TOPIC 5
PERIMETER AND NETWORK SECURITY

Defending and attacking the network environment

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

Source: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

Logo: @creative_vanesa (*Instagram*)

Topic goals

- **Know the basics about network terminology and technologies**
  - Complementing topic 1
- **Understand how to design a secure network infrastructure**
- **Know the basics of network enumeration and machine / service fingerprinting**
  - Typical second phase of a pentesting operation / CTF (our “kill chain”)
- **Know about software that may disable common network-based attacks**
- **We will not cover details about Linux/Windows network configuration**
  - Including common tools (`netstat` / `nslookup`)
  - This is done in ASR!

INDEX

< Go to Index

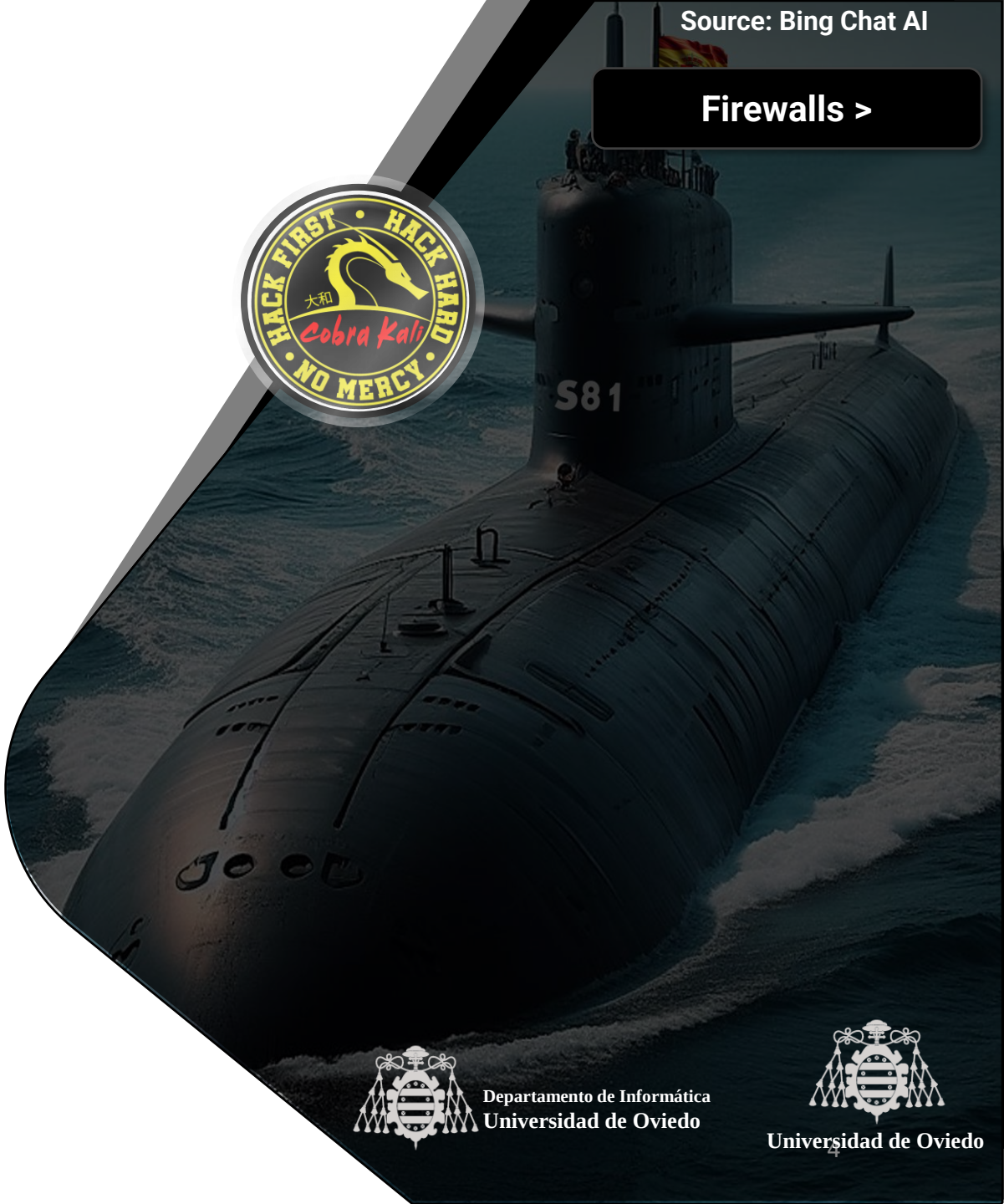
ADDITIONAL NETWORKING CONCEPTS

Complementing the first theory topic with new definitions

*Icons by Bing Chat AI

Source: Bing Chat AI

Firewalls >



Departamento de Informática
Universidad de Oviedo

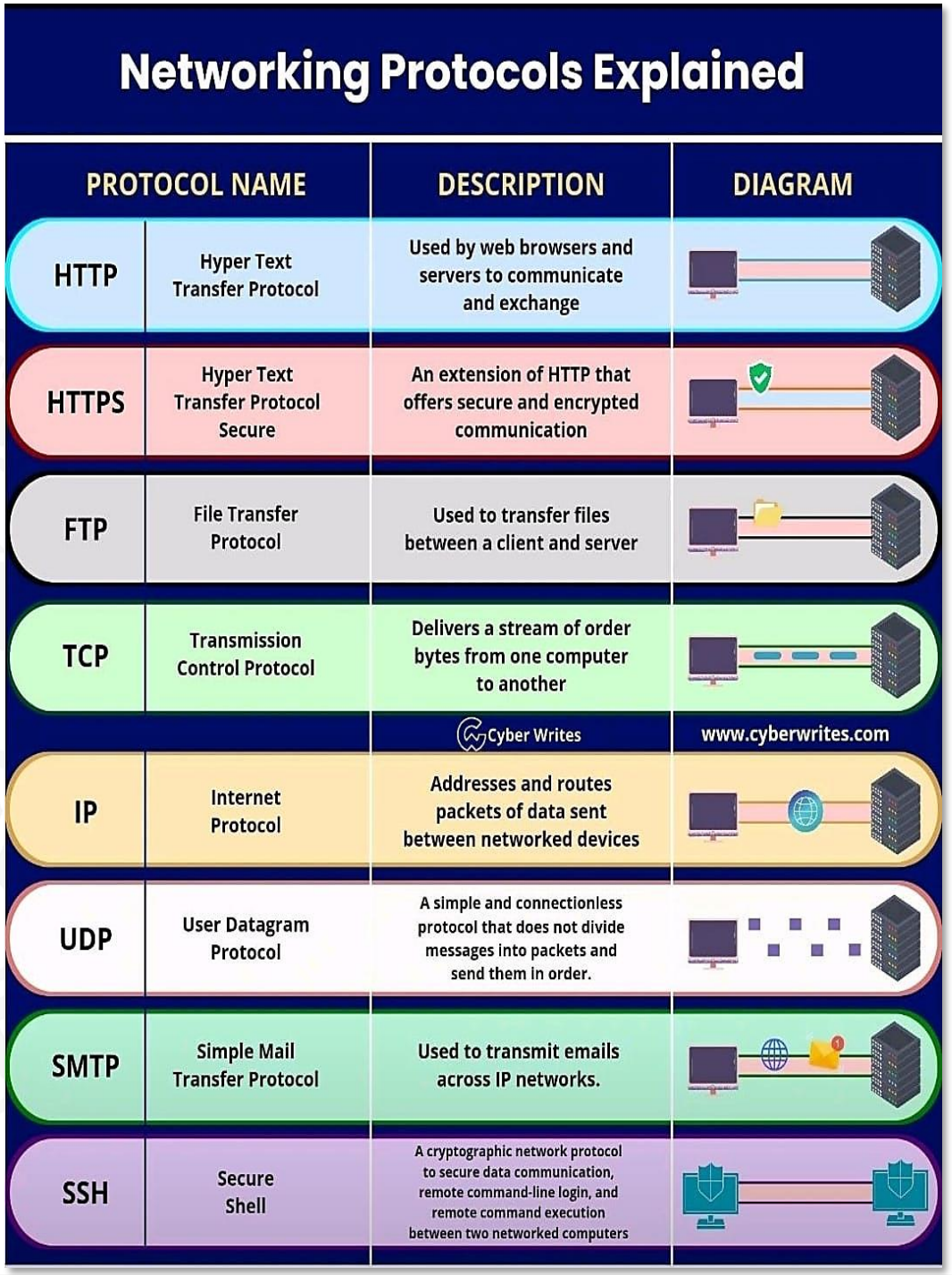
What are you going to find in this block?

- **In this block you will learn**
  - That there are **many different network** protocols, all with different functions
  - The **different types of firewalls** that exist and what their rules look like
  - What a **DMZ** is
  - The special use we can give to the **host file**

NETWORK PROTOCOLS

Computer Security

- As we said in topic 1, they define the rules of **communication** between + services (software)
  - Rules are typically defined in RFC (Request For Comments) documents
- There are many protocols: TCP, IP, UDP, FTP, HTTP, SMTP...
  - Each has its own set of rules that must be enforced to enable communication using them
- On Internet, the most important are
  - **IP** (Internet Protocol)
    - It uses IP addresses as machine addressing scheme (**Topic 1**): the basis of Internet!
    - More details about it are reviewed in the ASR course
  - **TCP** (Transmission Control Protocol)
- Network protocols can be blocked by firewall configuration (ASR)



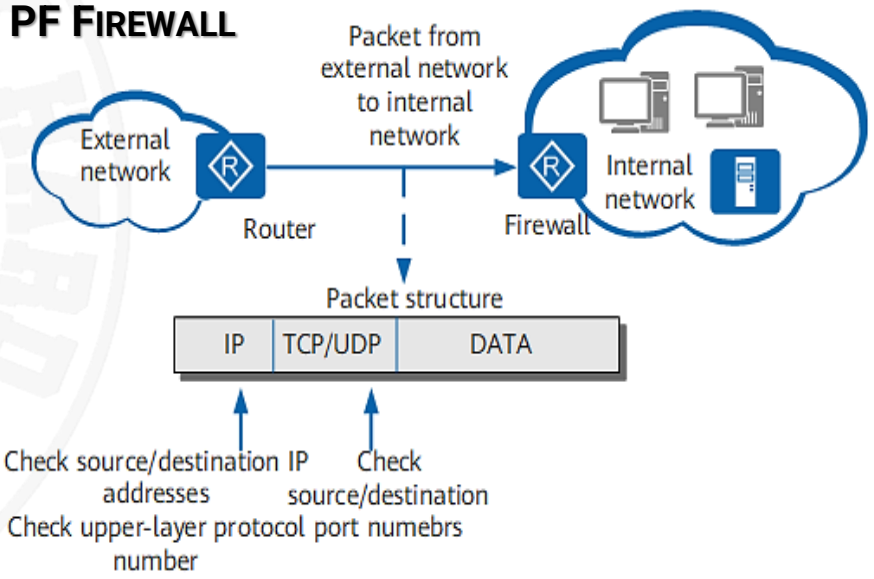
Remember: Firewalls

- **Designed to block unauthorized access (IPs, entire networks, protocols…)**
  - Typically **allowing outgoing traffic**
  - Part of a computer system (software)
  - Or a whole network (specialized hardware)
  - Also provides connection logging and auditing functions
- **Firewalls can be either software, hardware or hybrid**
  - **Hardware firewalls** are machines whose **hardware is especially designed** to maximize network throughput and packet processing power
    - The most expensive but more powerful option
    - They allow faster processing and enhanced rule customization
  - **Hybrid firewalls** are advanced software-based firewalls (E.g.: OS) **running on standard hardware**
    - A compromise between processing power and cost
    - Also implement powerful rule customization features
  - **Software firewalls** is just running **a firewall program** on your PC
    - Cheap (or free!) solution, but with less processing power
    - Typically, they implement less rule customization features

Firewalls: Packet-filtering (PF)

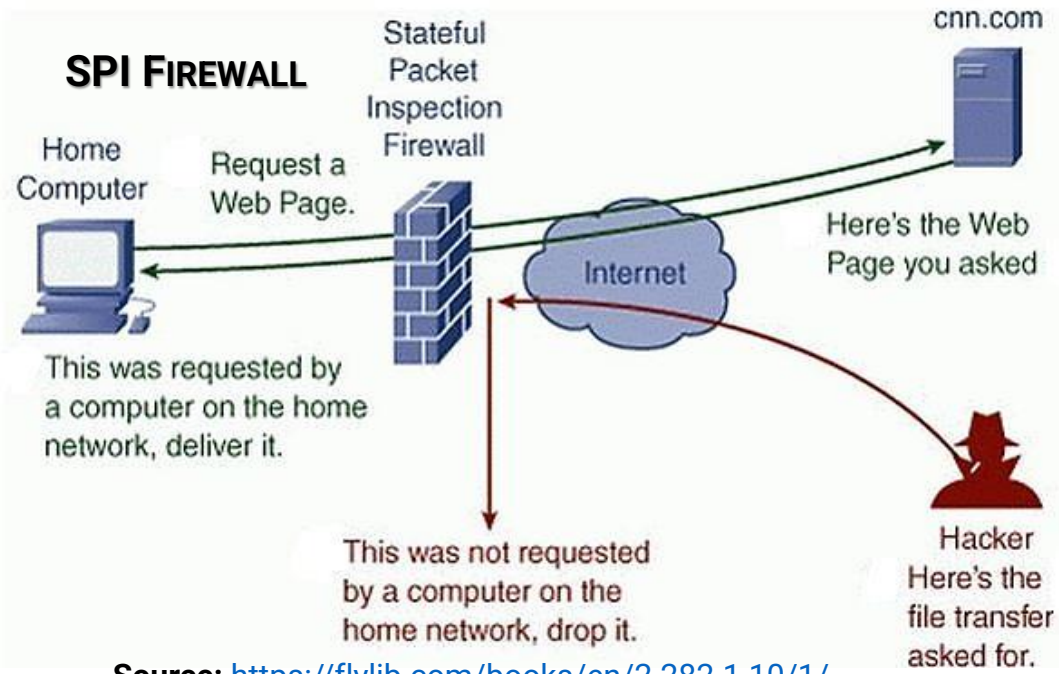
- **Checks this data of every received network packet**
  - Source and destination address
  - Protocol
  - Destination port number
- **Data is processed like this**
  - Packets are examined one by one, and dropped if they do not comply with its **ruleset**
    - No packet context (service, connection...) is used to decide if drop or accept packets
  - Ex.: You define a rule block `telnet` access
    - A PF firewall will drop **any** TCP packet destined for port 23, with no further consideration
  - Linux has an integrated PF firewall with multiple frontends
    - Ufw
    - IPSet (https://wiki.archlinux.org/title/Ipset)
    - Firewalld

Source:
https://support.huawei.com/enterprise/es/doc/EDOC1000154776/88191a64/packet-filtering-firewall



Firewalls: Stateful Packet Inspection (SPI)

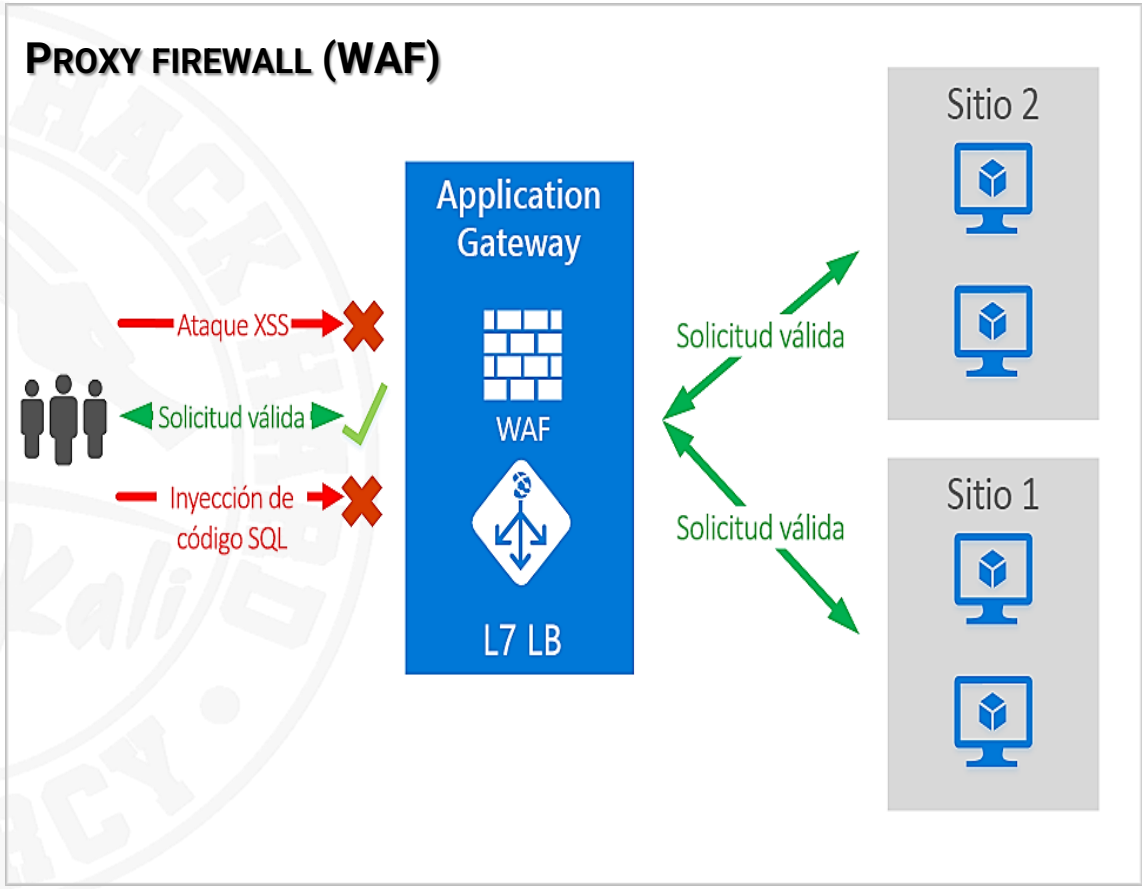
- **Dynamic packet-filtering firewalls with a table tracking all open connections**
  - When new packets arrive, the firewall compares information in each packet header to that state table
  - And determines **whether it is part of an already established connection** or not
    - If it is, then the packet is allowed through **without further analysis**
    - If not, it is evaluated according **to a rule set for new connections**
  - Advanced SPI firewalls allow powerful rules
    - Time, geo-based …
    - Also including **intrusion detection** (IDS)
    - Among other features…
  - ConfigServer is a free SPI firewall product
    - https://www.configserver.com/cp/csf.html
  - Some Linux distributions are just SPI firewalls
    - IPFire (https://www.ipfire.org/)
    - pfSense (https://www.pfsense.org/)



