Examen para BRS06.

Intento 1.

Pregunta 1

La política menos restrictiva en lo que respecta al acceso desde un dispositivo es

a. COPE
b. BYOD
c. COBE

Pregunta 2

¿Cuáles son los puertos conocidos asociados a un servicio?

a. 0-10
b. 50000-60000
c. 0-1024

Pregunta 3

¿El framework de seguridad ENS tiene alguna medida de protección que haga referencia a protección perimetral? ¿Verdadero o falso?
Seleccione una:

Verdadero
Falso

Pregunta 4

Los firewall para servicios Web (WAF) ¿Qué capa OSI analizan para poder para proteger la red de los ataque Web?

a. Capa 1 física
b. Capa 7 aplicación
c. Capa 2 enlace

Pregunta 5

Los firewall de primera generación no analizan la capa de

a. Transporte
b. Red
c. Aplicación

Pregunta 6

La creación de VLANs desde el punto de vista de la seguridad permite:

a. Controlar los flujos de información
b. No tener que instalar firewalls en el sistema
c. No necesitar administrar algunas partes de la red porque son más seguras.

Pregunta 7

¿Los switches no necesitan configuración segura poque sólo trabajan en capa 2? ¿Verdadero o falso?
Seleccione una:

Verdadero
Falso

Pregunta 8

¿Qué protocolo debe ser analizado con especial cuidado en las conexiones de los firewall porque es utilizado para la exfiltración de información?

a. SNMP
b. DNS
c. Kerberos

Pregunta 9

Uno de los ataques contra la segmentación en VLANs es

a. CDP spoofing
b. VLAN hacking
c. VLAN hoping

Pregunta 10

Los NGFW aglutinan capacidades de otros dispositivos de protección como por ejemplo

a. IPS
b. WAF
c. IDS
d. Todas son correctas

Intento 2.

Pregunta 1

Los administradores del servicio web de la compañía, ¿debería tener la mismas medidas de protección de acceso que un usuario del servicio? ¿Verdadero o falso?
Seleccione una:

Verdadero
Falso

Pregunta 2

El CASB sirve para proteger los servicios alojados en las instalaciones de la compañía. ¿Verdadero o falso?
Seleccione una:

Verdadero
Falso

Pregunta 3

Los firewall son dispositivos que permiten aumentar la velocidad en la red. ¿Verdadero o falso?
Seleccione una:

Verdadero
Falso

Pregunta 4

El valor de un octeto en IPv4 varía entre

a. 100-200
b. 1-10
c. 0-255

Pregunta 5

Si dispongo de 2 firewall para construir mi DMZ dentro del sistema. Indica la afirmación cierta desde el punto de vista de la seguridad.

a. Deben ser los más barato posibles
b. Deben ser de distinto fabricante
c. Deben ser los más rápidos del mercado

Pregunta 6

Las reglas que se definan en un firewall se hacen en base a:

a. Los datos de las IP de origen de los paquetes
b. Los datos de las IP de origen, IP de destino, protocolo y puerto de destino de los paquetes
c. Los datos de las IP de origen o IP de destino de los paquetes

Pregunta 7

Un ataque contra el protocolo ARP puede ser:

a. ARP snooping
b. NO ARP
c. IP spoofing

Pregunta 8

El control de acceso a la infraestructura de un servicio en cloud (SaaS) es responsabilidad de:

a. El Cliente del servicio
b. El Gobierno del país que alberga la infraestructura
c. Proveedor del servicio

Pregunta 9

¿Cuál es una de las limitaciones de los firewall de segunda generación?

a. No analizan la información de los protocolos cifrados
b. Se apagan cada 24 horas
c. Sólo funcionan para redes domésticas

Pregunta 10

¿Qué medida de seguridad podemos implementar contra el ataque de fuerza bruta en los servicios web?

a. CAPTCHA
b. Política de contraseña de 5 caracteres con obligación de una mayúscula
c. No permitir el registro de nombres de usuarios comunes

Intento 3.

Pregunta 1

La interconexión de nuestros servicios web con los servicios de nuestros proveedores debe ser

a. Cifrado
b. Basado en usuario y contraseña admin/admin
c. Por protocolo HTTP

Pregunta 2

Es una buena medida de seguridad segmentar el tráfico de operación de administración a través de VLAN. ¿Verdadero o falso?
Seleccione una:

Verdadero
Falso

Pregunta 3

¿Cuál es una metodología de desarrollo seguro?

a. Kali
b. OSSTM
c. OWASP

Pregunta 4

Los metadatos de los documentos publicados en la web no son importantes para la seguridad. ¿Verdadero o falso?
Seleccione una:

Verdadero
Falso

Pregunta 5

¿Existen proveedores de servicios de firewall en la nube? ¿Verdadero o falso?
Seleccione una:

Verdadero
Falso

Pregunta 6

Un WAF es un:

a. Firewall
b. Antivirus
c. Router

Pregunta 7

La regla final de un firewall debe ser:

a. Deny-any
b. Any-any
c. Forget-all

Pregunta 8

La defensa en profundidad se basa en:

a. Colocar los servidores en la planta más baja del edificio
b. Establecer niveles o capas en la arquitectura, donde pasar de una capa a otra esté controlado por mecanismos de protección como firewalls.
c. Ocultar todas las contraseñas en ficheros con nombres comunes del sistema operativo para que no sean rastreables.

Pregunta 9

¿Porque es útil conocer los métodos de evasión de las medidas de protección de un firewall?

a. Para ser nombrado hacker del mes
b. Para colocar el firewall en una capa más interna.
c. Para saber si soy vulnerable a ellas con las configuraciones de seguridad aplicadas.

Pregunta 10

Una medida de bastionado de un switch es:

a. Activar todos los protocolos de capa 2
b. Apagar los puertos no utilizados o asignarlos a una VLAN de "puertos sin uso".
c. Dejar todo el tráfico por la VLAN 1.