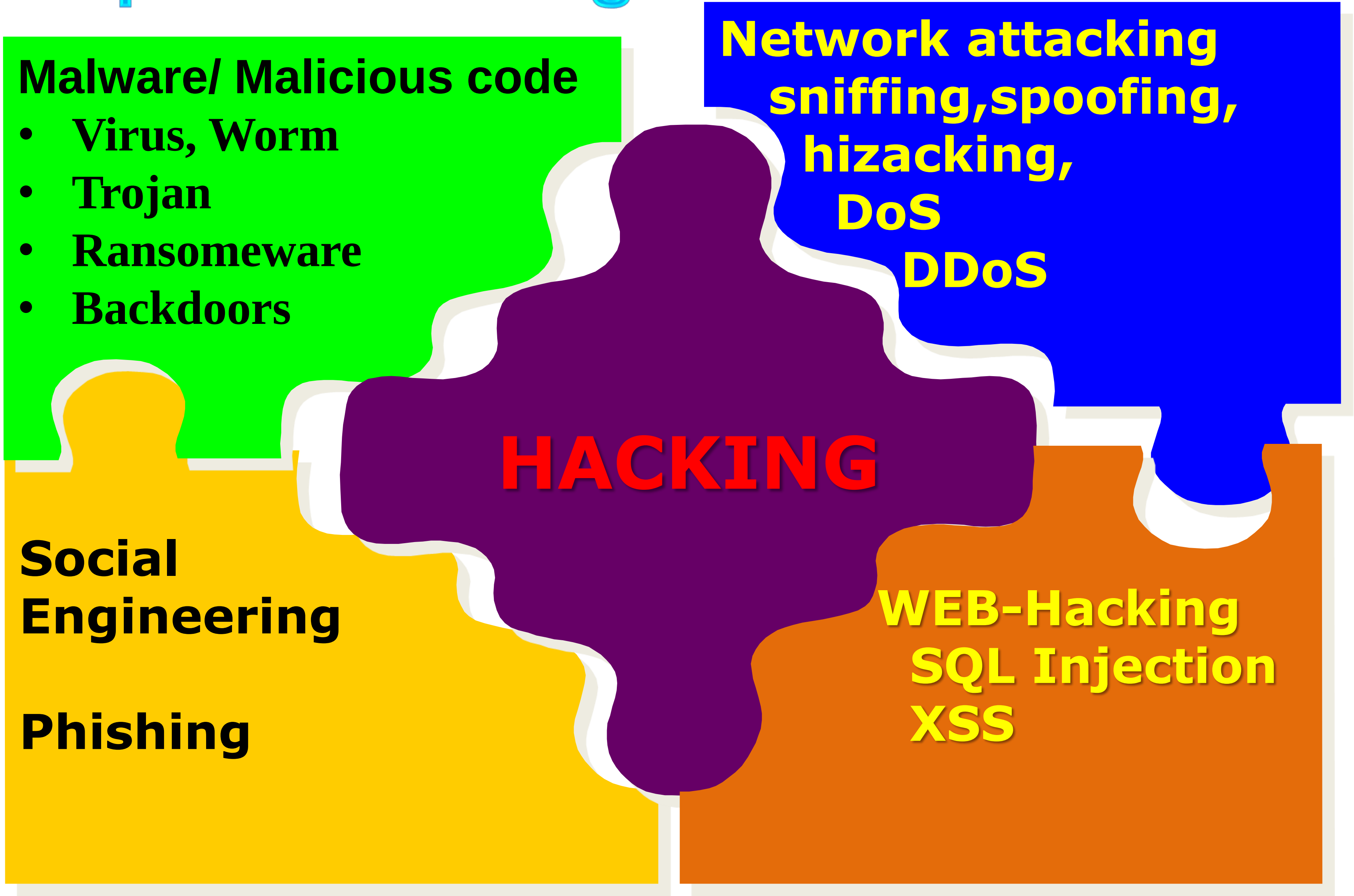
Phases of Hacking

Map of attacking



Malware/ Malicious code

- Virus, Worm
- Trojan
- Ransomeware
- Backdoors

Network attacking
sniffing,spoofing,
hizacking,
DoS
DDoS

HACKING

Social
Engineering

Phishing

WEB-Hacking
SQL Injection
XSS

Cyber attacking targets just on target’s vulnerability

Various threats occur in all Information system sections , as long as the vulnerability exists

vulnerability?

Vulnerability?

⇒Weak port of target information system

⇒ Weak port of software program logics

=> Weak port of networking

Vulnerability?

Weak point of information from the security sight

- On program logics
- On parameters
- On options
- On sharing methods
- On HW,NW,protocol

