Grupo 10	Ejemplo Segundo Control de Seguretat Informàtica	Q1: 04-11-2019
Nombre:	Apellidos:	

Test. 3 puntos.
Tiempo de resolución estimado: **20 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**. Que puede hacer un Firewall

- ☒ Puede controlar el trafico de entrada y salida
- ☐ Puede controlar el comportamiento de las aplicaciones
- ☐ Puede filtrar correos controlando su contenido
- ☒ Puede decidir que conexiones permitir

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

- ☐ Los firewalls aceleran las conexiones TCP
- ☐ Los proxies solo administran el control de acceso y los logs de una red informática
- ☒ Los proxies auditan el contenido de los paquetes mientras que los firewalls solo verifican las cabeceras de los paquetes
- ☒ Los proxies se utilizan comúnmente para anonimizar internet conexiones
- ☐ Los firewalls son más seguros que los servidores proxy

3. **MR**. Los objetivos de los proxies son

- ☒ controlar las conexiones web de clientes internos
- ☒ establecer políticas de equilibrio de carga
- ☒ ocultar el servidor real a los usuarios
- ☒ ofrecer servicios como cifrado o compresión de datos
- ☒ permitir comunicaciones anónimas

4. **RU**. Marca la afirmación correcta

- ☐ IPSec opera a nivel de aplicación
- ☐ IPSec opera a nivel de transporte
- ☒ IPSec opera a nivel de red
- ☐ IPSec opera a nivel de enlace

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

- ☐ Gw-to-Gw para acceso remoto a un solo servidor
- ☒ H-to-Gw para acceso de un usuario externo a los servicios internos de una empresa
- ☒ H-to-H para administrar de forma remota otro ordenador
- ☒ Gw-to-Gw para establecer una conexión segura entre sistemas diferentes

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

- ☒ El modo tunnel de IPSec se usa generalmente para la VPN Gw-to-Gw
- ☐ IPSec AH proporciona cifrado de los paquetes
- ☐ IPSec ESP solo puede usar el modo transport
- ☒ IPSec SA sirve para que los dos extremos establezcan una asociación segura usando determinados parámetros de seguridad

7. **RU**. Que es OWASP

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

8. **RU**. Un ataque XSS consiste en

- ☐ Cuando se consigue inyectar un código malicioso en un servidor web
- ☐ 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 deserializar un objeto, se consigue introducir un cambio que modifica el comportamiento de una aplicación

9. **MR**. Una auditoria de seguridad a nivel de aplicaciones

- ☒ Consiste en revisar la seguridad y la integridad de las aplicaciones
- ☒ Consiste en evaluar las posibles vulnerabilidades encontradas en las aplicaciones y los servidores
- ☒ Consiste en revisar la seguridad y la integridad de los servidores
- ☐ Consiste en revisar las operaciones diarias de los usuarios
- ☐ Consiste en monitorizar los paquetes que entran y salen de un host

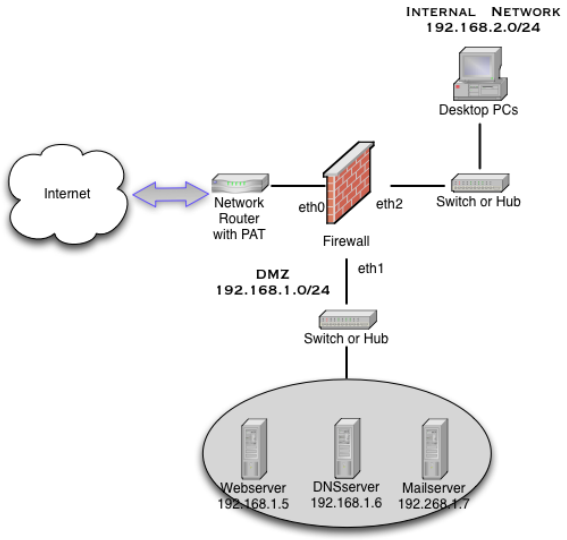
10. **RU**. Information gathering es una etapa de la auditoria que consiste en

- ☐ Explotar una vulnerabilidad
- ☐ Analizar manualmente posibles vulnerabilidades
- ☐ Escanear aplicaciones y servidores para descubrir que hay de abierto
- ☒ Buscar datos sobre servicios o documentos determinados que no deberían ser públicos

Grupo 10	Ejemplo Segundo Control de Seguretat Informàtica	Q1: 4-11-2019
Nombre:	Apellidos:	

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

1) Tiempo de resolución estimado: **20 minutos**
(**4 puntos**). La empresa de inversiones "Límit de Risc, S.L." te ha contratado para diseñar las políticas de seguridad de su red. La empresa dispone de 100 PCs, un servidor web (TCP-80), un servidor de DNS (UDP-53) y un servidor de mail (TCP-25, TCP-143). Se ha reservado el rango 50.0.0.0/29 para el NAT estático y la 50.0.0.10 para el PAT.



a) Define las políticas de seguridad por defecto

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

b) Se tiene que poder configurar el firewall exclusivamente desde el PC 192.168.0.100

iptables -t filter -A INPUT -i eth2 -s 192.168.0.100 -p TCP -dport ssh -j ACCEPT
iptables -t filter -A OUTPUT -o eth2 -d 192.168.0.100 -m state –state established -j ACCEPT

c) Configurar, si necesario, reglas de NAT/PAT. Motivar la respuesta.

