1. DH e RSA hanno scopi differenti: quello di RSA é di essere molto più veloce nella fase di cifratura/decifrazione
   - F
2. Il SUID è il bit che permette di lanciare con sudo il programma su cui è settato
   - F
3. La collocazione di sistemi in cloud ha unicamente effetti positivi sulla sicurezza
   - F
4. Un vantaggio degli Host-based IDS è che possono classificare più accuratamente il rischio associato a un pacchetto di rete
   - V
5. L'indice di Coincidenza è la probabilità che due lettere scelte a caso in un testo siano diverse
   - F
6. Le capability list sono delle liste associate a ogni soggetto del sistema
   - V
7. Nei cifrari a trasposizione le statistiche dei digrammi e trigrammi permettono di dedurre la dimensione della tabella di cifratura
   - V
8. In Unix il comando passwd si usa per verificare la robustezza della password
   - F
9. Nell'autenticazione passiva Prover e Verifier confrontano la conoscenza di un segreto
   - V
10. Con una Local File Inclusion possiamo recuperare file interni al web server
    - V
11. ASLR è un meccanismo di protezione del kernel linux per randomizzare gli spazi di memoria
    - V
12. Se un sito è protetto da TLS non è possibile eseguire una SQL Injection
    - F
13. Nel cifrario con sostituzione monoalfabetica lo spazio delle chiavi è grande 26
    - V
14. Nel test di Kasiski c'è la fattorizzazione e scelta delle distanze con un fattore comune
    - V
15. Secure Boot è il nome specifico dato all'implementazione di trusted boot basata su UEFI
    - V
16. Il valore esadecimale 0x90 indica un carattere NEUTRO nell'assembler x86
    - F
17. Le ACL e le Capabilities sono la stessa cosa
    - F
18. Data chiave pubblica (e, n) e chiave privata (d, n) la cifratura consiste nel calcolare: c = m^e mod n
    - V
19. Esistono tre tipi fondamentali di firewall Packet filter, Application-level gateway, Circuit-level gateway
    - V
20. Un vantaggio dei Network-based IDS è che non interferiscono col funzionamento dei sistemi monitorati
    - V
21. HTTPS è HTTP con una canale di comunicazione in SSL cifrato
    - V
22. Un Intrusion Detection System può bloccare un attacco in corso
    - F

23. Tra i fattori di autenticazione c'è qualcosa che si conosce (Password, PIN)
    - V
24. DNS Spoofing è una tecnica di esfiltrazione dati
    - F
25. CBC sta per Cipher Block Chaining e consiste nel Cifrare un blocco modificandolo col contributo del blocco cifrato precedente
    - V
26. I log sono utili solo a fini forensi (cioè per comprendere un attacco dopo che si è compiuto)
    - F
27. L'approccio default deny su firewall significa che tutto il traffico viene bloccato
    - F
28. Nell'autenticazione attiva Prover e Verifier si scambiano ogni volta un dato diverso
    - V
29. DNS Spoofing è una tecnica di falsificazione dei pacchetti di richiesta inviati dalla vittima al sistema DNS
    - F
30. Il Command and Control è il computer incaricato di gestire le comunicazioni con gli elementi di una botnet
    - V
31. Ogni file del filesystem Unix è protetto da un set di permessi codificati in 12 bit
    - V
32. Gli algoritmi di cifratura a blocchi cifrano in sequenza frammenti del testo in chiaro
    - F
33. La proprietà one-way degli hash significa che dato un hash è possibile soltanto calcolare l'hash di un testo o ritrovare il testo dato un hash ma non entrambe le azioni
    - F
34. La collocazione di sistemi in cloud migliora (generalmente) la disponibilità dei servizi
    - V
35. DH e RSA hanno scopi differenti: quello di DH è scambiare una chiave condivisa tra due parti
    - V
36. La strcpy in linguaggio C non è una funzione pericolosa nel generare vulnerabilità di buffer overflow
    - F
37. 2FA e 2 step authentication sono esattamente la stessa cosa.
    - F
38. Il registro EIP in x86 indica il valore dell'indirizzo di ritorno
    - F
39. Gli attacchi attivi sono come quelli passivi l'unica differenza consiste nel fatto che vengono eseguiti a real-time
    - F
40. La proprietà di diffusione misura il grado in cui le proprietà statistiche degli elementi del testo cifrato vengono sparse sugli elementi del testo in chiaro
    - F
41. Nell'attacco dei cifrari a sostiuzioni il fatto che alcune lettere siano più frequenti di altri nel linguaggio naturale non ha nessuna importanza
    - F
42. Un EDR può essere definito come una variante evoluta di Network-based IDS
    - F
43. Il comando find / -type f -perm /6000 mi permette di trovare i file col SUID attivato
    - F

