Security of information systems

http://www.gipsa-lab.grenoble-inp.fr/~jean-marc.thiriet/miscit/miscit_en.html

Jean-Marc THIRIET, Cyril BRAS

jean-marc.thiriet@univ-grenoble-alpes.fr

4. Cyber-attacks

- Legal considerations
- Why hackers are interested in Information systems and personal computers?
- Hidden economy of cyber-criminality
- Notions of vulnerability, treath, attack
- Type of attacks
- Security organisms

Legal considerations

- Rappel réglementaire :
  - **le seul fait** de collecter des données à caractère personnel par un moyen frauduleux est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende (article 226-18 du Code pénal) => Collect data in a fraudulent (non legal) way, 5 years in jail, 300 000 € penalty
  - **le seul fait** de s'introduire frauduleusement dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans de prison et de 30 000 euros d'amende (article 321-1 du même code) => Fraudulent introduction in an information system, 2 years in jail, 30 000 € penalty

Legal considerations

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 ?

- 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 ?

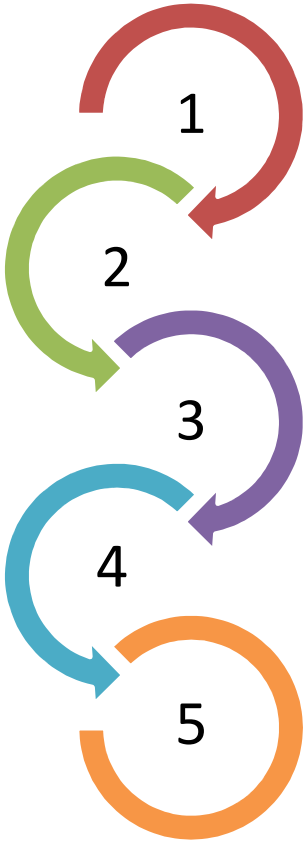
- Cyber Delinquency:
  - Individuals attracted by the lure of gain
  - The "hacktivists“
  - Political, religious, etc.
  - Direct competitors of a targeted organization
  - Civil servants in the service of a country
  - Mercenaries acting for the account of sponsors...

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

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)

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 …

4. Cyber-attacks

- Recipe :
  - Attacks categorization
  - Attack strategy
  - Information recognition and collection
  - Scan services and ports
  - Obtaining Access
  - Extension of acquired privileges
  - Trace Coverage
  - Risk Analysis: Nature of Harm

Types of attacks

The types of attacks are classified in two categories:

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

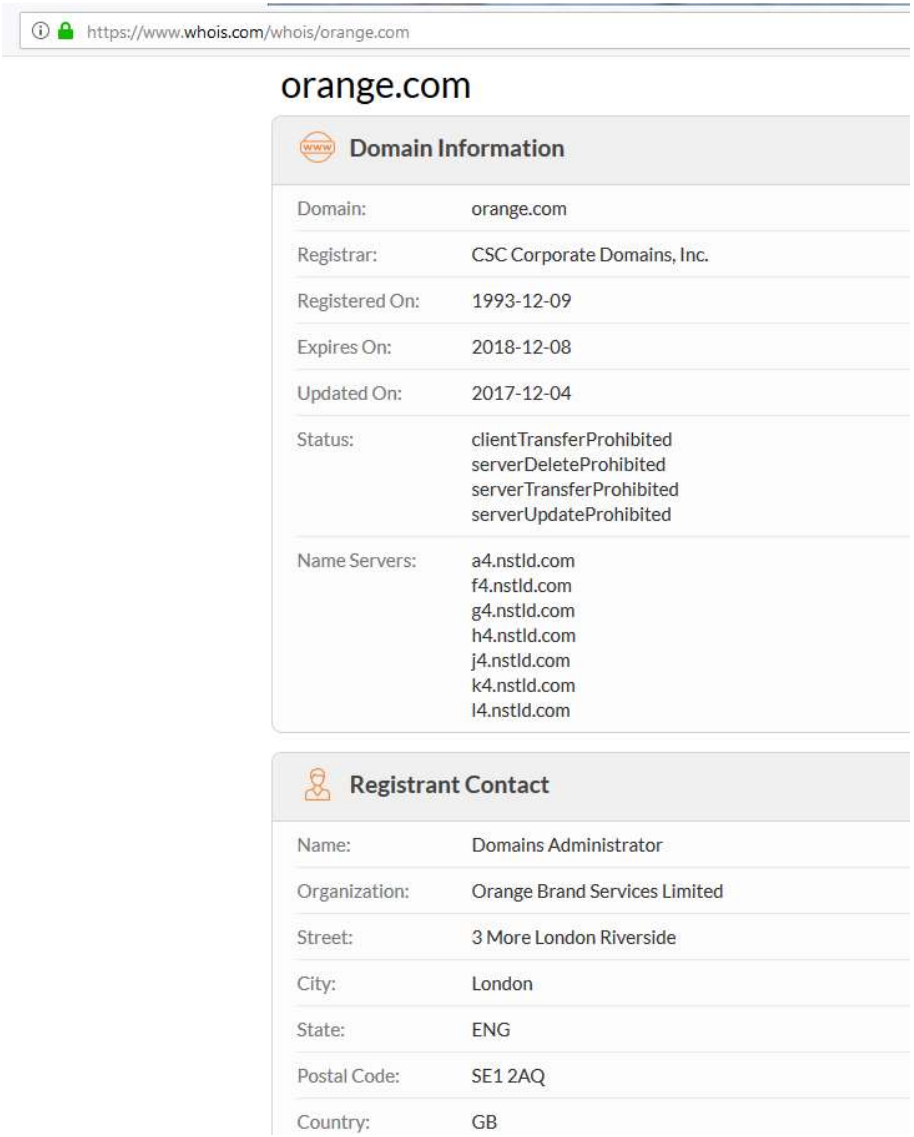
4.2.1 Recognition and collection of information (1/4)

- Domain names, DNS servers, blocks of assigned IP addresses
- IP addresses accessible from outside
- Services presenting a valid target
  - www, ftp, e-mail…
- Types of machines on which the services are carried out
  - Operating systems and number of version => use of the exploitable known faults
- Mechanisms available for the control of the access to the network
- Type of firewall and IDS (Intrusion Detection System)