No es necesario ya que se ve en la figura que hay un router de acceso que se encarga de hacer PAT

d) El servidor web debe ser accesible desde la red interna y desde Internet

iptables -A FORWARD -i eth1 -d 192.168.1.5 -p TCP -dport http -j ACCEPT
iptables -A FORWARD -o eth1 -s 192.168.1.5 -p TCP -sport http -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) (**0,5 puntos**) Indicar cual es la diferencia entre un HIDS y un NIDS.

Un Network IDS monitorea el tráfico en segmentos de red o dispositivos de red particulares; se pueden distribuir varios sensores por la infraestructura y capturar el trafico para analizar actividades sospechosas.
Un Host IDS monitorea las características de un solo host y los eventos que ocurren en este host y busca alguna actividad sospechosa.
Por lo tanto, la diferencia principal es que uno se ocupa de lo que pasa en la red, el otro de un host en concreto.

b) (**0,5 puntos**) Indicar porque en IPSec se sigue usando AH si ESP ya proporciona autentificación.

AH proporciona integridad para cabeceras IP y sus contenidos, mientras ESP solo protege el contenido

c) (**1 punto**) Identifica por lo menos 5 de los riesgos más críticos en las aplicaciones identificados por OWASP

Inyección de datos no confiables enviados en un comando o una query a un interprete
Proceso de gestión de autentificación y sesión mal implementado
Exposición involuntaria de datos sensibles
Control de acceso mal implementado, permitiendo accesos o acciones que deberían estar prohibidas
Cross site scripting (XSS) cuando un usuario ejecuta un código malicioso escrito por un atacante al acceder a una web

d) (**1 punto**) Explicar en que consiste hacer una prueba de intrusión en las auditorias de seguridad

Una vez puesto en funcionamiento aplicaciones o servicios, consiste en hacer una serie de pruebas para comprobar su seguridad desde el lado del usuario. Generalmente consiste de varias etapas:

1. Pruebas para adquirir toda la información posible sobre lo que se está auditando, sobretodo información que no debería estar disponible (estructura de la red, nombre de los equipos internos, @IP, ficheros, etc.)
2. Pruebas de escaneo del sistema para detectar que hay accesible y abierto
3. Análisis (manual o automática) de los datos obtenidos en el punto 1 y 2 para encontrar vulnerabilidades
4. Explotación de las vulnerabilidades bien a través de exploit ya conocidos o desarrollando nuevos para saber hasta donde se pueden hacer daños al sistema

Basic Iptables Options

Here are explanations for some of the iptables options you will see in this tutorial. Don't worry about understanding everything here now, but remember to come back and look at this list as you encounter new options later on.

1. `-A` - Append this rule to a rule chain. Valid chains for what we're doing are INPUT, FORWARD and OUTPUT, but we mostly deal with INPUT in this tutorial, which affects only incoming traffic.
2. `-L` - List the current filter rules.
3. `-m conntrack` - Allow filter rules to match based on connection state. Permits the use of the `--ctstate` option.
4. `--ctstate` - Define the list of states for the rule to match on. Valid states are:
    1. NEW - The connection has not yet been seen.
    2. RELATED - The connection is new, but is related to another connection already permitted.
    3. ESTABLISHED - The connection is already established.
    4. INVALID - The traffic couldn't be identified for some reason.
5. `-m limit` - Require the rule to match only a limited number of times. Allows the use of the `--limit` option. Useful for limiting logging rules.
    1. `--limit` - The maximum matching rate, given as a number followed by "/second", "/minute", "/hour", or "/day" depending on how often you want the rule to match. If this option is not used and `-m limit` is used, the default is "3/hour".
6. `-p` - The connection protocol used.
7. `--dport` - The destination port(s) required for this rule. A single port may be given, or a range may be given as `start:end`, which will match all ports from `start` to `end`, inclusive.
8. `-j` - Jump to the specified target. By default, iptables allows four targets:
    1. `ACCEPT` - Accept the packet and stop processing rules in this chain.
    2. `REJECT` - Reject the packet and notify the sender that we did so, and stop processing rules in this chain.
    3. `DROP` - Silently ignore the packet, and stop processing rules in this chain.
    4. `LOG` - Log the packet, and continue processing more rules in this chain. Allows the use of the `--log-prefix` and `--log-level` options.
9. `--log-prefix` - When logging, put this text before the log message. Use double quotes around the text to use.
10. `--log-level` - Log using the specified syslog level. 7 is a good choice unless you specifically need something else.
11. `-i` - Only match if the packet is coming in on the specified interface.
12. `-I` - Inserts a rule. Takes two options, the chain to insert the rule into, and the rule number it should be.
    1. `-I INPUT 5` would insert the rule into the INPUT chain and make it the 5th rule in the list.
13. `-v` - Display more information in the output. Useful for if you have rules that look similar without using `-v`.
14. `-s --source` - address[/mask] source specification
15. `-d --destination` - address[/mask] destination specification
16. `-o --out-interface` - output name[+] network interface name ([+] for wildcard)