EXAMEN LA SSIT (MASTER TC&TM), 21 IANUARIE 2021, TEST (45 minute) _____
(ATENȚIE: Întrebările au un SINGUR răspuns corect!!!) *(Nume - Prenume)*

1. La analiza fisierelor cu loguri de pe un server web descoperiti mai multe inregistrari ce contin expresia **1 = 1**. Ce tip de atac la nivel aplicatie ati descoperit?
   a. Cross-site Scripting
   b. Cross Site Request Forgery
   c. SQL injection
   d. OS command injection

2. Care din urmatoarele NU reprezinta o cerinta de securizare a resurselor de tip S3 in sistemul AWS?
   a. Logare access la resursele de tip S3
   b. Versionare obiecte stocate in S3
   c. Criptare obiecte stocate in S3 folosind SSE, KMS, CMS, CSE
   d. Activare flag “Public” pentru a facilita accesul utilizatorilor la date

3. Folosirea acelorasi mecanisme de control pentru a securiza toate datele companiei, reprezinta o abordare “Defence in Depth” de tipul:
   a. Uniform Protection
   b. Protected Enclaves
   c. Information Centric
   d. Threat vector

4. La rularea comenzii `'ls -l'` în directorul `'/etc'`, fișierul `'/etc/vimrc'` prezintă următoarele informații:

   ```
   -rw-r--r-- 1 root root 841 Jan 18 06:17 vimrc
   ```

   Care afirmație este, în acest caz, adevărată?
   a. Fișierul poate fi modificat de către un utilizator care are 'User ID' (UID) = 0.
   b. Fișierul este executabil.
   c. Nici un utilizator din sistem nu poate citi conținutul fișierului, chiar dacă are suficiente permisiuni în directorul '/etc'.
   d. Fișierul poate fi modificat de către utilizatorii din grupul 'root'.

5. Care ar putea fi impactul pierderii sau manipularii gresite a datelor confidentiale intr-o firma?
   a. Penalitati severe legislative
   b. Impact devastator asupra reputatiei si dezvoltarii companiei
   c. Pierderea increderii clientilor
   d. Toate cele de mai sus

6. Care sunt etapele, in ordine cronologica, parcurse de un atacator de tip APT:
   a. Reconnaissance, Weaponisation, Delivery, Exploitation, Installation, Command&Control, Actions
   b. Exploitation, Privilege Escalation, Command&Control, Data Exfiltration
   c. Reconnaissance, Delivery, Exploitation, Command&Control, Actions
   d. Intelligence gathering, Command&Control, Exploitation, Privilege Escalation, Data Exfiltration

7. Pentru a asigura securitatea la nivel de retea a serverelor de baze de data acestea trebuie plasate:
   a. In zona publica pentru a permite accesul facil al utilizatorilor din Internet
   b. In zona de DMZ pentru a nu permite accesul din exterior
   c. Securitatea unui server de baze de date este asigurata prin criptarea datelor sensitive
   d. In zona privata, dedicata sistemelor interne si fara acces din exterior

8. Un fișier '/etc/syslog.conf' conține următoarele linii de configurare:

   ```
   kern.*                      /dev/console
   *.info; cron.=err           /var/log/messages
   cron.*                      /var/log/cron
   ```

   Pe baza acestor informații, rezultă că:
   a. Nici un mesaj emis din interiorul kernelul Linux nu este afișat în consolă.
   b. Mesajele emise de serviciul 'cron' sunt salvate în fișierul '/var/log/messages', indiferent de prioritatea acestora.
   c. Mesajele având prioritatea 'err' sunt salvate în fișierul '/var/log/messages', indiferent de sursa acestora.
   d. Mesajele având prioritatea 'debug' sunt salvate în fișierul '/var/log/messages', indiferent de sursa acestora.

9. Care dintre afirmatiile urmatoare, referitoare la utilizarea contului de `root` in AWS, este adevarata:
   a. Contul de `root` este utilizat pentru operatiunile zilnice de administrare
   b. Credentialele contului de `root` sunt partajate cu colegii de echipa pentru un acces facil la sistemul AWS
   c. Contul de `root` trebuie protejat prin activarea MFA si a unei proceduri de tip “break glass”
   d. Accesul la toate resursele din sistemul AWS se asigneaza prin contul de `root`