

TOPIC 1: INTRODUCTION

“This world doesn’t need a hero; it
needs a professional”



JOSÉ MANUEL REDONDO LÓPEZ “S-81 ISAAC PERAL” PROJECT V3.0



Departamento de Informática
Universidad de Oviedo



Universidad de Oviedo

Logo: @creative_vanesa (Instagram)



INDEX

- ▶ **Ethical code**
- ▶ **Introduction**
- ▶ **Basic terminology**
 - Malware types
- ▶ **Networking basics**
 - Machine Networks
 - DNS
- ▶ **Machines as targets**
 - From an internal point of view
- ▶ **Users as targets**
- ▶ **What's next? Course organization**

[< Go to Index](#)

ETHICAL CODE

Hackers are NOT criminals, hence you must abide to an 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**

- **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 are using (no DoS...) (it is your legal "playground")
 - By the **capacity** (resources) of your infrastructure (it is your legal private "playground")

- **Some of these techniques are purely for intrusion**
 - Web shells, privilege escalation, 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! 😊



INTRODUCTION: LEARNING GOALS



José Manuel
Redondo López

- Know different **concepts** related to computer systems security
- Identify the **risks** that may compromise the security of a computer system
- Know the **vulnerabilities, threats, attack techniques** and other things involved in computer systems security
- Identify different types of **damages** that may be caused to a computer system

- **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

● 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 course 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 course ([IFA](#)) deals with this
- Will only mention risk management
 - The Project Management course (4th year) ([DPPI](#)) will deal with this
- Will only mention law-related topics
 - The Social, Legal, Ethical and Professional Aspects of C. Eng. ([ASLEPI](#)) course (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**



José Manuel
Redondo López

- **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 escalation**

ATTACKS AGAINST **INTEGRITY**



José Manuel
Redondo López

- **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)

- **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!



José Manuel
Redondo López

- 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
- 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/>

What can happen to your data?

Data can be stolen

Impact on the confidentiality of your data

- Exploiting stolen data and selling it on the black market
- Using stolen data to gain unauthorized access to organizations
- Using stolen data for blackmail—organizational or individual—to manipulate your organization's decision making process
- Conducting espionage to steal confidential data and intellectual property, which can result in a hit to stock value or ruin an organization's reputation

Data can be corrupted

Impact on the integrity of your data

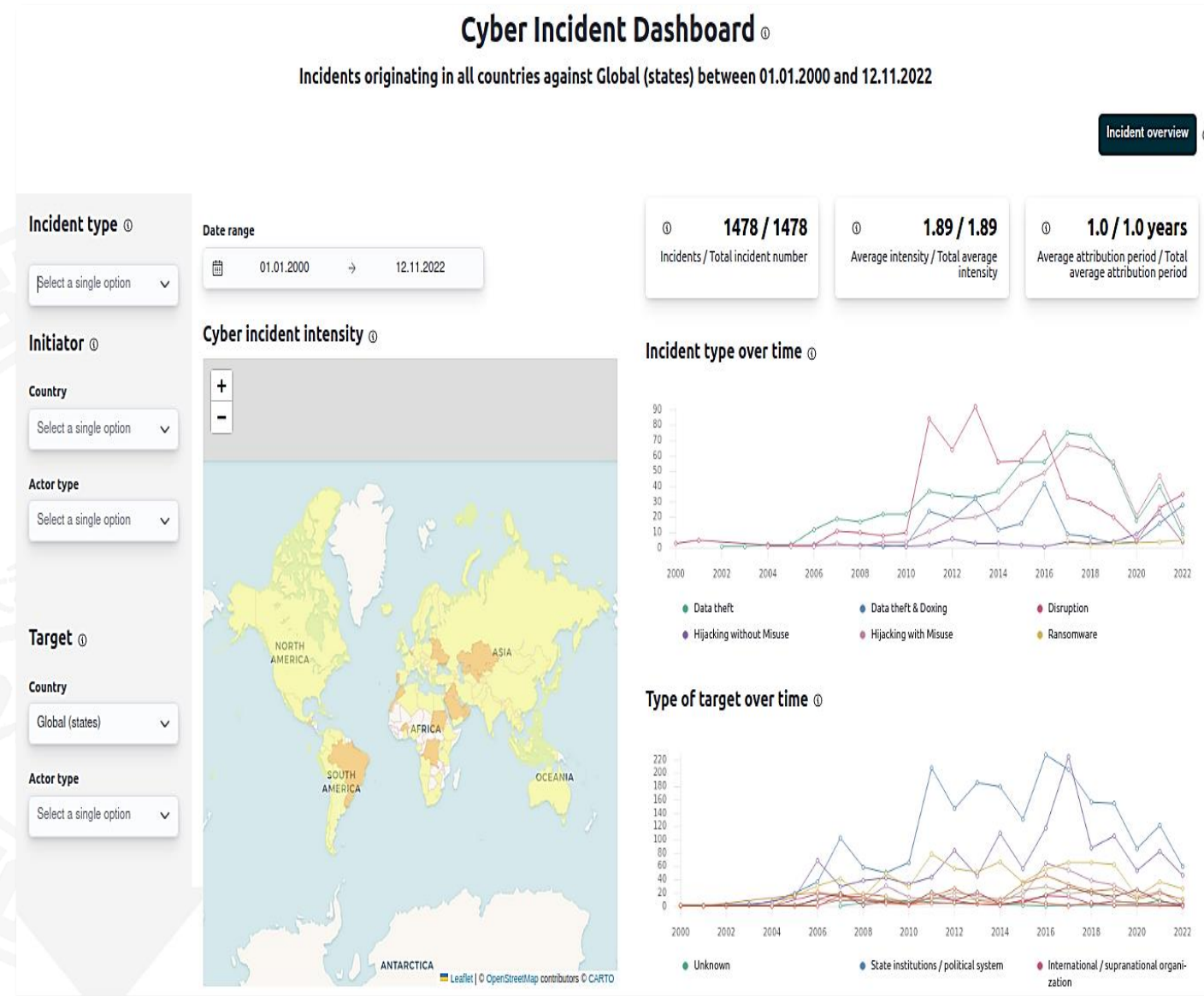
- Carrying out fraudulent transactions
- Altering and deleting data in transit by unauthorized entities
- Accidental alteration or deletion of data by authorized users

Data can be destroyed or locked down

Impact on the availability of your data

- Physical destruction of data or the systems holding the data
- Ransomware attacks that lock down your system have become a common method of attack among threat actors
- Denial of service (DOS/DDOS) attacks prevent your organization from carrying out business operations

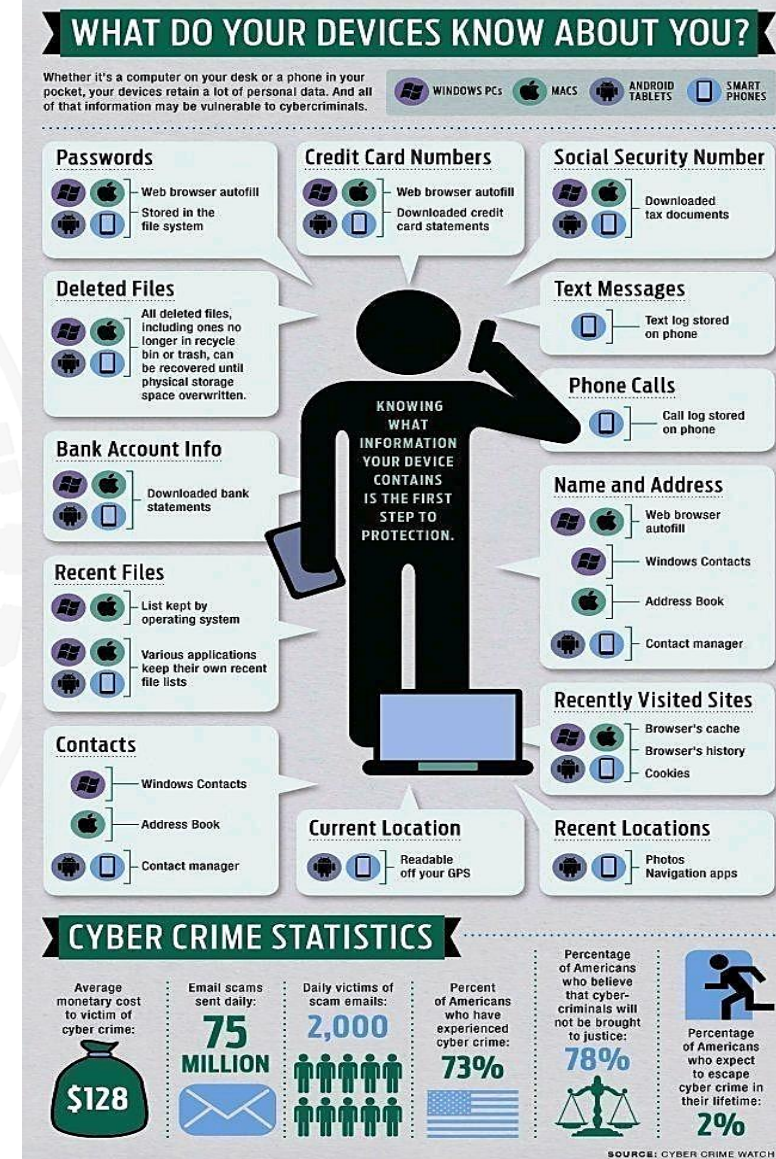
- **Cybersecurity-related profiles are in high demand**
 - <https://cso.computerworld.es/ciberseguridad/cuales-son-los-perfiles-mas-buscados-en-los-departamentos-de-seguridad>
- **Because attacks are constant, and worldwide**
 - <https://cybermap.kaspersky.com/>
 - Examples are in the news daily...
-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



Source: <https://m.facebook.com/compotechcyber/posts/>

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

- 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



THE WORLD OF SECURITY FROM A BEGINNER PERSPECTIVE



José Manuel
Redondo López

- 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](#)

[Malware types >](#)

BASIC TERMINOLOGY

Understanding basic concepts and “buzzwords” 😊



- **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)
 - 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...

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

- **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

[illegible]

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 switch 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 necessarily reflect when the entry was updated in CVE.
Phase (Legacy)	
Assigned (20200210)	

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

- **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...

- **(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

BASIC TERMINOLOGY: TYPES OR ATTACKERS (OR “ADVERSARIES”)



José Manuel
Redondo López

● **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**: Revenge, political revindication, display of technical knowledge...
- **Economical**: Private data theft or exfiltration, stealing industrial secrets, money...
- **Political**: Alter the outcome of electoral processes
- **Terrorism**: Paralyze, disrupt or disable government or company infrastructures
 - To cause fear or harm the society
- ... *(even “for the lulz”, using a twisted sense of humor)*

BASIC TERMINOLOGY: SECURITY TEAMS



José Manuel
Redondo López

- **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/>

Malware types

Types of programs created to harm you



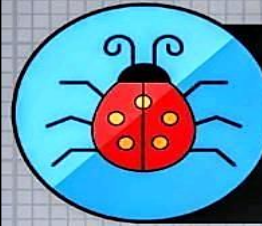
MALWARE (MALICIOUS SOFTWARE)



José Manuel
Redondo López

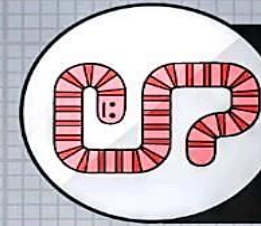
- **Software aiming to gain unauthorized access**
 - Or cause any kind of harm in computer systems
 - Also known as **malicious code**
- **Some common effects are**
 - **Cause failures:** Virus, worms, trojans...
 - **Steal personal / private information:** Spyware, Keyloggers, Stealers...
 - **Distributed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

Types of Malware



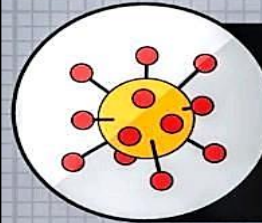
BUGS

A type of error, flaw or failure that produces an undesirable or unexpected result. Bugs typically exist in a website's source code and can cause a wide range of damage.



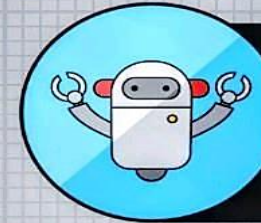
WORMS

A worm relies on security failures to replicate and spread itself to other computers. They are often hidden in attachments and will consume bandwidth and overload a web server.



VIRUS

A piece of code that is loaded onto your website or computer without your knowledge. It can easily multiply and be transmitted as an attachment or file.



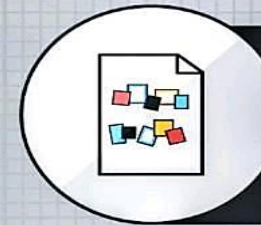
BOTS

A software program created to perform specific tasks. Bots can send spam or be used in a DDoS attack to bring down an entire website.



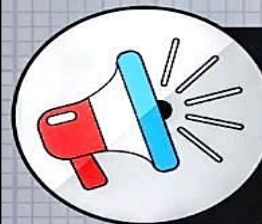
TROJAN HORSES

Much like the myth, a Trojan disguises itself as a normal file and tricks users into downloading it, consequently installing malware.



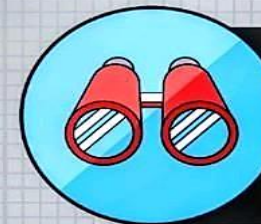
RANSOMWARE

Ransomware denies access to your files and demands payment through Bitcoin in order for access to be granted again.



ADWARE

A type of malware that automatically displays unwanted advertisements. Clicking on one of these ads could redirect you to a malicious site.



