📑 Informe de Auditoría – Práctico de Ciberseguridad en Linux

Estudiante: ________________________

Curso: 3° Bachillerato Tecnológico – Ciberseguridad

Fecha: 01/10/2025

Introducción

Breve explicación sobre el objetivo del práctico: aplicar herramientas de Linux para resolver casos de uso en ciberseguridad, recolectar evidencias y generar un informe tipo auditoría.

Caso 1

Descripción: ...

Comandos utilizados:

```
nmap -sV -O 192.168.1.1 -oN inventario_red.txt
```

Salida obtenida (fragmento):

```
# Nmap 7.98 scan initiated Wed Sep 24 22:05:53 2025 as: nmap -sV -O -oN inventario_red.txt -oX C:\\Users\\ADMINI~1\\AppData\\Local\\Temp\\1\\zenmap-l3ikamiu.xml 192.168.1.1
```

```
Nmap scan report for pfSense.home.arpa (192.168.1.1)

Host is up (0.0015s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT   STATE SERVICE VERSION

53/tcp open  domain  Unbound

80/tcp open  http    nginx

MAC Address: 00:15:5D:17:65:1F (Microsoft)
```

```
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running (JUST GUESSING): FreeBSD 11.X (97%)

OS CPE: cpe:/o:freebsd:freebsd:11.2

Aggressive OS guesses: FreeBSD 11.2-RELEASE (97%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop


OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

# Nmap done at Wed Sep 24 22:06:10 2025 -- 1 IP address (1 host up) scanned in 17.31 seconds
```

Análisis: ...

Caso 2

Descripción: ...

Comandos utilizados:

```
ss-tulnp 192.168.1.1
```

Salida obtenida (fragmento):

```
Starting Nmap 7.98 ( https://nmap.org ) at 2025-09-24 22:10 +0200

Nmap scan report for pfSense.home.arpa (192.168.1.1)

Host is up (0.0011s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT   STATE SERVICE

53/tcp open  domain

80/tcp open  http
```

MAC Address: 00:15:5D:17:65:1F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 5.31 seconds

Análisis: ...

Caso 3

Descripción: ...

Comandos utilizados:

```
grep "Failed password" /var/log/auth.log | awk '{print
$1,$2,$3,$11}' | sort | uniq -c | sort -nr > intentos_fallidos.txt
```

