Université Grenoble Alpes

M33-2. Cyber-attacks

M33-2. Cyber-attaques

- Introduction
  - Law aspects
  - Why hackers have an interest in IT companies or personnal compueters?
  - Cybercriminality a new kind of economy
  - Concepts of vulnerability, threat and attack

Law aspects

- French law:
  - **The mere fact** of collecting personal data by fraudulent means is punishable by five years of imprisonment and a fine of € 300,000 (article 226-18 du Code pénal)
  - **the mere fact** of fraudulently entering into all or part of an automated data processing system is punishable by two years in prison and a fine of € 30,000 (article 321-1 du même code).

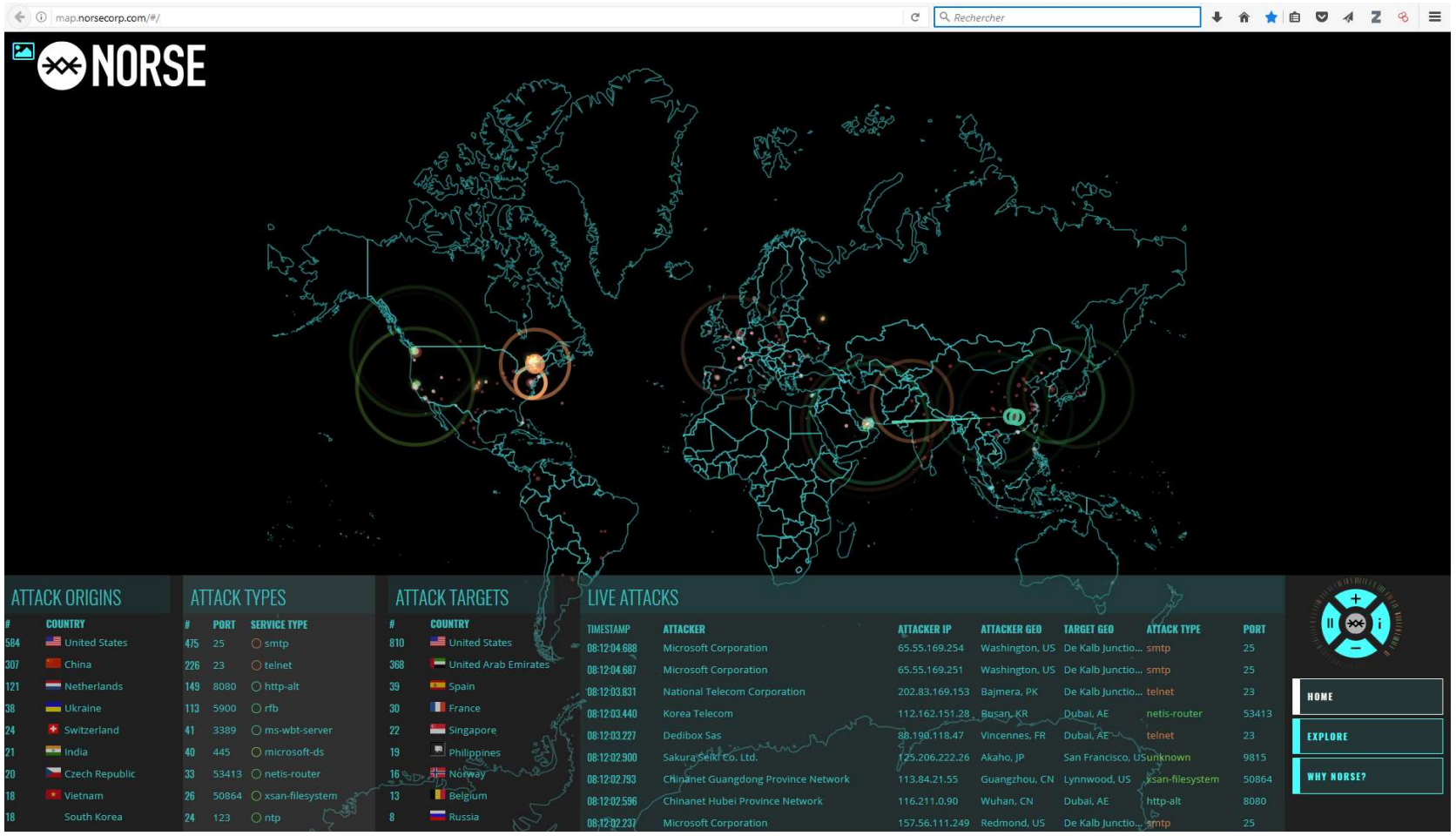
Law aspects

- **Article 323-3-1 du code pénal**
  - The fact, without lawful reason, of importing, holding, offering, assigning or making available any equipment, instrument, computer program or any data designed or specially adapted to commit one or more of the offenses set forth in sections 323-1 to 323-3 are punishable by the penalties provided respectively for the offense itself or for the most severely punished offense.

Law aspects

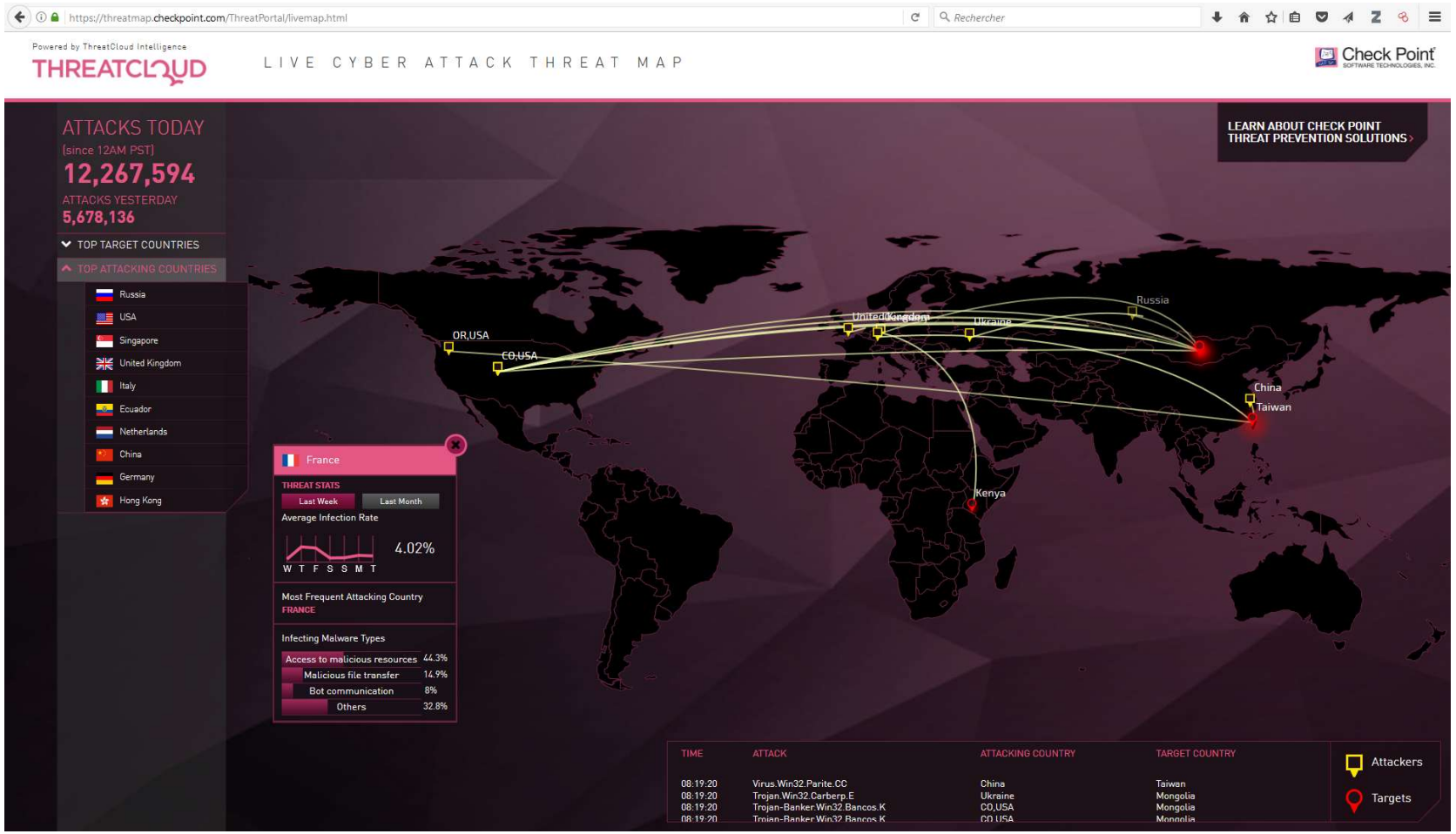
The use of methods described in this course involves the responsibility of users in case of use!

Why do pirates take an interest in organizations IT or individuals computers ?



Why do pirates take an interest in organizations IT or individuals computers ?

Why do pirates take an interest in organizations IT or individuals computers ?



Why do pirates take an interest in organizations IT or individuals computers ?

- Motivations change
  - 80s and 90s: lots of enthusiastic hackers
  - Nowadays: Mostly organized and thoughtful actions

Why do pirates take an interest in organizations IT or individuals computers ?

	THREAT AGENTS						
	Cyber-criminals	Insiders	Nation States	Corporations	Hacktivists	Cyber-terrorists	Script kiddies
Malware	✓	✓	✓	✓	✓	✓	✓
Web-based attacks	✓		✓	✓	✓	✓	✓
Web application attacks	✓		✓	✓	✓	✓	✓
Denial of Service	✓		✓	✓	✓	✓	✓
Botnets	✓		✓	✓	✓	✓	✓
Phishing	✓	✓	✓	✓	✓		✓
Spam	✓	✓	✓	✓			
Ransomware	✓	✓	✓	✓			✓
Insider threat	✓		✓	✓		✓	
Physical manipulation / damage / theft / loss	✓	✓	✓	✓	✓	✓	✓
Exploit kits	✓		✓	✓			
Data breaches	✓	✓	✓	✓	✓	✓	✓
Identity theft	✓	✓	✓	✓	✓	✓	✓
Information leakage	✓	✓	✓	✓	✓	✓	✓
Cyber espionage		✓	✓	✓			

Legend:
Primary group for threat: ✓
Secondary group for threat: ✓

Why do pirates take an interest in organizations IT or individuals computers ?

- Cyber Delinquency:
  - Individuals attracted by the lure of gain
  - The "hacktivists“
  - Political, religious, etc.
  - Direct competitors of a targeted organization
  - Civil servants in the service of a country
  - Mercenaries acting for the account of sponsors...

Why do pirates take an interest in organizations IT or individuals computers ?

- **Financial gains** (access to information, then monetization and resale)Users, emails
  - Internal organization of the company
  - Customer Files
  - Passwords, bank account numbers, credit cards

- Use of resources (then reselling or making available as "service")
  - Bandwidth & storage space (hosting music, movies et others contents)
  - Zombies (botnets)

- **Shakedown**
  - Deny of service
  - Data modifications

- **Spying**
  - Industrial / Competitors
  - From states

Why do pirates take an interest in organizations IT or individuals computers ?

Top Threats 2019-2020		Assessed Trends	Change in Ranking
1	Malware	---	---
2	Web-based Attacks	---	↗
3	Phishing	↗	↗
4	Web application attacks	---	↙
5	Spam	↙	↗
6	Denial of service	↙	↙
7	Identity theft	↗	↗
8	Data breaches	---	---
9	Insider threat	↗	---
10	Botnets	↙	↙
11	Physical manipulation, damage, theft and loss	---	↙
12	Information leakage	↗	↙
13	Ransomware	↗	↗
14	Cyberespionage	↙	↗
15	Crytojacking	↙	↙

Legend: Trends: ↙ Declining, --- Stable, ↗ Increasing **Ranking:** ↗ Going up, --- Same, ↙ Going down

Source : ENISA Threat Landscape 2020

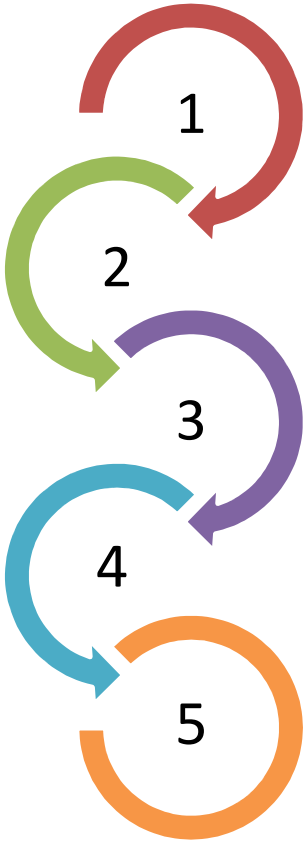
Université Grenoble Alpes

THE DARKNET:
The Underground for the Underground

erest in
omputers ?

