**1 KTS ypatumai**

**1**. Koks yra tinklų saugos tikslas?

**Tinklų saugos tiklas užtikrinti informacijos perdavimo saugumą.**

Apsaugoti tinklus, įskaitant įrangą, serverius, turinį ir aplikacijas nuo atakų su intencija užtikrinti duomenų ir sistemų pateikiamumą, konfidencialumą ir vientisumą.

**2**. Koks yra saugaus tinklo apibrėžimas?

**– paprasčiausias tinklas, kuris savo dizainu ir funkcijomis apsaugo tuo tinklu prieinamas informacines vertybes nuo išorinių ir vidinių grėsmių.**

**3**. Ko reikia norint efektyviai sukurti saugią infrastruktūrą?

**Reikalinga analizė ir planavimas saugumo politikos ir procedūrų rengimo metu, o taip pat panaudoti saugumą užtikrinančius produktus.**

**4**. Kokia eilės tvarka atliekamas tinklo saugumo užtikrinimas pagal Cisco kompanijos pasiūlytą koncepciją "Security wheel".

**a) saugant tinklą,   
b) stebint tinklą.   
c) testuojant tinklą,   
d) diegiant naujas priemones.**

**5**. Kokios yra saugaus tinklo charakteristikos?

a) Konfidencialumas (*Confidentiality*)

b) Vientisumas (*Integrity)*

c) Prieinamumas (*Availability*)

d) Apskaitomumas (*Accountability)*

e) Patikrinamumas (*Auditability*)

**6**. Kokie yra šiuolaikinio Interneto teikiami privalumai?

Bendravimas ir duomenų apsikeitimas didele Sparta. Pigūs kaštai.

* Internetas yra naudingas, dėl mažesnės duomenų perdavimo kainos (dideliais atstumais), nei naudojant duomenų perdavimo skirtinę liniją ar tradicinės telefonijos kanalus, nes kitais tinklais (mobiliojo, palydovinio ar tradicinės telefonijos) perduodant duomenis kaina yra žymiai didesnė.
* Internetas yra naudingas, dėl galimybių suteikimo plataus mąsto elektroninėms paslaugoms naudoti.
* Internetu galima perduoti įvairialypę informaciją (tekstinę, garsinę ir vaizdinę).
* Prie informacijos galima prieiti kiekvieną dieną bet kuriuo paros laiku.

**7**. Kokias rizikas gali patirti vartotojai dėl Internetinių sistemų naudojimo?

Teisingas atsakymas yra: Kompiuterių sistemų ar duomenų bazių neveikimas (angl. non-availability)., Duomenų praradimas., Konfidencialios informacijos perėmimas., Nukentėjimas nuo diversijų (pvz., panaudojus kenkėjišką programinę įrangą)., Nukentėjimas nuo klastojimo (pvz., IP, DNS, el.pašto adresų)., Neautorizuotas priėjimas prie duomenų bazių.

**8**. Kokios yra sisteminės Interneto saugos problemos?

Teisingas atsakymas yra:

* Internetas buvo sukurtas vykdant tyrimų projektą, turinčių tarpusavyje pasitikėjimą, mažos ir uždaros bendruomenės narių komunikavimui.,
* Kuriant Interneto protokolus saugumas buvo neįvertinimas (pvz., dažnai pasitaikanti RFC dok. citata yra "šiame dok. saugumo klausimai yra nenagrinėjami").,
* Internetas nėra centralizuotai kontroliuojamas, nes nėra vienintelės administravimo institucijos, taip pat Interneto negali kontroliuoti nei vienos valstybės valdžios institucija.

**9**. Kokios Interneto savybės yra patraukliausios įsilaužėliams?

Teisingas atsakymas yra: Milijonai sistemų su prisijungimo galilmybėmis., Tūkstančiai tinkle sujungtų tarpusavyje., Didelis skaičius klaidų sistemų programinėse įrangose

a) Milijonai sistemų, prie kurių galima prisijungti. Norint tai padaryti, tereikia Kodėl neužtenka tik įdiegti ugniasienę, kodėl reikalingas jo palaikymas? suvesti prisijungimo duomenis.   
b) Tūkstančiai tarpusavyje sujungtų tinklų (kiekvienos organizacijos tinklas yra prijungtas prie interneto).   
c) Daug klaidų sistemų programinėse įrangose. Nepaisydami to programinės įrangos gamintojai pirmąsias savo produktų versijas dažnai stengiasi parduoti ir tik po kurio laiko pasiūlo atnaujintas versijas su ištaisytomis klaidomis.   
d) Daug sistemų su saugumo spragomis.   
e) Interneto vartotojai lengvai prieina prie įsilaužti ir atakuoti naudojamų įrankių.   
f) Įsilaužimui ir atakoms skirtų įrankių naudojimas yra paprastas ir pakankamai lengvai suprantamas.

**10**. Kokios sąlygos yra palankios įsilaužėliams?

Teisingas atsakymas yra: Atakos pasinaudojant Internetu yra lengvai įvykdomos, mažai rizikuojama ir sunkiai susekamos., Įsilaužėlių įrankiai funkcionalūs, sudaro galimybes vykdyti didelio mąsto atakas, lengvai panaudojami naujokų., Interneto protokolų ir aplikacijų sudėtingumas ir kompleksiškumas auga priklausomai nuo šiandieninių poreikių IT-sistemoms.

**11**. Į kokias kategorijas galima klasifikuoti įsilaužėlius?

Teisingas atsakymas yra:

a) Iš savų žmonių rato   
b) Įsilaužėliai paaugliai.   
c) Kriminaliniai nusikaltėliai.   
d) Industriniai šnipai.   
e) Užsienio valstybių žvalgai

F) Kompiuterių specialistai

**12**. Kokios yra palankios galimybės įsilaužimams Internete?

Teisingas atsakymas yra: Skubus kompiuterių ir tinklų technologijų įsisavinimas., Elektroninių paslaugų teikimo poreikis Internete sparčiai auga., Tūkstančiai eksploatuojamų pažeidžiamumų., Trūksta žinių informacijos saugos srityje., Informacijos saugos srities personalo trūkumas., Įgyvendinamų įstatymų trūkumas.

a) Skubus kompiuterių ir tinklų įsisavinimas.   
b) Elektroninių paslaugų teikimo poreikis internete sparčiai auga   
c) Tūkstančiai eksploatuojamų saugumo spragų  
d) Trūksta žinių informacijos saugos srityje.   
e) Informacijos saugos personalo trūkumas   
f) Įgyvendinamų įstatymų trūkumas  
g) tarptautinis tinklas  
h) 99% įsilaužimų įvykdoma panaudojant jeu žinomas spragas

**13**. Kokios tendencijos yra interneto saugos srityje?

Teisingas atsakymas yra:

Interneto vartotojų skaičius auga.,

Įsibrovėlių kvalifikacija ir darbo efektyvumas auga.,

Auga įsilaužimo įrankių funkcionalumas.,

Auga įsilaužimų skaičius,

Protokolai ir aplikacijos sudėtingėja.,

Sudėtingėja interneto tinklas.,

Informacinių sistemų ir tinklų infrastruktūroje esančios fundamentalios saugos problemos negali būti greitai išspręstos.,

Saugumo incidentų tyrimų grupių kiekis auga, tačiau rodiklis įvertinant interneto vartotojų kiekį mažėja.,

Gamintojai tęsia programinės įrangos gamybą su pažeidžiamumais.

**14**. Kokios paslaugos sukūrimas 1993 metais įtakojo spartaus interneto vartotojų skaičiaus augimo pradžią?

**WWW paslauga su "NCSA Mosaic" naršykle.**

**15**. Į kokias tris dideles grupes gali būti išskirtos rizikos?

**Vidinis tiekėjas, išorinis tiekėjas, vartotojas**

Rizikos neprijungtoms nei prie interneto nei prie vidinio įmonės tinklo kompiuterinėms sistemoms

Rizikos kompiuterinėms sistemoms prijungtoms prie įmonės tinklo

Rizikos kompiuterinėms sistemoms prijungtoms prie interneto tinklo

**16**. Kokių organizacijų interneto svetainėse pateikiama informacija apie tinklinių kompiuterių (angl. hosts) skaičių internete?

Teisingas atsakymas yra: RIPE (Réseaux IP Européens)., ISC (angl. Internet Systems Consortium, Inc.).

**17**. Kokių organizacijų interneto svetainėse pateikiama informacija apie incidentų ir pažeidžiamumų skaičių?

**Tarptautinė „Anti-Phishing“ darbo grupė ir CSI/FBI (Federal Bureau of Investigation)**

CERT (Computer Emergency Response Team)

**18**. Kokių organizacijų interneto svetainėse pateikiama informacija apie kompiuterinių nusikaltimų skaičių, nukentėjusių įmonių skaičių ir jų patirtus finansinius nuostolius?

**c. CERT (angl. Computer Emergency Response Team).**

**d. FBI (angl. Federal Bureau of Investigation).**

**19**. Kuris iš šių apibrėžimų atitinka kirmino (angl. worm) apibrėžimą?

Teisingas atsakymas yra: Tai programa arba algoritmas, kuris dauginasi ir plinta tinklais, dažniausiai atlieka nepageidaujamą poveikį.

**20**. Kuris iš šių apibrėžimų atitinka Trojan horse (angl. Trojos arklys) apibrėžimą?

Trojos arklys (Trojan Horse) – tai destruktyvi ir nesidauginanti programa, kuri dažnai yra

užmaskuota kaip atliekanti naudingas funkcijas.

Tai destruktyvi ir nesidauginanti programa, kuri dažnai yra užmaskuota kaip atliekanti naudingas funkcijas. Veikianti trojos arklio programa yra ypatingai pavojinga, nes sudaro virtualų koridorių, per kurį užkrėstasis kompiuteris ir jo resursai tampa prieinami iš išorės

**21**. Kuris iš šių apibrėžimų geriau atitinka paslaugos išjungimo (angl. denial of service) atakos apibrėžimą?

Teisingas atsakymas yra: Kai kompiuteris, serveris ar kitas resursas prijungtas prie interneto užtvindomas tūkstančiais IP paketų vienu metu naudojant suklastotus siuntėjo IP adresus, tuo laikotarpiu kompiuteriai, serveriai ar kiti resursai tinklu tampa neprieinami.

**22**. Kuris iš šių apibrėžimų geriau atitinka suklastojimo (angl. spoofing) atakos apibrėžimą?

Teisingas atsakymas yra: Tai metodas naudojamas neautorizuotam priėjimui prie kompiuterio, serverio ar kito resurso, kai įsilaužėlis siunčia žinutę su suklastotu adresu ar kitokiu identifikatoriumi..

**23**. Kuris iš šių apibrėžimų geriau atitinka sudarkymo (angl. defacement) atakos apibrėžimą?

Sudarkymo (Defacement) ataka – tai internetinės svetainės išvaizdos pakeitimas, siekiant įspėti tos svetainės administratorius apie esančias saugumo spragas ir parodyti įsilaužėlio išmonę ir žinias.

**24**. Kuris iš šių apibrėžimų atitinka "phishing" (angl. password fishing) apibrėžimą?

Slaptažodžių „žvejojimo“ (Password Fishing) ataka – tai ataka, kurios metu bandoma išgauti prisijungimo prie sistemų slaptažodžius ar kitus konfidencialius duomenis, pasinaudojant nepageidaujamais elektroninio pašto laiškais (Spam) ar suklastotomis internetinėmis svetainėmis

.

**25**. Kokios rizikos gali atsirasti kompiuterinėse sistemose neprijungtoms nei prie interneto nei prie vidinio įmonės tinklo?

Teisingas atsakymas yra: Nepateikiamumas (sistemos neveikimas)., Duomenų praradimas, vagystė, piknaudžiavimas (pasinaudojimas duomenimis)., Žmogiškasis faktorius (dažnai nepageidaujamas).

**26**. Kokios rizikos gali atsirasti kompiuterinėse sistemose prijungtoms prie įmonės tinklo?

Teisingas atsakymas yra: Neautorizuota arba paprasta prieiga prie konfidencialios informacijos., Įmonės veiklos valdymo perkėlimas į elektroninę erdvę (pvz., popierinių dok. ir komunikacijas telefonu keičia dok. valdymo sistemos, elektroninės balso pašto sistemos).

**27**. Kokios rizikos gali atsirasti kompiuterinėse sistemose prijungtoms prie interneto tinklo?

Kompiuterinėms sistemoms, prijungtoms prie interneto tinklo, gali kilti šios grėsmės:

a) Duomenų praradimo.

b) Konfidencialios informacijos praradimo.

c) Kompiuterinių sistemų veiklos sutrikimo dėl paslaugų perpildymo, kenkėjiškų programų naudojimo.

d) Prestižo praradimo.

e) Tapatybės suklastojimo.

**28**. Kokios pagrindinės rizikos patiriamos siunčiant duomenis internetu?

Teisingas atsakymas yra: Žinučių suklastojimas., Adresų klastojimas., Internetinių parduotuvių ir bankininkystės apgaulė., Nelegalus ar abejotinas internetinis verslas., Duomenų apsaugos pažeidimai., Neapibrėžti internetinės erdvės įstatymai.

**29**. Kokios priemonės gali būti panaudotos norint panaikinti žinučių ir adresų klastojimo rizikas?

Teisingas atsakymas yra: Viešo rakto ir kitus kokybiškus kriptografinius metodus..

**30**. Kur yra silpniausia vieta apgaudinėjant vartotojus naudojančius internetines parduotuves ir bankininkystės sistemas?

Teisingas atsakymas yra: Nepakankamai yra prižiūrimi vartotojų kompiuteriai, kuriuose yra neapsaugotas priėjimas prie slaptažodžių, paslėptų programų veikla, kurios įvykdo nepageidaujamus pinigų pervedimus..

**31**. Dėl kokių sąlygų internete klesti nelegalus, abejotinas internetinis verslas ir kitokia kriminalinė veikla?

Teisingas atsakymas yra: Dėl didelio vartotojų skaičiaus pasiekiamumo., Dėl anonimiškumo išlaikymo

**Suklastotas internetinis verslas ir kitokia kriminalinė veikla internete klesti dėl didelio vartotojų skaičiaus ir jų anonimiškumo.**

Kiekvienoje valstybėje internetinės erdvės įstatymai skiriasi arba jų iš viso nėra. Sukčių, įsilaužėlių ir piktavalių abejotinai veiklai tirti reikalingas tarptautinis bendradarbiavimas.

**32**. Kokias galimybes turi interneto tiekėjas rinkti duomenis apie vartotojų duomenų persiuntimus, net kai naudojami saugaus perdavimo algoritmai?

**Interneto tiekėjas gali rinkti duomenis apie vartotojų duomenų persiuntimą, skaityti vartotojų elektroninius laiškus. Pašto serverį administruojantis interneto tiekėjas gali kontroliuoti duomenų siuntimą iš**

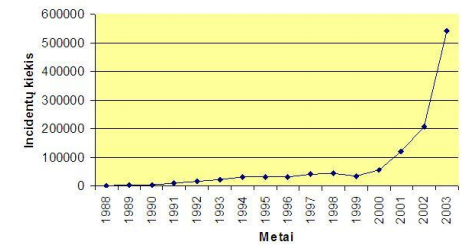
**internetinių svetainių net tada, kai naudojami saugaus perdavimo algoritmai.**

Pašto serverį administruojantis ISP gali kontroliuti duomenų siuntimą iš internetinių svetainių, net kai naudojami saugūs perdavimo algoritmai.

**33**. Kurie iš šių išvardintų punktų tinka šiuolaikinio Interneto apibūdinimui?

Šiuolaikinis internetas yra paplitęs visuose žemynuose ir juo naudojasi įvairių kultūrų žmonės. Jis turi užtikrinti informacijos perdavimo saugumą. Saugumas, tai:   
a) Konfidencialumas (Confidentiality) – informacija turi būti pateikta tik tam, kam priklauso, ir niekam kitam.   
b) Vientisumas (Integrity) – duomenys neiškraipyti nuo jų sukūrimo iki sunaikinimo.   
c) Prieinamumas (Availability) – tinklo išteklių pateikimas autorizuotiems vartotojams.   
d) Apskaitomumas (Accountability) – įrašų darymas apie bet kurio vartotojo veiksmą.   
e) Patikrinamumas (Auditability) – galimybės patikrinti saugumą audito metodais.

**34**. Kokia kreive galima atvaizduoti saugumo incidentų kitimą nuo 1983 iki 2003 m. pagal CERT org. surinktą statistiką?



**35**. Kuri iš žemiau apibūdintų atakų būtų paskirstyta paslaugų išjungimo (DDoS) ataka?

Teisingas atsakymas yra: Vienu ir tuo pačiu metu pakenkiama vienam pvz,. kompiuteriui, sistemai ir t.t., naudojant daugelį atakavimo šaltinių.

**Paskirstyta paslaugos blokavimo (DDoS) ataka – tai ataka, kai vienu metu pakenkiama tik vienam objektui (pvz., kompiuteriui, sistemai ir t. t.) naudojant daugelį atakavimo šaltinių.**

Vienu ir tuo pačiu metu pakenkiama vienam pvz,. kompiuteriui, sistemai ir t.t., naudojant daugelį atakavimo šaltinių apibūdintų atakų būtų paskirstyta paslaugų blokavimo (DDoS) ataka.

