



ECDL
Magyarország



ECDL **VIZSGAPÉLDATÁR**

IT biztonság

Syllabus 1.0

www.ecdl.hu

IT BIZTONSÁG

A IT BIZTONSÁG MODUL TARTALMA

A modul 30 feladatot tartalmaz. Közülük egyet kell megoldani. A feladatok megoldása során előre elkészített fájlokat kell használni, amelyeket a vizsgaközpont tesz elérhetővé a vizsgázó számára.

ÁLTALÁNOS IRÁNYELVEK A MEGOLDÁSHOZ ÉS A JAVÍTÁSHOZ

A vizsgán csak akkreditált szoftvert lehet használni, egyéb programok használata nem megengedett.

Az elméleti kérdések megválaszolására a vizsgaközpont által megadott válasz-fájlt kell használni.

A vizsgaközpont a feladatokban szereplő meghajtó-, könyvtár- (mappa-), fájlnev hivatkozásokat és sűgótémákat másra cserélheti, amennyiben ezt a feladat megoldhatósága indokoltta teszi. Hasonlóan kell eljárni az adott környezetben nem értelmezhető megnevezésekkel is.

Nyomtatáskor az alapértelmezés szerinti, vagy a vizsgaközpont által megjelölt nyomtatót kell használni.

A központ fájlba történő nyomtatást is kérhet, ilyenkor a megadott helyen és névvel kell létrehozni a fájlt.

A feladatlapok végén olvasható „Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.” utasítást a vizsgaközpont érvényben hagyhatja vagy törölheti saját igényének, illetve a feladatlap javíthatóságának megfelelően.

Az egyes részfeladatokra 1 pont adható. A pontszámok nem oszthatók.

Az elérhető maximális pontszám: **32**.

A sikeres vizsgához a vizsgázónak legalább **24** pontot kell megszereznie.

A vizsgázó által megoldott vizsgafeladatot a vizsgáztató a nemzetközileg meghatározott irányelveknek megfelelően értékeli.

A vizsgán semmilyen segédeszköz nem használható.

A vizsgafeladat megoldásához a rendelkezésre álló idő 45 perc.

(Az „Általános irányelvek a megoldáshoz és a javításhoz” című részt a vizsga megkezdése előtt a vizsgázónak meg kell kapnia.)

1. FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
- 1.1. Melyik tevékenység kiberbűnözés?
- bedarálás
 - adathalászat
 - etikus hackelés
 - titkosítás
- 1.2. Mit jelent a "hackelés" fogalma?
- az adatokhoz való jogosulatlan hozzáférés megszerzése
 - félrevezetni a személyazonosságunkról valakit az interneten
 - vírusirtóval eltávolítani az összes rosszindulatú szoftvert a gépünkről
 - számítógépeket lopni az épületbe való betöréssel
- 1.3. Melyik jelent „vis maior” fenyegetést az adatokra?
- emberi tevékenység
 - adatlopás
 - tűz
 - vírusok
- 1.4. Mi a személyes adatok védelmének célja?
- az etikus hackelés megelőzése
 - a személyazonosság-lopás megakadályozása
 - helyet lehessen megtakarítani a számítógép háttértárolóján
 - a számítógépes vírusok elkerülése
- 1.5. Melyik információbiztonsági tulajdonság biztosítja a tárolt adatok jogosulatlan hozzáférés elleni védelmét?
- bizalmasság
 - sértetlenség
 - rendelkezésre állás
 - hitelesség
- 1.6. Melyik állítás igaz az informatikai biztonsági szabályzatokra?
- csak az informatikusokra vonatkoznak
 - csak a pénzügyi intézmények számára fontosak
 - csak olvasni kell, de nem kell megvalósítani
 - fontosak, mivel követendő szabályokat adnak a felhasználók számára.
- 1.7. Melyik NEM közvetlen következménye a szélhámosságnak?
- a személyes adatok mások által hozzáférhetővé váltak

- b) hozzáférhetővé vált mások által a számítógép-rendszer
- c) a tűzfalat kikapcsolják
- d) a begyűjtött adatokat csalásra fogják felhasználni

1.8. Melyik a személyazonosság-lopás módszere?

- a) hamis név használata egy közösségi oldalon
- b) nem megfelelő kulcs használata dokumentum titkosításának feloldásához
- c) adatok elektromágneses eszközökkel történő megsemmisítése
- d) információbúvárkodás

1.9. Mi használható egy rosszindulatú program elrejtésére?

- a) kikérdezés
- b) rendszerszinten tevékenykedő kártékony kód
- c) biometria
- d) bankkártya-lemásolás

1.10. Mit lehet adatlopásra használni?

- a) zombi-hálózat szoftverét
- b) adatok elektromágneses eszközökkel történő megsemmisítését
- c) alhálózatokat
- d) bedarálást

1.11. Mi a vírusirtó szoftverek korlátja?

- a) vírus-ellenőrzés közben figyelni kell a működését
- b) nem lehetséges a vírus-ellenőrzést ütemezni
- c) naprakészen kell tartani a vírusdefiníciós fájlokat
- d) karanténba teszi a fertőzött fájlokat

1.12. Mi igaz a karanténban lévő fájlokra?

- a) szoftverfrissítések
- b) ezek törölve lettek a számítógépről
- c) visszaállíthatók, ha szükséges
- d) vírusdefiníciós fájlok

1.13. Mi a célja a szoftverfrissítések telepítésének?

- a) töröljük az internetről letöltött és ideiglenesen tárolt fájlokat
- b) kijavítjuk egy program hibáját vagy biztonsági kockázatát
- c) töröljük a sütiket
- d) engedélyezzük az automatikus kiegészítést





1.14. Melyik írja le a LAN-t?

- a) kis földrajzi területen több összekötött számítógép együttese
- b) olyan nyilvános hálózat, mely megengedi a biztonságos kapcsolódást más nyilvános számítógépekhez
- c) nagy kiterjedésű területen összekapcsolt számítógépek együttese
- d) ugyanabban a helyiségben elhelyezett hálózati eszközök együttese

1.15. Mi a tűzfal feladata?

- a) törölni a sütiket a számítógépről vagy a hálózatról
- b) a mentéshez biztosítani a biztonságos háttér-adattárolókat
- c) védeni a hálózatot a betörésektől
- d) automatikusan frissíteni a digitális tanúsítványokat

1.16. Melyik ikon jelenti a drótnélküli hálózatot?

- a) 
- b) 
- c) 
- d) 

1.17. Mi a biztonsági kihatása a hálózatra való csatlakozásnak?

- a) nem lehet hozzáférni a privát hálózathoz
- b) megfertőződhet a számítógép rosszindulatú szoftverekkel
- c) a fájlhoz történő hozzáférés a hálózaton keresztül lelassul
- d) az összes internetről letöltött és ideiglenesen tárolt fájl törlődik

1.18. Miért szükséges jelszó alkalmazása a drótnélküli hálózatok hozzáféréséhez?

- a) megelőzi a hálózathoz való csatlakozási késedelmet
- b) biztosítja a vírusirtó szoftver naprakészségét
- c) így csak jogos felhasználó használhatja a hálózatot
- d) megvédi a hálózati tűzfalat



1.19. Melyik biometria védelem?

- a) adatok mentése
- b) bankkártya lemásolása
- c) kikérdezés
- d) retina-szkennelés

1.20. Mihez kell ragaszkodni egy on-line pénzügyi tranzakció elvégzésekor?

- a) a web-oldal biztonságához
- b) az automatikus kiterjesztés bekapcsolásához
- c) a Lomtárnak a tranzakciót követő kiürítéséhez
- d) a tranzakciót követő elektromágneses törléshez

1.21. Melyik ikon jelzi a biztonságos web-oldalt?

- a) 
- b) 

c)



d)



- 1.22. Melyik támadás irányítja át a web-oldal forgalmát egy hamisított web-oldalra?
- a) crackelés
 - b) eltérítéssel adathalászat
 - c) etikus hackelés
 - d) információ-szerzés
- 1.23. Melyik a böngészők által a számítógépen tárolt apró szöveg?
- a) tűzfal
 - b) trójai program
 - c) rendszerszinten rejtőző kártékony kód
 - d) süti
- 1.24. Mitől kell tartanunk a közösségi média használatakor?
- a) biometria
 - b) etikus hackelés
 - c) internetes zaklatás
 - d) titkosított fájlok
- 1.25. Mi biztosítja azt, hogy csak a címzettek olvashassanak el egy elektronikus levelet?
- a) az elektronikus levél aláírással való ellátása
 - b) az elektronikus levél titkosítása
 - c) egyszerű szöveges elektronikus levél formázása
 - d) definíciós fájl hozzáadása az elektronikus levélhez
- 1.26. Mi használ bejegyzett cégneveket személyes biztonsági adatok megszerzéséhez?
- a) adathalászat
 - b) kifigyelés
 - c) billentyűzet-leütés naplózás
 - d) zombi-hálózati szoftver
- 1.27. Mi a valós idejű szöveges kommunikáció két vagy több személy között?
- a) elektronikus levél
 - b) fájl-megosztás
 - c) eltérítéssel adathalászat
 - d) azonnali üzenetküldés
- 1.28. Mi segít biztosítani a bizalmasságot az azonnali üzenetküldés során?
- a) a tűzfal bekapcsolása
 - b) a tűzfal kikapcsolása
 - c) a fájl-megosztás korlátozása
 - d) titkosítás használata

- 1.29. Mi használható az eszközök fizikai biztonságának növelésére?
- vírusirtó szoftver
 - titkosított szöveges dokumentumok
 - biztonsági kábel
 - elektromagnetikus törlés
- 1.30. Melyik módszer törli visszaállíthatatlanul az adatokat?
- jelszavas tömörítés alkalmazása
 - az adatokat tartalmazó lemez bedarálása
 - a fájlok Lomtárba mozgatása
 - adatok titkosított merevlemezre való elhelyezése
2. Nyissa meg a vizsgaközpont által megadott mappában található **biztonsag.doc** fájlt! Tegye megnyitás-védetté a fájlt, a **guard** jelszó használatával! Mentse el és zárja be a **biztonsag** fájlt! [1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **promocio.ppt** fájlról az **aprilisi_mentes** könyvtárba! [1 pont]
- Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

2. FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
 - 1.1. Mi a "jelszó crackelés" jelentése?
 - a) személyes adatokat lopni on-line módon
 - b) rendszeresen megváltoztatni a jelszót az előírásoknak megfelelően
 - c) nem megfelelő jelszavak egymás utáni bevitele
 - d) a jelszó nyílt szöveges verziójának megszerzése
 - 1.2. Mi jelent fenyegetést az adatokra?
 - a) titkosítás
 - b) emberi tevékenység
 - c) biometria
 - d) sütik
 - 1.3. Mi az üzletileg érzékeny információk védelmének célja?
 - a) biztosítani a makrók engedélyezését
 - b) megakadályozni a vírusok terjedését
 - c) megelőzni az ügyfelek adataival való visszaélést
 - d) megakadályozni az internetes zaklatás előfordulását
 - 1.4. Mi akadályozza meg az adatokhoz való jogosulatlan hozzáférést?
 - a) a fájlok tömörítése
 - b) internet-szűrő alkalmazása
 - c) adatmentés készítése
 - d) jelszóhasználat
 - 1.5. Melyik az európai adatvédelmi szabályozás?
 - a) 1995 Európai Adatvédelmi Irányelv
 - b) 2001 Információs Társadalom Irányelv
 - c) 1995 Európai Adat Információ Szabályzat
 - d) 2002 Irányelv a személyes adatok védelméhez és az elektronikus kommunikációhoz
 - 1.6. Melyik a személyazonosság-lopás leírása?
 - a) felhasználói név használata az interneten
 - b) felvenni más személy azonosságát haszonszerzés céljából
 - c) munkahelyi adatok megadása internetes vásárláskor
 - d) tartalomellenőrző szoftverek használata internetezés közben
 - 1.7. Mi a makrók tiltásának hatása
 - a) a makró nem fog futni
 - b) a makró törölve lesz a fájlból

- c) a makró még mindig helyesen fog futni
- d) a makró akkor fog működni, ha a tűzfal be van kapcsolva

1.8. Mi a titkosított adatok előnye?

- a) nem lehet törölni
- b) gyorsabban lehet menteni
- c) nem tartalmazhatnak vírusokat vagy rosszindulatú kódokat
- d) kulcs nélkül nem lehet elolvasni

1.9. Melyik célja a tulajdonos engedélye nélkül a számítógépre való feltelepülés?

- a) tűzfal
- b) tartalomellenőrző szoftver
- c) rosszindulatú programkód
- d) vírusirtó szoftver és vírusdefiníciós fájlok

1.10. Mi vezethet rosszindulatú programkódok telepítéséhez?

- a) a makrók letiltása az alkalmazásokban
- b) hátsó kapu használata a rendszerbiztonság megkerüléséhe
- c) a "vis maior" esetekre való hivatkozás
- d) biometrikus védelem alkalmazása a felhasználók személyazonosságának megállapításához

1.11. Melyik egy fertőző rosszindulatú szoftver?

- a) a féreg
- b) a süti
- c) a tűzfal
- d) a digitális tanúsítvány

1.12. Melyik igaz a rosszindulatú programkódokra?





- a) a billentyűzetleütés naplózás a begépelte adatot rögzíti
- b) billentyűzet-leütés naplózását a <shift> billentyű lenyomásával lehet engedélyezni a számítógépen
- c) a modemes tárcsázó egy szoftver, ami szűri az interneten végzett telefonhívásokat
- d) a modemes tárcsázó egy személy, aki telefonhívásokat végez az interneten

1.13. Hogyan működnek a vírusirtó szoftverek?

- a) fertőzésmentesített fájlokat helyeznek a karanténba
- b) észlelik a vírusokat, de nem törlik automatikusan őket
- c) észlelik a vírusokat, de nem képesek felismerni a trójai programokat
- d) ütemezett keresést használnak a vírusok észlelésére

1.14. Mi a virtuális magánhálózat (VPN)?

- a) nem kell jelszó a hálózati csatlakozáshoz
- b) megengedi bárki csatlakozását egy magánhálózathoz
- c) biztonságos saját hozzáférést biztosít a hálózathoz
- d) kis földrajzi területen több összekötött számítógép együttese

- 1.15. Mi a tűzfal korlátja?
- a) fertőzött fájlokat helyez a karanténba
 - b) nem értesít automatikusan a hálózati behatolásakor
 - c) csökkenti a rosszindulatú programkódok hálózatban való megjelenésének lehetőségét
 - d) nem lehet létrehozni további szabályokat a bejövő hálózati forgalom kezelésére
- 1.16. Mi a WPA
- a) Wired Protected Access
 - b) Wi-Fi Protected Access
 - c) Wired Prevention Access
 - d) Wi-Fi Password Access.
- 1.17. Mit kell figyelembe venni nem védett drótnélküli hálózat használatakor?
- a) a hálózati tűzfalat ki kell kapcsolni
 - b) a sütiket frissíteni kell
 - c) az adatokhoz hozzá akarnak férni mások is
 - d) az egyszer használatos jelszó ki lesz kapcsolva
- 1.18. Melyik a védett drótnélküli hálózat ikonja?
- a) 
 - b) 
 - c) 
 - d) 
- 1.19. Melyik számít jó jelszónak?
- a) jBloggs_12091980
 - b) 12092010
 - c) jb
 - d) jenniferBloggs
- 1.20. Mi azonosítja a biztonságos web-oldalakat?
- a) .org
 - b) .com
 - c) https
 - d) htt
- 1.21. Mit jelent az eltérítéssel történő adathalászat (pharming)?
- a) a biztonsági forgalom irányítása tiltási és engedélyezési listákat alkalmazó szoftverrel
 - b) a webforgalom átirányítása egy hamisított web-oldalra
 - c) a kifizetés egyik módszere
 - d) az ideiglenesen letöltött és tárolt internet-fájlok megszerzése

- 1.22. Mi gyorsítja fel egy ismétlődő adatbevitelt is tartalmazó on-line űrlap kitöltését?
- automatikus kiegészítés
 - makrók tiltása
 - titkosítás
 - elektromagnetikus törlés
- 1.23. Milyen adatokat kell rendszeres időközönként ellenőrizni és törölni a böngészőből?
- makrókat
 - sütiket
 - digitális tanúsítványokat
 - vírusdefiníciós fájlokat
- 1.24. Melyik célja a weboldalakhoz való hozzáférés ellenőrzése és korlátozása?
- reklámokat megjelenítő szoftver
 - kémszoftver
 - adathalász szoftver
 - tartalomellenőrző szoftver
- 1.25. Mit nem szabad közzétenni egy közösségi oldalon?
- zenei érdeklődést
 - becenevet
 - otthoni címet
 - kedvenc televízióműsort
- 1.26. Melyik az a titkosított kód, amely egy személy azonosságát társítja egy fájlhoz?
- jelszavas tömörített fájl
 - digitális aláírás
 - makró
 - makrózott titkosított szöveg
- 1.27. Mi az adathalászat?
- lopott bankkártya adatainak felhasználása on-line vásárlásnál
 - információkat kifigyelni valaki válla felett
 - félrevezetni valakit az interneten értékes információk megszerzéséért
 - az informatikai biztonsági hiányosságok tesztelése
- 1.28. Mi jelenti a legnagyobb kitétséget a rosszindulatú programkódoknak?
- hozzáférés biztonságos weboldalhoz
 - levélcsatolmány megnyitása
 - elektronikus levél írása
 - adatok mentése
- 1.29. Mi az azonnali üzenetküldés sebezhetősége?
- hátsó ajtó hozzáférés
 - valós idejű hozzáférés
 - vis maior

d) információbúvárkodás

1.30. Mi jelenti az adatok végleges megsemmisítését?

- a) eltérítéssel adathalászat
- b) áramellátás kiesése
- c) tárcsázás
- d) elektromágneses törlés

2. Keresse meg a vizsgaközpont által megadott mappában található **level.doc** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a **lock** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **halozat.doc** fájlról a **marciusi_mentes** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

3. FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Mi az információ információbiztonsági szempontból?

- a) adatfeldolgozás kimenete
- b) logikai állítások kombinációja
- c) nyers és nem szervezett tények összessége
- d) feldolgozandó ábrák

1.2. Melyik tevékenység jogellenes internet vagy számítógéphasználat közben?

- a) etikus hackelés
- b) elektromágneses megsemmisítés
- c) kiberbűnözés
- d) digitális aláírás

1.3. Mi NEM fenyegeti az adatokat?

- a) emberi tevékenység
- b) zombi-hálózati szoftverek
- c) rosszindulatú programkódok
- d) hozzáférés-védelmi szoftverek

1.4. Mi az oka a személyes adatok védelmének?

- a) csalások megelőzése
- b) süti karbantartása
- c) hátsó ajtó biztosítása
- d) elektromágneses törlés

1.5. Melyik információbiztonsági jellemző biztosítja az adatok jogosulatlan módosítása elleni védelmét?

- a) rendelkezésre állás
- b) sértetlenség
- c) bizalmasság
- d) hozzáférhetőség

1.6. Mi a szélhámosság közvetlen következménye?

- a) jogosulatlan hozzáférés a számítógéphez
- b) tárhely-problémákhoz vezet
- c) alkalmazza a süti blokkolási beállításait
- d) törli a könyvjelzőket a böngészőből

1.7. Mi a kikérdezés?

- a) szöveges üzenetküldés a telefonszolgáltató weboldaláról

- b) jelszó-visszaállítási eljárások összessége
- c) üzenetküldés azonnali üzenetküldővel
- d) személyes információk begyűjtése megtévesztéssel

1.8. Mi a titkosítás korlátja?

- a) a fájl tulajdonosa könnyen azonosítható
- b) a titkosító kulcs elvesztésével az adat könnyen helyreállítható
- c) a titkosító kulcs elvesztésével az adat használhatatlanná válik
- d) a ktitkosított adat nem felhasználható

1.9. Mi a rosszindulatú programkód?

- a) vírusirtó szoftverek rendszeres futtatásának ütemezésére használt számítógépes program
- b) engedély nélkül használt szoftverek
- c) tűzfal-beállítások ellenőrzésére használatos szoftver
- d) számítógépes rendszerekbe engedély nélküli beszivárgást lehetővé tévő szoftver

1.10. Melyik az a rosszindulatú programkód, amelyik a felhasználó engedélye nélkül gyűjt adatokat a böngészési szokásairól?

- a) kémsoftver
- b) zombi-hálózat szoftvere
- c) tárcsázók
- d) eltérítéses adathalászat

1.11. Mi az előnye a vírusirtóknak?

- a) megakadályozzák a kifinomult támadásokat
- b) frissítik a digitális tanúsítványokat
- c) felismerik a vírusokat a számítógépen
- d) megakadályozzák az információ-búvárkodást

1.12. Mi igaz a karanténban lévő fájlokra?

- a) nem lehet letölteni
- b) nem lehet fertőzésmentesíteni
- c) nem lehet törölni
- d) nem lehet megfertőzni

1.13. Miért kell vírusdefiníciós fájlokat letölteni?

- a) frissíti az ideiglenesen letöltött és tárolt fájlokat
- b) frissíti a sütiket
- c) lehetővé teszi az új fenyegetések elleni védelmet
- d) frissíti az elektromágneses törléseket végző szoftvert

1.14. Hogyan nevezik az irodában vagy otthon összekapcsolt számítógépeket?

- a) LAN
- b) VPN
- c) WAN

d) USB





1.15. Mi a hálózati adminisztrátor feladata?

- a) fenntartani az épület elektromos hálózatának folyamatos működőképességét
- b) biztosítani a hálózati adatokhoz a nyilvános hozzáférést
- c) biztosítani, hogy az adatokat ne mentse le a rendszerbe
- d) fenntartani a munkatársak szükséges adathozzáférést a hálózaton

1.16. Mi akadályozza meg a jogosulatlan belépést a hálózatba egy külső helyszínről?

- a) elektromágneses törlés
- b) tűzfalak
- c) adathalászat
- d) digitális tanúsítványok

1.17. Melyik ikon jelenti a csatlakoztatható vezetékes hálózatot?

- a) 
- b) 
- c) 
- d) 

1.18. Mi a hálózatra történő csatlakozás biztonsági vonatkozása?

- a) adatok biztonsági mentése
- b) fájlok tömörítése
- c) személyes adatok védelme
- d) információbúvárkodás

1.19. Miért kell jelszóval védeni a vezeték nélküli hálózatokat?

- a) elindítja a vírusirtó szoftvert
- b) megakadályozza a jogosulatlan adat-hozzáférést
- c) biztosítja a süti engedélyezését
- d) megakadályozza az adathalászatra irányuló támadásokat

1.20. Mi igazolja, hogy az üzenet küldője valóban az, akinek állítja magát?

- a) digitális tanúsítvány
- b) süti
- c) makró
- d) letöltött és ideiglenesen tárolt internet fájlok

1.21. Mikor használnak egyszer használatos jelszót?

- a) a laptopra való első bejelentkezéskor
- b) amikor a jelszót elküldik e-mailben
- c) amikor tűzfalat állítanak be
- d) VPN-be való bejelentkezéskor

- 1.22. Melyik adat törölhető a böngésző által?
- kititkosított adat
 - titkosított adat
 - automatikus kiegészítés adata
 - billentyűzet-leütéseket naplózó adat
- 1.23. Melyikkel korlátozható az interneten töltött időtartam?
- adathalász szoftver
 - szülői felügyelet szoftver
 - tárcsázó
 - süтик
- 1.24. Melyik a közösségi oldalakon előforduló fenyegetés?
- bedarálás
 - elektromágneses törlés
 - bankkártya adatainak a lemásolása
 - szexuális kizsákmányolás
- 1.25. Milyen eljárás biztosítja az e-mailek bizalmasságát?
- titkosítás
 - kikérdezés
 - eltérítéses adathalászat
 - kititkosítás
- 1.26. Mi a digitális aláírás eszköze?
- szoftver, ami átirányítja egy weboldal forgalmát egy hamisított weboldalra
 - egy matematikai séma az üzenet hitelességének biztosítására
 - egy bonyolult módszer, mely beszúrja az aláírást az üzenet végére
 - szoftver, mely engedélyezési és tiltólistákat alkalmaz a bejövő hálózati forgalom irányítására
- 1.27. Melyik fogalom írja le a banki adatokat bekérő hamisított elektronikus leveleket?
- kifigyelés
 - internetes zaklatás
 - adathalászat
 - crackelés
- 1.28. Mi tartalmazhat rosszindulatú programkódot?
- levélcsatolmány
 - süтик
 - tűzfal
 - digitális aláírás
- 1.29. Melyik nyújt védelmet az adatvesztés ellen?
- süтик
 - kikérdezés

- c) titkosított USB lemez használata
- d) mentések

1.30. Miért van szükség az adatok visszaállíthatatlan törlésére?

- a) az áramingadozásból adódó meghibásodások miatt
- b) az adatok más általi visszaállíthatatlansága miatt
- c) hogy tartalomellenőrző szoftvert lehessen telepíteni
- d) hogy törölni lehessen minden sütit

2. Nyissa meg a vizsgaközpont által megadott mappában található **hossaferes.doc** fájlt! Tegye megnyitás-védetté a fájlt, a **guard** jelszó használatával! Mentse el és zárja be a **hossaferes** fájlt! [1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **rendszer.doc** fájlról a **juniusi_mentes** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

4. FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
 - 1.1. Melyik kiberbűnözés az alábbiak közül?
 - a) okostelefon ellopása
 - b) internetes számla on-line befizetése
 - c) bankkártya adatok ellopása on-line
 - d) internetes rádióhallgatása on-line
 - 1.2. Melyik eljárás tartalmazza az informatikai biztonsági sebezhetőségek tesztelését?
 - a) crackelés
 - b) etikus hackelés
 - c) bankkártya adatainak lemásolása
 - d) kikérdezés
 - 1.3. Miért kell védeni az üzletileg érzékeny információkat?
 - a) mert megakadályozza az adatlopást
 - b) ütemezett mentések lefutásának biztosítása miatt
 - c) kéretlen üzenetek blokkolása miatt
 - d) a biztonságos weboldalak azonosításáért
 - 1.4. Melyik nyújt védelmet a jogosulatlan adat-hozzáférés ellen?
 - a) bonyolult fájlnevek
 - b) billentyűzet-leütés naplózása
 - c) eltérítéssel adathalászat
 - d) titkosítás
 - 1.5. Melyik információbiztonsági tulajdonság biztosítja az adatok jogosulatlan hozzáférés vagy felfedés elleni védelmét?
 - a) bizalmasság
 - b) sértetlenség
 - c) rendelkezésre állás
 - d) hitelesség
 - 1.6. Melyik európai szabályozást kell betartani a személyes adatok védelmének vonatkozásában??
 - a) 1997 Európai Adatvédelmi Szabályozás
 - b) 2001 Európai Információs Társadalmi Irányelv
 - c) 1995 Európai Adatvédelmi Irányelv
 - d) 2001 Európai Irányelv az Információ-Technológiáról

1.7. Melyik tartozik a szélhámosság módszerei közé?

- a) közösségi oldalakhoz több fiókkal rendelkezni
- b) valaki válla fölött megszerezni az információkat
- c) videó- és hanghívásokat kezdeményezni az interneten
- d) meghivatkozni más weboldalát egy közösségi oldalról

1.8. Mi a személyazonosság-lopás közvetlen következménye?

- a) a pénzügyi adatokat mások is használhatják
- b) a vírusirtó nem működik a továbbiakban
- c) a letöltött és ideiglenesen tárolt fájlokat törölni fogják
- d) a mentés ütemezését megváltoztatják

1.9. Melyik szoftvert készítek és küldik károkozási célból?

- a) szimmetrikus vagy aszimmetrikus elvű titkosító szoftverek
- b) tűzfalak
- c) rosszindulatú programkódok
- d) vírusirtó szoftverek

1.10. Mit használnak a rosszindulatú programkódok elrejtésére?

- a) rendszerszinten tevékenykedő kártékony kódokat
- b) elektromágneses elven alapuló adattörlési módszereket
- c) tűzfalakat
- d) bedarálást

1.11. Mi egy fertőző, rosszindulatú program?

- a) a süti
- b) a vírus
- c) a digitális tanúsítvány
- d) a digitális aláírás

1.12. Melyik képes megfertőzni és irányítani egy számítógépet a tulajdonos engedélye nélkül?

- a) biometria
- b) vírus-definíciós fájl
- c) süti
- d) zombi-hálózat

1.13. Mi a vírusirtó szoftverek előnye?

- a) megvizsgálják a számítógépet hogy nem fertőződnek-e meg
- b) megakadályozzák a tartalom-ellenőrző szoftverek elindítását
- c) minden adatot mentenek
- d) a korábban törölt fájlokat visszaállítják a számítógép háttértárolójára

1.14. Mi akadályozza meg a hálózathoz kívülről történő jogosulatlan hozzáférést?

- a) fájlok hozzáférés-védelmi beállításai
- b) tartalom-ellenőrző program

- c) zombi-hálózati szoftver
- d) tűzfalak





1.15. Mi biztosítja a vezeték nélküli biztonságot?

- a) WAN
- b) LAN
- c) Média Hozzáférési Kontroll (MAC)
- d) számítógépes hálózathoz hátsó kaput nyitó szoftver

1.16. Mi eredményezhet jogosulatlan adathozzáférést??

- a) elektromágneses törlés
- b) adat-hozzáférés vezeték nélküli forgalom lehallgatásakor
- c) biometrikus védelmi intézkedésen alapuló hozzáférés-védelmi szoftver telepítése
- d) digitális tanúsítvány