Source: https://flylib.com/books/en/2.282.1.10/1/

Firewalls: Proxy firewall

- **Provides application-layer filtering**
  - Examines packet **contents**
    - Differentiating valid requests, data…
    - And **malicious code** disguised on them!
  - Also known as
    - Application firewalls or gateway firewalls
    - Web Application Firewall (WAF) for web application protection specifically
  - E. g.: they could allow/deny specific `ssh` commands from particular users
    - A PF firewall can only control incoming requests between hosts
    - **They do not know about users**! (don't use packet data to make decisions): **a proxy firewall does**
  - `mod_security` is a very popular WAF
    - We will describe it in future slides

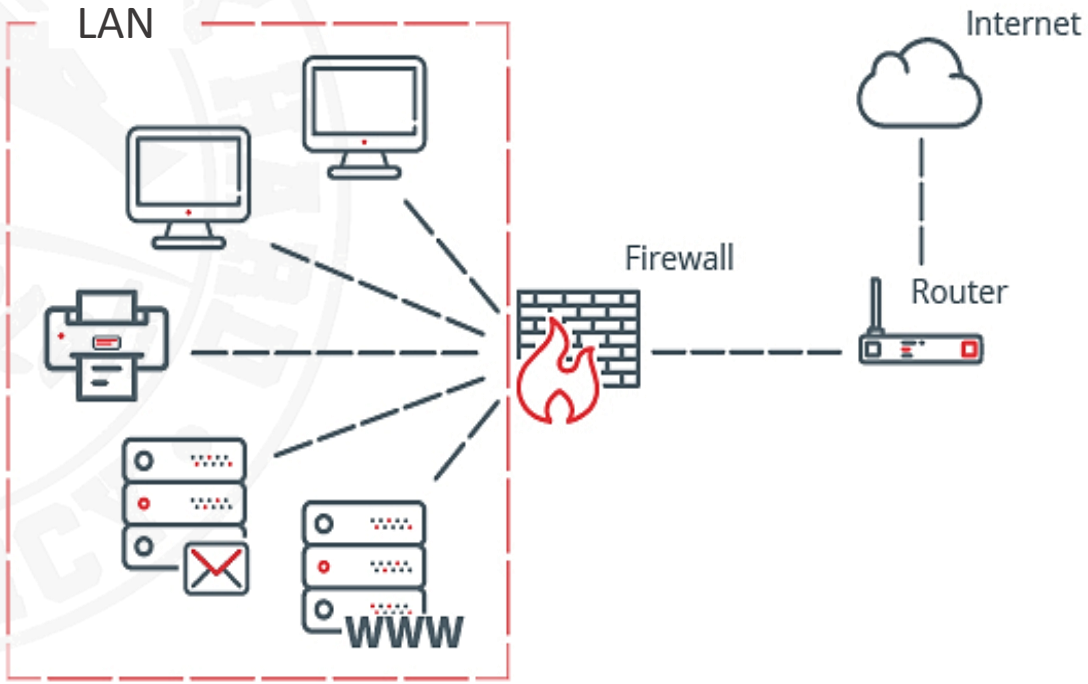


Source: https://learn.microsoft.com/es-es/azure/web-application-firewall/ag/ag-overview

Firewall rulesets

- A series of **filtering rules** indicate which types of communications are
  - **Allowed** (`ALLOW`)
  - **Rejected** (`REJECT`)
  - **Dropped** (`DROP`)
    - Rejected **without noticing the sender**
  - In the image connections are allowed from anywhere using IPv4 or IPv6
    - But only to ports 22 (`ssh`) or 80 (`http`)!

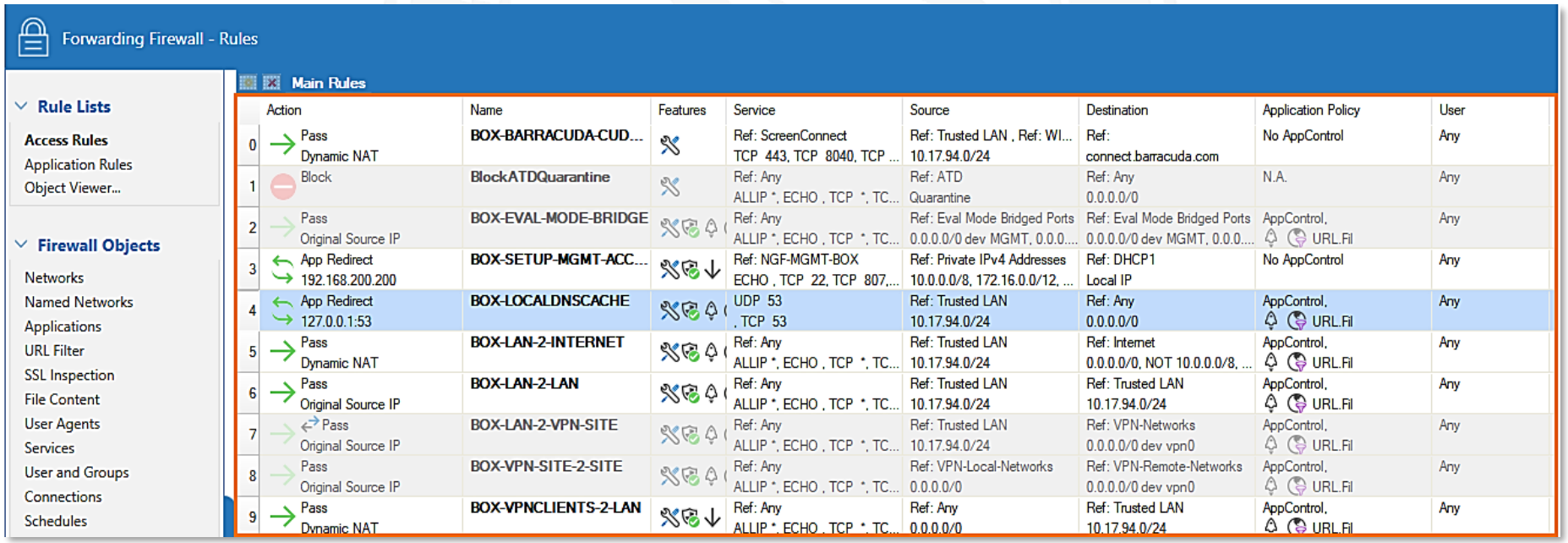
```
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       Anywhere
80                         ALLOW       Anywhere
Apache                     ALLOW       Anywhere
22 (v6)                    ALLOW       Anywhere (v6)
80 (v6)                    ALLOW       Anywhere (v6)
Apache (v6)                ALLOW       Anywhere (v6)
```



Source: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

Firewall rulesets: Examples

- **Firewall rules operate with triplets (IP, port, protocol):**
  1. "*This server can only be accessed by the IP 192.168.3.10, when connecting to the port 22 using TCP*": **only that machine can connect through SSH (22), rest of connections are dropped**
  2. "*TCP traffic between 192.168.10.0/24 and 192.168.25.0/24 are only allowed through port 3306*": **MySQL (port 3306) connections are only possible between any machine on the network *192.168.10.X* to any machine on the network *192.168.25.X***
  3. "*TCP/UDP traffic from any IP address are only allowed to the 192.168.59.15 address, port 443*": **Traffic from the internet can only connect to that web server using HTTPs (port 443)**

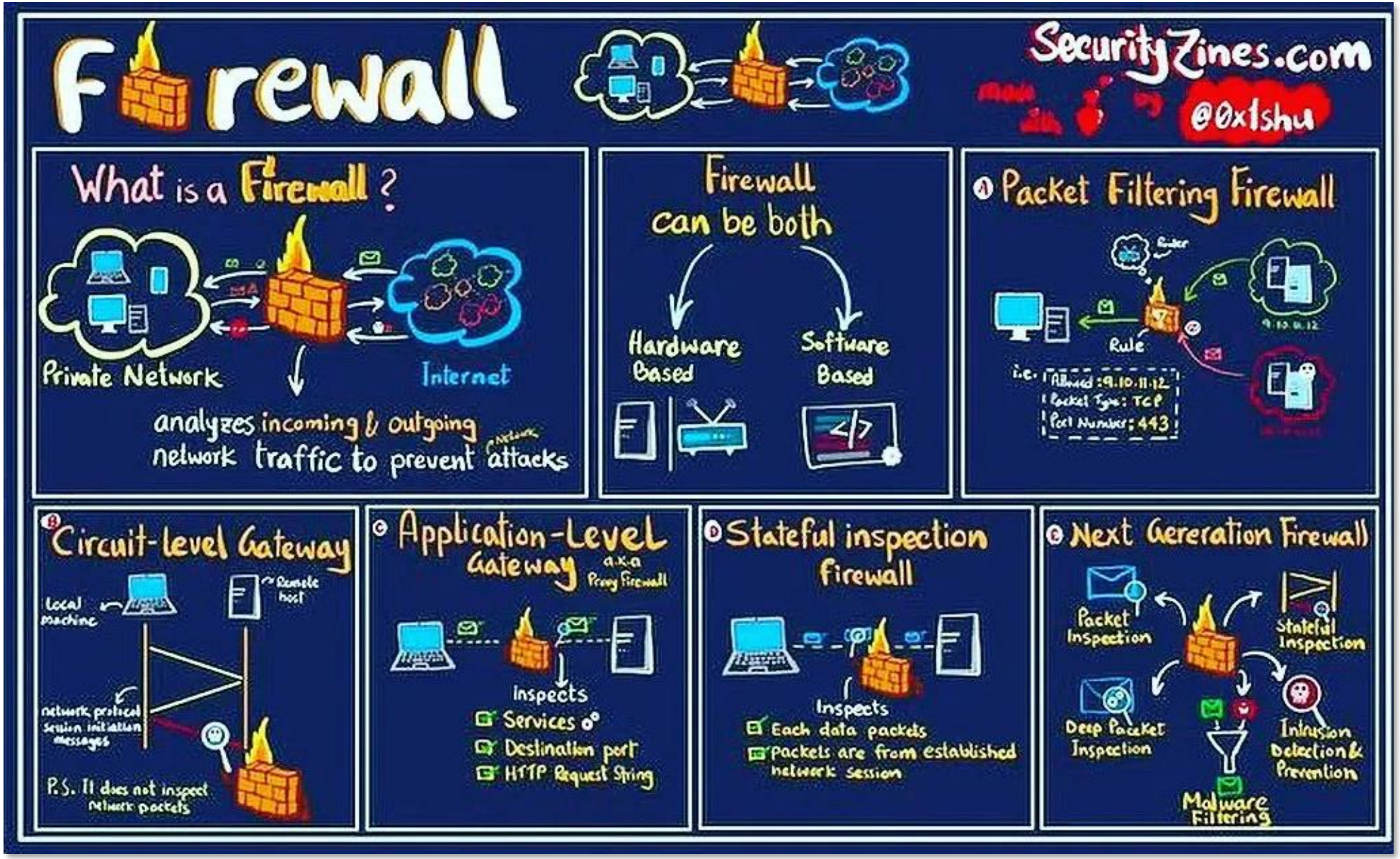


Source: https://campus.barracuda.com/product/cloudgenfirewall/doc/79463228/firewall-rule-list-interface-and-icons

Host firewalls vs Perimetral firewalls

- **Every device should have a firewall installed with adequate rules**
  - These are called **host firewalls** (e. g. iptables from ASR and its interface, ufw)
  - Normally with an ingress **allow list** approach
    - **All incoming traffic is dropped unless explicitly allowed**
    - **Outgoing traffic** (connections initiated on the own machine to the outside) **is normally allowed**
  - Rules 1 and 3 in the previous examples are typical host firewall rules
- **When firewalls can restrict connections between different networks or zones, they are called perimetral firewalls**
  - Typically, custom hardware or Linux distros that only implement firewall functionality
  - Usually drop all connections not explicitly allowed between two networks bidirectionally
  - They are a "**first line of defense**"
    - If broken, attackers will have access to the restricted network
  - Rule 2 on the previous example is a typical perimetral firewall rule

SUMMARY: FIREWALLS

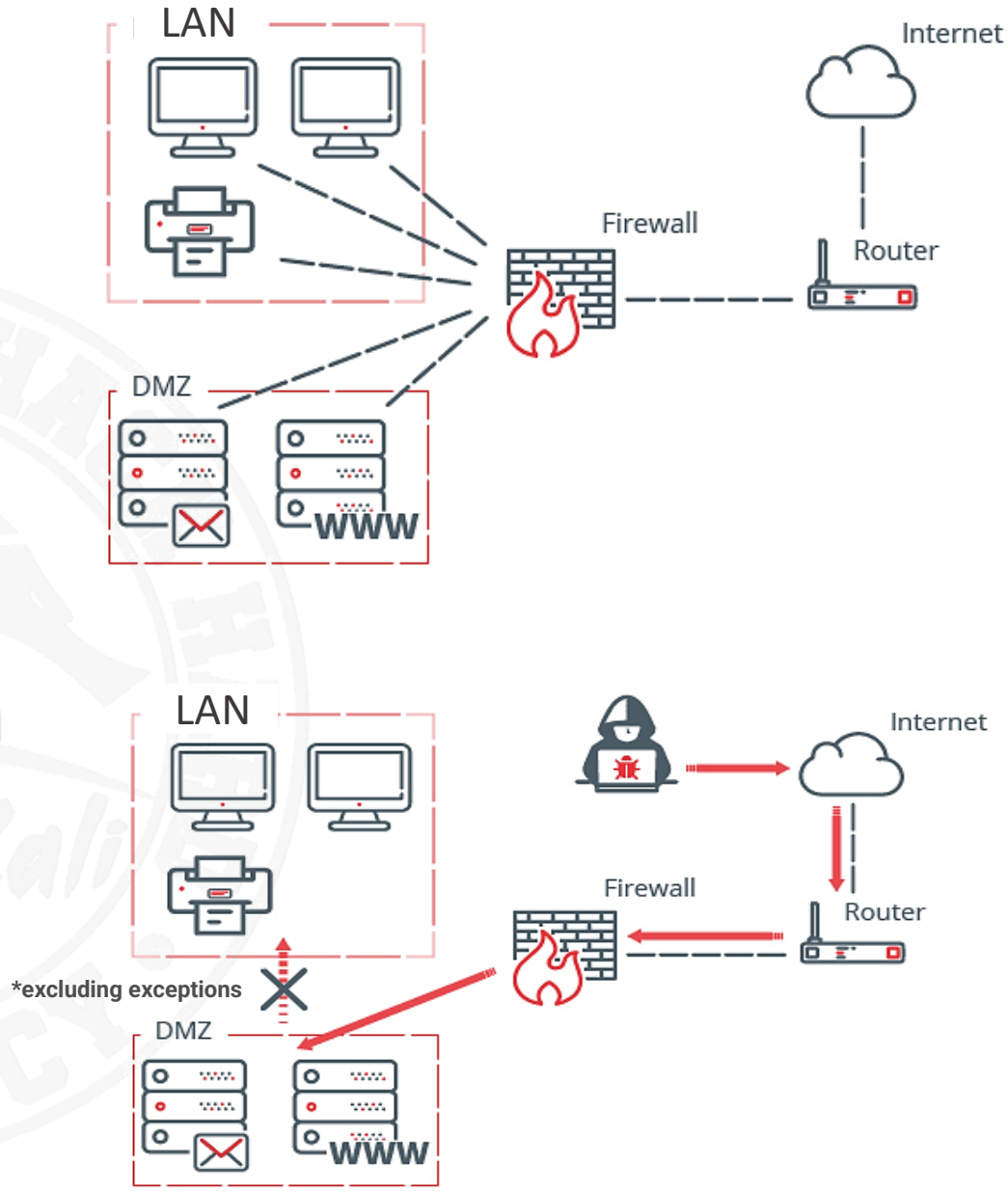


Next Generation Firewalls combine many functionalities into a single product. They are the most modern (and expensive), but understanding in detail what they do requires a specific networking course

DEMILITARIZED ZONES (DMZS)

Computer Security

- **Isolated network zones** on a company network
- Should hold every company resource accessible from Internet
  - Web servers, email servers…
- **Implemented via (perimetral) firewalls**
- Servers in a DMZ allow connections both **from Internet and the company's local network**
  - Connections from the DMZ to the local network are normally forbidden (**exceptions can be made**)
  - If a DMZ server is compromised, access to the important data in the LAN is very complicated
    - DMZ servers are the most likely to be compromised
    - They face the highest threat exposure