Phases of Hacking

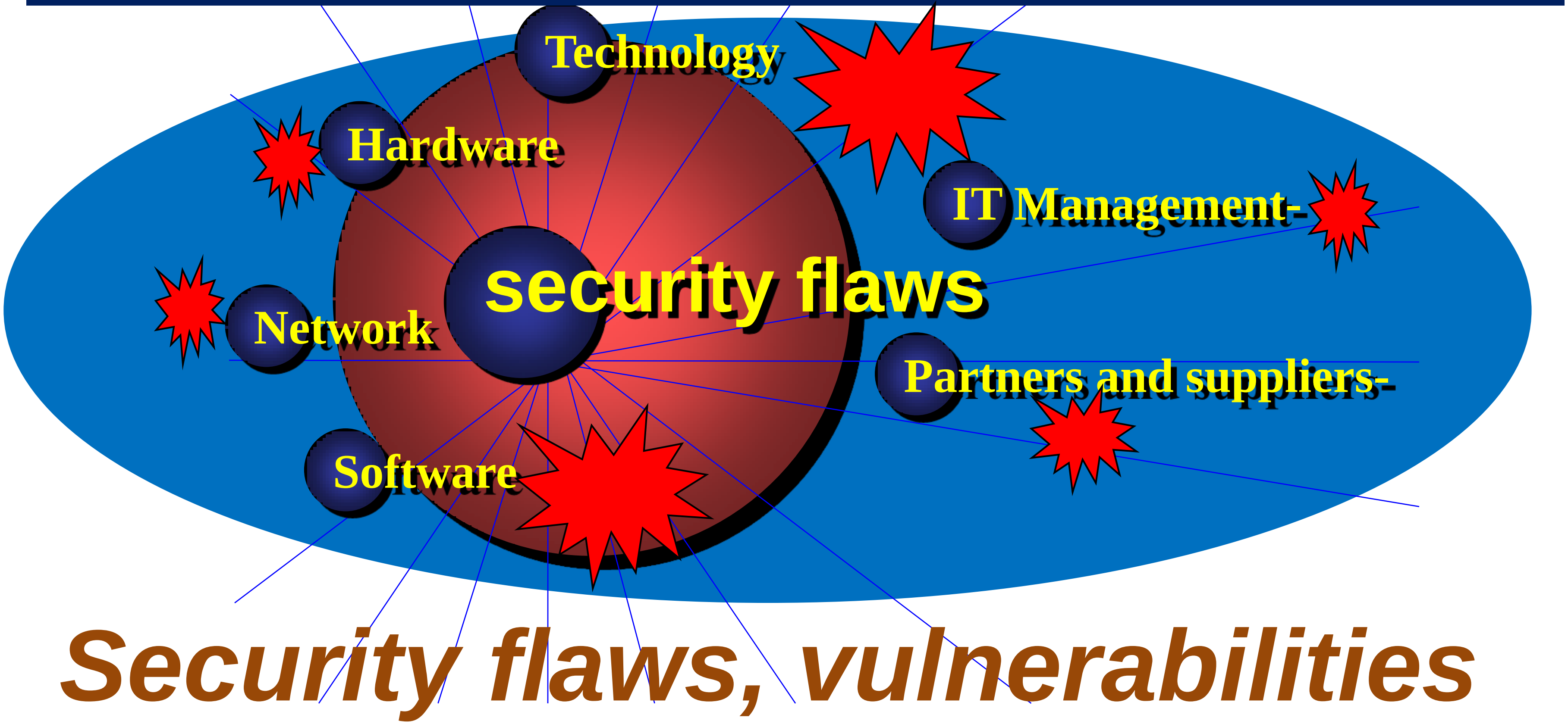
Some case of software vulnerability

Application, operating system, database program may have security vulnerabilities in terms of information security

- Program logic itself
- Option in the program logic, table
- Software parameter
- Method of sharing resource
- Invalid password etc.,,
- File sharing itself

Vulnerability?

Where there is a security vulnerability, there is a hacking attack!!

