CONCORSO PUBBLICO A 53 POSTI PER ISPETTORE INFORMATICO DEL CNVVF - SICUREZZA INFORMATICA

Id	Quesito	Risp_esatta	Risp_errata_1	Risp_errata_2	Materia
1	Cos'è la crittografia?	È quel procedimento che consiste nel codificare e decodificare un messaggio	È un oggetto fisico nel quale viene inserito un messaggio segreto	È il messaggero di un messaggio segreto	SICUREZZA INFORMATICA
2	Quali sono le caratteristiche principali dei sistemi di crittografia?	Segretezza, autenticità, integrità	Velocità e mobilità	Rintracciabilità, occultamento, facilità di decodifica	SICUREZZA INFORMATICA
3	A cosa serve una chiave in un algoritmo di codifica?	È una stringa alfanumerica che implementa l'algoritmo di codifica/decodifica dell'informazione protetta	È una parola riservata che utilizza il mittente del messaggio per codificarlo e non deve essere data a nessuno	È un codice che corrisponde all'identificazione del mittente	SICUREZZA INFORMATICA
4	In crittografia un cifrario a sostituzione:	è un metodo di cifratura in cui ogni lettera del testo in chiaro viene sostituita con un'altra lettera secondo uno schema regolare	è un metodo di cifratura che prevede l'utilizzo di soli numeri, da 0 a 9, per rappresentare un qualsiasi messaggio	è un metodo di cifratura in cui le lettere del messaggio sono cifrate indipendentemente l'uno dall'altro e nel quale la trasformazione dei simboli successivi varia con il procedere della cifratura	SICUREZZA INFORMATICA
5	Secondo la crittografia simmetrica:	viene utilizzata la stessa chiave per la codifica/decodifica del messaggio	sono utilizzate chiavi diverse per la codifica/decodifica del messaggio	non vengono utilizzate chiavi	SICUREZZA INFORMATICA
6	Cosa si intende per "Attacco a Forza Bruta" di un sistema di elaborazione?	Un metodo di attacco ad un sistema di elaborazione in cui si provano tutti i possibili metodi di accesso fino a che si trova quello effettivamente corretto	Un metodo di attacco ad un sistema di elaborazione in cui si provano tutti i metodi di accesso più probabili, scartando quelli meno probabili	Un metodo di attacco ad un sistema di elaborazione in cui si generano in modo casuale i metodi di accesso da utilizzare	SICUREZZA INFORMATICA
7	Cosa indica la sigla "Https" nell'indirizzo di una pagina web?	La pagina web adotta un protocollo che integra l'interazione del protocollo HTTP attraverso un meccanismo di crittografia di tipo Transport Layer Security (SSL/TLS)	La pagina lascia entrare solo gli utenti provvisti di un apposito certificato di sicurezza installato sul proprio computer	La pagina web è ospitata su server Linux	SICUREZZA INFORMATICA
8	La crittoanalisi è quella scienza che:	studia come decifrare un messaggio senza esserne “autorizzati”	studia algoritmi sicuri per codificare messaggi	studia i mezzi trasmissivi che vengono utilizzati per l'invio di messaggi segreti	SICUREZZA INFORMATICA
9	Cos’è una VPN?	L’acronimo di Virtual Private Network ed è un metodo di connessione di rete che crea una connessione crittografata e sicura	Un collegamento non crittografato tra due reti	Un DBMS condiviso sulla rete	SICUREZZA INFORMATICA
10	Cosa significa SSL?	Secure Sockets Layer	Secure System Layer	Standard Sockets Layer	SICUREZZA INFORMATICA
11	Cosa si intende per Malware?	Un software realizzato con intenti dannosi	Un dispositivo hardware utilizzato nei datacenter	Un software antivirus	SICUREZZA INFORMATICA
12	Il termine inglese “phishing”:	si riferisce ad e-mail ingannevoli e a siti fraudolenti progettati per indurre gli utenti a rivelare dati personali sensibili	si riferisce ad un tipo di virus	è un esempio di password veramente sicura	SICUREZZA INFORMATICA
13	In una rete a stella, un pacchetto di dati per passare da un nodo ad un altro:	deve passare necessariamente per il nodo centrale della rete	può utilizzare la connessione diretta tra i due nodi	deve necessariamente transitare tra tutti i nodi intermedi presenti tra il nodo di origine e quello di destinazione	SICUREZZA INFORMATICA

CONCORSO PUBBLICO A 53 POSTI PER ISPETTORE INFORMATICO DEL CNVVF - SICUREZZA INFORMATICA

14	Come funziona una rete ad anello?	I nodi della rete sono disposti a forma di cerchio creando appunto un anello	I nodi della rete prevedono un nodo centrale cui sono connessi tutti gli altri nodi	Ogni nodo della rete è connesso direttamente con tutti gli altri tramite collegamenti fisici	SICUREZZA INFORMATICA
15	Secondo la crittografia Asimmetrica:	sono utilizzate chiavi diverse per la codifica/decodifica del messaggio	viene utilizzata la stessa chiave per la codifica/decodifica del messaggio	nessuna delle altre risposte è corretta	SICUREZZA INFORMATICA
16	A cosa serve un Firewall?	È un componente hardware o software preposto alla difesa perimetrale di una rete	È un software preposto alla ricerca e rimozione di virus e malware su una rete	È un antivirus implementato su un dispositivo hardware	SICUREZZA INFORMATICA
17	Quale tra i seguenti è un esempio di “virus”?	Un programma che, introdotto subdolamente in un computer, causa dei danni anche seri ai dati o ai programmi in esso archiviati	Uno studente che violando le protezioni di accesso modifica i propri voti nell’archivio elettronico della scuola	Un programmatore che nasconde in un programma una parte di codice che gli consentirà, in futuro, di avere accesso al sistema	SICUREZZA INFORMATICA
18	Qual è il termine utilizzato per descrivere un mezzo, segretamente introdotto dal progettista, per consentire accesso ad un sistema?	Backdoor	Trapdoor	Spyware	SICUREZZA INFORMATICA
19	L’azione con cui un hacker cambia o falsifica informazioni su un archivio in rete è chiamata:	data diddling	sniffing	denial of service	SICUREZZA INFORMATICA
20	Tra i seguenti strumenti, quale ha come scopo principale quello di impedire accessi non autorizzati, via internet, ad un computer?	Firewall	Spyware blocker	Popup blocker	SICUREZZA INFORMATICA
21	Cosa di intende in Informatica per "Furto di Identità"?	Una condotta criminale perpetrata spacciandosi per un'altra persona su un sistema informatico	La perdita, da parte di un utente, delle proprie credenziali di accesso ad un sistema	La sottrazione di un dispositivo informatico (es. pc, smartphone) contenente dati personali sensibili	SICUREZZA INFORMATICA
22	A cosa serve il software "Jhon the ripper"?	È un software open source, che consente di hackerare/recuperare una password	È un software open source che determina gli indirizzi IP in una rete di computer	È un software in grado di identificare un mittente di un pacchetto di dati anche se offuscato	SICUREZZA INFORMATICA
23	Cosa si intende per tecnica di attacco SQL-Injection?	Una tecnica usata per attaccare applicazioni che gestiscono dati attraverso database relazionali sfruttando il linguaggio SQL	Una tecnica che utilizza tutte le possibili chiavi di accesso generate automaticamente per cercare di accedere ad un database SQL	Una tecnica usata per attaccare applicazioni che gestiscono dati attraverso database che non utilizzano il linguaggio SQL	SICUREZZA INFORMATICA
24	Cosa si intende per Ransomware?	È un tipo di malware che blocca l’accesso ai dati della vittima e minaccia di pubblicarli o cancellarli se non viene pagato un riscatto	È un software utilizzato per "sniffare" pacchetti dati su una rete	È una tipologia di virus che mira al rallentamento di un PC sovraccaricando la memoria	SICUREZZA INFORMATICA
25	Cosa si intende per metodo di attacco "Drive-by" ?	È un metodo di attacco in cui siti web insicuri vengono modificati da un malintenzionato che inserisce uno script dannoso nel codice di una delle pagine	È un metodo di attacco in cui un malintenzionato cerca di prendere il controllo del PC di un utente tramite una mail che incorpora un codice malevolo	Nessuna delle altre risposte è esatta	SICUREZZA INFORMATICA
26	Il DHCP permette di:	assegnare automaticamente un indirizzo IP, DNS e WINS	tradurre gli indirizzi IP di host esterni al dominio in nomi	tradurre gli indirizzi IP di host esterni al dominio in indirizzi IP	SICUREZZA INFORMATICA
27	I protocolli POP e SMTP sono utilizzati da:	programmi di posta elettronica	browser web	fogli di calcolo	SICUREZZA INFORMATICA
28	Il protocollo SMTP viene utilizzato per:	l'invio dei messaggi di posta elettronica	leggere i messaggi di posta elettronica dal server	la telefonia su internet	SICUREZZA INFORMATICA