**36**. Kaip vadinama saugaus tinklo charakteristika, kai naudojant atitinkamus saugumo ir audito metodus galima patikrinti kokia yra tinklo saugumo kontrolė.

Patikrinamumas (Auditability)

**37**. Kaip vadinama saugaus tinklo charakteristika, kai užtikrinama, kad sukuriamas įrašas apie kiekvieną atliktą veiksmą su bet kuriuo vartotoju, sistema ar tinklu.

Apskaitomumas (*Accountability*)

**38**. Kaip vadinama saugaus tinklo charakteristika, kai užtikrinama, kad tinklo resursai autorizuotų vartotojų yra pasiekiami.

Teisingas atsakymas yra: Pateikiamumas (angl. availability).

**39**. Kaip vadinama saugaus tinklo charakteristika, kai užtikrinama, kad duomenys yra tikslūs (neiškraipyti) nuo sukūrimo iki sunaikinimo juos naudojant, persiunčiant ir saugojant.

Vientisumas (*Integrity*)

**40**. Kaip vadinama saugaus tinklo charakteristika, kai garantuojama, kad informacija pateikiama tik tam kuriam priklauso tą informacija naudotis ir niekam kitam.

Teisingas atsakymas yra: Konfidencialumas (angl. confidentiality)..

**41**. Kurie iš išvardintų variantų yra teisingi? a)Tinklų sauga nėra ... b) Tinklų sauga yra …

V1:

Teisingas atsakymas yra: Tinklų sauga nėra ugniasienės įdiegimas., Tinklų sauga nėra tik specialus technologinis sprendimas

V2:

Teisingas atsakymas yra: Tinklų sauga nėra tik bitų ir baitų sauga (pvz. Šifravimas). Tinklų sauga nėra tik produktas arba specialios programinės įrangos įdiegimas

**42**. Kokios priemonės naudojamos tradicinei tinklų apsaugai nuo atakų?

**Tinklo saugumas užtikrinamas nuolat atliekant tokius veiksmus:**

**a) saugant tinklą,**

**b) stebint tinklą.**

**c) testuojant tinklą,**

**d) diegiant naujas priemones.**

* Užkardos
* Maršrutų parinktuvai su prieigos sąrašais
* Įsilaužimo aptikimo sistemos

**43**. Nuo kokių grėsmių yra saugomos informacinės vertybės esančios saugiame tinkle?

**Atskleidimo grėsmė** yra informacijos pateikimas ne tam asmeniui, kuriam ji skirta. Ši grėsmė kyla kiekvieną kartą, kai bandoma neteisėtai pasinaudoti kokia nors konfidencialia informacija, saugoma kompiuterių sistemoje ar perduodama iš vienos sistemos į kitą.   
**Vientisumo pažeidimo grėsmė** yra bet koks neplanuotas saugomų ar perduodamų duomenų keitimas (modifikacija ar trynimas). Manoma, kad vientisumo grėsmė dažniausiai kyla komercinėms struktūroms, o atskleidimo – valstybinėms.   
**Atsisakymo aptarnauti arba atsisakymo grėsmė** kyla kiekvieną kartą, kai tam tikrais veiksmais blokuojamas priėjimas prie kokios nors kompiuterių sistemos informacijos. Kad draudžiama informacija nebūtų pasiekiama, ji blokuojama gali būti nuolatos. Visuotinėse kompiuterių sistemose dažniausiai pasitaiko atsisakymo aptarnauti, o vietinėse – atskleidimo ir vientisumo pažeidimo grėsmių.

1 Atskleidimo grėsme

2 Vientisumo pažeidimo grėsmė

3 Atsisakymo aptarnauti grėsmė

**44**. Kuris iš šių apibrėžimų atitinka viruso (angl. viruse) apibrėžimą?

Teisingas atsakymas yra: Be vartotojo žinios į kompiuterį įdiegta programa ar programos kodo dalis, kuri vykdo destrukcinius ir dauginimosi veiksmus..

**45**. Kuris iš šių apibrėžimų geriau atitinka mobiliojo viruso apibrėžimą?

Teisingas atsakymas yra: Tai kenkėjiškas programinis kodas plintantis judriojo telefono ryšio tinklais, kurie pažeidžia judriojo ryšio vartotojų įrenginių programinę įrangą.

**2 KTS problemos**

**1**. Kokie slaptažodžiai yra lengvai atspėjami?

Teisingas atsakymas yra: Tie, kurių sandara yra labai paprasta..

Gali būti naudojami žinomi arba dažniausiai pasitaikantys, populiariausi prieigos kodai, pvz.: administrator, guest, field, service ir pan. bei atitinkamų slaptažodžių spėjimai, taip pat žodžiai iš žodynų.  
Pvz.: field/service; guest/guest; admin/admin

**2**. Išvardinkite kokie yra slaptažodžio perėmimo metodai.

Teisingas atsakymas yra: Slaptažodžių atspėjimas., Slaptažodžių nuskaitymas iš paketų (angl. sniffing)., Slaptažodžių įveikimas (angl. cracking)., Slaptažodžių monitoringas., Slaptažodžių žvejojimas.

**3**. Kokios sąlygos reikalingos įsilaužėliui vykdančiam slaptažodžių nuskaitymą iš paketų?

Slaptažodžių nuskaitymas iš paketų – dar vadinamas slaptažodžių šniukštinėjimu – yra būdas, leidžiantis aptikti slaptažodžius ir vartotojo identifikatorius nuskaitant ir analizuojant duomenų paketus vietiniuose tinkluose IP protokolo lygmenyje. Šniukštinėjimo įrankiai lengvai randami internete arba pateikiami kartu su operacinėmis sistemomis kaip protokolų analizės įrankiai. Įsilaužėliai šiuos įrankius gali panaudoti dvejopai: šniukštinėjimo programą piktavališkai įkelti į nusitaikytą sistemą arba ją paleisti įsilaužėlio valdomame tinklo mazge, turint tikslą aptikti vartotojo prisijungimo duomenis (2.3.3 pav.). Automatinė prisijungimo duomenų aptikimo procedūra vykdoma įjungus filtro arba trigerio funkciją ieškojimo paketuose Login, Password ir kt

**4**. Kokios sąlygos reikalingos įsilaužėliui vykdančiam slaptažodžių įveikimo ataką?

Teisingas atsakymas yra: Įsilaužėlio valdomas tinklo įrenginys su galimybę nuskaityti kiekvieno paketo turinį., Vartotojų srautai keliautų pro įsilaužėlio tinklo įrenginį.

**5**. Kurie iš šių apibūdinimų yra teisingi slaptažodžio "žvejojimo" programos veikimo principui aprašyti?

Teisingas atsakymas yra: "Žvejojimo" programa parodo vartotojo prisijungimo duomenims suvesti langą, tokį patį kaip operacinės sistemos., Suvesti slaptažodžiai yra siunčiami įsilaužėliui.

**6**. Kokios sąlygos reikalingos norint vykdyti buferio perpildymo ataką?

Teisingas atsakymas yra: Sėkmingai atrasti, kad programos turi buferio perpildymo spragas., Turi būti priėjimas per tinklą., Buferi nekontroliuoja įrašomų duomenų ilgio.

**7**. Kas gali atsitikti jei priimamų duomenų dydis yra per didelis, kai nekontroliuojamas įrašomų į buferį duomenų ilgis?

Teisingas atsakymas yra: Gali būti perpildytas nutolusio tinklo elemento steko buferis., Perpildžius buferį gali būti sugadinti kituose atminties regionuose esantys duomenys..

**8**. Kokios galimos grėsmės dirbant su tinklo įrenginio valdymo programa, įvedus nepatikrintą sintaksę?

Atsiranda buferio perpildymo galimybė. Įsilaužėliai pasinaudoja paliktomis spragomis, įveda į programas specialiuosius simbolius ir taip paveikia programas ar operacines sistemas ir jų darbą.   
Dėl šios priežasties pasitaiko tinklo paslaugų teikimo sutrikimų, stringa įrenginio valdymo programos, ypač jei į įrenginio valdymo programą, su kuria dirba administratoriaus, įvedama nepatikrinta sintaksė. Administratoriaus kompiuterio operacinė sistema taip pat gali strigti dėl nepatikrintos sintaksės, tačiau tai neturi poveikio tinklo įrenginiams ir jais teikiamų paslaugų veikimui.

**9**. Dėl kokių priežasčių yra galimos trumpalaikės įsilaužimo sąlygos?

Teisingas atsakymas yra: **Dėl neteisingai sukurtos programinės įrangos.**

**10**. Kokiais būdais, už tinklų administravimą atsakingi darbuotojai, neapgalvoję gali sukelti saugos pažeidimo situacijas?

*(Vadovėlis: 2.3.8.* **Žinių trūkumas ir neatsargumas***, p. 80)*

a) Neteisingai sukonfigūruoti tinklo infrastruktūros įrenginiai, nepakankamas arba iš viso nėra apribojimų prie tinklo prieigos arba pačių tinklų.

b) Instaliavus tinklo įrenginius ar sistemas, naudojama standartinė gamintojo konfigūracija, t.y. neatliekami parametrų derinimo darbai: nepakeičiami standartiniai prisijungimo vardai, standartiniai slaptažodžiai, duomenų perdavimas be šifravimo, neišjungiamos nenaudojamos paslaugos ar funkcijos, kurios gali tapti saugumo spragomis ir kelti grėsmę.

c) Neatsargiai naudojamos senos programinės įrangos versijos su žinomomis saugumo spragomis.

**11**. Kokie sprendimai turi būti priimti įmonėje, kad įmonėje nekiltų grėsmės dėl darbuotojų žinių trūkumo ar neatsargumo?

*(Vadovėlis: 2.3.8.* **Žinių trūkumas ir neatsargumas***, p. 81)*



**12**. Kokie yra socialinio įsibrovimo būdai?

Teisingas atsakymas yra: Įtikinti administratorių, kad be priežiūros paliktų administravimo teisėmis prijungtą sistemą., Šnipinėti įmonės tinklo infrastruktūrą apsimetinėjant darbuotoju išgalvotos paslaugos arba vartotoju.

**13**. Kokios priežastys įmonėje lemia žemą saugumo standartų lygio egzistavimą?

(Vadovėlis: 2.3.10. **Nepasiruošusios įmonės (Defective Organizations)**, p. 81)  
a) nepakankamas kvalifikuotų IT saugos specialistų kiekis;   
b) nepakankami IT personalo mokymai;   
**c)** neįdiegta arba įdiegta nepakankamos kokybės saugumo politika.

**14**. Kokiais požymiais virusų programos skiriasi nuo įprastinių programų?

(Vadovėlis: 2.3.11. **Virusai, Trojos arkliai ir nepageidaujamos žinutės**, p. 81)  
Nuo įprastų programų skiriasi tuo, kad įdiegiamos į sistemą be vartotojo žinios arba apgaulės būdu. Jos yra piktavalės ir sugeba pačios plisti.

**15**. Kokią žalą kelia tinklams nepageidaujamų žinučių siuntnėjimas?

Teisingas atsakymas yra: Sumažina bendrąjį tinkle pralaidumą., Apkrauna tinkle Paslaugų teikiančias sistemas., Reikia papildomų investicijų sistemoms kovojančioms su nepageidaujamų žinučių siuntimu

(Vadovėlis: 2.3.11. **Virusai, Trojos arkliai ir nepageidaujamos žinutės**, p. 81)  
Nepageidaujamų žinučių siuntinėjimas mažina bendrąjį tinklo pralaidumą ir apkrauna tinklų paslaugas teikiančias sistemas.

**16**. Kokios sąlygos reikalingos norint žinutę perimti, sufalsifikuoti jos turinį ir pakeisti siuntėjo adresą?

Teisingas atsakymas yra: Vartotojų žinutės turi keliauti pro įsilaužėlio valdomą tinklo įrenginį (pvz.,maršrutizatorių, pašto serverį) kuris turi galimybę nuskaityti kiekvieno paketo turinį., Vartotojų žinutės turi būti neužšifruotos.

**17**. Kokie variantai galimi norint periimti prisijungimo, bei kitus duomenis, naudojantis internetinės bankininkystės ir prekybos sistemomis, kai duomenų srautas yra užšifruotas?

(Vadovėlis: 2.1.6. **Pagrindinės grėsmės, kylančios naudojantis internetu**, p. 65)  
Nepakankama kompiuterių priežiūra. Juose gali būti neapsaugotas priėjimas prie slaptažodžių, veikti paslėptos programos, kurios atliks nepageidaujamą pinigų pavedimą.  
Kitas variantas yra „phishing“, kai vartotojas dėl vienokių ar kitokių priežasčių (pradingo prisijungimo duomenys ir pan.) prašomas atsiųsti savo prisijungimo duomenis.

**18**. Kaip žiniatinklio paslaugų teikėjai pažeidžia vartotojų duomenų apsaugos teises?

(Vadovėlis: 2.1.6. **Pagrindinės grėsmės, kylančios naudojantis internetu**, p. 65)  
Interneto tiekėjas gali rinkti duomenis apie vartotojų duomenų persiuntimą, skaityti vartotojų elektroninius laiškus. Pašto serverį administruojantis interneto tiekėjas gali kontroliuoti duomenų siuntimą iš internetinių svetainių net tada, kai naudojami saugaus perdavimo algoritmai.

**19**. Kiek toli galima nusiusti ICMP užklausos (ECHO request) žinutę, kai įrenginio su tokiu IP adresu iš viso nėra?

Tikslaus atsakymo neradau. Išbandžiau per CMD tracert su IP 1.1.1.1, tai paketas nuėjo iki mano ISP gateway ir viskas. Jei kas nors žino tikslų atsakymą, parašykit.

Manau: Iki įrenginio tinklo maršrutizatoriaus (Kadangi jis jau žinos apie tinkle esančius IP?)

**20**. Kokius parametrus skeneryje turi užduoti šnipas, norint pradėti skenavimą?

Teisingas atsakymas yra: Konkrečius IP adresų rėžius..

**21**. Kokį tinklo lygmens protokolą naudoja tarpinių mazgų skeneris?

Teisingas atsakymas yra: ICMP

**22**. Koks atsakymo žinutės pavadinimas, kai prievadai atidaryti, naudojant TCP SYN skenavimo metodą?

Teisingas atsakymas yra: SYN ACK

Jeigu atliekant TCP SYN skenavimą prievadai bus atviri, jie atsakys siųsdami SYN.ACK paketą.



**23**. Kaip skiriasi žinučių siuntimas, kai prie vadai uždaryti, tarp naudojamų TCP SYN ir TCP connect () skenavimo metodų?

Skenavimas šiuo metodu panašus į TCP SYN, bet skenuotojas, gavęs atsaką SYN.ACK, pats pirmiau nusiunčia ACK, o tada RST vėliavėlę, taip nutraukdamas susijungimą.



Teisingas atsakymas yra: Nesiskiria..

**24**. Kokia situacija su portais, jei naudojant TCP FIN skenavimo metodą, gaunamas žinutės atsakymas RST?

**b. Prievadai uždari.**

**25**. Kodėl UDP skenavimo metodas yra sudėtingesnis už TCP skenavimo metodus?

Teisingas atsakymas yra: Nes UDP protokolas nenumato siųsti atsakymo žinutes..

**26**. Kokią informaciją galima išgauti naudojant protokolų analizatorių?

*(Vadovėlis: 2.3.12.* **Tinklo infrastruktūros šnipinėjimas***, p. 81)*

Protokolų analizatoriai įrašo visus tinklu siunčiamus paketus ir ieško, kokios paslaugos veikia, taip pat nustato vartotojų vardus ir slaptažodžius.

**27**. Kokia nepageidaujama informacija persiunčiama reklamjuostės tekste?

Teisingas atsakymas yra: Įrenginio arba operacinės sistemos pavadinimas, versija..

savo programos ar OS (operacinės sistemos) versija, gamintojas ir kitokias detales

**28**. Kodėl naudojant "fingerprint" metodą ir siunčiant tokias pačias užklausas į skirtingas sistemas gaunami skirtingi atsakymai?

Teisingas atsakymas yra: Todėl, kad užklausos nėra standartinės

Nes kiekvienos sistemos veikimo principas kitoks (naudoja skirtingą programinę įrangą,atidaryti skirtingi servisai tinkle, skirtingai siunčia paketus)

**29**. Kokios rizikos gali atsirasti kompiuterinėse sistemose neprijungtoms nei prie interneto nei prie vidinio įmonės tinklo?

Teisingas atsakymas yra: Nepateikiamumas (sistemos neveikimas)., Duomenų praradimas, vagystė, piknaudžiavimas (pasinaudojimas duomenimis)., Žmogiškasis faktorius (dažnai nepageidaujamas).

**30**. Kokios rizikos gali atsirasti kompiuterinėse sistemose prijungtoms prie interneto tinklo?

Teisingas atsakymas yra: Duomenų praradimas (įterpimas, ištrynimas, falsifikacija)., Konfidencialios informacijos praradimas., Kompiuterinių sistemų darbo strigimas: paslaugų perpildymas; malware., Prestižo praradimas visuomenėje., Tapatybės suklastojimas.

