Kódolás és IT biztonság gyakorló

Total points 19/100

2022.-es évfolyam által készített gyakorló
Akiknek el lett küldve szeretném megkérni hogy ne észnélkül küldözgessék tovább :)

✓ A szoftver verifikációja során buffer overflow támadást intéz a rendszer ellen melyik biztonsági tesztelést hajtja épp végre ? 1/1

- (●) Penetrációs teszt ✓
- ( ) Sérülékenység tesztelés
- ( ) Statikus elemzés
- ( ) Dinamikus elemzés

✗ Mi lesz az int visszatérési értéke az alábbi függvénynek ha a következő paraméterekkel lesz meghívva ? (C vagy C++ nyelven) 0/1

```
a=INT-MIN
b=1
int subtract(int a ,int b){
   return a-b;
}
```

- (●) 1 ✗
- ( ) 0
- ( ) INT-MIN
- ( ) INT-MAX

Correct answer

- (●) INT-MAX

✗ A veszteségmentes tömörítés mindig ... 0/1

- (●) Mindig egynél kisebb tömörítést eredményez ✗
- ( ) Legfőbb felhasználási területe mindig a videókódolás
- ( ) lehetővé teszi hogy a tömörített adathalmazból tökéletesen visszaállítsuk az eredeti adathalmazt
- ( ) csak az adatok hálózaton keresztüli mozgatásánál fontos

Correct answer

- (●) lehetővé teszi hogy a tömörített adathalmazból tökéletesen visszaállítsuk az eredeti adathalmazt

✗ Mely elem nem része az aktuális OWASP top 10 listának? 0/1

- (●) Cross-side Scripting ✗
- ( ) Injection
- ( ) XML eternal entities
- ( ) Cross-Site Request Forgery

Correct answer

- (●) Cross-Site Request Forgery

✗ A PNG milyen arányú tömörítést ad? 0/1

- (●) 1:10 ✗
- ( ) 1:1
- ( ) 10:30
- ( ) 1:2

Correct answer

- (●) 1:1

✗ A VPN-ek arra valók hogy ... 0/1

- (●) Virtuális csomagkapcsolatokat hozzunk létre ✗
- ( ) Különböző hálózatokat úgy kössünk össze ,mintha egy hálózatba lennének
- ( ) Kókusztejet igyunk (ezt nem én találtam ki vicceskedésből , ez tényleg így volt a vizsgán)
- ( ) Képzetes virtuális forgalmakat szűrjünk

Correct answer

- (●) Különböző hálózatokat úgy kössünk össze ,mintha egy hálózatba lennének

✗ Az alábbi állítások közül melyik HAMIS? 0/1

- (●) A fejlesztőknek különböző korlátokkal kell szembe nézniük a fejlesztés során ✗
- ( ) A támadónak elég egyetlen sérülékenységet találnia, míg a fejlesztőnek mindenre figyelnie kell ahhoz, hogy a szoftver biztonságos legyen
- ( ) A programozás során használt rendszerek nem segítik a programozó munkáját
- ( ) Nehéz mérni a biztonságot

Correct answer

- (●) A programozás során használt rendszerek nem segítik a programozó munkáját

✗ Melyik programozási hiba NEM vezethet SQL injectiönhöz? 0/1

- (●) A bemenet egy string műveletekkel végzett feldolgozása ✗
- ( ) A bemenet hosszának nem megfelelő ellenőrzése
- ( ) A bemenet nem megfelelő escapelése
- ( ) Prepared statementek alkalmazásának elmulasztása

Correct answer

- (●) A bemenet hosszának nem megfelelő ellenőrzése

✗ Mi a tömörítési arány ? 0/1

- (●) Az eredeti fájl mérete osztva a tömörített fájl méretével ✗
- ( ) Az eredeti fájl méretének és a kódolási nyereségnek a szorzata
- ( ) Faktoriális alapú futamhossz kódolásnál (RLE) használt paraméter
- ( ) Tömörített fájl mérete osztva az eredeti fájl méretével

Correct answer

- (●) Tömörített fájl mérete osztva az eredeti fájl méretével

✗ Miért alkalmazunk SIEM megoldásokat ? 0/1

- (●) Kevesebb adatot kelljen az IDS-nek feldolgoznia ✗
- ( ) A hálozaton ne lehessen SQL Injection támadást végrehajtani
- ( ) Átlássuk a sok riasztást és megtaláljuk köztük a fontosakat
- ( ) Gyorsabban tudjon szűrni a csomagszűrű

Correct answer

- (●) Átlássuk a sok riasztást és megtaláljuk köztük a fontosakat

✗ Az alábbiak közül mit korlátoz a Same Origin Policy 0/1

- (●) Más szerverről származó kép megjelenítése ✗
- ( ) Más szerverről származó JavaScript függvény tartalmának a kiolvasása végrehajtáshoz
- ( ) Más szerverről származó stíluslap (stylesheet) alapján megjelenítés módosítása
- ( ) Egy Iframe URL mezőjének beállítása egy másik szerver címére

Correct answer

- (●) Más szerverről származó JavaScript függvény tartalmának a kiolvasása végrehajtáshoz

✗ Az alábbiak közül melyik lehet egy fajta kvantálás? 0/1

- (●) Matematikai kvantorok használata ✗
- ( ) Egy digitális kép reprezentálásához szükséges színek számának csökkentése
- ( ) Kvantum kriptográfiával kapcsolatos számítások
- ( ) Egy digitális kép reprezentálásakor használt szintér meghatározására

Correct answer

- (●) Egy digitális kép reprezentálásához szükséges színek számának csökkentése

✗ Célzott alkalmazásnál használt bináris malware minták elemzése segítségével... 0/1

- (●) A támadó kiléte szinte mindig kideríthető ✗
- ( ) Megakadályozható hogy adatot lopjanak a rendszerünkből
- ( ) Új kriptográfiai minták alkalmazására kaphatunk új ötleteket
- ( ) Felfedezhetőek a belejük kódolt vezérlőszervek nevei,vagy címei

