| Grupo 10 | Exemple de examen de laboratori de SI | Q1: 09-12-2019 |
|---|---|---|
| Nombre: | Apellidos: | |

**Test. 10 puntos**.
Tiempo de resolución estimado: **50 minutos**
Las preguntas pueden ser

- Respuesta única (RU). Una respuesta RU correcta cuenta 0.X puntos.
- Multirespuesta (MR). Una respuesta MR correcta cuenta 0.Y puntos, la mitad si hay un solo error, 0 en los otros casos. En las MR puede haber desde una hasta todas respuestas correctas.

```
syseng@debian:~$ ipt
Chain INPUT (policy DROP 319 packets, 20708 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        6   324 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
2    19830   50M ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           ctstate RELATED,ESTABLISHED
3        0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0           icmptype 8
4        0     0 ACCEPT     tcp  --  *      *       172.16.1.0/24        0.0.0.0/0           tcp dpt:22
5        0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
6        1    52 ACCEPT     udp  --  *      *       0.0.0.0/0            0.0.0.0/0


Chain FORWARD (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      760  131K ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           ctstate RELATED,ESTABLISHED
2      180 12095 ACCEPT     all  --  lan    wan     0.0.0.0/0            0.0.0.0/0


Chain OUTPUT (policy DROP 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1    20945 3786K ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0
2        0     0 ACCEPT     all  --  *      lo      0.0.0.0/0            0.0.0.0/0
```

1. **MR**. De acuerdo a la configuración de un firewall con la iptables de la figura, marca la o las afirmaciones correctas

- ☐ Cualquier origen puede comunicarse con este firewall usando cualquier aplicación
- ☒ La regla por defecto en OUTPUT no se usará nunca
- ☒ Permite el forward de conexiones ya establecidas que solo podrán venir de la interfaz wan a la interfaz lan
- ☒ Cualquier origen de la red 172.16.1.0/24 puede conectarse por ssh (puerto 22) al firewall
- ☒ Si se hace un ping al firewall (icmp), este podrá contestar

2. **MR**. Marca la o las afirmaciones correctas respecto a la figura anterior

- ☐ Si se eliminaran las líneas 2 y 3 de INPUT, el firewall solo aceptaría comunicaciones de aplicaciones que usan UDP
- ☐ Introduciendo iptables -P FORWARD -j ACCEPT, el firewall permitiría el forward de todos los datagramas
- ☐ Cambiando la regla por defecto de INPUT a ACCEPT, el fireall aceptaría cualquier conexión por TCP
- ☒ Si se cambiara la línea 2 de FORWARD, permitiendo cualquier interfaz de entrada y salida, el firewall permitiría cualquier forward

3. **MR**. Cual es la función de MailPot y FakeDNS en la practica de análisis de código malicioso

- ☐ Deshabilitar el código malicioso
- ☒ Interceptar los correos que el código malicioso intenta enviar
- ☐ Hacerle creer que el sistema ha sido infectado y por lo tanto el código malicioso puede parar de replicarse
- ☐ Permitir que se reproduzca y se propague por correo

4. **RU**. Cual es el propósito del texto “test” en el código malicioso Windows Live Messanger

- ☐ Al introducir este texto como correo electrónico, se borra el código malicioso
- ☒ Al introducir este texto como correo electrónico, se entra en la configuración del código malicioso
- ☐ Al introducir este texto como contraseña, enseña quien es el autor del código malicioso
- ☐ Al introducir este texto como contraseña, se bloque la reproducción de este código malicioso

```
alert tcp $HOME_NET any <> any [80,443] (msg:"???"; content: "eBay.com"; sid: 10000005; rev:001;)

alert tcp any any -> 147.83.2.135 80 (content: "POST"; nocase; msg: "???"; threshold: type both, track by_src, count 30, seconds 60;
                                      sid: 10000006; rev:001;)
```

5. **RU**. Cual es la función de la primera regla de la configuración del snort de la figura anterior

- ☐ Salta una alarma cada vez que cualquier IP intenta acceder a cualquier host del dominio eBay.com
- ☒ Salta una alarma si un host de la red interna intenta acceder a la web de eBay.com
- ☐ No funciona ya que la regla está mal escrita
- ☐ Salta una alarma si un host de la red interna intenta acceder a cualquier host del dominio eBay.com

6. **RU**. Cual es la función de la segunda regla de la configuración del snort de la figura anterior

- ☒ Salta una alarma si alguien intenta enviar un POST HTTP a la web 147.83.2.135 más de 30 veces en 60 segundos
- ☐ Salta una alarma si más de 30 hosts intentan atacar la web 147.83.2.135 con POST HTTP masivos en un rango de tiempo de 60 segundos
- ☐ No funciona ya que la regla está mal escrita
- ☐ Salta una alarma si salen de la web 147.83.2.135 más de 30 POST HTTP en 60 segundos

7. **MR**. La aplicación web de la practica 1 usa un método concreto para determinar las cookies de autentificación. Sabiendo que todas empiezan por 65432, determinar cuales serían los otros caracteres para el usuario andrea

- ☐ 65432zdqcmz
- ☐ 65432boesfb
- ☒ 65432bfseob
- ☐ 65432zmcqdz
- ☐ 65432aerdna

8. **MR**. En la practica 1 de seguridad en aplicaciones web, como se ha podido modificar el precio del televisor

- ☐ Se ha interceptado la descarga de la web en el navegador local, se ha modificado el campo del precio antes de recibir este contenido y una vez recibido con el precio modificado, se ha dado a comprar
- ☐ Se ha enviado la solicitud de compra, se ha interceptado la respuesta del servidor con la confirmación de la compra y se ha modificado el campo del precio
- ☐ Se ha interceptado el contenido de la web de compra, se ha eliminado el código javascript de validación de la compra, se ha modificado el campo del precio y finalmente se ha dado a comprar
- ☒ Se ha interceptado el envío del comando comprar, se ha modificado el campo del precio antes de enviar la petición de compra al servidor y finalmente se ha enviado con el precio modificado

9. **RU**. En la practica de análisis forense, indicar como ha sido manipulada la imagen

- ☐ Se ha comprimido con una contraseña
- ☐ Se ha dividido en varios bloques y distribuidos por todo el disquete
- ☒ Se ha modificado el número de sectores asignados al fichero
- ☐ Se ha modificado el tamaño del fichero, añadiendo bits a 0 al final
- ☐ Se ha usado la extensión png cuando realmente es una imagen jpeg

10. **RU**. En la practica de análisis forense, cuantos ficheros diferentes se pueden encontrar en el disquete

- ☐ 1
- ☐ 2
- ☒ 3
- ☐ 4
- ☐ 5
- ☐ No se sabe