Grupo 10	Segundo Control de Seguretat Informàtica	Q1: 15-11-2019
Nombre:	Apellidos:	

Test. 3 puntos.
Tiempo de resolución estimado: **15 minutos**
Las preguntas pueden ser

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

1. **MR**. Indica que puede hacer un Proxy

- ☐ Detectar intrusos en una red segura
- ☒ Eludir restricciones regionales
- ☒ Filtrar correos controlando su contenido
- ☒ Decidir que conexiones permitir
- ☐ Proteger la red contra ataques desde dentro de la misma red segura

2. **MR**. Un IDS

- ☒ detecta un ataque al comparar la actividad de la red con una base de datos de ataques conocidos
- ☒ crea un modelo de comportamiento normal y detecta desviaciones
- ☐ puede ser de tipo intercepting o transparent
- ☒ puede ser basado en firmas o en anomalías

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

- ☒ Un HIDS puede simular una trampa (honeypot)
- ☐ Un NIDS puede ser DIDS, HIDS o ambos
- ☒ Snort es un ejemplo de NIDS
- ☒ Un DIDS puede detectar intrusos tanto en hosts como en segmentos de red
- ☐ Un IDS se crea combinando firewalls y proxies

4. **MR**. Indica que puede hacer un firewall

- ☐ Proteger la red contra ataques desde dentro de la misma red segura
- ☐ Proteger la red contra nuevos ataques cuando la regla por defecto es aceptar
- ☒ Monitorear el tráfico entrante y saliente
- ☐ Proteger la red contra malas configuraciones de los servicios autorizados

5. **MR**. Marca cuales de los siguientes usos de VPN es correcto

- ☒ Gw-to-Gw para establecer una conexión segura entre sistemas diferentes
- ☐ H-to-Gw para acceso remoto a un solo servidor
- ☐ Gw-to-Gw para acceso de usuarios de Internet a los servicios internos de una empresa
- ☒ H-to-H para proporcionar seguridad extremo-a-extremo

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

- ☒ IPSec AH proporciona integridad total de los paquetes
- ☐ IPSec ESP proporciona integridad solo a las cabeceras de los paquetes
- ☒ IPSec puede funcionar con AH, ESP o ambos
- ☐ Para IPSec AH se usa el modo túnel y para ESP se usa el modo transport

7. **RU**. Para la gestión de las vulnerabilidades, el punto inicial más importante es

- ☒ Tener un inventario donde se indica y describa cuales son los activos de la entidad
- ☐ Tener una herramienta de escaneo online que controle constantemente el acceso al sistema
- ☐ Instalar un analizador de código automático que detecte fallo y proporcione alarmas al programador
- ☐ Hacer una prueba de intrusión con las vulnerabilidades conocidas
- ☐ Hacer un modelo de posibles amenazas

8. **RU**. Un ataque de tipo "insecure deserialization" consiste en

- ☐ Cuando el proceso de autentificación está mal implementado y se puede pasar una sesión por URL
- ☐ Cuando se consigue introducir un código malicioso en un XML que será procesado posteriormente
- ☐ Cuando un usuario accede a una web sin darse cuenta que hay un código malicioso inyectado en la URL
- ☒ Cuando al procesar datos, se consigue introducir un cambio en un objeto que modifica el comportamiento de una aplicación

9. **RU**. Metasploit es

- ☐ Una herramienta para escanear posibles vulnerabilidades
- ☐ Una base de datos de exploits
- ☐ Un gestor de vulnerabilidades
- ☐ Una herramienta de análisis estático para comprobar la calidad de un código
- ☒ Una herramienta de desarrollo de exploits
- ☐ Una fundación creada para ayudar el desarrollo de software seguro

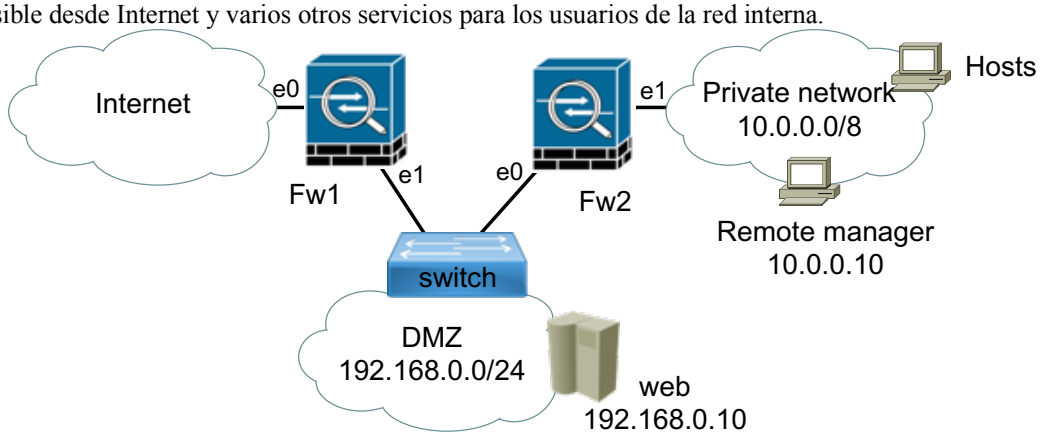
10. **MR**. Indicar cuales de los siguientes pasos hacen parte de una prueba de intrusión en una auditoria de seguridad

- ☒ Pruebas de escaneo del sistema para detectar que hay accesible y abierto
- ☒ Pruebas de explotación de vulnerabilidades para verificar el posible daño causado
- ☒ Análisis de los resultados de un escaneo y descubrimiento de vulnerabilidades
- ☒ Pruebas para adquirir toda la información posible sobre lo que se está auditando

Grupo 10	Segundo Control de Seguretat Informàtica	Q1: 15-11-2019
Nombre:	Apellidos:	

Problemas. 7 puntos.
Tiempo de resolución estimado: **35 minutos**.