SPYWARE

A type of malware that functions by spying on a user's activity. This type of spying includes monitoring a user's activity, keystrokes and more.

Source:

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



How does an Antivirus works?

by @SecurityGuill



Signature-Based Detection



- This is the oldest and **most used** method.
- This method consists in analyzing the hard disk, looking for the **signature of the malware**, which is present in the **database** of the software, if knows this malware.
- The signature is a **piece of code** or a **string** of the malware that **identifies it**. Each malware has its **own signature**, which must be known to the antivirus.
- This method is **not effective against new malware** or so-called **polymorphic malware**, whose signature changes with **each replication**.

Behavioural-Based Detection



- This concentrates more in analysing the **behaviour** of the program and determining whether it is likely **malicious** in purpose.
- This mechanism detects malware only while the malware performs **malware actions**.
- For example if the program **attempts to disable security controls** that can be an indicator that it is likely malicious. If the antivirus program witnesses an attempt to **change or modify a file** or **communicate over the Web**, it may **take action** and **warn you** of the threat. It may also **block** the threat depending on how you adjust its **security settings**.

Heuristic-Based Analysis



- Heuristic analysis is a method of detecting malware by **examining code for suspicious properties**.
- Heuristic analysis can employ a number of different techniques.
- One method, known as **static analysis**, involves **decompiling** a suspect program & **examining its source code**. This code is then **compared to malware that are already known**. If a particular percentage of the source code matches anything in the heuristic database, the code is **flagged as a possible threat**.
- Another method is known as **dynamic analysis**. It **isolates** the suspicious program or piece of code inside a specialized **virtual machine/sandbox**. It examines each command as the malware activated & looks for any **suspicious behaviors**, such as self-replication, overwriting files, etc..



Follow @SecurityGuill on Twitter for more about Infosec / Cybersecurity

MALWARE EVASION TECHNIQUES



José Manuel
Redondo López

- **Fingerprinting its environment when run**
 - E. g.: do not run if inside a VM
- **Confusing the detection methods of security tools**
 - Avoiding detection by technologies like signature-based antivirus software, etc.
- **Timing-based evasion**
 - Running at certain times or following certain actions
 - E. g.: executes only during certain vulnerable periods (e. g. the boot process)
- **Obfuscating internal data**
 - So that automated tools can not detect it as malware
 - **Droppers**: the actual malicious code is downloaded (in one or more parts) when a program is run
 - It is a mere downloader (+ executor of the downloaded software), with no other harmful effects
- **Using stolen certificates of reputable sources**
 - To disable anti-malware and virus protection that check the origin of the files
- **Information hiding techniques (stegomalware)**

MALWARE BY EFFECT: CAUSE SYSTEM FAILURE. PROPAGATORS



José Manuel
Redondo López

● 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 are long-running software (system services) or modified/fake versions of popular 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



José Manuel
Redondo López

- **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



What is a Fork Bomb ?

by @Guillaume_Lpl

• The most common form of the fork bomb is:

```
:(){:|:&};;
```

• In a more explicit form:

```
:(){  
:|:&  
};  
:
```

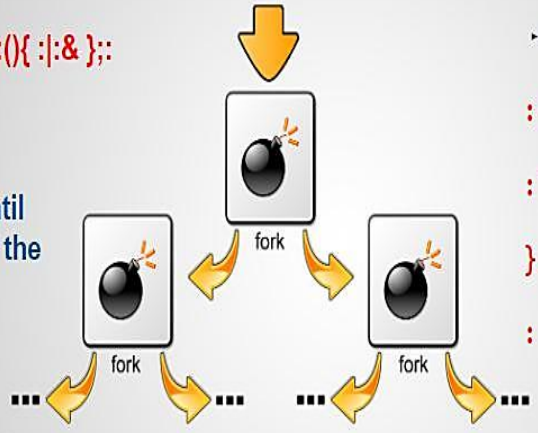
• The principle of a "Fork Bomb" is to **multiply a process until reaching the limits of the system**.

• The multiplication of processes **saturates the system** and quickly **consumes all available resources**.

• The set leads to a **system freeze** and / or a **denial of service**. (DoS)

• One simple way to **protect your system** is to **set limits on the number of processes that users can instantiate**, "max user processes", via the "**ulimit**" function.

• The maximum number of processes of a user can be **queried directly via the "-u" option of "ulimit"**



Follow @Guillaume_Lpl on Twitter for more things about Infosec

MALWARE BY EFFECT: CAUSE SYSTEM FAILURE. TROJAN



José Manuel
Redondo López

- **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**

● 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)

● 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



José Manuel
Redondo López

- **Block computer usage and/or its data**

- By taking full control of their functions/files and **ask for a ransom** to recover it back

- **The usually come in different variants**

- **Screen lockers**: user cannot login until a ransom is paid (e. g.: police scam)
- **Cryptolockers**: important user files are encrypted and irrecoverable without a decryption key
 - That must be bought paying a ransom

- **Pay instructions are shown when infection is completed**

- Not when first infecting the computer
- 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/infections...
- 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



- **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

- **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**

- **Term that designates 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"

- **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**



What is a Bug Bounty ?

by @Guillaume_Lpl

What is it?

- A **bug bounty program** is a deal offered by many **websistes**, **organizations** & **software developers** by which individuals can receive **recognition** & **compensation** for **reporting bugs**, especially those pertaining to **exploits** and **vulnerabilities**.



- These programs allow the developers to **discover** and **resolve bugs** before the general public is aware of them.

- A large numbers of organizations have set up a bug bounty program : **Mozilla**, **Facebook**, **Google**, **Microsoft**, **Reddit**, & more...



Advantages of a Bug Bounty Program

- **Continuous Testing**: Each change you make to configuration and each software patch you apply will inherently make your **security posture different from the last pentest** that was performed. Bug bounties are typically open for **continuous testing**.

This means that **pentesters are constantly evaluating your network/app/website**.



- **"More eyes than you could ever pay"**: 1000s of penetration testers evaluating your products, and you **only pay the ones who find bugs**.



- **Breach are expensive to recover from**. Sometimes it's better to set up a bug bounty program, especially if your product is **collecting data** or **impacting your production**.



Some Bug Bounty Platforms



hackerone

• HackerOne



bugcrowd

• BugCrowd

YES WE H/CK

• YesWeHack



Synack

• Synack



safehats

• SafeHats



Follow @Guillaume_Lpl on Twitter for more about Infosec / Cybersecurity

CONCEPTS, CONCEPTS, CONCEPTS...



José Manuel
Redondo López

- There are way more concepts, but don't get overwhelmed...enough for now! 😊

Source: <https://www.govloop.com/your-cybersecurity-cheat-sheet-2/>



NCSC Glossary

This glossary explains some common words and phrases relating to cyber security, originally published via the @NCSC Twitter channel throughout December. The NCSC is working to demystify the jargon used within the cyber industry. For an up-to-date list, please visit www.ncsc.gov.uk/glossary.

Antivirus



Software that is designed to detect, stop and remove viruses and other kinds of malicious software.

Botnet



A network of infected devices, connected to the Internet, used to commit co-ordinated cyber attacks without their owners' knowledge.

Bring your own device (BYOD)



An organisation's strategy or policy that allows employees to use their own personal devices for work purposes.

Cloud



Where shared compute and storage resources are accessed as a service (usually online), instead of hosted locally on physical services.

Cyber attack



Malicious attempts to damage, disrupt or gain unauthorised access to computer systems, networks or devices, via cyber means.

Cyber security



The protection of devices, services and networks - and the information on them - from theft or damage.

Denial of Service (DoS)



When legitimate users are denied access to computer services (or resources), usually by overloading the service with requests.

Digital footprint



A 'footprint' of digital information that a user's online activity leaves behind.

Encryption



A mathematical function that protects information by making it unreadable by everyone except those with the key to decode it.

End user device



Collective term to describe modern smartphones, laptops and tablets that connect to an organisation's network.

Firewall



Hardware or software which uses a defined rule set to constrain network traffic to prevent unauthorised access to (or from) a network.

Internet of Things (IoT)



Refers to the ability of everyday objects (rather than computers and devices) to connect to the Internet. Examples include kettles, fridges and televisions.

Macro



A small program that can automate tasks in applications (such as Microsoft Office) which attackers can use to gain access to (or harm) a system.

Patching



Applying updates to firmware or software to improve security and/or enhance functionality.

Phishing



Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.

Ransomware



Malicious software that makes data or systems unusable until the victim makes a payment.

Software as a Service (SaaS)



Describes a business model where consumers access centrally-hosted software applications over the Internet.

Social engineering



Manipulating people into carrying out specific actions, or divulging information, that's of use to an attacker.

Spear-phishing



A more targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts.

Trojan



A type of malware or virus disguised as legitimate software, that is used to hack into the victim's computer.

Two-factor authentication (2FA)



The use of two different components to verify a user's claimed identity. Also known as multi-factor authentication.

Water-holing (watering hole attack)



Setting up a fake website (or compromising a real one) in order to exploit visiting users.

Whaling



Highly targeted phishing attacks (masquerading as legitimate emails) that are aimed at senior executives.

Whitelisting



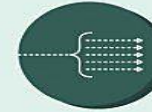
Authorising approved applications for use within organisations in order to protect systems from potentially harmful applications.

types of CYBERATTACKS



MALWARE

Malicious computer code used to corrupt, destroy, or steal digital information. Malware includes viruses and worms, in addition to spyware that monitors user activity and ransomware that holds data hostage.



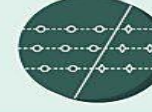
DISTRIBUTED DENIAL OF SERVICE (DDoS)

An interruption of network service, executed by sending such high volumes of traffic or data to a single network that it becomes overloaded and inoperable.



ADVANCED PERSISTENT THREAT

A continuous, sophisticated hacking process that allows an individual to enter and occupy a network for an extended amount of time in order to monitor or extract data from the target.



STRUCTURED QUERY LANGUAGE INJECTION

An attack that alters a database search in a web-based application, allowing a hacker to obtain unauthorized access to sensitive information in a database.



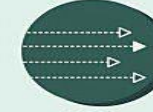
APPLICATION-LAYER ATTACK

An attack that causes fault in a server's operating system or applications, allowing an attack to bypass normal access controls to gain increased access to a system.



INSIDER THREAT

Employee use of government personnel, facilities, information, equipment, networks or system to inflict harm on the United States. Insider threats can take many forms, from releasing confidential information to deploying advanced malware from within a network firewall.



PHISHING

An attempt to extract sensitive information from an individual by masquerading as a trusted entity or person, usually via email or websites.



SPAM

Messages sent or posted online that contain irrelevant, unsolicited, and often misleading information.

types of HACKERS



INADVERTENT INSIDERS

Employees or contractors for an organization who compromise agency security through unintentional misuse of cyber systems.



MALICIOUS INSIDERS

Employees or contractors of an organization who intentionally expose government information, systems, or personnel to external individuals.



HACKTIVISTS

Hackers motivated by political, religious, or personal beliefs to expose or deface cyber networks of perceived opponents.



CYBER CRIMINALS

Professional hackers who use malware, phishing, and other tactics for illegal monetary gain.



STATE OPERATIVES

Hackers employed by a nation-state to inflict military or financial harm on other nation-states via cyber networks.



TROLLS

Individuals who target websites, social media accounts, systems, or other online portals without damaging or exposing information for the sake of receiving recognition or expressing malice.



WHITE HAT HACKERS

Individuals who expose weaknesses in cyber systems for their private or public sector employers in order to remedy vulnerabilities before external hackers attack.

CONCEPTS, CONCEPTS, CONCEPTS...



José Manuel
Redondo López

- In any case, having a glossary of terms at your disposal for future use is nice
- You can always return to it when you find a term you are not familiar with!
- These glossaries will become less useful the more experience you gain in this field!

 **101 Blockchains** | **CYBER SECURITY THREATS**

DIFFERENT KINDS OF CYBER SECURITY THREATS

 BRING YOUR OWN DEVICE (BYOD) POLICIES Using personal devices infected with a virus at work can easily compromise the organization's network as well.	 SHADOW IT SYSTEMS Usually, these IT systems aren't compatible with an organization's central IT system. As a result, data loss and security threat keep rising.	 FLAWS IN INTERNET OF THINGS (IIOT) Devices connected through a flawed Internet of Things is more to security issues.	 INSIDE MAN Bad players within an organization can easily breach security because of easy access.
 DDOS The distributed denial-of-service attack floods the organization's network with traffic and ultimately shuts it down.	 MALWARE ATTACK Malicious software programs can get ahold of your sensitive information without you even noticing.	 CRYPTO-MALWARE This malware get access to your computer's processing power and use it to mine cryptocurrencies.	 PHISHING EMAIL Phishing emails contain the trojan horse or ransomware viruses. 97% of the people can't tell the difference and open it, releasing the virus.
 DATA BREACH Many use obsolete data storage networks that are prone to data breaches.	 INSECURE APPLICATION USER INTERFACE (API) The lack of proper security measures in the Application User Interface can cause security breaches.	 CLOUD ABUSE Most of the cloud storage can be accessed by hacking the Virtual Machine.	 SINGLE FACTOR PASSWORDS Using only a single factor password isn't enough to offer full security in 2019 because they are easy to crack.
 FILELESS MALWARE This malware don't exist as a file in the hard drive and work in the background.	 STEGWARE Stegware are malicious files hidden within another file, such as video, image, messages, etc.	 ZERO-DAY THREATS Most of the programs come with security holes, and cybercriminals find this security lopes and use it.	 WHALING It's a form of phishing attack where the attacker convinces to be reliable but later abuses the data.

