Examen para BRS09.

Intento 1.

Pregunta 1

¿Qué dos modos de funcionamiento tiene el sistema FTP?

a. Prueba/Error
b. Activo/Pasivo
c. TCP/UDP.

Pregunta 2

¿Fue NAT concebido como un mecanismo de seguridad? ¿Verdadero o falso?
Seleccione una:

a. Verdadero
b. Falso

Pregunta 3

¿Es el protocolo SSH vulnerable ataques de fuerza bruta? ¿Verdadero o falso?
Seleccione una:

a. Verdadero
b. Falso

Pregunta 4

Indica la técnica que evita la explotación de vulnerabilidades asociadas con la corrupción de memoria.

a. TryHarder
b. TTP
c. ASLR

Pregunta 5

Las tarjetas de red pueden utilizar el protocolo IPv6, si no lo vamos a utilizar, ¿es conveniente dejarlo habilitado? ¿Verdadero o falso?
Seleccione una:

a. Verdadero
b. Falso

Pregunta 6

¿Por qué otro servicio seguro se puede sustituir telnet?
Seleccione una:

a. FTP
b. SSH
c. SNMP

Pregunta 7

¿Qué medida de refuerzo implementarías para el acceso remoto de un administrador?

a. Acceso 2FA
b. Entrar con la cuenta de máximos privilegios
c. Contraseña mínima de 30 caracteres

Pregunta 8

¿Es el servicio de telnet considerado como inseguro? ¿Verdadero o falso?
Seleccione una:

a. Verdadero
b. Falso

Pregunta 9

¿Cuál es el protocolo utilizado por TFTP?

a. TCP
b. UDP
c. ICMP

Pregunta 10

¿Qué servicio es el más seguro?

a. TFTP
b. FTP
c. SSH

Intento 2.

Pregunta 1

¿Cómo se denominan las medidas complementarias que se aplican al no poder aplicar algunas medidas de bastionado?

a. Medidas compensatorias
b. Medidas no seguras
c. Medidas no confiables

Pregunta 2

Indica cuál de la siguiente herramienta es proactiva.

a. Firewall local de Windows
b. IDS
c. IPS

Pregunta 3

Para qué puede ser utilizado el cliente de telnet como herramienta de testeo

a. Fingerprint
b. DoS
c. Bruteforce

Pregunta 4

Cuál de los siguientes no es un método de protección contra la autenticación

Seleccione una:

a. Certificados digitales
b. MFA
c. Usuarios genéricos de administración

Pregunta 5

Para qué reforzamos la seguridad de nuestro sistema con un CAPTCHA

a. Evitar la fuga de información
b. Evitar los ataques de fuerza bruta y recopilación de información de usuarios
c. No permitir la subida de ficheros

Pregunta 6

Identifica el mecanismo de Windows que impide la ejecución de código fuera de la direcciones reservadas.

a. IOCs
b. Nomemory
c. DEP

Pregunta 7

¿Qué herramienta nos permite conocer el estado de vulnerabilidades del sistema?

a. Tripwire
b. nodejs
c. Nessus

Pregunta 8

En una red con direccionamiento estático, ¿qué protocolo deberíamos eliminar?

a. ARP
b. SMB
c. DHCP

Pregunta 9

¿Con un antivirus estamos a salvo de cualquier ataque? ¿Verdadero o falso?
Seleccione una:

a. Verdadero
b. Falso

Pregunta 10

¿Qué medida adicional de refuerzo aplicaríamos para los accesos remotos de administradores?

a. Utilizar la herramienta WinSCP
b. Limitar la sesión a 1 minuto
c. 2FA

Intento 3.

Pregunta 1

¿Qué herramienta de sysinternal nos permite monitorizar los procesos?

a. Whois
b. NTFSInfo
c. Procmon

Pregunta 2

Las cuentas de servicios no deberían poder realizar la autenticación de sesiones interactivas. ¿Verdadero o falso?
Seleccione una:

a. Verdadero
b. Falso

Pregunta 3

El término que denomina los sistemas obsoletos y sin posibilidad de actualización pero que es necesario mantener en el sistema se denominan

a. Antiguos
b. Legacy
c. Old systems

Pregunta 4

Los sistemas MDM me ayudarán a controlar la seguridad de:

a. Dispositivos móviles
b. Firewall
c. Proxy.

Pregunta 5

¿Cuántos canales establece el protocolo FTP?

a. 2
b. 1
c. 4

Pregunta 6

¿Existe una versión segura del protocolo FTP? ¿Verdadero o falso?
Seleccione una:

a. Verdadero
b. Falso

Pregunta 7

¿Qué herramienta del entorno Linux se utiliza para el control de la ejecución de software?

a. OSSEC
b. AppLocker
c. AppArmour

Pregunta 8

Qué dispositivo nos ayudará a recoger información de la red para enviarlo a un IDS

a. Tap
b. IPS
c. Router

Pregunta 9

¿Cómo se denomina la estrategia de reducir los servicios de un sistema a los mínimos necesarios?

a. Privilegios mínimos
b. Medida compensatoria
c. Reducción de la superficie de exposición

Pregunta 10

¿Qué herramienta de la siguiente es un HIDS?:

a. nmap
b. Putty
c. Wazuh