

# Phases of Hacking

# Map of attacking

## Malware/ Malicious code

- Virus, Worm
- Trojan
- Ransomware
- 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**

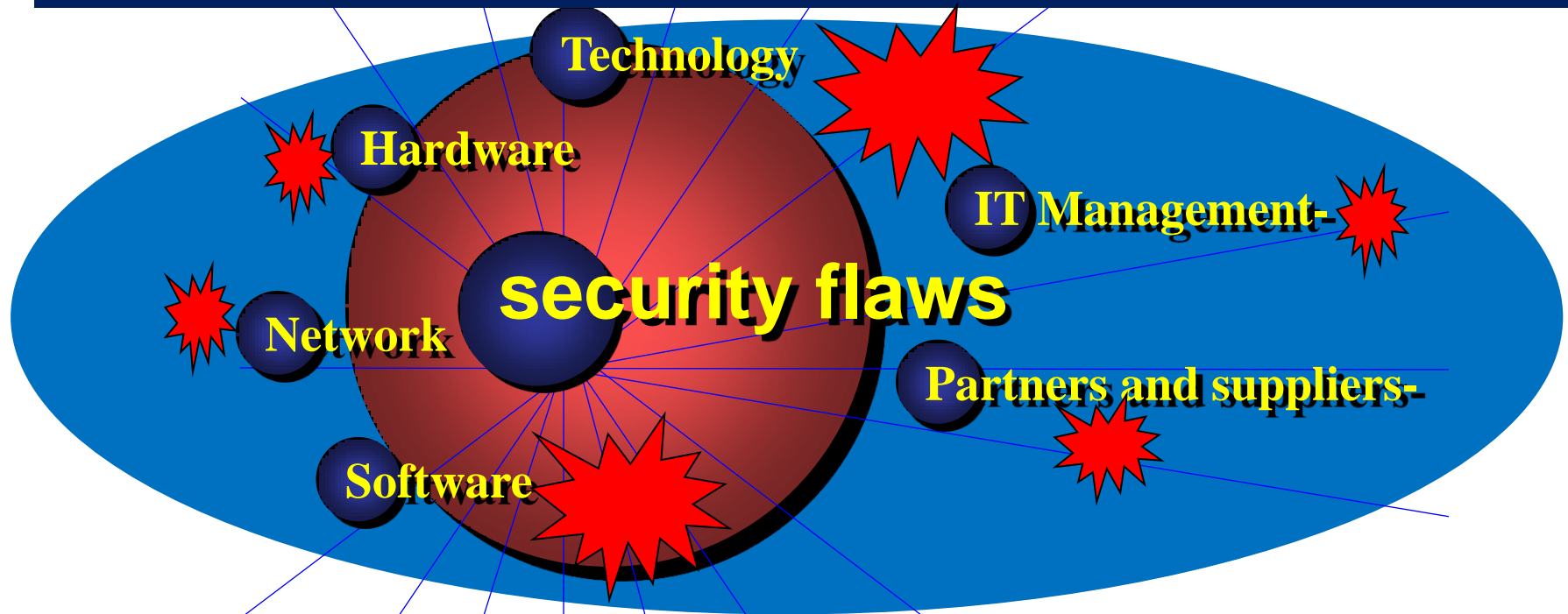
**Method of  
sharing  
resource**

**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	
<a href="#">CVE-2023-38686</a>	Sydent is an identity server for the Matrix communications protocol. Prior to certificates. This makes Sydent's emails vulnerable to interception via a man in the middle attack. This is patched in Sydent 2.5.6. This should happen automatically when using properly issued certificates. Those who have not updated should update their self signed certificate if using only one, to the trust store of your operating system. This is a patch for the SMTP server to a loopback or non-routable address under one's control which is not a good idea.
<a href="#">CVE-2023-38325</a>	The cryptography package before 41.0.2 for Python mishandles SSH certificates, which can lead to a denial of service or a remote code execution if the user is not careful.
<a href="#">CVE-2023-37462</a>	XWiki Platform is a generic wiki platform offering runtime services for applications. It is possible to inject code into the platform via a programming rights, or a dangerous payload. It is possible to check if an existing installation is vulnerable to this attack. XWiki 14.4.8, 14.10.4 and 15.0-rc-1. Users are advised to upgrade. The fix is to update the skins code. XWikiSkinsSheet and users unable to upgrade are advised to not use the skins code.
<a href="#">CVE-2023-37276</a>	aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. It is possible to inject code into the platform via a programming rights, or a dangerous payload. It is possible to check if an existing installation is vulnerable to this attack. aiohttp 3.8.4, 3.8.5, 3.8.6, 3.8.7, 3.8.8, 3.8.9, 3.9.0, 3.9.1, 3.9.2, 3.9.3, 3.9.4, 3.9.5, 3.9.6, 3.9.7, 3.9.8, 3.9.9, 3.10.0, 3.10.1, 3.10.2, 3.10.3, 3.10.4, 3.10.5, 3.10.6, 3.10.7, 3.10.8, 3.10.9, 3.11.0, 3.11.1, 3.11.2, 3.11.3, 3.11.4, 3.11.5, 3.11.6, 3.11.7, 3.11.8, 3.11.9, 3.12.0, 3.12.1, 3.12.2, 3.12.3, 3.12.4, 3.12.5, 3.12.6, 3.12.7, 3.12.8, 3.12.9, 3.13.0, 3.13.1, 3.13.2, 3.13.3, 3.13.4, 3.13.5, 3.13.6, 3.13.7, 3.13.8, 3.13.9, 3.14.0, 3.14.1, 3.14.2, 3.14.3, 3.14.4, 3.14.5, 3.14.6, 3.14.7, 3.14.8, 3.14.9, 3.15.0, 3.15.1, 3.15.2, 3.15.3, 3.15.4, 3.15.5, 3.15.6, 3.15.7, 3.15.8, 3.15.9, 3.16.0, 3.16.1, 3.16.2, 3.16.3, 3.16.4, 3.16.5, 3.16.6, 3.16.7, 3.16.8, 3.16.9, 3.17.0, 3.17.1, 3.17.2, 3.17.3, 3.17.4, 3.17.5, 3.17.6, 3.17.7, 3.17.8, 3.17.9, 3.18.0, 3.18.1, 3.18.2, 3.18.3, 3.18.4, 3.18.5, 3.18.6, 3.18.7, 3.18.8, 3.18.9, 3.19.0, 3.19.1, 3.19.2, 3.19.3, 3.19.4, 3.19.5, 3.19.6, 3.19.7, 