**31**. Kokios rizikos gali atsirasti kompiuterinėse sistemose prijungtoms prie įmonės tinklo?

Teisingas atsakymas yra: Neautorizuota arba paprasta prieiga prie konfidencialios informacijos., Įmonės veiklos valdymo perkėlimas į elektroninę erdvę (pvz., popierinių dok. ir komunikacijas telefonu keičia dok. valdymo sistemos, elektroninės balso pašto sistemos).

**32**. Kokios yra rizikos įvertinimo fazės?

Teisingas atsakymas yra:

* Analizės srities užfiksavimas ir sąsajų nustatymas tarp sričių.
* Rizikų įsisavinimas (angl. Acquisition) atliekant scenarijaus anaalizę arba imituojant.
* Rizikų įvertinimas naudojant metodus
* Rezultatų interpretavimas

**33**. Koks yra kardinalaus rizikos įvertinimo metodo apibrėžimas?

Teisingas atsakymas yra: Kiekvieno saugos incidento financinė žala yra dauginama iš pasikartojimo tikimybės per metu.

**34**. Koks yra ordinalaus rizikos įvertinimo metodo apibrėžimas?

Teisingas atsakymas yra: Informacinės sistemos fragmentuojamos į objektus ir rizikos vertinamos kategorijomis nuo labai neįtikėtinų iki labai tikėtinų.

**35**. Kokie yra rizikos matricos pagrindiniai parametrai?

Teisingas atsakymas yra: žalos apimtis., įvykio pasikartojimo tikimybė.

**36**. Kiek prioritetų lygių naudojama rizikų įvertinimo diagramoje?

Teisingas atsakymas yra: 3..

**37**. Kokius grėsmių šaltinius žmogus gali valdyti ir kontroliuoti?

Teisingas atsakymas yra: Organizaciniai trūkumai., Techniniai gedimai., Tyčiniai veiksmai., Žmogiškas faktorius.

**38**. Kuris iš išvardintų teiginių apibrėžia saugumo spragas, kurioms yra žinomos saugumo priemonės, tačiau netaikomos?

Tradicinė rizikos analizė apima galimos rizikos bendrovei analizę, pateisinant atsakomąsias   
priemones. Ji yra būtinas saugos politikos plėtros elementas, nes telkiasi ties tam tikrų prioritetų saugos politika. Deja, tradicinė rizikos analizė dažnai nepastebi daugelio galimų pavojų kategorijų, nes ji didžiausią dėmesį skiria atakos rezultatui arba tikslui.   
Pavyzdžiui, atliekant tradicinę rizikos analizę paprastai teigiama, kad neteisėtai įsilaužėlio perimta klientų informacija sukelią riziką ir, norint ją sumažinti, reikia užblokuoti klientų duomenų bazę. Tokia analizė vadinama „iš apačios į viršų“ ir pradedama nuo įsibrovėlio tikslo. Po to nustatoma, kokių reikia imtis atsakomųjų priemonių.

**39**. Kokia iš išvardintų kombinacijų geriausiai apibrėžia IT saugos sryties riziką?

Rizikos samas klausimas, ką gali padaryti įsilaužėlis, pasinaudodamas saugumo spragomis, padedančiomis pasiekti piktavališką tikslą. Tokia rizikos analizė patraukli ir tuo, kad gali būti atlikta tiek prieš įdiegiant saugos sistemas, tiek jas įdiegus.

**40**. Kokia priežastis lemia buferio persipildymą?

Teisingas atsakymas yra: Dėl to, kad į buferį įrašomų duomenų ilgis viršija leistiną..

**41**. Kuris iš pateiktų teiginių aprašo tinklo šniukštinėjimą (angl. Sniffing)?

Teisingas atsakymas yra: Šniukštinėjant tinkle galima matyti duomenis siunčiamus paketų viduje

Ataka, atliekama panaudojant programas, kurios stebi tinklais perduodamus duomenis. Slaptažodžių nuskaitymas iš paketų.

**42**. Kokie yra du pagrindiniai rizikos analizės metodai?

Kardinalus ir ordinarus.

**43**. Kokios atakos veikimas pagrįstas identiškų el. laiškų daugkartiniu siuntimu atitinkamu gavėjo adresu?

Teisingas atsakymas yra: Nepageidaujamų žinučių siuntimas (angl. spamming)..

**44**. Kuri iš išvardintų atakų yra galima, atlikus operacinės sistemos buferio perpildymą?

paslaugos išjungimo atakos (DoS)

**45**. Kokiais būdais, už tinklų administravimą atsakingi darbuotojai, neapgalvoję gali sukelti saugos pažeidimo situacijas?

(Vadovėlis: 2.3.8. **Žinių trūkumas ir neatsargumas**, p. 80)  
a) Neteisingai sukonfigūruoti tinklo infrastruktūros įrenginiai, nepakankamas arba iš viso nėra apribojimų prie tinklo prieigos arba pačių tinklų.   
b) Instaliavus tinklo įrenginius ar sistemas, naudojama standartinė gamintojo konfigūracija, t.y. neatliekami parametrų derinimo darbai: nepakeičiami standartiniai prisijungimo vardai, standartiniai slaptažodžiai, duomenų perdavimas be šifravimo, neišjungiamos nenaudojamos paslaugos ar funkcijos, kurios gali tapti saugumo spragomis ir kelti grėsmę.   
c) Neatsargiai naudojamos senos programinės įrangos versijos su žinomomis saugumo spragomis.

**46**. Kokie yra socialinio įsibrovimo būdai?

(Vadovėlis: ***2.3.9. Socialinis įsibrovimas (Social Hacking)***, p. 81)  
a) Skatinti administravimo paslaugas turint tikslą įgauti pasitikėjimą ir prieiti prie reikiamos informacijos.   
b) Įtikinti administratorių, kad be priežiūros paliktų administravimo teisėmis prijungtą sistemą.   
c) Įtikinti administratorių įvykdyti savo funkcijas prie slaptažodžiams išgauti paruošto kompiuterio.   
d) Šnipinėti įmonės tinklo infrastruktūrą apsimetant išgalvotą paslaugą teikiančiu darbuotoju arba vartotoju.

**47**. Kokios priežastys įmonėje lemia žemą saugumo standartų lygio egzistavimą?

a) nepakankamas kvalifikuotų IT saugos specialistų kiekis;

b) nepakankami IT personalo mokymai;

**c)** neįdiegta arba įdiegta nepakankamos kokybės saugumo politika.

**48**. Kaip žiniatinklio paslaugų teikėjai pažeidžia vartotojų duomenų apsaugos teises?

(Vadovėlis: 2.1.6. **Pagrindinės grėsmės, kylančios naudojantis internetu**, p. 65)  
Interneto tiekėjas gali rinkti duomenis apie vartotojų duomenų persiuntimą, skaityti vartotojų elektroninius laiškus. Pašto serverį administruojantis interneto tiekėjas gali kontroliuoti duomenų siuntimą iš internetinių svetainių net tada, kai naudojami saugaus perdavimo algoritmai.

Tame pdf’e atsakymo I sita klausima neradau, bet ten jis kazka per paskaita snekejo kad ten laiko duomenis cache kur cacha gali nuskaityt belekas. Tai atsakymas sitas turetu but manau.

**49**. Kokios rizikos gali atsirasti kompiuterinėse sistemose neprijungtoms nei prie interneto nei prie vidinio įmonės tinklo?

Teisingas atsakymas yra: Nepateikiamumas (sistemos neveikimas)., Duomenų praradimas, vagystė, piknaudžiavimas (pasinaudojimas duomenimis)., Žmogiškasis faktorius (dažnai nepageidaujamas).

**3 Protokolų naudojamų Internete problemos**

**147**. Kaip parenkamas suklastotas IP adresas IP spoofing atakai atlikti?

(Vadovėlis: 2.4.1.1. IP adresų klastojimas – 85p)

Suklastotas IP siuntėjo adresas, parenkamas iš aukos vidinio tinklo srities (potinklio);

**148**. Kokį poveikį tinklo įrenginiams galima padaryti siunčiant specialiai nustatytas ICMP žinutes?

Teisingas atsakymas yra:

* Sumažinti pasirinkto tinklo įrenginio paketų siuntimo spartą.,
* Pasirinktame tinklo įrenginyje pakeisti fragmentų dydžius.,
* Nusiųsti atsakymą į pasirinktą tinklo įrenginį, kad paketų gavėjęs yra nepasiekiamas.,
* Pasirinktame tinklo įrenginyje pakeisti paketų siuntimo maršrutą

**149**. Kurie trys ICMP protokolo žinutės "type" lauko kodai dažniausiai naudojami ICMP atakoms įvykdyti?

Teisingas atsakymas yra: Adresatas nepasiekiamas (angl. Destination unreachable)., Šaltinio pristabdymas (angl. Source Quench)., Nukreipimas (ang. Redirect).

(Vadovėlis: 2.4.1.2. ICMP atakos – 86p)

ICMP atakoms įvykdyti dažniausiai naudojami šie trys ICMP protokolo žinutės *Type* lauko kodai:

a) „Adresatas nepasiekiamas“ (lauko reikšmė – 3).

b) „Šaltinio pristabdymas“ (lauko reikšmė – 4).

c) „Nukreipimas“ (lauko reikšmė – 5).

**150**. Kaip elgiasi paketų siuntėjas, gavęs ICMP žinutę, kurios "type" lauko reikšme "adresatas nepasiekiamas"?

(Vadovėlis: 2.4.1.2. ICMP atakos – 86p)

Pagal žinutėje esančius duomenis siuntėjas teoriškai gali nustatyti, kuris sujungimas neveikia, ir jį nutraukti. Tačiau, kai kurie paketų siuntėjai, gavę ICMP žinutę, kurios *Type* lauko reikšmė – „Adresatas nepasiekiamas“, neanalizuoja informacijos, kuriuo prievadu jis yra nepasiekiamas, ir nutraukia visus sujungimus ( tarp jų – ir veikiančius). Informacijos neanalizuoja ir kai kurių gamintojų ICMP programiniai moduliai.

**151**. Kokios apsaugos priemonės naudojamos prieš "Adresatas nepasiekiamas" ICMP žinučių piktavališką siuntimą?

Teisingas atsakymas yra: Sukonfiguruojami maršrutizatoriai taip, kad trumpalaikiais periodais, iš išorinio tinklo į vidinį, leistų siusti ribotą ICMP žinučių kiekį., Tinklo valdymo sistemos gali aptikti neįprastą ICMP žinučių siuntimą ir sugeneruoti aliarmą.

**152**. Kokia įtaka tinklo įrenginiams galima daryti kol periodiškai siunčiamos jiems "Šaltinio pristabdymas" ICMP žinutės?

Teisingas atsakymas yra: Sumažinti tų įrenginių paketų siuntimo spartas.

**153**. Kokių tikslų siekiama periodiškai siunčiant "Šaltinio pristabdymas" ICMP žinutes į tinklo įrenginius?

Teisingas atsakymas yra: Esant kritinėms tinklo sąlygoms siekiama išvengti perkrovų tinkle., Puolantieji siekia sumažinti tinklo įrenginių pralaidumą taip sukeliant vartotojų nepasitenkinimą.

**154**. Kokios apsaugos priemonės naudojamos prieš "Šaltinio pristabdymas" ICMP žinučių piktavališką siuntimą?

a) Maršruto parinktuvuose ir užkardose uždraudžiamas ICMP žinučių „Šaltinio pristabdymas“ persiuntimas.

b) Maršruto parinktuvuose išjungiama spartos mažinimo funkcija priimant ICMP žinutes „Šaltinio pristabdymas“.

**155**. Kokią f-ją atlieka (jei įjungta) maršrutizatoriai priėmę "Nukreipimas" ICMP žinutę?

Teisingas atsakymas yra: Pakeičia paketų siuntimo krypti..

**156**. Kokios apsaugos priemonės naudojamos prieš " Nukreipimas" ICMP žinučių piktavališką siuntimą?

Tokių žinučių – draudimas jas priimti šias žinutes maršruto parinktuvuose.

**157**. Koks "Ping of Death" atakos veikimo principas?

Teisingas atsakymas yra: Puolantysis siunčia didesnį nei 65535 baitų dydžio ICMP-echo-request sufragmentuotą paketą, o gavėjo įrenginys bando apdoroti tokį perilgą paketą ir užsikerta.

**158**. Koks yra "šaltinio maršrutizavimo" atakos veikimo principas?

Puolantysis siunčia IP paketus su nustatytu fiktyviu siuntėjo adresu esant parinkčiai „Laisvas šaltinio maršrutas“, taip toli esantis kompiuteris ar kitoks įrenginys tampa nepasiekiamas.

**159**. Kokios apsaugos priemonės naudojamos prieš IP paketų, su nustatyta "laisvas šaltinio maršrutas" opcija, piktavališką siuntimą?

Teisingas atsakymas yra: Sukonfiguruojami maršrutizatoriai ir ugnesienės taip, kad iš išorinio tinklo į vidinį nepraleistų IP paketų su suklastotais vidniais siuntėjo adresais.

**160**. Koks yra RIP atakos veikimo principas?

Teisingas atsakymas yra: Puolantysis suklastoja RIP paketą jame nustatydamas, kad jo kompiuteris turi trumpesnį maršruto kelią, tuomet visi vartotojų paketai maršrutizuojami pro puolančiojo kompiuterį, kuris iš tų paketų gali skaityti informaciją..

**161**. Kokios apsaugos priemonės naudojamos prieš siunčiamų RIP paketų piktavališką panaudojimą?

**Turi būti sukonfigūruojami maršrutizatoriai taip, kad maršrutų pakeitimai su RIP būtų vykdomi ne taip lengvai arba turi būti naudojami kiti maršrutizavimo protokolai ir atitinkami šifravimo metodai.**

209. Koks yra EGP atakos veikimo principas?

Teisingas atsakymas yra: Puolantysis simuliuoja autonominį tinklų sietuvą ir išsiųsdamas specialiai nustatytas EGP žinutes nukreipia tarptinklinius srautus per savo sistemą..

**162**. Koks yra EGP atakos veikimo principas?

Teisingas atsakymas yra: Puolantysis simuliuoja autonominį tinklų sietuvą ir išsiųsdamas specialiai nustatytas EGP žinutes nukreipia tarptinklinius srautus per savo sistemą..

**163**. Koks yra ARP atakos veikimo principas?

Teisingas atsakymas yra: Puolantysis inicijuoja tinklo įrenginių paiešką tinkle neegzistuojančiais IP adresais naudodamas ARP paketus, kurie siunčiami į visus lokalaus tinklo įrenginius vienu metu taip sukeliant transiliacijos audrą, dėl kurios susidaro tinklo perkrova.

**164**. Ar turi galimybes puolantysis, TCP fragmentų siuntimo metu, praeiti pro paketų filtravimo sistemą?

Teisingas atsakymas yra: Kai paketų filtras kontroliuoja TCP portų numerius ir SYN vėliavėles, vartotojo inicijuoto TCP sujungimo metu,.

**165**. Kaip išsidėstę fragmentai sudaro įreguliarius atvejus?

1) Surinkus per ilgus fragmentus (*Overlong Fragments*), IP paketo dydis būna didesnis už maksimaliai leistiną (>65535 baitų), (mirtino „Ping“ – ICMP paketo siuntimas).

2) Iš dalies vienas kitą dengiantys fragmentai (*Overlapping Fragments*).

3) Fragmentai, esantys kitų fragmentų viduje (*Interlocking Fragments*) .

**166**. Kokios UDP protokolo savybės skirtingai nei TCP leidžia vykdyti UDP-"Hijacking" ataką?

Teisingas atsakymas yra: Nėra UDP paketų numeracijos., UDP paketų gavėjęs nesiunčia patvirtinimo paketų siuntėjui.

**167**. Koks yra UDP "spoofing" atakos veikimo principas?

UDP „Spoofing“ atakos metu išoriniame tinkle esantis puolantysis norėdamas apeiti užkardą naudoja vietinio tinklo srities siuntėjo IP adresą ir siunčia UDP paketus į iš anksto paruoštą programą, esančią taikinio kompiuteryje.

**168**. Su kokiu tikslu puolantysis vykdo DNS atakas?

Teisingas atsakymas yra: Kad vartotojas nežinodamas, pagal puolančiojo suklastotus DNS lentelės adresus arba domenus, vietoje norimos sistemos, prisijungtų prie puolančiojo padirbtos ir identiškai atrodančios sistemos., Kad puolantysis galėtų sužinoti apie vartotoją (auką) vertingą informaciją (tinklo dizainą, struktūrą ir adresaciją).

**169**. Koks DNS atakos įvykdymo principas, kad galima būtų nukreipti vartotojus į puolančiojo padirbtas ir identiškai atrodančias sistemas?

Puolantysis DNS sistemoje modifikuoja „in-addr.arpa“ lentelę taip, kad įprastiniai domenų vardai būtų susieti su puolančiojo padirbtų ir identiškai atrodančių sistemų IP adresais.