CREATED BY 101BLOCKCHAINS.COM

- 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!**

[< Go to Index](#)

[Machine networks >](#)

[DNS >](#)

NETWORKING BASICS: HOW TO REACH TARGET MACHINES

You can't hack what you can't see!



HOW MACHINES COMMUNICATE AMONG EACH OTHER?



José Manuel
Redondo López

- **When we want to communicate with other users in social networks...**
 - We locate these users and send a message to them
 - Then, the other 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 between them!**
 - And trust me, nowadays **there are a LOT** of different machines communicating between them!



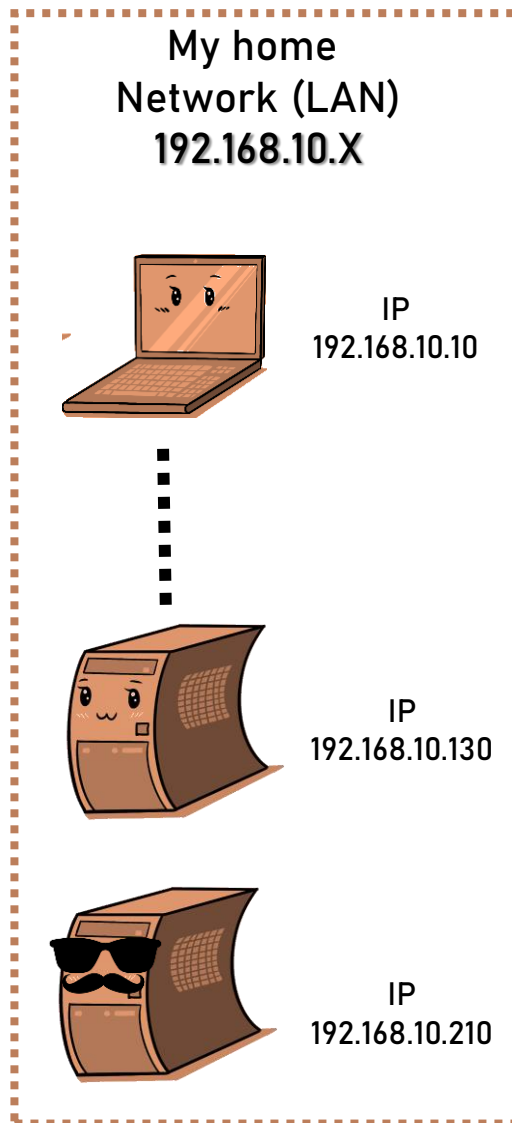
Source: <https://formatalent.com/cursos-de-m2m-machine-to-machine>

HOW MACHINES COMMUNICATE AMONG EACH OTHER?

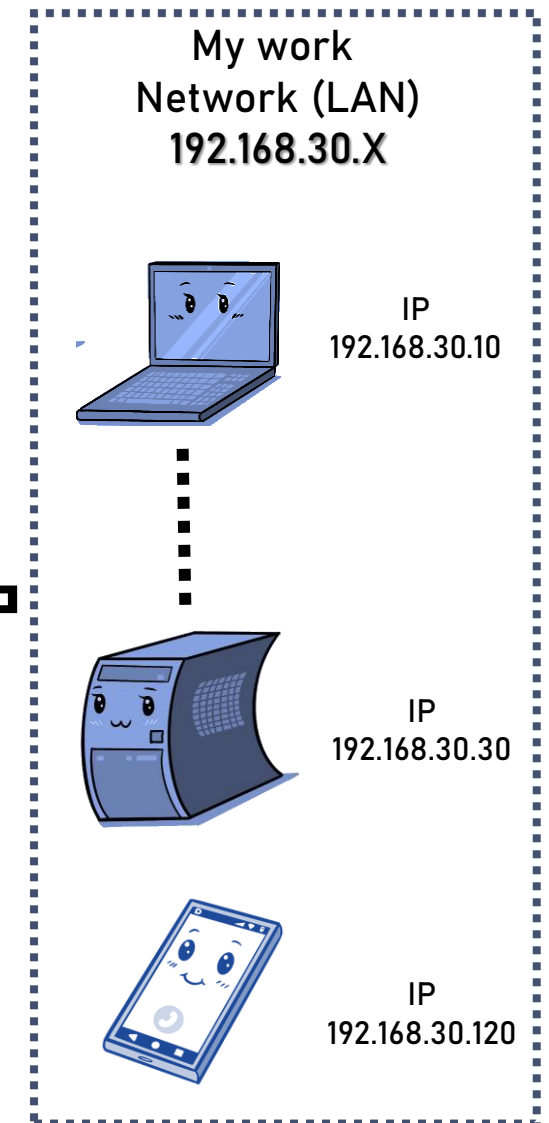
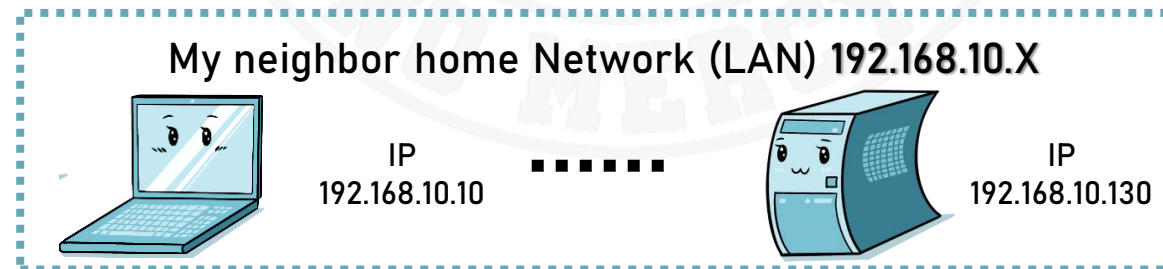
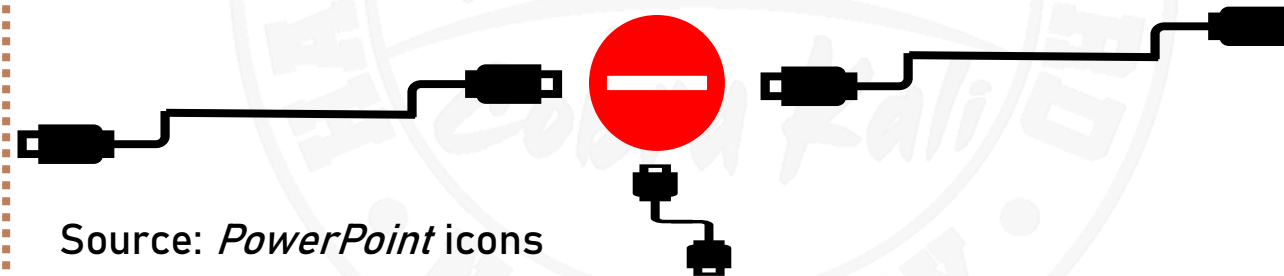


José Manuel
Redondo López

- **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! Yes, but they have IPs 😊**
 - **A machine IP is what distinguishes a machine 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!
- **We are in social networks, but machines are in IP networks**
 - The approach is the same!
 - Let's remember concepts from **FCR** 😊



- **LAN: a network that interconnects computers within a limited area**
 - Residence, school, laboratory, university 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!



- **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**
 - They 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)



José Manuel
Redondo López

- **CIDR is a bit-based standard that uses prefixes to display IP addresses with their routing properties**
 - Facilitates routing by grouping address blocks into entries in a single 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 usesyntax 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)



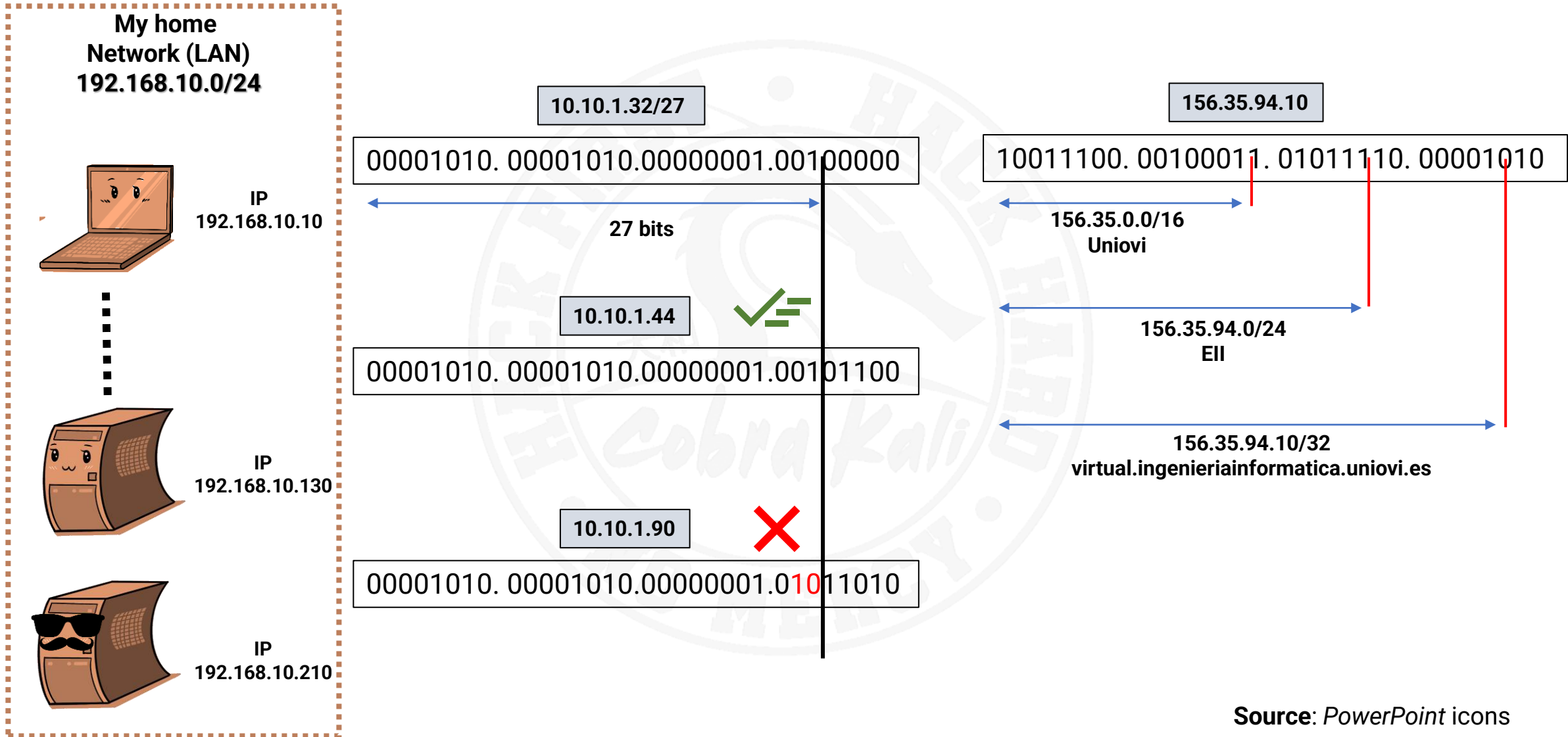
José Manuel
Redondo López

- **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)
 - An 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)



José Manuel
Redondo López



CLASSLESS INTER-DOMAIN ROUTING (CIDR)



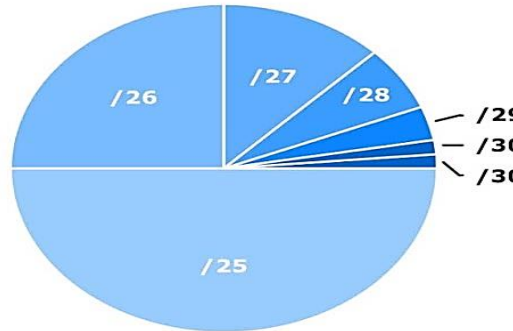
José Manuel
Redondo López

- Small and large LANs (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
- ISPs usually have /21 or lower

IPv4 SUBNETTING

packetlife.net

Subnets				Decimal to Binary			
CIDR	Subnet Mask	Addresses	Wildcard	Subnet Mask		Wildcard	
/32	255.255.255.255	1	0.0.0.0	255	1111 1111	0	0000 0000
/31	255.255.255.254	2	0.0.0.1	254	1111 1110	1	0000 0001
/30	255.255.255.252	4	0.0.0.3	252	1111 1100	3	0000 0011
/29	255.255.255.248	8	0.0.0.7	248	1111 1000	7	0000 0111
/28	255.255.255.240	16	0.0.0.15	240	1111 0000	15	0000 1111
/27	255.255.255.224	32	0.0.0.31	224	1110 0000	31	0001 1111
/26	255.255.255.192	64	0.0.0.63	192	1100 0000	63	0011 1111
/25	255.255.255.128	128	0.0.0.127	128	1000 0000	127	0111 1111
/24	255.255.255.0	256	0.0.0.255	0	0000 0000	255	1111 1111
/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				

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

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

CLASSLESS INTER-DOMAIN ROUTING (CIDR): RESERVED ADDRESSES



José Manuel
Redondo López

- **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**

- **Internet growth depleted the pool of available IPv4 addresses**
 - For this reason, a new version of IP (IPv6), **using 128 bits**, was standardized
 - Using 128 bits 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/>

Machine Networks

Machines never talk alone 😊



- **In a social network you can normally communicate with every user of the same social 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 that match the same CIDR
 - Machines in the same network can normally communicate among others
 - 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!