3.19.8, 3.19.9, 3.20.0, 3.20.1, 3.20.2, 3.20.3, 3.20.4, 3.20.5, 3.20.6, 3.20.7, 3.20.8, 3.20.9, 3.21.0, 3.21.1, 3.21.2, 3.21.3, 3.21.4, 3.21.5, 3.21.6, 3.21.7, 3.21.8, 3.21.9, 3.22.0, 3.22.1, 3.22.2, 3.22.3, 3.22.4, 3.22.5, 3.22.6, 3.22.7, 3.22.8, 3.22.9, 3.23.0, 3.23.1, 3.23.2, 3.23.3, 3.23.4, 3.23.5, 3.23.6, 3.23.7, 3.23.8, 3.23.9, 3.24.0, 3.24.1, 3.24.2, 3.24.3, 3.24.4, 3.24.5, 3.24.6, 3.24.7, 3.24.8, 3.24.9, 3.25.0, 3.25.1, 3.25.2, 3.25.3, 3.25.4, 3.25.5, 3.25.6, 3.25.7, 3.25.8, 3.25.9, 3.26.0, 3.26.1, 3.26.2, 3.26.3, 3.26.4, 3.26.5, 3.26.6, 3.26.7, 3.26.8, 3.26.9, 3.27.0, 3.27.1, 3.27.2, 3.27.3, 3.27.4, 3.27.5, 3.27.6, 3.27.7, 3.27.8, 3.27.9, 3.28.0, 3.28.1, 3.28.2, 3.28.3, 3.28.4, 3.28.5, 3.28.6, 3.28.7, 3.28.8, 3.28.9, 3.29.0, 3.29.1, 3.29.2, 3.29.3, 3.29.4, 3.29.5, 3.29.6, 3.29.7, 3.29.8, 3.29.9, 3.30.0, 3.30.1, 3.30.2, 3.30.3, 3.30.4, 3.30.5, 3.30.6, 3.30.7, 3.30.8, 3.30.9, 3.31.0, 3.31.1, 3.31.2, 3.31.3, 3.31.4, 3.31.5, 3.31.6, 3.31.7, 3.31.8, 3.31.9, 3.32.0, 3.32.1, 3.32.2, 3.32.3, 3.32.4, 3.32.5, 3.32.6, 3.32.7, 3.32.8, 3.32.9, 3.33.0, 3.33.1, 3.33.2, 3.33.3, 3.33.4, 3.33.5, 3.33.6, 3.33.7, 3.33.8, 3.33.9, 3.34.0, 3.34.1, 3.34.2, 3.34.3, 3.34.4, 3.34.5, 3.34.6, 3.34.7, 3.34.8, 3.34.9, 3.35.0, 3.35.1, 3.35.2, 3.35.3, 3.35.4, 3.35.5, 3.35.6, 3.35.7, 3.35.8, 3.35.9, 3.36.0, 3.36.1, 3.36.2, 3.36.3, 3.36.4, 3.36.5, 3.36.6, 3.36.7, 3.36.8, 3.36.9, 3.37.0, 3.37.1, 3.37.2, 3.37.3, 3.37.4, 3.37.5, 3.37.6, 3.37.7, 3.37.8, 3.37.9, 3.38.0, 3.38.1, 3.38.2, 3.38.3, 3.38.4, 3.38.5, 3.38.6, 3.38.7, 3.38.8, 3.38.9, 3.39.0, 3.39.1, 3.39.2, 3.39.3, 3.39.4, 3.39.5, 3.39.6, 3.39.7, 3.39.8, 3.39.9, 3.40.0, 3.40.1, 3.40.2, 3.40.3, 3.40.4, 3.40.5, 3.40.6, 3.40.7, 3.40.8, 3.40.9, 3.41.0, 3.41.1, 3.41.2, 3.41.3, 3.41.4, 3.41.5, 3.41.6, 3.41.7, 3.41.8, 3.41.9, 3.42.0, 3.42.1, 3.42.2, 3.42.3, 3.42.4, 3.42.5, 3.42.6, 3.42.7, 3.42.8, 3.42.9, 3.43.0, 3.43.1, 3.43.2, 3.43.3, 3.43.4, 3.43.5, 3.43.6, 3.43.7, 3.43.8, 3.43.9, 3.44.0, 3.44.1, 3.44.2, 3.44.3, 3.44.4, 3.44.5, 3.44.6, 3.44.7, 3.44.8, 3.44.9, 3.45.0, 3.45.1, 3.45.2, 3.45.3, 3.45.4, 3.45.5, 3.45.6, 3.45.7, 3.45.8, 3.45.9, 3.46.0, 3.46.1, 3.46.2, 3.46.3, 3.46.4, 3.46.5, 3.46.6, 3.46.7, 3.46.8, 3.46.9, 3.47.0, 3.47.1, 3.47.2, 3.47.3, 3.47.4, 3.47.5, 3.47.6, 3.47.7, 3.47.8, 3.47.9, 3.48.0, 3.48.1, 3.48.2, 3.48.3, 3.48.4, 3.48.5, 3.48.6, 3.48.7, 3.48.8, 3.48.9, 3.49.0, 3.49.1, 3.49.2, 3.49.3, 3.49.4, 3.49.5, 3.49.6, 3.49.7, 3.49.8, 3.49.9, 3.50.0, 3.50.1, 3.50.2, 3.50.3, 3.50.4, 3.50.5, 3.50.6, 3.50.7, 3.50.8, 3.50.9, 3.51.0, 3.51.1, 3.51.2, 3.51.3, 3.51.4, 3.51.5, 3.51.6, 3.51.7, 3.51.8, 3.51.9, 3.52.0, 3.52.1, 3.52.2, 3.52.3, 3.52.4, 3.52.5, 3.52.6, 3.52.7, 3.52.8, 3.52.9, 3.53.0, 3.53.1, 3.53.2, 3.53.3, 3.53.4, 3.53.5, 3.53.6, 3.53.7, 3.53.8, 