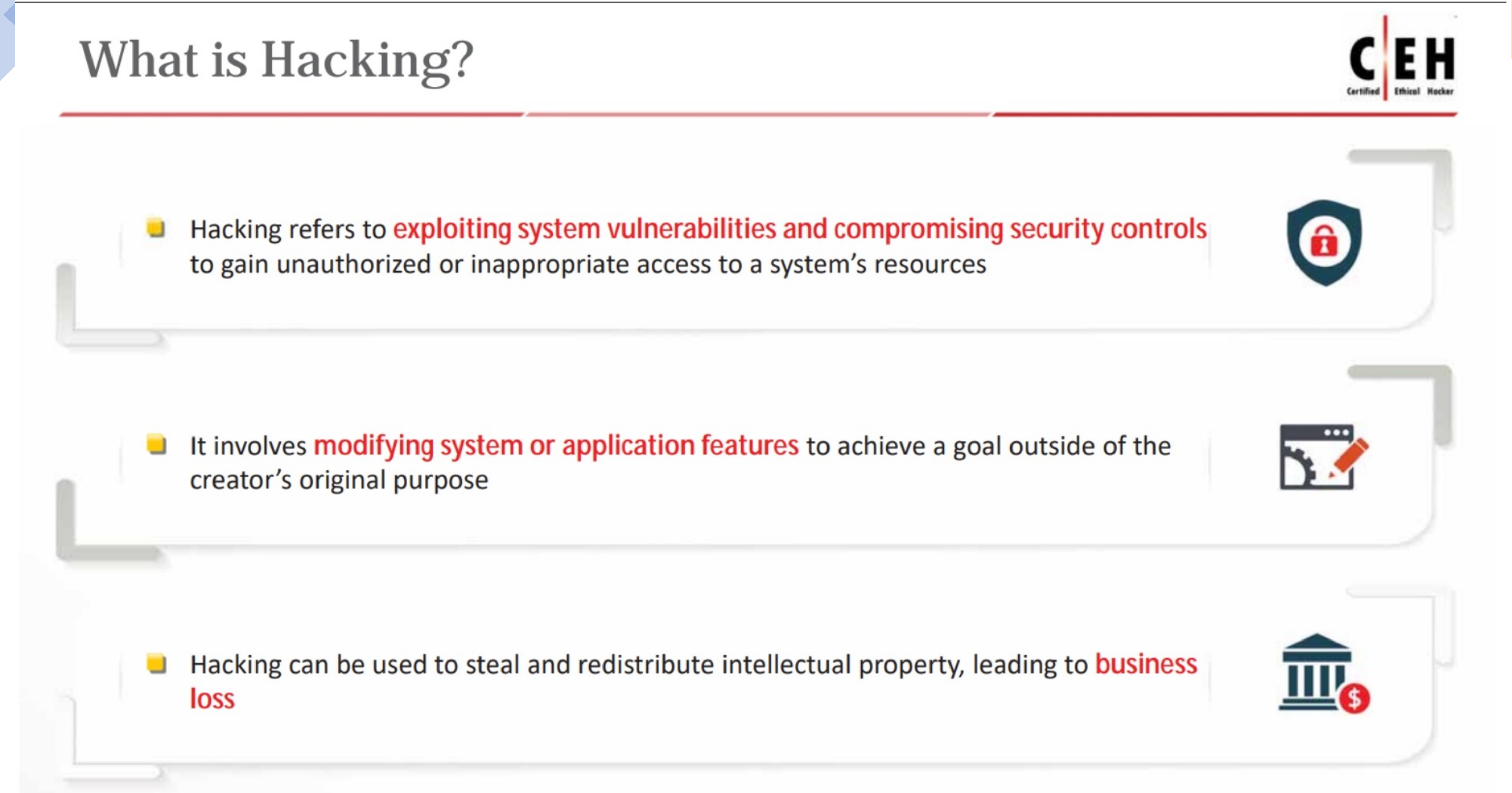
JOURNEE DE LA CYBER SECURITE

Annaba, le 8 mars 2023

Hacking éthique

Dr. Feriel BOUAKKAZ



What is Hacking?

- Hacking refers to **exploiting system vulnerabilities and compromising security controls** to gain unauthorized or inappropriate access to a system's resources
- It involves **modifying system or application features** to achieve a goal outside of the creator's original purpose
- Hacking can be used to steal and redistribute intellectual property, leading to **business loss**

Hacker Classes

C|EH Certified Ethical Hacker

01

Black Hats

Individuals with extraordinary computing skills; they resort to malicious or destructive activities and are also known as crackers

02

White Hats

Individuals who use their professed hacking skills for defensive purposes and are also known as security analysts. They have permission from the system owner

03

Gray Hats

Individuals who work both offensively and defensively at various times

04

Suicide Hackers

Individuals who aim to bring down the critical infrastructure for a "cause" and are not worried about facing jail terms or any other kind of punishment

05

Script Kiddies

An unskilled hacker who compromises a system by running scripts, tools, and software that were developed by real hackers

06

Cyber Terrorists

Individuals with wide range of skills who are motivated by religious or political beliefs to create fear through the large-scale disruption of computer networks

07

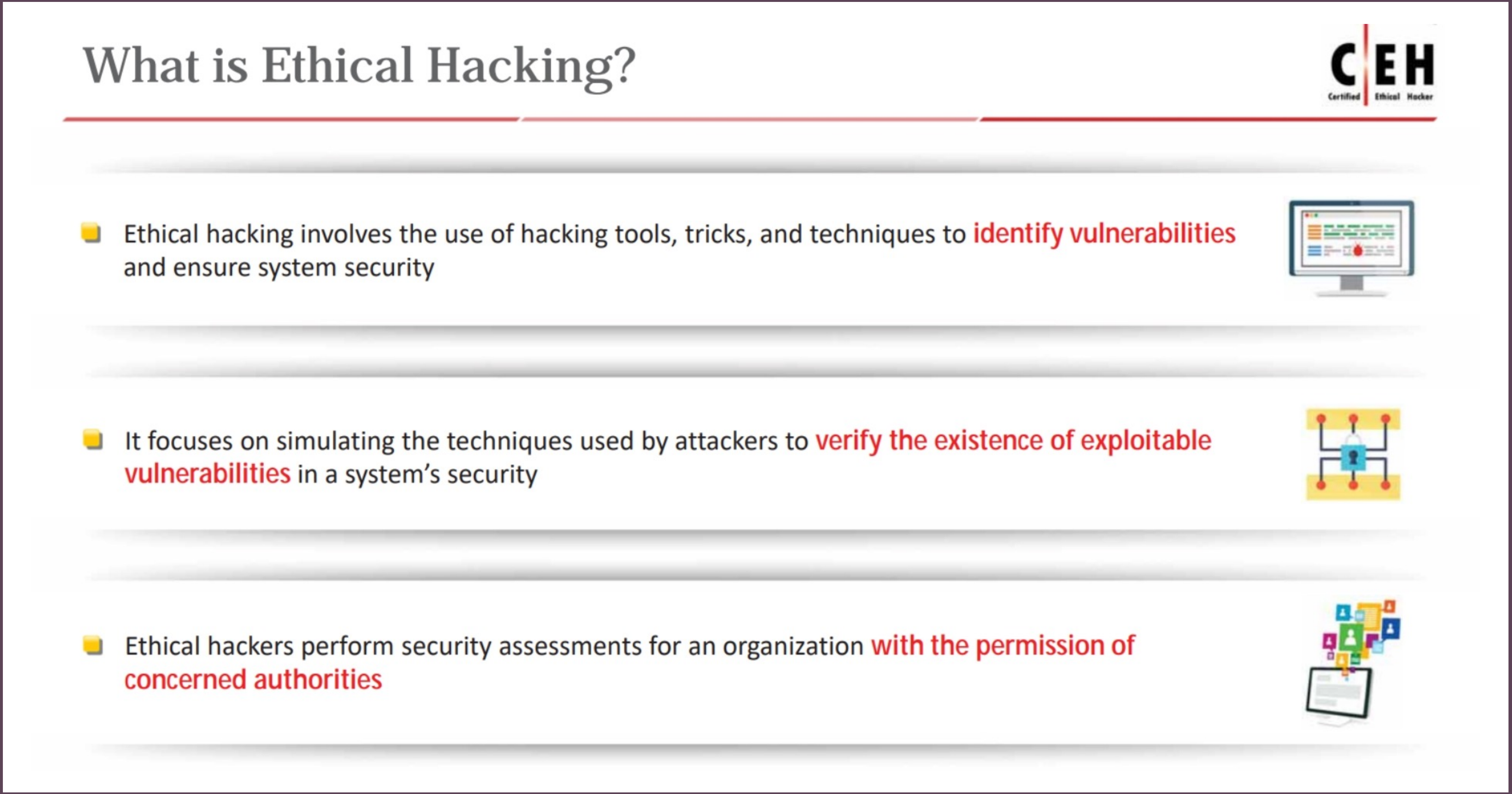
State-Sponsored Hackers

Individuals employed by the government to penetrate and gain top-secret information from and do damage to the information systems of other governments

08

Hacktivist

Individuals who promote a political agenda by hacking, especially by using hacking to deface or disable website



What is Ethical Hacking?

- Ethical hacking involves the use of hacking tools, tricks, and techniques to identify vulnerabilities and ensure system security
- It focuses on simulating the techniques used by attackers to verify the existence of exploitable vulnerabilities in a system's security
- Ethical hackers perform security assessments for an organization with the permission of concerned authorities

Black-box, gray-box and white-box testing !

BLACK -BOX TESTING
ZERO KNOWLEDGE

GRAY -BOX TESTING
SOME KNOWLEDGE

WHITE -BOX TESTING
FULL KNOWLEDGE

Définie dans le contrat de prestation

Continual/Adaptive Security Strategy

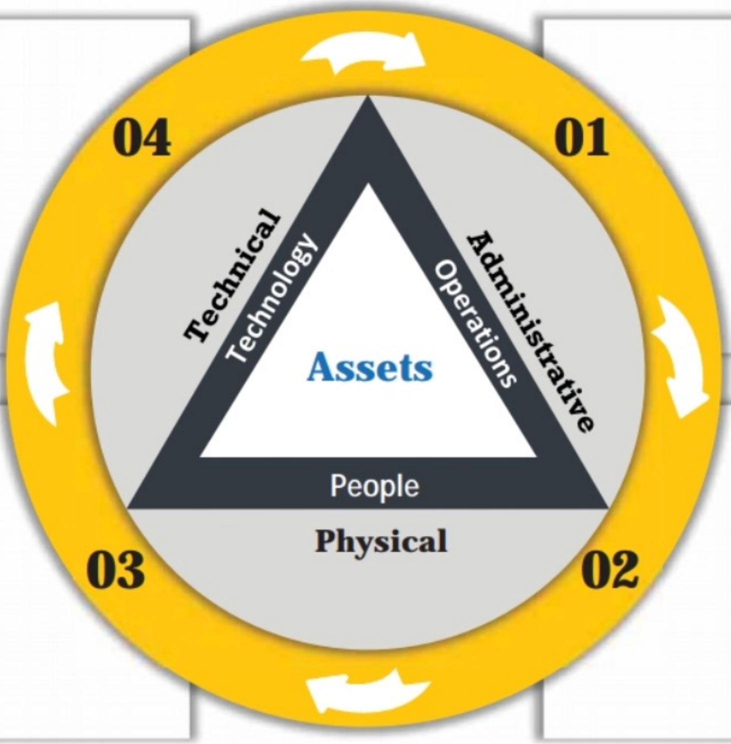
- ❑ Organizations should adopt **adaptive security strategy**, which involves implementing all the four network security approaches
- ❑ The adaptive security strategy consists of four security activities corresponding to each security approach

Predict

- ➢ Risk and Vulnerability Assessment
- ➢ Attack Surface Analysis
- ➢ Threat Intelligence

Protect

- ➢ Defense-in-depth Security Strategy
  - ▪ Protect endpoints
  - ▪ Protect network
  - ▪ Protect data



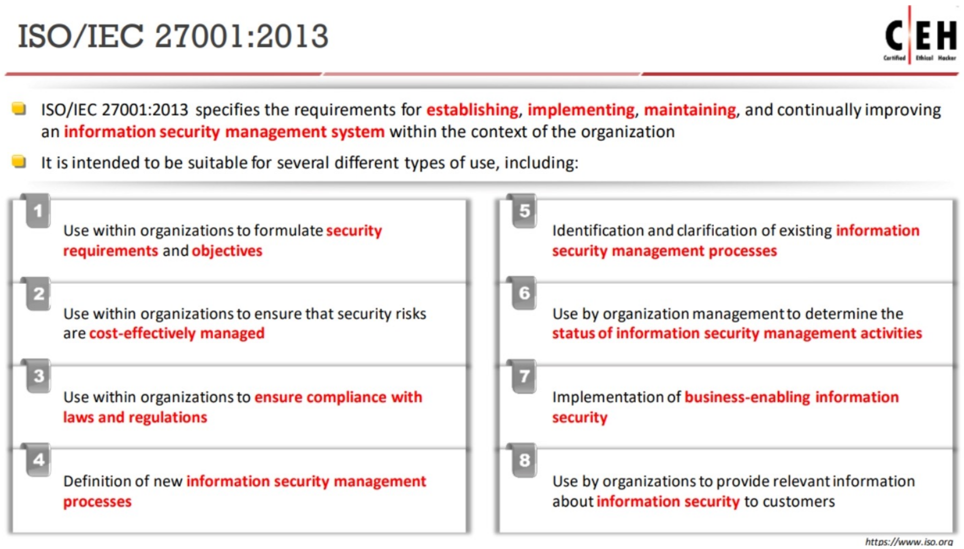
Respond

- ➢ Incident Response

Detect

- ➢ Continuous Threat Monitoring

Lois et standards !