● 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 to your connected Facebook account
 - Not posts, not other user histories...
- But with machines, you **CAN** communicate machines in different networks
 - Thanks to special machines that act as “**bridges**” or “**gateways**” between both
 - And that is what we are about to explain!
 - But first, we need to review two concepts regarding IPs

PUBLIC AND PRIVATE IPs. NAT



José Manuel
Redondo López

- **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 addresses**
 - 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?



José Manuel
Redondo López

- 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
 - Is **posted with the group id / name / hashtag** (a valid IP on the receiver machine network) to the outside
 - The real user that issued the message is not visible
 - If someone replies to the message
 - Only the original sender receives this response
 - 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
 - Information to do this is handled by software like iptables (see [ASR](#))

Source: <https://www.profesionalreview.com/2020/08/22/modo-nat-ques/>

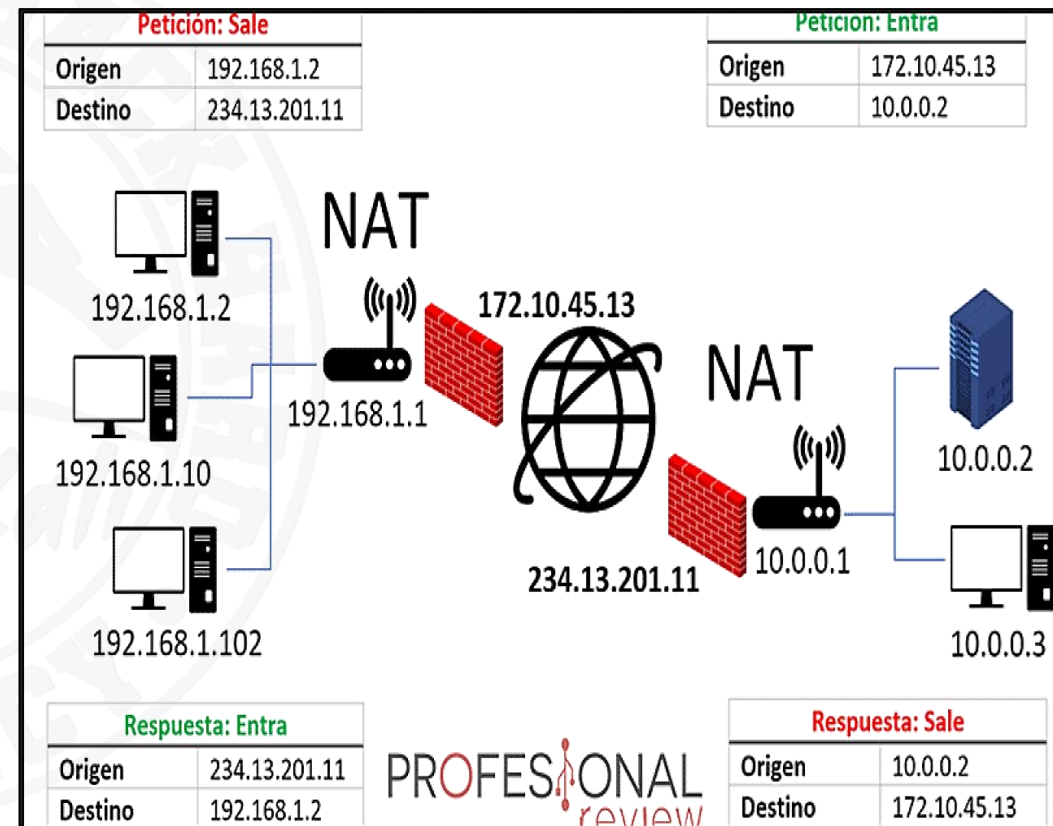
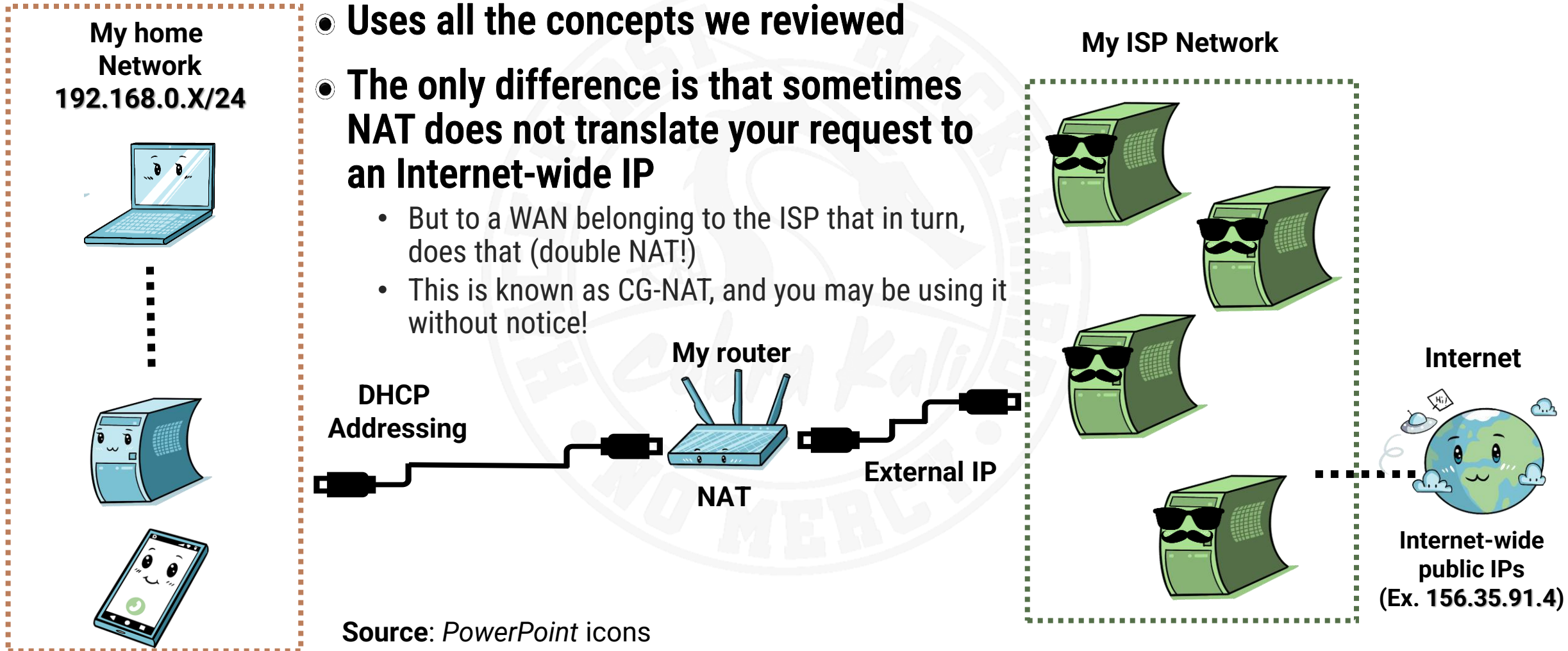


DIAGRAM: TYPICAL HOME ISP NAT + DHCP ROUTER



José Manuel
Redondo López

- This is the typical home network layout
- Uses all the concepts we reviewed
- The only difference is that sometimes NAT does not translate your request 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)



José Manuel
Redondo López

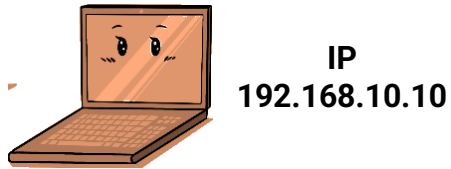
- **Routers assign IPs to its network devices manually or automatically**
- **DHCP is the protocol that assigns IP addresses automatically and dynamically**
 - This means that a device does not have to have the same IP address all the time, but also does not worry about how to obtain it 😊
 - You will 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
 - Typically, the own router
 - The DHCP server then assigns an IP address to that system for a fixed time 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 to devices on internet with minimal effort (and just one IP)**

GATEWAYS / NETWORK BRIDGES / ROUTERS / SWITCHES

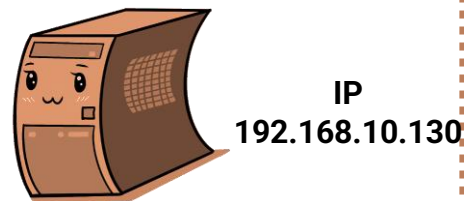


José Manuel
Redondo López

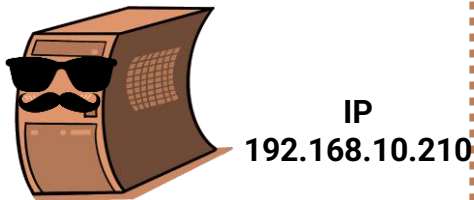
Accounting (LAN)
192.168.10.X



IP
192.168.10.10



IP
192.168.10.130



IP
192.168.10.210

● 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

Staff (LAN) 192.168.20.X



IP
192.168.20.10

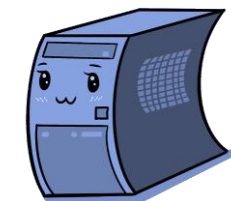


IP
192.168.20.130

Sales (LAN)
192.168.30.X



IP
192.168.30.10



IP
192.168.30.30



IP
192.168.30.120

TO SUMMARIZE...



José Manuel
Redondo López

- **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 course!

DNS

Domain Name Service



IPs ARE DIFFICULT TO REMEMBER!



José Manuel
Redondo López

- **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`”
 - (Maybe Elon Musk is going to change that 😊)
- **Even more, 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 😊**
- **Every machine in the world has an IP assigned, but we never 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)



José Manuel
Redondo López

● Hierarchical and decentralized naming system for computers, services, or other resources connected to any network

- Associates IP addresses with human-readable domain names assigned to entities
 - E. g. 156.35.94.1 is www.ingenieriainformatica.uniovi.es
- Delegates the responsibility of assigning domain names and mapping those names to Internet resources
 - By designating **authoritative DNS name servers** for each domain
 - Network admins may also delegate authority over sub-domains to other name servers
 - Provides distributed and fault-tolerant service to avoid a single large central database

● 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 utility [nslookup](#) from that course

DOMAIN NAME SYSTEM (DNS)



José Manuel
Redondo López

- **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
 - Today it works with IPv4 and IPv6
- **The translation process is automatic and transparent**
 - That's what makes the Internet possible today
- **In order 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

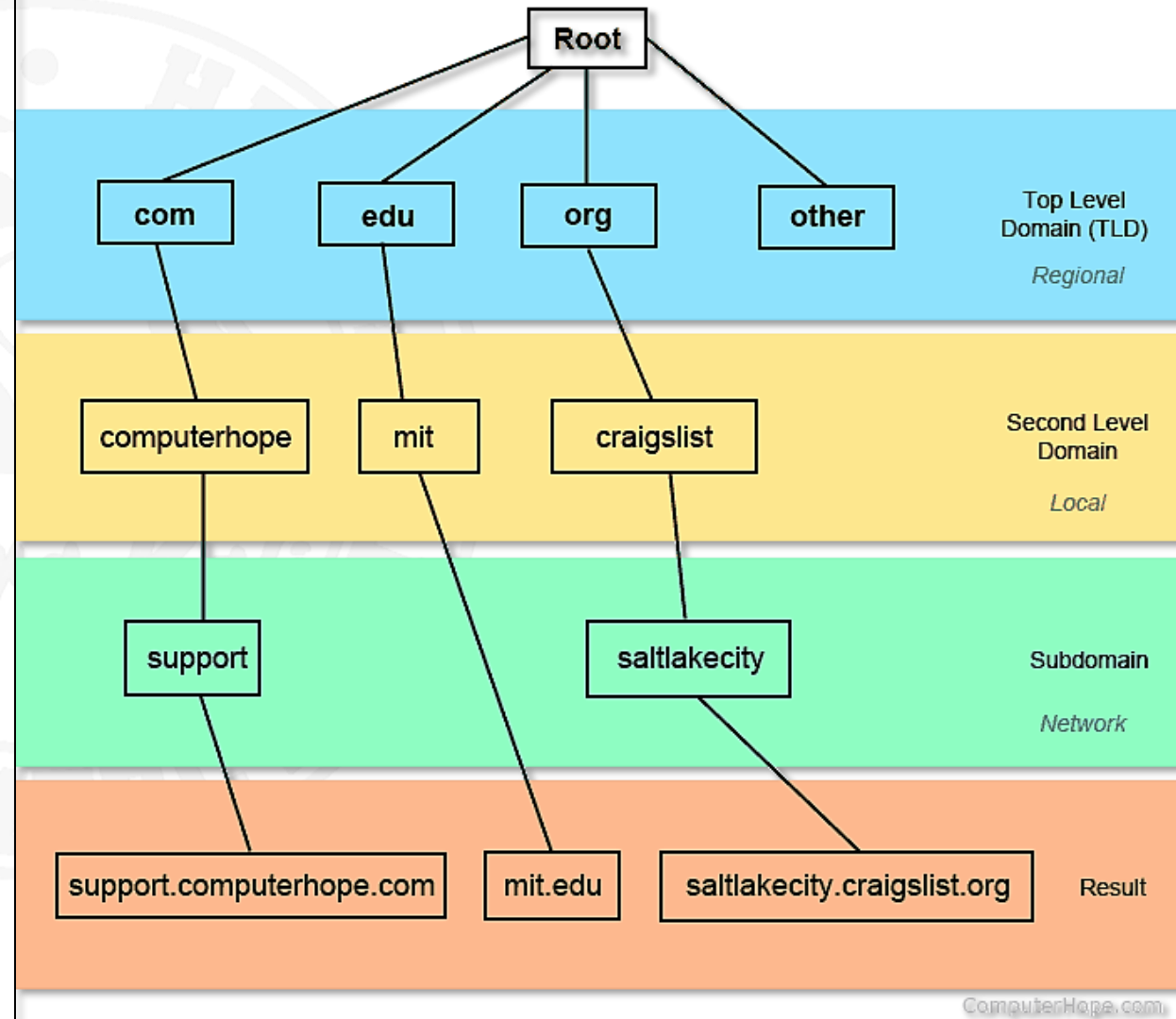
DOMAIN NAMES



José Manuel
Redondo López

- **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)**

Domain Naming Hierarchy



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

● DNS works hierarchically

- Top-level domains or TLDs can have multiple subdomains below them
- In the previous diagram, `.mit` and `.craigslist` are part of the top-level `.edu` and `.org` domains respectively
- These are called **subdomains** (SLDs)
 - Domains that are part of a larger domain
 - In the example, `mit` and `craigslist` are second-tier domains under their own TLD
- And, of course, below these SLDs there may be many other subdomains
 - For example, below `.com`, we could 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 more general