The new economy of cybercrime

- A majority of delinquent acts on the Internet are committed by organized criminal groups, professionals and involving many actors



Specialized groups in the **development of computer malware and viruses**

Groups in charge of **exploitation and marketing** of services for carrying out computer attacks

One or more **hosts** that store malicious content, either dishonest hosts or host themselves attacked and whose servers are controlled by hackers

Groups in charge of **sailing** stolen data, and mainly bank card data

Financial intermediaries to collect money that are generally based on networks of **mules**

The new economy of cybercrime

- Some values to illustrate the market of cybercrime ..

from 2 to 10 $ — The average marketing price of **bank card numbers** by country and the ceilings

5 $ — The average rental rate for 1 hour of a **botnet**, system to saturate a website

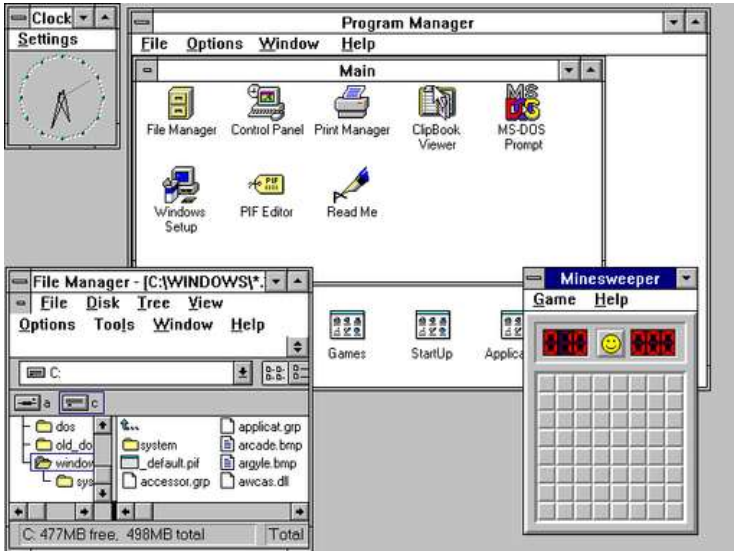
2.399 $ — The marketing price of **malware** "Citadel" to intercept credit card numbers
(+ A monthly subscription of $ 125)

The 3 cyber layers

- Physical layer
  - Network equipments, wires
  - Computers
  - …

The 3 cyber layers

- The logical layer :
  - Operating System
  - Office productivity software
  - Web browser
  - …

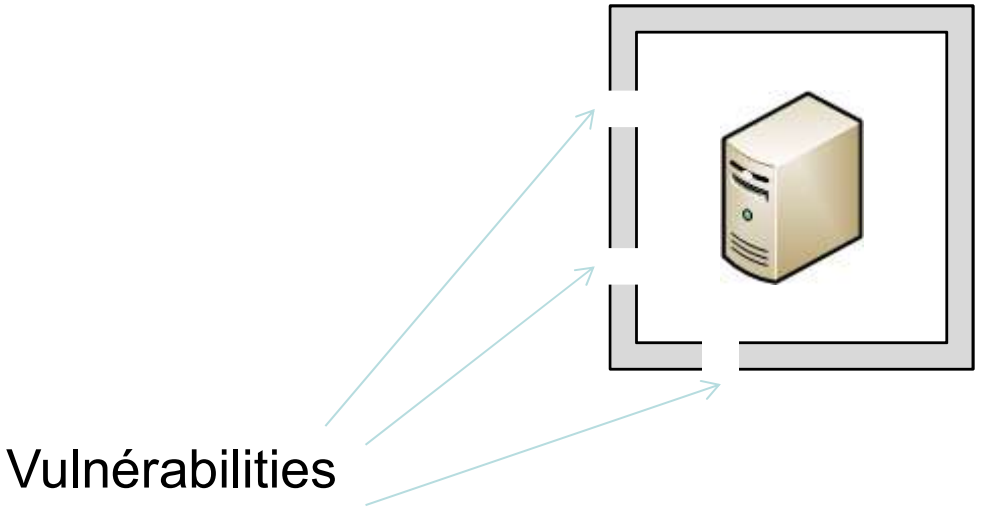


The 3 cyber layers

- The semantic layer, what we understand :
  - About an e-mail
  - About a web page
  - About a document
  - …

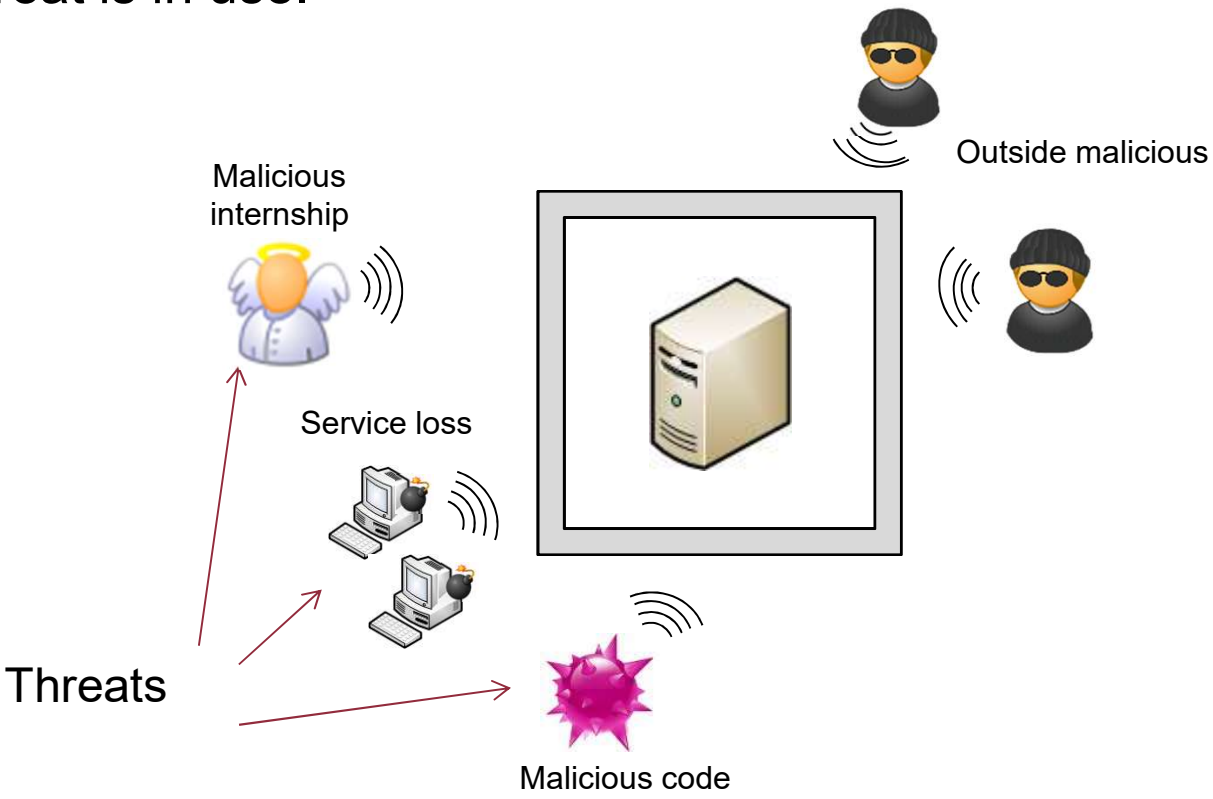
Vulnerability, threats, attack concepts

- **Vulnerability**
- **Weakness in something** (in terms of design, implementation, installation, configuration or use).



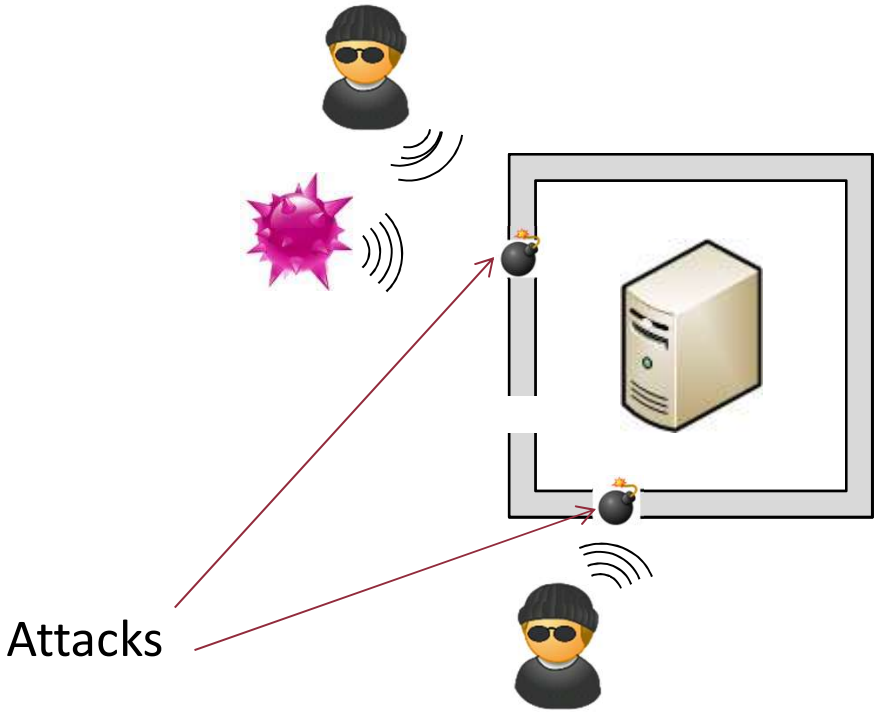
Vulnerability, threats, attack concepts

- **Threat**
- **Potential cause of an incident**, that could produce damages if the threat is in use.



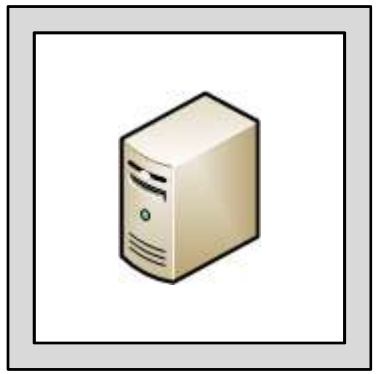
Vulnerability, threats, attack concepts

- **Attack**
- **Malicious action** designed to impair security. An attack is the **realization of a threat**, and it needs **a vulnerability exploit.**



Vulnerability, threats, attack concepts

- **Attack**
- An attack could only occur (and succeed) only is there is a vulnerability.



•Thus, security experts work is to be sure that the IT has no vulnerability.

•In the real world, the main objective is to be able to control vulnerabilities better than trying to have 0 vulnerabilities which is an out of reach objective.

M33-2. Cyber-attaques

- Basics
  - IT ressources vulnerables to attacks
  - Target types
  - Potential threats sources
  - Attackers types

2.1 Type of computer resources vulnerable to the attacks

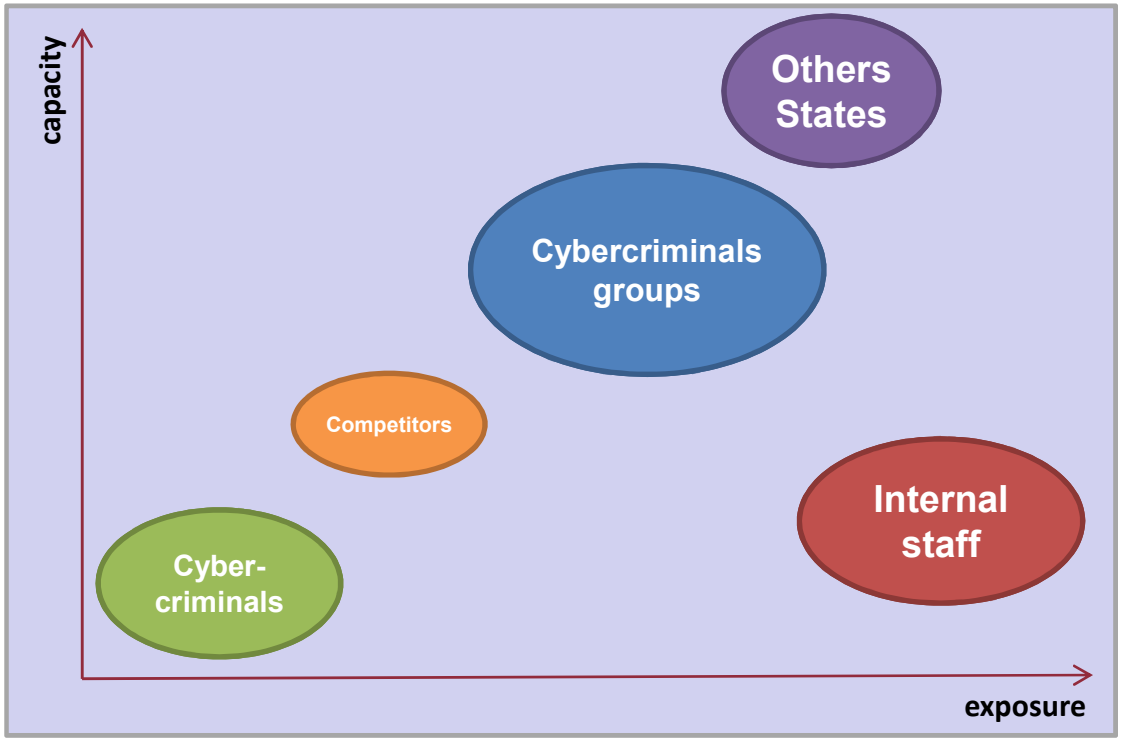
- Servers
  - Obtaining a slave machine to tackle other targets
- Clients
  - Machine potentially less protected
  - Vulnerable via a wireless connection
- Other terminals (wireless)
  - Cellular phones
  - PDA, …
- Disk space
  - Backup of illegal files
- Bandwidth
  - Use of a pirated network to reach/attack other networks
- Personal and confidential information

hardware

2.1 Types of targets

- Convenient target *(cible opportune)*
  - By “chance”: detected by the pirates in the search of least protected machines or servers
  - What to do?: update the systems
  - To test the system (try to find faults)
- Chosen target *(cible de choix)*
  - Precise Target: strategic interest of the company …

Sources potentielles de menaces



Map example of main threat sources applying to IT

Capacity
Threat source knowledge and ressources

Exposure
Threat source opportunities and interest

Attention : this map must be adapted to each organization because threats depends on sectors.

