

# **M11 – Seguretat Informàtica – UF1**

**Pràctica 4 Recollida activa d'informació\_v05**

**Nil Massó**



ASIX 2			
M11 – Seguretat Informàtica – UF1		Tipus	Individual
Cognoms, Nom:	Massó Cabaña, Nil	Curs	2022-23
Observacions:			

## Table of Contents

Enllaços:.....	1
Pràctica 4 – Recollida activa d'informació i logs.....	1
Exercici 1: Interrogació de DNS amb dnsenum (3 punts).....	1
Exercici 2: Nmap (5 punts).....	5
Exercici 3: Rsyslog (2 punts).....	14

- A l'hora d'avaluar i qualificar el treball es tindran en compte els aspectes estètics, de correctesa lingüística (sintàctica i ortogràfica) a més del que s'hagi comentat al cicle formatiu sobre la redacció de documentació tècnica i manuals.

- El mòdul professional pertany a uns estudis orientats al món laboral, cosa que fa que un cop complerts els requisits mínims la nota resultant serà condicionada per la quantitat i qualitat del treball individual realitzat per cada alumne.

- **Recordeu crear una portada i un índex.**

## Enllaços:

<https://digi.ninja/projects/zonetransferme.php>

<https://ns1.com/blog/understanding-afsdb-records>

<http://scanme.nmap.org/>

<https://en.wikipedia.org/wiki/Syslog>

<https://www.thegeekdiary.com/understanding-rsyslog-filter-options/>

<https://juanjoselo.wordpress.com/2018/01/06/gestion-de-logs-centralizados-con-rsyslog/>

<https://www.the-art-of-web.com/system/rsyslog-config/>

<https://geek-university.com/rsyslog/>

<https://linux.die.net/man/8/logrotate>

## Pràctica 4 – Recollida activa d'informació i logs.

Fes els exercicis següents. Contesteu directament sota dels enunciats. Poseu-hi captures de pantalla si ho considereu necessari.

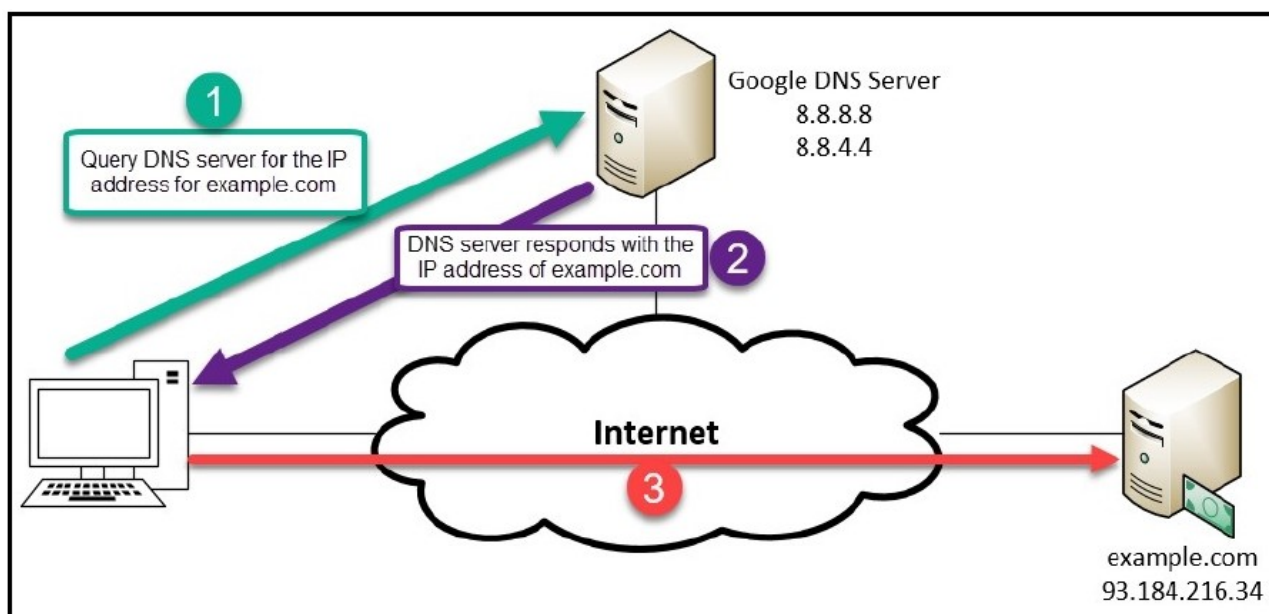
### **Recordeu a citar TOTES les fonts utilitzades**