**170**. Koks "IP-bombardavimo" atakos veikimo princip Kas nusako saugos politiką? as?

Teisingas atsakymas yra: Puolantysis instaliuoja į vartotojų kompiuterius programas, vadinamas agentais, kurios TCP arba UDP portais laukia signalo su nurodytu atakos pradžios laiku; atakai prasidėjus, vienu metu visi kompiuteriai (agentų pagalba) generuoja paketus ir siunčia nustatytu IP adresu (t.y. į aukos sistemą)..

**171**. Kokios apsaugos priemonės naudojamos prieš "IP-bombardavimo" atakas?

Teisingas atsakymas yra: Filtravimo programų instaliavimas didžiuosiuose Interneto tinklo sietuvuose., Antivirusinių ir paieškos programų instaliavimas vartotojų kompiuteriuose, kad galima būtų aptikti ir išjungti agentus.

**172**. Koks "SYN- Flooding " atakos veikimo principas?

Teisingas atsakymas yra: Kiekvieną TCP-SYN užklausą priimanti sistema laukia tolimesnių TCP susijungimų valdymo veiksmų, tam užrezervuoja įvairius sistemos resursus, todėl vienu metu nusiuntus labai daug TCP-SYN užklausų ir nevykdant tolimesnių sujungimo sudarymo veiksmų galima išbaigti visus sistemos (aukos) resursus (įvykdyti ataką)

Atakos metu kiekviena TCP-SYN užklausą priimanti sistema laukia tolesnių TCP sujungimo valdymo veiksmų rezervuodama įvairius sistemos išteklius. Todėl vienu metu nusiuntus labai daug TCP-SYN užklausų ir nevykdant tolesnių sujungimo sudarymo veiksmų (TCP – *Handshake-Sequence*) galima išbaigti visus sistemos (aukos) išteklius ir taip įvykdyti ataką

**173**. Kokios apsaugos priemonės naudojamos prieš "SYN- Flooding" atakų įvykdimą?

* a) *Timeout* intervalo mažinimas, kurio metu bus trumpiau rezervuojami ištekliai (greičiau atlaisvinamos atmintinės).

1. b) Sujungimui identifikuoti naudoti tik identifikuojančių duomenų santrumpas (*Hash)* (išnaudojama mažiau atmintinės).
2. c) Tam pačiam vartotojui leisti sudaryti ribotą sujungimų kiekį.

**174**. Koks "TCP eilės numerio" atakos veikimo principas?

Teisingas atsakymas yra: Puolantysis esantis išoriniame tinkle, TCP/IP paketuose suklastoja siuntėjo IP adresą, kad praeitų pro ugnesienę ir siunčia į vidiniame tinkle esančią sistemą (serverį), kurią nori nulaužti; sistema sudarinėdama TCP sujungimą atsakimus siunčia vidinio tinklo vartotojui (suklastotu IP adresu), nors puolantysis ir tiksliai nežinantis kokie tie atsakymai gali su didele tikimybę spėti TCP eilės numerį ir toliau vykdyti reikiamas operacijas su vidiniame tinkle esančią sistema.

**175**. Kokios apsaugos priemonės naudojamos prieš "TCP eilės numerio" atakų įvykdimą?

a) Sukonfigūruoti užkardas arba paketų filtrus taip, kad iš išorinio tinklo ateinantys paketai su vidinio tinklo IP adresais nebūtų persiunčiami į vidinį tinklą.

b) Vidiniame tinkle esančios sistemos (serveriai) privalo turėti papildomus autentifikavimo mechanizmus ir autentifikuoti ne tik pagal vidinio tinklo vartotojų IP adresus.

c) Turi būti naudojami atsitiktinių skaičių generatoriai TCP eilės numeriams sudaryti.

**176**. Koks "TCP sujungimo nutraukimo" atakos veikimo principas?

TCP sujungimo nutraukimo atakos atveju TCP/IP dviejų vartotojų sujungimo metu puolantysis siunčia TCP/IP paketą su nustatyta RST arba FIN vėliavėle ir tinkamu TCP eilės numeriu į aukos sistemą, kuri pradeda atmetinėti visus po to priimtus paketus ir visiškai nutraukia sujungimą.

**177**. Koks "TCP sujungimo perėmimo" atakos veikimo principas?

Teisingas atsakymas yra: Veikiančio TCP/IP sujungimo metu tarp vartotojo ir sistemos (serverio), puolantysis siunčia TCP/IP paketą su tinkamu TCP eilės numeriu vienam vartotojui, jei įsilaužėlio paketai priimami anksčiau tai vartotojo paketai yra atmetami , tokiu būdu puolantysis gali įvykdyti įvairias operacijas prisijungusio vartotojo teisėmis.

TCP sujungimo perėmimo atakos veikimo principas – veikiančio TCP/IP vartotojo ir sistemos (serverio) sujungimo metu puolantysis į aukos sistemą vietoj paketų su RST arba FIN vėliavėle siunčia TCP/IP paketus su tinkamu TCP eilės numeriu. Jei įsilaužėlio paketai priimami anksčiau, vartotojo paketai yra atmetami. Taip puolantysis gali įvykdyti įvairias operacijas prisijungusio vartotojo teisėmis.

**178**. Kokios apsaugos priemonės naudojamos prieš "TCP sujungimo perėmimo" atakų įvykdimą?

Apsisaugoti galima koduojant komunikuojančių partnerių duomenis.

**179**. Kokios problemas sudaro el. pašto paslaugai netobulas SMTP protokolo veikimas?

Teisingas atsakymas yra: Negali būti patikrintas siuntėjo el. pašto adreso autentiškumas.

**180**. Kokios papildomos priemonės gali būti naudojamos siuntėjo el. pašto adreso autentiškumui nustatyti?

Gali būti pasitelkta papildoma priemonė – elektroninio parašo panaudojimą užtikrinanti programa.

**181**. Kokios yra silpnosios vietos komunikavimui naudojant "telnet" protokolą?

Teisingas atsakymas yra: Telnet protokolo žinutėmis duomenys koduojami AsCII format (kas parašyta matoma atviru tekstu) įskaitant vartotojo vardus ir slaptažodžius, todėl srautų turinio monotoringo programų pagalba, įdiegtų magistralinio tinkle mazguose, galima atskleisti daug vertingos informacijos kitokių atakų vykdymui., Vartotojai nepatikrinę panaudoja puolančiųjų sukurtus telnet programas, kurios nežinant vartotojui jo siunčiamus ir gaunamus duomenis registruoja ir persiunčia užpuolėjui.

a) Protokolo žinutėse duomenys koduojami ASCII formatu (atviru tekstu), įskaitant vartotojo vardus ir slaptažodžius. Todėl magistralinio tinklo mazguose įdiegtos srautų turinio stebėjimo programos padeda atskleisti daug vertingos informacijos, panaudotinos atakoms vykdyti.

b) Vartotojai panaudoja nepatikrintas puolančiųjų sukurtas *Telne*t programas, kurios registruoja siunčiamus ir gaunamus duomenis ir persiunčia užpuolėjui nežinant vartotojui.

**182**. Kokios yra apsaugos priemonės naudojant "telnet" protokolą?

a. **Naudoti vienkartinius slaptažodžius.**

b. **Naudoti tik kartu su žinomų gamintojų operacinėmis sistemomis pateiktas telnet programas.**

**183**. Kokios yra apsaugos priemonės naudojant ftp protokolą?

Teisingas atsakymas yra: Jungiantis prie FTP serverio anoniminio vartotojo prisijungimo vardu turi būti uždraustos rašymo teisės, nes puolantysis gali į ftp serverį įrašyti "rhost" bylą ir taip įvykdyti nuotolinio prisijungimo ataką., Slaptažodžių duomenų bylos turėtų būti nepasikiamos vartotojų naudojančių anoniminio prisijungimą

**184**. Kuris iš šių metodų yra nesusijęs su "Denial of Service" ataka?

Teisingas atsakymas yra: Zonos persiuntimas..

Paslaugos blokavimo ataka (Denial of Service) – tai ataka, kai kompiuteris, serveris ar kitas prie interneto prijungtas objektas užtvindomas tūkstančiais IP paketų vienu metu – tam naudojami suklastoti siuntėjo IP adresai. Tuo metu kompiuteriai, serveriai ar kiti objektai tinklui tampa neprieinami, nes tūkstančiai vienu metu priimamų paketų stabdo įprastinį darbą ir pajaučiama, kad paslauga yra išjungta.

**185**. Kokia ataka užtvindina tinklus su trasliacijos būdu siunčiamais paketais, todėl tinklas yra perpildomas?

Teisingas atsakymas yra: "Smurf".

**186**. Kuri ataka yra tiesiogiai susijusi su IP paketų fragmentavimu?

Teisingas atsakymas yra: "TearDrop"..

**187**. Koks veiksmas yra "Land" atakos pagrindas?

Teisingas atsakymas yra: Veikiančio TCP sujungimo atakavimas..

**188**. Kuri ataka yra tiesiogiai susijusi su IP paketų fragmentavimu ir dideliu ICMP paketu?

Teisingas atsakymas yra: Mirtinas “Ping” (angl. Ping of death)

**88psl. ?**  
**IP fragmentavimo atakos.** Kai paketų filtras kontroliuoja TCP prievadų numerius ir SYN vėliavėles, vartotojo inicijuoto TCP sujungimo metu puolantysis gali nusiųsti savo papildomus TCP fragmentus vartotojo IP adresu. Galimi trys variantai, kai tam tikru būdu išsidėstę fragmentai sudaro nereguliariuosius atvejus:

**189**. Kuris atakos tipas IP lygmenyje sukeitinėja IP paketus tam, kad įtikintų sistemą, kad komunikacija vyksta su žinomu kompiuteriu ir jam suteikia priėjimo prie sistemos teises?

Teisingas atsakymas yra: IP adreso falsifikacijos ataka

**190**. Koks DNS atakos įvykdymo principas, kad galima būtų sužinoti apie vartotoją (auką) vertingą informaciją (tinklo dizainą, struktūrą ir adresaciją)?

Teisingas atsakymas yra: Jei DNS serveryje yra apribotas priėjimas prie zonos duomenų tiek, kad būtų galima nuskaityti iš bet kurio serverio, tai puolantysis per TCP 53 prievadą negali tų duomenų lengvai nuskaityti.

**191**. Kokį poveikį tinklo įrenginiams galima padaryti siunčiant specialiai nustatytas ICMP žinutes?

Teisingas atsakymas yra:

* Sumažinti pasirinkto tinklo įrenginio paketų siuntimo spartą.,
* Pasirinktame tinklo įrenginyje pakeisti fragmentų dydžius.,
* Nusiųsti atsakymą į pasirinktą tinklo įrenginį, kad paketų gavėjęs yra nepasiekiamas.,
* Pasirinktame tinklo įrenginyje pakeisti paketų siuntimo maršrutą.

**192**. Koks "Ping of Death" atakos veikimo principas?

Teisingas atsakymas yra: Puolantysis siunčia didesnį nei 65535 baitų dydžio ICMP-echo-request sufragmentuotą paketą, o gavėjo įrenginys bando apdoroti tokį perilgą paketą ir užsikerta..

**193**. Kokios apsaugos priemonės naudojamos prieš IP paketų, su nustatyta "laisvas šaltinio maršrutas" opcija, piktavališką siuntimą?

Teisingas atsakymas yra: Sukonfiguruojami maršrutizatoriai ir ugnesienės taip, kad iš išorinio tinklo į vidinį nepraleistų IP paketų su suklastotais vidniais siuntėjo adresais.

**194**. Ar turi galimybes puolantysis, TCP fragmentų siuntimo metu, praeiti pro paketų filtravimo sistemą?

Teisingas atsakymas yra: Kai paketų filtras kontroliuoja TCP portų numerius ir SYN vėliavėles, vartotojo inicijuoto TCP sujungimo metu,.

**195**. Kaip išsidėstę fragmentai sudaro įreguliarius atvejus?

Galimi trys variantai, kai tam tikru būdu išsidėstę fragmentai sudaro nereguliariuosius atvejus:   
1) Surinkus per ilgus fragm

ntus (Overlong Fragments), IP paketo dydis būna didesnis už maksimaliai leistiną (>65535 baitų), (mirtino „Ping“ – ICMP paketo siuntimas).   
2) Iš dalies vienas kitą dengiantys fragmentai (Overlapping Fragments)   
3) Fragmentai, esantys kitų fragmentų viduje (Interlocking Fragments)

**196**. Koks "IP-bombardavimo" atakos veikimo principas?

Teisingas atsakymas yra: Puolantysis instaliuoja į vartotojų kompiuterius programas, vadinamas agentais, kurios TCP arba UDP portais laukia signalo su nurodytu atakos pradžios laiku; atakai prasidėjus, vienu metu visi kompiuteriai (agentų pagalba) generuoja paketus ir siunčia nustatytu IP adresu (t.y. į aukos sistemą)..

**197**. Kas gali sukelti atakas?

Teisingas atsakymas yra: Hakeriai, atakuodami iš Interneto., Autorizuoti vartotojai, kurie siekia įgyti papildomas privilegijas, kurioms jie nėra autorizuoti., Autorizuoti vartotojai, kurie siekia piktam panaudoti jiems suteiktas privilegijas

**198**. Kas nėra traktuojama kaip įsilaužimas?

Teisingas atsakymas yra: Naudojimasis tinklo teikiamom paslaugomis..

**199**. Jei tinklo administratorius nėra uždraudęs naudotis FTP paslauga, ar naudojimasis ja iš išorės bus traktuojama kaip įsilaužimas?

Tačiau reikia nepamišti, kad tie patys veiksmai įvairiuose tinkluose gali būti traktuojami skirtingai, pvz., viename tinkle yra laisvas priėjimas prie FTP serverio, o kitame tinkle ši paslauga gali būti tiekiama tik autorizuotiems vartotojams. Tai lemia kiekvieno konkretaus tinklo saugos politika, kuri numato, kokios paslaugos kokiai vartotojų grupei teikiamos ir kitus darbo tinkle principus

**4 Užkardos**

**48**. Kodėl nepakanka atskiriems kompiuteriams taikomos saugos ir reikia dar tinklo saugos?

Teisingas atsakymas yra: Todėl, kad tinklo apimtis gali būti didelė ir yra lengviau saugoti įėjimą į tinklą..

**49**. Kas tai yra ugniasienė?

Teisingas atsakymas yra: Tai sistema, skirta užkirsti kelią neautorizuotam priėjimui prie saugomo tinklo..

**50**. Kokiu atveju ugniasienė tinkamai saugos nuo išorinių grėsmių?

Teisingas atsakymas yra: Kai ji bus tinkamai sukonfigūruota, Kai pro ją eis visos komunikacijos su išore.

**51**. Kodėl ugniasienė turi būti diegiama tame taške, kuriame tinklas jungiasi su Internetu?

Teisingas atsakymas yra: Tada yra galimybė išanalizuoti visą į tinklą ateinantį srautą.

**52**. Kodėl visas į tinklą ateinantis srautas turi eiti pro ugniasienę?

Teisingas atsakymas yra: Todėl, kad tada galima užtikrinti, kad srautas bus patikrintas.

**53**. Kas apsprendžia ugniasienių konfigūravimo taisykles?

Teisingas atsakymas yra: Saugos politika

**54**. Kas apsprendžia ugniasienių konfigūravimo taisykles?

Teisingas atsakymas yra: Saugos politika

**55**. Su kuo susiejamos ugniasienių konfigūravimo taisyklės?

Tinklo saugos taisyklėmis.

**56**. Kas nusako saugos politiką?

Teisingas atsakymas yra: Organizacijos interesai.

**57**. Kodėl neužtenka tik įdiegti ugniasienę, kodėl reikalingas jo palaikymas?

Teisingas atsakymas yra: Gali atsirasti naujų tinkle teikiamų paslaugų išoriniams klientams, Gali būt nutrauktas kažkurių paslaugų tiekimas išoriniams klientams., Gali būti fiksuojamos spragos ugniasienės veikloje.

**58**. Ką reiškia paslaugų kontrolė?

Teisingas atsakymas yra: Yra tikrinama, ar tos paslaugos saugomame tinkle yra suteikiamos išorės vartotojams., Yra tikrinama ar vidinio tinklo vartotojai gali kreiptis šių paslaugų į išorinį tinklą

**59**. Kuo skiriasi paketus filtruojančios ugniasienės nuo aplikacinio lygmens vartų?

Teisingas atsakymas yra: Skiriasi tuo, kurio lygmens taisyklėmis operuoja..

**60**. Ar skiriasi paketus filtruojančios ugniasienės nuo aplikacinio lygmens vartų?

Paketus filtruojančios užkardos blokuoja visus paketus, išskyrus leistinus. Paketų filtravimas yra greitas ir remiasi 3–4 (tinklo ir transporto) lygmens informacija. Tarpiniai serveriai išardo tiesioginį ryšį tarp interneto ir vidinių kompiuterių. Tarpiniai serveriai paslepia vidinį tinklą. Kiekvienai kliento ir serverio komunikacijos sesijai reikės dviejų susijungimų:   
nuo kliento iki užkardos (tarpinio serverio)   
nuo užkardos iki serverio.   
Taikomojo sluoksnio vartai – tai tarpinių serverių rūšis, kai sprendimą apie srauto praleidimą viena ar kita kryptimi lemia atitinkamo taikomojo sluoksnio protokolo taisyklės.