Example : State administration IT don't face the threats as a e-shop website or a university

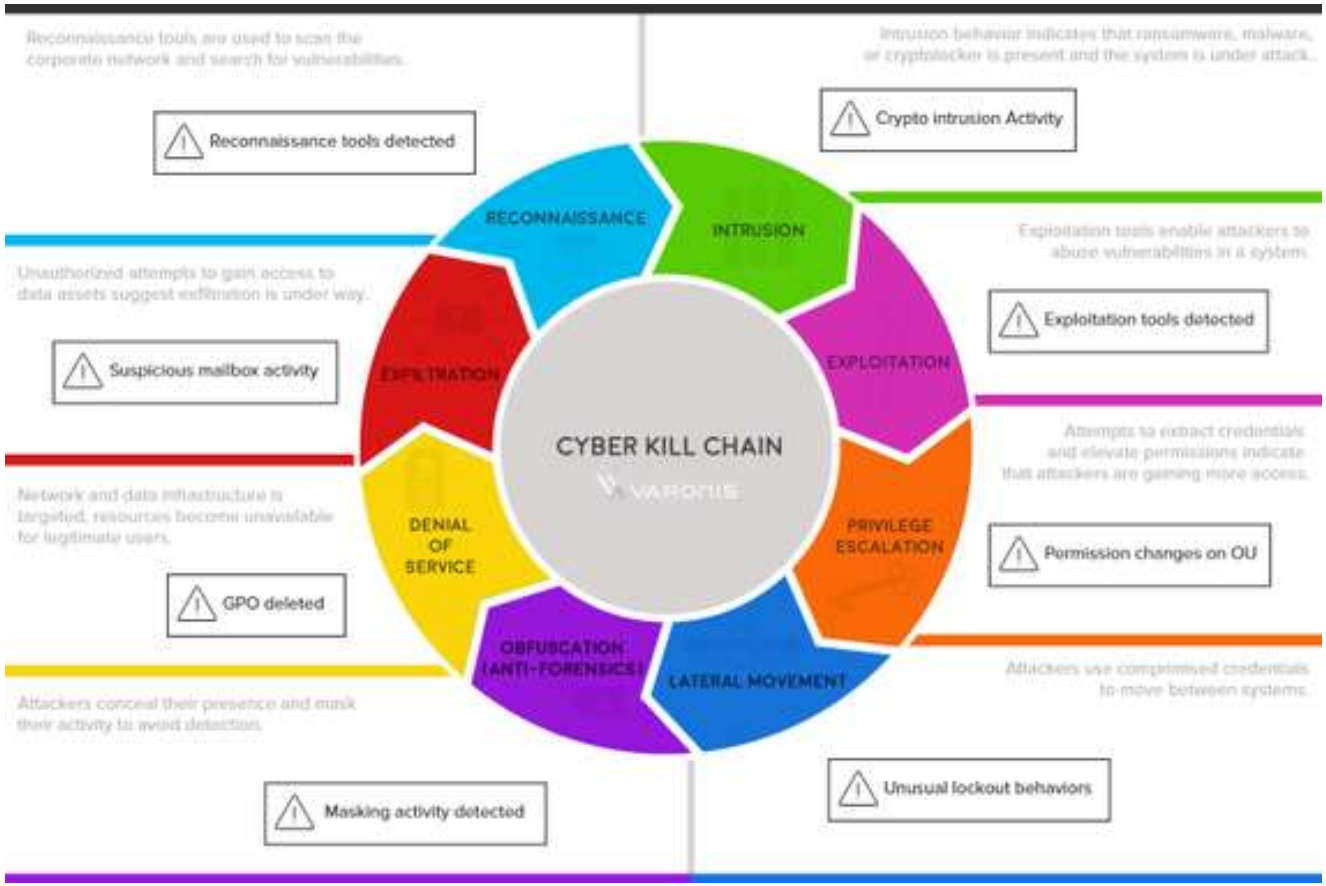
Types d'attaquants

- Hackers (skilled computer expert who seeks and exploits weaknesses in a computer system or computer network)
  - A **white hat** hacker breaks security for non-malicious reasons, either to test their own security system, perform penetration tests or vulnerability assessments for a client - or while working for a security company which makes security software. The term is generally synonymous with ethical hacker.
  - A **blue hat** hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch, looking for exploits so they can be closed.
  - A "**black hat**" hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain" (Moore, 2005). Black hat hackers form the stereotypical, illegal hacking groups often portrayed in popular culture, and are "the epitome of all that the public fears in a computer criminal".
  - A **grey hat** hacker lies between a black hat and a white hat hacker. A grey hat hacker may surf the Internet and hack into a computer system for the sole purpose of notifying the administrator that their system has a security defect, for example. They may then offer to correct the defect for a fee.
  - A **script kiddie** (also known as a skid or skiddie) is an unskilled hacker who breaks into computer systems by using automated tools written by others (usually by other black hat hackers), hence the term script (i.e. a prearranged plan or set of activities) kiddie (i.e. kid, child—an individual lacking knowledge and experience, immature), usually with little understanding of the underlying concept.
  - A **hacktivist** is a hacker who utilizes technology to publicize a social, ideological, religious or political message.

Types d'attaquants

- Pirates organizations
  - Sharing of finds
  - Motivations through challenges (challenges)
  - Mercenaries
  - State Actors

M33-2. Cyber-attaques



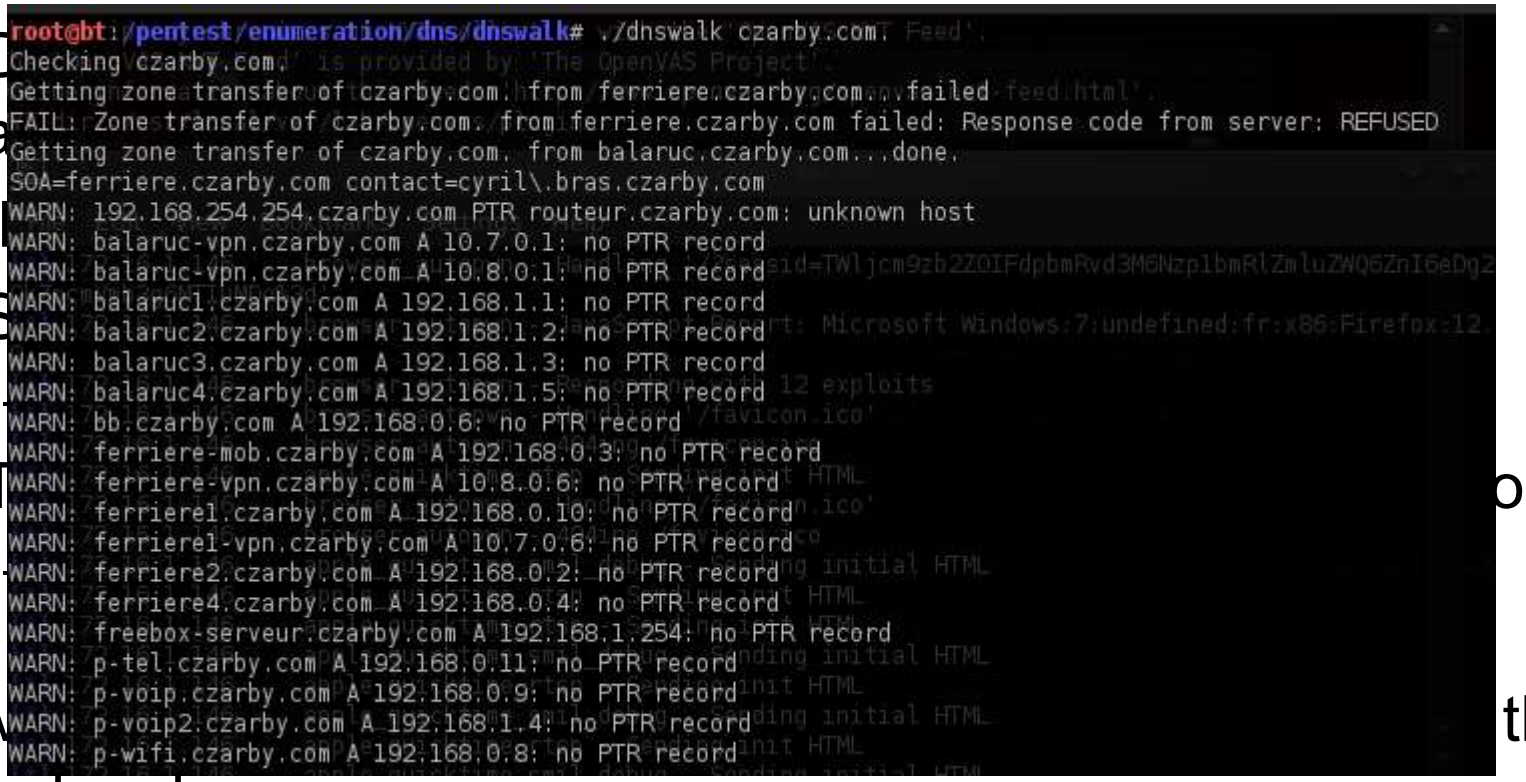
2.3 Types of attacks (4/4)

The types of attacks are classified in two categories:

- Passive attacks
  - Interception, listening
- Active attacks
  - Modification
  - Interruption
  - Denial of service

2.2.1 Recognition and collection of information (1/3)

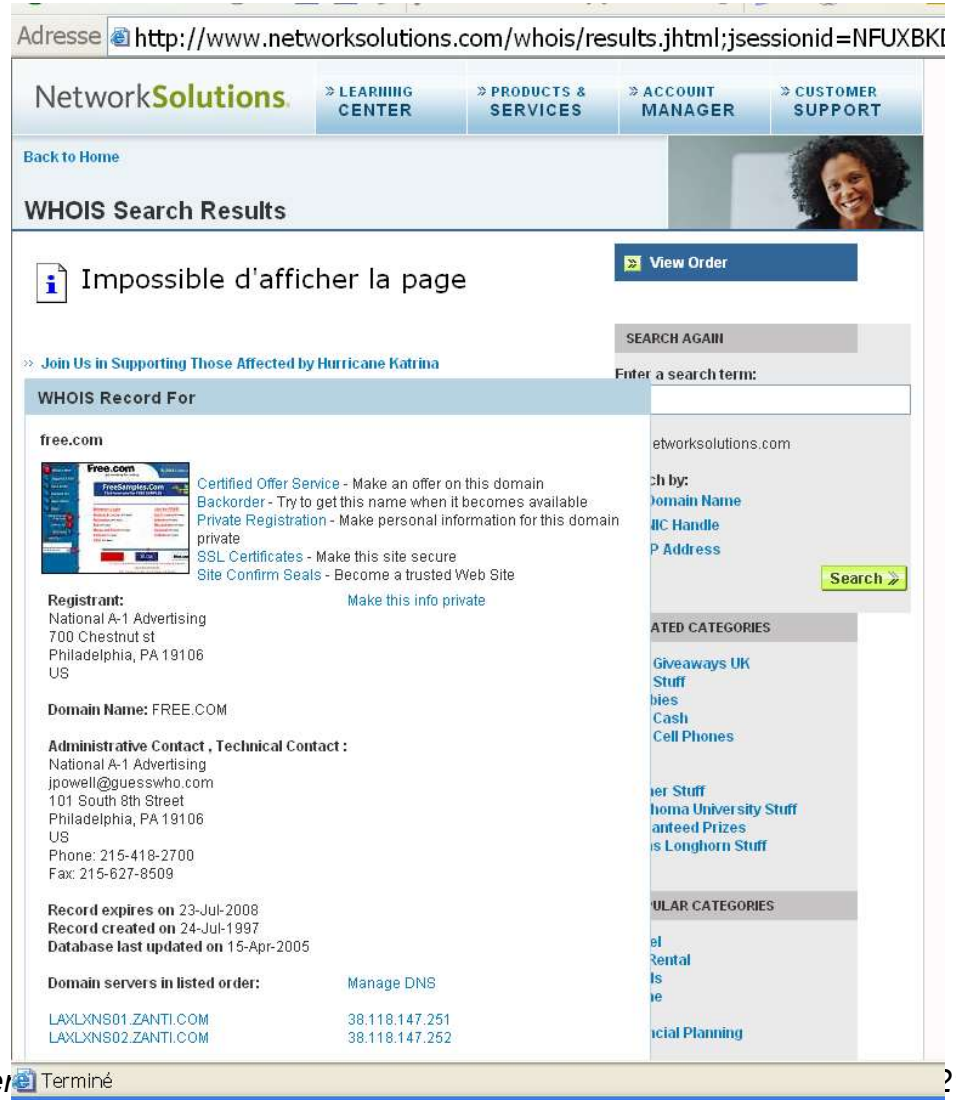
- D
a
- I
- S
- T out
- M the network
- Type of firewall and IDS (Intrusion Detection System)



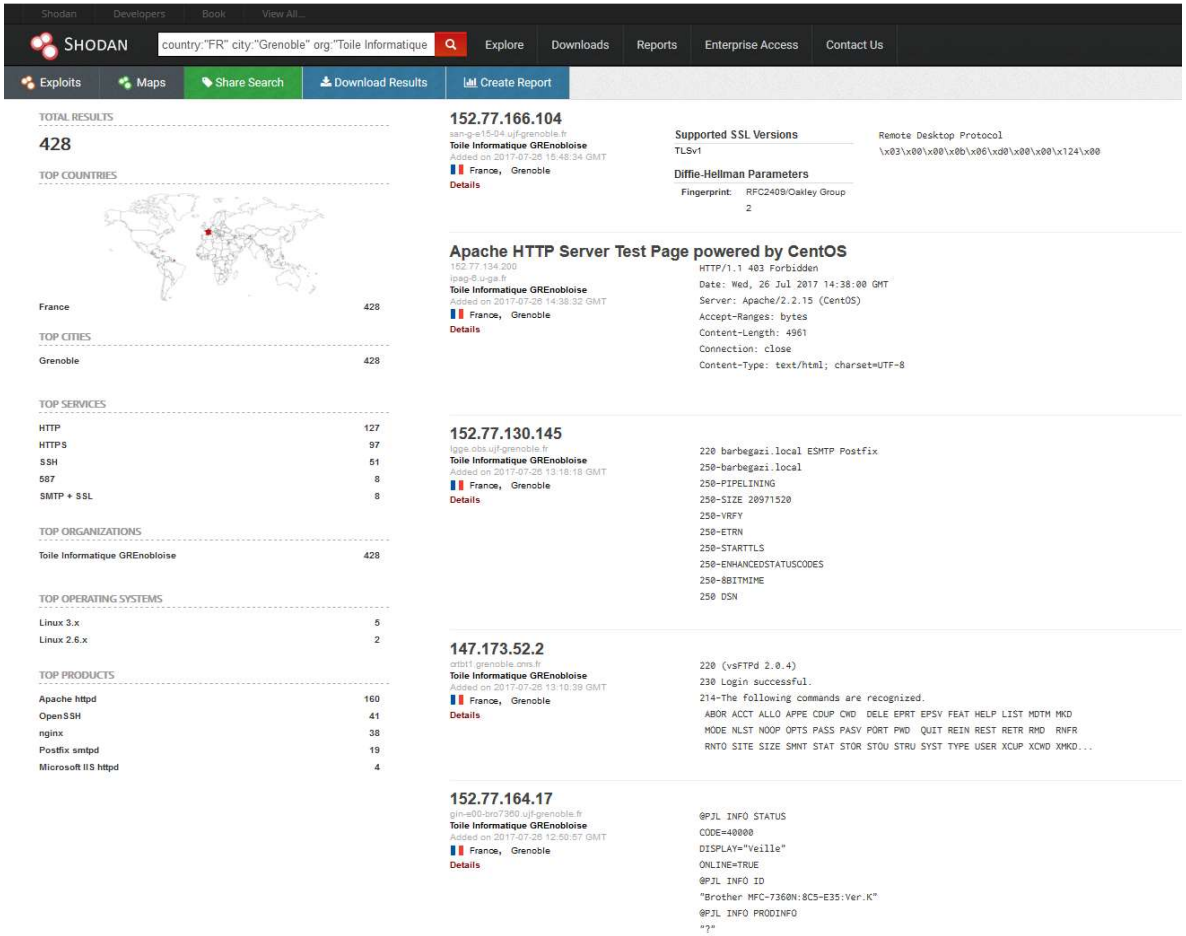
2.2.1 Recognition and collection of information (2/3)