3.53.9, 3.54.0, 3.54.1, 3.54.2, 3.54.3, 3.54.4, 3.54.5, 3.54.6, 3.54.7, 3.54.8, 3.54.9, 3.55.0, 3.55.1, 3.55.2, 3.55.3, 3.55.4, 3.55.5, 3.55.6, 3.55.7, 3.55.8, 3.55.9, 3.56.0, 3.56.1, 3.56.2, 3.56.3, 3.56.4, 3.56.5, 3.56.6, 3.56.7, 3.56.8, 3.56.9, 3.57.0, 3.57.1, 3.57.2, 3.57.3, 3.57.4, 3.57.5, 3.57.6, 3.57.7, 3.57.8, 3.57.9, 3.58.0, 3.58.1, 3.58.2, 3.58.3, 3.58.4, 3.58.5, 3.58.6, 3.58.7, 3.58.8, 3.58.9, 3.59.0, 3.59.1, 3.59.2, 3.59.3, 3.59.4, 3.59.5, 3.59.6, 3.59.7, 3.59.8, 3.59.9, 3.60.0, 3.60.1, 3.60.2, 3.60.3, 3.60.4, 3.60.5, 3.60.6, 3.60.7, 3.60.8, 3.60.9, 3.61.0, 3.61.1, 3.61.2, 3.61.3, 3.61.4, 3.61.5, 3.61.6, 3.61.7, 3.61.8, 3.61.9, 3.62.0, 3.62.1, 3.62.2, 3.62.3, 3.62.4, 3.62.5, 3.62.6, 3.62.7, 3.62.8, 3.62.9, 3.63.0, 3.63.1, 3.63.2, 3.63.3, 3.63.4, 3.63.5, 3.63.6, 3.63.7, 3.63.8, 3.63.9, 3.64.0, 3.64.1, 3.64.2, 3.64.3, 3.64.4, 3.64.5, 3.64.6, 3.64.7, 3.64.8, 3.64.9, 3.65.0, 3.65.1, 3.65.2, 3.65.3, 3.65.4, 3.65.5, 3.65.6, 3.65.7, 3.65.8, 3.65.9, 3.66.0, 3.66.1, 3.66.2, 3.66.3, 3.66.4, 3.66.5, 3.66.6, 3.66.7, 3.66.8, 3.66.9, 3.67.0, 3.67.1, 3.67.2, 3.67.3, 3.67.4, 3.67.5, 3.67.6, 3.67.7, 3.67.8, 3.67.9, 3.68.0, 3.68.1, 3.68.2, 3.68.3, 3.68.4, 3.68.5, 3.68.6, 3.68.7, 3.68.8, 3.68.9, 3.69.0, 3.69.1, 3.69.2, 3.69.3, 3.69.4, 3.69.5, 3.69.6, 3.69.7, 3.69.8, 3.69.9, 3.70.0, 3.70.1, 3.70.2, 3.70.3, 3.70.4, 3.70.5, 3.70.6, 3.70.7, 3.70.8, 3.70.9, 3.71.0, 3.71.1, 3.71.2, 3.71.3, 3.71.4, 3.71.5, 3.71.6, 3.71.7, 3.71.8, 3.71.9, 3.72.0, 3.72.1, 3.72.2, 3.72.3, 3.72.4, 3.72.5, 3.72.6, 3.72.7, 3.72.8, 3.72.9, 3.73.0, 3.73.1, 3.73.2, 3.73.3, 3.73.4, 3.73.5, 3.73.6, 3.73.7, 3.73.8, 3.73.9, 3.74.0, 3.74.1, 3.74.2, 3.74.3, 3.74.4, 3.74.5, 3.74.6, 3.74.7, 3.74.8, 3.74.9, 3.75.0, 3.75.1, 3.75.2, 3.75.3, 3.75.4, 3.75.5, 3.75.6, 3.75.7, 3.75.8, 3.75.9, 3.76.0, 3.76.1, 3.76.2, 3.76.3, 3.76.4, 3.76.5, 3.76.6, 3.76.7, 3.76.8, 3.76.9, 3.77.0, 3.77.1, 3.77.2, 3.77.3, 3.77.4, 3.77.5, 3.77.6, 3.77.7, 3.77.8, 3.77.9, 3.78.0, 3.78.1, 3.78.2, 3.78.3, 3.78.4, 3.78.5, 3.78.6, 3.78.7, 3.78.8, 3.78.9, 3.79.0, 3.79.1, 3.79.2, 3.79.3, 3.79.4, 3.79.5, 3.79.6, 3.79.7, 3.79.8, 3.79.9, 3.80.0, 3.80.1, 3.80.2, 3.80.3, 3.80.4, 3.80.5, 3.80.6, 3.80.7, 3.80.8, 3.80.9, 3.81.0, 3.81.1, 3.81.2, 3.81.3, 3.81.4, 3.81.5, 3.81.6, 3.81.7, 3.81.8, 3.81.9, 3.82.0, 3.82.1, 3.82.2, 3.82.3, 3.82.4, 3.82.5, 3.82.6, 3.82.7, 3.82.8, 3.82.9, 3.83.0, 3.83.1, 3.83.2, 3.83.3, 3.83.4, 3.83.5, 3.83.6, 3.83.7, 3.83.8, 3.83.9, 3.84.0, 3.84.1, 3.84.2, 3.84.3, 3.84.4, 3.84.5, 3.84.6, 3.84.7, 3.84.8, 3.84.9, 3.85.0, 3.85.1, 3.85.2, 3.85.3, 3.85.4, 3.85.5, 3.85.6, 3.85.7, 3.85.8, 3.85.9, 3.86.0, 3.86.1, 3.86.2, 3.86.3, 3.86.4, 3.86.5, 3.86.6, 3.86.7, 3.86.8, 3.86.9, 3.87.0, 3.87.1, 3.87.2, 3.87.3, 3.87.4, 3.87.5, 3.87.6, 3.87.7, 3.87.8, 3.87.9, 3.88.0, 