Salida obtenida (fragmento):

```
3 Jan 2 05:51:42 218.92.0.249
```

```
  2 Jan 4 07:14:54 36.110.228.254
  2 Jan 4 04:12:51 83.222.191.90
  2 Jan 4 03:25:32 182.215.66.232
  2 Jan 2 05:47:18 218.92.0.249
  2 Jan 2 04:11:48 47.93.4.43
  1 Jan 4 07:19:26 oracle
  1 Jan 4 07:14:55 36.110.228.254
  1 Jan 4 06:43:48 111.67.203.28
  1 Jan 4 06:43:44 es
  1 Jan 4 06:40:53 kafka
  1 Jan 4 06:40:46 hadoop
  1 Jan 4 06:40:37 14.50.17.15
  1 Jan 4 06:40:33 hadoop
  1 Jan 4 06:19:37 deploy
```

```
1 Jan 4 06:19:36 178.160.211.111

1 Jan 4 06:17:16 178.160.211.111

1 Jan 4 05:48:17 debian

1 Jan 4 05:45:28 metricbeat

1 Jan 4 04:15:20 120.157.48.236

1 Jan 4 04:12:51 user

1 Jan 4 04:12:51 guest

1 Jan 4 03:39:05 117.50.187.153

1 Jan 4 03:39:02 117.50.187.153

1 Jan 4 03:38:53 117.50.187.153

1 Jan 4 03:35:59 test

1 Jan 4 03:25:33 182.215.66.232

1 Jan 4 02:40:38 mysql

1 Jan 4 02:16:52 mysql

1 Jan 4 01:36:28 user

1 Jan 4 01:20:36 test

1 Jan 4 01:20:22 23.95.213.210

1 Jan 4 01:04:55 master

1 Jan 4 00:41:07 sonar

1 Jan 4 00:25:49 190.115.3.147

1 Jan 4 00:25:21 oracle

1 Jan 4 00:10:05 nfsnobody

1 Jan 4 00:10:04 161.132.48.181

1 Jan 4 00:08:53 oracle

1 Jan 4 00:07:51 usr

1 Jan 4 00:00:42 oracle
```

```
1 Jan 3 23:48:07 minecraft
1 Jan 3 23:48:05 172.93.223.152
1 Jan 3 23:45:27 minecraft
1 Jan 3 23:29:08 oracle
1 Jan 3 23:05:13 hadoop
1 Jan 3 22:49:20 hadoop
1 Jan 3 22:41:11 oracle
1 Jan 3 21:54:44 hadoop
1 Jan 3 21:52:15 test
1 Jan 3 20:03:33 102.211.152.45
1 Jan 3 19:58:52 nao
1 Jan 3 18:22:14 zxfang
1 Jan 3 18:20:59 user
1 Jan 3 17:59:39 1111
1 Jan 3 17:45:34 142.93.231.154
1 Jan 3 17:38:30 142.93.231.154
1 Jan 3 17:31:28 nsrecover
1 Jan 3 17:10:21 zhangyifan
1 Jan 3 16:24:35 chenlu
1 Jan 3 15:58:29 star
1 Jan 3 15:45:24 195.178.110.67
1 Jan 3 15:38:51 195.178.110.67
1 Jan 3 15:32:19 195.178.110.67
1 Jan 3 15:19:16 ljh
1 Jan 3 15:06:10 v
1 Jan 3 14:51:38 185.236.23.4
```

```
1 Jan 3 14:51:36 kafka
1 Jan 3 14:49:22 nfsnobody
1 Jan 3 14:46:35 q
1 Jan 3 14:41:01 20.54.133.96
1 Jan 3 14:33:33 b
1 Jan 3 14:27:04 a
1 Jan 3 14:18:50 guolili
1 Jan 3 14:18:37 guolili
1 Jan 3 10:26:11 pi
1 Jan 3 08:58:29 runner
1 Jan 3 08:49:54 209.38.19.214
1 Jan 3 08:45:29 209.38.19.214
1 Jan 3 08:45:27 dev
1 Jan 3 08:43:17 209.38.19.214
1 Jan 3 08:41:10 209.38.19.214
1 Jan 3 07:54:45 wang
1 Jan 3 07:41:41 dev
1 Jan 3 07:39:04 209.38.86.137
1 Jan 3 07:36:54 209.38.86.137
1 Jan 3 03:28:19 8.245.24.52
1 Jan 3 03:28:16 8.245.24.52
1 Jan 3 00:30:32 tron
1 Jan 3 00:17:05 postgres
1 Jan 3 00:14:57 usr
1 Jan 2 23:45:57 polygon
1 Jan 2 23:20:29 zxfang
```

```
1 Jan 2 23:07:45 45.148.10.240

1 Jan 2 23:01:24 gr

1 Jan 2 22:48:39 ubuntu

1 Jan 2 22:35:56 ubuntu

1 Jan 2 22:23:12 ps

1 Jan 2 22:10:28 zhangyifan

1 Jan 2 22:04:06 students

1 Jan 2 21:57:44 45.148.10.240

1 Jan 2 21:50:54 156.241.0.65

1 Jan 2 21:50:52 156.241.0.65

1 Jan 2 21:50:50 156.241.0.65

1 Jan 2 21:25:54 chenlu

1 Jan 2 21:00:27 star

1 Jan 2 20:47:45 45.148.10.240

1 Jan 2 20:41:25 45.148.10.240

1 Jan 2 20:35:03 45.148.10.240

1 Jan 2 20:22:22 validator

1 Jan 2 20:16:02 ubuntu

1 Jan 2 17:58:54 154.19.165.62

1 Jan 2 17:58:51 154.19.165.62

1 Jan 2 17:58:49 154.19.165.62

1 Jan 2 17:02:22 guest

1 Jan 2 17:02:08 guest

1 Jan 2 16:33:40 101.168.52.168

1 Jan 2 16:33:18 101.168.52.168

1 Jan 2 16:28:14 test
```

```
1 Jan 2 16:27:54 101.168.52.168

1 Jan 2 16:25:31 a

1 Jan 2 15:20:41 wang

1 Jan 2 15:12:21 user1

1 Jan 2 15:07:43 170.64.170.111