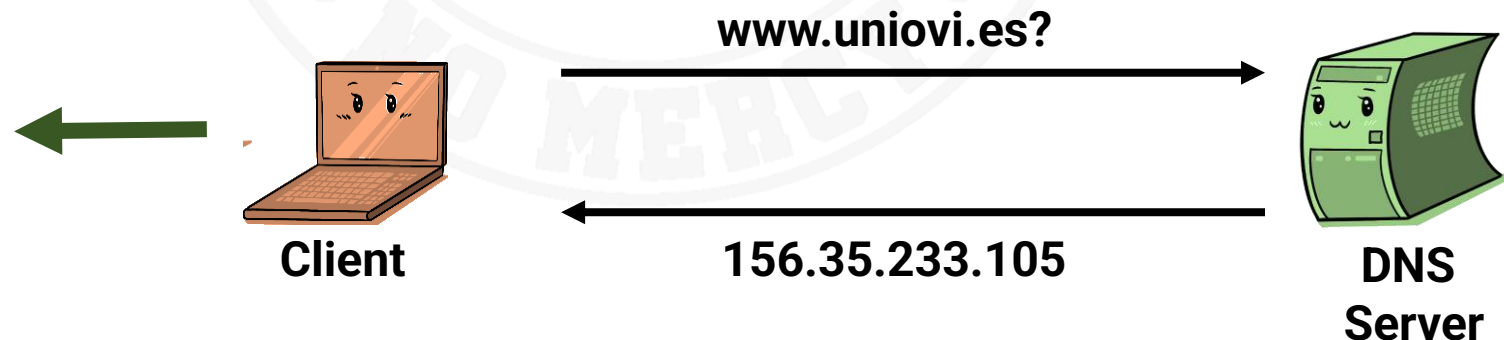
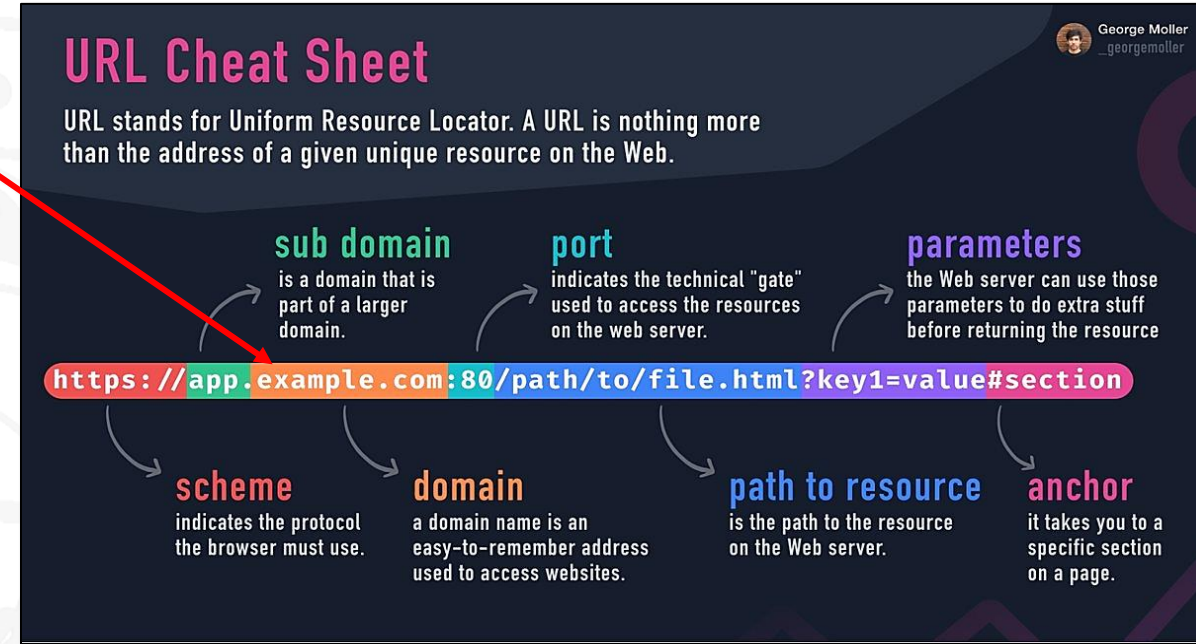
● Let's see how this works!

How DNS WORKS



José Manuel
Redondo López

- What happens when you type a URL and press enter?
 - From the client point of view, not much
 - It asks for the IP of a **domain name** to its DNS
 - If the DNS server knows the IP belonging to this 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...



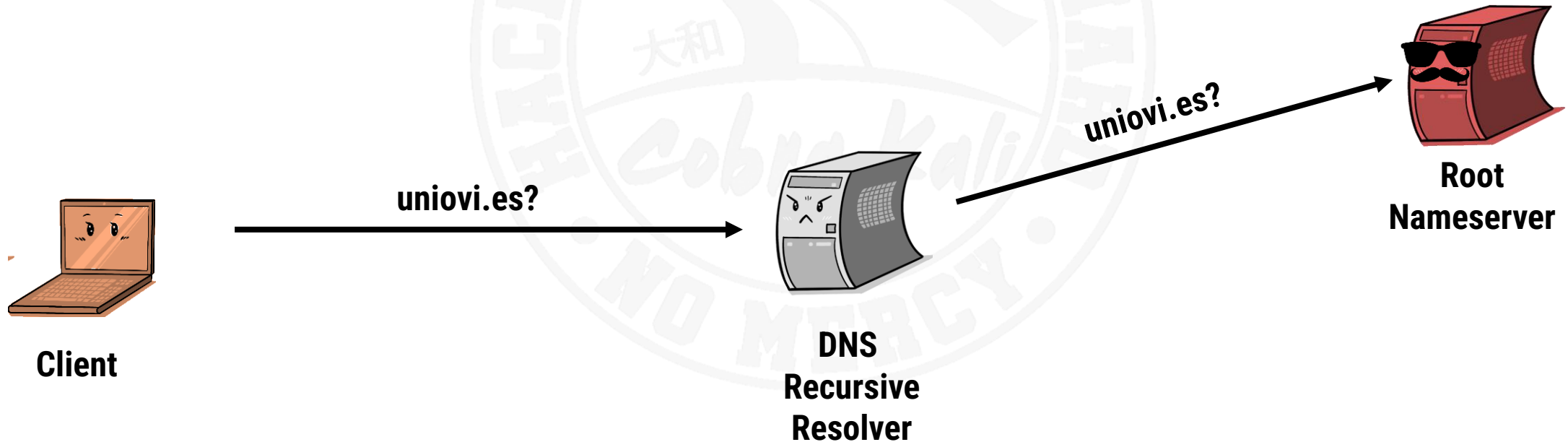
How DNS WORKS



José Manuel
Redondo López

● 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 a root nameserver is known



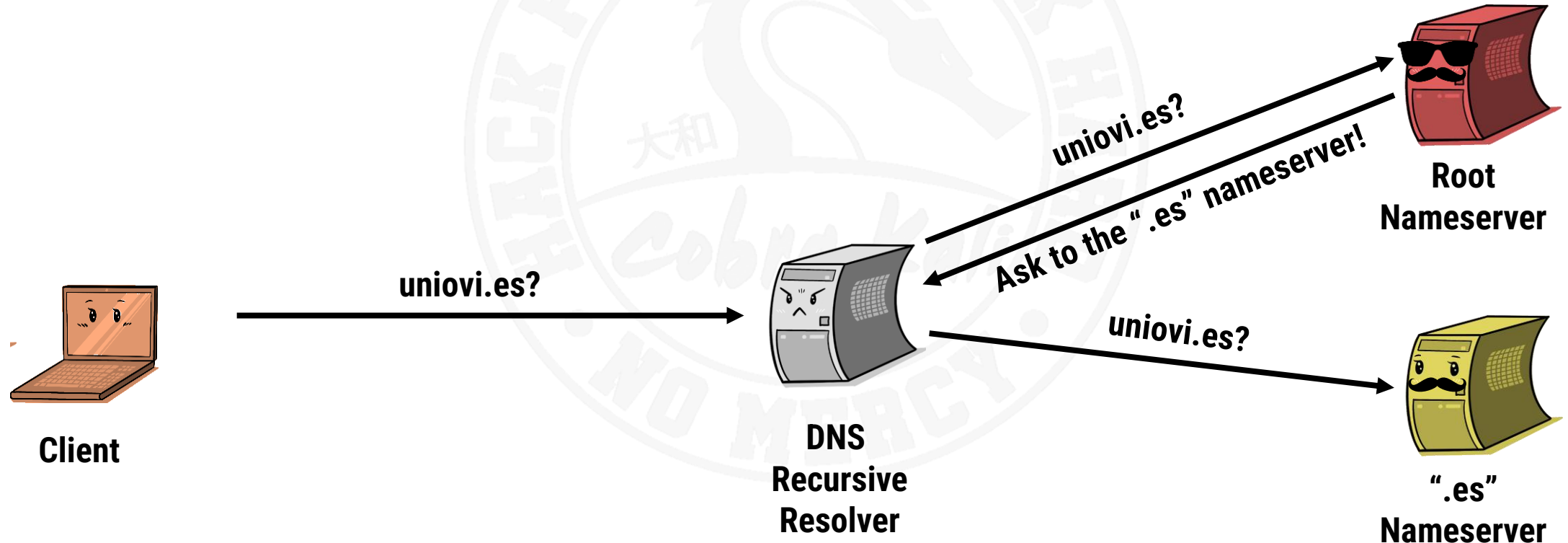
How DNS WORKS



José Manuel
Redondo López

● 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



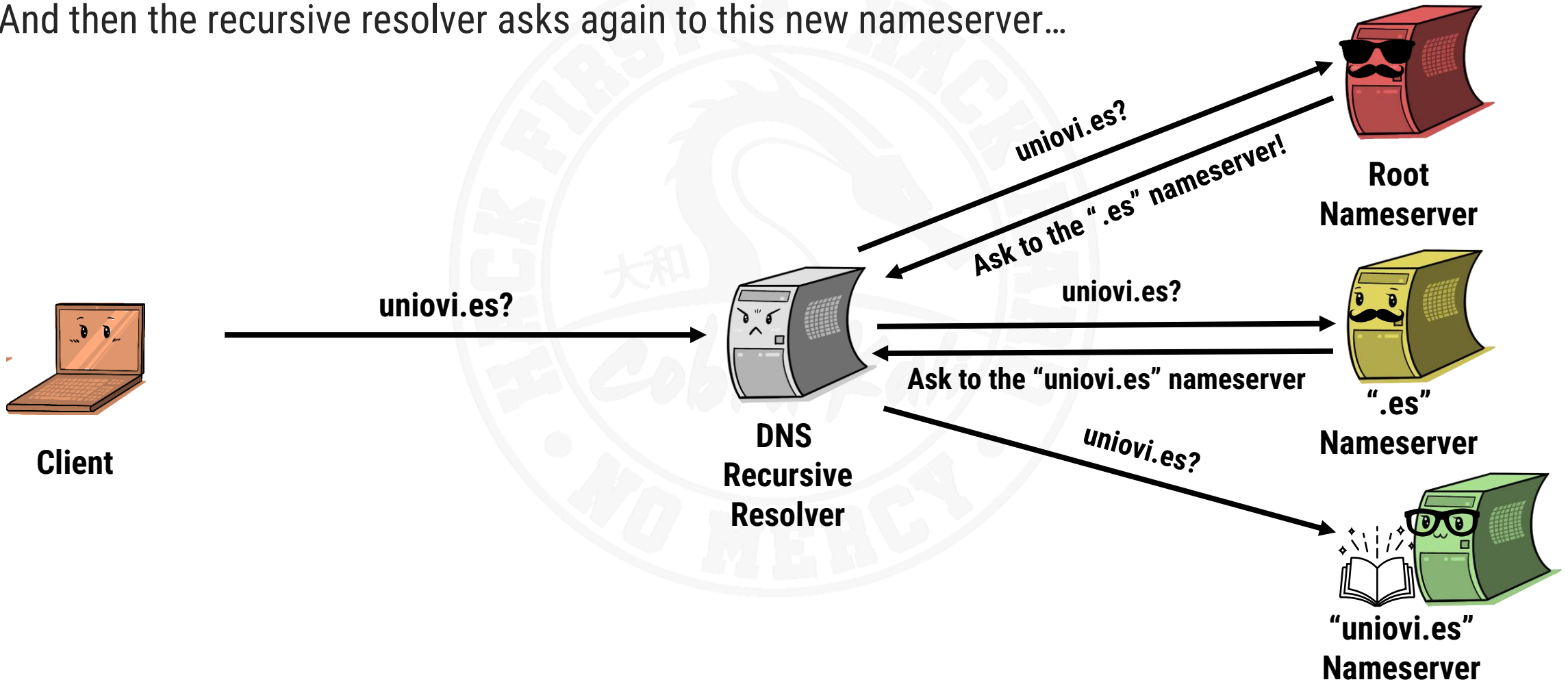
How DNS WORKS



José Manuel
Redondo López

- 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...