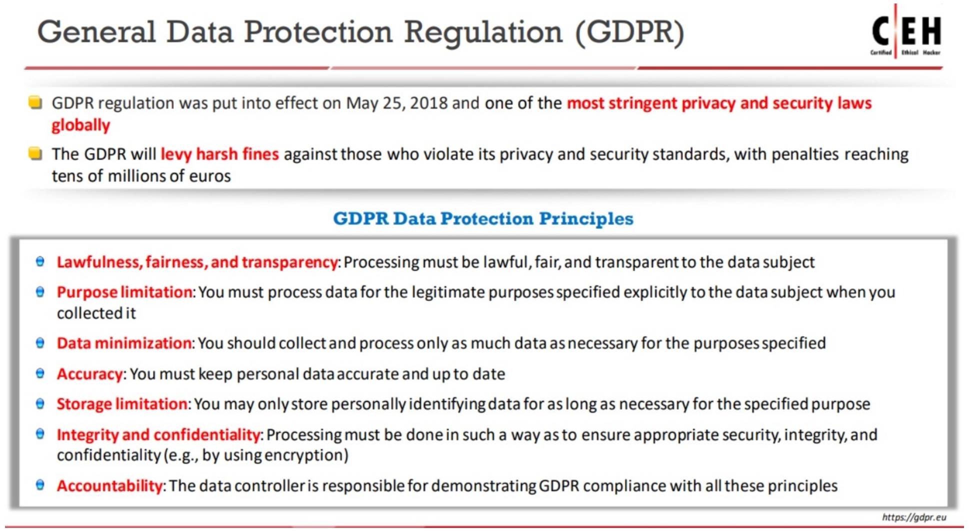


ISO/IEC 27001:2013

- ISO/IEC 27001:2013 specifies the requirements for **establishing**, **implementing**, **maintaining**, and continually improving an **information security management system** within the context of the organization
- It is intended to be suitable for several different types of use, including:

1. Use within organizations to formulate **security requirements** and **objectives**
2. Use within organizations to ensure that security risks are **cost-effectively managed**
3. Use within organizations to **ensure compliance with laws and regulations**
4. Definition of new **information security management processes**
5. Identification and clarification of existing **information security management processes**
6. Use by organization management to determine the **status of information security management activities**
7. Implementation of **business-enabling information security**
8. Use by organizations to provide relevant information about **information security** to customers

https://www.iso.org



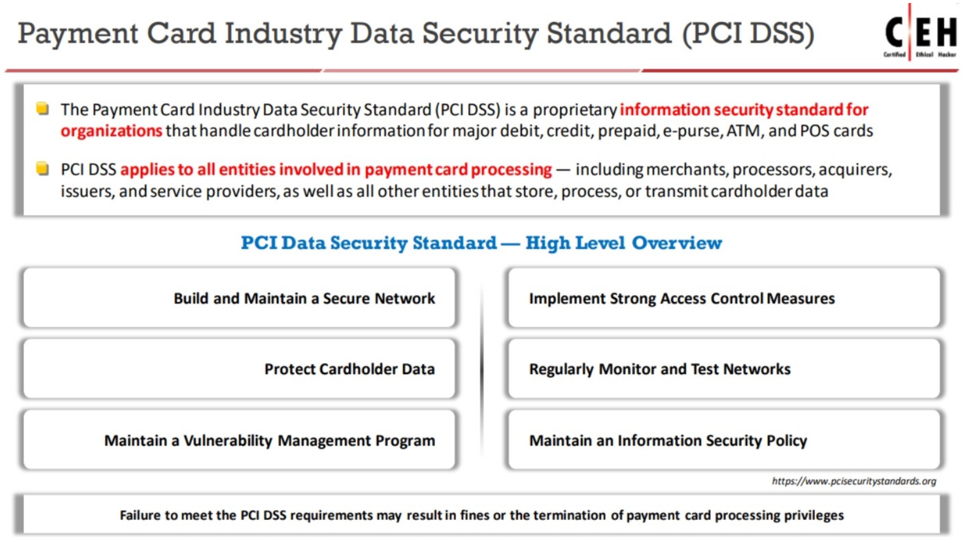
General Data Protection Regulation (GDPR)

- GDPR regulation was put into effect on May 25, 2018 and one of the **most stringent privacy and security laws globally**
- The GDPR will **levy harsh fines** against those who violate its privacy and security standards, with penalties reaching tens of millions of euros

GDPR Data Protection Principles

- **Lawfulness, fairness, and transparency**: Processing must be lawful, fair, and transparent to the data subject
- **Purpose limitation**: You must process data for the legitimate purposes specified explicitly to the data subject when you collected it
- **Data minimization**: You should collect and process only as much data as necessary for the purposes specified
- **Accuracy**: You must keep personal data accurate and up to date
- **Storage limitation**: You may only store personally identifying data for as long as necessary for the specified purpose
- **Integrity and confidentiality**: Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g., by using encryption)
- **Accountability**: The data controller is responsible for demonstrating GDPR compliance with all these principles

https://gdpr.eu



Payment Card Industry Data Security Standard (PCI DSS)

- The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary **information security standard for organizations** that handle cardholder information for major debit, credit, prepaid, e-purse, ATM, and POS cards
- PCI DSS **applies to all entities involved in payment card processing** — including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder data

PCI Data Security Standard — High Level Overview

Build and Maintain a Secure Network

Protect Cardholder Data

Maintain a Vulnerability Management Program

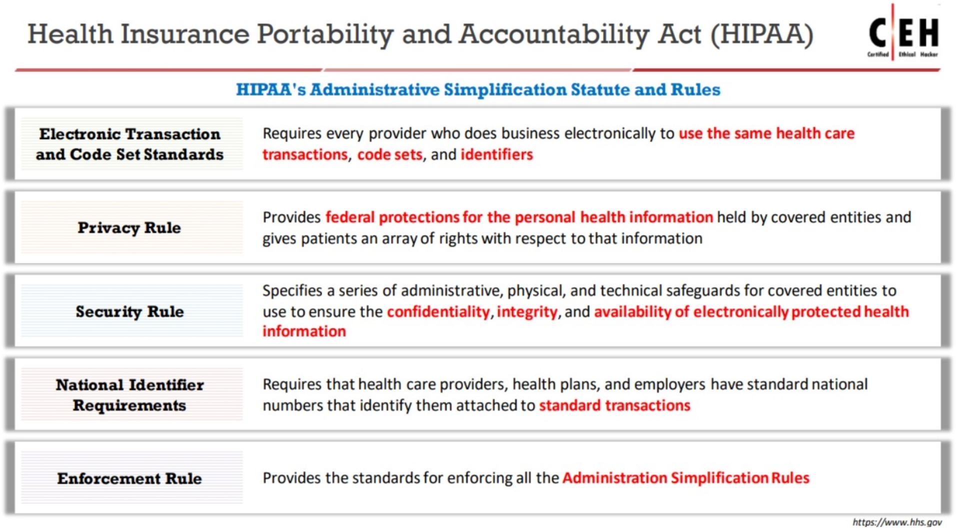
Implement Strong Access Control Measures

Regularly Monitor and Test Networks

Maintain an Information Security Policy

https://www.pcisecuritystandards.org

Failure to meet the PCI DSS requirements may result in fines or the termination of payment card processing privileges



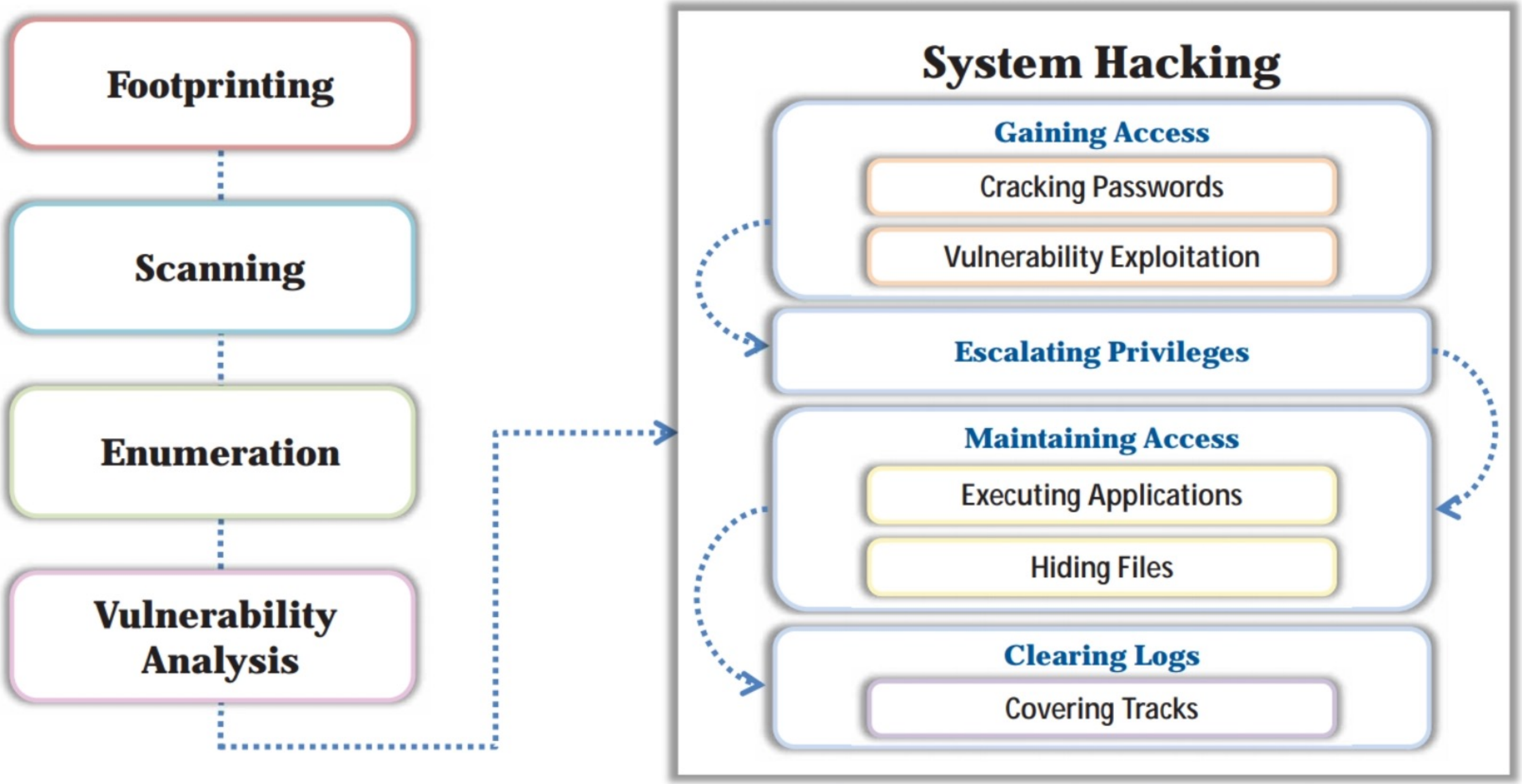
Health Insurance Portability and Accountability Act (HIPAA)

HIPAA's Administrative Simplification Statute and Rules

Electronic Transaction and Code Set Standards	Requires every provider who does business electronically to **use the same health care transactions**, **code sets**, and **identifiers**
Privacy Rule	Provides **federal protections for the personal health information** held by covered entities and gives patients an array of rights with respect to that information
Security Rule	Specifies a series of administrative, physical, and technical safeguards for covered entities to use to ensure the **confidentiality**, **integrity**, and **availability of electronically protected health information**
National Identifier Requirements	Requires that health care providers, health plans, and employers have standard national numbers that identify them attached to **standard transactions**
Enforcement Rule	Provides the standards for enforcing all the **Administration Simplification Rules**

https://www.hhs.gov

CEH Hacking Methodology (CHM)