3.88.1, 3.88.2, 3.88.3, 3.88.4, 3.88.5, 3.88.6, 3.88.7, 3.88.8, 3.88.9, 3.89.0, 3.89.1, 3.89.2, 3.89.3, 3.89.4, 3.89.5, 3.89.6, 3.89.7, 3.89.8, 3.89.9, 3.90.0, 3.90.1, 3.90.2, 3.90.3, 3.90.4, 3.90.5, 3.90.6, 3.90.7, 3.90.8, 3.90.9, 3.91.0, 3.91.1, 3.91.2, 3.91.3, 3.91.4, 3.91.5, 3.91.6, 3.91.7, 3.91.8, 3.91.9, 3.92.0, 3.92.1, 3.92.2, 3.92.3, 3.92.4, 3.92.5, 3.92.6, 3.92.7, 3.92.8, 3.92.9, 3.93.0, 3.93.1, 3.93.2, 3.93.3, 3.93.4, 3.93.5, 3.93.6, 3.93.7, 3.93.8, 3.93.9, 3.94.0, 3.94.1, 3.94.2, 3.94.3, 3.94.4, 3.94.5, 3.94.6, 3.94.7, 3.94.8, 3.94.9, 3.95.0, 3.95.1, 3.95.2, 3.95.3, 3.95.4, 3.95.5, 3.95.6, 3.95.7, 3.95.8, 3.95.9, 3.96.0, 3.96.1, 3.96.2, 3.96.3, 3.96.4, 3.96.5, 3.96.6, 3.96.7, 3.96.8, 3.96.9, 3.97.0, 3.97.1, 3.97.2, 3.97.3, 3.97.4, 3.97.5, 3.97.6, 3.97.7, 3.97.8, 3.97.9, 3.98.0, 3.98.1, 3.98.2, 3.98.3, 3.98.4, 3.98.5, 3.98.6, 3.98.7, 3.98.8, 3.98.9, 3.99.0, 3.99.1, 3.99.2, 3.99.3, 3.99.4, 3.99.5, 3.99.6, 3.99.7, 3.99.8, 3.99.9, 4.0.0, 4.0.1, 4.0.2, 4.0.3, 4.0.4, 4.0.5, 4.0.6, 4.0.7, 4.0.8, 4.0.9, 4.1.0, 4.1.1, 4.1.2, 4.1.3, 4.1.4, 4.1.5, 4.1.6, 4.1.7, 4.1.8, 4.1.9, 4.2.0, 4.2.1, 4.2.2, 4.2.3, 4.2.4, 4.2.5, 4.2.6, 4.2.7, 4.2.8, 4.2.9, 4.3.0, 4.3.1, 4.3.2, 4.3.3, 4.3.4, 4.3.5, 4.3.6, 4.3.7, 4.3.8, 4.3.9, 4.4.0, 4.4.1, 4.4.2, 4.4.3, 4.4.4, 4.4.5, 4.4.6, 4.4.7, 4.4.8, 4.4.9, 4.5.0, 4.5.1, 4.5.2, 4.5.3, 4.5.4, 4.5.5, 4.5.6, 4.5.7, 4.5.8, 4.5.9, 4.6.0, 4.6.1, 4.6.2, 4.6.3, 4.6.4, 4.6.5, 4.6.6, 4.6.7, 4.6.8, 4.6.9, 4.7.0, 4.7.1, 4.7.2, 4.7.3, 4.7.4, 4.7.5, 4.7.6, 4.7.7, 4.7.8, 4.7.9, 4.8.0, 4.8.1, 4.8.2, 4.8.3, 4.8.4, 4.8.5, 4.8.6, 4.8.7, 4.8.8, 4.8.9, 4.9.0, 4.9.1, 4.9.2, 4.9.3, 4.9.4, 4.9.5, 4.9.6, 4.9.7, 4.9.8, 4.9.9, 5.0.0, 5.0.1, 5.0.2, 5.0.3, 5.0.4, 5.0.5, 5.0.6, 5.0.7, 5.0.8, 5.0.9, 5.1.0, 5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.1.5, 5.1.6, 5.1.7, 5.1.8, 5.1.9, 5.2.0, 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.2.5, 5.2.6, 5.2.7, 5.2.8, 5.2.9, 5.3.0, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 5.3.5, 5.3.6, 5.3.7, 5.3.8, 5.3.9, 5.4.0, 5.4.1, 5.4.2, 5.4.3, 5.4.4, 5.4.5, 5.4.6, 5.4.7, 5.4.8, 5.4.9, 5.5.0, 5.5.1, 5.5.2, 5.5.3, 5.5.4, 5.5.5, 5.5.6, 5.5.7, 5.5.8, 5.5.9, 5.6.0, 5.6.1, 5.6.2, 5.6.3, 5.6.4, 5.6.5, 5.6.6, 5.6.7, 5.6.8, 5.6.9, 5.7.0, 5.7.1, 5.7.2, 5.7.3, 5.7.4, 5.7.5, 5.7.6, 5.7.7, 5.7.8, 5.7.9, 5.8.0, 5.8.1, 5.8.2, 5.8.3, 5.8.4, 5.8.5, 5.8.6, 5.8.7, 5.8.8, 5.8.9, 5.9.0, 5.9.1, 5.9.2, 5.9.3, 5.9.4, 5.9.5, 5.9.6, 5.9.7, 5.9.8, 5.9.9, 6.0.0, 6.0.1, 6.0.2, 6.0.3, 6.0.4, 6.0.5, 6.0.6, 6.0.7, 6.0.8, 6.0.9, 6.1.0, 6.1.1, 6.1.2, 6.1.3, 6.1.4, 6.1.5, 6.1.6, 6.1.7, 6.1.8, 6.1.9, 6.2.0, 6.2.1, 6.2.2, 6.2.3, 6.2.4, 6.2.5, 6.2.6, 6.2.7, 6.2.8, 6.2.9, 6.3.0, 6.3.1, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.6, 6.3.7, 6.3.8, 6.3.9, 