Prova V01 per selezione 03_2023DIVSAE

Avviso di Selezione pubblica per l'assunzione a tempo pieno e indeterminato di 2 posizioni per la Divisione Sicurezza, Ambiente & Emergenza in Lepida ScpA

* Indica una domanda obbligatoria

1. Email *

2. COGNOME *

3. NOME *

RISPONDI ALLE DOMANDE. VIENE RICHIESTA UNA SOLA RISPOSTA PER SINGOLA DOMANDA. LE OPZIONI PROPOSTESONO PRECEDUTE DA UN CODICE ALFANUMERICO DI 4 LETTERE E DA UN TRATTINO (-)

4. 1. Un attaccante introduce codice “malevolo” nel browser della vittima con l’obiettivo di dirottare le sessioni dell’utente e reindirizzarlo verso un sito pericoloso. Di che tipo di attacco si tratta? *

Contrassegna solo un ovale.

- KOON - Cross-Site Scripting (XSS)
- LTDQ - XML injection
- XSZP - SQL injection
- KBHT - LDAP injection

5. 2. Quale protocollo è responsabile della verifica dell’integrità delle connessioni? *

Contrassegna solo un ovale.

- MINK - ICMP
- GLUK - ARP
- HJXS - UDP
- TYDY - FTP

6. 3. Il protocollo SNMP consente la configurazione, la gestione ed il monitoraggio di dispositivi di rete collegati a una LAN. A quale livello del modello ISO/OSI opera? *

Contrassegna solo un ovale.

- OXWF - Livello di applicazione
- RIIY - Livello di trasporto
- KLVC - Livello di rete
- FEHO - Livello fisico

7. 4. Lo scopo dell'hashing è quello di garantire quale delle seguenti caratteristiche di un dato? *

Contrassegna solo un ovale.

- ZMNX - Integrità
- CTMR - Confidenzialità
- AZHP - Riservatezza
- DSZB - Nessuna di quelle citate

8. 5. Qual è il modo migliore per proteggersi da un attacco ransomware? *

Contrassegna solo un ovale.

- ISYX - Tutte le modalità citate
- BILL - Installando e aggiornando regolarmente il software antivirus
- QBAA - Mantenendo il sistema operativo sempre aggiornato
- PEOK - Facendo attenzione nell'aprire email o allegati sospetti

9. 6. Che cos'è una vulnerabilità "zero-day"? *

Contrassegna solo un ovale.

- LYCQ - Una falla nel software che non è stata ancora scoperta dallo sviluppatore
- KAFE - Un tipo di attacco ransomware che non è mai stato visto prima
- TBQK - Un metodo per infettare un computer facendo installare ed eseguire un programma all'utente
- ZSET - Un tipo di attacco di phishing con un target specifico di individui

10. 7. Quali sono i metodi comunemente utilizzati in un attacco DDoS? *

Contrassegna solo un ovale.

- QIJQ - Spoofing, amplification e botnets
- BXSO - Tutte le tecniche citate
- CXEW - Phishing, ransomware e social engineering
- RQDQ - SQL injection, cross-site scripting e clickjacking

11. 8. Qual è l'effetto di un attacco DDoS sui siti web e su una rete? *

Contrassegna solo un ovale.

- VCWF - Rallentare il sito web o la rete fino al punto di renderla inutilizzabile
- VGPN - Rubare informazioni personali dal sito web o dalla rete
- RPDW - Cancellare in modo permanente i dati sul sito web o sulla rete
- WKSE - Non ha alcun effetto sul sito web o su una rete

12. 9. Quale tra le seguenti non è una fase del processo di incident response? *

Contrassegna solo un ovale.

- VJDB - Scanning
- THUN - Containement
- CXBZ - Follow-up
- PNKK - Remediation

13. 10. Che cos'è un exploit? *

Contrassegna solo un ovale.