CONCORSO PUBBLICO A 53 POSTI PER ISPETTORE INFORMATICO DEL CNVVF - SICUREZZA INFORMATICA

29	Con l'indirizzo IP 127.0.0.1 viene solitamente indicato:	il proprio computer, altrimenti detto Localhost	un qualsiasi computer sulla rete	una periferica di stampa sulla rete	SICUREZZA INFORMATICA
30	Cosa si intende per Clickjacking?	Un exploit in cui viene nascosto del codice dannoso nel codice dei pulsanti apparentemente innocui o di altri contenuti cliccabili presenti in un sito web	Un tipo di attacco in cui un noto sito viene clonato allo scopo di ingannare un visitatore	Una tecnica utilizzata per oscurare un sito	SICUREZZA INFORMATICA
31	Quando si hanno i primi riscontri storici della crittoanalisi?	Intorno al IX secolo d.C. ad opera degli arabi	Intorno al II secolo d.C. ad opera dei romani	Intorno al XVI secolo ad opera dei francesi	SICUREZZA INFORMATICA
32	Nella crittografia a cosa corrisponde il principio di "Autenticazione"?	Il destinatario deve poter essere sicuro dell'identità del mittente	Il messaggio non deve essere leggibile da terzi	Il mittente non deve poter negare di aver inviato il messaggio	SICUREZZA INFORMATICA
33	Nella crittografia a cosa corrisponde il principio di "Integrità"?	Il destinatario deve poter essere sicuro che il messaggio non sia stato modificato	Il destinatario deve poter essere sicuro dell'identità del mittente	Il messaggio non deve essere leggibile da terzi	SICUREZZA INFORMATICA
34	La firma digitale garantisce il "Non ripudio", ovvero:	il mittente (firmatario) non può disconoscere il documento	il mittente (firmatario) può disconoscere il documento	il destinatario può rifiutare il messaggio	SICUREZZA INFORMATICA
35	La macchina "Enigma" fu un dispositivo elettromeccanico per cifrare e decifrare messaggi, utilizzato dal servizio delle forze armate:	tedesche durante la seconda guerra mondiale	giapponesi durante la seconda guerra mondiale	americane durante la seconda guerra mondiale	SICUREZZA INFORMATICA
36	Secure Sockets Layer (SSL) è un protocollo crittografico che opera a livello di:	trasporto	fisico	data Link	SICUREZZA INFORMATICA
37	Che cosa è l'e-mail spoofing?	La falsificazione dell'indirizzo mittente, nell'intestazione di un' e-mail, per far apparire che provenga da un mittente diverso da quello effettivo	La sostituzione fraudolenta dell'indirizzo destinatario di un'e-mail per farla giungere ad un destinatario diverso da quello effettivo	L'invio di grandi quantità di messaggi indesiderati (generalmente commerciali)	SICUREZZA INFORMATICA
38	Kerberos è un protocollo di rete per l'autenticazione forte che usa:	tecniche di crittografia simmetrica	crittografia a chiave pubblica	tecniche di crittografia asimmetrica	SICUREZZA INFORMATICA
39	La firma digitale:	serve a dimostrare l'autenticità di un documento digitale inviato su un canale non sicuro	è una firma autografa, scansionata e salvata sul pc	è la chiave pubblica del destinatario di un documento digitale	SICUREZZA INFORMATICA
40	La crittografia a chiave privata è detta anche:	crittografia simmetrica	crittografia asimmetrica	public-encryption	SICUREZZA INFORMATICA
41	Cosa significa DDoS?	Distributed Denial of Service	Denial of Service	Distributed Reflected DoS	SICUREZZA INFORMATICA
42	Le procedura di sicurezza possono:	ridurre ma non eliminare il rischio	eliminare il rischio	avere costi proibitivi	SICUREZZA INFORMATICA
43	Un buona protezione contro i crimini informatici aiuta a:	proteggere la privacy	aumentare lo spazio disponibile sul computer	diminuire il numero di cookies che si scaricano durante la navigazione	SICUREZZA INFORMATICA
44	La maggior parte dei sistemi informatici si basa esclusivamente sull'autenticazione basata su:	password	crittografia	smart key	SICUREZZA INFORMATICA
45	Quale sistema informatico ha la funzionalità e lo scopo di identificare una persona sulla base di una o più caratteristiche fisiologiche?	Sistema di riconoscimento biometrico	Biomisurazione	Intelligenza Artificiale	SICUREZZA INFORMATICA
46	Un attacco che impedisce agli utenti di accedere ad un sito Web a causa di un bombardamento di traffico è detto:	denial of service (DoS)	cavallo di Troia	cracking	SICUREZZA INFORMATICA

