

Grupo 10	Ejemplo Segundo Control de Seguretat Informàtica	Q1: 04-11-2019
Nombre:		Apellidos:
<p><b>Test. 3 puntos.</b>            Tiempo de resolución estimado: <b>20 minutos</b>            Las preguntas pueden ser</p> <ul style="list-style-type: none"> <li>• Respuesta única (RU). Una respuesta RU correcta cuenta 0.3 puntos.</li> <li>• 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.</li> </ul>		
<p>1. <b>MR.</b> Que puede hacer un Firewall</p> <p><input type="checkbox"/> Puede controlar el trafico de entrada y salida</p> <p><input type="checkbox"/> Puede controlar el comportamiento de las aplicaciones</p> <p><input type="checkbox"/> Puede filtrar correos controlando su contenido</p> <p><input type="checkbox"/> Puede decidir que conexiones permitir</p>		<p>2. <b>MR.</b> Marca la o las afirmaciones correctas</p> <p><input type="checkbox"/> Los firewalls aceleran las conexiones TCP</p> <p><input type="checkbox"/> Los proxies solo administran el control de acceso y los logs de una red informática</p> <p><input type="checkbox"/> Los proxies auditan el contenido de los paquetes mientras que los firewalls solo verifican las cabeceras de los paquetes</p> <p><input type="checkbox"/> Los proxies se utilizan comúnmente para anonimizar internet conexiones</p> <p><input type="checkbox"/> Los firewalls son más seguros que los servidores proxy</p>
<p>3. <b>MR.</b> Los objetivos de los proxies son</p> <p><input type="checkbox"/> controlar las conexiones web de clientes internos</p> <p><input type="checkbox"/> establecer políticas de equilibrio de carga</p> <p><input type="checkbox"/> ocultar el servidor real a los usuarios</p> <p><input type="checkbox"/> ofrecer servicios como cifrado o compresión de datos</p> <p><input type="checkbox"/> permitir comunicaciones anónimas</p>		<p>4. <b>RU.</b> Marca la afirmación correcta</p> <p><input type="checkbox"/> IPSec opera a nivel de aplicación</p> <p><input type="checkbox"/> IPSec opera a nivel de transporte</p> <p><input type="checkbox"/> IPSec opera a nivel de red</p> <p><input type="checkbox"/> IPSec opera a nivel de enlace</p>
<p>5. <b>MR.</b> Marca cuales de los siguientes usos de VPN es correcto</p> <p><input type="checkbox"/> Gw-to-Gw para acceso remoto a un solo servidor</p> <p><input type="checkbox"/> H-to-Gw para acceso de un usuario externo a los servicios internos de una empresa</p> <p><input type="checkbox"/> H-to-H para administrar de forma remota otro ordenador</p> <p><input type="checkbox"/> Gw-to-Gw para establecer una conexión segura entre sistemas diferentes</p>		<p>6. <b>MR.</b> Marca la o las afirmaciones correctas</p> <p><input type="checkbox"/> El modo tunnel de IPSec se usa generalmente para la VPN Gw-to-Gw</p> <p><input type="checkbox"/> IPSec AH proporciona cifrado de los paquetes</p> <p><input type="checkbox"/> IPSec ESP solo puede usar el modo transport</p> <p><input type="checkbox"/> IPSec SA sirve para que los dos extremos establezcan una asociación segura usando determinados parámetros de seguridad</p>
<p>7. <b>RU.</b> Que es OWASP</p> <p><input type="checkbox"/> Una herramienta para escanear posibles vulnerabilidades</p> <p><input type="checkbox"/> Una herramienta de desarrollo de exploits</p> <p><input type="checkbox"/> Un gestor de vulnerabilidades</p> <p><input type="checkbox"/> Una herramienta de análisis estático para comprobar la calidad de un código</p> <p><input type="checkbox"/> Una base de datos de exploits</p> <p><input type="checkbox"/> Una fundación creada para ayudar el desarrollo de software seguro</p>		<p>8. <b>RU.</b> Un ataque XSS consiste en</p> <p><input type="checkbox"/> Cuando se consigue inyectar un código malicioso en un servidor web</p> <p><input type="checkbox"/> Cuando se consigue introducir un código malicioso en un XML que será procesado posteriormente</p> <p><input type="checkbox"/> Cuando un usuario accede a una web sin darse cuenta que hay un código malicioso inyectado en la URL</p> <p><input type="checkbox"/> Cuando al deserializar un objeto, se consigue introducir un cambio que modifica el comportamiento de una aplicación</p>
<p>9. <b>MR.</b> Una auditoria de seguridad a nivel de aplicaciones</p> <p><input type="checkbox"/> Consiste en revisar la seguridad y la integridad de las aplicaciones</p> <p><input type="checkbox"/> Consiste en evaluar las posibles vulnerabilidades encontradas en las aplicaciones y los servidores</p> <p><input type="checkbox"/> Consiste en revisar la seguridad y la integridad de los servidores</p> <p><input type="checkbox"/> Consiste en revisar las operaciones diarias de los usuarios</p> <p><input type="checkbox"/> Consiste en monitorizar los paquetes que entran y salen de un host</p>		<p>10. <b>RU.</b> Information gathering es una etapa de la auditoria que consiste en</p> <p><input type="checkbox"/> Explotar una vulnerabilidad</p> <p><input type="checkbox"/> Analizar manualmente posibles vulnerabilidades</p> <p><input type="checkbox"/> Escanear aplicaciones y servidores para descubrir que hay de abierto</p> <p><input type="checkbox"/> Buscar datos sobre servicios o documentos determinados que no deberían ser públicos</p>

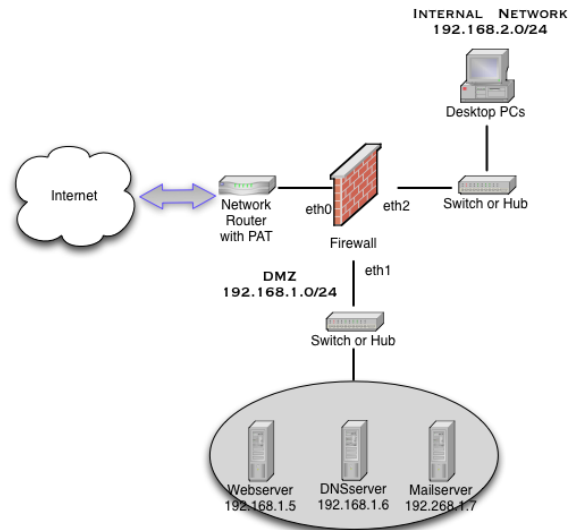
<b>Grupo 10</b>	<b>Ejemplo Segundo Control de Seguretat Informàtica</b>	<b>Q1: 4-11-2019</b>
Nombre:	Apellidos:	

**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.



- Define las políticas de seguridad por defecto
- Se tiene que poder configurar el firewall exclusivamente desde el PC 192.168.0.100
- Configurar, si necesario, reglas de NAT/PAT. Motivar la respuesta.
- El servidor web debe ser accesible desde la red interna y desde Internet

**(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.

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

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

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

# 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)