Verifica le tue abilità – *Esercitazioni per l'esame ECDL*

Quando le risposte sono etichettate da cerchietti, significa che il quesito ha una sola risposta esatta; quando invece sono etichettate da quadratini, significa che più di una risposta è corretta.

ESERCITAZIONE 2

Tempo a disposizione: 45 minuti

1 Il termine backdoor indica: 2.1.2

Ⓐ un errore di programmazione che rende un sistema vulnerabile agli accessi esterni
Ⓑ un accesso segreto a un sistema o a un singolo computer
Ⓒ un virus che spia il computer sul quale si installa
Ⓓ una funzione di ogni sistema operativo per consentire l'accesso remoto al computer

2 L'acronimo VPN indica una rete: 3.1.1

Ⓐ privata che opera generalmente all'interno di un singolo edificio
Ⓑ pubblica estesa su un territorio molto ampio
Ⓒ privata diffusa su un territorio molto ampio che utilizza una infrastruttura pubblica di trasporto
Ⓓ pubblica che opera in un territorio, limitato generalmente a una città, accessibile solo a utenti registrati

3 Indica quali delle seguenti affermazioni sono corrette. 4.1.2

Ⓐ I siti di commercio elettronico sono in genere protetti.
Ⓑ Nei siti protetti le informazioni viaggiano in forma criptata.
Ⓒ I siti protetti usano il protocollo https.
Ⓓ Tutte le risposte precedenti sono corrette.

4 Il protocollo WEP per la sicurezza delle trasmissioni WiFi: 3.3.2

Ⓐ corrisponde a Wired Equivalent Privacy
Ⓑ di fatto assicura un livello di sicurezza paragonabile a quello delle reti cablate
Ⓒ è più sicuro del wpa
Ⓓ usa password di accesso di 24 caratteri alfanumerici

5 La firma digitale garantisce che: 5.1.2

Ⓐ il destinatario può verificare l'autenticità del mittente di un messaggio
Ⓑ il destinatario non può modificare un documento firmato da qualcun altro
Ⓒ il mittente non può disconoscere un documento che ha firmato o un messaggio che ha inviato
Ⓓ tutte le risposte precedenti sono corrette

6 La confidenzialità nell'ambito della messaggistica istantanea fa riferimento: 5.2.3

Ⓐ alla possibilità di scambiarsi in sicurezza allegati personali (proprie foto, filmati ecc.)
Ⓑ alla possibilità di scambiarsi informazioni personali amichevoli e riservate
Ⓒ alla possibilità di scambiarsi messaggi che non possono essere decifrati da altri interlocutori
Ⓓ al fatto che per poter comunicare bisogna essere iscritti allo stesso gruppo di amici

7 Le copie di riserva dei dati vanno: 6.1.3

Ⓐ fatte sempre una volta a giorno
Ⓑ pianificate a seconda della situazione in cui si opera
Ⓒ fatte quando si teme che ci possano essere dei problemi ai dispositivi
Ⓓ fatte sempre dallo stesso operatore

8 Per keylogger si intende: 2.2.2

Ⓐ un virus che fa apparire sullo schermo messaggi pubblicitari
Ⓑ un malware capace di registrare ciò che un utente digita sulla tastiera
Ⓒ un malware che devia il traffico telefonico dei computer collegati a Internet mediante modem, verso connessioni molto costose
Ⓓ un software capace di generare delle chiavi per criptare i file

9 Indica quali delle seguenti affermazioni, relative a un crimine informatico, sono vere o false. 1.212

a Lo si commette tutte le volte che si scarica un file video senza aver chiesto l'autorizzazione. V F
b Lo si commette quando si inviano messaggi pubblicitari non richiesti per posta elettronica. V F
c Lo si commette tutte le volte che si diffonde un virus, anche inconsapevolmente. V F
d Lo si commette quando si manomette l'hardware di un sistema informatico. V F

10 Indica quale fra le seguenti non è da considerare una minaccia ai dati causata da situazioni di forza maggiore. 1.1.4

Ⓐ Lo straripamento di un fiume.
Ⓑ Un incendio.
Ⓒ Una guerra.
Ⓓ Una cancellazione dovuta a inesperienza di chi utilizza il sistema.