**61**. Ar skiriasi grandinės lygmens vartai nuo aplikacinio lygmens vartų?

Teisingas atsakymas yra: Skiriasi filtravimo lygmeniu

Taikomojo sluoksnio vartai – tai tarpinių serverių rūšis, kai sprendimą apie srauto praleidimą viena ar kita kryptimi lemia atitinkamo taikomojo sluoksnio protokolo taisyklės.   
Grandinės lygmens vartai, prieš perduodami srautą atlieka tikrinimą, ar susijungimas yra leistinas. Programinė įranga veikia specialiu SOCKS protokolu.

**62**. Kurio tipo ugniasienės negali paslėpti vidinio tinklo adresų?

Teisingas atsakymas yra: Paketus filtruojančios ugniasienės..

**63**. Kurio tipo ugniasienės negali paslėpti vidinio tinklo adresų?

Teisingas atsakymas yra: Paketus filtruojančios ugniasienės..

**64**. Ar gali paketai patekti į išorinį tinklą nepraeidami pro maršrutizatorių?

Teisingas atsakymas yra: Negali, jei nėra kito išėjimo į Internetą., Gali, jei tinklas susijungia su išoriniu tinklu per modemus

**65.** Ar reikia filtruoti ir iš vidinio tinklo išeinančius paketus?

Teisingas atsakymas yra: Reikia, nes atakos gali kilti ir iš vidinio tinklo ir būti nukreiptos į išorę.

**66.** Kokie veiksmai vykdomi konfigūruojant ugniasienę?

Teisingas atsakymas yra: Sudaromos filtravimo, įrašų kaupimo, aliarmų pranešimų taisyklės.

**67**. Kokių veiksmų nevykdo ugniasienės?

Teisingas atsakymas yra: Atlieka prisijungiančių vartotojų slaptažodžių tikrinimą..

**68**. Ar gali paketinis filtras įvertinti, kas yra perduodama paketo viduje (paketo apkrovą)?

Paketiniai filtrai netikrina paketo apkrovos, paketų sąryšio

**69**. Turime tokią taisyklę išeinančiam srautui: "praleisti paketus, kurie eina iš x.x.x.x šaltinio adreso į \* paskirties adreso 22 prievadą". Ką galėtų reikšti tokia paketinio filtravimo taisyklė?

Teisingas atsakymas yra: Būtų praleidžiami ssh paketai į bet kokį kompiuterį išorėje, einantys iš adreso x.x.x.x.

**70**. Ar reikia drausti vidinio tinklo adreso buvimą šaltinio adresu įeinančiame sraute?

Labai svarbu tinkamai išdėstyti taisykles: pradedant specialiomis ir baigiant bendrosiomis. Jose turi būti numatyta, kad įeinančio srauto paketų šaltinio adresai nesutaptų su vidinio tinklo adresais.

**71**. Ar reikia drausti išorinio tinklo adreso buvimą šaltinio adresu išeinančiame sraute?

Teisingas atsakymas yra: Paketo siuntėju negali būti išorinio tinklo kompiuteriai, kadangi paketas eina iš vidinio tinklo..

Labai svarbu tinkamai išdėstyti taisykles: pradedant specialiomis ir baigiant bendrosiomis. Jose turi būti numatyta, kad išeinančio srauto paketų šaltinio adresai nesutaptų su išorinio tinklo adresais.

**72**. Kokiems paketams taikoma taisyklė pagal nutylėjimą?

Teisingas atsakymas yra: Tiems, kurie netenkino jokios kitos taisyklės

**73**. Ar reikia įsiminti būvio informaciją ugniasienėje?

Teisingas atsakymas yra: Taip, tai leidžia patikrinti, kad paketas ateina pagal protokolo reikalavimus.

**74**. Jei yra trūkumų paketiniame filtravime, tai kodėl jis naudojamas?

Teisingas atsakymas yra: Leidžia greitai nufiltruoti didelę dalį žinomai blogų paketų

**75**. Ar gali viešai naudojami serveriai būti ekranuojamame (maskuojamame) vidiniame tinkle?

Teisingas atsakymas yra: Negali, nes jie tada neturės viešai prieinamo IP adreso..

**76**. Ar galimas tiesioginis paketų kelias į maršrutizatorių iš vidinio tinklo kompiuterių ekranuojančio bastioninio kompiuterio architektūroje?

Teisingas atsakymas yra: Ne.

**77**. Kodėl reikia pašalinti nesusijusius su paketų perdavimu servisus iš bastioninio kompiuterio?

Teisingas atsakymas yra: Spragos šiuose servisuose gali leisti perimti šio kompiuterio valdymą.

**78**. Kaip galima daug vidinių kompiuterių adresų pakeisti vienu bastioninio kompiuterio adresu?

Norint paslėpti vidinį tinklą nuo išorės, su išorėje esančiais kompiuteriais jungiamasi tik per vieną tinklo kompiuterį, vadinamą bastioniniu kompiuteriu (tarpiniu serveriu).

Teisingas atsakymas yra: Pasinaudojama skirtingais bastioninio kompiuterio prievadais..

**79**. Ar skiriasi taikomųjų programų lygmens vartai nuo paketinio filtravimo ugniasienių.

Paketas išanalizuojamas giliau nei filtruojant, nes yra vertinami ne tik siuntėjo/gavėjo adresai bei prievadai, bet ir taikomojo protokolo detalės.

**80**. Kodėl reikalingas taikomojo protokolo detalių vertinimas ugniasienėje?

Teisingas atsakymas yra: Ataka gali būti susijusi su taikomajame protokole naudojamais metodais, su nesaugiu veikimu.

**81**. Kodėl netikslinga visą į vidinį tinklą ateinantį srautą filtruoti naudojant taikomųjų programų vartus?

Šio tipo užkardos veikia lėtai, todėl taikytinos atskiram srautui, o ne kiekvienam į tinklą ateinančiam paketui filtruoti.

Teisingas atsakymas yra: Netikslinga, nes šio tipo ugniasienė sulėtina srautą filtruodama visus paketus pagal taikomąjį protokolą..

**82**. Ar reikia kelių aplikacinio lygmens proxy?

Teisingas atsakymas yra: Taip, nes kiekvienas iš jų supranta savą taikomąjį protokolą.

**83**. Ar reikia kelių aplikacinio lygio proxy?

Taip, nes kiekvienas iš jų supranta savą taikomąjį protokolą.

**84**. Kur tikslinga sudėti viešam priėjimui teikiamas paslaugas?

Teisingas atsakymas yra: Atskirame vidinio tinklo potinklyje..

**85**. Ar pakanka tinklą saugoti viena ugniasiene?

Teisingas atsakymas yra: Ne, nes ugniasienę sukompromitavus visas tinklas tampa atviras atakoms.

**86**. Kuriame potinklyje didesnė atakų rizika DMZ ar vidiniame potinklyje?

Teisingas atsakymas yra: DMZ.

**87**. Kodėl papildoma ugniasienė turi būti stipresnė?

Teisingas atsakymas yra: Todėl, kad atakuotojas, įsilaužęs į DMZ arba pažeidęs įėjimą saugančią ugniasienę, negalėtų laisvai prieiti prie vidinio tinklo.

**88**. Ar grandinės lygmens vartai susiję su taikomųjų protokolų ypatumais?

Nesusiję. Šitie tarpiniai serveriai nenagrinėja taikomojo lygmens informacijos kaip taikomojo sluoksnio vartai, taigi nereikia atskiro tarpinio serverio kiekvienam taikomajam protokolui.

**89**. Ar susijęs grandinės lygio vartų filtravimas su taikomaisiais protokolais?

Teisingas atsakymas yra: Ne, jie dirba žemesniame lygmenyje nei taikomųjų programų lygmuo.

**90**. Ar gali bet kuris išorinis kompiuteris siųsti paketus per grandinės lygio ugniasienę?

Teisingas atsakymas yra: Jei yra tam autentifikuotas ir turi įrangą.

**91**. Ar gali išoriniai vartotojai tiesiogiai komunikuoti su vidiniais kompiuteriais esant grandinės lygmens ugniasienei?

(Vadovėlis: 3.1.24. SOCS veikimo principai – 102p)

Negali. Išoriniai kompiuteriai mato tik tarpinio serverio IP adresą ir niekada tiesiogiai nekomunikuoja su vidiniais tinklo kompiuteriais.

**92**. Kuris teiginys apie ugniasienę, įdiegtą namų kompiuteryje nėra teisingas?

Teisingas atsakymas yra: Ji saugo nuo virusų

(Skaidrės: pask7 – 43p)  
•Grėsmės:

– Skenavimo, įsilaužimo, prijungimo prie “botnet”, perėmimo, išvedimo iš rikiuotės, informacijos konfidencialumo paradimo.

• Užkarda pajėgi :

blokuoti priėjimą prie jūsų kompiuterio.

**93**. Ar tikslinga universiteto duomenų bazes saugančių kompiuterių tinklą atskirti nuo bendro universiteto tinklo?

Teisingas atsakymas yra: Taip.

Tikslinga, nes universiteto tinkle yra paslaugų skirtų išoriniams vartotojams ir studentams, kurių spragos gali būti panaudotos atakoms.

(Dėl šito neesu visiškai tikras. Čia žiūrint kaip pažiūrėsi į tą tinklą. Jei klystu, pataisykit.)

**94**. Ko negali ugniasienės?

Teisingas atsakymas yra:

* apsaugoti nuo tų susijungimų, kurie neina pro jas,
* apsaugoti nuo naujų atakų rūšių.

**95**. Kokio tipo ugniasienių nėra?

Teisingas atsakymas yra: Paketinio lygmens vartai

96. Kokių veiksmų netlieka ugniasienės?

Atlieka prisijungiančių vartotojų slaptažodžių tikrinimą

**5 IPsec protokolas**

**1**. Kuriame OSI lygyje užtikrina apsaugą IPSec protokolas?

Teisingas atsakymas yra: Tinkliniame lygyje.

**2**. Kokios atakos yra nukreiptos prieš IP paketą tinkliniame lygyje?

Informacija yra perduodama tinklais – ji sudedama į IP paketus. Kadangi IP nėra saugus protokolas, todėl galima:

suklastoti IP adresą (IP *Address Spoofing*),

modifikuoti IP paketo turinį,

atsakyti senu turiniu,

paketo perdavimo metu peržiūrėti jo turinį.

**3**. Kokios apsaugos neteikia IPSec protokolas?

Teisingas atsakymas yra: Apsaugos nuo paketo perėmimo..

ESP protokolas užtikrina duomenų vientisumą, konfidencialumą (taip pat ribotą srauto kontrolės konfidencialumą), apsaugo nuo seno paketo panaudojimo – tai reiškia, kad protokolas gali užtikrinti IP paketo sekos numerio tikrumą, tačiau jis negali lemti paketų atėjimo tvarkos. AH protokolas autentifikuoja duomenų šaltinį, užtikrina duomenų vientisumą, apsaugo nuo seno paketo atkartojimo, gali teikti „negalėjimo paneigti“ apsaugą. AH protokolas negarantuoja duomenų konfidencialumo.

**4**. Pasiekiamumas saugos požiūriu reiškia tai, kad ....

Teisingas atsakymas yra: visi sistemos ištekliai yra pasiekiami visiems vartotojams, visi sistemos vartotojai gali pasiekti išteklius, visi autorizuoti sistemos vartotojai gali pasiekti išteklius

**5**. Autentiškumas IPSec kontekste reiškia ..

Duomenų autentiškumas yra patvirtinamas įrodant, kad tai tie patys duomenys, kurie buvo perduoti, t. y. jų tikrumas ir vientisumas nebuvo pažeisti nei perdavimo metu, nei po to. Taigi duomenų autentiškumas priklauso nuo jų sudarytojo, kuris turi užtikrinti duomenų tikrumą ir vientisumą iki juos perduodant, taip pat nuo duomenų vientisumo išlaikymo duomenų perdavimo metu. Todėl norint užtikrinti duomenų autentiškumą, turi būti naudojamos priemonės, skirtos jiems apsaugoti nuo sąmoningo ar nesąmoningo pakeitimo, sugadinimo, suklastojimo, praradimo jo perdavimo ir saugojimo metu. Būtent IPSec protokolas atlieka duomenų šaltinio autentiškumo kontrolę. Tai saugos funkcija, kuri tikrina duomenų šaltinio identiškumą. Ši paslauga paprastai teikiama kartu su vientisumo tikrinimo paslauga

**6**. Vientisumo užtikrinimas leidžia aptikti tai, kad....

Teisingas atsakymas yra: IP datagrama nėra pakeista

Vientisumo tikrinimas – tai saugos funkcija, kuri padeda pastebėti bet kokį duomenų pakeitimą. IPSec kontekste yra palaikomos dvi vientisumo užtikrinimo formos:

Besąryšis (*Connectionless Integrity*) vientisumo užtikrinimas.

Dalinio eiliškumo vientisumo (*Partial Sequence Integrity*) užtikrinimas.

**7**. Kaip suprantate konfidencionalumo užtikrinimo paslaugą?

Teisingas atsakymas yra: Tai yra saugos paslauga, kuri apsaugo duomenis nuo neautorizuoto atskleidimo., Tai yra paslauga, kuri padaro duomenis prieinamais tik autorizuotam vartotojui

**8**. Kas sudaro IPSec protokolą?

IPSec – ne vienas protokolas, o jų grupė [1, 4, 5, 6, 7]. IPSec naudoja du srauto saugą užtikrinančius protokolus:

AH – IP autentifikacinės antraštės protokolą,

ESP – saugaus IP paketo apkrovos įpakavimo protokolą.

IPSec

atlikdama savo veiksmus pasitelkia šifravimo raktų valdymo procedūras ir protokolus:

• ISAKMP – interneto saugos asociacijų ir raktų valdymo protokolą (*Internet Security Association and Key Management Protocol* – ISAKMP), kuris nusako automatinį saugos asociacijų (SA) įkūrimą ir šifrų raktų valdymą.

• IKE – raktų apsikeitimo protokolą (*Internet Key Exchange* – IKE).

IPSec protokolų ir jų naudojimo būdų pasirinkimą nulemia vartotojų, taikomųjų programų, organizacijų keliami reikalavimai.

**9**. Jei IP paketą saugo IPSec protokolas, ar ir toliau jis išlaiko IP protokolo standartiniu paketu?

Teisingas atsakymas yra: TAIP

IPSec protokolo apsaugoti IP paketai ir toliau išlieka standartiniais IP paketais.

**10**. Kas tai yra saugos asociacija?

Teisingas atsakymas yra: Tai saugos parametrų rinkinys, kuris surišamas su viena kryptimi perduodamu srautu..

**11**. Saugos parametrų rinkinys, kuris surišamas su viena kryptimi perduodamu srautu yra vadinamas ...?

Saugos asociacija

**12**. Kokios paslaugos neteikia AH protokolas lyginant su ESP protokolu?

**a. AH neteikia duomenų konfidencionalumo paslaugos**

**13**. Jei komunikuojant dviems kompiuteriams yra naudojamas tuneliavimo režimas tarp vartų, IPSec protokolas saugos komunikacijas.....?

Teisingas atsakymas yra: Kelyje nuo vienų iki kitų vartų..

**14**. Kuo skiriasi IPSec naudojami darbo režimai?

Teisingas atsakymas yra: Transporto režime apsaugomi tik IP paketo duomenys, o tuneliavimo režime apsaugomas visas paketas..

**15**. Transporto režime taikant IPSec yra apsaugomi ....?

Teisingas atsakymas yra: Tik IP paketo duomenys.

**16**. Kuriuose tinklo įrenginiuose gali būti įdiegiamas IPSec protokolas?

Teisingas atsakymas yra: Tik darbo stotyse, Tinkliniuose įrenginiuose, darbo stotyse, serveriuose.

**17**. Kokiu atveju AH antraštė autentifikuoja visą siunčiamą paketą?

Teisingas atsakymas yra: Taikant AH paslaugą tuneliavimo režime..

**18**. Kokiam tikslui naudojamas SN laukas ir koks ryšys su SN lauku naudojamu IP antraštėje?

Teisingas atsakymas yra: SN laukas naudojamas apsaugai prieš pakartotino paketo panaudojimo atakas. Ryšio su IP SN nėra..

SN – eilės numeris (32 bitai). Jis reikalingas siekiant išvengti pakartotinio paketo panaudojimo. Nutylėjus protokolas reikalauja, kad siuntėjas didintų SN reikšmę – tai efektyvu, jei gavėjas šią reikšmę tikrina

„Sekos numeris – SN“ yra skaičius, didėjantis su kiekvienu IP paketu, kurį siunčia to paties tinklo mazgas (kompiuteris) tam pačiam gavėjui ir kai SA yra ta pati.

**19**. Kaip yra patikrinamas gauto paketo autentiškumas?

Teisingas atsakymas yra: Sulyginti gautą MAC reikšmę su suskaičiuota MAC reikšme, skaičiuojant ją priimtam paketui.

**20**. Kuo skiriasi transporto režimo autentifikavimo paslauga, kai ji teikiama ESP ir AH protokolais?

Teisingas atsakymas yra: ESP transporto režime neautentifikuoja originalios IP antraštės laukų.