- User names, groups, routing tables, SNMP information (techniques of enumeration of the sources of the system)
- Physical location of the equipment and systems
- Used network protocols (IP, IPv6, IPSec, SSL)
- Cartography of the network
- Type of access connections
  - Traditional access (frame relay, broad band)
  - Access by classical telephone (modem)
  - Wi-Fi Access
- Approach by “social engineering” (consists in questioning people and recovering information by trapping them)
  - Information on the people, their names, telephone numbers, situation in the company, addresses…

2.2.1 Recognition and collection of information: WHOIS (3/3)

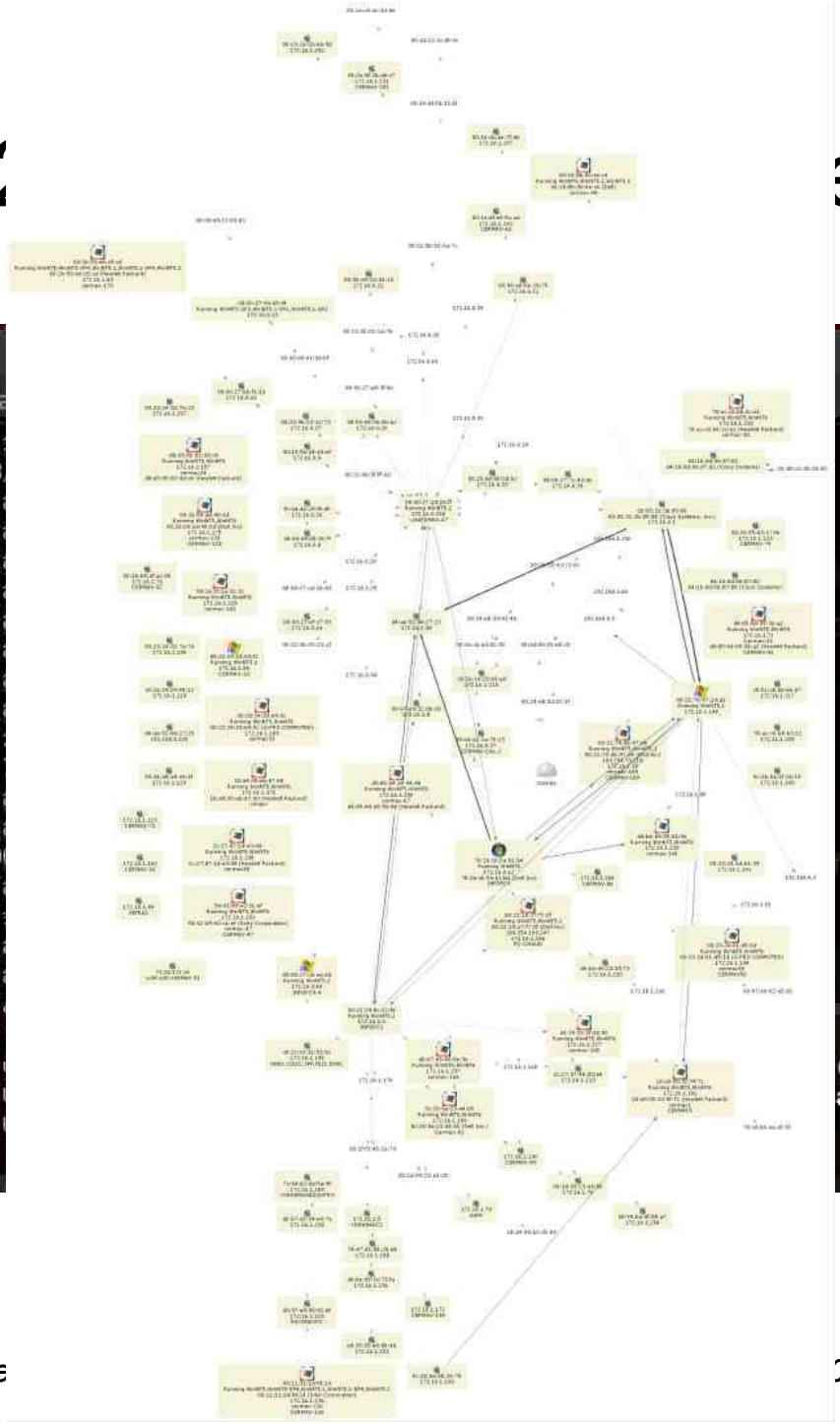


2.2.1 Recognition and collection of information: WHOIS (3/3)



2.2.2 es and the

- Detailed Sca k Mapper)
- the



2.2.4 Obtaining an access

- Tackle at the operating system level
  - Use of the functionalities of the O.S.
- Tackle at the application level
  - Use of the functionalities of the application
- Attack benefiting from a bad configuration
  - “Opened” system, default configuration (administrator name and password!), many activated functionalities
- Attack using lodged scripts
  - Scripts available on the system and sometimes activated by default (Unix/Linux)
  - Détournement de requêtes SQL lors de l’interrogation d’une base de données via interface web
- Automated Attack (ex: scan of port 80 of a whole C-class block of addresses in order to seek a fault)
- Targeted Attack : much rarer but difficult to detect (experienced pirates)

2.2.5 Extension of the acquired privileges

- If the pirate succeeded in entering on the system with a “weak” password => extension of the rights (authorizations)
  - To carry out code to obtain privilege
  - To seek to decipher other passwords
  - To scan for non ciphered passwords
  - To seek possible inter-network relations
  - To identify badly configured files or shared resources permissions

2.2.6 Cover the traces

- To dissimulate to the administrator the fact that one penetrated the system
  - Windows: To eliminate the entries (inputs) in the event logs and the registers
  - Unix: to empty the file of history (execution of the program *log wiper*)
  - ! The attacker cleans the log files but does not remove them!

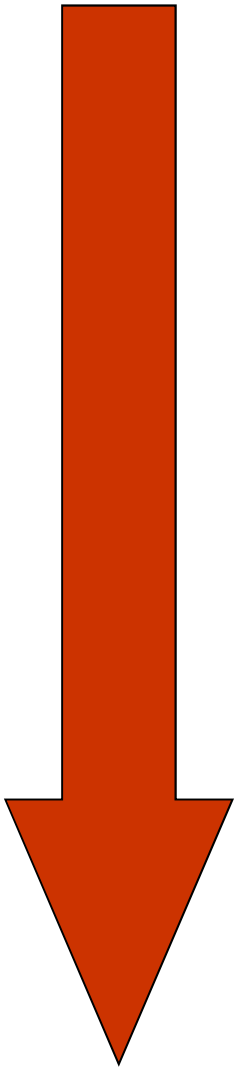
Risk Analysis:
Type of incidents as a level of gravity

Tolerable

Dangerous

Inadmissible

Very critical



- Simple observation
- Record of observed data
- Penetration with a false identity
- Identity substitution
- Modifications of data (limited)
- Destruction of data (limited)
- Perturbations of the services (slow down)
- Denial of service
- Destruction of service
- Stop of the machine (boot required)
- Stop of a server (loss of all the data, needs a reinstallation…)

M33-2. Cyber-attaques

- Définitions :
  - Les types d'attaques
  - Attaques TOIP
  - Les attaques APT
  - Détection des attaques
  - Étude de cas

Attacks types and solutions

- Deny Of Service DOS
- Sniffing
- Scanning
- Social engineering
- Cracking
- Spoofing
- Man in the middle
- Hijacking
- Buffer overflow

Attacks types and solutions

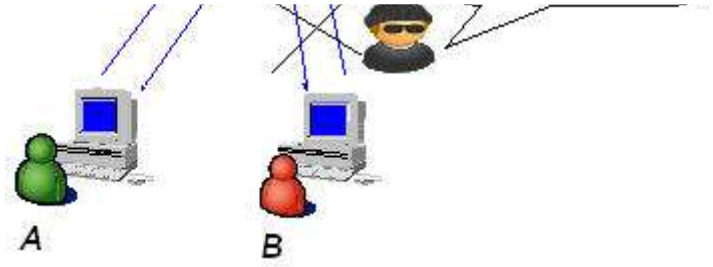
- Deny of Service (DOS)

How to protect?

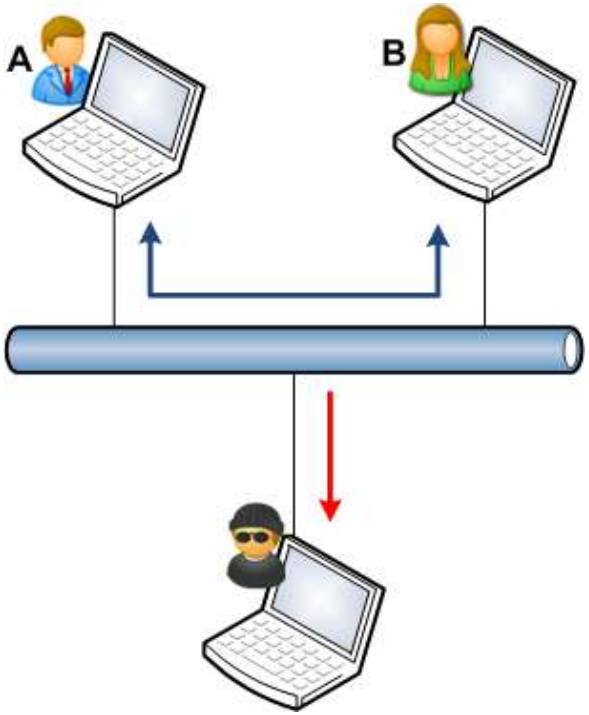
- No real solution
- Use of a probe for the detection of the attack

access the network

  - Used against a server as a client
  - All the OS are concerned

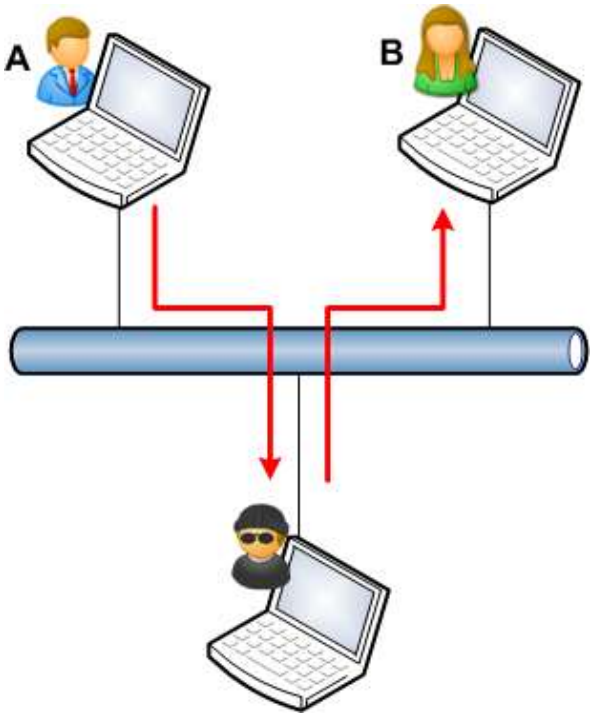


Les types d'attaques



Passive listening

The attacker is able to listen to conversations between A and B (**confidentiality** violation of exchanges).



Active Listening

The attacker is able to fit into the conversation between A and B without them knowing about it (breach of **confidentiality** and **integrity** of the exchanges).

Attacks types and solutions

- Sniffing

How to protect yourself?
Preferably use a switch rather than a hub.
Use encrypted protocols for sensitive information such as passwords.
Use a sniffer detector.
Taken not to leave equipment connected without

Attacks types and solutions

- Scanning
  - Scan all ports of a

How to protect yourself?

Scan your machine for open ports know

Close unnecessary ports using a firewall

Use an intrusion IDS

scanner will deduce if the ports are open.

  - Allows to know the weaknesses of a machine and so know where to attack.

Attacks types and solutions

- Social Engeneering
  - It is a technic to

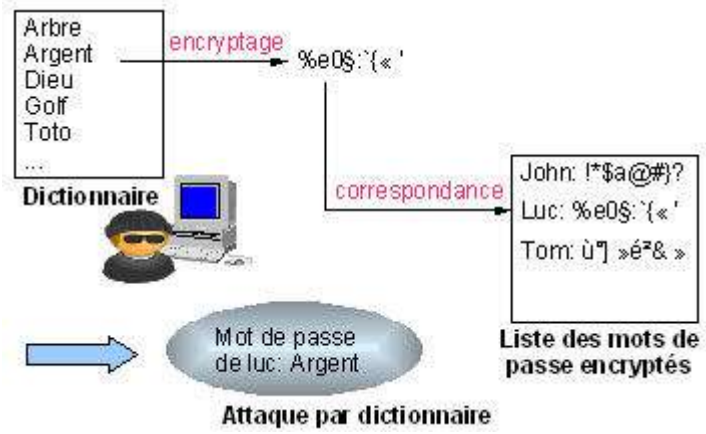
How to protect yourself?
Be well advised
Pay attention to the information that is left on the Internet
and in particular on socials networks

phone, letter, mail

  - If it is done well it can be very efficent

Attacks types and solutions

- Cracking : Breaking passwords
  - Guess victim's password
  - Too often passwords used are to easy (children names, birth date…)
  - Uses dedicated software often based on signature comparisons
  - Hash functions used to encode passwords only works in one direction



Attacks types and solutions

- Cracking :
  - dictionary attack: software tests all passwords stored
  - hybrid attack : software tests all passwords stored in a text file and adds combinations. For

How to protect yourself?

