TOPIC 5. PERIMETER AND NETWORK SECURITY

Defending and attacking the network environment

JOSÉ MANUEL REDONDO LÓPEZ *"S-81 ISAAC PERAL"* PROJECT V3.0

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

Logo: @creative_vanesa (*Instagram*)

Topic goals

José Manuel
Redondo López

- **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

Firewalls >

Source: zona-militar.com

Additional Networking Concepts

Complementing the first theory topic with new definitions

NETWORK PROTOCOLS

José Manuel
Redondo López

- **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 in order to enable communication
- **On Internet, the most important are**
  - **IP** (Internet Protocol)
    - It uses IP addresses as machine addressing scheme (Topic 1): the basis of the modern Internet!
    - More details about this protocol are reviewed in the ASR course
  - **TCP** (Transmission Control Protocol)
- **Network protocols can be blocked by firewall configuration (ASR)**

Firewalls

New types of network traffic controllers

Remember: Firewalls

José Manuel
Redondo López

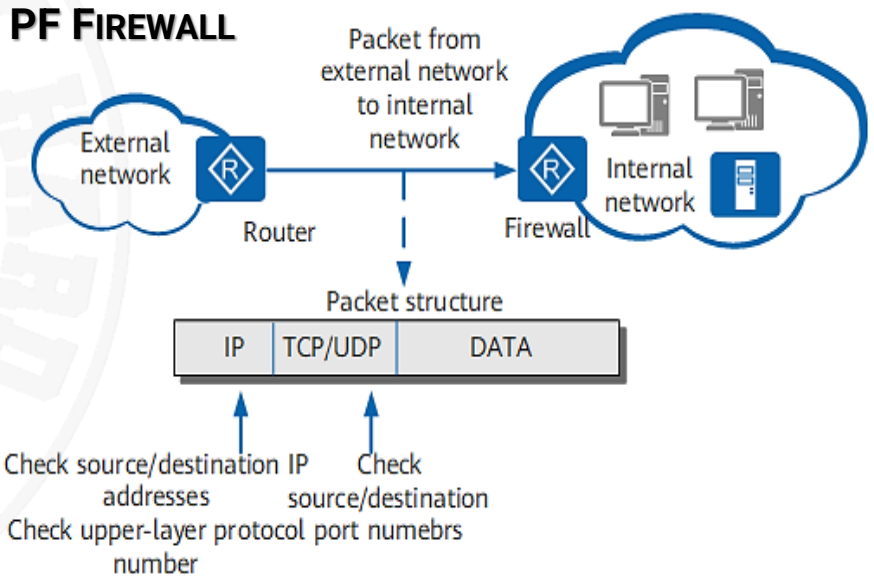
- **Designed to block unauthorized access, typically allowing outgoing traffic**
  - Part of a computer system (**software**)
  - Or a whole network (**specialized hardware**)
  - Also provides connection logging and auditing functions
- **Therefore, firewalls can be either software, hardware or hybrid**
  - **Hardware firewalls** are custom 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 a powerful software-based firewalls running on standard PC 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)

José Manuel
Redondo López

- **Checks this data of every received network packet**
  - Source and destination address
  - Protocol
  - Destination port number
- **Data is processed like this**
  - Packets are dropped if they do not comply with its **ruleset**
  - Examines packets one by one
    - 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
  - Linux has an integrated PF firewall with multiple frontends
    - Ufw
    - IPSet (https://wiki.archlinux.org/title/Ipset)
    - Firewalld

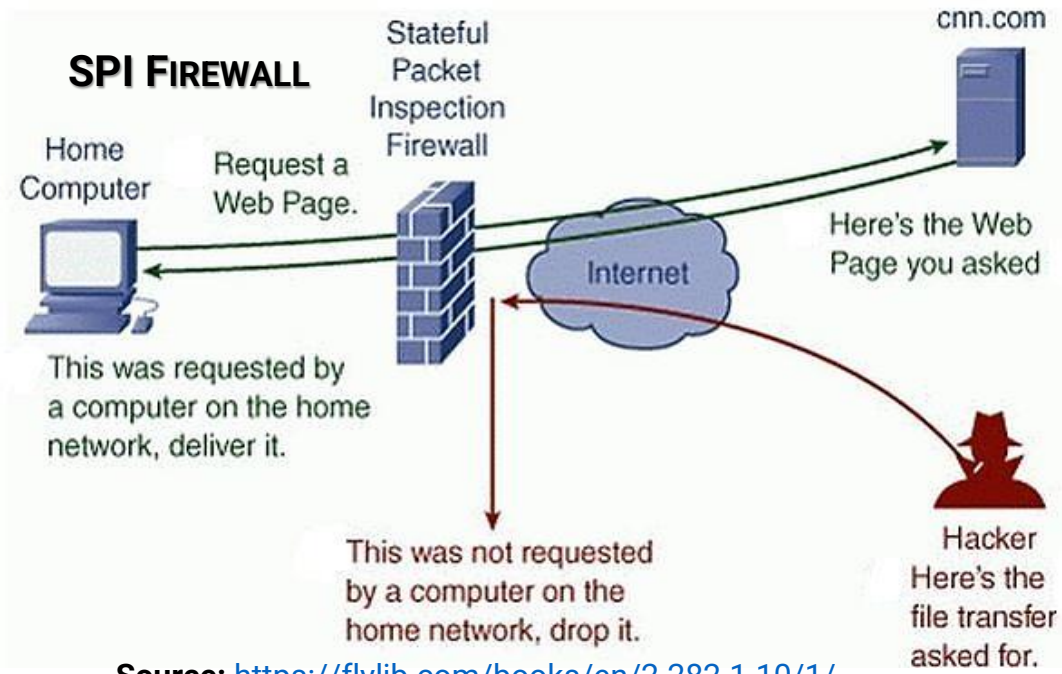
Source:
https://support.huawei.com/enterprise/es/doc/EDOC1000154776/88191a64/packet-filtering-firewall



Firewalls: Stateful Packet Inspection (SPI)

José Manuel
Redondo López

- **Dynamic packet-filtering firewalls with a table tracking all open connections**
  - When new packets arrive, the firewall compares information in the 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 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/)

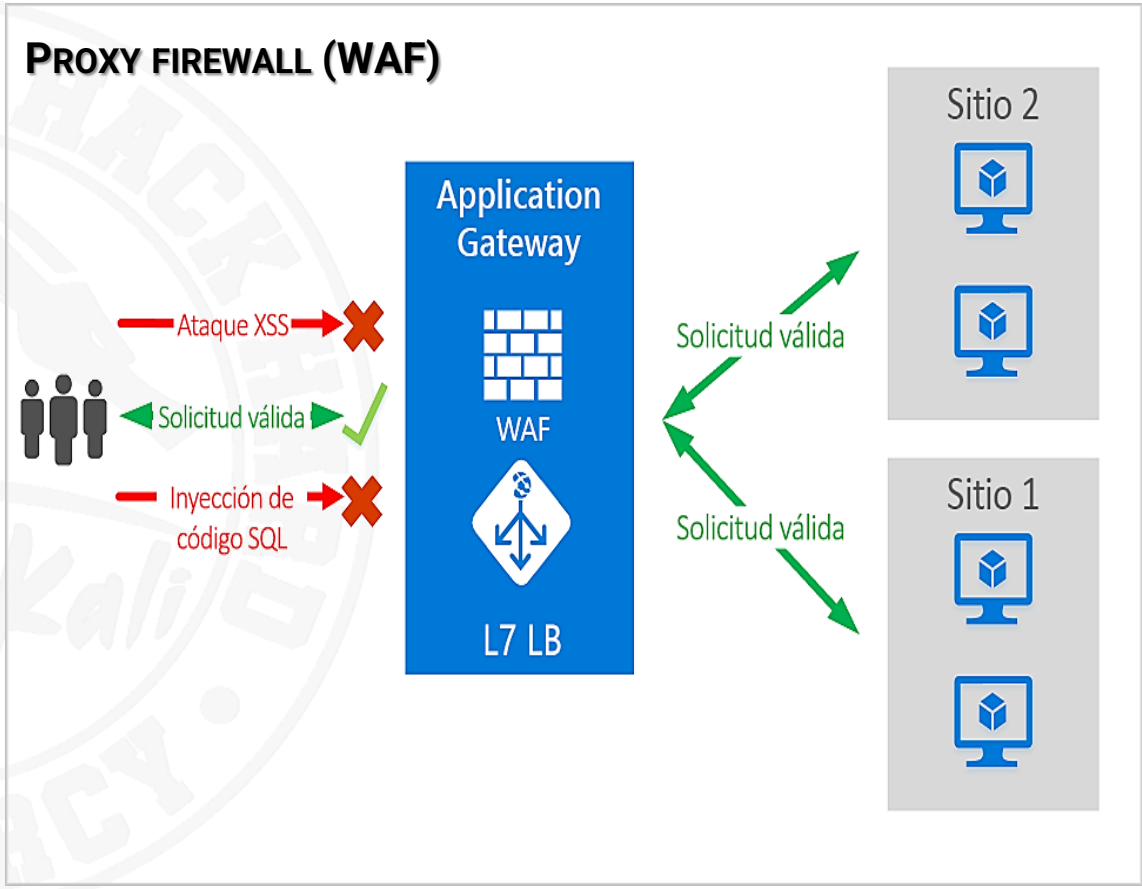


Source: https://flylib.com/books/en/2.282.1.10/1/

Firewalls: Proxys (aka WAFs)

José Manuel
Redondo López

- **Provides application-layer filtering**
  - Examine 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 `telnet` commands from particular users
    - A PF firewall can only control general incoming requests from particular hosts
    - **Not users**! (don't use packet data to take decisions)
  - `mod_security` is a very popular WAF
    - We will describe it in future slides

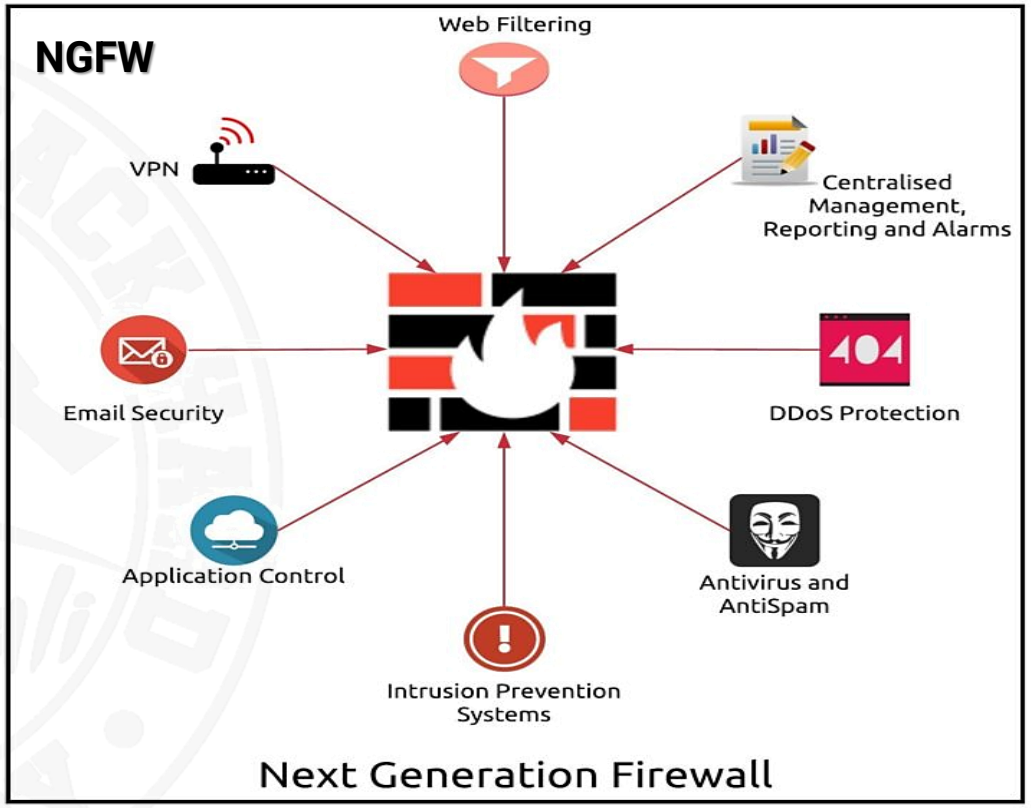


Source: https://learn.microsoft.com/es-es/azure/web-application-firewall/ag/ag-overview

Firewalls: Next-Generation Firewalls (NGFW)

José Manuel
Redondo López

- **Firewalls that use a multi-layered approach**
  - Combining features of traditional enterprise firewalls with more powerful functionality
    - **Intent-based networking**, including SSL/SSH traffic inspection
      - https://www.cisco.com/c/en/us/solutions/intent-based-networking.html
    - **Deep packet inspection** (DPI)
      - https://digitalguardian.com/blog/what-deep-packet-inspection-how-it-works-use-cases-dpi-and-more)
    - **Reputation-based malware detection**
    - **Application awareness**
- **Fortinet sells products of this type**
  - https://www.fortinet.com/lat/products/next-generation-firewall



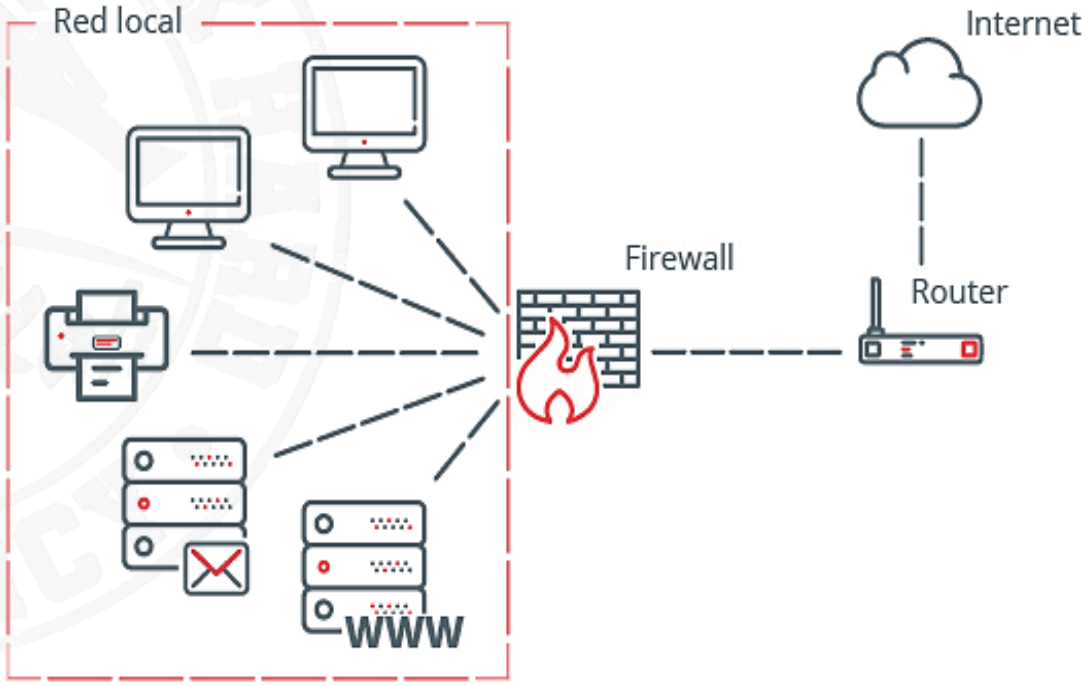
Source: https://firewall.firm.in/what-is-a-next-generation-firewall-ngfw/

Firewall rulesets

José Manuel
Redondo López

```
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)
```

- **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)!

