Grupo 10	Examen de laboratori de Seguretat Informàtica	Q1: 13-12-2019
Nombre:	Apellidos:	

Test. 10 puntos.
Tiempo de resolución estimado: **55 minutos**
Las preguntas pueden ser

- Respuesta única (RU). Una respuesta RU correcta cuenta 0.5 puntos.
- Multirespuesta (MR). Una respuesta MR correcta cuenta 0.75 puntos, 0.3 si hay un solo error, 0 en los otros casos. En las MR puede haber desde una hasta todas respuestas correctas.

1. **MR**. Marca la o las afirmaciones correctas

- [x] Un CSR contiene una clave pública auto-firmada
- [x] Un certificado de autoridad (CA) raíz contiene una clave pública auto-firmada
- [ ] Un certificado de usuario siempre se incluye en un fichero PKCS#12
- [ ] Las opciones 2 y 3 anteriores son ciertas

2. **MR**. Un path concreto del servidor Apache se protege con TLS con autenticación de cliente. Si los certificados de usuario están firmados por una CA que a su ve está firmada por otra CA en la que se confía, entonces marcar la o las afirmaciones correctas

- [x] La variable de configuración SSLVerifyClient puede estar a "require"
- [ ] El directorio en el path debe llamarse "private"
- [x] La variable de configuración SSLVerifyDepth puede estar a 2
- [x] La variable de configuración SSLVerifyDepth puede estar a 3

3. **MR**. Dado el comando siguiente "`openssl req -new -extensions v3_req -keyout key.pem -out cert-req.pem`", marca la o las afirmaciones correctas

- [ ] Siempre forma parte de un proceso de generación de un certificado para un servidor web
- [ ] Solicita un formato de CSR versión 3 con extensiones propietarias
- [x] Sirve para generar un certificado versión 3 con extensiones
- [x] Las opciones 1 y 2 son falsas

4. **MR**. Sobre la práctica realizada de Análisis Forense, marcar la o las afirmaciones correctas

- [ ] El sistema de ficheros de la imagen es FAT16
- [x] El tamaño del cluster es 512 y el del sector también
- [x] A uno de los ficheros se le había modificado el tamaño en la FAT
- [ ] Todas las opciones anteriores son falsas

5. **MR**. Sobre la aplicación Autopsy, marca la o las afirmaciones correctas

- [x] Permite recuperar ficheros borrados con sectores discontinuos
- [ ] Solo sirve para analizar sistema Windows
- [x] En un caso abierto, se pueden analizar varios sistemas de ficheros
- [ ] La aplicación detecta los ficheros en función de su magic number

6. **RU**. En la tabla filter de iptables NO podemos realizar

- [ ] El filtrado de paquetes basado en el estado de una conexión
- [ ] Hacer logging de eventos de red
- [x] Modificar las cabeceras de los paquetes
- [ ] Filtrar por puerto, IP origen e IP destino a la vez

7. **RU**. Queremos denegar todo el tráfico HTTP de salida hacia el destino 1.2.3.4, ¿cuál sería el comando correcto?

- [x] iptables -I OUTPUT 1 -p tcp --dport 80 --dst 1.2.3.4 -j DROP
- [ ] iptables -A OUTPUT -p udp --dport 80 --dst 1.2.3.4 -j DROP
- [ ] iptables -A OUTPUT --dport 80 --dst 1.2.3.4 -j DROP
- [ ] iptables -A OUTPUT any 1.2.3.4 --dport 80 -j DROP

8. **MR**. En referencia al fichero de logs que guarda Snort en `/var/log/snort/snort.log.*`

- [ ] Es un fichero de texto con todos los eventos que han pasado en el sistema
- [x] Es un fichero binario con todos los eventos que han cumplido algunas de las reglas especificadas en la configuración
- [ ] Detalla la configuración actual de Snort y permite visualizarla
- [ ] Es un fichero que mantiene la información sobre los servicios actualmente en ejecución en el sistema

9. **MR**. Con el objetivo de detectar ataques DDoS vistos en el lab con Snort debemos especificar en las reglas

- [ ] Es suficiente en detectar flujos con la IP Origen: `track by_src`
- [x] Es necesario detectar inicios de conexiones con el `flag: S`
- [ ] Es necesario detectar conexiones establecidas por destino: `track by_dst`
- [x] Es necesario detectar flujos con la IP Destino: `track by_dst`