Choose a strong password and do not write on a medium other than your own memory

Regularly change password

all possible combinations. So this kind of attack always work. However this solution may not work in a human time.

Attacks types and solutions

- Spoofing

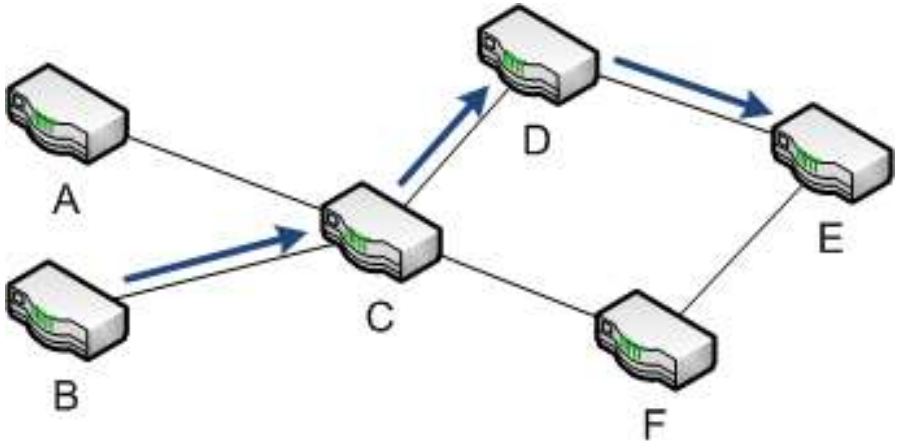
How to protect yourself?

No solution to prevent

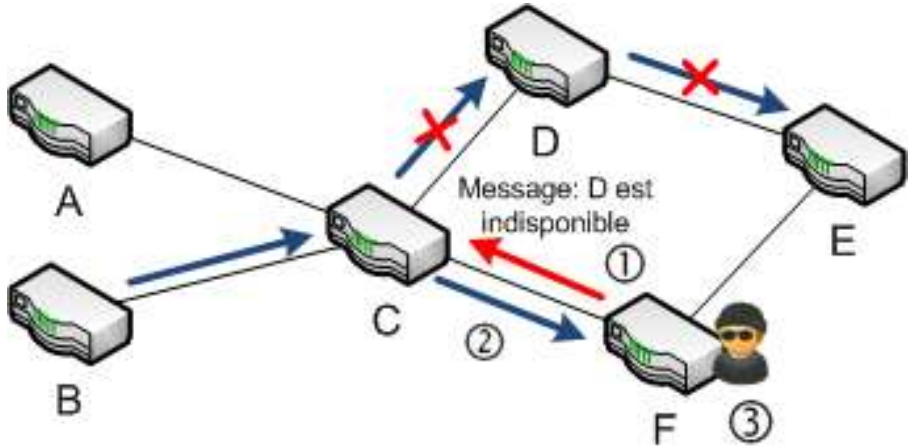
Use mechanisms to determine the trust (electronic signature mail, secure protocols ...)

– Of website = Phishing

Les types d'attaques



Each router has a routing table that tells which neighboring router to transmit the datagrams. This table can be updated dynamically according to network events (BGP, RIP, OSPF, etc.).



Aim of the attack: **to route the packets** to the network E, to the network F controlled by the attacker.

Method :

The attacker uses a weakness of the routing protocol to indicate to the router C that the router D is unavailable, and that the router F can route the packets to E;

②outer C therefore transfers the packets for E to F so that they can be routed to destination;

③ Depending on the purpose of the attacker, the attacker can decide whether to route the packets to E.

Attacks types and solutions

- Man in the middle
  - Purpose: to insert

How to protect yourself?

Use secure protocols in interactions between machines

Only connect to trusted machines.

trying to connect. Now, if a pirate decides to be the computer A to B and B to A, then all communication between A and B will be sent to the pirate.

Attacks types and solutions

- Hijacking
  - Intercept a session

How to protect yourself?

Use secure protocols

  - User password not necessary

Attacks types and solutions

- Buffer over flow

How to protect yourself?

No direct solution since it is based on errors or weaknesses in programming

Be sure to apply patches and updates to programs you use.

not check the length of the string passed as a parameter, an attacker can compromise the machine by entering something to long.

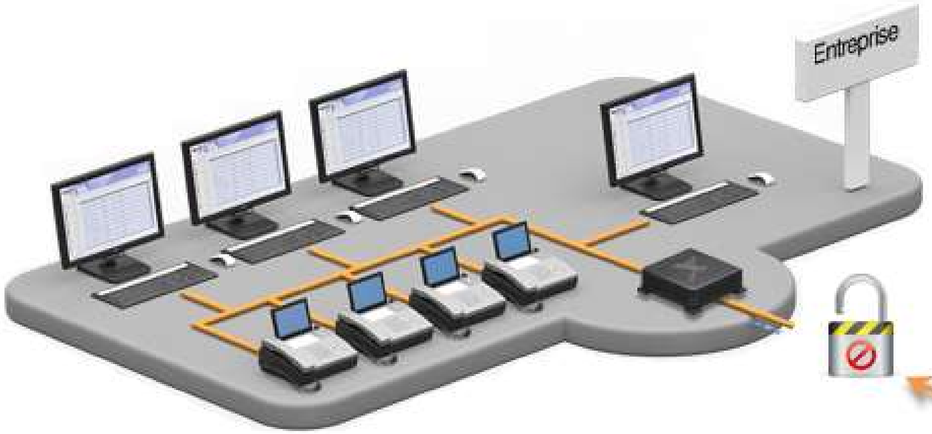
VOIP attacks

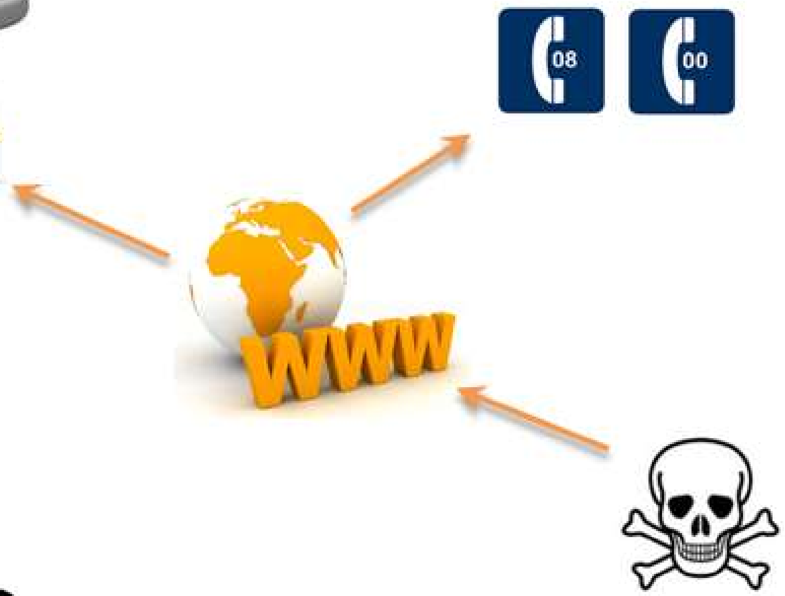
- 3 Types of attacks
  - Over IP
  - Voicemail
  - Administrator

UGA

3 Ils détournent des appels frauduleusement vers l'international (Cuba, Balkans, Afrique) et les numéros surtaxés (0899) et les revendent à des opérateurs internationaux.

Faille : Toutes les destinations sont autorisées sur le standard téléphonique.





2 Ils se connectent sur le standard téléphonique en trouvant les identifiants / mot de passe d'un compte utilisateur par brute force.

Faille : Mot de passe trop simple (0000, 1234, etc.)

1 Les pirates utilisent le réseau Internet pour chercher des installations téléphoniques non-sécurisées.

Faille : Firewall non activé ou mal paramétré

VOIP attacks

- Voicemail

Most of the time, users within companies do not customize access code to their voicemail. Some PBXs then give the possibility to make calls. This fault is used by hackers to turn the phone user's gateway to send to premium rate numbers, numbers of servers games, recharge account numbers (such as Paypal).

VOIP attacks

- Example of pirates methodology
  On the voicemail
  - Allowing to be returned before or after filing message.
  - Allows remote configuration

  Pirates procedure
  - Try to call company phone numbers
  - If they come on a voicemail? Menu navigation (browsing, configuration)? Entering the password? Phone number for tranfer…
  - Call to the user, transferred to voicemail which itself refers to a distant destination ...!
  - How to avoid being identified immediately, disable forwarding after use.

VOIP attacks

- Administrator

Phone systems had a management interface that can be hacked if the personal identifiers are not so complex.

The risks are the following:

Transfer call authorization to outside

Programming transfer

- User,
- Messaging
- IVR (Interactive Voice Server)

Managing passwords (reset)

Trace log management

VOIP attacks

- Example of pirates methodology
  1 - Access to the PBX administration
    - Find IP Address
    - Follow configuration documentation
    - Trying default constructor passwords

  2 - Changing the configuration
    - Configure transfers

  3 - After use
    - Restore Configuration
    - Delete the server log

  4 - Provide the following
    - Explorer configuration
    - Possibly other open access to government

VOIP attacks

- Piracy consequences

Companies face enormous financial consequences. Many hacks are reported every day in France and several tens of million euros pirated each year.

Piracy Telecom fraud represents ten thousand euros to hundred thousand euros. The largest recorded case in France is 600.000 euros.

Most of the time, piracy takes place during closed business days periods, especially during weekends, holidays. The company can not detect the problem because nobody controls it. Just few hours of hacking could cost ten thousand euros.

VOIP attacks

- Piracy consequences

For example the case of a french company : Between Christmas and New Year's Day, it was closed. Hackers have penetrated easily the system information using email. Conclusion: 70.000 euros lost.

The main destinations pirated nowaday are the following : Taiwan, Somalia, Cuba, Cayman Islands, Estonia, North Korea, Azerbaibjan, Slovenia, Afghanistan, Global Satellite, Globastar, Egypt, Nigeria, Togo, Sri Lanka, Benin, Ethiopia.

Web attacks

a. Identity theft via cookies

Like all applications, web applications are vulnerable. We will see two of them:

- Weakness based on cookies;
  - This allows - for example - an attacker to bypass an authentication mechanism.

- Weakness based on poorly developed source code.
  - This allows, for example, an attacker to bypass an authentication mechanism, access data to disclose or corrupt it.

Web attacks

a. Identity theft via cookies

Cookies are files managed by web browsers to store (and reuse) user information, for example :

- Its identifier;
- Its preferences for display and layout of the web page

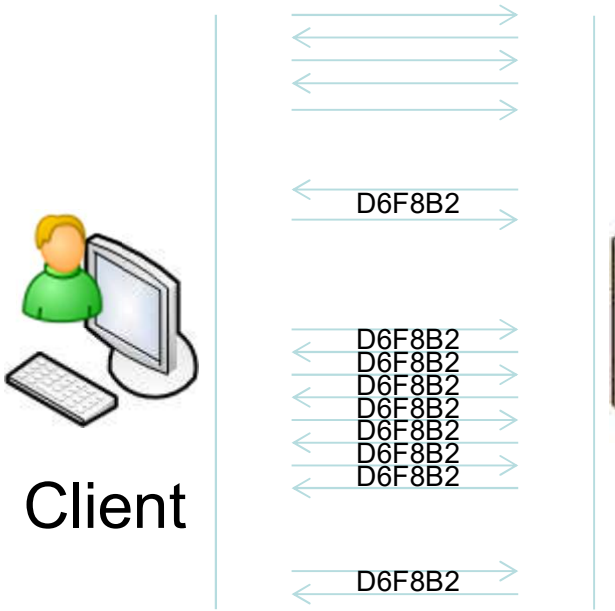
Cookies are required for all dynamic web pages that require to identify or authenticate the user, including allowing the implementation of sessions :

- The merchant sites (in order to display the basket of the user logged in) ;
- The banking sites (to display the account balance of the logged in user and not the account of another customer) ;
- The sites "in general" (in order to display ads targeted on our navigation).

It is possible - under certain conditions - to usurp the identity of a user on a website if one gets to retrieve its cookie of identification.

Web attacks

Usual operation of a connection on a website requiring authentication (merchant site, banking site, etc.) :



① Authentication phase (via a password in general);

② Identification cookie generation phase *. The user is now logged in "on his account"

③ "Navigation" phase: the cookie is included in all exchanges so that the server can identify the user's connection;

④ Logout Phase: The user's session is now closed. The cookie is disabled.

- An identification cookie is actually a random, unique character string, long enough that it can't be generated twice by mistake.
  Example of an identification cookie : D6F8B2BE3ED3040D9A3C10-D6F8B2A305D048B9

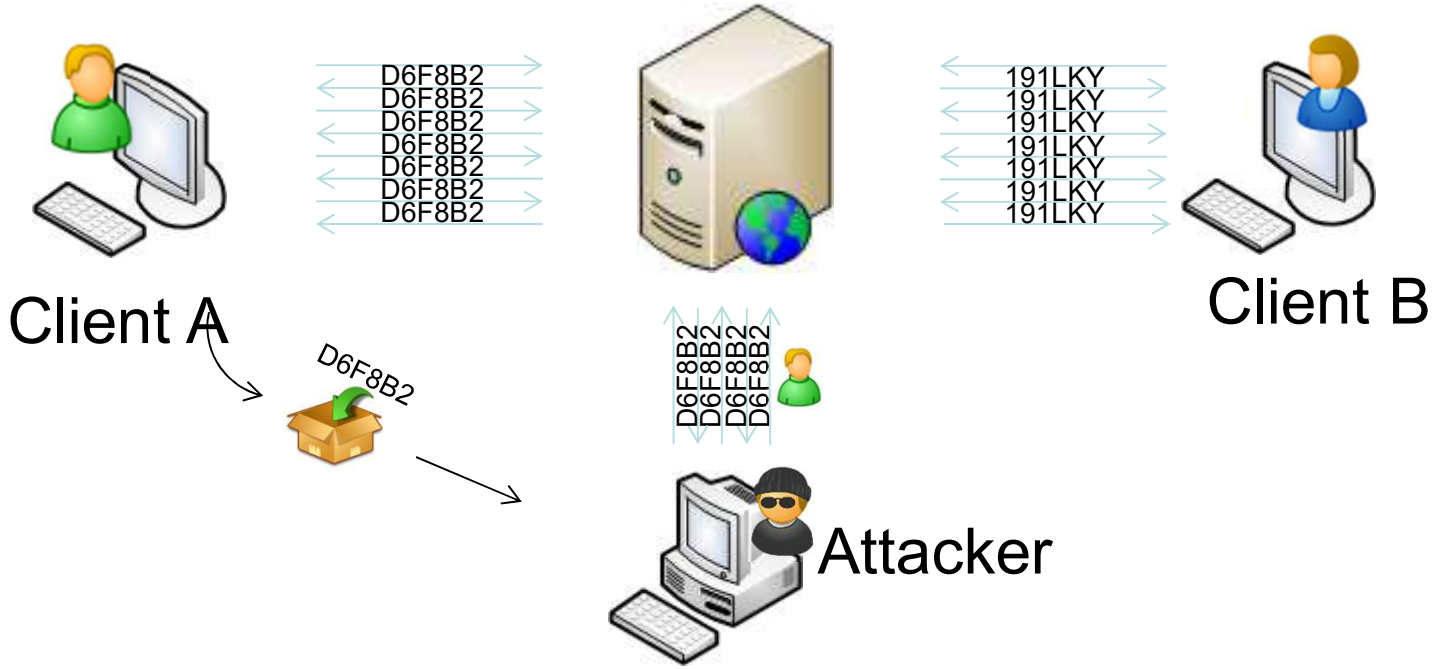
Web attacks

At any time of a connection, each user of the website thus has its own cookie, unique to him. The server is therefore able to identify to whom belongs each connection, and therefore to display the web pages of its own.