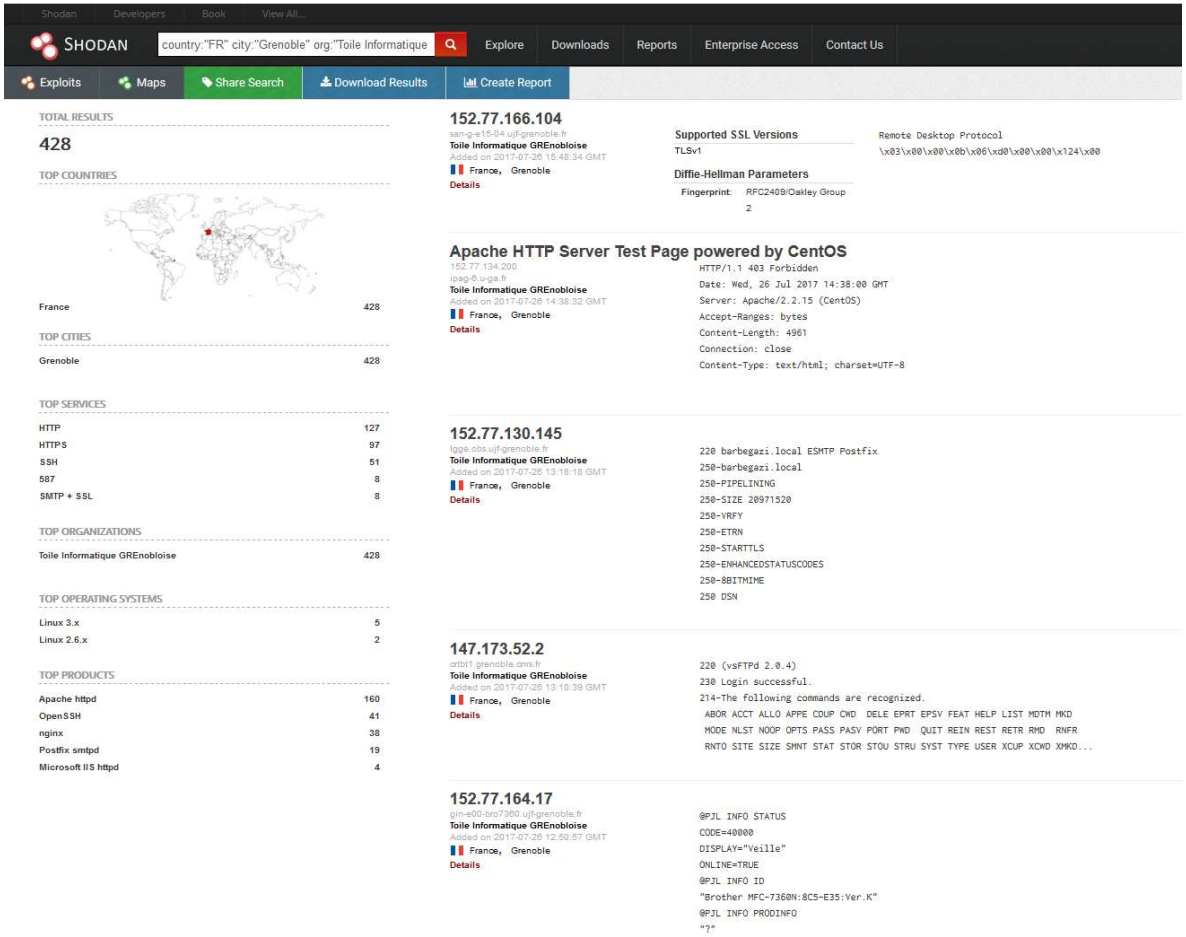
4.2.1 Recognition and collection of information (2/4)

- 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/TLS)
- 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…

4.2.1 Recognition and collection of information: WHOIS (3/4)



Recognition and collection of information : Shodan (4/4)



4.2.2 Scan of the services and the ports

- Detailed Scan of a target (NMAP = Network Mapper)

4.2.3 Enumeration

- Extraction of information on the valid accounts and the resources
  - network resources and shared resources
  - users and groups (as a function of the Operating system)
  - applications
  - character strings sent in response by the equipment

4.2.4 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)
  - Hijacking SQL queries when querying a database via web interface
- 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)

4.2.5 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

4.2.6 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!

- Next Slide 67

4.2.7. 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

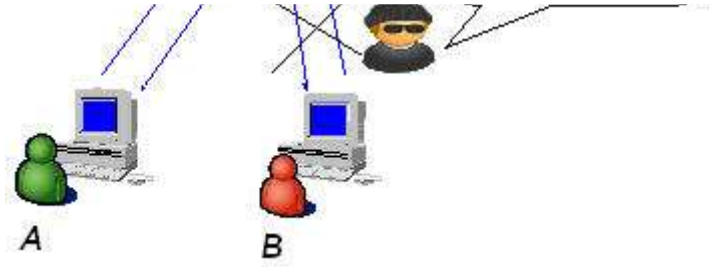
- Deny of Service (DOS)

How to protect?

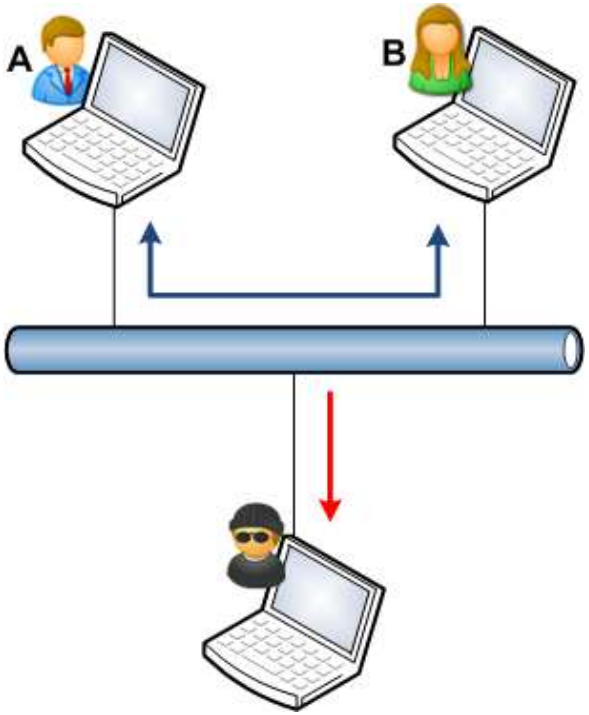
- No real solution
- Use of a probe for the detection of the attack

access the network

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

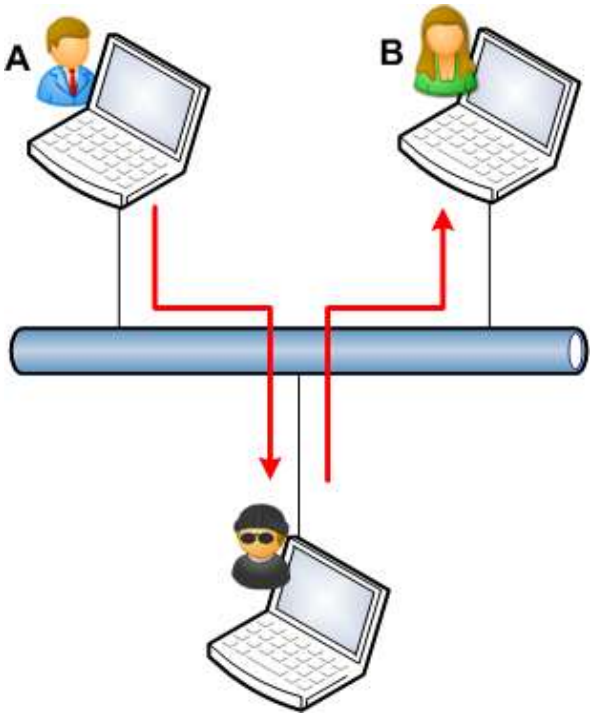


Les types d'attaques



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

their responses, the 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

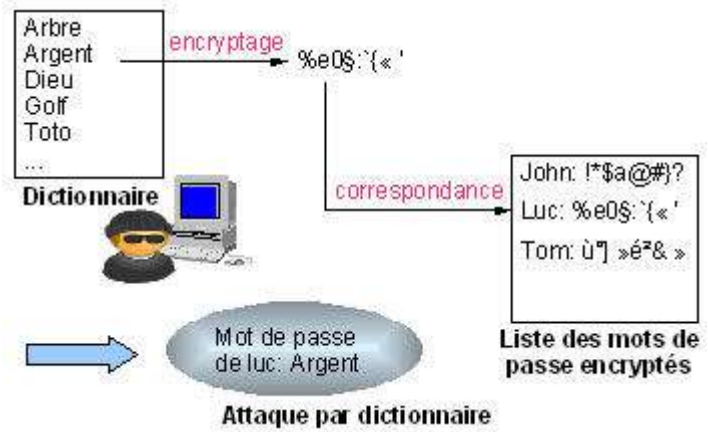
How to protect yourself?
Be well advised
Pay attention to the information that is left on the Internet and in particular on socials networks

