Iniziato	Friday, 11 June 2021, 09:30
Stato	Completato
Terminato	Friday, 11 June 2021, 10:03
Tempo impiegato	33 min. 36 secondi
Valutazione	**25,8** su un massimo di 32,0 (**80**%)

Domanda **1**

Completo

Punteggio ottenuto 1,0 su 1,0

Data chiave pubblica (e, n) e chiave privata (d, n) la cifratura consiste nel calcolare: c = m^e mod n

a. FALSO

b. VERO

Domanda **2**

Completo

Punteggio ottenuto 1,0 su 1,0

Nel modello Infrastrutturale della certificazione delle chiavi pubbliche l'autenticità della chiave pubblica è data da un soggetto terzo fidato che emette la certificazione

a. VERO

b. FALSO

Domanda **3**

Completo

Punteggio ottenuto 1,0 su 1,0

Gli attacchi passivi non modificano i dati in transito

- a. VERO
- b. FALSO

Domanda **4**

Completo

Punteggio ottenuto 1,0 su 1,0

Le ACL sono liste associate ad ogni soggetto del sistema

- a. VERO
- b. FALSO

Domanda **5**

Completo

Punteggio ottenuto -0,8 su 1,0

I bit di autorizzazione sono di 3 tipi R,W,X (read,write,execute)

- a. VERO
- b. FALSO

Domanda **6**

Completo

Punteggio ottenuto 1,0 su 1,0

DH e RSA hanno scopi differenti: quello di RSA é di essere molto più veloce nella fase di cifratura/decifrazione

- a. VERO
- b. FALSO

Domanda **7**

Completo

Punteggio ottenuto 1,0 su 1,0

Il salt è una password aggiuntiva di secondo livello

- a. VERO
- b. FALSO

Domanda **8**

Completo

Punteggio ottenuto 1,0 su 1,0

La fiducia nell'autenticità di una Root Certification Authority è perfettamente verificabile dal corrispondente certificato

- a. FALSO
- b. VERO

Domanda **9**

Completo

Punteggio ottenuto 1,0 su 1,0

Measured Boot si riferisce a un processo generale, che tipicamente usa un TPM come hardware root of trust

- a. VERO
- b. FALSO

Domanda **10**

Completo

Punteggio ottenuto 1,0 su 1,0

L'IP spoofing consiste nell'assumere un indirizzo IP diverso da quello regolarmente assegnato al proprio sistema

- (●) a. VERO
- ( ) b. FALSO

Domanda **11**

Completo

Punteggio ottenuto 1,0 su 1,0

Nei cifrari a sostiuzione polialfabetica conoscere il contenuto di una parte del messaggio non aiuta la decifrazione dell'intero testo

- ( ) a. VERO
- (●) b. FALSO

Domanda **12**

Completo

Punteggio ottenuto 1,0 su 1,0

Con una Local File Inclusion possiamo recuperare file interni al web server

- (●) a. VERO
- ( ) b. FALSO

Domanda **13**

Completo

Punteggio ottenuto 1,0 su 1,0

L'indice di Coincidenza è la probabilità che due lettere scelte a caso in un testo siano diverse

- a. FALSO
- b. VERO

Domanda **14**

Completo

Punteggio ottenuto -0,8 su 1,0

Il comando find / -type f -perm /6000 mi permette di trovare i file col SUID attivato.

- a. FALSO
- b. VERO

Domanda **15**

Completo

Punteggio ottenuto -0,8 su 1,0

I canarini sono un meccanismo di protezione del kernel linux per segnalare un overflow in memoria

- a. VERO
- b. FALSO

Domanda **16**

Completo

Punteggio ottenuto 1,0 su 1,0

La collocazione di sistemi in cloud ha unicamente effetti positivi sulla sicurezza

- a. VERO
- b. FALSO

Domanda **17**

Completo

Punteggio ottenuto 1,0 su 1,0

Nelle SQL Injection di tipo union select, il numero di colonne da usare per la query è un dato fondamentale per la riuscita dell'attacco

- a. VERO
- b. FALSO

Domanda **18**

Completo

Punteggio ottenuto 1,0 su 1,0

Un Intrusion Detection System può bloccare un attacco in corso

- a. VERO
- b. FALSO

Domanda **19**

Completo

Punteggio ottenuto 1,0 su 1,0

Il controllo dell'integrità dei file è uno dei metodi usati dagli HIDS

- a. VERO
- b. FALSO

Domanda **20**

Risposta non data

Punteggio max.: 1,0

FIDO alliance è un sistema di generazione degli OTP

- a. FALSO
- b. VERO

Domanda **21**

Completo

Punteggio ottenuto 1,0 su 1,0

I log sono utili solo a fini forensi (cioè per comprendere un attacco dopo che si è compiuto)

- a. FALSO
- b. VERO

Domanda **22**

Completo

Punteggio ottenuto 1,0 su 1,0

Nel test di Kasiski c'è la fattorizzazione e scelta delle distanze con un fattore comune

- (●) a. VERO
- ( ) b. FALSO

Domanda **23**

Completo

Punteggio ottenuto 1,0 su 1,0

Tra i fattori di autenticazione c'è qualcosa che si possiede fisicamente, come un Pin o una Password

- (●) a. FALSO
- ( ) b. VERO

Domanda **24**

Completo

Punteggio ottenuto 1,0 su 1,0

2FA e 2 step authentication sono esattamente la stessa cosa.

- ( ) a. VERO
- (●) b. FALSO

Domanda **25**

Completo

Punteggio ottenuto 1,0 su 1,0

Le chiavi di autenticazione usate da Secure Boot sono aggiornabili senza interruzioni di servizio

- a. FALSO
- b. VERO

Domanda **26**

Completo

Punteggio ottenuto 1,0 su 1,0

Le botnet sono reti di computer infetti chiamati zombie

- a. VERO
- b. FALSO

Domanda **27**

Completo

Punteggio ottenuto 1,0 su 1,0

L'ARP poisoning consiste nel convincere un host che l'IP di una vittima è associato al MAC dell'attaccante

- a. FALSO
- b. VERO

Vai a...

Parte II - esercizi ▶

Domanda **28**

Completo

Punteggio ottenuto 1,0 su 1,0

Le capability list sono delle liste associate a ogni soggetto del sistema

- a. VERO
- b. FALSO

Domanda **29**

Completo

Punteggio ottenuto 1,0 su 1,0

La cifratura dei dischi protegge da qualsiasi tentativo di esfiltrazione dei dati

- a. FALSO
- b. VERO

Domanda **30**

Completo

Punteggio ottenuto 1,0 su 1,0

La strcpy in linguaggio C non è una funzione pericolosa nel generare vulnerabilità di buffer overflow

- a. FALSO
- b. VERO

Domanda **31**

Completo

Punteggio ottenuto 1,0 su 1,0

Nei cifrari a trasposizione le statistiche dei digrammi e trigrammi permettono di dedurre la dimensione della tabella di cifratura

- a. FALSO
- b. VERO

Domanda **32**

Completo

Punteggio ottenuto 1,0 su 1,0

Un vantaggio degli Host-based IDS è che possono classificare più accuratamente il rischio associato a un pacchetto di rete

- a. FALSO
- b. VERO