**21**. Jei IPSec dirba tuneliavimo režime, kuriame iš nurodytų laukų yra patalpinamas originalus IP paketas?

Teisingas atsakymas yra: Visas originalus šifruotas IP paketas talpinamas "Apkrovos duomenų" lauke..

**22**. ESP šifruoja perduodamą paketą. Kokią saugos charakteristiką tai užtikrina?

Teisingas atsakymas yra: Konfidencionalumą

**23**. Ką reiškia pavadinimas simetrinis blokinis šifravimo algoritmas?

Simetrinis todėl, kad tas pats raktas taikomas tiek šifruojant, tiek iššifruojant informaciją. Blokinis, nes šifruojamas informacijos blokas.

**24**. Ar gali būti rankiniu būdu užduodami šifravimo raktai?

Gali. Šifravimui reikalingos su raktais susijusios informacijos paieška gali būti užduodama įvedant ją rankomis komandos eilutėje arba naudojant grafinę sąsają. Šis metodas žinomas kaip rankinis raktų nustatymas „Manual Keying“. Tai patogus, tačiau turintis nemažai trūkumų būdai.

**25**. Kokia pagrindinė IKE protokolo paskirtis?

Teisingas atsakymas yra: Ssusiderėti ir saugiai pateikti autentifikuotą su raktais susijusią informaciją, įkurti saugos asociacijas.

IKE protokolas naudojamas ryšiui sukurti pirmajame etape, kai šalys susitaria dėl šifravimo metodų, raktų ir kitų duomenų, kuriuos naudos sukuriant apsaugotą ryšio sesiją – saugos asociaciją.

**26**. Dėl kokių parametrų deramasi įkuriant SA?

Teisingas atsakymas yra: Autentifikavimo mechanizmo ir jo parametrų, Šifravimo algoritmo (jo modos, raktų ilgio, pradinio vektoriaus), Raktų reikšmių ir raktų galiojimo laiko, SA atnaujinimo periodo

**27**. Dėl kokių parametrų nėra deramasi įkuriant SA?

Teisingas atsakymas yra: SPI indekso

IPsec siuntėjo ir gavėjo IP adresą.

Saugos parametrų indeksą SPI (*Security Parameter Index*), nurodomą AH arba ESP antraštėse ir saugomą atitinkamose SA duomenų bazėse.

Protokolą – AH arba ESP.

Darbo režimą – tunelio arba transporto.

Šifravimo algoritmus ir raktus.

Asociacijos gyvavimo laiką

**28**. Kaip siunčiamame pakete yra nusakoma, kokia apsauga yra pritaikyta šiame pakete?

Teisingas atsakymas yra: Tai yra užduodama per SPI, Tai yra nurodoma į paketą įdedant SA

**29**. Kam reikalingas IKE SA?

Teisingas atsakymas yra: Įkūrus IKE SA kartu yra įkuriamas saugus kanalas deryboms dėl IPSec SA.

**30**. Kurioje IKE protokolo veiklos stadijoje susiderama dėl IPSec SA?

Teisingas atsakymas yra: 2-oje fazėje

**31**. Kurioje fazėje veikiant IKE protokolui vyksta bendraujančių pusių tarpusavio autentifikacija?

Teisingas atsakymas yra: Įkuriant derybų kanalą.

**32**. Kuo grindžiama autentifikacija jei yra perduodamas sertifikatas?

Viešuoju raktu? autentifikaciją (naudoja viešojo rakto sertifikatus)

Svarbiausi sertifikato elementai: versija, serijos numeris, algoritmo identifikatorius, leidėjas, galiojimo terminas, subjektas (serveris arba klientas), subjekto viešojo rakto informacija, viešojo rakto algoritmas, subjekto viešasis raktas, leidėjo unikalus identifikatorius (neprivalomas), subjekto unikalus identifikatorius (neprivalomas), išplėtimai (neprivalomi), sertifikato parašo algoritmas, sertifikato parašas.

Kai serveris naršyklei pateikia sertifikatą, ji patikrina [5]:

a) Galiojimo datą – jei sertifikatas nebegalioja, parodomas klaidos pranešimas.

b) Pasirašiusios organizacijos patikimumą – sertifikatą generuoti gali bet kas, tačiau jį turi patvirtinti patikima sertifikatų tarnyba. Šiuolaikinėse naršyklėse jau būna įdiegti patikimų ir pripažintų organizacijų šakniniai sertifikatai, pagal kuriuos atliekamas žemesnio lygmens sertifikatų patikrinimas. Jei sertifikatas neišsaugotas atmintyje, naršyklė jį pateikia vartotojui, kad jis pats patikrintų sertifikato patikimumą.

c) Parašą – sertifikato vientisumui patikrinti.

d) Serverio tapatybę (*Identity*) – ar sertifikate nurodytas serverio vardas sutampa su sertifikatą pateikiančio serverio vardu.

**33**. Ar gali pagrindinio režimo komunikacijas pradėti bet kuri pusė?

Teisingas atsakymas yra: Taip

**34**. Koks pagrindinio režimo antros pranešimų poros tikslas?

Teisingas atsakymas yra: Sukurti simetrinio šifravimo raktą

**35**. Kodėl pagrindinio režimo trečiame žingsnyje komunikuojančios pusės turi autentifikuotis?

Teisingas atsakymas yra: Jei nevyks autentifikacija dalyviu gali prisistatyti bet kas.

**36**. Kokiu tikslu pagrindinio režimo 3-ia pranešimų pora yra tvirtinami ankstesniuose pranešimuose siųsti duomenys?

**37**. Kodėl reikalingos dvi saugos asociacijos komunikacijai tarp dviejų pusių?

Teisingas atsakymas yra: Gali būti pritaikomi skirtingi saugos parametrai..

**38**. Kodėl antra komunikuojanti pusė nesiūlo keleto saugos algoritmų rinkinių?

Teisingas atsakymas yra: Todėl, kad ji turi pasirinkti vieną rinkinį iš pasiūlytų..

**39**. Kodėl saugos asociacijoje yra užfiksuojami bendraujančių pusių IP adresai?

Teisingas atsakymas yra: Todėl, kad kiekviena SA suriša saugos parametrus su konkrečia komunikavimo kryptimi., Tam, kad būtų galima pagal IP adresus nustatyti, ar teisingai yra pritaikyta apsauga atėjusiam paketui.

**40**. Pagal ką yra atrandami paketo saugos parametrai SAD?

Teisingas atsakymas yra: Pagal pakete nurodytą SPI.

**41**. Kodėl neužtenka dviejų SA komunikacijai tarp dviejų pusių nusakyti?

**42**. Ar tuneliavimo režimo atveju gali būti perduodamas nešifruotas IP paketas?

Teisingas atsakymas yra: Taip, jei pritaikomas tik AH protokolas

Esant tunelio režimui, tikrasis IP paketas yra „įvelkamas“ į kitą IP paketą ir jam yra suteikiama nauja IPSec antraštė (AH arba ESP). Tunelio režimas apsaugo visą IP paketą, nes užšifruojami ne tik paketo duomenys, bet ir antraštės.

**43**. Kas saugoma SPD?

SPD (*Security Policy Database*) duomenų bazė, kurioje saugomos taisyklės, koks IPSec srautas turi būti apdorojamas, o koks – ignoruojamas. Šios taisyklės panašios į užkardų paketų filtravimo taisykles.

**44**. Kodėl reikalinga saugos politikos duomenų bazė?

Joje yra visi kriterijai, pagal kuriuos nusprendžiama, ar paketams reikia taikyti IPSec apsaugą (pvz., paskirties IP adresas, paskirties prievado numeris, šaltinio IP adresas, duomenų jautrumo lygis, transporto protokolas ir kt.)

**45**. Ar gali būti paketas sunaikinamas (atmetamas) IPSec mazge?

Taip.

**46**. Kas yra daroma su priimtu paketu, jei pagal SPI nepavyksta atrasti tinkamos SA SAD?

Teisingas atsakymas yra: Paketas numetamas.

**47**. Ar galima situacija, kad siunčiamam paketui nėra taikoma IPSec apsauga?

Teisingas atsakymas yra: Taip, jei pagal saugos taisykles numatyta praleisti – paketas persiunčiamas.

**48**. Kada yra sukuriamos naujos SA?

b. **Kai to paprašo aukštesnio lygmens (vartotojo lygmens) protokolas.**

c.**Kai gaunamas IPSec apsaugotas IP paketas**

**49**. Ką reiškia IPSec protokolo skaidrumas?

Teisingas atsakymas yra: Aplikacijos gali nejausti IPSec protokolo veiklos..

**50**. Ar galima paketui pritaikyti ir transporto ir tuneliavimo režimą kartu?

Teisingas atsakymas yra: Galima, jei kelyje tarp vartų taikomas tuneliavimas, o paketui jau pritaikyta transporto režimo apsauga.

**51.** PPTP teikia saugumą:

Teisingas atsakymas yra: OSI modelio ryšio lygmenyje

Kuris iš šių apibrėžimų geriau atitinka suklastojimo (angl. spoofing) atakos apibrėžimą?

Pasirinkite vieną ar daugiau:

Teisingas atsakymas yra: Tai metodas naudojamas neautorizuotam priėjimui prie kompiuterio, serverio ar kito resurso, kai įsilaužėlis siunčia žinutę su suklastotu adresu ar kitokiu identifikatoriumi..

Paketų autentiškumo nustatymas naudojamas:

Teisingas atsakymas yra: Duomenų kilmės autentiškumui užtikrinti., Pažeistų, pakeistų paketų nustatymui.

Kurie teiginiai apie PPTP protokolą teisingi?

Teisingas atsakymas yra: PPTP atlieka duomenų šifravimą ir glaudinimą., PPTP naudoja PAP autentifikavimo protokolą

Pažymėkite šifravimo algoritmus:

Teisingas atsakymas yra: DES, 3DES, IDEA

Kokias galimybes turi interneto tiekėjęs rinkti duomenis apie vartotojų duomenų persiuntimus, net kai naudojami saugaus perdavimo algoritmai?

Teisingas atsakymas yra: Skaityti vartotojų el. laiškus, kai pašto serverį administruoja interneto tiekėjęs..

Kuris teiginys teisingas (-i)?

Teisingas atsakymas yra: Simetriniai raktai: tas pats raktas naudojas duomenų užšifravimui ir iššifravimui., Asimetriniai raktai: viešas raktas naudojamas duomenų užšifravimui, privatus – iššifravimui.

Kuris teiginys teisingas (-i)?

Teisingas atsakymas yra: VPT tinklai naudoja raktų apsikeitimo technologijas., VPT tinklai naudoja šifravimo technologijas.

Kuris teiginys teisingas?

Teisingas atsakymas yra: Asimetriniai raktai skirstomi ir viešus ir privačius..

Kuris teiginys neteisingas (-i)?

Teisingas atsakymas yra: VPT tinklai nenaudoja autentiškumo nustatymo metodų..

Kuris teiginys neteisingas (-i)?

Teisingas atsakymas yra: VPT tinklai nenaudoja autentiškumo nustatymo metodų..

Įrenginių autentiškumo nustatymui naudojami:

Pasirinkite vieną ar daugiau:

Teisingas atsakymas yra: Daliniai (pre-shared) simetriniai raktai., Daliniai (pre-shared) asimetriniai raktai., Skaitmeniniai sertifikatai.

Išrinkite teisingą teiginį

Teisingas atsakymas yra: AH(Authentication Header ) gali neapsaugoti nuo paketų nepakartojamumo..

Kurie iš išvardintų objektų yra L2TP komponentai?

Teisingas atsakymas yra: Tinklo prieigos serveris (NAS), L2TP prieigos telktuvas (LAC), L2TP tinklo serveris (LNS)

L2TP teikia saugumą:

Teisingas atsakymas yra: OSI modelio ryšio lygmenyje

PSec teikia saugum

Teisingas atsakymas yra: OSI modelio tinklo lygmenyje..

Kas iš išvardintų yra PPTP pažeidžiamumai leidžiantys įsilaužėliui atakuoti PPTP protokolu veikiantį VPT tinklą?

Teisingas atsakymas yra: GRE protokolo naudojamas paketavimas., Nešifruotų slaptažodžių perdavimas tinklu.

Kurie teiginiai teisingi?

Teisingas atsakymas yra: IKE turi du veikimo etapus., IKE turi keturis veikimo režimus., Agresyvus režimas nėra IKE etapas.

Kurie teiginiai teisingi (-as)?

Teisingas atsakymas yra: Naudojant PPTP, yra užšifruojami tik PPP duomenys., PPTP yra paprastesnis protokolas negu L2TP

Kurie teiginiai teisingi (-as)?

Teisingas atsakymas yra:Naudojant DH algoritmą, privatus raktas nėra persiunčiamas tinkle. DH algoritmas nėra atspaarus tarpinio žmogaus (man-in-the-middle) atakai.

IPSec pagrindiniai komponentai:

Teisingas atsakymas yra:

a. AH ir ESP protokolai.

c. Raktų valdymo protokolai.

d. Šifravimo ir autentifikacijos algoritmai.

Pagrindiniai VPT tipai:

b. Nuotolinės prieigos

c. Tarptinklinio sujungimo

Orginali IP antraštė yra užšifruojama:

a. Transporto režime.

Jei IP paketą saugo IPSec protokolas, ar ir toliau jis išlaiko IP protokolo standartiniu paketu?

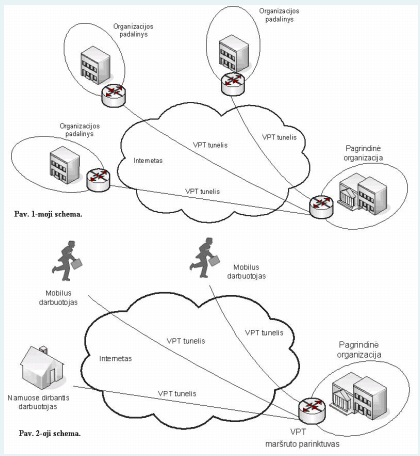
Pasirinkite vieną:

Teisingas atsakymas yra: TAIP..

Kurie iš šių išvardintų punktų tinka šiuolaikinio Interneto apibūdinimui?

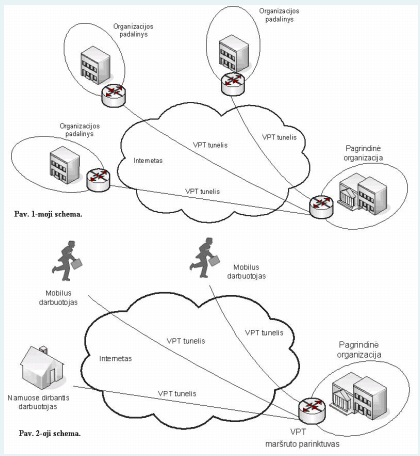
Teisingas atsakymas yra: Internetas yra paplitęs globaliu mastu ir apima skirtingas kultūras, skirtingų valstybių politikos įtakoja mažai, nėra vieningų standartų kovai prieš Internetinius nusikaltimus., Internetas panaudotas individualių tinklų, taip pat viešų prisijungimo taškų sukūrimui: prie bibliotekų, valstybinių institucijų, el. parduotuvių ir t.t., Internetas vis daugiau pritaikomas vidinių tinklų (Intranetų) sudarymui - VPN tinklai vietoje skirtinių linijų, mobilieji abonentai gali prisijungti per bevielio ryšio prieigą.

Kuri schema teisingiausiai pavaizduoja tarptinklinio sujungimo VPT:



Teisingas atsakymas yra: 1-moji schema.

Kuri schema teisingiausiai pavaizduoja nuotolinės prieigos VPT?



Teisingas atsakymas yra: 2-roji schema.

Kurie VPT protokolai veikia 2 OSI modelio lygmenyje?

Teisingas atsakymas yra: PPTP, L2TP

Pažymėkite VPT protokolus:

Teisingas atsakymas yra: PPTP, IPSec, L2TP

VPT susjungimų režimai(-as):

Teisingas atsakymas yra: Transporto režimas, Tuneliavimo režimas

IKE yra:

Teisingas atsakymas yra: Raktų valdymo protokkolas

Kokiu tikslu pagrindinio režimo 3-ia pranešimų pora yra tvirtinami ankstesniuose pranešimuose siųsti duomenys?

Teisingas atsakymas yra: Tuo patvirtinama, kad šios komunikacijos pusės Dalyvavo ankstesniuose pranešimų persiuntimuose. Tuo abi pusės autentifikuojasi

Kurie iš pateiktų pažeidžiamumų aprašymų yra teisingi?

Teisingas atsakymas yra: IPSec gali būti pažeidžiamas naudojant tarpinio žmogaus ataką

Kuri iš išvardintų atakų yra efektyviausia naudoti prieš IPSec protokolu veikiantį VPT tinkle?

Teisingas atsakymas yra: Grubios jėgos ataka., Tarpinio žmogaus ataka

Kuris iš išvardintų atakų yra galima, atlikus operacinės sistemos buferio perpildymą?

Teisingas atsakymas yra: Paslaugos išjungimo (angl. Denial of service)

Kurie iš išvardintų režimų, nėra IPSec režimai?