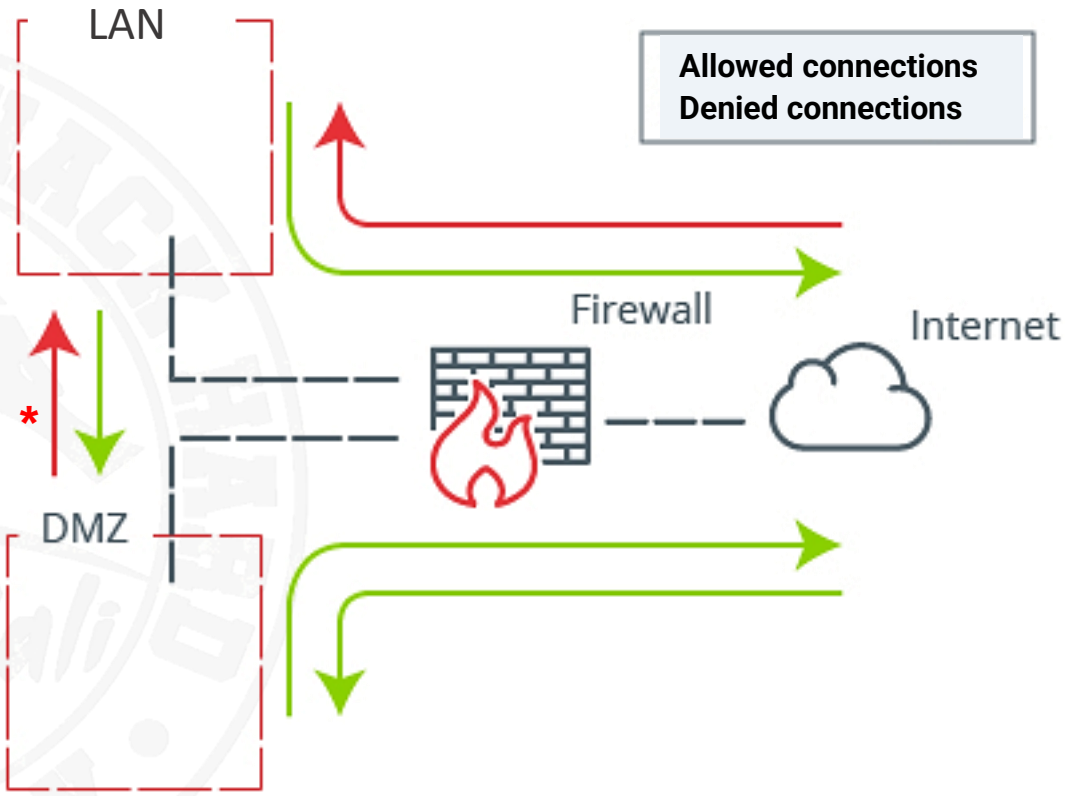


Source: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

Demilitarized zones (DMZs)

Source network	Destination network	Action
Internet	DMZ	Allow
Internet	LAN	Deny
DMZ	Internet	Allow
DMZ	LAN	Deny*
LAN	DMZ	Allow
LAN	Internet	Allow

*Access to certain ports, services or machines from specific machines can be allowed

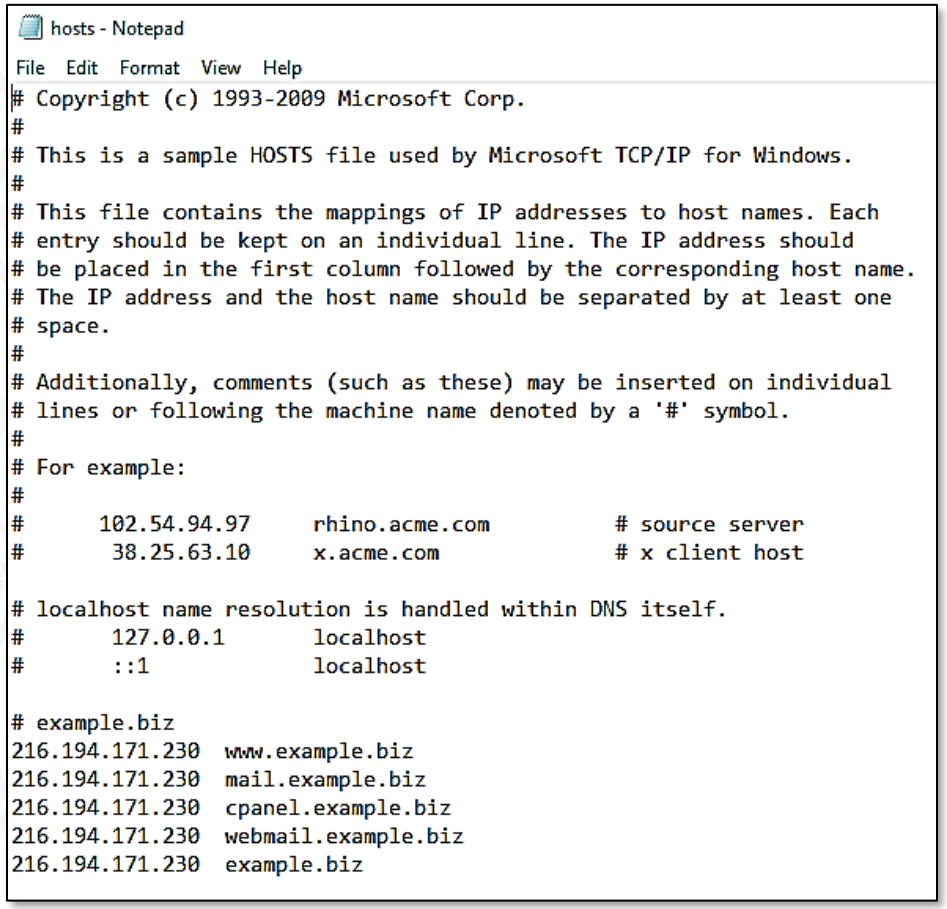


- **Firewalls are required to implement DMZs**
  - They establish network segments
  - Decide if allowing or disallowing communications between them
- **The table shows the recommended action with network traffic that come from and go to different network segments**

Source: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

HOST FILES

- **Local file for domain name to IP translation**
  - Described in ASR
  - Everything on this file has priority to be consulted and resolved
    - First than perform any query to a remote DNS!
    - If it has the name information, it is resolved, **and the DNS is not used**
- **Present in all major OS**
  - Linux: `/etc/hosts`
  - Windows: `C:\Windows\System32\drivers\etc\hosts`
- **Could be used to implement local DNS name filters in a simple way**
  - https://github.com/StevenBlack/hosts
  - This implements a malicious URL blocker for **ANY** program in our machine that makes remote connections



Think you've understood it all? Evaluate yourself!

?

- You can do the following
  - Understand that there are **many network protocols** and that each one has a function
    - And that a firewall can block per protocol, thus preventing all associated services
  - Know how to distinguish each **type of typical firewall**: PF, SPI and Proxy, host, perimeter...
  - Properly understand what **firewall rules** allow you to do
    - And the traffic control capability they give you
  - Properly understand the concept of **DMZ**
  - Understand what a **host file** is for and its relationship with DNS

< Go to Index

Source: Bing Chat AI

Network attacks >

Insecure Designs >

SNI >

SECURE NETWORK DESIGN PRINCIPLES

How to create a truly secure network

*Icons by Bing Chat AI

Departamento de Informática
Universidad de Oviedo

What are you going to find in this block?

- **In this block you will learn**
  - The different **types of typical network attacks**
  - How network **attacks are evolving** today
  - What action you can take **against them**
  - The **Zero Trust** concept
  - Conceptually **insecure network designs**

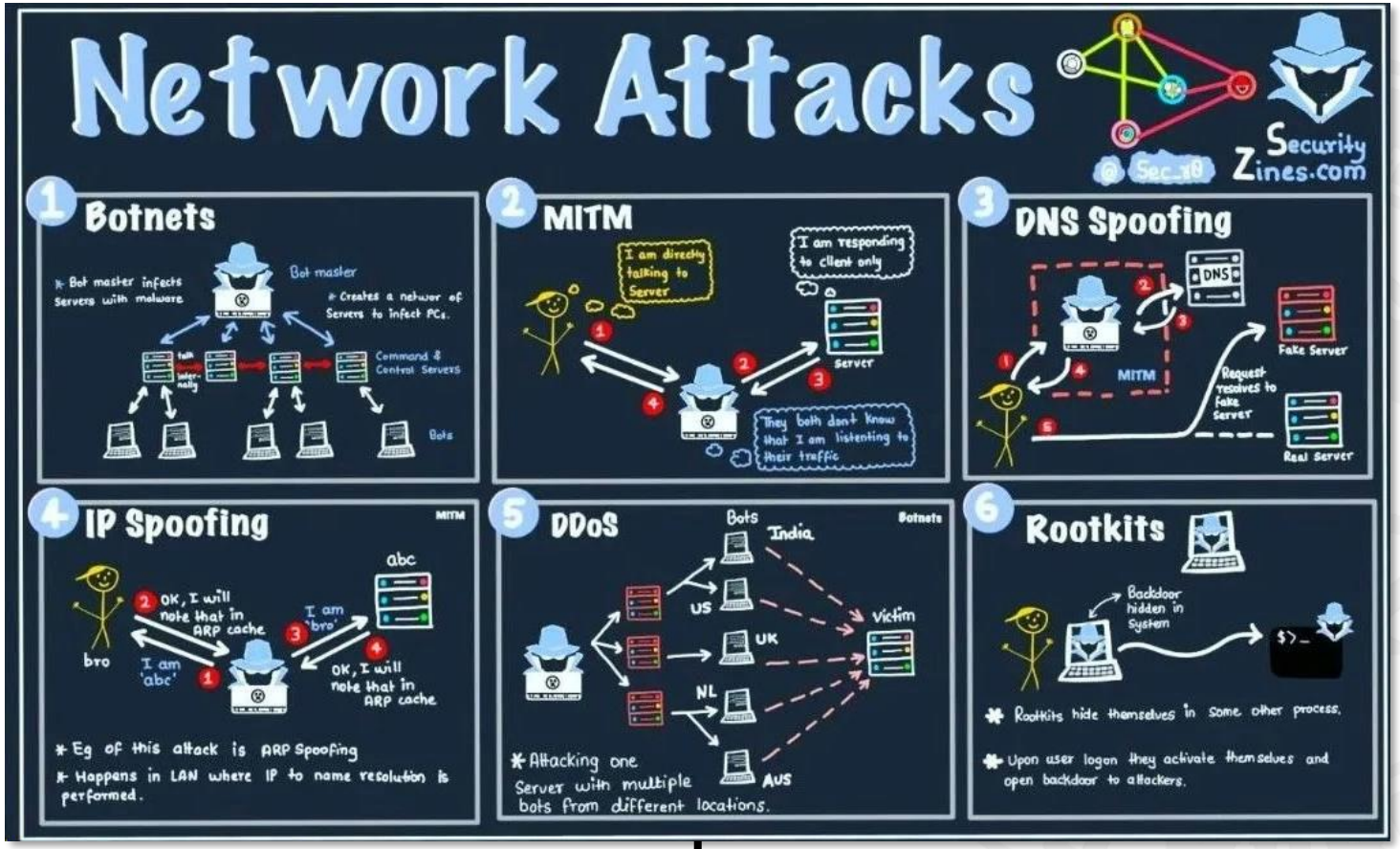
Network attacks

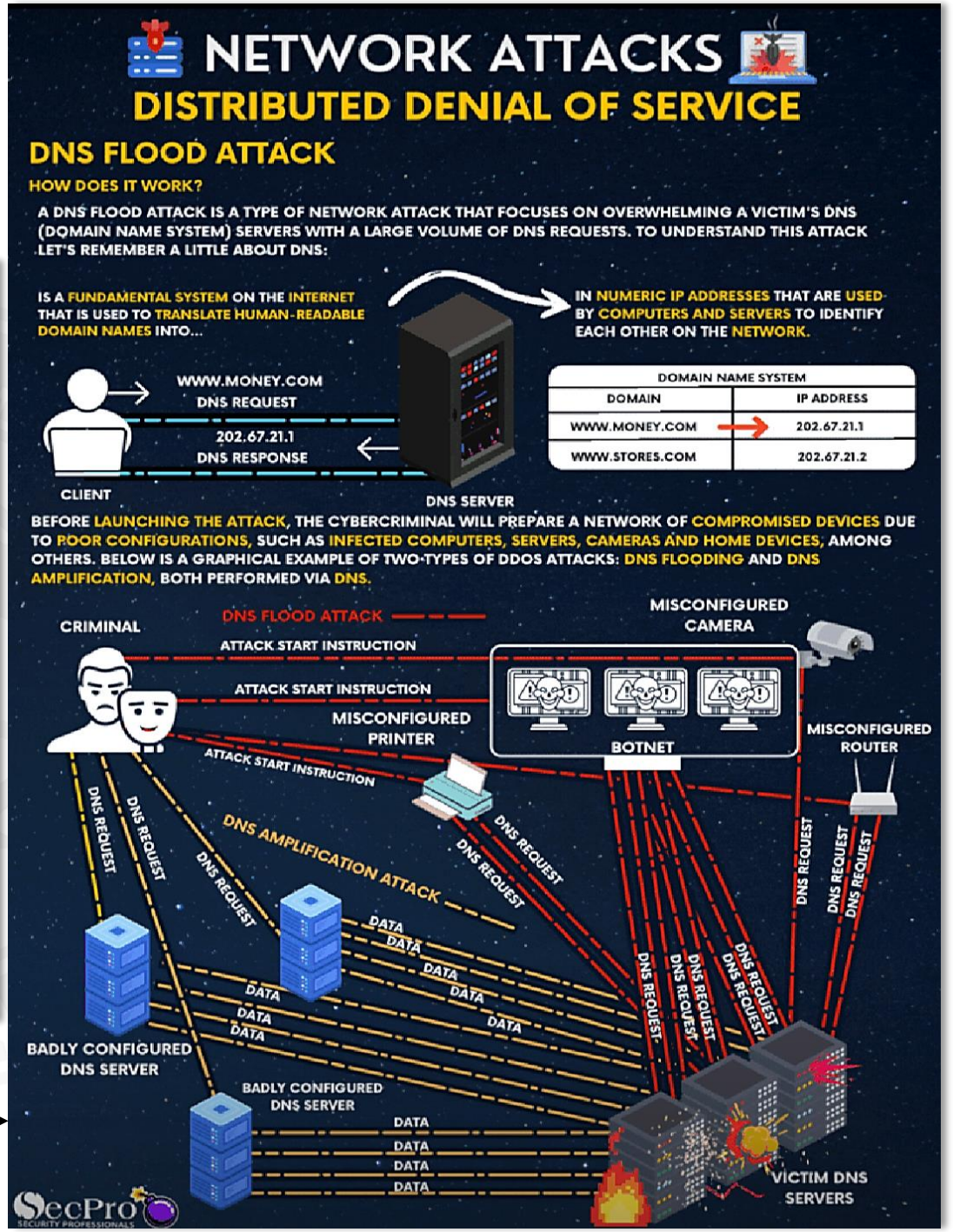
How networks are attacked nowadays

*Icons by Bing Chat AI

TRADITIONAL NETWORK ATTACKS

Computer Security





Network attacks today

- **Cyberattacks try to exploit the weakest link in a network**
- **Traditionally, the stronger defenses are placed on network perimeters**
  - The machines that manage the network traffic that connects with machines in other networks
  - Stateful firewalls, Intrusion Detection Systems (IDS), network access segmentation, VLANs…
  - Increased employee awareness about their existence and acceptable usage
  - The defenses of the "inside" machines (endpoints) **were weaker**
    - The paradigm was that perimeter defenses were enough
- **The network perimeter is no longer the primary target**
  - So, *what it is attacked nowadays network-wise?*

In an interconnected world, network perimeters usually have very strong defenses nowadays. Source: Bing Chat AI

NETWORK ATTACKS TODAY

Bring Your Own Device (BYOD) scenarios

- **Allowing employees to use personal devices for work may increase productivity**
- But gives attackers new entry points to a network
- Undetectable to perimeter defenses, as the device is directly introduced inside the perimeter

Remote work

- **Advances in technology (and the pandemic crisis) increased it**
- But it could reduce the effectiveness of perimeter security
  - Employee devices at home **are not covered by their defenses**…
- Connection via VPN bypasses most of these defenses
  - Client - network communication cannot be inspected
- Malware can then be “injected” from the client computer to the company’s network

Source: Bing Chat AI

Cloud applications

- **83% of enterprise workloads will move to the cloud in the 2020s**
- Without a way to secure connections to these applications, attackers will compromise the network
- ¡Regardless of the investment in perimeter cybersecurity!