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

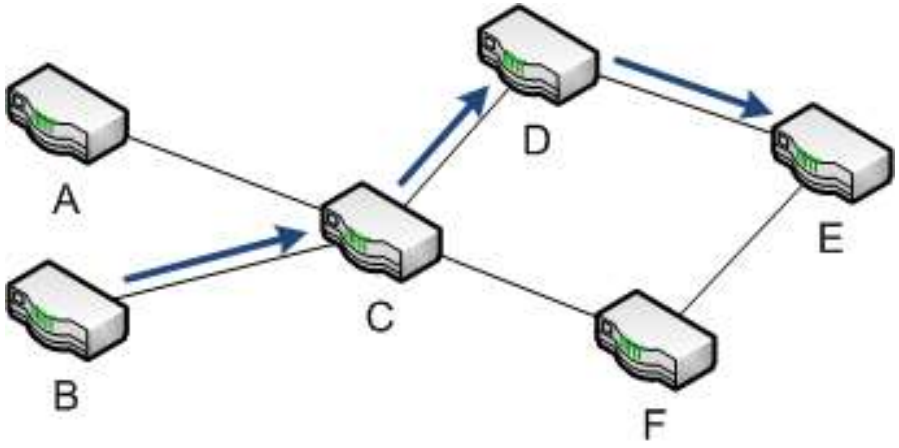
How to protect yourself?

No solution to prevent

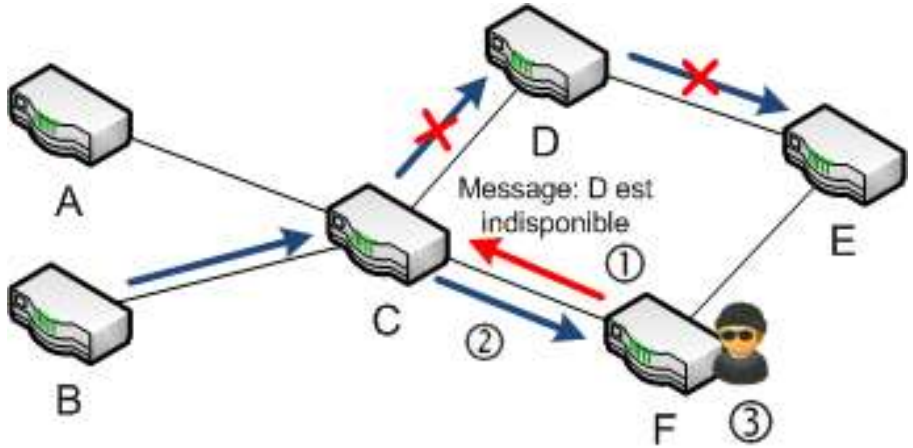
Use mechanisms to determine the trust (electronic signature mail, secure protocols ...)

  - 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

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

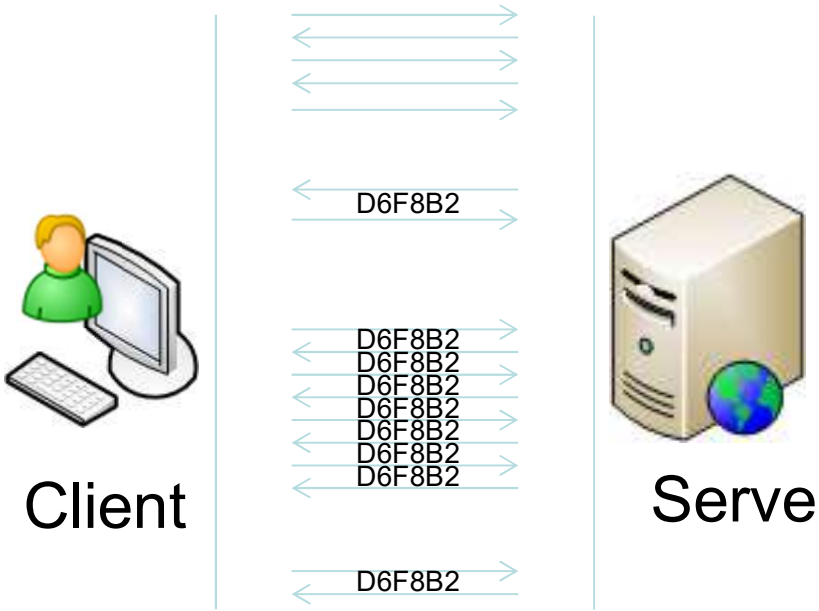
Cookies are required for all dynamic web pages that require to identify or authenticate the user, including allowing the implementation of sessions :