44. DH e RSA hanno scopi differenti: quello di RSA é di scambiarsi la chiave simmetrica di cifratura
    - F
45. Il miglior attacco a RSA è la ricerca dei fattori del modulo
    - V
46. Il controllo dell'accesso è decidere se un soggetto può eseguire una specifica operazione su di un oggetto
    - V
47. I sistemi a sfida e risposta sono tipicamente implementati condividendo un segreto come ad esempio una chiave simmetrica
    - F
48. Lo sniffing può compromettere la riservatezza dei dati
    - V
49. La cifratura dei dischi protegge da qualsiasi tentativo di esfiltrazione dei dati
    - F
50. Nel modello RBAC (Role-based access control) i permessi sono assegnati ai ruoli
    - V
51. Una tecnica comune di esfiltrazionze dei dati è attraverso richieste DNS contenenti i dati da esfiltrare
    - V
52. 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
    - V
53. FIDO alliance è un sistema di generazione degli OTP
    - F
54. Suricata può funzionare sia da IDS che da IPS
    - V
55. Gli attacchi passivi non modificano i dati in transito
    - V
56. L'IP spoofing consiste nel cercare di recuperare l'IP della vittima
    - F
57. Le ACL sono liste associate ad ogni soggetto del sistema
    - F
58. I due paradigmi fondamentali per il controllo dell'accesso sono DAC (Discretionary access control) e TAC (Tertiary access control)
    - F
59. La proprietà collision-free degli hash significa che non si può trovare una coppia di documenti con lo stesso hash
    - V
60. Lo scopo del TOTP è quello di forzare l'utente a cambiare periodicamente la password
    - F
61. Nel modello web of trust della certificazione delle chiavi pubbliche l'autenticità della chiave pubblica è attestata dagli altri utenti
    - V
62. Il controllo dell'integrità dei file è uno dei metodi usati dagli HIDS
    - V
63. Measured Boot si riferisce a un processo generale, che tipicamente usa un TPM come hardware root of trust
    - V
64. Il miglior attacco a RSA è la forza bruta

- F

65. L'ARP poisoning consiste nel convincere un host che l'IP di una vittima è associato al MAC dell'attaccante
    - V
66. I canarini sono un meccanismo di protezione del kernel linux per segnalare un overflow in memoria
    - F
67. Nei cifrari a sostiuzione polialfabetica le frequenze di un carattere cifrato derivano da contributi di diversi caratteri in chiaro
    - V
68. Code Injection si verifica quando dell'input non sanitizzato viene interpretato come codice
    - V
69. X.509 è la versione di SSL più utilizzata
    - F
70. Uno dei presupposti per la robustezza degli algoritmi a chiave asimmetrica è che non esistono modi efficenti di fattorizzare il modulo
    - V
71. Ogni file del filesystem Unix è descritto da 12 i-node
    - F
72. Inserire un ritardo di pochi secondi tra due login errate non è una misura efficace per mitigare gli attacchi brute force
    - F
73. Tra i fattori di autenticazione c'è qualcosa che si possiede fisicamente, come un Pin o una Password
    - F
74. Le chiavi di autenticazione usate da Secure Boot sono aggiornabili senza interruzioni di servizio
    - F
75. Lo sniffing non richiede accesso fisico alla rete
    - F
76. I bit di autorizzazione sono di 3 tipi R,W,X (read,write,execute)
    - V
77. Nelle time based sql-injection è importante il tempo di computazione della query sql
    - V
78. Il salt è una password aggiuntiva di secondo livello
    - F
79. La fiducia nell'autenticità di una Root Certification Authority è perfettamente verificabile dal corrispondente certificato
    - F
80. Gli algoritmi di cifratura a blocchi sono così definiti perchè si arrestano non appena la cifrazione è considerata sicura
    - F
81. Il salt è una variazione random inserita dal sistema all'atto della scelta della password
    - V
82. Il tasso di " falsi positivi " non è un parametro importante per la qualità di un IDS
    - F
83. Nei cifrari a sostituzione polialfabetica conoscere il contenuto di una parte del messaggio non aiuta la decifrazione dell'intero testo
    - F
84. 802.1x è uno standard di autenticazione utilizzato nelle connessioni fisiche
    - V
85. Le botnet sono reti di computer infetti chiamati zombie

- V

86. Diffie Hellmann è uno schema di cifratura a chiave simmetrica
    - F
87. Uno dei presupposti per la robustezza degli algoritmi a chiave asimmetrica è che non esistono modi efficienti di invertire l'esponenziale modulare
    - V
88. Una password che utilizza tutti i tipi di caratteri è sempre più robusta di una che utilizza solo una categoria (es. lettere maiuscole)
    - F
89. Nel modello Infrastrutturale della certificazione delle chiavi pubbliche l'autenticità della chiave pubblica è data da un soggetto terzo fidato che emette la certificazione
    - V
90. L'IP spoofing consiste nell'assumere un indirizzo IP diverso da quello regolarmente assegnato al proprio sistema
    - V
91. cifrato vengono sparse sugli elementi del testo in chiaro -F
92. È bene tenere ben protette e inaccessibili entrambe le chiavi generate da un'entità per l'impiego con l'algoritmo RSA -F
93. Nel modello web of trust non ci sono entità super-partes, l'autenticità è garantita da qualcuno di fidato. Questo rende il modello molto poco scalabile -V