6.4.0, 6.4.1, 6.4.2, 6.4.3, 6.4.4, 6.4.5, 6.4.6, 6.4.7, 6.4.8, 6.4.9, 6.5.0, 6.5.1, 6.5.2, 6.5.3, 6.5.4, 6.5.5, 6.5.6, 6.5.7, 6.5.8, 6.5.9, 6.6.0, 6.6.1, 6.6.2, 6.6.3, 6.6.4, 6.6.5, 6.6.6, 6.6.7, 6.6.8, 6.6.9, 6.7.0, 6.7.1, 6.7.2, 6.7.3, 6.7.4, 6.7.5, 6.7.6, 6.7.7, 6.7.8, 6.7.9, 6.8.0, 6.8.1, 6.8.2, 6.8.3, 6.8.4, 6.8.5, 6.8.6, 6.8.7, 6.8.8, 6.8.9, 6.9.0, 6.9.1, 6.9.2, 6.9.3, 6.9.4, 6.9.5, 6.9.6, 6.9.7, 6.9.8, 6.9.9, 7.0.0, 7.0.1, 7.0.2, 7.0.3, 7.0.4, 7.0.5, 7.0.6, 7.0.7, 7.0.8, 7.0.9, 7.1.0, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.1.5, 7.1.6, 7.1.7, 7.1.8, 7.1.9, 7.2.0, 7.2.1, 7.2.2, 7.2.3, 7.2.4, 7.2.5, 7.2.6, 7.2.7, 7.2.8, 7.2.9, 7.3.0, 7.3.1, 7.3.2, 7.3.3, 7.3.4, 7.3.5, 7.3.6, 7.3.7, 7.3.8, 7.3.9, 7.4.0, 7.4.1, 7.4.2, 7.4.3, 7.4.4, 7.4.5, 7.4.6, 7.4.7, 7.4.8, 7.4.9, 7.5.0, 7.5.1, 7.5.2, 7.5.3, 7.5.4, 7.5.5, 7.5.6, 7.5.7, 7.5.8, 7.5.9, 7.6.0, 7.6.1, 7.6.2, 7.6.3, 7.6.4, 7.6.5, 7.6.6, 7.6.7, 7.6.8, 7.6.9, 7.7.0, 7.7.1, 7.7.2, 7.7.3, 7.7.4, 7.7.5, 7.7.6, 7.7.7, 7.7.8, 7.7.9, 7.8.0, 7.8.1, 7.8.2, 7.8.3, 7.8.4, 7.8.5, 7.8.6, 7.8.7, 7.8.8, 7.8.9, 7.9.0, 7.9.1, 7.9.2, 7.9.3, 7.9.4, 7.9.5, 7.9.6, 7.9.7, 7.9.8, 7.9.9, 8.0.0, 8.0.1, 8.0.2, 8.0.3, 8.0.4, 8.0.5, 8.0.6, 8.0.7, 8.0.8, 8.0.9, 8.1.0, 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.1.5, 8.1.6, 8.1.7, 8.1.8, 8.1.9, 8.2.0, 8.2.1, 8.2.2, 8.2.3, 8.2.4, 8.2.5, 8.2.6, 8.2.7, 8.2.8, 8.2.9, 8.3.0, 8.3.1, 8.3.2, 8.3.3, 8.3.4, 8.3.5, 8.3.6, 8.3.7, 8.3.8, 8.3.9, 8.4.0, 8.4.1, 8.4.2, 8.4.3, 8.4.4, 8.4.5, 8.4.6, 8.4.7, 8.4.8, 8.4.9, 8.5.0, 8.5.1, 8.5.2, 8.5.3, 8.5.4, 8.5.5, 8.5.6, 8.5.7, 8.5.8, 8.5.9, 8.6.0, 8.6.1, 8.6.2, 8.6.3, 8.6.4, 8.6.5, 8.6.6, 8.6.7, 8.6.8, 8.6.9, 8.7.0, 8.7.1, 8.7.2, 8.7.3, 8.7.4, 8.7.5, 8.7.6, 8.7.7, 8.7.8, 8.7.9, 8.8.0, 8.8.1, 8.8.2, 8.8.3, 8.8.4, 8.8.5, 8.8.6, 8.8.7, 8.8.8, 8.8.9, 8.9.0, 8.9.1, 8.9.2, 8.9.3, 8.9.4, 8.9.5, 8.9.6, 8.9.7, 8.9.8, 8.9.9, 9.0.0, 9.0.1, 9.0.2, 9.0.3, 9.0.4, 9.0.5, 9.0.6, 9.0.7, 9.0.8, 9.0.9, 9.1.0, 9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.1.7, 9.1.8, 9.1.9, 9.2.0, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.2.7, 9.2.8, 9.2.9, 9.3.0, 9.3.1, 9.3.2, 9.3.3, 9.3.4, 9.3.5, 9.3.6, 9.3.7, 9.3.8, 9.3.9, 9.4.0, 9.4.1, 9.4.2, 9.4.3, 9.4.4, 9.4.5, 9.4.6, 9.4.7, 9.4.8, 9.4.9, 9.5.0, 9.5.1, 9.5.2, 9.5.3, 9.5.4, 9.5.5, 9.5.6, 9.5.7, 9.5.8, 9.5.9, 9.6.0, 9.6.1, 9.6.2, 9.6.3, 9.6.4, 9.6.5, 9.6.6, 9.6.7, 9.6.8, 9.6.9, 9.7.0, 9.7.1, 9.7.2, 9.7.3, 9.7.4, 9.7.5, 9.7.6, 9.7.7, 9.7.8, 9.7.9, 9.8.0, 9.8.1, 9.8.2, 9.8.3, 9.8.4, 9.8.5, 9.8.6, 9.8.7, 9.8.8, 9.8.9, 9.9.0, 9.9.1, 9.9.2, 9.9.3, 9.9.4, 9.9.5, 9.9.6, 9.9.7, 9.9.8, 9.9.9, 10.0.0, 10.0.1, 10.0.2, 10.0.3, 10.0.4, 10.0.5, 10.0.6, 10.0.7, 10.0.8, 10.0.9, 10.1.0, 10.1.1, 10.1.2, 10.1.3, 10.1.4, 10.1.5, 10.1.6, 10.1.