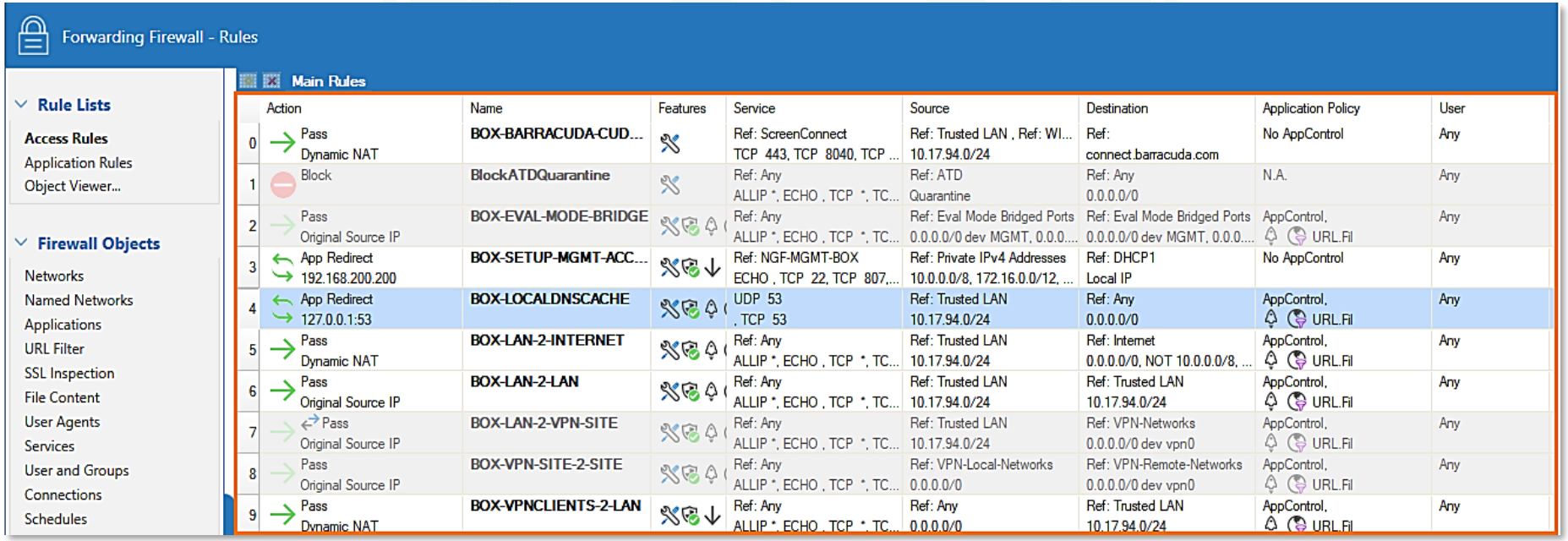


Source: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

FIREWALL RULESETS: EXAMPLES

José Manuel
Redondo López

- **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

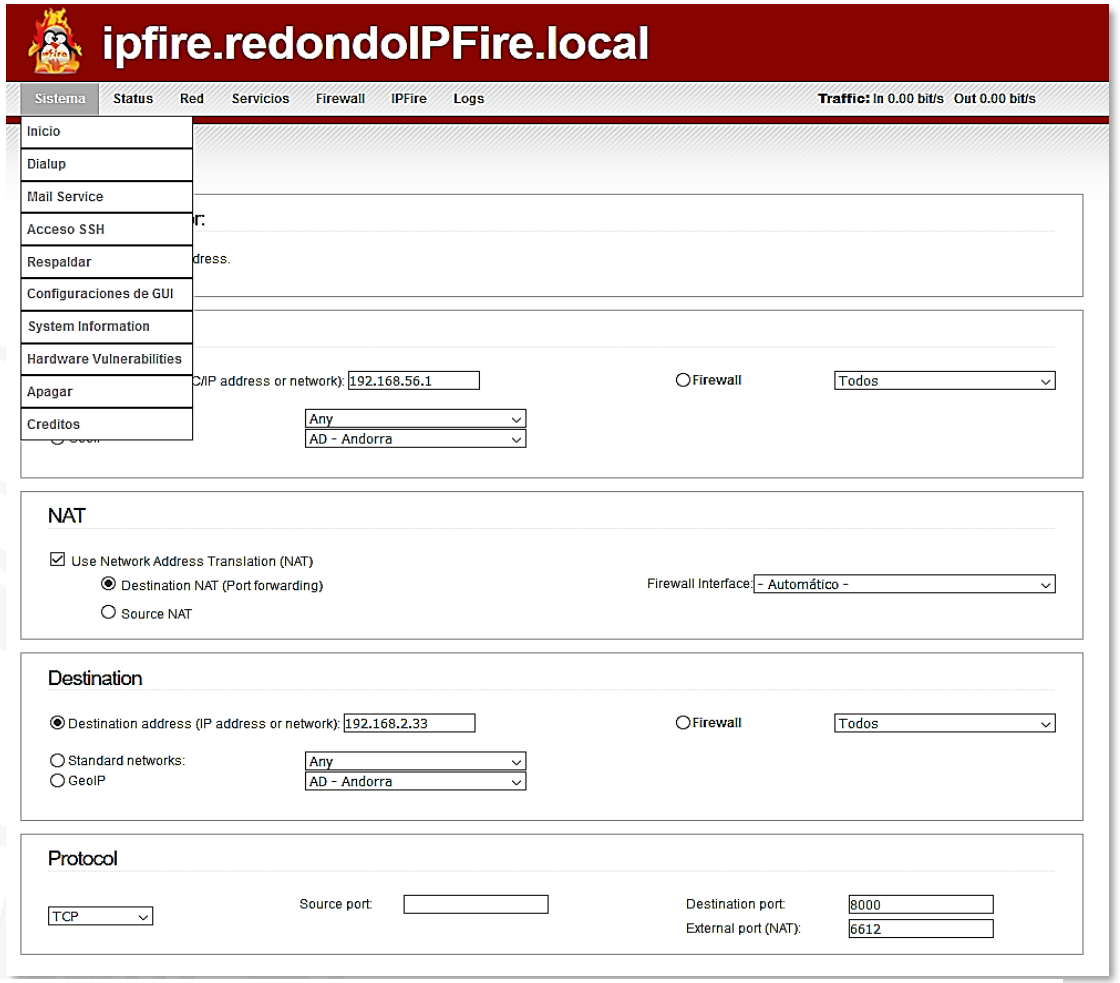
José Manuel
Redondo López

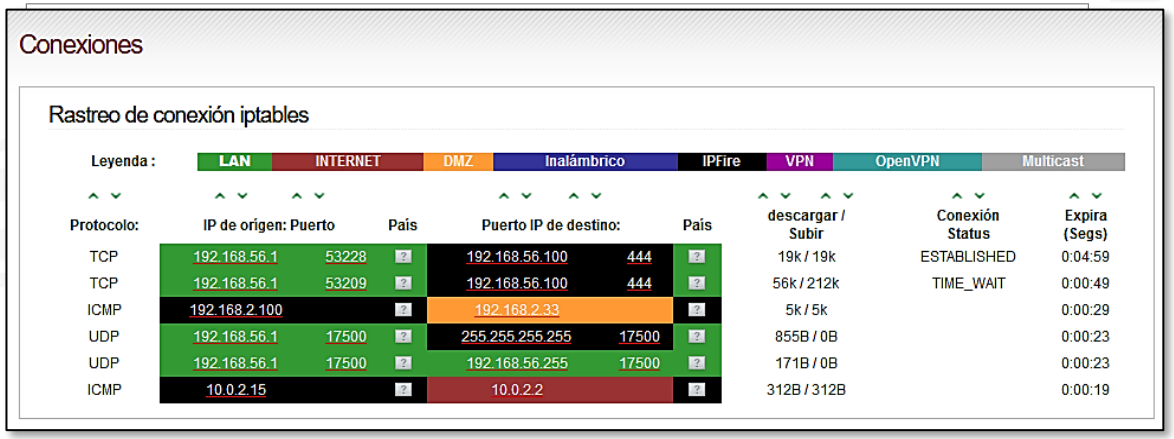
- **Every device should have a firewall installed with adequate rules**
  - These are called host firewalls (e. g. iptables from ASR and its interface, ufw)
  - Normally with an ingress **allow list** approach
    - **All incoming traffic is dropped unless explicitly allowed**
    - **Outgoing traffic** (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

PERIMETRAL FIREWALLS

José Manuel
Redondo López

- **The images show the free perimetral SPI firewall IPFire**
- **Their rules can be complex**
  - Sometimes they need maintenance / optimization
  - With programs like Springbok
  - https://ciberseguridad.blog/optimizando-la-ciberseguridad-del-firewall/
- **The zones from `firewalld` (ASR) can be used to make it work as a perimetral firewall**

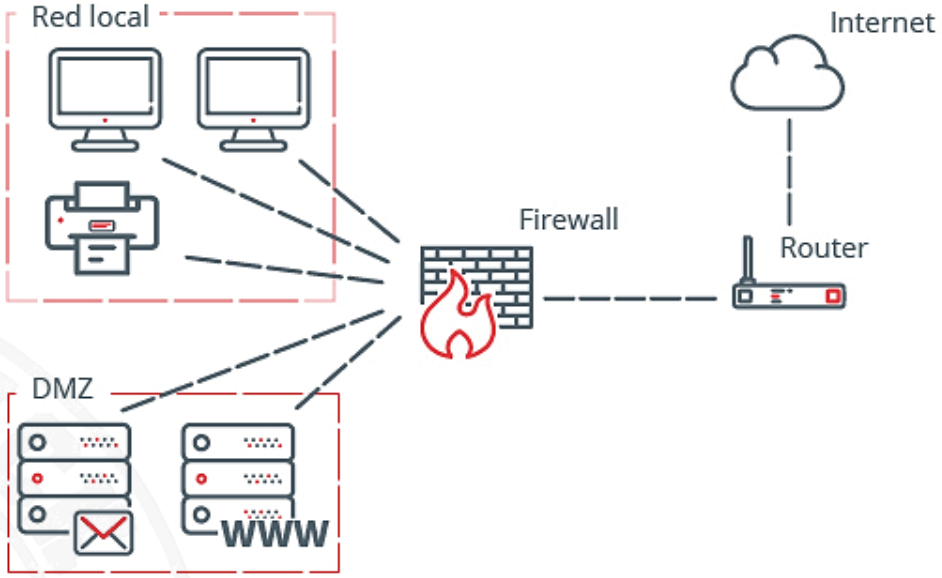


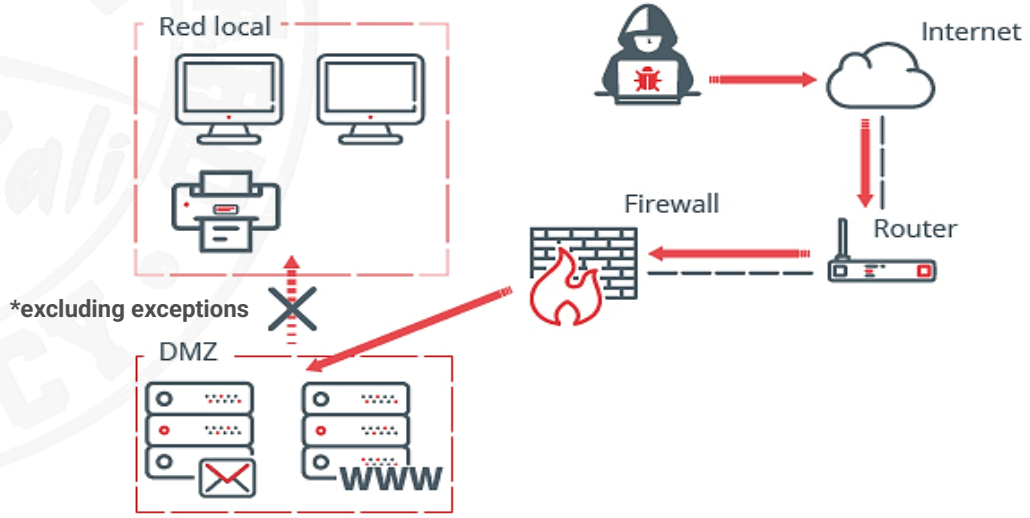


Demilitarized zones (DMZs)

José Manuel
Redondo López

- **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





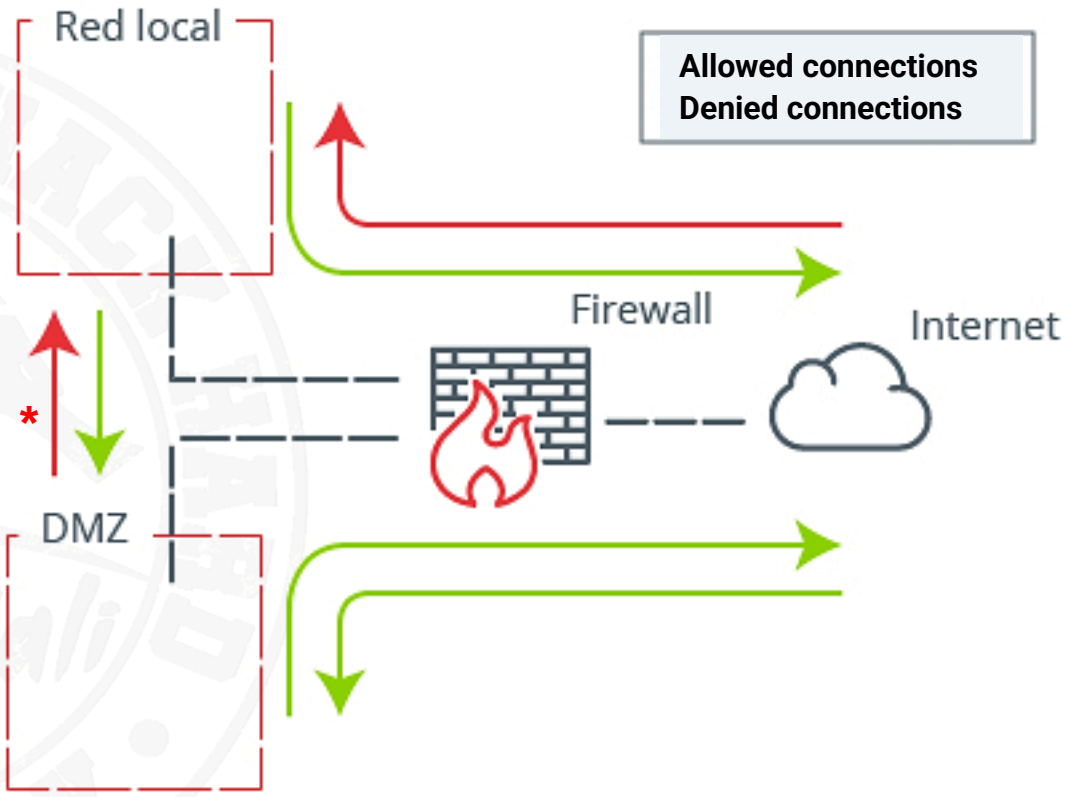
Source: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

Demilitarized zones (DMZs)

José Manuel
Redondo López

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 services / machines from specific machines and to concrete ports can be made



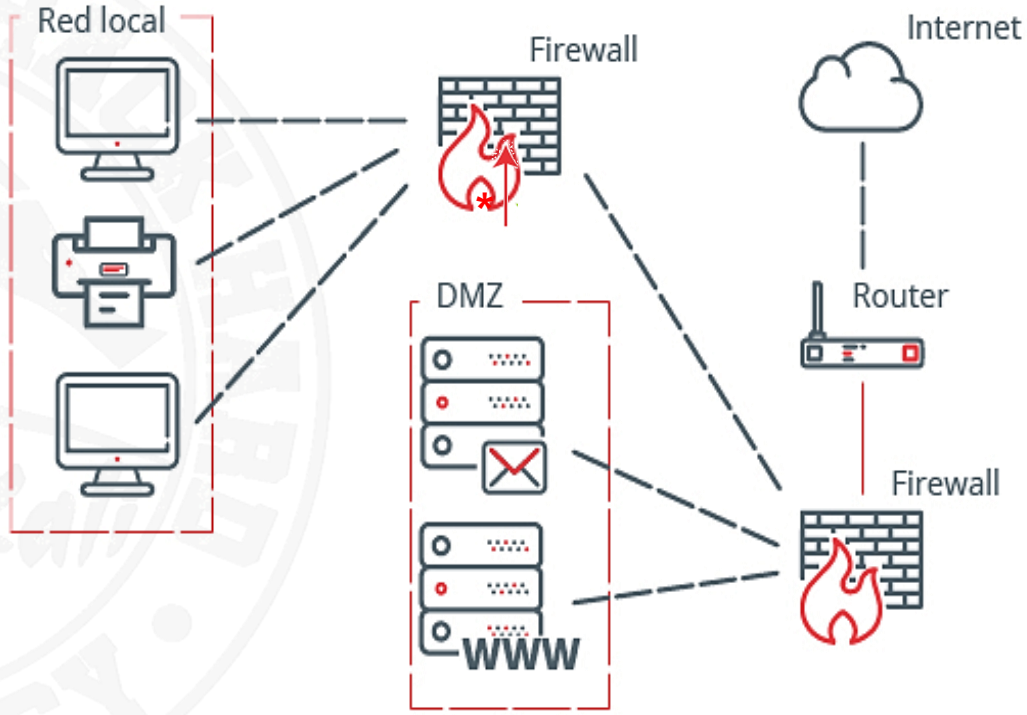
- **Firewalls are required to implement DMZs**
  - They establish network segments
  - Decide if allowing or disallowing communications between them
- **The table shows the recommended action with network traffic that come from and go to different network segments**

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

Demilitarized zones (DMZs)

José Manuel
Redondo López

- **Two firewalls increase network security**
  - Firewalls isolate the DMZ both from the internet and the LAN side
  - Strict connection control can be established in both sides of the DMZ
  - Facilitates creating networks in different address spaces, so they cannot see each other
- **Maximum protection against DMZ intrusions**
  - Minimizing their potential impact
  - Attackers will be confined inside the DMZ
- **The SNI example we will see, uses multiple double-firewalled network segments**

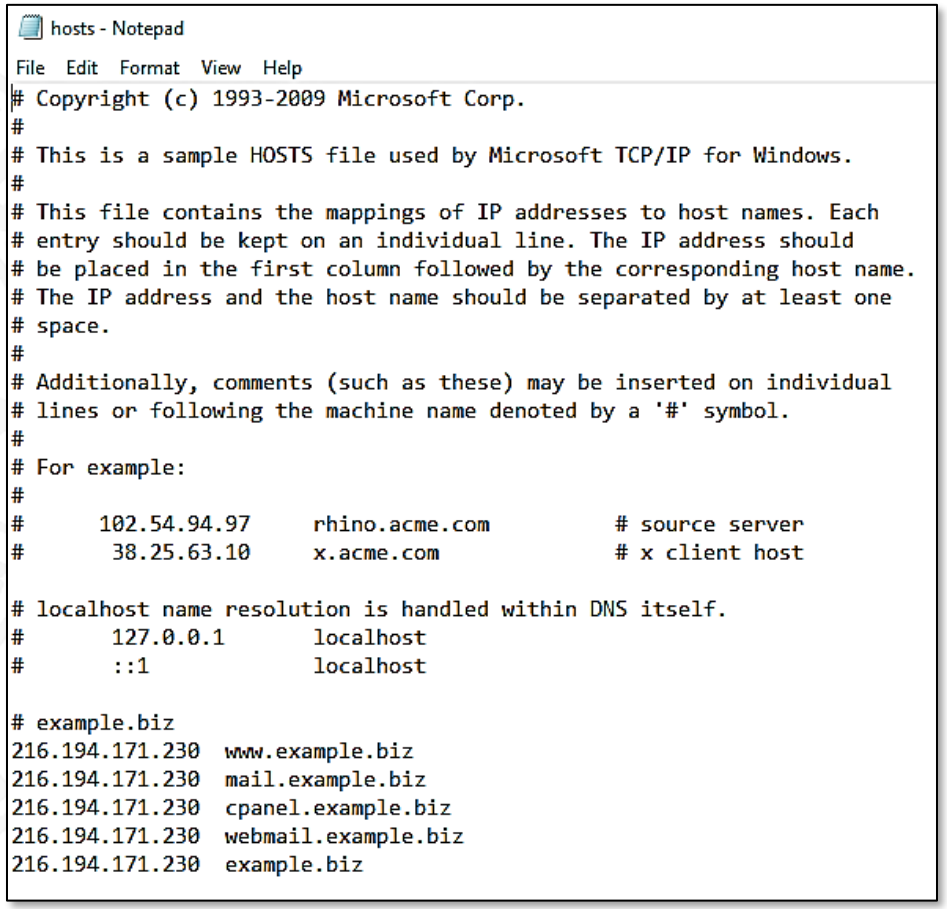


Source: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

Host files

José Manuel
Redondo López

- **Local file for domain name to IP translation**
  - Described in ASR
  - Everything on this file has priority to be consulted and resolved
    - First than 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 that makes remote connections

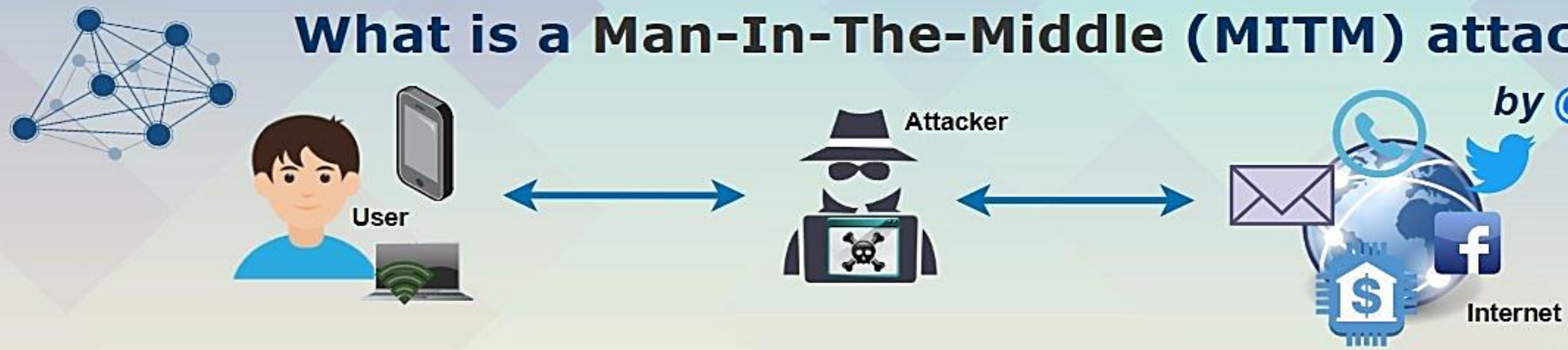


Network-based attacks: Man in the Middle (MitM)

José Manuel
Redondo López

What is a Man-In-The-Middle (MITM) attack ?

by @SecurityGuill



Types of MITM attacks

- **IP spoofing** : the attacker can trick you into thinking you're interacting with a website or someone you're not.
- **DNS spoofing** : force a user to a fake website rather the real one.
- **HTTPS spoofing** : the attacker can fool your browser into believing it's a trusted website.
- **Email hijacking** : the attacker can spoof companies email (bank, ...) and send their own instructions.
- **Wi-Fi eavesdropping** : the attacker can set up a Wi-Fi access point. When a user connects, the attacker can intercept login creds, information, online activity...