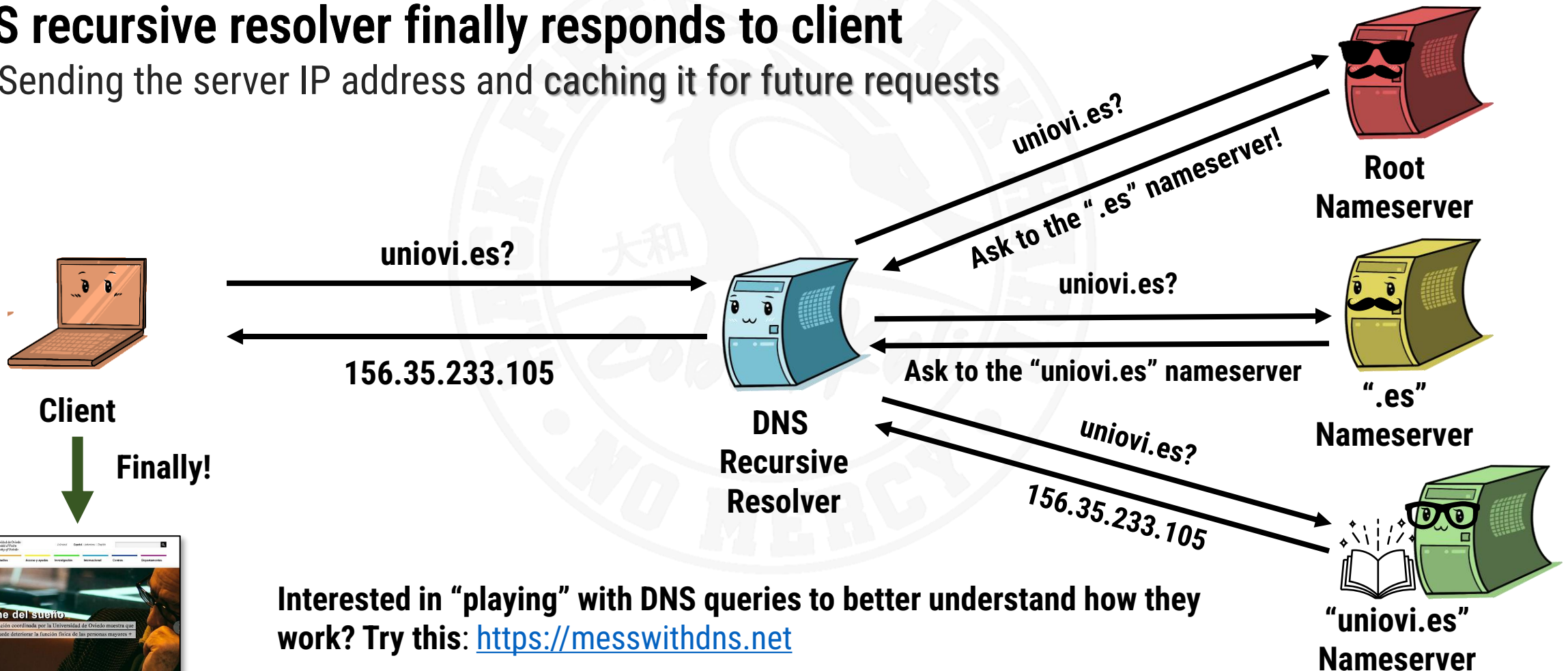


How DNS WORKS



José Manuel
Redondo López

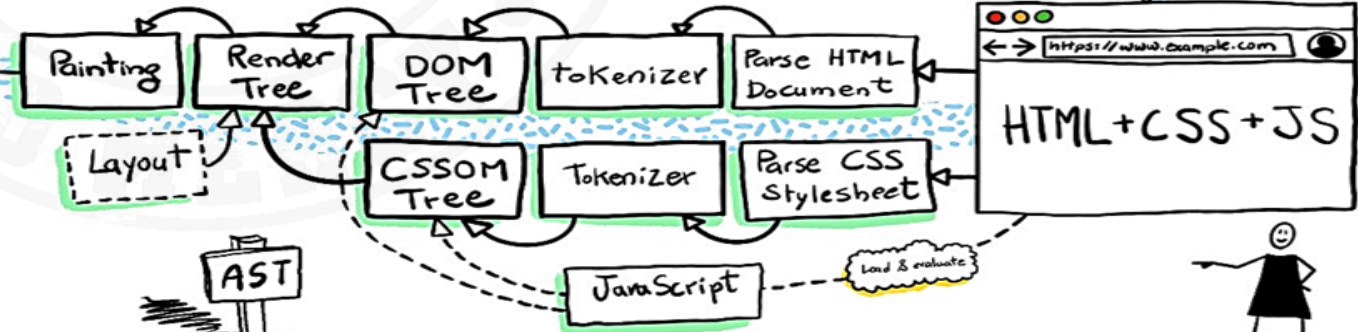
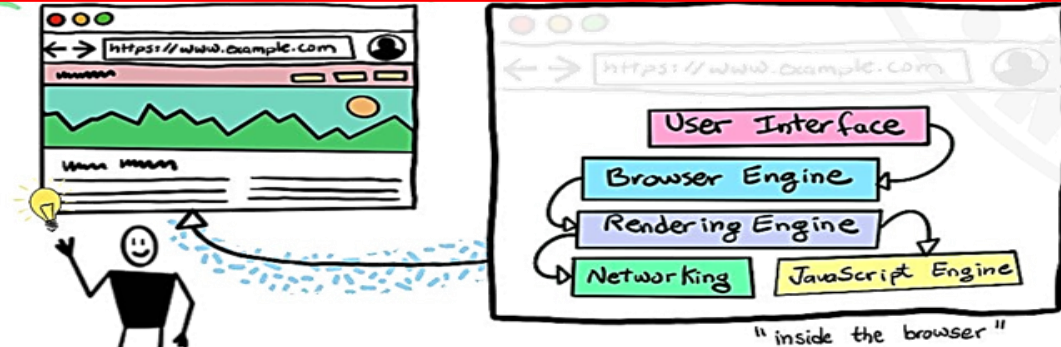
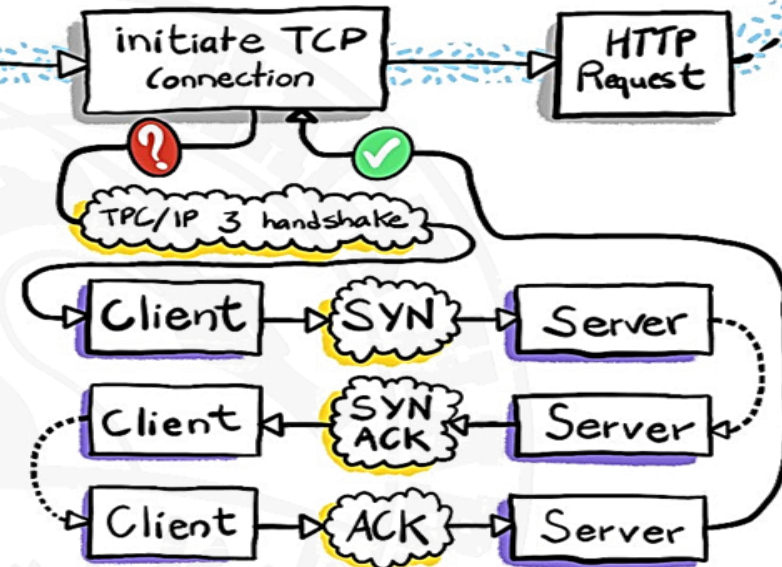
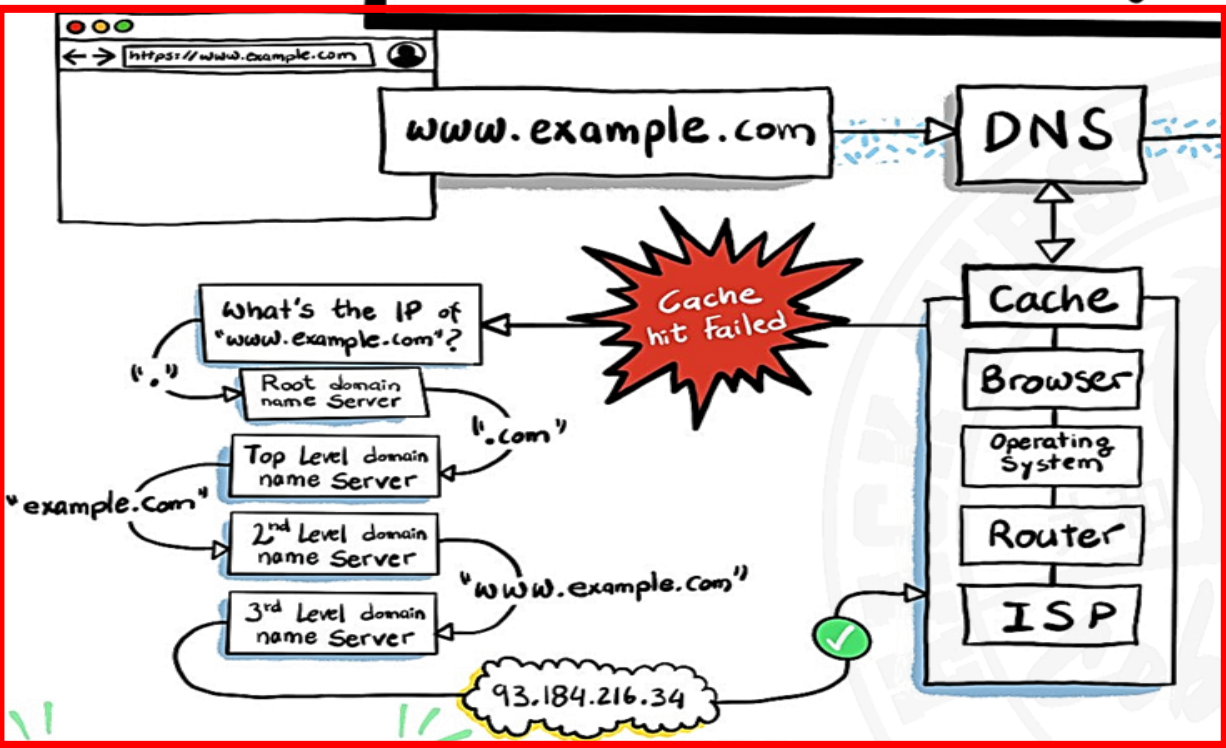
- This SLD domain nameserver is marked as authoritative for `uniovi.es`, so it replies with the server IP address
- DNS recursive resolver finally responds to client
 - Sending the server IP address and caching it for future requests



WHAT HAPPENS* WHEN YOU TYPE IN A URL IN AN ADDRESS BAR IN A BROWSER?

* a brief overview

The Internet is Complicated...



[< Go to Index](#)

[Internal view >](#)

TARGETING MACHINES

A machine from an external point of view



WHAT IS A MACHINE FROM THE OUTSIDE?



José Manuel
Redondo López

- Once we reach a target machine, we have an external view of what it offers to the users
- This 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

● 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 IP **156.35.94.1**
 - To browse it we need a proper client that connects to port **80**
 - Which is the one that offers the HTTP service (our official web page) by default

● 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 machines outside yours
 - E. g.: Web server, Minecraft server...
- **Opening ports under CG-NAT does not work! (beware!)**

ABOUT PORTS...