- 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

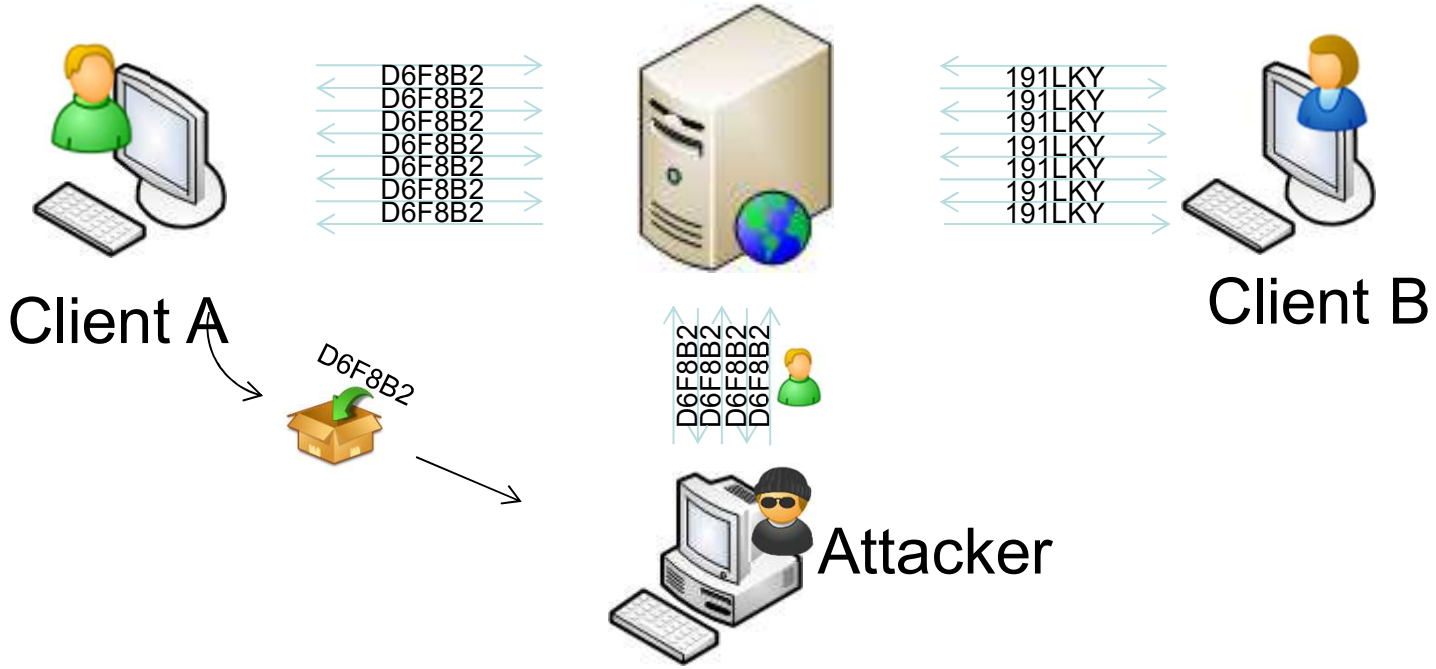
Web attacks

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

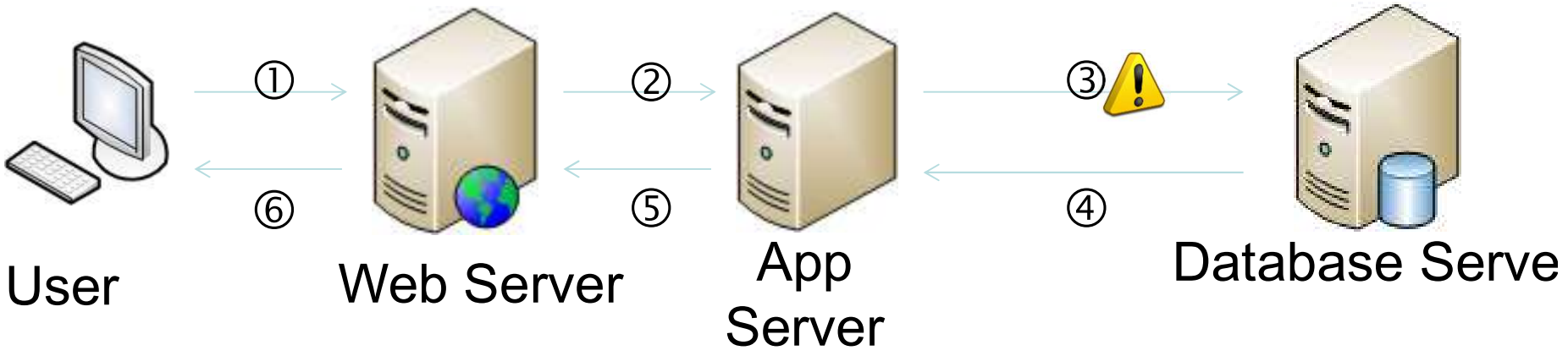
- An SQL injection attack allows an attacker to **interact directly with the database of a website** (although access to this database is of course prohibited);

- 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

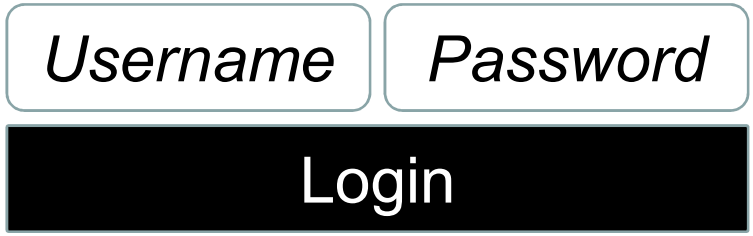
- The purpose of an SQL injection attack is to divert the SQL query from step 3 (previous slide), and - depending on the context - create its own malicious SQL query ;

- 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'
```

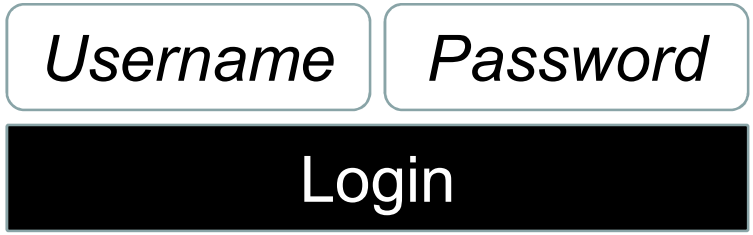
So a normal request could be :

```
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.

