TOPIC 1: INTRODUCTION

"This world doesn't need a hero; it needs a professional"

JOSÉ MANUEL REDONDO LÓPEZ *"S-81 ISAAC PERAL"* PROJECT V4.0




Source: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

Logo: @creative_vanesa (*Instagram*)

INDEX

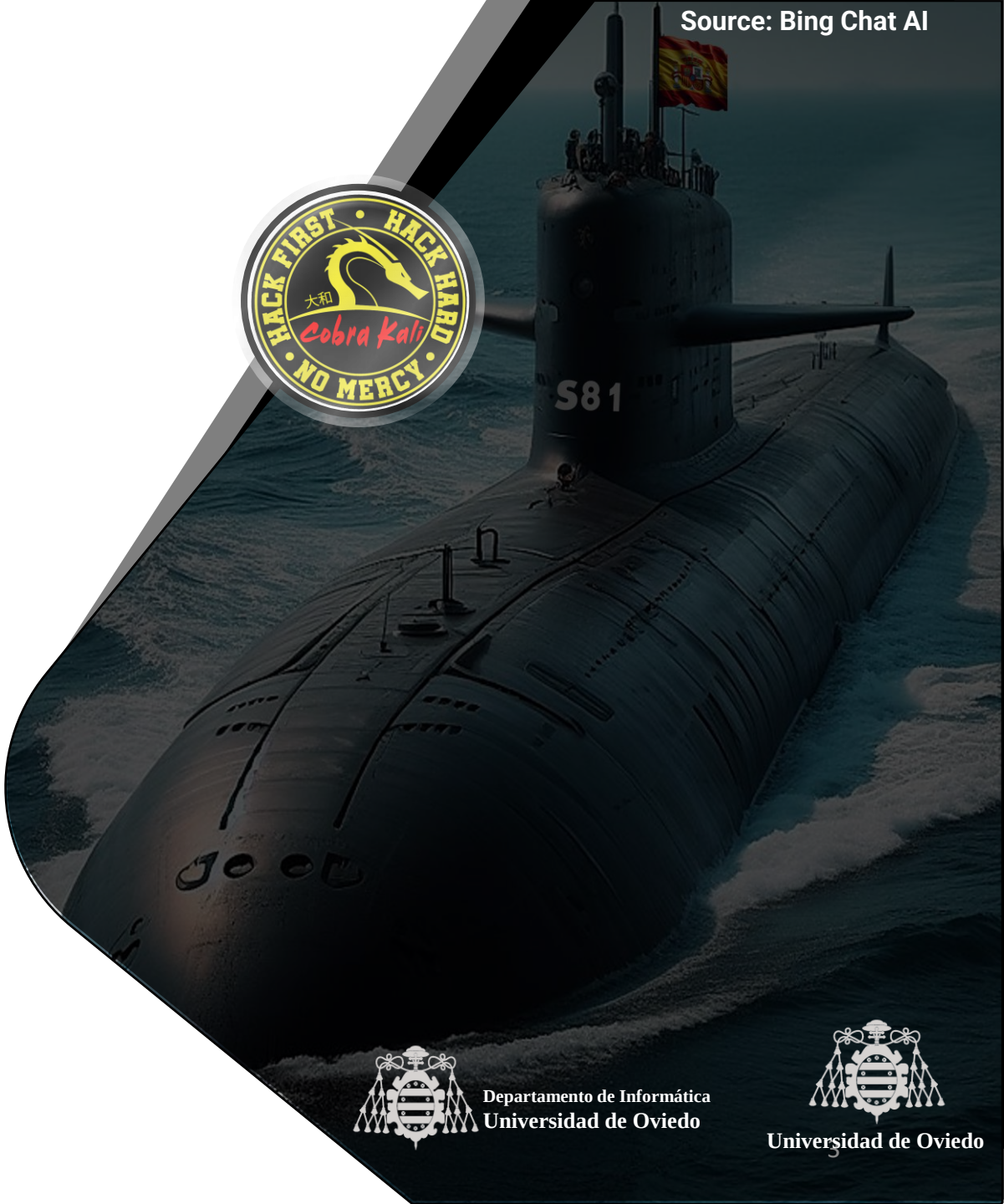
< Go to Index

ETHICAL CODE

Hackers are NOT criminals, hence you must abide to an ethical code

*Icons by Bing Chat AI

Source: Bing Chat AI



ETHICAL CODE

- **We are going to describe several real pentesting techniques and tools**
  - Using them against targets without authorization **IS A CRIME**
  - Misusing some of them can do a lot of damage or disable a target
- **You MUST abide to this code of ethics**
  - Becoming a criminal will sooner or later ruin your life and others'
    - There will be always someone that know more than you, and may "hunt" you
    - You can leave families without any form of income (**it is NOT funny**)
    - You can even indirectly kill people (**it is a major crime**)
      - Do not believe me? Search about ransomware on health institutions…
  - Defending against criminals is a way of obtaining a well-paid job
    - **But for that, you need to know how they operate**
    - That's the reason why we teach certain things
  - **Your choice, your responsibility, your life**

ETHICAL CODE

- **ANY unauthorized use of any of these tools and techniques means that you are committing a crime**
  - And that the odds of being "hunted" are very high
- **ALWAYS use these techniques against authorized targets**
  - **You've been hired** to assess the security of some systems (it is your job)
  - You are working with a legal **cybersecurity training platform** (it is your legal “playground”)
  - You are targeting a system **you created** locally as a training ground (it is your private “playground”)
    - Typically called “pentest labs” (you can also find prebuilt ones too)
- **ALWAYS apply these techniques following the established rules / limits**
  - By the **contract** you signed (it is your job)
  - By the rules of the **platform** you use (no DoS...) (it is your legal “playground”)
  - By the **capacity** (resources) of your infrastructure (it is your legal private “playground”)

ETHICAL CODE

- **Some of these techniques are purely for intrusion**
  - Web shells, privilege scalation, Metasploit characteristics...
- **They can be used to evaluate the severity of a vulnerability**
  - But also, **in hacking and CTF contests** or “legal hacking playground” sites
    - Hack the Box, Try to Hack me…
    - **That’s the reason why we explain these techniques!**
    - You win obtaining information or data ("**flags**") by exploiting vulnerabilities
    - And they also are a **very useful learning resource**
  - By preparing you to be able to tackle typical CTF challenges…
    - We are setting a baseline for your future cybersecurity self-education (if you like this world)
    - Even if not, **you will be able to be a much better software engineer**
    - Your applications are less likely to be “assaulted” ☺

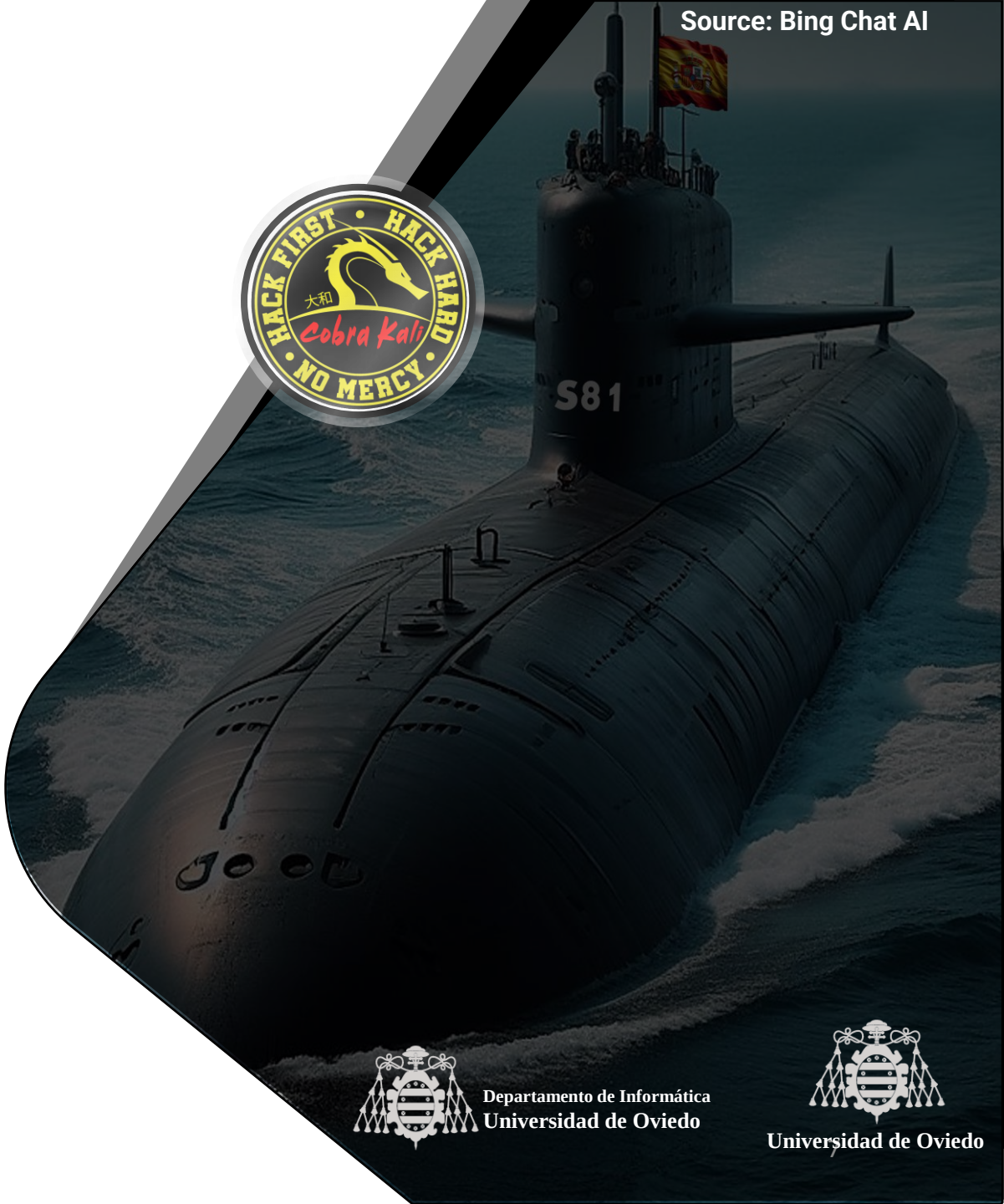
< Go to Index

INTRODUCTION

Battlecruiser operational! ☺

*Icons by Bing Chat AI

Source: Bing Chat AI



Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

Introduction: Learning goals

- **We aim to enable you to do the following things over the computing systems you manage**
  1. Know different **concepts** related to their security
  2. Identify the **risks** that may compromise their security
  3. Know the **vulnerabilities**, **threats**, **attack techniques** and other things involved in its security
  4. Identify different types of **damages** that may be caused to them

COMPUTER SECURITY

- A computer system is **secure** when it **responds as intended**
  - Allows every legitimate user to perform all operations that they are authorized to
  - Prevents users to perform unauthorized operations
- Additionally, it also **guarantees legitimate users three things**
  - **Confidentiality**: Private data are only **viewable** by their legitimate owners
  - **Integrity**: Data can be **modified** only by their legitimate owners
  - **Availability**: Data are always readily **accessible** to their legitimate owners
- So, the goals of computer systems security are
  - To **identify vulnerabilities** that a computer system may have
  - To create and set up **countermeasures** against them
  - **To avoid existing threats** that **exploit** these vulnerabilities

Computer systems security

- **This comprises**
  - Studying possible **threats**, **risks**…
  - Improve the security of computer systems (**hardening**)
  - Design **security management policies** for information systems (ISMS)
  - **Ethical Hacking**, **pentesting**, and computer **forensics**
- **Because of it, this year is related to several others**
  - Will skip multiple system administration topics to focus only on system hardening ones
    - Our "brother course", Network and Systems Administration (ASR) deals with this
  - Will skip forensics
    - The optional Computer Forensics and Audit year (IFA) deals with this
  - Will only mention risk management
    - The Project Management year (4th year) (DPPI) will deal with this
  - Will only mention law-related topics
    - The Social, Legal, Ethical and Professional Aspects of C. Eng. (ASLEPI) year (4th year) will deal with this
  - Will not focus on web security, only its foundations
    - The Master on Web Engineering (MIW) of the "Cobra Kali" initiative will deal with this

ATTACKS AGAINST CONFIDENTIALITY

- **Unauthorized system access (impersonation)**
  - Access to restricted data (files, private information…)
  - Access to restricted software (licensed products, custom software…)
- **Unauthorized communication access (sniffing)**
  - Access to data that the target sends and/or receives
  - Messages, files, private information…
- **Physical access to a computer (installing malware, stealing data…)**
  - Or a storage device (stealing data or the device itself)
- **Logical or physical access to data/software backups**
- **Access to restricted or private data / software**
  - By **social engineering** techniques
  - Through **malware** or **privilege scalation**

ATTACKS AGAINST INTEGRITY

- **Same attacks that against confidentiality,**
  - But **not limited to just accessing information / software**
- **Once unauthorized access is achieved, attackers may**
  - **Introduce fake or malicious** data / software
  - **Corrupt** existing data / software (trojanized versions)
  - **Modify** existing data / software to attain other unwanted effects
    - Denial of service, increase resource consumption, propagate fake information, alter the company operations…
- **Compromising integrity in communication channels is usually performed by Attacker-in-the-Middle (AitM) attacks**
  - Previously called “Man-in-the-Middle” (MitM)

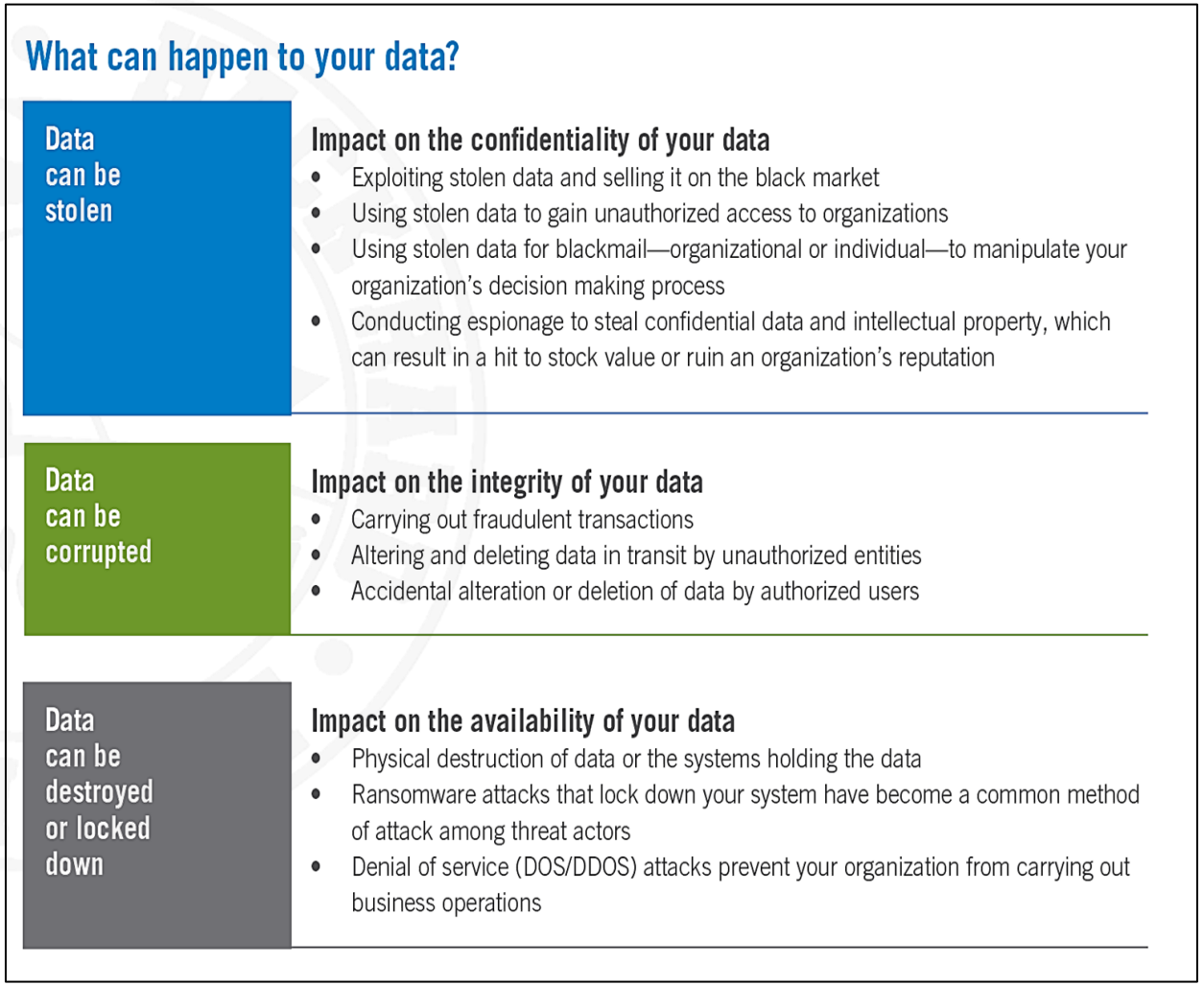
ATTACKS AGAINST AVAILABILITY

- All forms of attack that aim to **deny or reduce the ability** of a computer system to provide a certain service or set of services
  - **Flooding** via certain malware types (substantially reducing performance)
  - **Resource exhaustion** through DoS (Denial of Service) or DDoS (Distributed DoS) attack variants
  - **Removing or purposely damaging existing hardware**, including communication hardware
  - System or important peripheral **power down**

DATA IS A TARGET!

- As you see, there are a lot of things that can happen to data
- Apart from security measures, there is one way to prevent critical data losses: **backups**
  - **Backup often**, and in external devices
  - Ideally, have **more than one** (rotate backups)
  - More ideally, **at least one should be in a different place**
    - Dropbox, OneDrive…can help
  - **Check that you can restore your backups once you do them!**
- Backup details and policies (**Windows / Linux**) are covered in **ASR**

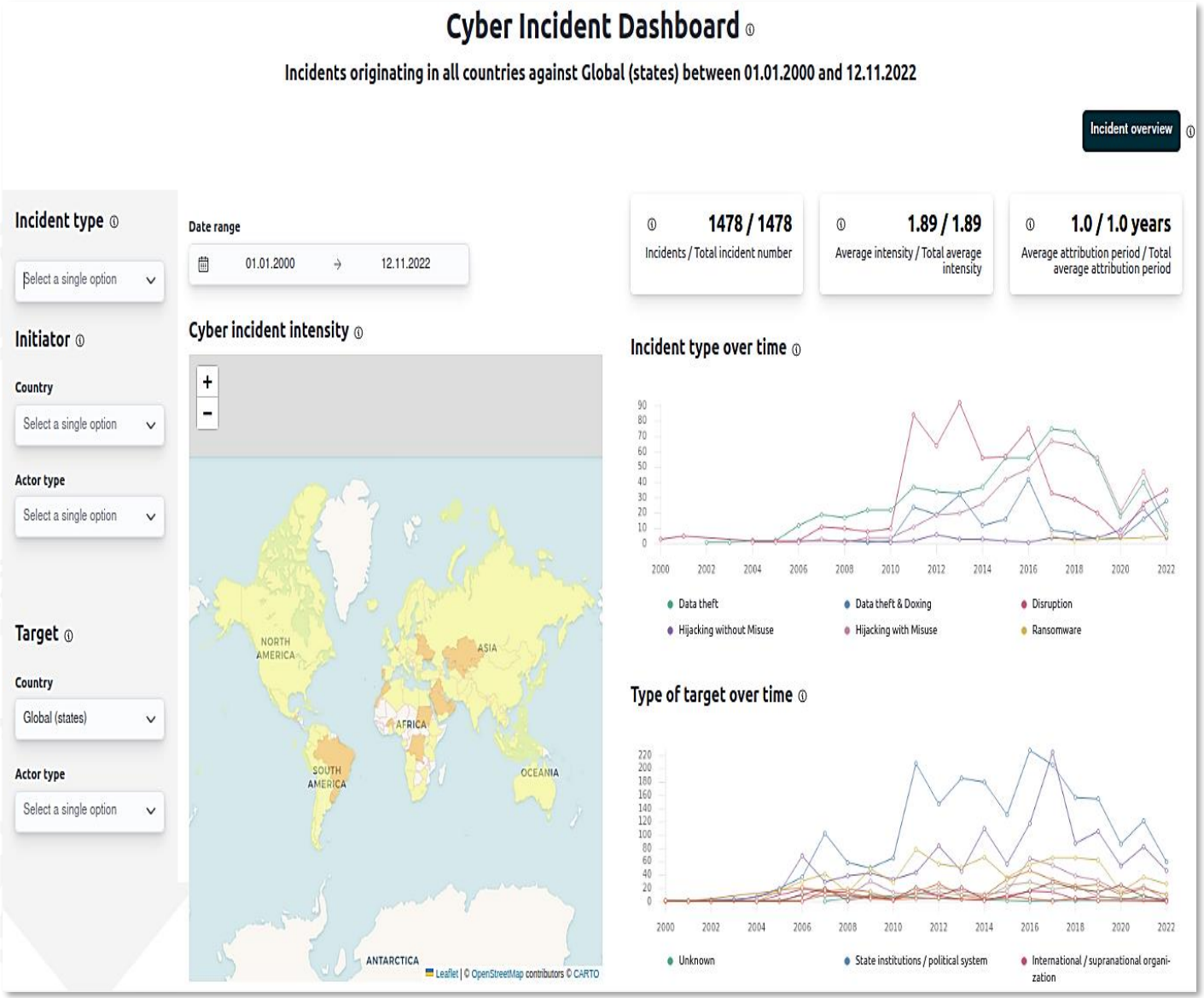
Source: https://www.cybervista.net/what-every-executive-really-needs-to-know-about-cyber-part-1/