MITM definition

- A **Man In The Middle attack** is a type of **cyberattack** where a malicious actor **inserts herself into a conversation between two parties**, impersonates both parties and gains access to **information** that the two parties were trying to send to each other.
- MITM attack allows an attacker to **intercept, send and receive data meant for someone else**, or not meant to be sent at all, **whitout either outside party knowing** until it is too late.

Some protective measures against this type of attack

- Make sure **HTTPS** is always in the URL bar of the websites you visit.
- **Never** connect to **public** Wi-Fi routers **directly.**
- If you can, use a **VPN.**
- **Update** your softwares.
- Be wary of potential **phising emails** from people asking you to **update** your password or other credentials.
- **Type manually the website address** into your brower.

*Follow **@SecurityGuill** on **Twitter** for more about **Infosec** / **Cybersecurity***

NETWORK-BASED ATTACKS: DNS POISONING

José Manuel
Redondo López

What is DNS Poisoning & How it works?

By @SecurityGuill

What is it?

• This attack **deceive DNS servers** to make them believe that they receive a **valid response** to a request they make, while the request is **fraudulent**.

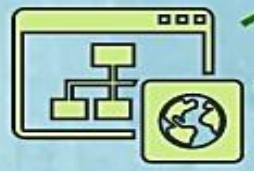
How it works?

• The attacker accesses **client DNS server** (using a flaw, a malware, an injection ...).
• He **injects fake DNS entry**
• The **client** sends a request. **asking** for the **real website**
• Request **resolves** to the **attacker website.**

1 : The attacker **injects fake DNS entry**

2 : The client sends a request asking for the real website

3 : Request resolves to the fake website



Protection measures

• A secure version of the DNS exists, **DNSSEC**, which is based on **electronic signatures** with a **certificate** that verifies the **authenticity of the data.**
• The same goes for other applications such as **browsers** that can **verify the authenticity of a page thanks to the certificates.**

Example

• This can redirect you to a **phishing website** (with interface of your bank for example), whose URL is identical to that of your bank's website.

Follow @SecurityGuill on Twitter for more things about Infosec!

NETWORK-BASED ATTACKS: DDOS

José Manuel
Redondo López

- **Attacks of this type are typically launched by botnets…**

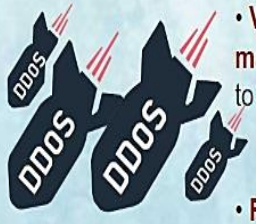
What is DDoS attack ? 1/2

By @Guillaume_Lpl

What is it?

• A **distributed denial of serivce** (DDoS) attack is a **brute-force** attempt to slow down or completely **crash a server.**

• The goal of a DDoS attack is to **cut off users from a server or network resource** by overwhelming it with **requests for service**.



DoS vs DDoS

• While a simple denial of service (DoS) involves **one attack computer and one victim**, distributed denials of service (DDoS) rely **on armies (thousands) of infected "bot" computers** (take a look at the infographic about **Botnet**!) able to carry out tasks **simultaneousl**.

Common types of DDoS attacks

• **Volume based** : include **UDP, ICMP and many other spoof-packet floods** that attempt to **consume bandwidth**.

• **Protocol attacks** : go after server ressources directly and include the **Smurf DDoS, Ping of Death and SYN floods**. If a large enough packets-per-second rate is achieved, the server will crash.

• **Application layer** : like Zero-Day DoS, they target apps by making what appear to be **legitimate requests (GET/POST) but at a very high volume**. If there are **enough requests in a short enough time period**, the victim's server shuts down.

Follow @Guillaume_Lpl on Twitter for more things about Infosec!

What is DDoS attack ? 2/2

By @Guillaume_Lpl

Impact of DDoS Attacks

• Depending on the severity of an attack, **resources could be offline for 24 hours, days, or even weeks**.

• **Money, time, clients, reputation** can be lost.

• During an attack, **no employees are able to access network ressource**, and in the case of Web servers running **eCommerce sites, no consumers will be able to purchase products or receive assistance**.

Some protection measures against DDoS attack

• **Limit the number of login** attempts any user can make before being "locked out" of an account.

• Tolerate a **web-server configuration against DDoS attacks**.

• Alter an **ISP firewall** to allow only the traffic complimenting to the services on the **company side.**

• Tweak a **firewall to fight SYN flood attacks**.

• Migrate public resources to **another IP address**.

• and more...

Follow @Guillaume_Lpl on Twitter for more things about Infosec!

NETWORK-BASED ATTACKS: BOTNET

José Manuel
Redondo López

What is a Botnet & How it works ? 1/2

Definition :

♦ **Botnets** consist of a group of computers known as "**zombie**", computers that have been **compromised** and that can be **controlled** by attackers with malicious intent **whithout users knowing it.**

♦ Any **internet connected device is able to be infected** : Computers, Smartphones, IoTs (IP cameras, TV, routers, ...)

Some uses for a Botnets :

♦ Commit **advertising fraud**

♦ Steal your **private data**

♦ **DDoS** attack

♦ **CryptoCurrency** mining

♦ Send **spam emails**

♦ **Brute force** attack

The most notorious Botnets :

♦ **Mirai** : he works by scanning the internet for IP add of **IoTs** devices.

- September 2016 attack on the **security blog of Bryan Krebs**. (DDoS attack)
- The October 2016 attack, where **Dyn DNS** was targeted : impact took **Twitter, Amazon, Netflix** ... (DDoS)

♦ **Zeus** : speards in the same way as Mirai.

- Zeus compromised **Bank of Ameriac, NASA, ABC, CISCO, Amazon** and others with **CyproLocker Ransomware spreading**

Follow **@Guillaume_Lpl** for more

What is a Botnet & How it works ? 2/2

by @Guillaume_Lpl

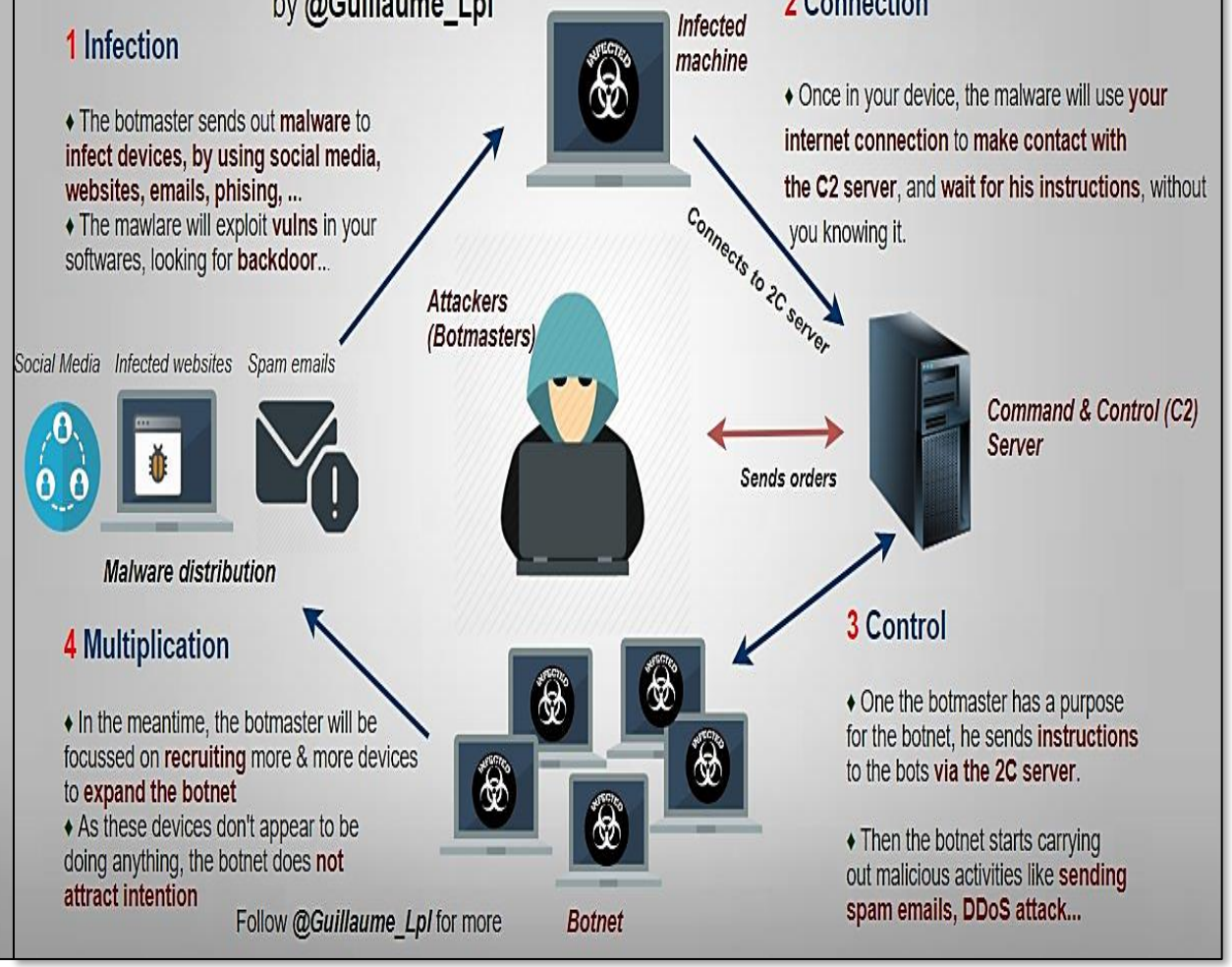
1 Infection

♦ The botmaster sends out **malware** to **infect devices, by using social media, websites, emails, phising, ...**

♦ The mawlare will exploit **vulns** in your softwares, looking for **backdoor**..

2 Connection

♦ Once in your device, the malware will use **your internet connection** to **make contact with the C2 server**, and **wait for his instructions**, without you knowing it.



3 Control

♦ One the botmaster has a purpose for the botnet, he sends **instructions** to the bots **via the 2C server**.

♦ Then the botnet starts carrying out malicious activities like **sending spam emails, DDoS attack...**

4 Multiplication

♦ In the meantime, the botmaster will be focussed on **recruiting** more & more devices to **expand the botnet**

♦ As these devices don't appear to be doing anything, the botnet does **not attract intention**

Follow **@Guillaume_Lpl** for more

More information: https://www.osi.es/servicio-antibotnet

< Go to Index

Source: zona-militar.com

Network attacks >

SNI >

Secure Network Design Principles

How to create a truly secure network

Network attacks and Insecure Designs

How networks are attacked nowadays

Network attacks today

José Manuel
Redondo López

- **Current cyberattacks look to exploit the weakest link in the network**
- **Evolving cybersecurity defenses put strong defenses on network perimeters**
  - Stateful firewalls, Intrusion Detection Systems (IDS), network access segmentation, VLANs…
  - Increased employee awareness
- **But the pure network perimeter is no longer the weakest link**
  - So, what it is attacked nowadays network-wise?

Network attacks today

José Manuel
Redondo López

- **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
    - Employees are not covered by their defenses
  - Connection via VPN bypasses most of these defenses
    - Client - network communication through VPNs usually cannot be inspected
  - Malware can then be “injected” from the client computer to the company’s network
- **Cloud**
  - **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

José Manuel
Redondo López

- **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
  - The goal is to obtain employee credentials, gaining access to the 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?

José Manuel
Redondo López

- **Use a multilayered approach**
- **Don't get rid of existing security solutions**
  - Perimeter defenses are just one layer of the multi-layered approach, not the only one
- **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 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 like pfSense or IPFire can do that with a Squid proxy plugin (ASR)

Network attacks today: What to do?

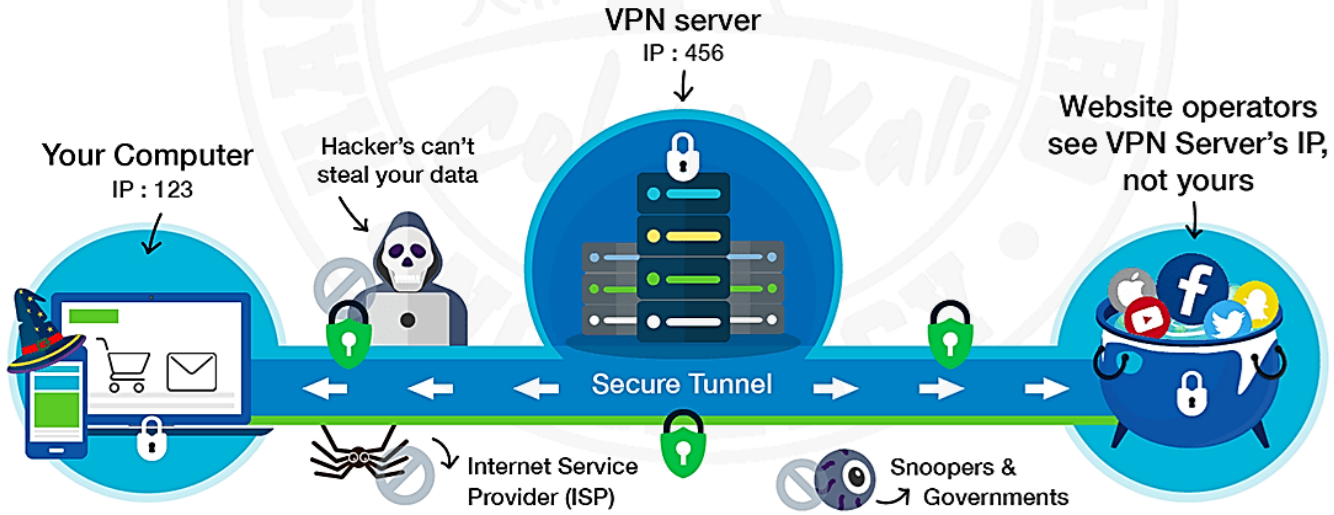
José Manuel
Redondo López

- **Endpoint detection**
  - Continuously monitor endpoints for suspicious activity
  - And send responses in real time when potentially malicious behavior is detected
  - **Intrusion Detection Systems** (IDS), **Intrusion Prevention Systems** (IPS), **SIEM**…
    - E. g.: 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**
  - Choose a remote browser isolation solution
  - Protecting users from zero-day attacks, unauthorized downloads, malicious content…
- **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?

José Manuel
Redondo López

- **Remote access controls**
  - Secure remote connections with strong gateways, VPNs…
  - 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

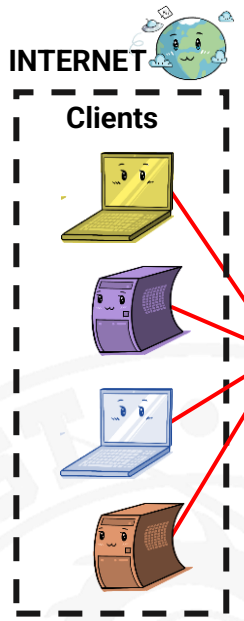


Source: https://blog.360totalsecurity.com/en/how-vpn-works

INADEQUATE NETWORK DESIGNS

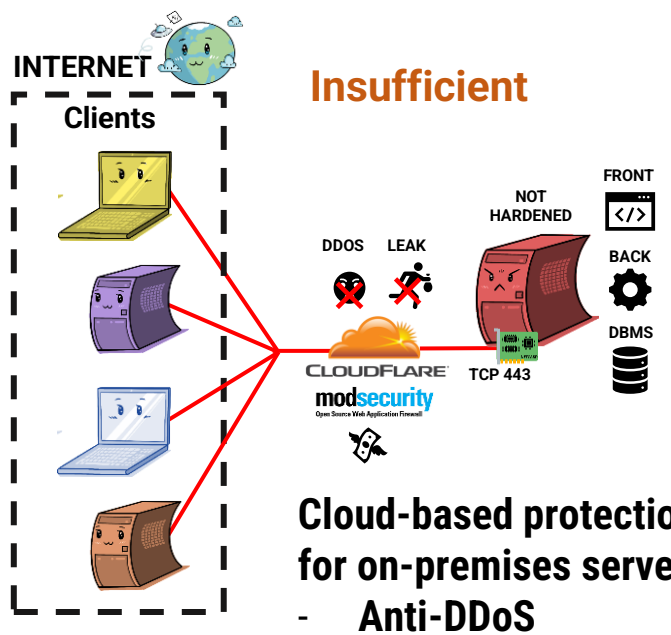
José Manuel Redondo López

- **All network security solutions turn them much 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)



Totally inadequate

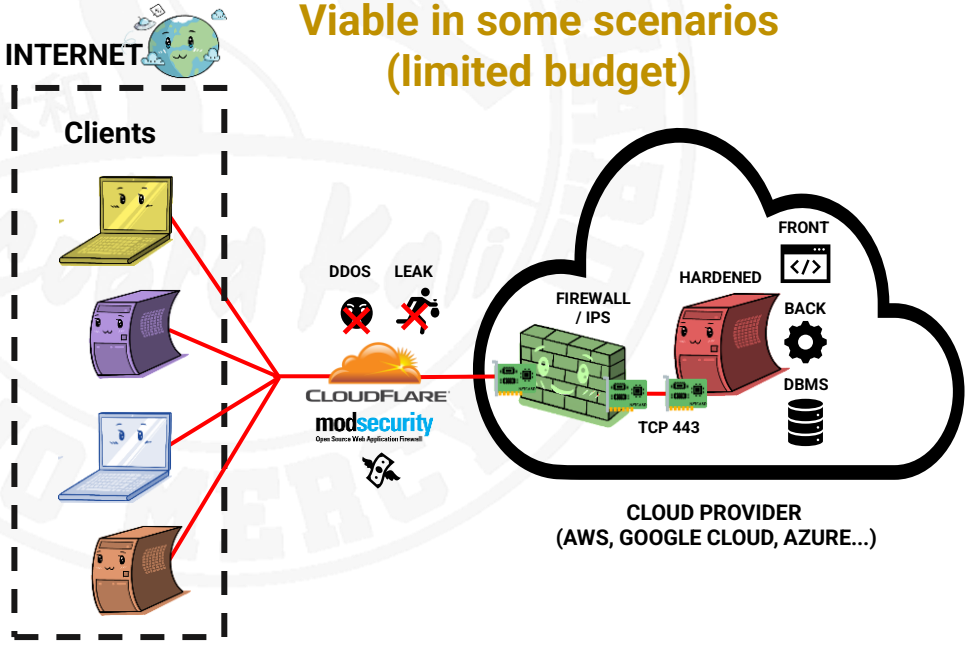
On-premises (local) single server with every app layer



Insufficient

Cloud-based protection for on-premises server
- **Anti-DDoS**
- **WAF**
- **Traffic filtering**
- **HTTPs only**

Viable in some scenarios (limited budget)



Cloud-based hosting
- **Hardened machines (CIS, STIGs)**
- **Automatic updates**
- **Perimetral defenses**
- **Firewall rules**
- **…**
- **(But only if we pay for them)**