Web attacks

But what happens if an attacker gets to steal a user's cookie and connects to the same server?

It passes for the user whose cookie he stole from the application server! It thus usurps the identity of the victim and accedes to his account.



Web attacks

The attacker can steal an identification cookie by different means :

– Either by listening to HTTP network traffic and by intercepting application data, including the cookie ;
  - Means of protection: the user **must ensure that the site to which he is connected uses HTTPS** (the cookie is therefore encrypted during transport).

– Or by stealing the cookie on the workstation using a system vulnerability ;
  - Means of protection: the user must **secure his operating system and software properly** (unnecessary services disabled, installation of security updates, anti-virus, etc. See Module 2 for more information).

– Or by stealing the cookie on the workstation via social engineering methods targeted at the user ;
  - Means of protection: the user must be **sensitized to social engineering methods** (phishing, spam, etc.) in order to “not walk into the trap”

– Or stealing the cookie through a vulnerability on the server ;
  - Means of protection: the server operator must **follow the best practices for securing and maintaining** the server's security condition, as well as **good application development practices**.

Web attacks

b. SQL Injection

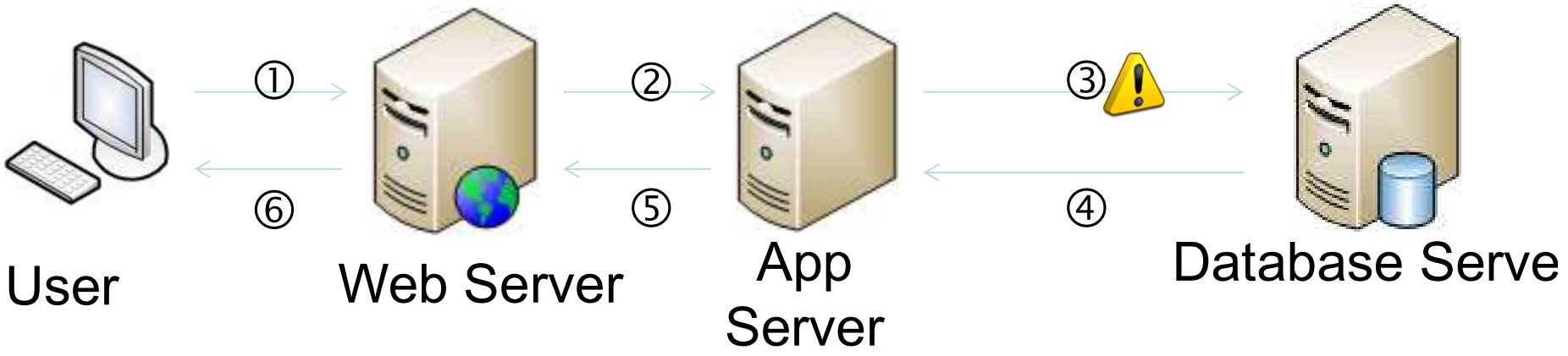
- An SQL injection attack allows an attacker to **interact directly with the database of a website** (although access to this database is of course prohibited);

- The purpose of this type of attack is generally to **circumvent the authentication mechanism, to access or to modify fraudulently** the confidential data of the database (passwords, telephones, credit card number, etc.) ;

- There are multiple possible variations, the next slide shows an example of bypassing a web page.

Web attacks

Software standard architecture of a database-based website



① The client browser prompts for a page ;
② The web server transfers the request to the application server ;
③ The application server generates an SQL query to retrieve the necessary information ;
④ The database server returns the result of the request to the application server ;
⑤ The application server transmits to the web server the information necessary to create the page to be displayed ;
⑥ Web server sends HTML pages to client browser.

Web attacks

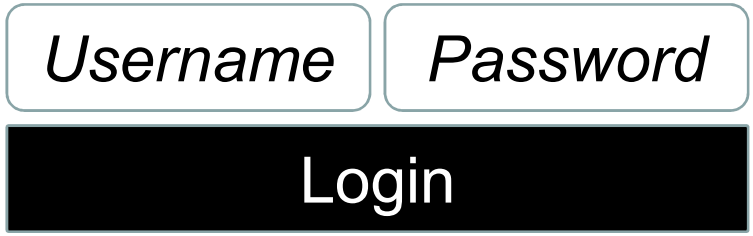
- The purpose of an SQL injection attack is to divert the SQL query from step 3 (previous slide), and - depending on the context - create its own malicious SQL query ;

- The following slide illustrates how such an attack can be conducted from a client browser.

Web attacks

WEB formular:

Enter your username and password and click Login :



$user contains the username entered in the form by the user.
$pwd contains the password.

SQL request to verify username and password is :

```
select count(*) from user where user='$user' and pwd='$pwd'
```

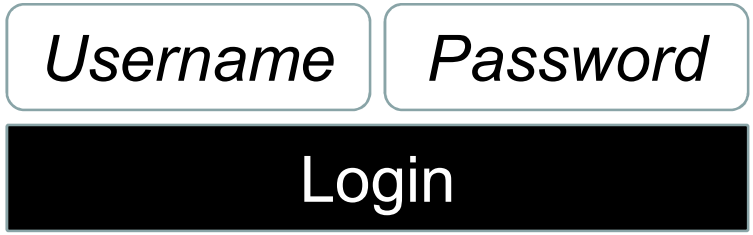
So a normal request could be :

```
select count(*) from user where user='thomas' and pwd='cykUfl9an'
```

Web attacks

WEB formular:

Enter your username and password and click Login.



But what's happening if an attacker enters those following caracters ?
Username : azerty
Password : **abcd' or 1=1/***

SQL request `select count(*) from user where user='$user' and pwd='$pwd'`
become :

```
select count(*) from user where user='azerty' and pwd='abcd' or 1=1/*'
```

This condition is always true

Web attacks

- The condition being always true, the request is always valid, whatever the password given by the attacker ！
  - The / * characters are used to ignore the end of the legitimate query.
- The weakness lies here in the application code: **the data** entered by the user (i.e. an attacker in our scenario) are **not verified / validated**; On the contrary, they are used as they are without any prior verification that they are "harmless“
- How to protect ?
  - **Systematically validate each external data** before using it ;
  - Use **prepared statements**, which have the advantage of being more resistant to injections ;
  - In general, **follow industry-recommended good development practices** regarding PHP code, Java, etc..

APT attacks

- Une **Advanced Persistent Threat** (***APT***) Is a type of stealth and ongoing computer piracy, often orchestrated by humans targeting a specific entity.

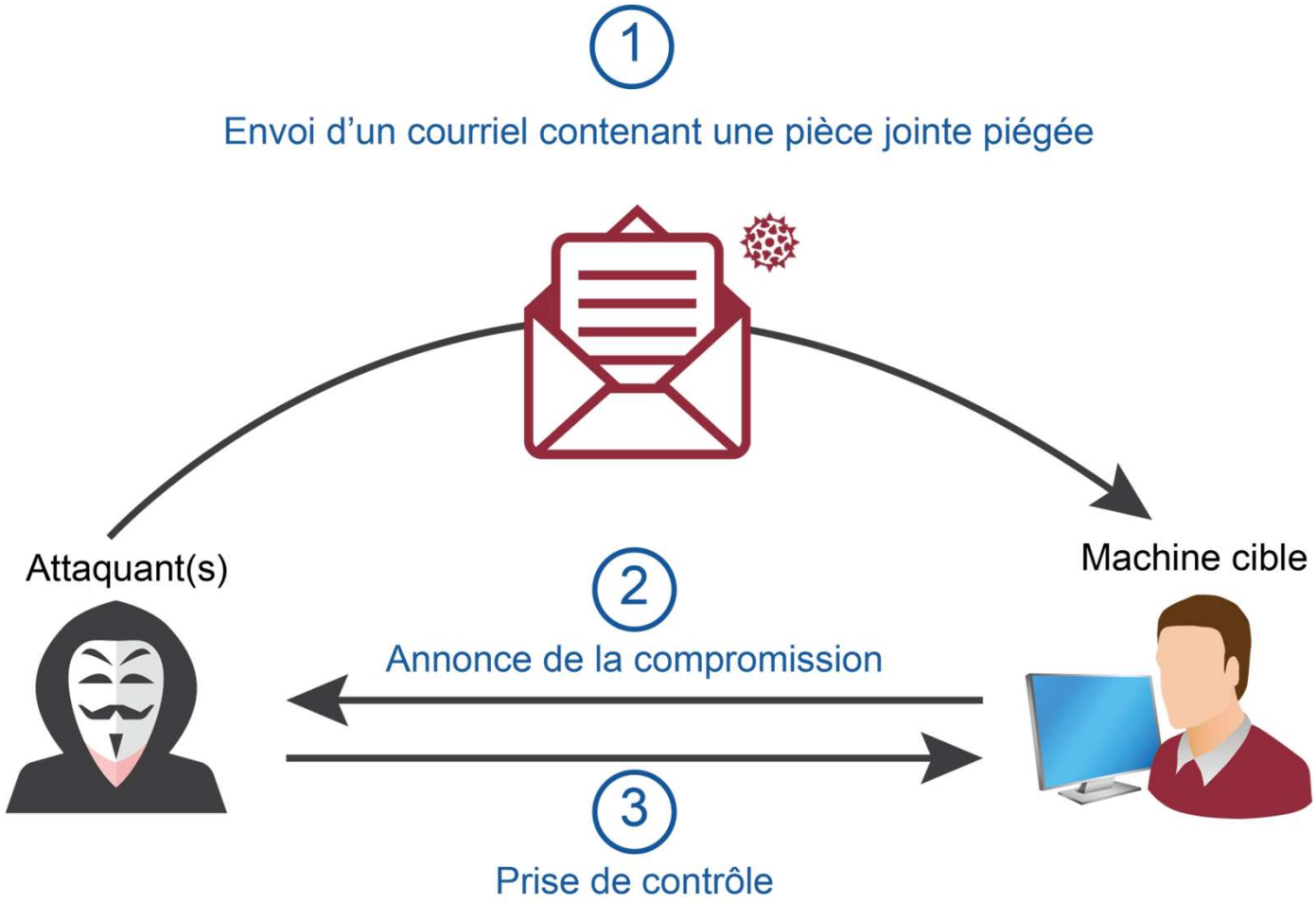
APT attacks

- A APT typically targets an organization for business reasons or a state for political reasons.
- An APT requires a high degree of concealment over a long period of time. The purpose of such an attack is to place personalized malicious code on one or more computers to perform specific tasks and remain unnoticed for as long as possible.

APT attacks

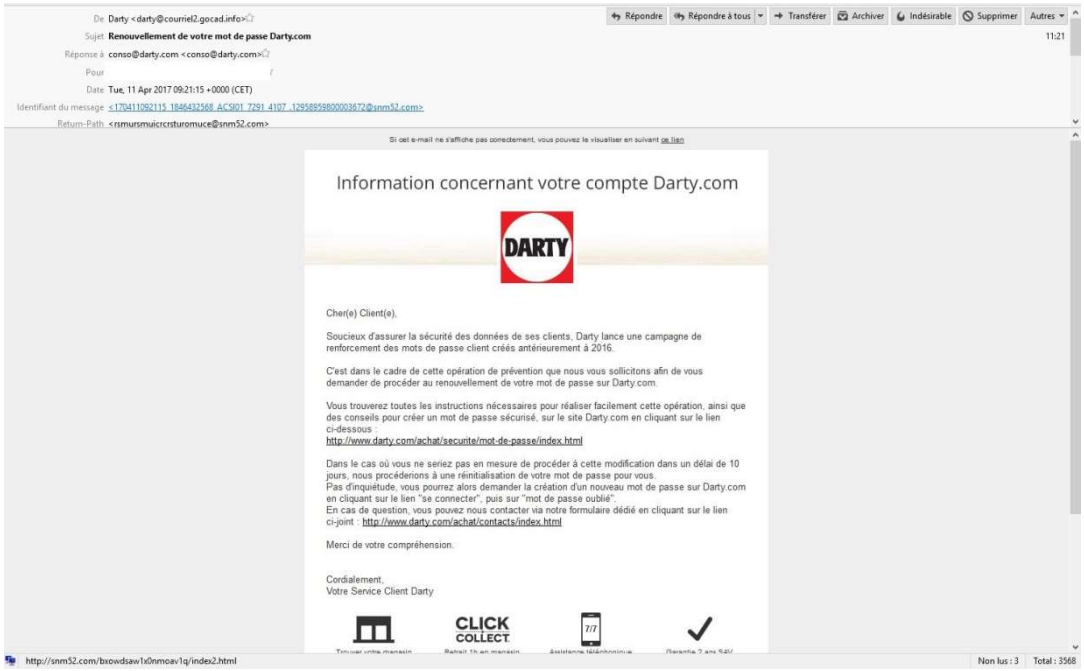
- The term *Advanced Persistent Threat* is also used to refer to a group, as a government, with both the ability and the intention to persistently and effectively target a specific entity.
- An individual, such as a hacker, is usually not referred to as an *Advanced Persistent Threat* because it does not have the resources to be both advanced and persistent.