SECURITY TODAY

Computer Security

- **Cybersecurity-related profiles are in high demand**
  - https://cso.computerworld.es/ciberseguridad/cuales-son-los-perfiles-mas-buscados-en-los-departamentos-de-seguridad
- **Because attacks are constant, and worldwide**
  - https://cybermap.kaspersky.com/
  - Examples are in the news daily…
- **They evolve with current affairs**
  - E. g.: The pandemic health crisis has greatly increased remote desktop (RDP) attacks
  - And ransomware…

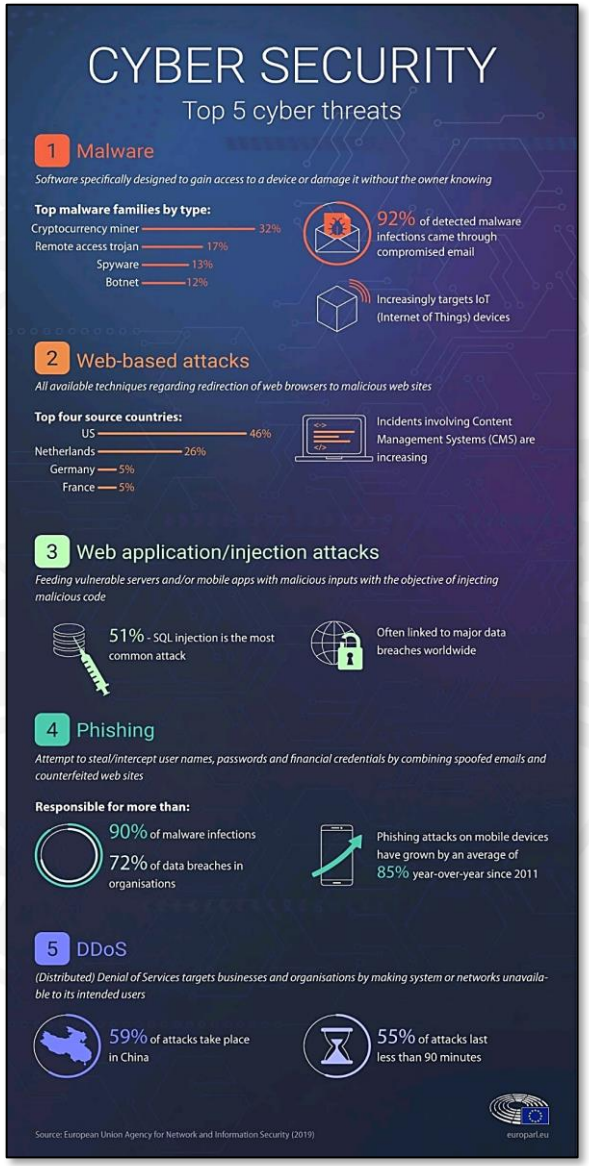


Source: https://eurepoc.eu/dashboard

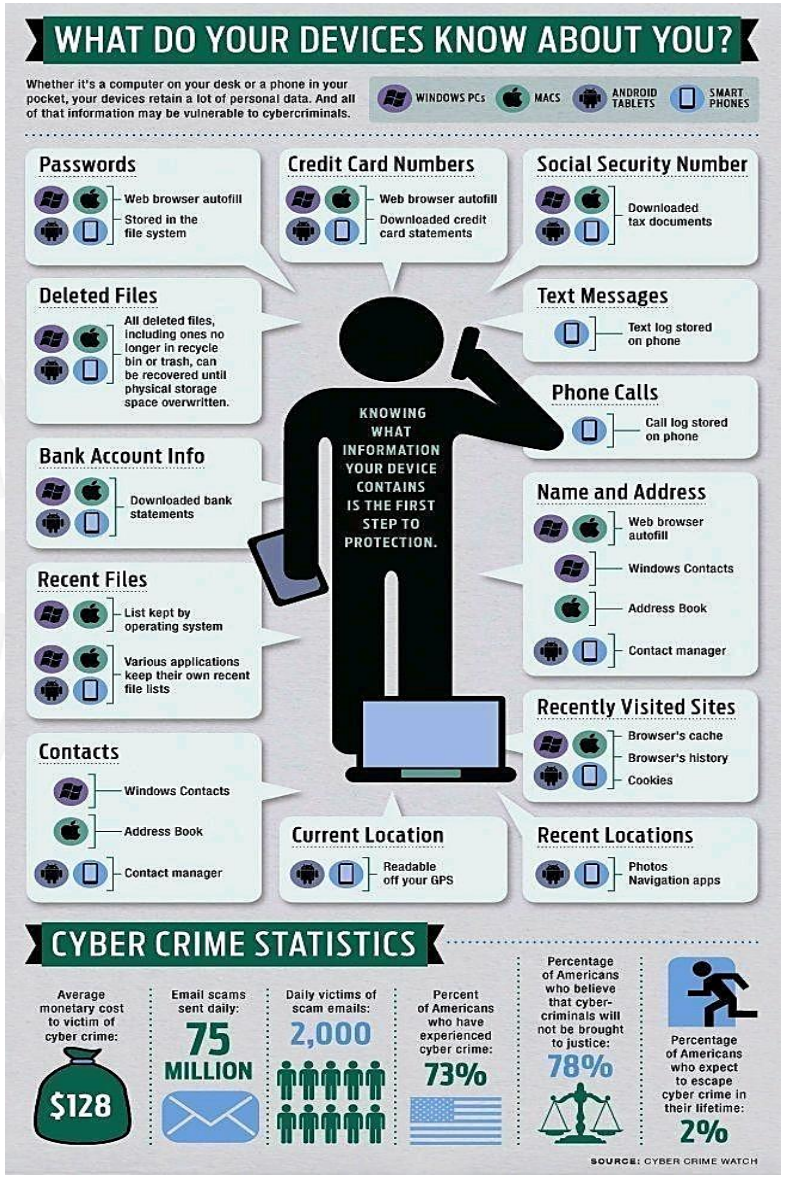
SECURITY TODAY

- Some types of attacks are more prevalent than others
- Access to individual devices is now much more profitable to criminals than years ago
- Therefore, **malware** and **phishing** are gaining importance to steal private user information
  - Normally partnered with **OSINT** (Open-Source INTelligence) techniques against users

Source: https://m.facebook.com/comptechcyber/posts/



Source: https://www.cybercrimeswatch.com/



THE WORLD OF SECURITY FROM A BEGINNER PERSPECTIVE

- We know that most of you don't have any security experience
- We also know that a lot of people believe that this world is something difficult and unreachable

THIS IS FAKE NEWS!

- We are going to approach it from a zero-knowledge perspective
  - We will first build the required base knowledge
  - And later, we are going to explore increasingly advanced topics
  - At the end, you will be able to **defend your systems** and **check its security** adequately
- Let's begin with **some basic concepts**

< Go to Index

Source: Bing Chat AI

Malware types >

BASIC TERMINOLOGY

Understanding basic concepts and “buzzwords” ☺

*Icons by Bing Chat AI

What are you going to find in this block?

- **In this block you will learn**
  - What is a **CVE** and what it represents
  - What is a **CVSS**
  - The concepts of **risk**, **attack**, and **damage**
  - What is a **security control**
  - What kind of **attackers** exist
  - What kind of **security teams** exist
  - Different **types of malware** and what they do

Basic terminology

- **Threat**: elements that poses any type of danger to systems, such as
  - **People** (legitimate or non-legitimate users)
  - **Software** (malware)
  - A **natural catastrophe** (flood, fire…) (physical security, **Seminar 2**)
  - Possible factors that take advantage of vulnerabilities
- **Vulnerability**: System (or applications) parts that may be attacked
  - These are the **weaker points of a system**, most probably chosen to initiate an attack
  - The **payload** is the code that performs the malicious action of an attack
- **Exploit**: Techniques or code that allow to take advantage of a vulnerability
  - To launch attacks of different types
  - These attacks may stop part of the system services, compromise their functionality, alter the behavior of some part of the system, corrupt/steal data…

Common Vulnerabilities and Exposures (CVE)

- Reference information for publicly known security vulnerabilities and exposures of any software
- The full known CVE database is accessible for free for most products
  - https://cve.mitre.org/
  - https://www.cvedetails.com/
  - ...
- Allows to search and obtain details of any known software vulnerability, classified by its version
  - MITRE Corporation maintains it
  - With funding from the National Cyber Security Division of the USA

Source: https://www.cvedetails.com/vulnerability-list/vendor_id-23/product_id-22264/Debian-Apache2.html

Debian » Apache2 : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity
1	CVE-2013-1048	264		+Priv	2013-03-06	2013-03-06	4.6	None	Local	Low

The Debian apache2ctl script in the apache2 package squeeze before 2.2.16-6+squeeze11, wheezy before 2.2.22-13, and sid before 2.2.22-13 for the Apache H properly create the /var/lock/apache2 lock directory, which allows local users to gain privileges via an unspecified symlink attack.

2	CVE-2012-0216			+Priv XSS +Info	2012-04-22	2017-08-28	4.4	None	Local	Medium

The default configuration of the apache2 package in Debian GNU/Linux squeeze before 2.2.16-6+squeeze7, wheezy before 2.2.22-4, and sid before 2.2.22-4, w example scripts under the doc/ URI, which might allow local users to conduct cross-site scripting (XSS) attacks, gain privileges, or obtain sensitive information v Apache HTTP Server.

Total number of vulnerabilities : 2 Page : 1 (This Page)

CVE-ID

CVE-2020-8832 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

The fix for the Linux kernel in Ubuntu 18.04 LTS for CVE-2019-14615 ("The Linux kernel did not properly clear data structures on context swit before 4.15.0-91.92, an attacker could use this vulnerability to expose sensitive information.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:https://security.netapp.com/advisory/ntap-20200430-0004/
- MISC:https://bugs.launchpad.net/ubuntu/+source/linux/+bug/1862840
- UBUNTU:USN-4302-1
- URL:https://usn.ubuntu.com/usn/usn-4302-1

Assigning CNA

Canonical Ltd.

Date Entry Created

20200210 Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not ne updated in CVE.

Phase (Legacy)

Assigned (20200210)

Source: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8832

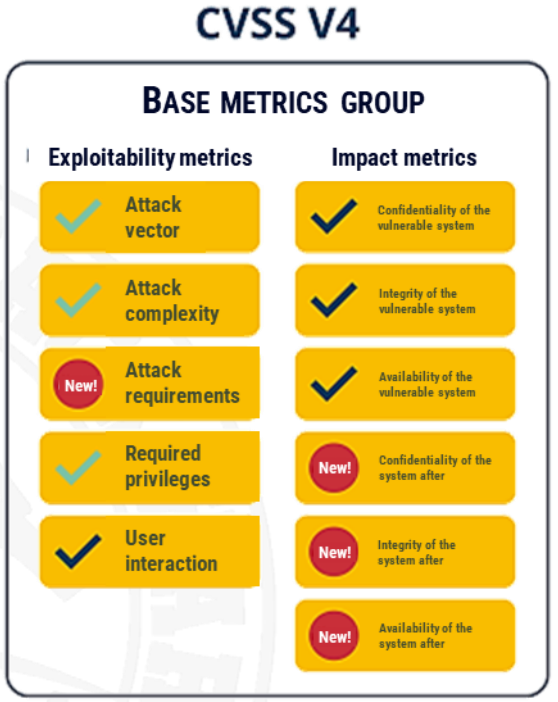
Common Vulnerabilities and Exposures (CVE)

- CVE allow us to speak a “common language” between different tools and sites dealing with vulnerabilities
- “This application is vulnerable to CVE-<year of discovery>-<unique ID>”
  - This way we can say **A LOT** in a simple phrase
  - We know where to go to find all known data about this vulnerability
- If a vulnerability is massively exploited, we can react and communicate it more efficiently
  - And this happens in real life! (see image)
  - You need to know a product and its version…and sometimes you can obtain it **with a simple browser** ☹

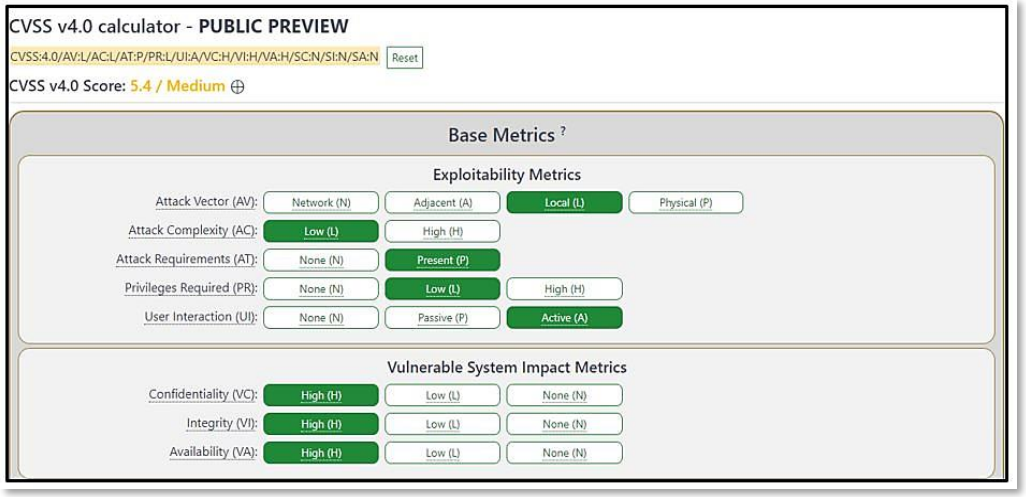
Source: https://es.linkedin.com/in/jsalasrodriguez

CVSS (Common Vulnerability Scoring System) 4.0

- **Therefore, the CVE is like a glossary that classifies known vulnerabilities**
  - And what is known about them
- **The severity of those vulnerabilities is scored with CVSS**
- **Very recently upgraded to version 4.0**
  - To make it clear that a CVSS **is not just a score**
  - It **includes more metrics** that better model the type of vulnerability, its impact, what it takes for it to be exploited (privileges, user interaction...), etc.
  - Also, **how the vulnerability impacts the CIA** seen previously



The CVSS metric group to characterize the severity of a CVE. Source: https://www.incibe.es/incibe-cert/blog/cvss-v40-avanzando-en-la-evaluacion-de-vulnerabilidades



Basic terminology

- **Risk**: Obtained by multiplying the magnitude of the damage provoked by an attack and the probability it occurs
  - *Risk = Threat x Vulnerability x Value of the target*
- **Attack**: Conscious and intentional action performed to cause damage to a computer system, composed by three core elements
  - **Reason**
  - **Method** (the exploit used to unfold it)
  - **Opportunity**
- **Damage**: Harm produced by a system failure, either accidental or provoked (attack)
  - Economical, technical, moral, brand / business image…

BASIC TERMINOLOGY

- **(Security) Control** or **Countermeasure**: Protection mechanism that mitigate or eliminate a risk and may focus on
  - Attack **prevention**
  - Attack **mitigation**
    - Slowdown, decreasing the attack surface, or increase the attack difficulty
  - Attack **redirection** to other hardened targets not subject to the attack
    - Or that may implement countermeasures or proactive responses to it
    - Blocklists of known attackers to apply over the whole infrastructure, alerts, reporting…
  - Attack **detection**
  - Attack **recovery**
  - Typically called **security controls** on most methodologies / standards / frameworks / protocols related to cybersecurity
  - There are many tools that recommend security controls (e.g., Lynis) or discover some that we lack according to those **standards or policies** (**Topic 4**)

Basic terminology: Types or attackers (or "adversaries")

- **Script kiddies** or **n00bs** (aka **skiddies**)
  - **Persons with little knowledge**, but with access to advanced tools to perform attacks
  - Typically, blindly or with little knowledge about what is happening "behind the curtain"
- **Pentesters** (white hat hackers)
  - **Legally hired professionals to test the security state of a system**
  - Using the same techniques as malicious attackers
  - But in controlled environments and with pre-established limitations (**contractual agreements**)
- **Crackers** (black hat hackers)
  - **Persons that harm systems with spurious reasons**
  - Intellectual, economical, political, terrorism, cyberwar…
  - *… (even "for the lulz", using a twisted sense of humor)*

A HACKER IS NOT A CRIMINAL (DESPITE THE PRESS)

Basic terminology: security teams

- **Red team**: independent group that challenges an organization to improve its security effectiveness by assuming an "adversarial role"
  - Hired to **act as actual attackers**, placing payloads, delivering exploits, performing the same actions…
  - However, after a period infiltrated, they report their findings, so security can be enhanced
  - Assess the overall security by testing various means of protection (technical, physical, human)
- **Blue team**: analyze information systems security
  - Identify flaws, verify the effectiveness of security measures, respond to incidents, hunt threats, perform forensics, and damage control operations
  - Ensure that all security measures are effective after their implementation
  - "Fight" against attackers/red teams to improve systems security, responding to their attacks and protecting an organization and their information with a defensive strategy
- **Purple team**: maximize the effectiveness of both teams
  - Integrating defensive tactics (Blue) with threats and vulnerabilities (Red) and sharing information
  - **More information**: https://danielmiessler.com/study/red-blue-purple-teams/

Source: *PowerPoint* icons

Malware types

Types of programs created to harm you

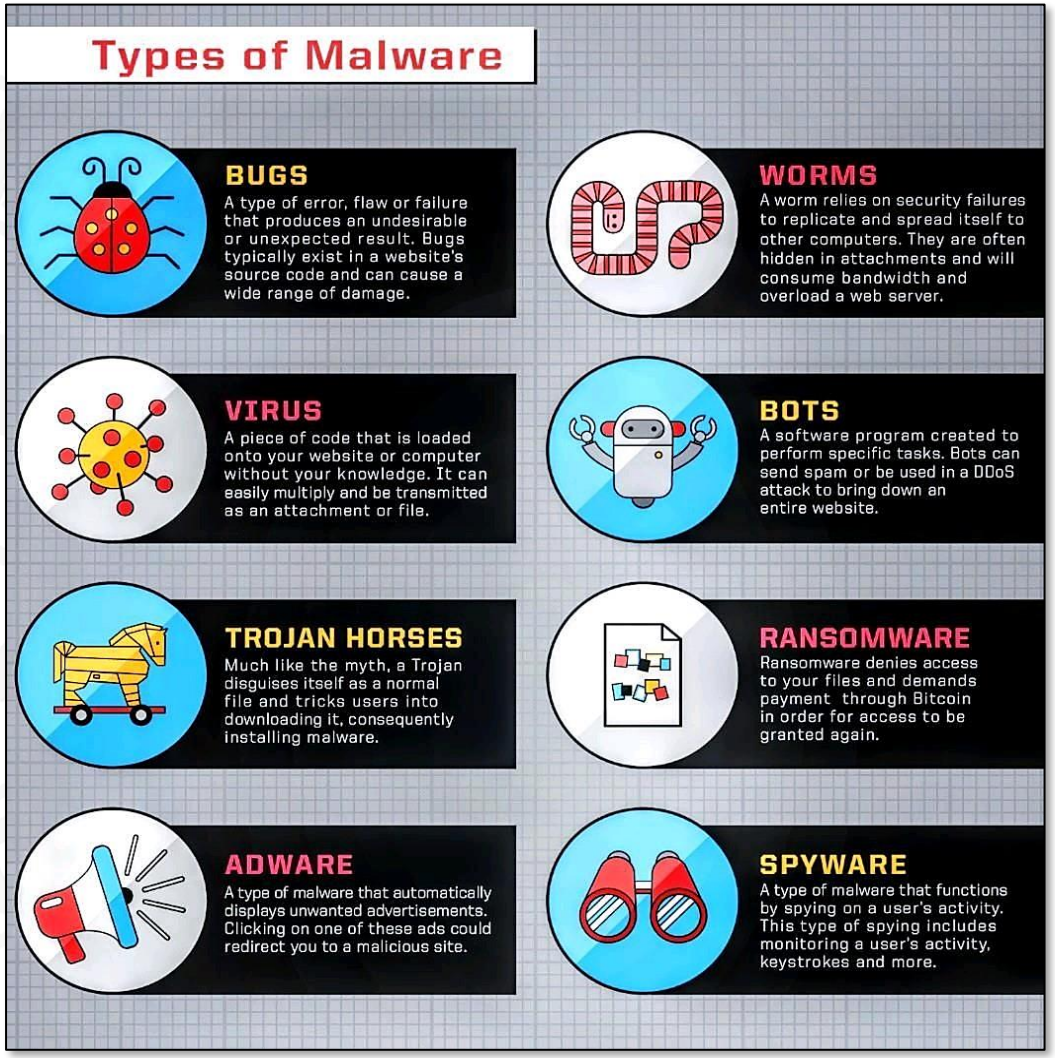
*Icons by Bing Chat AI

Source: Bing Chat AI

Malware (Malicious software)