NETWORK ATTACKS TODAY

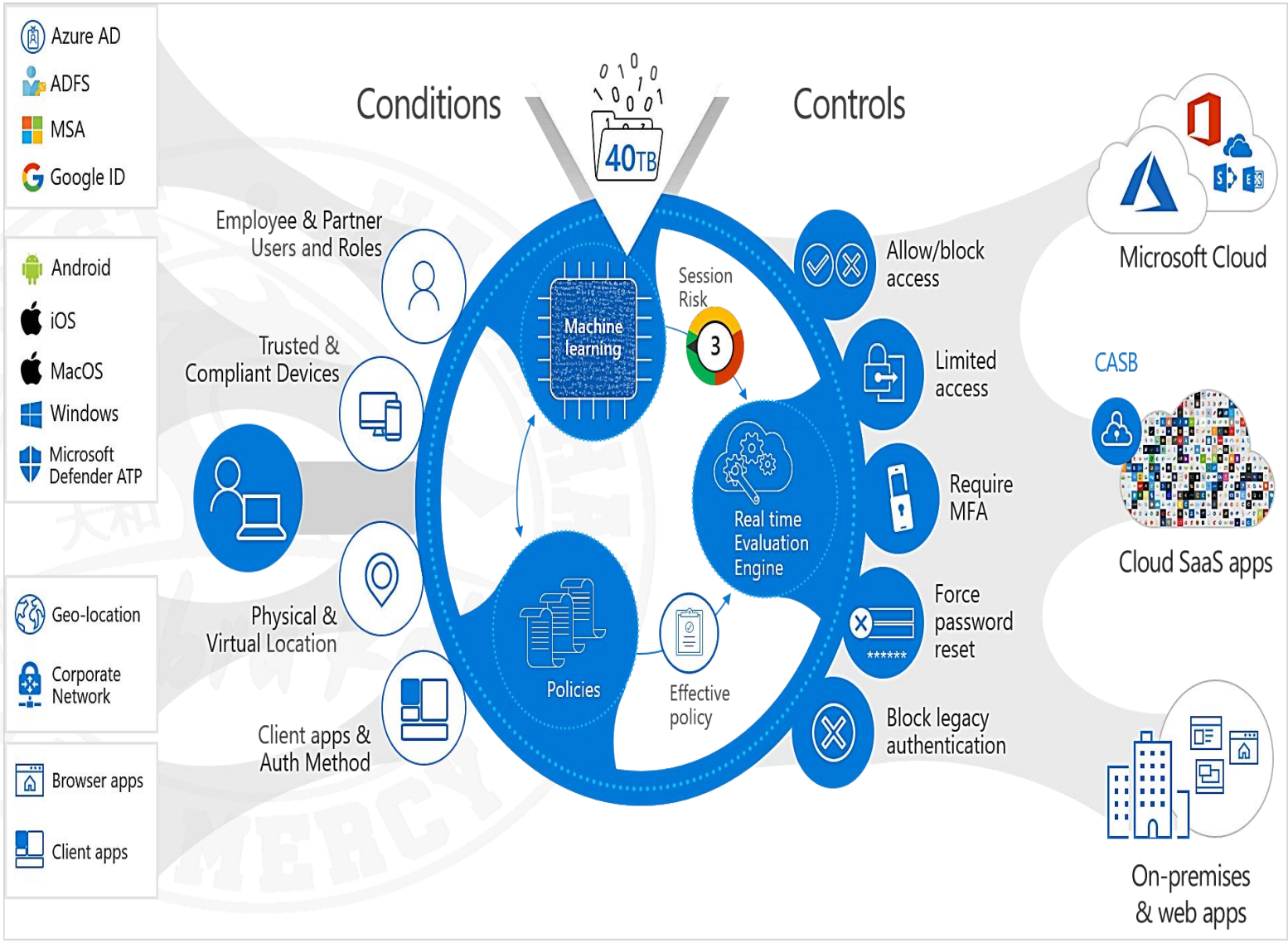
- **Attackers are no longer taking traditional approaches to getting into perimeter defenses**
- **Instead, they target endpoint (user / employee) devices**
  - Typically compromising vulnerable Internet browser activity
  - And using social engineering (combining with OSINT, **Group Works**)
  - The goal is to obtain employee credentials, gaining access to the company network
- **This is not an attack to the perimeter defenses**
  - It is an **impersonation** of a legitimate network user
  - Remember the Twitter 2020 bitcoin scam? https://en.wikipedia.org/wiki/2020_Twitter_bitcoin_scam
- **Detecting this class of attacks ("inside jobs") is therefore much harder**
  - Requires specialized and very advanced security tools
  - Like UEBAs, User and Entity Behavior Analytics - see **Topic 6**

Network attacks today: What to do?

- Use a **multilayered approach**
- **Don't get rid of existing security solutions**
  - Perimeter defenses are just one layer of the multi-layered approach, but not the only one anymore
- Apply a new model (**Zero trust**)
  - To both perimeter defenses and endpoint security strategy
  - Instead of trust all internal traffic, **validate each user and device accessing resources**
  - E. g.: a recent NASA case related to lack of zero trust in devices
    - https://www.bbc.com/news/technology-48743043
  - A popular implementation is Google's BeyondCorp: https://cloud.google.com/beyondcorp?hl=es
- **Assume that there will be new untrusted endpoints** accessing the network
- **URL filtering**
  - Restrict web traffic to prevent users from accessing known malicious sites
  - They could lead to compromised credentials and endpoints
  - Stateful perimetral firewalls (pfSense, IPFire…) can do that with a Squid proxy plugin (ASR)

¿ZERO TRUST?

- **Security system that only allow access to devices that comply a series of conditions**
  - Its user and role, network, geolocation, compliance status (**Topic 4**), used application...
- **Continuously check the devices (not only once)**
  - Using Machine Learning and real-time information (user behavior and device changes)
- **Grants access or forces user (re)authentication**



Source: https://www.infusedinnovations.com/blog/secure-modern-workplace/conditional-access/zero-trust-security-concepts-and-microsoft-365

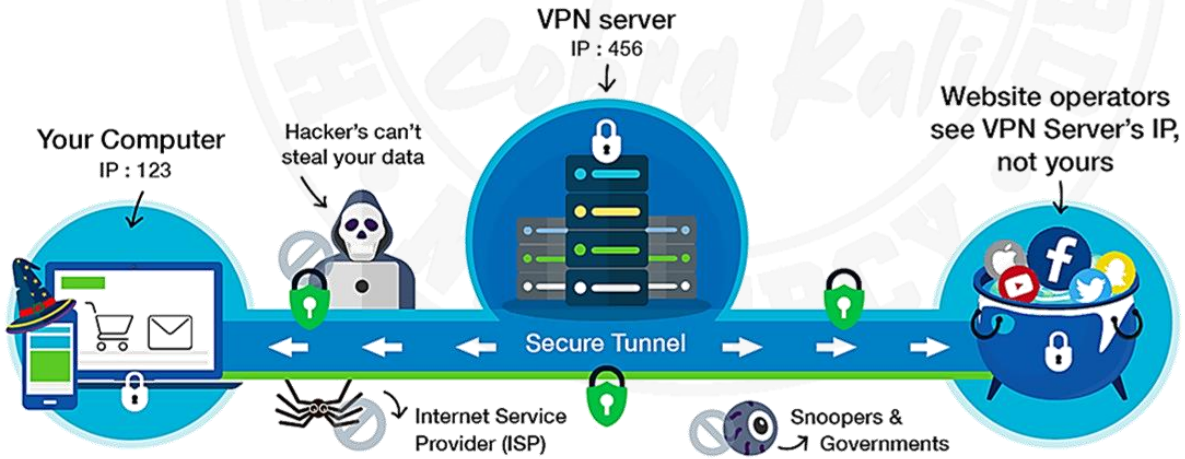
Network attacks today: What to do?

- **Facilitate endpoint anomaly detection**
  - Continuously monitor endpoints for suspicious activity
  - And send alerts in real time when potentially malicious behavior is detected
  - **EDR/XDR (Topic 3), Intrusion Detection Systems** (IDS), **Intrusion Prevention Systems** (IPS), **SIEM**…
    - E. g.: Wazuh, OSSEC Alienvault, Suricata, Snort …
    - **SIEM** systems that centralize log analysis to detect anomalous behavior
  - https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips
- **Isolate the browser (E.g.: A remote browser isolation solution, VMs…)**
  - Protecting users from zero-day attacks, unauthorized downloads, malicious content…
  - And in case of requiring **maximum privacy**, use ToR Browser (ToR network, **Topic 2**)
- **Protect access to services via firewall or other means**
  - https://www.tecmint.com/secure-linux-tcp-wrappers-hosts-allow-deny-restrict-access/

Network attacks today: What to do?

- **Control the remote access**
  - Secure remote connections with secured gateways, VPNs…
    - Do not confuse this with a traditional VPN service, that only anonymizes and protect the connection source
    - We need **a VPN between the employee and the organization** (like the Uniovi one! ☺)
    - Or a **peer-to-peer (P2P) VPN** that connects only the devices we want to each other, like a LAN
    - **Never expose RDP, the Remote Desktop Protocol**
  - Implement two-factor authentication for all users and devices
  - Log all remote sessions
  - Implement a highly secure remote access solution and policy
    - https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/9638-como-implantar-una-politica-de-acceso-remoto-seguro.html

Source: https://blog.360totalsecurity.com/en/how-vpn-works



A peer-to-peer VPN, such as ZeroTier, is an ideal solution in many scenarios by giving secure access + full control of the VPN service + ease of installation and use. The other option is to install your own VPN server (purchased, using Wireguard…)

➢ Exercises **L7B4_VPN, L7B4_VPNP2P**

Insecure network designs

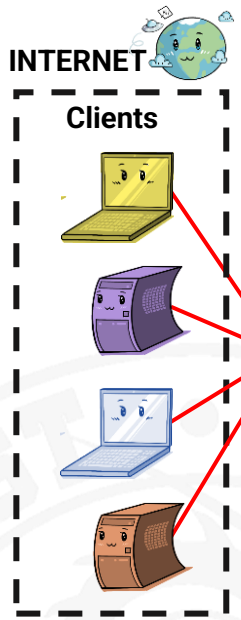
How to NOT design a network

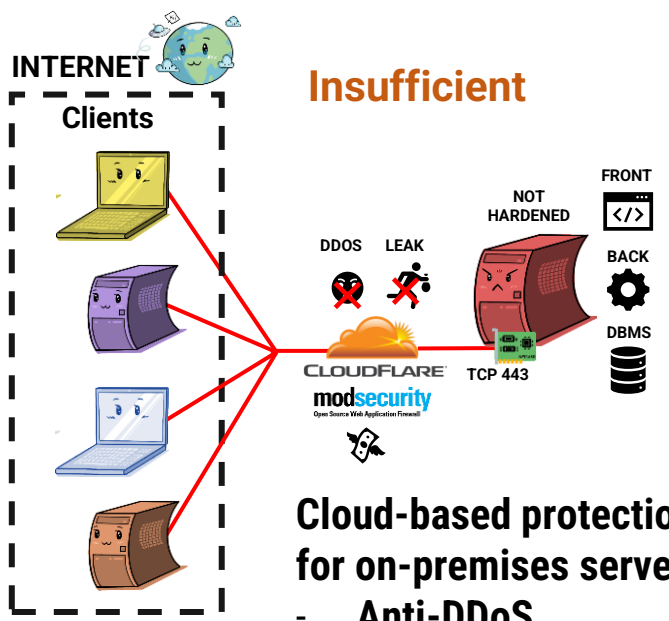
*Icons by Bing Chat AI

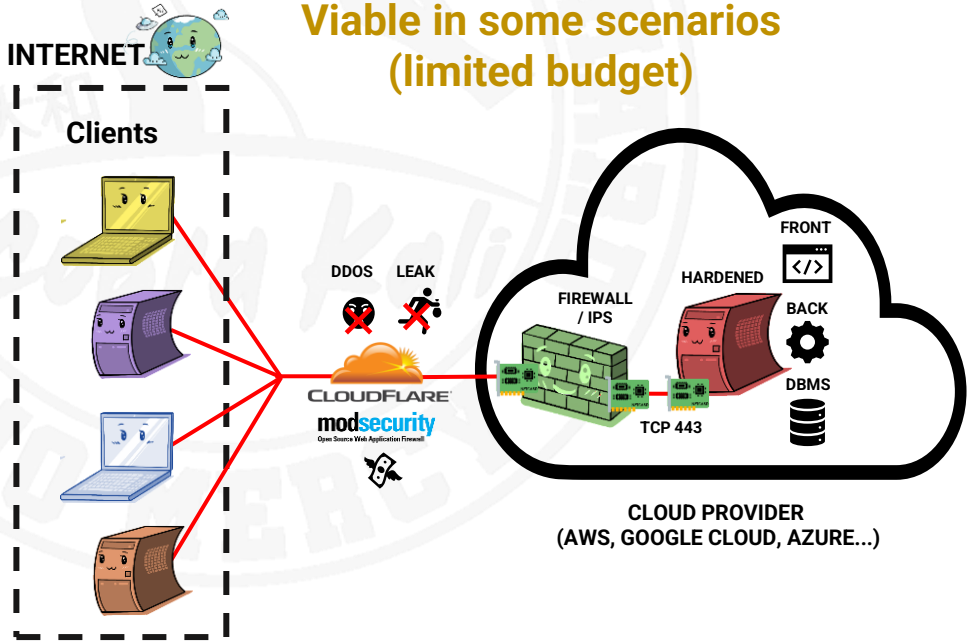
Inadequate network designs

Computer Security

- Adding security to network infrastructures turn them more complex
- Solutions with a single server holding every service (front, back, DBMS,…) are inadequate
  - Single Point of Failure due to no network segmentation
  - No machine specialization that allow optimized services
  - Cloud-based protection only fixes part of the problems (Ex.: Cloudflare)
  - Cloud-based hosting is insufficient, even if paying premium services
  - Application code must be created with security practices (Topic 6)







* Logos are property of the corresponding companies. Icons from *PowerPoint*

Moving to the cloud: "Cloud native" is not a "miracle cure"

- **Cloud solutions may be very expensive if not properly scaled or managed**
- **And they may also have security problems**
  - The code of the software hosted in the cloud must follow a methodology/rules for **secure application development** (**Topic 6**)
  - The **database** may be badly configured or may not adequately protect sensitive information
  - We can unconsciously **"break" the security baseline** that the cloud provider implements if we make inadequate platform modifications
    - We need to know what we are doing, even when the cloud manages most of it
    - Like deploying CIS-hardened machines (**Topic 4**) and modifying some of their security controls
  - We must know how to properly arrange / setup **communications** between the different machines we put on the cloud, using the vendor tools
    - We must study the available options to take advantage of the cloud provider features
  - We might have something in production that we **don't really/fully understand or control**
    - **Cybersecurity knowledge is needed** to make the most of the tools

TOWARDS A REAL SOLUTION

- **The security level of our infrastructure depends on**
  - **Budget** (strong security require strong investments)
    - To implement network segmentation (not single servers, multiple specialized ones in different networks)
    - For good hardening procedures (**Topic 4**) and security appliances (EDR/XDR, firewalls, IDS, IPS, SIEMs…seen later)
  - Ability to handle infrastructures of different complexities
  - Criticalness of data/services
  - Legal regulations/certifications to be met, software policies compliance, ISMS implementation, and security audit reviews (**Topic 4**)
- **Let's see an example of a secure (and complex) infrastructure, the SNI**
  - Secure Network Infrastructure
  - All or part of these elements can be deployed in a cloud provider
  - To save management cost / money (private, public, hybrid clouds)

Think you've understood it all? Evaluate yourself!

?

- **You can do the following**
  - *Be clear that, while perimeter defenses are still essential, modern attacks are focused on preventing them from being able to examine the traffic that originates an attack*
    - *And to do this, they attack users, external devices connected via VPN, cloud resources, or any means that allows bypassing the perimeter defenses*
  - *Understanding the concept of Zero Trust*
  - *Understand the importance and the means to detect anomalies*
  - *Understand the importance and the means to isolate browsing or preserving your privacy*
  - *Understand the difference between a traditional VPN service, an organization's VPN, and a P2P VPN*
  - *Be clear that having all services on a single server is an inadequate network design, and that the design must fit the available budget*

Secure Network Infrastructure (SNI)

How to design a strong network architecture

*Icons by Bing Chat AI

Source: Bing Chat AI

LAN Administración >

Seguridad Extra >

What are you going to find in this block?