Footprinting

Scanning

Enumeration

Vulnerability Analysis

System Hacking

Gaining Access

- Cracking Passwords
- Vulnerability Exploitation

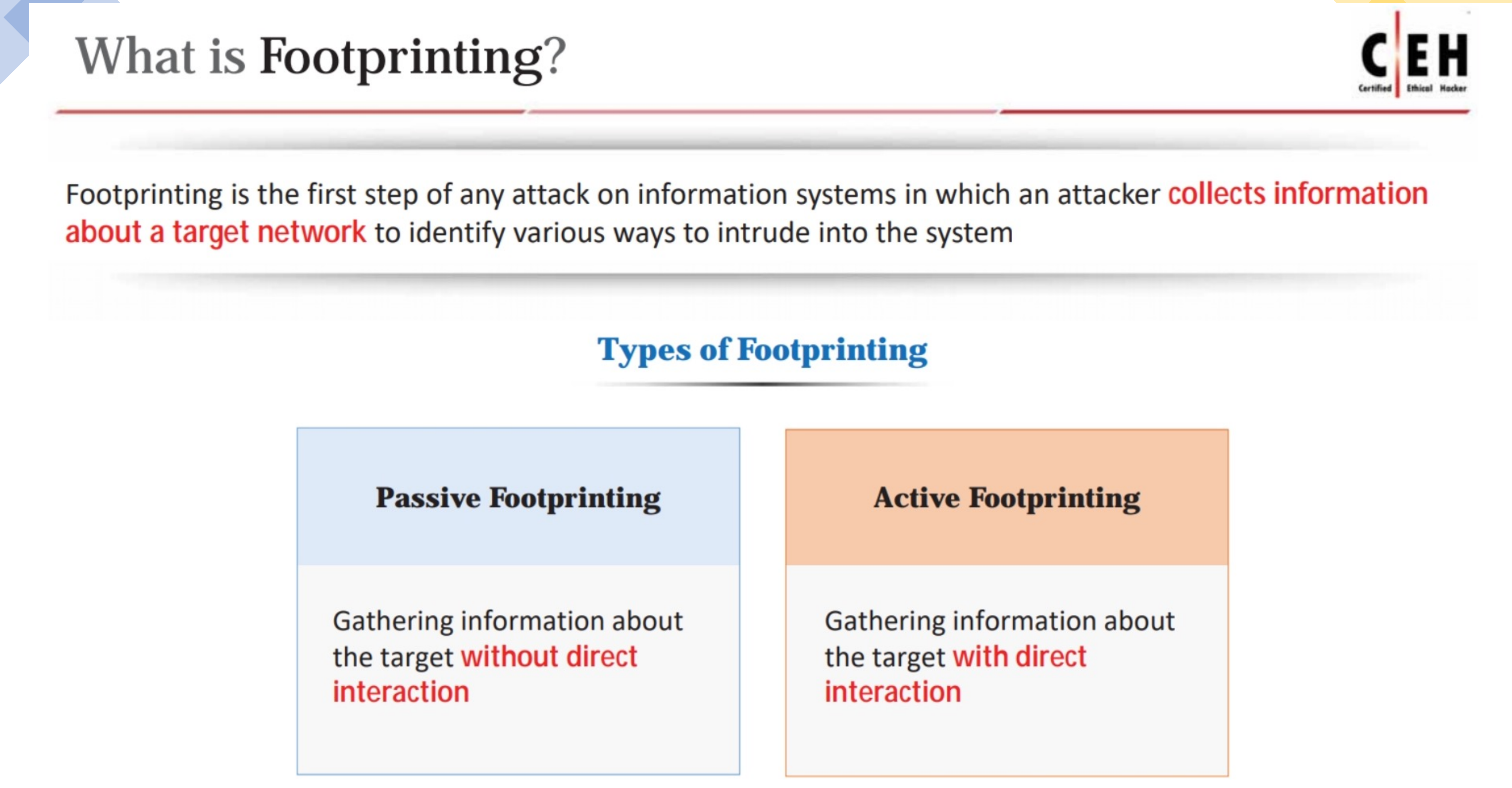
Escalating Privileges

Maintaining Access

- Executing Applications
- Hiding Files

Clearing Logs

- Covering Tracks



What is Footprinting?

Footprinting is the first step of any attack on information systems in which an attacker collects information about a target network to identify various ways to intrude into the system

Types of Footprinting

Passive Footprinting	Active Footprinting
Gathering information about the target without direct interaction	Gathering information about the target with direct interaction

Information Obtained in Footprinting

Organization information

- Employee details
- Telephone numbers
- Branch and location details
- Background of the organization
- Web technologies
- News articles, press releases, and related documents

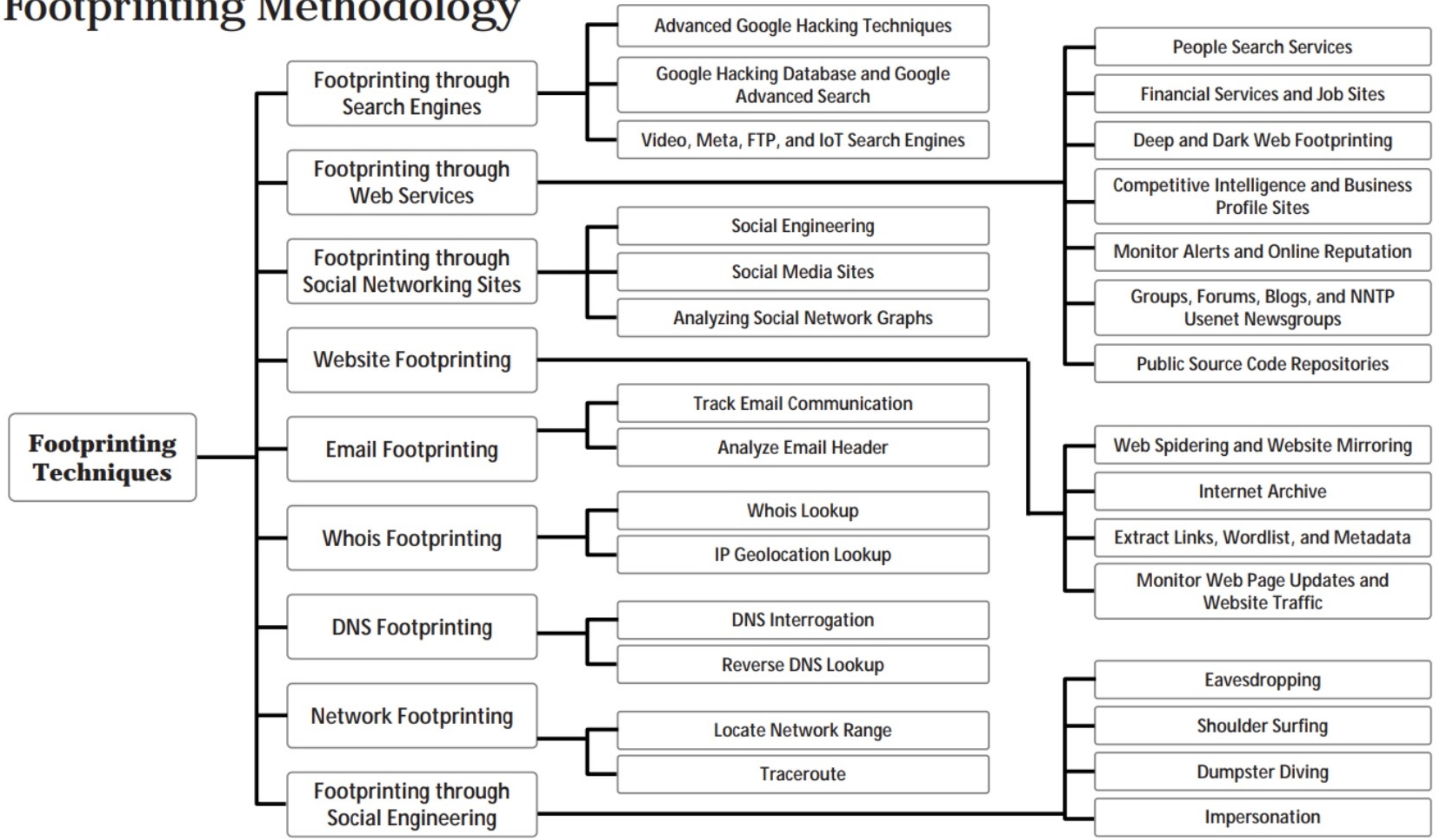
Network information

- Domain and sub-domains
- Network blocks
- Network topology, trusted routers, and firewalls
- IP addresses of the reachable systems
- Whois records
- DNS records

System information

- Web server OS
- Location of web servers
- Publicly available email addresses
- Usernames and passwords

Footprinting Methodology



- **Footprinting Techniques**
  - Footprinting through Search Engines
    - Advanced Google Hacking Techniques
    - Google Hacking Database and Google Advanced Search
    - Video, Meta, FTP, and IoT Search Engines
  - Footprinting through Web Services
    - People Search Services
    - Financial Services and Job Sites
    - Deep and Dark Web Footprinting
    - Competitive Intelligence and Business Profile Sites
    - Monitor Alerts and Online Reputation
    - Groups, Forums, Blogs, and NNTP Usenet Newsgroups
    - Public Source Code Repositories
  - Footprinting through Social Networking Sites
    - Social Engineering
    - Social Media Sites
    - Analyzing Social Network Graphs
  - Website Footprinting
    - Web Spidering and Website Mirroring
    - Internet Archive
    - Extract Links, Wordlist, and Metadata
    - Monitor Web Page Updates and Website Traffic
  - Email Footprinting
    - Track Email Communication
    - Analyze Email Header
  - Whois Footprinting
    - Whois Lookup
    - IP Geolocation Lookup
  - DNS Footprinting
    - DNS Interrogation
    - Reverse DNS Lookup
  - Network Footprinting
    - Locate Network Range
    - Traceroute
  - Footprinting through Social Engineering
    - Eavesdropping
    - Shoulder Surfing
    - Dumpster Diving
    - Impersonation

Footprinting Using Advanced Google Hacking Techniques

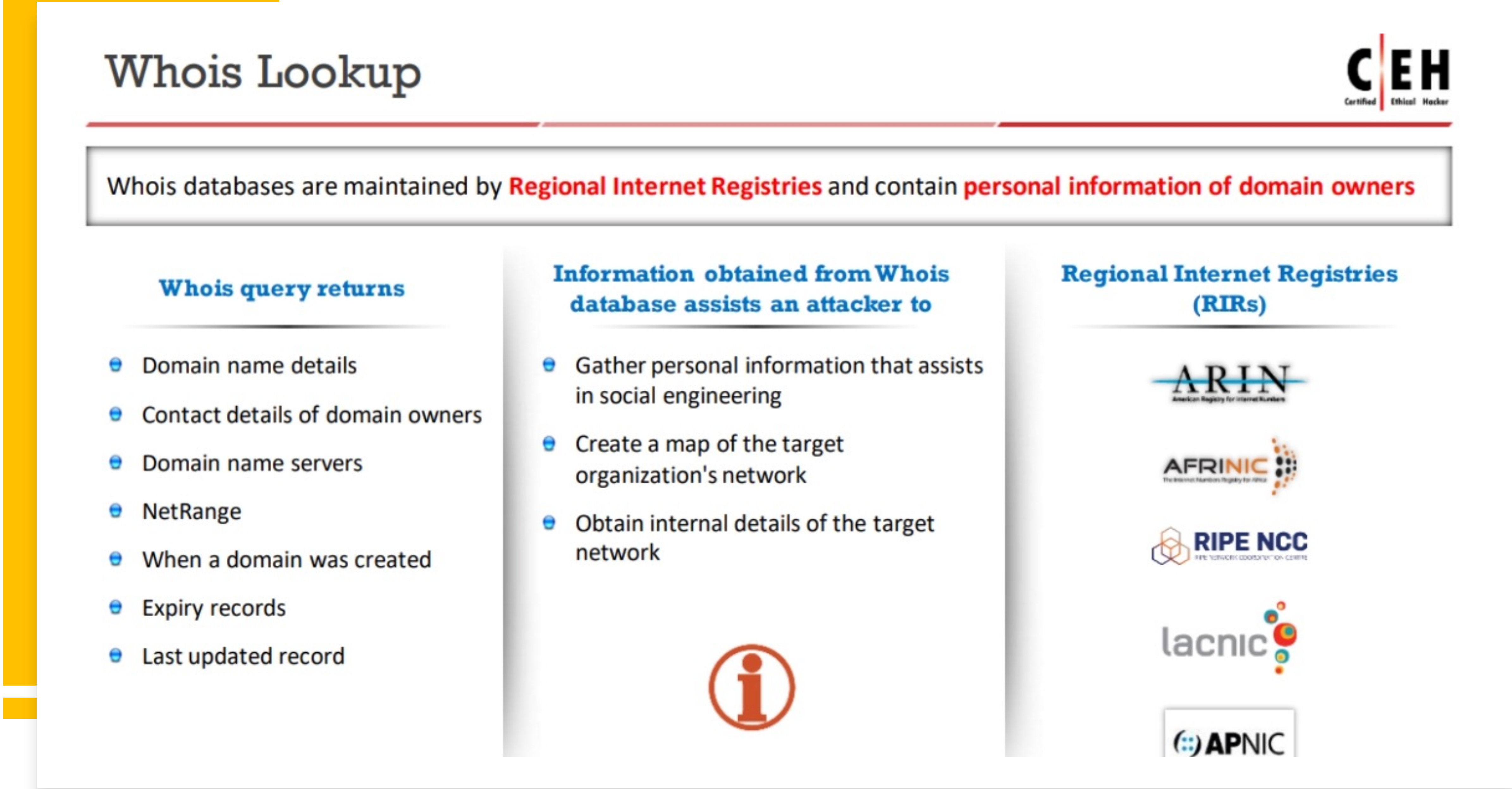
C|EH Certified Ethical Hacker

- Google hacking refers to the use of advanced Google search operators for **creating complex search queries** to extract sensitive or hidden information that helps attackers **find vulnerable targets**