1) Tiempo de resolución estimado: **20 minutos**
(**4 puntos**). La empresa "Complicado SL" te ha contratado para diseñar las políticas de seguridad de su infraestructura. La empresa dispone de una red privada (10.0.0.0/8) y una red DMZ (192.168.0.0/24). La red DMZ tiene un servidor web (TCP-80) accesible desde Internet y varios otros servicios para los usuarios de la red interna.



Determinar la configuración de los firewalls Fw1 y Fw2 sabiendo que:

- Fw1 y Fw2 se deben poder configurar de forma remota usando ssh desde el remote manager 10.0.0.10
- Fw1 se ocupa de proporcionar conectividad: i) desde Internet al servidor web usando la @IP 20.0.0.1 y ii) desde la red interna a Internet usando PAT.
- Fw2 se ocupa de proteger la red interna permitiendo que los hosts de la red interna solamente puedan: i) acceder a todos los servicios de la DMZ, y ii) conectarse a Internet y que este conteste

a) Define la configuración de Fw1

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP

iptables -t filer -A INPUT -i e1 -s 10.0.0.10 -p TCP -dport ssh -j ACCEPT
iptables -t filer -A OUTPUT -o e1 -d 10.0.0.10 -m state --state established -j ACCEPT

iptables -t nat POSTROUTING -i e1 -o e0 -s 192.168.0.10 -j SNAT --to-source 20.0.0.1
iptables -t nat PREROUTING -i e0 -o e1 -d 20.0.0.1 -j DNAT --to-destination 192.168.0.10

iptables -t nat POSTROUTING -i e1 -o e0 -s 10.0.0.0/8 -j MASQUERADE
```

b) Define la configuración de Fw2

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

iptables -t filer -A INPUT -i e1 -s 10.0.0.10 -p TCP -dport ssh -j ACCEPT
iptables -t filer -A OUTPUT -o e1 -d 10.0.0.10 -m state --state established -j ACCEPT

iptables -t filter -A FORWARD -i e1 -o e0 -s 10.0.0.0/8 -j ACCEPT
iptables -t filter -A FORWARD -i e0 -o e1 -d 10.0.0.0/8 -m state --state established -j ACCEPT
```

2) Tiempo de resolución estimado: **15 minutos**
(**3 puntos**) Contesta a las siguientes preguntas usando el espacio reservado en esta misma hoja

a) (**0.75 puntos**) En el problema 1. se ha usado una arquitectura compuesta por dos firewalls. Indicar que ventaja o ventajas puede tener esta configuración respecto a i) una con un único firewall sin DMZ y ii) una con un único firewall con DMZ.

Respecto a un único firewall sin DMZ: hay una zona DMZ que se puede proteger, que además puede usar direccionamiento privado
Respecto a un único firewall con DMZ:

- Si se ha considerado el caso con la DMZ expuesta: la DMZ está protegida y además puede usar direccionamiento privado
- Si se ha considerado el caso con firewall de 3 interfaces: los firewalls necesitan solo 2 interfaces, la configuración es más simple ya que cada firewall se ocupa de proteger una única parte del sistema

b) (**0.75 punto**) Indicar en que consiste un ataque de tipo Broken Authentication, que se puede conseguir y como se puede evitar

Este tipo de ataque se refiere a aprovechar alguna vulnerabilidad en todo lo relacionado con el proceso de login, gestión de sesiones y de credenciales. Si está mal programado, un atacante puede conseguir entrar en una sesión, capturando cookies enviadas en claro, por ejemplo, no reiniciando una sesión cuando se entra por otro dispositivo o guardando contraseñas en claro. Se puede evitar 1) usando HTTPS en toda la sesión, 2) usando la opción HTTPOnly cuando se envían las cookies de sesión, 3) pedir la confirmación de la identidad cuando se abre una sesión de un dispositivo desconocido o regenerar los identificadores de sesión para cada petición, 4) mantener las contraseñas cifradas concatenadas con una cadena aleatoria.

c) (**0.75 punto**) En IPSec se puede usar el protocolo AH o el protocolo ESP. Pero hay casos (raros) en los cuales se usan ambos. Prueba a deducir porque se puede llegar a necesitar los dos.

Cuando se negocia y establece una SA (Security Association), se puede decidir si usar AH, ESP o ambos.
El modo ESP proporciona cifrado, autentificación y integridad del contenido del datagrama. Pero ESP no protege la cabecera del control de integridad y puede haber casos que este control sea necesario. Por ejemplo, en el caso del modo transporte y arquitectura VPN de tipo H-to-H interesa que el control de la integridad sea sobre todo el datagrama para evitar que haya alguna manipulación de la cabecera en el camino. Por eso, se da la posibilidad de usar ambos, encapsulando un datagrama con ambas cabeceras AH y ESP.

d) (**0.75 puntos**) Explicar en que consiste un information gathering en una auditorias de seguridad

Consiste se está auditando a nivel de seguridad un sistema, el primer paso que se realiza es el information gathering. Esta fase consiste en obtener toda la información posible de los servidores o servicios que se están auditando. Información que en principio no deberíamos encontrar. Esta información puede ser: direcciones IP, nombres de los servidores, servicios externos usados, servidores virtualizados, ficheros internos de los servidores no protegidos, metadatos de los documentos. Finalmente, se puede buscar si algo de nuestro sistema está siendo publicado en la Deep Web o paginas conocidas de distribución de sitios comprometidos.