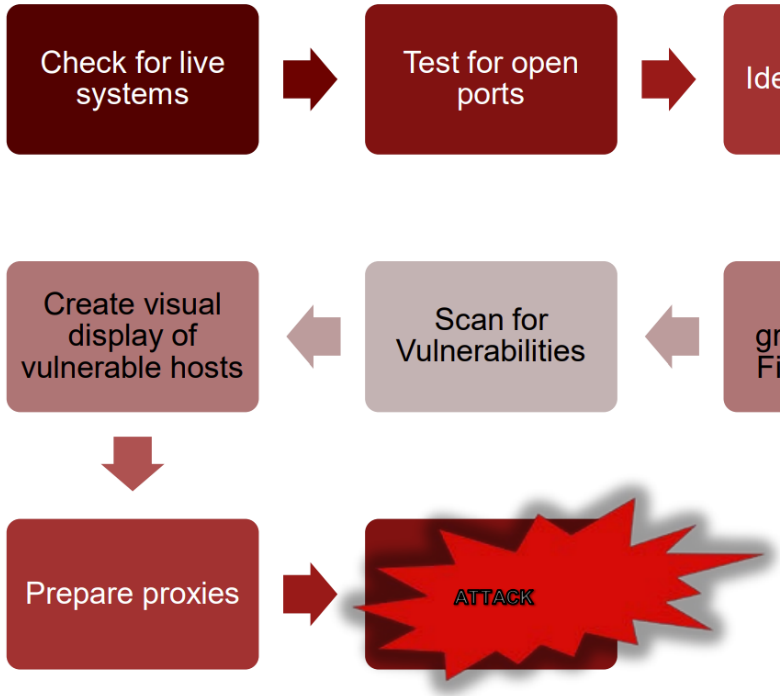
In scanning, the attacker uses the details gathered during reconnaissance to identify specific vulnerabilities

Scanning can be considered a logical extension (and overlap) of the active reconnaissance.

Types of Scanning

- Types of Scanning
  - Network Scanning – Ping sweep
  - Port Scanning – Determine open and listening services
  - Vulnerability Scanning – Fingerprint services and identify vulnerable services
- Port scanners can be used to detect listening ports to find information about the nature of services running on the target machine.
- An attacker can gather critical network information such as the mapping of systems, routers, and firewalls by using simple tools such as Traceroute or netdiscover
- vulnerability scanners that can search for several known vulnerabilities on a target network and can potentially detect thousands of vulnerabilities. E.g. Nessus, openvas etc.

Scanning Methodology Diagram



zumaroc

Network Scanning

Ping Sweep

- A basic network scanning method used to determine which IP addresses map to "live" hosts.
- A ping sweep consists of ICMP ECHO requests sent to multiple hosts.
- If a given address is live, it will return an ICMP ECHO reply.
  - Tools Used: Angry IP Scanner, NMAP, HPING

Firewalking

- A tool that utilizes Traceroute-based techniques to analyze IP packet responses to determine firewall or packet filters and map networks.

Port Scanning

The process of identifying open TCP or UDP ports on a system.

Enables a hacker to learn about services running on a host.

Each service on a system is typically associated with a well-known port number

- Telnet (23)
- HTTP (80)
- POP3 (110)

Common Tools

- NMAP
- HPING

Service Enumeration

Follows scanning and involves finding out as much as possible about what was discovered during scanning.

Typically involves connecting to a target to gather the information.

- Examples of what is sought during enumeration
  - Open file shares on workstations and servers
  - User and group account information
  - Mountable file shares
  - Anonymous FTP login

Banner Grabbing / OS Fingerprinting

- Used to determine the OS running on a target system
- Common tools
  - Nmap, netcat

Vulnerability Scanning

Involves sending packets or requests to targets to figure out vulnerabilities or weaknesses that can be exploited

Takes place after network and port scanning

- Common tools
  - Nessus, qualys, openvas

Phase 3 – Gaining Access

Gaining access is the most important phase of an attack in terms of potential damage.