- **Software aiming to gain unauthorized access**
  - Or cause any kind of harm in computer systems
  - Also known as **malicious code**
  - Software to **detect and delete** them are generally known as antimalware
- **Some common effects are**
  - **Cause failures**: Virus, worms, trojans…
  - **Steal personal / private information**: Spyware, Keyloggers, Stealers…
  - **Distributed / coordinated attacks**: Botnets…
  - **Insert ads** (with additional malicious effects): Adware, Hijackers…
  - **Extortion / financial damage**: Ransomware…
  - **Other**: Rogue software, rootkits…

Source: https://m.facebook.com/viehgroup/photos/types-of-malwarebugs-worms-virus-bots-trojanhorse-ransomware-adware-spyware/2432740090357492/



➢ Exercises **L1B3_MALSCAN**, **L1B3_VIRUST**

Malware by effect: Cause system failure. Propagators

Virus

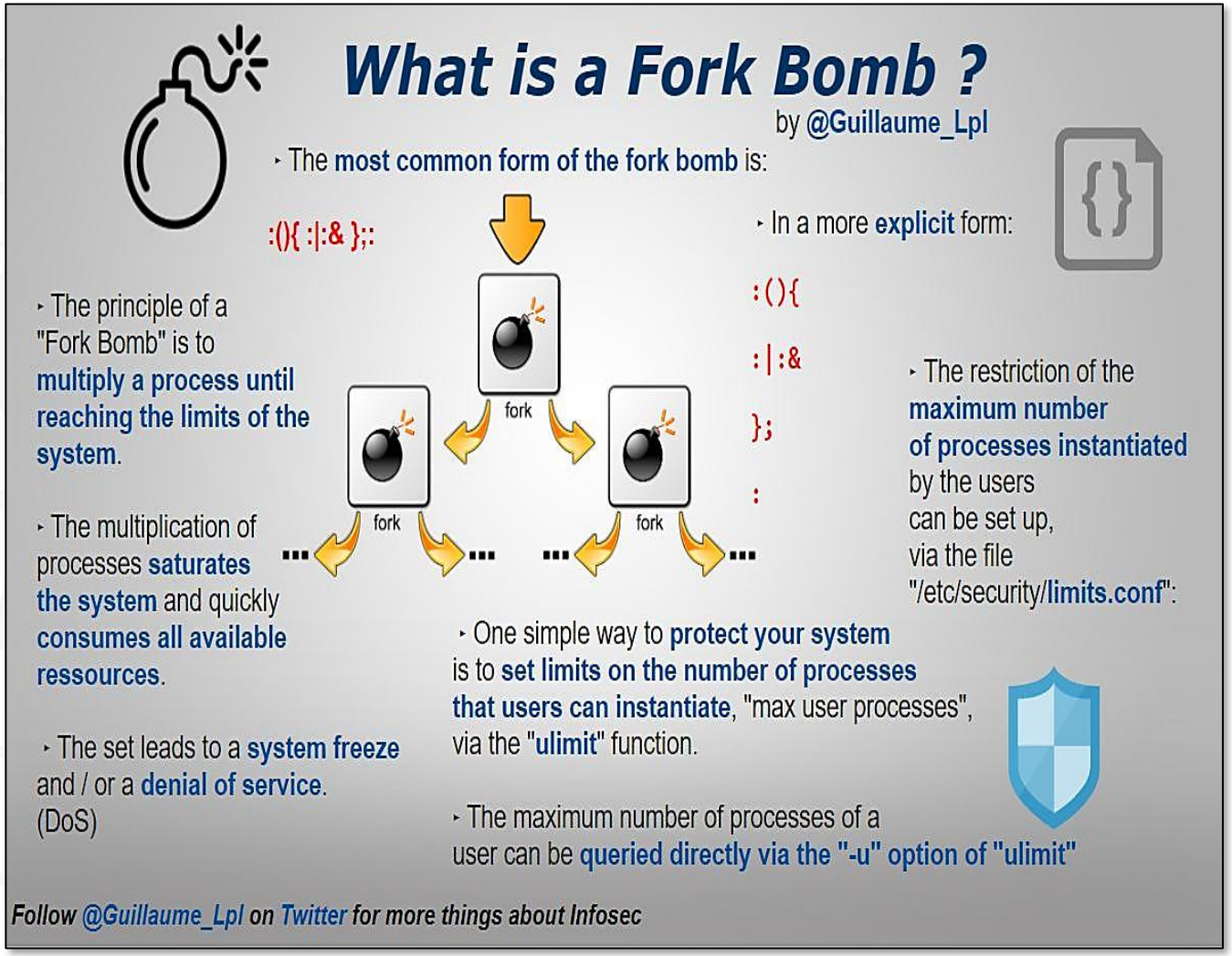
- **Malware created with a double purpose: harm and propagate**
- Cause any type of **harm** when executed: destroy information, impede normal usage…
- **Propagate** to other computers through different means
  - Removable storage devices, shared folders (e. g. SMB protocol), internet-based services…
- They usually have a "**hosting program**" that, once run, launch the virus and their effects
  - Typically, they are long-running software (system services) or modified/fake versions of applications

Worms

- **Malware with an aggressive replication ability**
- Replicates itself in a computer or a computer network to **increase resource usage** so
  - The computers or networks may cease their activity
  - The performance is compromised so normal operation is no longer possible
- Propagation often exploits an existing vulnerability in a service
  - E. g.: EternalBlue, https://en.wikipedia.org/wiki/EternalBlue
- Opposite to viruses, they do not need (and do not infect) other software

Malware by effect: Cause system failure. Wabbit

- **Denial-of-service malware**
- A process continually replicates to deplete resources
  - Slowing down or crashing a system by resource starvation
- Worms without the propagation ability
- **Fork bombs** are the most known example
  - Implementing them is simple: https://en.wikipedia.org/wiki/Fork_bomb



Malware by effect: Cause system failure. Trojan

- **Malware disguised as legitimate software (drivers, tools…)**
- **Usually implement a legitimate functionality**
  - But also comes with hidden harmful effects (backdoor, spyware, showing ads….)
- **Found in non-official download sites (e. g.: Softonic)**
  - And in unofficial app markets…or even official ones!
  - Legitimate programs with “enhanced” or “additional features” that turn out malicious or annoying
  - Mobile markets are plagued with this type of malware (**beware**!)
    - Especially Android’s Google Play Store
- **Currently, supply chain attacks cases are also increasing using trojans**
  - Official versions of legitimate software, but trojanized in its official servers / mirrors
  - IoT devices or other electronic appliances (battery chargers, …) with preinstalled trojans
- **Malware implementing dropper techniques are typically trojans**
  - The actual malicious code is downloaded (in one or more parts) when a program is run

Malware by effect: Stealing information

- **Spyware**
  - **Obtains information about individuals**, computers, or organizations without consent
  - Even fulfilling a set of legal requirements, or downloaded from official sites (anti-cheat…)
  - They collect data in background
    - Files, contacts, emails, accounts, passwords, visited URLs, browsing habits, timetables, visited places…
    - This information is later **sold**, **sent to ad companies**, or **criminal organizations**
  - If it is embedded in trojanized legitimate software, they are usually called **stealers**
- **Keyloggers**
  - **Steals information** by monitoring keyboard presses, mouse movement, screen captures…
  - This user behavioral information is later sent to a third party
    - That may use it to gain some benefit (access to bank accounts, extortion…) or sell it
  - Used also to steal accounts and passwords, disclose private conversations…
  - …or for **usability and usage pattern study** (illegal if the user is not informed and consents)

Malware by effect: Annoying / malicious ads

Adware

- **Software showing intrusive ads in browsers / apps**
- Using pop-up windows, full-screen advertisements, misleading tactics, fake warnings…
  - Imitating typical Windows / Linux UI, fake buttons, worrisome messages ("you've been infected!")…
- Most try to fool users to click in the ad so they can run their payload
  - Malicious ads have been found into legitimate products
  - Inserted by ad services that do not (or cannot) enforce correct limitations to the ads they serve
- Sometimes ads are used by programs to obtain economical benefits
  - Program usage licenses are seldom read / understood
  - **Ads may collect a substantial amount of data**, or perform unwanted or unregulated operations

Browser hijackers

- **Block or difficult browser usage** to gain financial benefits or search engine positioning
- Replacing the starting web page with an ad-ridden one (increasing ad visits and earned money)
- Randomly redirecting to unwanted pages (porn, shops, download pages…) to increase their visits
- Tampering search results to redirect to certain pages, or force using of certain search engines
- They usually **focus in earning money by clicking / visiting ads**, not stealing money from users

Types of malware by effect: Financial damage / extortion. Ransomware

- **Block computer usage and/or its data**
  - By taking full control of their functions/files and **ask for a ransom** to recover it back
- **Important user files are encrypted and irrecuperable without a decryption key, that must be bought paying a ransom**
- **Pay instructions are shown when infection is completed**
  - Not when first infecting the device
  - They may remain dormant a certain amount of time until triggered, ensuring maximum harm
  - They use non-traceable paying methods (e. g.: cryptocurrencies)
- **Data may not be recovered** even if the ransom is paid
  - Decipher key not sent or faulty, corrupted data, multiple extortions…
  - Using non-infected backups is the most advisable solution
  - Hence a solid backup strategy is mandatory!
- **More information**: https://www.osi.es/es/actualidad/avisos/ransomware

Source: TrendMicro

RANSOMWARE

Computer Security

The Ransomware Kill Chain

RECONNAISSANCE

During the Reconnaissance phase, the attacker collects as much information as possible: mailing lists, social media presence, potential vulnerabilities...

During the Weaponization phase, attackers prepare their malicious software. There is a plethora of techniques to disguise the payload in a benign-looking file, (pdf, word, excel...), or in a compromised or malicious website.

DELIVERY

During the Delivery phase, the malicious payload (the dropper) is delivered to the intended target through an infected link to a file or site, an infected attachment, visiting infected websites (watering-hole, exploit kit or drive-by-download attacks) or malvertising.

During the Exploitation phase, existing vulnerabilities will be leveraged to deliver malicious code onto the system to get a better foothold.

INSTALLATION

Once the dropper is on the victim's computer, the Installation process starts. Typically it connects to the Command & Control (C2) server to download key data (a malicious executable file, in some cases the encrytion key...).

There are variants of ransomware that operate on a self-propagation basis and will attempt to infect system files and spread to other hosts. Then, the ransomware starts to encrypt files on the infected computer, and possibly on the network and cloud storage, too.

ACTIONS ON OBJECTIVES

Now, following a succesful installation, C2 establishment and encryption across the existing infrastructure (local hosts, network and cloud resources), we reach the Actions on Objectives phase. The ransomware displays a ransom message to the victim. Typically, the desktop wallpaper is used for this purpose.

Finally, the criminals expect the ransom to be paid in cryptocurrency in a wallet they own. If the victim does not pay, the data is either lost (encryption keys deleted) or breached.

WEAPONIZATION

EXPLOITATION

COMMAND & CONTROL

Cyber Startup Observatory©

cyberstartupobservatory.com

Malware and Ransomware

Cyber Writes
cyberwrites.com

It Is A Type Of Malicious Software That Encrypts Files, Usually The User'S Office Files, And Extorts Money From The Affected Party In Exchange For A "Ransom" For The Affected Information.

How Does It Work?

It All Starts With The Infection Of The Computer By Means Of These Possible Attack Vectors:

Attachments In Emails | Phishing | Downloads | Remote Connection | Malicious Websites

Here Is An Example Of A Ransomware Attack:

Criminal

1 The Cybercriminal Creates The Ransomware And Injects It Into A File, Then Uploads The File Into An Email For Phishing Attacks.

Victim

2 Remember, For It To Work, The Attacker Must Convince The Victim To Download The File.

Victim

Mail:
Bargain Prices!
Check The Document

3 Click On The Link And Download The Ransomware

4 Ransomware Evades Security Measures With Malicious Techniques And Installs Itself.

5 The Ransomware Attempts To Establish A Connection To Command And Control (C&C) Servers Controlled By The Attacker. This Allows The Attacker To Monitor And Control The Infected Machines.

Command And Control Server

Attempts To...

6

7 The Cybercriminal Analyzes The Data, Saves And Encrypts It (And Can Delete It If Desired) From The Victim'S Computer And Clouds.

8 Once The Data Has Been Encrypted, The Criminal Asks For The Money.

Infect Other Devices

ADMIN

Escalate Privileges

Malware by effect: Rootkit

- **Unsolicited and unauthorized software that installs itself with superuser privileges**
- **Their goal is usually to steal information or creating a backdoor**
  - While remaining in the system undetected by the user
  - They may be composed by fake system / hidden / critical files that imitate legitimate ones
  - They usually implement process hiding techniques
    - That do not show them in typical process lists or process information and management software
- **Rootkit-enabled backdoors can be used to introduce additional malware**
- **This technique was also used by copy-prevention or anti-cheating software**
  - By legal companies!
  - This caused a great controversy when discovered
  - https://en.wikipedia.org/wiki/Sony_BMG_copy_protection_rootkit_scandal

Malware by effect: Rogue software

- **Fake programs** claiming to implement functionalities that they do not
- Variants include
  - **Fake antivirus**: even (falsely) claiming that computers are infected to fool users to download them
  - **Malware "cleaning" tools**: again, claiming fake infections
    - They may even turn themselves into additional malware, such as spyware
  - **OS "optimizers"**: That do not really perform any type of optimization
    - And can also hide malware
- Typical in mobile device app stores, especially Android
  - And even in the official store!
- Once installed, they may run a payload with other malware type

CRIMEWARE

- **Any software specially created to commit crimes**
  - Financial, data theft…
- **They are not infected legitimate programs**
  - But software created with the purpose of committing certain crimes
  - Identity theft, password stealing, confidential data capture…
- **They may replicate themselves, like worms**
- **They may be created to be sold to other criminals without the capability of creating their own malware**
  - Exploit packages, exploiting tools…
  - **Ransomware-as-a-Service** (RaaS) is one of the most dangerous current examples
    - *You want to implement a ransomware campaign against someone, but you don't have the knowledge?*
    - No problem! They **rent** you all necessary tools and instruction manuals
      - Or ask for a percentage of the "earnings"

Backdoors

- **Alternative / unofficial methods to access** a computer or software
- Allow attackers to access / control systems without using normal authentication mechanisms
  - Once inside the system, they may gain rights to perform privileged operations
  - **They are a serious security risk**
- Why do they exist?
  - **Intentionally created** by the software developers or any third-party library it uses
    - Maybe without malicious intentions…undocumented “testing” accounts, “control panels” for development that were not deactivated when passing to the production stage…
  - A **consequence of an unintended vulnerability**
    - E. g.: old versions of web pages / services accidentally left online
  - Created by **crimeware**

And now what?

- To explore the different aspects of the cybersecurity world, we need legal targets of study
- Targets may be
  - **Machines** and **networks** of machines
  - **Persons** (yes, they are targets too!)
- This comprises
  - **Create them**
    - Our own custom-made targets (never real ones, as it is illegal unless a contract exists)
    - Using Open-Source INTelligence (OSINT): information available publicly on the Internet
  - **Being able to reach them**
    - And this requires more basic technical knowledge, **specially when locating machines and networks**
    - **Let's go for it!**

Think you've understood it all? Evaluate yourself!

- **You can do the following**
  - *You know what's in a CVE in general and why it's important in security*
  - *You know what the CVSS scoring system is, what kind of elements it contains, and how to interpret a CVSS score*
  - *You understand what a security risk is, and how it's calculated*
  - *You distinguish between attack and damage*
  - *You understand what a security control is, and its contents related to the prevention and response to attacks*
  - *You know the difference between a script kiddie, a pentester, and a cracker*
    - *And, above all, what is NOT a hacker*
  - *You know the difference between a red team, a blue team, and a purple team*
  - *You can distinguish the different types of malware that exist and what they do: Viruses, worms, wabbits, trojans, spyware, keylogger, adware, hijackers, ransomware, rootkit, rogue software, crimeware, and backdoor*
  - *You understand the ransomware kill chain, how it acts, and how it compromises an infrastructure*

< Go to Index

Source: Bing Chat AI

Machine networks >

DNS >

NETWORKING BASICS

You can’t hack what you can’t see!

*Icons by Bing Chat AI

What are you going to find in this block?

- **In the first part of this block, you'll learn**
  - How **communication between machines** is done
  - How to interpret **an IPv4 address** and a **CIDR mask of a network**
- **In the second, you'll learn**
  - That machines in different networks can also communicate with each other if there are elements that allow them to "jump" between networks
  - What is a **private IP** and a public IP
  - What is **NAT** and what is it used for
  - How you have (probably) **set up your internet connection at home**
- **In the third, you'll learn**
  - **Why DNS exists,** and the function it fulfills within the connections to machines we make every day
  - How the DNS naming system **is organized**
  - How a typical DNS request **works in general**

How machines communicate among each other?

- **When we want to communicate with other users in social networks…**
  - We locate these users and send a message to them
  - Then, these users interact with us according to the social network protocols
    - Likes, retweets, gifs, emojis, memes…
- **Curiously, this is the same principle that machines use to communicate with each other!**
  - And trust me, nowadays **there are a LOT** of different machine types communicating between them!

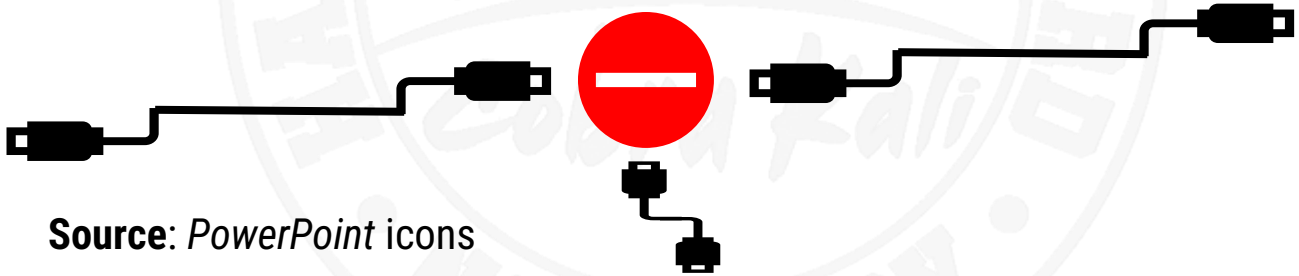
Source: https://formatalent.com/cursos-de-m2m-machine-to-machine

How machines communicate among each other?