Popular Google advanced search operators

Search Operator	Purpose
[cache:]	Displays the web pages stored in the Google cache
[link:]	Lists web pages that have links to the specified web page
[related:]	Lists web pages that are similar to the specified web page
[info:]	Presents some information that Google has about a particular web page
[site:]	Restricts the results to those websites in the given domain

Search Operator	Purpose
[allintitle:]	Restricts the results to those websites containing all the search keywords in the title
[intitle:]	Restricts the results to documents containing the search keyword in the title
[allinurl:]	Restricts the results to those containing all the search keywords in the URL
[inurl:]	Restricts the results to documents containing the search keyword in the URL
[location:]	Finds information for a specific location



Whois Lookup

CEH Certified Ethical Hacker

Whois databases are maintained by **Regional Internet Registries** and contain **personal information of domain owners**

Whois query returns

- Domain name details
- Contact details of domain owners
- Domain name servers
- NetRange
- When a domain was created
- Expiry records
- Last updated record

Information obtained from Whois database assists an attacker to

- Gather personal information that assists in social engineering
- Create a map of the target organization's network
- Obtain internal details of the target network

Regional Internet Registries (RIRs)

ARIN

AFRINIC

RIPE NCC

lacnic

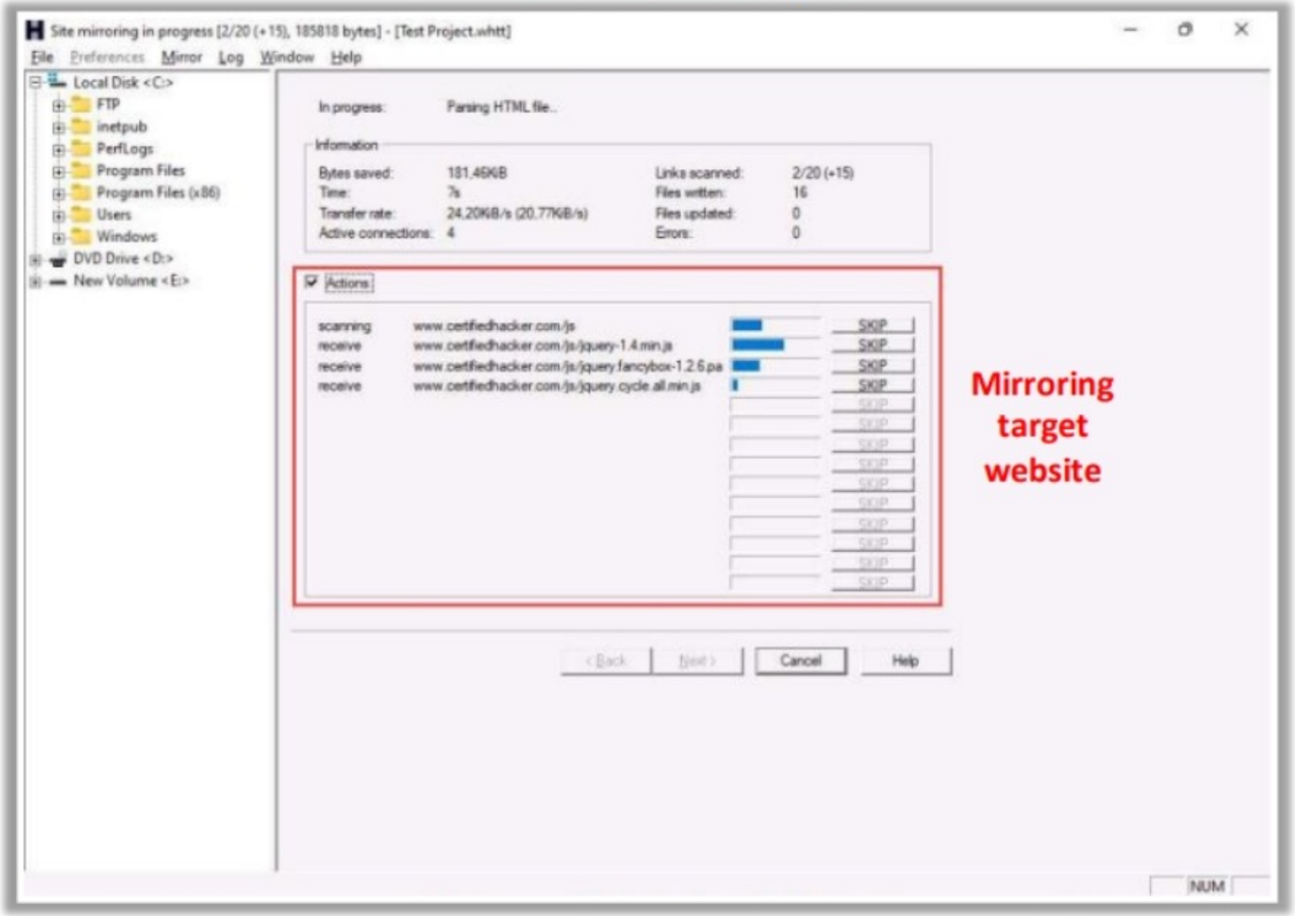
APNIC

Mirroring Entire Website

- Mirroring an entire website onto a local system enables an attacker to browse website offline; it also assists in finding **directory structure** and other valuable information from the mirrored copy without sending multiple requests to web server

- Web mirroring tools, such as HTTrack Web Site Copier, and Cyotek WebCopy, allow you to **download a website to a local directory**, recursively building all directories, HTML, images, flash, videos, and other files from the server to your computer

HTTrack Web Site Copier



In progress: Parsing HTML file..

Information

Bytes saved: 181.46KB
Time: 7s
Transfer rate: 24.20KB/s (20.77KB/s)
Active connections: 4
Links scanned: 2/20 (+15)
Files written: 16
Files updated: 0
Errors: 0

```
scanning   www.certifiedhacker.com/js
receive    www.certifiedhacker.com/js/jquery-1.4.min.js
receive    www.certifiedhacker.com/js/jquery.fancybox-1.2.6.pa
receive    www.certifiedhacker.com/js/jquery.cycle.all.min.js
```

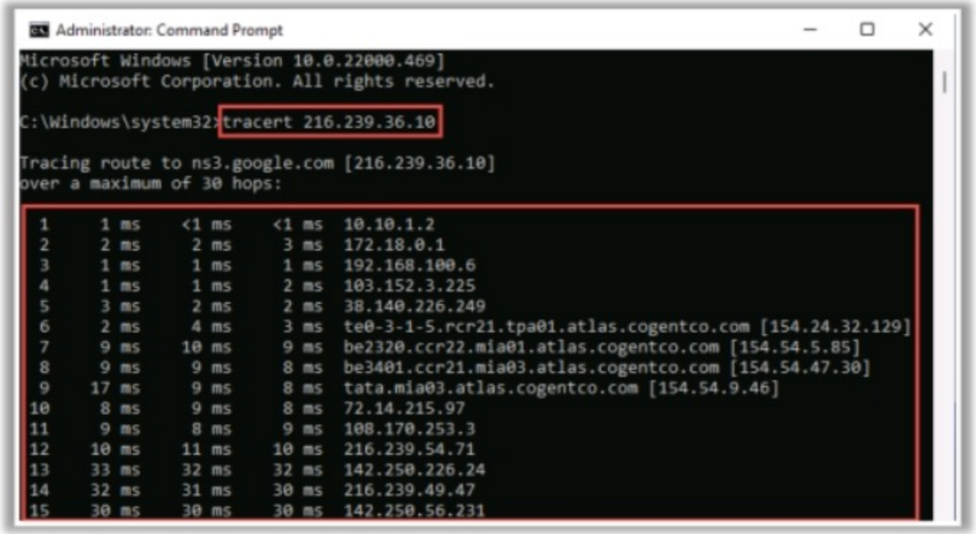
Mirroring target website

https://www.httrack.com

Traceroute

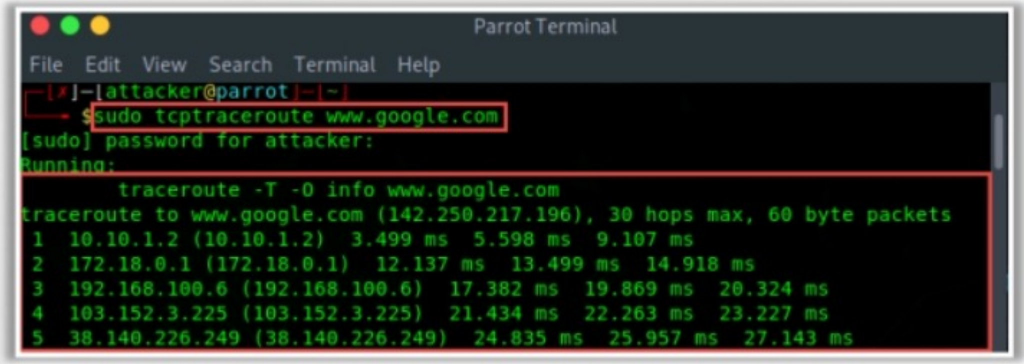
- Traceroute programs work on the concept of **ICMP protocol** and **use the TTL field in the header of ICMP packets** to discover the routers on the path to a target host

IMCP Traceroute



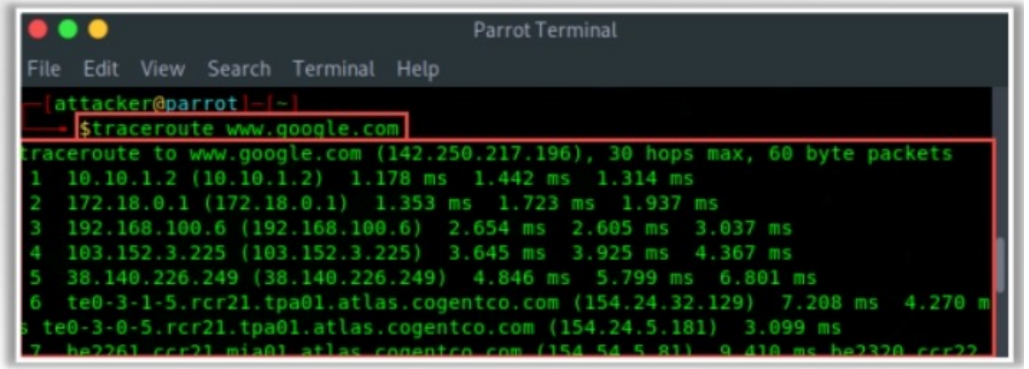
```
Microsoft Windows [Version 10.0.22000.469]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>tracert 216.239.36.10

Tracing route to ns3.google.com [216.239.36.10]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  10.10.1.2
  2     2 ms     2 ms     3 ms  172.18.0.1
  3     1 ms     1 ms     1 ms  192.168.100.6
  4     1 ms     1 ms     2 ms  103.152.3.225
  5     3 ms     2 ms     2 ms  38.140.226.249
  6     2 ms     4 ms     3 ms  te0-3-1-5.rcr21.tpa01.atlas.cogentco.com [154.24.32.129]
  7     9 ms    10 ms     9 ms  be2320.ccr22.mia01.atlas.cogentco.com [154.54.5.85]
  8     9 ms     9 ms     8 ms  be3401.ccr21.mia03.atlas.cogentco.com [154.54.47.30]
  9    17 ms     9 ms     8 ms  tata.mia03.atlas.cogentco.com [154.54.9.46]
 10     8 ms     9 ms     8 ms  72.14.215.97
 11     9 ms     8 ms     9 ms  108.170.253.3
 12    10 ms    11 ms    10 ms  216.239.54.71
 13    33 ms    32 ms    32 ms  142.250.226.24
 14    32 ms    31 ms    30 ms  216.239.49.47
 15    30 ms    30 ms    30 ms  142.250.56.231
```