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

José Manuel
Redondo López

- **Cloud solutions may still have application-based security problems (topic 6)**
  - The code must follow a methodology/rules for **secure application development**
  - 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
  - We must know how to properly arrange / setup **communications** between the different machines we put on the cloud, using the vendor tools
    - Again, we must know what we are doing to take advantage of the cloud provider features
  - We might have something in production that we **don't really/fully understand or control**
    - Relying only on third-party products is not enough
    - **Cybersecurity knowledge is needed** to make the most of the tools we pay for

TOWARDS A REAL SOLUTION

José Manuel
Redondo López

- **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 (Firewalls, IDS, IPS, SIEMs…see 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**
  - All or part of these elements can be deployed in a cloud provider
  - To save management cost / money (private, public, hybrid clouds)

Secure Network Infrastructure (SNI)

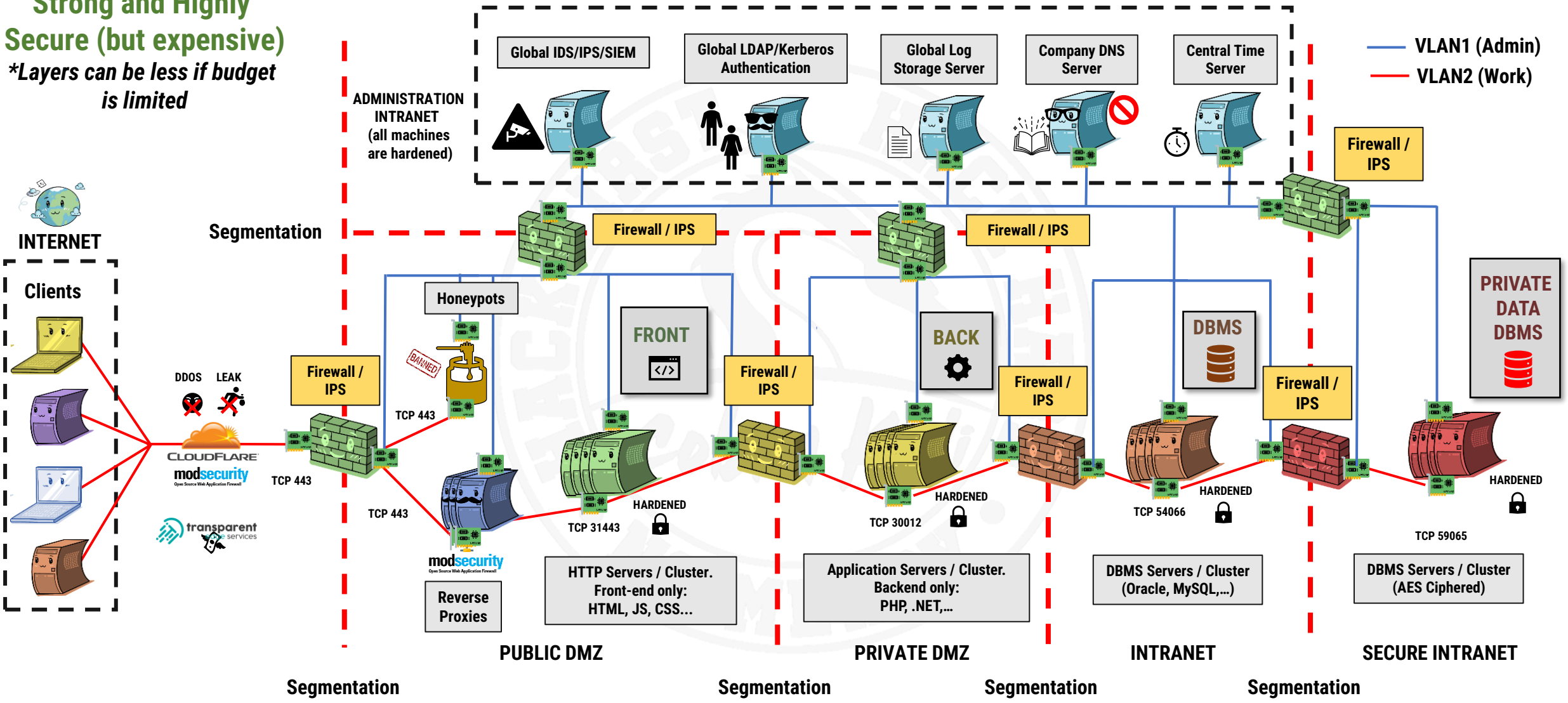
How to design a strong network architecture

SECURE NETWORK INFRASTRUCTURE (SNI)

José Manuel
Redondo López

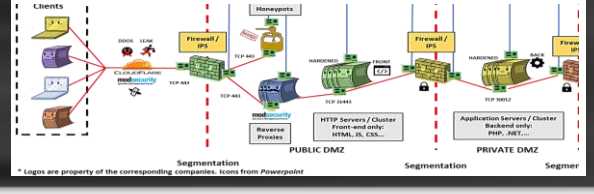
Strong and Highly Secure (but expensive)

Layers can be less if budget is limited



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

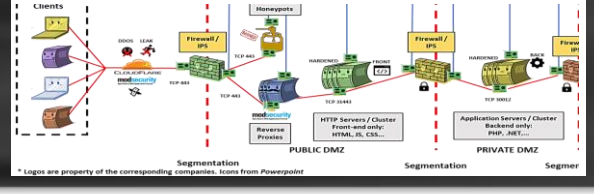
SNI: Main components



José Manuel
Redondo López

- **A secure configuration baseline for all servers**
  - Infrastructure OS and services are configured and secured using an adequate **security framework** (ISO 27001)
    - Based on validated security control lists (CIS, STIGs, …previous topic)
    - 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**
    - **Webmail, browsing, watch videos…**
- **"External" network and application firewalls (WAF)**
  - Reduce threats from application-based attacks (code injections, etc.) that network firewalls cannot detect
  - Individual host-based PF firewalls, only opening authorized ports, for each server: `ufw`, `firewalld`

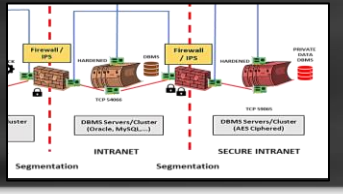
SNI: Main components



José Manuel Redondo López

- **Two double-firewalled 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
    - 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.)

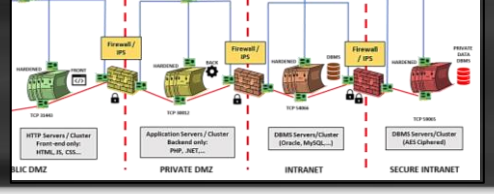
SNI: Main components



José Manuel Redondo López

- **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 don't do that here)
    - We want our public-facing services to be reachable in the usual places
  - Web services must use **ALWAYS** an adequate encryption (`tcp/443`)
  - Non-standard TCP and UDP ports are 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

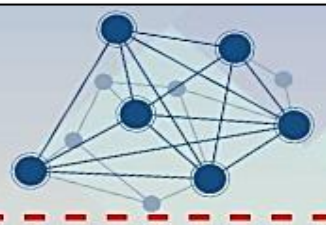


José Manuel
Redondo López

- **The configuration of the network firewalls is critical**
  - **Rules** must be configured to **strongly restrict and control** inbound and outbound traffic
  - We must 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

HONEYPOTS

José Manuel
Redondo López



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**.

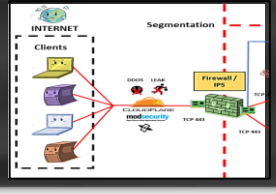
- The risks are many since our device is intended to be **compromised**. One of the advantages of this solution is that it's possible to obtain **more information** about attackers.

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***

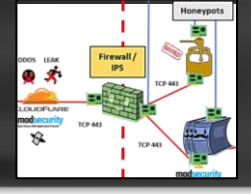
SNI: Content Delivery Network (CDN)



José Manuel Redondo López

- **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**

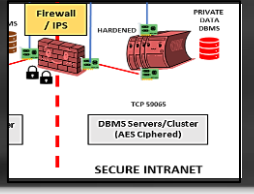
SNI: Public DMZ



José Manuel Redondo López

- **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

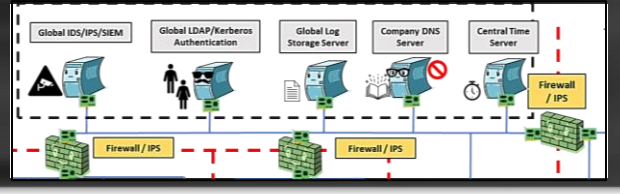
SNI: SECURE LAN



José Manuel Redondo López

- **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 cryptography topic)
  - Can only be retrieved through **a very strict security policy**
    - An **extremely limited number** of systems, network administration staff / apps, and application processes 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 approved, information is decrypted for processing needs
    - Those information outflows are severely restricted, documented in detail, and restricted by firewalls
    - Also monitored and approved by management **to comply with the current law**

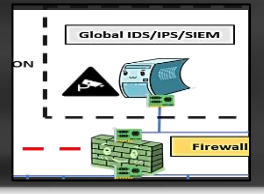
SNI: Administration LAN



José Manuel Redondo López

- **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)
  - System log (syslog) server(s) (`syslog`)
- **All these servers are also firewalled from the DMZs and the secure LAN**
  - To allow better control and protection

SNI: ADMINISTRATION LAN. GLOBAL IDS/IPS/SIEM



José Manuel
Redondo López

- **This architecture has properly managed network-based (NIDS) and host-based intrusion-detection system(s) (HIDS)**
  - **NIDS** (Suricata, SNORT…) **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: OSSEC, AIDE, tripwire…
- **NIDSs and HIDSs send information to an intrusion-detection console system in the management LAN for tracking and monitoring**
  - Alienvault OSSIM (SIEM) is an event management system able to do that

IDS/IPS

José Manuel
Redondo López

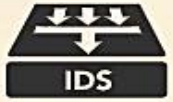
What is IDS & IPS ?

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**.

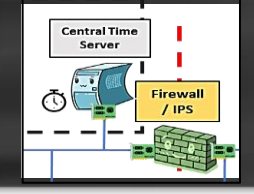
• IPS systems proactively **reject network packet** based on a **security profile** if these packets represents a **known threat**.

• 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

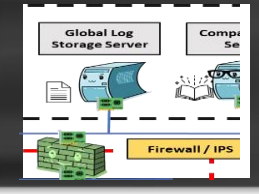
SNI: Administration LAN. Central time server



José Manuel Redondo López

- **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
  - 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

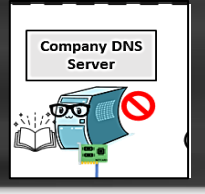
SNI: Administration LAN. Global log storage servers



José Manuel Redondo López

- **Capturing 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 Storage Area Network (SAN) device
  - 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 recording 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)

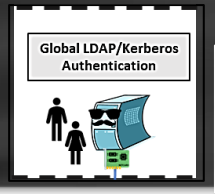
SNI: Administration LAN. Company DNS servers



José Manuel Redondo López

- **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 supporting user interaction
      - Like having an adblocker plugin without installing one and **working with all devices** passing through the DNS
      - Not only web browsers!
      - Therefore, reducing the probability of attacks
    - Example: **PiHole** (https://pi-hole.net/)
  - We can also block connections to certain web sites for other reasons
    - Any non-blocked requests for DNS should be forwarded to the Internet service provider's (ISP) DNS servers
    - For resolution or further forwarding
- **However, because of potential threats to DNS servers, consider relying on the ISP's DNS for public queries**

SNI: Administration LAN. Global Kerberos / LDAP authentication



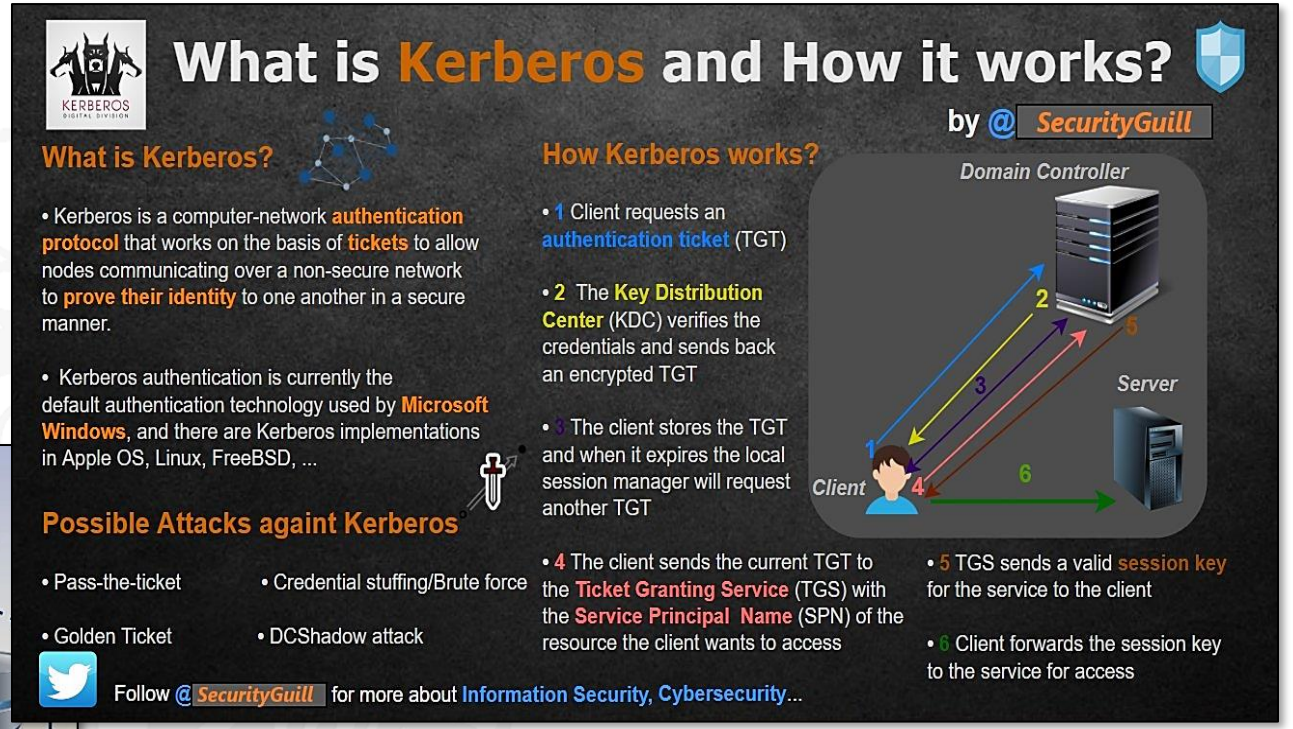
José Manuel Redondo López

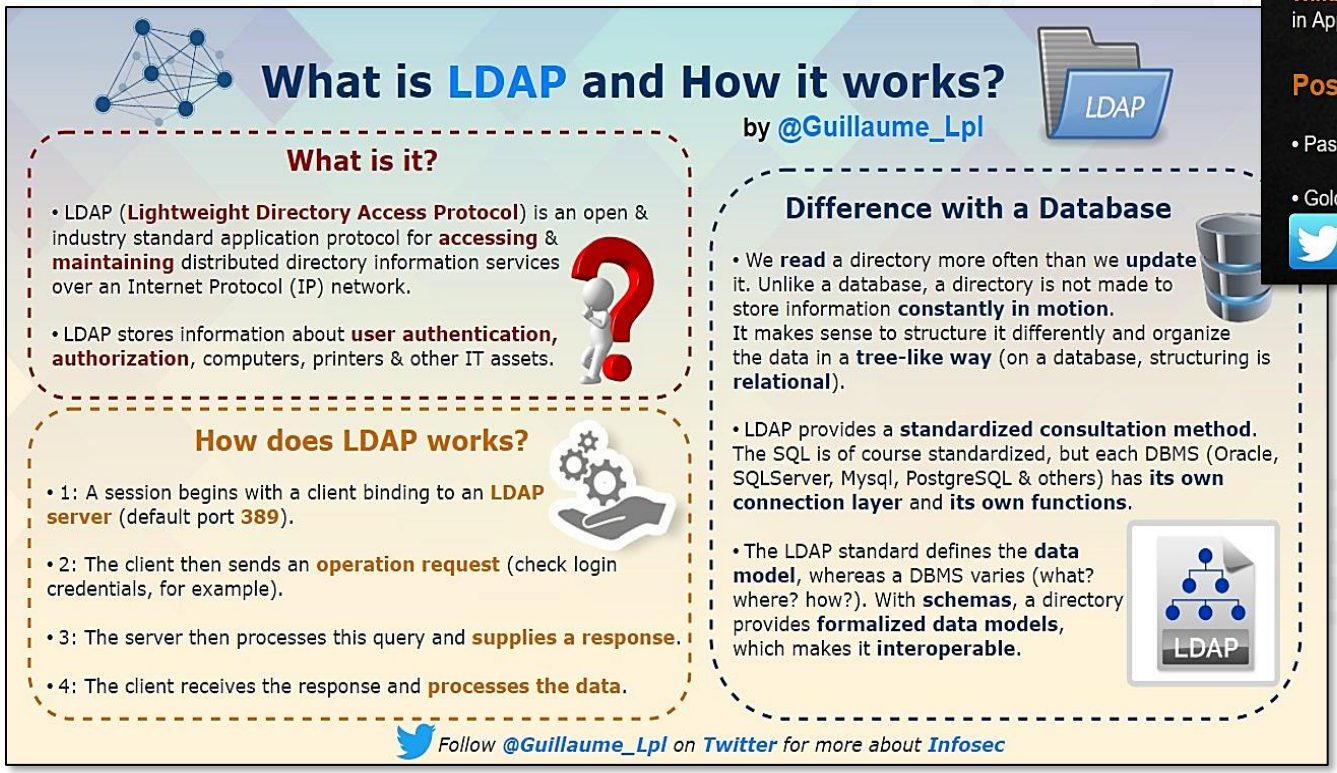
- **The Kerberos authentication protocol is one of the most secure ones**
  - Supported by all major popular OS (more details in ASR)
  - Kerberos uses strong cryptography so a client can prove its identity to a server (and vice versa) through an insecure network connection
  - After that, they can also 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 MitM 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 authentication mechanism can be used as a complement**

KERBEROS / LDAP

José Manuel
Redondo López

THESE DIAGRAMS ARE PROVIDED ONLY AS REFERENCE



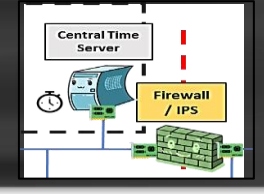


SNI: Extra security measures: Subnetting

José Manuel
Redondo López

- **Several enhancements can increase the security level of the base 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
  - The complexity of the network architecture
- **But also, significantly reduces…**
  - The likelihood that an attacker gaining access to systems
  - The implementation time to fine-tune the network monitoring activities

SNI: Extra security measures. VLANs



José Manuel Redondo López

- **VLANs logically segregate network traffic**
  - Used to separate traffic based on its “risk”, quality of service, or other considerations
  - 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

SNI: Extra security measures. VMs

José Manuel
Redondo López

- **Nowadays, most of the complex machine infrastructures are implemented through virtual machines or containers**
- **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: VMs can be regenerated**
  - If a HIDS detects that a server has been corrupted, it can be configured to reboot it
    - But a second “clean” hot-swappable image will replace the corrupted one
  - 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 immediately removed due to this response mechanism

