Protección y Seguridad de la Información (junio 2009)

Nombre.: Apellidos.:

1.- DVL

a) Distribución GNU/Linux que aglutina las principales herramientas en ataque orientada a la realización de auditorías de seguridad

b) Distribución GNU/Linux repleta de inseguridades orientada al aprendizaje

c) Distribución GNI/Linux que incluye los desarrollos LVS orientada a Alta Disponibilidad

d) Ninguna de las anteriores

2.- La herramienta Xprobe está orientada a

a) Backups en modo cliente-servidor

b) Detección de sniffers en un segmento de red

c) Cifrar sesiones de trabajo que no soporten SSL

d) Identificación remota de sistemas operativos basada en ICMP

3.- Un amigo está haciendo referencia al nmap y te habla de un idle scan

a) Hace referencia a la decodificación de firmas para identificar el sistema operativo de un sistema remoto de forma pasiva

b) Hace referencia a un escaneo de puertos

c) Hace referencia a un escaneo suplantando otras IPs

d) Hace referencia a un escaneo mediante retardos

4.- Si enviamos un paquete FIN a un sistema generalmente nos responderá

a) FIN ante un puerto cerrado y nada si está abierto

b) RST|ACK ante un puerto abierto y nada si está cerrado

c) RST|ACK ante un puerto cerrado y nada si está abierto

d) Ninguna de las anteriores

Nombre.: Apellidos.:

5.- El proceso de firma digital

a) Cifra la huella con la clave pública del emisor

b) Cifra la huella con la clave pública del receptor

c) Cifra la huella con la clave privada del emisor

d) Ninguna de las anteriores es correcta

6.- Si ejecutamos el comando # ac

a) Total de tiempo de cpu utilizado por los procesos de un usuario, en este caso del root

b) Información de fecha, hora, etc., de las sesiones abiertas por un usuario, en este caso del root

c) Relación de comandos ejecutados en el proceso de accounting, en este caso del root

d) Total de horas de conexión de un usuario, en este caso del root

7.- zabbix

a) Herramienta de monitorización distribuida

b) Herramienta para backups distribuidos

c) Herramienta de detección de interfaces en modo promisc

d) Ninguna de las anteriores

8.- ISO27002

a) Guía de buenas prácticas en seguridad

b) Estándar que se centra en la gestión de la seguridad de la información (análisis de riesgos, planes de contingencia, etc.)

c) Guía de fases para “securizar” redes WIFI

d) Estándar que define configuraciones seguras de plataformas de “backups”

Nombre.: Apellidos.:

9.- En una red de tomas de tierra, ¿qué es el TGB?

a) Barra principal

b) Barras secundarias

c) Backbone de la red de tomas de tierra

d) Ninguna de las anteriores

10.- ¿Qué hace un RAID01?

a) RAID1 sobre dos RAID0

b) RAID0 sobre dos RAID1

c) RAID0 sobre dos RAID lineales

d) No existen los RAID01. Únicamente existen los RAID10

11.- LTO4

a) 400MB nativos

b) 200GB nativos

c) 400GB nativos

d) 800GB nativos

12.- ¿Qué otro nombre se utiliza para designar un RAID-0?

a) striking

b) mirror

c) stripping

d) lineal

13.- ¿Qué entorno de trabajo es el característico del software Tivoli?

a) Sniffers

b) Gestión de almacenamiento y backups

c) DDoS

d) Filtrado por tcpwrappers

Nombre.: Apellidos.:

14.- ¿Qué método de sniffing hace spoofing sobre los conmutadores pensando en un entorno de medio switched?

a) MAC Flooding

b) ARP Spoofing

c) MAC Trusted

d) MAC Duplicating

15.- Puerto 514

a) ntp

b) X509 – Autoridades Certificadoras

c) syslog

d) Ninguno anteriores

16.- Atendiendo al nivel de importancia de los mensajes de log, ¿qué afirmación es correcta?

a) EMERG menor importancia que CRIT

b) ALERT menor importancia que CRIT

c) CRIT menor importancia que CRIT ☺

d) Ninguna de las anteriores

17.- Direcciones IPV6

a) 32

b) 64

c) 128

d) 256

18.- /etc/nsswitch.conf

a) Esquema de fuentes para hosts, dns, autenticación, etc.

b) Esquema de resolución del sistema y el dominio.

c) Configuración de correspondencia entre máquinas y direcciones Ethernet

d) Ninguna de las anteriores

Nombre.: Apellidos.:

19.- Port Security en CISCO

a) enable switchport port-security

b) port-security on

c) switchport port-security

d) port-security activate de una … vez

20.- AES

a) clásico

b) flujo

c) bloque

d) asimétrico

Respuestas del examen:

1. b
2. d
3. c
4. c
5. c
6. d
7. a
8. b
9. b
10. a
11. d
12. c
13. b
14. a
15. c
16. b
17. c
18. a
19. c
20. c