CONCORSO PUBBLICO A 53 POSTI PER ISPETTORE INFORMATICO DEL CNVVF - SICUREZZA INFORMATICA

47	Com'è definito un software predisposto per aggiornare un programma e rimuovere vulnerabilità di sicurezza?	Patch di sicurezza	Security repairs	Refresh patches	SICUREZZA INFORMATICA
48	Qual è il nome di un programma applicativo che raccoglie le informazioni dell'utente e le invia a qualcuno tramite Internet?	Spybot	Libreoffice	Fax Mailer	SICUREZZA INFORMATICA
49	Il software dannoso è noto come:	Malware	Badware	Patch	SICUREZZA INFORMATICA
50	Quale tra le seguenti è la migliore buona pratica nella manutenzione di un sistema operativo?	Mantenere il sistema operativo costantemente aggiornato	Utilizzare una password di accesso robusta di almeno 16 caratteri	Utilizzare un Antivirus ed un Firewall	SICUREZZA INFORMATICA
51	Nella scelta di una password di accesso ad una risorsa è buona norma:	evitare l'uso di parole ovvie, di senso compiuto, associabili all'username, o anagrammi	registrare le proprie password sul PC in modo da velocizzare l'accesso	rendere una password immutabile nel tempo	SICUREZZA INFORMATICA
52	Com'è consigliabile scegliere i caratteri che compongono una password?	Utilizzare combinazioni di caratteri maiuscoli, minuscoli, numeri e caratteri speciali	Usare testi o parole semplici da ricordare	Usare combinazioni di caratteri minuscoli o maiuscoli e unicamente numeri	SICUREZZA INFORMATICA
53	Cosa si intende per IP Spoofing?	Una tecnica utilizzata dagli hacker per attaccare un sistema di elaborazione, che consiste nel mettere nel pacchetto IP un indirizzo sorgente fasullo	Una proprietà dei moderni antivirus che sono in grado di determinare la provenienza di un pacchetto di dati sulla rete e di bloccarlo se necessario	Una funzione del sistema operativo	SICUREZZA INFORMATICA
54	In crittografia il Data Encryption Standard (DES):	è un algoritmo a chiave simmetrica	è un algoritmo a chiave asimmetrica	è un algoritmo a chiave ibrida	SICUREZZA INFORMATICA
55	Cos'è il MAC ADDRESS?	Un indirizzo univoco di una risorsa sulla rete	Un indirizzo che individua un gruppo di periferiche su una rete	Un indirizzo univoco che viene assegnato sempre dal sistemista di rete in fase di configurazione iniziale	SICUREZZA INFORMATICA
56	La firma digitale si basa su un algoritmo a crittografia:	asimmetrica o a doppia chiave	simmetrica o a chiave singola	ibrida con la generazione di N chiavi, ognuna da usare ad ogni firma	SICUREZZA INFORMATICA
57	In quale tra le seguenti configurazioni di rete ogni nodo è collegato ad un elaboratore centrale?	A stella	Ad anello	A bus	SICUREZZA INFORMATICA
58	Quanti sono i gruppi di cifre, separati da un punto, che definiscono gli indirizzi IP V4?	4	6	8	SICUREZZA INFORMATICA
59	Se viene mostrato un lucchetto accanto all'indirizzo web presente nella barra degli indirizzi del browser significa che il sito che si sta visitando :	è sicuro	non è sicuro	non è aggiornato alle ultime disposizioni in termini di sicurezza	SICUREZZA INFORMATICA
60	La Firma digitale è uno strumento ormai molto diffuso per:	la semplificazione dei procedimenti amministrativi nella PA e nelle relazioni tra la PA e i cittadini e le imprese	la crittografia, l'invio e la ricezione di documenti riservati	il riconoscimento di un utente all'acceso ad un sistema di elaborazione	SICUREZZA INFORMATICA
61	Cosa è un CAPTCHA ?	Un test fatto per verificare che un utente che sta accedendo ad una risorsa è un umano piuttosto che un computer	Un tipo di pacchetto dati con specifiche funzionalità strutturali che ne impediscono la contraffazione	Un elemento di un server web che ha lo scopo di monitorare le attività degli utenti fino al logout	SICUREZZA INFORMATICA
62	La firma digitale soddisfa il requisito di "Autenticazione", ovvero:	è possibile verificare/certificare l'identità del mittente	è possibile risalire alla chiave privata del mittente	non è possibile verificare/certificare l'identità del mittente	SICUREZZA INFORMATICA

CONCORSO PUBBLICO A 53 POSTI PER ISPETTORE INFORMATICO DEL CNVVF - SICUREZZA INFORMATICA

63	La firma digitale soddisfa il requisito di Integrità ovvero:	si ha certezza che il documento non sia stato alterato dopo la firma	è possibile modificare il documento dopo la firma	non si ha certezza che il documento sia stato alterato dopo la firma	SICUREZZA INFORMATICA
64	Un software antivirus protegge la rete aziendale in modo più efficace quando:	è installato su tutti i PC della rete ed è tenuto costantemente aggiornato	su ogni PC della rete sono installati contemporaneamente due antivirus di due produttori diversi	sullo stesso PC viene installato anche un Firewall	SICUREZZA INFORMATICA
65	In una rete aziendale, quando è consigliabile procedere all'aggiornamento di un software?	Appena l'aggiornamento viene reso disponibile dal produttore	Entro 30 giorni dal rilascio dell'aggiornamento	Solo quando è disponibile anche un nuovo aggiornamento del sistema operativo	SICUREZZA INFORMATICA
66	In ambito aziendale come ci si dovrebbe comportare in caso di eccessive notifiche da parte di strumenti quali Antivirus e/o Firewall?	Segnalare immediatamente le notifiche ricevute al responsabile IT in modo che il sistema venga sottoposto a controllo	Ignorare le notifiche in quanto sono di pertinenza da parte del personale IT	Disattivare se possibile le notifiche quando diventano eccessive	SICUREZZA INFORMATICA
67	Quale tra le seguenti password è la più sicura?	X6M#!MX901	9U8PATSW	23355762	SICUREZZA INFORMATICA
68	Quale tra le seguenti password è la più sicura?	GLE!3BEXXN	PAOLO	PAOLO123	SICUREZZA INFORMATICA
69	Quale tra le seguenti password è la più sicura?	LX!U377HE%	135791113	AMMINISTRAZIONE	SICUREZZA INFORMATICA
70	Cos'è un protocollo desktop remoto?	Un servizio di accesso remoto ad un PC su rete intranet/internet tramite interfaccia grafica	Un servizio di accesso remoto ad un PC su rete intranet/internet tramite shell testuale	La condivisione dello schermo fatta da un PC in una rete LAN	SICUREZZA INFORMATICA
71	A cosa serve la tecnologia SSL?	È una tecnologia che crea connessioni crittografate tra un server web e un browser web, utilizzata per proteggere le informazioni nelle transazioni online e nei pagamenti digitali per mantenere la riservatezza dei dati	È una tecnologia che si utilizza per velocizzare una rete a scapito della sicurezza	È una tecnologia utilizzata solo a scopo militare per garantire una comunicazione telefonica sicura tra due interlocutori	SICUREZZA INFORMATICA
72	Che cos'è un exploit?	Un software o una sequenza di comandi che sfrutta un errore o una vulnerabilità di un sistema di elaborazione per prenderne il controllo	La messa in sicurezza di un sistema informatico per correggerne una vulnerabilità	Un tipo di hacker che ha come scopo l'individuazione di potenziali criticità di un sistema per permetterne la risoluzione	SICUREZZA INFORMATICA
73	Cosa di intende per "Penetration Test" ?	Un test che si effettua su un sistema informatico eseguito allo scopo di valutarne le difese contro attacchi informatici	Il tentativo di accedere ad un sistema informatico con lo scopo di renderlo inutilizzabile o sottrarre dati	Un'attività che ha lo scopo di rendere irraggiungibile una risorsa sulla rete	SICUREZZA INFORMATICA
74	A cosa serve il protocollo Diffie-Hellman?	A consentire lo scambio di una chiave tra due corrispondenti utilizzando un canale non sicuro	A generare un insieme di chiavi che possono essere utilizzate tra due corrispondenti che utilizzano un canale di comunicazione protetto	È un cifrario che utilizza un sistema di cifratura a sostituzione	SICUREZZA INFORMATICA
75	Cosa si intente per attacco DDos?	Un attacco informatico ad un sito web per metterlo offline tramite un bombardamento di richieste verso il server che ospita il sito	Un tipo di attacco che cerca di ottenere i privilegi di amministratore di un sistema utilizzando delle falle di sicurezza conosciute per quel sistema	Un tipo di attacco in cui il malintenzionato cerca di entrare in possesso di credenziali valide tramite azioni di ingegneria sociale	SICUREZZA INFORMATICA