Correct answer

- (●) Felfedezhetőek a beléjük kódolt vezérlőszervek nevei,vagy címei

---

✗ Az alábbiak közül melyik nem igaz ? 0/1
A publikus sérülékenységek

- (●) A kereshető adatbázisokban nyilvánosan elérhetőek ✗
- ( ) nyilvánosságra hozatala hátráltatja a védekezést mert a támadók számára is elérhetővé teszi a kihasználható hibák számát
- ( ) Hibás válasz 1 de nem látszódik a képen
- ( ) Hibás válasz 2 de nem látszódik a képen

Correct answer

- (●) nyilvánosságra hozatala hátráltatja a védekezést mert a támadók számára is elérhetővé teszi a kihasználható hibák számát

---

✓ Mi a hibajavító illetve detektáló képessége egy n=22 k=11 q=23 paraméterű reed solomon kódnak ? 1/1

- (●) 5,11 ✓
- ( ) 5,12
- ( ) 3,7
- ( ) Ehhez még tudni kéne a csatornázási hiba lehetőségét is

---

✗ Mit jelent a gyakorlatban, hogy egy jelszó saltolva tárolunk? 0/1

- (●) A jelszót egy, a FIPS-140 elvárasainak megfelelő titkosítóalgoritmussal titkosítjuk, majd az eredményt tároljuk. ✗
- ( ) Egy megfelelően választott egyiranyú függvényt alkalmazunk a jelszó és egy másik, felhasználó-specifikus véletlen érték megfelelő kombinációján, majd a függvény értékét tároljuk
- ( ) A jelszón egy megfelelően választott egyirányú függvényt alkalmazunk,majd ennek értékét tároljuk
- ( ) A jelszón egy megfelelően választott egyirányú függvényt alkalmazunk egymás után több ezerszer

Correct answer

- (●) Egy megfelelően választott egyiranyú függvényt alkalmazunk a jelszó és egy másik, felhasználó-specifikus véletlen érték megfelelő kombinációján, majd a függvény értékét tároljuk

---

✗ Mi a trójai malware ? 0/1

- (●) Olyan program amely magát átmásolva nagy hálózatokat támad meg ✗
- ( ) Olyan program, amely kártékony dolgokat csinál miközben rendes programnak álcázza magát
- ( ) Trójai falovakat installáló backsatter támadás
- ( ) Program amelyeknek célpontja görög célpontok támadása

Correct answer

- (●) Olyan program, amely kártékony dolgokat csinál miközben rendes programnak álcázza magát

---

✗ Az alábbi python modoluk közül melyikeket használná fuzzoláshoz? 0/1

- (●) dahuffman ✗
- ( ) pcryptodome
- ( ) tkinter
- ( ) python-afl

Correct answer

- (●) python-afl

✗ Az alábbiak közül melyik írja le a CBC kódolást ? 0/1

- (●) Opció: 1 ✗
- ( ) Opció: 2

Opció: 3

Opció: 4

Correct answer

Opció: 4

✗ Az alábbiak közül melyik növeli a biztonsági kockázatot ? 0/1

- Rendszeres biztonsági tesztelés ✗
- Kihasználható sérülékenységek
- Biztonsági mechanizmusok
- Biztonságtudatosság növelése

Correct answer

Kihasználható sérülékenységek

✓ Mit jelent a gyakorlatban, hogy egy jelszó tárolásánal stretchinget alkalmazunk? 1/1

- A tárolandó érték kiszámításakor a megfelelően választott és felparaméterezett egyiranyú függvényt nem egyszer, hanem egymás utan akár többszazezerszer hivjuk meg ✓
- A jelszón egy megfelelően választott egyiranyú függvényt alkalmazunk, majd a függvény értékét tároljuk.
- A jelszót egy, a FIPS-140 elvárasainak megfelelő titkositóalgoritmussal titkositjuk, majd az eredményt tároljuk.
- Egy megfelelően választott egyiranyú függvényt alkalmazunk a jelszó és egy másik, felhasználó-specifikus véletlen érték megfelelő kombinációján, majd a függvény értékét tároljuk

---

✓ Melyik nem igaz ? 1/1
Egy biztonsági kezelés során az ún. incidens fázisban történik ...

- Az incidenst lehetővé tevő sérülékenységek kijavítása ✓
- Az incidens kezelési stratégia kialakítása
- A bizonyítékok gyüjtése és elemzése
- A rendszer eredeti állapotba történő visszaállítása

✗ Az alábbiak közül melyik modern rejtjelező algoritmus? 0/1

- Enigma ✗
- Caesar
- RSA
- Szkütálé

Correct answer

RSA

Feedback

Ezt művészet nem eltalálni :)

✓ Az alábbiak közül melyik szoftverfejlesztéssel kapcsolatos döntés során jelenik meg a "least privilege" tervezési elv 1/1

- Az adatbázishoz való kapcsolódás során használt felhasználói fiók kialakításakor ✓
- Az alapértelmezett konfigurációs értékek kialakításakor
- A felhasználói dokumentációban a szoftver belső müködésével kapcsolatos információk részletezésénél
- A GUI-n található gombok elhelyezkedésének megtervezésekor

✓ Az alábbiak közül melyik számit leginkább észlelést célzó biztonsági mechanizmusnak ? 1/1

- Rootki detekció ✓
- Address Space Layout Randomization (ASLR)
- Rejtjelezés
- Tűzfal

A potyogós/Cascade/vienna vírusa 0/1

- [x] Aktivizálásakor emberek haltak meg
- [ ] Aktivizálásakor lepotyogtak a betűk a kijelzőn
- [ ] Aktivizálásakor falevelek estek le (első cyber-physical attack)
- [ ] Aktivizálásakor eljatszotta a PC buzzer-en a yankee docdle-t