#### **Recollida activa d'informació.**

Utilitzem mètodes d'aproximació que suposen fer un contacte directe amb l'objectiu. Ens permet aconseguir dades i detalls que no podem assolir fent una aproximació amb OSINT (open-source intelligence). Podem aconseguir de primera mà informació sensible i rellevant del sistema operatiu i dels serveis disponibles. També podem esbrinar la quantitat de dispositius en línia i el rol del dispositiu a la xarxa i els recursos que proporciona als seus clients. Però l'aproximació activa també suposa un risc de detecció.

### **Exercici 1: Interrogació de DNS amb dnsenum (3 punts)**

Sabem que un servidor de DNS pot donar servei a xarxes públiques i a xarxes privades.



Font: Learn Kali Linux 2019. Glen D. Singh.

I que hi han DNS públics a internet. Fins i tot alguns de maliciosos que ens poden redirigir a websites i dominis falsos.

DNS de confiança:

- Cloudflare DNS: <https://1.1.1.1/>
- Google Public DNS: <https://developers.google.com/speed/public-dns/>
- Cisco OpenDNS: <https://www.opendns.com/>

I els DNS no només ens tradueixen un hostname a una adreça IP, també poden resoldre altres tipus d'informació:

Record Type	Description
A	Maps hostname to IPv4 address
AAAA	Maps hostname to IPv6 address
MX	Maps domain to mail server
NS	Points to domain's nameserver
CNAME	Canonical naming used for aliases of a domain
SOA	Authority for a domain
SRV	Service records
PTR	Maps an IP address to a hostname
RP	Responsible person
HINFO	Host information
TXT	Text record

DNS record types

Font: Learn Kali Linux 2019. Glen D. Singh.

Per a testejar quins registres de DNS tenim en una organització, realitzarem una enumeració DNS. Fins i tot podem arribar a copiar aquesta informació i transferir-la a un altre DNS secundari i augmentar la disponibilitat i la tolerància a errors. Però això pot portar a descobrir la topologia d'una xarxa si no es separen els espais de noms interns i externs.

Segons el país, accedir a aquesta informació pot ser il·legal. **Només realitza la cerca en el domini que s'indica a la pràctica.**