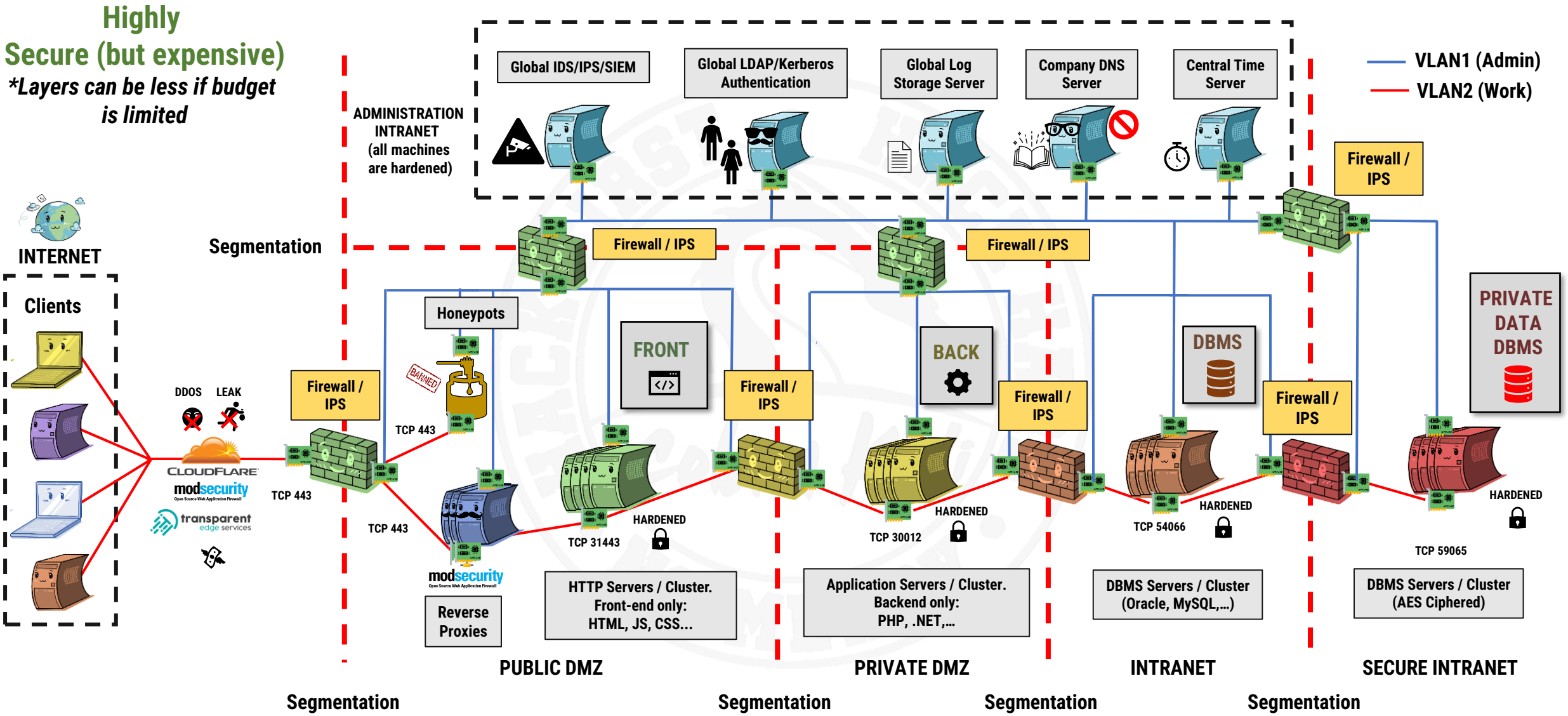
- **In this block you will learn**
  - How to design a **highly secure network** infrastructure
  - The enormous **importance of layered** isolation for security
  - The concept of **Honeypot**, **CDN**, and **VLAN**
  - The importance of having a fully isolated infrastructure **management network**
    - And its main components
  - The Importance of endpoint **surveillance** with IDS/IPS
  - And related to this, that of **correlating all the events** produced
    - And **analyze** them with a SIEM and their relationship with a SOC

SECURE NETWORK INFRASTRUCTURE (SNI)

Computer Security

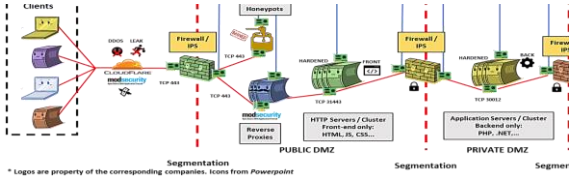
Highly Secure (but expensive)

Layers can be less if budget is limited



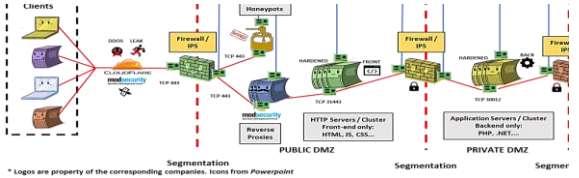
* Logos are property of the corresponding companies. Icons from *PowerPoint*. *This infrastructure is derived from:* https://pciguru.files.wordpress.com/2013/12/200511-theultrasecurenetworkarchitecture.pdf

SNI: Main components



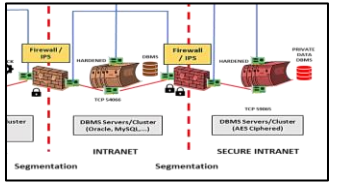
- **A secure configuration baseline for all servers**
  - Infrastructure OS and services are configured and secured using an adequate **security framework** (E. g.: ISO 27001, **Topic 4**)
    - Based on validated security control lists (CIS, STIGs, …)
    - Using stricter security policies for public-facing servers
  - Application code follows **secure code development methodologies and practices** (**Topic 6**)
  - Properly secured DBMS, with appropriate role and permission systems
  - **Critical role servers do not accept interactive user behavior**
    - You cannot use a machine in which you view webmail, browse, watch videos…for these services
- **"External" network and application firewalls (proxy firewalls-WAF)**
  - Reduce threats from application-based attacks (code injections, etc.) that network firewalls cannot detect
  - You must also use individual **host-based PF firewalls**, only opening authorized ports, for each server: `ufw`, `firewalld`

SNI: Main components



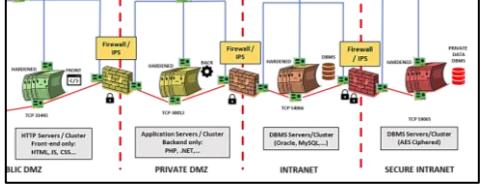
- **Two double-firewalled (SPI/NGFW) DMZs**
  - **The public one faces Internet, the other is private**
  - Servers in the **public DMZ** contain **application UI logic only**
    - And are isolated (perimetral SPI firewall) from the systems with the application logic in the private DMZ
  - Servers in this **private DMZ** contain the **application/business logic**
    - Server-side code, PHP, ASP, …
    - And links to internal systems for additional processing capabilities
  - This allows more detailed rules for accessing the application logic
    - Better preventing unauthorized calls to functionalities
    - So, application-based attacks will have a much more difficult time to work!
- **Two double-firewalled internal LANs**
  - **The internal LAN** containing the employee-accessible servers
    - And systems that do not store sensitive information
  - **The secure LAN**, containing servers with **encrypted and sensitive information**
    - That could be used for identity theft or other frauds (credit card numbers, checking account numbers, etc.) and hence **its protection is critical**

SNI: Main components



- **A common service-port placement policy**
  - Default ports for HTTPS (`tcp/443`) are only used in the public DMZ
    - **HTTP usage must be removed in every part of the infrastructure**
    - We want our public-facing services to be reachable in the usual places
  - Web services must use **ALWAYS** an adequate encryption
    - TLS 1.3 if possible
  - **Non-standard TCP and UDP ports will be used** for all other connections to necessary services
    - Reduces the possibility of outside attackers accidentally identifying services and information assets
    - A lot of attacks are fully automated and only look for standard service ports
- **All unused ports and protocols need to be closed**

SNI: Firewalls

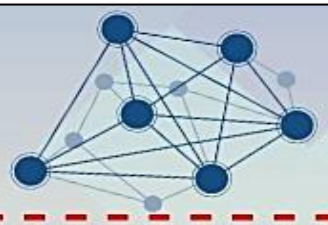


Computer Security

- The configuration of the **network firewalls** is critical
  - **Rules** must be configured to **strongly restrict and control** inbound and outbound traffic
    - Forwarding ports to other machines to achieve the best possible **network isolation**
  - Requires a mechanism to identify servers fulfilling a critical role (i. e. static IP assignment)
  - For example, **the public DMZ network firewall…**
    - Will allow only inbound and outbound TCP traffic to the respective IP addresses of the public-facing HTTP servers (reverse proxies / honeypots)
    - The reverse proxies totally hide the underlying network architecture
  - **Between the public DMZ and the private DMZ…**
    - Only port 30012 should be open
    - Restricting their communications to the IP addresses of the servers involved in our example
  - **Between the private DMZ and the internal LAN…**
    - Only ports required to communicate to the various servers should be open
    - And restricted to their specific authorized origin IP addresses
  - Likewise, **between the internal LAN and the secure LAN…**
    - Only the port necessary to gain access to the encrypted DBMS server should be open
    - And restricted to allowed IP addresses in the internal LAN

➢ Exercise **L7B1_FWFORWARD**

HONEYPOTS



What is a Honeypot?

by @SecurityGuill

What is a Honeypot?

- A Honeypot is an "**under surveillance**" system that is **exposed voluntarily** on the internet.
- The goal is to expose devices on the internet (often they are virtual) and to **monitor** them to retrieve information about **attackers**.
- Normally, these are systems to which people should **not have access**, this means that any **traffic arriving on a Honeypot is considered suspicious**.

2 Types of Honeypot

- Honeypot with **Low interaction**: consist of **emulating operating systems** and **services**. Activity is therefore limited to the degree of emulation offered by the honeypot.
- Honeypot with **Strong interaction**: they are different because they often involve the use of **real operating systems** and **real applications**.

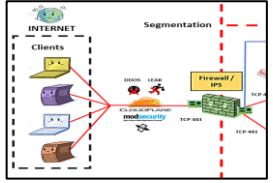
- The risks are many since our device is intended to be **compromised**. One of the advantages of this solution is that it's possible to obtain **more information** about attackers.

Application areas

- The use of a Honeypot can be applied in **two** different environments.
- **Production environment**: the main objective of a production honeypot is to **verify that the security measures are applied**, improve the protection of their network, discover vuln in their applications...
- **Research environment**: the goal is to collect as **much information about attackers** and their procedures. Some data collected: **network traffic**, **files sent** (malwares), **dumps**, what **ports** are most attacked, which **countries** come the attacks...

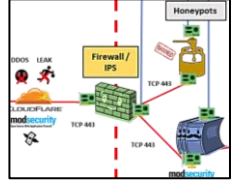
Follow @SecurityGuill on Twitter for more about Infosec / Cybersecurity

SNI: Content Delivery Network (CDN)



- **Cloud service providing an extra security layer**
  - Requests to the perimeter firewall are filtered by CDNs like CloudFlare or TransparentEdge
- **Provide very advanced security features**
  - Comprehensive and powerful **DDoS protection**
  - Ensures **proper https connections**
  - **Web Application Firewall:** `mod_security` with a custom ruleset
    - Protecting against XSS, SQL Injection, XSRF, parameter poisoning, private file filtering…
    - And data leaks due to misconfiguration
  - **"Collective intelligence"** techniques to prevent new threats
  - Reputation-based protection/blocking against potentially **malicious client connections**
  - Protection against **comment spam**
  - Protection against **hotlinking or content stealing**
  - …
- **Even by only hiring free services we obtain a security benefit**

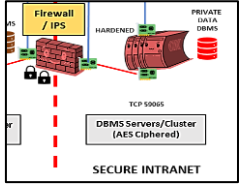
SNI: PUBLIC DMZ



- It is accessible from the outside, but not every machine it holds
  - **Reverse proxies + WAF**: **The only machines** reachable behind the perimeter firewall
    - Distributes requests to the appropriate machines, according to its type / port inside the public DMZ
    - This allows you to **hide the type and number** of servers deployed in the public DMZ
    - **A WAF should be installed on these servers** (unless we paid a CDN for it)
    - Other security measures could be implemented in these servers
      - Blocking repeated unsuccessful access attempts for popular services: Fail2Ban
      - Blocking port scanning techniques, like the ones implemented by `nmap`: PortSentry
  - **Honeypot**: Captures attack attempts by users or automated attack tools, blocking their IPs
    - We can derive plain-http connection attempts to the honeypot
    - **Real servers must use encrypted connections always!**
      - Real clients will not attempt to downgrade HTTPs to HTTP
      - It is an indication of potentially malicious activities
    - Opening ports associated to known vulnerable servers, but putting the honeypot behind them
      - There is software to block scan attempts to these "trap" ports: PortSentry
    - More resources about honeypots: https://github.com/paralax/awesome-honeypots

➢ Exercises **L7B2_FAIL2BAN, L7B2_PORTSENTRY**

SNI: SECURE LAN

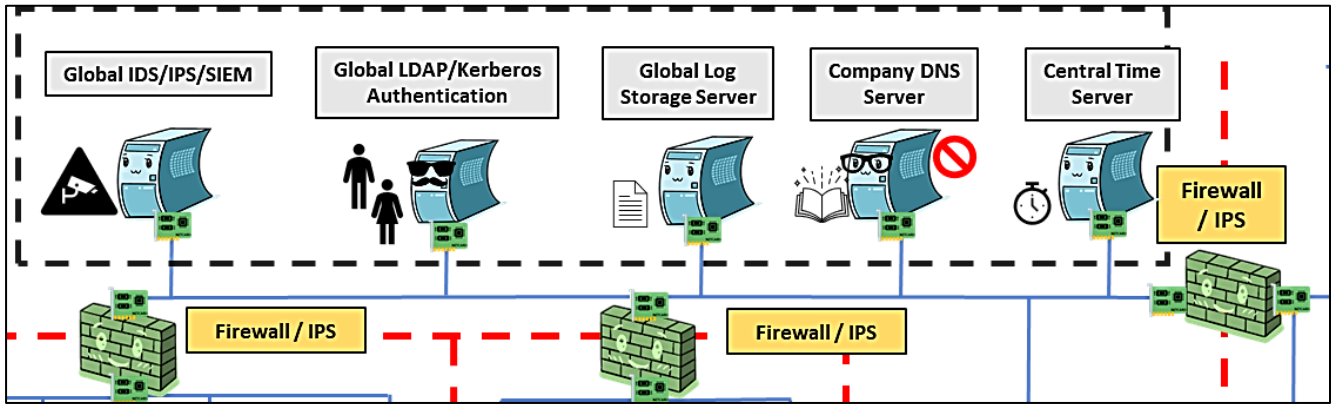


- **Servers located in the secure LAN implement an additional level of security by storing encrypted information only**
- **The key to securing servers in this LAN is that information…**
  - Comes in only from authorized places (thanks to the firewall)
  - Is encrypted and stored using a strong ciphering method (AES, see **Topic 2**)
  - Can only be retrieved through **a very strict security policy**
- **An extremely limited number of systems, administration staff, and applications have access to these servers (and the secure LAN itself)**
  - Application processes with access to these servers **are restricted and monitored**
    - To ensure that only appropriate information flows are processed
    - When access is approved, information is decrypted for processing needs
  - Those information outflows are severely restricted, documented in detail, and limited by firewalls
  - Also monitored and approved by management **to comply with the current law**

Think you've understood it all? Evaluate yourself!

?

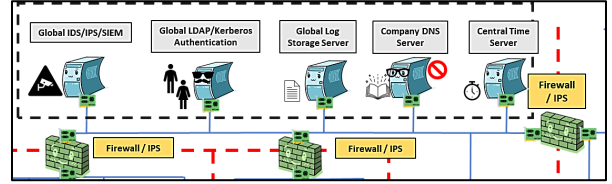
- **You can do the following**
  - *Understand that the key to create a highly secure network design is network segmentation, isolating different functionalities in several layers*
  - *Be aware that a first step is to separate the frontend from the backend in a web service*
  - *Understand when it would be worthwhile to separate the data stored by the application into two separate networks*
  - *Understand that we must place many security measures at the points of the infrastructure that are exposed to the Internet, such as WAFs, CDNs, professional firewalls...*
    - *And understanding the functionality of each of them*
  - *Understand why any service that is not exposed to the Internet should be offered on non-standard ports*
    - *And that all other ports should be shut down*



Administration LAN of the SNI

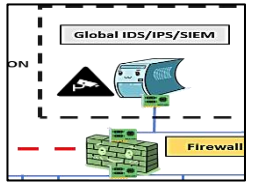
*Icons by Bing Chat AI

SNI: Administration LAN



- All components are supervised via a management / monitoring system
- Implemented in a protected **administration LAN**, composed by
  - Intrusion Detection/Prevention System(s) (IDS/IPS)
  - Security Information and Event Management (SIEM)
  - Domain Name Services (DNS)
  - Kerberos servers (authentication)
  - Time server(s)
  - Centralized system log server(s) (`syslog`)
- All these servers are also firewalled from the DMZs and the secure LAN
  - To allow better control and protection

GLOBAL IDS/IPS/SIEM



- **This architecture has properly managed network-based (NIDS) and host-based intrusion-detection system(s) (HIDS)**
  - **NIDS** (Suricata, SNORT, Maltrail…) **monitor critical DMZ subnets and secure LAN**
    - This allows detecting any network-based attacks or unexpected network traffic anomalies
    - Additional NIDSs can be placed on other network segments, but this may result in significant amounts of tuning to minimize false positive alerts and other issues
  - **HIDS** detect file changes, brute force attacks, etc., on the servers they should be installed
    - All servers in the DMZs and in the secure LAN
    - Any servers that process sensitive information in the internal LAN
    - Examples of popular HIDS software are: Wazuh, OSSEC, AIDE, Tripwire, Maltrail…
- **NIDSs and HIDSs send information to an intrusion-detection console system in the management LAN for tracking and monitoring**
  - For example, Alienvault OSSIM (SIEM) is an event management system able to do that

➢ Exercises **L7B3_IDSMALTRAIL, L7B3_WAZUHSCAN**

IDS/IPS

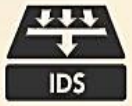
What is IDS & IPS ?

by @ SecurityGuill

What is an IDS?

- An IDS (**Intrusion Detection System**) **analyzes** and **monitors network traffic** for signs that attackers use a **known cyber threat** to **infiltrate** or **steal data** from your **network**.

- IDS systems **compare current network activity with a database of known attacks** to detect various types of behaviors such as security policy violations, malware and port scanners.



- With IDS systems, it is necessary for a human or other system to **take over to review the results** and **determine the actions to be implemented**, which can be a full-time job depending on the amount of traffic generated by day.

Common points

- **Both read network packets** and **compare the contents to a database of known threats.**

Why you need IDS/IPS Technology

- **Conformity reasons** (To prove that you have implemented the necessary means to protect your data)
- To **protect your data** (especially if you collect a **large amount** of **personnal data**)
- **Automation**

What is an IPS?

- An IPS (**Intrusion Prevention System**) acts in the same area of the network as a **firewall**, between the outside world and the **internal network**.