1.17. Melyik ikon jelzi a nem védett vezeték nélküli hálózatot?

- a) 
- b) 
- c) 
- d) 

1.18. Hogyan történik a hálózati bejelentkezés?

- a) felhasználói névvel és jelszóval
- b) automatikus kiegészítéssel
- c) titkosított felhasználói névvel
- d) digitális tanúsítvánnyal

1.19. Melyik a jó szabály a jelszavakra?




- a) használjon minél kevesebb karaktert a jelszóban
- b) időnként változtassa meg a jelszavát
- c) ossza meg a jelszavát a barátaival
- d) a jelszóban sose használjon vegyesen betűket és számokat

1.20. Melyik weboldalnál található http előtag a https helyett?

- a) on-line bank
- b) keresőmotor
- c) on-line webáruház
- d) biztonságos weboldal

1.21. Melyik jelöli a biztonságos weboldalakat?

- a) 

- b) 
- c) 
- d) 

- 1.22. Mely fájlok tartalmazhatnak nyilvános kulcsokat és más hitelesítő adatokat?
- a) vírusdefiníciós fájlok
 - b) titkosított adatbázis-mentési fájlok
 - c) makrók
 - d) digitális tanúsítványok
- 1.23. Miért kell a sütiket blokkolni a böngészőkben?
- a) hogy vírusirtó szoftvert lehessen telepíteni
 - b) hogy hozzá lehessen férni a web-alapú elektronikus levelezési fiókokhoz
 - c) hogy böngészhessünk ismeretlen weblapokon
 - d) hogy megakadályozzuk az internetes zaklatást
- 1.24. Mi lenne az eredménye annak, ha egy közösségi oldalon a személyes adatokat a nyilvánosság számára hozzáférhetővé tennénk?
- a) a személyes adatokhoz csak a barátok férhetnének hozzá
 - b) a személyes adatokat bárki megnézheti
 - c) a barátok barátai láthatnák a személyes adatokat
 - d) a barátok módosíthatnák a személyes adatokat
- 1.25. Mi tartalmazhat rosszindulatú programkódot vagy vírust?
- a) X509v3 digitális tanúsítványok
 - b) tűzfalak
 - c) digitális aláírások
 - d) csalárd elektronikus levelek
- 1.26. Mi használja az adatok megszerzéséhez hamisított weboldalak linkjeit?
- a) rendszerszinten tevékenykedő kártékony kódok
 - b) tárcsázó programok
 - c) adathalászat
 - d) bankkártya-lemásolás
- 1.27. Miért NEM szabad megnyitni egy ismeretlen csatolmányt?
- a) rosszindulatú programkódokat tartalmazhat
 - b) lehet, hogy nagyon nagy a fájl
 - c) lehet, hogy titkosító kulcs szükséges a megnyitásához
 - d) lehetséges, hogy digitális tanúsítványt tartalmaz
- 1.28. Melyik lehet az azonnali üzenetküldés sebezhetősége?
- a) vírusdefiníciós fájlok

- b) on-line emelt díjas tárcsázó programok
- c) digitális tanúsítványok
- d) rosszindulatú programkódok

1.29. Melyik egy lehetséges mentési tulajdonság?

- a) bankkártya lemásolás
- b) ütemezés
- c) kikérdezés
- d) elektromágneses törlés

1.30. Mi NEM eredményezi az adatok végleges törlését?

- a) az adatok átmozgatása a Lomtárba
- b) a háttértároló elektromágneses törlése
- c) a szoftveres adatmegsemmisítő eszközök használata
- d) a DVD-k bedarálása

2. Keresse meg a vizsgaközpont által megadott mappában található **iroszer.doc** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a **safe** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **ertesites.xls** fájlról a **juliusi_mentes** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

5. FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
 - 1.1. Melyik tevékenység kiberbűnözés?
 - a) bedarálás
 - b) adathalászat
 - c) etikus hackelés
 - d) titkosítás
 - 1.2. Mit jelent a "hackelés" fogalma?
 - a) az adatokhoz való jogosulatlan hozzáférés megszerzése
 - b) félrevezetni a személyazonosságunkról valakit az interneten
 - c) vírusirtóval eltávolítani az összes rosszindulatú szoftvert a gépünkről
 - d) számítógépeket lopni az épületbe való betöréssel
 - 1.3. Melyik jelent „vis maior” fenyegetést az adatokra?
 - a) emberi tevékenység
 - b) adatlopás
 - c) tűz
 - d) vírusok
 - 1.4. Mi a személyes adatok védelmének célja?
 - a) az etikus hackelés megelőzése
 - b) a személyazonosság-lopás megakadályozása
 - c) helyet lehessen megtakarítani a számítógép háttértárolóján
 - d) a számítógépes vírusok elkerülése
 - 1.5. Melyik információbiztonsági tulajdonság biztosítja a tárolt adatok jogosulatlan hozzáférés elleni védelmét?
 - a) bizalmasság
 - b) sértetlenség
 - c) rendelkezésre állás
 - d) hitelesség
 - 1.6. Melyik állítás igaz az informatikai biztonsági szabályzatokra?
 - a) csak az informatikusokra vonatkoznak
 - b) csak a pénzügyi intézmények számára fontosak
 - c) csak olvasni kell, de nem kell megvalósítani
 - d) fontosak, mivel követendő szabályokat adnak a felhasználók számára
 - 1.7. Melyik NEM közvetlen következménye a szélhámosságnak?
 - a) a személyes adatok mások által hozzáférhetővé váltak

- b) a személyes adatok mások által hozzáférhetővé válna
- c) a tűzfalat kikapcsolják
- d) a begyűjtött adatokat csalásra fogják felhasználni

1.8. Melyik a személyazonosság-lopás módszere?

- a) hamis név használata egy közösségi oldalon
- b) nem megfelelő kulcs használata dokumentum titkosításának feloldásához
- c) adatok elektromágneses eszközökkel történő megsemmisítése
- d) információbúvárkodás

1.9. Mi használható egy rosszindulatú program elrejtésére?

- a) kikérdezés
- b) rendszerszinten tevékenykedő kártékony kód
- c) biometria
- d) bankkártya-lemásolás

1.10. Mit lehet adatlopásra használni?

- a) zombi-hálózat szoftverét
- b) adatok elektromágneses eszközökkel történő megsemmisítését
- c) alhálózatokat
- d) bedarálást

1.11. Mi a vírusirtó szoftverek korlátja?

- a) vírus-ellenőrzés közben figyelni kell a működését
- b) nem lehetséges a vírus-ellenőrzést ütemezni
- c) naprakészen kell tartani a vírusdefiníciós fájlokat
- d) karanténba teszi a fertőzött fájlokat

1.12. Mi igaz a karanténban lévő fájlokra?

- a) szoftverfrissítések
- b) ezek törölve lettek a számítógépről
- c) visszaállíthatók, ha szükséges
- d) vírusdefiníciós fájlok

1.13. Mi a célja a szoftverfrissítések telepítésének??

- a) töröljük az internetről letöltött és ideiglenesen tárolt fájlokat
- b) kijavítjuk egy program hibáját vagy biztonsági kockázatát
- c) töröljük a sütiket
- d) engedélyezzük az automatikus kiegészítést

1.14. Melyik írja le a LAN-t?

- a) kis földrajzi területen több összekötött számítógép együttese
- b) olyan nyilvános hálózat, mely megengedi a biztonságos kapcsolódást más nyilvános számítógépekhez
- c) nagy kiterjedésű területen összekapcsolt számítógépek együttese
- d) ugyanabban a helyiségben elhelyezett hálózati eszközök együttese

1.15. Mi a tűzfal feladata?

- a) törölni a sütiket a számítógépről vagy a hálózatról
- b) a mentéshez biztosítson biztonságos háttér-adattárolókat
- c) védje a hálózatot a betörésektől
- d) automatikusan frissítse a digitális tanúsítványokat





1.16. Mi a WPA?

- a) Wired Protected Access
- b) Wi-Fi Protected Access
- c) Wired Prevention Access
- d) Wi-Fi Password Access

1.17. Mit kell figyelembe venni nem védett drótnélküli hálózat használatakor?

- a) a hálózati tűzfalat ki kell kapcsolni
- b) a sütiket frissíteni kell
- c) az adatokhoz hozzá akarnak férni mások is
- d) az egyszer használatos jelszó ki lesz kapcsolva

1.18. Melyik a védett drótnélküli hálózat ikonja?

- a) 
- b) 
- c) 
- d) 

1.19. Melyik számít jó jelszónak?

- a) jBloggs_12091980
- b) 12092010
- c) jb
- d) jenniferBloggs

1.20. Mi azonosítja a biztonságos web-oldalakat?

- a) .org
- b) .com
- c) https
- d) http

1.21. Mit jelent az eltérítéssel adathalászat (pharming)?

- a) a biztonsági forgalom irányítása tiltási és engedélyezési listákat alkalmazó szoftverrel
- b) a webforgalom átirányítása egy hamisított web-oldalra
- c) a kifizetés egyik módszere
- d) az ideiglenesen letöltött és tárolt internet-fájlok megszerzése

- 1.22. Mi gyorsítja fel egy ismétlődő adatbevitelt is tartalmazó on-line űrlap kitöltését?
- automatikus kiegészítés
 - makrók tiltása
 - titkosítás
 - elektromagnetikus törlés
- 1.23. Milyen adatokat kell rendszeres időközönként ellenőrizni és törölni a böngészőből?
- makrókat
 - sütiket
 - digitális tanúsítványokat
 - vírusdefiníciós fájlokat
- 1.24. Melyik célja a weboldalakhoz való hozzáférés ellenőrzése és korlátozása?
- reklámokat megjelenítő szoftver
 - kémszoftver
 - adathalász szoftver
 - tartalomellenőrző szoftver
- 1.25. Mit nem szabad közzétenni egy közösségi oldalon?
- zenei érdeklődést
 - becenevet
 - otthoni címet
 - kedvenc televízióműsort
- 1.26. Melyik az a titkosított kód, amely egy személy azonosságát társítja egy fájlhoz?
- jelszavas tömörített fájl
 - digitális aláírás
 - makrózott titkosított szöveg
 - ideiglenesen letöltött és tárolt fájl
- 1.27. Mi az adathalászat?
- lopott bankkártya adatainak felhasználása on-line vásárlásnál
 - információkat kifigyelni valaki válla felett
 - félrevezetni valakit az interneten értékes információk megszerzéséért
 - az informatikai biztonsági hiányosságok tesztelése
- 1.28. Mi jelenti a legnagyobb kitétséget a rosszindulatú programkódoknak?
- hozzáférés biztonságos weboldalhoz
 - levélcsatolmány megnyitása
 - elektronikus levél írása
 - adatok mentése
- 1.29. Mi az azonnali üzenetküldés sebezhetősége?
- hátsó ajtó hozzáférés
 - valós idejű hozzáférés
 - vis maior

d) információbúvárkodás

1.30. Mi jelenti az adatok végleges megsemmisítését?

- a) eltérítéssel adathalászat
- b) áramellátás kiesése
- c) tárcsázás
- d) elektromágneses törlés

2. Nyissa meg a vizsgaközpont által megadott mappában található **biztonsag.doc** fájlt! Tegye megnyitás-védetté a fájlt, a **guard** jelszó használatával! Mentse el és zárja be a **biztonsag** fájlt! [1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **promocio.ppt** fájlról az **aprilisi_mentes** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

6. FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Melyik tevékenység kiberbűnözés?

- a) bedarálás
- b) adathalászat
- c) etikus hackelés
- d) titkosítás

1.2. Mit jelent a "hackelés" fogalma?

- a) az adatokhoz való jogosulatlan hozzáférés megszerzése
- b) félrevezetni a személyazonosságunkról valakit az interneten
- c) vírusirtóval eltávolítani az összes rosszindulatú szoftvert a gépünkről
- d) számítógépeket lopni az épületbe való betöréssel

1.3. Melyik jelent „vis maior” fenyegetést az adatokra?

- a) emberi tevékenység
- b) adatlopás
- c) tűz
- d) vírusok

1.4. Mi a személyes adatok védelmének célja?

- a) az etikus hackelés megelőzése
- b) a személyazonosság-lopás megakadályozása
- c) helyet lehessen megtakarítani a számítógép háttértárolóján
- d) a számítógépes vírusok elkerülése

1.5. Melyik információbiztonsági tulajdonság biztosítja a tárolt adatok jogosulatlan hozzáférés elleni védelmét?

- a) bizalmasság
- b) sértetlenség
- c) rendelkezésre állás
- d) hitelesség

1.6. Melyik állítás igaz az informatikai biztonsági szabályzatokra?

- a) csak az informatikusokra vonatkoznak
- b) csak a pénzügyi intézmények számára fontosak
- c) csak olvasni kell, de nem kell megvalósítani
- d) fontosak, mivel követendő szabályokat adnak a felhasználók számára

1.7. Melyik NEM közvetlen következménye a szélhámosságnak?

- a) a személyes adatok mások által hozzáférhetővé váltak

- b) hozzáférhetővé vált mások által a számítógép-rendszer
- c) a tűzfalat kikapcsolják
- d) a begyűjtött adatokat csalásra fogják felhasználni

1.8. Melyik a személyazonosság-lopás módszere?

- a) hamis név használata egy közösségi oldalon
- b) nem megfelelő kulcs használata dokumentum titkosításának feloldásához
- c) adatok elektromágneses eszközökkel történő megsemmisítése
- d) információbúvárkodás

1.9. Mi használható egy rosszindulatú program elrejtésére?

- a) kikérdezés
- b) rendszerszinten tevékenykedő kártékony kód
- c) biometria
- d) bankkártya-lemásolás

1.10. Mit lehet adatlopásra használni?

- a) zombi-hálózat szoftverét
- b) adatok elektromágneses eszközökkel történő megsemmisítését
- c) alhálózatokat
- d) bedarálást

1.11. Mi a vírusirtó szoftverek korlátja?

- a) vírus-ellenőrzés közben figyelni kell a működését
- b) nem lehetséges a vírus-ellenőrzést ütemezni
- c) naprakészen kell tartani a vírusdefiníciós fájlokat
- d) karanténba teszi a fertőzött fájlokat

1.12. Mi igaz a karanténban lévő fájlokra?

- a) szoftverfrissítések
- b) ezek törölve lettek a számítógépről
- c) visszaállíthatók, ha szükséges
- d) vírusdefiníciós fájlok

1.13. Mi a célja a szoftverfrissítések telepítésének?

- a) töröljük az internetről letöltött és ideiglenesen tárolt fájlokat
- b) kijavítjuk egy program hibáját vagy biztonsági kockázatát
- c) töröljük a sütiket
- d) engedélyezzük az automatikus kiegészítést

1.14. Melyik írja le a LAN-t?

- a) kis földrajzi területen több összekötött számítógép együttese
- b) olyan nyilvános hálózat, mely megengedi a biztonságos kapcsolódást más nyilvános számítógépekhez
- c) nagy kiterjedésű területen összekapcsolt számítógépek együttese
- d) ugyanabban a helyiségben elhelyezett hálózati eszközök együttese

1.15. Mi a tűzfal feladata?

- a) törölni a sütiket a számítógépről vagy a hálózatról
- b) a mentéshez biztosítson biztonságos háttér-adattárolókat
- c) védje a hálózatot a betörésektől
- d) automatikusan frissítse a digitális tanúsítványokat





1.16. Mi a WPA?

- a) Wired Protected Access
- b) Wi-Fi Protected Access
- c) Wired Prevention Access
- d) Wi-Fi Password Access

1.17. Mit kell figyelembe venni nem védett drótnélküli hálózat használatakor?

- a) a hálózati tűzfalat ki kell kapcsolni
- b) a sütiket frissíteni kell
- c) az adatokhoz hozzá akarnak férni mások is
- d) az egyszer használatos jelszó ki lesz kapcsolva

1.18. Melyik a védett drótnélküli hálózat ikonja?

- a) 
- b) 
- c) 
- d) 

1.19. Melyik számít jó jelszónak?

- a) jBloggs_12091980
- b) 12092010
- c) jb
- d) jenniferBloggs

1.20. Mi azonosítja a biztonságos web-oldalakat?

- a) .org
- b) .com
- c) https
- d) http

1.21. Mit jelent az eltérítéssel adathalászat (pharming)?

- a) a biztonsági forgalom irányítása tiltási és engedélyezési listákat alkalmazó szoftverrel
- b) a webforgalom átirányítása egy hamisított web-oldalra
- c) a kifizetés egyik módszere
- d) az ideiglenesen letöltött és tárolt internet-fájlok megszerzése

- 1.22. Mi gyorsítja fel egy ismétlődő adatbevitelt is tartalmazó on-line űrlap kitöltését?
- automatikus kiegészítés
 - makrók tiltása
 - titkosítás
 - elektromagnetikus törlés
- 1.23. Milyen adatokat kell rendszeres időközönként ellenőrizni és törölni a böngészőből?
- makrókat
 - sütiket
 - digitális tanúsítványokat
 - vírusdefiníciós fájlokat
- 1.24. Melyik célja a weboldalakhoz való hozzáférés ellenőrzése és korlátozása?
- reklámokat megjelenítő szoftver
 - kémszoftver
 - adathalász szoftver
 - tartalomellenőrző szoftver
- 1.25. Mit nem szabad közzétenni egy közösségi oldalon?
- zenei érdeklődést
 - becenevet
 - otthoni címet
 - kedvenc televízióműsort
- 1.26. Melyik az a titkosított kód, amely egy személy azonosságát társítja egy fájlhoz?
- jelszavas tömörített fájl
 - digitális aláírás
 - makrózott titkosított szöveg
 - ideiglenesen letöltött és tárolt fájl
- 1.27. Mi az adathalászat?
- lopott bankkártya adatainak felhasználása on-line vásárlásnál
 - információkat kifigyelni valaki válla felett
 - félrevezetni valakit az interneten értékes információk megszerzéséért
 - az informatikai biztonsági hiányosságok tesztelése
- 1.28. Mi jelenti a legnagyobb kitéettséget a rosszindulatú programkódoknak?
- hozzáférés biztonságos weboldalhoz
 - levélcsatolmány megnyitása
 - elektronikus levél írása
 - adatok mentése
- 1.29. Mi az azonnali üzenetküldés sebezhetősége?
- hátsó ajtó hozzáférés
 - valós idejű hozzáférés
 - vis maior

d) információbúvárkodás

1.30. Mi jelenti az adatok végleges megsemmisítését?

- a) eltérítéssel adathalászat
- b) áramellátás kiesése
- c) tárcsázás
- d) elektromágneses törlés

2. Keresse meg a vizsgaközpont által megadott mappában található **level.doc** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a **lock** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **halozat.doc** fájlról a **marciusi_mentes** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

7. FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]

1.1. Melyik tevékenység kiberbűnözés?

- a) bedarálás
- b) adathalászat
- c) etikus hackelés
- d) titkosítás

1.2. Mit jelent a "hackelés" fogalma?

- a) az adatokhoz való jogosulatlan hozzáférés megszerzése
- b) félrevezetni a személyazonosságunkról valakit az interneten
- c) vírusirtóval eltávolítani az összes rosszindulatú szoftvert a gépünkről
- d) számítógépeket lopni az épületbe való betöréssel

1.3. Melyik jelent „vis maior” fenyegetést az adatokra?

- a) emberi tevékenység
- b) adatlopás
- c) tűz
- d) vírusok

1.4. Mi a személyes adatok védelmének célja?

- a) az etikus hackelés megelőzése
- b) a személyazonosság-lopás megakadályozása
- c) helyet lehessen megtakarítani a számítógép háttértárolóján
- d) a számítógépes vírusok elkerülése

1.5. Melyik információbiztonsági tulajdonság biztosítja a tárolt adatok jogosulatlan hozzáférés elleni védelmét?

- a) bizalmasság
- b) sértetlenség
- c) rendelkezésre állás
- d) hitelesség

1.6. Melyik állítás igaz az informatikai biztonsági szabályzatokra?

- a) csak az informatikusokra vonatkoznak
- b) csak a pénzügyi intézmények számára fontosak
- c) csak olvasni kell, de nem kell megvalósítani
- d) fontosak, mivel követendő szabályokat adnak a felhasználók számára

1.7. Melyik NEM közvetlen következménye a szélhámosságnak?

- a) a személyes adatok mások által hozzáférhetővé váltak

- b) hozzáférhetővé vált mások által a számítógép-rendszer
- c) a tűzfalat kikapcsolják
- d) a begyűjtött adatokat csalásra fogják felhasználni

1.8. Melyik a személyazonosság-lopás módszere?

- a) hamis név használata egy közösségi oldalon
- b) nem megfelelő kulcs használata dokumentum titkosításának feloldásához
- c) adatok elektromágneses eszközökkel történő megsemmisítése
- d) információbúvárkodás

1.9. Mi használható egy rosszindulatú program elrejtésére?

- a) kikérdezés
- b) rendszerszinten tevékenykedő kártékony kód
- c) biometria
- d) bankkártya-lemásolás

1.10. Mit lehet adatlopásra használni?

- a) zombi-hálózat szoftverét
- b) adatok elektromágneses eszközökkel történő megsemmisítését
- c) alhálózatokat
- d) bedarálást

1.11. Mi a vírusirtó szoftverek korlátja?

- a) vírus-ellenőrzés közben figyelni kell a működését
- b) nem lehetséges a vírus-ellenőrzést ütemezni
- c) naprakészen kell tartani a vírusdefiníciós fájlokat
- d) karanténba teszi a fertőzött fájlokat

1.12. Mi igaz a karanténban lévő fájlokra?

- a) szoftverfrissítések
- b) ezek törölve lettek a számítógépről
- c) visszaállíthatók, ha szükséges
- d) vírusdefiníciós fájlok

1.13. Mi a célja a szoftverfrissítések telepítésének?

- a) töröljük az internetről letöltött és ideiglenesen tárolt fájlokat
- b) kijavítjuk egy program hibáját vagy biztonsági kockázatát
- c) töröljük a sütiket
- d) engedélyezzük az automatikus kiegészítést

1.14. Melyik írja le a LAN-t?

- a) kis földrajzi területen több összekötött számítógép együttese
- b) olyan nyilvános hálózat, mely megengedi a biztonságos kapcsolódást más nyilvános számítógépekhez
- c) nagy kiterjedésű területen összekapcsolt számítógépek együttese
- d) ugyanabban a helyiségben elhelyezett hálózati eszközök együttese





1.15. Mi a tűzfal feladata?

- a) törölni a sütiket a számítógépről vagy a hálózatról
- b) a mentéshez biztosítson biztonságos háttér-adattárolókat
- c) védje a hálózatot a betörésektől
- d) automatikusan frissítse a digitális tanúsítványokat

1.16. Mi eredményezhet jogosulatlan adathozzáférést?

- a) elektromágneses törlés
- b) adat-hozzáférés vezeték nélküli forgalom lehallgatásakor
- c) biometrikus védelmi intézkedésen alapuló hozzáférés-védelmi szoftver telepítése
- d) digitális tanúsítvány

1.17. Melyik ikon jelzi a nem védett vezeték nélküli hálózatot?

- a) 
- b) 
- c) 
- d) 

1.18. Hogyan történik a hálózati bejelentkezés?

- a) felhasználói névvel és jelszóval
- b) automatikus kiegészítéssel
- c) titkosított felhasználói névvel
- d) digitális tanúsítvánnyal




1.19. Melyik a jó szabály a jelszavakra?

- a) használjon minél kevesebb karaktert a jelszóban
- b) időnként változtassa meg a jelszavát
- c) ossza meg a jelszavát a barátaival
- d) a jelszóban sose használjon vegyesen betűket és számokat

1.20. Melyik weboldalnál található http előtag a https helyett?

- a) on-line bank
- b) keresőmotor
- c) on-line webáruház
- d) biztonságos weboldal

1.21. Melyik jelöli a biztonságos weboldalakat?

- a) 
- b) 
- c) 



d)

- 1.22. Mely fájlok tartalmazhatnak nyilvános kulcsokat és más hitelesítő adatokat?
- vírusdefiníciós fájlok
 - titkosított adatbázis-mentési fájlok
 - makrók
 - digitális tanúsítványok
- 1.23. Miért kell a sütitket blokkolni a böngészőkben?
- hogy vírusirtó szoftvert lehessen telepíteni
 - hogy hozzá lehessen férni a web-alapú elektronikus levelezési fiókokhoz
 - hogy böngészhessünk ismeretlen weblapokon
 - hogy megakadályozzuk az internetes zaklatást
- 1.24. Mi lenne az eredménye annak, ha egy közösségi oldalon a személyes adatokat a nyilvánosság számára hozzáférhetővé tennénk?
- a személyes adatokhoz csak a barátok férhetnének hozzá
 - a személyes adatokat bárki megnézheti
 - a barátok barátai láthatnák a személyes adatokat
 - a barátok módosíthatnák a személyes adatokat
- 1.25. Mi tartalmazhat rosszindulatú programkódot vagy vírust?
- X509v3 digitális tanúsítványok
 - tűzfalak
 - digitális aláírások
 - csalárd elektronikus levelek
- 1.26. Mi használja az adatok megszerzéséhez hamisított weboldalak linkjeit?
- rendszerszinten tevékenykedő kártékony kódok
 - tárcsázó programok
 - adathalászat
 - bankkártya-lemásolás
- 1.27. Miért NEM szabad megnyitni egy ismeretlen csatolmányt?
- rosszindulatú programkódokat tartalmazhat
 - lehet, hogy nagyon nagy a fájl
 - lehet, hogy titkosító kulcs szükséges a megnyitáshoz
 - lehetséges, hogy digitális tanúsítványt tartalmaz
- 1.28. Melyik lehet az azonnali üzenetküldés sebezhetősége?
- vírusdefiníciós fájlok
 - on-line emelt díjas tárcsázó programok
 - digitális tanúsítványok
 - rosszindulatú programkódok

- 1.29. Melyik egy lehetséges mentési tulajdonság?
- a) bankkártya lemásolás
 - b) ütemezés
 - c) kikérdezés
 - d) elektromágneses törlés
- 1.30. Mi NEM eredményezi az adatok végleges törlését?
- a) az adatok átmozgatása a Lomtárba
 - b) a háttértároló elektromágneses törlése
 - c) a szoftveres adatmegsemmisítő eszközök használata
 - d) a DVD-k bedarálása
2. Nyissa meg a vizsgaközpont által megadott mappában található **hossaferes.doc** fájlt! Tegye megnyitás-védetté a fájlt, a **guard** jelszó használatával! Mentse el és zárja be a **hossaferes** fájlt! [1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **rendszer.doc** fájlról a **juniusi_mentes** könyvtárba! [1 pont]
- Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

8. FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
- 1.1. Mi a "jelszó crackelés" jelentése?
- a) személyes adatokat lopni on-line módon
 - b) rendszeresen megváltoztatni a jelszót az előírásoknak megfelelően
 - c) nem megfelelő jelszavak egymás utáni bevitele
 - d) a jelszó nyílt szöveges verziójának megszerzése
- 1.2. Mi jelent fenyegetést az adatokra?
- a) titkosítás
 - b) emberi tevékenység
 - c) biometria
 - d) sütik
- 1.3. Mi az üzletileg érzékeny információk védelmének célja?
- a) biztosítani a makrók engedélyezését
 - b) megakadályozni a vírusok terjedését
 - c) megelőzni az ügyfelek adataival való visszaélést
 - d) megakadályozni az internetes zaklatást
- 1.4. Mi akadályozza meg az adatokhoz való jogosulatlan hozzáférést?
- a) a fájlok tömörítése
 - b) internet-szűrő alkalmazása
 - c) adatmentés készítése
 - d) jelszóhasználat
- 1.5. Melyik az európai adatvédelmi szabályozás?
- a) 1995 Európai Adatvédelmi Irányelv
 - b) 2001 Információs Társadalom Irányelv
 - c) 1995 Európai Adat Információ Szabályzat
 - d) 2002 Irányelv a személyes adatok védelméhez és az elektronikus kommunikációhoz
- 1.6. Melyik a személyazonosság-lopás leírása?
- a) felhasználói név használata az interneten
 - b) felvenni más személy azonosságát haszonszerzés céljából
 - c) munkahelyi adatok megadása internetes vásárláskor
 - d) tartalomellenőrző szoftverek használata internetezés közben
- 1.7. Mi a makrók tiltásának hatása?
- a) a makró nem fog futni
 - b) a makró törölve lesz a fájlból

- c) a makró még mindig helyesen fog futni
- d) a makró akkor fog működni, ha a tűzfal be van kapcsolva

1.8. Mi a titkosított adatok előnye?

- a) nem lehet törölni
- b) gyorsabban lehet menteni
- c) nem tartalmazhatnak vírusokat vagy rosszindulatú kódokat
- d) kulcs nélkül nem lehet elolvasni

1.9. Melyik célja a tulajdonos engedélye nélkül a számítógépre való feltelepülés?

- a) tűzfal
- b) tartalomellenőrző szoftver
- c) rosszindulatú programkód
- d) vírusirtó szoftver és vírusdefiníciós fájlok

1.10. Mi vezethet rosszindulatú programkódok telepítéséhez?

- a) a makrók letiltása az alkalmazásokban
- b) hátsó kapu használata a rendszerbiztonság megkerüléséhez
- c) a "vis maior" esetekre való hivatkozás
- d) biometrikus védelem alkalmazása a felhasználók személyazonosságának megállapításához