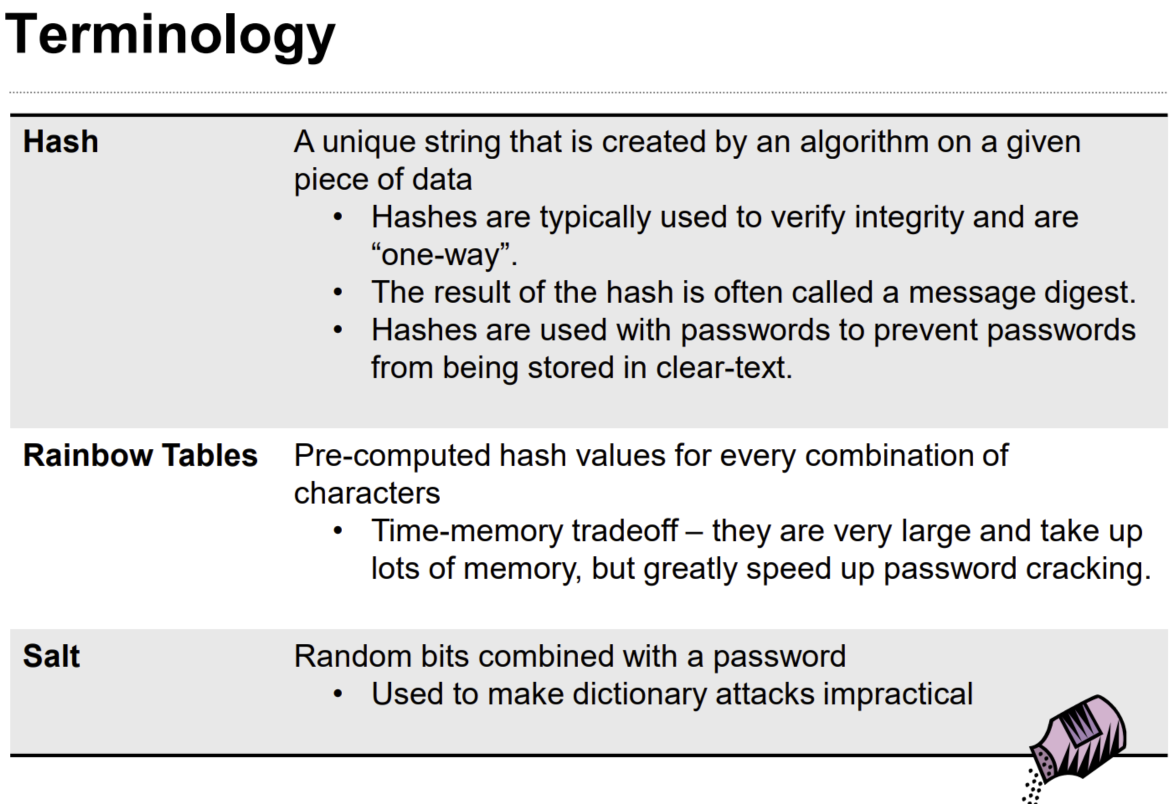
Attackers need not always gain access to the system to cause damage. For instance,

- denial-of-service attacks can either exhaust resources or stop services from running on the target system.

This can occur from exploiting discovered vulnerabilities, deception (social engineering) or theft.

Factors that influence the chances of an attacker gaining access into a target system include the architecture and configuration of the target system, the skill level of the perpetrator, and the initial level of access obtained.

Terminology



Terminology

Hash	A unique string that is created by an algorithm on a given piece of data • Hashes are typically used to verify integrity and are “one-way”. • The result of the hash is often called a message digest. • Hashes are used with passwords to prevent passwords from being stored in clear-text.
Rainbow Tables	Pre-computed hash values for every combination of characters • Time-memory tradeoff – they are very large and take up lots of memory, but greatly speed up password cracking.
Salt	Random bits combined with a password • Used to make dictionary attacks impractical

Authentication

- A method for confirming a user’s identity.
- Commonly done using a username password combination, but can also include electronic keys, certificates, or biometrics.
- Using combinations of authentication mechanisms is known as “multi-factor” authentication and is usually significantly stronger than just a username/password

Authentication Techniques

Basic	Simple web application authentication	Sends usernames and passwords in the clear (base 64 encoded)
Digest	A “Challenge – Response” authentication	Sends an encoded message (the Challenge) to a client, which responds with an encoded copy of the username and password
NTLM	Microsoft’s proprietary authentication implementation	Three versions exist (LM, NTLM, NTLMv2), each providing stronger security than its predecessor, at the expense of compatibility with older systems.
Kerberos	Ticket-granting authentication method	Designed to protect against eavesdropping and replay attacks

Authentication Techniques

Forms	Web applications solicit usernames and passwords through web pages	Simply passes the input values to the application, which makes the authentication determination
Access Tokens	A multi-factor authentication method	Hardware device displays a random number, which must be combined with a PIN or password for authentication. A server is able to determine the random number displayed on the device and can validate it along with the entered password.
Biometrics	Authentication mechanism based on unique properties of the human body (voice, fingerprint, iris, etc.)	Something you “are”

Password Cracking Techniques

Passive

- Sniffing passwords from the network without the target’s knowledge
  - Common tools for password sniffing: Ettercap, ScoopLM, KerbCrack, sslsniff