CONCORSO PUBBLICO A 53 POSTI PER ISPETTORE INFORMATICO DEL CNVVF - SICUREZZA INFORMATICA

76	Cos'è un computer zombie?	Un computer che, all'insaputa del proprietario, è stato compromesso da un cracker o infettato da un virus in maniera tale da permettere a persone non autorizzate di assumerne, in parte o per intero, il controllo	Un computer connesso ad internet che utilizza un sistema operativo e/o un antivirus obsoleti e pertanto potrebbe essere facilmente vittima di cracker o virus	Un computer che si collega ad internet senza utilizzare software di protezione	SICUREZZA INFORMATICA
77	Uno scanner di vulnerabilità è:	un programma progettato per ricercare e mappare le debolezze di un'applicazione, di un computer o di una rete	un'applicazione che acquisisce pacchetti TCP/IP, che possono essere utilizzati in modo dannoso	una situazione in cui una persona o un programma si maschera con successo come un altro	SICUREZZA INFORMATICA
78	Cos'è uno sniffer?	Un'applicazione che acquisisce pacchetti TCP/IP, che possono essere utilizzati in modo dannoso per acquisire password e altri dati	Una situazione in cui una persona o programma si maschera con successo come un altro falsificando i dati	Un programma progettato per ricercare e mappare le debolezze di un computer o di una rete	SICUREZZA INFORMATICA
79	Gli "hacker etici" o "White Hat Hackers":	lavorano per aziende come specialisti della sicurezza e tentano di trovare falle di sicurezza attraverso l'hacking	sono responsabili della scrittura di malware e la loro motivazione principale è di solito per un guadagno personale o finanziario	mirano a rubare dati, in particolare informazioni finanziarie, informazioni personali e credenziali di login	SICUREZZA INFORMATICA
80	Come si definisce un programma atto a registrare (log) ogni pressione dei tasti su un computer?	Keylogger	Worm	Cracker	SICUREZZA INFORMATICA
81	Come si definiscono le applicazioni dannose che inducono un utente a eseguirli, fingendo di essere utili?	Cavalli di Troia o Trojan horses	Keylogger	Cracker	SICUREZZA INFORMATICA
82	Un Rootkit è:	una situazione in cui una persona o programma si maschera con successo come un altro, falsificando i dati e ottenendo un accesso illegittimo	un programma progettato per ricercare e mappare le debolezze di un'applicazione, di un computer o di una rete	un'applicazione che acquisisce pacchetti TCP/IP, che possono essere utilizzati in modo dannoso	SICUREZZA INFORMATICA
83	Nell'invio di una PEC, il messaggio viene considerato consegnato quando:	il gestore del servizio PEC lo rende disponibile nella casella di posta elettronica certificata del destinatario	il destinatario dà conferma di lettura	il destinatario legge il messaggio e il gestore del servizio PEC invia al mittente un messaggio di avvenuta consegna	SICUREZZA INFORMATICA
84	In Informatica, si definisce "Traceroute":	un software in grado di seguire il percorso dei pacchetti sulla rete	un software in grado di controllare tutti i pacchetti in ingresso verificando che non contengano Malware	un parametro della connessione di rete di un computer che opera su un rete LAN	SICUREZZA INFORMATICA
85	Cosa si intende in informatica per fuga di dati?	La divulgazione di informazioni sensibili, confidenziali o protette in modo intenzionale o non intenzionale a terzi non interessati	La sottrazione di dati da parte di soggetti terzi ottenuta con metodi fraudolenti	La perdita di dati sensibili dovuta al malfunzionamento di dispositivi di memorizzazione	SICUREZZA INFORMATICA
86	Cosa si intende in Informatica per "Software Canaglia"?	Un software che induce gli utenti a credere che ci sia un virus sul loro computer e mira a convincerli ad installare un falso strumento di rimozione che installa effettivamente un virus/malware sul proprio computer	Un software che, sebbene rilasciato come Freeware, al momento dell'utilizzo chiede all'utente di pagare una royalties	Un software che blocca il pc dell'utente chiedendo un riscatto in termini economici per sbloccarlo	SICUREZZA INFORMATICA

87	Come funziona un attacco "Buffer OverFlow"?	L'obiettivo di un attacco Buffer Overflow è di sovvertire la funzione di un programma privilegiato, in modo che un attaccante possa prendere il controllo di questo programma e se il programma ha i privilegi sufficienti, controllare l'intero host	L'obiettivo di un attacco Buffer Overflow è di inviare ad un sistema un gran numero di richieste in modo da saturarne la capacità di risposta e di fatto bloccarlo	L'obiettivo di un attacco Buffer Overflow è di provare ad acquisire i privilegi di accesso di un sistema remoto provando tutte le possibili combinazioni di password possibili	SICUREZZA INFORMATICA
88	L'algoritmo RSA è di tipo a chiave:	asimmetrica	simmetrica	segreta	SICUREZZA INFORMATICA
89	L'algoritmo Diffie-Hellman è di tipo a chiave:	asimmetrica	segreta	simmetrica	SICUREZZA INFORMATICA
90	A cosa serve lo strumento NMAP?	È un software libero, creato per effettuare port scanning, cioè mirato all'individuazione di porte aperte su un computer bersaglio o anche su range di indirizzi IP	È un software antivirus/malware	È un software commerciale a pagamento, creato per effettuare port scanning, cioè mirato all'individuazione di porte aperte su un computer bersaglio o anche su range di indirizzi IP	SICUREZZA INFORMATICA
91	In cosa consiste un "Attacco con dizionario"?	Il malintenzionato utilizza un dizionario di password comuni che viene utilizzato per tentare di ottenere l'accesso al computer e alla rete di un utente	Il malintenzionato prova ad attaccare un sistema utilizzando tutte le possibili combinazioni di password e quelle più promettenti vengono memorizzate su un database per successivi riutilizzi	È equivalente all'attacco a Forza Bruta	SICUREZZA INFORMATICA
92	Cosa si intende per "Informatica Forense"?	Quella parte dell'informatica che si occupa dell'analisi dei dati e dei dispositivi digitali che possono essere coinvolti in crimini informatici	Quella parte dell'informatica che si occupa della sicurezza delle reti	Quella parte dell'informatica che si occupa della lotta alla pirateria informatica	SICUREZZA INFORMATICA
93	Quale tra le seguenti distribuzioni Linux è specificatamente orientata alle indagini forensi?	Caine	Fedora	Ubuntu Studio	SICUREZZA INFORMATICA
94	Il MAC ADDRESS è un codice formato da ____ bit.	48	56	128	SICUREZZA INFORMATICA
95	A cosa serve il software "Eraser"?	A cancellare un file o una directory in modo sicuro, ovvero che non siano più recuperabili	A recuperare un file in precedenza cancellato	È un comando del sistema operativo Windows che consente di proteggere il Cestino con un nome utente ed una password	SICUREZZA INFORMATICA
96	A cosa serve il software "Veracrypt"?	A creare delle partizioni o dei volumi criptati e protetti	A togliere la protezione da una partizione o da un volume in precedenza criptati	Ad eseguire un "penetration test" su un volume criptato per verificarne la tenuta	SICUREZZA INFORMATICA
97	Cosa si intende per "SEO poisoning attack" ?	I malintenzionati creano siti web dannosi e utilizzano tattiche di ottimizzazione dei motori di ricerca per renderli prominenti nei risultati della ricerca, in modo che un utente non possa sospettare che si tratta di un sito malevolo	È una tecnica che danneggia il posizionamento di un sito nei risultati di ricerca	I malintenzionati cercano di prendere il controllo di un sito, sfruttando la vulnerabilità delle istruzioni utilizzate dal sito per il posizionamento SEO	SICUREZZA INFORMATICA
98	Secondo le linee guida dell'Agid, la memorizzazione delle password degli utenti di un sistema informatico:	devono essere memorizzate utilizzando tecniche di hashing sicuro con algoritmi forti come PBKDF2, bcrypt o SHA-512	devono essere memorizzate utilizzando l'algoritmo SHA1 o MD5	possono essere non criptate se c'è certezza dell'identità dell'utente	SICUREZZA INFORMATICA

