Modulo 2 – Quiz finale: Sicurezza di rete dei sistemi operativi

1 - Qual è l'obiettivo principale della sicurezza dei sistemi operativi?

A) Migliorare la velocità del sistema operativo
B) Proteggere il sistema operativo da accessi non autorizzati e vulnerabilità
C) Consentire un accesso amministrativo illimitato
D) Garantire che il sistema operativo abbia un aspetto visivamente accattivante

2 - Quale dei seguenti è un esempio di una comune minaccia alla sicurezza del sistema operativo?

A) Patch obsolete e aggiornamenti mancanti
B) Utilizzo di un tema in modalità scura
C) Compressione dei file
D) Installazione di font

3 - Perché le patch e gli aggiornamenti software sono fondamentali per la sicurezza del sistema operativo?

A) Rendono il sistema operativo più moderno
B) Aggiungono nuovi driver hardware
C) Risolvono le vulnerabilità di sicurezza prima che gli hacker possano sfruttarle
D) Sono opzionali e non riguardano la sicurezza

4 - Quale metodo viene comunemente utilizzato per gestire chi può accedere a un sistema?

A) Controllo degli accessi
B) Compressione dei file
C) Caching di rete
D) Backup dei dati

5 - Quale tecnica migliora la sicurezza disabilitando i servizi non necessari?

A) Whitelist delle applicazioni
B) Rafforzamento del sistema operativo
C) Crittografia
D) Antivirus

6 - Perché gli account predefiniti dovrebbero essere rimossi o limitati?

A) Spesso sono insicuri e vengono sfruttati dagli hacker
B) Rallentano le prestazioni del sistema
C) Non sono compatibili con i software moderni
D) Occupano troppo spazio su disco

7 - Che cos'è la whitelist delle applicazioni?

A) Consentire l'esecuzione solo delle applicazioni approvate
B) Bloccare tutte le applicazioni per impostazione predefinita
C) Crittografare le applicazioni durante l'esecuzione
D) Disinstallare le applicazioni inutilizzate

8 - Quale delle seguenti opzioni aiuta a rilevare attività insolite o dannose del sistema operativo?

A) Deframmentazione
B) Registrazione e monitoraggio
C) Pulizia del disco
D) Virtualizzazione

6 - Che cos'è la corruzione della memoria?

A) Un problema con la RAM lenta
B) Quando gli aggressori sfruttano i difetti nella gestione della memoria
C) Un errore di archiviazione sul disco rigido
D) Un aggiornamento del sistema operativo configurato in modo errato

10 - Cosa fa la Prevenzione dell'esecuzione dei dati (DEP)?

A) Impedisce che la memoria venga utilizzata per eseguire codice dannoso
B) Crittografa tutti i file di sistema
C) Elimina la memoria danneggiata
D) Crea nuove partizioni di memoria

11 - Qual è lo scopo della Randomizzazione del layout dello spazio di indirizzamento (ASLR)?

A) Per nascondere gli account utente agli hacker
B) Per disporre in modo casuale le posizioni di memoria, rendendo più difficile lo sfruttamento delle vulnerabilità
C) Per crittografare il traffico di rete
D) Per bloccare indirizzi IP sconosciuti

12 - Quale di queste NON è una minaccia comune alla sicurezza della rete?

A) Attacchi Man-in-the-Middle
B) Sniffing dei pacchetti
C) SQL injection
D) Deframmentazione dei dischi rigidi

13 - Qual è lo scopo dell'utilizzo di una VPN?

A) Per bloccare gli annunci pubblicitari sui siti web
B) Per creare un tunnel crittografato per il trasferimento sicuro dei dati
C) Per ridurre la velocità di Internet
D) Per eseguire la scansione alla ricerca di virus

14 - Qual è lo standard di sicurezza wireless attualmente considerato il più potente?

A) WEP
B) WPA
C) WPA2
D) WPA3

15 - Perché il Wi-Fi pubblico è considerato pericoloso?

A) Consuma più batteria
B) Spesso ha una crittografia debole o assente, esponendo i dati degli utenti
C) È più lento del Wi-Fi privato
D) Non consente download di grandi dimensioni

Laboratorio 2.1 – Configurazione delle politiche di sicurezza su una macchina virtuale

16 - Perché le macchine virtuali sono utili per esercitarsi nei laboratori di sicurezza?

A) Sono più veloci delle macchine fisiche
B) Isolano gli ambienti, riducendo i rischi per il sistema ospite
C) Correggono automaticamente le vulnerabilità
D) Non richiedono risorse hardware

17 - Quale strumento Windows applica le politiche relative alle password?

A) Editor criteri di gruppo
B) Task Manager
C) Gestione dispositivi
D) Esplora file

18 - In Linux, quale file aiuta a definire le politiche relative alle password?

A) /etc/login.defs
B) /etc/services
C) /etc/networks
D) /etc/hosts

16 - Qual è lo scopo della limitazione dei privilegi amministrativi?