- IPS systems proactively **reject network packet** based on a **security profile** if these packets represents a **known threat**.

- The goal of the IPS is to **capture dangerous packets** and **remove them before they reach their target**.
- It is more passive than an IDS and simply requires **regular updating of the database** to incorporate **new threat information**.

Follow @ SecurityGuill on Twitter for more about Infosec / Cybersecurity

IPS vs IDS

IPS	IDS
IPS is a control system which accepts and rejects a packet based on the ruleset.	IDS is a detection and monitoring tool which do not take action on their own.
IPS	IDS
IPS requires that the database to regularly updated with new threat data.3	IDS requires human or another system to examine results.
IPS	IDS
It should be placed after the firewall device in a network.	IDS should be placed after the firewall.
IPS	IDS
IPS provides detection and reaction support.	IDS provides decoupling detection and reaction functionalities.
IPS	IDS
In IPS, configuration mode is inline mode or as end host.	In IDS, configuration mode is the inline mode, generally on layer 2.

www.educba.com

IDS/IPS

Computer Security

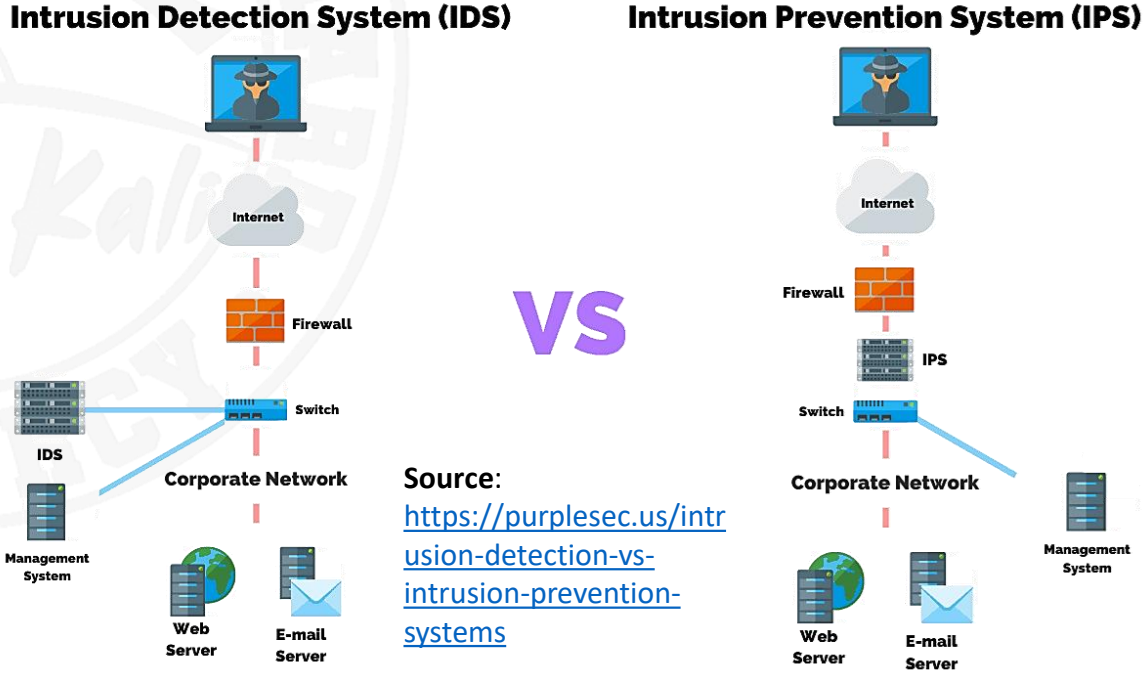
- **Serious computer / infrastructure security requires these systems**
  - An IDS uses a **reactive** approach: Warns, but do not block about what it detects
  - An IPS uses a **proactive** approach: Blocks what it detects
- **Both can (and should) be combined on a network**
- **Require "training" and adaptation to each context to prevent false positives**
  - You need to progressively adapt them to not to interfere with legitimate traffic

IDS Vs IPS

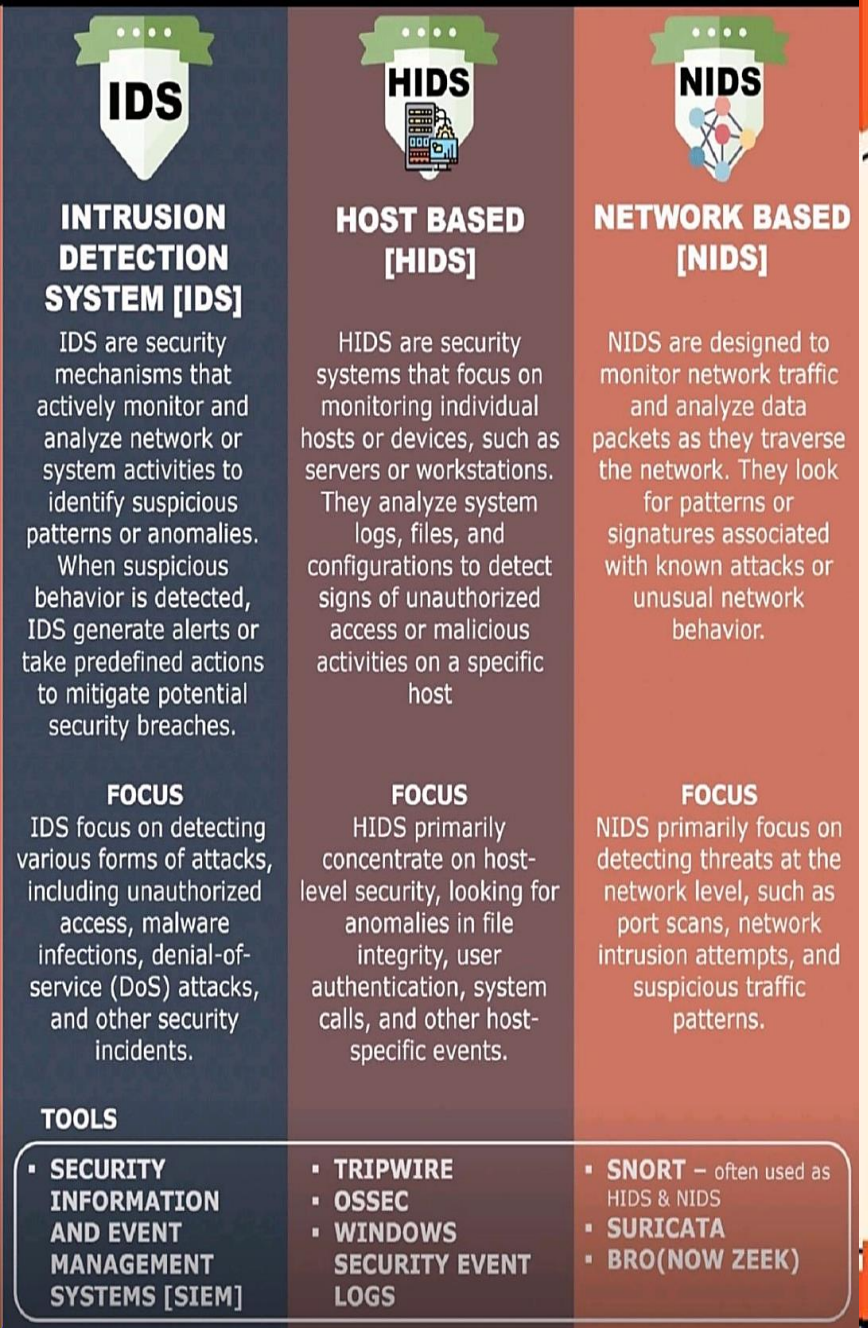
Most organizations have either an IDS or an IPS, and many have both as part of their security information and event management framework.

	IDS	IPS
NAME	Intrusion detection system	Intrusion prevention system
DESCRIPTION	A system that monitors network traffic for suspicious activity and alerts users when such activity is discovered.	A system that monitors network traffic and alerts for suspicious activity, like an IDS, but also takes preventative action against suspicious activity.
LOCATION	A host-based intrusion detection system is installed on the client computer. A network-based intrusion detection system resides on the network.	Located between a company's firewall and the rest of its network.
USE	Warns of suspicious activity taking place, but it doesn't prevent it.	Warns of suspicious activity taking place and prevents it.
FALSE POSITIVE	IDS false positives are usually just a minor inconvenience. Although the IDS incorrectly labels legitimate traffic as malicious, it does not prevent the traffic from entering the network.	IPS false positives can be more serious. When an IPS mistakes legitimate traffic for a threat, it stops the legitimate traffic from entering the network, which could impact any part of the organization, not just the IT team.

Source: https://www.linkedin.com/in/sabrinakaur



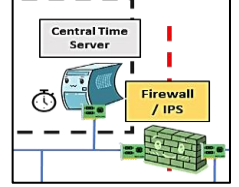
Source: https://purplesec.us/intrusion-detection-vs-intrusion-prevention-systems



Source:
https://www.facebook.com/redback/?locale=az_AZ

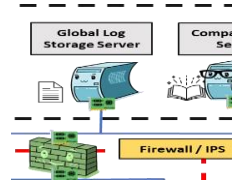
Source: https://pe.linkedin.com/posts/luis-gastulo-salazar-081732129_xdr-vs-siem-activity-7046894404757803008-quco

CENTRAL TIME SERVER



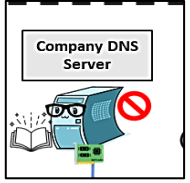
- **Ensures proper results of the analysis of the information stored in log server(s)**
- **Determining the time standard to use on the network is vital**
  - A single, consistent time zone and time-keeping method for all devices is critical
  - So every log entry of any device can be **correctly ordered** chronologically
  - Especially when diagnosing or identifying an attack that may be occurring against multiple devices in different parts of the network
- **All network devices (routers, switches, firewalls, servers,...), should use Universal Coordinated Time (UTC)**
  - Using UTC allows all events to be shown in the same timeframe without performing time zone conversions
- **This also prevent weird behavior with updates or with OS system files**
  - If time is accidentally out-of-sync with external servers that interactuate with our infrastructure, strange errors could be reported

GLOBAL LOG STORAGE SERVERS



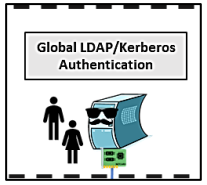
- **It is necessary to capture system log (`syslog`) information**
- **From all infrastructure devices (firewalls, routers, switches, servers…) and other critical systems**
  - Into a centralized log system (**Topic 3**)
  - Large organizations typically have servers attached to a large Network-Attached Storage (NAS) through a high-capacity Storage Area Network (SAN)
  - This way, a large amount of storage is available to the store logs of the whole infrastructure
- **All critical devices must be transmitting their log information to the server for preservation and further analysis**
  - Analysis that may be done with ML/IA techniques like the ones given in the SI course
- **These critical systems should be logging as many successful and failed events as possible (Topic 3 details which ones)**
  - Only then can we can maintain a complete picture of events for analysis and diagnostic
  - This also applies to application events of the software running in our infrastructure (**Topic 6**)

Internal DNS servers



- **Setting up DNS servers for internal use only has advantages**
  - Blocking accesses to known malicious sites (malware, ads…)
    - **There are suitable IP blocklists available**
      - https://github.com/StevenBlack/hosts, https://blocklistproject.github.io/Lists/
  - Especially important in servers with interactive user interaction
    - Like having an adblocker plugin, but **working with all devices** passing through the DNS
    - Therefore, reducing the probability of attacks and…not only web browsers!
  - Example: PiHole (https://pi-hole.net/)
- **We can also block connections to certain web sites for other reasons**
  - Any non-blocked requests should be forwarded to the Internet service provider's (ISP) DNS servers
- **However, because of potential threats to DNS servers, consider relying on the ISP's DNS for public queries**
  - Especially to secure public DNS providers, such as NextDNS, etc. (**Lab 1**)
  - But in this case by making an account and **using its extended capabilities**

Global Kerberos / LDAP authentication



- **The Kerberos authentication protocol is one of the most secure ones**
  - Supported by all major popular OS (more details in ASR)
  - Kerberos uses strong cryptography so a client can prove its identity to a server (and vice versa) through an insecure network connection
  - After that, they can also encrypt all their communications to ensure privacy and data integrity
- **All servers should use Kerberos to authenticate among them**
  - Every individual application transaction session should generate its own Kerberos keys
  - This way sessions are individually secured and encrypted
- **Minimizes AitM attacks, packet sniffing and session hijacking**
  - It also provides an extra level of security by encrypting all communications between systems
  - Even if an attacker finds a way into the internal network, all communication is encrypted
  - Windows Active Directory infrastructures use Kerberos as an authentication mechanism
- **Biometrics or other MFA can be used as a complement (see Topic 6)**

Think you've understood it all? Evaluate yourself!

?

- **You can do the following**
  - *Understand that having a separate management network is paramount to maintaining a high level of security*
  - *Understand the security role of IDSs, IPSs, and SIEMs*
  - *Understand why it's so important to have a synchronized time server that's central and unique to your entire infrastructure*
  - *Understand why it's so important to have a central, single log storage server for the entire infrastructure*
  - *Understand what security task an internal DNS server can cover*
  - *Understand what the Kerberos protocol and LDAP are for in an enterprise's infrastructure*

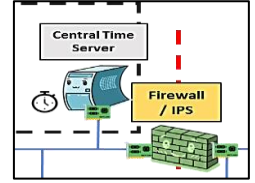
Extra security measures of the SNI

*Icons by Bing Chat AI

SUBNETTING

- **Several enhancements can increase the security level of the architecture**
- **The first is to extend the usage of multiple IP subnets to the whole infrastructure**
  - And not only the management LAN
  - Firewalls **with multiple NICs** can be used to isolate different subnets between network layers
  - Each DMZs **could have its own IP subnets that do not reflect any other subnet**
    - i.e., if the `10.x.x.x` subnet is used internally, and the `192.168.x.x` private subnet is used for the management LAN, the DMZs should use IP addresses in the `172.16-31.x.x` subnets
  - The secure LAN should also have its own IP subnet, not used in any other
- **The use of multiple IP subnets will increase the amount of routing and the complexity of the network architecture**
- **But also, significantly reduces the likelihood that an attacker gaining access to systems**
  - And the implementation time to fine-tune the network monitoring activities

VLANs



- **VLANs logically segregate network traffic**
  - **Used to separate traffic** based on its "risk", quality of service, or other considerations. Ex.:
    - Operational control and monitoring traffic
    - Different internal LANs traffic
    - Internet-originated traffic and transactions
- **VLAN1 is recommended for control and monitoring**
  - Only network, system, and security administration personnel should have access to it
  - Should use static IP addressing, with a different scheme of any other network
  - Most servers come with several NICs; one of them can be configured to use only VLAN1
  - This allows servers to be monitored and controlled over a secure network
    - That can only be accessed by network and system administration personnel
- **Other VLANs can be added (VoIP, employee networks (browsing…), Wi-Fi…)**
  - The key to good VLAN implementations **is to rigorously plan them**
  - Attacks that allow to circumvent VLAN segregation are based on VLAN misconfiguration

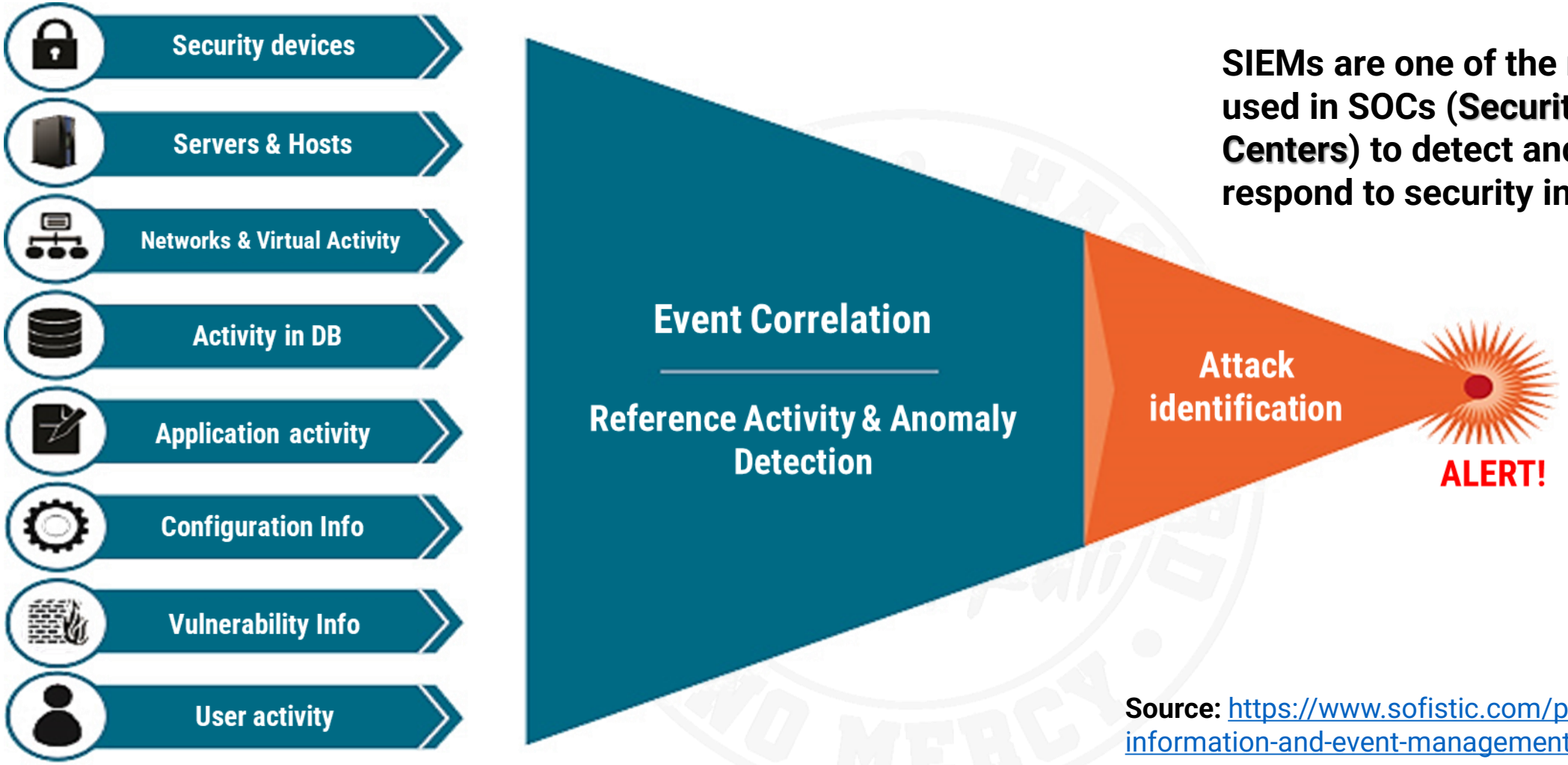
Virtual Machines

- **Nowadays, most of the complex machine infrastructures are implemented through virtual machines or containers (like our labs!)**
- **The ability to run multiple OS on a physical computer or a computer cluster maximizes hardware usages and simplifies their deployment**
- **But this also has security benefits: they can be regenerated**
  - If a HIDS detects that a server has been corrupted, it can be configured to reboot it
    - But from a second “clean” hot-swappable image, that will replace the corrupted one
  - So the system restarts from a known uncompromised image
    - And is then placed back in service
    - If an attacker compromises a server, any rootkits or malware is automatically wiped out!
      - The server always reboots from a clean, known image
  - Attack effects are detected and removed due to this response mechanism