Obre un terminal a la teva màquina de Kali Linux i executa *dnsenum*. **Captura la pantalla i comenta el que hi veus i què es pot fer amb els paràmetres.** (1 punt)

```

dnsenum VERSION:1.2.6
Usage: dnsenum [Options] <domain>
[Options]:
Note: If no -f tag supplied will default to /usr/share/dnsenum/dns.txt or
the dns.txt file in the same directory as dnsenum.pl
GENERAL OPTIONS:
--dnsserver <server>      Use this DNS server for A, NS and MX queries.
--enum                   Shortcut option equivalent to --threads 5 -s 15 -w.
-h, --help               Print this help message.
--noreverse              Skip the reverse lookup operations.
--nocolor                Disable ANSIColor output.
--private                Show and save private ips at the end of the file domain_ips.txt.
--subfile <file>         Write all valid subdomains to this file.
-t, --timeout <value>    The tcp and udp timeout values in seconds (default: 10s).
--threads <value>        The number of threads that will perform different queries.
-v, --verbose            Be verbose: show all the progress and all the error messages.
GOOGLE SCRAPING OPTIONS:
-p, --pages <value>      The number of google search pages to process when scraping names,
                        the default is 5 pages, the -s switch must be specified.
-s, --scrap <value>      The maximum number of subdomains that will be scraped from Google (default 15).
BRUTE FORCE OPTIONS:
-f, --file <file>        Read subdomains from this file to perform brute force. (Takes priority over default dns.txt)
-u, --update <a|g|r|z>   Update the file specified with the -f switch with valid subdomains.
                        a (all)      Update using all results.
                        g            Update using only google scraping results.
                        r            Update using only reverse lookup results.
                        z            Update using only zonetransfer results.
-r, --recursion          Recursion on subdomains, brute force all discovered subdomains that have an NS record.
WHOIS NETRANGE OPTIONS:
-d, --delay <value>      The maximum value of seconds to wait between whois queries, the value is defined randomly, default: 3s.
-w, --whois              Perform the whois queries on c class network ranges.
                        **Warning**: this can generate very large netranches and it will take lot of time to perform reverse lookups.
REVERSE LOOKUP OPTIONS:
-e, --exclude <regex>    Exclude PTR records that match the regex expression from reverse lookup results, useful on invalid hostnames.
OUTPUT OPTIONS:
-o --output <file>       Output in XML format. Can be imported in MagicTree (www.gremwell.com)

```

Assegura't que la màquina virtual té accés a internet (per ex. Amb el mode NAT) i prova el domini zonetransfer.me amb ***dnsenum zonetransfer.me***

**Posa una captura de pantalla on es vegin els 2 servidors de noms descoberts. Comenta quins tipus de registres de DNS hi veus (1 punt)**

### Name Servers:

nsztm1.digi.ninja.	6337	IN	A	81.4.108.41
nsztm2.digi.ninja.	6337	IN	A	34.225.33.2

**Posa una captura on es vegin dos servidors de noms que es puguin descobrir a partir dels altres dos i les seves adreces IP. (1 punt)**

### Name Servers:

dns1.zoneedit.com.	239	IN	A	139.177.204.42
dns2.zoneedit.com.	254	IN	A	50.116.13.244

### Name Servers:

dns2.zoneedit.com.	14	IN	A	50.116.13.244
dns1.zoneedit.com.	300	IN	A	139.177.204.42

## Exercici 2: Nmap (5 punts)

NMAP és un programa opensource que serveix per realitzar rastreig de ports, de serveis, de versions, etc. Actualment es multiplataforma i el seu desenvolupament el porta la comunitat. És una de les eines imprescindibles per qualsevol sysadmin i s'utilitza per avaluar la seguretat informàtica en una xarxa informàtica. NMAP envia diferents paquets definits als equips i l'analitza les respostes. Té uns estats definits pels ports que analitza i també pot funcionar amb scripts d'anàlisi ja predefinits. Serveixi doncs aquesta pràctica perquè comenceu a veure'n el funcionament.

L'objectiu és escanejar i identificar els hosts vius que hi ha a la xarxa, trobar els ports oberts, identificar els serveis i fer un diagrama de la xarxa. **Fer un escaneig sense permís és il·legal a molts països. La pròpia pàgina de NMAP ens proporciona un servidor on fer-hi els testos:** <http://scanme.nmap.org>

I per altra banda feu servir una màquina virtual **metasploitable 2** perquè hi feu els testos. La pots trobar al Moodle.

Per tant cal fer la pràctica analitzant els diferents apartats **SOBRE ELS 2 SERVIDORS. Pots tenir el Kali Linux en mode NAT i en mode bridge host only. I la metasploitable en mode bridge host only.**

Al Moodle també hi trobareu un cheatsheet, que és una fulla resum amb diferents comandes de NMAP que us puguin fer falta. En tot cas, la pròpia pàgina de NMAP i moltes altres a Internet en contenen moltíssima informació.

Aprofitant els diferents flags que podem posar als paquets TCP, podem determinar ports, sistemes operatius, serveis i si hi ha un Firewall.