Correct answer

- [x] Aktivizálásakor lepotyogtak a betűk a kijelzőn

Melyik forgalmat engedheti át az alábbi szűrű szabály? 0/1
src=10.10.10.0/24 dst=10.20.10.0/24 sport=any dport=380 ALLOW

- [x] A 10.20.10.0/24 hálózatban lévő webszerverek felől érkező adatforgalmat
- [ ] A 10.20.10.0/24 hálózatban lévő webszerverek felé menő adatforgalmat
- [ ] Ez a szabály nem enged át semmilyen forgalmat
- [ ] Egy cég publikus szerverére érkező forgalmat

Correct answer

- [x] A 10.20.10.0/24 hálózatban lévő webszerverek felé menő adatforgalmat

Mit jelent 'padding' CBC mód esetén? 0/1

- [x] Azt jelenti hogy minden üzenetet egyforma méretűvé alakítunk extra bájtok hozzáadásának segítségével
- [ ] Azt jelenti hogy egy üzenet végéhez annyi extra bájtot fűzünk hogy az üzenetnek a hossza a blokkszám egész számú többszöröse legyen
- [ ] Azt jelenti hogy nyílt üzenethez egy vele megegyező hosszúságú véletlenszerű XOR-olunk rejtjelezés előtt
- [ ] A nyílt üzenetek blokkokra osztását jelenti rejtjelezés előtt

Correct answer

- [x] Azt jelenti hogy egy üzenet végéhez annyi extra bájtot fűzünk hogy az üzenetnek a hossza a blokkszám egész számú többszöröse legyen

Az alábbiak közül melyik tudásalapú (knowledge-based) authentikációs megoldás 0/1

- [x] SMS-ben adott tokenek használata
- [ ] PIN kódok használata
- [ ] Telefonos Authenticátor alkalmazások használata
- [ ] Arcfelismerő alkalmazások használata

Correct answer

- [x] PIN kódok használata

Milyen alkalmazási területen használnuk tipikusan veszteségmentes (loss-less) tömörítést 0/1

- [x] Szimmetrikus kulcsú rejtjelezésnél
- [ ] Számítógépen tárolt fájlok méretének csökkentésére
- [ ] Videókódolásnál streaming céljából
- [ ] MP3 szabványú zeneszámok esetén

Correct answer

- [x] Számítógépen tárolt fájlok méretének csökkentésére

Kinek a jogosultságával fog futni az alábbi kód ha én (gergő ládi) probálom meg elindítani? 0/1
-rwsr-xr-x 8 bob alice 220k Oct 24 13:37 program

- [x] Senkiével mert nincs jogom hozzá
- [ ] Bob
- [ ] Alice
- [ ] Gergő Ládi

Correct answer

- [x] Bob

Hogyan határozzuk meg a veszteséges tömörítés esetén a veszteség mértékét ? 0/1

- (●) Forrástípusonként azon statisztikai tulajdonsága alapján meghatározott standard táblázatokban publikált formulák (sourced stat)felhasználásával ✗
- ( ) Videó és kép esetén sajnos nincsen még általánosan elfogadott módszer
- ( ) A tömörítő algoritmusokhoz tartozó tömörítési torzítás képlet alapján számoljuk
- ( ) Szubjektív érzékelési tesztek alapján kerül meghatározásra

Correct answer

- (●) Szubjektív érzékelési tesztek alapján kerül meghatározásra

✗ Mi az IV-vel támasztott fő követelmény CBC kódolás esetén? 0/1

- (●) Az IV hosszabb kell legyen mint a kulcs ✗
- ( ) Az IV-t a kulcsból kell származtatni
- ( ) Az IV értéke nem prediktálható(megjósolhatatlan) kell hogy legyen
- ( ) Az IV értéke titkos kell hogy legyen

Correct answer

- (●) Az IV értéke nem prediktálható(megjósolhatatlan) kell hogy legyen

✗ Mit jelent a három 'A' betű az 'AAA' betűszóban 0/1

- (●) Access control, alteration, administration ✗
- ( ) Authentication, authorization, accounting
- ( ) Authorization, access control, accounting
- ( ) Authentication, access control, administration

Correct answer

- (●) Authentication, authorization, accounting

✗ Mi a CVE ? 0/1

- (●) Elektromos autók sérülékenységének kihasználására egy technika ✗
- ( ) Egy online platform kritikus sérülékenységek tesztelésére
- ( ) Egy paraméter az operációs rendszerben amivel ellenőrizhetjük a jelenleg használt virtuális környezetet
- ( ) Egy adatbázis ami minden ismert sérülékenységet tartalmaz

Correct answer

- (●) Egy adatbázis ami minden ismert sérülékenységet tartalmaz

✗ Miért előnyös nem-egyenletes kvantálás használata JPEG algoritmusban ? (Válassza ki az igaz állítást) 0/1

- (●) Egyáltalán nem előnyös , mert ezzel tipikusan ronthatnánk a tömörítési arányon (ezért használnánk egyenletes kvantálót) ✗
- ( ) Azért ,mert ezzel finomabban meg lehet jeleníteni egy kép fontosnak számító tartalmi részét
- ( ) Azért, mert az alacsony térfrekvencias komponenseket finomabb felbontasban kell kvantalni, lévén a érzékelésünk (szemünk) erre érzékenyebb, mint a maqas frekvenciás komponensekre
- ( ) Az ok az hogy ezzel tudjuk optimálisan illeszteni a DCT transzformációt a ZIG-ZAG scan transzformációhoz

Correct answer

- (●) Azért, mert az alacsony térfrekvencias komponenseket finomabb felbontasban kell kvantalni, lévén a érzékelésünk (szemünk) erre érzékenyebb, mint a maqas frekvenciás komponensekre

