1. ¿Cuál de las siguientes capas de OSI es responsable de la conversión de protocolo, el cifrado/descifrado de datos y de la compresión de datos?.

Seleccione una:

1. No sabe/No contesta.
2. Red.
3. Presentación.
4. Enlace de datos.
5. Transporte.
6. ¿Cuáles de los siguientes son los tipos de claves que se utilizan en un esquema de cifrado asimétrico?.

Seleccione una:

1. Clave pública y clave privada.
2. No sabe/No contesta.
3. Clave pública y clave de usuario.
4. NTFS.
5. SSL.
6. ¿Cuál de los siguientes es un sistema informático diseñado para actuar como señuelo y engañar a los atacantes mientras se analizan las técnicas y herramientas que están usando para llevar a cabo el ataque?.

Seleccione una:

1. Honeypot.
2. Bation Host.
3. No sabe/No contesta.
4. Firewall.
5. Intrusion Detection System (IDS).
6. ¿En cuál de los siguientes ataques se envía un paquete ICMP de más de 65.536 bytes al sistema de destino?.

Seleccione una:

1. No sabe/No contesta.
2. Jolt.
3. Ping of Death.
4. Teardrop.
5. Fraggle.
6. En cuál de las siguientes capas del modelo OSI se definen los números de puerto?.

Seleccione una:

1. Transporte.
2. Física.
3. Red.
4. Presentación.
5. No sabe/No contesta.
6. Trabajas como administrador de seguridad de red. La empresa tiene una red basada en Windows. Estás a cargo de la seguridad de los datos de la empresa. Mientras realizas un análisis del registro de amenazas, observas que uno de los administradores de la base de datos está robando datos confidenciales. ¿Qué tipo de amenaza es esta?.

Seleccione una:

1. Malware.
2. No sabe/No contesta.
3. Zombie.
4. Externa.
5. Interna.
6. ¿Cuál de las siguientes es una dirección IP válida para redes de clase B?.

Seleccione una:

1. No sabe/No contesta.
2. 80.33.5.7
3. 212.136.45.8
4. 225.128.98.7
5. 172.157.88.3
6. Trabajas como administrador de red. La red está conectada a Internet. La red tiene un servidor web al que pueden acceder los usuarios de Internet. Por razones de seguridad, deseas mantener el servidor web separado de otros servidores de la red. ¿Dónde colocarás el servidor web?.

Seleccione una:

1. DMZ.
2. VPN.
3. No sabe/No contesta.
4. Con el servidor de bases de datos.
5. Con el servidor de autentificación.
6. ¿Cuál de los siguientes es un campo de 16 bits en un segmento TCP que identifica el número de puerto origen de la aplicación/programa que lo está enviando?.

Seleccione una:

1. Puerto origen.
2. Tamaño de ventana.
3. Número de sencuencia.
4. Longitud de encabezado.
5. No sabe/No contesta.
6. ¿Cuál de los siguientes es un sistema de detección de intrusos que monitoriza y analiza los componentes internos de un sistema informático en lugar de los paquetes de red en sus interfaces externas?.

Seleccione una:

1. NIDS.
2. HIDS.
3. No sabe/No contesta.
4. IPS.
5. DMZ.
6. ¿En cuál de los siguientes logs de eventos de un sistema Windows podemos encontrar los eventos relacionados con los inicios de sesión de usuarios?.

Seleccione una:

1. Security.
2. System.
3. Application.
4. No sabe/No contesta.
5. Network.
6. ¿Cuál de las siguientes herramientas es un analizador de protocolos de código abierto que puede capturar tráfico en tiempo real?.

Seleccione una:

1. NetResident.
2. Bridle.
3. Wireshark.
4. NetWitness.
5. No sabe/No contesta.
6. ¿Cuál de los siguientes protocolos de la pila TCP/IP es el responsable de devolver la dirección MAC asociada a la dirección IP en una red local?.

Seleccione una:

1. No sabe/No contesta.
2. RARP.
3. ARP.
4. DHCP.
5. PIM.
6. ¿Cuál de las siguientes es la mejor contramedida para el ramsonware de cifrado?.

Seleccione una:

1. Analizar el ramsonware para obtener la clave de descifrado de los datos cifrados.
2. Pagar un rescate.
3. Mantener un backup fuera de línea.
4. No sabe/No contesta.
5. Utilizar varios softwares antivirus.
6. Estás realizando una auditoría de seguridad interna y tienes la intención de averiguar qué puertos están abiertos en todos los servidores. ¿Cuál es la mejor forma de averiguarlo?.

Seleccione una:

1. Físicamente en cada servidor.
2. Hacer telnet a todos los puertos de cada servidor.
3. No sabe/No contesta.
4. Escanear los servidores con Nmap.
5. Escanear los servidores con MBSA.
6. Which of the following is a public IP address?.

Seleccione una:

1. 172.16.14.14
2. 8.8.8.8
3. 192.168.10.10
4. 10.11.12.13
5. No sabe/No contesta.
6. Which of the following is the standard path for log files in Linux?.

Seleccione una:

1. /usr/bin/
2. /var/log
3. No sabe/No contesta.
4. /etc/
5. /root/
6. You have been tasked to install system updates o a Debian based server. Which of the following Bah commands would you to accomplish the task?.

Seleccione una:

1. apt
2. updatedb
3. No sabe/No contesta
4. Install
5. Yum
6. Which of the following resource records should you configure in a DNS Server to be able to find a Mail Server?.

Seleccione una:

1. PTR
2. MX
3. NS
4. No sabe/No contesta
5. AAAA
6. Which of the following Linux Bash commands should you use to delete a file?.

Seleccione una:

1. No sabe/No contesta
2. dd
3. del
4. ls
5. rm
6. Which of the following is the RID (Relative Identifier) assigned to domain Administrator user un Windows systems?.

Seleccione una:

1. 1
2. Random
3. 0
4. No sabe/No contesta
5. 500
6. Which of the following layers of the OSI model provides sequence numbers?.

Seleccione una:

1. Network.
2. Transport.
3. Application.
4. Data Link.
5. No sabe/No contesta.
6. Which of the following is the unique ID that identifies a wireless network?.

Seleccione una:

1. BSSID
2. SSID
3. Channel
4. SID
5. No sabe/No contesta
6. A switch is considered a device operating in which layer of the OSI model?.

Seleccione una:

1. No sabe/No contesta.
2. Network.
3. Transport.
4. Data Link.
5. Physical.
6. Which of the following Poweshell cmdlets could you use to get help for others cmdlets?.

Seleccione una:

1. No sabe/No contesta
2. Get-Help
3. Get-Info
4. man
5. Get-Command
6. Which of the following is Microsoft’s public cloud computing platform?.

Seleccione una:

1. Horizon
2. Azure
3. No sabe/No contesta
4. GCP
5. AWS
6. Which of the following is a hashing algorithm?.

Seleccione una:

1. DES
2. WEP
3. SHA-1
4. AES
5. No sabe/No contesta
6. Which of the following Linux Bash command could you use to get running processes?:

Seleccione una:

1. ps
2. mv
3. Get-Process
4. tasklist
5. No sabe/No contesta
6. Which of the following is hardware or software appliance used to filter packets on a network?.

Seleccione una:

1. DNS
2. Firewall
3. Domain Controller
4. No sabe/No contesta
5. DHCP
6. Which of the folloging is NOT a Windows Server version?.

Seleccione una:

1. Windows Server 2016
2. Windows Server 2022
3. Windows Server 2013
4. Windows Server 2019
5. No sabe/No contesta



