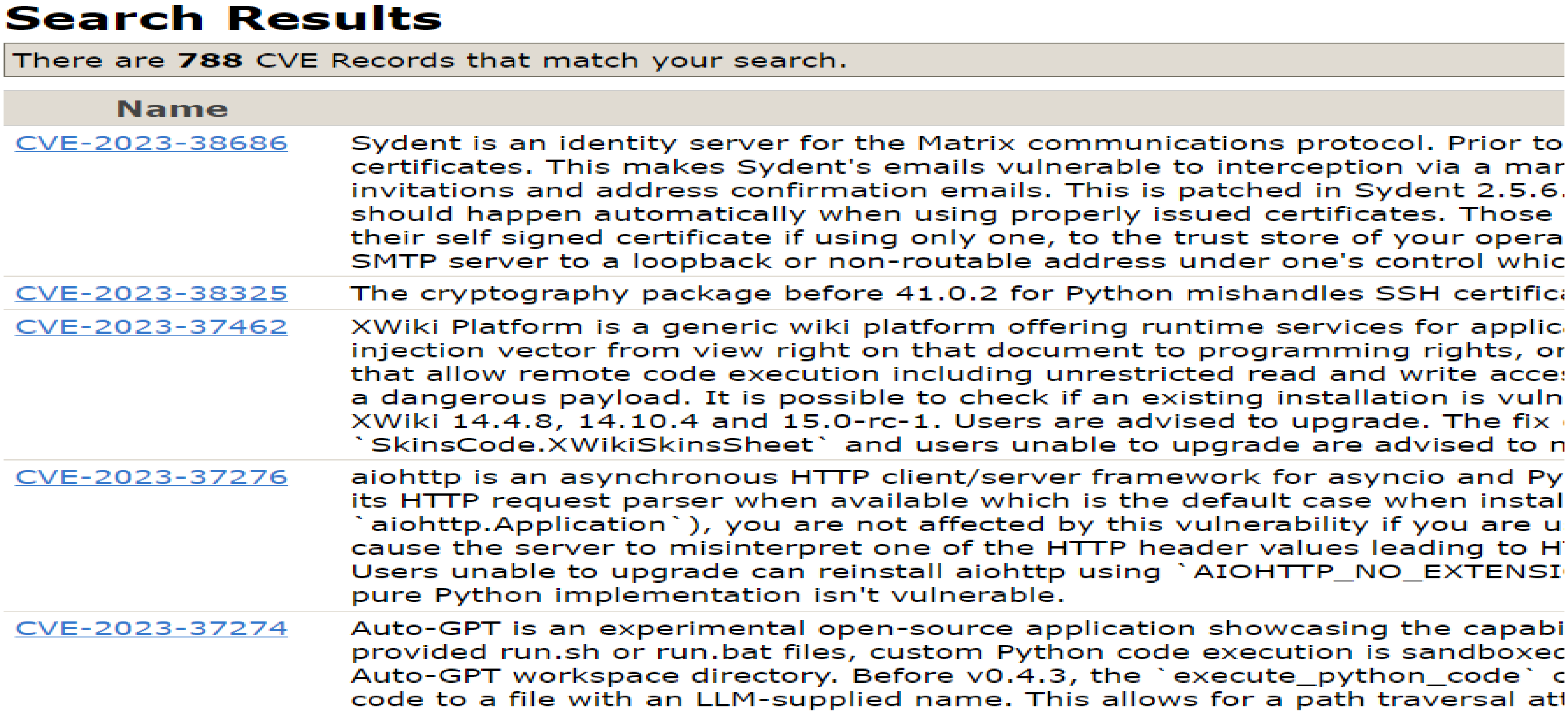


Security flaws, vulnerabilities

vulnerability in Python

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=python

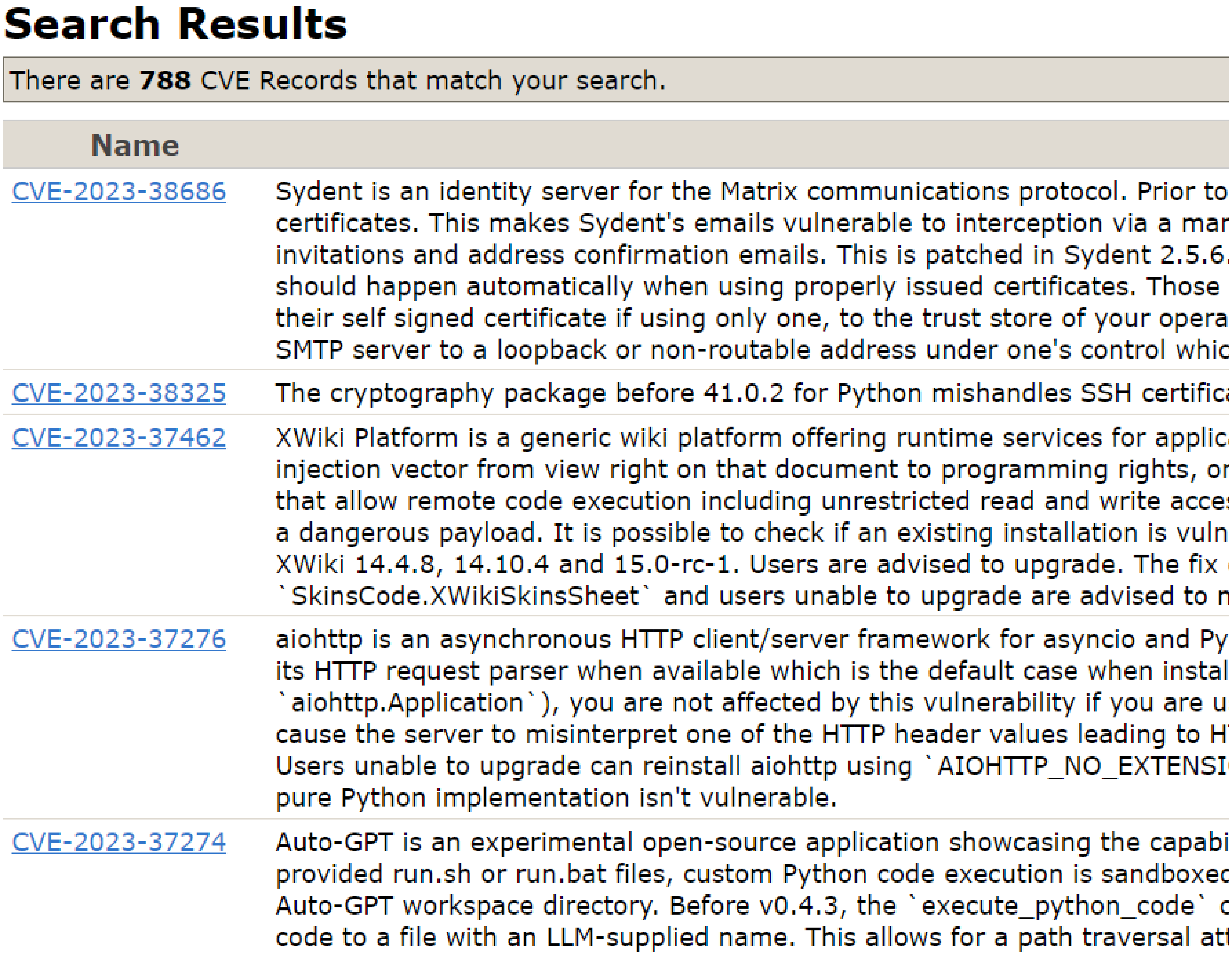
There are **788** CVE Records that match your search.



Search Results

There are **788** CVE Records that match your search.

Name	
CVE-2023-38686	Sydent is an identity server for the Matrix communications protocol. Prior to certificates. This makes Sydent's emails vulnerable to interception via a mar invitations and address confirmation emails. This is patched in Sydent 2.5.6. should happen automatically when using properly issued certificates. Those their self signed certificate if using only one, to the trust store of your opera SMTP server to a loopback or non-routable address under one's control whic
CVE-2023-38325	The cryptography package before 41.0.2 for Python mishandles SSH certific
CVE-2023-37462	XWiki Platform is a generic wiki platform offering runtime services for applic injection vector from view right on that document to programming rights, or that allow remote code execution including unrestricted read and write acce a dangerous payload. It is possible to check if an existing installation is vuln XWiki 14.4.8, 14.10.4 and 15.0-rc-1. Users are advised to upgrade. The fix `SkinsCode.XWikiSkinsSheet` and users unable to upgrade are advised to r
CVE-2023-37276	aiohttp is an asynchronous HTTP client/server framework for asyncio and Py its HTTP request parser when available which is the default case when instal `aiohttp.Application`), you are not affected by this vulnerability if you are u cause the server to misinterpret one of the HTTP header values leading to H Users unable to upgrade can reinstall aiohttp using `AIOHTTP_NO_EXTENSI pure Python implementation isn't vulnerable.
CVE-2023-37274	Auto-GPT is an experimental open-source application showcasing the capabi provided run.sh or run.bat files, custom Python code execution is sandboxed Auto-GPT workspace directory. Before v0.4.3, the `execute_python_code` c code to a file with an LLM-supplied name. This allows for a path traversal at



Search Results

There are **788** CVE Records that match your search.