✗ Miért hasheljük az üzenetet digitális aláírás előtt ? 0/1

- (●) Így rövidebb aláíró kulcs is elegendő ✗
- ( ) Így az aláírás mellett egyben rejtjelezzük az üzenetet
- ( ) Így nehezebb az aláírás hamisítása
- ( ) Így gyorsabb az alárírás kiszámítása

Correct answer

- (●) Így gyorsabb az alárírás kiszámítása

✗ Melyik védelem a legkevésbé hatékony XSS támadással szemben ? 0/1

- (●) HTTP only Cookie beállítása ✗
- ( ) CSP alkalmazása
- ( ) Whitelist alapú input validálás
- ( ) Blacklist alapú input validálás

Blacklist alapú input validálás

Correct answer

Blacklist alapú input validálás

✓ Mire használatos a CHMOD parancs? 1/1

- [x] Modosíthatjuk vele egy fájl jogosultsági bitjeit
- [ ] Átállítja a wifi adapter által használt aktuális csatorna módot
- [ ] Felhasználói módok között válthatunk vele
- [ ] Root jogosultságot adhatunk vele a felhasználóknak és vehetünk el tőlük

✗ Egy memória korrupciós hibát milyen hibaként detektál általában a LINUX rendszer ? 0/1

- [x] Memória hiba (memory error)
- [ ] Hozzáférési Hiba (Access violation)
- [ ] Szegmenciós hiba (segmentation fault)
- [ ] Végrehajtási hiba (execution error)

Correct answer

Szegmenciós hiba (segmentation fault)

✗ Mi az ASLR alapötlete? 0/1

- [x] A visszatérési címek ellenőrzése minden egyes függvényhívás végén
- [ ] A különböző szegmensek helyének elmozdítása a memóriában
- [ ] A memória titkosítása
- [ ] A kernel írhatóságának a letiltása

Correct answer

A különböző szegmensek helyének elmozdítása a memóriában

✗ Az alábbiak közül melyik szoftvertervezéssel kapcsolatos tervezés folyamán jelenik meg a psychological acceptability tervezési elv 0/1

- [x] A felhasználói dokumentációban a szoftver belső müködésével kapcsolatos információk részletezésénél
- [ ] Az adatbázishoz való kapcsolódás során használt elérési cím meghatározásakor
- [ ] A felhasználói jelszavak biztonsági szabályzatának kidolgozásakor
- [ ] Az alapértelmezett konfigurációs értékek kiszámításakor

Correct answer

A felhasználói jelszavak biztonsági szabályzatának kidolgozásakor

✓ Mi a Zig-zag scan feladata a JPEG kódolásnál ? 1/1

- [x] Sorba rendezi a DCT transzformáció outputjának frekvenciakomponenseit olyan módon hogy az alacsony és magas frekvencia komponensek szeperálódjanak a kiemeneti scan vektorába
- [ ] A pixelek kvázi-random elrendezésével hatékonyabban tudunk tömöríteni mert ezzel növeljük a DPCM kódoló bemeneti entrópiáját
- [ ] Hibás válasz 1 nem látszódik a képen
- [ ] Hibás válasz 2 nem látszódik a képen

✗ Egy célzott támadásban APT használt domainek vizsgálatával... 0/1

- [x] Mindig megtalálható az igazi támadó és így jogi eljárás indítható ellene
- [ ] További Domaineken át további vezérlőszervereket fedezhetünk fel
- [ ] Megakadályozhatjuk az adatok tömeges ellopását
- [ ] Törölni tudjuk az ellopot adatokat a támadó szerveréről

Correct answer

További Domaineken át további vezérlőszervereket fedezhetünk fel

✗ Az alábbiak közül melyik az Incident Response Team feladata? 0/1

- [x] A bejelentett bughoz tartozó kódrészek vizsgálata
- [ ] A bejelentett buhoz tartozó patch implementálása
- [ ] A hírek folyamatos követése

Az elkészült patch tesztelése

Correct answer

A hírek folyamatos követése

✗ Mi igaz egy állapot alapú szűrű működésére 0/1

A SYN-SYN/ACK+ACK csomagok után a kapcsolat kikerül a kapcsolat tablaból ✗

A sikeres FIN csomag utan a kapesolat bekerül a kapcsolat táblába.

Az RST csomag után a kapcsolat tábla alaphelyzetbe áll (teljes tartalma törődik)

A SYN-SYN/ACK+ACK csomagok után a kapcsolat bekerül a kapcsolat táblába

Correct answer

A SYN-SYN/ACK+ACK csomagok után a kapcsolat bekerül a kapcsolat táblába

---

✗ Hogyan definiáljuk a biztonsági kockázatot ? 0/1

Fenyegetések szorozva a sérülékenységekkel ✗

Támadási felület mérete szorozva potenciális veszteség

Sikeres támadás valószínűsége szorozva a támadás impaktjával

Potenciális veszteség osztva a támadási elleni intézkedések hatékonyságával

Correct answer

Sikeres támadás valószínűsége szorozva a támadás impaktjával

✗ A szoftvere sérült bemeneti adatot érzékel , hogyan kezelje a szoftver a helyzetet ? 0/1

A szoftvernek meg kell probálnia helyreállítani az adatot ✗

A szoftvernek így is végre kell hajtania a leprogramozott számításokat

A szóftvernek naplóznia kell a sérült bemeneti adatot

A bemeneti adatot vissza kell utasítani és az eseményt naplózni kell

Correct answer

A bemeneti adatot vissza kell utasítani és az eseményt naplózni kell

---

✗ Mire alkalmas egy CRC kód ? 0/1

Tömörítés ✗

Hibajavítás

Törölt karakterek visszaállítása

Hibadetektálás

Correct answer

Hibadetektálás

✗ Az alábbi kockázatok közül melyikkel NEM foglalkozik az IT biztonság? 0/1

Adatok illetéktelen módosítása ✗

IT rendszer altal nyújtott szolgaltatasok elérhetetlenné tétele

Véletlen hardware hibak előfordulasa

Adatokhoz történő illetéktelen hozzáférés

Correct answer

Véletlen hardware hibak előfordulasa

✗ Melyek a kiberbűnözői csoport jellemzői ? 0/1

Limitált technikai képességek, limitált erőforrás szerző képesség ,erős erőforrások ✗