Primer de tot us passo una mica d'explicació de com funciona NMAP i després caldrà doncs que executeu les següents comandes sobre els 2 servidors i en mostreu la captura amb la comanda i el resultat.

Només indicant la comanda NMAP i la IP del servidor ja podem fer un petit inici d'anàlisi del mateix. També ho podeu fer amb el hostname enlloc de la IP directament posant nmap i el nom del servidor. Si



voleu obtenir més detall, cal que afegiu el paràmetre `-v` entre `nmap` i el nom/IP del servidor. En cas de tenir múltiples servidors, els podem afegir a un fitxer (un servidor per línia) i dir-li a `nmap` que ho analitzi des d'allà. En aquest cas cal preparar el fitxer (per exemple `servidors.txt`) i després llançar la següent comanda -> `nmap -iL servidors.txt`.

En cas d'anàlisi de xarxes, també podem analitzar una subxarxa sencera, per exemple fent `nmap 192.168.1.0/24`. Dins una subxarxa també podem decidir excloure'n algun de l'anàlisi. Per exemple segons el cas anterior, si no volem el servidor 192.168.1.100 llançaríem la comanda -> `nmap 192.168.1.0/24 --exclude 192.168.1.100`.

Si volem informació sobre el sistema operatiu, farem servir el paràmetre `-O` -> `sudo nmap -O IP/hostname`. NMAP té molts tipus d'escaneig. Un dels és només analitzar la resposta a ping, pel que en aquest cas hem de fer: `nmap -sP IP`.

Amb NMAP per defecte només mirem els ports TCP. Sabeu que el port web és el 80, pel que si volem fer un anàlisi sobre l'estat d'aquest port per un servidor X, ens cal llançar -> `nmap -p 80 IP`. Si en canvi volem fer l'anàlisi per UDP (ports de DNS per exemple) cal fer -> `Nmap -sU 53 IP`.

Si volem saber totes les versions dels serveis escoltant als ports cal que llancem -> `nmap -sV IP`.

També si volem llistar tots els ports i el seu estat segons `nmap` però no volem fer-ho amb control de ping (per si tenen ICMP deshabilitat) hem de llançar -> `nmap -PN IP`.

Per anar ràpid podem fer un anàlisi dels 100 ports més utilitzats, per això ho farem amb -> `nmap -F IP`. Si volem escanejar tots els ports d'una màquina cal fer -> `nmap -p "*" IP`. Si per contra només volem fer-ho amb els TCP cal fer -> `nmap -sT IP` i en canvi si només volem els UDP cal fer-ho amb `nmap -sU IP`.

Fins i tot hi ha una interfície gràfica anomenada Zenmap. Disponible en Windows, Linux i macOS. NMAP té moltes maneres diferents de fer el mateix, trobareu molta informació a Internet. Després d'aquesta petita explicació cal doncs que feu, **pels 2 servidors** que hem dit al principi, **excepte si s'indica el contrari, el següent (Recordeu a posar-me les captures de tot lo necessari i les justificacions que creieu.)**:

- a sobre el metasploitable, feu un *nmap* simple sobre la IP del servidor escollit.  
(0,5 punts)



```

└─$ nmap 192.168.122.174
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-23 16:25 UTC
Nmap scan report for 192.168.122.174
Host is up (0.00043s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

```

- b sobre l'altre servidor, feu un *nmap* simple sobre el hostname del servidor (0,5 punts)

```

└─$ nmap scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-23 16:29 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.18s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    filtered domain
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