1.11. Melyik egy fertőző rosszindulatú szoftver?

- a) a féreg
- b) a süti
- c) a tűzfal
- d) a digitális tanúsítvány

1.12. Melyik igaz a rosszindulatú programkódokra?







- a) a billentyűzetleütés naplózás a begépelte adatot rögzíti
- b) billentyűzet-leütés naplózását a <shift> billentyű lenyomásával lehet engedélyezni a számítógépen
- c) a modemes tárcsázó egy szoftver, ami szűri az interneten végzett telefonhívásokat
- d) a modemes tárcsázó egy személy, aki telefonhívásokat végez az interneten

1.13. Hogyan működnek a vírusirtó szoftverek?

- a) fertőzésmentesített fájlokat helyeznek a karanténba
- b) észlelik a vírusokat, de nem törlik automatikusan őket
- c) észlelik a vírusokat, de nem képesek felismerni a trójai programokat
- d) ütemezett keresést használnak a vírusok észlelésére

1.14. Mi a virtuális magánhálózat (VPN)?

- a) nem kell jelszó a hálózati csatlakozáshoz
- b) megengedi bárki csatlakozását egy magánhálózathoz
- c) biztonságos saját hozzáférést biztosít a hálózathoz
- d) kis földrajzi területen több összekötött számítógép együttese

- 1.15. Mi a tűzfal korlátja?
- fertőzött fájlokat helyez a karanténba
 - nem értesít automatikusan a hálózati behatoláskor
 - csökkenti a rosszindulatú programkódok hálózatban való megjelenésének lehetőségét
 - nem lehet létrehozni további szabályokat a bejövő hálózati forgalom kezelésére
- 1.16. Melyik ikon jelenti a drótnélküli hálózatot?
- 
 - 
 - 
 - 
- 1.17. Mi a biztonsági kihatása a hálózatra való csatlakozásnak?
- nem lehet hozzáférni a privát hálózathoz
 - megfertőződhet a számítógép rosszindulatú szoftverekkel
 - a fájlokhoz történő hozzáférés a hálózaton keresztül lelassul
 - az összes internetről letöltött és ideiglenesen tárolt fájl törlődik
- 1.18. Miért szükséges jelszó alkalmazása a drótnélküli hálózatok hozzáféréséhez?
- megelőzi a hálózathoz való csatlakozási késedelmet
 - biztosítja a vírusirtó szoftver naprakészségét
 - így csak jogos felhasználó használhatja a hálózatot
 - megvédi a hálózati tűzfalat
- 1.19. Melyik biometria védelem?
- adatok mentése
 - bankkártya lemásolása
 - kikérdezés
 - retina-szkennelés
- 1.20. Mihez kell ragaszkodni egy on-line pénzügyi tranzakció elvégzésekor?
- a web-oldal biztonságához
 - az automatikus kiterjesztés bekapcsolásához
 - a Lomtárnak a tranzakciót követő kiürítéséhez
 - a tranzakciót követő elektromágneses törléshez
- 1.21. Melyik ikon jelzi a biztonságos web-oldalt?
- 
 - 

c)



d)



- 1.22. Melyik támadás irányítja át a web-oldal forgalmát egy hamisított web-oldalra?
- a) crackelés
 - b) eltérítései adathalászat
 - c) etikus hackelés
 - d) információ-szerzés
- 1.23. Melyik a böngészők által a számítógépen tárolt apró szöveg?
- a) tűzfal
 - b) trójai program
 - c) rendszerszinten rejtőző kártékony kód
 - d) süti
- 1.24. Mitől kell tartanunk a közösségi média használatakor?
- a) biometria
 - b) etikus hackelés
 - c) internetes zaklatás
 - d) titkosított fájlok
- 1.25. Mi biztosítja azt, hogy csak a címzettek olvashassanak el egy elektronikus levelet?
- a) az elektronikus levél aláírással való ellátása
 - b) az elektronikus levél titkosítása
 - c) egyszerű szöveges elektronikus levél formázása
 - d) definíciós fájl hozzáadása az elektronikus levélhez
- 1.26. Mi használ bejegyzett cégneveket személyes biztonsági adatok megszerzéséhez?
- a) adathalászat
 - b) kifigyelés
 - c) billentyűzet-leütés naplózás
 - d) zombi-hálózati szoftver
- 1.27. Mi a valós idejű szöveges kommunikáció két vagy több személy között?
- a) elektronikus levél
 - b) fájl-megosztás
 - c) eltérítései adathalászat
 - d) azonnali üzenetküldés
- 1.28. Mi segít biztosítani a bizalmasságot az azonnali üzenetküldés során?
- a) a tűzfal bekapcsolása
 - b) a tűzfal kikapcsolása
 - c) a fájl-megosztás korlátozása
 - d) titkosítás használata

- 1.29. Mi használható az eszközök fizikai biztonságának növelésére?
- vírusirtó szoftver
 - titkosított szöveges dokumentumok
 - biztonsági kábel
 - elektromagnetikus törlés
- 1.30. Melyik módszer törli visszaállíthatatlanul az adatokat?
- az adatok Lomtárba mozgatása
 - az adatokat tartalmazó lemez bedarálása
 - jelszavas tömörítés alkalmazása
 - adatok titkosított merevlemezre való elhelyezése
2. Keresse meg a vizsgaközpont által megadott mappában található **iroszer.doc** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a **safe** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **ertesites.xls** fájlról a **juliusi_mentes** könyvtárba! [1 pont]
- Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

9. FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
- 1.1. Mi a "jelszó crackelés" jelentése?
- személyes adatokat lopni on-line módon
 - rendszeresen megváltoztatni a jelszót az előírásoknak megfelelően
 - nem megfelelő jelszavak egymás utáni bevitele
 - a jelszó nyílt szöveges verziójának megszerzése
- 1.2. Mi jelent fenyegetést az adatokra?
- titkosítás
 - emberi tevékenység
 - biometria
 - süтик
- 1.3. Mi az üzletileg érzékeny információk védelmének célja?
- biztosítani a makrók engedélyezését
 - megakadályozni a vírusok terjedését
 - megelőzni az ügyfelek adataival való visszaélést
 - megakadályozni az internetes zaklatást
- 1.4. Mi akadályozza meg az adatokhoz való jogosulatlan hozzáférést?
- a fájlok tömörítése
 - internet-szűrő alkalmazása
 - adatmentés készítése
 - jelszóhasználat
- 1.5. Melyik az európai adatvédelmi szabályozás?
- 1995 Európai Adatvédelmi Irányelv
 - 2001 Információs Társadalom Irányelv
 - 1995 Európai Adat Információ Szabályzat
 - 2002 Irányelv a személyes adatok védelméhez és az elektronikus kommunikációhoz
- 1.6. Melyik a személyazonosság-lopás leírása?
- felhasználói név használata az interneten
 - felvenni más személy azonosságát haszonszerzés céljából
 - munkahelyi adatok megadása internetes vásárláskor
 - tartalomellenőrző szoftverek használata internetezés közben
- 1.7. Mi a makrók tiltásának hatása?
- a makró nem fog futni
 - a makró törölve lesz a fájlból

- c) a makró még mindig helyesen fog futni
- d) a makró akkor fog működni, ha a tűzfal be van kapcsolva

1.8. Mi a titkosított adatok előnye?

- a) nem lehet törölni
- b) gyorsabban lehet menteni
- c) nem tartalmazhatnak vírusokat vagy rosszindulatú kódokat
- d) kulcs nélkül nem lehet elolvasni

1.9. Melyik célja a tulajdonos engedélye nélkül a számítógépre való feltelepülés?

- a) tűzfal
- b) tartalomellenőrző szoftver
- c) rosszindulatú programkód
- d) vírusirtó szoftver és vírusdefiníciós fájlok

1.10. Mi vezethet rosszindulatú programkódok telepítéséhez?

- a) a makrók letiltása az alkalmazásokban
- b) hátsó kapu használata a rendszerbiztonság megkerüléséhez
- c) a "vis maior" esetekre való hivatkozás
- d) biometrikus védelem alkalmazása a felhasználók személyazonosságának megállapításához

1.11. Melyik egy fertőző rosszindulatú szoftver?

- a) a féreg
- b) a süti
- c) a tűzfal
- d) a digitális tanúsítvány

1.12. Melyik igaz a rosszindulatú programkódokra?





- a) a billentyűzetleütés naplózás a begépelte adatot rögzíti
- b) billentyűzet-leütés naplózását a <shift> billentyű lenyomásával lehet engedélyezni a számítógépen
- c) a modemes tárcsázó egy szoftver, ami szűri az interneten végzett telefonhívásokat
- d) a modemes tárcsázó egy személy, aki telefonhívásokat végez az interneten

1.13. Hogyan működnek a vírusirtó szoftverek?

- a) fertőzésmentesített fájlokat helyeznek a karanténba
- b) észlelik a vírusokat, de nem törlik automatikusan őket
- c) észlelik a vírusokat, de nem képesek felismerni a trójai programokat
- d) ütemezett keresést használnak a vírusok észlelésére

1.14. Mi a virtuális magánhálózat (VPN)?

- a) nem kell jelszó a hálózati csatlakozáshoz
- b) megengedi bárki csatlakozását egy magánhálózathoz
- c) biztonságos saját hozzáférést biztosít a hálózathoz
- d) kis földrajzi területen több összekötött számítógép együttese

- 1.15. Mi a tűzfal korlátja?
- fertőzött fájlokat helyez a karanténba
 - nem értesít automatikusan a hálózati behatoláskor
 - csökkenti a rosszindulatú programkódok hálózatban való megjelenésének lehetőségét
 - nem lehet létrehozni további szabályokat a bejövő hálózati forgalom kezelésére
- 1.16. Mi akadályozza meg a jogosulatlan belépést a hálózatba egy külső helyszínről?
- elektromágneses törlés
 - tűzfalak
 - adathalászat
 - digitális tanúsítványok
- 1.17. Melyik ikon jelenti a csatlakoztatható vezetékes hálózatot?
- 
 - 
 - 
 - 
- 1.18. Mi a hálózatra történő csatlakozás biztonsági vonatkozása?
- adatok biztonsági mentése
 - fájlok tömörítése
 - személyes adatok védelme
 - információbúvárkodás
- 1.19. Miért kell jelszóval védeni a vezeték nélküli hálózatokat?
- elindítja a vírusirtó szoftvert
 - megakadályozza a jogosulatlan adat-hozzáférést
 - biztosítja a süti engedélyezését
 - megakadályozza az adathalászatra irányuló támadásokat
- 1.20. Mi igazolja, hogy az üzenet küldője valóban az, akinek állítja magát?
- digitális tanúsítvány
 - süti
 - makró
 - letöltött és ideiglenesen tárolt internet fájlok
- 1.21. Mikor használnak egyszer használatos jelszót?
- a laptopra való első bejelentkezéskor
 - amikor a jelszót elküldik e-mailben
 - amikor tűzfalat állítanak be
 - VPN-be való bejelentkezéskor

- 1.22. Melyik adat törölhető a böngésző által?
- a) kititkosított adat
 - b) titkosított adat
 - c) automatikus kiegészítés adata
 - d) billentyűzet-leütéseket naplózó adat
- 1.23. Melyikkel korlátozható az interneten töltött időtartam?
- a) adathalász szoftver
 - b) szülői felügyelet szoftver
 - c) tárcsázó
 - d) süti
- 1.24. Melyik a közösségi oldalakon előforduló fenyegetés?
- a) bedarálás
 - b) elektromágneses törlés
 - c) bankkártya adatainak a lemásolása
 - d) szexuális kizsákmányolás
- 1.25. Milyen eljárás biztosítja az e-mailek bizalmasságát?
- a) titkosítás
 - b) kikérdezés
 - c) eltérítéssel adathalászat
 - d) kititkosítás
- 1.26. Mi a digitális aláírás eszköze?
- a) szoftver, ami átirányítja egy weboldal forgalmát egy hamisított weboldalra
 - b) egy matematikai séma az üzenet hitelességének biztosítására
 - c) egy bonyolult módszer, mely beszűri az aláírást az üzenet végére
 - d) szoftver, mely engedélyezési és tiltólistákat alkalmaz a bejövő hálózati forgalom irányítására
- 1.27. Melyik fogalom írja le a banki adatokat bekérő hamisított elektronikus leveleket?
- a) kifigyelés
 - b) internetes zaklatás
 - c) adathalászat
 - d) crackelés
- 1.28. Mi tartalmazhat rosszindulatú programkódot?
- a) levélcsatolmány
 - b) süti
 - c) tűzfal
 - d) digitális aláírás
- 1.29. Melyik nyújt védelmet az adatvesztés ellen?
- a) süti
 - b) kikérdezés

- c) titkosított USB lemez használata
- d) mentések

1.30. Miért van szükség az adatok visszaállíthatatlan törlésére?

- a) az áramingadozásból adódó meghibásodások miatt
- b) az adatok más általi visszaállíthatatlansága miatt
- c) hogy tartalomellenőrző szoftvert lehessen telepíteni
- d) hogy törölni lehessen minden sütit

2. Nyissa meg a vizsgaközpont által megadott mappában található **biztonsag.doc** fájlt! Tegye megnyitás-védetté a fájlt, a **guard** jelszó használatával! Mentse el és zárja be a **biztonsag** fájlt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **promocio.ppt** fájlról az **aprilisi_mentes** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

10.FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
- 1.1. Mi a "jelszó crackelés" jelentése?
- személyes adatokat lopni on-line módon
 - rendszeresen megváltoztatni a jelszót az előírásoknak megfelelően
 - nem megfelelő jelszavak egymás utáni bevitele
 - a jelszó nyílt szöveges verziójának megszerzése
- 1.2. Mi jelent fenyegetést az adatokra?
- titkosítás
 - emberi tevékenység
 - biometria
 - sütik
- 1.3. Mi az üzletileg érzékeny információk védelmének célja?
- biztosítani a makrók engedélyezését
 - megakadályozni a vírusok terjedését
 - megelőzni az ügyfelek adataival való visszaélést
 - megakadályozni az internetes zaklatást
- 1.4. Mi akadályozza meg az adatokhoz való jogosulatlan hozzáférést?
- a fájlok tömörítése
 - internet-szűrő alkalmazása
 - adatmentés készítése
 - jelszóhasználat
- 1.5. Melyik az európai adatvédelmi szabályozás?
- 1995 Európai Adatvédelmi Irányelv
 - 2001 Információs Társadalom Irányelv
 - 1995 Európai Adat Információ Szabályzat
 - 2002 Irányelv a személyes adatok védelméhez és az elektronikus kommunikációhoz
- 1.6. Melyik a személyazonosság-lopás leírása?
- felhasználói név használata az interneten
 - felvenni más személy azonosságát haszonszerzés céljából
 - munkahelyi adatok megadása internetes vásárláskor
 - tartalomellenőrző szoftverek használata internetezés közben
- 1.7. Mi a makrók tiltásának hatása?
- a makró nem fog futni
 - a makró törölve lesz a fájlból

- c) a makró még mindig helyesen fog futni
- d) a makró akkor fog működni, ha a tűzfal be van kapcsolva

1.8. Mi a titkosított adatok előnye?

- a) nem lehet törölni
- b) gyorsabban lehet menteni
- c) nem tartalmazhatnak vírusokat vagy rosszindulatú kódokat
- d) kulcs nélkül nem lehet elolvasni

1.9. Melyik célja a tulajdonos engedélye nélkül a számítógépre való feltelepülés?

- a) tűzfal
- b) tartalomellenőrző szoftver
- c) rosszindulatú programkód
- d) vírusirtó szoftver és vírusdefiníciós fájlok

1.10. Mi vezethet rosszindulatú programkódok telepítéséhez?

- a) a makrók letiltása az alkalmazásokban
- b) hátsó kapu használata a rendszerbiztonság megkerüléséhez
- c) a "vis maior" esetekre való hivatkozás
- d) biometrikus védelem alkalmazása a felhasználók személyazonosságának megállapításához

1.11. Melyik egy fertőző rosszindulatú szoftver?

- a) a féreg
- b) a süti
- c) a tűzfal
- d) a digitális tanúsítvány

1.12. Melyik igaz a rosszindulatú programkódokra?

- a) a billentyűzetleütés naplózás a begépelte adatot rögzíti
- b) billentyűzet-leütés naplózását a <shift> billentyű lenyomásával lehet engedélyezni a számítógépen
- c) a modemes tárcsázó egy szoftver, ami szűri az interneten végzett telefonhívásokat
- d) a modemes tárcsázó egy személy, aki telefonhívásokat végez az interneten

1.13. Hogyan működnek a vírusirtó szoftverek?

- a) fertőzésmentesített fájlokat helyeznek a karanténba
- b) észlelik a vírusokat, de nem törlik automatikusan őket
- c) észlelik a vírusokat, de nem képesek felismerni a trójai programokat
- d) ütemezett keresést használnak a vírusok észlelésére

1.14. Mi a virtuális magánhálózat (VPN)?

- a) nem kell jelszó a hálózati csatlakozáshoz
- b) megengedi bárki csatlakozását egy magánhálózathoz
- c) biztonságos saját hozzáférést biztosít a hálózathoz
- d) kis földrajzi területen több összekötött számítógép együttese





1.15. Mi a tűzfal korlátja?

- a) fertőzött fájlokat helyez a karanténba
- b) nem értesít automatikusan a hálózati behatolásakor
- c) csökkenti a rosszindulatú programkódok hálózatban való megjelenésének lehetőségét
- d) nem lehet létrehozni további szabályokat a bejövő hálózati forgalom kezelésére

1.16. Mi eredményezhet jogosulatlan adathozzáférést?

- a) elektromágneses törlés
- b) adat-hozzáférés vezeték nélküli forgalom lehallgatásakor
- c) biometrikus védelmi intézkedésen alapuló hozzáférés-védelmi szoftver telepítése
- d) digitális tanúsítvány

1.17. Melyik ikon jelzi a nem védett vezeték nélküli hálózatot?

- a) 
- b) 
- c) 
- d) 

1.18. Hogyan történik a hálózati bejelentkezés?

- a) felhasználói névvel és jelszóval
- b) automatikus kiegészítéssel
- c) titkosított felhasználói névvel
- d) digitális tanúsítvánnyal




1.19. Melyik a jó szabály a jelszavakra?

- a) használjon minél kevesebb karaktert a jelszóban
- b) időnként változtassa meg a jelszavát
- c) ossza meg a jelszavát a barátaival
- d) a jelszóban sose használjon vegyesen betűket és számokat

1.20. Melyik weboldalnál található http előtag a https helyett?

- a) on-line bank
- b) keresőmotor
- c) on-line webáruház
- d) biztonságos weboldal

1.21. Melyik jelöli a biztonságos weboldalakat?

- a) 
- b) 
- c) 



d)

- 1.22. Mely fájlok tartalmazhatnak nyilvános kulcsokat és más hitelesítő adatokat?
- vírusdefiníciós fájlok
 - titkosított adatbázis-mentési fájlok
 - makrók
 - digitális tanúsítványok
- 1.23. Miért kell a sütitket blokkolni a böngészőkben?
- hogy vírusirtó szoftvert lehessen telepíteni
 - hogy hozzá lehessen férni a web-alapú elektronikus levelezési fiókokhoz
 - hogy böngészhessünk ismeretlen weblapokon
 - hogy megakadályozzuk az internetes zaklatást
- 1.24. Mi lenne az eredménye annak, ha egy közösségi oldalon a személyes adatokat a nyilvánosság számára hozzáférhetővé tennénk?
- a személyes adatokhoz csak a barátok férhetnének hozzá
 - a személyes adatokat bárki megnézheti
 - a barátok barátai láthatnák a személyes adatokat
 - a barátok módosíthatnák a személyes adatokat
- 1.25. Mi tartalmazhat rosszindulatú programkódot vagy vírust?
- X509v3 digitális tanúsítványok
 - tűzfalak
 - digitális aláírások
 - csalárd elektronikus levelek
- 1.26. Mi használja az adatok megszerzéséhez hamisított weboldalak linkjeit?
- rendszerszinten tevékenykedő kártékony kódok
 - tárcsázó programok
 - adathalászat
 - bankkártya-lemásolás
- 1.27. Miért NEM szabad megnyitni egy ismeretlen csatolmányt?
- rosszindulatú programkódokat tartalmazhat
 - lehet, hogy nagyon nagy a fájl
 - lehet, hogy titkosító kulcs szükséges a megnyitáshoz
 - lehetséges, hogy digitális tanúsítványt tartalmaz
- 1.28. Melyik lehet az azonnali üzenetküldés sebezhetősége?
- vírusdefiníciós fájlok
 - on-line emelt díjas tárcsázó programok
 - digitális tanúsítványok
 - rosszindulatú programkódok

- 1.29. Melyik egy lehetséges mentési tulajdonság?
- a) bankkártya lemásolás
 - b) ütemezés
 - c) kikérdezés
 - d) elektromágneses törlés
- 1.30. Mi NEM eredményezi az adatok végleges törlését?
- a) az adatok átmozgatása a Lomtárba
 - b) a háttértároló elektromágneses törlése
 - c) a szoftveres adatmegsemmisítő eszközök használata
 - d) a DVD-k bedarálása
2. Keresse meg a vizsgaközpont által megadott mappában található **level.doc** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a **lock** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **halozat.doc** fájlról a **marciusi_mentes** könyvtárba! [1 pont]
- Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

11.FELADAT

1. Nyissa meg a válaszfájl nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
- 1.1. Mi az információ információbiztonsági szempontból?
- a) adatfeldolgozás kimenete
 - b) logikai állítások kombinációja
 - c) nyers és nem szervezett tények összessége
 - d) feldolgozandó ábrák
- 1.2. Melyik tevékenység jogellenes internet vagy számítógéphasználat közben?
- a) etikus hackelés
 - b) elektromágneses megsemmisítés
 - c) kiberbűnözés
 - d) digitális aláírás
- 1.3. Mi NEM fenyegeti az adatokat?
- a) emberi tevékenység
 - b) zombi-hálózati szoftverek
 - c) rosszindulatú programkódok
 - d) hozzáférés-védelmi szoftverek
- 1.4. Mi az oka a személyes adatok védelmének?
- a) csalások megelőzése
 - b) sütik karbantartása
 - c) hátsó ajtó biztosítása
 - d) elektromágneses törlés
- 1.5. Melyik információbiztonsági jellemző biztosítja az adatok jogosulatlan módosítása elleni védelmét?
- a) rendelkezésre állás
 - b) sértetlenség
 - c) bizalmasság
 - d) hozzáférhetőség
- 1.6. Mi a szélhámosság közvetlen következménye?
- a) jogosulatlan hozzáférés a számítógéphez
 - b) tárhely-problémákhoz vezet
 - c) alkalmazza a sütik blokkolási beállításait
 - d) törli a könyvjelzőket a böngészőből
- 1.7. Mi a kikérdezés?
- a) szöveges üzenetküldés a telefonszolgáltató weboldaláról

- b) jelszó-visszaállítási eljárások összessége
- c) üzenetküldés azonnali üzenetküldővel
- d) személyes információk begyűjtése megtévesztéssel

1.8. Mi a titkosítás korlátja?

- a) a fájl tulajdonosa könnyen azonosítható
- b) a titkosító kulcs elvesztésével az adat könnyen helyreállítható
- c) a titkosító kulcs elvesztésével az adat használhatatlanná válik
- d) a ktitkosított adat nem felhasználható

1.9. Mi a rosszindulatú programkód?

- a) vírusirtó szoftverek rendszeres futtatásának ütemezésére használt számítógépes program
- b) engedély nélkül használt szoftverek
- c) tűzfal-beállítások ellenőrzésére használatos szoftver
- d) számítógépes rendszerekbe engedély nélküli beszivárgást lehetővé tévő szoftver

1.10. Melyik az a rosszindulatú programkód, amelyik a felhasználó engedélye nélkül gyűjt adatokat a böngészési szokásairól?

- a) kémsoftver
- b) zombi-hálózat szoftvere
- c) tárcsázók
- d) eltérítéses adathalászat

1.11. Mi az előnye a vírusirtóknak?

- a) megakadályozzák a kifigyelést
- b) frissítik a digitális tanúsítványokat
- c) felismerik a vírusokat a számítógépen
- d) megakadályozzák az információ-búvárkodást

1.12. Mi igaz a karanténban lévő fájlokra?

- a) nem lehet letölteni
- b) nem lehet fertőzésmentesíteni
- c) nem lehet törölni
- d) nem lehet megfertőzni

1.13. Miért kell vírusdefiníciós fájlokat letölteni?

- a) frissíti az ideiglenesen letöltött és tárolt fájlokat
- b) frissíti a sütiket
- c) lehetővé teszi az új fenyegetések elleni védelmet
- d) frissíti az elektromágneses törléseket végző szoftvert

1.14. Hogyan nevezik az irodában vagy otthon összekapcsolt számítógépeket?


- a) LAN
- b) VPN
- c) WAN

d) USB

1.15. Mi a hálózati adminisztrátor feladata?

- a) fenntartani az épület elektromos hálózatának folyamatos működőképességét
- b) biztosítani a hálózati adatokhoz a nyilvános hozzáférést
- c) biztosítani, hogy az adatokat ne mentsék le a rendszerbe
- d) fenntartani a munkatársak szükséges adathozzáférést a hálózaton

1.16. Melyik ikon jelenti a drótnélküli hálózatot?

a) 

b) 

c) 

d) 

1.17. Mi a biztonsági kihatása a hálózatra való csatlakozásnak?

- a) nem lehet hozzáférni a privát hálózathoz
- b) megfertőződhet a számítógép rosszindulatú szoftverekkel
- c) a fájlokhoz történő hozzáférés a hálózaton keresztül lelassul
- d) az összes internetről letöltött és ideiglenesen tárolt fájl törlődik

1.18. Miért szükséges jelszó alkalmazása a drótnélküli hálózatok hozzáférésehez?

- a) megelőzi a hálózathoz való csatlakozási késedelmet
- b) biztosítja a vírusirtó szoftver naprakészségét
- c) így csak jogos felhasználó használhatja a hálózatot
- d) megvédi a hálózati tűzfalat

1.19. Melyik biometria védelem?

- a) adatok mentése
- b) bankkártya lemásolása
- c) kikérdezés
- d) retina-szkennelés

1.20. Mihez kell ragaszkodni egy on-line pénzügyi tranzakció elvégzésekor?

- a) a web-oldal biztonságához
- b) az automatikus kiterjesztés bekapcsolásához
- c) a Lomtárnak a tranzakciót követő kiürítéséhez
- d) a tranzakciót követő elektromágneses törléshez

1.21. Melyik ikon jelzi a biztonságos web-oldalt?

a) 

b) 

c)



d)



- 1.22. Melyik támadás irányítja át a web-oldal forgalmát egy hamisított web-oldalra?
- a) crackelés
 - b) eltérítéssel adathalászat
 - c) etikus hackelés
 - d) információ-szerzés
- 1.23. Melyik a böngészők által a számítógépen tárolt apró szöveg?
- a) tűzfal
 - b) trójai program
 - c) rendszerszinten rejtőző kártékony kód
 - d) süti
- 1.24. Mitől kell tartanunk a közösségi média használatakor?
- a) biometria
 - b) etikus hackelés
 - c) internetes zaklatás
 - d) titkosított fájlok
- 1.25. Mi biztosítja azt, hogy csak a címzettek olvashassanak el egy elektronikus levelet?
- a) az elektronikus levél aláírással való ellátása
 - b) az elektronikus levél titkosítása
 - c) egyszerű szöveges elektronikus levél formázása
 - d) definíciós fájl hozzáadása az elektronikus levélhez
- 1.26. Mi használ bejegyzett cégneveket személyes biztonsági adatok megszerzéséhez?
- a) adathalászat
 - b) kifigyelés
 - c) billentyűzet-leütés naplózás
 - d) zombi-hálózati szoftver
- 1.27. Mi a valós idejű szöveges kommunikáció két vagy több személy között?
- a) elektronikus levél
 - b) fájl-megosztás
 - c) eltérítéssel adathalászat
 - d) azonnali üzenetküldés
- 1.28. Mi segít biztosítani a bizalmasságot az azonnali üzenetküldés során?
- a) a tűzfal bekapcsolása
 - b) a tűzfal kikapcsolása
 - c) a fájl-megosztás korlátozása
 - d) titkosítás használata

- 1.29. Mi használható az eszközök fizikai biztonságának növelésére?
- vírusirtó szoftver
 - titkosított szöveges dokumentumok
 - biztonsági kábel
 - elektromagnetikus törlés
- 1.30. Melyik módszer törli visszaállíthatatlanul az adatokat?
- az adatok Lomtárba mozgatása
 - az adatokat tartalmazó lemez bedarálása
 - jelszavas tömörítés alkalmazása
 - adatok titkosított merevlemezre való elhelyezése
2. Nyissa meg a vizsgaközpont által megadott mappában található **hossaferes.doc** fájlt! Tegye megnyitás-védetté a fájlt, a **guard** jelszó használatával! Mentse el és zárja be a **hossaferes** fájlt! [1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **rendszer.doc** fájlról a **juniusi_mentes** könyvtárba! [1 pont]
- Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

12. FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
- 1.1. Mi az információ információbiztonsági szempontból?
- a) adatfeldolgozás kimenete
 - b) logikai állítások kombinációja
 - c) nyers és nem szervezett tények összessége
 - d) feldolgozandó ábrák
- 1.2. Melyik tevékenység jogellenes internet vagy számítógéphasználat közben?
- a) etikus hackelés
 - b) elektromágneses megsemmisítés
 - c) kiberbűnözés
 - d) digitális aláírás
- 1.3. Mi NEM fenyegeti az adatokat?
- a) emberi tevékenység
 - b) zombi-hálózati szoftverek
 - c) rosszindulatú programkódok
 - d) hozzáférés-védelmi szoftverek
- 1.4. Mi az oka a személyes adatok védelmének?
- a) csalások megelőzése
 - b) süti karbantartása
 - c) hátsó ajtó biztosítása
 - d) elektromágneses törlés
- 1.5. Melyik információbiztonsági jellemző biztosítja az adatok jogosulatlan módosítása elleni védelmét?
- a) rendelkezésre állás
 - b) sértetlenség
 - c) bizalmasság
 - d) hozzáférhetőség
- 1.6. Mi a szélhámosság közvetlen következménye?
- a) jogosulatlan hozzáférés a számítógéphez
 - b) tárhely-problémákhoz vezet
 - c) alkalmazza a süti blokkolási beállításait
 - d) törli a könyvjelzőket a böngészőből
- 1.7. Mi a kikérdezés?
- a) szöveges üzenetküldés a telefonszolgáltató weboldaláról

- b) jelszó-visszaállítási eljárások összessége
- c) üzenetküldés azonnali üzenetküldővel
- d) személyes információk begyűjtése megtévesztéssel

1.8. Mi a titkosítás korlátja?

- a) a fájl tulajdonosa könnyen azonosítható
- b) a titkosító kulcs elvesztésével az adat könnyen helyreállítható
- c) a titkosító kulcs elvesztésével az adat használhatatlanná válik
- d) a ktitkosított adat nem felhasználható

1.9. Mi a rosszindulatú programkód?

- a) vírusirtó szoftverek rendszeres futtatásának ütemezésére használt számítógépes program
- b) engedély nélkül használt szoftverek
- c) tűzfal-beállítások ellenőrzésére használatos szoftver
- d) számítógépes rendszerekbe engedély nélküli beszivárgást lehetővé tévő szoftver

1.10. Melyik az a rosszindulatú programkód, amelyik a felhasználó engedélye nélkül gyűjt adatokat a böngészési szokásairól?