José Manuel
Redondo López

- 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 are typically 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)
- There are **passive** tools with the same purpose
 - Just listen to traffic, more “stealth”
 - E.g.: **netdiscover**

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 Ensimg
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	

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

by Jeremy Stretch

v1.1

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

- **Programs that run associated with a network port**
 - They “listen” to it
 - 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! 😊**

- **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 responses pre-determined for that 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



José Manuel
Redondo López

- 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 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

● 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)

```
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
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-fw
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!



José Manuel
Redondo López

● 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?



José Manuel
Redondo López

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



And once you are in...A machine from an internal point of view

Main aspects to consider inside any machine



MACHINE ENTITIES FROM A SECURITY POINT OF VIEW



José Manuel
Redondo López

- **Once we are inside a machine, there are three main entities we must consider from a security point of view**
 - Users
 - Files and partitions
 - Programs (software)
- **We will deal with this more thoroughly in the OS security topic**
- **But the entities itself were reviewed in the **SO** course**

FILES AND PARTITIONS



José Manuel
Redondo López

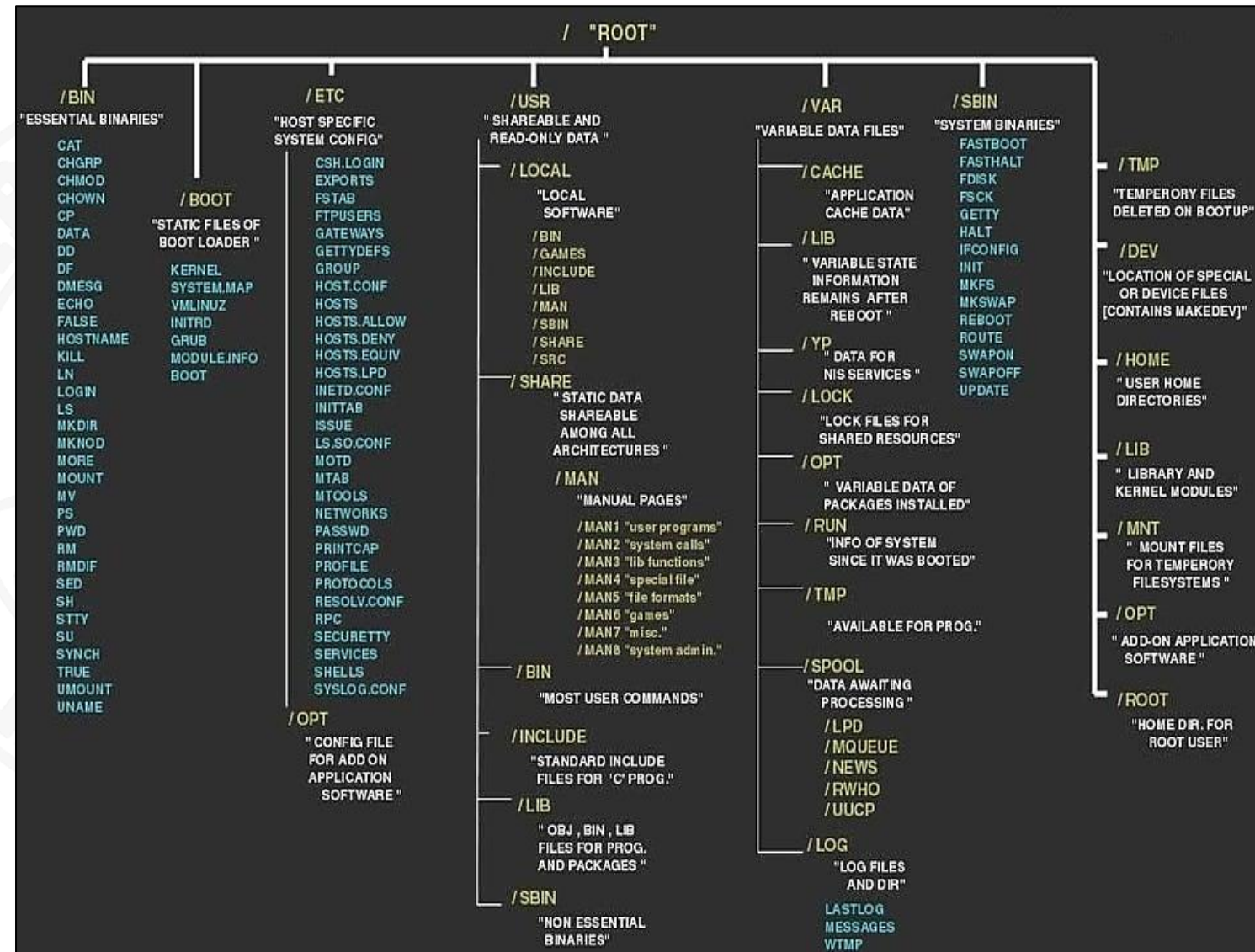
● Every OS has a predefined structure of directories, files and partitions

- Partitions group files under a directory in an isolated storage space
- Typically, transparent to the user

● The image shows a typical Linux installation

- We need to know where are the critical parts of the filesystem
 - Private files, device files, important services, logs...
- Without this knowledge, we cannot perform security operations effectively

Source: <https://www.wifislax.com/sistema-de-archivos-linux-en-una-sola-imagen/>



● Inside any OS we have

- **Commands:** invoked by users to achieve different effects
 - The image shows the typical commands of a Linux system
 - More complete listing: <https://ss64.com/bash/>
- **Background running applications**
 - They are called **services** (Windows) or **Daemons** (Linux)
 - Provide different features to the OS
 - Most are required to proper OS operation
 - They are running continuously or periodically (programmed)
 - Or once a certain application runs

File Commands

ls - directory listing
ls -al - formatted listing with hidden files
cd *dir* - change directory to *dir*
cd - change to home
pwd - show current directory
mkdir *dir* - create a directory *dir*
rm *file* - delete *file*
rm -r *dir* - delete directory *dir*
rm -f *file* - force remove *file*
rm -rf *dir* - force remove directory *dir* *
cp *file1 file2* - copy *file1* to *file2*
cp -r *dir1 dir2* - copy *dir1* to *dir2*; create *dir2* if it doesn't exist
mv *file1 file2* - rename or move *file1* to *file2*
 if *file2* is an existing directory, moves *file1* into directory *file2*
ln -s *file link* - create symbolic link *link* to *file*
touch *file* - create or update *file*
cat > *file* - places standard input into *file*
more *file* - output the contents of *file*
head *file* - output the first 10 lines of *file*
tail *file* - output the last 10 lines of *file*
tail -f *file* - output the contents of *file* as it grows, starting with the last 10 lines

Process Management

ps - display your currently active processes
top - display all running processes
kill *pid* - kill process id *pid*
killall *proc* - kill all processes named *proc* *
bg - lists stopped or background jobs; resume a stopped job in the background
fg - brings the most recent job to foreground
fg *n* - brings job *n* to the foreground

File Permissions

chmod *octal file* - change the permissions of *file* to *octal*, which can be found separately for user, group, and world by adding:

- 4 - read (r)
- 2 - write (w)
- 1 - execute (x)

Examples:

chmod 777 - read, write, execute for all
chmod 755 - rwx for owner, rx for group and world
 For more options, see **man chmod**.

SSH

ssh *user@host* - connect to *host* as *user*
ssh -p *port user@host* - connect to *host* on port *port* as *user*
ssh-copy-id *user@host* - add your key to *host* for *user* to enable a keyed or passwordless login

Searching

grep *pattern files* - search for *pattern* in *files*
grep -r *pattern dir* - search recursively for *pattern* in *dir*
command* | grep *pattern - search for *pattern* in the output of *command*
locate *file* - find all instances of *file*

System Info

date - show the current date and time
cal - show this month's calendar
uptime - show current uptime
w - display who is online
whoami - who you are logged in as
finger *user* - display information about *user*
uname -a - show kernel information
cat /proc/cpuinfo - cpu information
cat /proc/meminfo - memory information
man *command* - show the manual for *command*
df - show disk usage
du - show directory space usage
free - show memory and swap usage
whereis *app* - show possible locations of *app*
which *app* - show which *app* will be run by default

Compression

tar cf *file.tar files* - create a tar named *file.tar* containing *files*
tar xf *file.tar* - extract the files from *file.tar*
tar czf *file.tar.gz files* - create a tar with Gzip compression
tar xzf *file.tar.gz* - extract a tar using Gzip
tar cjf *file.tar.bz2* - create a tar with Bzip2 compression
tar xjf *file.tar.bz2* - extract a tar using Bzip2
gzip *file* - compresses *file* and renames it to *file.gz*
gzip -d *file.gz* - decompresses *file.gz* back to *file*

Network

ping *host* - ping *host* and output results
whois *domain* - get whois information for *domain*
dig *domain* - get DNS information for *domain*
dig -x *host* - reverse lookup *host*
wget *file* - download *file*
wget -c *file* - continue a stopped download

Installation

Install from source:

./configure
make
make install
dpkg -i *pkg.deb* - install a package (Debian)
rpm -Uvh *pkg.rpm* - install a package (RPM)

Shortcuts

Ctrl+C - halts the current command
Ctrl+Z - stops the current command, resume with **fg** in the foreground or **bg** in the background
Ctrl+D - log out of current session, similar to **exit**
Ctrl+W - erases one word in the current line
Ctrl+U - erases the whole line
Ctrl+R - type to bring up a recent command
!! - repeats the last command
exit - log out of current session

* use with extreme caution.

USERS ACCORDING TO THEIR CAPABILITIES: PRIVILEGED USER ACCOUNTS



José Manuel
Redondo López

- **These have more privileges than ordinary users**
 - Able to install/remove software, upgrade the OS, modify system or application configurations...
- **They might also have access to files that are not normally accessible to standard users**
- **We can normally identify these privileged accounts**
 - **Root / Administrator account:** the system administrator, able to perform any change in the OS <https://www.ssh.com/iam/user/root/>
 - **System accounts:** usually with known user IDs, created during the OS install for management
 - **Service accounts:** run applications/other processes
 - Also created to own data and configuration files
 - They are not intended to be allowed interactive login (bash terminals)
 - Or be used by people in any way
 - Only for administrative operations

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/
n
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/no
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
```


USERS ACCORDING TO THEIR CAPABILITIES: “ORDINARY” USER ACCOUNTS



José Manuel
Redondo López

● OS users that only perform “normal” operations

- Like creating documents, editing photos, browsing, playing games... any operation that **do not require any special privilege**
- Some of them may be **sudoers**
 - Tools like `sudo` can be used to grant certain users **the ability to run selected commands as root**
 - This way, the need for an enabled interactive `root` account disappears
 - Only selected users (the ones in the `sudoers` group) can temporarily “upgrade” themselves to `root` to execute administrative operations
 - Once the operation ends, the user returns to their normal privilege status
- Not every user is a `sudoer`
 - All beyond the first created user (that is usually a sudoer automatically) must be manually added to this group

● In case of attack, the criminal will try to log in as `root` or as a `sudoer`

- If it is not possible, it will try to perform a **privilege scalation**
- We will deal with this later in the course!

[< Go to Index](#)

TARGETING USERS

Attacks that target humans



- [illegible]

José Manuel Redondo López

- | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|--|--|--|---|---|---|---|--|--|--|--|---|---|--|---|---|
| <div>  PrivacyTests.org </div> <div> News About    </div> | | | | | | | | | | | | | | | | | | | |
| No. 3 | | | | Open-source tests of web browser privacy. | | | | | | | | Updated 2021-11-02 | | | | | | | |
| <div> ✓ = Passed privacy test ✗ = Failed privacy test — = No such feature </div> | | | | | | | | | | | | | | | | | | | |
| 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 | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ | | | | | | | | | | | | |

● **Massively-sent fraudulent / unwanted email with multiple goals**

- **Advertisement** sites of certain products not normally found in typical web stores (Viagra...), or related to illegal / alegal activities
- **Scams** (Nigerian scam, fraudulent fundraises, mules...)
- Spread **malware**
- Spread **phishing** campaigns
- ... *(many, many new forms of fraud appear frequently)*

● **Apart from the email payload potential effects, they also might**

- Saturate (and therefore perform a DoS) networks / email servers (zip bombs)
- Initiate a scam or fraud (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 another type of fraud later
- **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 course
 - To know more about lots of fraud types, how they are implemented, and possible ways of identifying them, you can check these presentations (in Spanish)
 - **Fraud types:** https://www.researchgate.net/publication/348307670_Redes_Mentiras_y_tus_Tarjetas_de_credito_Fraudes_Online
 - **Fraud identification:** https://www.researchgate.net/publication/359146160_Las_Ciberestafas_en_la_Actualidad_Formas_de_reconocerlas_y_prevenirilas

- **Unwanted messages or publications with fake/biased information of various types**
 - Present in emails, social networks (Twitter, Facebook...), instant messaging applications (WhatsApp, Telegram...), SMS...
 - Also present in some newspaper (intentional disinformation or **fake news**)
- **Mostly aiming to harvest active email accounts**
 - That are later targets of phishing / 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**

- **Computer attack strategy in which the victim belongs to a concrete user group (organization, industry, or region)**
 - The attacker guesses or observes **which websites this group often uses**
 - 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 users of the group
- **This makes these attacks harder to detect and research**

DRIVE-BY DOWNLOAD (AKA AUTOMATIC DOWNLOADS)



José Manuel
Redondo López

- **Websites that download and install spyware / malware without their user's consent or awareness**
- **This type of downloads can also happen when viewing an e-mail message 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
- **Normally these attacks are 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

ADVANCED PERSISTENT THREAT (APT)



José Manuel
Redondo López

- **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 it remains, 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 advanced actors
 - With specific goals, seeking to steal, spy, or disrupt
- **Some utilize “traditional” vectors**
 - Social engineering, human intelligence...to access a physical location to enable network attacks

- **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

- **OSINT 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, blogs, forums, and electronic means associated with specific citizens such as telephones or user-created content
 1. This also includes Youtube and social networks
 2. It is the main source of information, since data appears time-sorted and is easily accessible
 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

OSINT TOOLS AND SOURCES



José Manuel
Redondo López

- The possible sources of information about a person / entity / company is **HUGE**