Fejlett technikai képességek ,fejlett információ szerző képesség ,limitált erőforrások

Fejlett technikai képességek ,fejlett információ szerző képesség ,erős erőforrások

Változó technikai képességek, limitált információ szerző képesség,limitált erőforrások

Correct answer

Fejlett technikai képességek ,fejlett információ szerző képesség ,erős erőforrások

---

✗ Mi a számítógépes vírus ? 0/1

- (●) Olyan program ami másnak adja ki magát mint amit végez ✗
- ( ) Automatizálható hibakihasználó szoftver , amely hibát kihasználva másolja magát
- ( ) Olyan kód ami másnak adja ki magát mint amit elvégez , de ártó szándékú kódolást végez
- ( ) Önreprodukáló számítógépes kód , önmagában életképtelen , terjedni képes

Correct answer

- (●) Önreprodukáló számítógépes kód , önmagában életképtelen , terjedni képes

✓ A statikus elemzés hátránya hogy ... 1/1

- (●) Elemzés során nincs futásidejű információnk ✓
- ( ) Alacsony kód lefedettséget biztosít
- ( ) Nehéz a kódban mélyen elhelyezkedő utasításokat elemezni
- ( ) csak jól ismert sérülékenységeket képes megtalálni

✓ Mi az a BLIND SQL Injection? 1/1

- (●) Olyan támadás aminek az eredménye nem közvetlenül látható a támadó számára ✓
- ( ) Amikor a támadó véletlenszerűen tudja csak módosítani az SQL lekérést
- ( ) Amikor az SQL lekérést csak egy köztes (PROXY) feldolgozó segítségével tudja módosítani
- ( ) Egy gyengén látók számára kifejlesztett segédalkalmazás SQL Injectionhöz

✓ Ha egy olyan MAC függvényt használunk melynek kimenete 16 bites és kulcsa 128 bites akkor hány probálkozás után tud egy nyers erőt (brutal force) alkalmazó támadó érvényes MAC címet generálni 1/1

- (●) Átlagosan 2^15 ✓
- ( ) Átlagosan 2^15*2^127
- ( ) Átlagosan 2^15+2^127
- ( ) Átlagosan 2^127

✗ Mit mond az economy of mechanism tervezési elv? 0/1

- (●) Az implementált biztonsági felügyeleti mechanizmusok költségeit figyelembe kell venni a tervezés során ✗
- ( ) Az implementációt a számunkra legegyszerűbb nyelven készítsük el
- ( ) A szoftver legyen kicsi és egyszerű
- ( ) Minnél kisebb legyen a kódbázis

Correct answer

- (●) A szoftver legyen kicsi és egyszerű

✗ Mi az (n,k,dmin) paraméter hármasa annak a kódnak amely tartalmaz minden páros paritású 10 bites szót ? 0/1

- (●) (10,9,4) ✗
- ( ) Ennyi adatból NEM lehet meghatározni
- ( ) (10,8,4)
- ( ) (10,9,2)

Correct answer

- (●) (10,9,2)

✗ Mi az a Stafford canary ? 0/1

- (●) A stack canary egy speciális fajtája , amikor nem véletlen értéket helyezünk a stackre hanem egy Stafford prímet ✗
- ( ) Függvényhíváskor a stacken elhelyezett érték ,melyet visszatéréskor ellenőriz a program
- ( ) Egy madárfajta , alakkanárik családjából
- ( ) A stackoverflow elleni védekezés elenni egyik módszer

Correct answer

- (●) Egy madárfajta , alakkanárik családjából

✓ Mi nem igaz a Content Security Policy-vel kapcsolatban 1/1

- (●) Használata inkompatibilis problémákat okozhat ✓

Egy whitelist alapú megközelítést kell használni a megközelítés során

Az alapértelmezett HTTP viselkedése , hogy nem engedi a beágyazott scripteket futni

Egy HTTP headerben célszerű küldeni a szerver oldal felől a kliens oldal számára

✗ A buffer overflownak (puffer túlcsordulásnak) melyik egy konkrét alesete? 0/1

- (●) code overflow (kód túlcsordulás) ✗
- ( ) stack overflow (stack túlcsordulás)
- ( ) memory overflow (memória túlcsordulás)
- ( ) kernel overflow (kernel túlcsordulás)

Correct answer

- (●) stack overflow (stack túlcsordulás)

✓ Melyik zóna NEM létezik egy válalkozási hálozatban? 1/1

- (●) Security ✓
- ( ) Internal
- ( ) External
- ( ) DMZ

✗ Mit nevezünk hash ütközésnek ? 0/1

- (●) Mikor találunk egy olyan üzenetet aminek hash értéke egy előre adott érték ✗
- ( ) Egy hash érték visszafejtésénel algoritmusát
- ( ) Két üzenetet melynek megegyező a hash értéke
- ( ) Két üzenetet melyeknek ellentmondó a tartalma

Correct answer

- (●) Két üzenetet melynek megegyező a hash értéke

✓ Hogyan optimalizal a Huffmann kódolas? Válassza ki az igaz állitast! 1/1

- (●) A kódoló Itteraciós lépésekben halad, egy fat épit levelektől a gyökér felé haladva, ahol egy lépésben a pillanatnyilag tekintett részgráfon összevon két csomópontot, amelyre irt gyakoriságok összege a legkisebb lehetséges értékű ✓
- ( ) A Huffmann kódolas bináris inputon dolgozik és ügy tömőrit, hogy kettonél hosszabb 0 bit futamokat egy a hosszuknak megfelelő decimalis karakterrel helyettesiti.
- ( ) A különböző bemeneti karaktereket azok csökkenő relatív gyakorisága szerint sorba rendezi, majd igy rendel hozzajuk kódszavak, hogy sorban egymas utaén veszi a abinaris stringeket növekvő hossz szerint, azaz a hozzarendelt kodszavak sora 0,1,00,01,10,11,000, 001....
- ( ) A kódoló a binaáis outputjaban a 0 és 1 bitek relativ gyakorisagat igyekszik 1/2 körüli értéken tartani, mert ez jelenti a véletlenszerű kimenetet, ami egyben a redundacia sikeres eltavolitását is jelzi.