- a) kémsoftver
- b) zombi-hálózat szoftvere
- c) tárcsázók
- d) eltérítéses adathalászat

1.11. Mi az előnye a vírusirtóknak?

- a) megakadályozzák a kifizyelést
- b) frissítik a digitális tanúsítványokat
- c) felismerik a vírusokat a számítógépen
- d) megakadályozzák az információ-búvárkodást

1.12. Mi igaz a karanténban lévő fájlokra?

- a) nem lehet letölteni
- b) nem lehet fertőzésmentesíteni
- c) nem lehet törölni
- d) nem lehet megfertőzni

1.13. Miért kell vírusdefiníciós fájlokat letölteni?

- a) frissíti az ideiglenesen letöltött és tárolt fájlokat
- b) frissíti a sütiket
- c) lehetővé teszi az új fenyegetések elleni védelmet
- d) frissíti az elektromágneses törléseket végző szoftvert

1.14. Hogyan nevezik az irodában vagy otthon összekapcsolt számítógépeket?

- a) LAN
- b) VPN
- c) WAN

d) USB

1.15. Mi a hálózati adminisztrátor feladata?

- a) fenntartani az épület elektromos hálózatának folyamatos működőképességét
- b) biztosítani a hálózati adatokhoz a nyilvános hozzáférést
- c) biztosítani, hogy az adatokat ne mentse le a rendszerbe
- d) fenntartani a munkatársak szükséges adathozzáférést a hálózaton





1.16. Mi a WPA?

- a) Wired Protected Access
- b) Wi-Fi Protected Access
- c) Wired Prevention Access
- d) Wi-Fi Password Access

1.17. Mit kell figyelembe venni nem védett drótnélküli hálózat használatakor?

- a) a hálózati tűzfalat ki kell kapcsolni
- b) a sütiket frissíteni kell
- c) az adatokhoz hozzá akarnak férni mások is
- d) az egyszer használatos jelszó ki lesz kapcsolva

1.18. Melyik a védett drótnélküli hálózat ikonja?

- a) 
- b) 
- c) 
- d) 

1.19. Melyik számít jó jelszónak?

- a) jBloggs_12091980
- b) 12092010
- c) jb
- d) jenniferBloggs

1.20. Mi azonosítja a biztonságos web-oldalakat?

- a) .org
- b) .com
- c) https
- d) http

1.21. Mit jelent az eltérítéssel adathalászat (pharming)?

- a) a biztonsági forgalom irányítása tiltási és engedélyezési listákat alkalmazó szoftverrel
- b) a webforgalom átirányítása egy hamisított web-oldalra
- c) a figyelés egyik módszere

- d) az ideiglenesen letöltött és tárolt internet-fájlok megszerzése
- 1.22. Mi gyorsítja fel egy ismétlődő adatbevitelt is tartalmazó on-line űrlap kitöltését?
- a) automatikus kiegészítés
 - b) makrók tiltása
 - c) titkosítás
 - d) elektromagnetikus törlés
- 1.23. Milyen adatokat kell rendszeres időközönként ellenőrizni és törölni a böngészőből?
- a) makrókat
 - b) sütitket
 - c) digitális tanúsítványokat
 - d) vírusdefiníciós fájlokat
- 1.24. Melyik célja a weboldalakhoz való hozzáférés ellenőrzése és korlátozása?
- a) reklámokat megjelenítő szoftver
 - b) kémsoftver
 - c) adathalász szoftver
 - d) tartalomellenőrző szoftver
- 1.25. Mit nem szabad közzétenni egy közösségi oldalon?
- a) zenei érdeklődést
 - b) becenevet
 - c) otthoni címet
 - d) kedvenc televízióműsort
- 1.26. Melyik az a titkosított kód, amely egy személy azonosságát társítja egy fájlhoz?
- a) jelszavas tömörített fájl
 - b) digitális aláírás
 - c) makrózott titkosított szöveg
 - d) ideiglenesen letöltött és tárolt fájl
- 1.27. Mi az adathalászat?
- a) lopott bankkártya adatainak felhasználása on-line vásárlásnál
 - b) információkat kifigyelni valaki válla felett
 - c) félrevezetni valakit az interneten értékes információk megszerzéséért
 - d) az informatikai biztonsági hiányosságok tesztelése
- 1.28. Mi jelenti a legnagyobb kitétséget a rosszindulatú programkódoknak?
- a) hozzáférés biztonságos weboldalhoz
 - b) levélcsatolmány megnyitása
 - c) elektronikus levél írása
 - d) adatok mentése
- 1.29. Mi az azonnali üzenetküldés sebezhetősége?
- a) hátsó ajtó hozzáférés

- b) valós idejű hozzáférés
- c) vis maior
- d) információbúvárkodás

1.30. Mi jelenti az adatok végleges megsemmisítését?

- a) eltérítéssel adathalászat
- b) áramellátás kiesése
- c) tárcsázás
- d) elektromágneses törlés

2. Keresse meg a vizsgaközpont által megadott mappában található **iroszer.doc** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a **safe** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **ertekeletes.xls** fájlról a **juliusi_mentes** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

13.FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
- 1.1. Mi az információ információbiztonsági szempontból?
- a) adatfeldolgozás kimenete
 - b) logikai állítások kombinációja
 - c) nyers és nem szervezett tények összessége
 - d) feldolgozandó ábrák
- 1.2. Melyik tevékenység jogellenes internet vagy számítógéphasználat közben?
- a) etikus hackelés
 - b) elektromágneses megsemmisítés
 - c) kiberbűnözés
 - d) digitális aláírás
- 1.3. Mi NEM fenyegeti az adatokat?
- a) emberi tevékenység
 - b) zombi-hálózati szoftverek
 - c) rosszindulatú programkódok
 - d) hozzáférés-védelmi szoftverek
- 1.4. Mi az oka a személyes adatok védelmének?
- a) csalások megelőzése
 - b) süti karbantartása
 - c) hátsó ajtó biztosítása
 - d) elektromágneses törlés
- 1.5. Melyik információbiztonsági jellemző biztosítja az adatok jogosulatlan módosítása elleni védelmét?
- a) rendelkezésre állás
 - b) sértetlenség
 - c) bizalmasság
 - d) hozzáférhetőség
- 1.6. Mi a szélhámosság közvetlen következménye?
- a) jogosulatlan hozzáférés a számítógéphez
 - b) tárhely-problémákhoz vezet
 - c) alkalmazza a süti blokkolási beállításait
 - d) törli a könyvjelzőket a böngészőből
- 1.7. Mi a kikérdezés?
- a) szöveges üzenetküldés a telefonszolgáltató weboldaláról

- b) jelszó-visszaállítási eljárások összessége
- c) üzenetküldés azonnali üzenetküldővel
- d) személyes információk begyűjtése megtévesztéssel

1.8. Mi a titkosítás korlátja?

- a) a fájl tulajdonosa könnyen azonosítható
- b) a titkosító kulcs elvesztésével az adat könnyen helyreállítható
- c) a titkosító kulcs elvesztésével az adat használhatatlanná válik
- d) a ktitkosított adat nem felhasználható

1.9. Mi a rosszindulatú programkód?

- a) vírusirtó szoftverek rendszeres futtatásának ütemezésére használt számítógépes program
- b) engedély nélkül használt szoftverek
- c) tűzfal-beállítások ellenőrzésére használatos szoftver
- d) számítógépes rendszerekbe engedély nélküli beszivárgást lehetővé tévő szoftver

1.10. Melyik az a rosszindulatú programkód, amelyik a felhasználó engedélye nélkül gyűjt adatokat a böngészési szokásairól?

- a) kémsoftver
- b) zombi-hálózat szoftvere
- c) tárcsázók
- d) eltérítéses adathalászat

1.11. Mi az előnye a vírusirtóknak?

- a) megakadályozzák a kifigyelést
- b) frissítik a digitális tanúsítványokat
- c) felismerik a vírusokat a számítógépen
- d) megakadályozzák az információ-búvárkodást

1.12. Mi igaz a karanténban lévő fájlokra?

- a) nem lehet letölteni
- b) nem lehet fertőzésmentesíteni
- c) nem lehet törölni
- d) nem lehet megfertőzni

1.13. Miért kell vírusdefiníciós fájlokat letölteni?

- a) frissíti az ideiglenesen letöltött és tárolt fájlokat
- b) frissíti a sütiket
- c) lehetővé teszi az új fenyegetések elleni védelmet
- d) frissíti az elektromágneses törléseket végző szoftvert

1.14. Hogyan nevezik az irodában vagy otthon összekapcsolt számítógépeket?

- a) LAN
- b) VPN
- c) WAN

d) USB





1.15. Mi a hálózati adminisztrátor feladata?

- a) fenntartani az épület elektromos hálózatának folyamatos működőképességét
- b) biztosítani a hálózati adatokhoz a nyilvános hozzáférést
- c) biztosítani, hogy az adatokat ne mentse le a rendszerbe
- d) fenntartani a munkatársak szükséges adathozzáférést a hálózaton

1.16. Mi eredményezhet jogosulatlan adathozzáférést?

- a) elektromágneses törlés
- b) adat-hozzáférés vezeték nélküli forgalom lehallgatásakor
- c) biometrikus védelmi intézkedésen alapuló hozzáférés-védelmi szoftver telepítése
- d) digitális tanúsítvány

1.17. Melyik ikon jelzi a nem védett vezeték nélküli hálózatot?

- a) 
- b) 
- c) 
- d) 

1.18. Hogyan történik a hálózati bejelentkezés?

- a) felhasználói névvel és jelszóval
- b) automatikus kiegészítéssel
- c) titkosított felhasználói névvel
- d) digitális tanúsítvánnyal



1.19. Melyik a jó szabály a jelszavakra?

- a) használjon minél kevesebb karaktert a jelszóban
- b) időnként változtassa meg a jelszavát
- c) ossza meg a jelszavát a barátaival
- d) a jelszóban sose használjon vegyesen betűket és számokat

1.20. Melyik weboldalnál található http előtag a https helyett?

- a) on-line bank
- b) keresőmotor
- c) on-line webáruház
- d) biztonságos weboldal

1.21. Melyik jelöli a biztonságos weboldalakat?

- a) 
- b) 

c)



d)



1.22. Mely fájlok tartalmazhatnak nyilvános kulcsokat és más hitelesítő adatokat?

- a) vírusdefiníciós fájlok
- b) titkosított adatbázis-mentési fájlok
- c) makrók
- d) digitális tanúsítványok

1.23. Miért kell a sütitet blokkolni a böngészőkben?

- a) hogy vírusirtó szoftvert lehessen telepíteni
- b) hogy hozzá lehessen férni a web-alapú elektronikus levelezési fiókokhoz
- c) hogy böngészhessünk ismeretlen weblapokon
- d) hogy megakadályozzuk az internetes zaklatást

1.24. Mi lenne az eredménye annak, ha egy közösségi oldalon a személyes adatokat a nyilvánosság számára hozzáférhetővé tennénk?

- a) a személyes adatokhoz csak a barátok férhetnének hozzá
- b) a személyes adatokat bárki megnézheti
- c) a barátok barátai láthatnák a személyes adatokat
- d) a barátok módosíthatnák a személyes adatokat

1.25. Mi tartalmazhat rosszindulatú programkódot vagy vírust?

- a) X509v3 digitális tanúsítványok
- b) tűzfalak
- c) digitális aláírások
- d) csalárd elektronikus levelek

1.26. Mi használja az adatok megszerzéséhez hamisított weboldalak linkjeit?

- a) rendszerszinten tevékenykedő kártékony kódok
- b) tárcsázó programok
- c) adathalászat
- d) bankkártya-lemásolás

1.27. Miért NEM szabad megnyitni egy ismeretlen csatolmányt?

- a) rosszindulatú programkódokat tartalmazhat
- b) lehet, hogy nagyon nagy a fájl
- c) lehet, hogy titkosító kulcs szükséges a megnyitásához
- d) lehetséges, hogy digitális tanúsítványt tartalmaz

1.28. Melyik lehet az azonnali üzenetküldés sebezhetősége?

- a) vírusdefiníciós fájlok
- b) on-line emelt díjas tárcsázó programok
- c) digitális tanúsítványok

d) rosszindulatú programkódok

1.29. Melyik egy lehetséges mentési tulajdonság?

- a) bankkártya lemásolás
- b) ütemezés
- c) kikérdezés
- d) elektromágneses törlés

1.30. Mi NEM eredményezi az adatok végleges törlését?

- a) az adatok átmozgatása a Lomtárba
- b) a háttértároló elektromágneses törlése
- c) a szoftveres adatmegsemmisítő eszközök használata
- d) a DVD-k bedarálása

2. Nyissa meg a vizsgaközpont által megadott mappában található **biztonsag.doc** fájlt! Tegye megnyitás-védetté a fájlt, a **guard** jelszó használatával! Mentse el és zárja be a **biztonsag** fájlt! [1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **promocio.ppt** fájlról az **aprilisi_mentes** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

14.FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
 - 1.1. Melyik kiberbűnözés az alábbiak közül?
 - a) okostelefon ellopása
 - b) internetes számla on-line befizetése
 - c) bankkártya adatok ellopása on-line
 - d) internetes rádióhallgatása on-line
 - 1.2. Melyik eljárás tartalmazza az informatikai biztonsági sebezhetőségek tesztelését?
 - a) crackelés
 - b) etikus hackelés
 - c) bankkártya adatainak lemásolása
 - d) kikérdezés
 - 1.3. Miért kell védeni az üzletileg érzékeny információkat?
 - a) mert megakadályozza az adatlopást
 - b) ütemezett mentések lefutásának biztosítása miatt
 - c) kéretlen üzenetek blokkolása miatt
 - d) a biztonságos weboldalak azonosításáért
 - 1.4. Melyik nyújt védelmet a jogosulatlan adat-hozzáférés ellen?
 - a) bonyolult fájlnevek
 - b) billentyűzet-leütés naplózása
 - c) eltérítéssel adathalászat
 - d) titkosítás
 - 1.5. Melyik információbiztonsági tulajdonság biztosítja az adatok jogosulatlan hozzáférés vagy felfedés elleni védelmét?
 - a) bizalmasság
 - b) sértetlenség
 - c) rendelkezésre állás
 - d) hitelesség
 - 1.6. Melyik európai szabályozást kell betartani a személyes adatok védelmének vonatkozásában?
 - a) 1997 Európai Adatvédelmi Szabályozás
 - b) 2001 Európai Információs Társadalmi Irányelv
 - c) 1995 Európai Adatvédelmi Irányelv
 - d) 2001 Európai Irányelv az Információ-Technológiáról

1.7. Melyik tartozik a szélhámosság módszerei közé?

- a) közösségi oldalakhoz több fiókkal rendelkezni
- b) valaki válla fölött megszerezni az információkat
- c) videó- és hanghívásokat kezdeményezni az interneten
- d) meghivatkozni más weboldalát egy közösségi oldalról

1.8. Mi a személyazonosság-lopás közvetlen következménye?

- a) a pénzügyi adatokat mások is használhatják
- b) a vírusirtó nem működik a továbbiakban
- c) a letöltött és ideiglenesen tárolt fájlokat törölni fogják
- d) a mentés ütemezését megváltoztatják

1.9. Melyik szoftvert készítek és küldik károkozási célból?

- a) szimmetrikus vagy aszimmetrikus elvű titkosító szoftverek
- b) tűzfalak
- c) rosszindulatú programkódok
- d) vírusirtó szoftverek

1.10. Mit használnak a rosszindulatú programkódok elrejtésére?

- a) rendszerszinten tevékenykedő kártékony kódokat
- b) elektromágneses elven alapuló adattörlési módszereket
- c) tűzfalakat
- d) bedarálást

1.11. Mi egy fertőző, rosszindulatú program?

- a) a süti
- b) a vírus
- c) a digitális tanúsítvány
- d) a digitális aláírás

1.12. Melyik képes megfertőzni és irányítani egy számítógépet a tulajdonos engedélye nélkül?

- a) biometria
- b) vírus-definíciós fájl
- c) süti
- d) zombi-hálózat

1.13. Mi a vírusirtó szoftverek előnye?

- a) megvizsgálják a számítógépet hogy nem fertőződnek-e meg
- b) megakadályozzák a tartalom-ellenőrző szoftverek elindítását
- c) minden adatot mentenek
- d) a korábban törölt fájlokat visszaállítják a számítógép háttértárolójára

1.14. Mi akadályozza meg a hálózathoz kívülről történő jogosulatlan hozzáférést?

- a) fájlok hozzáférés-védelmi beállításai
- b) tartalom-ellenőrző program

- c) zombi-hálózati szoftver
- d) tűzfalak





1.15. Mi biztosítja a vezeték nélküli biztonságot?

- a) WAN
- b) LAN
- c) Média Hozzáférési Kontroll (MAC)
- d) számítógépes hálózathoz hátsó kaput nyitó szoftver

1.16. Mi a tűzfal korlátja?

- a) fertőzött fájlokat helyez a karanténba
- b) nem értesít automatikusan a hálózati behatolásakor
- c) csökkenti a rosszindulatú programkódok hálózatban való megjelenésének lehetőségét
- d) nem lehet létrehozni további szabályokat a bejövő hálózati forgalom kezelésére

1.17. Melyik ikon jelenti a csatlakoztatható vezetékes hálózatot?

- a) 
- b) 
- c) 
- d) 

1.18. Mi a hálózatra történő csatlakozás biztonsági vonatkozása?

- a) adatok biztonsági mentése
- b) fájlok tömörítése
- c) személyes adatok védelme
- d) információbúvárkodás

1.19. Miért kell jelszóval védeni a vezeték nélküli hálózatokat?

- a) elindítja a vírusirtó szoftvert
- b) megakadályozza a jogosulatlan adat-hozzáférést
- c) biztosítja a süti engedélyezését
- d) megakadályozza az adathalászatra irányuló támadásokat

1.20. Mi igazolja, hogy az üzenet küldője valóban az, akinek állítja magát?

- a) digitális tanúsítvány
- b) süti
- c) makró
- d) letöltött és ideiglenesen tárolt internet fájlok

1.21. Mikor használnak egyszer használatos jelszót?

- a) a laptopra való első bejelentkezéskor
- b) amikor a jelszót elküldik e-mailben
- c) amikor tűzfalat állítanak be

- d) VPN-be való bejelentkezéskor
- 1.22. Melyik adat törölhető a böngésző által?
- a) kititkosított adat
 - b) titkosított adat
 - c) automatikus kiegészítés adata
 - d) billentyűzet-leütéseket naplózó adat
- 1.23. Melyikkel korlátozható az interneten töltött időtartam?
- a) adathalász szoftver
 - b) szülői felügyelet szoftver
 - c) tárcsázó
 - d) sütik
- 1.24. Melyik a közösségi oldalakon előforduló fenyegetés?
- a) bedarálás
 - b) elektromágneses törlés
 - c) bankkártya adatainak a lemásolása
 - d) szexuális kizsákmányolás
- 1.25. Milyen eljárás biztosítja az e-mailek bizalmasságát?
- a) titkosítás
 - b) kikérdezés
 - c) eltérítéssel adathalászat
 - d) kititkosítás
- 1.26. Mi a digitális aláírás eszköze?
- a) szoftver, ami átirányítja egy weboldal forgalmát egy hamisított weboldalra
 - b) egy matematikai séma az üzenet hitelességének biztosítására
 - c) egy bonyolult módszer, mely beszúrja az aláírást az üzenet végére
 - d) szoftver, mely engedélyezési és tiltólistákat alkalmaz a bejövő hálózati forgalom irányítására
- 1.27. Melyik fogalom írja le a banki adatokat bekérő hamisított elektronikus leveleket?
- a) kifigyelés
 - b) internetes zaklatás
 - c) adathalászat
 - d) crackelés
- 1.28. Mi tartalmazhat rosszindulatú programkódot?
- a) levélcsatolmány
 - b) süti
 - c) tűzfal
 - d) digitális aláírás

- 1.29. Melyik nyújt védelmet az adatvesztés ellen?
- a) sütit
 - b) kikérdezés
 - c) titkosított USB lemez használata
 - d) mentések
- 1.30. Miért van szükség az adatok visszaállíthatatlan törlésére?
- a) az áramingadozásból adódó meghibásodások miatt
 - b) az adatok más általi visszaállíthatatlansága miatt
 - c) hogy tartalomellenőrző szoftvert lehessen telepíteni
 - d) hogy törölni lehessen minden sütit
2. Nyissa meg a vizsgaközpont által megadott mappában található **secure.doc** fájlt! Tegye megnyitás-védetté a fájlt, a **guard** jelszó használatával! Mentse el és zárja be a **secure** fájlt!
[1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **promotion.ppt** fájlról az **april backup** könyvtárba! [1 pont]
- Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

15.FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
- 1.1. Melyik kiberbűnözés az alábbiak közül?
- a) okostelefon ellopása
 - b) internetes számla on-line befizetése
 - c) bankkártya adatok ellopása on-line
 - d) internetes rádióhallgatása on-line
- 1.2. Melyik eljárás tartalmazza az informatikai biztonsági sebezhetőségek tesztelését?
- a) crackelés
 - b) etikus hackelés
 - c) bankkártya adatainak lemásolása
 - d) kikérdezés
- 1.3. Miért kell védeni az üzletileg érzékeny információkat?
- a) mert megakadályozza az adatlopást
 - b) ütemezett mentések lefutásának biztosítása miatt
 - c) kéretlen üzenetek blokkolása miatt
 - d) a biztonságos weboldalak azonosításáért
- 1.4. Melyik nyújt védelmet a jogosulatlan adat-hozzáférés ellen?
- a) bonyolult fájlnevek
 - b) billentyűzet-leütés naplózása
 - c) eltérítéssel adathalászat
 - d) titkosítás
- 1.5. Melyik információbiztonsági tulajdonság biztosítja az adatok jogosulatlan hozzáférés vagy felfedés elleni védelmét?
- a) bizalmasság
 - b) sértetlenség
 - c) rendelkezésre állás
 - d) hitelesség
- 1.6. Melyik európai szabályozást kell betartani a személyes adatok védelmének vonatkozásában?
- a) 1997 Európai Adatvédelmi Szabályozás
 - b) 2001 Európai Információs Társadalmi Irányelv
 - c) 1995 Európai Adatvédelmi Irányelv
 - d) 2001 Európai Irányelv az Információ-Technológiáról

1.7. Melyik tartozik a szélhámosság módszerei közé?

- a) közösségi oldalakhoz több fiókkal rendelkezni
- b) valaki válla fölött megszerezni az információkat
- c) videó- és hanghívásokat kezdeményezni az interneten
- d) meghivatkozni más weboldalát egy közösségi oldalról

1.8. Mi a személyazonosság-lopás közvetlen következménye?

- a) a pénzügyi adatokat mások is használhatják
- b) a vírusirtó nem működik a továbbiakban
- c) a letöltött és ideiglenesen tárolt fájlokat törölni fogják
- d) a mentés ütemezését megváltoztatják

1.9. Melyik szoftvert készítek és küldik károkozási célból?

- a) szimmetrikus vagy aszimmetrikus elvű titkosító szoftverek
- b) tűzfalak
- c) rosszindulatú programkódok
- d) vírusirtó szoftverek

1.10. Mit használnak a rosszindulatú programkódok elrejtésére?

- a) rendszerszinten tevékenykedő kártékony kódokat
- b) elektromágneses elven alapuló adattörlési módszereket
- c) tűzfalakat
- d) bedarálást

1.11. Mi egy fertőző, rosszindulatú program?

- a) a süti
- b) a vírus
- c) a digitális tanúsítvány
- d) a digitális aláírás

1.12. Melyik képes megfertőzni és irányítani egy számítógépet a tulajdonos engedélye nélkül?





- a) biometria
- b) vírus-definíciós fájl
- c) süti
- d) zombi-hálózat

1.13. Mi a vírusirtó szoftverek előnye?

- a) megvizsgálják a számítógépet hogy nem fertőződnek-e meg
- b) megakadályozzák a tartalom-ellenőrző szoftverek elindítását
- c) minden adatot mentenek
- d) a korábban törölt fájlokat visszaállítják a számítógép háttértárolójára

1.14. Mi akadályozza meg a hálózathoz kívülről történő jogosulatlan hozzáférést?

- a) fájlok hozzáférés-védelmi beállításai
- b) tartalom-ellenőrző program

- c) zombi-hálózati szoftver
d) tűzfalak
- 1.15. Mi biztosítja a vezeték nélküli biztonságot?
- a) WAN
b) LAN
c) Média Hozzáférési Kontroll (MAC)
d) számítógépes hálózathoz hátsó kaput nyitó szoftver
- 1.16. Mi a WPA?
- a) Wired Protected Access
b) Wi-Fi Protected Access
c) Wired Prevention Access
d) Wi-Fi Password Access
- 1.17. Mit kell figyelembe venni nem védett drótnélküli hálózat használatakor?
- a) a hálózati tűzfalat ki kell kapcsolni
b) a sütiket frissíteni kell
c) az adatokhoz hozzá akarnak férni mások is
d) az egyszer használatos jelszó ki lesz kapcsolva
- 1.18. Melyik a védett drótnélküli hálózat ikonja?
- a) 
- b) 
- c) 
- d) 
- 1.19. Melyik számít jó jelszónak?
- a) jBloggs_12091980
b) 12092010
c) jb
d) jenniferBloggs
- 1.20. Mi azonosítja a biztonságos web-oldalakat?
- a) .org
b) .com
c) https
d) http
- 1.21. Mit jelent az eltérítéssel adathalászat (pharming)?
- a) a biztonsági forgalom irányítása tiltási és engedélyezési listákat alkalmazó szoftverrel
b) a webforgalom átirányítása egy hamisított web-oldalra

- c) a figyelés egyik módszere
 - d) az ideiglenesen letöltött és tárolt internet-fájlok megszerzése
- 1.22. Mi gyorsítja fel egy ismétlődő adatbevitelt is tartalmazó on-line űrlap kitöltését?
- a) automatikus kiegészítés
 - b) makrók tiltása
 - c) titkosítás
 - d) elektromagnetikus törlés
- 1.23. Milyen adatokat kell rendszeres időközönként ellenőrizni és törölni a böngészőből?
- a) makrókat
 - b) sütitket
 - c) digitális tanúsítványokat
 - d) vírusdefiníciós fájlokat
- 1.24. Melyik célja a weboldalakhoz való hozzáférés ellenőrzése és korlátozása?
- a) reklámokat megjelenítő szoftver
 - b) kémsoftver
 - c) adathalász szoftver
 - d) tartalomellenőrző szoftver
- 1.25. Mit nem szabad közzétenni egy közösségi oldalon?
- a) zenei érdeklődést
 - b) becenevet
 - c) otthoni címet
 - d) kedvenc televízióműsort
- 1.26. Melyik az a titkosított kód, amely egy személy azonosságát társítja egy fájlhoz?
- a) jelszavas tömörített fájl
 - b) digitális aláírás
 - c) makrözött titkosított szöveg
 - d) ideiglenesen letöltött és tárolt fájl
- 1.27. Mi az adathalászat?
- a) lopott bankkártya adatainak felhasználása on-line vásárlásnál
 - b) információkat figyelni valaki válla felett
 - c) félrevezetni valakit az interneten értékes információk megszerzéséért
 - d) az informatikai biztonsági hiányosságok tesztelése
- 1.28. Mi jelenti a legnagyobb kitétséget a rosszindulatú programkódoknak?
- a) hozzáférés biztonságos weboldalhoz
 - b) levélcsatolmány megnyitása
 - c) elektronikus levél írása
 - d) adatok mentése