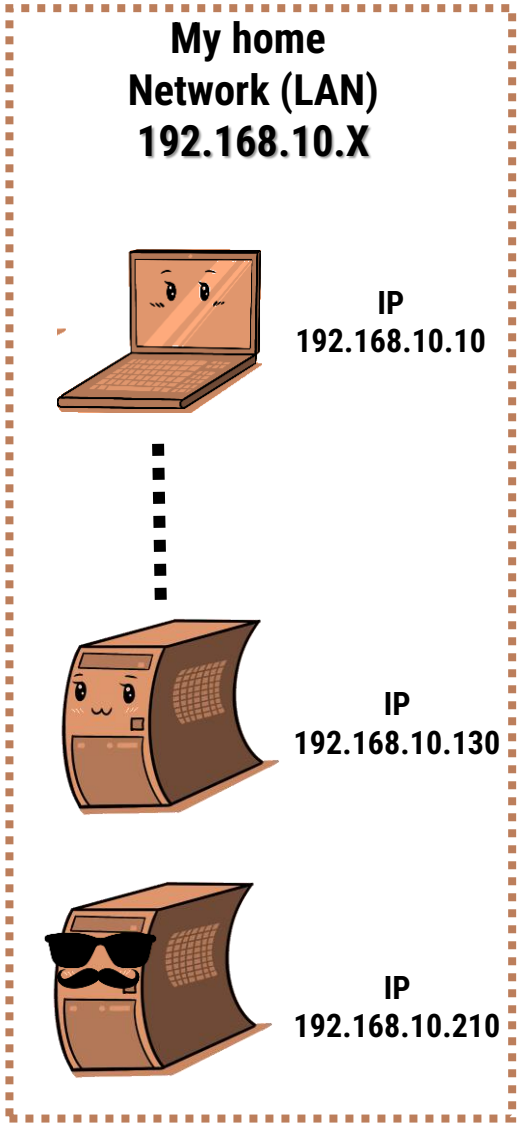
- **In every social network we have a unique identifier that distinguishes us from others**
  - In Twitter, if I want to communicate with Cesar Granda (ex-student, and professional hacker) I must write to @CacharroHacks
- **But machines do not have IDs! Yeah, but they have IPs ☺**
  - **A machine IP is what distinguishes it from other machines** in a network
  - Machines able to communicate **DIRECTLY** among **them CANNOT have the same IP**
    - The same way two users of the SAME social network cannot have the same ID
    - User / machine spoofing! (known as “IP collision”)
- **We are in social networks, but machines are in IP networks**
  - The approach is the same!
  - Let’s remember concepts from FCR ☺

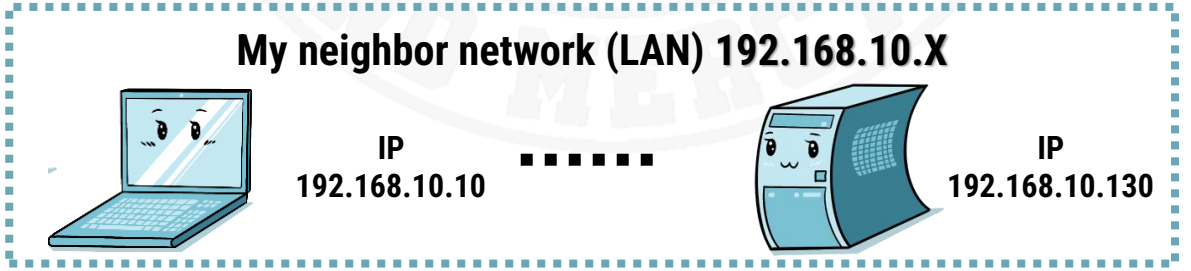
IP NETWORKS

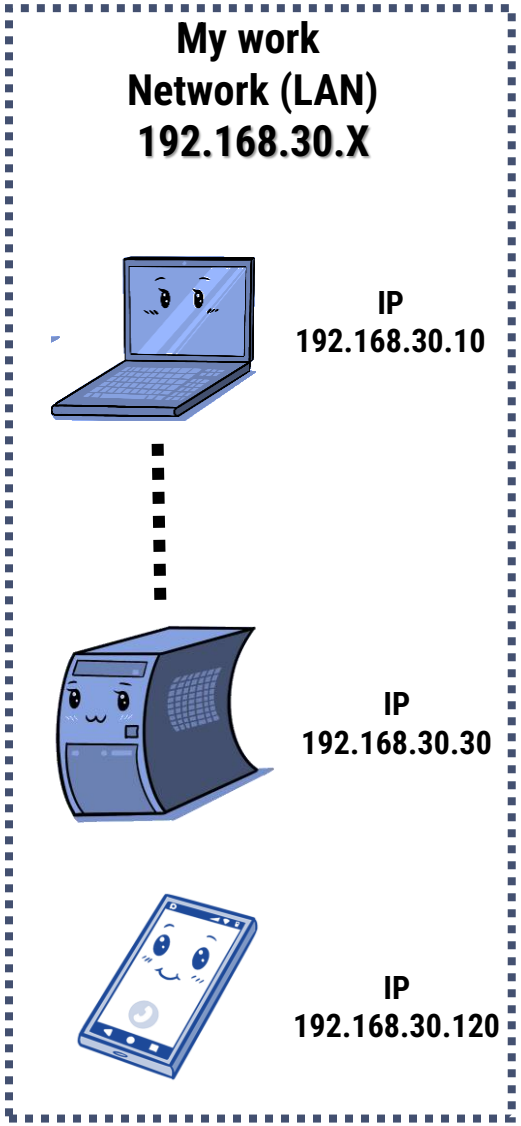
- **LAN**: a network that interconnects machines within a limited area
  - Residence, school, laboratory, campus, office…
- **Without the help of other devices, machines in different LANs cannot see each other**
  - This also means that two machines in different LANs can have the same IP
  - The problem occurs with machines in the same LAN!



Source: *PowerPoint* icons







IP v4 ADDRESSES

- **The internet protocol belongs to the network layer**
  - Remember network layers and protocols from FCR?
- **Internet protocol addresses (IP addresses) are the basis of current communications**
  - Each connected device (computer, phone, tablet, Raspberry, IoT bulb...) has an IP address
  - It is what allows us to communicate and connect with it
  - That is, it is its **contact address**
- **Historically, IP version 4 (IPv4) has been used**
  - Their addresses consist of four 8-bit groups, for example `192.168.1.100` (32 bits)
  - Each of the numbers between the dots (.) is a byte, that is, an 8-bit data
  - Therefore, each number is in the 0-255 range
  - **They have been exhausted**: worldwide networks are (slowly) **transitioning to IPv6** (128 bits)

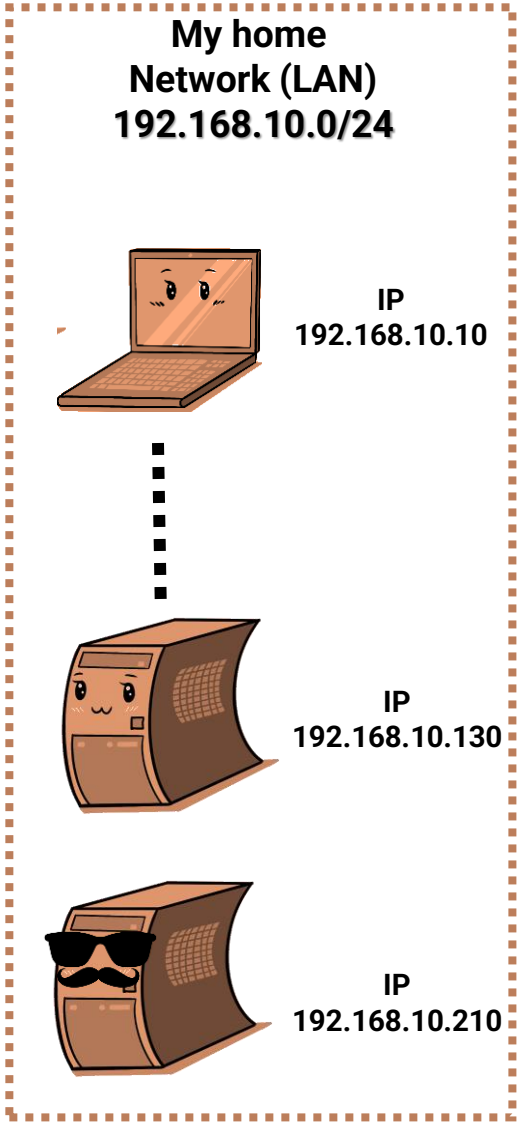
Classless Inter-Domain Routing (CIDR)

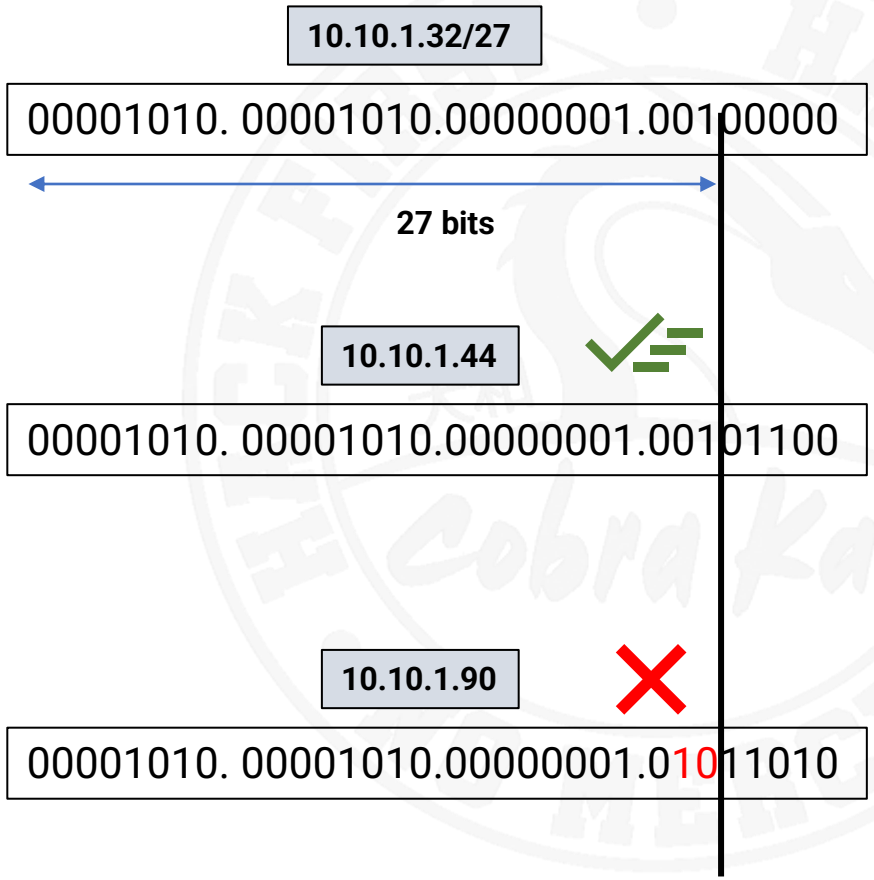
- **CIDR is a bit-based standard that uses prefixes to display IP addresses with their routing properties**
  - Facilitates routing by grouping address blocks into single entries of a routing table
  - In other words, is a way of representing multiple IPs (groups of IPs) with the same identifier
- **These groups are called CIDR blocks**
  - IPs in the same CIDR block share an initial bit sequence (of a certain length) in their binary form
  - This sequence is called **prefix**
- **IPv4 CIDR blocks use a syntax close to IP addresses:** `A.B.C.D/N`
  - A decimal IPv4 address with dots, followed by a forward slash
  - Then a number (N) from 0 to 32
  - This number is the length of the prefix
    - The number of initial bits **shared by all machines in the represented network**
    - Counting from the most significant bit

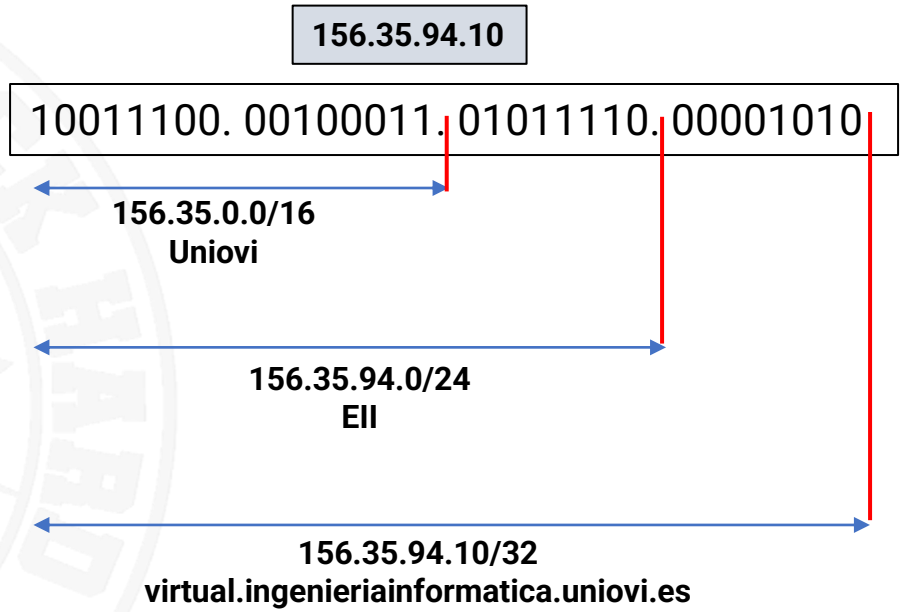
Classless Inter-Domain Routing (CIDR)

- **Specifying only the network size omits the address of the notation**
  - Therefore, a `/20` block is a CIDR block with an unspecified 20-bit prefix
- **An IP address is part of a CIDR block (match the CIDR prefix) if the initial N bits of the address and the indicated by the CIDR prefix are the same**
  - An IPv4 address is 32-bit, so an N-bit CIDR prefix leaves 32-N bits unmatched
  - Meaning that $2^{(32-N)}$ IPv4 addresses can match a given N-bit CIDR prefix
  - **Shorter CIDR prefixes match more addresses, while longer prefixes match less**
    - Shorter prefixes mean less networks with more potential machines (a few large networks)
    - Larger means more networks with less potential machines (lots of small networks)
    - A single address can match multiple CIDR prefixes of different lengths
  - Sometimes this is represented by a bit mask (`255.255.255.0` vs `/24`)
- **CIDR is also used for IPv6 addresses and the semantics are identical**
  - The length of the prefix may vary from 0 to 128, due to the higher number of bits

Classless Inter-Domain Routing (CIDR)







Do you want to practice this?
https://www.ipaddressguide.com/cidr

Source: *PowerPoint* icons

Classless Inter-Domain Routing (CIDR)

Computer Security

- Small and large LANs (N from /28 to /24) are the most used nowadays
- For laboratories and tests, it is very common to use /24
  - Up to 256 machines in the network
- The /31 are used to create point-to-point links between devices
  - Two devices communicated directly
- ISPs (e. g.: Telecable) usually have /21 or lower

IPv4 Subnetting

packetlife.net

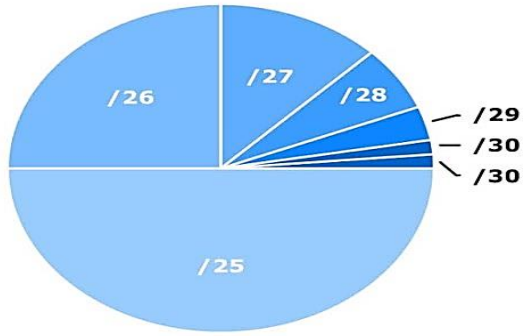
Subnets

CIDR	Subnet Mask	Addresses	Wildcard
/32	255.255.255.255	1	0.0.0.0
/31	255.255.255.254	2	0.0.0.1
/30	255.255.255.252	4	0.0.0.3
/29	255.255.255.248	8	0.0.0.7
/28	255.255.255.240	16	0.0.0.15
/27	255.255.255.224	32	0.0.0.31
/26	255.255.255.192	64	0.0.0.63
/25	255.255.255.128	128	0.0.0.127
/24	255.255.255.0	256	0.0.0.255
/23	255.255.254.0	512	0.0.1.255
/22	255.255.252.0	1,024	0.0.3.255
/21	255.255.248.0	2,048	0.0.7.255
/20	255.255.240.0	4,096	0.0.15.255
/19	255.255.224.0	8,192	0.0.31.255
/18	255.255.192.0	16,384	0.0.63.255
/17	255.255.128.0	32,768	0.0.127.255
/16	255.255.0.0	65,536	0.0.255.255
/15	255.254.0.0	131,072	0.1.255.255
/14	255.252.0.0	262,144	0.3.255.255
/13	255.248.0.0	524,288	0.7.255.255
/12	255.240.0.0	1,048,576	0.15.255.255
/11	255.224.0.0	2,097,152	0.31.255.255
/10	255.192.0.0	4,194,304	0.63.255.255
/9	255.128.0.0	8,388,608	0.127.255.255
/8	255.0.0.0	16,777,216	0.255.255.255
/7	254.0.0.0	33,554,432	1.255.255.255
/6	252.0.0.0	67,108,864	3.255.255.255
/5	248.0.0.0	134,217,728	7.255.255.255
/4	240.0.0.0	268,435,456	15.255.255.255
/3	224.0.0.0	536,870,912	31.255.255.255
/2	192.0.0.0	1,073,741,824	63.255.255.255
/1	128.0.0.0	2,147,483,648	127.255.255.255
/0	0.0.0.0	4,294,967,296	255.255.255.255

Decimal to Binary

Subnet Mask		Wildcard	
255	1111 1111	0	0000 0000
254	1111 1110	1	0000 0001
252	1111 1100	3	0000 0011
248	1111 1000	7	0000 0111
240	1111 0000	15	0000 1111
224	1110 0000	31	0001 1111
192	1100 0000	63	0011 1111
128	1000 0000	127	0111 1111
0	0000 0000	255	1111 1111

Subnet Proportion



Classful Ranges

A	0.0.0.0 – 127.255.255.255
B	128.0.0.0 - 191.255.255.255
C	192.0.0.0 - 223.255.255.255
D	224.0.0.0 - 239.255.255.255
E	240.0.0.0 - 255.255.255.255

Reserved Ranges

RFC 1918	10.0.0.0 - 10.255.255.255
Localhost	127.0.0.0 - 127.255.255.255
RFC 1918	172.16.0.0 - 172.31.255.255
RFC 1918	192.168.0.0 - 192.168.255.255

Terminology

CIDR
Classless interdomain routing was developed to provide more granularity than legacy classful addressing; CIDR notation is expressed as /XX

VLSM
Variable-length subnet masks are an arbitrary length between 0 and 32 bits; CIDR relies on VLSMs to define routes

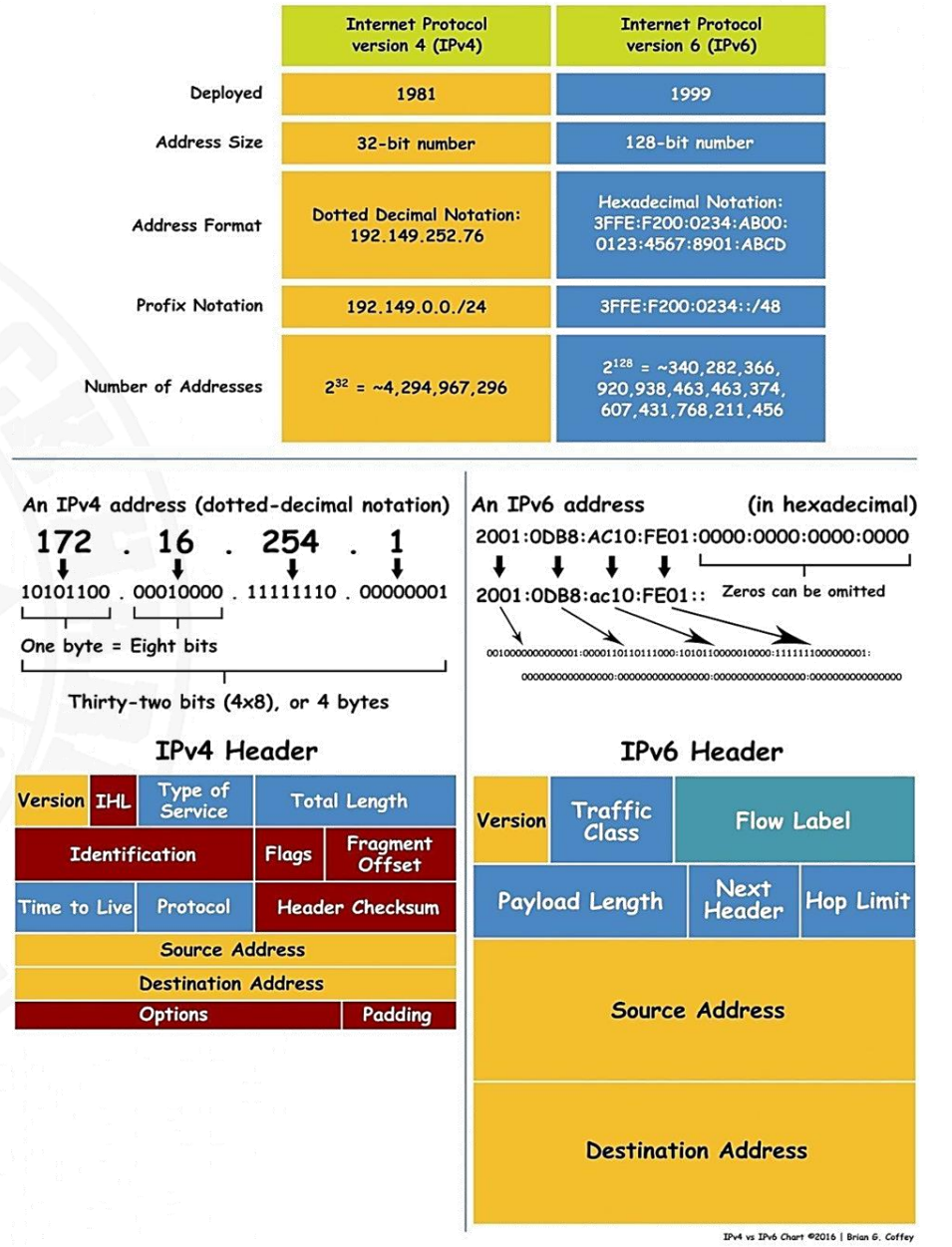
by Jeremy Stretch v2.0

Classless Inter-Domain Routing (CIDR): Reserved addresses

- Small and large LANs are the most deployed network types
- Typically, the first address of a subnet (all host bits to 0) is reserved to refer to the network itself
  - Example: `192.168.35.0`
- The last address (all host bits to 1) is used as a broadcast address for all hosts on the network
  - Example: `192.168.35.255`
  - Address to send a message to all hosts in the network at the same time
- This reduces the number of addresses available for hosts by 2

IP v6 ADDRESSES

- **Internet growth depleted the pool of available IPv4 addresses**
  - A new version of IP (IPv6), **using 128 bits**, was standardized
  - This means much larger (2^{128}) addressing space
- **As IPv4, IPv6 addresses also identify a network interface of a device**
  - But connected to an IPv6 computer network
- **An IPv6 address is represented as eight groups of four hexadecimal digits**
  - Each group representing 16 bits
  - The groups are separated by colons (`:`)
  - **Example**: `2001:0db8:85a3:0000:0000:8a2e:0370:7334`
- **More information**
  - https://www.ipv6.com/general/ipv6-addressing/



Think you've understood it all? Evaluate yourself!

?