TCP Traceroute

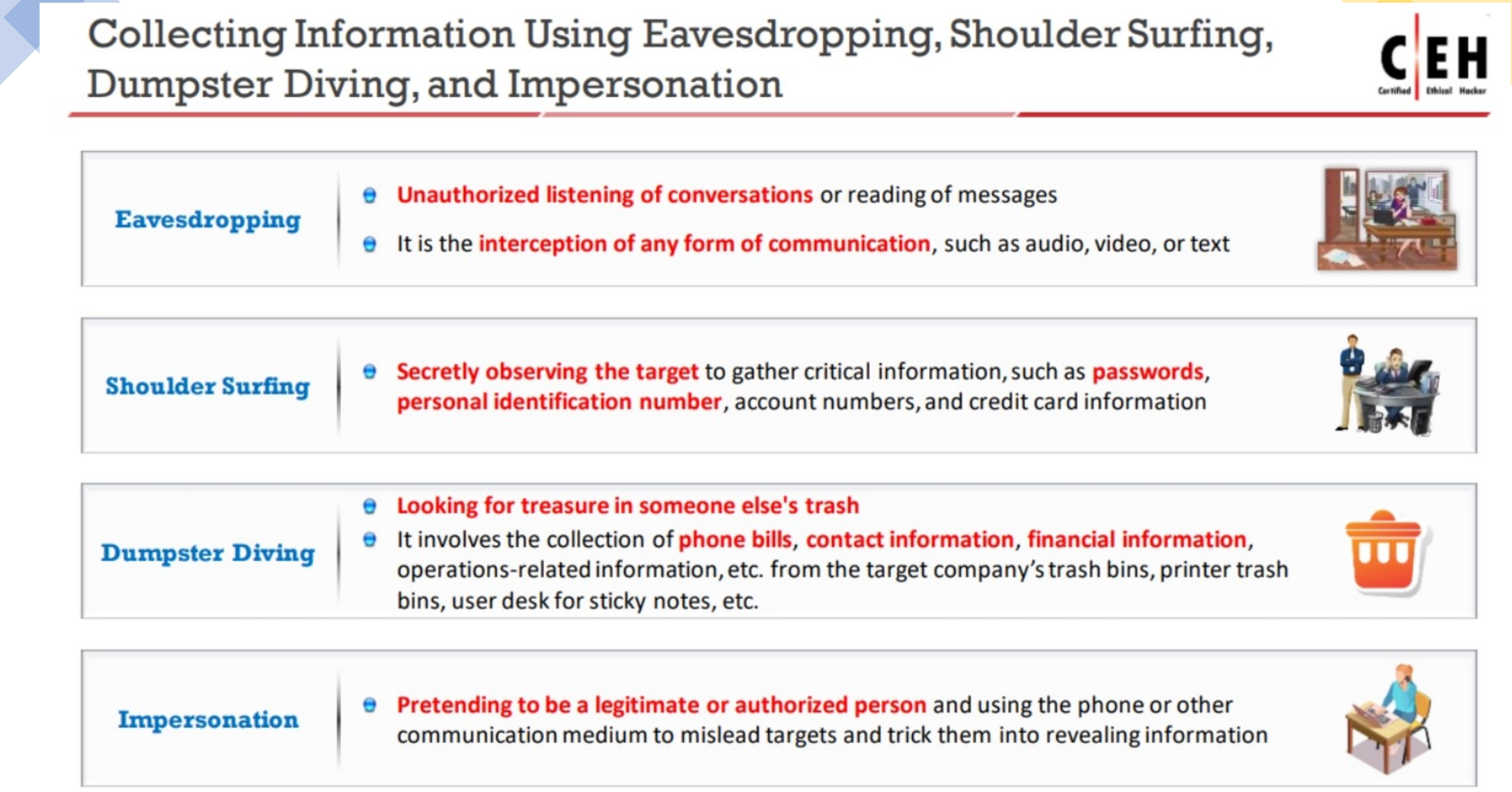


```
┌─[✗]─[attacker@parrot]─[~]
└──╼ $sudo tcptraceroute www.google.com
[sudo] password for attacker:
Running:
        traceroute -T -O info www.google.com
traceroute to www.google.com (142.250.217.196), 30 hops max, 60 byte packets
 1  10.10.1.2 (10.10.1.2)  3.499 ms  5.598 ms  9.107 ms
 2  172.18.0.1 (172.18.0.1)  12.137 ms  13.499 ms  14.918 ms
 3  192.168.100.6 (192.168.100.6)  17.382 ms  19.869 ms  20.324 ms
 4  103.152.3.225 (103.152.3.225)  21.434 ms  22.263 ms  23.227 ms
 5  38.140.226.249 (38.140.226.249)  24.835 ms  25.957 ms  27.143 ms
```

UDP Traceroute



```
┌─[attacker@parrot]─[~]
└──╼ $traceroute www.google.com
traceroute to www.google.com (142.250.217.196), 30 hops max, 60 byte packets
 1  10.10.1.2 (10.10.1.2)  1.178 ms  1.442 ms  1.314 ms
 2  172.18.0.1 (172.18.0.1)  1.353 ms  1.723 ms  1.937 ms
 3  192.168.100.6 (192.168.100.6)  2.654 ms  2.605 ms  3.037 ms
 4  103.152.3.225 (103.152.3.225)  3.645 ms  3.925 ms  4.367 ms
 5  38.140.226.249 (38.140.226.249)  4.846 ms  5.799 ms  6.801 ms
 6  te0-3-1-5.rcr21.tpa01.atlas.cogentco.com (154.24.32.129)  7.208 ms  4.270 m
s te0-3-0-5.rcr21.tpa01.atlas.cogentco.com (154.24.5.181)  3.099 ms
 7  be2261.ccr21.mia01.atlas.cogentco.com (154.54.5.81)  9.410 ms be2320.ccr22
```



Collecting Information Using Eavesdropping, Shoulder Surfing, Dumpster Diving, and Impersonation

Eavesdropping

- Unauthorized listening of conversations or reading of messages
- It is the interception of any form of communication, such as audio, video, or text

Shoulder Surfing

- Secretly observing the target to gather critical information, such as passwords, personal identification number, account numbers, and credit card information

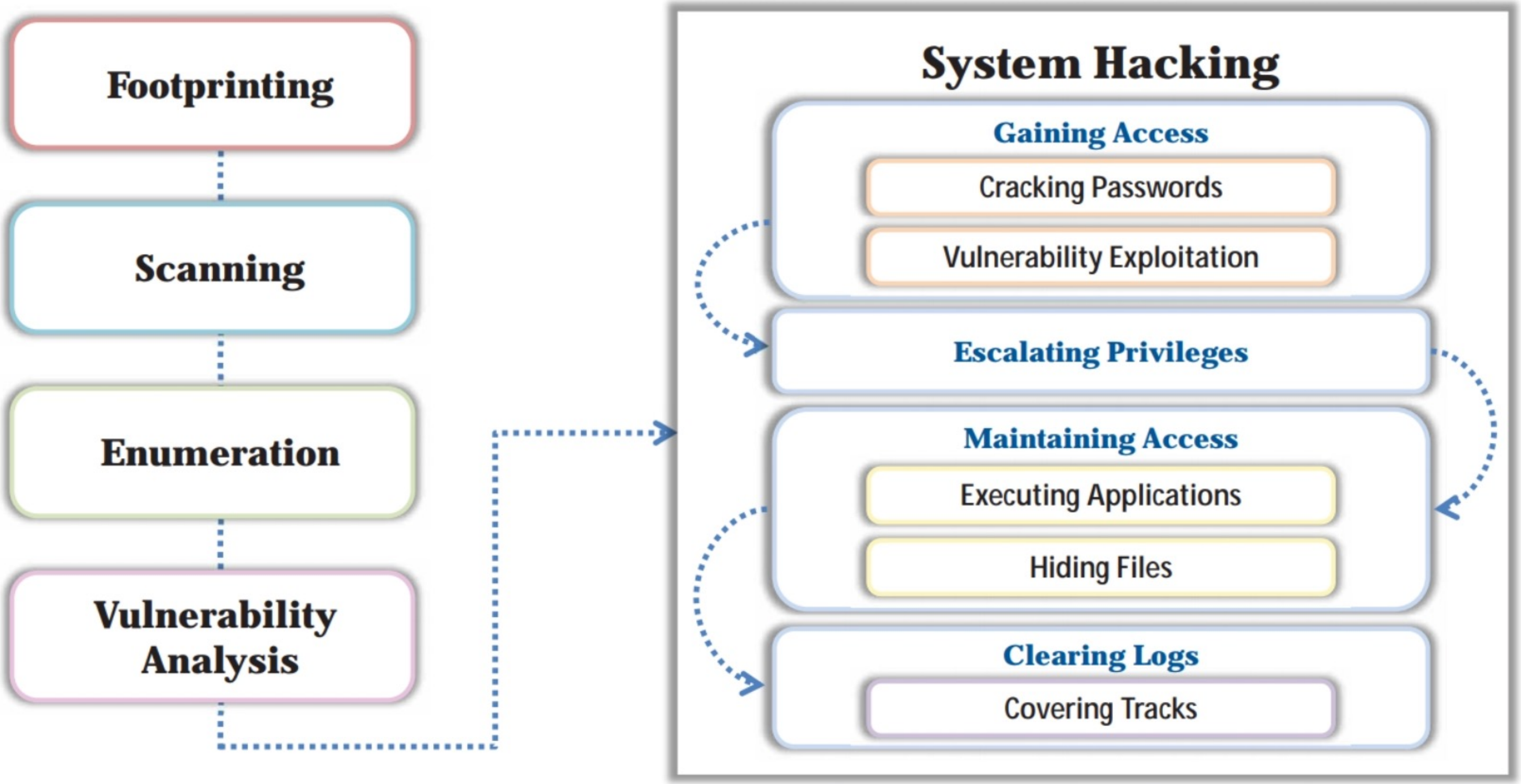
Dumpster Diving

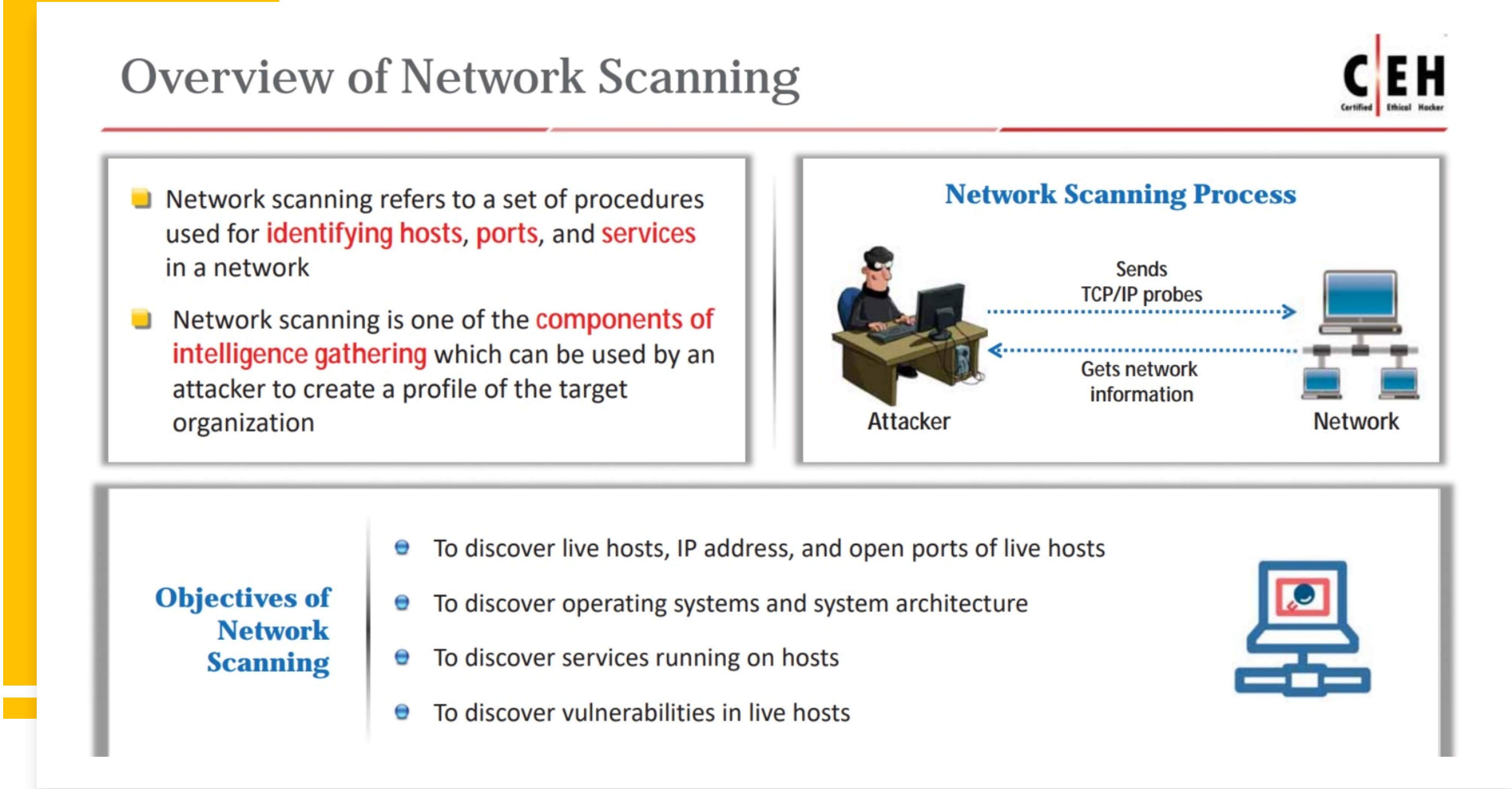
- Looking for treasure in someone else's trash
- It involves the collection of phone bills, contact information, financial information, operations-related information, etc. from the target company's trash bins, printer trash bins, user desk for sticky notes, etc.