1.29. Mi az azonnali üzenetküldés sebezhetősége?

- a) hátsó ajtó hozzáférés
- b) valós idejű hozzáférés
- c) vis maior
- d) információbúvárkodás

1.30. Mi jelenti az adatok végleges megsemmisítését?

- a) eltérítéssel adathalásza
- b) áramellátás kiesése
- c) tárcsázás
- d) elektromágneses törlés

2. Keresse meg a vizsgaközpont által megadott mappában található **letter.doc**! Tömörítse össze a fájlt és tegye megnyitásvédetté a **lock** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **network.doc** fájlról a **march** backup könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

16.FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
 - 1.1. Melyik kiberbűnözés az alábbiak közül?
 - a) okostelefon ellopása
 - b) internetes számla on-line befizetése
 - c) bankkártya adatok ellopása on-line
 - d) internetes rádióhallgatása on-line
 - 1.2. Melyik eljárás tartalmazza az informatikai biztonsági sebezhetőségek tesztelését?
 - a) crackelés
 - b) etikus hackelés
 - c) bankkártya adatainak lemásolása
 - d) kikérdezés
 - 1.3. Miért kell védeni az üzletileg érzékeny információkat?
 - a) mert megakadályozza az adatlopást
 - b) ütemezett mentések lefutásának biztosítása miatt
 - c) kéretlen üzenetek blokkolása miatt
 - d) a biztonságos weboldalak azonosításáért
 - 1.4. Melyik nyújt védelmet a jogosulatlan adat-hozzáférés ellen?
 - a) bonyolult fájlnevek
 - b) billentyűzet-leütés naplózása
 - c) eltérítéssel adathalászat
 - d) titkosítás
 - 1.5. Melyik információbiztonsági tulajdonság biztosítja az adatok jogosulatlan hozzáférés vagy felfedés elleni védelmét?
 - a) bizalmasság
 - b) sértetlenség
 - c) rendelkezésre állás
 - d) hitelesség
 - 1.6. Melyik európai szabályozást kell betartani a személyes adatok védelmének vonatkozásában?
 - a) 1997 Európai Adatvédelmi Szabályozás
 - b) 2001 Európai Információs Társadalmi Irányelv
 - c) 1995 Európai Adatvédelmi Irányelv
 - d) 2001 Európai Irányelv az Információ-Technológiáról

1.7. Melyik tartozik a szélhámosság módszerei közé?

- a) közösségi oldalakhoz több fiókkal rendelkezni
- b) valaki válla fölött megszerezni az információkat
- c) videó- és hanghívásokat kezdeményezni az interneten
- d) meghivatkozni más weboldalát egy közösségi oldalról

1.8. Mi a személyazonosság-lopás közvetlen következménye?

- a) a pénzügyi adatokat mások is használhatják
- b) a vírusirtó nem működik a továbbiakban
- c) a letöltött és ideiglenesen tárolt fájlokat törölni fogják
- d) a mentés ütemezését megváltoztatják

1.9. Melyik szoftvert készítek és küldik károkozási célból?

- a) szimmetrikus vagy aszimmetrikus elvű titkosító szoftverek
- b) tűzfalak
- c) rosszindulatú programkódok
- d) vírusirtó szoftverek

1.10. Mit használnak a rosszindulatú programkódok elrejtésére?

- a) rendszerszinten tevékenykedő kártékony kódokat
- b) elektromágneses elven alapuló adattörlési módszereket
- c) tűzfalakat
- d) bedarálást

1.11. Mi egy fertőző, rosszindulatú program?

- a) a süti
- b) a vírus
- c) a digitális tanúsítvány
- d) a digitális aláírás

1.12. Melyik képes megfertőzni és irányítani egy számítógépet a tulajdonos engedélye nélkül?

- a) biometria
- b) vírus-definíciós fájl
- c) süti
- d) zombi-hálózat

1.13. Mi a vírusirtó szoftverek előnye?

- a) megvizsgálják a számítógépet hogy nem fertőződnek-e meg
- b) megakadályozzák a tartalom-ellenőrző szoftverek elindítását
- c) minden adatot mentenek
- d) a korábban törölt fájlokat visszaállítják a számítógép háttértárolójára

1.14. Mi akadályozza meg a hálózathoz kívülről történő jogosulatlan hozzáférést?





- a) fájlok hozzáférés-védelmi beállításai
- b) tartalom-ellenőrző program

- c) zombi-hálózati szoftver
- d) tűzfalak

1.15. Mi biztosítja a vezeték nélküli biztonságot?

- a) WAN
- b) LAN
- c) Média Hozzáférési Kontroll (MAC)
- d) számítógépes hálózathoz hátsó kaput nyitó szoftver

1.16. Melyik ikon jelenti a drótnélküli hálózatot?

- a) 
- b) 
- c) 
- d) 

1.17. Mi a biztonsági kihatása a hálózatra való csatlakozásnak?

- a) nem lehet hozzáférni a privát hálózathoz
- b) megfertőződhet a számítógép rosszindulatú szoftverekkel
- c) a fájlokhoz történő hozzáférés a hálózaton keresztül lelassul
- d) az összes internetről letöltött és ideiglenesen tárolt fájl törlődik

1.18. Miért szükséges jelszó alkalmazása a drótnélküli hálózatok hozzáféréséhez?

- a) megelőzi a hálózathoz való csatlakozási késedelmet
- b) biztosítja a vírusirtó szoftver naprakészségét
- c) így csak jogos felhasználó használhatja a hálózatot
- d) megvédi a hálózati tűzfalat

1.19. Melyik biometria védelem?




- a) adatok mentése
- b) bankkártya lemásolása
- c) kikérdezés
- d) retina-szkennelés

1.20. Mihez kell ragaszkodni egy on-line pénzügyi tranzakció elvégzésekor?

- a) a web-oldal biztonságához
- b) az automatikus kiterjesztés bekapcsolásához
- c) a Lomtárnak a tranzakciót követő kiürítéséhez
- d) a tranzakciót követő elektromágneses törléshez

1.21. Melyik ikon jelzi a biztonságos web-oldalt?

- a) 

- b) 
- c) 
- d) 

- 1.22. Melyik támadás irányítja át a web-oldal forgalmát egy hamisított web-oldalra?
- a) crackelés
 - b) eltérítéssel adathalászat
 - c) etikus hackelés
 - d) információ-szerzés
- 1.23. Melyik a böngészők által a számítógépen tárolt apró szöveg?
- a) tűzfal
 - b) trójai program
 - c) rendszerszinten rejtőző kártékony kód
 - d) süti
- 1.24. Mitől kell tartanunk a közösségi média használatakor?
- a) biometria
 - b) etikus hackelés
 - c) internetes zaklatás
 - d) titkosított fájlok
- 1.25. Mi biztosítja azt, hogy csak a címzettek olvashassanak el egy elektronikus levelet?
- a) az elektronikus levél aláírással való ellátása
 - b) az elektronikus levél titkosítása
 - c) egyszerű szöveges elektronikus levél formázása
 - d) definíciós fájl hozzáadása az elektronikus levélhez
- 1.26. Mi használ bejegyzett cégneveket személyes biztonsági adatok megszerzéséhez?
- a) adathalászat
 - b) figyelés
 - c) billentyűzet-leütés naplózás
 - d) zombi-hálózati szoftver
- 1.27. Mi a valós idejű szöveges kommunikáció két vagy több személy között?
- a) elektronikus levél
 - b) fájl-megosztás
 - c) eltérítéssel adathalászat
 - d) azonnali üzenetküldés
- 1.28. Mi segít biztosítani a bizalmasságot az azonnali üzenetküldés során?
- a) a tűzfal bekapcsolása
 - b) a tűzfal kikapcsolása

- c) a fájl-megosztás korlátozása
 - d) titkosítás használata
- 1.29. Mi használható az eszközök fizikai biztonságának növelésére?
- a) vírusirtó szoftver
 - b) titkosított szöveges dokumentumok
 - c) biztonsági kábel
 - d) elektromagnetikus törlés
- 1.30. Melyik módszer törli visszaállíthatatlanul az adatokat?
- a) az adatok Lomtárba mozgatása
 - b) az adatokat tartalmazó lemez bedarálása
 - c) jelszavas tömörítés alkalmazása
 - d) adatok titkosított merevlemezre való elhelyezése
2. Nyissa meg a vizsgaközpont által megadott mappában található **access.doc** fájlt! Tegye megnyitás-védetté a fájlt, a **guard** jelszó használatával! Mentse el és zárja be az **access** fájlt!
[1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **system.doc** fájlról a **june backup** könyvtárba! [1 pont]
- Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

17.FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
- 1.1. Mi a "jelszó crackelés" jelentése?
- a) személyes adatokat lopni on-line módon
 - b) rendszeresen megváltoztatni a jelszót az előírásoknak megfelelően
 - c) nem megfelelő jelszavak egymás utáni bevitele
 - d) a jelszó nyílt szöveges verziójának megszerzése
- 1.2. Mi jelent fenyegetést az adatokra?
- a) titkosítás
 - b) emberi tevékenység
 - c) biometria
 - d) sütik
- 1.3. Mi az üzletileg érzékeny információk védelmének célja?
- a) biztosítani a makrók engedélyezését
 - b) megakadályozni a vírusok terjedését
 - c) megelőzni az ügyfelek adataival való visszaélést
 - d) megakadályozni az internetes zaklatást
- 1.4. Mi akadályozza meg az adatokhoz való jogosulatlan hozzáférést?
- a) a fájlok tömörítése
 - b) internet-szűrő alkalmazása
 - c) adatmentés készítése
 - d) jelszóhasználat
- 1.5. Melyik az európai adatvédelmi szabályozás?
- a) 1995 Európai Adatvédelmi Irányelv
 - b) 2001 Információs Társadalom Irányelv
 - c) 1995 Európai Adat Információ Szabályzat
 - d) 2002 Irányelv a személyes adatok védelméhez és az elektronikus kommunikációhoz
- 1.6. Melyik a személyazonosság-lopás leírása?
- a) felhasználói név használata az interneten
 - b) felvenni más személy azonosságát haszonszerzés céljából
 - c) munkahelyi adatok megadása internetes vásárláskor
 - d) tartalomellenőrző szoftverek használata internetezés közben
- 1.7. Mi a makrók tiltásának hatása?
- a) a makró nem fog futni
 - b) a makró törölve lesz a fájlból

- c) a makró még mindig helyesen fog futni
- d) a makró akkor fog működni, ha a tűzfal be van kapcsolva

1.8. Mi a titkosított adatok előnye?

- a) nem lehet törölni
- b) gyorsabban lehet menteni
- c) nem tartalmazhatnak vírusokat vagy rosszindulatú kódokat
- d) kulcs nélkül nem lehet elolvasni

1.9. Melyik célja a tulajdonos engedélye nélkül a számítógépre való feltelepülés?

- a) tűzfal
- b) tartalomellenőrző szoftver
- c) rosszindulatú programkód
- d) vírusirtó szoftver és vírusdefiníciós fájlok

1.10. Mi vezethet rosszindulatú programkódok telepítéséhez?

- a) a makrók letiltása az alkalmazásokban
- b) hátsó kapu használata a rendszerbiztonság megkerüléséhez
- c) a "vis maior" esetekre való hivatkozás
- d) biometrikus védelem alkalmazása a felhasználók személyazonosságának megállapításához

1.11. Mi a vírusirtó szoftverek korlátja?

- a) vírus-ellenőrzés közben figyelni kell a működését
- b) nem lehetséges a vírus-ellenőrzést ütemezni
- c) naprakészen kell tartani a vírusdefiníciós fájlokat
- d) karanténba teszi a fertőzött fájlokat

1.12. Mi igaz a karanténban lévő fájlokra?

- a) szoftverfrissítések
- b) ezek törölve lettek a számítógépről
- c) visszaállíthatók, ha szükséges
- d) vírusdefiníciós fájlok

1.13. Mi a célja a szoftverfrissítések telepítésének?

- a) töröljük az internetről letöltött és ideiglenesen tárolt fájlokat
- b) kijavítjuk egy program hibáját vagy biztonsági kockázatát
- c) töröljük a sütiket
- d) engedélyezzük az automatikus kiegészítést





1.14. Melyik írja le a LAN-t?

- a) kis földrajzi területen több összekötött számítógép együttese
- b) olyan nyilvános hálózat, mely megengedi a biztonságos kapcsolódást más nyilvános számítógépekhez
- c) nagy kiterjedésű területen összekapcsolt számítógépek együttese
- d) ugyanabban a helyiségben elhelyezett hálózati eszközök együttese

1.15. Mi a tűzfal feladata?

- a) törölni a sütiket a számítógépről vagy a hálózathoz
- b) a mentéshez biztosítani biztonságos háttér-adattárolókat
- c) védeni a hálózatot a betörésektől
- d) automatikusan frissíteni a digitális tanúsítványokat

1.16. Melyik ikon jelenti a drótnélküli hálózatot?

- a) 
- b) 
- c) 
- d) 

1.17. Mi a biztonsági kihatása a hálózatra való csatlakozásnak?

- a) nem lehet hozzáférni a privát hálózathoz
- b) megfertőződhet a számítógép rosszindulatú szoftverekkel
- c) a fájlhoz történő hozzáférés a hálózaton keresztül lelassul
- d) az összes internetről letöltött és ideiglenesen tárolt fájl törlődik

1.18. Miért szükséges jelszó alkalmazása a drótnélküli hálózatok hozzáférésehez?

- a) megelőzi a hálózathoz való csatlakozási késedelmet
- b) biztosítja a vírusirtó szoftver naprakészségét
- c) így csak jogos felhasználó használhatja a hálózatot
- d) megvédi a hálózati tűzfalat




1.19. Melyik biometria védelem?

- a) adatok mentése
- b) bankkártya lemásolása
- c) kikérdezés
- d) retina-szkennelés

1.20. Mihez kell ragaszkodni egy on-line pénzügyi tranzakció elvégzésekor?

- a) a web-oldal biztonságához
- b) az automatikus kiterjesztés bekapcsolásához
- c) a Lomtárnak a tranzakciót követő kiürítéséhez
- d) a tranzakciót követő elektromágneses törléshez

1.21. Melyik jelöli a biztonságos weboldalakat?

- a) 
- b) 
- c) 



d)

- 1.22. Mely fájlok tartalmazhatnak nyilvános kulcsokat és más hitelesítő adatokat?
- vírusdefiníciós fájlok
 - titkosított adatbázis-mentési fájlok
 - makrók
 - digitális tanúsítványok
- 1.23. Miért kell a sütiket blokkolni a böngészőkben?
- hogy vírusirtó szoftvert lehessen telepíteni
 - hogy hozzá lehessen férni a web-alapú elektronikus levelezési fiókokhoz
 - hogy böngészhessünk ismeretlen weblapokon
 - hogy megakadályozzuk az internetes zaklatást
- 1.24. Mi lenne az eredménye annak, ha egy közösségi oldalon a személyes adatokat a nyilvánosság számára hozzáférhetővé tennénk?
- a személyes adatokhoz csak a barátok férhetnének hozzá
 - a személyes adatokat bárki megnézheti
 - a barátok barátai láthatnák a személyes adatokat
 - a barátok módosíthatnák a személyes adatokat
- 1.25. Mi tartalmazhat rosszindulatú programkódot vagy vírust?
- X509v3 digitális tanúsítványok
 - tűzfalak
 - digitális aláírások
 - csalárd elektronikus levelek
- 1.26. Mi használja az adatok megszerzéséhez hamisított weboldalak linkjeit?
- rendszerszinten tevékenykedő kártékony kódok
 - tárcsázó programok
 - adathalászat
 - bankkártya-lemásolás
- 1.27. Miért NEM szabad megnyitni egy ismeretlen csatolmányt?
- rosszindulatú programkódokat tartalmazhat
 - lehet, hogy nagyon nagy a fájl
 - lehet, hogy titkosító kulcs szükséges a megnyitáshoz
 - lehetséges, hogy digitális tanúsítványt tartalmaz
- 1.28. Melyik lehet az azonnali üzenetküldés sebezhetősége?
- vírusdefiníciós fájlok
 - on-line emelt díjas tárcsázó programok
 - digitális tanúsítványok
 - rosszindulatú programkódok

1.29. Melyik egy lehetséges mentési tulajdonság?

- a) bankkártya lemásolás
- b) ütemezés
- c) kikérdezés
- d) elektromágneses törlés

1.30. Mi NEM eredményezi az adatok végleges törlését?

- a) az adatok átmozgatása a Lomtárba
- b) a háttértároló elektromágneses törlése
- c) a szoftveres adatmegsemmisítő eszközök használata
- d) a DVD-k bedarálása

2. Keresse meg a vizsgaközpont által megadott mappában található **pencils.doc** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a **safe** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **sales.xls** fájlról a **july backup** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

18.FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
- 1.1. Mi a "jelszó crackelés" jelentése?
- a) személyes adatokat lopni on-line módon
 - b) rendszeresen megváltoztatni a jelszót az előírásoknak megfelelően
 - c) nem megfelelő jelszavak egymás utáni bevitele
 - d) a jelszó nyílt szöveges verziójának megszerzése
- 1.2. Mi jelent fenyegetést az adatokra?
- a) titkosítás
 - b) emberi tevékenység
 - c) biometria
 - d) sütik
- 1.3. Mi az üzletileg érzékeny információk védelmének célja?
- a) biztosítani a makrók engedélyezését
 - b) megakadályozni a vírusok terjedését
 - c) megelőzni az ügyfelek adataival való visszaélést
 - d) megakadályozni az internetes zaklatást
- 1.4. Mi akadályozza meg az adatokhoz való jogosulatlan hozzáférést?
- a) a fájlok tömörítése
 - b) internet-szűrő alkalmazása
 - c) adatmentés készítése
 - d) jelszóhasználat
- 1.5. Melyik az európai adatvédelmi szabályozás?
- a) 1995 Európai Adatvédelmi Irányelv
 - b) 2001 Információs Társadalom Irányelv
 - c) 1995 Európai Adat Információ Szabályzat
 - d) 2002 Irányelv a személyes adatok védelméhez és az elektronikus kommunikációhoz
- 1.6. Melyik a személyazonosság-lopás leírása?
- a) felhasználói név használata az interneten
 - b) felvenni más személy azonosságát haszonszerzés céljából
 - c) munkahelyi adatok megadása internetes vásárláskor
 - d) tartalomellenőrző szoftverek használata internetezés közben
- 1.7. Mi a makrók tiltásának hatása?
- a) a makró nem fog futni
 - b) a makró törölve lesz a fájlból

- c) a makró még mindig helyesen fog futni
- d) a makró akkor fog működni, ha a tűzfal be van kapcsolva

1.8. Mi a titkosított adatok előnye?

- a) nem lehet törölni
- b) gyorsabban lehet menteni
- c) nem tartalmazhatnak vírusokat vagy rosszindulatú kódokat
- d) kulcs nélkül nem lehet elolvasni

1.9. Melyik célja a tulajdonos engedélye nélkül a számítógépre való feltelepülés?

- a) tűzfal
- b) tartalomellenőrző szoftver
- c) rosszindulatú programkód
- d) vírusirtó szoftver és vírusdefiníciós fájlok

1.10. Mi vezethet rosszindulatú programkódok telepítéséhez?

- a) a makrók letiltása az alkalmazásokban
- b) hátsó kapu használata a rendszerbiztonság megkerüléséhez
- c) a "vis maior" esetekre való hivatkozás
- d) biometrikus védelem alkalmazása a felhasználók személyazonosságának megállapításához

1.11. Mi egy fertőző, rosszindulatú program?

- a) a süti
- b) a vírus
- c) a digitális tanúsítvány
- d) a digitális aláírás

1.12. Melyik képes megfertőzni és irányítani egy számítógépet a tulajdonos engedélye nélkül?

- a) biometria
- b) vírus-definíciós fájl
- c) süti
- d) zombi-hálózat

1.13. Mi a vírusirtó szoftverek előnye?

- a) megvizsgálják a számítógépet hogy nem fertőződnek-e meg
- b) megakadályozzák a tartalom-ellenőrző szoftverek elindítását
- c) minden adatot mentenek
- d) a korábban törölt fájlokat visszaállítják a számítógép háttértárolójára

1.14. Mi akadályozza meg a hálózathoz kívülről történő jogosulatlan hozzáférést?

- a) fájlok hozzáférés-védelmi beállításai
- b) tartalom-ellenőrző program
- c) zombi-hálózati szoftver
- d) tűzfalak





1.15. Mi biztosítja a vezeték nélküli biztonságot?

- a) WAN
- b) LAN
- c) Média Hozzáférési Kontroll (MAC)
- d) számítógépes hálózathoz hátsó kaput nyitó szoftver

1.16. Mi eredményezhet jogosulatlan adathozzáférést?

- a) elektromágneses törlés
- b) adat-hozzáférés vezeték nélküli forgalom lehallgatásakor
- c) biometrikus védelmi intézkedésen alapuló hozzáférés-védelmi szoftver telepítése
- d) digitális tanúsítvány

1.17. Melyik ikon jelzi a nem védett vezeték nélküli hálózatot?

- a) 
- b) 
- c) 
- d) 

1.18. Hogyan történik a hálózati bejelentkezés?

- a) felhasználói névvel és jelszóval
- b) automatikus kiegészítéssel
- c) titkosított felhasználói névvel
- d) digitális tanúsítvánnyal



1.19. Melyik a jó szabály a jelszavakra?

- a) használjon minél kevesebb karaktert a jelszóban
- b) időnként változtassa meg a jelszavát
- c) ossza meg a jelszavát a barátaival
- d) a jelszóban sose használjon vegyesen betűket és számokat

1.20. Melyik weboldalnál található http előtag a https helyett?

- a) on-line bank
- b) keresőmotor
- c) on-line webáruház
- d) biztonságos weboldal

1.21. Melyik ikon jelzi a biztonságos web-oldalt?

- a) 
- b) 



- 1.22. Melyik támadás irányítja át a web-oldal forgalmát egy hamisított web-oldalra?
- a) crackelés
 - b) eltérítéssel adathalászat
 - c) etikus hackelés
 - d) információ-szerzés
- 1.23. Melyik a böngészők által a számítógépen tárolt apró szöveg?
- a) tűzfal
 - b) trójai program
 - c) rendszerszinten rejtőző kártékony kód
 - d) süti
- 1.24. Mitől kell tartanunk a közösségi média használatakor?
- a) biometria
 - b) etikus hackelés
 - c) internetes zaklatás
 - d) titkosított fájlok
- 1.25. Mi biztosítja azt, hogy csak a címzettek olvashassanak el egy elektronikus levelet?
- a) az elektronikus levél aláírással való ellátása
 - b) az elektronikus levél titkosítása
 - c) egyszerű szöveges elektronikus levél formázása
 - d) definíciós fájl hozzáadása az elektronikus levélhez
- 1.26. Mi használ bejegyzett cégneveket személyes biztonsági adatok megszerzéséhez?
- a) adathalászat
 - b) kifigyelés
 - c) billentyűzet-leütés naplózás
 - d) zombi-hálózati szoftver
- 1.27. Mi a valós idejű szöveges kommunikáció két vagy több személy között?
- a) elektronikus levél
 - b) fájl-megosztás
 - c) eltérítéssel adathalászat
 - d) azonnali üzenetküldés
- 1.28. Mi segít biztosítani a bizalmasságot az azonnali üzenetküldés során?
- a) a tűzfal bekapcsolása
 - b) a tűzfal kikapcsolása
 - c) a fájl-megosztás korlátozása
 - d) titkosítás használata

- 1.29. Mi használható az eszközök fizikai biztonságának növelésére?
- vírusirtó szoftver
 - titkosított szöveges dokumentumok
 - biztonsági kábel
 - elektromagnetikus törlés
- 1.30. Melyik módszer törli visszaállíthatatlanul az adatokat?
- az adatok Lomtárba mozgatása
 - az adatokat tartalmazó lemez bedarálása
 - jelszavas tömörítés alkalmazása
 - adatok titkosított merevlemezre való elhelyezése
2. Nyissa meg a vizsgaközpont által megadott mappában található **secure.doc** fájlt! Tegye megnyitás-védetté a fájlt, a **guard** jelszó használatával! Mentse el és zárja be a **secure** fájlt!
[1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **promotion.ppt** fájlról az **april backup** könyvtárba! [1 pont]
- Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

19.FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
- 1.1. Mi az információ információbiztonsági szempontból?
- a) adatfeldolgozás kimenete
 - b) logikai állítások kombinációja
 - c) nyers és nem szervezett tények összessége
 - d) feldolgozandó ábrák
- 1.2. Melyik tevékenység jogellenes internet vagy számítógéphasználat közben?
- a) etikus hackelés
 - b) elektromágneses megsemmisítés
 - c) kiberbűnözés
 - d) digitális aláírás
- 1.3. Mi NEM fenyegeti az adatokat?
- a) emberi tevékenység
 - b) zombi-hálózati szoftverek
 - c) rosszindulatú programkódok
 - d) hozzáférés-védelmi szoftverek
- 1.4. Mi az oka a személyes adatok védelmének?
- a) csalások megelőzése
 - b) süti karbantartása
 - c) hátsó ajtó biztosítása
 - d) elektromágneses törlés
- 1.5. Melyik információbiztonsági jellemző biztosítja az adatok jogosulatlan módosítása elleni védelmét?
- a) rendelkezésre állás
 - b) sértetlenség
 - c) bizalmasság
 - d) hozzáférhetőség
- 1.6. Mi a szélhámosság közvetlen következménye?
- a) jogosulatlan hozzáférés a számítógéphez
 - b) tárhely-problémákhoz vezet
 - c) alkalmazza a süti blokkolási beállításait
 - d) törli a könyvjelzőket a böngészőből
- 1.7. Mi a kikérdezés?
- a) szöveges üzenetküldés a telefonszolgáltató weboldaláról

- b) jelszó-visszaállítási eljárások összessége
- c) üzenetküldés azonnali üzenetküldővel
- d) személyes információk begyűjtése megtévesztéssel

1.8. Mi a titkosítás korlátja?

- a) a fájl tulajdonosa könnyen azonosítható
- b) a titkosító kulcs elvesztésével az adat könnyen helyreállítható
- c) a titkosító kulcs elvesztésével az adat használhatatlanná válik
- d) a ktitkosított adat nem felhasználható

1.9. Mi a rosszindulatú programkód?

- a) vírusirtó szoftverek rendszeres futtatásának ütemezésére használt számítógépes program
- b) engedély nélkül használt szoftverek
- c) tűzfal-beállítások ellenőrzésére használatos szoftver
- d) számítógépes rendszerekbe engedély nélküli beszivárgást lehetővé tevő szoftver

1.10. Melyik az a rosszindulatú programkód, amelyik a felhasználó engedélye nélkül gyűjt adatokat a böngészési szokásairól?