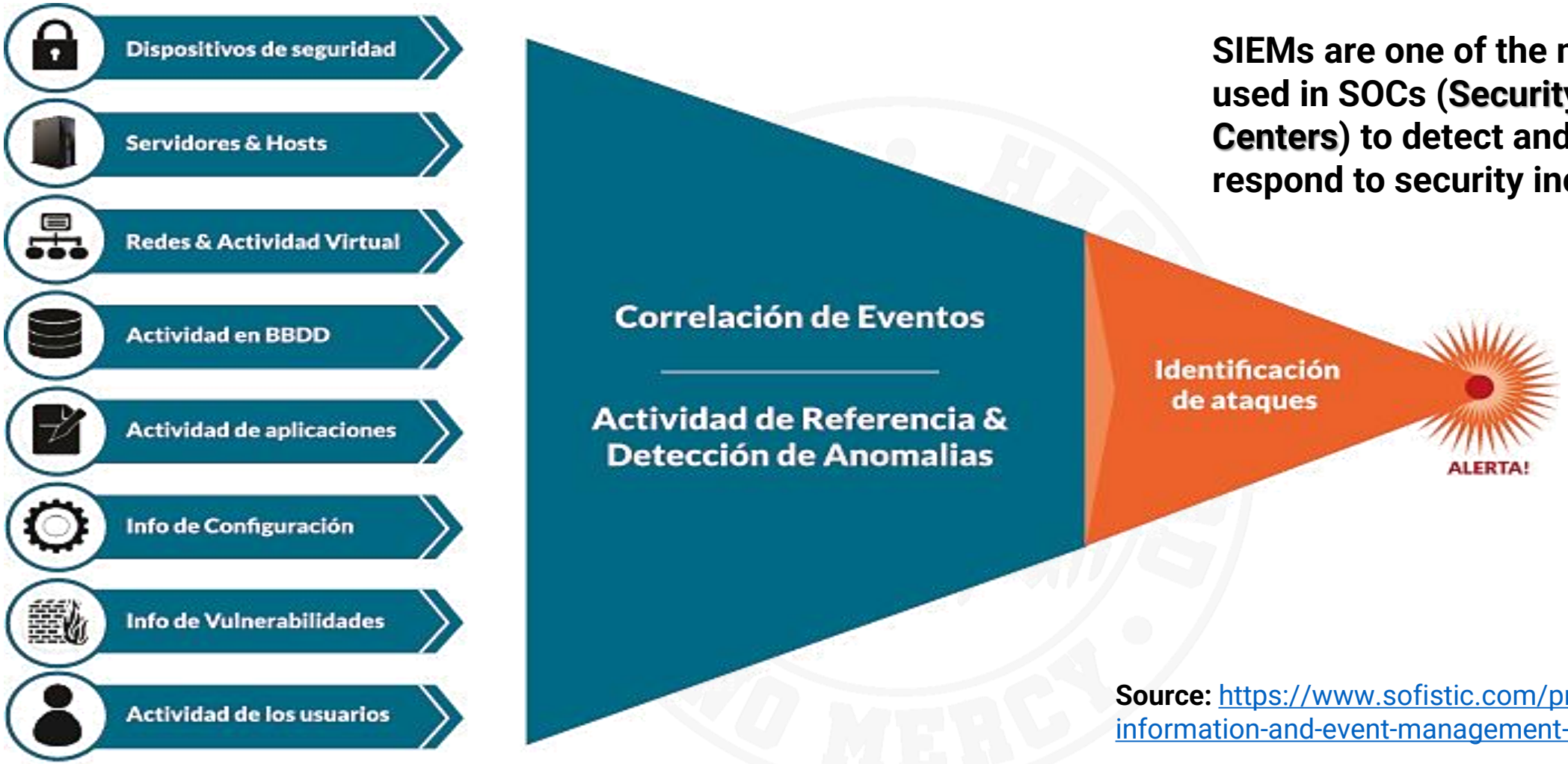
SNI: Extra security measures. IDS correlation engine

José Manuel
Redondo López

- **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 syslog and alert information (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 **IA 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**)

SNI: Extra security measures. IDS correlation engine

José Manuel
Redondo López



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/

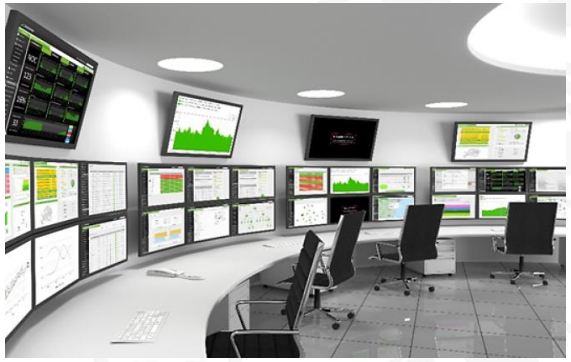
Fuentes de datos extensivas + Inteligencia = Visión práctica y extremadamente precisa

SECURITY OPERATIONS CENTER (SOC)

José Manuel
Redondo López

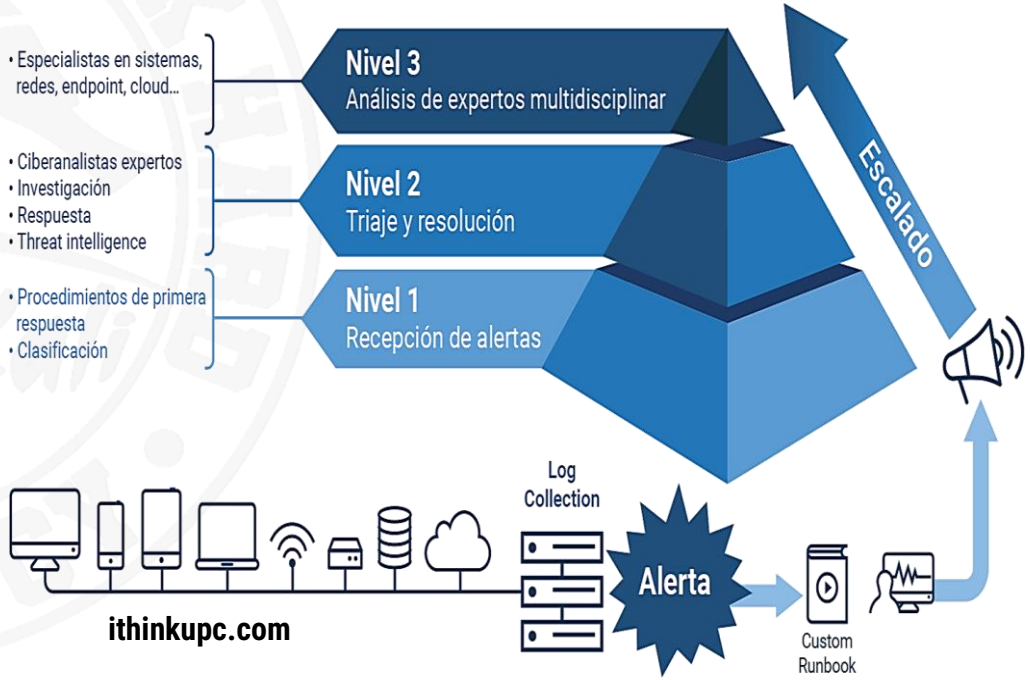
- It is important to understand what a SOC is, and how it performs surveillance
- There are many open positions to work in them!

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

< Go to Index

Source: zona-militar.com

Active scanning >

Gathering info >

Other techniques >

Introduction to Network Pentesting

How to check the security of a network

THE MITRE ATT&CK

https://attack.mitre.org/

José Manuel
Redondo López

- **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 next topic) 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

José Manuel
Redondo López

- **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 CIS Benchmark technical security control to "**fight against**" 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

José Manuel
Redondo López

- **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**

T1595: Active Scanning

Probing the adversary to obtain information about it

T1595: Active scanning

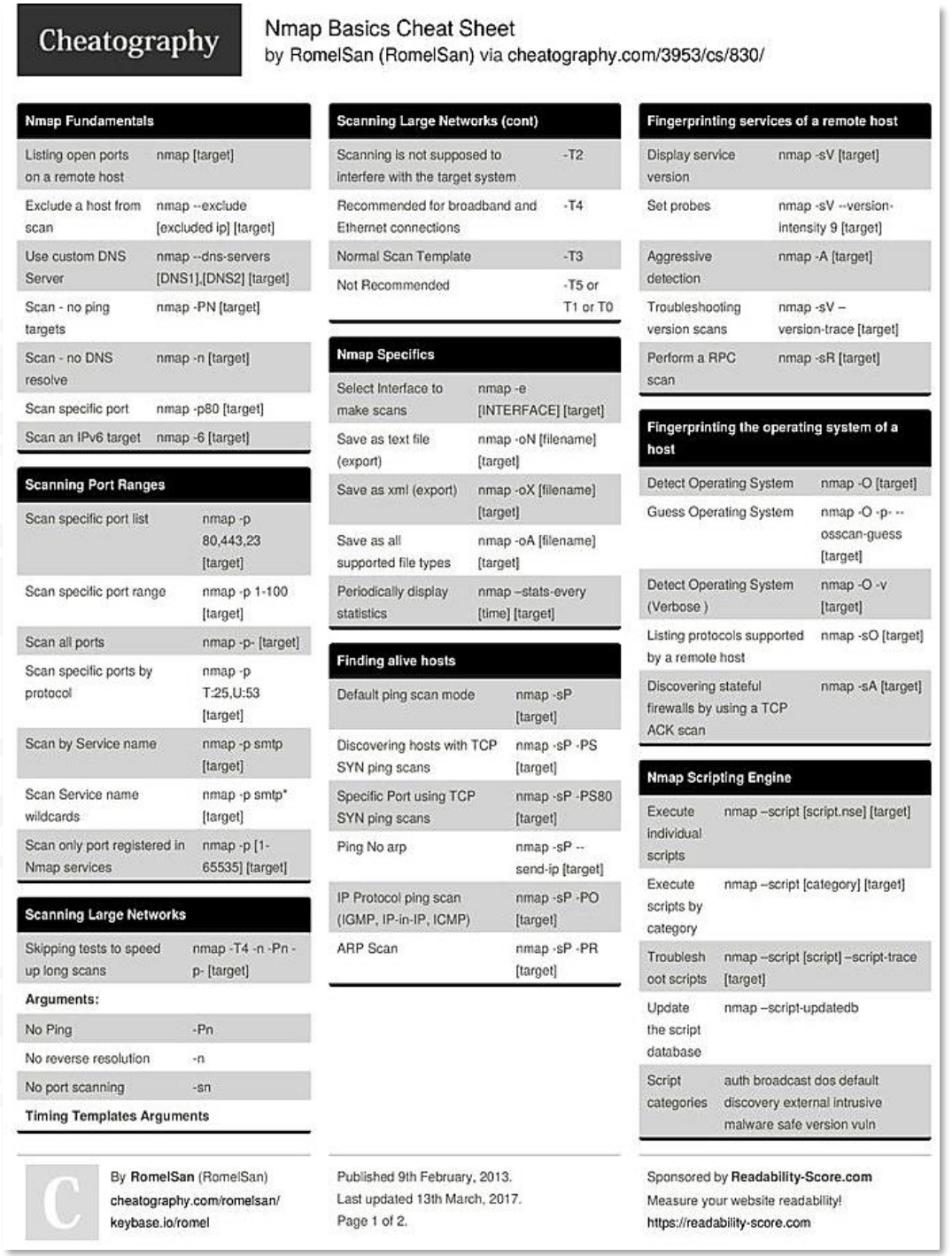
José Manuel
Redondo López

- **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
  - 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**
- **Automated vulnerability scan software (Seminar 3) can also be included in this category**

ACTIVE SCANNING TECHNIQUES

José Manuel
Redondo López

- **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 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. QUICK NMAP ENUMERATION

José Manuel
Redondo López

- `nmap --top-ports 20 --open` **gives us a quick and effective scan**
  - Scans the statistically N most used ports worldwide (N is 20 in this example)
  - Only shows ports open or half-open (special state)
  - If we add the `-il <file>` option, it will scan multiple Ips read from a file
- **This is recommended to quickly identify the type of target and what it runs**
  - **Advisable before perform a "deeper" scan**
- **Labs 8-9 study `nmap` possibilities**
  - Providing cheatsheets to facilitate your work

```
root@kali:~# nmap --top-ports 20 --open 192.168.14.2
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-02 13:10 CEST
Nmap scan report for 192.168.14.2
Host is up (0.00066s latency).
Not shown: 14 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:D5:89:36 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
root@kali:~#
```

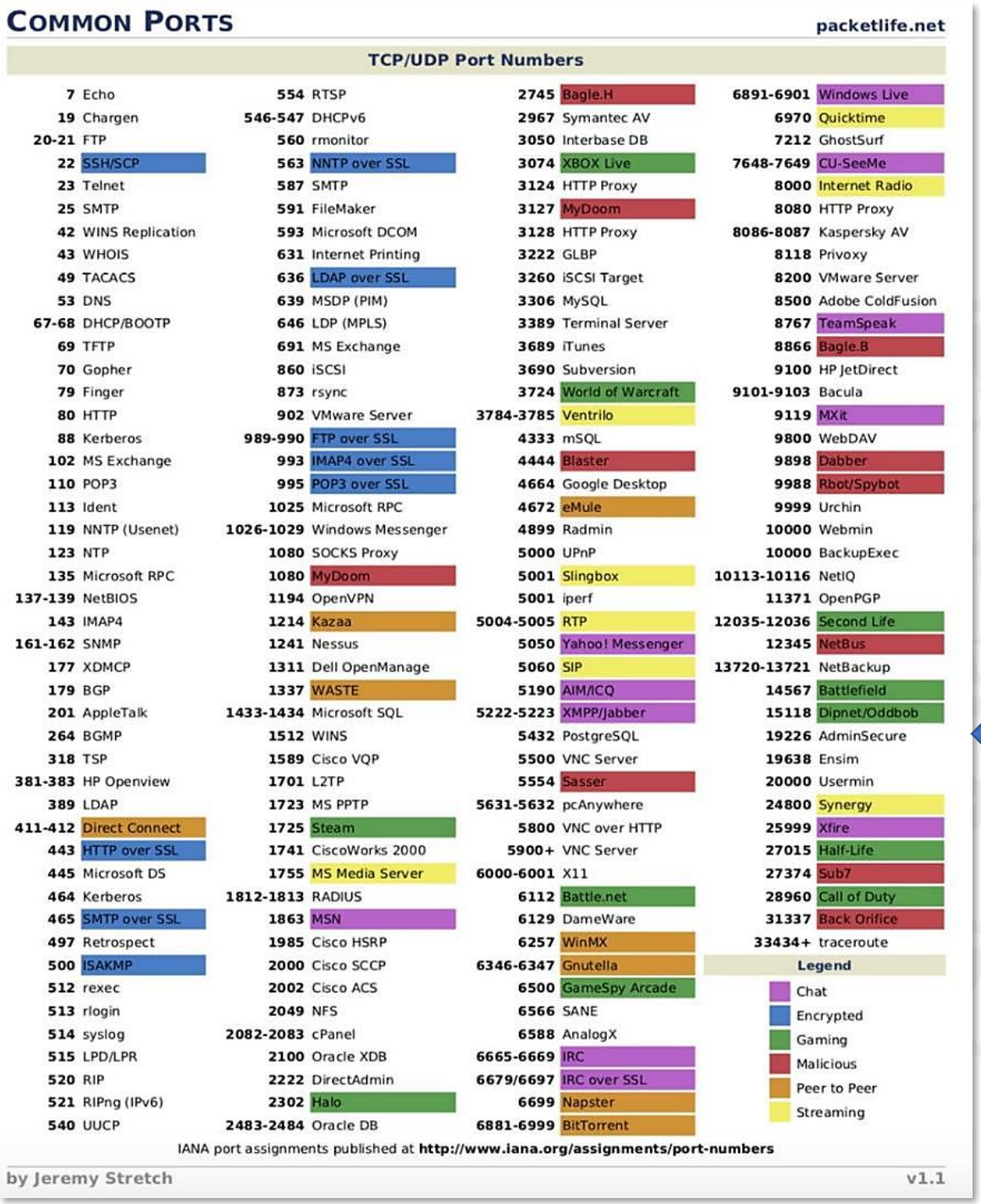
Active scanning. Nmap. What does this mean?

José Manuel
Redondo López

```
root@kali:~# nmap --top-ports 20 --open 192.168.14.2
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-02 13:10 CEST
Nmap scan report for 192.168.14.2
Host is up (0.00066s latency).
Not shown: 14 closed ports
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
23/tcp  open  telnet
80/tcp  open  http
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:D5:89:36 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
root@kali:~#
```

Services running in the target machine: each one may be an opportunity to acquire further information, identify vulnerabilities, or launch exploits: we have 6 different potential ways of going forward

VirtualBox virtual machine



Common Ports

packetlife.net

TCP/UDP Port Numbers

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

Legend

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

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

by Jeremy Stretch v1.1

```
# Nmap 6.40 scan initiated Fri Sep  5 16:51:52 2014 as: nmap -sS -oN portsopen 1
92.168.89.191
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.89.191
Host is up (0.00069s latency).
Not shown: 982 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1030/tcp open  iad1
1033/tcp open  netinfo
1034/tcp open  zincite-a
1035/tcp open  multidropper
```

- Port numbers bellow 1024 are normally assigned to well-known services
- Port numbers over 1000 are "free“, although some known services are typically there
- Unknown open ports may indicate malware presence!