- **You can do the following**
  - *You understand that within the same network, IPs identify different machines and that, therefore, there cannot be two machines with the same IP*
  - *You understand the concept of LAN*
  - *You know what IPv4 looks like and its structure*
    - *And why they can only be composed of numbers from 0 to 255*
  - *Understand the concept of a CIDR mask and what it is for*
    - *As well as the technique that is used to know whether an IP belongs to a given CIDR mask*
  - *You know what the two typically reserved IP addresses in a network are for*
  - *Understand what IPv6 was created for and its overall structure*

Machine networks

Machines never talk alone ☺

*Icons by Bing Chat AI

Understanding machine networks

- **In a social network you can normally communicate with every user of that network**
  - Unless the user isolates itself from others (private accounts, closed groups…)
- **In a machine network, you can communicate with every device which has an IP compatible with yours**
  - Devices **whose IP matches the same CIDR**
  - Machines in the same network can normally communicate between them
  - Unless they also restrict this to specific machines
    - For example, by using **firewalls**
  - They have also their closed groups / private accounts-like mechanism as in social networks!

Understanding machine networks

- **But what happens if senders and receivers are in different networks?**
- **In social networks, communication between different networks is not possible or is heavily restricted**
  - You cannot send a tweet to a Facebook user
  - However, you can send an Instagram history or photo to your connected Facebook account
- **But you CAN communicate machines in different networks**
  - Thanks to special devices that act as "**bridges**" or "**gateways**" between both networks
  - And that is what we are about to explain!
  - But first, we need to review two concepts regarding IPs

Public and private IPs. NAT

- As we said, IPv4 no longer has addresses for all Internet-connected devices
- A system was developed to use a group of IPs only in LANs: **private IPs**
  - `192.168.0.0 - 192.168.255.255`
  - `10.0.0.0 - 10.255.255.255`
  - `172.16.0.0 - 172.16.255.255`
- Different LANs in the world can use these address ranges
  - But they **cannot be used on Internet**
- Typically, a router assigns one private IP to each device connected to it
  - Forming its private LAN
- And it sends all connections outside its private LAN over a unique IP
  - Valid on the network that is "on the other side" of the router
  - “Translating” private IPs to IPs that can be used on the "other side" network
  - At some point in this chain of connections, the translated IP is **public and valid over the Internet**
  - This translation mechanism is called **NAT** (Network Address Translation)

NAT?

- The NAT concept from a social network perspective is like “reverse” user groups
- Posting to a user group means that every user in this group receive the message
- But this is the opposite!
  - Any message created by a group member (machine)
    - Is **posted with the group id / name / hashtag** (a valid IP on the receiver machine network) to the outside
    - The user (machine) that issued the message is not visible
  - If someone replies to the message
    - Only the original sender receives this response
  - Therefore
    - Requests are translated to IPs of the destination net
    - Responses are translated to IPs of the origin network
      - And routed only to the machine that originated the request
    - This is handled by software like iptables (see ASR)

Source: https://www.profesionalreview.com/2020/08/22/modo-nat-que-es/

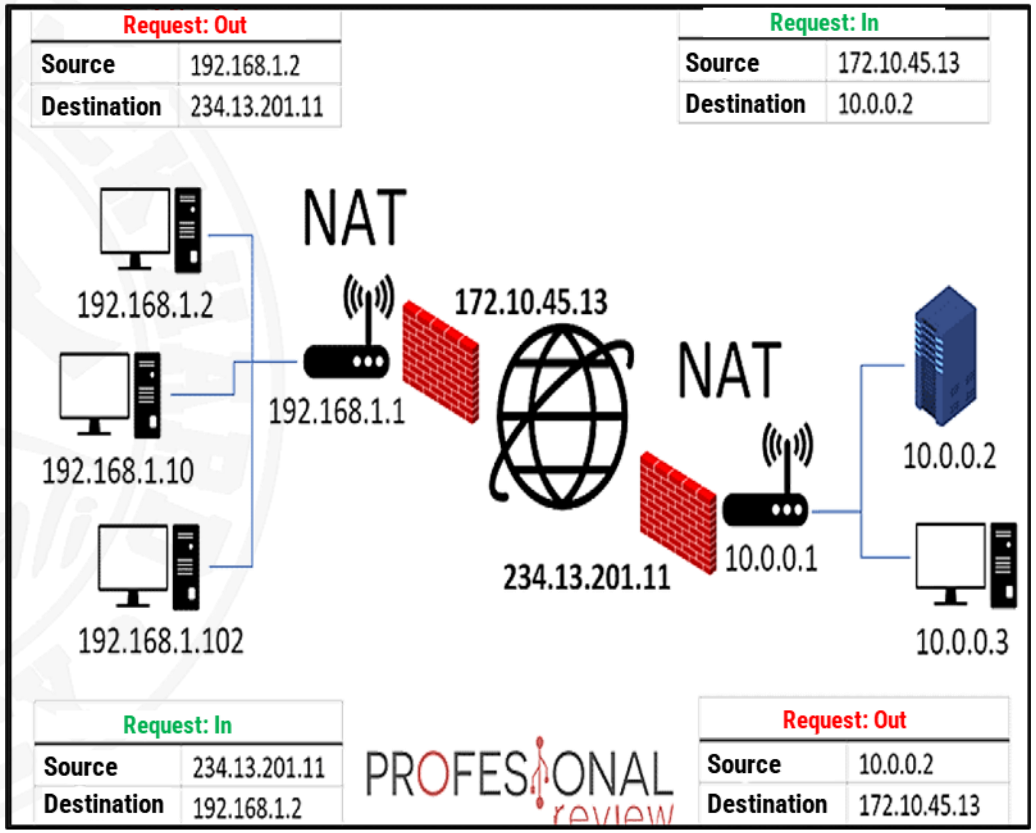
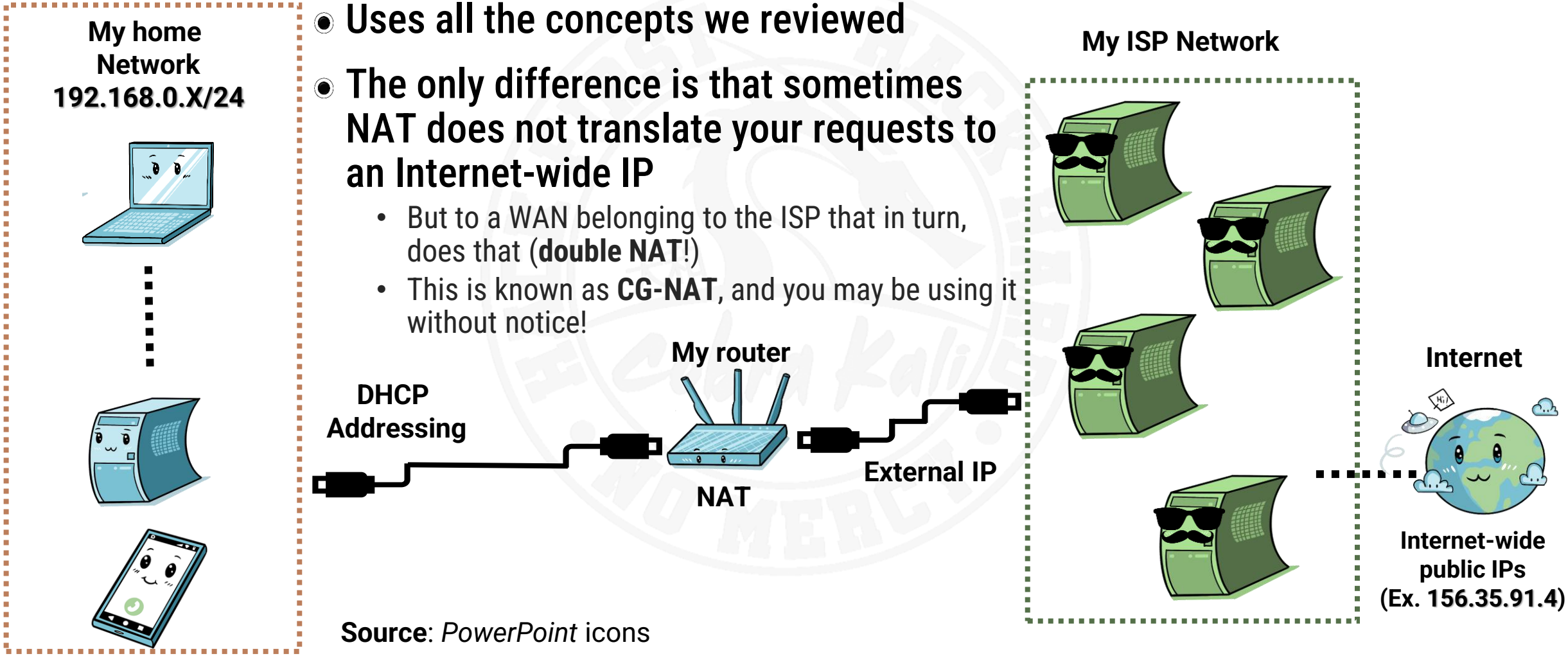


Diagram: Typical home ISP NAT + DCHP router

- This is the typical home network layout
- Uses all the concepts we reviewed
- The only difference is that sometimes NAT does not translate your requests to an Internet-wide IP
  - But to a WAN belonging to the ISP that in turn, does that (**double NAT**!)
  - This is known as **CG-NAT**, and you may be using it without notice!



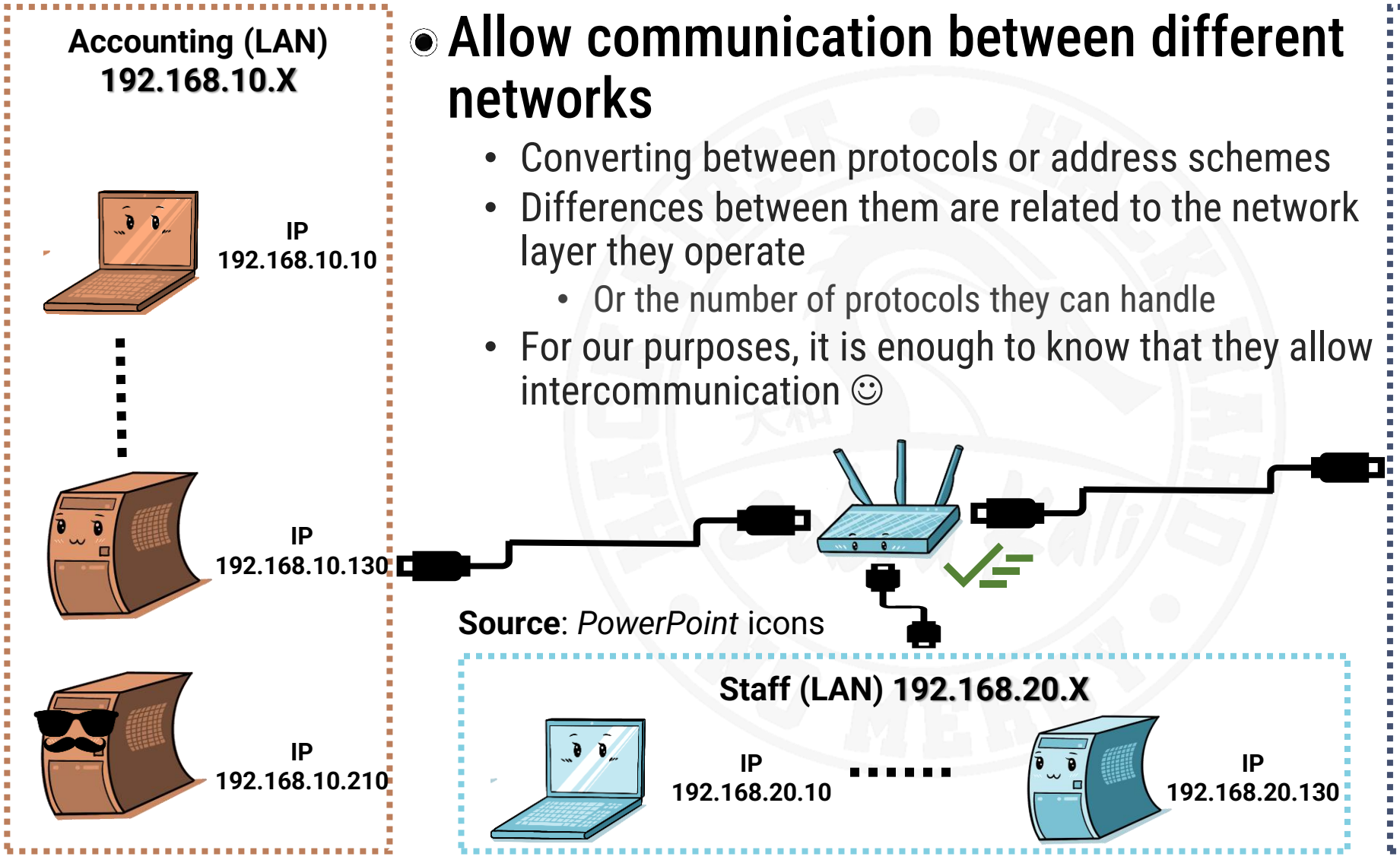
Source: *PowerPoint* icons

DHCP (Dynamic Host Configuration Protocol)

- **Routers assign IPs to its network devices manually or automatically**
- **DHCP is the protocol that assigns IP addresses automatically and dynamically**
  - This means that a device does not have to have the same IP address all the time, but also does not worry about how to obtain it ☺
  - You will see more details about DHCP in ASR
- **It is very typical of local networks**
  - When a device connects to a LAN, it requests an IP address to a DHCP server (Ex.: the router)
  - The DHCP server then assigns an IP address to that system for a fixed period, known as **lease**
  - Each time you connect to the LAN, you are likely to receive a different (**dynamic**) IP address
    - But usually in the same range
    - For example, `192.168.0.0` - `192.168.255.255` (Private IPs)
- **This, combined with NAT on a router, ensures that any home / office / … can connect devices to Internet with minimal effort (and with just one IP)**

Gateways / Network bridges / Routers / Switches

- **Allow communication between different networks**
  - Converting between protocols or address schemes
  - Differences between them are related to the network layer they operate
    - Or the number of protocols they can handle
  - For our purposes, it is enough to know that they allow intercommunication ☺



Source: *PowerPoint* icons

To summarize…

- **It is a little more complicated that social networks**
- **Your machine IP (identifier) determines the machines which you can "talk" directly to**
  - There are "compatible" IPs (match the CIDR of your network)
  - And "incompatible" ones (do no match it)
- **To "talk" with machines in different networks you need a "translator"**
  - Gateways, network bridges, routers or switches are different types of translators
  - That are used depending on the protocols and the network topology
- **This way any machine can potentially talk with any other in the world…**
  - But normally, there are elements that forbid communications for security reasons (like firewalls)
  - We will talk about them later in the year!

Think you've understood it all? Evaluate yourself!

?

- **You can do the following**
  - *You understand that, within the same network, machines can communicate with each other*
    - *Unless there's something that prevents it, like a firewall*
  - *You understand that there are elements that allow communication between machines that are placed in different independent networks, such as gateways, routers...*
  - *You understand that, thanks to that, today we have a huge number of different interconnected networks*
    - *And that, as users, they do a job that we only see when they fail*
  - *You understand what a private IP is and why your home PC has one*
  - *You know what the concept of NAT is, and how it allows you to have many devices connected to the internet with a single router and a single public IP*
  - *You understand the great deal of network management work that the DHCP protocol takes off our shoulders*

DNS

Domain Name Service

*Icons by Bing Chat AI

Source: Bing Chat AI

IPs ARE DIFFICULT TO REMEMBER!

- **In social networks we use unique hashtags to remember users**
  - They are far easier to remember (and search) than a series of numbers (IPv4) or hexadecimal characters (IPv6)
  - `@hibarikky` is far easier to remember than "`TwitterUser13224343245`"
    - If Twitter still exist while you are reading this ☺
- **Users normally have a common named tied to their hashtag**
  - "Tomás Balaguer" is much easier to remember (and search) than `@eftomas`
- **Apart from that, we (almost) never browse using IPs (it's hacker's stuff! ☺)**
- **Every machine in a network has an IP assigned, but we do not use it, we use its unique "name" (E. g.: `www.facebook.com`)**
  - How is that possible?
  - Because there is a "**translation**" service that converts IPs to names and vice versa
  - This is the **DNS** (Domain Name System) service!

Domain Name System (DNS)

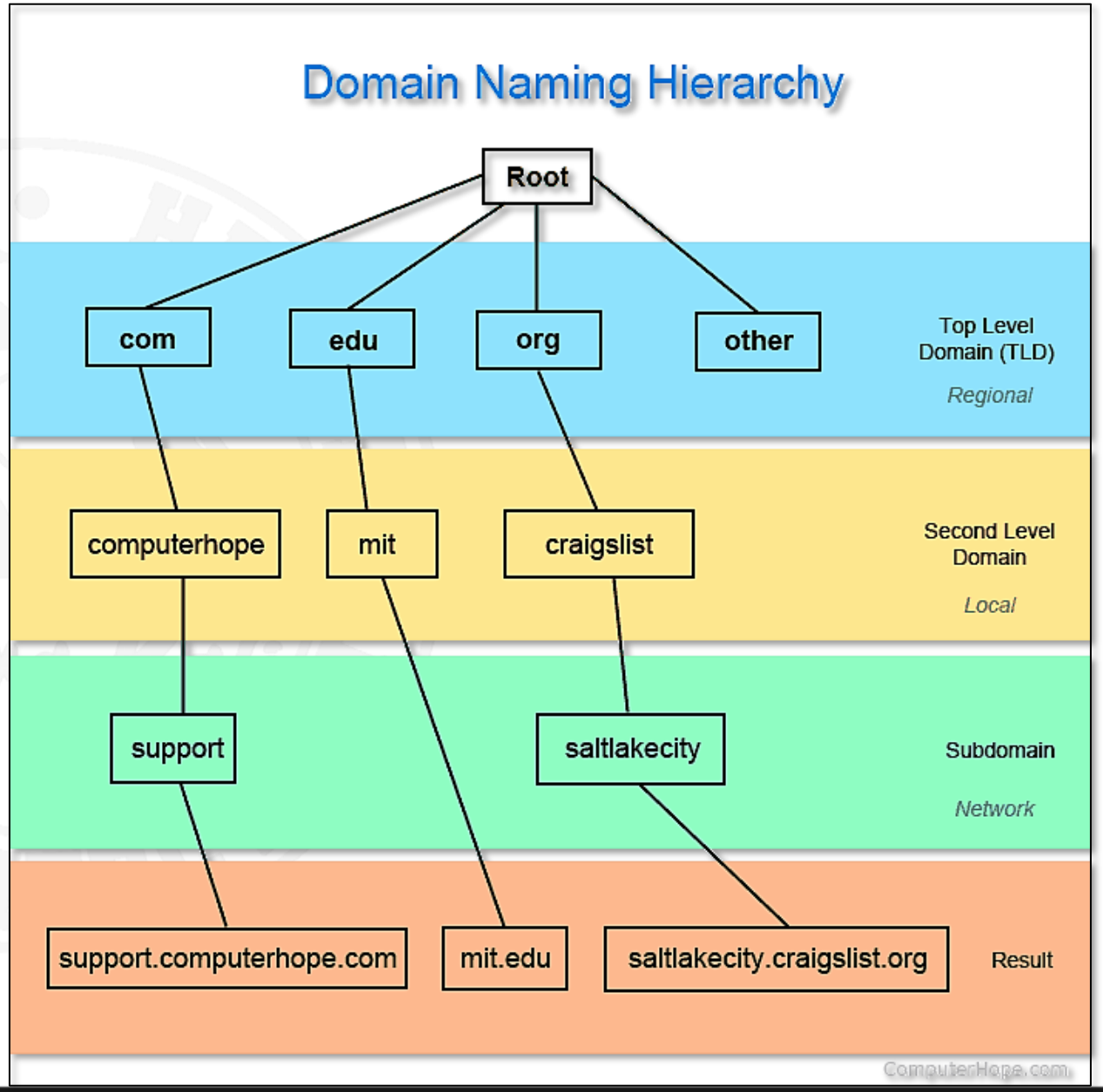
- **Hierarchical and decentralized naming system for devices, services, or other resources connected to any network**
  - Associates IP addresses with human-friendly domain names assigned to these entities
    - E. g. `156.35.94.1` is www.ingenieriainformatica.uniovi.es
  - **It is distributed**: it can delegate the responsibility of assigning domain names and mapping those names to Internet resources to other entities
    - By designating **authoritative DNS name servers** for each domain
      - The one that answers the requests for a **zone** of the DNS namespace (the zone boss! ☺)
    - Network admins may also **delegate authority** over sub-domains to other name servers
    - Therefore, it is a distributed and fault-tolerant service that avoids using single large central DB
- **A DNS name server stores the DNS records for a domain**
  - They answer queries to their name database
  - You will see plenty of details about DNS in ASR
    - Here we only need to understand the basics about how it works to continue
    - Remember the `nslookup` tool from ASR