- a) kémsoftver
- b) zombi-hálózat szoftvere
- c) tárcsázók
- d) eltérítéses adathalászat

1.11. Mi a vírusirtó szoftverek korlátja?

- a) vírus-ellenőrzés közben figyelni kell a működését
- b) nem lehetséges a vírus-ellenőrzést ütemezni
- c) naprakészen kell tartani a vírusdefiníciós fájlokat
- d) karanténba teszi a fertőzött fájlokat

1.12. Mi igaz a karanténban lévő fájlokra?

- a) szoftverfrissítések
- b) ezek törölve lettek a számítógépről
- c) visszaállíthatók, ha szükséges
- d) vírusdefiníciós fájlok

1.13. Mi a célja a szoftverfrissítések telepítésének?

- a) töröljük az internetről letöltött és ideiglenesen tárolt fájlokat
- b) kijavítjuk egy program hibáját vagy biztonsági kockázatát
- c) töröljük a sütiket
- d) engedélyezzük az automatikus kiegészítést

1.14. Melyik írja le a LAN-t?





- a) kis földrajzi területen több összekötött számítógép együttese
- b) olyan nyilvános hálózat, mely megengedi a biztonságos kapcsolódást más nyilvános számítógépekhez

- c) nagy kiterjedésű területen összekapcsolt számítógépek együttese
- d) ugyanabban a helyiségben elhelyezett hálózati eszközök együttese

1.15. Mi a tűzfal feladata?

- a) törölni a sütiket a számítógépről vagy a hálózatról
- b) a mentéshez biztosítson biztonságos háttér-adattárolókat
- c) védje a hálózatot a betörésektől
- d) automatikusan frissítse a digitális tanúsítványokat

1.16. Melyik ikon jelenti a drótnélküli hálózatot?

- a) 
- b) 
- c) 
- d) 

1.17. Mi a biztonsági kihatása a hálózatra való csatlakozásnak?

- a) nem lehet hozzáférni a privát hálózathoz
- b) megfertőződhet a számítógép rosszindulatú szoftverekkel
- c) a fájlokhoz történő hozzáférés a hálózaton keresztül lelassul
- d) az összes internetről letöltött és ideiglenesen tárolt fájl törlődik

1.18. Miért szükséges jelszó alkalmazása a drótnélküli hálózatok hozzáféréséhez?

- a) megelőzi a hálózathoz való csatlakozási késedelmet
- b) biztosítja a vírusirtó szoftver naprakészességét
- c) így csak jogos felhasználó használhatja a hálózatot
- d) megvédi a hálózati tűzfalat

1.19. Melyik biometria védelem?

- a) adatok mentése
- b) bankkártya lemásolása
- c) kikérdezés
- d) retina-szkennelés

1.20. Mihez kell ragaszkodni egy on-line pénzügyi tranzakció elvégzésekor?

- a) a web-oldal biztonságához
- b) az automatikus kiterjesztés bekapcsolásához
- c) a Lomtárnak a tranzakciót követő kiürítéséhez
- d) a számítógép tranzakciót követő elektromágneses törlésének az elvégzéséhez

1.21. Melyik jelöli a biztonságos weboldalakat?

- a) 

- b) 
- c) 
- d) 

- 1.22. Mely fájlok tartalmazhatnak nyilvános kulcsokat és más hitelesítő adatokat?
- a) vírusdefiníciós fájlok
 - b) mentési fájlok
 - c) makrók
 - d) digitális tanúsítványok
- 1.23. Miért kell a sütiket blokkolni a böngészőkben?
- a) hogy vírusirtó szoftvert lehessen telepíteni
 - b) hogy hozzá lehessen férni a web-alapú elektronikus levelezési fiókokhoz
 - c) hogy böngészhessünk ismeretlen weblapokon
 - d) hogy megakadályozzuk az internetes zaklatást
- 1.24. Mi lenne az eredménye annak, ha egy közösségi oldalon a személyes adatokat a nyilvánosság számára hozzáférhetővé tennénk?
- a) a személyes adatokhoz csak a barátok férhetnének hozzá
 - b) a személyes adatokat bárki megnézheti
 - c) a barátok barátai láthatnák a személyes adatokat
 - d) a barátok módosíthatnák a személyes adatokat
- 1.25. Mi tartalmazhat rosszindulatú programkódot vagy vírust?
- a) X509v3 digitális tanúsítványok
 - b) tűzfalak
 - c) digitális aláírások
 - d) csalárd elektronikus levelek
- 1.26. Mi használja az adatok megszerzéséhez hamisított weboldalak linkjeit?
- a) rendszerszinten tevékenykedő kártékony kódok
 - b) tárcsázó programok
 - c) adathalászat
 - d) bankkártya-lemásolás
- 1.27. Miért NEM szabad megnyitni egy ismeretlen csatolmányt?
- a) rosszindulatú programkódokat tartalmazhat
 - b) lehet, hogy nagyon nagy a fájl
 - c) lehet, hogy titkosító kulcs szükséges a megnyitásához
 - d) lehetséges, hogy digitális tanúsítványt tartalmaz
- 1.28. Melyik lehet az azonnali üzenetküldés sebezhetősége?
- a) vírusdefiníciós fájlok

- b) on-line emelt díjas tárcsázó programok
- c) digitális tanúsítványok
- d) rosszindulatú programkódok

1.29. Melyik egy lehetséges mentési tulajdonság?

- a) bankkártya lemásolás
- b) ütemezés
- c) kikérdezés
- d) elektromágneses törlés

1.30. Mi NEM eredményezi az adatok végleges törlését?

- a) az adatok átmozgatása a Lomtárba
- b) a háttértároló elektromágneses törlése
- c) a szoftveres adatmegsemmisítő eszközök használata
- d) a DVD-k bedarálása

2. Keresse meg a vizsgaközpont által megadott mappában található **letter.doc**! Tömörítse össze a fájlt és tegye megnyitásvédetté a **lock** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **network.doc** fájlról a **march** backup könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

20.FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
- 1.1. Mi az információ információbiztonsági szempontból?
- a) adatfeldolgozás kimenete
 - b) logikai állítások kombinációja
 - c) nyers és nem szervezett tények összessége
 - d) feldolgozandó ábrák
- 1.2. Melyik tevékenység jogellenes internet vagy számítógéphasználat közben?
- a) etikus hackelés
 - b) elektromágneses megsemmisítés
 - c) kiberbűnözés
 - d) digitális aláírás
- 1.3. Mi NEM fenyegeti az adatokat?
- a) emberi tevékenység
 - b) zombi-hálózati szoftverek
 - c) rosszindulatú programkódok
 - d) hozzáférés-védelmi szoftverek
- 1.4. Mi az oka a személyes adatok védelmének?
- a) csalások megelőzése
 - b) süti karbantartása
 - c) hátsó ajtó biztosítása
 - d) elektromágneses törlés
- 1.5. Melyik információbiztonsági jellemző biztosítja az adatok jogosulatlan módosítása elleni védelmét?
- a) rendelkezésre állás
 - b) sértetlenség
 - c) bizalmasság
 - d) hozzáférhetőség
- 1.6. Mi a szélhámosság közvetlen következménye?
- a) jogosulatlan hozzáférés a számítógéphez
 - b) tárhely-problémákhoz vezet
 - c) alkalmazza a süti blokkolási beállításait
 - d) törli a könyvjelzőket a böngészőből
- 1.7. Mi a kikérdezés?
- a) szöveges üzenetküldés a telefonszolgáltató weboldaláról

- b) jelszó-visszaállítási eljárások összessége
- c) üzenetküldés azonnali üzenetküldővel
- d) személyes információk begyűjtése megtévesztéssel

1.8. Mi a titkosítás korlátja?

- a) a fájl tulajdonosa könnyen azonosítható
- b) a titkosító kulcs elvesztésével az adat könnyen helyreállítható
- c) a titkosító kulcs elvesztésével az adat használhatatlanná válik
- d) a ktitkosított adat nem felhasználható

1.9. Mi a rosszindulatú programkód?

- a) vírusirtó szoftverek rendszeres futtatásának ütemezésére használt számítógépes program
- b) engedély nélkül használt szoftverek
- c) tűzfal-beállítások ellenőrzésére használatos szoftver
- d) számítógépes rendszerekbe engedély nélküli beszivárgást lehetővé tévő szoftver

1.10. Melyik az a rosszindulatú programkód, amelyik a felhasználó engedélye nélkül gyűjt adatokat a böngészési szokásairól?

- a) kémsoftver
- b) zombi-hálózat szoftvere
- c) tárcsázók
- d) eltérítéses adathalászat

1.11. Melyik egy fertőző rosszindulatú szoftver?

- a) a féreg
- b) a süti
- c) a tűzfal
- d) a digitális tanúsítvány

1.12. Melyik igaz a rosszindulatú programkódokra?

- a) a billentyűzetleütés naplózás a begépelte adatot rögzíti
- b) billentyűzet-leütés naplózását a <shift> billentyű lenyomásával lehet engedélyezni a számítógépen
- c) a modemes tárcsázó egy szoftver, ami szűri az interneten végzett telefonhívásokat
- d) a modemes tárcsázó egy személy, aki telefonhívásokat végez az interneten

1.13. Hogyan működnek a vírusirtó szoftverek?

- a) fertőzésmentesített fájlokat helyeznek a karanténba
- b) észlelik a vírusokat, de nem törlik automatikusan őket
- c) észlelik a vírusokat, de nem képesek felismerni a trójai programokat
- d) ütemezett keresést használnak a vírusok észlelésére

1.14. Mi a virtuális magánhálózat (VPN)?

- a) nem kell jelszó a hálózati csatlakozáshoz
- b) megengedi bárki csatlakozását egy magánhálózathoz

- c) biztonságos saját hozzáférést biztosít a hálózathoz
- d) kis földrajzi területen több összekötött számítógép együttese

1.15. Mi a tűzfal korlátja?

- a) fertőzött fájlokat helyez a karanténba
- b) nem értesít automatikusan a hálózati behatoláskor
- c) csökkenti a rosszindulatú programkódok hálózatban való megjelenésének lehetőségét
- d) nem lehet létrehozni további szabályokat a bejövő hálózati forgalom kezelésére





1.16. Mi a WPA?

- a) Wired Protected Access
- b) Wi-Fi Protected Access
- c) Wired Prevention Access
- d) Wi-Fi Password Access

1.17. Mit kell figyelembe venni nem védett drótnélküli hálózat használatakor?

- a) a hálózati tűzfalat ki kell kapcsolni
- b) a sütiket frissíteni kell
- c) az adatokhoz hozzá akarnak férni mások is
- d) az egyszer használatos jelszó ki lesz kapcsolva

1.18. Melyik a védett drótnélküli hálózat ikonja?

- a) 
- b) 
- c) 
- d) 

1.19. Melyik számít jó jelszónak?




- a) jBloggs_12091980
- b) 12092010
- c) jb
- d) jenniferBloggs

1.20. Mi azonosítja a biztonságos web-oldalakat?

- a) .org
- b) .com
- c) https
- d) http

1.21. Melyik ikon jelzi a biztonságos web-oldalt?

- a) 

- b) 
- c) 
- d) 

- 1.22. Melyik támadás irányítja át a web-oldal forgalmát egy hamisított web-oldalra?
- a) crackelés
 - b) eltérítéssel adathalászat
 - c) etikus hackelés
 - d) információ-szerzés
- 1.23. Melyik a böngészők által a számítógépen tárolt apró szöveg?
- a) tűzfal
 - b) trójai program
 - c) rendszerszinten rejtőző kártékony kód
 - d) süti
- 1.24. Mitől kell tartanunk a közösségi média használatakor?
- a) biometria
 - b) etikus hackelés
 - c) internetes zaklatás
 - d) titkosított fájlok
- 1.25. Mi biztosítja azt, hogy csak a címzettek olvashassanak el egy elektronikus levelet?
- a) az elektronikus levél aláírással való ellátása
 - b) az elektronikus levél titkosítása
 - c) egyszerű szöveges elektronikus levél formázása
 - d) definíciós fájl hozzáadása az elektronikus levélhez
- 1.26. Mi használ bejegyzett cégneveket személyes biztonsági adatok megszerzéséhez?
- a) adathalászat
 - b) figyelés
 - c) billentyűzet-leütés naplózás
 - d) zombi-hálózati szoftver
- 1.27. Mi a valós idejű szöveges kommunikáció két vagy több személy között?
- a) elektronikus levél
 - b) fájl-megosztás
 - c) eltérítéssel adathalászat
 - d) azonnali üzenetküldés
- 1.28. Mi segít biztosítani a bizalmasságot az azonnali üzenetküldés során?
- a) a tűzfal bekapcsolása
 - b) a tűzfal kikapcsolása

- c) a fájl-megosztás korlátozása
- d) titkosítás használata

1.29. Mi használható az eszközök fizikai biztonságának növelésére?

- a) vírusirtó szoftver
- b) titkosított szöveges dokumentumok
- c) biztonsági kábel
- d) elektromagnetikus törlés

1.30. Melyik módszer törli visszaállíthatatlanul az adatokat?

- a) az adatok Lomtárba mozgatása
- b) az adatokat tartalmazó lemez bedarálása
- c) jelszavas tömörítés alkalmazása
- d) adatok titkosított merevlemezre való elhelyezése

2. Nyissa meg a vizsgaközpont által megadott mappában található **access.doc** fájlt! Tegye megnyitás-védetté a fájlt, a **guard** jelszó használatával! Mentse el és zárja be az **access** fájlt!
[1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **system.doc** fájlról a **june backup** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

21.FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
- 1.1. Melyik kiberbűnözés az alábbiak közül?
- a) okostelefon ellopása
 - b) internetes számla on-line befizetése
 - c) bankkártya adatok ellopása on-line
 - d) internetes rádióhallgatása on-line
- 1.2. Melyik eljárás tartalmazza az informatikai biztonsági sebezhetőségek tesztelését?
- a) crackelés
 - b) etikus hackelés
 - c) bankkártya adatainak lemásolása
 - d) kikérdezés
- 1.3. Miért kell védeni az üzletileg érzékeny információkat?
- a) mert megakadályozza az adatlopást
 - b) ütemezett mentések lefutásának biztosítása miatt
 - c) kéretlen üzenetek blokkolása miatt
 - d) a biztonságos weboldalak azonosításáért
- 1.4. Melyik nyújt védelmet a jogosulatlan adat-hozzáférés ellen?
- a) bonyolult fájlnevek
 - b) billentyűzet-leütés naplózása
 - c) eltérítéssel adathalászat
 - d) titkosítás
- 1.5. Melyik információbiztonsági tulajdonság biztosítja az adatok jogosulatlan hozzáférés vagy felfedés elleni védelmét?
- a) bizalmasság
 - b) sértetlenség
 - c) rendelkezésre állás
 - d) hitelesség
- 1.6. Melyik európai szabályozást kell betartani a személyes adatok védelmének vonatkozásában?
- a) 1997 Európai Adatvédelmi Szabályozás
 - b) 2001 Európai Információs Társadalmi Irányelv
 - c) 1995 Európai Adatvédelmi Irányelv
 - d) 2001 Európai Irányelv az Információ-Technológiáról

1.7. Melyik tartozik a szélhámosság módszerei közé?

- a) közösségi oldalakhoz több fiókkal rendelkezni
- b) valaki válla fölött megszerezni az információkat
- c) videó- és hanghívásokat kezdeményezni az interneten
- d) meghivatkozni más weboldalát egy közösségi oldalról

1.8. Mi a személyazonosság-lopás közvetlen következménye?

- a) a pénzügyi adatokat mások is használhatják
- b) a vírusirtó nem működik a továbbiakban
- c) a letöltött és ideiglenesen tárolt fájlokat törölni fogják
- d) a mentés ütemezését megváltoztatják

1.9. Melyik szoftvert készítek és küldik károkozási célból?

- a) szimmetrikus vagy aszimmetrikus elvű titkosító szoftverek
- b) tűzfalak
- c) rosszindulatú programkódok
- d) vírusirtó szoftverek

1.10. Mit használnak a rosszindulatú programkódok elrejtésére?

- a) rendszerszinten tevékenykedő kártékony kódokat
- b) elektromágneses elven alapuló adattörlési módszereket
- c) tűzfalakat
- d) bedarálást

1.11. Mi a vírusirtó szoftverek korlátja?

- a) vírus-ellenőrzés közben figyelni kell a működését
- b) nem lehetséges a vírus-ellenőrzést ütemezni
- c) naprakészen kell tartani a vírusdefiníciós fájlokat
- d) karanténba teszi a fertőzött fájlokat

1.12. Mi igaz a karanténban lévő fájlokra?

- a) szoftverfrissítések
- b) ezek törölve lettek a számítógépről
- c) visszaállíthatók, ha szükséges
- d) vírusdefiníciós fájlok

1.13. Mi a célja a szoftverfrissítések telepítésének?

- a) töröljük az internetről letöltött és ideiglenesen tárolt fájlokat
- b) kijavítjuk egy program hibáját vagy biztonsági kockázatát
- c) töröljük a sütiket
- d) engedélyezzük az automatikus kiegészítést

1.14. Melyik írja le a LAN-t?





- a) kis földrajzi területen több összekötött számítógép együttese
- b) olyan nyilvános hálózat, mely megengedi a biztonságos kapcsolódást más nyilvános számítógépekhez

- c) nagy kiterjedésű területen összekapcsolt számítógépek együttese
- d) ugyanabban a helyiségben elhelyezett hálózati eszközök együttese

1.15. Mi a tűzfal feladata?

- a) törölni a sütiket a számítógépről vagy a hálózatról
- b) a mentéshez biztosítson biztonságos háttér-adattárolókat
- c) védje a hálózatot a betörésektől
- d) automatikusan frissítse a digitális tanúsítványokat

1.16. Melyik ikon jelenti a drótnélküli hálózatot?

- a) 
- b) 
- c) 
- d) 

1.17. Mi a biztonsági kihatása a hálózatra való csatlakozásnak?

- a) nem lehet hozzáférni a privát hálózathoz
- b) megfertőződhet a számítógép rosszindulatú szoftverekkel
- c) a fájlokhoz történő hozzáférés a hálózaton keresztül lelassul
- d) az összes internetről letöltött és ideiglenesen tárolt fájl törlődik

1.18. Miért szükséges jelszó alkalmazása a drótnélküli hálózatok hozzáféréséhez?

- a) megelőzi a hálózathoz való csatlakozási késedelmet
- b) biztosítja a vírusirtó szoftver naprakészességét
- c) így csak jogos felhasználó használhatja a hálózatot
- d) megvédi a hálózati tűzfalat

1.19. Melyik biometria védelem?

- a) adatok mentése
- b) bankkártya lemásolása
- c) kikérdezés
- d) retina-szkennelés

1.20. Mihez kell ragaszkodni egy on-line pénzügyi tranzakció elvégzésekor?

- a) a web-oldal biztonságához
- b) az automatikus kiterjesztés bekapcsolásához
- c) a Lomtárnak a tranzakciót követő kiürítéséhez
- d) a tranzakciót követő elektromágneses törléséhez

1.21. Mikor használnak egyszer használatos jelszót?

- a) a laptopra való első bejelentkezéskor
- b) amikor a jelszót elküldik e-mailben
- c) amikor tűzfalat állítanak be

- d) VPN-be való bejelentkezéskor
- 1.22. Melyik adat törölhető a böngésző által?
- a) kititkosított adat
 - b) titkosított adat
 - c) automatikus kiegészítés adata
 - d) billentyűzet-leütéseket naplózó adat
- 1.23. Melyikkel korlátozható az interneten töltött időtartam?
- a) adathalász szoftver
 - b) szülői felügyelet szoftver
 - c) tárcsázó
 - d) sütik
- 1.24. Melyik a közösségi oldalakon előforduló fenyegetés?
- a) bedarálás
 - b) elektromágneses törlés
 - c) bankkártya adatainak a lemásolása
 - d) szexuális kizsákmányolás
- 1.25. Milyen eljárás biztosítja az e-mailek bizalmasságát?
- a) titkosítás
 - b) kikérdezés
 - c) eltérítéssel adathalászat
 - d) kititkosítás
- 1.26. Mi a digitális aláírás eszköze?
- a) szoftver, ami átirányítja egy weboldal forgalmát egy hamisított weboldalra
 - b) egy matematikai séma az üzenet hitelességének biztosítására
 - c) egy bonyolult módszer, mely beszűri az aláírást az üzenet végére
 - d) szoftver, mely engedélyezési és tiltólistákat alkalmaz a bejövő hálózati forgalom irányítására
- 1.27. Melyik fogalom írja le a banki adatokat bekérő hamisított elektronikus leveleket?
- a) kifigyelés
 - b) internetes zaklatás
 - c) adathalászat
 - d) crackelés
- 1.28. Mi tartalmazhat rosszindulatú programkódot?
- a) levélcsatolmány
 - b) süti
 - c) tűzfal
 - d) digitális aláírás

- 1.29. Melyik nyújt védelmet az adatvesztés ellen?
- a) sütik
 - b) kikérdezés
 - c) titkosított USB lemez használata
 - d) mentések
- 1.30. Miért van szükség az adatok visszaállíthatatlan törlésére?
- a) az áramingadozásból adódó meghibásodások miatt
 - b) az adatok más általi visszaállíthatatlansága miatt
 - c) hogy tartalomellenőrző szoftvert lehessen telepíteni
 - d) hogy törölni lehessen minden sütit
2. Keresse meg a vizsgaközpont által megadott mappában található **pencils.doc** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a **safe** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **sales.xls** fájlról a **july backup** könyvtárba! [1 pont]
- Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

22. FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
- 1.1. Melyik kiberbűnözés az alábbiak közül?
- a) okostelefon ellopása
 - b) internetes számla on-line befizetése
 - c) bankkártya adatok ellopása on-line
 - d) internetes rádióhallgatása on-line
- 1.2. Melyik eljárás tartalmazza az informatikai biztonsági sebezhetőségek tesztelését?
- a) crackelés
 - b) etikus hackelés
 - c) bankkártya adatainak lemásolása
 - d) kikérdezés
- 1.3. Miért kell védeni az üzletileg érzékeny információkat?
- a) mert megakadályozza az adatlopást
 - b) ütemezett mentések lefutásának biztosítása miatt
 - c) kéretlen üzenetek blokkolása miatt
 - d) a biztonságos weboldalak azonosításáért
- 1.4. Melyik nyújt védelmet a jogosulatlan adat-hozzáférés ellen?
- a) bonyolult fájlnevek
 - b) billentyűzet-leütés naplózása
 - c) eltérítéssel adathalászat
 - d) titkosítás
- 1.5. Melyik információbiztonsági tulajdonság biztosítja az adatok jogosulatlan hozzáférés vagy felfedés elleni védelmét?
- a) bizalmasság
 - b) sértetlenség
 - c) rendelkezésre állás
 - d) hitelesség
- 1.6. Melyik európai szabályozást kell betartani a személyes adatok védelmének vonatkozásában?
- a) 1997 Európai Adatvédelmi Szabályozás
 - b) 2001 Európai Információs Társadalmi Irányelv
 - c) 1995 Európai Adatvédelmi Irányelv
 - d) 2001 Európai Irányelv az Információ-Technológiáról

1.7. Melyik tartozik a szélhámosság módszerei közé?

- a) közösségi oldalakhoz több fiókkal rendelkezni
- b) valaki válla fölött megszerezni az információkat
- c) videó- és hanghívásokat kezdeményezni az interneten
- d) meghivatkozni más weboldalát egy közösségi oldalról

1.8. Mi a személyazonosság-lopás közvetlen következménye?

- a) a pénzügyi adatokat mások is használhatják
- b) a vírusirtó nem működik a továbbiakban
- c) a letöltött és ideiglenesen tárolt fájlokat törölni fogják
- d) a mentés ütemezését megváltoztatják

1.9. Melyik szoftvert készítek és küldik károkozási célból?

- a) szimmetrikus vagy aszimmetrikus elvű titkosító szoftverek
- b) tűzfalak
- c) rosszindulatú programkódok
- d) vírusirtó szoftverek

1.10. Mit használnak a rosszindulatú programkódok elrejtésére?

- a) rendszerszinten tevékenykedő kártékony kódokat
- b) elektromágneses elven alapuló adattörlési módszereket
- c) tűzfalakat
- d) bedarálást

1.11. Mi az előnye a vírusirtóknak?

- a) megakadályozzák a kifinomult támadásokat
- b) frissítik a digitális tanúsítványokat
- c) felismerik a vírusokat a számítógépen
- d) megakadályozzák az információ-búvárkodást

1.12. Mi igaz a karanténban lévő fájlokra?

- a) nem lehet letölteni
- b) nem lehet fertőzésmentesíteni
- c) nem lehet törölni
- d) nem lehet megfertőzni

1.13. Miért kell vírusdefiníciós fájlokat letölteni?

- a) frissíti az ideiglenesen letöltött és tárolt fájlokat
- b) frissíti a sütiket
- c) lehetővé teszi az új fenyegetések elleni védelmet
- d) frissíti az elektromágneses törléseket végző szoftvert

1.14. Hogyan nevezik az irodában vagy otthon összekapcsolt számítógépeket?

- a) LAN
- b) VPN
- c) WAN

d) USB





1.15. Mi a hálózati adminisztrátor feladata?

- a) fenntartani az épület elektromos hálózatának folyamatos működőképességét
- b) biztosítani a hálózati adatokhoz a nyilvános hozzáférést
- c) biztosítani, hogy az adatokat ne mentse le a rendszerbe
- d) fenntartani a munkatársak szükséges adathozzáférést a hálózaton

1.16. Mi akadályozza meg a jogosulatlan belépést a hálózatba egy külső helyszínről?

- a) elektromágneses törlés
- b) tűzfalak
- c) adathalászat
- d) digitális tanúsítványok

1.17. Melyik ikon jelenti a csatlakoztatható vezetékes hálózatot?

- a) 
- b) 
- c) 
- d) 

1.18. Mi a hálózatra történő csatlakozás biztonsági vonatkozása?

- a) adatok biztonsági mentése
- b) fájlok tömörítése
- c) személyes adatok védelme
- d) információbúvárkodás

1.19. Miért kell jelszóval védeni a vezeték nélküli hálózatokat?

- a) elindítja a vírusirtó szoftvert
- b) megakadályozza a jogosulatlan adat-hozzáférést
- c) biztosítja a süti engedélyezését
- d) megakadályozza az adathalászatra irányuló támadásokat

1.20. Mi igazolja, hogy az üzenet küldője valóban az, akinek állítja magát?

- a) digitális tanúsítvány
- b) süti
- c) makró
- d) letöltött és ideiglenesen tárolt internet fájlok

1.21. Mit jelent az eltérítéssel adathalászat (pharming)?

- a) a biztonsági forgalom irányítása tiltási és engedélyezési listákat alkalmazó szoftverrel
- b) a webforgalom átirányítása egy hamisított web-oldalra
- c) a figyelés egyik módszere
- d) az ideiglenesen letöltött és tárolt internet-fájlok megszerzése

- 1.22. Mi gyorsítja fel egy ismétlődő adatbevitelt is tartalmazó on-line űrlap kitöltését?
- automatikus kiegészítés
 - makrók tiltása
 - titkosítás
 - elektromagnetikus törlés
- 1.23. Milyen adatokat kell rendszeres időközönként ellenőrizni és törölni a böngészőből?
- makrókat
 - sütiket
 - digitális tanúsítványokat
 - vírusdefiníciós fájlokat
- 1.24. Melyik célja a weboldalakhoz való hozzáférés ellenőrzése és korlátozása?
- reklámokat megjelenítő szoftver
 - kémszoftver
 - adathalász szoftver
 - tartalomellenőrző szoftver
- 1.25. Mit nem szabad közzétenni egy közösségi oldalon?
- zenei érdeklődést
 - becenevet
 - otthoni címet
 - kedvenc televízióműsort
- 1.26. Melyik az a titkosított kód, amely egy személy azonosságát társítja egy fájlhoz?
- jelszavas tömörített fájl
 - digitális aláírás
 - makrózott titkosított szöveg
 - ideiglenesen letöltött és tárolt fájl
- 1.27. Mi az adathalászat?
- lopott bankkártya adatainak felhasználása on-line vásárlásnál
 - információkat kifigyelni valaki válla felett
 - félrevezetni valakit az interneten értékes információk megszerzéséért
 - az informatikai biztonsági hiányosságok tesztelése
- 1.28. Mi jelenti a legnagyobb kitétséget a rosszindulatú programkódoknak?
- hozzáférés biztonságos weboldalhoz
 - levélcsatolmány megnyitása
 - elektronikus levél írása
 - adatok mentése
- 1.29. Mi az azonnali üzenetküldés sebezhetősége?
- hátsó ajtó hozzáférés
 - valós idejű hozzáférés
 - vis maior

d) információbúvárkodás

1.30. Mi jelenti az adatok végleges megsemmisítését?

- a) eltérítéssel adathalászat
- b) áramellátás kiesése
- c) tárcsázás
- d) elektromágneses törlés

2. Nyissa meg a vizsgaközpont által megadott mappában található **secure.doc** fájlt! Tegye megnyitási-védetté a fájlt, a **guard** jelszó használatával! Mentse el és zárja be a **secure** fájlt!
[1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **promotion.ppt** fájlról az **april backup** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

23.FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
 - 1.1. Melyik tevékenység kiberbűnözés?
 - a) bedarálás
 - b) adathalászat
 - c) etikus hackelés
 - d) titkosítás
 - 1.2. Mit jelent a “hackelés” fogalma?
 - a) az adatokhoz való jogosulatlan hozzáférés megszerzése
 - b) félrevezetni a személyazonosságunkról valakit az interneten
 - c) vírusirtóval eltávolítani az összes rosszindulatú szoftvert a gépünkről
 - d) számítógépeket lopni az épületbe való betöréssel
 - 1.3. Melyik jelent „vis maior” fenyegetést az adatokra?
 - a) emberi tevékenység
 - b) adatlopás
 - c) tűz
 - d) vírusok
 - 1.4. Mi a személyes adatok védelmének célja?
 - a) az etikus hackelés megelőzése
 - b) a személyazonosság-lopás megakadályozása
 - c) helyet lehessen megtakarítani a számítógép háttértárolóján
 - d) a számítógépes vírusok elkerülése
 - 1.5. Melyik információbiztonsági tulajdonság biztosítja a tárolt adatok jogosulatlan hozzáférés elleni védelmét?
 - a) bizalmasság
 - b) sértetlenség
 - c) rendelkezésre állás
 - d) hitelesség
 - 1.6. Melyik állítás igaz az informatikai biztonsági szabályzatokra?
 - a) csak az informatikusokra vonatkoznak
 - b) csak a pénzügyi intézmények számára fontosak
 - c) csak olvasni kell, de nem kell megvalósítani
 - d) fontosak, mivel követendő szabályokat adnak a felhasználók számára.
 - 1.7. Melyik NEM közvetlen következménye a szélhámosságnak?
 - a) a személyes adatok mások által hozzáférhetővé váltak

- b) hozzáférhetővé vált mások által a számítógép-rendszer
- c) a tűzfalat kikapcsolják
- d) a begyűjtött adatokat csalásra fogják felhasználni

1.8. Melyik a személyazonosság-lopás módszere?

- a) hamis név használata egy közösségi oldalon
- b) nem megfelelő kulcs használata dokumentum titkosításának feloldásához
- c) adatok elektromágneses eszközökkel történő megsemmisítése
- d) információbűvárkodás

1.9. Mi használható egy rosszindulatú program elrejtésére?

- a) kikérdezés
- b) rendszerszinten tevékenykedő kártékony kód
- c) biometria
- d) bankkártya-lemásolás

1.10. Mit lehet adatlopásra használni?

- a) zombi-hálózat szoftverét
- b) adatok elektromágneses eszközökkel történő megsemmisítését
- c) alhálózatokat
- d) bedarálást

1.11. Melyik egy fertőző rosszindulatú szoftver?

- a) a féreg
- b) a süti
- c) a tűzfal
- d) a digitális tanúsítvány

1.12. Melyik igaz a rosszindulatú programkódokra?





- a) a billentyűzetleütés naplózás a begépelte adatot rögzíti
- b) billentyűzet-leütés naplózását a <shift> billentyű lenyomásával lehet engedélyezni a számítógépen
- c) a modemes tárcsázó egy szoftver, ami szűri az interneten végzett telefonhívásokat
- d) a modemes tárcsázó egy személy, aki telefonhívásokat végez az interneten

