Seguridad del sistema

Este tema está divido en cinco partes con pesos diferentes.

1. Configuración de un router

Peso	3
Objetivos	Configurar un sistema para transferir paquetes IP, efectuar la traducción de dirección de red (NAT, *IP masquerading*) y entender su importancia en la protección de una red. Configurar la redirección de puertos, la administración de las reglas de filtrado y la prevención de ataques.

a. Competencias principales

- Archivos y herramientas de configuración iptables y ip6tables.
- Archivos y herramientas de configuración para la gestión de las tablas de enrutamiento.
- Rangos de direcciones privadas IPv4, direcciones locales únicas (*Unique Local Addresses*) y direcciones de enlace local (*Link Local Addresses*) IPv6.
- Redirección de puertos y transmisión IP (*IP forwarding*).
- Listar y escribir reglas y filtros basados en el protocolo, la dirección o los puertos de origen o destino, para aceptar o bloquear paquetes IP.
- Guardar y cargar configuraciones de filtrado.

b. Elementos empleados

- `/proc/sys/net/ipv4/`
- `/proc/sys/net/ipv6/`

- `/etc/services`
- `iptables`
- `ip6tables`

2. Gestión de servidores FTP

Peso	2
Objetivos	Configurar un servidor FTP para descargar y enviar archivos de forma anónima. Este objetivo incluye las precauciones que se tienen que tomar en el caso en que el envío anónimo esté autorizado y también la configuración de accesos de los usuarios.

a. Competencias principales

- Archivos y herramientas de configuración de Pure-FTPd y vsftpd.
- Conocimientos básicos de ProFTPd.
- Comprender las diferencias entre las conexiones FTP pasivas y activas.

b. Elementos empleados

- `vsftpd.conf`
- Opciones principales en línea de comandos de Pure-FTPd.

c. Shell seguro (SSH)

Peso	4
Objetivos	Configurar y proteger un servidor SSH. Administrar las claves y la configuración para los usuarios. Encapsular un protocolo de software en SSH y administrar las conexiones.

d. Competencias principales

- Archivos y herramientas de configuración de OpenSSH.
- Restricciones de conexión para el superusuario y los usuarios normales.
- Gestión de las claves del servidor y del cliente para las conexiones sin contraseña.
- Uso de múltiples conexiones a partir de muchas máquinas para evitar las pérdidas de conexión remota cuando se cambia la configuración.

e. Elementos empleados

- `ssh`
- `sshd`
- `/etc/ssh/sshd_config`
- `/etc/ssh/`
- Archivos de claves privadas y públicas.
- `PermitRootLogin`, `PubKeyAuthentication`, `AllowUsers`, `PasswordAuthentication` y `Protocol`.

3. Tareas de seguridad

Peso	3
Objetivos	Administrar la recepción de alertas de seguridad de diferentes fuentes, instalar, configurar y ejecutar sistemas de detección de intrusión y aplicar correctivos de fallos conocidos o problemas de seguridad.

a. Competencias principales

- Herramientas que permitan barrer la red (*scan*) y comprobar los puertos en un servidor.
- Sitios y organizaciones que informan de las alertas de seguridad: Bugtraq, CERT u otros.
- Herramientas para implementar un sistema de detección de intrusión (IDS).
- Conocimientos básicos de OpenVAS y Snort.

b. Elementos empleados

- `telnet`
- `nmap`
- `fail2ban`
- `nc`
- `iptables`

4. OpenVPN

Peso	2
Objetivos	Configurar una VPN (red privada virtual) e implementar conexiones punto a punto o de sitio a sitio protegidas.

a. Competencias principales

- OpenVPN

b. Elementos empleados

- `/etc/openvpn/`
- `openvpn`