```

- c sobre els 2 servidors, feu el *nmap -v*. (0,5 punts)

```
$ nmap -v scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-23 16:32 UTC
Initiating Ping Scan at 16:32
Scanning scanme.nmap.org (45.33.32.156) [2 ports]
Completed Ping Scan at 16:32, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:32
Completed Parallel DNS resolution of 1 host. at 16:32, 0.00s elapsed
Initiating Connect Scan at 16:32
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Completed Connect Scan at 16:32, 11.27s elapsed (1000 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.17s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    filtered domain
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 11.54 seconds
```

```

kali@kali:~$ nmap -v 192.168.122.174
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-23 16:33 UTC
Initiating Ping Scan at 16:33
Scanning 192.168.122.174 [2 ports]
Completed Ping Scan at 16:33, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:33
Completed Parallel DNS resolution of 1 host. at 16:33, 0.00s elapsed
Initiating Connect Scan at 16:33
Scanning 192.168.122.174 [1000 ports]
Discovered open port 22/tcp on 192.168.122.174
Discovered open port 80/tcp on 192.168.122.174
Discovered open port 5900/tcp on 192.168.122.174
Discovered open port 53/tcp on 192.168.122.174
Discovered open port 443/tcp on 192.168.122.174
Discovered open port 25/tcp on 192.168.122.174
Discovered open port 3306/tcp on 192.168.122.174
Discovered open port 23/tcp on 192.168.122.174
Discovered open port 21/tcp on 192.168.122.174
Discovered open port 139/tcp on 192.168.122.174
Discovered open port 111/tcp on 192.168.122.174
Discovered open port 6667/tcp on 192.168.122.174
Discovered open port 2121/tcp on 192.168.122.174
Discovered open port 6000/tcp on 192.168.122.174
Discovered open port 514/tcp on 192.168.122.174
Discovered open port 5432/tcp on 192.168.122.174
Discovered open port 512/tcp on 192.168.122.174
Discovered open port 1524/tcp on 192.168.122.174
Discovered open port 8180/tcp on 192.168.122.174
Discovered open port 1099/tcp on 192.168.122.174
Discovered open port 2049/tcp on 192.168.122.174
Discovered open port 513/tcp on 192.168.122.174
Discovered open port 8009/tcp on 192.168.122.174
Completed Connect Scan at 16:33, 0.00s elapsed (1000 total ports)
Nmap scan report for 192.168.122.174
Host is up (0.0011s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  mircoregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds

```

File Actions Edit View Help

Nmap done: 1 IP address (1 host up)

kali@kali:~\$

kali@kali:~\$ nmap -v sapalomera.cat

Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-23 16:33 UTC

Nmap scan report for sapalomera.cat

Host is up (0.018s latency).

Not shown: 98 filtered ports

PORT STATE SERVICE

80/tcp open http

443/tcp open https

Nmap done: 1 IP address (1 host up)

kali@kali:~\$

kali@kali:~\$ nmap -v 80 sapalomera.cat

Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-23 16:33 UTC

Nmap scan report for sapalomera.cat

Host is up (0.14s latency).

PORT STATE SERVICE

80/tcp open http

Nmap done: 1 IP address (1 host up)

kali@kali:~\$

kali@kali:~\$ nmap -v sapalomera.cat



- d Per tots dos servidors, intenteu trobar la versió del sistema operatiu amb el paràmetre -O. (0,5 punts)

```
MAC Address: 52:54:00:B8:BC:CD (QEMU virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

```
Device type: general purpose|firewall
Running (JUST GUESSING): Linux 2.6.X|3.X (85%), WatchGuard Fireware 11.X (85%)
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10 cpe:/o:watchguard:fireware:11.8
Aggressive OS guesses: Linux 2.6.32 (85%), Linux 2.6.32 or 3.10 (85%), WatchGuard Fireware 11.8 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 23 hops
```

- e Pels dos, feu un *nmap -sP*. (0,5 punts)

```
(root@kali)-[~]
# nmap -sP scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-23 16:44 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.18s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

(root@kali)-[~]
# nmap -sP 192.168.122.174
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-23 16:45 UTC
Nmap scan report for 192.168.122.174
Host is up (0.00076s latency).
MAC Address: 52:54:00:B8:BC:CD (QEMU virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