1.13. Hogyan működnek a vírusirtó szoftverek?

- a) fertőzésmentesített fájlokat helyeznek a karanténba
- b) észlelik a vírusokat, de nem törlik automatikusan őket
- c) észlelik a vírusokat, de nem képesek felismerni a trójai programokat
- d) ütemezett keresést használnak a vírusok észlelésére

1.14. Mi a virtuális magánhálózat (VPN)?

- a) nem kell jelszó a hálózati csatlakozáshoz
- b) megengedi bárki csatlakozását egy magánhálózathoz
- c) biztonságos saját hozzáférést biztosít a hálózathoz
- d) kis földrajzi területen több összekötött számítógép együttese

- 1.15. Mi a tűzfal korlátja?
- fertőzött fájlokat helyez a karanténba
 - nem értesít automatikusan a hálózati behatolásakor
 - csökkenti a rosszindulatú programkódok hálózatban való megjelenésének lehetőségét
 - nem lehet létrehozni további szabályokat a bejövő hálózati forgalom kezelésére
- 1.16. Mi a WPA?
- Wired Protected Access
 - Wi-Fi Protected Access
 - Wired Prevention Access
 - Wi-Fi Password Access
- 1.17. Mit kell figyelembe venni nem védett drótnélküli hálózat használatakor?
- a hálózati tűzfalat ki kell kapcsolni
 - a sütiket frissíteni kell
 - az adatokhoz hozzá akarnak férni mások is
 - az egyszer használatos jelszó ki lesz kapcsolva
- 1.18. Melyik a védett drótnélküli hálózat ikonja?
- 
 - 
 - 
 - 
- 1.19. Melyik számít jó jelszónak?
- jBloggs_12091980
 - 12092010
 - jb
 - jenniferBloggs
- 1.20. Mi azonosítja a biztonságos web-oldalakat?
- .org
 - .com
 - https
 - http
- 1.21. Mit jelent az eltérítéssel adathalászat (pharming)?
- a biztonsági forgalom irányítása tiltási és engedélyezési listákat alkalmazó szoftverrel
 - a webforgalom átirányítása egy hamisított web-oldalra
 - a kifizetés egyik módszere
 - az ideiglenesen letöltött és tárolt internet-fájlok megszerzése

- 1.22. Mi gyorsítja fel egy ismétlődő adatbevitelt is tartalmazó on-line űrlap kitöltését?
- automatikus kiegészítés
 - makrók tiltása
 - titkosítás
 - elektromagnetikus törlés
- 1.23. Milyen adatokat kell rendszeres időközönként ellenőrizni és törölni a böngészőből?
- makrókat
 - sütiket
 - digitális tanúsítványokat
 - vírusdefiníciós fájlokat
- 1.24. Melyik célja a weboldalakhoz való hozzáférés ellenőrzése és korlátozása?
- reklámokat megjelenítő szoftver
 - kémszoftver
 - adathalász szoftver
 - tartalomellenőrző szoftver
- 1.25. Mit nem szabad közzétenni egy közösségi oldalon?
- zenei érdeklődést
 - becenevet
 - otthoni címet
 - kedvenc televízióműsort
- 1.26. Melyik az a titkosított kód, amely egy személy azonosságát társítja egy fájlhoz?
- jelszavas tömörített fájl
 - digitális aláírás
 - makrózott titkosított szöveg
 - ideiglenesen letöltött és tárolt fájl
- 1.27. Mi az adathalászat?
- lopott bankkártya adatainak felhasználása on-line vásárlásnál
 - információkat kifigyelni valaki válla felett
 - félrevezetni valakit az interneten értékes információk megszerzéséért
 - az informatikai biztonsági hiányosságok tesztelése
- 1.28. Mi jelenti a legnagyobb kitétséget a rosszindulatú programkódoknak?
- hozzáférés biztonságos weboldalhoz
 - levélcsatolmány megnyitása
 - elektronikus levél írása
 - adatok mentése
- 1.29. Mi az azonnali üzenetküldés sebezhetősége?
- hátsó ajtó hozzáférés
 - valós idejű hozzáférés
 - vis maior

d) információbúvárkodás

1.30. Mi jelenti az adatok végleges megsemmisítését?

- a) eltérítéssel adathalászat
- b) áramellátás kiesése
- c) tárcsázás
- d) elektromágneses törlés

2. Keresse meg a vizsgaközpont által megadott mappában található **iroszer.doc** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a **safe** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **ertesites.xls** fájlról a **juliusi_mentes** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

24.FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
- 1.1. Mi a "jelszó crackelés" jelentése?
- a) személyes adatokat lopni on-line módon
 - b) rendszeresen megváltoztatni a jelszót az előírásoknak megfelelően
 - c) nem megfelelő jelszavak egymás utáni bevitele
 - d) a jelszó nyílt szöveges verziójának megszerzése
- 1.2. Mi jelent fenyegetést az adatokra?
- a) titkosítás
 - b) emberi tevékenység
 - c) biometria
 - d) sütik
- 1.3. Mi az üzletileg érzékeny információk védelmének célja?
- a) biztosítani a makrók engedélyezését
 - b) megakadályozni a vírusok terjedését
 - c) megelőzni az ügyfelek adataival való visszaélést
 - d) megakadályozni az internetes zaklatást
- 1.4. Mi akadályozza meg az adatokhoz való jogosulatlan hozzáférést?
- a) a fájlok tömörítése
 - b) internet-szűrő alkalmazása
 - c) adatmentés készítése
 - d) jelszóhasználat
- 1.5. Melyik az európai adatvédelmi szabályozás?
- a) 1995 Európai Adatvédelmi Irányelv
 - b) 2001 Információs Társadalom Irányelv
 - c) 1995 Európai Adat Információ Szabályzat
 - d) 2002 Irányelv a személyes adatok védelméhez és az elektronikus kommunikációhoz
- 1.6. Melyik a személyazonosság-lopás leírása?
- a) felhasználói név használata az interneten
 - b) felvenni más személy azonosságát haszonszerzés céljából
 - c) munkahelyi adatok megadása internetes vásárláskor
 - d) tartalomellenőrző szoftverek használata internetezés közben
- 1.7. Mi a makrók tiltásának hatása?
- a) a makró nem fog futni
 - b) a makró törölve lesz a fájlból

- c) a makró még mindig helyesen fog futni
- d) a makró akkor fog működni, ha a tűzfal be van kapcsolva

1.8. Mi a titkosított adatok előnye?

- a) nem lehet törölni
- b) gyorsabban lehet menteni
- c) nem tartalmazhatnak vírusokat vagy rosszindulatú kódokat
- d) kulcs nélkül nem lehet elolvasni

1.9. Melyik célja a tulajdonos engedélye nélkül a számítógépre való feltelepülés?

- a) tűzfal
- b) tartalomellenőrző szoftver
- c) rosszindulatú programkód
- d) vírusirtó szoftver és vírusdefiníciós fájlok

1.10. Mi vezethet rosszindulatú programkódok telepítéséhez?

- a) a makrók letiltása az alkalmazásokban
- b) hátsó kapu használata a rendszerbiztonság megkerüléséhez
- c) a "vis maior" esetekre való hivatkozás
- d) biometrikus védelem alkalmazása a felhasználók személyazonosságának megállapításához

1.11. Mi az előnye a vírusirtóknak?

- a) megakadályozzák a kifinomult támadásokat
- b) frissítik a digitális tanúsítványokat
- c) felismerik a vírusokat a számítógépen
- d) megakadályozzák az információ-búvárkodást

1.12. Mi igaz a karanténban lévő fájlokra?








- a) nem lehet letölteni
- b) nem lehet fertőzésmentesíteni
- c) nem lehet törölni
- d) nem lehet megfertőzni

1.13. Miért kell vírusdefiníciós fájlokat letölteni?

- a) frissíti az ideiglenesen letöltött és tárolt fájlokat
- b) frissíti a sütiket
- c) lehetővé teszi az új fenyegetések elleni védelmet
- d) frissíti az elektromágneses törléseket végző szoftvert

1.14. Hogyan nevezik az irodában vagy otthon összekapcsolt számítógépeket?

- a) LAN
- b) VPN
- c) WAN
- d) USB

- 1.15. Mi a hálózati adminisztrátor feladata?
- fenntartani az épület elektromos hálózatának folyamatos működőképességét
 - biztosítani a hálózati adatokhoz a nyilvános hozzáférést
 - biztosítani, hogy az adatokat ne mentse le a rendszerbe
 - fenntartani a munkatársak szükséges adathozzáférést a hálózaton
- 1.16. Mi akadályozza meg a jogosulatlan belépést a hálózatba egy külső helyszínről?
- elektromágneses törlés
 - tűzfalak
 - adathalászat
 - digitális tanúsítványok
- 1.17. Melyik ikon jelenti a csatlakoztatható vezetékes hálózatot?
- 
 - 
 - 
 - 
- 1.18. Mi a hálózatra történő csatlakozás biztonsági vonatkozása?
- adatok biztonsági mentése
 - fájlok tömörítése
 - személyes adatok védelme
 - információbúvárcodás
- 1.19. Miért kell jelszóval védeni a vezeték nélküli hálózatokat?
- elindítja a vírusirtó szoftvert
 - megakadályozza a jogosulatlan adat-hozzáférést
 - biztosítja a süti engedélyezését
 - megakadályozza az adathalászatra irányuló támadásokat
- 1.20. Mi igazolja, hogy az üzenet küldője valóban az, akinek állítja magát?
- digitális tanúsítvány
 - süti
 - makró
 - letöltött és ideiglenesen tárolt internet fájlok
- 1.21. Melyik jelöli a biztonságos weboldalakat?
- 
 - 
 - 



d)

- 1.22. Mely fájlok tartalmazhatnak nyilvános kulcsokat és más hitelesítő adatokat?
- vírusdefiníciós fájlok
 - titkosított adatbázis-mentési fájlok
 - makrók
 - digitális tanúsítványok
- 1.23. Miért kell a sütitket blokkolni a böngészőkben?
- hogy vírusirtó szoftvert lehessen telepíteni
 - hogy hozzá lehessen férni a web-alapú elektronikus levelezési fiókokhoz
 - hogy böngészhessünk ismeretlen weblapokon
 - hogy megakadályozzuk az internetes zaklatást
- 1.24. Mi lenne az eredménye annak, ha egy közösségi oldalon a személyes adatokat a nyilvánosság számára hozzáférhetővé tennénk?
- a személyes adatokhoz csak a barátok férhetnének hozzá
 - a személyes adatokat bárki megnézheti
 - a barátok barátai láthatnák a személyes adatokat
 - a barátok módosíthatnák a személyes adatokat
- 1.25. Mi tartalmazhat rosszindulatú programkódot vagy vírust?
- X509v3 digitális tanúsítványok
 - tűzfalak
 - digitális aláírások
 - csalárd elektronikus levelek
- 1.26. Mi használja az adatok megszerzéséhez hamisított weboldalak linkjeit?
- rendszerszinten tevékenykedő kártékony kódok
 - tárcsázó programok
 - adathalászat
 - bankkártya-lemásolás
- 1.27. Miért NEM szabad megnyitni egy ismeretlen csatolmányt?
- rosszindulatú programkódokat tartalmazhat
 - lehet, hogy nagyon nagy a fájl
 - lehet, hogy titkosító kulcs szükséges a megnyitáshoz
 - lehetséges, hogy digitális tanúsítványt tartalmaz
- 1.28. Melyik lehet az azonnali üzenetküldés sebezhetősége?
- vírusdefiníciós fájlok
 - on-line emelt díjas tárcsázó programok
 - digitális tanúsítványok
 - rosszindulatú programkódok

- 1.29. Melyik egy lehetséges mentési tulajdonság?
- a) bankkártya lemásolás
 - b) ütemezés
 - c) kikérdezés
 - d) elektromágneses törlés
- 1.30. Mi NEM eredményezi az adatok végleges törlését?
- a) az adatok átmozgatása a Lomtárba
 - b) a háttértároló elektromágneses törlése
 - c) a szoftveres adatmegsemmisítő eszközök használata
 - d) a DVD-k bedarálása
2. Nyissa meg a vizsgaközpont által megadott mappában található **hossaferes.doc** fájlt! Tegye megnyitás-védetté a fájlt, a **guard** jelszó használatával! Mentse el és zárja be a **hossaferes** fájlt! [1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **rendszer.doc** fájlról a **juniusi_mentes** könyvtárba! [1 pont]
- Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

25.FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
- 1.1. Mi az információ információbiztonsági szempontból?
- a) adatfeldolgozás kimenete
 - b) logikai állítások kombinációja
 - c) nyers és nem szervezett tények összessége
 - d) feldolgozandó ábrák
- 1.2. Melyik tevékenység jogellenes internet vagy számítógéphasználat közben?
- a) etikus hackelés
 - b) elektromágneses megsemmisítés
 - c) kiberbűnözés
 - d) digitális aláírás
- 1.3. Mi NEM fenyegeti az adatokat?
- a) emberi tevékenység
 - b) zombi-hálózati szoftverek
 - c) rosszindulatú programkódok
 - d) hozzáférés-védelmi szoftverek
- 1.4. Mi az oka a személyes adatok védelmének?
- a) csalások megelőzése
 - b) süti karbantartása
 - c) hátsó ajtó biztosítása
 - d) elektromágneses törlés
- 1.5. Melyik információbiztonsági jellemző biztosítja az adatok jogosulatlan módosítása elleni védelmét?
- a) rendelkezésre állás
 - b) sértetlenség
 - c) bizalmasság
 - d) hozzáférhetőség
- 1.6. Mi a szélhámosság közvetlen következménye?
- a) jogosulatlan hozzáférés a számítógéphez
 - b) tárhely-problémákhoz vezet
 - c) alkalmazza a süti blokkolási beállításait
 - d) törli a könyvjelzőket a böngészőből
- 1.7. Mi a kikérdezés?
- a) szöveges üzenetküldés a telefonszolgáltató weboldaláról

- b) jelszó-visszaállítási eljárások összessége
- c) üzenetküldés azonnali üzenetküldővel
- d) személyes információk begyűjtése megtévesztéssel

1.8. Mi a titkosítás korlátja?

- a) a fájl tulajdonosa könnyen azonosítható
- b) a titkosító kulcs elvesztésével az adat könnyen helyreállítható
- c) a titkosító kulcs elvesztésével az adat használhatatlanná válik
- d) a ktitkosított adat nem felhasználható

1.9. Mi a rosszindulatú programkód?

- a) vírusirtó szoftverek rendszeres futtatásának ütemezésére használt számítógépes program
- b) engedély nélkül használt szoftverek
- c) tűzfal-beállítások ellenőrzésére használatos szoftver
- d) számítógépes rendszerekbe engedély nélküli beszivárgást lehetővé tevő szoftver

1.10. Melyik az a rosszindulatú programkód, amelyik a felhasználó engedélye nélkül gyűjt adatokat a böngészési szokásairól?

- a) kémsoftver
- b) zombi-hálózat szoftvere
- c) tárcsázók
- d) eltérítéses adathalászat

1.11. Mi egy fertőző, rosszindulatú program?

- a) a süti
- b) a vírus
- c) a digitális tanúsítvány
- d) a digitális aláírás

1.12. Melyik képes megfertőzni és irányítani egy számítógépet a tulajdonos engedélye nélkül?

- a) biometria
- b) vírus-definíciós fájl
- c) süti
- d) zombi-hálózat

1.13. Mi a vírusirtó szoftverek előnye?

- a) megvizsgálják a számítógépet hogy nem fertőződnek-e meg
- b) megakadályozzák a tartalom-ellenőrző szoftverek elindítását
- c) minden adatot mentenek
- d) a korábban törölt fájlokat visszaállítják a számítógép háttértárolójára

1.14. Mi akadályozza meg a hálózathoz kívülről történő jogosulatlan hozzáférést?

- a) fájlok hozzáférés-védelmi beállításai
- b) tartalom-ellenőrző program

- c) zombi-hálózati szoftver
- d) tűzfalak





1.15. Mi biztosítja a vezeték nélküli biztonságot?

- a) WAN
- b) LAN
- c) Média Hozzáférési Kontroll (MAC)
- d) számítógépes hálózathoz hátsó kaput nyitó szoftver

1.16. Mi eredményezhet jogosulatlan adathozzáférést?

- a) elektromágneses törlés
- b) adat-hozzáférés vezeték nélküli forgalom lehallgatásakor
- c) biometrikus védelmi intézkedésen alapuló hozzáférés-védelmi szoftver telepítése
- d) digitális tanúsítvány

1.17. Melyik ikon jelzi a nem védett vezeték nélküli hálózatot?

- a) 
- b) 
- c) 
- d) 

1.18. Hogyan történik a hálózati bejelentkezés?

- a) felhasználói névvel és jelszóval
- b) automatikus kiegészítéssel
- c) titkosított felhasználói névvel
- d) digitális tanúsítvánnyal

1.19. Melyik a jó szabály a jelszavakra?




- a) használjon minél kevesebb karaktert a jelszóban
- b) időnként változtassa meg a jelszavát
- c) ossza meg a jelszavát a barátaival
- d) a jelszóban sose használjon vegyesen betűket és számokat

1.20. Melyik weboldalnál található http előtag a https helyett?

- a) on-line bank
- b) keresőmotor
- c) on-line webáruház
- d) biztonságos weboldal

1.21. Melyik ikon jelzi a biztonságos web-oldalt?

- a) 

- b) 
- c) 
- d) 

- 1.22. Melyik támadás irányítja át a web-oldal forgalmát egy hamisított web-oldalra?
- a) crackelés
 - b) eltérítéssel adathalászat
 - c) etikus hackelés
 - d) információ-szerzés
- 1.23. Melyik a böngészők által a számítógépen tárolt apró szöveg?
- a) tűzfal
 - b) trójai program
 - c) rendszerszinten rejtőző kártékony kód
 - d) süti
- 1.24. Mitől kell tartanunk a közösségi média használatakor?
- a) biometria
 - b) etikus hackelés
 - c) internetes zaklatás
 - d) titkosított fájlok
- 1.25. Mi biztosítja azt, hogy csak a címzettek olvashassanak el egy elektronikus levelet?
- a) az elektronikus levél aláírással való ellátása
 - b) az elektronikus levél titkosítása
 - c) egyszerű szöveges elektronikus levél formázása
 - d) definíciós fájl hozzáadása az elektronikus levélhez
- 1.26. Mi használ bejegyzett cégneveket személyes biztonsági adatok megszerzéséhez?
- a) adathalászat
 - b) figyelés
 - c) billentyűzet-leütés naplózás
 - d) zombi-hálózati szoftver
- 1.27. Mi a valós idejű szöveges kommunikáció két vagy több személy között?
- a) elektronikus levél
 - b) fájl-megosztás
 - c) eltérítéssel adathalászat
 - d) azonnali üzenetküldés
- 1.28. Mi segít biztosítani a bizalmasságot az azonnali üzenetküldés során?
- a) a tűzfal bekapcsolása
 - b) a tűzfal kikapcsolása

- c) a fájl-megosztás korlátozása
- d) titkosítás használata

1.29. Mi használható az eszközök fizikai biztonságának növelésére?

- a) vírusirtó szoftver
- b) titkosított szöveges dokumentumok
- c) biztonsági kábel
- d) elektromagnetikus törlés

1.30. Melyik módszer törli visszaállíthatatlanul az adatokat?

- a) az adatok Lomtárba mozgatása
- b) az adatokat tartalmazó lemez bedarálása
- c) jelszavas tömörítés alkalmazása
- d) adatok titkosított merevlemezre való elhelyezése

2. Keresse meg a vizsgaközpont által megadott mappában található **level.doc** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a **lock** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **halozat.doc** fájlról a **marciusi_mentes** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

26.FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
 - 1.1. Melyik kiberbűnözés az alábbiak közül?
 - a) okostelefon ellopása
 - b) internetes számla on-line befizetése
 - c) bankkártya adatok ellopása on-line
 - d) internetes rádióhallgatása on-line
 - 1.2. Melyik eljárás tartalmazza az informatikai biztonsági sebezhetőségek tesztelését?
 - a) crackelés
 - b) etikus hackelés
 - c) bankkártya adatainak lemásolása
 - d) kikérdezés
 - 1.3. Miért kell védeni az üzletileg érzékeny információkat?
 - a) mert megakadályozza az adatlopást
 - b) ütemezett mentések lefutásának biztosítása miatt
 - c) kéretlen üzenetek blokkolása miatt
 - d) a biztonságos weboldalak azonosításáért
 - 1.4. Melyik nyújt védelmet a jogosulatlan adat-hozzáférés ellen?
 - a) bonyolult fájlnevek
 - b) billentyűzet-leütés naplózása
 - c) eltérítéssel adathalászat
 - d) titkosítás
 - 1.5. Melyik információbiztonsági tulajdonság biztosítja az adatok jogosulatlan hozzáférés vagy felfedés elleni védelmét?
 - a) bizalmasság
 - b) sértetlenség
 - c) rendelkezésre állás
 - d) hitelesség
 - 1.6. Melyik európai szabályozást kell betartani a személyes adatok védelmének vonatkozásában?
 - a) 1997 Európai Adatvédelmi Szabályozás
 - b) 2001 Európai Információs Társadalmi Irányelv
 - c) 1995 Európai Adatvédelmi Irányelv
 - d) 2001 Európai Irányelv az Információ-Technológiáról

1.7. Melyik tartozik a szélhámosság módszerei közé?

- a) közösségi oldalakhoz több fiókkal rendelkezni
- b) valaki válla fölött megszerezni az információkat
- c) videó- és hanghívásokat kezdeményezni az interneten
- d) meghivatkozni más weboldalát egy közösségi oldalról

1.8. Mi a személyazonosság-lopás közvetlen következménye?

- a) a pénzügyi adatokat mások is használhatják
- b) a vírusirtó nem működik a továbbiakban
- c) a letöltött és ideiglenesen tárolt fájlokat törölni fogják
- d) a mentés ütemezését megváltoztatják

1.9. Melyik szoftvert készítek és küldik károkozási célból?

- a) szimmetrikus vagy aszimmetrikus elvű titkosító szoftverek
- b) tűzfalak
- c) rosszindulatú programkódok
- d) vírusirtó szoftverek

1.10. Mit használnak a rosszindulatú programkódok elrejtésére?

- a) rendszerszinten tevékenykedő kártékony kódokat
- b) elektromágneses elven alapuló adattörlési módszereket
- c) tűzfalakat
- d) bedarálást

1.11. Mi a vírusirtó szoftverek korlátja?

- a) vírus-ellenőrzés közben figyelni kell a működését
- b) nem lehetséges a vírus-ellenőrzést ütemezni
- c) naprakészen kell tartani a vírusdefiníciós fájlokat
- d) karanténba teszi a fertőzött fájlokat

1.12. Mi igaz a karanténban lévő fájlokra?

- a) szoftverfrissítések
- b) ezek törölve lettek a számítógépről
- c) visszaállíthatók, ha szükséges
- d) vírusdefiníciós fájlok

1.13. Mi a célja a szoftverfrissítések telepítésének?

- a) töröljük az internetről letöltött és ideiglenesen tárolt fájlokat
- b) kijavítjuk egy program hibáját vagy biztonsági kockázatát
- c) töröljük a sütiket
- d) engedélyezzük az automatikus kiegészítést

1.14. Melyik írja le a LAN-t?





- a) kis földrajzi területen több összekötött számítógép együttese
- b) olyan nyilvános hálózat, mely megengedi a biztonságos kapcsolódást más nyilvános számítógépekhez

- c) nagy kiterjedésű területen összekapcsolt számítógépek együttese
- d) ugyanabban a helyiségben elhelyezett hálózati eszközök együttese

1.15. Mi a tűzfal feladata?

- a) törölni a sütiket a számítógépről vagy a hálózatról
- b) a mentéshez biztosítson biztonságos háttér-adattárolókat
- c) védje a hálózatot a betörésektől
- d) automatikusan frissítse a digitális tanúsítványokat

1.16. Melyik ikon jelenti a drótnélküli hálózatot?

- a) 
- b) 
- c) 
- d) 

1.17. Mi a biztonsági kihatása a hálózatra való csatlakozásnak?

- a) nem lehet hozzáférni a privát hálózathoz
- b) megfertőződhet a számítógép rosszindulatú szoftverekkel
- c) a fájlokhoz történő hozzáférés a hálózaton keresztül lelassul
- d) az összes internetről letöltött és ideiglenesen tárolt fájl törlődik

1.18. Miért szükséges jelszó alkalmazása a drótnélküli hálózatok hozzáféréséhez?

- a) megelőzi a hálózathoz való csatlakozási késedelmet
- b) biztosítja a vírusirtó szoftver naprakészességét
- c) így csak jogos felhasználó használhatja a hálózatot
- d) megvédi a hálózati tűzfalat

1.19. Melyik biometria védelem?

- a) adatok mentése
- b) bankkártya lemásolása
- c) kikérdezés
- d) retina-szkennelés

1.20. Mihez kell ragaszkodni egy on-line pénzügyi tranzakció elvégzésekor?

- a) a web-oldal biztonságához
- b) az automatikus kiterjesztés bekapcsolásához
- c) a Lomtárnak a tranzakciót követő kiürítéséhez
- d) a tranzakciót követő elektromágneses törléshez

1.21. Mit jelent az eltérítéssel adathalászat (pharming)?

- a) a biztonsági forgalom irányítása tiltási és engedélyezési listákat alkalmazó szoftverrel
- b) a webforgalom átirányítása egy hamisított web-oldalra
- c) a kifigyelés egyik módszere

- d) az ideiglenesen letöltött és tárolt internet-fájlok megszerzése
- 1.22. Mi gyorsítja fel egy ismétlődő adatbevitelt is tartalmazó on-line űrlap kitöltését?
- a) automatikus kiegészítés
 - b) makrók tiltása
 - c) titkosítás
 - d) elektromagnetikus törlés
- 1.23. Milyen adatokat kell rendszeres időközönként ellenőrizni és törölni a böngészőből?
- a) makrókat
 - b) sütitket
 - c) digitális tanúsítványokat
 - d) vírusdefiníciós fájlokat
- 1.24. Melyik célja a weboldalakhoz való hozzáférés ellenőrzése és korlátozása?
- a) reklámokat megjelenítő szoftver
 - b) kémsoftver
 - c) adathalász szoftver
 - d) tartalomellenőrző szoftver
- 1.25. Mit nem szabad közzétenni egy közösségi oldalon?
- a) zenei érdeklődést
 - b) becenevet
 - c) otthoni címet
 - d) kedvenc televízióműsort
- 1.26. Melyik az a titkosított kód, amely egy személy azonosságát társítja egy fájlhoz?
- a) jelszavas tömörített fájl
 - b) digitális aláírás
 - c) makrózott titkosított szöveg
 - d) ideiglenesen letöltött és tárolt fájl
- 1.27. Mi az adathalászat?
- a) lopott bankkártya adatainak felhasználása on-line vásárlásnál
 - b) információkat kifigyelni valaki válla felett
 - c) félrevezetni valakit az interneten értékes információk megszerzéséért
 - d) az informatikai biztonsági hiányosságok tesztelése
- 1.28. Mi jelenti a legnagyobb kitétséget a rosszindulatú programkódoknak?
- a) hozzáférés biztonságos weboldalhoz
 - b) levélcsatolmány megnyitása
 - c) elektronikus levél írása
 - d) adatok mentése
- 1.29. Mi az azonnali üzenetküldés sebezhetősége?
- a) hátsó ajtó hozzáférés

- b) valós idejű hozzáférés
- c) vis maior
- d) információbúvárkodás

1.30. Mi jelenti az adatok végleges megsemmisítését?

- a) eltérítéssel adathalászat
- b) áramellátás kiesése
- c) tárcsázás
- d) elektromágneses törlés

2. Nyissa meg a vizsgaközpont által megadott mappában található **biztonsag.doc** fájlt! Tegye megnyitás-védetté a fájlt, a **guard** jelszó használatával! Mentse el és zárja be a **biztonsag** fájlt! [1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **promocio.ppt** fájlról az **aprilisi_mentes** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

27.FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
 - 1.1. Melyik tevékenység kiberbűnözés?
 - a) bedarálás
 - b) adathalászat
 - c) etikus hackelés
 - d) titkosítás
 - 1.2. Mit jelent a "hackelés" fogalma?
 - a) az adatokhoz való jogosulatlan hozzáférés megszerzése
 - b) félrevezetni a személyazonosságunkról valakit az interneten
 - c) vírusirtóval eltávolítani az összes rosszindulatú szoftvert a gépünkről
 - d) számítógépeket lopni az épületbe való betöréssel
 - 1.3. Melyik jelent „vis maior” fenyegetést az adatokra?
 - a) emberi tevékenység
 - b) adatlopás
 - c) tűz
 - d) vírusok
 - 1.4. Mi a személyes adatok védelmének célja?
 - a) az etikus hackelés megelőzése
 - b) a személyazonosság-lopás megakadályozása
 - c) helyet lehessen megtakarítani a számítógép háttértárolóján
 - d) a számítógépes vírusok elkerülése
 - 1.5. Melyik információbiztonsági tulajdonság biztosítja a tárolt adatok jogosulatlan hozzáférés elleni védelmét?
 - a) bizalmasság
 - b) sértetlenség
 - c) rendelkezésre állás
 - d) hitelesség
 - 1.6. Melyik állítás igaz az informatikai biztonsági szabályzatokra?
 - a) csak az informatikusokra vonatkoznak
 - b) csak a pénzügyi intézmények számára fontosak
 - c) csak olvasni kell, de nem kell megvalósítani
 - d) fontosak, mivel követendő szabályokat adnak a felhasználók számára
 - 1.7. Melyik NEM közvetlen következménye a szélhámosságnak?
 - a) a személyes adatok mások által hozzáférhetővé váltak