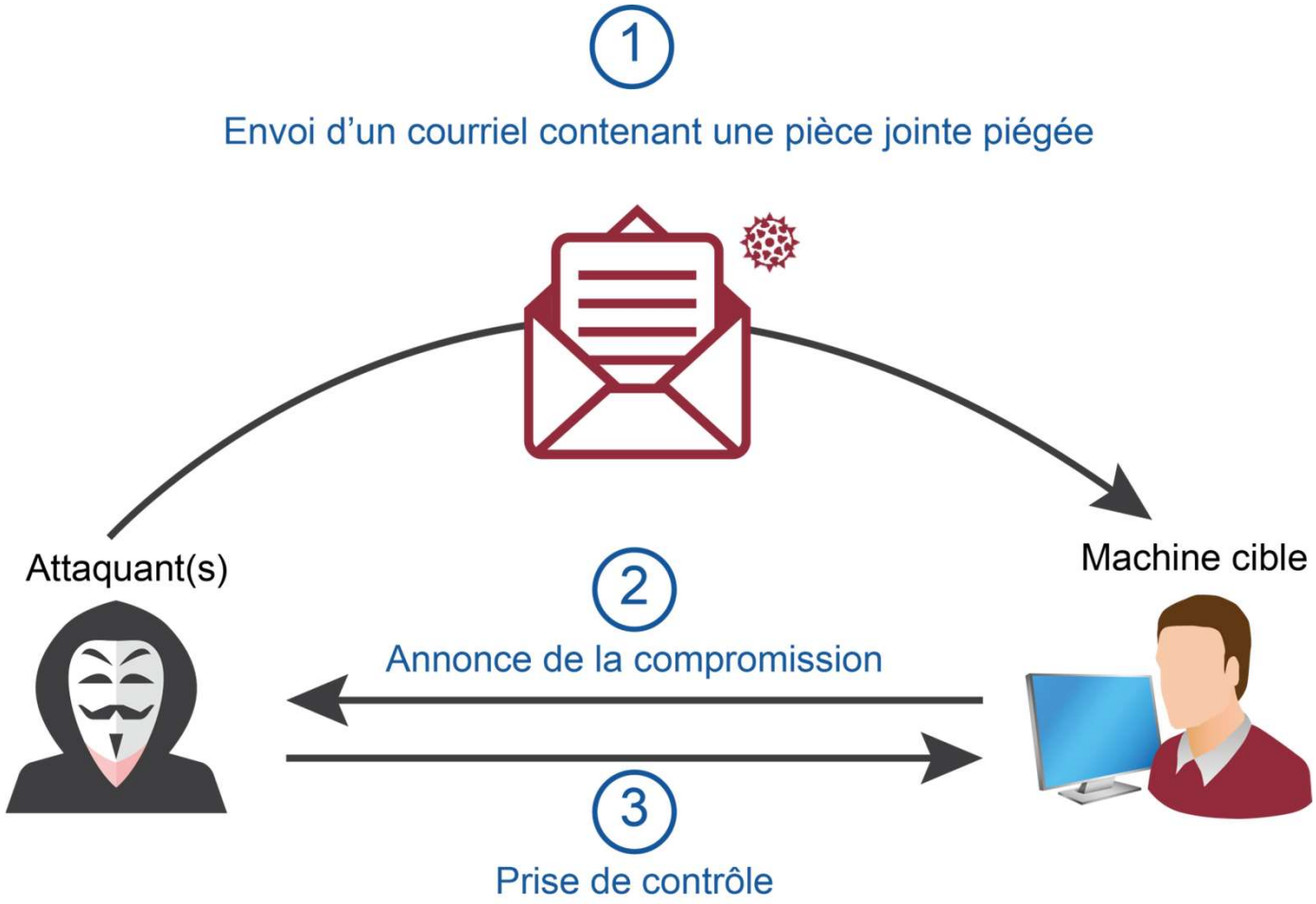
APT attacks

- 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

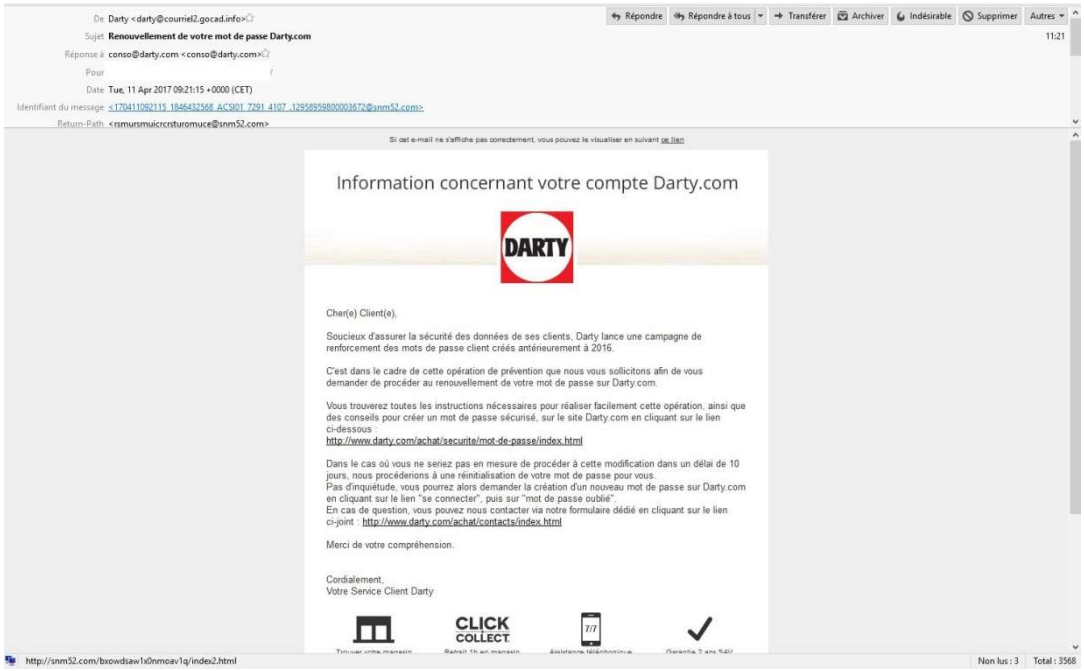
- The term *Advanced Persistent Threat* is also used to refer to a group, as a government, with both the ability and the intention to persistently and effectively target a specific entity.
- An individual, such as a hacker, is usually not referred to as an *Advanced Persistent Threat* because it does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

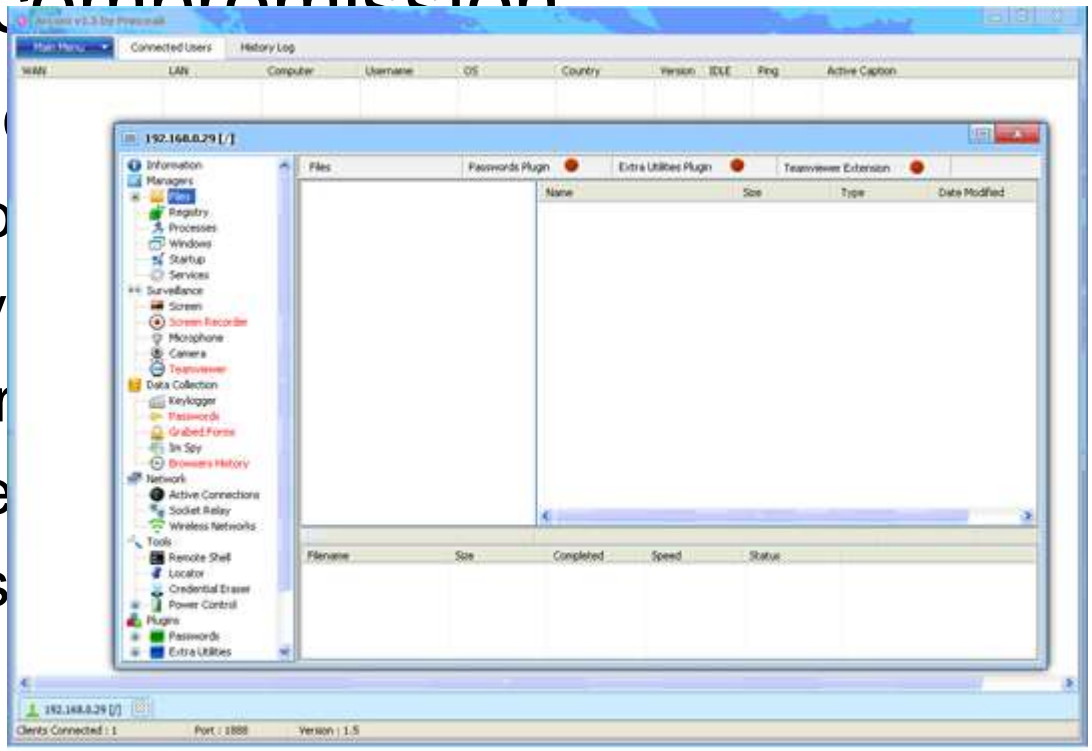
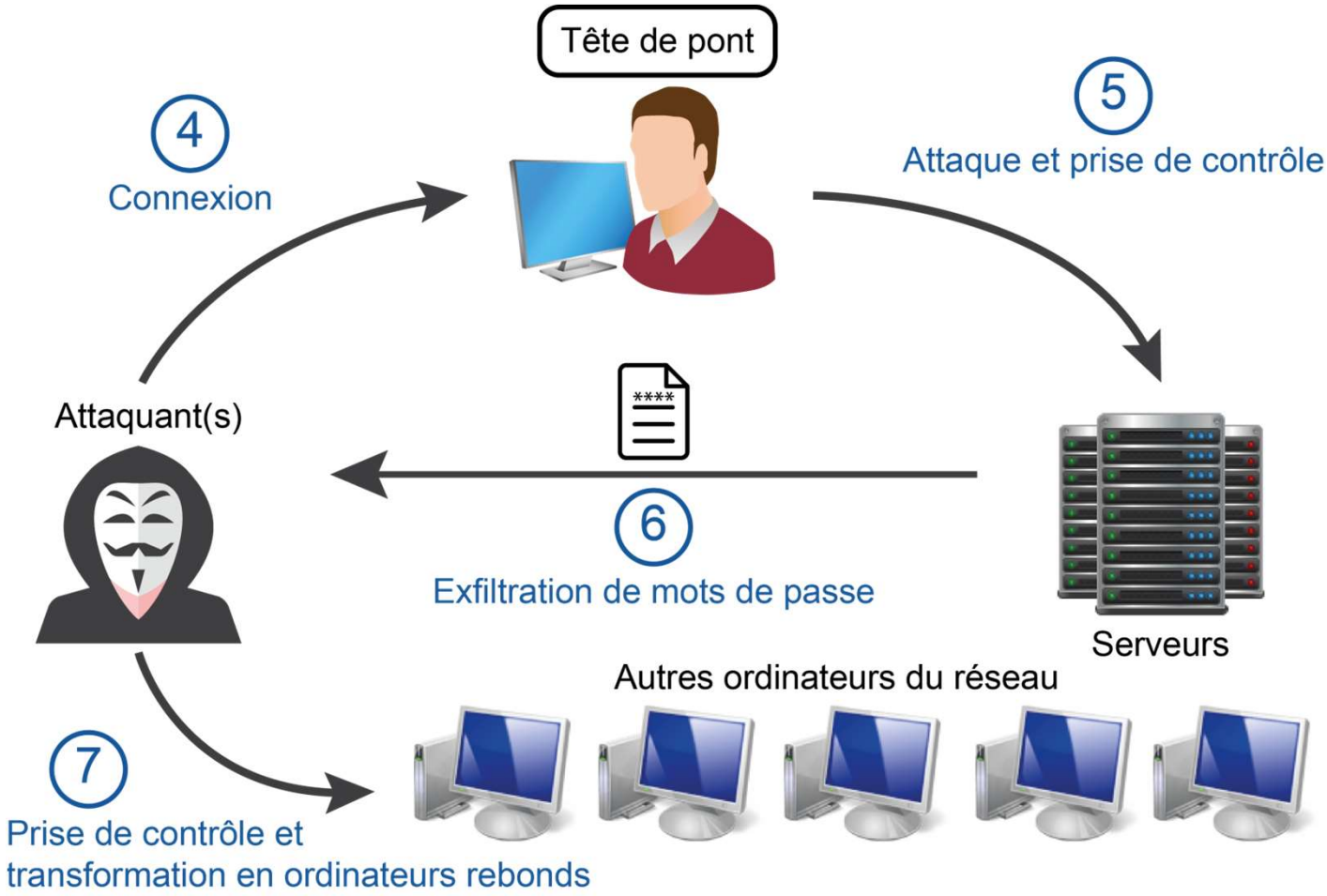


