Test modulo CyberSecurity

Consegna: Entro la mezzanotte del 18/10/2024, inviare una mail a info@phoenixnetacad.com

Con oggetto: ELIS_Cybersecurity_TESTFINALE_{TUONOME}_{TUOCOGNOME}

In allegato inserire il file excel compilato con la tabella e le reative risposte.

1. Quale dei seguenti elementi NON fa parte della CIA Triad?

A) Confidenzialità
B) Integrità
C) Autenticazione
D) Disponibilità

2. Il concetto di "Integrità" nella CIA Triad si riferisce a:

A) Limitare l'accesso ai dati solo alle persone autorizzate
B) Garantire che i dati non vengano modificati in modo non autorizzato
C) Assicurare la disponibilità dei dati quando necessario
D) Autenticare l'identità degli utenti

3. Qual è la caratteristica principale del modello DAD Triad?

A) Disponibilità, Accesso e Divulgazione
B) Negazione, Accesso e Divulgazione
C) Divulgazione, Alterazione e Distruzione
D) Distruzione, Autenticazione e Disponibilità

4. Un attacco APT (Advanced Persistent Threat) è caratterizzato da:

A) Un attacco rapido e visibile
B) Un attacco non sofisticato
C) Accesso persistente e non rilevato nel tempo
D) Un attacco causato da uno script kiddie

5. Gli "Script Kiddies" sono considerati:

A) Attori altamente sofisticati
B) Attaccanti che utilizzano strumenti creati da altri senza una profonda comprensione
C) Gruppi organizzati di criminalità informatica
D) Utenti interni con accesso autorizzato ai sistemi

6. Quale dei seguenti è un attore malevolo comunemente associato allo spionaggio industriale?

A) APT
B) Criminal Syndicate
C) Competitors
D) Insiders

7. Il rootkit è un tipo di malware che:

A) Cripta i file per chiedere un riscatto
B) Offre accesso remoto nascosto e persistente a un sistema compromesso

C) Si diffonde autonomamente in rete
D) Monitora le attività degli utenti per rubare informazioni

8. Il ransomware è un tipo di malware che:

A) Ruba informazioni sensibili da un sistema
B) Cripta i file e richiede un pagamento per decriptarli
C) Si diffonde senza intervento umano
D) Raccoglie dati personali senza il consenso dell'utente

9. Il trojan è noto per:

A) Autoreplicarsi come i virus
B) Mascherarsi da software legittimo per eseguire codice malevolo
C) Bloccare l'accesso a un sistema tramite DDoS
D) Monitorare il traffico di rete senza rilevazione

10. Quale dei seguenti malware NON richiede un file per essere eseguito?

A) Spyware
B) Fileless malware
C) Trojan
D) Worm

11. Qual è la caratteristica principale del spyware?

A) Crittografare file per estorcere denaro
B) Raccogliere segretamente informazioni sugli utenti
C) Fornire accesso remoto non autorizzato a un sistema
D) Modificare il codice sorgente di un software legittimo

12. Quale vulnerabilità è tipicamente sfruttata da un insider malevolo?

A) SQL Injection
B) Accesso autorizzato ma utilizzato in modo non etico
C) Sniffing di pacchetti
D) Attacchi DDoS

13. Un attacco SQL Injection è utilizzato principalmente per:

A) Interrompere i servizi di rete
B) Manipolare query SQL e accedere ai dati
C) Ottenere il controllo di un host remoto
D) Intercettare le comunicazioni tra due utenti

14. Nel contesto di una CMD Injection, un attaccante può:

A) Eseguire comandi di sistema arbitrari su un server compromesso
B) Interrompere il funzionamento di un sistema tramite DoS
C) Modificare i dati in un database
D) Iniettare malware in un sito web

15. Quale delle seguenti vulnerabilità OWASP consente a un attaccante di caricare file malevoli su un server?

A) Cross-Site Scripting (XSS)
B) Broken Access Control
C) File Upload
D) SQL Injection