The course of an advanced attack



The course of an advanced attack

- Initial compromission
  - *Phishing* and *spear phishing*



The course of an advanced attack

- Initial compromission
  - Use
    - Co
    - By
    - Wr
    - De
    - Us

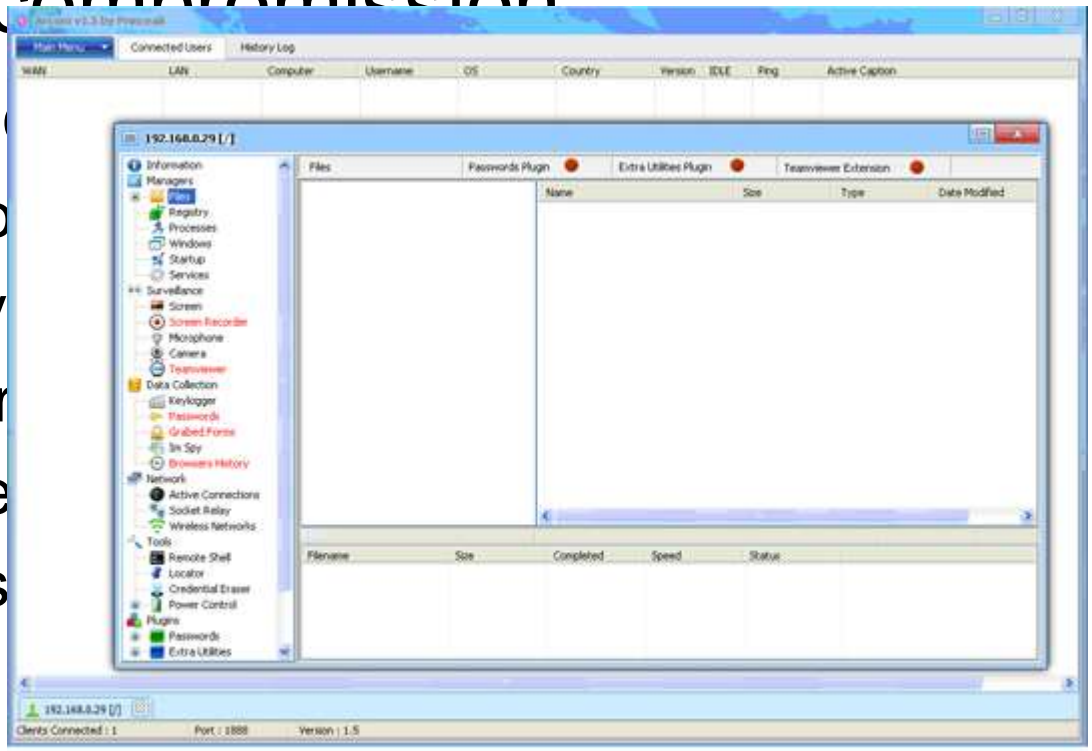
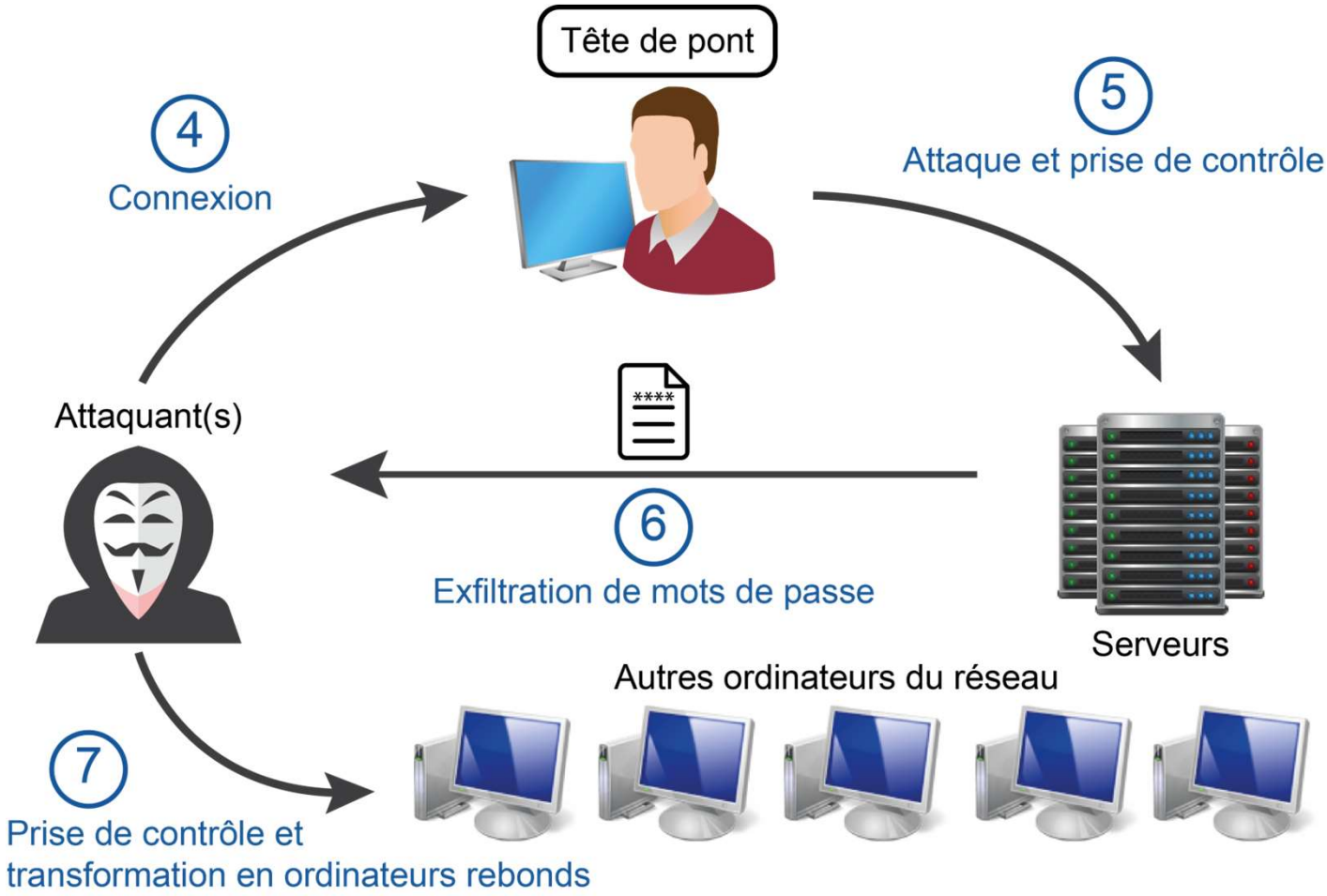


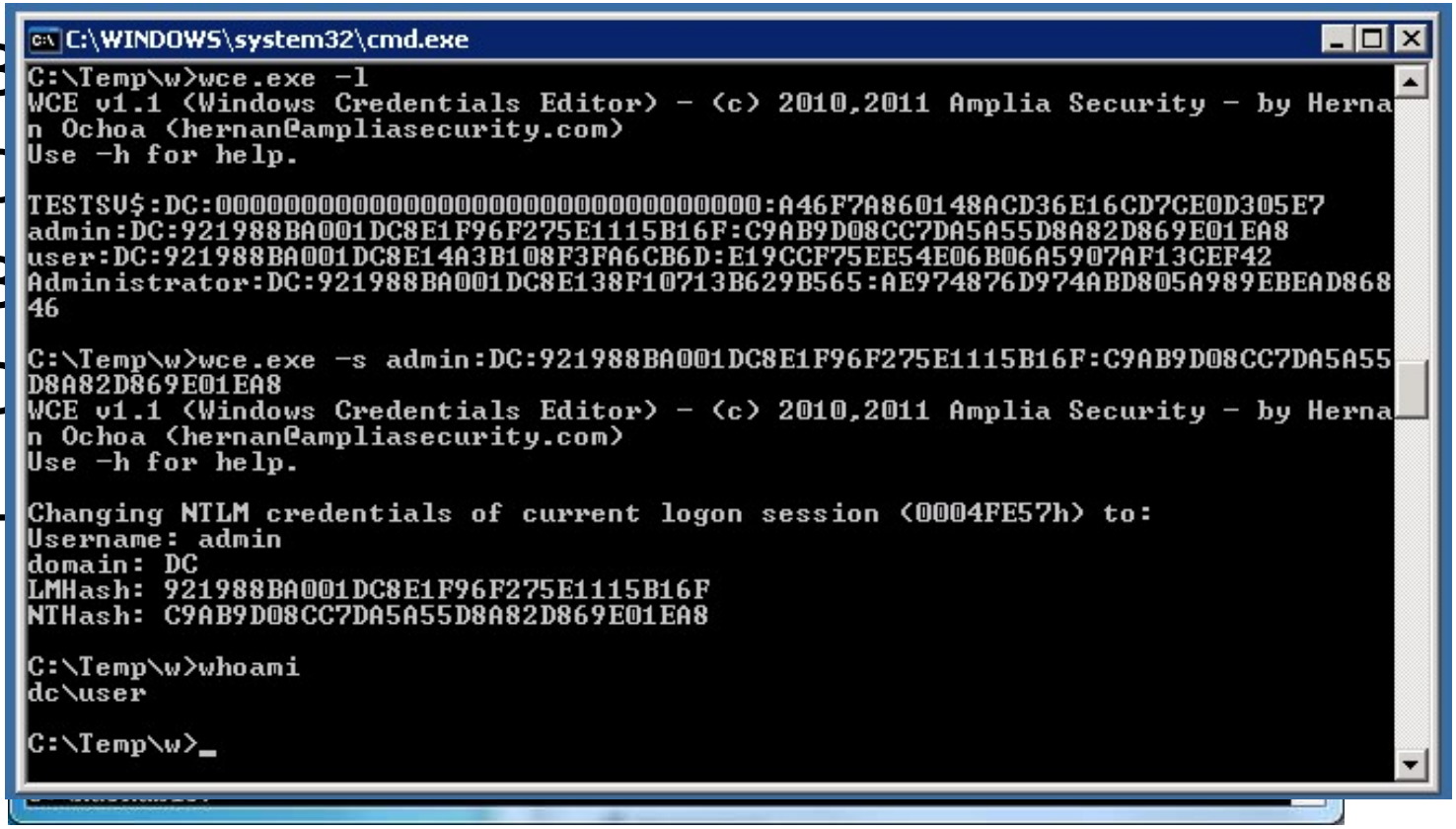
Figure 2. Cybercriminals use this to control compromised systems