10. **RU**. Para poder detectar ataques de denegación de servicio

- [ ] Solo se tienen que usar las claves `count` y `seconds` en las reglas
- [ ] Basta con detectar accesos con `track by_src` y `track by_dst`
- [x] Es necesario usar las dos opciones anteriores para que funcione
- [ ] Ninguna de las anteriores

11. **MR**. En la practica de seguridad en aplicaciones web, que técnicas se podrían implementar para modificar el precio del viaje de Boston a Seattle

- [x] Interceptar la descarga de la web en el navegador local, modificar el campo del precio antes de recibir este contenido y una vez recibido con el precio modificado, dar a comprar
- [ ] Enviar la solicitud de compra, interceptar la respuesta del servidor con la confirmación de la compra y modificar el campo del precio
- [ ] Interceptar el contenido de la web de compra, eliminar el código javascript de validación de la compra, modificar el campo del precio y finalmente dar a comprar
- [x] Interceptar el envío del comando comprar, modificar el campo del precio antes de enviar la petición de compra al servidor y finalmente enviar con el precio modificado

12. **RU**. En la practica de seguridad en aplicaciones web, indicar como se ha podido conseguir autenticarse como usuario webgoat sin usar una contraseña

- [ ] Se ha interceptado la respuesta negativa al darle a Login y simplemente se ha modificado en positiva
- [ ] Se ha interceptado la descarga de la página web y se ha borrado el form de la contraseña
- [x] Se ha interceptado la propia solicitud de Login con solo el usuario y se ha borrado el campo de la contraseña
- [ ] Se ha interceptado el código java y se han eliminado las líneas que validan del campo contraseña

13. **RU**. En la practica de análisis de código malicioso, que información contiene el fichero msnsettings.dat

- [ ] Es el fichero que luego se envía por correo
- [ ] Es donde se guardan la contraseña y el nombre de usuario
- [ ] Es el fichero de log del código donde se va anotando todas las operaciones del usuario
- [x] Es el fichero de configuración del código malicioso

14. **MR**. En la practica de análisis de código malicioso, marca la o las afirmaciones correctas

- [x] Al hacer el login, el código malicioso intenta resolver el nombre de un servidor de correo por DNS
- [x] El código malicioso pretende enviar por correo electrónico un mensaje que contiene el usuario y la contraseña introducida en el Windows Live Messanger
- [x] RegShot permite descubrir que el código malicioso ha modificado varios registros de Windows y ha creado 2 ficheros nuevos
- [ ] Analizando con OllyDbg las operaciones realizada por el código malicioso, se descubre que mastercleanex es la palabra clave para deshabilitar el virus

```
vivek@nixcraft:~$ sudo iptables -t filter -L --line-numbers -n
Chain INPUT (policy DROP )
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  10.98.222.0/24       0.0.0.0/0
2    ACCEPT     udp  --  192.168.122.0/24     0.0.0.0/0
3    ACCEPT     all  --  0.0.0.0/0            192.168.122.0/24     ctstate RELATED,ESTABLISHED
4    ACCEPT     tcp  --  192.168.122.0/24     0.0.0.0/0            tcp dpt:80
5    REJECT     all  --  0.0.0.0/0            0.0.0.0/0


vivek@nixcraft:~$ sudo iptables -t nat -L --line-numbers -n
Chain PREROUTING (policy ACCEPT)
num  target     prot opt source               destination

Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
num  target     prot opt source               destination
1    MASQUERADE  all  --  10.98.222.0/24      0.0.0.0/0
2    MASQUERADE  tcp  --  192.168.122.0/24    0.0.0.0/0
```

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

- [x] El host con @IP 192.168.122.10 se puede conectar a un servidor web de Internet
- [ ] El host con @IP 192.168.122.100 puede usar un servidor DNS (que usa UDP) de Internet para resolver un nombre
- [ ] El firewall hará el forward de cualquier paquete ya que la política por defecto es ACCEPT
- [ ] Un host de Internet se puede conectar al servidor con @IP 10.98.222.10
- [ ] El firewall podrá comunicarse con cualquier otro dispositivo