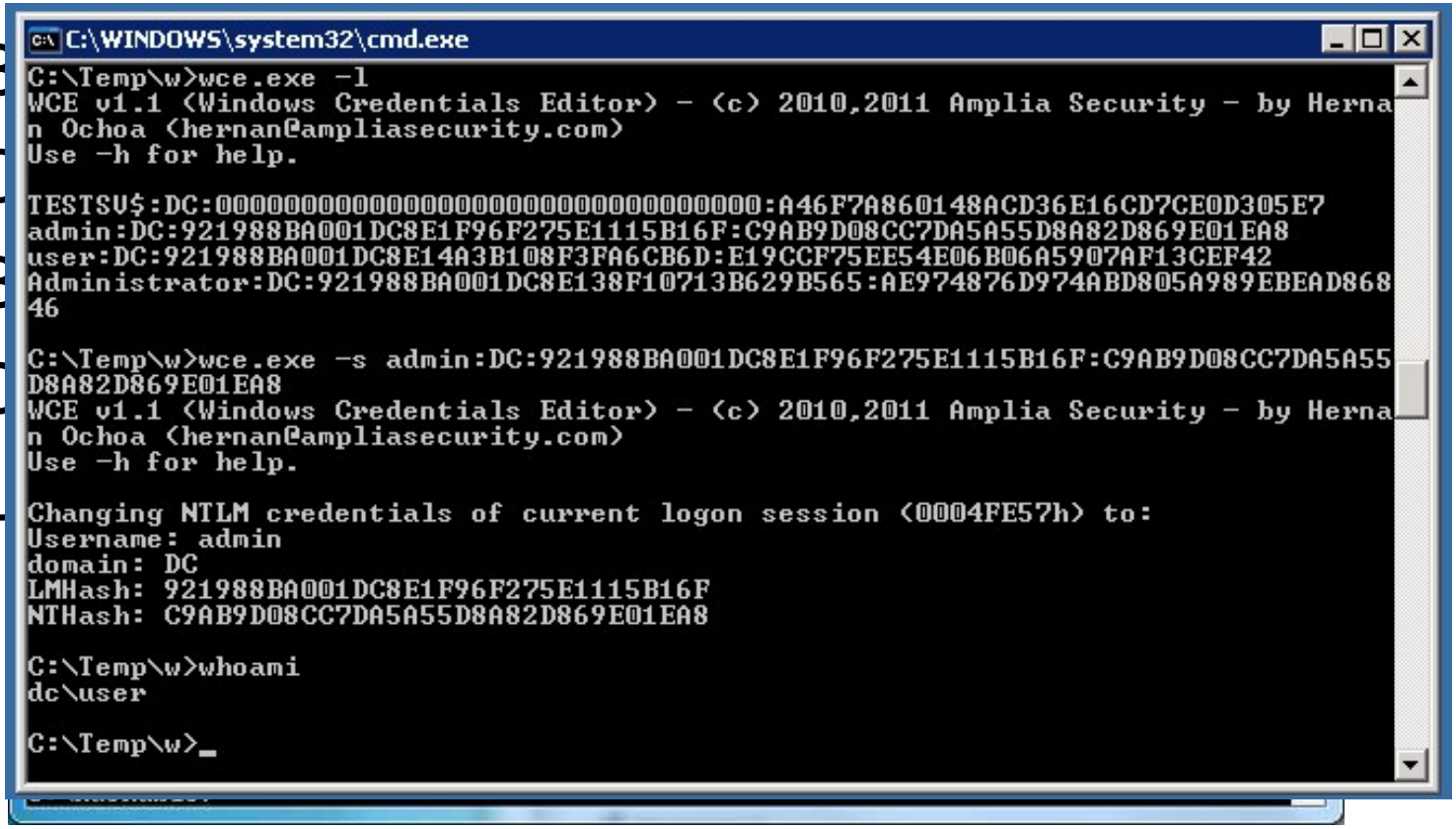
Figure 2. Cybercriminals use this to control compromised systems