The course of an advanced attack

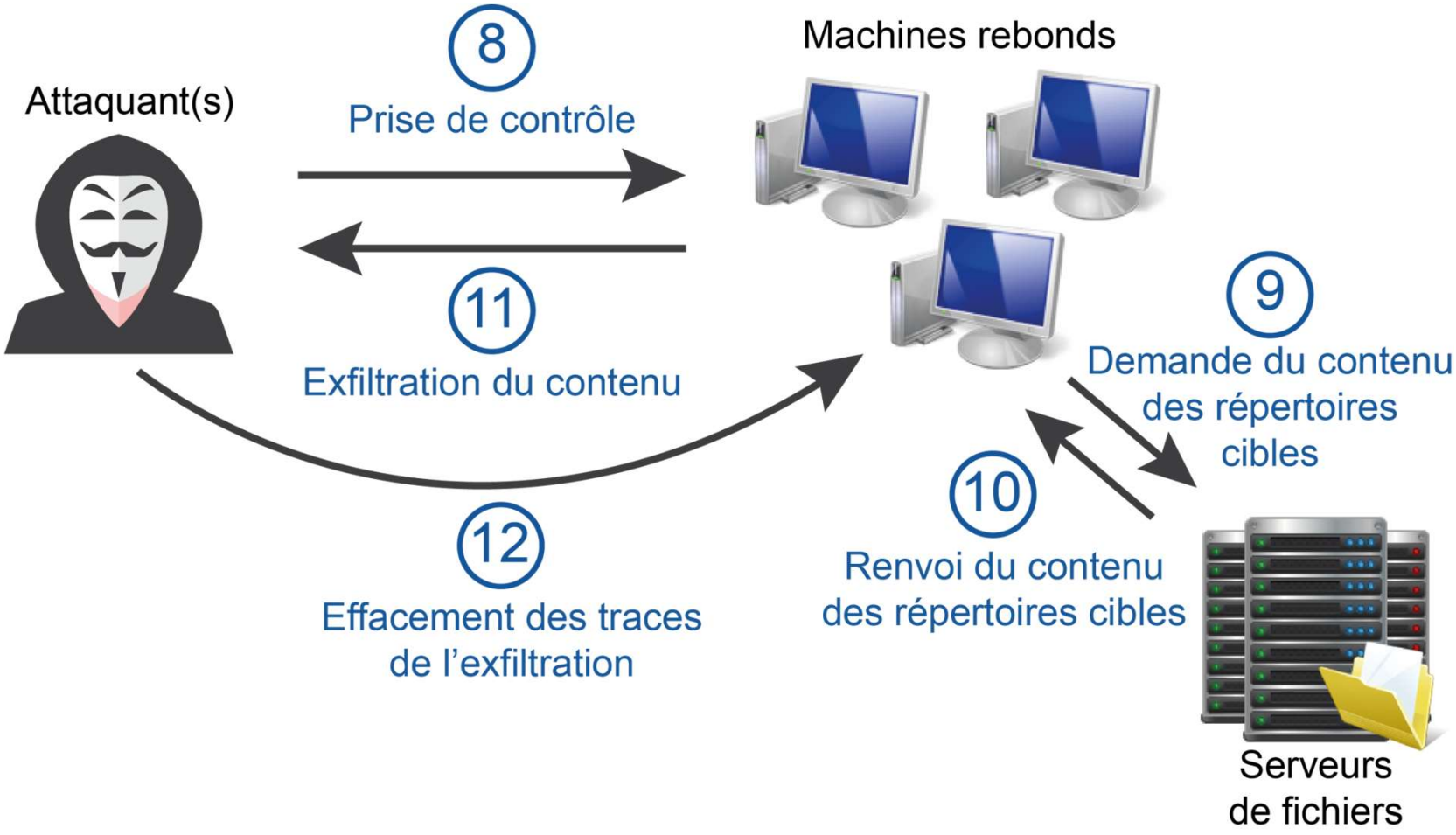


The course of an advanced attack

- Reinforced access and lateral movements
  - E
  - C
  - E
  - D
  - L

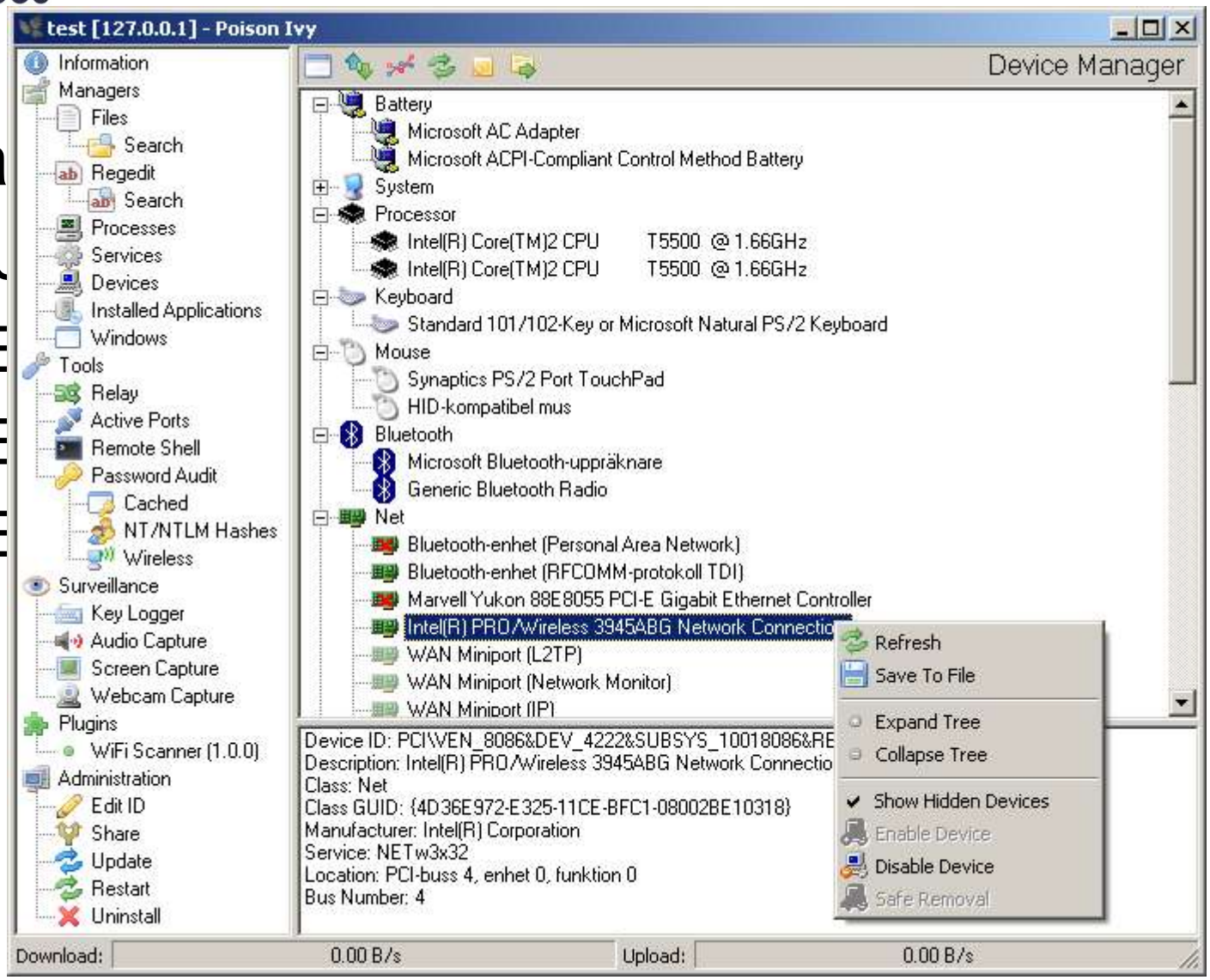


The course of an advanced attack



The course of an advanced attack

- Da
  - U
  - E
  - E
  - E

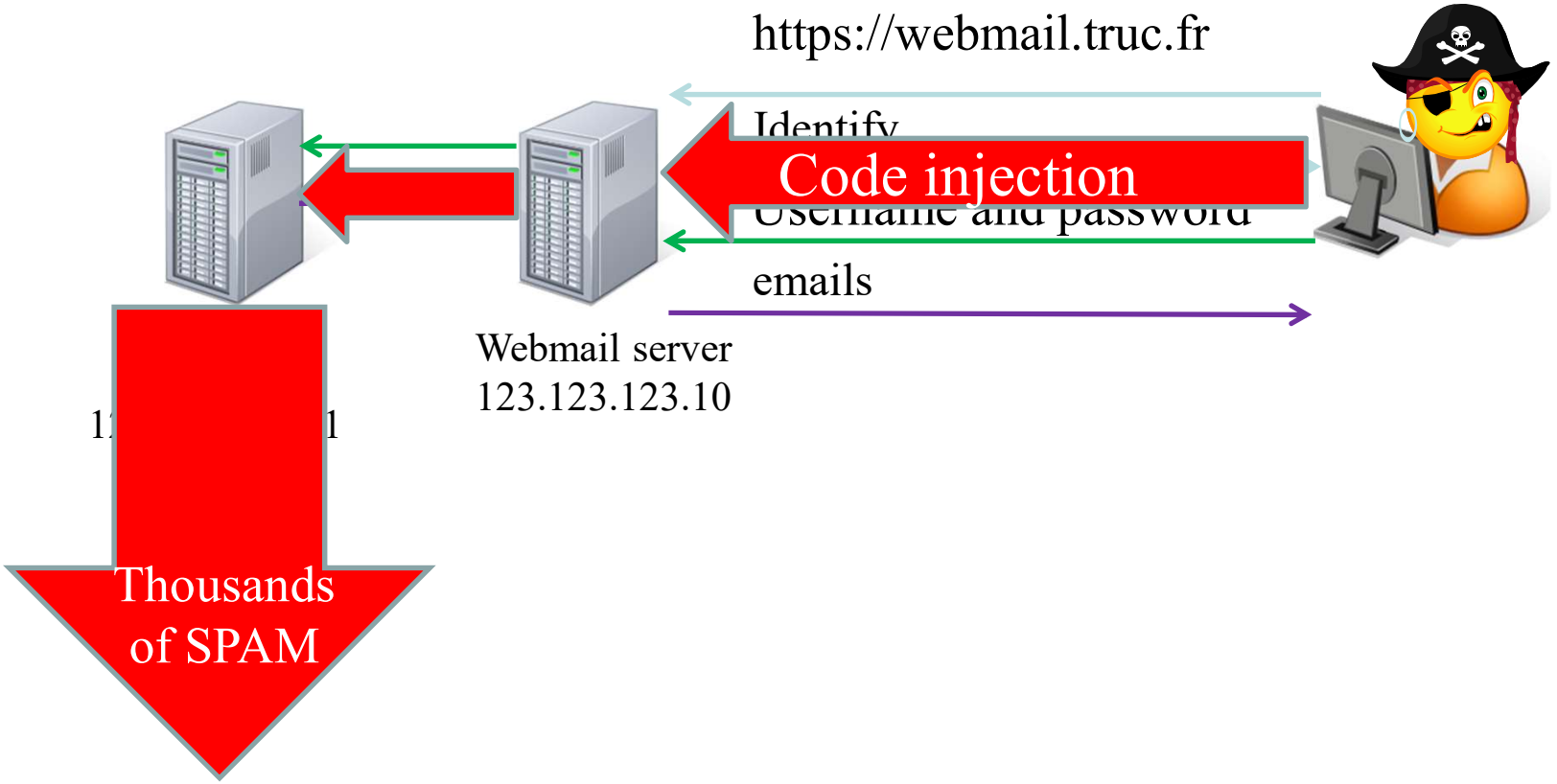


Detection of attacks

- By human beings (culture)
- By specialised software or hardware (anti-virus, firewalls)
- By ports normally non open (alert scans)
- By abnormal reactions
  - During connections, when you are absent
  - Of the applications (slow, double validation)
- By abnormal overloads
  - Network resources
  - Processor, disk, memory resources
- By invalid data
- By data losses

Every abnormal event should incitate to remain very "attentive" !

Case study


https://webmail.truc.fr
Identify
Code injection
Username and password
emails
Webmail server
123.123.123.10
Thousands
of SPAM

Case study

- Logs analysis on webmail server

41.203.69.1 - - [30/Aug/2013:17:43:07 +0200] "GET / HTTP/1.1" 200 4383
41.203.69.1 - - [30/Aug/2013:17:43:07 +0200] "GET /skins/classic/common.css?s=13
66058542 HTTP/1.1" 200 14668
41.203.69.1 - - [30/Aug/2013:17:43:07 +0200] "GET /skins/classic/images/favicon.
ico HTTP/1.1" 200 1150
41.203.69.1 - - [30/Aug/2013:17:43:07 +0200] "GET /plugins/jqueryui/js/i18n/jque
ry.ui.datepicker-fr.js?s=1366058541 HTTP/1.1" 200 1008
41.203.69.1 - - [30/Aug/2013:17:43:08 +0200] "GET /program/js/jstz.min.js?s=1366
058541 HTTP/1.1" 200 4984
41.203.69.1 - - [30/Aug/2013:17:43:08 +0200] "GET /program/js/common.js?s=136605
8565 HTTP/1.1" 200 14799

Case study

- Logs analysis on mail server

Aug 30 17:43:36 serveur36 dovecot: imap-login: Login: user=<hxxxXXXxx>, method=PLAIN, rip=123.123.123.10, lip=123.123.123.11, mpid=1250, TLS
Aug 30 17:43:36 serveur36 dovecot: imap(hxxxXXXxx): Debug: Effective uid=30207, gid=100, home=/home/hxxxXXXxx
Aug 30 17:43:36 serveur36 dovecot: imap(hxxxXXXxx): Debug: fs: root=/home/hxxxXXXxx/mail, index=, control=, inbox=/var/mail/hxxxXXXxx
Aug 30 17:43:36 serveur36 dovecot: imap(hxxxXXXxx): Disconnected: Logged out bytes=29/399
Aug 30 17:43:37 serveur36 dovecot: imap-login: Login: user=<hxxxXXXxx>, method=PLAIN, rip=123.123.123.10, lip=123.123.123.11, mpid=1251, TLS
Aug 30 17:43:37 serveur36 dovecot: imap(hxxxXXXxx): Debug: Effective uid=30207, gid=100, home=/home/hxxxXXXxx
Aug 30 17:43:37 serveur36 dovecot: imap(hxxxXXXxx): Debug: fs: root=/home/hxxxXXXxx/mail, index=, control=, inbox=/var/mail/hxxxXXXxx
Aug 30 17:43:37 serveur36 dovecot: imap(hxxxXXXxx): Disconnected: Logged out bytes=44/533

From hxxxxXXXxx@serveur36.truc.fr Sat Aug 31 14:33:50 2013
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8;
 format=flowed
Content-Transfer-Encoding: 7bit
Date: Sat, 31 Aug 2013 13:33:49 +0100
From: Norman Chan <norman@mail.com>
To: undisclosed-recipients:;
Bcc: hr832000@yahoo.com, hrabino11@yahoo.com, hracca666@yahoo.com,
 hradsky5@yahoo.com, hraeh76@yahoo.com, hrafael99@yahoo.com,
 hraffin@yahoo.com, hraiskin@yahoo.com, hrajappa@yahoo.com,
 hralizadeh_2007@yahoo.com, hrandell1@yahoo.com,
 hranislav_niciforovic@yahoo.com, ... **(thousand addresses….)**
Subject: Hi
Organization: Norman Chan
Reply-To: mrcchannorman@qq.com
Mail-Reply-To: mrcchannorman@qq.com
Message-ID: <ef05796bed486b07e7d63f8fc8c4a02d@cermav.cnrs.fr>
X-Sender: norman@mail.com
User-Agent: Roundcube Webmail/0.9.0
X-UID: 582
Status: R
X-Keywords:
Content-Length: 247

--
Hello, I'm Norman Chan, Tak-Lam, S.B.S., J.P, Chief Executive, Hong Kong Monetary Authority (HKMA). I have a Business worth $47.1M USD for you to handle with me. Contact me on my email (mrcchannorman@qq.com) for more details of the business

URLs

- Organizations
  - https://www.ssi.gouv.fr
  - https://www.ncsc.gov.uk
  - https://www.enisa.europa.eu
  - https://www.cisa.gov
  - https://attack.mitre.org/
  - https://www.cvedetails.com/
- Threat intelligence
  - https://fraudguard.io
  - https://observatory.mozilla.org
  - https://www.shodan.io
  - https://www.virustotal.com
  - https://app.any.run
  - https://haveibeenpwned.com
  - https://osintframework.com/
  - https://www.nomoreransom.org/
  - https://www.exploit-db.com/
  - https://www.threatcrowd.org/
  - https://www.ipneighbour.com/

References

- **Sécurité et espionnage informatique : connaissance de la menace APT**, Cédric Pernet, *Eyrolles*
- **Hackers heroes of the computer revolution**, S. Levy, 2010, *O'Reilly*
- **Learn Social Engineering**, *Dr E. Orzkaya,* 2018, *Packt*
- **Cybersecurity – Attack and defense strategies**, Y Diogenes E. Ozkaya, 2019, *Packt*
- **Digital Forensics and incident response**, G. Johansen, 2017, *Packt*
- **Network scanning cookbook,** S. Jetty, 2018, *Packt*

Exercises

- 1. What are the differences between an active attack and a passive attack?
- 2. What are the conditions of success of an attack?
- 3. Analysis of a Web site (preceding list, to be completed…), contents, interest, interesting or uninteresting parts
- 4. 2nd step to the memoir on security: propose a classification of attacks, with the corresponding strategy to avoid these classes of attacks
- 5. Try to identify some tools (software) which can be used for attacks