CONCORSO PUBBLICO A 53 POSTI PER ISPETTORE INFORMATICO DEL CNVVF - SICUREZZA INFORMATICA

99	Un attacco "Port Scanning":	prevede la scansione di tutte le possibili porte TCP/UDP aperte su un host, al fine di studiarne la configurazione e individuarne le debolezze o i punti di attacco	prevede la scansione di tutti gli indirizzi IP di un host, fino a trovarne uno che sia attaccabile	può essere effettuato esclusivamente in ambiente Linux	SICUREZZA INFORMATICA
100	La sicurezza fisica di un sistema informativo riguarda prevalentemente:	la sicurezza dell'edificio che ospita il sistema informativo, come la videosorveglianza o il sistema antincendio	il DBMS utilizzato e le sue copie di backup	l'aggiornamento del sistema operativo che ospita il sistema informativo	SICUREZZA INFORMATICA
101	Cosa è il "Keylogging" ?	L'intercettazione (mediante software malware o dispositivi hardware collegati al computer attaccato) dei dati digitati sulla tastiera dall'utente durante una normale sessione di lavoro	L'intercettazione del traffico sulle porte Usb che si effettua tramite un Malware installato sul computer attaccato	L'intercettazione dei dati inviati alle periferiche (es. stampante) effettuata tramite un Malware installato sul computer attaccato	SICUREZZA INFORMATICA
102	I sistemi di business continuity e di disaster recovery:	sono tutte quelle attività legate al lato "fisico", come i sistemi antincendio o antiallagamento e altro, legati al ripristino di un sistema di elaborazione a seguito di un evento catastrofico	sono tutte le procedure informatiche che vengono attivate in caso di interruzione di un servizio On Line, in caso di attacco informatico	nessuna delle altre risposte è esatta	SICUREZZA INFORMATICA
103	Cosa si intende per DMZ (demilitarized zone)?	Quella parte della rete aziendale che eroga servizi verso l'esterno, che quindi deve essere accessibile dalla rete esterna	Quella parte della rete aziendale cui non è consentito l'accesso a nessuno per nessun motivo	Quella parte della rete aziendale ad uso esclusivo dei vertici aziendali	SICUREZZA INFORMATICA
104	Un firewall collega generalmente:	rete esterna, rete interna e DMZ di una organizzazione, impostando le regole di accesso e diniego alle varie risorse in base alle policy di sicurezza	esclusivamente reti e sottoreti interne di una organizzazione	solo reti esterne (in pratica blocca tutto il traffico in ingresso verso una rete locale)	SICUREZZA INFORMATICA
105	A cosa serve un "Proxy Server" ?	È un componente, hardware o software, che riceve una richiesta da un client interno e la trasferisce all'esterno della rete aziendale	È un software che controlla i pacchetti di dati che provengono da un server esterno verificando che siano privi di software dannosi	È un dispositivo hardware utilizzato per espandere una rete locale	SICUREZZA INFORMATICA
106	Com'è possibile inibire l'accesso a determinati siti in un sistema informatico aziendale?	Utilizzando un Proxy Server ed impostando una black list nelle impostazioni di configurazione	Agendo nelle impostazioni Bios del PC, caricandovi una black list di siti non autorizzati	Nelle impostazioni della scheda di rete	SICUREZZA INFORMATICA
107	Cosa si intende in informatica per Sandbox?	Un'area di test in cui eseguire operazioni critiche (es. apertura di allegati sospetti di e-mail) senza la possibilità di arrecare danni al sistema	Un'applicazione informatica che serve per testare l'accesso ad una risorsa protetta simulando il comportamento di un software malevolo	Un'area della rete interna di una organizzazione il cui accesso è inibito a tutti tranne che ai vertici aziendali	SICUREZZA INFORMATICA
108	In un sistema a crittografia asimmetrica:	ogni utente dispone di due chiavi, una privata ed una pubblica	ogni utente deve condividere la sua chiave privata con il destinatario del messaggio affinché questo possa essere decodificato	tutti gli utenti dispongono esclusivamente di chiavi pubbliche	SICUREZZA INFORMATICA
109	In un sistema a crittografia asimmetrica, chi rilascia la chiave pubblica?	Un soggetto terzo di fiducia, pubblico o privato, chiamato Certification Authority, che opera nel rispetto delle leggi nazionali ed europee	L'utente che invia un messaggio criptato	Esclusivamente il produttore del sistema operativo in uso da parte dell'utente, che riceve il messaggio per ovvi problemi di compatibilità	SICUREZZA INFORMATICA

CONCORSO PUBBLICO A 53 POSTI PER ISPETTORE INFORMATICO DEL CNVVF - SICUREZZA INFORMATICA

110	In un sistema crittografico asimmetrico:	gli utenti non devono scambiarsi le chiavi, solo la chiave pubblica è condivisa, la chiave privata verrà conservata e mantenuta segreta dall'utente	devono essere condivise sia la chiave pubblica che quella privata	non deve essere condivisa né la chiave pubblica né quella privata	SICUREZZA INFORMATICA
111	In un sistema crittografico simmetrico, qual è il momento più critico?	Lo scambio della chiave	L'invio del messaggio	La ricezione del messaggio	SICUREZZA INFORMATICA
112	L'hash di un file è:	una stringa di caratteri ottenuta dal file originale, applicando un algoritmo di codifica non reversibile	un gruppo di 4 byte ottenuto dal file originale, applicando un algoritmo SHA1	un numero da 1 a 100 ottenuto dal file originale, applicando un algoritmo	SICUREZZA INFORMATICA
113	Le funzioni hash sono molto usate in crittografia e nell'analisi forense per:	certificare l'integrità di un documento	verificare che il documento sia privo di malware	certificare che il documento non contenga elementi riservati che non devono essere condivisi	SICUREZZA INFORMATICA
114	Gli algoritmi crittografici di hash sono progettati:	per garantire con alta probabilità che due file differenti vengano rimappati su due hash differenti	in modo che due file differenti vengano rimappati su un unico hash	in modo che a partire da un unico file di partenza sia possibile generare un numero N di Hash	SICUREZZA INFORMATICA
115	A partire dall'Hash di un file è possibile risalire al contenuto del file originale?	No	Sì	Sì, solo se il file è di tipo ASCII	SICUREZZA INFORMATICA
116	Un attacco tramite "Elevazione di privilegi" si ha quando un utente:	o un programma con privilegi limitati, riesce ad elevare i propri privilegi sfruttando un bug di un sistema informatico	di tipo amministratore conferisce accidentalmente dei privilegi ad un utente di gerarchia inferiore	amministratore disattivato, viene riattivato da un malintenzionato ed usato per accedere liberamente ad un sistema informatico	SICUREZZA INFORMATICA
117	Cosa si intende per Ingegneria Sociale?	Lo studio di una persona o di un'organizzazione allo scopo di carpirne informazioni riservate	Lo studio dell'infrastruttura tecnologia (generalmente hardware) di un'organizzazione effettuata da un hacker	Un'attività che mira a penetrare una rete wireless	SICUREZZA INFORMATICA
118	Cosa si intende per "Steganografia Digitale" ?	Una tecnica grazie alla quale l'autore nasconde informazioni segrete all'interno di un messaggio apparentemente innocuo	Una tecnica, grazie alla quale l'autore cifra un messaggio utilizzando un apposito algoritmo e una chiave	Una tecnica, grazie alla quale l'autore cifra un messaggio utilizzando la sostituzione delle lettere	SICUREZZA INFORMATICA
119	In cosa consiste un sistema di autenticazione forte?	È un metodo di autenticazione elettronica che prevede due o più verifiche di autenticazione, per esempio PIN e password	È un metodo di autenticazione che prevede il riconoscimento diretto dell'utente da parte di una persona fisica	È un metodo di autenticazione che prevede il riconoscimento dell'utente attraverso la risoluzione di alcuni Captcha	SICUREZZA INFORMATICA
120	I virus del settore di avvio:	si installano nel settore di avvio (boot sector) dei dischi fissi e a volte cambiano l'indirizzo di avvio in modo da farlo corrispondere a un nuovo settore modificato e dannoso	sono dei virus che eseguono il loro codice all'avvio del PC e risiedono in file che si trovano nella directory di installazione del sistema operativo	sono virus che infettano la scheda madre del PC e si installano nelle memorie preposte all'avvio della macchina	SICUREZZA INFORMATICA
121	I macro virus:	prendono di mira fogli elettronici e database dei programmi "office", annidandosi nelle macro o in porzioni di codice definito dall'utente	sono virus di elevate dimensioni	sono virus che infettano i file eseguibili	SICUREZZA INFORMATICA
122	I virus polimorfici:	infettano un oggetto con un codice virale sempre differente	mantengono il proprio codice virale inalterato nel tempo	esistono esclusivamente in ambiente Apple/Mac	SICUREZZA INFORMATICA
123	Sono sintomi che un PC è potenzialmente infetto da un virus:	inaspettato e improvviso rallentamento del dispositivo, scomparsa di file o cartelle, navigazione su Internet lenta	impossibile avvio del PC segnalato da beep intermittenti, quando si preme sul pulsante di accensione	la comparsa di una schermata blu con errori relativi a driver e/o periferiche, in ambiente Windows	SICUREZZA INFORMATICA