IDS CORRELATION ENGINE

- Add a **syslog/IDS/IPS correlation engine application** over our centralized log server
  - **Security Information and Event Management** or **SIEM**
- They search patterns in all log and alert information received from all the components of the infrastructure (from IDS/IPS and SNMP)
  - These could indicate an attack or a network anomaly that should be investigated
  - Patterns may be identified by rule-based systems or other **AI techniques** explained in the SI course
- Appropriate rules for correlation engines are necessary
  - Requires **careful planning and information monitoring**
  - However, once implemented, these systems can significantly reduce the number of alerts
  - Network and security administration employees can focus on the more likely threats and anomalies (**threat hunting**)

IDS CORRELATION ENGINE



SIEMs are one of the main tools used in SOCs (Security Operations Centers) to detect and early respond to security incidents

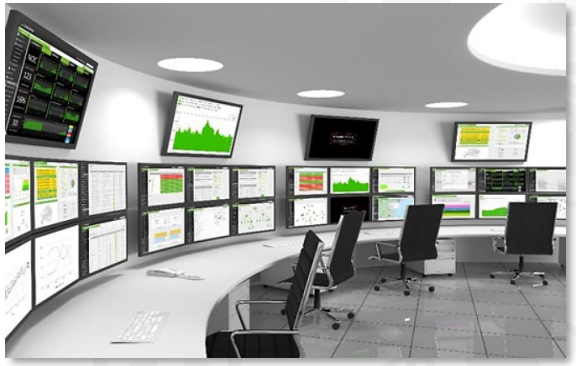
Source: https://www.sofistic.com/productos/security-information-and-event-management-siem/

Extensive data sources + Intelligence = Practical and extremely precise vision

Security Operations Center (SOC)

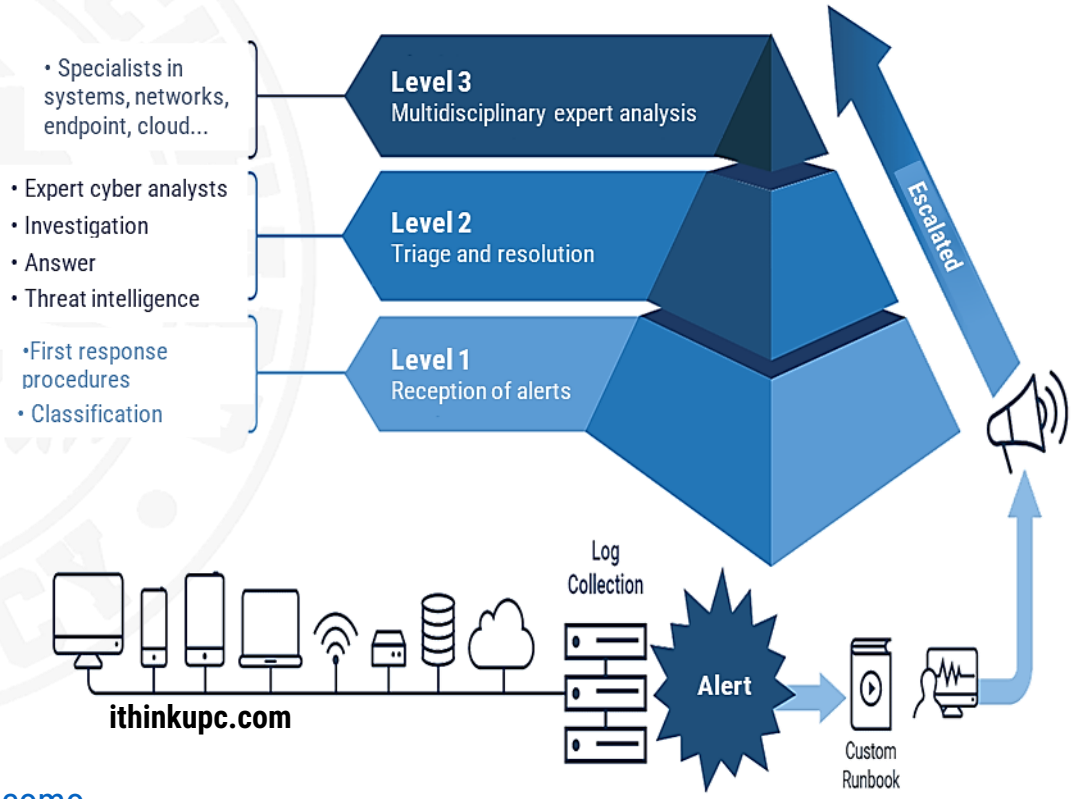
- It is important to understand what a SOC is, and how it performs surveillance
- There are many open positions to work in them!

All this client system information is examined in the SOC control room (own or rented), with specialized programs



Detected alerts are managed by SOC operators following documented response procedures
If the alert is severe, is "escalates" to higher SOC levels to appropriately deal with it
If it is very severe, it escalated to level 3, to be managed by the most experienced and specialized personnel

Source: https://digitalguardian.com/blog/how-build-security-operations-center-soc-peoples-processes-and-technologies



Source: https://blog.elhacker.net/2021/03/que-es-como-funciona-centro-de-operaciones-de-seguridad-soc.html

SOAR (Security Orchestration, Automation & Response)

Computer Security

- A suite of services and tools that automate the prevention and response to cyberattacks
- Unify integrations and define how tasks should be executed
- Develop an incident response plan tailored to an organization's needs
- In other words: it provides maximum automation when dealing with security incidents

SIEM

SECURITY INFORMATION AND EVENT MANAGEMENT

SIEM systems are designed to provide real-time analysis of security alerts generated throughout an organization's technology infrastructure. By collecting and aggregating log data, SIEM tools offer a holistic view of an organization's information security, enabling the detection of anomalous activities and potential security incidents.

KEY FEATURES OF SIEM:

Log Management: SIEM solutions collect, store, and analyze log data from various sources, such as network devices, servers, and applications.

Real-time Monitoring: SIEM allows for real-time monitoring of security events, enabling rapid response to potential threats.

Correlation and Analysis: SIEM tools correlate events from different sources to identify patterns and potential security incidents.

Alerts and Notifications: Automated alerts and notifications are triggered when suspicious activities or security incidents are detected.

Focus: Providing a vigilant eye on your digital landscape, offering insights into anomalous activities and potential risks.

SOAR

SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE

SOAR platforms take cybersecurity automation to the next level by integrating technologies, streamlining processes, and orchestrating responses to security incidents. These platforms aim to enhance the efficiency and effectiveness of incident response activities, allowing organizations to respond to threats in a more organized and automated manner.

KEY FEATURES OF SOAR:

Orchestration: SOAR platforms automate and orchestrate workflows across various security tools and processes, reducing manual intervention.

Automation: Automation in SOAR accelerates incident response by automating repetitive tasks and standardizing response procedures.

Incident Investigation and Response: SOAR facilitates thorough investigation and response to security incidents by providing playbooks, case management, and collaboration tools.

Integration with Threat Intelligence: SOAR platforms integrate with threat intelligence feeds to enhance detection capabilities and automate responses based on the latest threat intelligence.

Focus: Streamlining workflows, automating repetitive tasks, and responding to incidents with precision and speed.

Think you've understood it all? Evaluate yourself!

?

- **You can do the following**
  - *Understand why having different IP ranges on different networks is an additional layer of isolation*
  - *Understand that VLANs are a way to completely isolate traffic belonging to different networks*
  - *Be aware that the use of virtual machines is also essential to isolate services between them*
  - *Understand that the correlation between the information and all the logs received from all systems, including using AI techniques, is essential to detect threats that are underway in the infrastructure*
    - *And that this needs rules to function properly*
  - *Understand that this analysis of the log information of all systems is the function of SIEM systems*
    - *And that SIEMs are a very important part of a SOC*

< Go to Index

INTRODUCTION TO NETWORK PENTESTING

How to check the security of a network

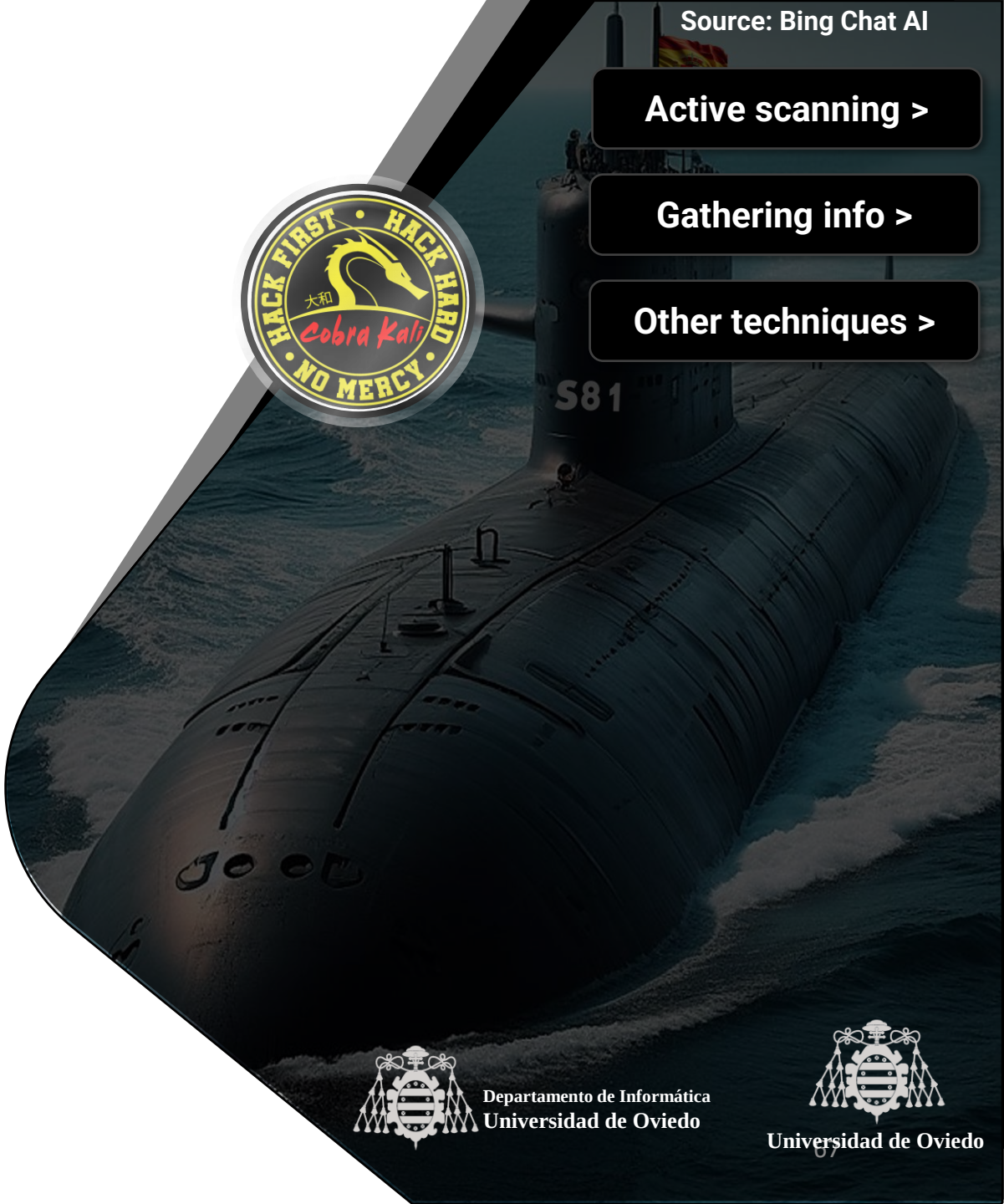
*Icons by Bing Chat AI

Source: Bing Chat AI

Active scanning >

Gathering info >

Other techniques >



Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

What are you going to find in this block?

- **In this block you will learn**
  - What the **MITRE ATT&CK** is, and how it relates to the CIS Benchmarks
  - The importance of the **reconnaissance stage** in initiating an attack
  - How to do an **active scan** of a machine
  - **Other possible forms of reconnaissance**

THE MITRE ATT&CK

https://attack.mitre.org/

- **Globally-accessible and free knowledge base of adversary tactics and techniques based on real-world observations**
  - Up to date, worldwide-used…the best source for learning how to “attack”!
- **Used as a foundation for the development of specific threat models (see Topic 6) and methodologies in all sectors and communities**
- **Divides tactics & techniques in 14 stages**
  - Called the adversary lifecycle
- **We will describe here the first one only: Reconnaissance**
  - This covers the first two stages of our “kill chain”
  - Rest of the stages belong to the exploiting and post-exploiting phases
    - It will be reviewed in the last theory topic
- **We provide here an introduction and some examples**
  - But you can follow the links to study attack techniques and tactics in detail

MITRE ATT&CK and the CIS Benchmarks

- **Do you remember this part of Topic 4? (CSC Controls)**
  - I did not tell you the whole truth...☺
- **Every CIS technical security control is MAPPED to a MITRE ATT&CK technique**
  - Although only for newer products versions…
- **What does this mean?**
  - That you can use each CIS Benchmark technical security control to "**fight against**" certain MITRE ATT&CK techniques!
  - **Defense and attack can be related this way!**

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

MITRE ATT&CK Mappings:

Techniques / Sub-techniques	Tactics	Mitigations
T1499, T1499.001	TA0005	M1022

TA0043. Reconnaissance

- The adversary is trying to gather information
- Everything that can be used to plan future operations and identify targets
  - The information also aids to future phases of the attack lifecycle
- Information can be obtained actively or passively
  - It may include data of the victim organization, infrastructure, staff…
- Let’s review some of its techniques