Domain Name System (DNS): To summarize

- **The domain name system or DNS allows remote machines to be accessed by an easy-to-remember name**
  - Instead of their unique IP
  - The name of a remote system is called a **domain name**
  - Therefore, DNS was designed to translate a domain name into an IP address
  - The reverse translation process (IP to domain name) can be also supported
  - It works with IPv4 and IPv6
- **The translation process is automatic and transparent**
  - That's what makes the Internet possible today
  - As it controls every site you browse to, it can be also a security element
    - Avoiding browsing to **previously known malicious sites**. E. g. NextDNS
- **To be scalable, it does not depend on a single file or server**
  - But of several ones worldwide
  - DNS servers have a hierarchical organization
  - And hence the dot-separated form of the names they resolve

Domain Names

- **Domain names must be registered with ICANN**
  - Internet Corporation for Assigned Names and Numbers
- **Usually through a company that works as an intermediary**
  - For example, the one we hire to host a site
- **Top-level domains are called TLDs**
  - They are the `.com`, `.edu`, `.org`…, and many others that we usually see at the end of the **Fully Qualified Domain Name** (FQDN)



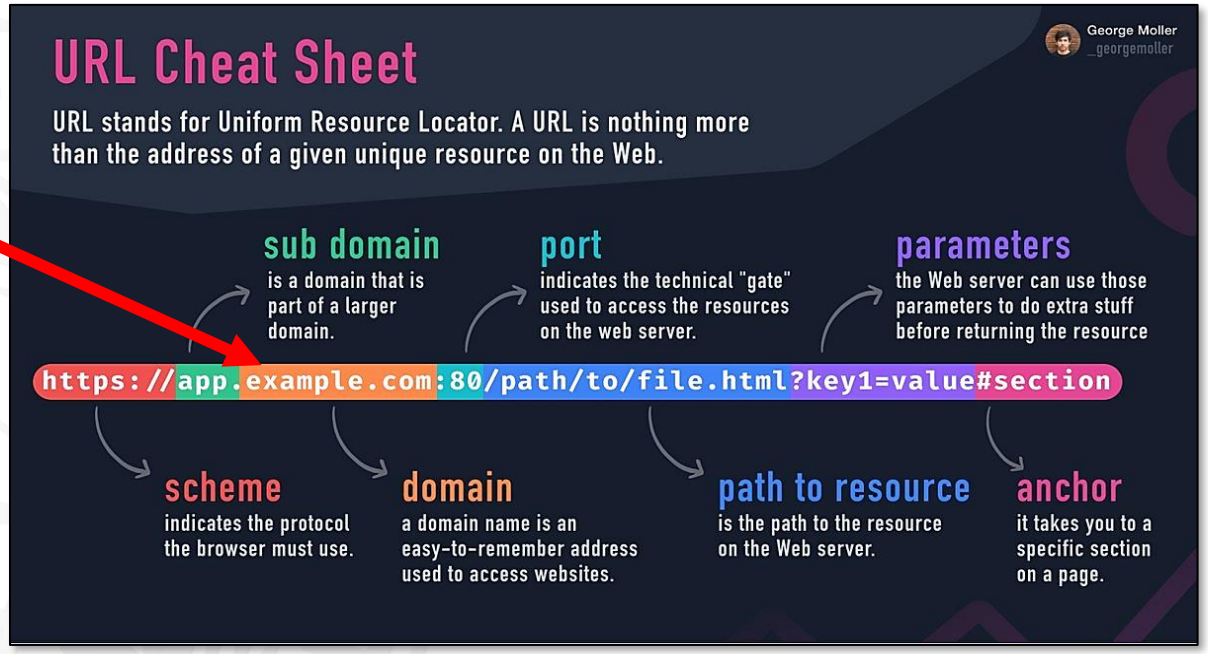
Source: https://www.computerhope.com/jargon/d/dns.htm

Domain names

- **As we said, DNS works hierarchically**
  - Top-level domains or TLDs can have multiple subdomains below them
  - In the previous diagram, `.mit` and `.craiglist` are part of the top-level `.edu` and `.org` domains respectively
  - These are called **subdomains** (SLD, Second-Level Domain)
    - Domains that are part of a larger domain
    - In the example, `mit` and `craiglist` are second-tier domains under their own TLD
  - And, of year, below these SLDs there **may be many other subdomains**
    - In the example, below `.com`, we have `computerhope.com` and `support.computerhope.com`
  - This subdivides the domain into parts
    - The leftmost part is always the most specific,
    - While the rightmost part is the most general
    - **Read it from right to left, separating sections using '.'**
      - E. g.: `support.computerhope.com`: Commerce (`com`) named "Computer Hope" (`computerhope`), "support" (`support`) section
- **The WHOIS service gives you information about a domain and its owner**

How DNS works

- **What happens when you type a URL and press Enter?**
  - From the client point of view, not much
    - It asks for the IP of **the domain name** to its DNS
  - If that DNS server knows the IP associated to the name, it just returns it
  - The complicated part starts when the DNS server does **not** know this IP
    - It has a limited amount of space to store these associations…



Client

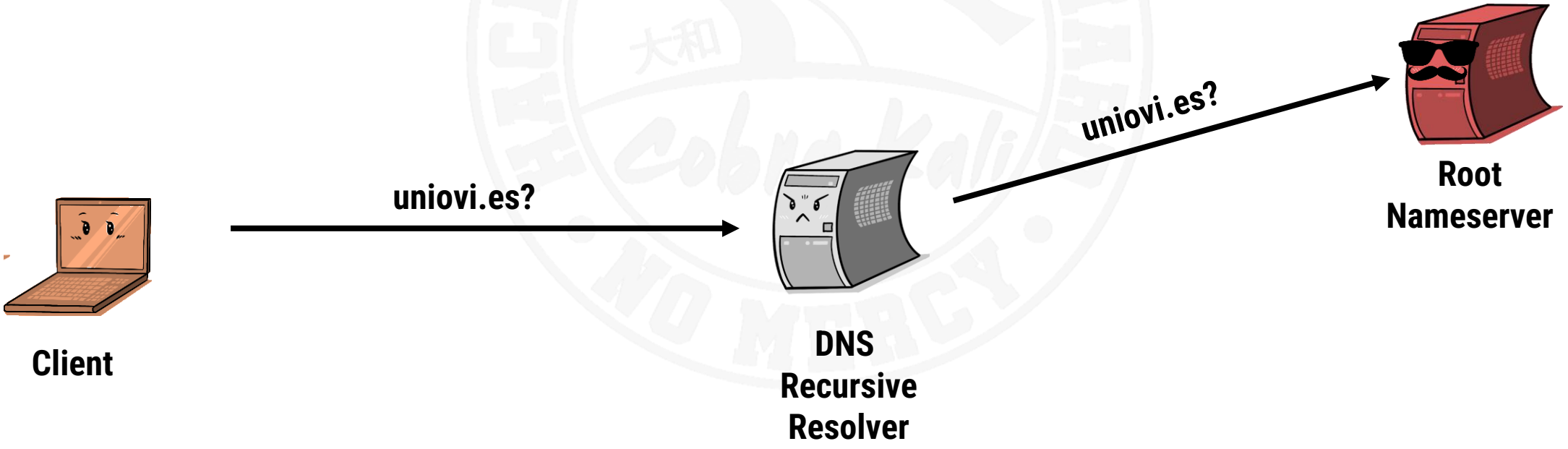
www.uniovi.es?

156.35.233.105

DNS Server

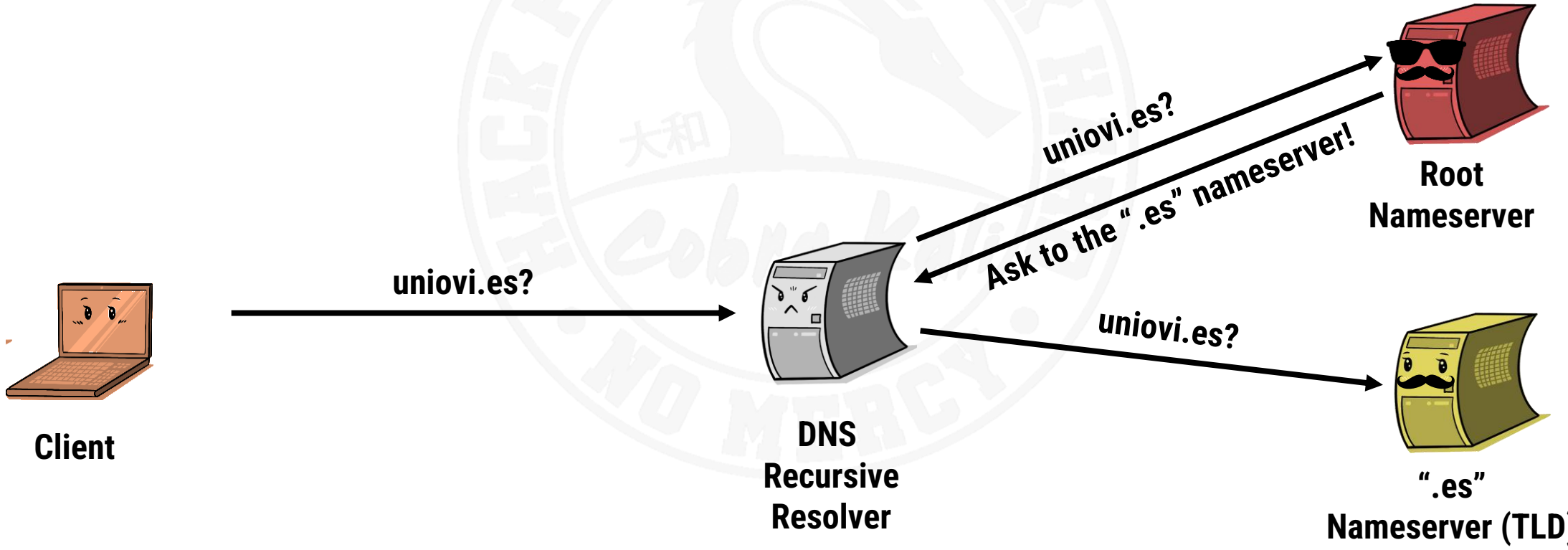
How DNS works

- **If the DNS server does not know the IP of the domain name, it uses a recursive resolution process to look for it**
  - First, the DNS recursive resolver sends DNS query to a **Root Nameserver**
  - The IP address of the root nameservers is known



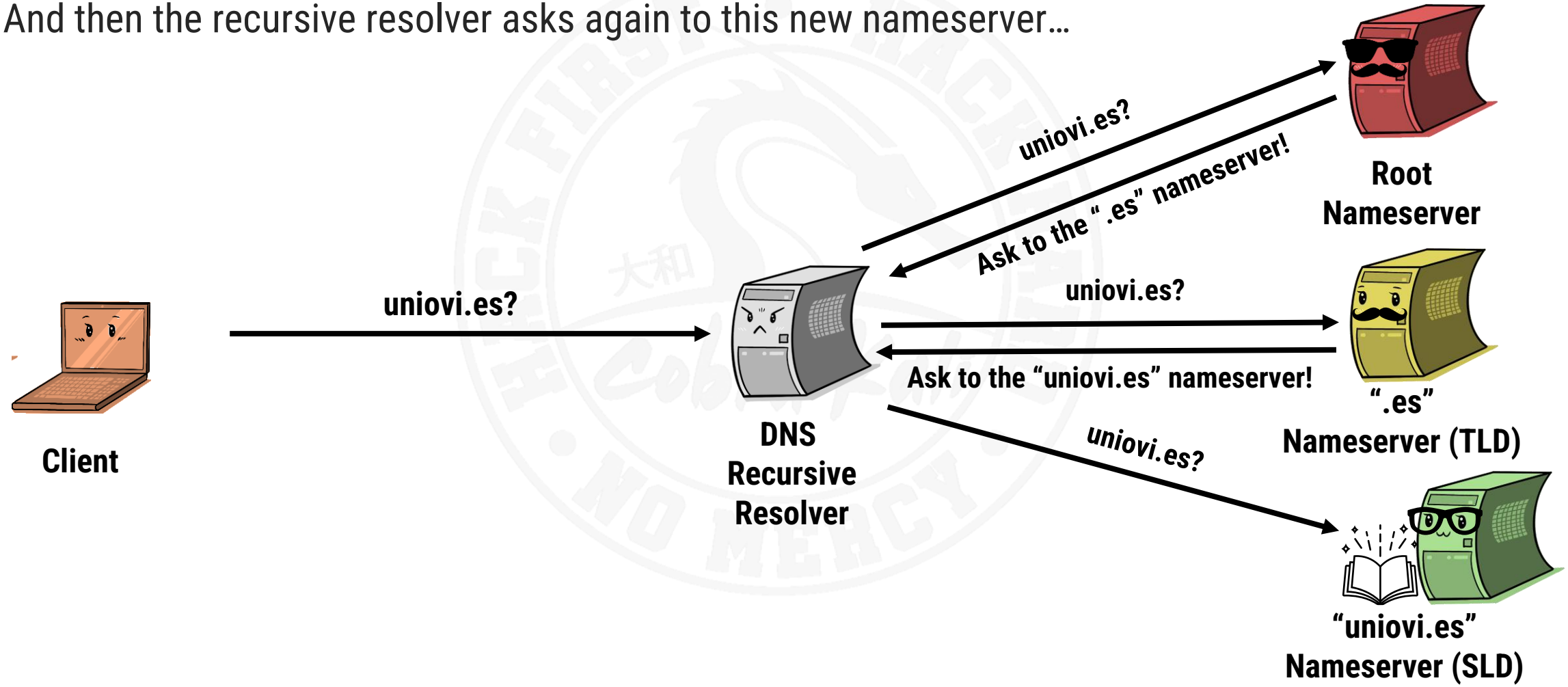
How DNS works

- **Then, the Root Nameserver responds with the IP address of the corresponding TLD nameserver**
  - "`.es`" nameserver in our case
  - The recursive resolver then asks this new nameserver for the domain name



How DNS works

- The TLD Nameserver then responds with the IP address of an adequate SLD domain nameserver (the "`uniovi.es`" nameserver)
  - And then the recursive resolver asks again to this new nameserver…



How DNS works

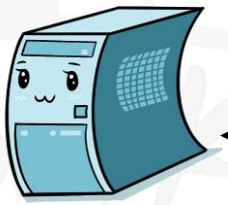
- This SLD domain nameserver is marked as **authoritative** for `uniovi.es`
  - So, it finally replies with the server IP address!
  - The DNS recursive resolver finally responds to client
  - Sending the server IP address and **caching it for future requests**

Client

Finally!

uniovi.es?

156.35.233.105



DNS Recursive Resolver

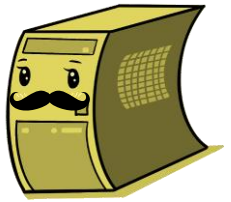
uniovi.es?

Ask to the " .es" nameserver!

Root Nameserver

uniovi.es?

Ask to the "uniovi.es" nameserver!



".es" Nameserver (TLD)

uniovi.es?

156.35.233.105

"uniovi.es" Nameserver (SLD)

Interested in "playing" with DNS queries to better understand how they work? Try this: https://messwithdns.net

Think you've understood it all? Evaluate yourself!

?

- **You can do the following**
  - *You understand that, without a DNS, we would have to remember every IP on every machine, and that's not humanly possible*
  - *You understand that if a DNS is hierarchical and decentralized, it is precisely to be resistant to failures of parts of its infrastructure*
  - *You know it's an authoritative DNS name server*
  - *You understand that if a DNS server doesn't know the IP of one machine, it delegates to others following a known algorithm*
  - *You know what the concept of TLDs and SLDs is*
  - *You understand what part of a URL is used in a DNS lookup*
  - *As a result of all the above, you understand that if someone managed to intervene in the world's DNS system to control responses, the Internet would go down*

< Go to Index

TARGETING MACHINES

Machines from different perspectives

*Icons by Bing Chat AI

Source: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

What are you going to find in this block?

- **In this block you will learn**
  - What is a machine **port** and what does it mean
  - What is and what does a **service** on a machine mean
  - What is a **protocol** and what does it mean
  - How the **nmap tool** can be used to see all the above
  - What is the basic security problem of a **public Wi-Fi** network

What is a machine from the outside?

- Once we reach a target machine, we have an **external** view of what it offers to the users
- It is comprised by
  - **Ports**, that have **services** that communicate with potential clients
  - Using certain **communication protocols**
    - Protocols are like the actions we can do in a social network
    - We can send messages in different formats: texts, images, memes, animated gifs, likes, retweets…
    - To communicate with others, social networks have a protocol of allowed message formats
    - This concept is no different to what happens with machines
- Let's review these concepts

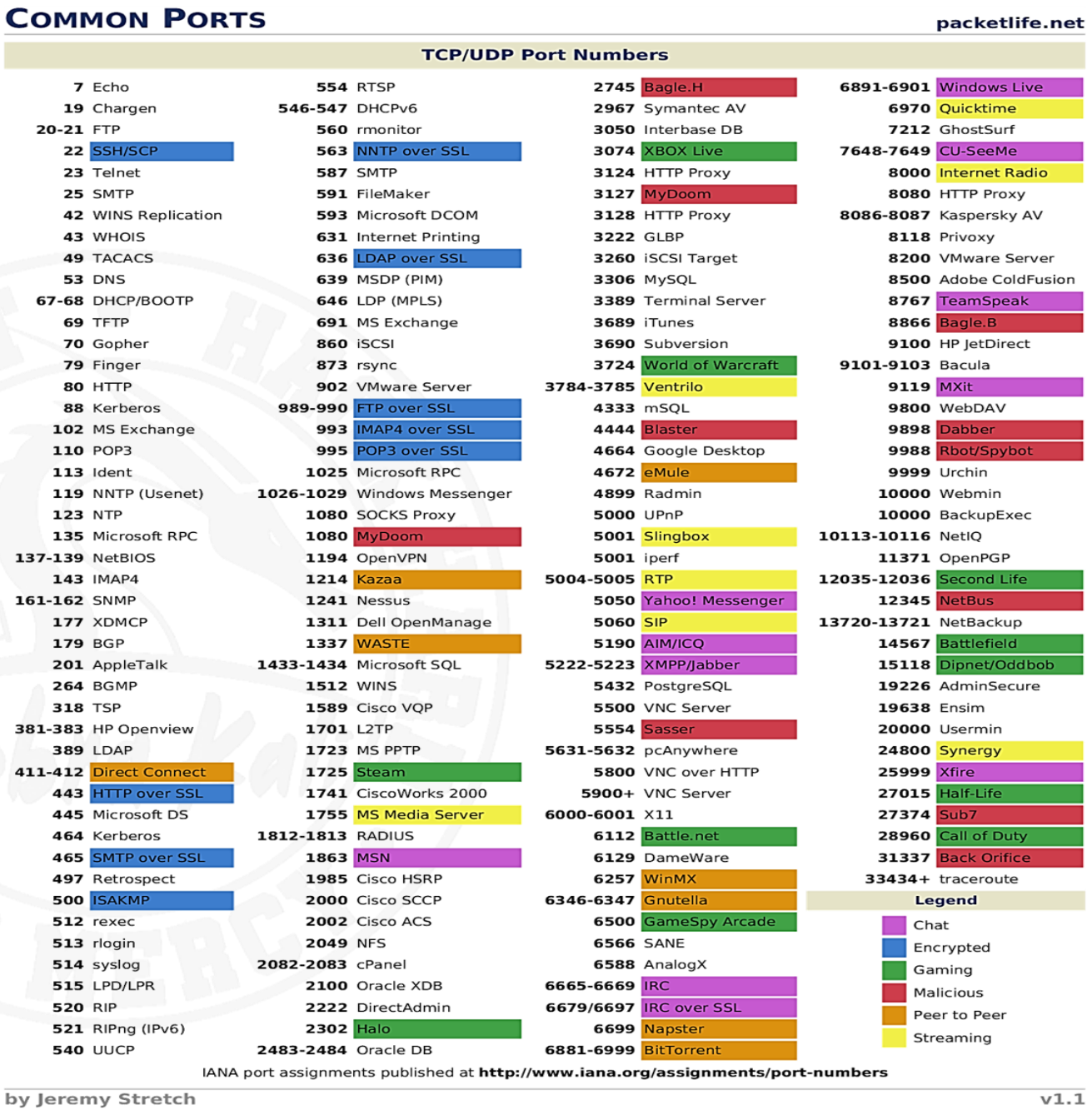
NETWORK PORTS

- **A port completes the access to a service offered by a machine**
  - The same machine can offer many services! (**one per port**)
  - The IP is the address of the machine to which we connect
  - The port marks **which service** (out of all that the machine offers) is used at that IP address
    - "I can get to the airport, but in the end, I'll have to choose which flight I'm going to catch" ☺
    - E.g., if our school's website is on the IP `156.35.94.1`
      - To browse it we need a proper client that connects to port `80` or `443` (HTTP(S) services)
    - And to connect securely as a user, use port 22 (**SSH service**)
- **There are 65,536 possible different ports on a machine**
  - The first 1,024 are generally referred to as "**common ports**", **reserved for typical known services**
    - The rest can be used to create programs that "listen" to connections and provide diverse services
  - The most used port numbers appear in the following slide
  - "**Opening a port**" means offering a service to external machines from yours
    - E. g..: Web server, Minecraft server…
  - **Opening ports under CG-NAT does not work! (beware!)**

About ports...