CONCORSO PUBBLICO A 53 POSTI PER ISPETTORE INFORMATICO DEL CNVVF - SICUREZZA INFORMATICA

124	Il noto virus CryptoLocker, si diffonde generalmente:	come allegato di e-mail che l'utente apre anche inconsapevolmente	tramite chat Messenger	tramite l'accesso a siti fake che simulano siti istituzionali	SICUREZZA INFORMATICA
125	Secondo le linee guida dell'Agid, per la realizzazione di applicazioni web è raccomandato:	prevedere ovunque il protocollo HTTPS e disattivare l'accesso tramite HTTP a tutte le risorse protette	prevedere l'uso del protocollo HTTP per la generalità delle applicazioni e utilizzare l'HTTPS solo in casi di reale criticità	di non utilizzare né il protocollo HTTP né HTTPS	SICUREZZA INFORMATICA
126	Che differenza c'è tra Hacker e Cracker?	L'hacker studia ed analizza i sistemi, mosso da curiosità e sete di conoscenza. Il Cracker è invece colui che commette reati informatici alterando abusivamente un sistema	Non ci sono differenze	Il Cracker studia e analizza i sistemi, mosso da curiosità e sete di conoscenza. L'hacker è invece colui che commette reati informatici alterando abusivamente un sistema	SICUREZZA INFORMATICA
127	Quali tra i seguenti sono definibili software per la sicurezza informatica?	Antivirus, Firewall, software di Backup	Sistemi operativi, programmi Office "like", software per la compressione dei dati	Software di configurazione delle periferiche	SICUREZZA INFORMATICA
128	Cosa si intende per Lamer?	Un aspirante Cracker dalle limitate conoscenze, il cui scopo è generalmente provocare danni ad un sistema informatico per diletto	Una tipologia di Hacker che lavora generalmente per agenzie governative	Un Hacker o Cracker dalle eccellenti conoscenze informatiche	SICUREZZA INFORMATICA
129	Il termine Newbie indica una persona:	inesperta in campo informatico ma che mostra l'intenzione a migliorarsi	una persona con capacità medie ma non ancora paragonabili a quelle di un Hacker professionista	una persona con capacità sopra la media	SICUREZZA INFORMATICA
130	In sicurezza informatica cosa si intende per "eventi accidentali"?	Tutti quegli eventi non legati ad attacchi informatici e causati da comportamenti anomali di utenti o guasti a componenti hardware	Tutti gli eventi legati ad attacchi informatici	Tutti quegli eventi non riconducibili all'interno dell'organizzazione in cui si è verificato l'evento	SICUREZZA INFORMATICA
131	Gli attacchi detti "Email Spoofing" sono quelli in cui:	un attaccante invia un'e-mail emulando un altro mittente	la vittima riceve una falsa email in cui per grafica e contenuto sembra che la sessa provenga da un ente istituzionale	l'utente attaccato viene invitato ad aprire un allegato che contiene il codice malevolo	SICUREZZA INFORMATICA
132	Si ha un attacco con manomissione dei campi di un Form HTML, quando:	un Hacker sfrutta i campi nascosti di un form HTML per inviare richieste a sua scelta	un Hacker realizza una pagina HTML con un form del tutto simile ad un'altra pagina reale, l'utente non si accorge della differenza ed inserisce i suoi dati personali nella pagina fake	un Hacker rende inaccessibile un form HTML su una pagina web	SICUREZZA INFORMATICA
133	Si ha un attacco con manomissione della stringa di Query URL quando:	l'hacker è in grado di vedere la stringa e modificarla a suo piacimento, se un form utilizza il metodo GET	l'hacker inibisce l'uso dei form su una certa pagina sfruttando una vulnerabilità del DBMS nell'esecuzione delle query	un hacker realizza una pagina HTML con un form del tutto simile ad un'altra pagina reale, l'utente non si accorge della differenza ed inserisce i suoi dati personali nella pagina fake	SICUREZZA INFORMATICA
134	Cosa si intende per "Port Forwarding"?	Un metodo per rendere all'esterno una risorsa situata nella propria rete privata	La scansione delle porte effettuata da un hacker per verificarne l'apertura	Il controllo delle porte di un computer effettuato da un software di protezione, allo scopo di rilevare la presenza di anomalie di sicurezza	SICUREZZA INFORMATICA
135	Dove si impostano le connessioni per implementare il "Port Forwarding"?	Nelle impostazioni del router	Nelle impostazioni del sistema operativo	Utilizzando software di terze parti	SICUREZZA INFORMATICA