A) Per impedire aggiornamenti software non necessari
B) Per ridurre la possibilità di attacchi di abuso o di escalation dei privilegi

C) Per migliorare la velocità degli accessi

D) Per consentire agli utenti il controllo completo del sistema

20 - Quale dei seguenti strumenti viene utilizzato per il monitoraggio del sistema in Linux?

A) Visualizzatore eventi

B) Syslog

C) Gestione disco

D) Editor del Registro

Laboratorio 2.2 – Analisi dei pacchetti con Wireshark

21 - Qual è lo scopo principale dell'analisi dei pacchetti?

A) Deframmentare i dischi rigidi

B) Esaminare e comprendere il traffico di rete

C) Disinstallare le applicazioni inutilizzate

D) Per velocizzare le prestazioni del sistema

22 - Quando si avvia Wireshark, cosa bisogna selezionare per primo?

A) Tipo di browser

B) Interfaccia di rete per acquisire il traffico

C) Strumento antivirus

D) Percorso Esplora file

23 - Quale filtro Wireshark useresti per visualizzare solo il traffico HTTP?

A) dns

B) http

C) icmp

D) tcp.port == 22

24 - Perché è importante individuare il traffico non crittografato?

A) Rivela la cronologia degli aggiornamenti del sistema
B) Aiuta a identificare i dati sensibili esposti agli attacchi
C) Migliora la velocità di Internet
D) Blocca le e-mail di spam

25 - Nella sfida di laboratorio, che tipo di query viene chiesto agli studenti di acquisire e analizzare?

A) Query FTP
B) Query DNS
C) Query SQL
D) Log VPN

Laboratorio 2.3 – Configurazione e test di una VPN

26 - Cosa nasconde principalmente una VPN a terzi?

A) Cronologia del browser
B) Indirizzo IP e contenuti del traffico di rete
C) Applicazioni installate
D) Specifiche hardware

27 - Quale test conferma che la tua VPN sta proteggendo il tuo traffico DNS?

A) Test di velocità
B) Test di perdita DNS
C) Scansione antivirus
D) Controllo dell'integrità dei file

28 - Cosa fail "kill switch" di una VPN?

A) Chiude la VPN dopo 1 ora
B) Impedisce l'accesso a Internet se la VPN si disconnette
C) Elimina la cronologia di navigazione dopo l'uso
D) Aumenta la velocità della VPN

26 - Perché è consigliabile confrontare le acquisizioni di rete con e senza VPN?

A) Per verificare se la VPN rallenta la navigazione
B) Per confermare che la crittografia sia applicata al traffico
C) Per testare le prestazioni del Wi-Fi
D) Per ridurre l'utilizzo della memoria

30 - Quale delle seguenti è un'impostazione opzionale comune nei client VPN?

A) Connessione automatica all'avvio
B) Compressione dei file
C) Modalità risparmio energetico
D) Colore dello sfondo

Risposte

1. **B** – Sicurezza del sistema operativo = protezione da accessi non autorizzati/vulnerabilità.
2. **A** – Le patch obsolete rappresentano un rischio elevato.
3. **C** – Gli aggiornamenti correggono le vulnerabilità prima che gli hacker possano sfruttarle.
4. **A** – Il controllo degli accessi gestisce gli accessi/le autorizzazioni.
5. **B** – L'hardening disabilita le funzionalità/i servizi non necessari.
6. **A** – Gli account predefiniti sono vulnerabili se non vengono limitati.
7. **A** – Whitelisting = vengono eseguite solo le app approvate.
8. **B** – I log rilevano attività anomale.
9. **B** – Corruzione della memoria = difetto nella gestione della memoria.
10. **A** – DEP blocca l'esecuzione da memorie non sicure.
11. **B** – ASLR randomizza la struttura della memoria.
12. **D** – La deframmentazione non è una minaccia per la rete.
13. **B** – Le VPN proteggono il traffico con la crittografia.
14. **D** – WPA3 è lo standard Wi-Fi più sicuro.
15. **B** – Il Wi-Fi pubblico spesso non dispone di crittografia.
16. **B** – Le VM isolano i laboratori e proteggono il sistema host.
17. **A** – Criteri relativi alle password: Editor criteri di gruppo.
18. **A** – /etc/login.defs gestisce le impostazioni delle password.
19. **B** – Il privilegio minimo riduce il rischio di abuso.
20. **B** – Syslog e auth.log sono strumenti di monitoraggio Linux.
21. **B** – Analisi dei pacchetti = studio del traffico di rete.
22. **B** – È necessario scegliere un'interfaccia di rete.
23. **B** – Il filtro "http" mostra i pacchetti HTTP.
24. **B** – Il traffico non crittografato espone dati sensibili.
25. **B** – Sfida = analizzare le query DNS.
26. **B** – La VPN nasconde l'IP e crittografa il traffico.
27. **B** – I test di perdita DNS confermano la privacy.
28. **B** – Il kill switch blocca il traffico in caso di interruzione della VPN.
29. **B** – Il confronto mostra l'effetto della crittografia.
30. **A** – La connessione automatica è un'impostazione VPN comune.