Computer Security

- **Ports higher than 1024 "usually" contain the services in the image**
  - But unlike reserved ones, it is not mandatory
  - Take this list with precaution!
- **Ports could be inspected using the `nmap` tool**
  - https://nmap.org/
  - It also allows us to know
    - What service is "behind" each port
    - If it is active (sends/receives requests)



Common Ports

packetlife.net

TCP/UDP Port Numbers

7	Echo	554	RTSP	2745	Bagle.H	6891-6901	Windows Live
19	Chargen	546-547	DHCPv6	2967	Symantec AV	6970	Quicktime
20-21	FTP	560	rmonitor	3050	Interbase DB	7212	GhostSurf
22	SSH/SCP	563	NNTP over SSL	3074	XBOX Live	7648-7649	CU-SeeMe
23	Telnet	587	SMTP	3124	HTTP Proxy	8000	Internet Radio
25	SMTP	591	FileMaker	3127	MyDoom	8080	HTTP Proxy
42	WINS Replication	593	Microsoft DCOM	3128	HTTP Proxy	8086-8087	Kaspersky AV
43	WHOIS	631	Internet Printing	3222	GLBP	8118	Privoxy
49	TACACS	636	LDAP over SSL	3260	iSCSI Target	8200	VMware Server
53	DNS	639	MSDP (PIM)	3306	MySQL	8500	Adobe ColdFusion
67-68	DHCP/BOOTP	646	LDP (MPLS)	3389	Terminal Server	8767	TeamSpeak
69	TFTP	691	MS Exchange	3689	iTunes	8866	Bagle.B
70	Gopher	860	iSCSI	3690	Subversion	9100	HP JetDirect
79	Finger	873	rsync	3724	World of Warcraft	9101-9103	Bacula
80	HTTP	902	VMware Server	3784-3785	Ventrilo	9119	MXit
88	Kerberos	989-990	FTP over SSL	4333	mSQL	9800	WebDAV
102	MS Exchange	993	IMAP4 over SSL	4444	Blaster	9898	Dabber
110	POP3	995	POP3 over SSL	4664	Google Desktop	9988	Rbot/Spybot
113	Ident	1025	Microsoft RPC	4672	eMule	9999	Urchin
119	NNTP (Usenet)	1026-1029	Windows Messenger	4899	Radmin	10000	Webmin
123	NTP	1080	SOCKS Proxy	5000	UPnP	10000	BackupExec
135	Microsoft RPC	1080	MyDoom	5001	Slingbox	10113-10116	NetIQ
137-139	NetBIOS	1194	OpenVPN	5001	iperf	11371	OpenPGP
143	IMAP4	1214	Kazaa	5004-5005	RTP	12035-12036	Second Life
161-162	SNMP	1241	Nessus	5050	Yahoo! Messenger	12345	NetBus
177	XDMCP	1311	Dell OpenManage	5060	SIP	13720-13721	NetBackup
179	BGP	1337	WASTE	5190	AIM/ICQ	14567	Battlefield
201	AppleTalk	1433-1434	Microsoft SQL	5222-5223	XMPP/Jabber	15118	Dipnet/Oddbob
264	BGMP	1512	WINS	5432	PostgreSQL	19226	AdminSecure
318	TSP	1589	Cisco VQP	5500	VNC Server	19638	Ensim
381-383	HP Openview	1701	L2TP	5554	Sasser	20000	Usermin
389	LDAP	1723	MS PPTP	5631-5632	pcAnywhere	24800	Synergy
411-412	Direct Connect	1725	Steam	5800	VNC over HTTP	25999	Xfire
443	HTTP over SSL	1741	CiscoWorks 2000	5900+	VNC Server	27015	Half-Life
445	Microsoft DS	1755	MS Media Server	6000-6001	X11	27374	Sub7
464	Kerberos	1812-1813	RADIUS	6112	Battle.net	28960	Call of Duty
465	SMTP over SSL	1863	MSN	6129	DameWare	31337	Back Orifice
497	Retrospect	1985	Cisco HSRP	6257	WinMX	33434+	traceroute
500	ISAKMP	2000	Cisco SCCP	6346-6347	Gnutella		
512	rexec	2002	Cisco ACS	6500	GameSpy Arcade		
513	rlogin	2049	NFS	6566	SANE		
514	syslog	2082-2083	cPanel	6588	AnalogX		
515	LPD/LPR	2100	Oracle XDB	6665-6669	IRC		
520	RIP	2222	DirectAdmin	6679/6697	IRC over SSL		
521	RIPng (IPv6)	2302	Halo	6699	Napster		
540	UUCP	2483-2484	Oracle DB	6881-6999	BitTorrent		

Legend

- Chat
- Encrypted
- Gaming
- Malicious
- Peer to Peer
- Streaming

IANA port assignments published at **http://www.iana.org/assignments/port-numbers**

by Jeremy Stretch v1.1

SERVICES

- **Programs that run associated with a network port**
  - They “listen” on it (to what? Request from clients in other machines, of year ☺)
  - They are processes, like the ones you saw in SO
- **These programs are run in the destination machine and wait for to incoming connections from clients**
  - When a client connects to them, and uses the appropriate communication protocol, the service processes the client request and sends a response
  - Or an error if the request is not valid
    - Or contains any kind of unexpected data / command…
- **This way, any machine can provide a service to other machines**
- **And this is the basis of machine communications nowadays! ☺**

COMMUNICATION PROTOCOL

- **System of rules that allow two or more entities of a communications system to transmit information (Ex.: TCP, UDP protocols)**
  - It defines the rules, syntax, semantics and synchronization of communication
  - And possible error recovery methods (remember FCR?)
- **Communication systems use well-defined formats to exchange messages**
  - Each message has an exact meaning, intended to elicit a response from a range of possible ones pre-determined for each situation
  - The specified behavior is typically independent of its implementation
    - Protocols are usually approved standards
- **To describe different aspects of a single communication, usually multiple protocols are needed**
  - A group of protocols designed to work together is known as a **protocol suite**
  - When implemented in software they are a **protocol stack**

NMAP FOR NETWORK RECONNAISSANCE

- Normally, this is the 1st step of a typical Pentesting / CTF operation: **Reconnaissance**
- Determines how many machines are "alive"
  - Able to receive traffic
  - This step does not necessarily identify ports / services yet
- Once done, each interesting machine is investigated further
  - This is the second step, **Enumeration** (**Topic 5**)

Nmap 7.80 Cheatsheet series (ingenieriainformatica.uniovi.es)

Part 1: Reconnaissance (Basic)

https://nmap.org/

GENERAL USAGE

nmap [Scan Type(s)] [Options] {target specification}

NOTES

Target specifications can be host names, IP addresses, ranges, networks, etc. (scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254)

Use these options to locate "alive machines" (sometimes only returns that, sometimes they also return some port / service information)

TARGET SPECIFICATION

-iL <inputfilename>: Input from from file a list of hosts/networks

-iR <num hosts>: Choose random targets

--exclude <host1[,host2][,host3],...>: Exclude hosts/networks

--excludefile <exclude_file>: Exclude list from file

RECONOISSANCE EXAMPLES

nmap -sn scanme.nmap.org

sudo nmap -PS22,80 scanme.nmap.org

sudo nmap --traceroute scanme.nmap.org

```
operario@kali:~$ nmap -sn 192.168.20.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-21 18:38 CEST
Nmap scan report for 192.168.20.10
Host is up (0.00085s latency).
Nmap done: 1 IP address (1 host up) scanned in 13.01 seconds
```

```
operario@kali:~$ sudo nmap -PS22,80 192.168.20.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-21 18:42 CEST
Nmap scan report for 192.168.20.10
Host is up (0.00012s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:67:7A:EF (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
```

HOST DISCOVERY OPTIONS (WAYS TO CHECK "ALIVE" MACHINES)

--dns-servers <serv1[,serv2],...>: Specify custom DNS servers

-n/-R: Never do DNS resolution/Always resolve [default: sometimes]

-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes

-Pn: Treat all provided hosts as online -- skip host discovery

-PO[protocol list]: IP Protocol Ping

-PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports

-sL: List Scan - simply list targets to scan

-sn: Ping Scan - disable port scan

--system-dns: Use OS's DNS resolver

--traceroute: Trace hop path to each host

PUTTING IT ALL TOGETHER...