✗ Mit nevezünk hibrid rejtjelezésnek ? 0/1

- (●) Amikor asszimetrikus kulcsú rejtjelezés mellet digitális aláirást is számolunk ✗
- ( ) Amikor szimmetrikus kulcsú rejtjelezés mellett MAC-et is számolunk
- ( ) Az adatot asszimetrikus kulcsú rejtjelezéssel kódoljuk és ennek a kulcsát rejtjelezzük szimmetrikus rejtjelezővel
- ( ) Az adatot szimetrikus kulcsú rejtjelezéssel kódoljuk és ennek a kulcsát rejtjelezzük asszimmetrikus rejtjelezővel

Correct answer

- (●) Az adatot szimetrikus kulcsú rejtjelezéssel kódoljuk és ennek a kulcsát rejtjelezzük asszimmetrikus rejtjelezővel

✗ Melyik felhasználó jogosultságával fog futni az alábbi program ha én Gergő Ládi probálom elindítani ? 0/1

```
-rwxr-sr-x 8 bob alice 220k Oct 24 13:37 program
```

- (●) Bob ✗
- ( ) Gergő Ládi
- ( ) Senkiével
- ( ) gergo.ladi

Correct answer

- (●) gergo.ladi

✗ Miért használunk szimmetrikus és asszimmetrikus kulcsú rejtjelezést is egyszerre hibrid rejtjelezés esetén? 0/1

- (●) Mert így egyszerre biztosítható hogy az adat titokban maradjon és a forrása hiteletsíthető legyen ✗
- ( ) Mert a dupla rejtjelezés dupla biztonságot jelent
- ( ) mert így gyorsabban tudunk nagy méretű adatot rejtjelezni
- ( ) Mert elméletileg nem lehetséges kulcsméretnél nagyobb méretű adat rejtjelezése

Correct answer

- (●) mert így gyorsabban tudunk nagy méretű adatot rejtjelezni

✗ Melyik nyelvet nem éríniti az integer túlcsordulás? 0/1

- (●) C/C++ ✗
- ( ) C#
- ( ) JAVA
- ( ) Python

Correct answer

- (●) Python

✗ Rejtjelező kódolás esetén a támadóról azt feltételezzük hogy... 0/1

- (●) Nem ismeri a kódolás algoritmusát,ezért nem tud dekódolni ✗
- ( ) nem ismeri a dekódoló kulcsot ezért nem tud dekódolni
- ( ) A csatornába megjelenő rejtjelező üzenteket módosítani tudja
- ( ) Meg tudja figyelni a csatornán átküldött rejtjelezett üzenetet

Correct answer

- (●) Meg tudja figyelni a csatornán átküldött rejtjelezett üzenetet

✗ Mit hívunk veszteséges tömörítésnek ? 0/1

- (●) Ha hashelünk ✗
- ( ) Ha a tömörítés során az adat egy részét eldobjuk
- ( ) Ha a titkosítás után nem tudjuk kititkosítani az üzenetet
- ( ) Ha a tömörítési algoritmusnak nincs inverze

Correct answer

- (●) Ha a tömörítés során az adat egy részét eldobjuk

✓ Milyen célt szolgál egy kriptográfiai hash függvény ? 1/1

- (●) Üzenet lenyomat számítás ✓
- ( ) Gyors keresés , rejtjelezés
- ( ) Üzenethitelesítés
- ( ) Integritásvédelem

✗ Hogyan kezeljük a kriptográfiai kulcsokat egy alkalmazásban? 0/1

- (●) Mindig akkor generáljuk őket mikor szükség van rájuk az alkalmazásban ,majd használat után rögtön töröljük is őket ,így sosem kerül tárolásra semmilyen formában ✗
- ( ) Mindig a jelszóból generáljuk őket pl úgy hogy a jelszót egyszerűen le hasheljük a SHA-256 függvénnyel
- ( ) Belekódoljuk őket az alkalmazásba így nem kell őket fájlba menteni és a háttértáron tárolni,ahol esetleg elérhető lenne a támadó számára
- ( ) Sosem kódoljuk őket bele az alkalmazásba, hanem beolvassuk őket egy jelszóval védett fájlból vaagy egy beírt jelszóból generáljuk

Correct answer

- (●) Sosem kódoljuk őket bele az alkalmazásba, hanem beolvassuk őket egy jelszóval védett fájlból vaagy egy beírt jelszóból generáljuk

✗ Kérdés 0/1

Tekintsük a

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \end{pmatrix}$$

generátor mátrixú, mod 7 aritmetikájú Reed-Solomon kódot. Mi az m=(4,2) üzenethez tartozó kódszó? Válassza ki az igaz állítást!