1 Jan 2 15:02:48 170.64.170.111

1 Jan 2 11:52:46 solana

1 Jan 2 11:36:22 node

1 Jan 2 11:28:22 validator

1 Jan 2 10:47:16 170.64.237.98

1 Jan 2 10:47:14 tools

1 Jan 2 10:45:03 elsearch

1 Jan 2 10:39:38 170.64.237.98

1 Jan 2 10:39:37 nginx

1 Jan 2 10:35:10 170.64.237.98

1 Jan 2 10:30:54 170.64.237.98

1 Jan 2 09:50:46 103.146.50.230

1 Jan 2 09:50:42 103.146.50.230

1 Jan 2 09:35:46 45.5.159.34

1 Jan 2 09:35:45 45.5.159.34

1 Jan 2 09:35:39 45.5.159.34

1 Jan 2 05:54:22 193.32.162.79

1 Jan 2 05:47:45 193.32.162.79

1 Jan 2 05:47:17 218.92.0.249

1 Jan 2 05:44:18 218.92.0.249

1 Jan 2 05:44:17 218.92.0.249
```

```
1 Jan 2 05:44:16 218.92.0.249

1 Jan 2 05:21:22 oneadmin

1 Jan 2 05:01:31 oneadmin

1 Jan 2 04:48:18 webmin

1 Jan 2 04:35:06 webadmin

1 Jan 2 04:11:32 47.93.4.43

1 Jan 2 04:02:03 193.32.162.79

1 Jan 2 03:55:26 hadoop

1 Jan 2 03:28:56 hadoop

1 Jan 2 03:09:02 oracle

1 Jan 2 02:55:51 loginuser

1 Jan 2 02:49:17 a3user

1 Jan 2 01:45:38 ubnt

1 Jan 2 01:41:04 81.17.25.50

1 Jan 2 01:40:55 81.17.25.50

1 Jan 2 01:38:14 0

1 Jan 2 01:17:16 simple

1 Jan 2 01:12:20 ftpuser

1 Jan 2 01:07:31 lab

1 Jan 2 01:03:01 102.211.152.45

1 Jan 1 23:44:42 185.246.128.133

1 Jan 1 23:16:04 142.93.231.154

1 Jan 1 22:54:44 142.93.231.154

1 Jan 1 22:47:41 142.93.231.154

1 Jan 1 22:33:31 user

1 Jan 1 22:26:25 142.93.231.154
```

```
1 Jan 1 22:19:19 142.93.231.154
1 Jan 1 22:12:11 142.93.231.154
1 Jan 1 22:05:05 142.93.231.154
1 Jan 1 21:57:57 142.93.231.154
1 Jan 1 21:50:51 142.93.231.154
1 Jan 1 21:43:42 142.93.231.154
1 Jan 1 21:36:37 142.93.231.154
1 Jan 1 21:31:21 oratest
1 Jan 1 21:31:04 103.54.18.7
1 Jan 1 21:30:51 103.54.18.7
1 Jan 1 21:29:22 142.93.231.154
1 Jan 1 21:22:13 142.93.231.154
1 Jan 1 20:46:28 142.93.231.154
1 Jan 1 20:39:21 vpn
1 Jan 1 20:11:00 user
1 Jan 1 19:49:34 1111
1 Jan 1 19:35:24 142.93.231.154
1 Jan 1 19:28:13 142.93.231.154
1 Jan 1 19:24:02 193.105.134.95
1 Jan 1 19:21:04 nsrecover
1 Jan 1 19:09:23 system
1 Jan 1 19:04:39 test
1 Jan 1 19:02:04 170.64.235.124
1 Jan 1 19:02:03 170.64.235.124
1 Jan 1 19:00:31 esroot
1 Jan 1 19:00:31 170.64.235.124
```

```
1 Jan 1 18:56:26 170.64.235.124

1 Jan 1 18:56:24 server

1 Jan 1 18:54:19 170.64.235.124

1 Jan 1 18:52:10 170.64.235.124

1 Jan 1 18:41:50 esroot

1 Jan 1 18:33:08 developer

1 Jan 1 18:31:16 185.246.128.133

1 Jan 1 18:28:50 170.64.237.191

1 Jan 1 18:28:49 lsfadmin

1 Jan 1 18:24:33 170.64.237.191

1 Jan 1 17:37:10 158.41.97.70

1 Jan 1 17:36:58 158.41.97.70

1 Jan 1 17:36:53 158.41.97.70

1 Jan 1 15:49:20 mcserver

1 Jan 1 15:49:19 195.26.247.217

1 Jan 1 15:47:14 openvswitch

1 Jan 1 15:33:17 ftp

1 Jan 1 11:53:47 deploy

1 Jan 1 11:51:32 121.229.42.32

1 Jan 1 11:51:22 121.229.42.32

1 Jan 1 08:31:48 systemv

1 Jan 1 08:31:44 168.187.50.230

1 Jan 1 08:14:20 168.187.50.230

1 Jan 1 08:14:19 168.187.50.230

1 Jan 1 08:11:44 es

1 Jan 1 07:08:59 pi
```

```
  1 Jan 1 06:46:08 postgres

  1 Jan 1 06:44:10 postgres

  1 Jan 1 06:41:43 vyos

  1 Jan 1 04:56:35 host

  1 Jan 1 04:23:05 ginie

  1 Jan 1 04:22:52 ginie

  1 Jan 1 04:08:58 asus

  1 Jan 1 03:36:49 user1

  1 Jan 1 03:13:18 shanghai

  1 Jan 1 02:57:11 zy

  1 Jan 1 02:41:28 mos

  1 Jan 1 02:33:32 mos

  1 Jan 1 02:32:40 120.157.56.121

  1 Jan 1 02:25:37 2.57.122.191

  1 Jan 1 02:00:54 mysql

  1 Jan 1 01:36:45 lzx

  1 Jan 1 01:28:19 2.57.122.191

  1 Jan 1 01:19:56 gr

  1 Jan 1 01:08:28 mysql

  1 Jan 1 01:03:51 ubuntu
```