- **Ports are communication endpoints**
  - Physical and wireless connections end at device ports
  - They identify a **process** or a network **service**
  - Multiplexing services in a single IP address
  - A port is always associated with an IP and the protocol of the communication
  - The most common protocols are **TCP** (Transmission Control Protocol) and **UDP** (User Datagram Protocol)
  - All three form the **destination or source network address** of a message
    - E.g.: `156.35.94.1:80/tcp` (typical web server)
  - Search engines such as Shodan or Censys do the same as `nmap` **with machines exposed on the Internet**

```
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2
f
Not shown: 972 filtered ports
PORT      STATE  SERVICE         VERSION
22/tcp    open   ssh             OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Lin
ux; protocol 2.0)
23/tcp    closed telnet
25/tcp    closed smtp
53/tcp    closed domain
80/tcp    open   http            Apache httpd 2.4.7 ((Ubuntu))
110/tcp   closed pop3
111/tcp   closed rpcbind
113/tcp   closed ident
135/tcp   closed msrpc
143/tcp   closed imap
199/tcp   closed smux
256/tcp   closed fw1-secureremote
554/tcp   closed rtsp
587/tcp   closed submission
993/tcp   closed imaps
995/tcp   closed pop3s
1025/tcp  closed NFS-or-IIS
1720/tcp  closed h323q931
3306/tcp  closed mysql
3389/tcp  closed ms-wbt-server
4446/tcp  closed n1-fwp
5900/tcp  closed vnc
8080/tcp  closed http-proxy
8090/tcp  closed opsmessaging
8888/tcp  closed sun-answerbook
9929/tcp  open   nping-echo       Nping echo
10617/tcp closed unknown
31337/tcp open   tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Mamma Mia!! This is not a Switch port!

- **Nintendo® recommended this to enable network play on Splatoon® and other games**
  - This means opening access in your router to all possible services to anybody
    - To the Switch® console IP address
    - Only for connections using the UDP protocol
  - All Switch® exposed services are visible from the outside!
- **What happens if this IP is assigned via DHCP? (typical case, btw…)**
  - Tomorrow another device may use it, and somebody may have access to all its services…
  - **It is a VERY BAD security advice!**

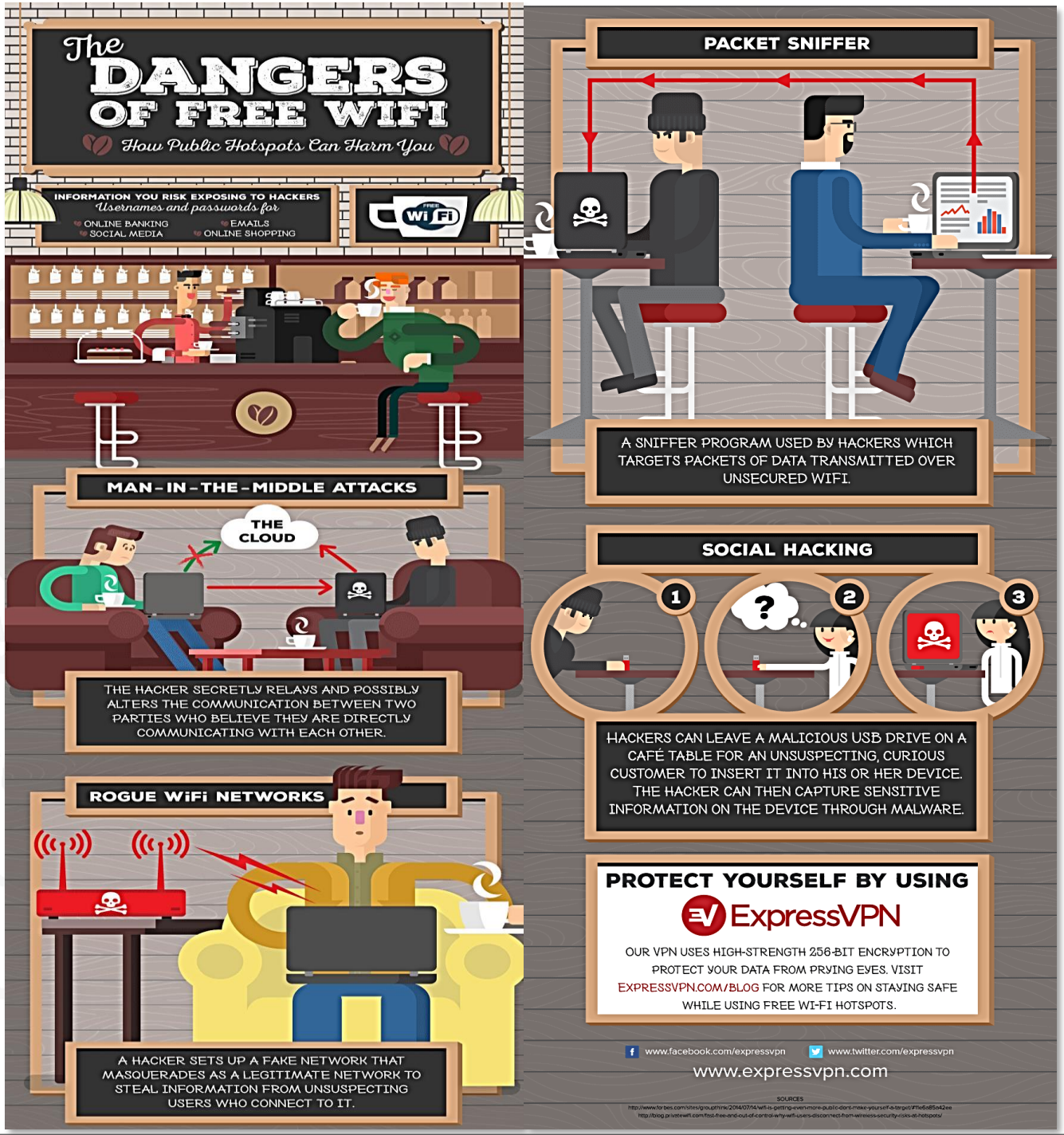
On a PC or smart device

1. Access your router's settings.
2. Locate the Port Forwarding settings. While the location will vary from router to router, it will typically be located in an area titled firewall, virtual server, security, or applications and gaming.
3. When asked for an application name, you can enter any word (Nintendo Switch, etc.)
4. Within the port range, enter the starting port and the ending port to forward. For the Nintendo Switch console, this is port **1 through 65535**.
5. Set the protocol as UDP.
6. Enter the IP address you assigned to the console.
7. Check Enable or Apply to turn on this rule.
8. Save the changes to the router.

What happens with Wi-Fi networks?

Computer Security

- **They are no different from wired networks in structure**
  - IPs, ports, services…
- **But they are exposed to more threats!**
  - Your data travels “free” in all directions in an open space
  - They could be picked up by anyone in the same Wi-Fi network
    - With a packet sniffer
    - To analyze, modify, or decrypt your traffic
  - Specially on free Wi-Fi networks!
    - **AVOID Free Wi-Fi at all costs**
    - Always use encrypted traffic (SSH, HTTPS) or VPNs (**Topic 5**)



Think you've understood it all? Evaluate yourself!

?

- **You can do the following**
  - *You know what a port means, the limit of ports a machine can have, and what it means to open one*
  - *You know how to distinguish between reserved and non-reserved ports*
  - *You understand the concept of service by "listening" on a machine*
  - *You understand the concept of protocol as strict rules that are established for communication between certain services*
  - *You understand how nmap allows you to see ports and services at work on a machine, as well as the protocols they use*
  - *You understand why a public Wi-Fi network is dangerous for your data*

< Go to Index

Targeting Users

Attacks that target humans

*Icons by Bing Chat AI

Source: Bing Chat AI

What are you going to find in this block?

- **In this block you will learn**
  - Why what you do while browsing, your tastes, your preferences, etc. (in short, your privacy) **are currency**
  - Which browsers are **most privacy-friendly**
  - What are the concepts of spam, phishing, hoax, watering hole, drive-by download, and APT
  - What is **OSINT** as a concept

PRIVACY

- **Users browsing history, behavior, physical and social characteristics, … are very interesting for ad companies**
  - And other companies that process these data for a profit
  - **If a service is "free", your data is the payment!**
- **The table shows user data collected by known services**
  - The only way to avoid this is to setup your browser with extensions that limit data acquisition techniques
  - Some tools (E. g.: Blacklight) give you an idea about **how prominent is this practice**

clario.

The companies that know most about you

#	Company	% of personal data collected	Email	Name	Age	Gender/Sex	Sexual Orientation	Marital Status	Race	Religious Belief	Live Location	Home Address	Employment Status	Job Title	Pet/Animal Ownership	Mobile Number	Landline Number	Type of Phone/Device	Hobbies	Interests	Height	Weight	Next of Kin	Mother's Maiden Name	Current Employers	Past Employers	Bank Account Details	Salary	Social Profile (Friends)	Social Profile (Hobies)	Social Profile (Interests)	Country of Birth	Allergies/Intolerances	Health & Lifestyle Info
1	Facebook	70.59%	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•		•	•				•	•	•			
2	Instagram	58.82%	•	•	•	•					•	•	•	•	•	•		•	•	•	•	•			•	•			•	•	•			
3	Tinder	55.88%	•	•	•	•	•	•			•		•	•	•	•		•	•	•	•						•		•	•	•			
4	Grindr	52.94%	•	•	•	•	•	•			•		•	•	•	•		•	•	•	•								•	•	•			
5	Uber	52.94%	•	•	•	•					•	•	•	•		•	•	•	•	•						•	•		•	•	•			
6	Strava	41.18%	•	•	•	•					•	•				•		•			•	•					•		•	•	•			
7	Tesco	38.24%	•	•	•	•		•				•				•	•	•									•		•	•	•			
8	Spotify	35.29%	•	•	•							•				•	•	•		•							•		•		•			
9	MyFitnessPal	35.29%	•	•	•							•				•	•	•				•	•				•					•		
10	Jet2	35.29%	•	•	•	•		•	•			•				•	•	•									•						•	
11	Credit Karma	32.35%	•	•	•									•	•	•		•				•	•				•	•						
12	Lidl Plus	32.35%	•	•	•						•	•			•	•	•	•									•						•	
13	Netflix	26.47%	•	•	•							•				•	•	•			•						•							
14	Nike	26.47%	•	•	•	•						•						•				•	•				•							
15	Asos	26.47%	•	•	•							•				•		•				•	•				•							
16	Depop	26.47%	•	•	•							•				•		•				•	•				•							
17	Ryanair	26.47%	•	•	•							•				•	•	•									•					•		
18	Ocado	26.47%	•	•	•							•				•	•	•									•						•	
19	Airbnb	26.47%	•	•	•	•						•			•	•		•									•							
20	American Airlines	26.47%	•	•	•							•				•	•	•									•					•		
21	Ikea	23.53%	•	•	•							•				•	•	•									•							
22	Trainline	23.53%	•	•	•						•	•				•		•									•							
23	Amazon	23.53%	•	•	•							•	•			•	•	•									•							
24	PayPal	23.53%	•	•	•							•				•		•							•		•							
25	eBay	23.53%	•	•	•							•				•	•	•									•							
26	Walmart	23.53%	•	•	•	•					•	•				•											•							
27	Deliveroo	20.59%	•	•							•	•				•	•										•						•	
28	Twitter	20.59%	•	•	•	•					•							•											•					
29	NHS COVID-19	20.59%	•	•	•						•	•						•																•
30	SlimmingWorld	20.59%		•	•	•												•				•	•											•
31	Google Maps	20.59%	•	•							•	•						•							•				•					
32	CVS Pharmacy	20.59%	•	•	•	•						•				•								•									
33	Amtrak	20.59%	•	•	•						•		•			•											•							
34	Sleepcycle	20.59%	•		•	•												•				•	•				•							
35	JustEat	17.65%	•	•								•						•									•						•	
36	Offerup	17.65%	•	•							•	•				•											•							
37	Doordash	17.65%	•	•							•	•				•											•							
38	McDonalds (USA)	14.71%	•	•							•					•											•							
39	TikTok	14.71%	•	•	•													•											•					
40	Protect Scotland	14.71%		•							•	•						•																•
41	CoStar	14.71%		•	•											•		•														•		
42	Bet365 USA	14.71%	•	•	•							•				•																		
43	Wetherspoon	14.71%	•	•							•							•									•							
44	Skybet	11.76%	•	•	•																						•							
45	Flo Period Tracker	11.76%	•		•													•																•
48	Whatsapp	11.76%	•	•												•		•																
47	Facetune	5.88%	•															•																
48	Pornhub	5.88%																•		•														

➢ Exercise **L2B4_PRIVACIDAD**

PRIVACY AND BROWSERS

Computer Security

- Browsers also collect user and navigation data while you use them
- This table shows different privacy tests
  - To help you choose the most adequate one if you are worried about these issues
- You don't need to understand the tests itself, just the amount that each browser passes

PrivacyTests.org News About

No. 3 — *Open-source tests of web browser privacy.* — *Updated 2021-11-02*

✓ = Passed privacy test ✗ = Failed privacy test – = No such feature

Desktop Browsers (click anywhere for more info)	Brave 1.31	Brave 1.31 Private	Brave 1.31 Tor	Chrome 95.0	Chrome 95.0 Private	Edge 95.0	Edge 95.0 Private	Firefox 93.0	Firefox 93.0 Private	Opera 80.0	Opera 80.0 Private	Safari 15.1	Safari 15.1 Private	Tor 10.5	Vivaldi 4.3	Vivaldi 4.3 Private
State Partitioning tests																
AltSvc	✗	✗	–	✗	✗	✗	✗	✓	✓	✗	✗	–	–	–	✗	✗
blob	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗
BroadcastChannel	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	✗	–	–	✓	✗	✗
CacheStorage	✓	✓	✓	✗	✓	✗	✗	✗	–	✗	✓	✓	✓	–	✗	✓
cookie	✓	✓	✓	✗	✓	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓
CSS cache	✓	✓	✗	✗	✗	✗	✗	✓	✓	✗	✓	✓	✓	✓	✓	✗
favicon cache	✓	✓	✓	✗	✓	✗	✓	✓	✓	✗	✓	✗	✗	✓	✗	✓
fetch cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
font cache	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✓	✓	✗	✗
H1 connection	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✓	✓	✗	✗
H2 connection	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✓	✓	✗	✗
H3 connection	✗	✗	–	✗	✗	✗	✗	✓	✓	✗	✗	–	–	–	✗	✗
HSTS cache	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	–	–	–	✗	✗
iframe cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
image cache	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✓	✓	✗	✗
indexedDB	✓	✓	✓	✗	✓	✗	✗	✗	–	✗	✓	✓	✓	–	✗	✓
localStorage	✓	✓	✓	✗	✓	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓
locks	✓	✓	✓	✗	✓	✗	✗	–	–	✗	✓	–	–	–	✗	✓
prefetch cache	✓	✓	✗	✗	✗	✗	✗	✓	✓	✗	✓	–	–	✓	✓	✗
ServiceWorker	✓	✓	✓	✗	✓	✗	✗	✗	–	✗	✓	✓	✓	–	✗	✓
SharedWorker	✓	✓	✓	✗	✓	✗	✗	✗	✓	✗	✓	–	–	✓	✗	✓
TLS Session ID	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Web SQL Database	✓	✓	✓	✗	✓	✗	✗	–	–	✗	✓	–	–	–	✗	✓
XMLHttpRequest cache	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Navigation tests																
document.referrer	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
sessionStorage	✓	✓	✓	✗	✓	✗	✗	✗	✓	✗	✓	✗	✗	✓	✗	✓
window.name	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✓	✗	✗	✗
HTTPS tests																
Insecure website	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Upgradable address	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
Upgradable hyperlink	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗
Upgradable image	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✗	✗	✗	✓	✓
Upgradable script	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

SPAM

- **Massively-sent fraudulent / unwanted email with multiple goals**
  - **Advertisement** sites of certain products not normally found in typical web stores, or related to illegal / alegal activities
  - **Scams** (Nigerian scam, fraudulent fundraises, mules, advance-fee scams…)
  - Spread **malware**
  - Spread **phising** campaigns
  - … *(many, many new forms of fraud appear constantly ☹)*
- **Apart from the email payload potential effects, they also might**
  - Saturate (and therefore perform a DoS) networks / email servers
    - E. g.: zip bombs, https://en.wikipedia.org/wiki/Zip_bomb
  - Initiate any type of scam or fraud (phishing)
- **Many times, accounts stolen by company data breaches are used to propagate spam campaigns more credibly**
  - The Have I been pwnd? service (https://haveibeenpwned.com/) allows you to **uncover these leaks**

PHISHING / SPEAR PHISHING

- **Messages (e-mail, Whatsapp, Telegram…) whose source appears to be legitimate (bank, company…) but are created with a malicious effect to fool users**
  - Steal user private information (logins, passwords, credit cards, email accounts…), run malware…
  - This information is key to commit many types of fraud later
  - Phishing attempts can also be typically found **during normal browsing** (malicious ads/scripts…)
    - A "**fortified browser**" may prevent many them (ad/script blocker, Google Safe Browsing, secure DNS…)
- **Spear phishing: Phishing attempts directed at specific individuals or companies**
  - Attackers often gather and use personal information about their target to increase success
  - E. g.: Threat Group-4127 (Fancy Bear APT group, Russia) used spear phishing tactics to target email accounts linked to Hillary Clinton's 2016 presidential campaign
- **Phishing is a type of fraud**
  - There are an enormous amount of fraud types, impossible to cover in this year
  - Our University offers a **free cyberfraud prevention course** that complements this one (in Spanish): https://uniovix.uniovi.es/course/view.php?id=62

HOAXES

- **Unwanted messages or publications with fake/biased information of various types**
  - Sent via emails, social networks (Twitter, Facebook…), instant messaging applications (WhatsApp, Telegram…), SMS…
  - Also present in some newspapers (intentional disinformation or **fake news**)
- **Mostly aiming to harvest active email accounts (those that are read)**
  - That are later targets of phising / spam attacks
  - They may also saturate the email system of a company
- **They are often used also to harm the reputation or public image of organizations / groups / individuals**
- **Websites like MalditoBulo (https://maldita.es/malditobulo/) can help us to discover some of them**

WATERING HOLE

- **Attack strategy in which the victim belongs to a concrete user group** (organization, industry, region…)
  - The attacker guesses or observes **which websites the group members often use**
  - Then targets them to **infect one or more of them with malware**
  - Eventually, some member of the targeted group becomes infected
  - And then, a **fully customized attack may be launched**
    - E. g.: hacks looking for specific information that may only attack users coming from specific IP addresses
    - Attacks are created considering all the information the attacker has about the members of the group
- **This makes these attacks harder to detect and investigate**
- **More information:** https://en.wikipedia.org/wiki/Watering_hole_attack

Drive-by download (aka Automatic downloads)

- Websites **that download and install spyware / malware without their user's consent** or **awareness**
  - Or with user's consent, but without understanding the consequences
- **This type of downloads can also happen when viewing a message attachment or clicking on a pop-up window**
  - The pop-up may display a fake error, warning or other misleading information
  - Once clicked, the download may initiate, and the attack can be unfolded
- **These attacks can be automatic, using existing web vulnerabilities**
  - Injecting a script that may request additional malicious scripts (with the actual exploits) to an attacker-controlled server
  - If the exploit succeeds, the malware may be executed
- More information: https://en.wikipedia.org/wiki/Drive-by_download

Advanced Persistent Threat (APT)

- **Stealth computer network threat actors** that gain unauthorized access to a network, and **remains undetected for an extended period**
  - The goal is to place custom malicious code on multiple computers for specific tasks
  - The more time they remain, the more damage / information stolen
- **They are typically a nation state or state-sponsored group (espionage)**
  - May also refer to other groups conducting large-scale targeted intrusions
- **Motivations are typically political or economic**
  - **Every major business sector** (government, defense, financial services, legal services, industrial, telecoms…) has recorded instances of attacks by APTs
  - With specific goals, seeking to steal, spy, or disrupt
- **Some utilize "traditional" vectors**
  - Social engineering (OSINT), human intelligence (HUMINT)…to access physical locations that enable network attacks

OSINT

- **Open-Source INTelligence** (OSINT) is the set of data collected from public sources to be used in the study of a target
- According to the U.S. Department of Defense

  "Publicly available information that is collected, exploited, and distributed on a predetermined basis to an appropriate audience, with the intention of meeting a specific research requirement "
- Therefore, it is a **legally accessible** set of public information
  - That can be used to find out certain data, routines, structures, etc. of a given collective / person / company
- There are specialized OSINT tools for every data source
  - https://ciberpatrulla.com/links/
- You will gain more OSINT experience thanks to…
  - The **Seminar 1**
  - The **Group works** of this course

OSINT

- It is used for national security, police, business / market research
- Sources of information can be divided into six categories
  1. **Media**: printed newspapers, magazines, radio and TV from one or more countries
  2. **Internet**: Online publications, **documents** (and its **metadata**), blogs, forums, and electronic means associated with specific citizens such as telephones or user-created content
     - Also includes Youtube and **social networks** and every previously published material (Wayback Machine)
     - It is the main source: search engines can be weaponized to Access sensitive data (Google Hacking)
  3. **Government public data**: reports, invoices, phone directories, press magazines, talks…
  4. **Professional and academic publications**: journals, conferences, symposia, academic articles, thesis, projects...
  5. **Commercial data**: financial and/or industrial studies, databases, images…
  6. **Other works**: technical reports, preprints, patents, articles in process, business documents, unpublished articles, newsletters…

➢ Exercises **L2B1_ROBOTS**, **L2B1_METADATOS**, **L2B2_GHACK**, **L2B2_WAYBACK**

Think you've understood it all? Evaluate yourself!

?

- **You can do the following**
  - *Understand that if a service is free, your data is the payment*
    - *And that data is used to show you ads that are more relevant to your tastes (supposedly)*
    - *And that, of course, this is a very lucrative way of financing for companies*
  - *Understand that even if your service isn't free, they could still be getting your data for profit*
  - *You understand what spam is, in general*
  - *You know how to distinguish phishing from spear phishing*
  - *You know what a hoax is and what it can be used for*
  - *Do you know what a watering hole is, and why it is considered a targeted attack on a collective*
  - *You know what a drive-by download is, and why they are dangerous*
  - *You know what an APT is, and usually what kind of intentions they have*
  - *You understand what OSINT is and how, thanks to it, everything that anyone publishes on Internet can be used against them in some way*

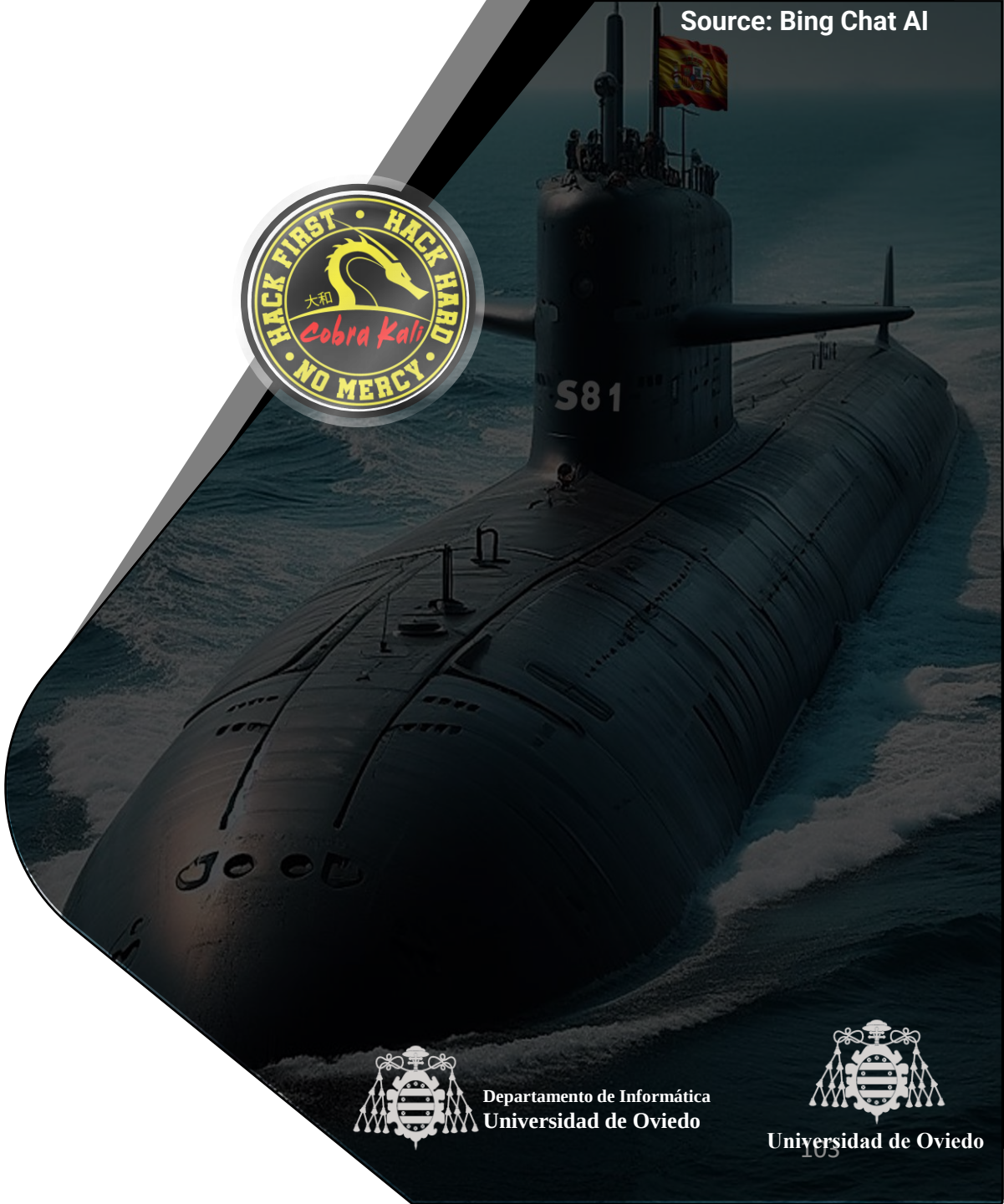
< Go to Index

And now...What's next?

Course organization

*Icons by Bing Chat AI

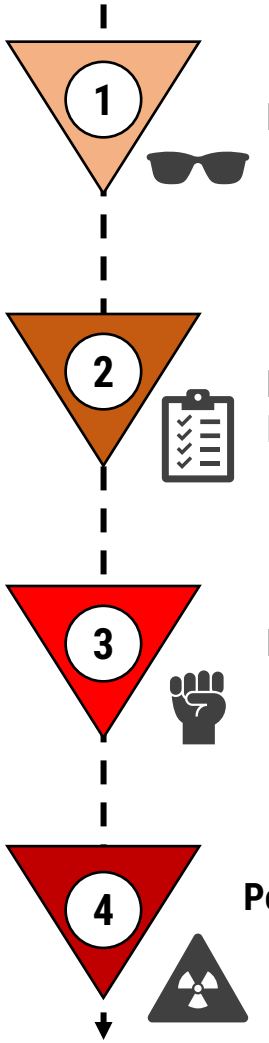
Source: Bing Chat AI



Defenses against the dark arts...

Computer Security

The "Cyber Kill Chain"



Reconnaissance

The observation stage: attackers typically assess the situation from the outside-in, to identify both targets and tactics for the attack

Enumeration / Intrusion

Based on what the attackers discovered in the reconnaissance phase, they're able to get into your systems: often leveraging malware or security vulnerabilities

Exploitation

Exploiting vulnerabilities and delivering malicious code onto the system, to get a better foothold

Post-Exploitation

- Privilege Escalation
- Lateral Movement
- Obfuscation / Anti-forensics
- Denial of Service
- Data Exfiltration
- Port scanning
- Pivoting
- Persistence

Malicious actions performed on exploited system to increase attack effects or do maximum damage

Attack	Defense
Topic 1	Topic 5
Topic 5	Topic 3 Topic 4 Topic 5
Topic 7	Topic 2 Topic 3 Topic 4 Topic 6
Topic 7	Topic 3 Topic 4

OSI LAYER	ACTIVITY	ATTACK VECTOR
7 APPLICATION LAYER	▪ User Interface and Software Application ▪ Web Browsing, Email Communication, File Transfer ▪ Protocols Like HTTP, SMTP, FTP	❶ Malware Injection ❷ Phishing Attacks ❸ Application-Level DDoS attacks
6 PRESENTATION LAYER	▪ Data Encryption & Decryption ▪ Data Compression & Expansion ▪ Viewing Compressed Files	❶ Data Encoding/Decoding Vulnerabilities ❷ Malicious Code Injection ❸ Format String attacks
5 SESSION LAYER	▪ Establishes, Manages and Terminates Connections ▪ Manages Session State ▪ Video Conferencing	❶ Session Hijacking ❷ Brute Force attacks ❸ Session fixation attacks
4 TRANSPORT LAYER	▪ Ensures end-to-end data delivery ▪ TCP and UDP Protocols ▪ Error Correction	❶ Man-in-the-middle attacks ❷ SYN/ACK Flooding ❸ TCP/IP Vulnerabilities
3 NETWORK LAYER	▪ Routing and Addressing ▪ IPV4, IPV6 and Routing Protocols [Example: OSPF] ▪ Subnet Configuration	❶ IP Spoofing ❷ Routing Table Manipulation ❸ DDoS Attack
2 DATA LINK LAYER	▪ Frames and error detection/correction ▪ Ethernet, WI-FI and bridging	❶ MAC address spoofing ❷ ARP Spoofing ❸ VLAN Hopping
1 PHYSICAL LAYER	▪ Physical medium and electrical/Optical Signaling ▪ Ethernet Cables, Fiber optics, etc., ▪ Radio waves in wireless links	❶ Physical Tampering ❷ Wiretapping ❸ Electromagnetic Interference

Ethical Hackers Academy.

Source: PowerPoint icons

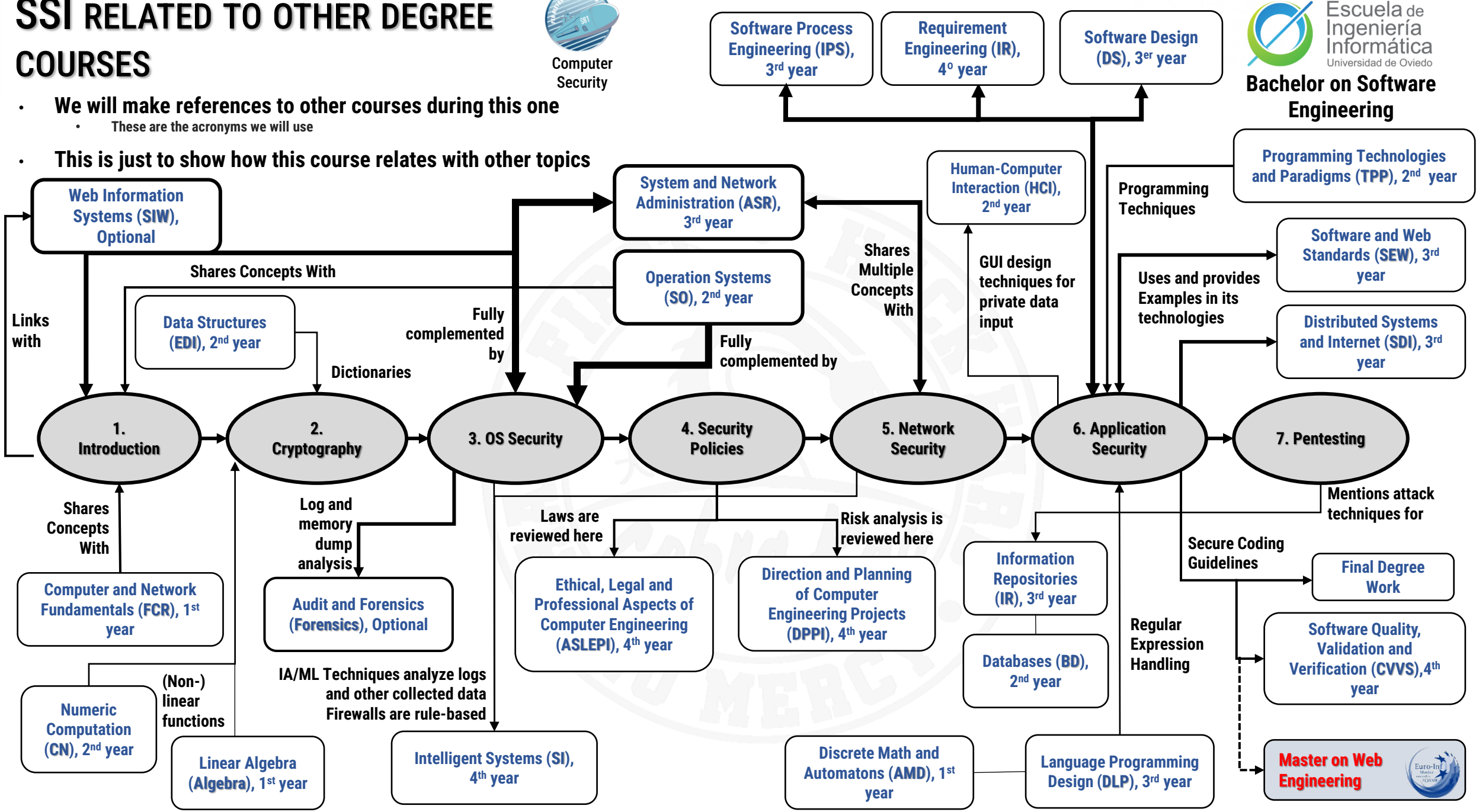
SSI RELATED TO OTHER DEGREE COURSES

Computer Security

- We will make references to other courses during this one
  - These are the acronyms we will use
- This is just to show how this course relates with other topics

Escuela de Ingeniería Informática
Universidad de Oviedo

Bachelor on Software Engineering



TOPIC 1: INTRODUCTION