- (●) (6,3,1,3,4,0) ✗
- ( ) (3,4,0,1,2,6)
- ( ) (6,3,1,2,5,0)

(5,3,2,4,1,6)

Correct answer

(6,3,1,2,5,0)

✓ Milyen programozási hibát használ ki a puffer túlcsordulás ? 1/1

- ✓ A program nem ellenőrzi, hogy mennyi adatot ír egy adott pufferbe
- A program hivatkozik egy már felszabadított puffer területre
- A program a puffer indexét addig növeli amíg az átfordul negatív értékbe és így kicímez a pufferből
- A programban memóriaszivárgás van, nem szabadít fel minden területet

✗ Mi igaz egy állapot alapú szűrűre? 0/1

- ✗ Jól lehet vele videótartalmak alapján szűrni
- Jelentősen gyorsítja a forgalmat
- Egy csomagról való döntést befolyásolhat a megelőző forgalom
- Jelentősen lassítja a forgalmat

Correct answer

Egy csomagról való döntést befolyásolhat a megelőző forgalom

✗ Az alábbiak közül melyik írja le helyesen a CBC módban történő blokkrejtjelezést 0/1

- ✗ Opció: 1 — $Y_i = E_K(X_i) \text{ XOR } Y_{i-1}$
- Opció 2 — $X_i \text{ XOR } Y_{i-1}$
- 3 — $Y_i = X_i \text{ XOR } E_K(Y_{i-1})$
- Opció: 4 — $Y_i = X_i \text{ XOR } E_K(Y_{i-1})$

Correct answer

Opció: 4

✗ Mi lehet az eredménye az alábbi szabálynak : 0/1

src=any dst=1.2.3.4 sport=any dport=80 DROP

- ✗ Minden forgalmat eldob
- A webszerver felé menő forgalmat átengedi
- A webszerver felől jövő forgalmat átengedi
- A webszerver felé menő forgalmat tiltja

Correct answer

A webszerver felé menő forgalmat tiltja

✗ Az alábbiak közül melyik egy valid séma (scheme) ? 0/1

- ✗ #comment
- php://
- ?article=1&x=3
- example.com:80

Correct answer

php://

✗ Sztereo hangfelvételt tömöritünk 64 kbit/sec tömöritett sebességre. A mintavételi frekvencia 44.1 kHz, egy mintat 16 biten ábrázolunk. Mekkora tömöritési arányt (R) értünk el? Valassza ki az igaz allitast! 0/1

- (●) R=0.5 ✗
- ( ) R < 0.02
- ( ) R > 0.14
- ( ) R=0.045

Correct answer

- (●) R=0.045

✗ Az alábbiak közül melyik birtokalapú (possesion-based) authentikációs megoldás 0/1

- (●) Újlenyomat alapú azonosítás használata ✗
- ( ) Tokengenerátor használata
- ( ) PBKDfV használata
- ( ) PIN-kód használata

Correct answer

- (●) Tokengenerátor használata

✗ Milyen előnyös tulajdonsága van egy hoszt alapú IDS-nek ? 0/1

- (●) Megtudja állítani a kártékony forgalmakat a hálózat határán ✗
- ( ) Elég egy példányt telepíteni belőle a hálózatba
- ( ) Visszajátszásos támadások ellen hatékonyan működik
- ( ) Bele tudok nézni a titkosított forgalomba

Correct answer

- (●) Bele tudok nézni a titkosított forgalomba

✗ Mi történik stackoverflow esetén ? 0/1

- (●) Elfogy a memória (betelik a stack) ✗
- ( ) Nem várt módon felülíródik a stack egy része
- ( ) Felülíródik egy függvény visszatérési értéke a stacken
- ( ) Nagy adatot írunk a stackre ezért felülírja a heap tetejét
- ( ) Bejelentkezünk a stackoverflow.com-ra

Correct answer

- (●) Nem várt módon felülíródik a stack egy része

✗ Egy alkalmazás szintű szűrőre nem igaz hogy 0/1

- (●) Lassítja a forgalmat ✗
- ( ) Az erőforrás igénye elhanyagolható
- ( ) Tud kiszűrni videó tartalmakat
- ( ) Tud meglátogatott URL-je alapján szűrni

Correct answer

- (●) Az erőforrás igénye elhanyagolható

✗ Mikor ajánlott JPEG formátum használata ? 0/1

- (●) Vektorgrafikus képeknél ✗
- ( ) Sok szöveget tartalma képeknél
- ( ) Digitális fényképek , festmények képei és valósághű képek esetén
- ( ) Sokszor szerkesztett képek esetén

Correct answer

- (●) Digitális fényképek , festmények képei és valósághű képek esetén

✗ Az alábbiak közül melyik lesz legnagyobb esélyel egy átlagos felhasználó azonosítója (UID-je) LINUX rendszerben 0/1

- (●) 0 ✗
- ( ) 1024
- ( ) S-1-5-21 -20521 11302-1767777339-725345543-11337
- ( ) bf70023a-876-4c44-9ba1-61 6bac57f399

Correct answer

1024

Feedback

Bármi ami nagyobb mint 1000 és egész szám

✗ Bináris szimmetrikus csatornát tekintünk ahol a hibázás valószínűsége 0,5 az n=3 kódszóhosszú ismétléses kódot használjuk hibadetekcióra Mennyi a valószínűsége hogy a detektáljuk az átvitel során ?? 0/1

- (●) 1/4 ✗
- ( ) 1/8
- ( ) 3/4
- ( ) 7/8

Correct answer

- (●) 7/8

✓ Milyen tulajdonságot garantál az NX bit (DEP) bekapcsolása 1/1

- (●) A stack szegmens nem lesz futtatható ✓
- ( ) A heap szegmens nem lesz olvasható
- ( ) A kód szegmens nem lesz írható
- ( ) A kernel szegmenshez semmilyen hozzáférés nem lesz engedélyezve

---

✗ Mi jellemzi a Zero-day sérülékenységeket 0/1

- (●) Ezek publikusan jól ismert sérülékenységek ✗
- ( ) Ezek nem publikus de a támadó által jól ismert sérülékenységek
- ( ) Ezek 1 napnál kevesebb idő alatt felfedezhető sérülékenységek
- ( ) Ezek minimális erőfeszítéssel gyorsan javítható sérülékenységek

Correct answer

- (●) Ezek nem publikus de a támadó által jól ismert sérülékenységek

---

✗ Mekkora a kimerítő kulcskeresés támadás átlagos komplexitása k bites kulcs esetén ? 0/1