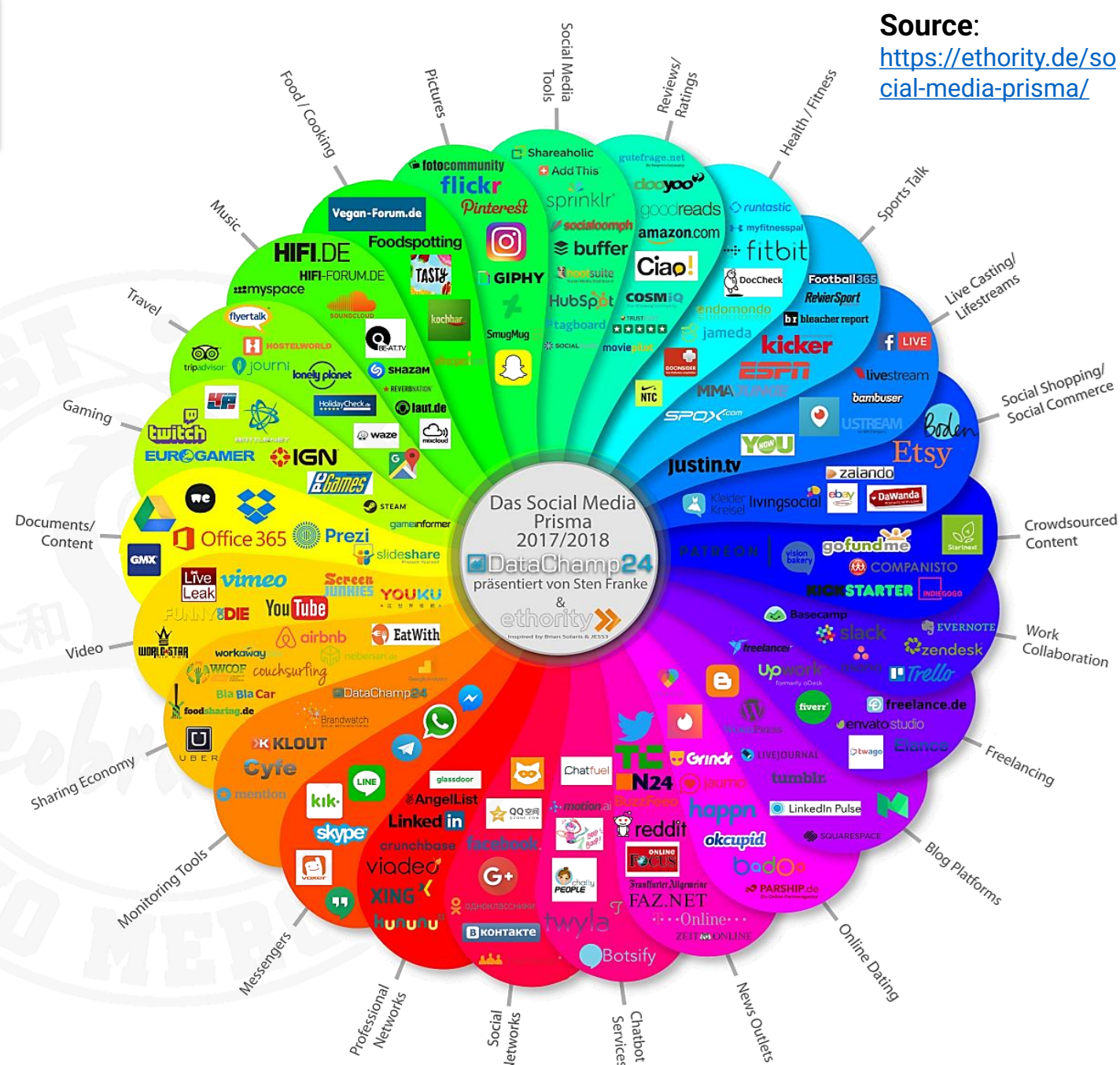
- The image shows some of them, divided by categories

- With them, it is very easy to find out a lot of information

- About a huge number of people worldwide
- Which is, by the way, scary...

- There are specialized OSINT tools for every data source

- <https://ciberpatrulla.com/links/>



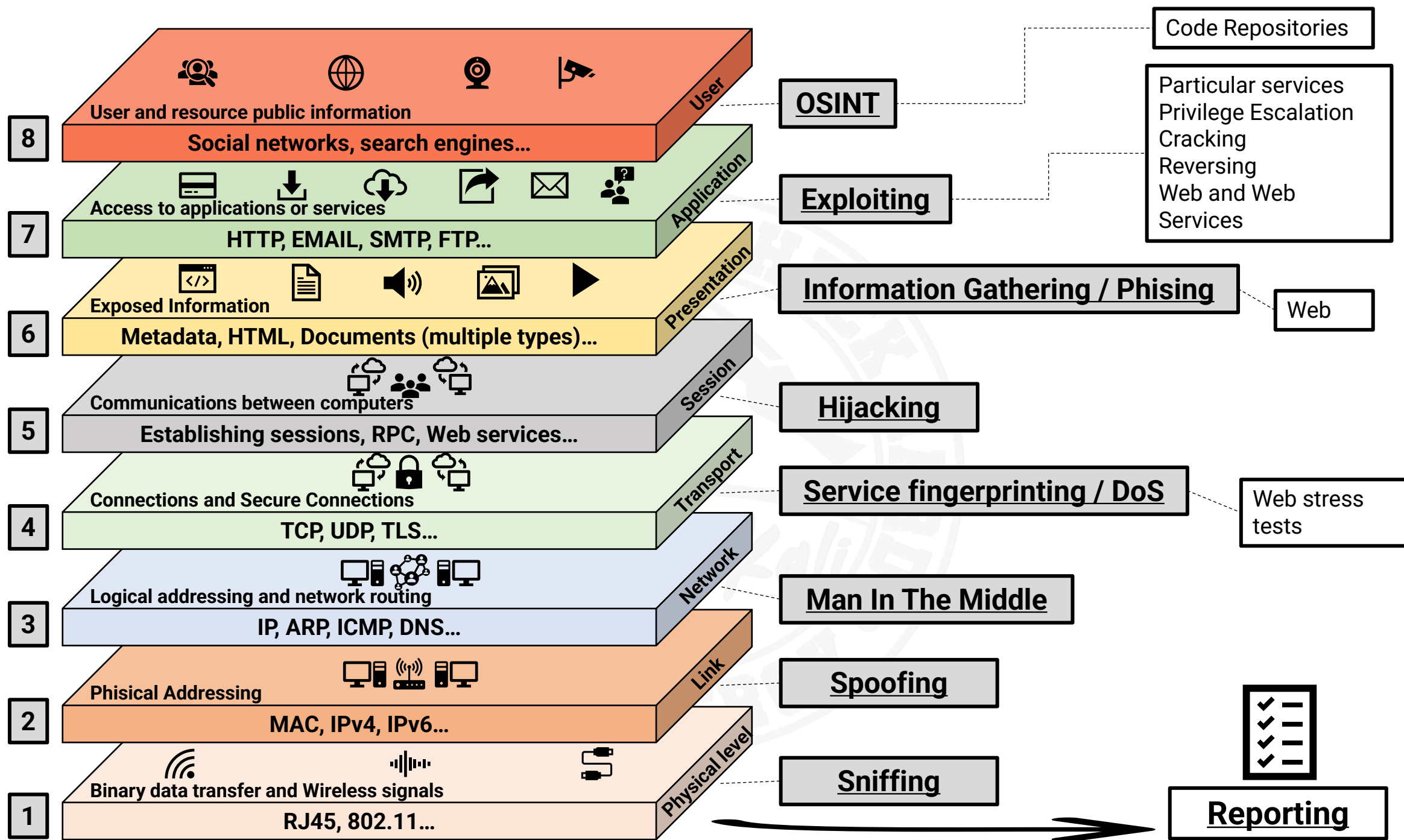
[< Go to Index](#)

AND NOW...

What's next?



The Attack Ecosystem

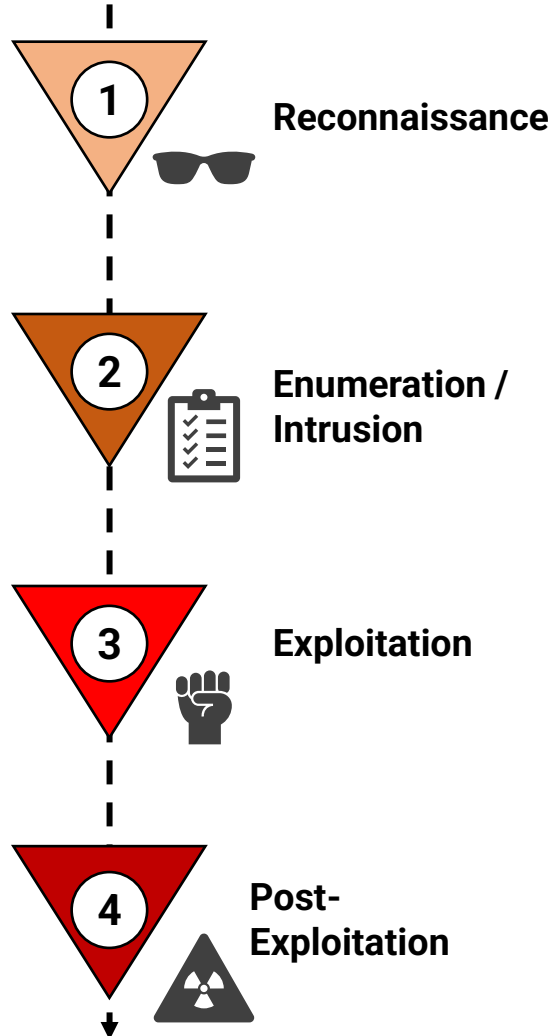


DEFENSES AGAINST THE DARK ARTS...



José Manuel
Redondo López

The “Cyber Kill Chain”



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

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

The act of exploiting vulnerabilities, and delivering malicious code onto the system, in order to get a better foothold

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 Methods Explained in

Topic 1

Topic 5

Topic 7

Topic 7

Possible defenses in

Topic 5

Topic 3
Topic 4
Topic 5

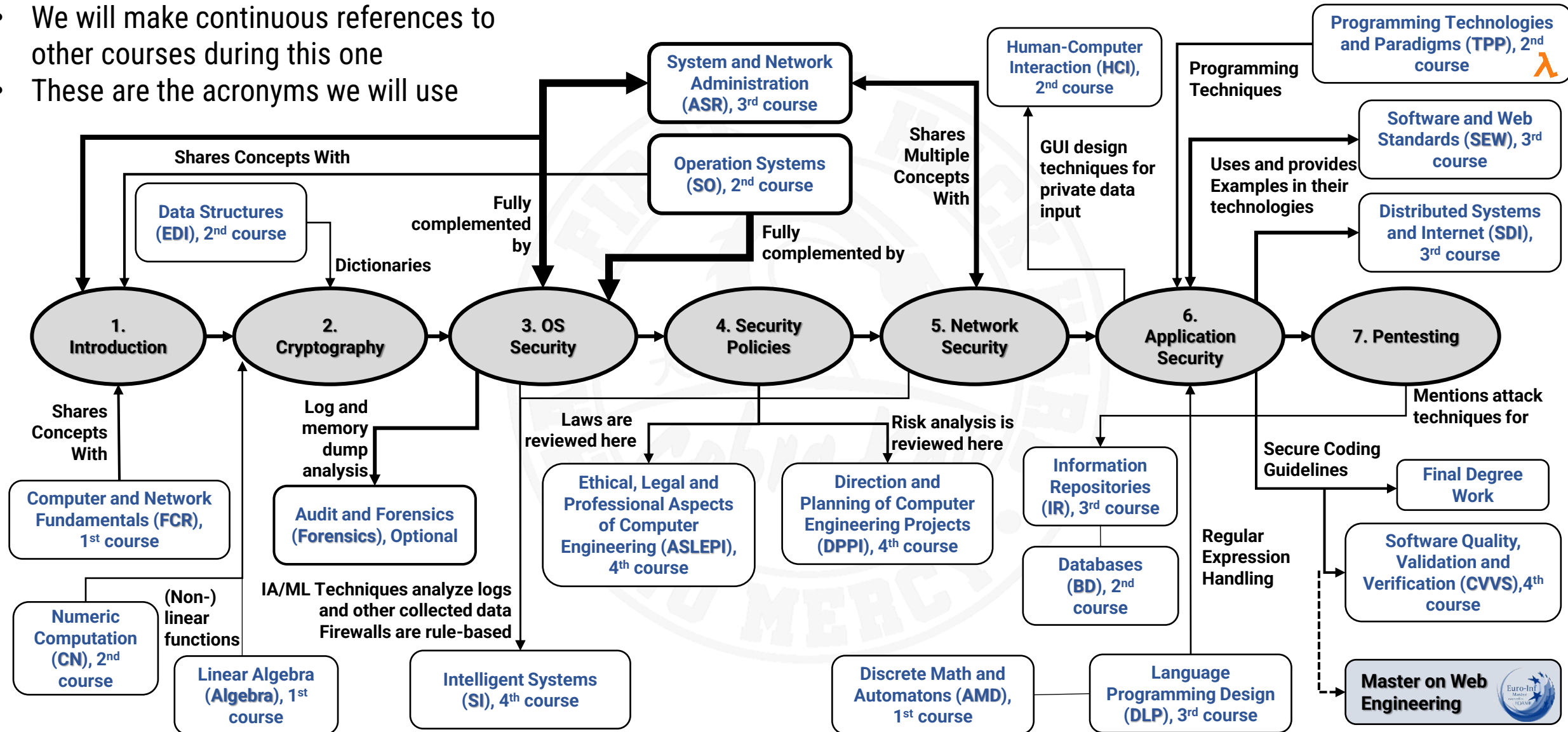
Topic 2
Topic 3
Topic 4
Topic 6

Topic 3
Topic 4

Source: PowerPoint icons

SSI RELATED TO OTHER DEGREE COURSES

- We will make continuous references to other courses during this one
- These are the acronyms we will use



SELF-EVALUATION ACHIEVEMENT LIST: INTRODUCTION



José Manuel
Redondo López

Rank	Concept
	Know the three type of attacks we can have against computer systems
	Know the basic concepts of cybersecurity and the basics of IP addressing
	Being able to determine the different types of networks we can have
	Know how DHCP and NAT works
	Understand the CIDR address scheme
	Understand the basic entities we can find in a machine from an external point of view
	Understand the basic entities we can find in a machine from an internal point of view
	Being able to distinguish the different malware types
	Know the different threats users may find nowadays
	Understand how DNS queries are processed
	Understand what happens every time we make an HTTP request
	My <body> is ready: Understand the basic concepts of security and networking

TOPIC 1: INTRODUCTION