ATT&CK®

T1595: Active Scanning

Probing the adversary to obtain information about it

*Icons by Bing Chat AI

T1595: Active scanning

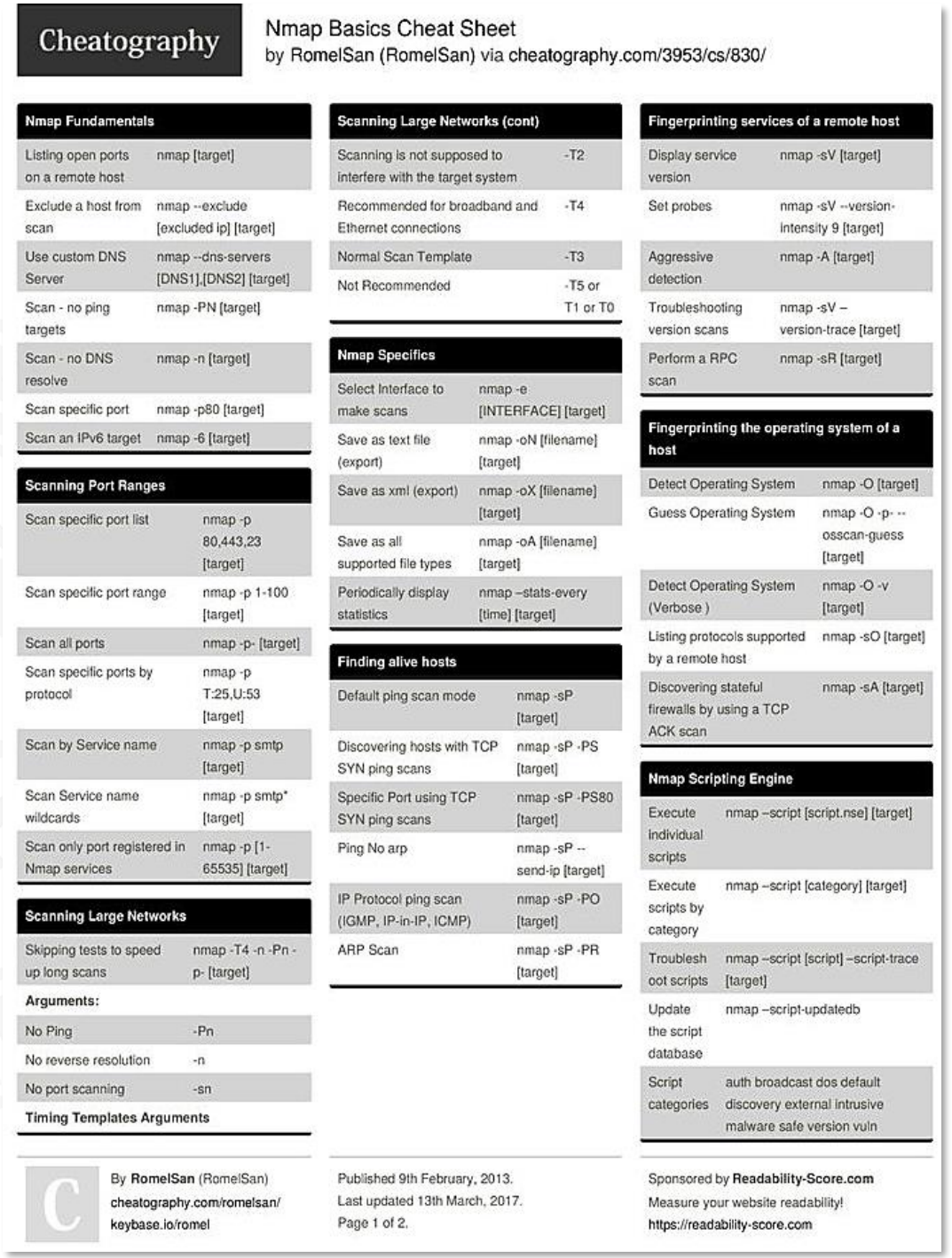
- The adversary actively probes victim infrastructure via network traffic
  - https://attack.mitre.org/techniques/T1595/
  - As opposed to other reconnaissance forms, that do not involve direct interaction with the infrastructure, **this one does**
  - It scans IP blocks and/or potential vulnerabilities
  - Interacts with the target infrastructure, trying to obtain as much information as possible
  - These active scans **may be easily detectable** by some of the network security solutions we mentioned: IDS, IPS…
- One of the most popular tools to do active scanning is **Nmap** (**Lab 8-9** will be dedicated to this tool)
- Automated vulnerability scan software (Seminar 3) can also be included in this category

➢ **Lab 8**: Complete block of exercises with **NMap Lv1**

Active scanning techniques

Computer Security

- **Active scan techniques have two objectives**
  - Locate “alive” systems (done on **Topic 1**)
  - Create a profile of each one to investigate them
- **After a Nmap scan we should determine**
  - How many **ports** are open in each system
  - What **services** are running behind these ports
    - Name, version, other useful information…
  - **Extended service information**
    - Potential vulnerabilities, configuration, files…
- **Services that use the HTTP protocol gives us new enumeration possibilities**
  - With specialized tools
  - Locate potential software vulnerabilities
    - General, specialized by its technology (CMS…)
  - Directories and potentially compromising files



Cheatography

Nmap Basics Cheat Sheet
by RomelSan (RomelSan) via cheatography.com/3953/cs/830/

Nmap Fundamentals

Listing open ports on a remote host	nmap [target]
Exclude a host from scan	nmap --exclude [excluded ip] [target]
Use custom DNS Server	nmap --dns-servers [DNS1],[DNS2] [target]
Scan - no ping targets	nmap -PN [target]
Scan - no DNS resolve	nmap -n [target]
Scan specific port	nmap -p80 [target]
Scan an IPv6 target	nmap -6 [target]

Scanning Port Ranges

Scan specific port list	nmap -p 80,443,23 [target]
Scan specific port range	nmap -p 1-100 [target]
Scan all ports	nmap -p- [target]
Scan specific ports by protocol	nmap -p T:25,U:53 [target]
Scan by Service name	nmap -p smtp [target]
Scan Service name wildcards	nmap -p smtp* [target]
Scan only port registered in Nmap services	nmap -p [1-65535] [target]

Scanning Large Networks

Skipping tests to speed up long scans	nmap -T4 -n -Pn -p- [target]
Arguments:	
No Ping	-Pn
No reverse resolution	-n
No port scanning	-sn
Timing Templates Arguments	

Scanning Large Networks (cont)

Scanning is not supposed to interfere with the target system	-T2
Recommended for broadband and Ethernet connections	-T4
Normal Scan Template	-T3
Not Recommended	-T5 or T1 or T0

Nmap Specifics

Select Interface to make scans	nmap -e [INTERFACE] [target]
Save as text file (export)	nmap -oN [filename] [target]
Save as xml (export)	nmap -oX [filename] [target]
Save as all supported file types	nmap -oA [filename] [target]
Periodically display statistics	nmap –stats-every [time] [target]

Finding alive hosts

Default ping scan mode	nmap -sP [target]
Discovering hosts with TCP SYN ping scans	nmap -sP -PS [target]
Specific Port using TCP SYN ping scans	nmap -sP -PS80 [target]
Ping No arp	nmap -sP --send-ip [target]
IP Protocol ping scan (IGMP, IP-in-IP, ICMP)	nmap -sP -PO [target]
ARP Scan	nmap -sP -PR [target]

Fingerprinting services of a remote host

Display service version	nmap -sV [target]
Set probes	nmap -sV --version-intensity 9 [target]
Aggressive detection	nmap -A [target]
Troubleshooting version scans	nmap -sV –version-trace [target]
Perform a RPC scan	nmap -sR [target]

Fingerprinting the operating system of a host

Detect Operating System	nmap -O [target]
Guess Operating System	nmap -O -p- --osscan-guess [target]
Detect Operating System (Verbose)	nmap -O -v [target]
Listing protocols supported by a remote host	nmap -sO [target]
Discovering stateful firewalls by using a TCP ACK scan	nmap -sA [target]

Nmap Scripting Engine

Execute individual scripts	nmap –script [script.nse] [target]
Execute scripts by category	nmap –script [category] [target]
Troubleshoot scripts	nmap –script [script] –script-trace [target]
Update the script database	nmap –script-updatedb
Script categories	auth broadcast dos default discovery external intrusive malware safe version vuln

By **RomelSan** (RomelSan)
cheatography.com/romelsan/
keybase.io/romel

Published 9th February, 2013.
Last updated 13th March, 2017.
Page 1 of 2.

Sponsored by **Readability-Score.com**
Measure your website readability!
https://readability-score.com

Active Scanning: Nmap detailed scan

- **NMap implements numerous system enumeration and port and service scanning techniques**
  - E. g.: `nmap -sS -A -sV -O –p -` runs a **detailed, slower, and more detectable** scan
  - Obtains the maximum information from the target
    - `-sS`: Use the TCP SYN scan type
      - Potentially more effective if there are firewalls
    - `-A`: Detects service / OS versions, performs a `traceroute`, and runs some scripts
    - `-sV`: Probe open ports
      - To determine services and versions running
    - `-O`: Enables OS type and version detection
    - `-p -`: Scans a range of ports
      - `-` scans all ports, but we can specify a range

```
root@kali:~# nmap -sS -A -sV -O -p - 192.168.14.2
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-02 13:11 CEST
Nmap scan report for 192.168.14.2
Host is up (0.00029s latency).
```

Port/protocol, port state, listening service on this port

```
21/tcp  open  ftp         OpenBSD ftpd 6.4 (Linux port 0.17)
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 42:62:a8:1b:16:da:24:bb:52:da:ef:b4:9e:86:87:31 (RSA)
|   256 77:73:2a:b7:4c:8b:97:33:c4:8f:f1:2d:39:97:82:56 (ECDSA)
|_  256 b6:46:3e:1c:0d:6b:81:2b:65:e6:aa:56:45:2c:1e:ee (ED25519)
23/tcp  open  telnet      Linux telnetd
80/tcp  open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
MAC Address: 08:00:27:D5:89:36 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: server1804; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1s, deviation: 0s, median: 1s
|_nbstat: NetBIOS name: SERVER1804, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: server1804
|   NetBIOS computer name: SERVER1804\x00
|   Domain name: \x00
|   FQDN: server1804
|_  System time: 2019-10-02T11:12:04+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
```

➢ **Lab 8**: Complete block of exercises with **NMap Lv2**

Active scanning. Interpreting Nmap results

Computer Security

```
root@kali:~# nmap -sS -A -sV -O -p - 192.168.14.2
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-02 13:11 CEST
Nmap scan report for 192.168.14.2
Host is up (0.00029s latency).
Not shown: 65529 closed ports
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         OpenBSD ftpd 6.4 (Linux port 0.17)
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoco
l 2.0)
| ssh-hostkey:
|   2048 42:62:a8:1b:16:da:24:bb:52:da:ef:b4:9e:86:87:31 (RSA)
|   256 77:73:2a:b7:4c:8b:97:33:c4:8f:f1:2d:39:97:82:56 (ECDSA)
|   256 b6:46:3e:1c:0d:6b:81:2b:65:e6:aa:56:45:2c:1e:ee (ED25519)
23/tcp  open  telnet      Linux telnetd
80/tcp  open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
MAC Address: 08:00:27:D5:89:36 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: server1804; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1s, deviation: 0s, median: 1s
|_nbstat: NetBIOS name: SERVER1804, NetBI
wn> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: server1804
|   NetBIOS computer name: SERVER1804\x00
|   Domain name: \x00
|   FQDN: server1804
|_  System time: 2019-10-02T11:12:04+00:0
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default
| smb2-security-mode:
```

Specific software (and its version) that provide the FTP and SSH services. Very useful to search for their vulnerabilities / exploits in DBs that list them (https://www.cvedetails.com/)

Public key of the machine to distinguish it from others when connection via SSH (PKI)

Web / telnet server and version: same as the previous services

SAMBA service (Microsoft file sharing SMB protocol, but its Linux implementation)

Standard PC (not a cell phone, printer, IoT device...) with a Linux on the same subnet as ours (1 hop implies that it has not "jumped" between networks)

Ubuntu version, although it could be fake. In addition, it can also be inferred by the specific versions of the exposed services (each OS version usually has slightly different versions of their services, and we could look in the repositories to see which versions are distributed with different versions of a concrete OS). Again, with this we can search for specific vulnerabilities of this version

SMB installation data

The NSE scripting engine allows you to take full advantage of NMap's capabilities and versatility. And remember: Unknown open ports can indicate the presence of malware!

Gathering technical and personal information

Techniques to study persons and websites

*Icons by Bing Chat AI

Person-related TA0043. Reconnaissance techniques

T1592. Gather Victim Host Information

- https://attack.mitre.org/techniques/T1592/
- **Administrative data** (e. g.: name, assigned IP, functionality, etc.)
- **Configuration** (e. g.: operating system, language, etc.)
- Information about hardware, software, and firmware elements
- NMap and Wazuh (with its inventory) can provide information like this

T1590. Gather Victim Network Information

- https://attack.mitre.org/techniques/T1590/
- **Administrative data** (e. g.: IP ranges, domain names and DNS properties, etc.)
- Specialized tools are usually used or Nmap NSE scripts (**Lab 8-9**)
- Specifics regarding its topology and operations
  - Network trust dependencies
  - Network topology
  - Network security appliances (like firewalls)
  - …

T1592. Gather Victim Host Information / T1590. Gather Victim Network Information

- **To enumerate services, you can**
  - Use **specialized tools** for each service you found
    - Ex.: `dig` (DNS), `Enum4Linux` (SMB), `SNMPWalk` (SMB), `WPScan` (WordPress), `dirb` (web pages)…
  - Search and use **nmap NSE scripts** linked to the service name (see the lab cheat sheets)
    - `locate *nse* grep <service name>`
    - And **use the documentation** of the scripts you find to see how we can run them against the target
      - https://nmap.org/nsedoc/
    - Most of them do not only perform enumeration tasks: it also allows exploiting vulnerabilities
    - For enumeration tasks only, it is advisable to search for the word "**enum**" in the script description
  - Use **Metasploit Auxiliary modules** (seen on **Topic 7**)

T1592. Gather Victim Host Information / T1590. Gather Victim Network Information

- You can find more information about the victim on more places, such as
  - **Specific files** on your website that reveal services, versions, information in general, etc.
  - The endpoints of the JavaScript files on your website
    - Traditionally, they tend to be less protected points (they are usually ignored as a route of attack)
  - If an organization has its code in a **public repository** (e.g. GitHub) it is another avenue of attack
    - It could contain private information ("hardcoding") (**Seminar 4**, **Topic 6**)
  - If **cloud storage** (e.g. Amazon S3) is used, it should also be reviewed
    - It could be **misconfigured** and expose private information
- Or you may consider to sniff and analyze the network traffic directly
  - Wireshark: https://www.wireshark.org/
    - Example: https://null-byte.wonderhowto.com/how-to/spy-traffic-from-smartphone-with-wireshark-0198549/
  - Sparrow-wifi - Graphical Wi-Fi Analyzer for Linux: https://github.com/ghostop14/sparrow-wifi
  - Ehtools Framework: https://github.com/entynetproject/ehtools

➢ Exercises **L89B4_SCRIPTSCAN**, **L89B4_JSSCAN**, **L89B4_S3SCAN**, **L89B4_GITHUBSCAN**

More TA0043. Reconnaissance techniques

- **T1589. Gather Victim Identity Information**
  - https://attack.mitre.org/techniques/T1589/
  - Personal data (e. g.: employee names, email addresses, etc.)
  - Sensitive details (such as credentials)
- **T1591. Gather Victim Org Information**
  - https://attack.mitre.org/techniques/T1591/
  - Names of divisions/departments, physical locations…
  - Specifics of business operations (relationships, business tempo (working hours/days)…)
  - Roles and responsibilities of key employees
- **All this info can be found on Internet (social networks, websites, etc.)**
  - There are lots of information about persons, companies, etc.
  - Leading to spear phising data-gathering techniques
  - **We will practice this in the Group works** (OSINT)

Other reconnaissance techniques

More techniques to obtain information about the victim

*Icons by Bing Chat AI

Other TA0043. Reconnaissance techniques

T1598. Phishing for Information

- https://attack.mitre.org/techniques/T1598/
- Attempt to trick targets into divulging information, frequently credentials or other actionable information
- This time the attacker do not aim to execute malicious code
- Attackers may use a spear phising third-party service, spear phising attachment, or link
- **We will see this in the Group works** (OSINT)

T1597. Search Closed Sources

- https://attack.mitre.org/techniques/T1597/
- Information about victims may be purchased from reputable private sources and databases
  - Such as paid subscriptions to feeds of technical/threat intelligence data (threat intelligence vendors)
- But it may be also purchased from less-reputable sources such as dark web or cybercrime black markets

Other TA0043. Reconnaissance techniques

- **T1596, Search Open Technical Databases**
  - https://attack.mitre.org/techniques/T1596/
  - Information about victims may be available in online DBs and repositories (registrations of domains/certificates…)
  - Also, in public collections of network data/artifacts gathered from traffic and/or scans
    - This includes DNS/Passive DNS, WHOIS, Digital Certificates, CDNs, Scan Databases (**Shodan**, **Censys**)
- **T1593, Search Open Websites/Domains**
  - https://attack.mitre.org/techniques/T1593/
  - Information about victims may be available in various online sites, such as social media or news sites
  - Also, those hosting information about business operations, such as hiring or requested/rewarded contracts
  - This also includes search engines (**Google Hacking**)

TA0043. Reconnaissance: Already reviewed techniques

- **Phishing for Information** was already reviewed in
  - **Seminar 1** (phishing against users)
    - Tinfoleak, Twint, Hunter.io, Social Mapper, Project Sherlock, and other tools
  - The complementary materials hosted here (and talk video)
    - https://www.researchgate.net/publication/359146160_Las_Ciberestafas_en_la_Actualidad_Formas_de_reconocerlas_y_prevenirlas
    - Describe multiple forms of phising and spear phising
- **Search Open Technical Databases** was covered in **Seminar 1** and **Laboratory 2**
  - Describing Shodan and Censys
- **Search Open Websites/Domains** topics were reviewed in
  - **Seminar 1** (Source code): GitGot, GitGraber and GitRob can obtain highly sensitive data
  - Google Hacking was described in **Seminar 1** and in **Laboratory 2**
- All this is also part of the **Group works** (OSINT)

Think you've understood it all? Evaluate yourself!

?

- **You can do the following**
  - *Understand what kind of information the MITRE ATT&CK contains and what it is used for*
  - *Understand that all CIS Benchmark technical security controls have a table at the end of their definition that maps the control to the techniques, tactics, and mitigation for attack contained in the MITRE ATT&CK*
  - *Have a clear understanding of what the reconnaissance stage of an attack is, and what part of it involves active machine scans*
  - ***About active scans***
    - *You understand what these scans are and the kind of information they can extract*
    - *You understand that there are basic and advanced scans that obtain more or less information, but in exchange for taking longer and have more risk to be detected by surveillance tools*
    - *To be aware that using the full capabilities of **NMap**, and to exploit its enormous versatility, is only possible by learning how to use its NSE scripting engine*
    - *You understand that obtaining information from an infrastructure does not end with its machines or networks, but also encompasses all kinds of services in use, files, code, cloud storage, and the people linked to it*
      - *And that, therefore, the OSINT of machines and people is an integral part of this reconnaissance stage*

TOPIC 5
PERIMETER AND NETWORK SECURITY

Departamento de Informática
Universidad de Oviedo