The course of an advanced attack

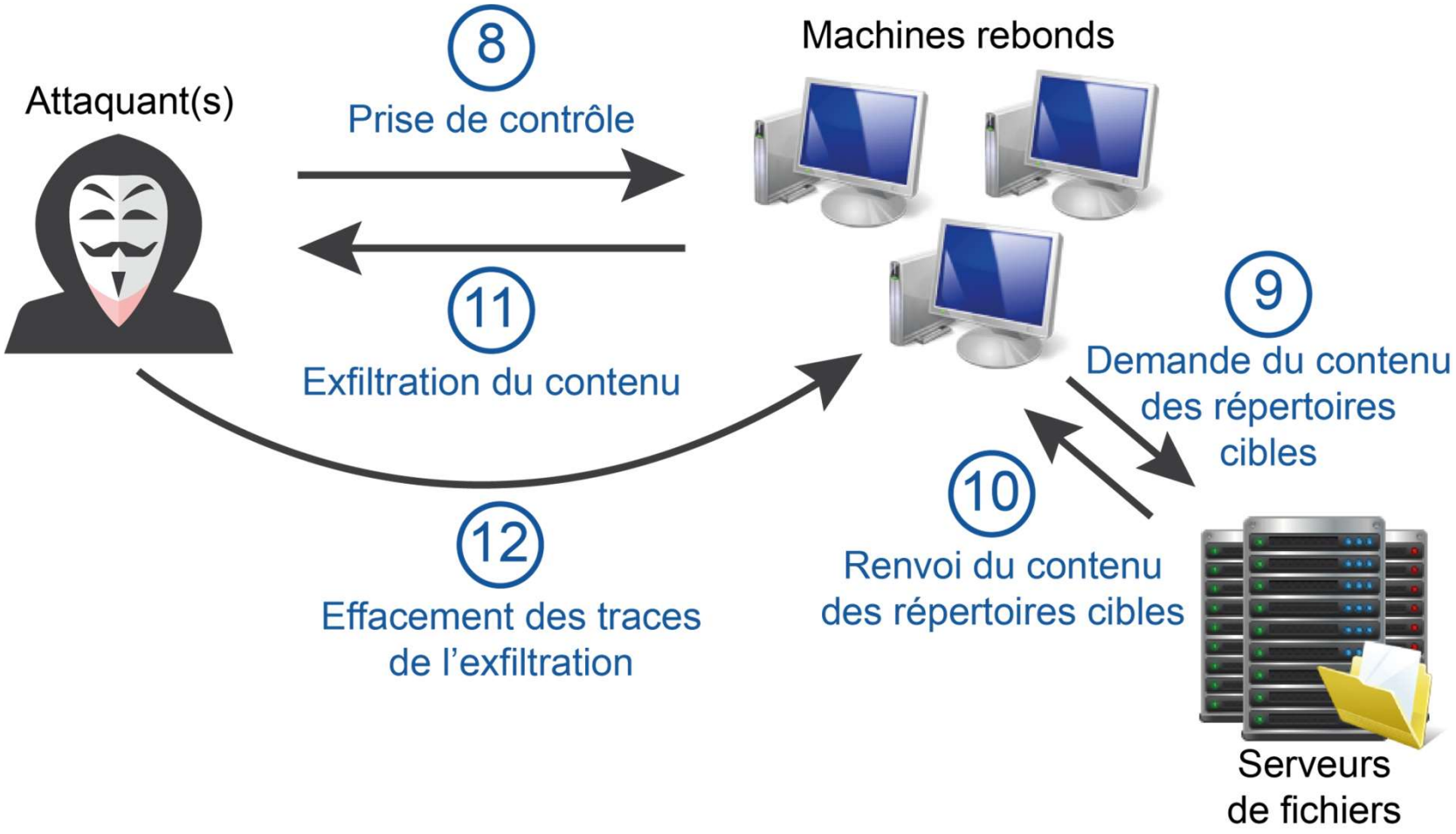


The course of an advanced attack

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

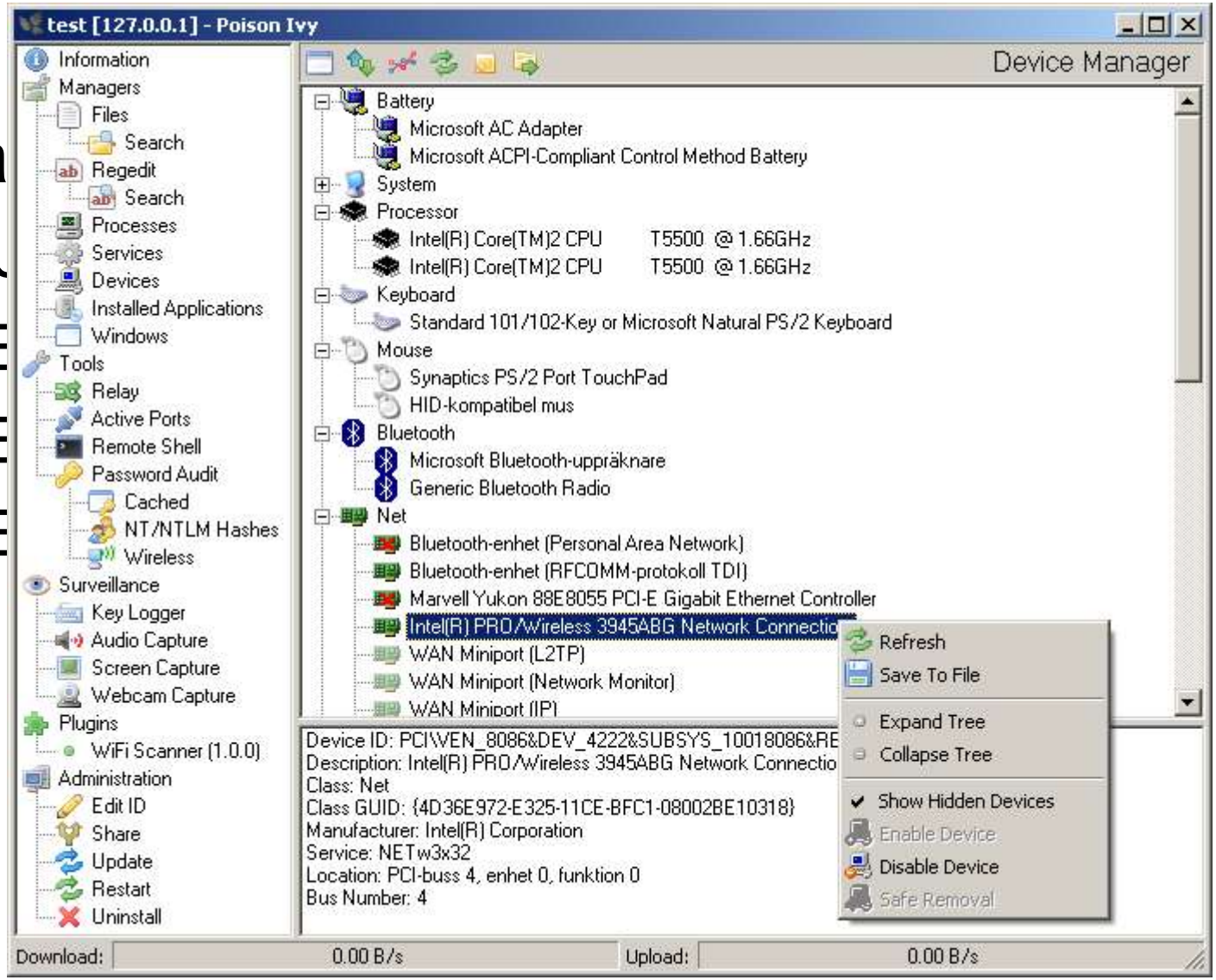


The course of an advanced attack



The course of an advanced attack

- Da
  - U
  - E
  - E
  - E



4.3 Types of attacks (1/3)

- DoS (Denial of service) : To decrease the system capabilities
  - DDoS (Distributed DoS) : idem but with an attack coming from several sites (http://grc.com/dos/grcdos.htm)
  - SYN Flood: the attacker floods a system with SYN synchronization packets in order to initiate connection requests (these requests are never finished) => strong exploitation of the processor resources, memory, network cards => Denial of service
  - UDP Flood: attack which submerges a system with UDP packets => prevent it from treating the valid requests for connection (often on the DNS port 53) (ICMP Flood: idem to submerge a system with ICMP messages (Internet Control Message Protocol) by using the Ping utility)
  - Ping of Death: possibility to “ping” with a too huge packet which can cause a whole range of uncontrolled reactions on the targeted system: Denial of service, shut down, freezing or restarting

4.3 Types of attacks (2/3)

- Scan of ports: Packets sent by using the port numbers in order to scan available services, hoping that a port answers
- Eavesdropping: the goal is to violate the confidentiality of the communication (by sniffing packets on the local area network or by intercepting wireless communications)
- Man-in-the-middle: the attacker acts between the two ends of the communication as if he were the awaited interlocutor: harmful effects on the confidentiality and possibly the integrity

4.3 Types of attacks (3/3)

- Java/ActiveX/ZIP/EXE: dangerous Java components or Active X hidden in Web pages, Trojan dissimulated in a ZIP/TAR or EXE file
- Breaking into a system: by violating the authentication or the access control, the attacker obtains the possibility of controlling the communication: effects on the confidentiality and the integrity
- Virus: shortcuts the authentication and the access control with the aim of carrying out destroying code: effects on the availability of the machine and/or the network
- Trojan: virus hidden in a function usually used, program being carried out on the pirated machine to send information to the pirate
- Worm *(ver)*: explore and automatically exploits the faults of a system, without action of the user => problems of availability

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" !