- b) hozzáférhetővé vált mások által a számítógép-rendszer
- c) a tűzfalat kikapcsolják
- d) a begyűjtött adatokat csalásra fogják felhasználni

1.8. Melyik a személyazonosság-lopás módszere?

- a) hamis név használata egy közösségi oldalon
- b) nem megfelelő kulcs használata dokumentum titkosításának feloldásához
- c) adatok elektromágneses eszközökkel történő megsemmisítése
- d) információbúvárkodás

1.9. Mi használható egy rosszindulatú program elrejtésére?

- a) kikérdezés
- b) rendszerszinten tevékenykedő kártékony kód
- c) biometria
- d) bankkártya-lemásolás

1.10. Mit lehet adatlopásra használni?

- a) zombi-hálózat szoftverét
- b) adatok elektromágneses eszközökkel történő megsemmisítését
- c) alhálózatokat
- d) bedarálást

1.11. Mi az előnye a vírusirtóknak?

- a) megakadályozzák a kifinomult támadásokat
- b) frissítik a digitális tanúsítványokat
- c) felismerik a vírusokat a számítógépen
- d) megakadályozzák az információ-búvárkodást

1.12. Mi igaz a karanténban lévő fájlokra?

- a) nem lehet letölteni
- b) nem lehet fertőzésmentesíteni
- c) nem lehet törölni
- d) nem lehet megfertőzni

1.13. Miért kell vírusdefiníciós fájlokat letölteni?

- a) frissíti az ideiglenesen letöltött és tárolt fájlokat
- b) frissíti a sütiket
- c) lehetővé teszi az új fenyegetések elleni védelmet
- d) frissíti az elektromágneses törléseket végző szoftvert

1.14. Hogyan nevezik az irodában vagy otthon összekapcsolt számítógépeket?

- a) LAN
- b) VPN
- c) WAN
- d) USB





1.15. Mi a hálózati adminisztrátor feladata?

- a) fenntartani az épület elektromos hálózatának folyamatos működőképességét
- b) biztosítani a hálózati adatokhoz a nyilvános hozzáférést
- c) biztosítani, hogy az adatokat ne mentse le a rendszerbe
- d) fenntartani a munkatársak szükséges adathozzáférést a hálózaton

1.16. Mi akadályozza meg a jogosulatlan belépést a hálózatba egy külső helyszínről?

- a) elektromágneses törlés
- b) tűzfalak
- c) adathalászat
- d) digitális tanúsítványok

1.17. Melyik ikon jelenti a csatlakoztatható vezetékes hálózatot?

- a) 
- b) 
- c) 
- d) 

1.18. Mi a hálózatra történő csatlakozás biztonsági vonatkozása?

- a) adatok biztonsági mentése
- b) fájlok tömörítése
- c) személyes adatok védelme
- d) információbúvárkodás

1.19. Miért kell jelszóval védeni a vezeték nélküli hálózatokat?

- a) elindítja a vírusirtó szoftvert
- b) megakadályozza a jogosulatlan adat-hozzáférést
- c) biztosítja a süti engedélyezését
- d) megakadályozza az adathalászatra irányuló támadásokat

1.20. Mi igazolja, hogy az üzenet küldője valóban az, akinek állítja magát?

- a) digitális tanúsítvány
- b) süti
- c) makró
- d) letöltött és ideiglenesen tárolt internet fájlok

1.21. Mit jelent az eltérítéssel adathalászat (pharming)?

- a) a biztonsági forgalom irányítása tiltási és engedélyezési listákat alkalmazó szoftverrel
- b) a webforgalom átirányítása egy hamisított web-oldalra
- c) a figyelés egyik módszere
- d) az ideiglenesen letöltött és tárolt internet-fájlok megszerzése

- 1.22. Mi gyorsítja fel egy ismétlődő adatbevitelt is tartalmazó on-line űrlap kitöltését?
- automatikus kiegészítés
 - makrók tiltása
 - titkosítás
 - elektromagnetikus törlés
- 1.23. Milyen adatokat kell rendszeres időközönként ellenőrizni és törölni a böngészőből?
- makrókat
 - sütiket
 - digitális tanúsítványokat
 - vírusdefiníciós fájlokat
- 1.24. Melyik célja a weboldalakhoz való hozzáférés ellenőrzése és korlátozása?
- reklámokat megjelenítő szoftver
 - kémszoftver
 - adathalász szoftver
 - tartalomellenőrző szoftver
- 1.25. Mit nem szabad közzétenni egy közösségi oldalon?
- zenei érdeklődést
 - becenevet
 - otthoni címet
 - kedvenc televízióműsort
- 1.26. Melyik az a titkosított kód, amely egy személy azonosságát társítja egy fájlhoz?
- jelszavas tömörített fájl
 - digitális aláírás
 - makrózott titkosított szöveg
 - ideiglenesen letöltött és tárolt fájl
- 1.27. Mi az adathalászat?
- lopott bankkártya adatainak felhasználása on-line vásárlásnál
 - információkat kifigyelni valaki válla felett
 - félrevezetni valakit az interneten értékes információk megszerzéséért
 - az informatikai biztonsági hiányosságok tesztelése
- 1.28. Mi jelenti a legnagyobb kitétséget a rosszindulatú programkódoknak?
- hozzáférés biztonságos weboldalhoz
 - levélcsatolmány megnyitása
 - elektronikus levél írása
 - adatok mentése
- 1.29. Mi az azonnali üzenetküldés sebezhetősége?
- hátsó ajtó hozzáférés
 - valós idejű hozzáférés
 - vis maior

d) információbúvárkodás

1.30. Mi jelenti az adatok végleges megsemmisítését?

- a) eltérítéssel adathalászat
- b) áramellátás kiesése
- c) tárcsázás
- d) elektromágneses törlés

2. Keresse meg a vizsgaközpont által megadott mappában található **iroszer.doc** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a **safe** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **ertesites.xls** fájlról a **juliusi_mentes** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

28.FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
 - 1.1. Melyik tevékenység kiberbűnözés?
 - a) bedarálás
 - b) adathalászat
 - c) etikus hackelés
 - d) titkosítás
 - 1.2. Mit jelent a "hackelés" fogalma?
 - a) az adatokhoz való jogosulatlan hozzáférés megszerzése
 - b) félrevezetni a személyazonosságunkról valakit az interneten
 - c) vírusirtóval eltávolítani az összes rosszindulatú szoftvert a gépünkről
 - d) számítógépeket lopni az épületbe való betöréssel
 - 1.3. Melyik jelent „vis maior” fenyegetést az adatokra?
 - a) emberi tevékenység
 - b) adatlopás
 - c) tűz
 - d) vírusok
 - 1.4. Mi a személyes adatok védelmének célja?
 - a) az etikus hackelés megelőzése
 - b) a személyazonosság-lopás megakadályozása
 - c) helyet lehessen megtakarítani a számítógép háttértárolóján
 - d) a számítógépes vírusok elkerülése
 - 1.5. Melyik információbiztonsági tulajdonság biztosítja a tárolt adatok jogosulatlan hozzáférés elleni védelmét?
 - a) bizalmasság
 - b) sértetlenség
 - c) rendelkezésre állás
 - d) hitelesség
 - 1.6. Melyik állítás igaz az informatikai biztonsági szabályzatokra?
 - a) csak az informatikusokra vonatkoznak
 - b) csak a pénzügyi intézmények számára fontosak
 - c) csak olvasni kell, de nem kell megvalósítani
 - d) fontosak, mivel követendő szabályokat adnak a felhasználók számára
 - 1.7. Melyik NEM közvetlen következménye a szélhámosságnak?
 - a) a személyes adatok mások által hozzáférhetővé váltak

- b) hozzáférhetővé vált mások által a számítógép-rendszer
- c) a tűzfalat kikapcsolják
- d) a begyűjtött adatokat csalásra fogják felhasználni

1.8. Melyik a személyazonosság-lopás módszere?

- a) hamis név használata egy közösségi oldalon
- b) nem megfelelő kulcs használata dokumentum titkosításának feloldásához
- c) adatok elektromágneses eszközökkel történő megsemmisítése
- d) információbúvárkodás

1.9. Mi használható egy rosszindulatú program elrejtésére?

- a) kikérdezés
- b) rendszerszinten tevékenykedő kártékony kód
- c) biometria
- d) bankkártya-lemásolás

1.10. Mit lehet adatlopásra használni?

- a) zombi-hálózat szoftverét
- b) adatok elektromágneses eszközökkel történő megsemmisítését
- c) alhálózatokat
- d) bedarálást

1.11. Mi egy fertőző, rosszindulatú program?

- a) a süti
- b) a vírus
- c) a digitális tanúsítvány
- d) a digitális aláírás

1.12. Melyik képes megfertőzni és irányítani egy számítógépet a tulajdonos engedélye nélkül?

- a) biometria
- b) vírus-definíciós fájl
- c) süti
- d) zombi-hálózat

1.13. Mi a vírusirtó szoftverek előnye?

- a) megvizsgálják a számítógépet hogy nem fertőződnek-e meg
- b) megakadályozzák a tartalom-ellenőrző szoftverek elindítását
- c) minden adatot mentenek
- d) a korábban törölt fájlokat visszaállítják a számítógép háttértárolójára

1.14. Mi akadályozza meg a hálózathoz kívülről történő jogosulatlan hozzáférést?

- a) fájlok hozzáférés-védelmi beállításai
- b) tartalom-ellenőrző program
- c) zombi-hálózati szoftver
- d) tűzfalak





1.15. Mi biztosítja a vezeték nélküli biztonságot?

- a) WAN
- b) LAN
- c) Média Hozzáférési Kontroll (MAC)
- d) számítógépes hálózathoz hátsó kaput nyitó szoftver

1.16. Mi eredményezhet jogosulatlan adathozzáférést?

- a) elektromágneses törlés
- b) adat-hozzáférés vezeték nélküli forgalom lehallgatásakor
- c) biometrikus védelmi intézkedésen alapuló hozzáférés-védelmi szoftver telepítése
- d) digitális tanúsítvány

1.17. Melyik ikon jelzi a nem védett vezeték nélküli hálózatot?

- a) 
- b) 
- c) 
- d) 

1.18. Hogyan történik a hálózati bejelentkezés?

- a) felhasználói névvel és jelszóval
- b) automatikus kiegészítéssel
- c) titkosított felhasználói névvel
- d) digitális tanúsítvánnyal

1.19. Melyik a jó szabály a jelszavakra?

- a) használjon minél kevesebb karaktert a jelszóban
- b) időnként változtassa meg a jelszavát
- c) ossza meg a jelszavát a barátaival
- d) a jelszóban sose használjon vegyesen betűket és számokat

1.20. Melyik weboldalnál található http előtag a https helyett?

- a) on-line bank
- b) keresőmotor
- c) on-line webáruház
- d) biztonságos weboldal

1.21. Mit jelent az eltérítéssel adathalászat (pharming)?

- a) a biztonsági forgalom irányítása tiltási és engedélyezési listákat alkalmazó szoftverrel
- b) a webforgalom átirányítása egy hamisított web-oldalra
- c) a figyelés egyik módszere
- d) az ideiglenesen letöltött és tárolt internet-fájlok megszerzése

- 1.22. Mi gyorsítja fel egy ismétlődő adatbevitelt is tartalmazó on-line űrlap kitöltését?
- automatikus kiegészítés
 - makrók tiltása
 - titkosítás
 - elektromagnetikus törlés
- 1.23. Milyen adatokat kell rendszeres időközönként ellenőrizni és törölni a böngészőből?
- makrókat
 - sütiket
 - digitális tanúsítványokat
 - vírusdefiníciós fájlokat
- 1.24. Melyik célja a weboldalakhoz való hozzáférés ellenőrzése és korlátozása?
- reklámokat megjelenítő szoftver
 - kémszoftver
 - adathalász szoftver
 - tartalomellenőrző szoftver
- 1.25. Mit nem szabad közzétenni egy közösségi oldalon?
- zenei érdeklődést
 - becenevet
 - otthoni címet
 - kedvenc televízióműsort
- 1.26. Melyik az a titkosított kód, amely egy személy azonosságát társítja egy fájlhoz?
- jelszavas tömörített fájl
 - digitális aláírás
 - makrózott titkosított szöveg
 - ideiglenesen letöltött és tárolt fájl
- 1.27. Mi az adathalászat?
- lopott bankkártya adatainak felhasználása on-line vásárlásnál
 - információkat kifigyelni valaki válla felett
 - félrevezetni valakit az interneten értékes információk megszerzéséért
 - az informatikai biztonsági hiányosságok tesztelése
- 1.28. Mi jelenti a legnagyobb kitétséget a rosszindulatú programkódoknak?
- hozzáférés biztonságos weboldalhoz
 - levélcsatolmány megnyitása
 - elektronikus levél írása
 - adatok mentése
- 1.29. Mi az azonnali üzenetküldés sebezhetősége?
- hátsó ajtó hozzáférés
 - valós idejű hozzáférés
 - vis maior

d) információbúvárkodás

1.30. Mi jelenti az adatok végleges megsemmisítését?

- a) eltérítéssel adathalászat
- b) áramellátás kiesése
- c) tárcsázás
- d) elektromágneses törlés

2. Nyissa meg a vizsgaközpont által megadott mappában található **hossaferes.doc** fájlt! Tegye megnyitás-védetté a fájlt, a **guard** jelszó használatával! Mentse el és zárja be a **hossaferes** fájlt! [1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **rendszer.doc** fájlról a **juniusi_mentes** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

29.FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
 - 1.1. Melyik tevékenység kiberbűnözés?
 - a) bedarálás
 - b) adathalászat
 - c) etikus hackelés
 - d) titkosítás
 - 1.2. Mit jelent a "hackelés" fogalma?
 - a) az adatokhoz való jogosulatlan hozzáférés megszerzése
 - b) félrevezetni a személyazonosságunkról valakit az interneten
 - c) vírusirtóval eltávolítani az összes rosszindulatú szoftvert a gépünkről
 - d) számítógépeket lopni az épületbe való betöréssel
 - 1.3. Melyik jelent „vis maior” fenyegetést az adatokra?
 - a) emberi tevékenység
 - b) adatlopás
 - c) tűz
 - d) vírusok
 - 1.4. Mi a személyes adatok védelmének célja?
 - a) az etikus hackelés megelőzése
 - b) a személyazonosság-lopás megakadályozása
 - c) helyet lehessen megtakarítani a számítógép háttértárolóján
 - d) a számítógépes vírusok elkerülése
 - 1.5. Melyik információbiztonsági tulajdonság biztosítja a tárolt adatok jogosulatlan hozzáférés elleni védelmét?
 - a) bizalmasság
 - b) sértetlenség
 - c) rendelkezésre állás
 - d) hitelesség
 - 1.6. Melyik állítás igaz az informatikai biztonsági szabályzatokra?
 - a) csak az informatikusokra vonatkoznak
 - b) csak a pénzügyi intézmények számára fontosak
 - c) csak olvasni kell, de nem kell megvalósítani
 - d) fontosak, mivel követendő szabályokat adnak a felhasználók számára
 - 1.7. Melyik NEM közvetlen következménye a szélhámosságnak?
 - a) a személyes adatok mások által hozzáférhetővé váltak

- b) hozzáférhetővé vált mások által a számítógép-rendszer
- c) a tűzfalat kikapcsolják
- d) a begyűjtött adatokat csalásra fogják felhasználni

1.8. Melyik a személyazonosság-lopás módszere?

- a) hamis név használata egy közösségi oldalon
- b) nem megfelelő kulcs használata dokumentum titkosításának feloldásához
- c) adatok elektromágneses eszközökkel történő megsemmisítése
- d) információbúvárkodás

1.9. Mi használható egy rosszindulatú program elrejtésére?

- a) kikérdezés
- b) rendszerszinten tevékenykedő kártékony kód
- c) biometria
- d) bankkártya-lemásolás

1.10. Mit lehet adatlopásra használni?

- a) zombi-hálózat szoftverét
- b) adatok elektromágneses eszközökkel történő megsemmisítését
- c) alhálózatokat
- d) bedarálást

1.11. Mi egy fertőző, rosszindulatú program?

- a) a süti
- b) a vírus
- c) a digitális tanúsítvány
- d) a digitális aláírás

1.12. Melyik képes megfertőzni és irányítani egy számítógépet a tulajdonos engedélye nélkül?

- a) biometria
- b) vírus-definíciós fájl
- c) süti
- d) zombi-hálózat

1.13. Mi a vírusirtó szoftverek előnye?

- a) megvizsgálják a számítógépet hogy nem fertőződnek-e meg
- b) megakadályozzák a tartalom-ellenőrző szoftverek elindítását
- c) minden adatot mentenek
- d) a korábban törölt fájlokat visszaállítják a számítógép háttértárolójára

1.14. Mi akadályozza meg a hálózathoz kívülről történő jogosulatlan hozzáférést?

- a) fájlok hozzáférés-védelmi beállításai
- b) tartalom-ellenőrző program
- c) zombi-hálózati szoftver
- d) tűzfalak





1.15. Mi biztosítja a vezeték nélküli biztonságot?

- a) WAN
- b) LAN
- c) Média Hozzáférési Kontroll (MAC)
- d) számítógépes hálózathoz hátsó kaput nyitó szoftver

1.16. Mi eredményezhet jogosulatlan adathozzáférést?

- a) elektromágneses törlés
- b) adat-hozzáférés vezeték nélküli forgalom lehallgatásakor
- c) biometrikus védelmi intézkedésen alapuló hozzáférés-védelmi szoftver telepítése
- d) digitális tanúsítvány

1.17. Melyik ikon jelzi a nem védett vezeték nélküli hálózatot?

- a) 
- b) 
- c) 
- d) 

1.18. Hogyan történik a hálózati bejelentkezés?

- a) felhasználói névvel és jelszóval
- b) automatikus kiegészítéssel
- c) titkosított felhasználói névvel
- d) digitális tanúsítvánnyal

1.19. Melyik a jó szabály a jelszavakra?

- a) használjon minél kevesebb karaktert a jelszóban
- b) időnként változtassa meg a jelszavát
- c) ossza meg a jelszavát a barátaival
- d) a jelszóban sose használjon vegyesen betűket és számokat

1.20. Melyik weboldalnál található http előtag a https helyett?

- a) on-line bank
- b) keresőmotor
- c) on-line webáruház
- d) biztonságos weboldal

1.21. Mikor használnak egyszer használatos jelszót?

- a) a laptopra való első bejelentkezéskor
- b) amikor a jelszót elküldik e-mailben
- c) amikor tűzfalat állítanak be
- d) VPN-be való bejelentkezéskor

- 1.22. Melyik adat törölhető a böngésző által?
- kititkosított adat
 - titkosított adat
 - automatikus kiegészítés adata
 - billentyűzet-leütéseket naplózó adat
- 1.23. Melyikkel korlátozható az interneten töltött időtartam?
- adathalász szoftver
 - szülői felügyelet szoftver
 - tárcsázó
 - süti
- 1.24. Melyik a közösségi oldalakon előforduló fenyegetés?
- bedarálás
 - elektromágneses törlés
 - bankkártya adatainak a lemásolása
 - szexuális kizsákmányolás
- 1.25. Milyen eljárás biztosítja az e-mailek bizalmasságát?
- titkosítás
 - kikérdezés
 - eltérítéssel adathalászat
 - kititkosítás
- 1.26. Mi a digitális aláírás eszköze?
- szoftver, ami átirányítja egy weboldal forgalmát egy hamisított weboldalra
 - egy matematikai séma az üzenet hitelességének biztosítására
 - egy bonyolult módszer, mely beszúrja az aláírást az üzenet végére
 - szoftver, mely engedélyezési és tiltólistákat alkalmaz a bejövő hálózati forgalom irányítására
- 1.27. Melyik fogalom írja le a banki adatokat bekérő hamisított elektronikus leveleket?
- kifigyelés
 - internetes zaklatás
 - adathalászat
 - crackelés
- 1.28. Mi tartalmazhat rosszindulatú programkódot?
- levélcsatolmány
 - süti
 - tűzfal
 - digitális aláírás
- 1.29. Melyik nyújt védelmet az adatvesztés ellen?
- süti
 - kikérdezés

- c) titkosított USB lemez használata
- d) mentések

1.30. Miért van szükség az adatok visszaállíthatatlan törlésére?

- a) az áramingadozásból adódó meghibásodások miatt
- b) az adatok más általi visszaállíthatatlansága miatt
- c) hogy tartalomellenőrző szoftvert lehessen telepíteni
- d) hogy törölni lehessen minden sütit

2. Keresse meg a vizsgaközpont által megadott mappában található **level.doc** fájlt! Tömörítse össze a fájlt és tegye megnyitásvédetté a **lock** jelszóval a többi beállítás változatlanul hagyásával együtt! [1 pont]
3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **halozat.doc** fájlról a **marciusi_mentes** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.

30.FELADAT

1. Nyissa meg a **válaszfájl** nevű fájlt. Írja a megfelelő helyre a nevét, kártyaszámát és írja be az elméleti kérdésekre a helyes válaszok betűjelét. Mentse el a fájlt. [30 pont]
- 1.1. Melyik kiberbűnözés az alábbiak közül?
- a) okostelefon ellopása
 - b) internetes számla on-line befizetése
 - c) bankkártya adatok ellopása on-line
 - d) internetes rádióhallgatása on-line
- 1.2. Melyik eljárás tartalmazza az informatikai biztonsági sebezhetőségek tesztelését?
- a) crackelés
 - b) etikus hackelés
 - c) bankkártya adatainak lemásolása
 - d) kikérdezés
- 1.3. Miért kell védeni az üzletileg érzékeny információkat?
- a) mert megakadályozza az adatlopást
 - b) ütemezett mentések lefutásának biztosítása miatt
 - c) kéretlen üzenetek blokkolása miatt
 - d) a biztonságos weboldalak azonosításáért
- 1.4. Melyik nyújt védelmet a jogosulatlan adat-hozzáférés ellen?
- a) bonyolult fájlnevek
 - b) billentyűzet-leütés naplózása
 - c) eltérítéssel adathalászat
 - d) titkosítás
- 1.5. Melyik információbiztonsági tulajdonság biztosítja az adatok jogosulatlan hozzáférés vagy felfedés elleni védelmét?
- a) bizalmasság
 - b) sértetlenség
 - c) rendelkezésre állás
 - d) hitelesség
- 1.6. Melyik európai szabályozást kell betartani a személyes adatok védelmének vonatkozásában?
- a) 1997 Európai Adatvédelmi Szabályozás
 - b) 2001 Európai Információs Társadalmi Irányelv
 - c) 1995 Európai Adatvédelmi Irányelv
 - d) 2001 Európai Irányelv az Információ-Technológiáról

1.7. Melyik tartozik a szélhámosság módszerei közé?

- a) közösségi oldalakhoz több fiókkal rendelkezni
- b) valaki válla fölött megszerezni az információkat
- c) videó- és hanghívásokat kezdeményezni az interneten
- d) meghivatkozni más weboldalát egy közösségi oldalról

1.8. Mi a személyazonosság-lopás közvetlen következménye?

- a) a pénzügyi adatokat mások is használhatják
- b) a vírusirtó nem működik a továbbiakban
- c) a letöltött és ideiglenesen tárolt fájlokat törölni fogják
- d) a mentés ütemezését megváltoztatják

1.9. Melyik szoftvert készítek és küldik károkozási célból?

- a) szimmetrikus vagy aszimmetrikus elvű titkosító szoftverek
- b) tűzfalak
- c) rosszindulatú programkódok
- d) vírusirtó szoftverek

1.10. Mit használnak a rosszindulatú programkódok elrejtésére?

- a) rendszerszinten tevékenykedő kártékony kódokat
- b) elektromágneses elven alapuló adattörlési módszereket
- c) tűzfalakat
- d) bedarálást

1.11. Melyik egy fertőző rosszindulatú szoftver?

- a) a féreg
- b) a süti
- c) a tűzfal
- d) a digitális tanúsítvány

1.12. Melyik igaz a rosszindulatú programkódokra?

- a) a billentyűzetleütés naplózás a begépelte adatot rögzíti
- b) billentyűzet-leütés naplózását a <shift> billentyű lenyomásával lehet engedélyezni a számítógépen
- c) a modemes tárcsázó egy szoftver, ami szűri az interneten végzett telefonhívásokat
- d) a modemes tárcsázó egy személy, aki telefonhívásokat végez az interneten

1.13. Hogyan működnek a vírusirtó szoftverek?

- a) fertőzésmentesített fájlokat helyeznek a karanténba
- b) észlelik a vírusokat, de nem törlik automatikusan őket
- c) észlelik a vírusokat, de nem képesek felismerni a trójai programokat
- d) ütemezett keresést használnak a vírusok észlelésére

1.14. Mi a virtuális magánhálózat (VPN)?

- a) nem kell jelszó a hálózati csatlakozáshoz
- b) megengedi bárki csatlakozását egy magánhálózathoz

- c) biztonságos saját hozzáférést biztosít a hálózathoz
- d) kis földrajzi területen több összekötött számítógép együttese

1.15. Mi a tűzfal korlátja?

- a) fertőzött fájlokat helyez a karanténba
- b) nem értesít automatikusan a hálózati behatoláskor
- c) csökkenti a rosszindulatú programkódok hálózatban való megjelenésének lehetőségét
- d) nem lehet létrehozni további szabályokat a bejövő hálózati forgalom kezelésére





1.16. Mi a WPA?

- a) Wired Protected Access
- b) Wi-Fi Protected Access
- c) Wired Prevention Access
- d) Wi-Fi Password Access

1.17. Mit kell figyelembe venni nem védett drótnélküli hálózat használatakor?

- a) a hálózati tűzfalat ki kell kapcsolni
- b) a sütiket frissíteni kell
- c) az adatokhoz hozzá akarnak férni mások is
- d) az egyszer használatos jelszó ki lesz kapcsolva

1.18. Melyik a védett drótnélküli hálózat ikonja?

- a) 
- b) 
- c) 
- d) 

1.19. Melyik számít jó jelszónak?




- a) jBloggs_12091980
- b) 12092010
- c) jb
- d) jenniferBloggs

1.20. Mi azonosítja a biztonságos web-oldalakat?

- a) .org
- b) .com
- c) https
- d) http

1.21. Melyik ikon jelzi a biztonságos web-oldalt?

- a) 

- b) 
- c) 
- d) 

- 1.22. Melyik támadás irányítja át a web-oldal forgalmát egy hamisított web-oldalra?
- a) crackelés
 - b) eltérítéssel adathalászat
 - c) etikus hackelés
 - d) információ-szerzés
- 1.23. Melyik a böngészők által a számítógépen tárolt apró szöveg?
- a) tűzfal
 - b) trójai program
 - c) rendszerszinten rejtőző kártékony kód
 - d) süti
- 1.24. Mitől kell tartanunk a közösségi média használatakor?
- a) biometria
 - b) etikus hackelés
 - c) internetes zaklatás
 - d) titkosított fájlok
- 1.25. Mi biztosítja azt, hogy csak a címzettek olvashassanak el egy elektronikus levelet?
- a) az elektronikus levél aláírással való ellátása
 - b) az elektronikus levél titkosítása
 - c) egyszerű szöveges elektronikus levél formázása
 - d) definíciós fájl hozzáadása az elektronikus levélhez
- 1.26. Mi használ bejegyzett cégneveket személyes biztonsági adatok megszerzéséhez?
- a) adathalászat
 - b) figyelés
 - c) billentyűzet-leütés naplózás
 - d) zombi-hálózati szoftver
- 1.27. Mi a valós idejű szöveges kommunikáció két vagy több személy között?
- a) elektronikus levél
 - b) fájl-megosztás
 - c) eltérítéssel adathalászat
 - d) azonnali üzenetküldés
- 1.28. Mi segít biztosítani a bizalmasságot az azonnali üzenetküldés során?
- a) a tűzfal bekapcsolása
 - b) a tűzfal kikapcsolása

- c) a fájl-megosztás korlátozása
- d) titkosítás használata

1.29. Mi használható az eszközök fizikai biztonságának növelésére?

- a) vírusirtó szoftver
- b) titkosított szöveges dokumentumok
- c) biztonsági kábel
- d) elektromagnetikus törlés

1.30. Melyik módszer törli visszaállíthatatlanul az adatokat?

- a) az adatok Lomtárba mozgatása
- b) az adatokat tartalmazó lemez bedarálása
- c) jelszavas tömörítés alkalmazása
- d) adatok titkosított merevlemezre való elhelyezése

2. Nyissa meg a vizsgaközpont által megadott mappában található **biztonsag.doc** fájlt! Tegye megnyitás-védetté a fájlt, a **guard** jelszó használatával! Mentse el és zárja be a **biztonsag** fájlt! [1 pont]

3. Készítsen biztonsági mentést a vizsgaközpont által megadott mappában található **promocio.ppt** fájlról az **aprilisi_mentes** könyvtárba! [1 pont]

Mentsen el és zárjon be minden megnyitott fájlt és alkalmazást.