Name	
CVE-2023-38686	Sydent is an identity server for the Matrix communications protocol. Prior to certificates. This makes Sydent's emails vulnerable to interception via a mar invitations and address confirmation emails. This is patched in Sydent 2.5.6. should happen automatically when using properly issued certificates. Those their self signed certificate if using only one, to the trust store of your opera SMTP server to a loopback or non-routable address under one's control whic
CVE-2023-38325	The cryptography package before 41.0.2 for Python mishandles SSH certifica
CVE-2023-37462	XWiki Platform is a generic wiki platform offering runtime services for applic injection vector from view right on that document to programming rights, or that allow remote code execution including unrestricted read and write acce a dangerous payload. It is possible to check if an existing installation is vuln XWiki 14.4.8, 14.10.4 and 15.0-rc-1. Users are advised to upgrade. The fix `SkinsCode.XWikiSkinsSheet` and users unable to upgrade are advised to n
CVE-2023-37276	aiohttp is an asynchronous HTTP client/server framework for asyncio and Py its HTTP request parser when available which is the default case when instal `aiohttp.Application`), you are not affected by this vulnerability if you are u cause the server to misinterpret one of the HTTP header values leading to H Users unable to upgrade can reinstall aiohttp using `AIOHTTP_NO_EXTENSI pure Python implementation isn't vulnerable.
CVE-2023-37274	Auto-GPT is an experimental open-source application showcasing the capabi provided run.sh or run.bat files, custom Python code execution is sandboxed Auto-GPT workspace directory. Before v0.4.3, the `execute_python_code` c code to a file with an LLM-supplied name. This allows for a path traversal at

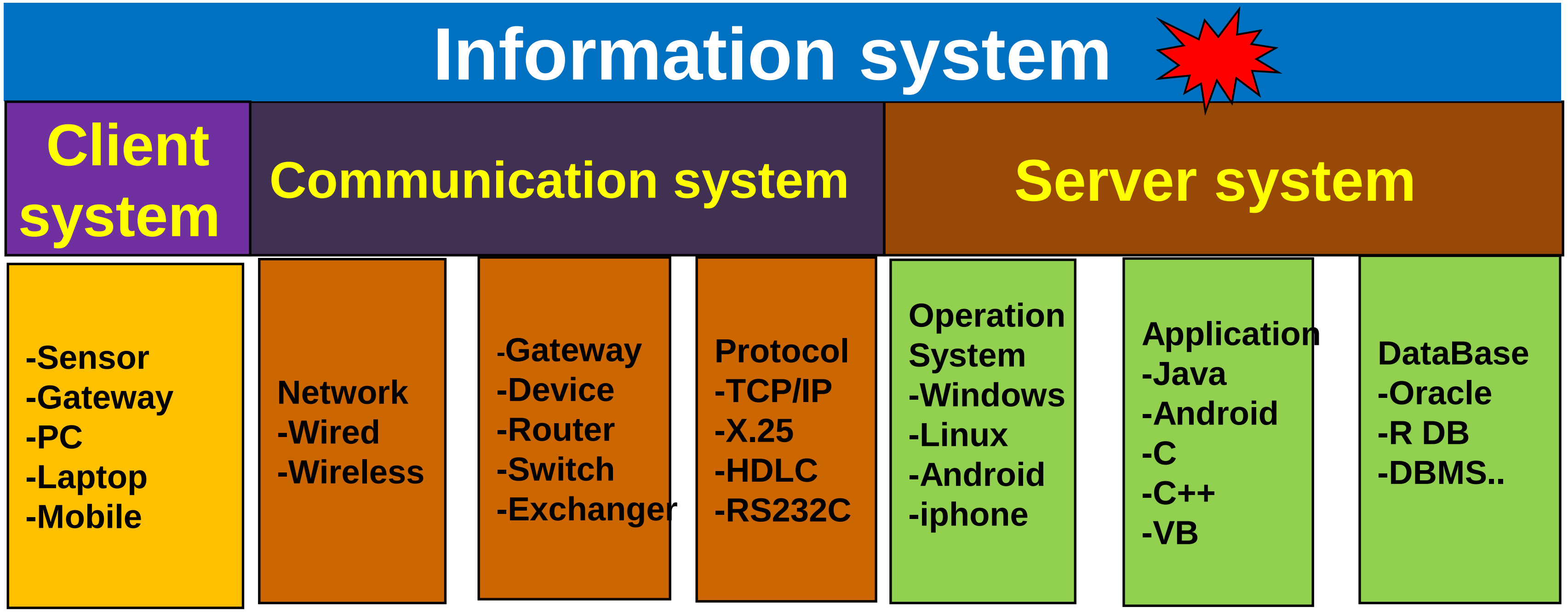
Phases of Hacking

What is the hacking steps

Not necessarily a hacker has to follow these steps in a sequential manner.

Cyber attacking target section

Various threats occur in all Information system sections , as long as the vulnerability exists



Information system

Client system

Communication system

Server system

-Sensor
-Gateway
-PC
-Laptop
-Mobile

Network
-Wired
-Wireless

-Gateway
-Device
-Router
-Switch
-Exchanger

Protocol
-TCP/IP
-X.25
-HDLC
-RS232C

Operation System
-Windows
-Linux
-Android
-iphone

Application
-Java
-Android
-C
-C++
-VB

DataBase
-Oracle
-R DB
-DBMS..