- (●) k^2 ✗
- ( ) 2^k
- ( ) 2^k/2
- ( ) 2^k-1

Correct answer

- (●) 2^k-1

✗ A DEFLTATE algoritmus azért hatékony mert 0/1

- (●) A GZIP-ben ezt használják ✗
- ( ) Kombinálja a futamhosszt és a Huffman kódolást
- ( ) Veszteséges tömörítést valósít meg
- ( ) Soha nem eredményez 1-nél nagyobb tömörítési arányt

Correct answer

- (●) Kombinálja a futamhosszt és a Huffman kódolást

✗ Egy hálozati IDS-nek az előnye 0/1

- (●) A forgalom manipulálása nélkül tudja vizsgálni a titkosított forgalmakat ✗
- ( ) Kisimítja a hálozati késleltetés ingadozását
- ( ) A hálózat határán megtudja találni a kártékony tartalmakat
- ( ) Megkönnyíti a virtuális magánhálozatok

Correct answer

- (●) A hálózat határán megtudja találni a kártékony tartalmakat

---

✗ Az alábbi állítások közül melyik hamis ? 0/1

- (●) A biztonsági ellenintézkedések célja a sérülékenységek elmininálása ✗

Az IT rendszerek üzemeltetőinek alapvető célja a támadók azonosítása , mert a támadók felszámolásával lehet a leghatékonyabban védekezni a támadásokkal szemnben

Az IT rendszerekben található sérülékenységek a rendszer kompromitálásához vezethetnek

Az IT rendszerek elleni támadások mindig valamilyen sérülékenységet használnak ki

Correct answer

Az IT rendszerek üzemeltetőinek alapvető célja a támadók azonosítása , mert a támadók felszámolásával lehet a leghatékonyabban védekezni a támadásokkal szemnben

✗ Az alábbiak közül melyik lehet egy felhasználó biztonsági azonosító SID-je windows rendszerben ? 0/1

0

bf70023a-876-4c44-9ba1-61 6bac57f399

102

S-1-5-21 -20521 11302-1767777339-725345543-11337

Correct answer

S-1-5-21 -20521 11302-1767777339-725345543-11337

✓ Melyik nyelvi tulajdonsága miatt lehet veszélyes a Javascript? 1/1

Felhasználó által okozott esemény és a javascript által okozott esemény gyakorlatilag egyenértékű

Minden objektum örököl egyet a globális prototipusból

A nyelvet kb 10 nap alatt fejlesztették ki

Minden változó globális scope-al rendelkezik

✗ 0/1

Tekintsük a $G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$ generátormátrixú Hamming kódot. Mi az $m=(1101)$ üzenethez tartozó kódszó? Válassza ki az igaz állítást!

1100100

1100101

1101100

1011100

Correct answer

1101100

✗ Mi a futamhossz kódolása az alábbi stringnek 0, 0,0,0,0 7,2,3,0,0,0,0,0 ,1,1? 0/1

({5,4},10) ({0,2},10)

({5,7},111) ({0,2},10)

({5,3},111) ({0,2},10)

({5,3},0111) ({1,1},0)

Correct answer

({5,3},111) ({0,2},10)

✓ Milyen szolgáltatást nyújt a MAC függvény ? 1/1

A MAC sikeres ellenőrzése esetén a vevő tudja, hogy az üzenet sértetlen és olyan valaki küldte aki ismeri a kulcsot

A MAC sikeres ellenőrzése esetén a vevő tudja, hogy az üzenet korábban keletkezett mint a MAC kulcs

A MAC egy olyan blokkrejtjelező mód ami egy üzenetben egy rejtjelezést biztosít

A MAC egy olyan függvény ami egy letagadhatatlan hash értéket állít elő

✗ Mik a célzott támadás jellemzői ? 0/1

Célpont nem véletlenszerűen választott ,ismert támadó eszközök használata

Célpont véletlenszerűen választott ,testreszabott támadó eszközök használata

Célpont véletlenszerűen választott ,ismert támadó eszközök használata

Célpont nem véletlenszerűen választott ,testreszabott támadó eszközök használata

Correct answer

Célpont nem véletlenszerűen választott ,testreszabott támadó eszközök használata

✕ Mi az adattömörítés célja ?
Válassza ki az igaz állítást

0/1

- (●) Képek , videók tömörítése során a tömörítő algoritmus csak a tartalom szempontjából releváns információt tartja meg ✕
- ( ) Az adattárolokon való tároláskor kevesebb átlagos bithiba várható ha kisebb méretre tömörítjük az adatfájlt
- ( ) A redundancia csökkentése támogatja a biztonságosabb rejtjelezést privát adatfájl esetén
- ( ) Kisebb bit/sec sebességű képességű komunikációs csatornán tudjuk képek egy halmazát adott idő alatt továbbítani

Correct answer

- (●) Kisebb bit/sec sebességű képességű komunikációs csatornán tudjuk képek egy halmazát adott idő alatt továbbítani

✕ A Kerchkoff-elv azt mondja ki hogy ...

0/1

- (●) A támadóról érdemes azt feltételezni hogy előbb utobb hozzáférhet a dekódoló kulcshoz ✕
- ( ) A rejtjelező algoritmusoknak mindig lehetnek algebrai gyengeségei
- ( ) A támadóról érdemes azt feltételezni hogy hozzájuthat ismert nyílt-szöveg rejtett szöveg párokhoz
- ( ) A támadóról érdemes feltételezni hogy ismerheti a dekódoló algoritmust

Correct answer

- (●) A támadóról érdemes feltételezni hogy ismerheti a dekódoló algoritmust

✕ Tudjuk hogy A XOR 0011=1001 Mennyi a értéke ?

0/1

- (●) 1100 ✕
- ( ) 1010
- ( ) 0001
- ( ) 1011

Correct answer

- (●) 1010