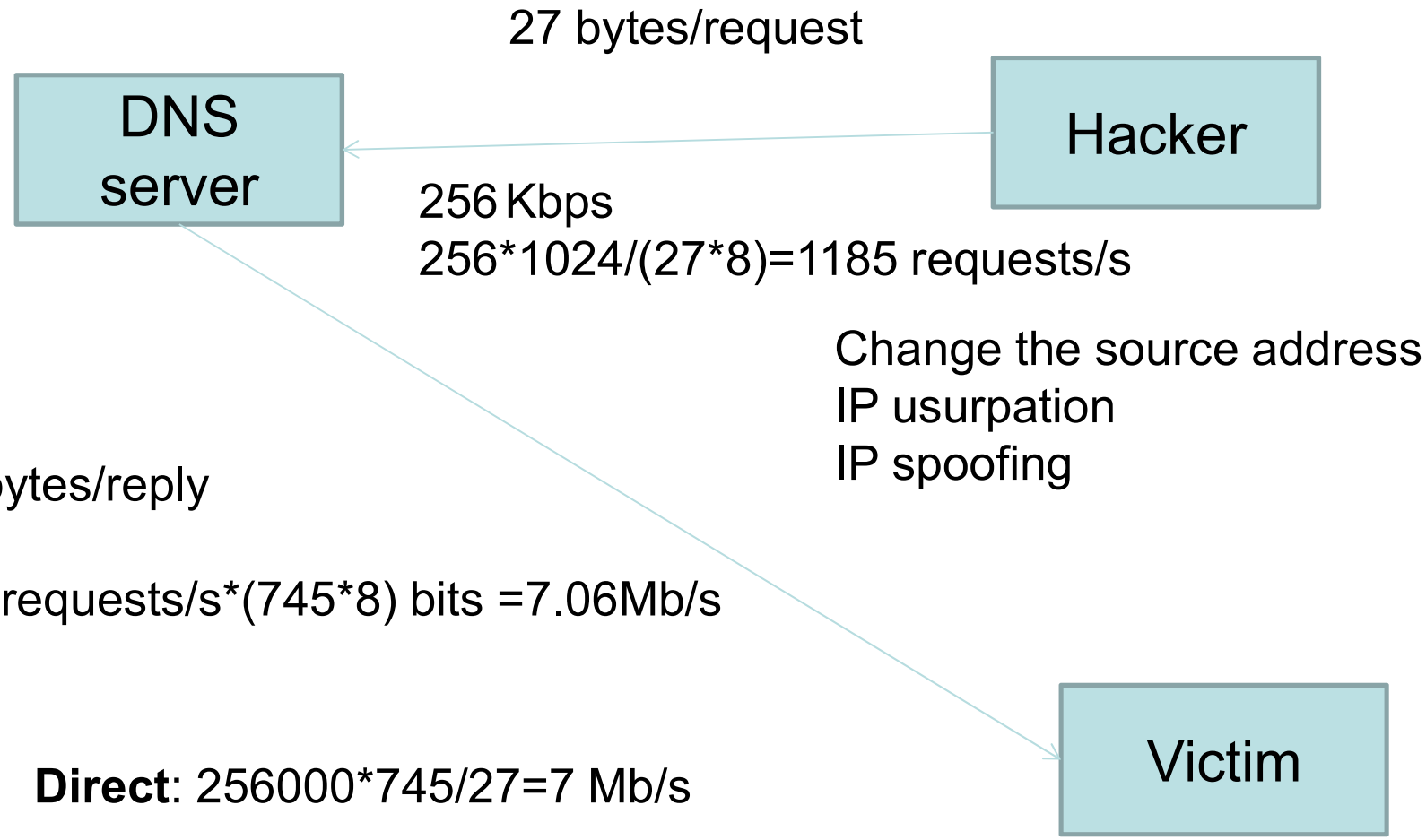
4.4 Organizations for security

- CERTA (Centre d'Expertise gouvernemental de Réponses et de Traitements des Attaques Informatiques / French governmental Center of Expertise for Answers and Treatments of the Data-processing Attacks)
  - www.certa.ssi.gouv.fr
- SANS (SysAdmin, Audit, Network, Security)
  - www.sans.org
  - Research on information security
- SCORE (Security Consensus Operational Readiness Evaluation)
  - www.sans.org/score
  - Community of professionals in security
- ISC (Internet storm center)
  - http://isc.sans.org
  - Logs (journal) concerning detections of intrusion
- ANSSI
  - www.ssi.gouv.fr
  - Agence Nationale de Sécurité des Systèmes d'Information

Comment attack Ex 3

- IP usurpation (the hacker is sending the DNS request to the DNS server using the actual IP source of the victim as her.his IP source)
- The DNS will send the responses to the victim
- I « pay » for 27 bytes/request and the victim receives 745 bytes/request => it acts as a digital amplifier
- It’s a third (tierce)-party attack
- I impose a strong denial of service to the victim

Attack by third party



Direct: 256000*745/27=7 Mb/s

URLs

- www.securite-informatique.gouv.fr
- www.insecure.org
- www.tigertools.net
- www.deter.com/unix/index.html
- www.nessus.org
- www.cerias.purdue.edu/coast/satan.html
- www.uk.research.att.com/archive/vnc
- www.iss.net
- www.wallix.com
- www.checkpoint.com
- www.laser.epfl.ch/securitereseaux
- www.urec.fr
- www.afnic.fr
- www.icann.org
- www.internic.ne
- www.isc.org
- www.loria.fr/services/moyens-info/securite/
- …

Sentences for security

- I should prove that I have done the best as possible compare to the actual/present state of the art
- Everything your system need should be explicitely authorized. Everything which is not authorized is FORBIDDEN.

References

- J.F. Aubry – Cours de Sûreté de Fonctionnement, INPL Lorraine, 2005.
- J.C. Laprie & al. – Guide de la sûreté de fonctionnement – Cépaduès, 1995.
- A. Villemeur – Sûreté de fonctionnement des systèmes industriels – Editions Eyrolles, Paris, 1988.
- S. Ghernaouti-Helie – *Sécurité informatique et réseaux, 4ème édition* – Dunod, 2013
- Security for industrial communication systems, Dacfey Dzung, Martin Naedele, Thomas P. Von Hoff, Mario Crevatin, pp. 1152-1177, Proceedings of the IEEE, Vol. 93, n° 6 "Industrial Communication Systems", June 2005
- La sécurité des réseaux-First steps, Tom Thomas, Cisco Press, 2005
- Les réseaux, édition 2005, G. Pujolle, Eyrolles 2004
- Course of Jean-Luc Noizette, ESSTIN, Nancy
- G. Avoine, P. Junod, P. Oechslin – Sécurité informatique, exercices corrigés – Vuibert, Paris, 2006.
- **Sécurité et espionnage informatique : connaissance de la menace APT**, Cédric Pernet, *Eyrolles*
- **Guide d'autodéfense numérique,** *éditions Tahin Party*
- **Cybertactique : Conduire la guerre numérique,** Bertrand Boyer, *Nuvis*
- **Learn Social Engineering***, Dr E. Orzkaya,* 2018, Packt

Deontology

- Students

  => signing of a computer (informatics) charter
- Engineer with Security aspects

  => responsibility
- The use of the methods described in this course engages the responsibility of the users!