Active Scanning: Nmap detailed scan

José Manuel Redondo López

- `nmap -sS -A -sV -O -p -` **runs a more detailed and slower scan**
- **Recommended to obtain more information about a 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).
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, NetBIOS user: <unknown>, NetBIOS MAC: <unkno
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+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
```

Active scanning. Interpreting nmap results: Linux example

José Manuel
Redondo López

```
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; 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:
```

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

The owner gave us the running Ubuntu version for free ☺. It could be fake, but in this case it's unlikely. 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 OS). Again, with this we can search for specific vulnerabilities of this version

SMB installation data

Active scanning. Scanning services: web

José Manuel
Redondo López

- **If the target has HTTP services running, there are a series of programs we can use to enumerate them specifically**
  - Burp proxy for deep HTTP Request / Response inspection (described in seminars)
  - HTTP directory enumeration tools
    - `dirb` (https://tools.kali.org/web-applications/dirb)
    - `dirbuster` (https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project/es): Like `dirb`
    - `gobuster` (https://github.com/OJ/gobuster): Brute-force tool to enumerate
      - URIs (directories and files)
      - DNS subdomains
      - Virtual hosts (different web pages on the same server)
  - CMSs identification tools
    - `wpscan` (https://github.com/wpscanteam/wpscan)
    - `droopescan` (https://github.com/droope/droopescan): CMS security scanner with a built-in plugin system
      - Allowing it to work with several ones
    - `Joomscan` (https://github.com/rezasp/joomscan): Open-source project to automate the detection of vulnerabilities on websites that use the **Joomla** CMS

ACTIVE SCANNING: HTTP ENUMERATION EXAMPLE. DIRB

José Manuel Redondo López

- **Searches hidden web content**
  - Unlinked directories, hidden websites,
  - "secret" parts (/admin, /login, /debug, /auth...)…
- **Detects "hidden" website parts**
  - Unlinked web pages
- **You may find hidden files by adding extensions to found files**
  - It can lead to downloading the source code of an application or other important files
    - E. g.: If we have a .php we can try to get .php.bak, .php.2, .php.old...
    - It can also be tested with .conf, .db, .txt...
  - A URL that ends in a directory name (no page) can generate a list of its contents
    - All your files would be visible to download!

dirb 2.22 Cheatsheet (ingenieriainformatica.uniovi.es)

HTTP directory and content discovery tool

https://tools.kali.org/web-applications/dirb

GENERAL USAGE

```
./dirb <url_base> [<wordlist_file(s)>] [options]
```

NOTES

```
<url_base> : Base URL to scan. (Use -resume for session resuming)
<wordlist_file(s)> : List of wordfiles. (wordfile1,wordfile2,wordfile3...)
```

HOTKEYS

```
'n' -> Go to next directory.
'q' -> Stop scan. (Saving state for resume)
'r' -> Remaining scan stats.
```

OPTIONS

```
-a <agent_string>: Specify your custom USER_AGENT.
-c <cookie_string>: Set a cookie for the HTTP request.
-f: Fine tunning of NOT_FOUND (404) detection.
-H <header_string>: Add a custom header to the HTTP request.
-i: Use case-insensitive search.
-l: Print "Location" header when found.
-N <nf_code>: Ignore responses with this HTTP code.
-o <output_file>: Save output to disk.
-p <proxy[:port]>: Use this proxy. (Default port is 1080)
-P <proxy_username:proxy_password>: Proxy Authentication.
-r: Don't search recursively.
-R: Interactive recursion. (Asks for each directory)
-S: Silent Mode. Don't show tested words. (For dumb terminals)
-t: Don't force an ending '/' on URLs.
-u <username:password>: HTTP Authentication.
-v: Show also NOT_FOUND pages.
-w: Don't stop on WARNING messages.
-X <extensions> / -x <exts_file>: Append each word with this extensions.
-z <milisecs>: Add a miliseconds delay to not cause excessive Flood.
```

EXAMPLES

```
./dirb http://url/directory/ (Simple Test)
./dirb http://url/ -X .html (Test files with '.html' extension)
./dirb http://url/ /usr/share/dirb/wordlists/vulns/apache.txt (Test with apache.txt wordlist)
./dirb https://secure_url/ (Simple Test with SSL)
```

Active scanning: Dirb. Linux example

José Manuel Redondo López

- **We see that Apache serves a phpMyAdmin, which implies**
  - Another attack vector, another product with potential vulnerabilities
  - The server has/works with a MySQL or similar
  - It retains unnecessary documentation / default files (sloppy installation?)
  - Many routes to look at its contents
- **This may locate installed products that are worth analyzing**
  - dirbuster and gobuster are similar
  - We can also use different wordlists

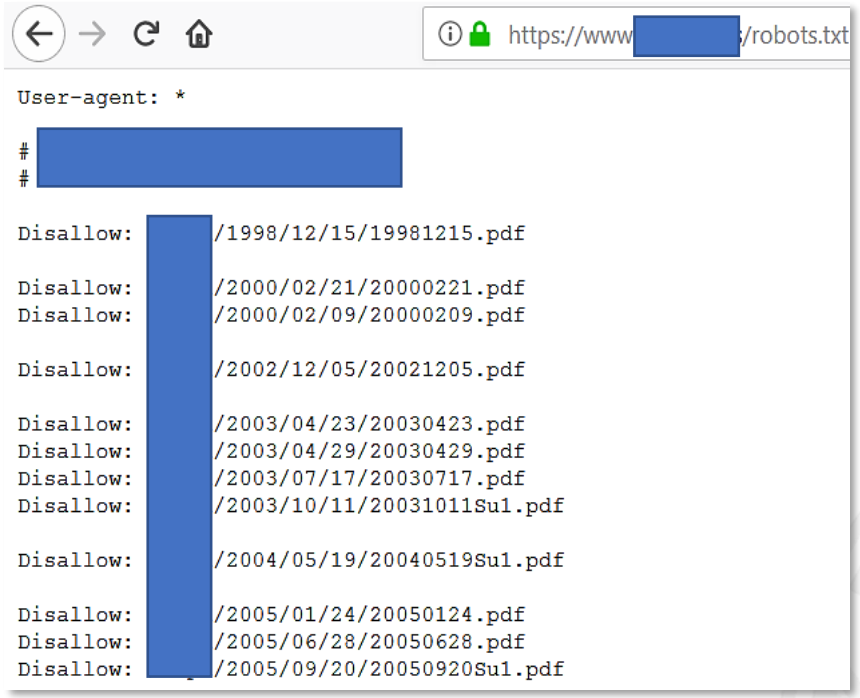
```
root@kali:~# dirb http://192.168.14.2

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Oct  2 14:54:34 2019
URL_BASE: http://192.168.14.2/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.14.2/ ----
+ http://192.168.14.2/index.html (CODE:200|SIZE:10918)
+ http://192.168.14.2/index.php (CODE:200|SIZE:95195)
==> DIRECTORY: http://192.168.14.2/javascript/
==> DIRECTORY: http://192.168.14.2/phpmyadmin/
+ http://192.168.14.2/server-status (CODE:403|SIZE:277)

---- Entering directory: http://192.168.14.2/javascript/ ----
==> DIRECTORY: http://192.168.14.2/javascript/jquery/

---- Entering directory: http://192.168.14.2/phpmyadmin/ ----
==> DIRECTORY: http://192.168.14.2/phpmyadmin/doc/
+ http://192.168.14.2/phpmyadmin/favicon.ico (CODE:200|SIZE:22486)
+ http://192.168.14.2/phpmyadmin/index.php (CODE:200|SIZE:10525)
==> DIRECTORY: http://192.168.14.2/phpmyadmin/js/
+ http://192.168.14.2/phpmyadmin/libraries (CODE:403|SIZE:277)
==> DIRECTORY: http://192.168.14.2/phpmyadmin/locale/
+ http://192.168.14.2/phpmyadmin/phpinfo.php (CODE:200|SIZE:10527)
+ http://192.168.14.2/phpmyadmin/setup (CODE:401|SIZE:459)
==> DIRECTORY: http://192.168.14.2/phpmyadmin/sql/
+ http://192.168.14.2/phpmyadmin/templates (CODE:403|SIZE:277)
==> DIRECTORY: http://192.168.14.2/phpmyadmin/themes/

---- Entering directory: http://192.168.14.2/javascript/jquery/ ----
+ http://192.168.14.2/javascript/jquery/jquery (CODE:200|SIZE:268026)

---- Entering directory: http://192.168.14.2/phpmyadmin/doc/ ----
==> DIRECTORY: http://192.168.14.2/phpmyadmin/doc/html/
```

ACTIVE SCANNING. ROBOTS.TXT FILE

José Manuel
Redondo López

- **Part of the Robot Exclusion Standard**
  - Used to indicate search engines that follow it to not to index the entries under the keyword `Disallow`
  - Accessible via: <my web URL>/robots.txt
- **Sometimes this is used to avoid search engines to index "sensitive" content...**
  - But doing this **declares that the content exist!**
  - And anyone can access this `robots.txt` file…
- **If we have files that are not public...**
  - **DON'T UPLOAD THEM TO THE SERVER**
  - Content not linked by any page is not indexed
    - Tools like **dirb** can still find them
  - Protect it with login and password
- **Only use this for public content we don't want to index**

```
User-agent: *
Disallow: /cp/bio
Disallow: /cp/top
Disallow: /news
Disallow: /blogtop
Disallow: /blogbio
Disallow: /bh
Disallow: /cp
Disallow: /showblog
Disallow: /index.php
Disallow: /index2.php
Disallow: /jump.php
Disallow: /past-technology-news
Disallow: /klip
Disallow: /?go=
Disallow: /?option=
Disallow: /?q=
Disallow: /?t=
Disallow: /?webmenu=
Disallow: /%22
Disallow: /c/a/Choosing%20
```



Why hide these specific .pdf files from the results of a search engine?

```
User-agent: *
Crawl-delay: 10
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /INSTALL.sqlite.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips/
Disallow: /user/logout/
Disallow: /node/add/
```

Why is this placed in a production website?

```
User-agent: *
Disallow: /advertise?
Disallow: /biz_share?
Disallow: /biz_attribute
Disallow: /biz_link
Disallow: /biz_update
Disallow: /bookmark?
Disallow: /flag_content?
Disallow: /invite_friends_service?
Disallow: /login?
Disallow: /mail?
Disallow: /map?
Disallow: /redir?
Disallow: /writeareview
Disallow: /signup?
Disallow: /talk/new_topic
Disallow: /thanx?
Disallow: /user_favorites?
Disallow: /weekly/signup
Disallow: /elite?
Disallow: /member_search_results
Disallow: /advertise?
Disallow: /syndicate/
```

Free web app map! If any of these subsections are not supposed to be public, we are now declaring their existence

More information: https://www.synopsys.com/blogs/software-security/robots-txt/

ACTIVE SCANNING. ANALYSIS OF WEBSITE SOURCE CODE

José Manuel
Redondo López

- **It is also convenient to examine a website source code**
- **Everything can contain important information!**
  - Comments with **usernames** / **passwords** (or clues about them)
  - Comments with typical data that **identify certain technologies** / CMS / APIs of the website: default comments from known frameworks (or directly declaring using a specific framework)
  - **"Secret" sections** that have not been "uncovered" by `dirbuster` or similar
  - **IPs/URLs** from other related systems that we previously do not know
  - **Access points** to well-known web services APIs
  - **API Keys**
  - **SGBD connection** strings/addresses
  - ... (anything!)

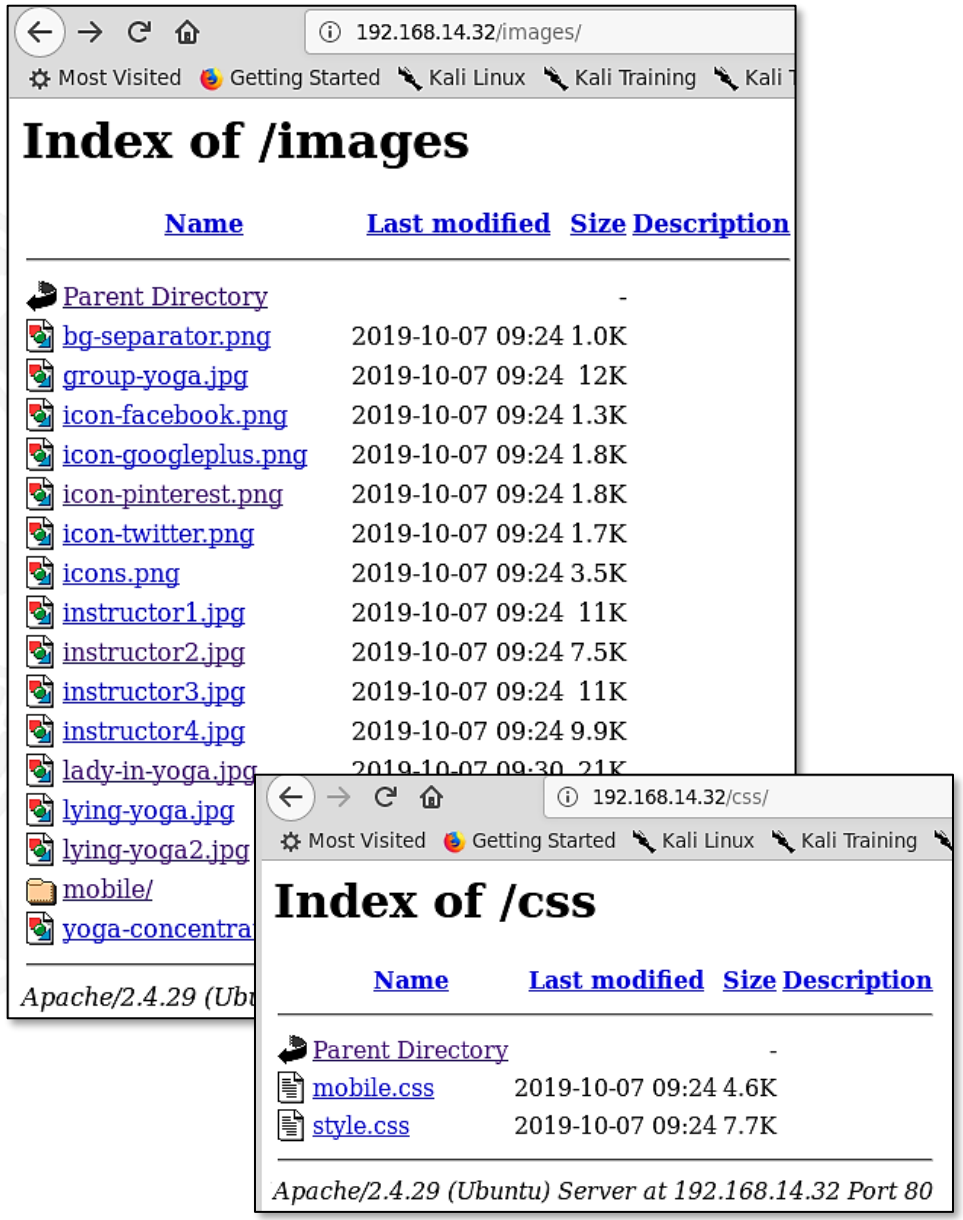
```
    <body>
        <link href="//maxcdn.bootstrapcdn.com/bootstrap/4.1.1/css/bootstrap.min.css" rel="stylesheet" id="bootstrap-css">
<script src="//maxcdn.bootstrapcdn.com/bootstrap/4.1.1/js/bootstrap.min.js"></script>
<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/3.2.1/jquery.min.js"></script>
<div class="d-flex justify-content-center align-items-center" id="main">
    <h1 class="mr-3 pr-3 align-top border-right inline-block align-content-center">Wrong</h1>
    <div class="inline-block align-middle">
        <h2 class="font-weight-normal lead" id="desc">you solved 0 out 3</h2>
    </div>
</div>
<!-- don't forget to remove /puzzle_code_file.zip -->
    </body>
</html>
```

Source: https://ironhackers.es/writeups/resolviendo-retos-de-ctf-parte-1/

Active scanning. Directory listing

José Manuel
Redondo López

- **Directory listings are serious and inadmissible configuration problems**
  - They happen when accessing to a route on the web without indicating a file
  - Instead of a default page, it lists all its contents
  - This allows us to see all the files, whether they are linked on the web pages or not
  - In addition, it gives away the server version
  - And indicates a very lousy administration
- **It is common to find more information, such as**
  - **Backup files with code**: Server code with passwords / users /other hardcoded private information
  - **Unlinked files/folders**
  - **Text/configuration files** with private data



Active scanning. Web fingerprinting

José Manuel
Redondo López

- **Website fingerprinting is a set of techniques to identify the technologies / APIs / products that were used to create them**
  - They can be frameworks or tools with a higher level of abstraction
  - Like CMSs: WordPress, Django, PhpBB...
- **The information we obtain can be contrasted with other sources of data**
  - Such as Nmap scans
  - Product vulnerability pages, CVEs of the products versions
- **There are several tools that serve this purpose. Examples**
  - Whatweb: https://tools.kali.org/web-applications/whatweb
- **Learn more: https://www.owasp.org/index.php/Fingerprint_Web_Application_(OTG-INFO-009)**

ACTIVE SCANNING. WEB FINGERPRINTING

José Manuel
Redondo López

Source: https://esgeeks.com/whatweb-escaner-web-nueva-generacion/

```
$ ./whatweb
[200] AtomFeed[/index.php?format=feed&amp;type=rss], Sc
ript, MetaGenerator[Joomla! 1.5 - Open Source Content Management], HTTPServer[Apache],
Google-Analytics[GA][791888], Apache, IP[ ], Joomla[1.5], Cookies[e964b8ff6
be2b1058b145da14a39e90d], Title[ ], Country[NEW
ZEALAND][NZ]
$ ./whatweb
[200] AtomFeed[/index.php?format=feed&amp;type=rss], Sc
ript, MetaGenerator[Joomla! 1.5 - Open Source Content Management], HTTPServer[Apache],
Google-Analytics[GA][791888], Apache, IP[ ], Joomla[1.5,1.5.19 - 1.5.22], C
ookies[e964b8ff6be2b1058b145da14a39e90d], Title[ ]
n], Country[NEW ZEALAND][NZ]
$ ./whatweb -a 3 -p joomla
[200] Joomla[1.5,1.5.19 - 1.5.22]
```

Whatweb

```
root@kali:~# whatweb
.es
http://.es [301 Moved Permanently] Apache, Citri
x-NetScaler, Cookies[NSC_Qpsubmft143_MC_IUUQ], Country[SPAIN][ES], HTTPServer[Ap
ache], HttpOnly[NSC_Qpsubmft143_MC_IUUQ], IP[156.35. ], RedirectLocation[ht
tp:// ], Title[301 Moved Permanently]
http:// [200 OK] Citrix-NetScaler, Cookies[COOKI
E_SUPPORT_GUEST_LANGUAGE_ID,JSESSIONID,NSC_Qpsubmft143_MC_IUUQ], Country[SPAIN][
ES], Email[ ], HttpOnly[NSC_Qpsubmft143_MC_IUUQ], IP[156.35.33.143],
JQuery[1.7.1], Java, Liferay[5.2.3 (Augustine / Build 5203 / May 20, 2009)][Sta
ndard Edition], Meta-Geo[ ]
, Principado de Asturias, Spain,Oviedo, Principado de Asturias, Spain], Script[t
ext/javascript], Title[ - Inicio], UncommonHead
ers[liferay-portal]
```

ACTIVE SCANNING: WAPITI

José Manuel
Redondo López

- **Popular web security pentesting tool**
  - https://sourceforge.net/projects/wapiti/files
- **Some of its features are**
  - Discovers many potential vulnerabilities
  - Generates vulnerability reports in various formats
  - Pause/resume attacks
  - Modules that implement different attack variants and can be enabled or disabled
  - Supports HTTP proxies and HTTPs
  - Restriction of the scanning scope
- **Tutorials**
  - https://jonathansblog.co.uk/wapiti-tutorial
  - https://www.securitynewspaper.com/2018/11/15/scan-websites-with-wapiti/

Wapiti 3 Cheatsheet (ingenieriainformatica.uniovi.es)

Website vulnerability scanner

https://wapiti.sourceforge.io/

GENERAL USAGE