- XURQ - Un programma o una tecnica che sfrutta una vulnerabilità in un sistema o un'applicazione per portare avanti un attacco malevolo
- REIC - Un tipo di malware che ruba dati sensibili da un sistema o da una rete
- JAML - Uno strumento software per identificare le vulnerabilità di sicurezza in un sistema o in una rete
- YONU - Un tipo di firewall che monitora e filtra il traffico di una rete in entrata e in uscita

14. 11. Quale tra queste non può essere considerata una email di phishing? *

Contrassegna solo un ovale.

- AABF - Una email spedita ad un elevato numero di destinatari senza il loro permesso
- HIYF - Una email che contiene un virus o altro tipo di malware
- SBDG - Una email che incoraggia il destinatario a cliccare su un link o a scaricare un allegato che compromette la sua sicurezza
- AGFM - Una email che sembra arrivare da un mittente legittimo ma che in realtà è un falso, progettata per truffare il destinatario per estorcere informazioni sensibili

15. 12. Che cos'è il whaling? *

Contrassegna solo un ovale.

- DASS - Un tipo di attacco di phishing che ha come target individui di alto profilo, come dirigenti o celebrità
- NMHU - Un tipo di attacco di phishing che ha come target individui facilmente ingannabili
- JCVF - Un tipo di attacco di phishing che prevede l'uso di tecniche multiple, come social engineering e malware
- WOBB - Un tipo di attacco di phishing portato avanti da un gruppo di hacker

16. 13. Quale tipo di attacco ha come obiettivo quello di rubare informazioni sensibili intercettando le comunicazioni tra due parti? *

Contrassegna solo un ovale.

- HRUH - Man-in-the-middle
- GFQN - Phishing
- OZEG - Brute-force
- NPHA - DDoS

17. 14. Nell'hacking etico, come si chiama la fase di raccolta delle informazioni dall'utente target? *

Contrassegna solo un ovale.

- KHHG - Reconnaissance
- UQKQ - Scanning
- DMLZ - Autenticazione
- NWOF - Mantenimento dell'autenticazione

18. 15. Qual è il metodo di code injection usato per attaccare un data base di un sistema o di un sito web? *

Contrassegna solo un ovale.

- YFCR - SQL Injection
- GMWX - Malicious code injection
- GFYQ - HTML injection
- FWDS - XML Injection

19. 16. Qual è il processo di verifica dell'identità di un utente o di un dispositivo prima di concedere l'accesso a una rete o ad un sistema? *

Contrassegna solo un ovale.

- KFZK - Autenticazione
- HRBY - Autorizzazione
- LTIE - Cifratura
- FXHL - Decifratura

20. 17. Che cos'è il vulnerability scanning? *

Contrassegna solo un ovale.

- MCWC - Un tipo di scansione attiva di un sistema target per identificare potenziali falle di sicurezza
- UOTC - Un tipo di attacco di social engineering
- VVQZ - Un tipo di firewall che monitora e filtra il traffico di rete in entrata e in uscita
- GNUI - Un tipo di crittografia utilizzato per proteggere i dati sensibili

21. 18. Un Penetration Test eseguito senza avere alcuna informazione sulla struttura interna del sistema e/o del codice del software che si sta testando, come si definice? *

Contrassegna solo un ovale.

- PCJY - Black-box
- SKGX - Grey-box
- JJZI - White-box
- SGPS - Green-box

22. 19. Quale di queste affermazioni relative al malware è errata: *

Contrassegna solo un ovale.

- HGBV - Agisce con il consenso informato del proprietario
- QNYW - Può essere un keylogger
- WUIH - Può danneggiare un sistema informatico
- KIBN - E' progettato per infiltrarsi in un sistema informatico

23. 20. Quale tra questi non può essere definito un Indicatore di Compromissione (IoC)? *

Contrassegna solo un ovale.

- TFVB - Protocollo di rete
- ELKO - Hash di un malware
- PTAO - URL malevolo
- HIQV - IP malevolo