Análisis: ...

Caso 4

Descripción: ...

Comandos utilizados:

```
FECHA=$(date +%Y%m%d) DESTINO="/backups/proyecto_$FECHA"
rsync -av --progress /home/proyecto/ $DESTINO
```

Salida obtenida (fragmento):

```
sh: rsync: not found
```

Análisis: ...

Caso 5

Descripción: ...

Comandos utilizados:

```
timeout 60 tcpdump -i hn1 port 443 -w trafico_https.pcap
```

Salida obtenida (fragmento):

```
tcpdump: listening on hn1, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
402467 packets captured

403128 packets received by filter

0 packets dropped by kernel
```

Análisis:

Archivo no legible.

Caso 6

Descripción: ...

Comandos utilizados:

```
DOMINIO="ejemplo.com"

whois $DOMINIO > dominio_info.txt

dig $DOMINIO ANY +noall +answer >> dominio_info.txt
```

Salida obtenida (fragmento):

Caso 7

Descripción: ...

Comandos utilizados:

[Pegar comandos aquí]

Salida obtenida (fragmento):

[Pegar salida aquí]

Análisis: ...

Caso 8

Descripción: ...

Comandos utilizados:

[Pegar comandos aquí]

Salida obtenida (fragmento):

[Pegar salida aquí]

Análisis: ...

Caso 9

Descripción: ...

Comandos utilizados:

```
sha256sum /etc/passwd > hash_actual.txt

diff hash_original.txt hash_actual.txt || echo "Archivo modificado"
```

Salida obtenida (fragmento):

```
Archivo modificado
```

Análisis:

```
cat hash_actual.txt
```

```
fac5de78308dcdfd1467e0935249d9ce8b5a084cbeecd3a758f838fd4dbaf746  /etc/passwd
```

Caso 10

Descripción: ...

Comandos utilizados:

[Pegar comandos aquí]

Salida obtenida (fragmento):

[Pegar salida aquí]

Análisis: ...

Conclusiones Generales

Síntesis del trabajo: ...

Referencias

- Agesic – Marco de Ciberseguridad (MCU)
- NIST Cybersecurity Framework
- ISO/IEC 27001
- OWASP Top 10