# Search Results

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

Name	
<a href="#">CVE-2023-38686</a>	Sydent is an identity server for the Matrix communications protocol. Prior to certificates. This makes Sydent's emails vulnerable to interception via a man in the middle attack. Invitations and address confirmation emails. This is patched in Sydent 2.5.6. The fix should happen automatically when using properly issued certificates. Those who have their self signed certificate if using only one, to the trust store of your operating system. SMTP server to a loopback or non-routable address under one's control which can be used to intercept emails.
<a href="#">CVE-2023-38325</a>	The cryptography package before 41.0.2 for Python mishandles SSH certificates.
<a href="#">CVE-2023-37462</a>	XWiki Platform is a generic wiki platform offering runtime services for applications. A remote code execution vector from view right on that document to programming rights, or that allow remote code execution including unrestricted read and write access to the file system. A dangerous payload. It is possible to check if an existing installation is vulnerable. XWiki 14.4.8, 14.10.4 and 15.0-rc-1. Users are advised to upgrade. The fix is available in XWiki 15.0-rc-2. Users unable to upgrade are advised to not use XWiki.
<a href="#">CVE-2023-37276</a>	aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. Its HTTP request parser when available which is the default case when installing aiohttp. If you are using aiohttp.Application(), you are not affected by this vulnerability if you are using aiohttp 3.8.0 or later. The cause is the server to misinterpret one of the HTTP header values leading to HTTP request smuggling. Users unable to upgrade can reinstall aiohttp using `AIOHTTP_NO_EXTENSIONS` flag. The pure Python implementation isn't vulnerable.
<a href="#">CVE-2023-37274</a>	Auto-GPT is an experimental open-source application showcasing the capabilities of GPT-4. It provides a run.sh or run.bat files, custom Python code execution is sandboxed in the Auto-GPT workspace directory. Before v0.4.3, the `execute_python_code` function executed code to a file with an LLM-supplied name. This allows for a path traversal attack.