- f I també pels dos, un *nmap -sV*. (0,5 punts)

```

[*] nmap -v 192.168.122.174 scanme.nmap.org
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-23 16:46 UTC
Nmap scan report for 192.168.122.174
Host is up (0.00017s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp       vsftpd 2.3.4
22/tcp    open  ssh       OpenSSH 4.7p1 Debian Squeeze (protocol 2.0)
23/tcp    open  telnet    Linux telnetd
25/tcp    open  smtp      Postfix smtpd
53/tcp    open  domain    ISC BIND 9.4.2
80/tcp    open  http      Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind   2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login     OpenBSD or Solaris rlogind
514/tcp   open  shell?
1099/tcp  open  java-rmi  GNU Classpath gmicregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs       2-4 (RPC #100003)
2223/tcp  open  ftp       ProFTPD 1.3.1
3306/tcp  open  mysql     MySQL 5.0.51A-Ubuntu
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 ~ 8.3.7
5900/tcp  open  vnc       VNC (protocol 3.3)
6000/tcp  open  x11       (access denied)
6067/tcp  open  irc       UnrealIRCd
6880/tcp  open  ajp13     Apache Jserv (Protocol v1.3)
8180/tcp  open  http      Apache Tomcat/Coyote JSP engine 1.1
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
_ =Port|SIA-TCP|V=7.91K|7MD=11/23Time=637E4E51KP=X86_64-pc-linux-gnuXr(NU
_FIL_XL_X=xelCouldnt|x2oGet|x2oadress|x2ofor|x2oYour|x2ohost|x2o(kali|
_CFI_VN);
MAC Address: 52:54:00:BB:BC:CD (QEMU virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.18s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01:f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh       OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
53/tcp    filtered domain
80/tcp    open  http      Apache httpd 2.4.7 ((Ubuntu))
9929/tcp  open  nping-echo Nping echo
13337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 84.64 seconds
```

g Novament pels dos, un *nmap -PN*. (0,5 punts)

```
└─$ nmap -PN 192.168.122.174 scanme.nmap.org
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-23 16:48 UTC
Nmap scan report for 192.168.122.174
Host is up (0.00025s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 52:54:00:B8:BC:CD (QEMU virtual NIC)

Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.17s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    filtered domain
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 2 IP addresses (2 hosts up) scanned in 13.67 seconds
```

h I finalment pels dos, un *nmap -F*. (0,5 punts)

```
# nmap -F 192.168.122.174 scanme.nmap.org STATE SERVICE
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-23 16:51 UTC
Nmap scan report for 192.168.122.174 3/tcp open: https
Host is up (0.00021s latency).
Not shown: 82 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
8009/tcp  open  ajp13
MAC Address: 52:54:00:B8:BC:CD (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up)
root@kali:~# nmap -F 80 sapalomera.cat
Starting Nmap 7.91 ( https://nmap.org )
Nmap scan report for sapalomera.cat
Host is up (0.14s latency).

PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up)
root@kali:~# nmap -F 2600:3c01::f03c:91ff:fe18:bb2f sapalomera.cat
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.19s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 97 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    filtered domain
80/tcp    open  http

Nmap done: 2 IP addresses (2 hosts up) scanned in 1.87 seconds
```



- i Per un dels 2, feu un anàlisi de tots els TCP amb *nmap -sT* i per l'altre, un anàlisi de tots els ports UDP amb. (0,5 punts)

```
└─$ nmap -sT 192.168.122.174
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-23 16:52 UTC
Nmap scan report for 192.168.122.174
Host is up (0.00050s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 52:54:00:B8:BC:CD (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```

- j Per acabar, feu un escombrat de ping i identifiqueu els hosts de la vostra xarxa. Si la meua xarxa és 192.168.1.0, jo faré *nmap -sn 192.168.1.0/24* (0,5 punts)