11 Un hacker etico: 1.1.3

A lavora per rendere più sicuri i sistemi informatici
B viola le protezioni dei sistemi informatici per compiere azioni illegali
C è chiamato anche *white hat*
D si occupa della liceità dei contenuti della rete

12 Lo *shoulder surfing* è: 1.3.2

A una tecnica utilizzata per scoprire le credenziali di un utente osservandolo alle spalle
B una tecnica che può utilizzare delle telecamere per scoprire le credenziali di un utente
C una persona che naviga sfruttando la connessione WiFi di un altro
D un tipo di malware che scopre le credenziali dell'utente mentre le digita sulla tastiera

13 Per distruggere di dati: 6.2.3

Ⓐ in forma cartacea è sufficiente strapparli
Ⓑ su un CD o su un DVD è necessario danneggiarlo
Ⓒ su un hard disk è necessario distruggerlo
Ⓓ su una chiavetta USB è sufficiente formattarla

14 In merito ai dati personali è vero che: 1.2.5

A il credo religioso è un dato sensibile
B non possono essere detenuti per un tempo superiore a quello necessario agli scopi per i quali sono stati raccolti
C possono essere utilizzati da tutti i dipendenti dell'azienda che li detiene
D nell'informativa per l'utente, se non sono dati sensibili, non è necessario specificare la natura obbligatoria o facoltativa del conferimento dei dati richiesti

15 Indica quali delle seguenti affermazioni sono vere o false. 3.4.2

a Una userID può essere conosciuta da tutti. V F
b Una password deve essere conosciuta da un singolo utente. V F
c Una userID deve essere modificata periodicamente. V F
d Una password deve essere modificata periodicamente. V F
e Una password serve per l'identificazione. V F
f Una userID serve per l'autenticazione. V F

16 Se si riceve un messaggio di posta da uno sconosciuto che contiene un allegato: 5.1.6

A bisogna aprire l'allegato e poi controllarlo con un antivirus
B non bisogna leggere il messaggio
C non bisogna aprire l'allegato
D bisogna salvare l'allegato e scrivere al mittente per capire il motivo dell'invio dell'allegato

17 Quale delle seguenti affermazioni *non* è corretta in riferimento alla messaggistica istantanea? 5.2.2

A Espone all'attacco di worm che possono creare delle backdoor.
B Non è rischiosa perché ci si scambia solo messaggi di testo.
C Espone all'attacco di virus di diverso tipo.
D Espone al rischio soprattutto se ci si scambia allegati.

18 Per posta elettronica: 5.1.4

A se non si dispone di un antivirus si possono ricevere messaggi non richiesti
B se non si dispone di un firewall si possono ricevere messaggi non richiesti
C l'invio di messaggi non richiesti è una pratica illegale
D i messaggi non richiesti vengono in parte filtrati da alcuni provider e inseriti in apposite cartelle

19 In un social network: 4.2.2

A bisogna limitare al massimo la visibilità delle informazioni contenute nel proprio account
B la visibilità delle informazioni contenute nel proprio account non può essere limitata perché altrimenti non si viene trovati da chi effettua le ricerche
C non è necessario limitare la visibilità delle informazioni contenute nel proprio account perché lo fanno le piattaforme se sono usate nel modo predefinito
D se non si limita la visibilità delle informazioni contenute nel proprio account ci si espone ad attacchi di virus

20 I dati privati da un browser: 4.1.9

A per impostazione di default vengono eliminati alla chiusura del programma
B possono essere eliminati in qualunque momento
C possono essere eliminati ma non mentre si naviga perché contengono dati importanti per la navigazione
D possono essere eliminati a scelta dell'utente utilizzando le funzioni del programma

21 Indica quali delle seguenti affermazioni sono vere o false se riferite al *pharming*. 4.1.3

a Può consistere in un indirizzamento automatico verso un sito trappola causato da una modifica del DNS del provider. V F
b Può consistere in un indirizzamento automatico verso un sito trappola causato da una modifica del file *hosts* sul computer dell'utente. V F
c Consiste nell'indirizzamento a un sito trappola a causa di errori nella digitazione di un indirizzo V F
d Il rischio di incapparci può essere limitato dall'uso di antivirus. V F

22 Le transazioni economiche via Internet: 4.1.1

A dovrebbero avvenire solo attraverso siti sicuri
B possono avvenire attraverso qualunque tipo di sito perché le informazioni viaggiano criptate
C possono avvenire attraverso qualunque tipo di sito perché generalmente in queste operazioni si utilizzano password monouso
D sono molto insicure, se si fanno degli acquisti è meglio pagare in contrassegno