Impersonation

- Pretending to be a legitimate or authorized person and using the phone or other communication medium to mislead targets and trick them into revealing information

CEH Hacking Methodology (CHM)





Overview of Network Scanning

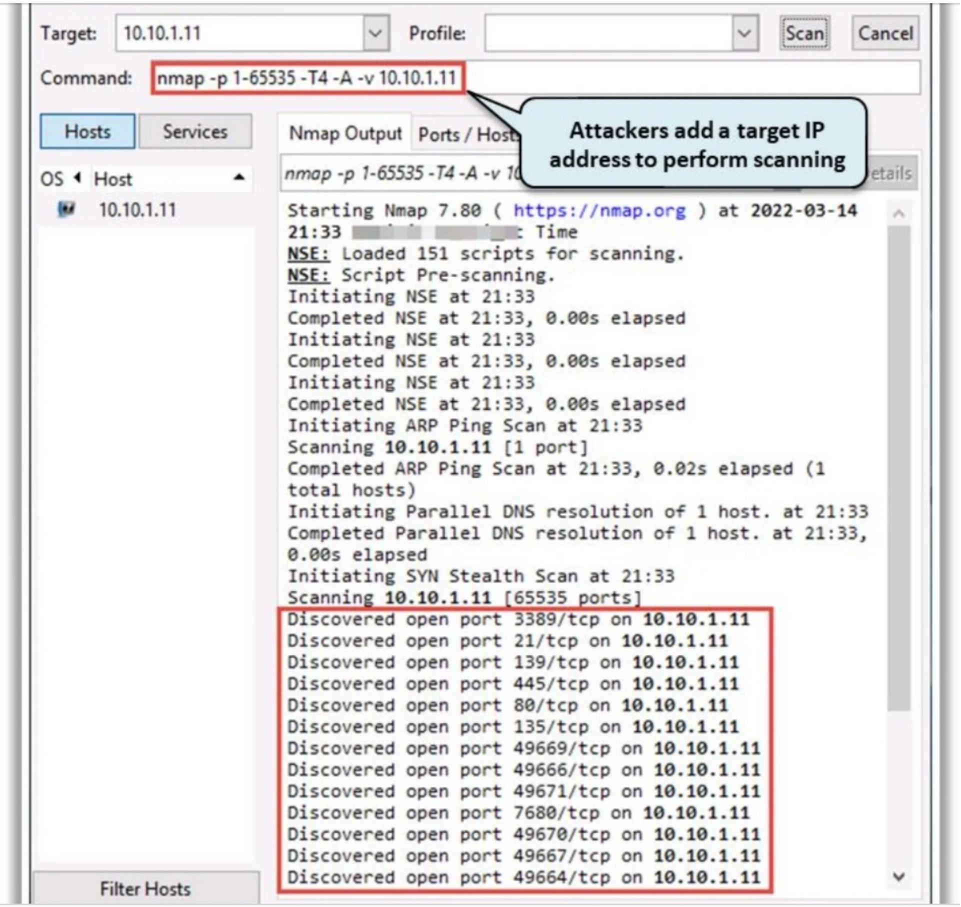
- Network scanning refers to a set of procedures used for identifying hosts, ports, and services in a network
- Network scanning is one of the components of intelligence gathering which can be used by an attacker to create a profile of the target organization

Network Scanning Process

Objectives of Network Scanning

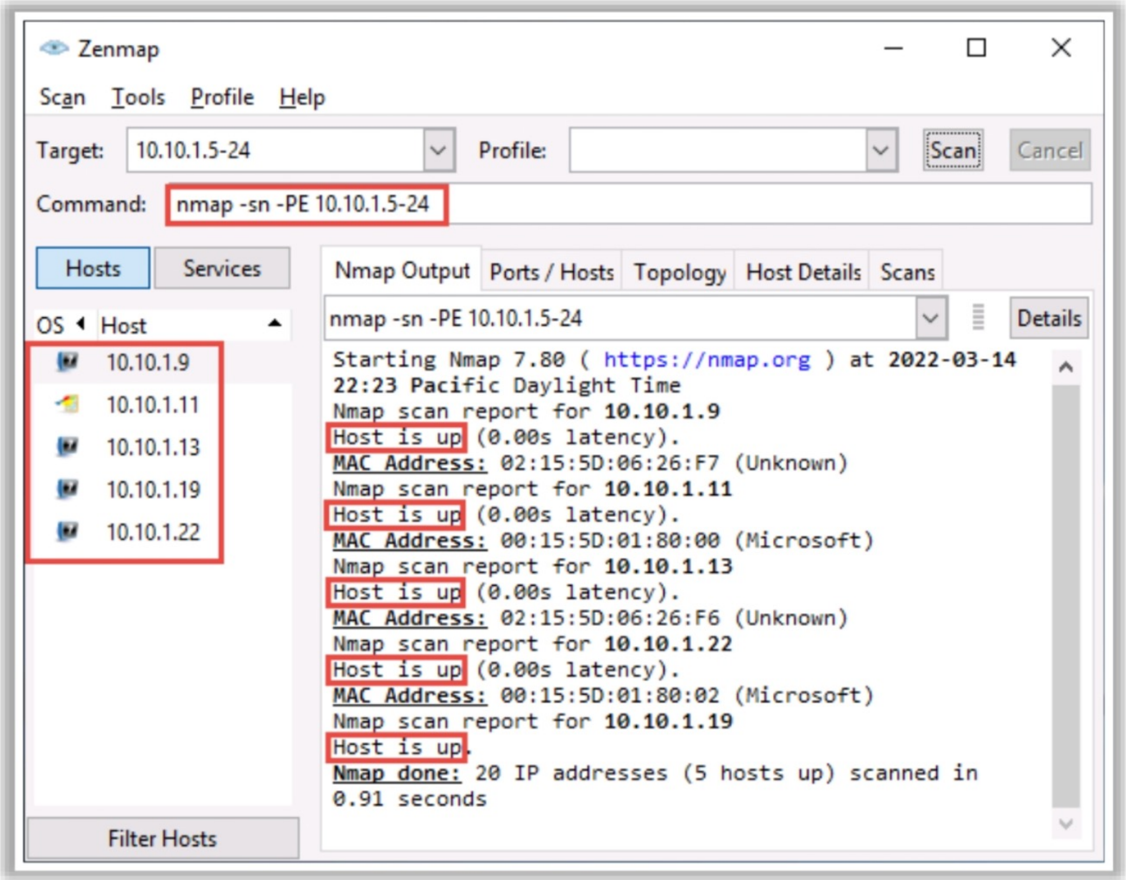
- To discover live hosts, IP address, and open ports of live hosts
- To discover operating systems and system architecture
- To discover services running on hosts
- To discover vulnerabilities in live hosts

Scan via NMAP



Attackers add a target IP address to perform scanning

```
nmap -p 1-65535 -T4 -A -v 10
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-14
21:33 [redacted] Time
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:33
Completed NSE at 21:33, 0.00s elapsed
Initiating NSE at 21:33
Completed NSE at 21:33, 0.00s elapsed
Initiating NSE at 21:33
Completed NSE at 21:33, 0.00s elapsed
Initiating ARP Ping Scan at 21:33
Scanning 10.10.1.11 [1 port]
Completed ARP Ping Scan at 21:33, 0.02s elapsed (1
total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:33
Completed Parallel DNS resolution of 1 host. at 21:33,
0.00s elapsed
Initiating SYN Stealth Scan at 21:33
Scanning 10.10.1.11 [65535 ports]
Discovered open port 3389/tcp on 10.10.1.11
Discovered open port 21/tcp on 10.10.1.11
Discovered open port 139/tcp on 10.10.1.11
Discovered open port 445/tcp on 10.10.1.11
Discovered open port 80/tcp on 10.10.1.11
Discovered open port 135/tcp on 10.10.1.11
Discovered open port 49669/tcp on 10.10.1.11
Discovered open port 49666/tcp on 10.10.1.11
Discovered open port 49671/tcp on 10.10.1.11
Discovered open port 7680/tcp on 10.10.1.11
Discovered open port 49670/tcp on 10.10.1.11
Discovered open port 49667/tcp on 10.10.1.11
Discovered open port 49664/tcp on 10.10.1.11
```



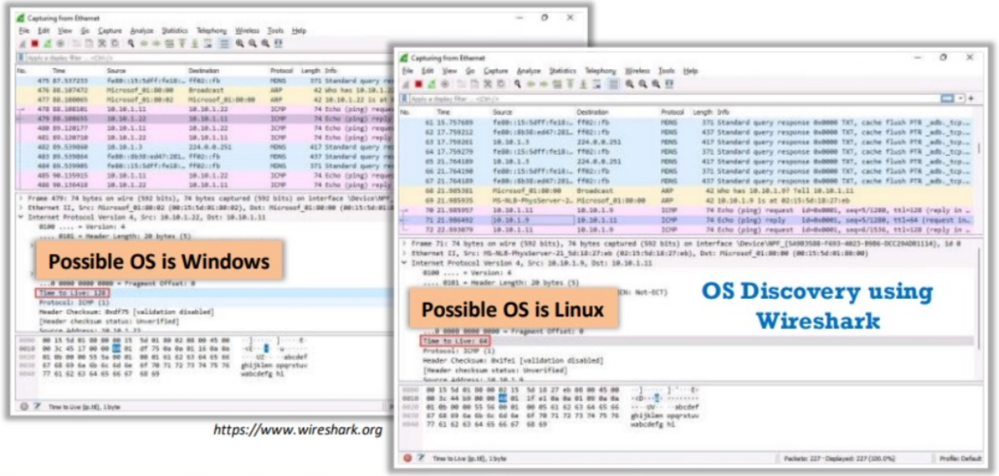
```
nmap -sn -PE 10.10.1.5-24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-14
22:23 Pacific Daylight Time
Nmap scan report for 10.10.1.9
Host is up (0.00s latency).
MAC Address: 02:15:5D:06:26:F7 (Unknown)
Nmap scan report for 10.10.1.11
Host is up (0.00s latency).
MAC Address: 00:15:5D:01:80:00 (Microsoft)
Nmap scan report for 10.10.1.13
Host is up (0.00s latency).
MAC Address: 02:15:5D:06:26:F6 (Unknown)
Nmap scan report for 10.10.1.22
Host is up (0.00s latency).
MAC Address: 00:15:5D:01:80:02 (Microsoft)
Nmap scan report for 10.10.1.19
Host is up.
Nmap done: 20 IP addresses (5 hosts up) scanned in
0.91 seconds
```

Figure 3.23: Ping Sweep output using Zenmap

Scan via NMAP

How to Identify Target System OS

- Attackers can identify the OS running on the target machine by looking at the **Time To Live (TTL)** and **TCP window size** in the IP header of the first packet in a TCP session
- **Sniff/capture the response** generated from the target machine using packet-sniffing tools like Wireshark and observe the TTL and TCP window size fields



Possible OS is Windows

Possible OS is Linux

OS Discovery using Wireshark

https://www.wireshark.org

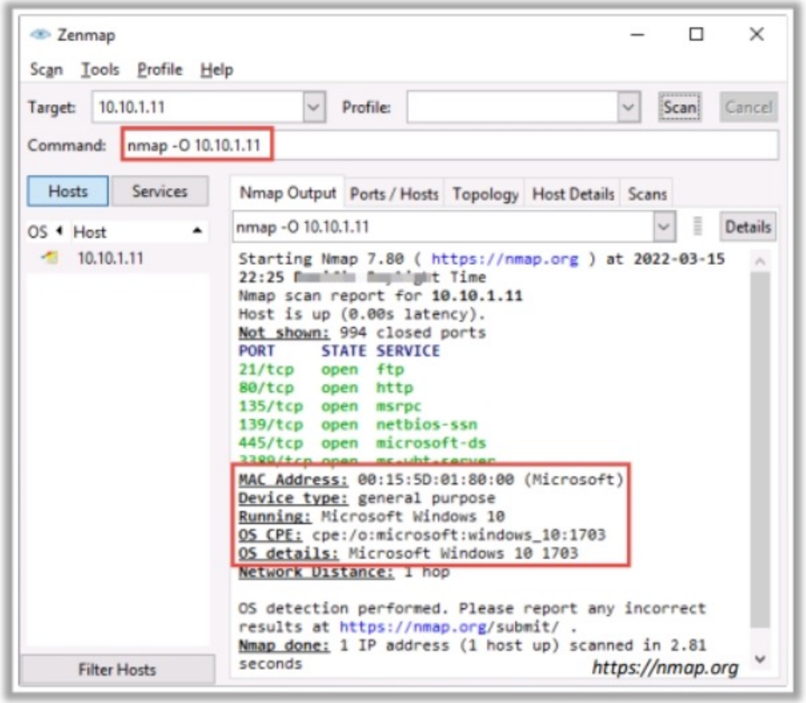
Window size values for OS

Operating System	Time To Live	TCP Window Size
Linux	64	5840
FreeBSD	64	65535
OpenBSD	255	16384
Windows	128	65,535 bytes to 1 Gigabyte
Cisco Routers	255	4128
Solaris	255	8760
AIX	255	16384

IDS and firewall detection

OS Discovery using Nmap

- In **Nmap**, the **-O** option is used to perform OS discovery, providing OS details of the target machine



Target: 10.10.1.11

Profile:

Command: nmap -O 10.10.1.11

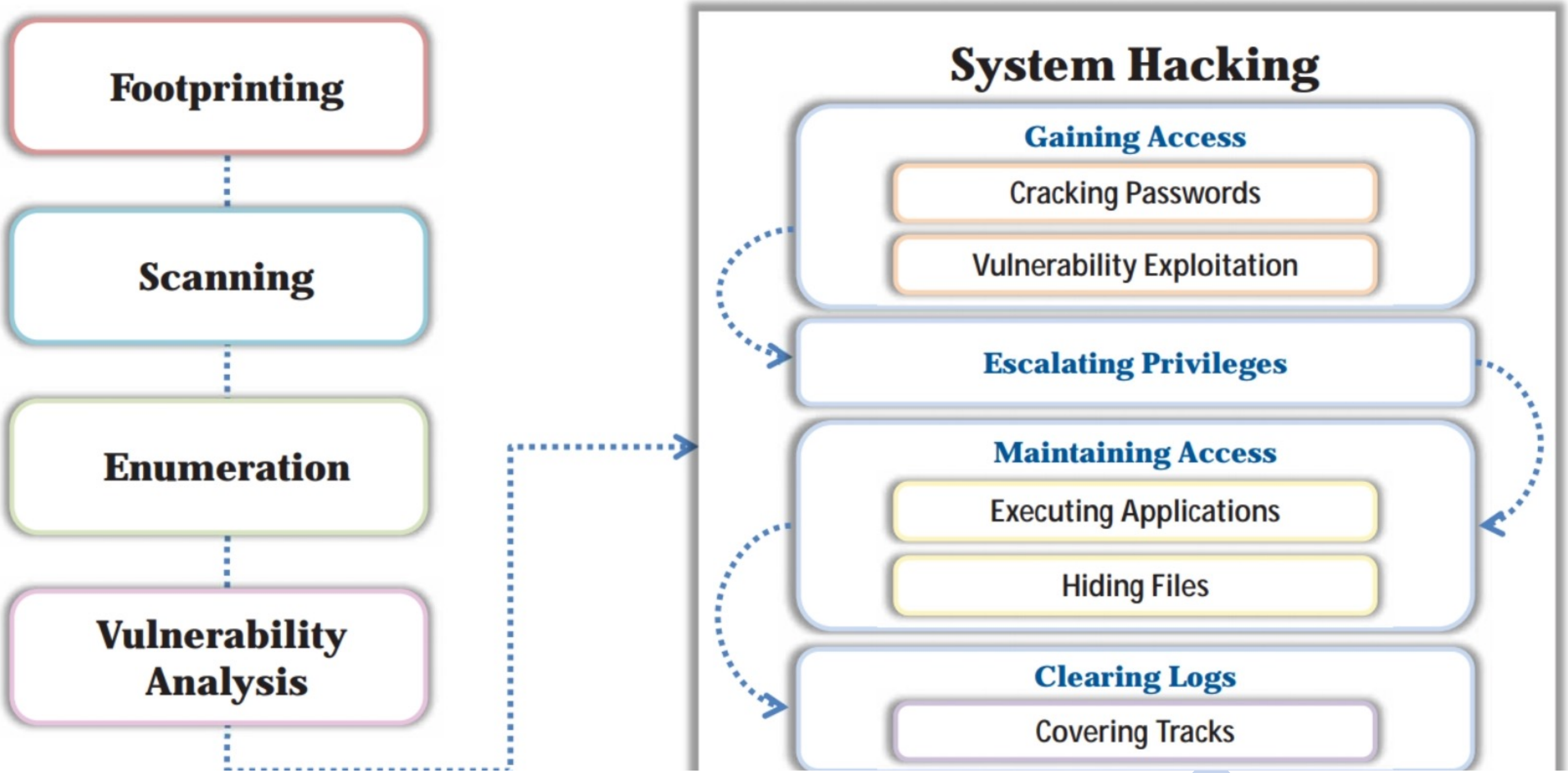
10.10.1.11

nmap -O 10.10.1.11

```
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-15
22:25 [redacted] Time
Nmap scan report for 10.10.1.11
Host is up (0.00s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:01:80:00 (Microsoft)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1703
OS details: Microsoft Windows 10 1703
Network Distance: 1 hop

OS detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.81
seconds
```

https://nmap.org

CEH Hacking Methodology (CHM)



Footprinting

Scanning

Enumeration

Vulnerability Analysis

System Hacking

Gaining Access

- Cracking Passwords
- Vulnerability Exploitation

Escalating Privileges

Maintaining Access

- Executing Applications
- Hiding Files

Clearing Logs

- Covering Tracks

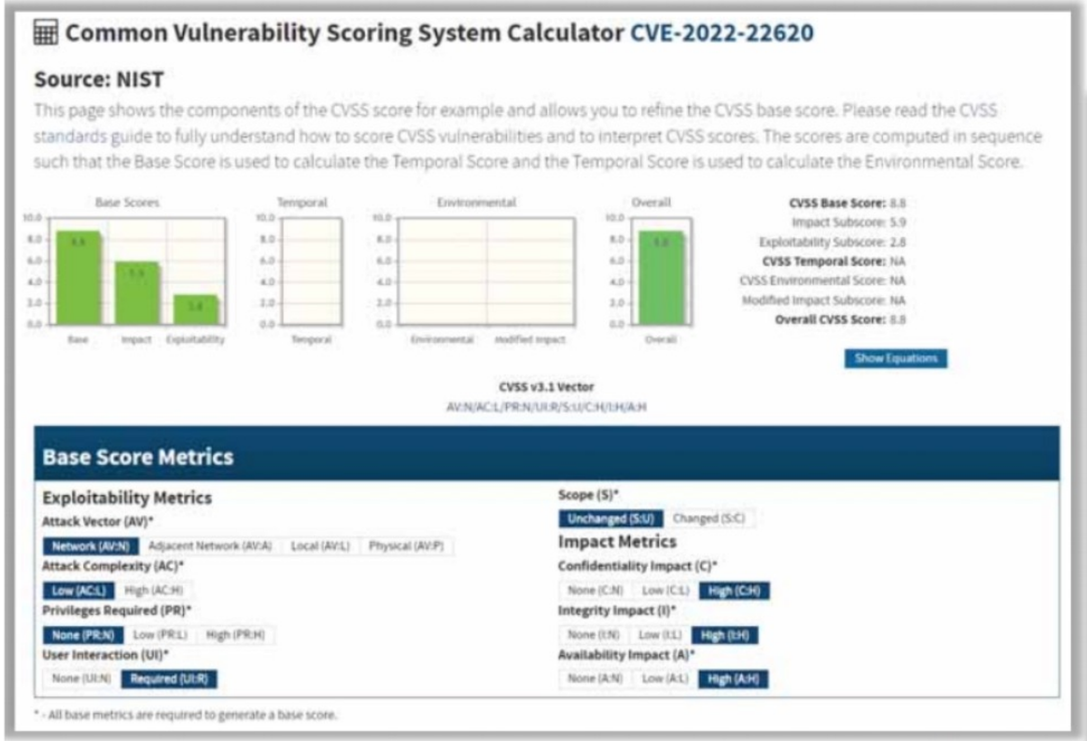
Examples of Vulnerabilities

Technological Vulnerabilities	Description
TCP/IP protocol vulnerabilities	HTTP, FTP, ICMP, SNMP, SMTP are inherently insecure
Operating System vulnerabilities	An OS can be vulnerable because: - It is inherently insecure - It is not patched with the latest updates
Network Device Vulnerabilities	Various network devices such as routers, firewall, and switches can be vulnerable due to: - Lack of password protection - Lack of authentication - Insecure routing protocols - Firewall vulnerabilities

Configuration Vulnerabilities	Description
User account vulnerabilities	Originating from the insecure transmission of user account details such as usernames and passwords, over the network
System account vulnerabilities	Originating from setting of weak passwords for system accounts
Internet service misconfiguration	Misconfiguring internet services can pose serious security risks. For example, enabling JavaScript and misconfiguring IIS, Apache, FTP, and Terminal services, can create security vulnerabilities in the network
Default password and settings	Leaving the network devices/products with their default passwords and settings
Network device misconfiguration	Misconfiguring the network device

Vulnerability Scoring Systems and Databases

Common Vulnerability Scoring System (CVSS)



Common Vulnerability Scoring System Calculator CVE-2022-22620

Source: NIST

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

CVSS Base Score: 8.8
Impact Subscore: 5.9
Exploitability Subscore: 2.8
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 8.8

CVSS v3.1 Vector
AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
[✓ Network (AV:N)] Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

Attack Complexity (AC)*
[✓ Low (AC:L)] High (AC:H)

Privileges Required (PR)*
[✓ None (PR:N)] Low (PR:L) High (PR:H)

User Interaction (UI)*
None (UI:N) [✓ Required (UI:R)]

Scope (S)*
[✓ Unchanged (S:U)] Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*
None (C:N) Low (C:L) [✓ High (C:H)]

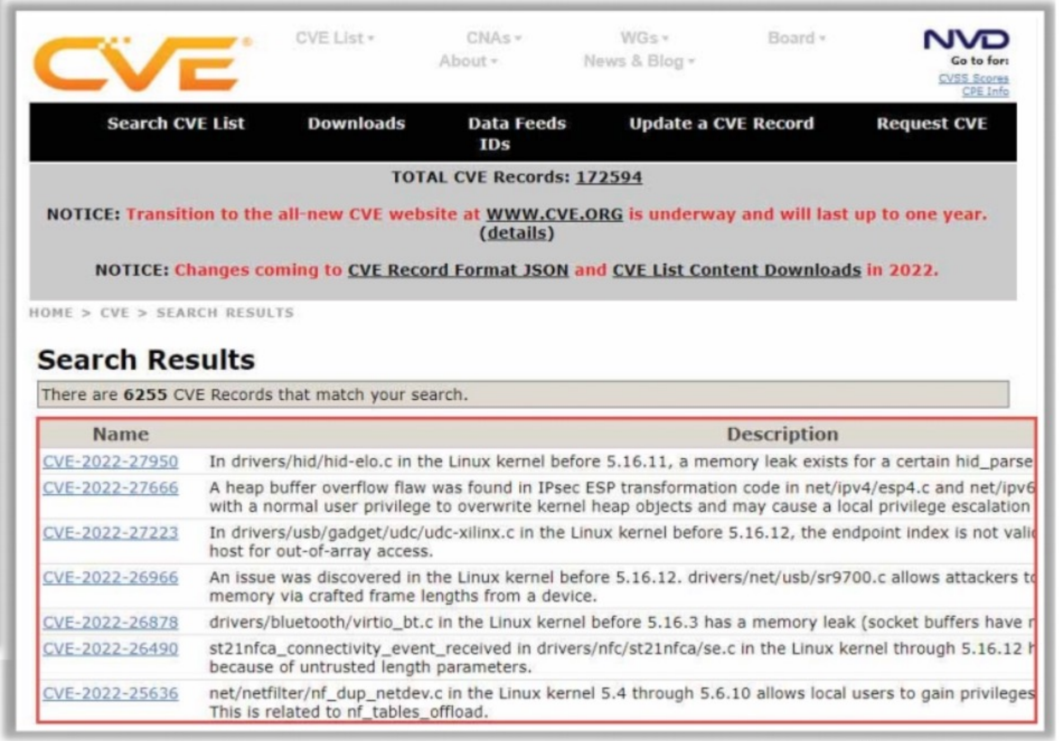
Integrity Impact (I)*
None (I:N) Low (I:L) [✓ High (I:H)]

Availability Impact (A)*
None (A:N) Low (A:L) [✓ High (A:H)]

* - All base metrics are required to generate a base score.

https://nvd.nist.gov

Common Vulnerabilities and Exposures (CVE)



TOTAL CVE Records: 172594

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG is underway and will last up to one year. (details)

NOTICE: Changes coming to CVE Record Format JSON and CVE List Content Downloads in 2022.

HOME > CVE > SEARCH RESULTS

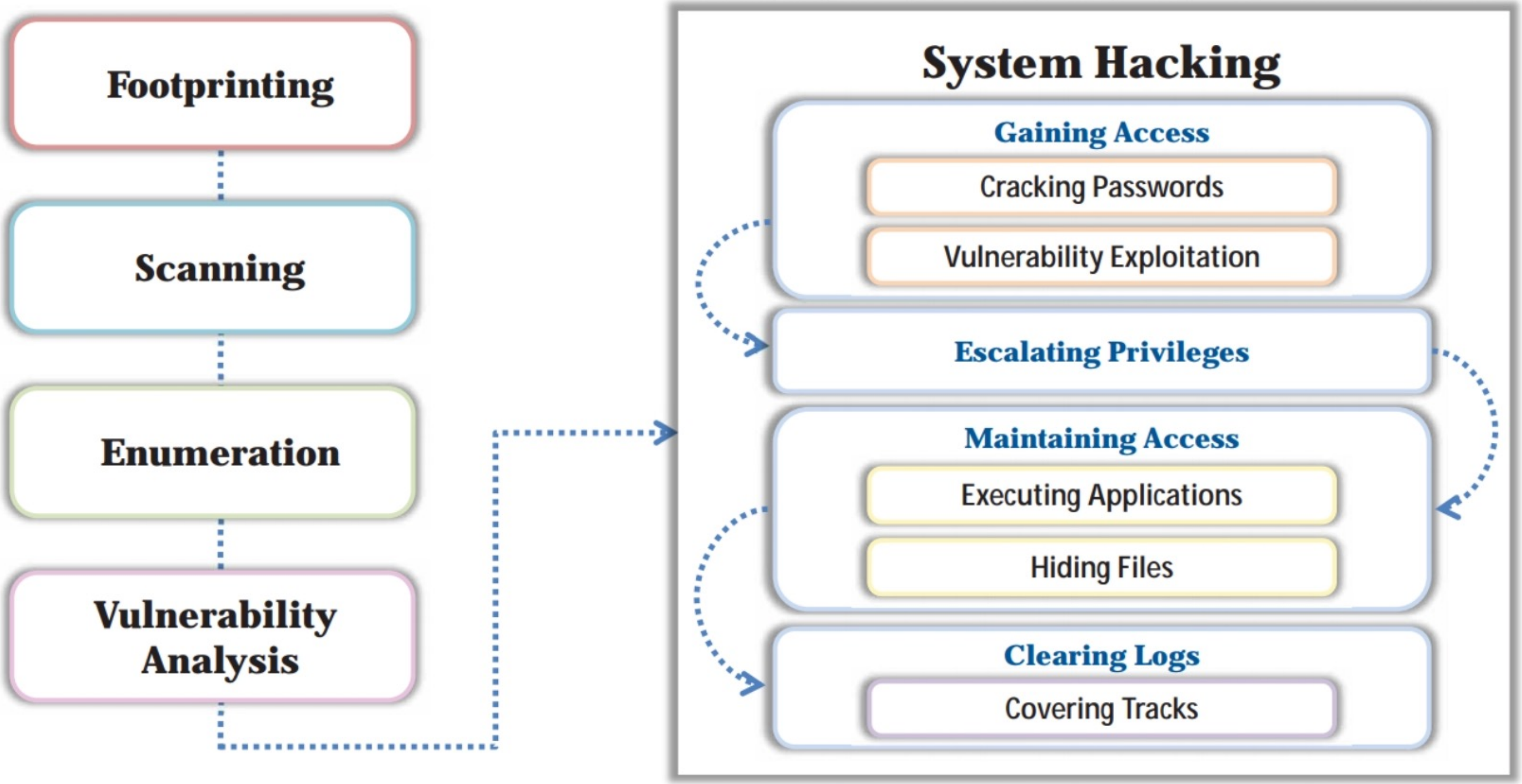
Search Results

There are **6255** CVE Records that match your search.