CONCORSO PUBBLICO A 53 POSTI PER ISPETTORE INFORMATICO DEL CNVVF - SICUREZZA INFORMATICA

136	A cosa serve lo SPID?	È un meccanismo che permette ai cittadini di accedere ai servizi online delle Pubbliche Amministrazioni e dei soggetti privati con un'unica Identità Digitale	È un meccanismo utilizzato dalle PA esclusivamente per la registrazione di dati ai fini di selezioni pubbliche	È un meccanismo che permette ai cittadini di accedere esclusivamente ai servizi online dell'Agenzia delle Entrate	SICUREZZA INFORMATICA
137	Come si ottiene lo SPID?	L'identità SPID è rilasciata dai Gestori di Identità Digitale (Identity Provider), soggetti privati accreditati da Agid che, nel rispetto delle regole emesse dall'Agenzia, forniscono le identità digitali e gestiscono l'autenticazione degli utenti	È possibile ottenere lo SPID unicamente presso il provider POSTE ITALIANE Spa	L'identità SPID è rilasciata da un qualsiasi istituto bancario a condizione che si trovi sul territorio nazionale o nel territorio dell'Unione Europea	SICUREZZA INFORMATICA
138	Quanti livelli di sicurezza implementa il sistema SPID?	3	4	5	SICUREZZA INFORMATICA
139	Cosa prevede il primo livello di sicurezza dello SPID per l'accesso ai servizi Online?	Il primo livello permette di accedere ai servizi online attraverso le credenziali SPID, nome utente e password	Il primo livello permette di accedere ai servizi online attraverso il proprio numero di SPID	Il primo livello permette di accedere ai servizi online attraverso un codice temporaneo che viene rilasciato tramite un'apposita applicazione	SICUREZZA INFORMATICA
140	Cosa prevede il secondo livello di sicurezza dello SPID per l'accesso ai servizi Online?	Il secondo livello permette l'accesso attraverso le credenziali SPID e la generazione di un codice temporaneo, o l'uso di un'app fruibile attraverso un dispositivo, come ad esempio uno smartphone	Il secondo livello permette l'accesso attraverso le credenziali SPID e la fornitura di un token in grado di generare un codice temporaneo	Il secondo livello permette l'accesso attraverso le credenziali SPID e l'invio di una e-mail alla propria PEC contenente un codice segreto	SICUREZZA INFORMATICA
141	Cosa prevede il terzo livello di sicurezza dello SPID per l'accesso ai servizi Online?	Il terzo livello prevede, oltre alle credenziali SPID, l'utilizzo di ulteriori soluzioni di sicurezza e di eventuali dispositivi fisici (es. smart card) che vengono erogati dal gestore dell'identità	Il terzo livello permette l'accesso attraverso le credenziali SPID e l'invio di una e-mail alla propria PEC contenente un codice segreto	Il terzo livello permette l'accesso attraverso le credenziali SPID e la risoluzione di un Captcha	SICUREZZA INFORMATICA
142	Chi può richiedere uno SPID?	Tutti i cittadini maggiorenni in possesso di un documento italiano in corso di validità	Tutti i cittadini che abbiano compiuto il venticinquesimo anno di età, in possesso di un documento italiano in corso di validità	Chiunque abbia un domicilio sul territorio italiano	SICUREZZA INFORMATICA
143	Secondo le raccomandazioni dell'Agid, cosa sono le misure minime di sicurezza ICT per le pubbliche amministrazioni?	Sono un riferimento pratico per valutare e migliorare il livello di sicurezza informatica delle amministrazioni, al fine di contrastare le minacce informatiche più frequenti	È un elenco di prodotti sia hardware che software, certificati e specificatamente raccomandati, per essere utilizzati dalla PA	È l'elenco del personale che ogni PA destina a scopi di sicurezza	SICUREZZA INFORMATICA
144	Secondo le raccomandazioni dell'Agid, le misure minime di sicurezza ICT per le pubbliche amministrazioni si basano su:	tre livelli di attuazione, ovvero minimo, standard e avanzato	un solo livello minimo, indipendentemente dalla natura e dimensione della PA	misure che ogni PA definisce in proprio	SICUREZZA INFORMATICA
145	La sigla Agid Basic Security Controls identifica:	otto classi di controlli che devono essere implementati per ottenere un determinato livello di sicurezza in una PA, secondo lo schema dell'Agid	la checklist di tutti i dispositivi hardware e software con relativi utilizzatori che sono presenti in una PA	l'elenco dei fornitori di prodotti e/o servizi di una PA. Ognuno di essi è necessario che disponga di tutte le certificazioni in base al tipo di prodotto/servizio fornito	SICUREZZA INFORMATICA
146	La classe di controlli AgiD Basic Security Controls ABSC10(CSC10) disciplina:	la gestione delle copie di sicurezza dei dati	l'uso appropriato dei privilegi di amministratore	le difese contro i Malware	SICUREZZA INFORMATICA

CONCORSO PUBBLICO A 53 POSTI PER ISPETTORE INFORMATICO DEL CNVVF - SICUREZZA INFORMATICA

147	La classe di controlli AgiD Basic Security Controls ABSC13(CSC13) disciplina:	la protezione dei dati	le difese contro i Malware	la gestione delle copie di sicurezza dei dati	SICUREZZA INFORMATICA
148	Cosa sono le Crypto API?	Sono delle librerie utilizzabili dagli sviluppatori per attività di codifica/decodifica di informazioni	Sono delle librerie utilizzabili dagli utenti finali per il controllo dell'accesso in applicazioni di rete	Sono dei software che gli utenti di un sistema remoto utilizzato per accedere in anonimato	SICUREZZA INFORMATICA
149	La crittografia a chiave simmetrica è anche chiamata a chiave:	privata	pubblica	segreta	SICUREZZA INFORMATICA
150	La crittografia a chiave asimmetrica è anche chiamata:	crittografia a coppia di chiavi	a chiave privata	a chiave segreta	SICUREZZA INFORMATICA
151	Come si può rimuovere una password da bios?	Utilizzando un ponticello della scheda madre	Avviando il computer dal disco del sistema operativo	Premendo ripetutamente il tasto F8 all'avvio e dal menù successivo scegliere l'avvio sicuro	SICUREZZA INFORMATICA
152	Cosa si intende per attacco Man-In-The-Middle?	Un tipo di attacco in cui un aggressore si interpone tra due sistemi di elaborazione intercettandone le comunicazioni	Un tipo di attacco in cui l'aggressore bombarda di richieste il sito da attaccare	Un tipo di attacco in cui l'aggressore cerca di ottenere un Exploit sul sito da attaccare	SICUREZZA INFORMATICA
153	Qual è la differenza principale tra la posta elettronica e la PEC?	La posta elettronica non fornisce certezza di invio e ricezione di un messaggio ne dell'identità del mittente, al contrario la PEC consente di avere prova opponibile dell'invio e della consegna di un documento elettronico	La posta elettronica garantisce la certezza di invio e ricezione di un messaggio oltre che dell'identità del mittente, al contrario la PEC non consente di avere prova opponibile dell'invio e della consegna di un documento elettronico	Posta elettronica e PEC sono equivalenti, si tratta infatti dello stesso strumento di invio e ricezione email che a seconda dei provider assume un nome o un altro	SICUREZZA INFORMATICA
154	Quale tra le seguenti affermazioni in merito alla posta elettronica e PEC è vera?	La posta elettronica sta alla lettera ordinaria come la PEC sta alla raccomandata	La posta elettronica sta alla raccomandata come la PEC sta alla lettera ordinaria	Non ci sono differenze sostanziali tra la posta elettronica e la PEC	SICUREZZA INFORMATICA
155	Nella tecnica della firma digitale, cosa utilizza il destinatario del messaggio per ottenerne il testo in chiaro?	La chiave pubblica del mittente	La propria chiave pubblica	La propria chiave privata	SICUREZZA INFORMATICA
156	Se l'utente A desidera inviare un messaggio crittografato all'utente B, il testo in chiaro è crittografato con la chiave pubblica:	dell'utente B	dell'utente A	di un ISP	SICUREZZA INFORMATICA
157	Un firewall con filtraggio di pacchetto:	filtra i pacchetti esaminando le intestazioni IP e TCP/UDP lasciando passare quelli che soddisfano le regole impostate	esegue un controllo antivirus di ogni pacchetto in ingresso, scartando quelli sospetti	tiene traccia di tutti i pacchetti in base alla provenienza ed alle porte TCP/UDP ma non applica alcun filtro	SICUREZZA INFORMATICA
158	In un MAC ADDRESS, il produttore del dispositivo è specificato da:	i primi tre byte dell'indirizzo	gli ultimi tre byte dell'indirizzo	i byte da 10 a 13	SICUREZZA INFORMATICA
159	Come difendersi da un attacco "Brute Force"?	Implementando una policy che bloccherà l'account dell'attaccante dopo alcuni tentativi di password non validi	Implementando una policy a livello di sistema operativo che bloccherà il server attaccato dopo alcuni tentativi di password non validi	Tenendo costantemente aggiornati antivirus e firewall	SICUREZZA INFORMATICA
160	Cosa si intende per hardening software di un server?	Tutte quelle operazioni di configurazione o aggiornamenti che hanno lo scopo di minimizzare eventuali attacchi informatici	Tutte quelle operazioni che mirano a migliorare l'hardware per far fronte ad eventuali eventi catastrofici	La variazione periodica di indirizzi e nomi logici del server in modo che lo stesso non sia facilmente identificabile sulla rete	SICUREZZA INFORMATICA