23 Le tecniche di sicurezza biometriche: 3.4.3

A sono più sicure di quelle tradizionali
B si utilizzano perché si perde meno tempo nell'identificazione
C non necessitano di particolari hardware
D si basano su caratteristiche che devono essere diverse nei diversi individui

24 Indica quali delle seguenti affermazioni sono vere o false. 6.2.2

a Cancellare dei dati con le funzionalità offerte dal sistema operativo equivale a distruggerli. V F
b I dati cancellati con le operazioni ordinarie restano memorizzati sul computer finché lo stesso non viene spento. V F
c I dati cancellati con le operazioni ordinarie restano memorizzati sul computer finché non vengono sovrascritti. V F
d Per cancellare in maniera definitiva i dati da un hard disk bisogna utilizzare dei software specifici. V F

25 Il backup dei dati: 6.1.2

A serve per fare in modo che più persone dispongano degli stessi dati
B serve per salvaguardare i dati importanti in caso di guasti
C permette di conservare cronologia e segnalibri del browser
D si può fare su hard disk esterni ma non su unità online

26 L'accesso a una rete: 3.4.1

A si può lasciare libero se l'accesso ai singoli computer è protetto da una password
B bisogna proteggerlo ma solo se si ha la necessità di disporre di tutta la banda
C bisogna proteggerlo per limitare le possibili intrusioni nella propria rete
D deve essere gestito da un amministratore di rete

27 L'accesso a una LAN aziendale di solito avviene: 3.2.1

A tramite cavo ethernet
B tramite bluetooth
C tramite WiFi
D mediante cavi USB

28 Un amministratore di rete: 3.2.1

A stabilisce le regole di accesso alla rete
B configura i router
C si occupa delle password di accesso
D tutte le risposte precedenti sono corrette

29 I software antivirus: 2.3.4

A anche se sono aggiornati non sono sicuri al 100%
B se non sono aggiornati perdono totalmente la loro efficacia
C vanno aggiornati solo se sono a pagamento
D vanno aggiornati annualmente, facendo riferimento alla data di installazione

30 L'ingegneria sociale si occupa: 1.3.1

A dei comportamenti degli utenti al fine di creare hardware con massimo di ergonomicità
B dei comportamenti degli utenti per creare software sempre più semplici da usare
C dei metodi per creare sistemi di connessione alle reti WiFi più sicuri
D dei metodi per ottenere le credenziali degli utenti in modo illegale

31 Il furto di identità lo compie chi: 1.3.3

A utilizza un falso nome per iscriversi a un social network
B sceglie come userID di posta elettronica un nome non suo
C non utilizza il suo nome nel dominio di un indirizzo Internet personale
D utilizza i dati di un'altra persona per ottenere dei vantaggi

32 Per *malware* si intende: 2.1.1

A un tipo di virus che si propaga principalmente con gli allegati di posta elettronica
B un tipo di virus che si propaga principalmente inserendosi nelle macro dei documenti creati con software d'ufficio
C tutto il software antivirus
D tutto il software creato con la funzione di arrecare danno al computer

33 Indica quali delle seguenti affermazioni sul contenuto presente su un computer da dismettere sono vere o false. 6.2.1

a È importante eliminare i dati perché altri potrebbero utilizzarli contro il nostro interesse. V F
b È importante eliminarlo perché altri potrebbero copiare i programmi installati a nostro nome. V F
c Se non abbiamo fatto cose illegali non c'è da preoccuparsi per i dati che rimangono V F
d Se un hard disk non è perfettamente ripulito diminuisce il valore dell'usato. V F

34 Quale delle seguenti affermazioni relative agli antivirus *non* è corretta 2.3.1

A Deve necessariamente avviarsi all'accensione del computer.
B È in grado di individuare un virus presente anche se non è attivo.
C Può individuare la presenza di un virus nella RAM.
D Potrebbe segnalare come virus programmi che non lo sono.

35 L'accesso a una rete wireless: 3.3.1

A per legge non può essere lasciato libero in nessun luogo
B se è lasciato libero facilita le intrusioni nella rete
C se è protetto richiede una userID e una password assegnati dall'amministratore
D se è protetto ogni utente deve avere una password personale per essere identificato

36 Il termine *adware* si riferisce a: 2.2.2

A un virus capace di compromettere le funzioni hardware del computer
B un software che mostra annunci pubblicitari
C un nome di un'applicazione antivirus
D un protocollo per le reti WiFi