Name	Description
CVE-2022-27950	In drivers/hid/hid-elo.c in the Linux kernel before 5.16.11, a memory leak exists for a certain hid_parse
CVE-2022-27666	A heap buffer overflow flaw was found in IPsec ESP transformation code in net/ipv4/esp4.c and net/ipv6 with a normal user privilege to overwrite kernel heap objects and may cause a local privilege escalation
CVE-2022-27223	In drivers/usb/gadget/udc/udc-xilinx.c in the Linux kernel before 5.16.12, the endpoint index is not vali host for out-of-array access.
CVE-2022-26966	An issue was discovered in the Linux kernel before 5.16.12. drivers/net/usb/sr9700.c allows attackers to memory via crafted frame lengths from a device.
CVE-2022-26878	drivers/bluetooth/virtio_bt.c in the Linux kernel before 5.16.3 has a memory leak (socket buffers have r
CVE-2022-26490	st21nfca_connectivity_event_received in drivers/nfc/st21nfca/se.c in the Linux kernel through 5.16.12 h because of untrusted length parameters.
CVE-2022-25636	net/netfilter/nf_dup_netdev.c in the Linux kernel 5.4 through 5.6.10 allows local users to gain privileges This is related to nf_tables_offload.

https://www.cve.org

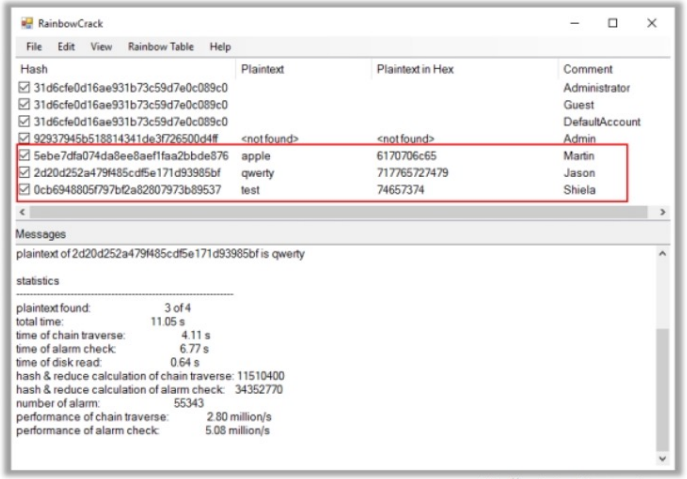
CEH Hacking Methodology (CHM)



Password-Cracking Tools

RainbowCrack

RainbowCrack cracks hashes with **rainbow tables**. It uses a **time-memory tradeoff** algorithm to crack hashes



```
Hash                                 Plaintext     Plaintext in Hex   Comment
☑ 31d6cfe0d16ae931b73c59d7e0c089c0                                    Administrator
☑ 31d6cfe0d16ae931b73c59d7e0c089c0                                    Guest
☑ 31d6cfe0d16ae931b73c59d7e0c089c0                                    DefaultAccount
☑ 92937945b518814341de3f726500d4ff   <not found>   <not found>        Admin
☑ 5ebe7dfa074da8ee8aef1faa2bbde876   apple         6170706c65         Martin
☑ 2d20d252a479f485cdf5e171d93985bf   qwerty        717765727479       Jason
☑ 0cb6948805f797bf2a82807973b89537   test          74657374           Shiela

Messages
plaintext of 2d20d252a479f485cdf5e171d93985bf is qwerty

statistics
-------------------------------------------------------
plaintext found:                    3 of 4
total time:                       11.05 s
time of chain traverse:             4.11 s
time of alarm check:                6.77 s
time of disk read:                0.64 s
hash & reduce calculation of chain traverse: 11510400
hash & reduce calculation of alarm check:   34352770
number of alarm:                  55343
performance of chain traverse:          2.80 million/s
performance of alarm check:            5.08 million/s
```

http://project-rainbowcrack.com

John the Ripper
https://www.openwall.com

hashcat
https://hashcat.net

THC-Hydra
https://github.com

Medusa
http://foofus.net

Secure Shell Bruteforcer
https://github.com

Password Cracking

- Password cracking techniques are used to **recover passwords** from computer systems
- Attackers use password cracking techniques to **gain unauthorized access** to vulnerable systems
- Most of the password cracking techniques are successful because of weak or easily **guessable passwords**

Types of Password Attacks

Non-Electronic Attacks

The attacker **does not need technical knowledge** to crack the password, hence it is known as a non-technical attack

- Shoulder Surfing
- Social Engineering
- Dumpster Diving

Active Online Attacks

The attacker performs password cracking by **directly communicating** with the victim's machine

- Dictionary, Brute Forcing, and Rule-based Attack
- Hash Injection Attack/Mask Attack
- LLMNR/NBT-NS Poisoning
- Trojan/Spyware/Keyloggers
- Password Guessing/Spraying
- Internal Monologue Attack
- Cracking Kerberos Passwords

Passive Online Attacks

The attacker performs password cracking **without communicating** with the authorizing party

- Wire Sniffing
- Man-in-the-Middle Attack
- Replay Attack

Offline Attacks

The attacker copies the target's **password file** and then tries to crack passwords on his own system at a different location

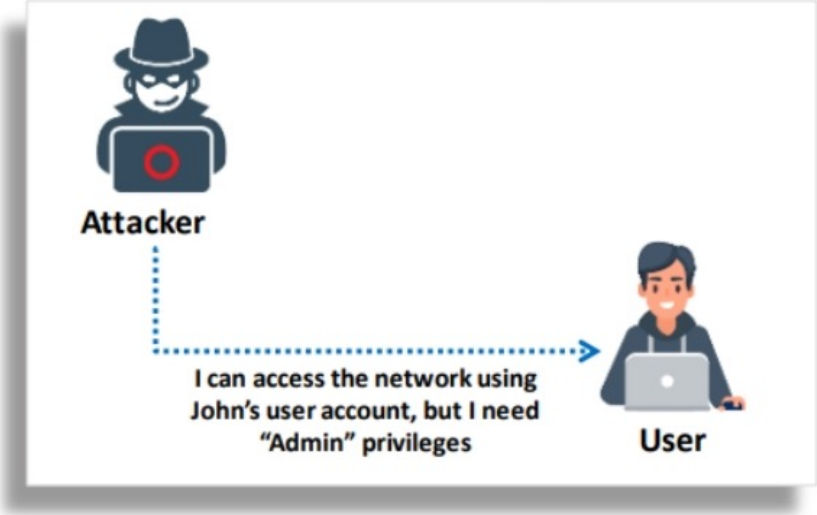
- Rainbow Table Attack (Pre-Computed Hashes)
- Distributed Network Attack

Privilege Escalation

- An attacker can gain access to the network using a **non-admin user account** and the next step would be to gain administrative privileges
- The attacker performs a privilege escalation attack that takes advantage of **design flaws**, **programming errors**, **bugs**, and **configuration oversights** in the OS and software application to gain administrative access to the network and its associated applications
- These privileges allow the attacker to **view critical/sensitive information**, delete files, or install malicious programs such as viruses, Trojans, or worms

Types of Privilege Escalation

1. **Horizontal Privilege Escalation**
   - Refers to acquiring the same privileges that have already been granted, by assuming the identity of another user with the same privileges
2. **Vertical Privilege Escalation**
   - Refers to gaining higher privileges than those existing

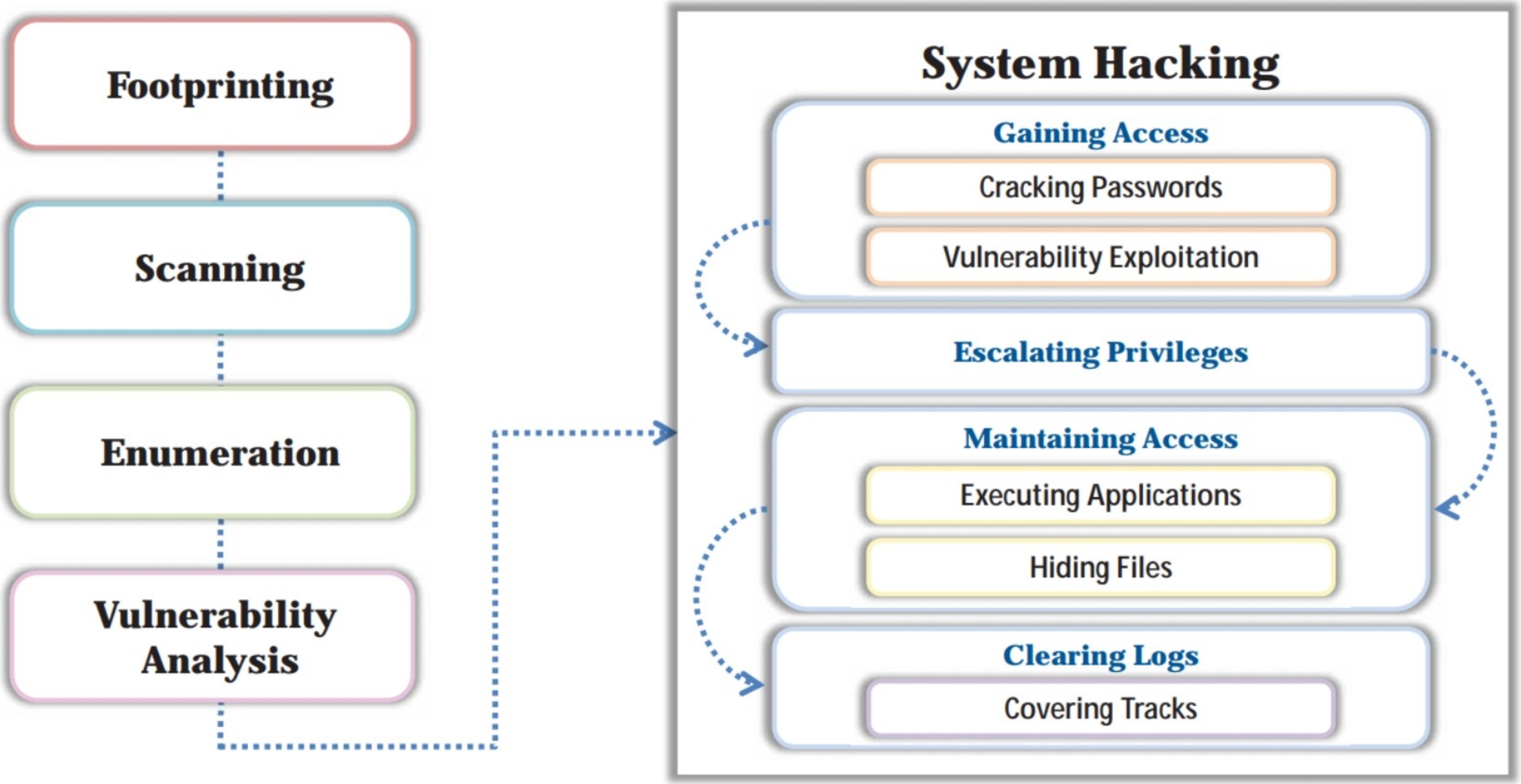


Attacker

I can access the network using John's user account, but I need "Admin" privileges

User

CEH Hacking Methodology (CHM)



Plateformes de CTF

- RootMe
- HackTheBox
- TryHackMe
- Hack Me

Merci pour votre attention

Sources

- Support de cours CEH, EC-council V12