CONCORSO PUBBLICO A 53 POSTI PER ISPETTORE INFORMATICO DEL CNVVF - SICUREZZA INFORMATICA

161	Cosa si intende per LDAP Injection?	Un tipo di attacco portato verso un'applicazione web dove gli hacker introducono del codice malevolo in un campo di input dell'interfaccia utente nel tentativo di ottenere accesso a informazioni non autorizzate	Un tipo di attacco che viene effettuato contro DBMS di rete allo scopo di bloccarne il funzionamento	Un tipo di attacco verso server Ftp allo scopo di modificare i permessi alle cartelle di rete e quindi garantire all'attaccante il libero accesso	SICUREZZA INFORMATICA
162	Secondo il Cifrario di Cesare, ogni lettera va sostituita con quella che si trova:	tre posti dopo	quattro posti dopo	cinque posti dopo	SICUREZZA INFORMATICA
163	Nella procedura di autenticazione forte con OTP (one time password):	viene generata una password che vale un solo accesso	l'utente ha a disposizione un solo tentativo di accesso	vengono generate N password, l'utente può utilizzarle indifferentemente per l'accesso	SICUREZZA INFORMATICA
164	L'attacco noto come "Ping of Death":	invia pacchetti di dati superando il limite massimo (65.536 byte) consentito dal TCP/IP ed a causa di questa tipologia di attacco, poiché i pacchetti di dati inviati sono più grandi di quelli che il server può gestire, il server può bloccarsi, riavviarsi o può andare in crash	sovraccarica il buffer del server con un numero di dati maggiore di quanto ne può contenere. In tal modo il buffer si riempie oltre il limite, corrompendo i dati presenti in memoria e determinando conseguentemente un'instabilità nel sistema	funziona inondando la vittima con messaggi SYN incompleti. L'host vittima assegna risorse di memoria che normalmente non vengono mai utilizzate, negando conseguentemente l'accesso agli utenti legittimi per mancanza di necessarie risorse	SICUREZZA INFORMATICA
165	Cosa è il Metasploit Project?	Uno strumento di penetration testing usato per valutare la sicurezza di un sistema informatico	Un noto gruppo Hacker	Uno strumento illegale che contiene una serie di tool di norma utilizzati per ottenere accessi illeciti a sistemi informatici a scopo malevolo	SICUREZZA INFORMATICA
166	Cosa si intende per "Payload" di un virus informatico?	Sono le azioni che il virus esegue dopo aver infettato il sistema	Sono le operazioni che il virus esegue per infettare un sistema	Corrisponde alla modalità di trasmissione di un virus informatico	SICUREZZA INFORMATICA
167	Secondo le linee guida Agid, per STRIDE si intende:	un processo metodologico che aiuta a individuare le minacce di sicurezza in un sistema complesso	un processo che minimizza i potenziali disagi dovuti a problemi fisici che potrebbero occorrere ad un sistema informatico	una checklist di buone pratiche che uno sviluppatore di sistemi informatici per la PA dovrebbe seguire	SICUREZZA INFORMATICA
168	Secondo le linee guida Agid, cosa si intende per "Information Disclosure"?	L'esposizione delle informazioni a persone non autorizzate alla loro visione	Le attività necessarie al ripristino di un servizio, tipicamente un sito istituzionale, a priorità elevata	La conservazione dei dati di registrazione degli utenti nei portali della PA	SICUREZZA INFORMATICA
169	L'identità digitale SPID può essere utilizzata per accedere ai servizi in rete delle Pubbliche Amministrazioni anche al di fuori del territorio italiano?	Sì, solo per le Pubbliche Amministrazioni dell'Unione Europea	No	Sì, per qualsiasi Pubblica Amministrazione estera	SICUREZZA INFORMATICA
170	Il comando Linux CHMOD, utilizzato su un server, consente di:	verificare, modificare e attribuire permessi particolari a file e cartelle contenute nello spazio web	escludere un utente da una cartella	aumentare o diminuire i privilegi di un utente	SICUREZZA INFORMATICA
171	Il comando Linux "chmod 777 nomefile":	assegna tutti i permessi al file"nomefile"	blocca l'esecuzione del file "nomefile" a tutti gli utenti	assegna il permesso di lettura al proprietario del file "nomefile"	SICUREZZA INFORMATICA
172	Il file system "ext4" è utilizzato:	in ambiente Linux	in ambiente Windows	in entrambi gli ambienti	SICUREZZA INFORMATICA
173	Il comando PING seguito da un indirizzo IP viene utilizzato per:	testare la connessione alla risorsa identificata dall'indirizzo IP	attivare o disattivare la risorsa identificata dall'indirizzo IP	mettere offline, ovvero non raggiungibile dagli utenti, la risorsa identificata dall'indirizzo IP	SICUREZZA INFORMATICA

174	Il comando IPCONFIG eseguito dal prompt dei comandi di Windows restituisce:	tutti i valori correnti della configurazione di rete TCP/IP	l'elenco delle porte attive con i relativi servizi	l'elenco degli indirizzi IP bloccati	SICUREZZA INFORMATICA
175	Il comando Linux CHOWN, utilizzato su un server, consente di:	modificare il proprietario e/o il gruppo assegnato di uno o più file e directory	verificare, modificare e attribuire permessi particolari a file e cartelle contenute nello spazio web	creare e manutenere uno o più utenti	SICUREZZA INFORMATICA
176	Per accedere alla shell di comandi testuali in ambiente Windows:	cliccare sul menù START con il tasto destro del mouse e scegliere l'opzione ESEGUI, poi digitare CMD	usare la combinazione di tasti WIN-SHIFT-S	cercare "Shell dei comandi", dal menù START alla lettera S	SICUREZZA INFORMATICA
177	In un sistema operativo Linux la cartella "/root" :	è una cartella particolare riservata all'utente con i massimi permessi amministrativi e contiene le impostazioni dei programmi relativi all'utente Root	contiene una serie di sottocartelle che corrispondono ai vari utenti del sistema con le loro impostazioni personali	è una cartella di sistema non accessibile a nessun utente	SICUREZZA INFORMATICA
178	Il comando NETSTAT -AN in ambiente Windows:	restituisce un elenco di porte attualmente aperte e relativi indirizzi IP. Viene anche specificato in che stato si trova la porta	Visualizza l'elenco delle porte chiuse o bloccate	Non esiste questo comando in ambiente Windows	SICUREZZA INFORMATICA
179	A cosa serve il comando TRACERT in ambiente Windows?	Se utilizzato con un indirizzo IP o con un dominio, visualizza tutti i nodi intermedi tra il proprio PC e quello di destinazione	Serve a visualizzare tutti gli indirizzi IP presenti nella propria rete locale	Se utilizzato con un indirizzo IP o con un dominio, verifica che la risorsa che si trova a quell'indirizzo abbia lo stesso sistema operativo del proprio computer	SICUREZZA INFORMATICA
180	Il comando Windows "shutdown" consente di:	impostare lo spegnimento del PC da riga di comando	impostare l'avvio remoto del PC da riga di comando	avviare un PC presente sulla propria rete LAN	SICUREZZA INFORMATICA