Active

- Actively trying (guessing) passwords
- Can be manual or automated

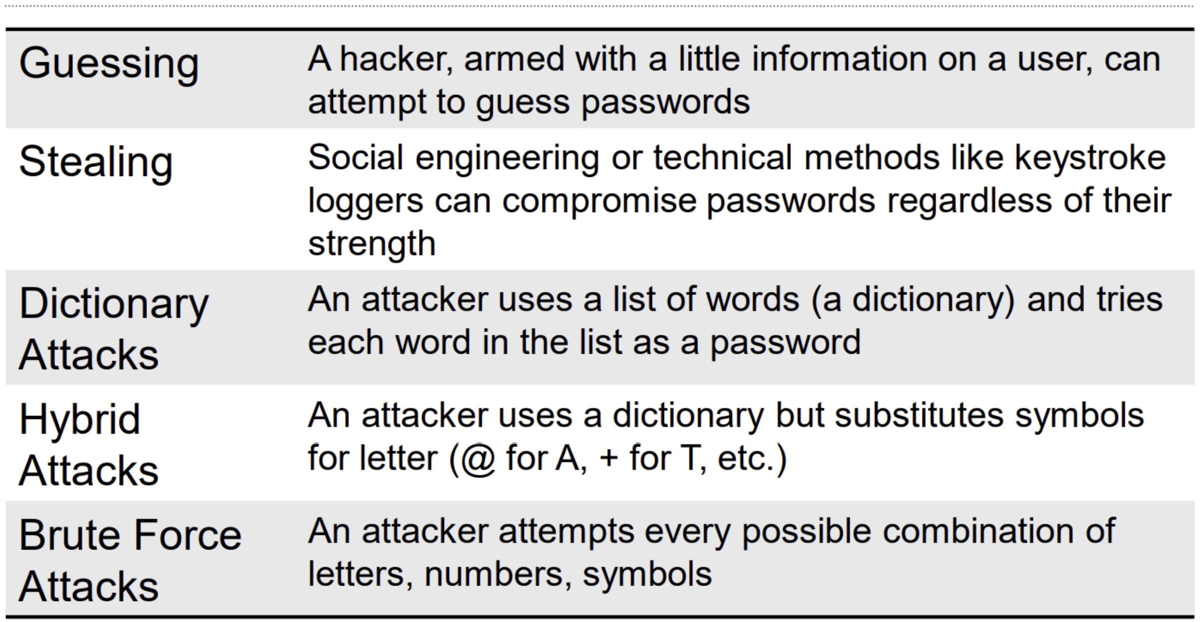
Offline

- A stolen copy of the password file is cracked at leisure

Non-electronic

- Gathering passwords through social engineering methods

Password Cracking Techniques



Guessing	A hacker, armed with a little information on a user, can attempt to guess passwords
Stealing	Social engineering or technical methods like keystroke loggers can compromise passwords regardless of their strength
Dictionary Attacks	An attacker uses a list of words (a dictionary) and tries each word in the list as a password
Hybrid Attacks	An attacker uses a dictionary but substitutes symbols for letter (@ for A, + for T, etc.)
Brute Force Attacks	An attacker attempts every possible combination of letters, numbers, symbols

Cont’d

Usernames and passwords are typically stored as “hashes” in a system password file.

- On Windows, these are stored in the SAM file as NTLM hashes.
- On Linux systems, they are stored in the /etc/shadow & /etc/passwd files as MD5 hashes.

Password cracking tools guesses a password, hashes it, and compares it to the one stored in the system password file.

- If the two match, the password is known – if they don’t, the password cracker repeats the process with a different guess.
- Rainbow tables speed up this process.

Maintaining Access

- Once an attacker gains access to the target system, the attacker can choose to use both the system and its resources, and further use the system as a launch pad to scan and exploit other systems, or to keep a low profile and continue exploiting the system.
- Attackers make use of backdoors, Trojans or rootkits to gain repeat access.
- SSH keys can also be used to gain persistence.
- Attackers can use Trojan horses to transfer usernames, passwords, and even credit card information stored on the system.
- They can maintain control over "their" system for a long time by "hardening" the system against other attackers, and sometimes, in the process, do render some degree of protection to the system from other attacks.

Covering Tracks

- An attacker would like to destroy evidence of his/her presence and activities for various reasons such as:
  - maintaining access.
  - evading detection.
- Erasing evidence of a compromise is a requirement for any attacker who would like to remain undetected.
- This usually starts with erasing the contaminated logins and any possible error messages that may have been generated in the system log file.

Clean Up Steps

- Delete contaminated log files.
- Alter system configuration so that future logins are not logged.
- rootkits can be used to disable logging altogether and discard all existing logs.
- Any files which have been modified should be changed back to their original state.
- An attacker can use the system as a cover to launch fresh attacks against other systems or use it as a means of reaching another system on the network without being detected. Thus, this phase of attack can turn into a new cycle of attack by using reconnaissance techniques all over again

References

- https://d3alc7xa4w7z55.cloudfront.net/static/upload/201/0123/2016-ossovernet_ethical_hacking.pdf
- https://fedvte.usalearning.gov/