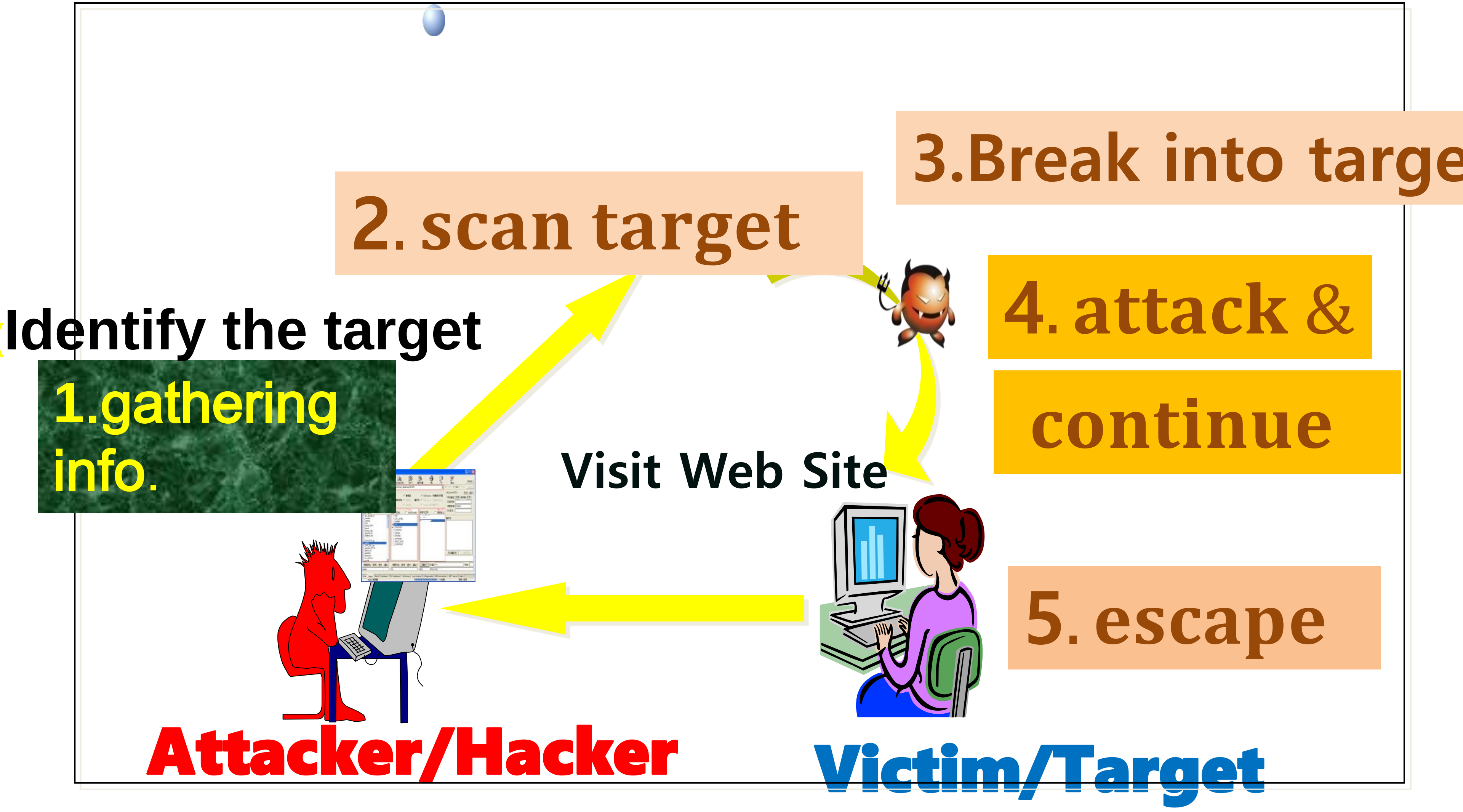
Cyber attacking weak point sectio

Phases of Hacking

Terms

- attacker=> hacker => packet sender
- defender=> target => victim => packet receiver

Attacker/Hacker vs Victim/Target



Identify the target

1.gathering info.