Teisingas atsakymas yra: Agresyvus režimas., Greitas režimas.

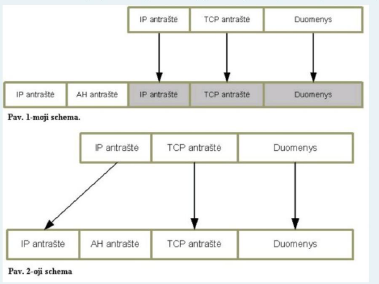
Saugumo asociacijos (SA):

Teisingas atsakymas yra: Apibrėžia, kokios saugumo paslaugos teikiamos kiekvienam vartotojui..

Saugumo asociacijos (SA) naudojamos (-a) duomenų bazės (-ė):

Teisingas atsakymas yra: SAD (Security Association Database )., SPD (Security Policy Database).

Kuri schema teisingai pavaizduoja duomenų įpakavimą naudojant transport režima?



Teisingas atsakymas yra: 2-roji schema

## 2. DMZ

**1**. Kur tikslinga tinkle įdiegti ugniasienę?

Tarp išorės ir DMZ (prieš internetą) (įėjimą sauganti užkarda) ir tarp DMZ ir vidinio tinklo (prieš vidinį tinklą) (papildoma užkarda).

**2**. Kokie laukai nėra vertinami taikant paketinį filtravimą?

Teisingas atsakymas yra: Taikomojo lygmens..

Vertinami:

1. Naudojama tik tinklo ir transporto lygmens informacija

2. IP šaltinio /gavėjo adresai

3. Fragmentacija

4. IP antraštės opcijos

5. protokolas (TCP, UDP, ICMP, t.t)

6. TCP arba UDP šaltinio /gavėjo prievadai

7. TCP vėliavėlės (SYN, ACK, FIN, RST, PSH, t.t.)

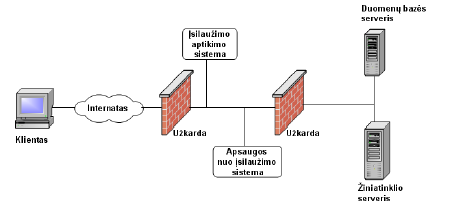
8. ICMP pranešimo tipas

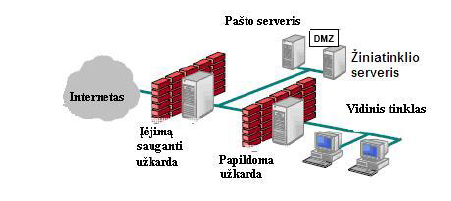
**3**. Ar saugu yra laikyti web serverį toje pačioje zonoje kaip ir darbuotojų darbo stotis?

Teisingas atsakymas yra: Tame pačiame potinklyje laikyti nėra saugu

**4**. Ar saugu yra laikyti išoriniams vartotojams pasiekiamą web serverį toje pačioje zonoje kaip ir darbuotojų darbo stotis?

Ne, nes “Žiniatinklio apsauga reikia rūpintis per visą jo gyvavimo ciklą“, web serveris lieka neapsaugotas :





**5**. Demilitarizuota zona- tai ....?

Teisingas atsakymas yra: Potinklis, skirtas patalpinimui serverių, teikiančių viešam naudojimui skirtas paslaugas..

**6**. Kodėl vidinį tinklą rekomenduotina saugoti nuo DMZ?

Teisingas atsakymas yra: Servisai gali būti su pažeidžiamumais ir juos pažeidus galimos atakos į vidinį organizacijos tinklą

7. Kokie kompiuteriai talpinami demilitarizuotoje zonoje?

Teisingas atsakymas yra: Serveriai, teikiantys paslaugas išoriniams klientams.

**8**. Kur reikėtų patalpinti Web serverį, skirtą vidiniams vartotojams?

Teisingas atsakymas yra: Intranete..

**9**. Su kokiomis problemomis susiduriama taikant perimetrinę saugą?

• Blogai sukonfigūravus perimetrą saugančią užkardą tinklas gali tapti atviru atakoms.

• Paketus filtruojančios užkardos gali neapsaugoti nuo atakų surištų su taikomaisiais protokolais.

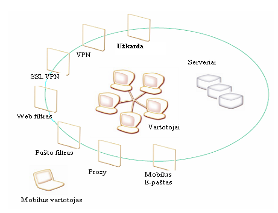
• VPN susijungimai gali likti nefiltruoti.

• Riziką perimetro saugai padidina bevieliai tinklai, jungimasis per modemus.

Paketus filtruojančios ugniasienės gali neapsaugoti nuo atakų surištų su taikomaisiais protokolais, todėl reikia naudoti ir taikomojo lygmens ugniasienes, kurios įneša vėlinimus \* VPN susijungimai gali likti nefiltruoti, nes šiais susijungimais duomenys keliauja šifruoti, ir jei galinis komunikavimo taškas nėra ugniasienė, ji gali tokio paketo ir neiššifruoti, tuo pačiu praleisdama atakas. \* Siūloma išeitis- stiprinti vidinę tinklo saugą.

**10**. Taikant perimetrinę apsaugą saugos priemonės yra talpinamos:

Tinklo perimetre.



Užkarda paprastai įrengiama vidinio tinklo perimetre

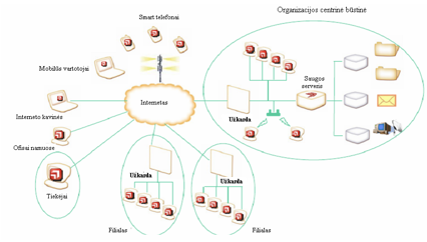
**11**. Kodėl šiuolaikinėms sistemoms vis mažiau tinka perimetrinė apsauga?

Teisingas atsakymas yra: Tai sąlygoja nauji komunikacijų būdai..

**12**. Kuris teiginys **netinka**, apibrėžiant giluminę apsaugą ?

Teisingas atsakymas yra: Tai situacija, kai saugos priemonės taikomos tik galiniuose vartotojų kompiuteriuose..

Giluminės (defense in depth) saugos principas: Duomenys; Taik.programos;Kompiuteris;Vidinis tinklas;Perimetras;Fizinė sauga



Kompanijos su laiku turės vis daugiau sistemų, kurios nebus tiesiogiai sujungtos su pagrindiniu tinklu ir apsaugot juos vien perimetro apsauga jau dabar darosi sunku. Naudojamas šifravimas, saugūs komunikavimo protokolai, saugios kompiuterinės sistemos, autentifikacija.

**13**. Ką reiškia galinio taško apsauga?

Tai reiškia, kad turi būti saugomas ne tik įėjimas į tinklą, bet ir jį sudarant elementai, sustiprinant kiekvieno kompiuterio apsaugą

• Klientams būtinos personalinės užkardos.

• Jas administruoti turėtų organizacijos saugos administratorius.

• Reikia riboti srautus, einančius iš (arba į) nutolusio vartotojo.

• Taikyti mažiausių privilegijų principus.

• Saugos priemones perkelti arčiau saugomų objektų.

Svarbiu momentu užtikrinant saugą yra ir galinio taško – kliento sauga. Klientiniai kompiuteriai turi būti gerai sukonfigūruoti, atnaujinti, neturėti žinomų pažeidžiamumų. Juose turi būti įdiegtos personalinės ugniasienės. Saugi sistema turi sugebėti atlikti „klientinių kompiuterių“ patikrinimą prieš tai, kai jiems suteikiama prieiga prie kritinių resursų.

**14**. Kas yra maršrutizavimas?

Teisingas atsakymas yra: Tai geriausių transportavimo kelių parinkimas.

**15**. Kuriame lygmenyje analizuoja paketus maršrutizatoriai?

Teisingas atsakymas yra: Tinkliniame

Maršrutizatoriai atlieka funkcijas aprašytas– trečiame OSI lygmenyje (**tinklo**). Maršrutizatorius turi atlikti trečio lygio paketo analizę ir parinkti pagal paketo paskirties adresą geriausią galimą maršrutą

**16**. Kam naudojami maršrutizavimo algoritmai?

Teisingas atsakymas yra: Perdavimo kelio nustatymui.

**17**. Kokia informacija remiantis paketas maršrutizatoriaus yra nukreipiamas link gavėjo?

Teisingas atsakymas yra: Paketo gavėjo IP adresu ir informacija iš maršrutizacijos lentelės.

**18**. Kas sąlygoja hierarchinį maršrutizavimą?

Teisingas atsakymas yra: Dideli informacijos kiekiai kuriuos reiktų saugoti kiekvieno maršrutizatoriaus maršrutizavimo lentelėse., Autonominis maršrutizavimo valdymas atskiruose tinkluose.

**19**. Kas tai yra autonominė sistema maršrutizavimo sistemoje?

• AS – tai tinklas, priklausantis vienam administraciniam vienetui.

• AS pasižymi:

• Vieninga administracija

• Ta pati maršrutizavimo politika.

• Maršrutizatoriai, priklausantys tai pačiai AS, vykdo tuos pačius “Intra-AS” (vidinius) maršrutizavimo protokolus.

• Maršrutizatoriai, priklausantys skirtingoms AS gali vykdyti skirtingus vidinius “Intra-AS” maršrutizavimo protokolus.

• Specialiai išskirti maršrutizatoriai vykdo vidinius ( “Intra-AS” ) maršrutizavimo protokolus, bendraudami su kitais maršrutizatoriais iš AS ir yra atsakingi už maršrutizavimą į paskirties vietas, esančias už AS ribų. Šie maršrutizatoriai vykdo išorinius ( *inter-AS* ) maršrutizavimo protokolus, bendraudami su kitais, tos pačios paskirties maršrutizatoriais iš kitų AS. Šio tipo maršrutizatoriai dar vadinami vartų ( gateway) maršrutizatoriais.

**20**. Autonominė sistema -tai...?

Teisingas atsakymas yra: AS tai tinklas, priklausantis vienam administraciniam vienetui.

**21**. Į kokius tipus išsiskiria maršrutizavime naudojami protokolai pagal tai, kur jie yra taikomi?

Dviejų tipų:

– Autonominės sistemos (domeno viduje ) veikiantys protokolai

• RIP - Routing Information Protocol

• OSPF - Open Shortest Path First

• IGRP - Interior Gateway Routing Protocol

– Išorinis, maršruto parinkimą tarp autonominių sričių užtikrinantis protokolas

• BGP - Border Gateway Protocol

**22**. Parenkant maršrutą paketui yra vertinamas ....?

IP paketas, kurio antraštėje yra informacija, reikalinga maršrutui parinkti.

Parinktuvas nustato ar gavėjo adresas yra tame pačiame vietiniame tinkle. Pakete įrašyti siuntėjo ir gavėjo IP adresai nurodo, kad jie priklauso skirtingiems tinklams. Parinktuvas iš kanalo sluoksnio paketo išima IP paketą ir, naudodamasis maršrutų lentele, pagal gavėjo adresą nustato, kokiam kitam mazgui kitame vietiniame tinkle jį reikia perduoti. Suradęs jo MAC adresą, suformuoja naują kanalo sluoksnio paketą ir jį išsiunčia.

**23**. Kokie papildomi reikalavimai kyla parenkant maršrutą bendravimui tarp autonominių sistemų (domenų)

Teisingas atsakymas yra: Saugumo, Politikos, Ekonominiai

**24**. Su kokiomis priežastimis **nėra** susiję BGP pažeidžiamumai?

Teisingas atsakymas yra: Paketų transportavimu

•BGP **yra** pažeidžiama , tai susiję:

–žmogaus klaidomis,

–atakomis,

–konfigūracijos klaidomis.

**25**. Kas sukelia BGP pažeidžiamumus?

Teisingas atsakymas yra: Žmogiškos klaidos, Konfigūracijos klaidos

**26**. Kokiu transporto protokolu naudojasi BGP ?

Teisingas atsakymas yra: TCP

**27**. Kokį maršrutizavimą užtikrina BGP?

Teisingas atsakymas yra: Dinaminį.

**28**. Kuo skiriasi informacija, saugoma Adj-RIBs-In ir Adj-RIBs-Out?

Teisingas atsakymas yra: Adj-RIBs-In saugo informaciją, kuri atėjo iš ASj, o Adj-RIBs-Out saugo informaciją perduodamą ASj.

**29**. Kokia informacija saugoma persiuntimo informacinėje bazėje?

Teisingas atsakymas yra: Tinklo prefiksas ir sekančio šuolio maršrutizatorius.

**30**. Kokia informacija nėra saugoma persiuntimo informacinėje bazėje?

Joje saugomas tinklo prefiksas bei sekančio šuolio informacija. Šioje bazėje yra tik unikalūs keliai, nėra antrinių kelių. FIB dydis sąlygoja paketo persiuntimo greitį.

Teisingas atsakymas yra: Persiunčiami paketai.

**31**. Kokia "Update“ pranešimo paskirtis?

“Update” pranešimai yra naudojami maršruto parinkimo informacijai perduoti tarp pygiaverčių (peer) BGP protokolu veikiančių maršruto parinktuvų. Vienu “Update” pranešimu galima paskelbti vieną naują maršrutą ir atšaukti kelis egzistavusiuosius.

Teisingas atsakymas yra: Atnaujinti maršrutizacijos informaciją..

**32**. Ar apdorojant gautą maršrutizavimo informaciją reikia atsižvelgti į lokalią politiką?

Teisingas atsakymas yra: Taip, nes kiekviename maršrutizatoriuje maršrutizavimo keliai yra palaikomi tie, kurie tenkina jo priimtą politiką..

**33**. Ar maršrutizatoriai yra susiję su paketo konfidencionalumo praradimo grėsme?

Teisingas atsakymas yra: Taip, nes pakeitus maršrutizavimo lenteles galima nukreipti srautą į tuos mazgus, kuriuos valdo atakuotojas..

**34**. Su kokiomis atakomis nesusiduria BGP?

Teisingas atsakymas yra: UDP flooding ataka.

**35**. Koks TCP reset atakos nukreiptos prieš maršrutizatorių tikslas?

• TCP reset -nutraukti tinklo sujungiamumą iki atstatymo, kuris gali užsitęsti.

**36**. Kodėl vietoje TCP RESET yra naudojama ICMP RESET ataka?

ICMP ataka yra paprastesnė.

• ICMP irgi gali sukelti sesijos nutraukimą.

• Siunčiami ICMP pranešimai apie techninės arba programinės įrangos klaidas.

• **Apsaugos priemonės**:

– TCP eilės numerių tikrinimas.

– Maršruto parinktuvų pasiekiamumo kontrolė – blokuojami ICMP 3 tipo paketai su kodais 2,3 ir 4.

– IPSec autentifikacija.

**37**. Kuo skiriasi sesijos perėmimo atakos tikslas nuo TCP reset atakos?

Teisingas atsakymas yra: sesijos perėmimo atakos tikslu gali būti maršrutų pakeitimas.

**38**. Kokiu būdu galima sukelti route flapping tipo ataką?

• „Route flap“ vyksta tada, kai maršrutas yra atšaukiamas ir vėl skelbiamas.

– Maršruto parinktuvas tampa perkrautu.

– Gali kilti arba atsitiktinai arba dėl tendencingos atakos.

**39**. Kodėl gavus labiau specifinį maršrutą gali kilti nestabilumai tinkle?

Teisingas atsakymas yra: Maršrutizatoriai bandys keisti savas lenteles ir skleisti šią klaidinančią informaciją savo kaimynams.

**40**. Kokiu tikslu įterpiami neteisingi maršrutai?

Teisingas atsakymas yra: Siekiant nukreipti paketus kitais keliais

• Įsilaužėlis paskelbia maršrutus ir gali nukreipti paketus tais maršrutais:

– kai įsilaužėlis įgauna priėjimą prie BGP maršrutizatoriaus;

– arba atakuotojas įsiterpia į sesiją.

• **Apsaugos priemonės** :

– maršrutų filtravimas;

– MD5 parašo taikymas.

**41**. Ką daryti su maršrutais, kurie turi nepriskirtus prefiksus?

Teisingas atsakymas yra: Numesti.

**42**. Kokie resursai gali būti išeikvojami?

Teisingas atsakymas yra: Atminties resursai skirti naujiems susijungimams sudaryti bei maršrutizacijos lentelių laikymui..

**43**. Kokiu tikslu yra nutraukiamas ryšys sujungimo nukirtimo atakoje?

Teisingas atsakymas yra: Siekiant nukreipti srautą kitais keliais.

**44**. Kodėl BGP protokolas yra pažeidžiamas SYN FLOODING atakos?

Kadangi BGP remiasi TCP/Ip tai šio tipo ataka irgi gali paveikti maršrutizatorių.

**45**. Kodėl sunku pastebėti nukirtimo ataką?

Maršrutizavimo protokolas suranda aplinkinius kelius ir nutrūkimas lieka nepastebėtas.

## 3. Wi-Fi

**1**. Bevielio ryšio tinklus (WLAN) aprašo IEEE \_\_\_\_\_\_ standartas.

Teisingas atsakymas yra: 802.11.