16. Qual è la differenza principale tra un attacco DoS e un DDoS?

A) Il DDoS utilizza più fonti per l'attacco
B) Il DoS è più efficace del DDoS
C) Il DDoS richiede l'intervento di un insider
D) Il DoS sfrutta vulnerabilità software, mentre il DDoS no

17. Quale delle seguenti è una caratteristica del virus?

A) Si diffonde autonomamente senza bisogno di un host
B) Necessita dell'interazione dell'utente per essere eseguito e si attacca a file eseguibili
C) Monitora il traffico di rete per rubare informazioni
D) Cifra i file dell'utente per richiedere un riscatto

18. Fileless malware sfrutta:

A) Un software legittimo in esecuzione su un sistema senza bisogno di file fisici
B) Codice malevolo che si diffonde attraverso email di phishing
C) La manipolazione di file PDF per iniettare codice malevolo
D) L'intercettazione di dati in transito

19. Nel contesto OWASP, cosa si intende per Cross-Site Scripting (XSS)?

A) Un attacco che altera i dati in un database
B) Un attacco che esegue script malevoli su un sito web per attaccare altri utenti
C) Un attacco denial-of-service
D) Un metodo per criptare le comunicazioni web

20. Quale dei seguenti attacchi può condurre a una reverse shell?

A) SQL Injection
B) Buffer Overflow
C) Phishing
D) File Upload

21. Phishing è una tecnica utilizzata per:

A) Catturare pacchetti di rete
B) Ottenere informazioni sensibili inducendo gli utenti a fornire i propri dati
C) Cifrare i file dell'utente per chiedere un riscatto
D) Bloccare un servizio tramite DoS

22. Un attacco di sniffing è utilizzato per:

A) Interrompere i servizi di rete tramite DDoS
B) Monitorare e catturare il traffico di rete per raccogliere informazioni sensibili
C) Iniettare malware in un sistema vulnerabile
D) Prendere il controllo di una sessione di rete

23. Un attacco Man-in-the-Middle (MITM) comporta:

A) Interrompere il traffico di rete per negare il servizio
B) Intercettare e modificare le comunicazioni tra due parti senza che esse lo sappiano
C) Distribuire malware tramite allegati email
D) Bloccare l'accesso a un sistema tramite un attacco DoS

24. Quale dei seguenti è un esempio di attacco di hijacking?

A) Manipolazione delle query SQL
B) Cattura di sessioni utente su una rete compromessa
C) Iniezione di malware in un sito web
D) Blocco del servizio attraverso un attacco DDoS

25. Qual è lo scopo di un exploit?

A) Bloccare un servizio tramite attacco DoS
B) Sfruttare una vulnerabilità software per eseguire codice malevolo
C) Rubare informazioni sensibili senza l'uso di malware
D) Monitorare l'attività di rete per raccogliere credenziali

26. Un worm è noto per:

A) Autoreplicarsi e diffondersi autonomamente su una rete
B) Iniettare malware tramite allegati email
C) Cifrare i file per chiedere un riscatto
D) Monitorare le attività dell'utente su un dispositivo infetto

27. Quale vulnerabilità è sfruttata da un attacco di SQL Injection?

A) L'invio di comandi arbitrari al server per modificare o accedere a un database
B) L'inserimento di script malevoli in un sito web
C) L'invio di pacchetti di rete alterati per monitorare la comunicazione
D) La manipolazione delle credenziali di autenticazione

28. Un attacco buffer overflow può:

A) Bloccare un servizio tramite DoS
B) Consentire l'esecuzione di codice arbitrario su un sistema compromesso
C) Rendere inaccessibili i file di sistema
D) Sfruttare una vulnerabilità per rubare dati di sessione

29. Quale attacco è mirato a compromettere la disponibilità di un sistema?

A) Phishing
B) Ransomware
C) Denial of Service (DoS)
D) Spyware

30. Gli attacchi fileless sono particolarmente difficili da rilevare perché:

A) Non lasciano tracce di file sul disco e si eseguono solo in memoria
B) Rimangono nascosti nelle email phishing
C) Richiedono l'installazione di un file eseguibile malevolo
D) Si diffondono rapidamente attraverso la rete