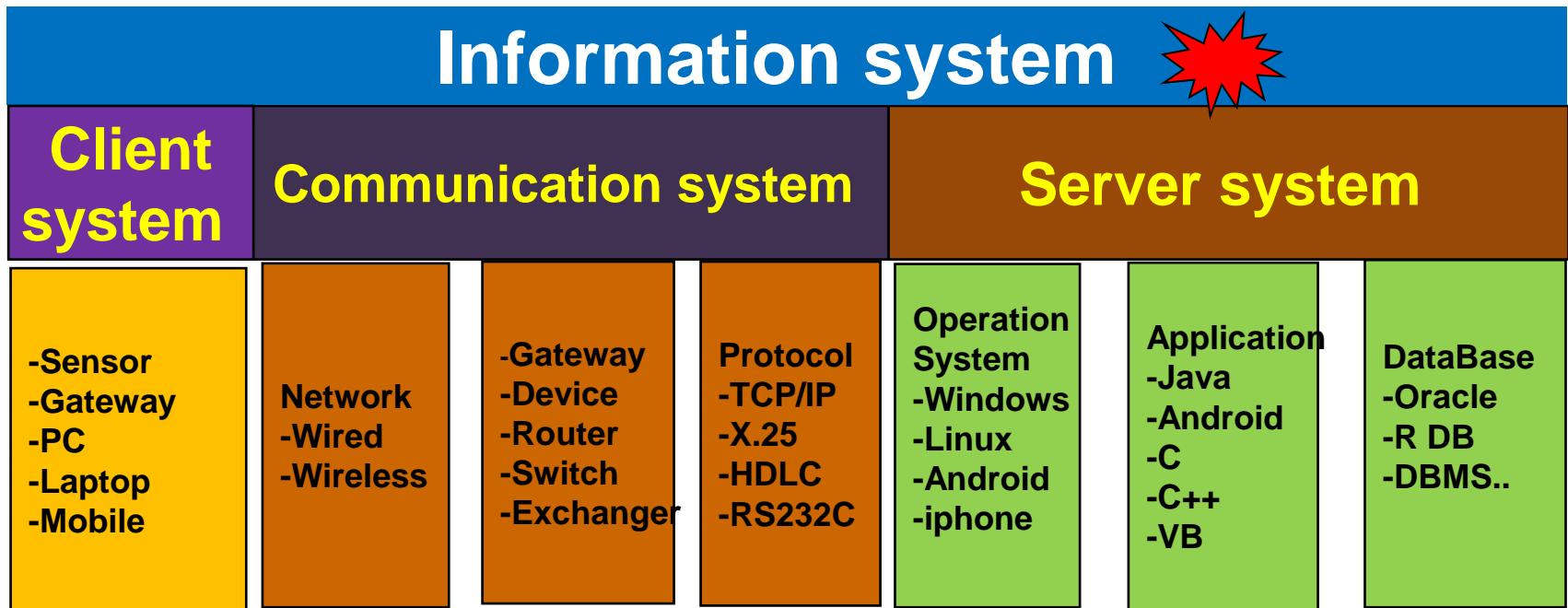
# Phases of Hacking

## 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



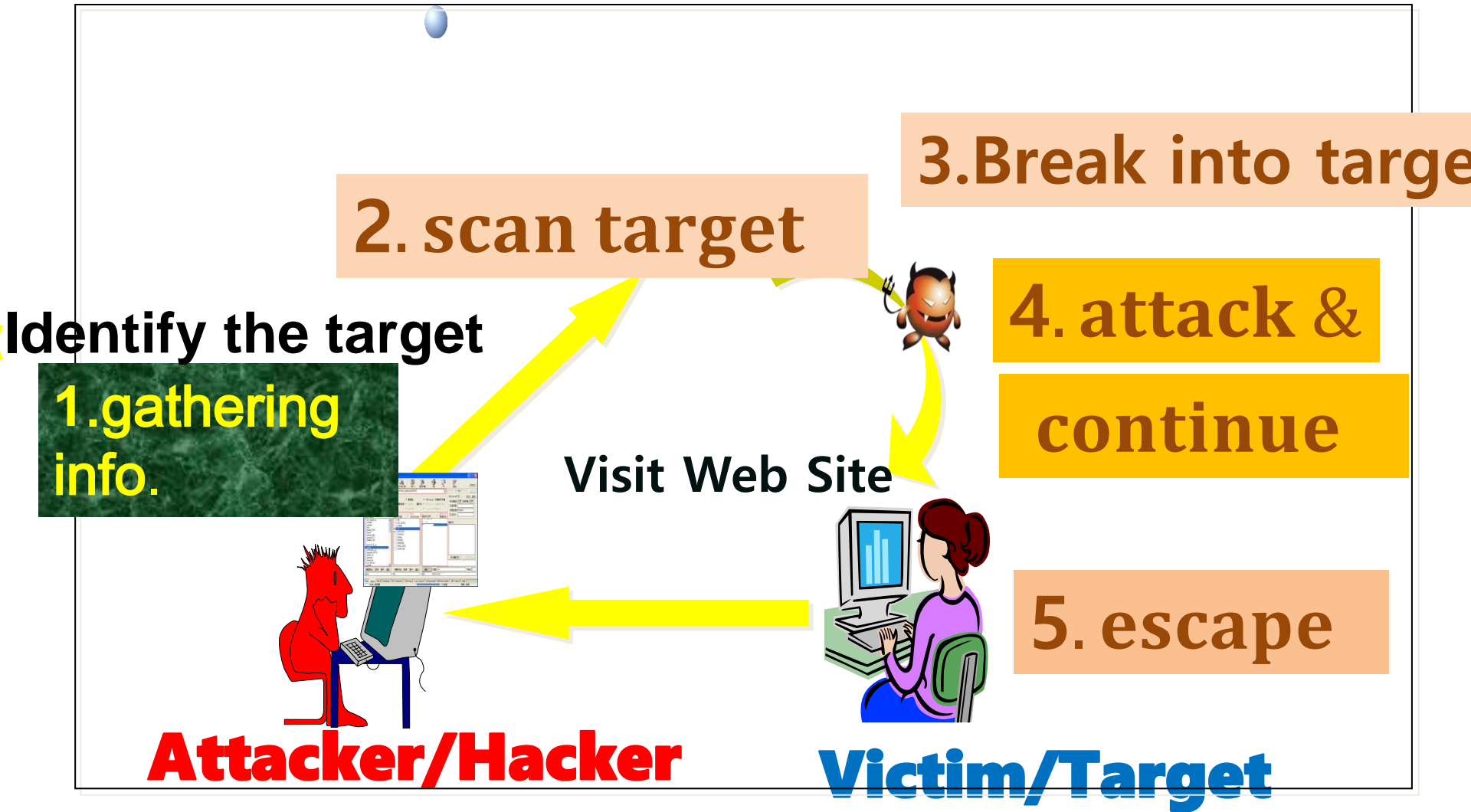
# Cyber attacking weak point section

# Phases of Hacking

## Terms

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

# Attacker/Hacker vs 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 Access Continue hacking until finishes

Clearing Tracks Modify/delete

# Phases of Hacking

Gather information / Reconnaissance:리  
코너신스

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.

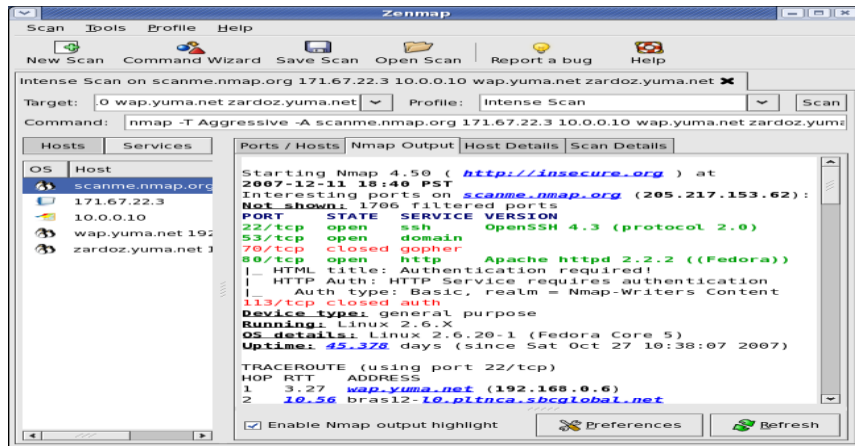
**Vulnerability Scanning:** Weaknesses or vulnerabilities which can be exploited. Usually done with help of automated tools