2. scan target

3.Break into targe

4. attack & continue

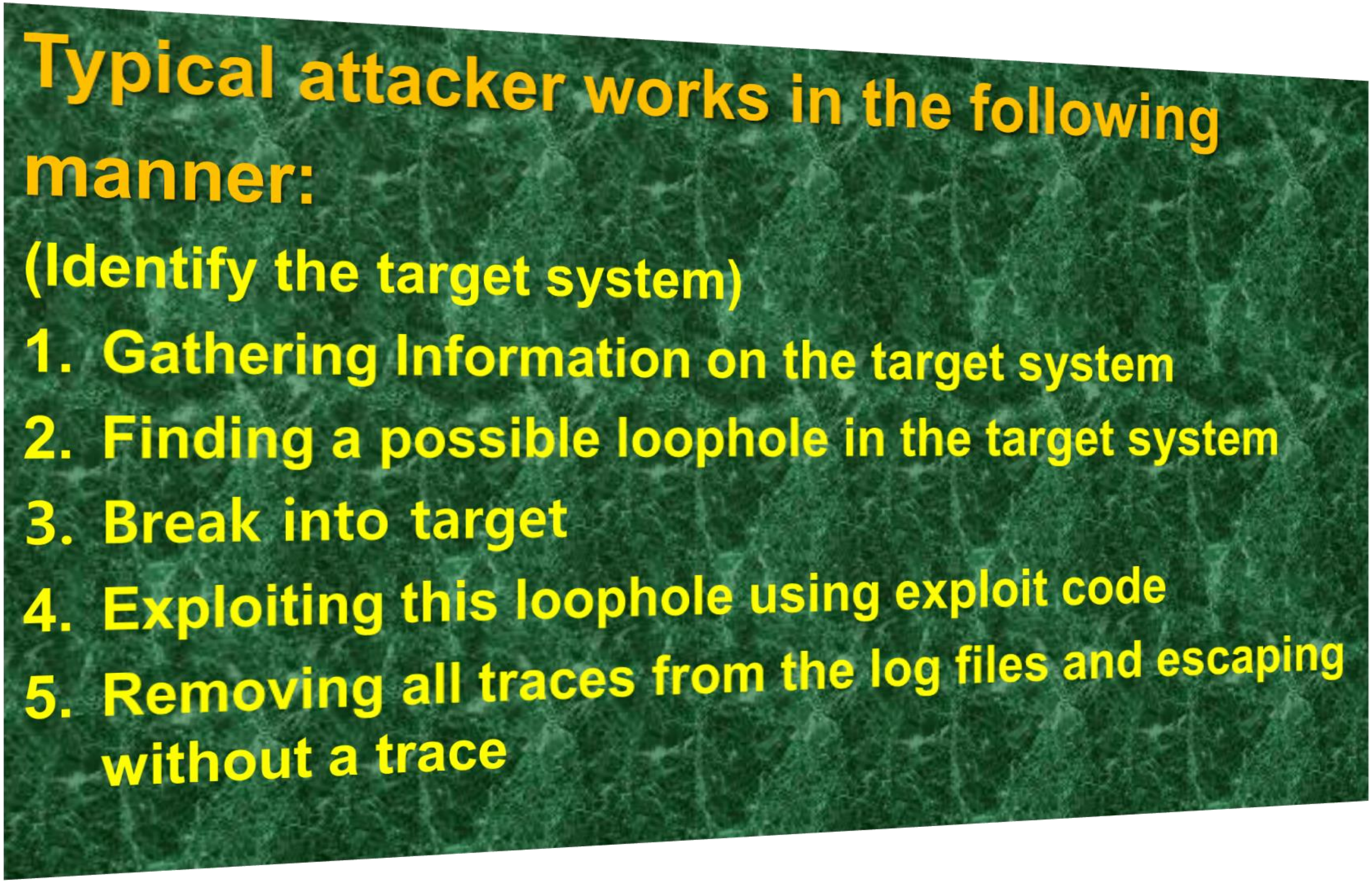
5. escape

Visit Web Site

Attacker/Hacker

Victim/Target

General hacking steps



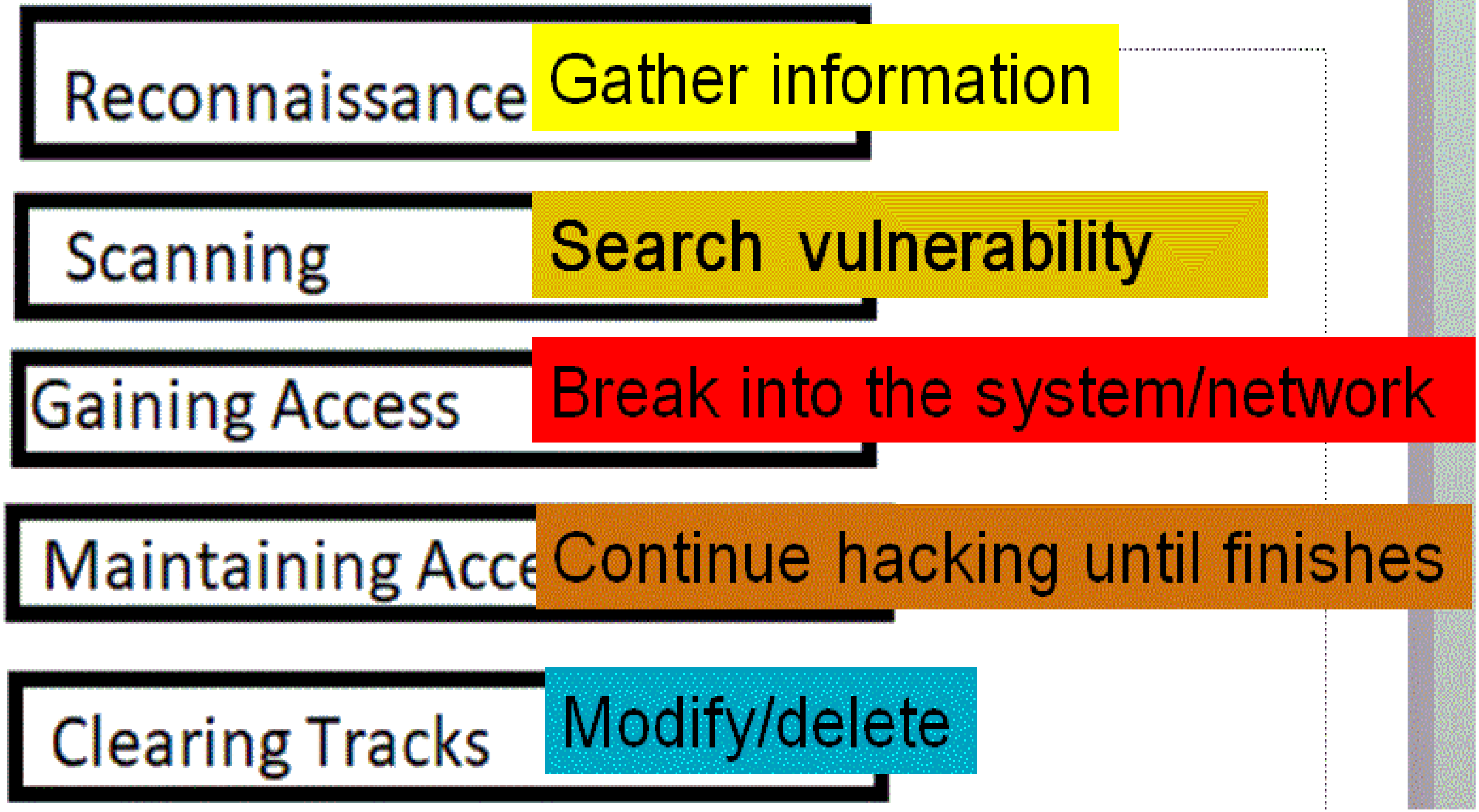
Typical attacker works in the following manner:

(Identify the target system)

1. Gathering Information on the target system
2. Finding a possible loophole in the target system
3. Break into target
4. Exploiting this loophole using exploit code
5. Removing all traces from the log files and escaping without a trace

Five steps Hacking

Identify the target system



Reconnaissance Gather information

Scanning Search vulnerability

Gaining Access Break into the system/network

Maintaining Acce Continue hacking until finishes

Clearing Tracks Modify/delete

https://www.greycampus.com/opencampus/ethical-hacking/phases-of-hacking

Phases of Hacking

Gather information / Reconnaissance:리코^너신스

Footprinting / information gathering

Collect as much information as possible about the target.

Usually collect information about three groups,

Network, Host, People involved

https://www.greycampus.com/opencampus/ethical-hacking/phases-of-hacking

Phases of Hacking

Scanning/Search vulnerability of targets

=> Port scanning

=> Network scanning

=> Vulnerability Scanning

Phases of Hacking

Scanning/search vulnerability of targets

Port scanning: information like open ports, Live systems, various services running on the host.

Network scanning: Topology of network, routers, firewalls servers if any, and host information and drawing a network diagram with the available information.

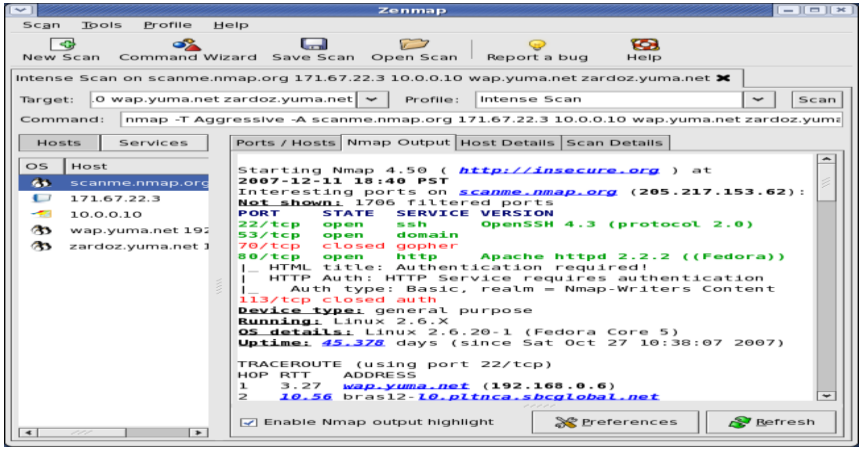
Vulnerability Scanning: Weaknesses or vulnerabilities which can be exploited. Usually done with help of automated tools

Collecting flaws

Finding a possible loophole in the target system

Various attacking tools are used for collecting flaws. The tools are versatile, powerful, and easily available on the internet. After collecting the vulnerability and then attacks by exploiting this loophole using exploit code

NMAP



Intense Scan on scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma.net

Target: .0 wap.yuma.net zardoz.yuma.net

Profile: Intense Scan

Command: nmap -T Aggressive -A scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma

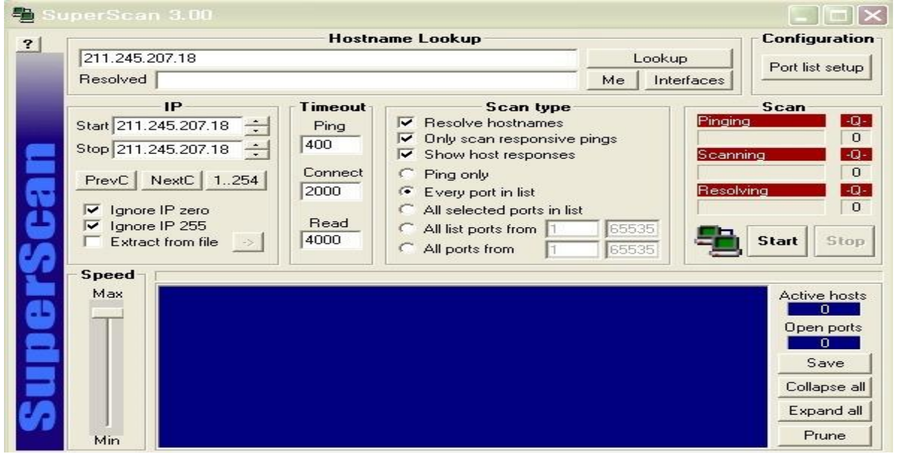
scanme.nmap.org
171.67.22.3
10.0.0.10
wap.yuma.net 192
zardoz.yuma.net 1

```
Starting Nmap 4.50 ( http://insecure.org ) at
2007-12-11 18:40 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
Not shown: 1706 filtered ports
PORT     STATE  SERVICE VERSION
22/tcp   open   ssh     OpenSSH 4.3 (protocol 2.0)
53/tcp   open   domain
70/tcp   closed gopher
80/tcp   open   http    Apache httpd 2.2.2 ((Fedora))
|_ HTML title: Authentication required!
|  HTTP Auth: HTTP Service requires authentication
|_   Auth type: Basic, realm = Nmap-Writers Content
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)
Uptime: 45.378 days (since Sat Oct 27 10:38:07 2007)

TRACEROUTE (using port 22/tcp)
HOP RTT   ADDRESS
1   3.27  wap.yuma.net (192.168.0.6)
2   10.56 bras12-10.pltnca.sbcglobal.net
```

☑ Enable Nmap output highlight

Superscan



Hostname Lookup: 211.245.207.18

Resolved:

IP Start: 211.245.207.18

IP Stop: 211.245.207.18

☑ Ignore IP zero
☑ Ignore IP 255
☐ Extract from file

Timeout: Ping 400; Connect 2000; Read 4000

Scan type:
☑ Resolve hostnames
☑ Only scan responsive pings
☑ Show host responses
○ Ping only
● Every port in list
○ All selected ports in list
○ All list ports from 1 65535
○ All ports from 1 65535

Scan: Pinging -Q- 0; Scanning -Q- 0; Resolving -Q- 0

Active hosts 0

Open ports 0

Gaining Access:

Breaks into the system/network using various tools or methods.

After entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data.

Gaining Access:

Sniffing the network using tool => Capture password => Break into the system/network

Attacking

Steal data & information

Information leaking

Delete the file & data

Changed the contents

Increase the traffic volume

Change the IP address

Maintaining Access:

Maintain the access to the target until he finishes the tasks he planned to accomplish

Hacker wants to maintain or persist the connection in the background without the knowledge of the user.

Use Trojans, Rootkits or other mal-code

Clearing Track

No thief wants to get caught.

An intelligent hacker always clears all evidence

so that in the later point of time, no one will find any traces leading to him.

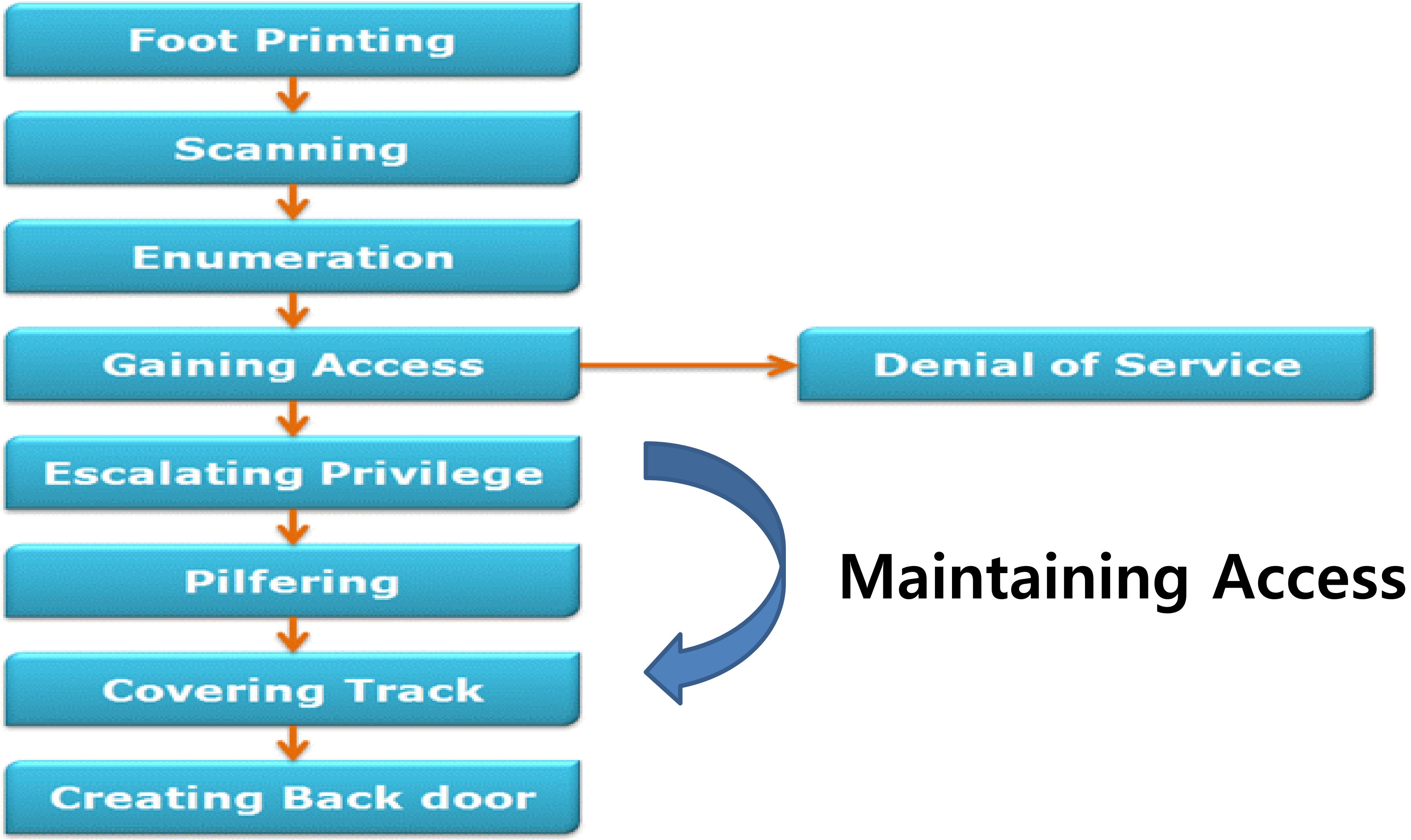
Logs, registry values, applications, folders, files he created.

Phases of NW hacking

NW hacking steps

It`s no standard model
but convenient if we understand
NW hacking process

NW hacking steps



Foot Printing

Scanning

Enumeration

Gaining Access

Denial of Service

Escalating Privilege

Pilfering

Covering Track

Creating Back door

Maintaining Access

8 steps of NW hacking

process	remark
1. Foot Printing	Pre Attacking, information gathering
2. Scanning	Port, Vulnerability Scanning
3. Enumeration	Collect resource sharing information of the system, get the detailed information
4. Gaining Access	Acquire the PW for access target system

8 steps of NW hacking

process	remark
5. Escalating Privilege	Enhance of system access and control
6. Pilfering	re-collecting the information needed to secure access to reliable systems & the process of collecting the desired information with root authority.
7. Covering Track	Clearing track, delete the log file
8. Creating Back Door	Creat back door for reentering the system