Információ-biztonság vizsga 2019.5.13. Név:_____, Neptun:_____

5 pontos kérdések (1-2 szavas, vagy mondatos válaszok):

1. Nevezzen meg egy csomag szintű támadást!
   Smurf, SYN flood
2. A gyakorlatban miért nem alkalmazható az OTP titkosítási módszer?
   A kulcs előállítása, és továbbítása sem megoldható a gyakorlatban.
3. Mire szolgál a CRL?
   Annak ellenőrzésére, hogy egy tanúsítványt visszavontak-e.
4. Milyen (UDP/TCP?) és melyik (0-65535?) porton működik az SSTP?
   TCP 443
5. Mi az OWASP TOP 10?
   A WEB alkalmazások 10 legkritikusabb biztonsági kockázatainak rendszeresen frissülő listája.
6. Milyen lényeges különbség van az IDS és az IPS között?
   Az IPS képes beavatkozni is.
7. Nevezzen meg legalább egy információbiztonsággal foglalkozó szabványt!
   ISO 27000
8. Mi az adat 3 védendő tulajdonsága?
   Bizalmasság, Sértetlenség, Rendelkezésre állás
9. Milyen OTP hitelesítő eszközöket ismer? (Legalább 3)
   HOTP, TOTP, OCRA
10. Mi a 3 azonosítási faktor?
    Valamit tudok, valamivel rendelkezem, valamilyen tulajdonságom van.

10 pontos kérdések:

1. Nevezzen meg legalább 5 a CVE-ben lévő információt!
   Elnevezés, Azonosító, CVSS (súlyosság), Érintett termék, Leírás, Következmény, Védekezési lehetőségek
2. Nevezzen meg legalább 3 WiFi IDS funkciót!
   Azonosítja a hálózatban a gyanús vagy kártékony aktivitásokat, Észreveszi a rendszer normális működésétől eltérő tevékenységeket, Naplózza, katalogizálja és osztályozza a rendszerfolyamatokat, Szokatlan/gyanús események esetén képes valós idejű riasztásokat generálni. (Folyamatosan keres: Hamis AP-kat, Kalóz AP-kat, Zavarforrásokat. Állandóan figyeli: WiFi eszközök MAC címét, és az eszközök tulajdonságait, Kliensek kapcsolódását, újra-kapcsolódását)
3. Egy szinte minden tűzfal mögül használható VPN kialakítása a cél. Melyiket választaná?
   a. SSTP
   b. IPsec
4. Fontos, hogy a továbbított információkat ne lehessen lehallgatni. Melyiket választaná és **miért**?
   a. AH
   b. ESP titkosít, míg az AH nem.
5. Rajzoljon le egy két tűzfalas DMZ konfigurációt!