```
└─$ nmap -sn 192.168.122.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2022-11-23 18:47 UTC
Nmap scan report for 192.168.122.1
Host is up (0.0054s latency).
Nmap scan report for kali (192.168.122.20)
Host is up (0.000092s latency).
Nmap scan report for nil-Standard-PC-i440FX-PIIX-1996 (192.168.122.44)
Host is up (0.0066s latency).
Nmap scan report for 192.168.122.174
Host is up (0.0017s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.57 seconds
```



### Exercici 3: Rsyslog (2 punts)

En aquest últim exercici cal que afegiu una sèrie de configuracions al final de l'arxiu **/etc/rsyslog.d/50-default.conf**. **No cal que modifiqueu la resta d'entrades del fitxer.**

Cal també que **creeu un fitxer de log propi per fer els testos**, feu les següents comandes:

```
sudo touch /var/log/activitat4.log  
sudo chown syslog:adm /var/log/activitat4.log
```

**Recordeu que després d'aplicar canvis a les configuracions cal reiniciar el daemon:**  
**/etc/init.d/rsyslog restart**

Aquestes han de 'seguir' les següents característiques (Poseu-me una captura a cada apartat que el demostrï) :

a) Cal una entrada que faci que totes les facilitats de tipus **'news'** amb el tipus de **prioritat de 0 (emerg) fins a 4 (warn)**. Aquest ha d'anar al log **/var/log/activitat4.log (0,5 punts)**

```
news.warn /var/log/activitat4.log
```

b) Cal enviar a **/var/log/activitat4.log** tot el que sigui de tipus **mail excepte** si es de prioritat **debug. (0,5 punts)**

```
mail.*;mail.none !debug /var/log/activitat4.log
```

c) I enviar a **/var/log/activitat4.log** tots els que siguin de prioritat **critical (2) i error (3) excepte** si són de la facilitat **daemon. (0,5 punts)**

```
*.crit;*.err;*.none !daemon /var/log/activitat4.log
```

d) Ara cal que ho demostreu amb la comanda **logger**. Per això feu el següent:

Recordeu que cal llançar : **logger -p *facilitat.prioritat* "missatge"**

Per la a) cal fer loggers que demostrï que els de tipus **news.alert** hi van i **news.info**, no

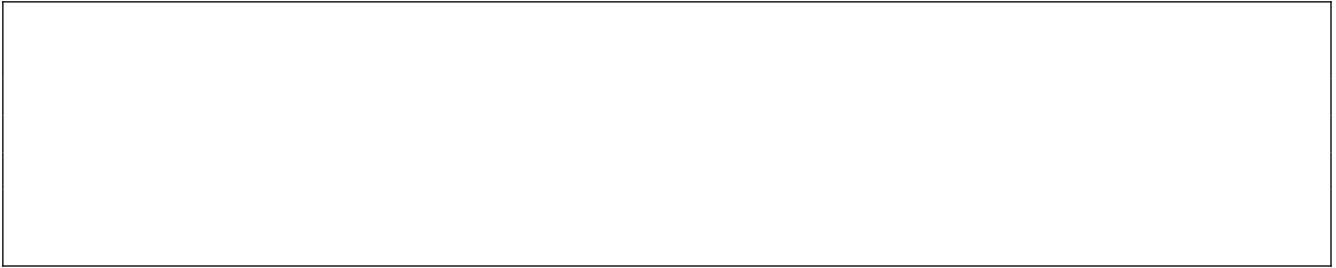
Per la b) cal fer loggers per demostrar que els de **mail.notice** hi van i **mail.debug**, no

Per la c) cal fer loggers per demostrar que els de tipus **cron.error** hi van i **daemon.error**, no.

Per la c) cal fer loggers per demostrar que els de tipus **auth.crit** hi van i **daemon.crit**, no

Només cal adjuntar una captura que demostrï el llançament de totes les comandes.

El contingut de missatge ha de ser sempre “**activitat4-exercici3**” (0,3 punts)



e) Finalment, cal que **demostrreu** que realment els **logs han anat** on havien d'anar. (1,2 punts )

Per tant **busqueu als logs que toquin** les coincidències del missatge “activitat4-exercici1” per tal de demostrar els apartats a, b i c. Feu una captura on es vegin tots o una per cada cas, segons com feu la demostració.