```
wapiti [-h] [-u URL] [--scope {page,folder,domain,url,punk}]
[-m MODULES_LIST] [--list-modules] [-l LEVEL] [-p PROXY_URL]
[--tor] [-a CREDENTIALS]
[--auth-type {basic,digest,kerberos,ntlm}] [-c COOKIE_FILE]
[--skip-crawl] [--resume-crawl] [--flush-attacks]
[--flush-session] [--store-session PATH] [-s URL] [-x URL]
[-r PARAMETER] [--skip PARAMETER] [-d DEPTH]
[--max-links-per-page MAX] [--max-files-per-dir MAX]
[--max-scan-time MINUTES] [--max-parameters MAX] [-S FORCE]
[-t SECONDS] [-H HEADER] [-A AGENT] [--verify-ssl {0,1}]
[--color] [-v LEVEL] [-f FORMAT] [-o OUPUT_PATH]
[--external-endpoint EXTERNAL_ENDPOINT_URL]
[--internal-endpoint INTERNAL_ENDPOINT_URL]
[--endpoint ENDPOINT_URL] [--no-bugreport] [--version]
```

EXAMPLES

wapiti http://<url> -n 10 -b folder -u -v 1 -f html -o /tmp/scan_report

wapiti http://<url>/path -u -n 5 -b domain -v 2 -o /tmp/outfile.html

wapiti http://<url>/path -u -n 5 -b domain -m "-all,sql,blindsql" -v 2 -o /tmp/outfile.html

OPTIONAL ARGUMENTS

-A AGENT, --user-agent AGENT: Set a custom user-agent to use for every requests	**--max-parameters MAX**: URLs and forms having more than MAX input parameters will be erased before attack.
-a CREDENTIALS, --auth-cred CREDENTIALS: Set HTTP authentication credentials	**--max-scan-time MINUTES**: Set how many minutes you want the scan to last (floats accepted)
--auth-type {basic,digest,kerberos,ntlm}: Set the authentication type to use	**--no-bugreport**: Don't send automatic bug report when an attack module fails
-c COOKIE_FILE, --cookie COOKIE_FILE: Set a JSON cookie file to use	**-o OUPUT_PATH, --output OUPUT_PATH**: Output file or folder
--color: Colorize output	**-p PROXY_URL, --proxy PROXY_URL**: Set the HTTP(S) proxy to use. Supported: http(s) and socks proxies
-d DEPTH, --depth DEPTH: Set how deep the scanner should explore the website	**-r PARAMETER, --remove PARAMETER**: Remove this parameter from urls
--endpoint ENDPOINT_URL: Url serving as endpoint for both attacker and target	**--resume-crawl**: Resume the scanning process (if stopped) even if some attacks were previously performed
--external-endpoint EXTERNAL_ENDPOINT_URL: Url serving as endpoint for target	**-S FORCE, --scan-force FORCE**: Easy way to reduce the number of scanned and attacked URLs. *Possible values*: paranoid, sneaky, polite, normal, aggressive, insane
-f FORMAT, --format FORMAT: Set output format. Supported: json, html (default), txt, openvas, vulneranet, xml	**-s URL, --start URL**: Adds an url to start scan with
--flush-attacks: Flush attack history and vulnerabilities for the current session	**--scope {page,folder,domain,url,punk}**: Set scan scope
--flush-session: Flush everything that was previously found for this target (crawled URLs, vulns, etc)	**--skip PARAMETER**: Skip attacking given parameter(s)
-H HEADER, --header HEADER: Set a custom header to use for every requests	**--skip-crawl**: Don't resume the scanning process, attack URLs scanned during a previous session
-h, --help: Show this help message and exit	**--store-session PATH**: Directory where to store attack history and session data.
--internal-endpoint INTERNAL_ENDPOINT_URL: Url serving as endpoint for attacker	**-t SECONDS, --timeout SECONDS**: Set timeout for requests
-l LEVEL, --level LEVEL: Set attack level	**--tor**: Use Tor listener (127.0.0.1:9050)
--list-modules: List Wapiti attack modules and exit	**-u URL, --url URL**: The base URL used to define the scan scope (default scope is folder)
-m MODULES_LIST, --module MODULES_LIST: List of modules to load	**-v LEVEL, --verbose LEVEL**: Set verbosity level (0: quiet, 1: normal, 2: verbose)
--max-files-per-dir MAX: Set how many pages the scanner should explore per directory	**--verify-ssl {0,1}**: Set SSL check (default is no check)
--max-links-per-page MAX: Set how many (in-scope) links the scanner should extract for each page	**--version**: Show program's version number and exit
	-x URL, --exclude URL: Adds an url to exclude from the scan

ACTIVE SCANNING: WPSCAN

José Manuel
Redondo López

- **WordPress is one of the most popular CMS to create webs**
  - Also, one of the most attacked
  - Periodic monitoring of WordPress installations is necessary
- **Wpscan finds vulnerabilities in WordPress core archives, plugins, or themes**
  - You can also discover weak passwords and security configuration issues
- **Tutorial**
  - https://blog.sucuri.net/espanol/2015/12/usando-wpscan-encontrando-vulnerabilidades-de-wordpress.html

wpscan 3.8.7 Cheatsheet (ingenieriainformatica.uniovi.es)

A vulnerability scanner for WordPress websites

https://github.com/wpscanteam/wpscan

GENERAL USAGE

```
wpscan --url URL [options]
```

NOTES

Allowed Protocols: http, https

Default Protocol if none provided: http

```
[+] URL: http://192.168.14.22/wordpress/
[+] Started: Thu Oct  3 15:20:31 2019

Interesting Finding(s):

[+] http://192.168.14.22/wordpress/
 | Interesting Entries:
 |  - Server: Microsoft-IIS/10.0
 |  - X-Powered-By: PHP/7.1.29, ASP.NET
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] http://192.168.14.22/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access
```

OPTIONS

--[no-]banner: Whether or not to display the banner (Default: true)

--[no-]update: Whether or not to update the Database

--api-token TOKEN: The WPVulnDB API Token to display vulnerability data

--connect-timeout SECONDS: The connection timeout in seconds (Default: 30)

--cookie-jar FILE-PATH: File to read and write cookies (Default: /tmp/wpscan/cookie_jar.txt)

--cookie-string COOKIE: Cookie string to use in requests, format: cookie1=value1[; cookie2=value2]

--detection-mode MODE: Default: mixed (Available choices: mixed, passive, aggressive)

--disable-tls-checks: Disables SSL/TLS certificate verification, and downgrade to TLS1.0+ (requires cURL 7.66 for the latter)

--exclude-content-based REGEXP_OR_STRING: Exclude all responses matching the Regexp (case insensitive) during parts of the enumeration. (Both the headers and body are checked. Regexp delimiters are not required.)

-f, --format FORMAT: Output results in the format supplied (Available choices: cli-no-colour, cli-no-color, json, cli)

--force: Do not check if the target is running WordPress

-h, --help: Display the simple help and exit

--hh: Display the full help and exit

--http-auth login:password: Credentials to send if HTTP auth is used in the server

--multicall-max-passwords MAX_PWD: Maximum number of passwords to send by request with XMLRPC multicall (Default: 500)

-o, --output FILE: Output to FILE

-P, --passwords FILE-PATH: List of passwords to use during the password attack. (If no --username/s option supplied, user enumeration will be run.)

--password-attack ATTACK: Force the supplied attack to be used rather than automatically determining one. (Available choices: wp-login, xmlrpc, xmlrpc-multicall)

--plugins-detection MODE: Use the supplied mode to enumerate Plugins. (Default: passive) (Available choices: mixed, passive, aggressive)

--plugins-version-detection MODE: Use the supplied mode to check plugins' versions. (Default: mixed) (Available choices: mixed, passive, aggressive)

--proxy protocol://IP:port: Supported protocols depend on the cURL installed

--proxy-auth login:password: Credentials to send to a potential proxy in the network, so scan can take place in these scenarios

--random-user-agent, --rua: Use a random user-agent for each scan

--request-timeout SECONDS: The request timeout in seconds (Default: 60)

--stealthy: Alias for --random-user-agent --detection-mode passive --plugins-version-detection passive

-t, --max-threads VALUE: The max threads to use (Default: 5)

-e, --enumerate [OPTS]: *Enumeration Process.*
Separator to use between the values: ','
Default: All Plugins, Config Backups (Value if no argument supplied: vp,vt,tt,cb,dbe,u,m)
Incompatible choices (only one of each group/s can be used):
- *vp, ap, p*
- *vt, at, t*

Available Choices:
vp Vulnerable plugins
ap All plugins
p Popular plugins
vt Vulnerable themes
at All themes
t Popular themes
tt Timthumbs
cb Config backups
dbe Db exports
u User IDs range. e.g: u1-5. Range separator to use: '-' (Value if no argument supplied: 1-10)
m Media IDs range. e.g m1-15. Range separator to use: '-' (Value if no argument supplied: 1-100)
(Permalink setting must be set to "Plain" for those to be detected)

--throttle MilliSeconds: Milliseconds to wait before doing another web request. If used, the max threads will be set to 1.

-U, --usernames LIST: List of usernames to use during the password attack. (Examples: 'a1', 'a1,a2,a3', '/tmp/a.txt')

--user-agent, --ua VALUE: Change the identification data that the tool sends to the server

-v, --verbose: Verbose mode

--version: Display the version and exit

--wp-content-dir DIR: The wp-content directory if custom or not detected, such as "wp-content"

--wp-plugins-dir DIR: The plugins directory if custom or not detected, such as "wp-content/plugins"

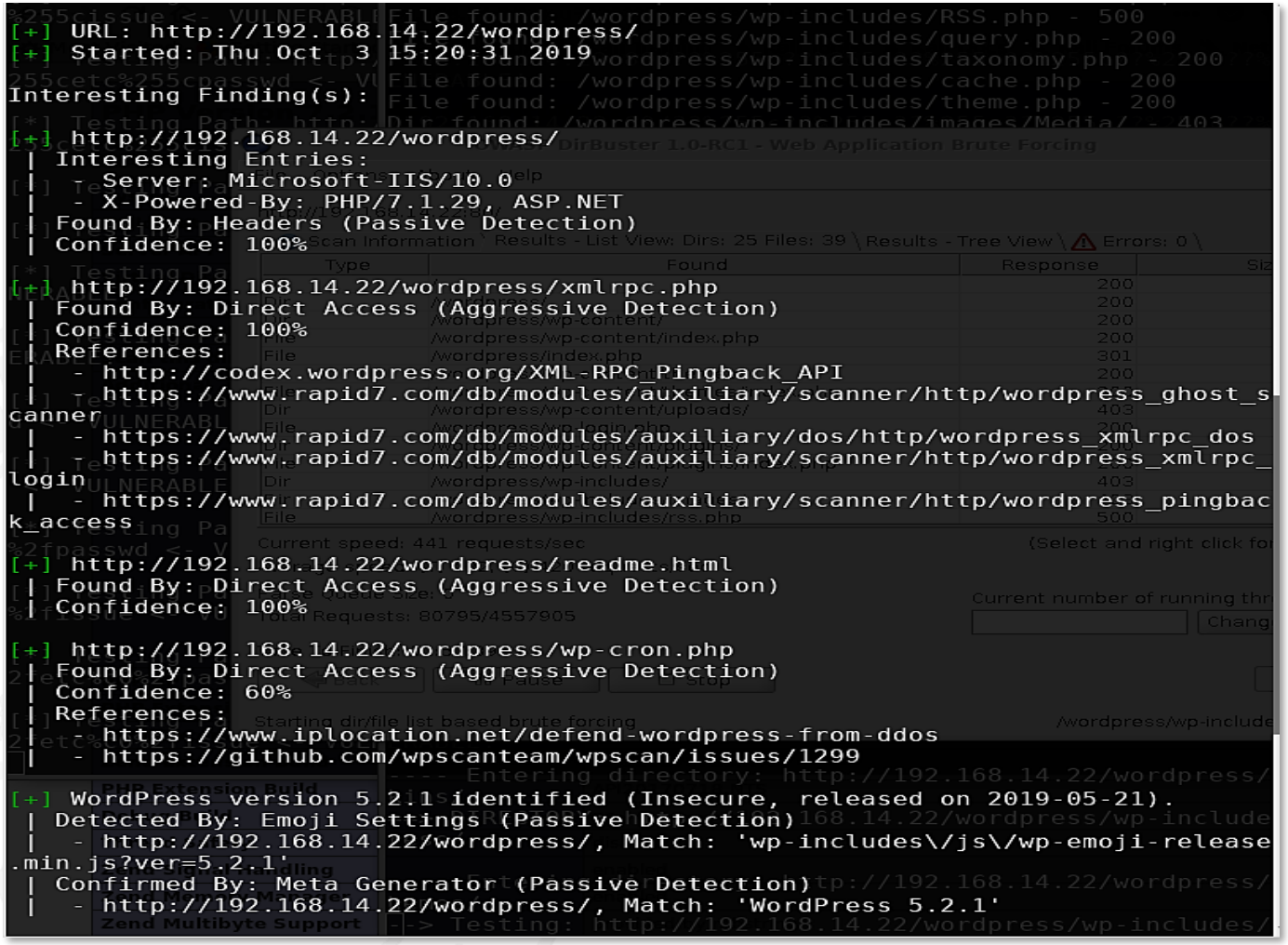
EXAMPLES

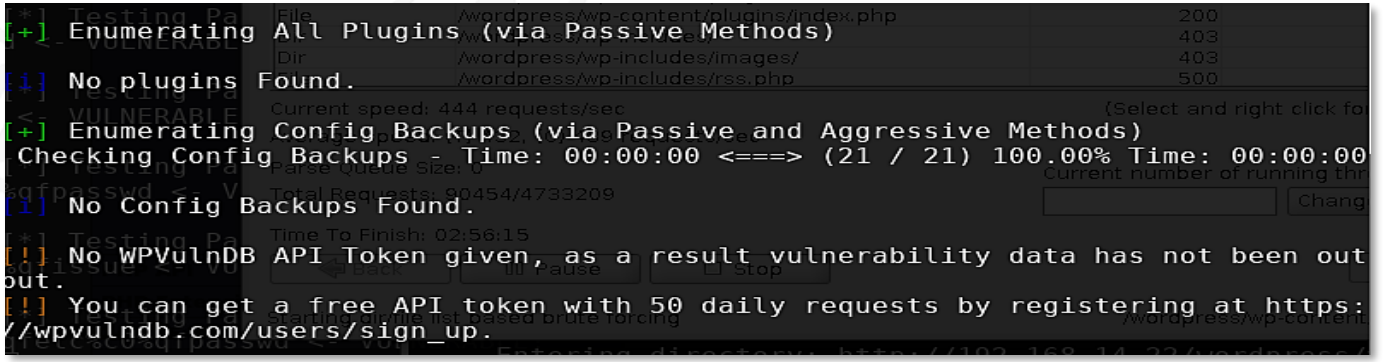
wpscan --url http://<url> --wp-content-dir /wp-content/ --enumerate vp --plugins-detection aggressive

Active scanning: WPScan. Example

José Manuel
Redondo López

- **This tool can find**
  - Possible vulnerabilities and links to how to exploit them
  - If it is a vulnerable old version
  - If we register on https://wpvulndb.com/, the tool provides comprehensive, detailed and automated vulnerability detection
  - Even if we don't, we can get quite a lot of information
- **Droopescan and Joomscan work the same way**





Gathering technical and personal information

Techniques to study persons and websites

Person-related TA0043. Reconnaissance techniques

José Manuel
Redondo López

- **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 other hardware, software, and firmware elements
  - **Nmap can also 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.)
  - Specifics regarding its topology and operations
    - Network Trust Dependencies, Network Topology, Network Security Appliances (like firewalls)…
    - Most of the times with specialized tools

More TA0043. Reconnaissance techniques

José Manuel
Redondo López

- **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

T1592. Gather victim host information
T1590. Gather victim network information: Enumerable protocols

José Manuel
Redondo López

- **There are a series of enumerable protocols that can be used to gather information about networks and hosts**
  - **DNS**: dig
  - **SMB (see ASR)**: Enum4Linux, but we could also use these alternatives
    - Smbclient and related tools (included in Kali)
      - https://blog.desdelinux.net/samba-smbclient/
      - https://eltallerdelbit.com/clientes-smb-samba
    - SMBMap: enumerates SMB/Samba shared files and folders in a domain
      - Lists shared drivers, drive permissions, contents, if upload or download is available…
      - It even runs commands remotely if possible
      - https://github.com/ShawnDEvans/smbmap
  - **SMNP**: SMNPWalk
  - *… (there are many, many more, like NFS (shown on ASR))*

T1592. Gather victim host information
T1590. Gather victim network information: Dig

José Manuel
Redondo López

- **Domain Information Groper (`dig`) is a tool to lookup in DNS registries**
  - It locates domain and subdomain names
- **Implements many DNS interactions**
  - But mainly locate all names tied to a base name
  - This way, we can locate unknown admin, backup, secondary… domains
  - These could be additional enumeration targets
  - Their security might be weaker that the main one
- **Tutorial**
  - https://www.hostinger.es/tutoriales/comando-dig-linux/

```
Last login: Tue Oct 27 14:52:49 on ttys001
Macintosh-6:~ [redacted] dig dyn.com

; <<>> DiG 9.8.3-P1 <<>> dyn.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64644
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 6

;; QUESTION SECTION:
;dyn.com.                       IN      A

;; ANSWER SECTION:
dyn.com.                10      IN      A       204.13.248.106

;; AUTHORITY SECTION:
dyn.com.                76528   IN      NS      ns1.p01.dynect.net.
dyn.com.                76528   IN      NS      ns2.p01.dynect.net.
dyn.com.                76528   IN      NS      ns4.p01.dynect.net.
dyn.com.                76528   IN      NS      ns3.p01.dynect.net.