# Collecting flaws

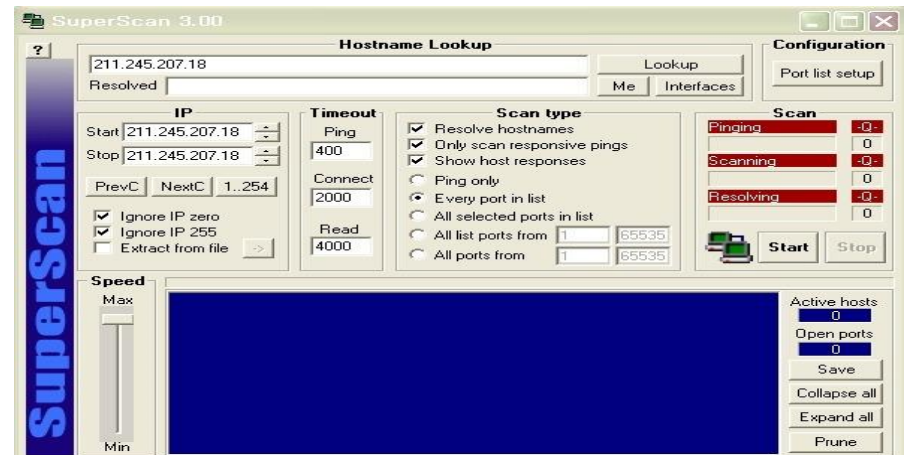
## Finding a possible loophole in the target system

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



### Superscan



# 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.

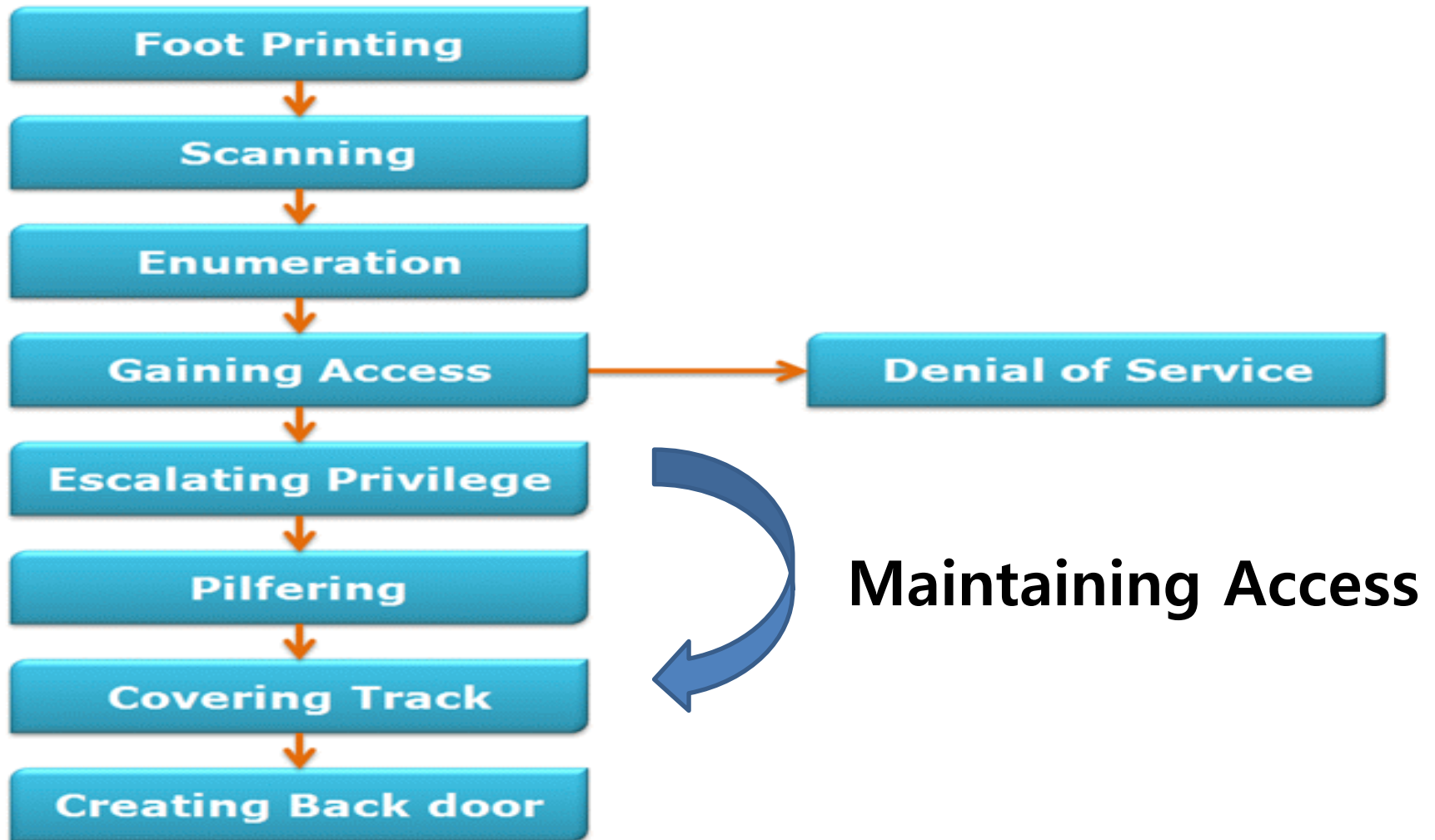


# Phases of NW hacking

# NW hacking steps

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

# NW hacking steps



# 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