;; ADDITIONAL SECTION:
ns1.p01.dynect.net.     86400   IN      A       208.78.70.1
ns1.p01.dynect.net.     300     IN      AAAA    2001:500:90:1::1
ns2.p01.dynect.net.     86400   IN      A       204.13.250.1
ns3.p01.dynect.net.     86400   IN      A       208.78.71.1
ns3.p01.dynect.net.     300     IN      AAAA    2001:500:94:1::1
ns4.p01.dynect.net.     86400   IN      A       204.13.251.1

;; Query time: 5 msec
;; SERVER: 172.16.12.127#53(172.16.12.127)
;; WHEN: Tue Oct 27 15:46:22 2015
;; MSG SIZE  rcvd: 247
```

T1592. Gather victim host information
T1590. Gather victim network information: Dig

José Manuel Redondo López

- **`dig` has a lot of options to interact with DNS servers**
  - The image shows typical queries and options of enumeration tasks
- **It is a quick way of knowing…**
  - Who manages the domain
  - Aliases
  - If they have a mail server
  - The DNS name of a certain IP
  - Everything you (commonly) need! ☺
- **Domains can also be explored with other tools and techniques**
  - https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Subdomains%20Enumeration.md

Cheatography

dig (english)
by TME520 (TME520) via cheatography.com/20978/cs/7226/

Syntax

dig [@server] [-b address] [-c class] [-f filename] [-k filename] [-m] [-p port#] [-q name] [-t type] [-x addr] [-y [hmac:]name:key] [-4] [-6] [name] [type] [class] [query-opt...]

Config

Tired of always typing the same options ? Create a Run Control file for dig.	`vi $HOME/.digrc`

$ cat $HOME/.digrc
+noall +answer

List specific types of RRs (Resource Records)

List address records	`dig -t A tme520.net`
List aliases	`dig -t CNAME tme520.net`
Find who manages a domain	`dig -t SOA tme520.net`
List mail servers	`dig tme520.net MX`
List name servers	`dig tme520.net NS`
List any type of Resource Record	`dig tme520.net ANY`

There are about 40 DNS Resources Records types, but you only have to know 5 of them:

- **A** : Address record (IPv4); AAAA for IPv6,
- **CNAME** : Canonical Name. Aliases to A or AAAA records,
- **SOA** : Start Of Authority: primary name server, email of the domain admin, domain serial number, and timers relating to refreshing the zone,
- **MX** : Mail eXchange. Points to a mail server,
- **NS** : Name Server (a DNS).

Output sections

HEADER	Displays the dig command version, the global options used, the type of operation (opcode), the status of the operation (NOERROR) and the message id (necessary to match responses to queries).
QUESTION	This is your input, the question that has been asked to the DNS.
ANSWER	The 2nd field is the time in seconds that the record may be cached (0 = don't cache), the 3rd field is the class (Internet (IN), Chaos (CH), Hesiod (HS)...), the 4th is the type (A, NS, CNAME, MX...) and the 5th, the IP.
AUTHORITY	This section contains the DNS name server that has the authority to answer your query (type: NS, Name Server).
ADDITIONAL	The additional section carries Resource Records related to the RRs from the other sections.
STATISTICS	Displays the time it took to get an answer, the IP of the DNS server used, the date and size of the message.

If you ever get confused about whether or not *dig* found any result for your query, check the ANSWER field from the header; if it's at 0, your query returned no proper answer.

Batch mode: multiple queries in one go

Using a list	`dig -f names.list`
Using several arguments	`dig centos.org MX +noall +answer suckless.org ANY +short`

Batch mode takes a filename as input; the file must be plain text and contain one domain per line:

```
$ cat names.list

redhat.com
ubuntu.com
perdu.com
```

Make that DNS talk !

Display only the ANSWER section	`dig opensuse.org +noall +answer`
Activate the short output	`dig perdu.com +short`
Reverse DNS (get name from IP)	`dig -x 208.97.177.124`
Use a specific DNS server	`dig @8.8.4.4 redhat.com`
Display the name resolution path	`dig google.com +trace`
Request a zone transfer	`dig microsoft.com AXFR`

A zone transfer is a mechanism allowing an administrator to replicate DNS databases across a set of DNS servers. There are two methods: full (aka AXFR) and incremental (aka IXFR). Zone transfers were often used by people wanting to retrieve a list of all the Resource Records of a DNS server. Nowadays, most servers will refuse your request, mostly for security reasons.

By **TME520** (TME520)
cheatography.com/tme520/
tme520.com

Published 16th February, 2016.
Last updated 12th May, 2016.
Page 1 of 1.

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
http://crosswordcheats.com

T1592. Gather victim host information
T1590. Gather victim network information: SMB. Enum4Linux

José Manuel
Redondo López

- **Having the SMB service open can be a great source of information**
- **This tool gets information from SMB-enabled machines like**
  - RID cycling (enumerating users on older systems)
  - List of users, group members, and shares
  - Detecting whether a host belongs to a domain or a workgroup
  - Identification of the OS of the server examined
  - Identifying the passwords policy used
- **Tutorials**
  - https://noticiasseguridad.com/tutoriales/enum4linux-extraiga-informacion-de-una-maquina-windows/
  - https://highon.coffee/blog/enum4linux-cheat-sheet/

```
root@kali:~# enum4linux 192.168.14.2
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux
/ ) on Wed Oct  2 14:44:31 2019

 ==========================
|    Target Information    |
 ==========================
Target ..... 192.168.14.2
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

 =====================================================
|    Enumerating Workgroup/Domain on 192.168.14.2    |
 =====================================================
[+] Got domain/workgroup name: WORKGROUP

 ============================================
|    Nbtstat Information for 192.168.14.2    |
 ============================================
Looking up status of 192.168.14.2
        SERVER1804      <00> -         B <ACTIVE>  Workstation Service
        SERVER1804      <03> -         B <ACTIVE>  Messenger Service
        SERVER1804      <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 ======================================
|    Session Check on 192.168.14.2    |
 ======================================
[+] Server 192.168.14.2 allows sessions using username '', password ''

 ============================================
|    Getting domain SID for 192.168.14.2    |
 ============================================
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
```

T1592. Gather Victim Host Information
T1590. Gather Victim Network Information: SMB. Enum4Linux

José Manuel
Redondo López

- **Thanks to this tool we can find very interesting information**
- **In this example**
  - That the passwords policy is very lax: the likelihood of weak passwords is very high
  - **That there is a user called "operario",** which is very useful for brute-force attacks
  - Names of system user groups: we are dealing with a Windows machine

```
[+] Password Info for Domain: SERVER1804

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: 37 days 6 hours 21 minutes
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: None
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: 37 days 6 hours 21 minutes

[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 5
```

```
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
S-1-5-32-1000 *unknown*\*unknown* (8)
```

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\operario (Local User)
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
S-1-5-32-500 *unknown*\*unknown* (8)
```

T1592. Gather Victim Host Information
T1590. Gather Victim Network Information: SNMPWalk

José Manuel Redondo López

- **Simple Network Management Protocol**
  - Used by network devices to exchange information
  - Eases to monitor, operate, and troubleshoot the network
  - The most used SNMP versions are version 1 (SNMPv1) and 2 (SNMPv2)
  - SNMP version 3 (SNMPv3) includes changes and is more secure
    - But has deployment issues and incompatibilities
- **SNMPWalk examines endpoints to discover SNMP vulnerabilities**
- **Tutorial:** https://hacking-etico.com/2014/03/27/leyendo-informacion-snmp-con-snmpwalk/

snmpwalk 5.9 Cheatsheet (ingenieriainformatica.uniovi.es)
Tool to discover flaws when using the SNMP protocol
http://www.net-snmp.org/

GENERAL USAGE

```
snmpwalk [OPTIONS] AGENT [OID]
```

NOTES

Be sure to understand the various entities handled by this protocol to properly understand how to use this tool

```
$ snmpwalk -v 2c -c public localhost
iso.3.6.1.2.1.1.1.0 = STRING: "Linux poftut1 4.10.0-37-generic #41~Ubuntu S
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (20220) 0:03:22.20
iso.3.6.1.2.1.1.4.0 = STRING: "me@poftut.com"
iso.3.6.1.2.1.1.5.0 = STRING: "poftut1"
iso.3.6.1.2.1.1.6.0 = STRING: "InPoftut"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.6.3.13.3.1.3
iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.2.1.92
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The MIB for Message Processing and Dispe
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The management information definitions f
"
```

OPTIONS

- **-c COMMUNITY**: set the community string
- **-h, --help**: display this help message
- **-H**: display configuration file directives understood
- **-v 1|2c|3**: specifies SNMP version to use
- **-V, --version**: display package version number (SNMP Version 1 or 2c specifi

SNMP Version 3 specific

- **-A PASSPHRASE**: set authentication protocol pass phrase
- **-a PROTOCOL**: set authentication protocol (MD5|SHA|SHA-224|SHA-256|SHA-384|S
- **-E ENGINE-ID**: set context engine ID (e.g. 800000020109840301)
- **-e ENGINE-ID**: set security engine ID (e.g. 800000020109840301)
- **-l LEVEL**: set security level (noAuthNoPriv|authNoPriv|authPriv)
- **-n CONTEXT**: set context name (e.g. bridge1)
- **-u USER-NAME**: set security name (e.g. bert)
- **-X PASSPHRASE**: set privacy protocol pass phrase
- **-x PROTOCOL**: set privacy protocol (DES|AES)
- **-Z BOOTS,TIME**: set destination engine boots/time

General communication options

- **-r RETRIES**: set the number of retries
- **-t TIMEOUT**: set the request timeout (in seconds)

Debugging

- **-d**: dump input/output packets in hexadecimal
- **-D[TOKEN[,...]]**: turn on debugging output for the specified TOKENs (ALL gives extremely verbose debugging output)

General options (I)

- **-C APPOPTS**: Set various application specific behaviours:
  - p: print the number of variables found
  - i: include given OID in the search range
  - I: don't include the given OID, even if no results are returned
  - c: do not check returned OIDs are increasing
  - t: Display wall-clock time to complete the walk
  - T: Display wall-clock time to complete each request
  - E {OID}: End the walk at the specified OID
- **-I INOPTS**: Toggle various defaults controlling input parsing:
  - b: do best/regex matching to find a MIB node
  - h: don't apply DISPLAY-HINTs
  - r: do not check values for range/type legality
  - R: do random access to OID labels
  - u: top-level OIDs must have '.' prefix (UCD-style)
  - s SUFFIX: Append all textual OIDs with SUFFIX before parsing
  - S PREFIX: Prepend all textual OIDs with PREFIX before parsing
- **-m MIB[:...]**: load given list of MIBs (ALL loads everything)
- **-M DIR[:...]**: look in given list of directories for MIBs (default: <user home>/.snmp/mibs:/usr/share/snmp/mibs:/usr/share/snmp/mibs/iana:/usr/share/snmp/mibs/ietf)

General options (II)

- **-L LOGOPTS**: Toggle various defaults controlling logging:
  - e: log to standard error
  - o: log to standard output
  - n: don't log at all
  - f file: log to the specified file
  - s facility: log to syslog (via the specified facility)
  - (variants)
  - [EON] pri: log to standard error, output or /dev/null for level 'pri' and above
  - [EON] p1-p2: log to standard error, output or /dev/null for levels 'p1' to 'p2'
  - [FS] pri token: log to file/syslog for level 'pri' and above
  - [FS] p1-p2 token: log to file/syslog for levels 'p1' to 'p2'
- **-O OUTOPTS**: Toggle various defaults controlling output display:
  - 0: print leading 0 for single-digit hex characters
  - a: print all strings in ascii format
  - b: do not break OID indexes down
  - e: print enums numerically
  - E: escape quotes in string indices
  - f: print full OIDs on output
  - n: print OIDs numerically
  - p PRECISION: display floating point values with specified PRECISION (printf format string)
  - q: quick print for easier parsing
  - Q: quick print with equal-signs
  - s: print only last symbolic element of OID
  - S: print MIB module-id plus last element
  - t: print timeticks unparsed as numeric integers
  - T: print human-readable text along with hex strings
  - u: print OIDs using UCD-style prefix suppression
  - U: don't print units
  - v: print values only (not OID = value)
  - x: print all strings in hex format
  - X: extended index format
- **-P MIBOPTS**: Toggle various defaults controlling MIB parsing:
  - u: allow the use of underlines in MIB symbols
  - c: disallow the use of "--" to terminate comments
  - d: save the DESCRIPTIONs of the MIB objects
  - e: disable errors when MIB symbols conflict
  - w: enable warnings when MIB symbols conflict
  - W: enable detailed warnings when MIB symbols conflict
  - R: replace MIB symbols from latest module

EXAMPLES

snmpwalk -v 2c -c public 192.168.56.10

T1592. Gather victim host information
T1590. Gather victim network information: What if we find other services?

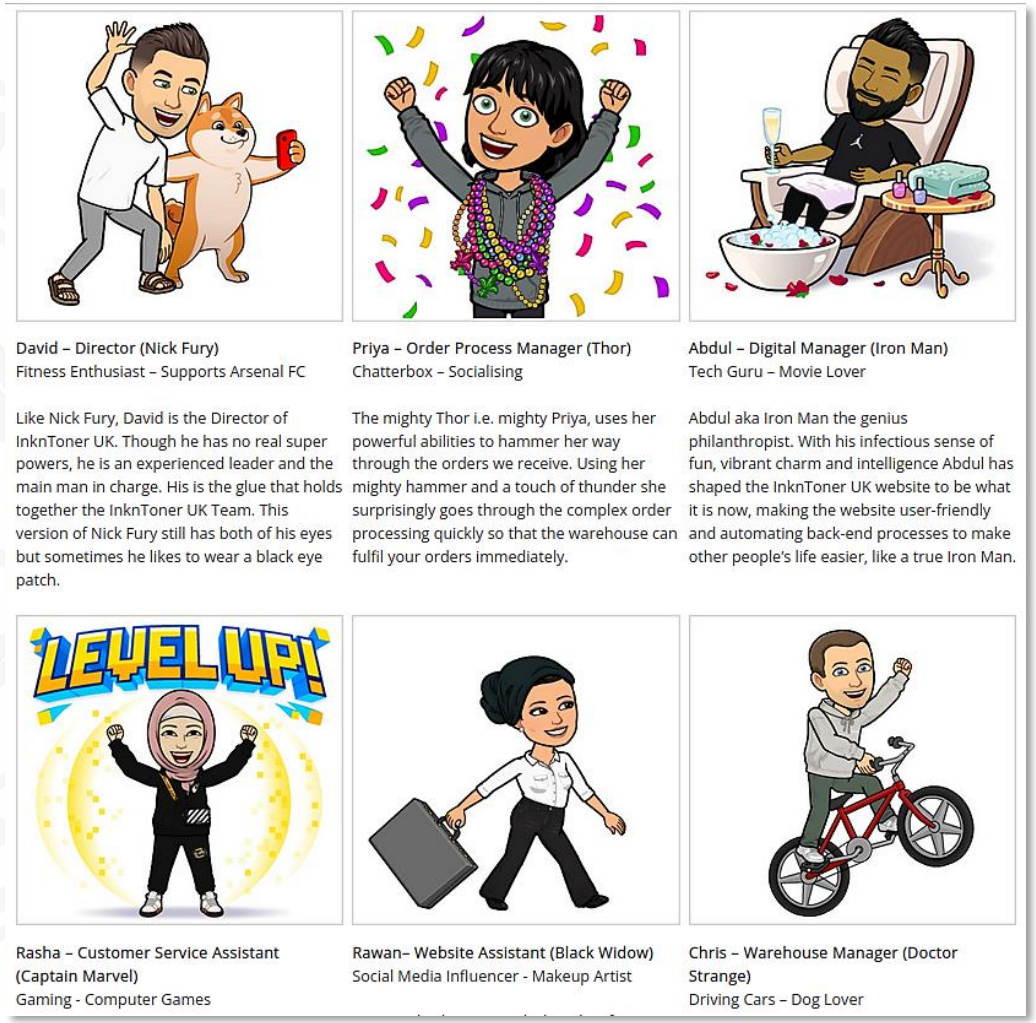
José Manuel Redondo López

- **If you locate services not covered here, there are two things you can make to enumerate them further**
  - Search and use **nmap NSE scripts** linked to the service name (see the 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 future topics)
- **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

T1589. Gather victim identity information
T1591. Gather victim org information: Simple OSINT in web pages

José Manuel Redondo López

- **The goal is to guess valid usernames**
  - Facilitating techniques like brute-force attacks later
  - Sometimes this information does not require technical skill, just using the published information
- **Companies with a public gallery of employees**
  - What if usernames are variations of these names?
    - `nick_fury`, `thor`, `iron_man`, `black_widow`, etc. could be valid usernames in this company…
    - At least, is a suitable starting point!
  - If unsuccessful, tools described in seminars may help locating usernames or other useful information
- **All this info can be used in social networks**
  - To gather data about employees and their roles
  - Leading to spear phising data-gathering techniques



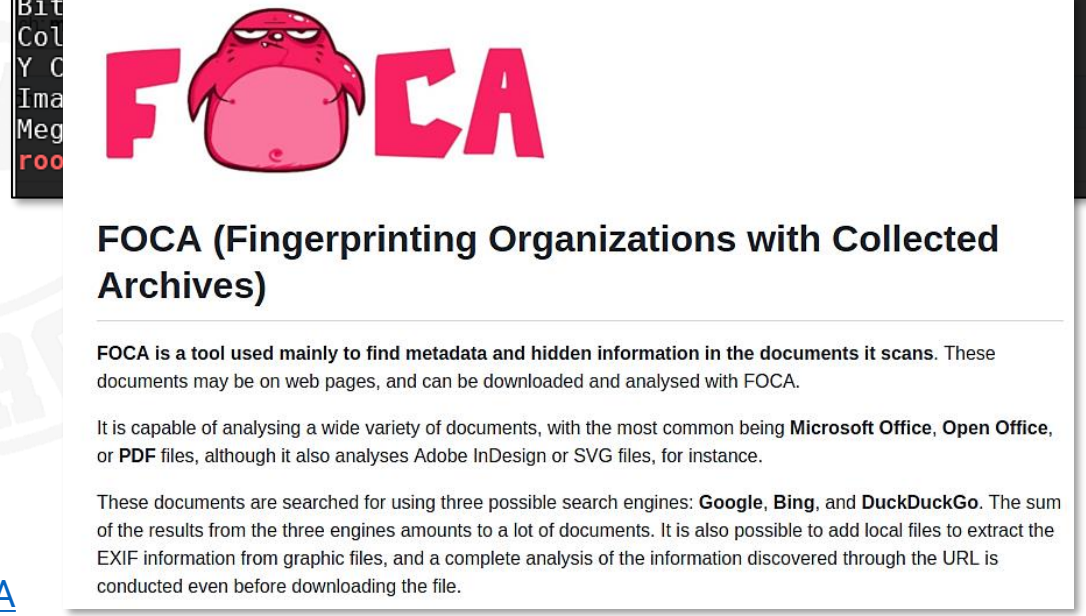
Source: https://www.inkntoneruk.co.uk/Meet-The-Team.html

T1589. Gather victim identity information
T1591. Gather victim org information: Metadata (exiftool)

José Manuel Redondo López

- **"Normal" images carry metadata**
  - Creation place / date, camera type / brand...
- **`exiftool` is one of the best tools to do it**
  - `apt-get install exiftool`
  - It was reviewed in lab 4
- **For other file types we can analyze their metadata with**
  - FOCA: https://www.elevenpaths.com/es/labstools/foca-2/index.html
  - Metashield: https://www.elevenpaths.com/es/tecnologia/metashield/index.html
- **Files can also be minified, encoded or obfuscated (see topic 2)**

```
root@kali:~/Descargas# exiftool lady-in-yoga.jpg
ExifTool Version Number         : 11.65
File Name                       : lady-in-yoga.jpg
Directory                       : .
File Size                       : 21 kB
File Modification Date/Time     : 2019:10:07 13:02:12+02:00
File Access Date/Time           : 2019:10:07 13:02:20+02:00
File Inode Change Date/Time     : 2019:10:07 13:02:12+02:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
Image Width                     : 283
Image Height                    : 676
Encoding Process                : Baseline DCT, Huffman coding
```



Source: https://github.com/ElevenPaths/FOCA

Other reconnaissance techniques

More techniques to obtain information about the victim

Other TA0043. Reconnaissance techniques

José Manuel
Redondo López

- **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
- **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

José Manuel
Redondo López

- **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

José Manuel
Redondo López

- **Phishing for Information was already reviewed in**
  - **Seminar 1** (phishing against users)
    - Tinfoleak, Twint, Hunter.io, Social Mapper, Project Sherlock, and other tools
  - Twint was also covered in **Laboratory 2**
  - 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

Self-evaluation Achievement List: Network security

José Manuel
Redondo López

Rank	Concept
	Understand the concept of DMZ
	Know about modern network attacks
	Know about the services provided by CDNs
	Know how to enumerate CMSs
	Be able to search resources to enumerate any possible network service
	Understand the concept of host firewall and its different types
	Being able to differentiate insecure from secure network designs
	Understand why network segmentation and defense in depth is important
	Know how to enumerate ports and services with active scans
	Know how to enumerate HTTP services and extract information from their files
	Understand the purpose and articulate the different reconnaissance techniques of MITRE ATT&CK
	Understand the multiple components of the Secure Network Infrastructure
	**We didn't start the firewall**: Learn how to protect and attack devices in a network

PERIMETER AND NETWORK SECURITY

Source: zona-militar.com