**2**. IEEE 802.11 standartas aprašo:

Belaidžių tinklų technologiją

Belaidžius tinklus (WLAN) klasifikuoja IEEE 802.11

**3**. Kokie yra pagrindiniai bevielio tinklo komponentai?

Belaidžio tinklo pagrindiniai komponentai:

•Prieigos taškas AP

•Įrenginys turintis belaidžio tinklo adapterį

•Belaidis tiltas

**4**. Bevielio tinklo pagrindiniai kadrų tipai:

Yra 3 pagrindiniai kadrų tipai:

–Valdymo kadrai

–Kontrolės kadrai

–Duomenų kadrai

**5**. Kuris (-ie) iš išvardintų standartų Europoje nenaudojamas(-i)?

Pagal skaidres 802.11a, bet realiai Google rašo, kad jau naudojamas ir Europoje 😊

**802.11j - standartas skirtas Japonijai ir praplečia 802.11a papildomu 4,9 GHz dažnio kanalu**

**6**. Sukūrus WEP protokolą buvo numatytas \_\_\_\_ bitų rakto ilgis.

Teisingas atsakymas yra: 40.

**7**. Kokį šifravimo algoritmą naudoja WEP ir koks didžiausias palaikomas rakto ilgis?

–**RC4 šifravimo algoritmas** ir XOR operacija

–Prieigos taškas gali turėti 4 bendro naudojimo raktus (40 **arba 104 bitų ilgio**)

–Naudojamas iniciacijos vektorius (IV)

•Prie rakto pridedamas 24 bitų iniciacijos vektorius

•Iniciacijos vektoriaus pagalba sukuriamas kintantis šifravimo raktas

WEP šifruoti naudojamas RC4 šifravimo algoritmas. 26 simboliai (104 bitų šifravimo raktas ir 24 bitų iniciacijos vektorius (šifruoti naudojami 128 bitai).

**8**. Kokia galima didžiausia teorinė tinklo sparta naudojant 802.11b standartą?

Teisingas atsakymas yra: 11 Mbps.

**9**. Kuri ryšio grandis bus apsaugota naudojant WEP?

Teisingas atsakymas yra: Klientas-prieigos taškas..

**10**. ACL (Access list) mechanizmas paremtas:

Teisingas atsakymas yra: Leidžiamų MAC adresų sąrašo sudarymu..

**11**. Bevielis tinklas identifikuojamas pagal \_\_\_\_\_\_\_.

Teisingas atsakymas yra: SSID

**12**. Žinant SSID galima:

Teisingas atsakymas yra: Prisijungti prie bevielio tinklo..

Sužinoti prieigos taško konfigūracijos duomenis, informaciją apie galimą duomenų perdavimo spartą, SSID ir naudojamą kanalą, įrangos gamintoją

SSID transliavimas belaidį tinklą padaro lengvai aptinkamą ne tik vartotojams, kurie juo naudojasi, bet ir įsilaužėliams. Jei būtų uždrausta transliuoti SSID (prieigos taške išjungiamas SSID transliavimas), tinklas saugesnis netaptų, jis tik būtų sunkiai aptinkamas.

**13**. Norint prisijungti prie bevielio tinklo reikia:

Klientas, norėdamas prisijungti prie įrenginio (AP - Access Point), siunčia paketą su AP SSID, o jį gavęs AP išsiunčia autentifikavimo atsakymo (patvirtinimo) paketą, jei gautasis SSID atitinka AP SSID. Visas atvirojo rakto autentifikavimo procesas yra atliekamas atviruoju tekstu (nešifruotu

Žinoti SSID ir slaptažodį (raktą).

**14**. WEP protokole šifravimui naudojamas:

Teisingas atsakymas yra: Raktas ir iniciacijos vektorius..

**15**. WEP protokole šifravimui naudojama \_\_\_ loginė operacija.

Teisingas atsakymas yra: XOR.

**16**. WLAN saugumo užtikrinimui gali būti naudojami VPT. Kurie iš šių teiginių teisingi?

Teisingas atsakymas yra: Naudojant PPTP protokolą, yra galimybė įsilaužti į tinklą sužinojus informaciją iš ryšio užmezgimo pirmųjų paketų., Naudojant IPSec protokolą, galimas tik statinis maršrutizavimas.

**17**. WLAN saugumo užtikrinimui gali būti naudojami VPT. Kurie iš šių teiginių teisingi?

Teisingas atsakymas yra: Naudojant PPTP protokolą, yra galimybė įsilaužti į tinklą sužinojus informaciją iš ryšio užmezgimo pirmųjų paketų., Naudojant IPSec protokolą, galimas tik statinis maršrutizavimas.

**18**. Kurie teiginiai apie IEEE 802.1x saugumo standartą yra teisingi?

Teisingas atsakymas yra: IEEE 802.1x saugumo standartas gali būti naudojamas tiek laidiniuose, tiek bevieliuose tinkluose

Prieigos taškai ir klientai tarpusavyje bendrauja duomenų kadrais

Belaidžių tinklų saugos mechanizmai:

•Atvira autentifikacija

•Bendrojo rakto autentifikacija

•WEP (Wired Equivalent Privacy)

•WPA (Wi-Fi Protected Access)

•802.1x

•802.11i

Duomenys belaidžiu tinklu perduodami radijo bangomis skleidžiant signalus, ir tai potencialiems įsilaužėliams suteikia daugiau galimybių perimti duomenis ir juos valdyti.

Dėl netinkamo belaidžio tinklo konfigūracijos nustatymo ar paviršutiniškos priežiūros įsilaužėliai gali nepastebėti naudotis įmonės ištekliais (internetu, prieiti prie darbuotojų ar įmonės failų) ar net perimti viso tinklo valdymą.

Dažna problema tampa ir belaidžių tinklų įrangos gamyklinės nuostatos (settings), kurios nėra pritaikytos aukštiems saugumo reikalavimams.

**19**. Kurie teiginiai apie tarpinio žmogaus ataką bevieliuose tinkluose teisingi?

Teisingas atsakymas yra: Tarpinio žmogaus ataka galima, dėl to kad tik klientas turi autentifikuotis prieigos taškui., Atakuotojas įsilaužia modifikuodamas EAP-success pranešimą siunčiamą iš prieigos taško klientui.

MITM (Man-in-the-Middle) „įsiterpusio žmogaus“ ataka gali būti atliekama dviem tikslais: siekiant slaptai nuskaityti duomenis arba modifikuoti tinklu siunčiamus duomenis prieš jiems pasiekiant gavėją. Tarpinio žmogaus ataka galima dėl to, kad tik klientas turi autentifikuotis prieigos taškui. Atakuotojas įsilaužia modifikuodamas EAP-success pranešimą, siunčiamą iš prieigos taško klientui.

**20**. Kurie teiginiai apie sesijos perėmimo ataką teisingi?

IEEE 802.1x saugumo standartas neapsaugo nuo sesijos perėmimo atakos

Atakuotojas, norėdamas pasinaudoti tinklo prieiga, ryšio sesiją perima siųsdamas „disassociate“ pranešimą klientui.

**21**. Silpniausią saugumą teikia:

Teisingas atsakymas yra: WEP.

**22**. Kurie teiginiai apie TKIP protokolą neteisingi?

•TKIP (Temporal Key Integrity Protocol)

–Naujas raktas generuojamas kas 10000 paketų arba 10 KB

**23**. Kurie protokolai bevieliuose tinkluose naudojami autentifikacijai?

Teisingas atsakymas yra: EAP, MS-CHAP2

**24**. Kokia funkciją atliekas bevieliuose tinkluose atlieka RADIUS serveris?

Teisingas atsakymas yra: Vartotojų autentifikacijos..

**25**. Kurie teiginiai apie VPT naudojimą bevieliuose tinkluose teisingi?

**26**. Ar VPT naudojimas bevieliame tinkle įtakoja duomenų perdavimo spartą?

Teisingas atsakymas yra: Taip..

**27**. Kurie teiginiai apie IEEE 802.11i saugumo standartą teisingi?

Teisingas atsakymas yra: IEEE 802.11i saugumo standartas išsprendžia visas žinomas saugumo problemas anksčiau naudotuose bevielių tinklų saugumo standartuose., 802.11i kitas pavadinimas yra WPA2., Ankstesniuose saugumo standartuose naudotas RC4 šifravimo algoritmas keičiamas į AES.

**28**. Kuriais iš išvardintų įrenginių gali pasinaudoti atakuotojas.

Teisingas atsakymas yra:

* Nešiojamas kompiuteris.,
* Stacionarus kompiuteris.,
* Delninis kompiuteris.,
* Mobilus telefonas.

**29**. Kurie(-is) iš išvardintų programinių paketų gali būti naudojami prieigos taškų aptikimui?

Network Stumbler, MiniStumbler, Wellenreiter

**30**. Kurie(-is) iš išvardintų programinių paketų gali būti naudojami bevielio tinklo auditui?

Paketas su AP SSID

Nešifruoto teksto paketas

NetStumbler (Network Stumbler), MiniStumbler, Kismet.  
 AirSnort, WepCrack.  
 Pavyzdžiui, Kismet aptinka pageidaujamą tinklą ir sužino apie jį reikalingą informaciją, Airsnort surenka paketus, o AirCrack suranda WEP raktą.

Šiais įrankiais naudojasi ne tik tinklo administratorius, norėdamas įvertinti savo tinklo saugumą, bet ir įsilaužėliai. Minėti įrankiais padeda patikrinti esamą tinklo saugumo būklę.

**31**. Kurie(-is) iš išvardintų įrankių gali būti naudojami bevieliu tinklu siunčiamų paketų surinkimui?

Teisingas atsakymas yra:

* AirSnort,
* AirCap,
* Kismet

**32**. Kuriais(-iuo) įrankiais naudojantis galima išsiaiškinti bevieliame tinkle naudojamą standartą?

Teisingas atsakymas yra: NetStumbler, Kismet

**33**. Kurie(-is) iš išvardintų įrankių gali būti naudojami surinktų paketų analizei?

–Kismet

–Tcpdump

**34**. Kurie teiginiai apie bevielius tinklus teisingi?

Teisingas atsakymas yra: Bevieliai tinklai yra labiausiai pažeidžiami DoS atakų., AP aprėpties zonoje nepavyks visiškai užkirsti kelio Dos atakai.

**35**. WEP rakto nulaužimui gali būti panaudota ši programinės įrangos kombinacija:

Teisingas atsakymas yra: AirSnort, AirCrack, Kismet

**36**. NetStumbler programinė įranga gali:

Teisingas atsakymas yra: Nustatyti bevielių tinklų buvimą., Nustatyti ar WEP yra įjungtas/išjungtas., Užfiksuoti SSID, signalo stiprumą, kanalo numerį.

**37**. NetStunbler programinė įranga negali:

Teisingas atsakymas yra: Nulaužti WEP raktą., Surinkti bevieliu tinklu siunčiamus paketus., Įvykdyti bet kokio tipo kenkėjišką ataką.

**Gali:**

**„Windows“** operacinėje sistemoje **surenka informaciją apie belaidžius tinklus**;

Šį įrankį galima naudoti **nustatant belaidžio tinklo konfigūraciją**, taip pat **patikrinti prieigos taško aprėpties zoną**, aptikti **suklastotus prieigos taškus**, „**wardriving**“. Taip pat ši programinė įrangą turi MiniStumbler versiją, pritaikyta delninukams su „Windows“ CE operacinėmis sistemomis.

Negali: Surinkti tam tikru belaidžio ryšio kanalu siunčiamus paketus, nustatyti WEP raktus.

**38**. Kismet programinė įranga gali:

Teisingas atsakymas yra: Nustatyti bevielių tinklų buvimą., Nustatyti ar WEP yra įjungtas/išjungtas., Užfiksuoti SSID, signalo stiprumą, kanalo numerį., Surinkti bevieliu tinklu siunčiamus paketus.

**39**. Ar SSID transliavimo uždraudimas užtikrins SSID slaptumą?

Teisingas atsakymas yra: Ne..

**40**. Ar bevielio tinklo prieigos taško signalo stiprumo sumažinimas gali turėti įtakos tinklo saugumui?

Teisingas atsakymas yra: Taip.

**41**. Kurie iš išvardintų veiksmų padidintų bevielio tinklo saugumą?

Teisingas atsakymas yra:

* Išjungti SSID transliavimą.,
* Išjungti DHCP paslaugą.,
* WEP protokolą pakeisti WPA protokolu.

**42**. Kurie iš išvardintų veiksmų gali **sumažinti** bevielio tinklo saugumą?

Belaidžio tinklo saugumo **padidinimo** taisyklės:

•WEP protokolą pakeisti WPA protokolu

•Išjungti SSID transliavimą

•Išjungti DHCP paslaugą

•Tinkluose, kur belaidžio tinklo dalis gali būti pakeičiama, jos atsisakyti ir naudoti laidinį tinklą, kuris yra saugesnis ir patikimesnis

•Naudoti papildomus aparatūrinius įrenginius belaidžio tinklo saugumui užtikrinti

**43**. Atakuotojai, kurie laužiasi į bevielius tinklus vadinami:

Teisingas atsakymas yra: Wardrivers.

**44**. Kurie patarimai norint išvengti bevielio tinklo saugumo problemų yra teisingi?

Teisingas atsakymas yra: Jei bevielis tinklas nėra būtinas, jo atsisakyti ir naudotis laidiniu tinklu., Naudoti papildomus aparatūrinius įrenginius bevielio tinklo saugumui užtikrinti.

•WEP protokolą pakeisti WPA protokolu

•Išjungti SSID transliavimą

•Išjungti DHCP paslaugą

•Tinkluose, kur belaidžio tinklo dalis gali būti pakeičiama, jos atsisakyti ir naudoti laidinį tinklą, kuris yra saugesnis ir patikimesnis

•Naudoti papildomus aparatūrinius įrenginius belaidžio tinklo saugumui užtikrinti

**XX.**

WEP ataka gali būti atliekama naudojant siunčiant prie belaidžio tinklo prisijungusiai „aukai“ žinomo turinio pranešimus (pvz., elektroninį laišką, užpildytą tarpo simboliais).

Prieš naudojant Aircrack programą reikia:

Nustatyti belaidžių tinklų buvimą (pvz., su *Kismet* programa).

Surinkti belaidžiu tinklu siunčiamus paketus (pvz., su *Kismet arba* AirSnort programomis).

**45.** Kurie(-is) iš išvardintų programinių paketų gali būti naudojami automatiniam prieigos taškų aptikimui, tą įrankį vežiojant skirtingose teritorijose?

Teisingas atsakymas yra: NetStumbler.

## 4. IPS

**1**. Kas gali sukelti atakas?

Atakų sukėlėjai gali būti tiek vidiniai, tiek išoriniai vartotojai.

Išoriniai piktavaliai vartotojai – įsilaužėliai (hacker) – puola tinklus, atakuodami iš interneto. J

Vidiniai tinklo vartotojai – autorizuoti vartotojai (turintys teisę atlikti tam tikrus veiksmus tinkle). Jie dažnai atakuoja siekdami įgyti papildomų privilegijų

Įsilaužėlius galima suskirstyti į kelias kategorijas: smalsuolius, mėgėjus ir profesionalus.

Smalsuoliai dažniausiai turi žemą įsibrauti reikalingą kvalifikaciją, naudojasi kitų išbandytais metodais ir priemonėmis (internete rastais atakų pavyzdžiais)

Mėgėjams įsibrovimai yra pomėgis: laisvalaikiu jie kelia savo kvalifikaciją, sunkumai jiems yra iššūkis. Profesionalūs įsilaužėliai pasižymi aukšta kvalifikacija ir ilgamete patirtimi. Jiems įsibrovimai yra pasipelnymo šaltinis, todėl užsibrėžto tikslo (jei tai atneš naudos) bus siekiama metodiškai, negailint nei laiko, nei pinigų

**2**. Kas nėra traktuojama kaip įsilaužimas?

Teisingas atsakymas yra: Naudojimasis tinklo teikiamom paslaugomis..

Įsilaužimas – tai bet kokie veiksmai, kurių tikslas pakenkti duomenų vientisumui, konfidencialumui ar prieinamumui. Tačiau reikia nepamišti, kad tie patys veiksmai įvairiuose tinkluose gali būti traktuojami skirtingai, pvz., viename tinkle yra laisvas priėjimas prie FTP serverio, o kitame tinkle ši paslauga gali būti tiekiama tik autorizuotiems vartotojams. Tai lemia kiekvieno konkretaus tinklo saugos politika, kuri numato, kokios paslaugos kokiai vartotojų grupei teikiamos ir kitus darbo tinkle principus [1, 5].

**3**. Jei tinklo administratorius nėra uždraudęs naudotis FTP paslauga, ar naudojimasis ja iš išorės bus traktuojama kaip įsilaužimas?

Ne

**4**. Ar gali tinklo sauga būt patikėta tik ugniasienei?

Teisingas atsakymas yra: Negali, reikalingi ir kiti saugos elementai

**5**. Ar gali tinklo sauga būt patikėta tik ugniasienei?

Teisingas atsakymas yra: Negali, reikalingi ir kiti saugos elementai

**6**. Kas nepriklauso prie tinklo saugos elementų?

**Priklauso** firewall, įsilaužimus aptinkančios, apsaugančios, antivirusinės programos.

**7**. Kiekvienas saugai skirtas įrankis gali būti vertinamas pagal tai, kaip jis atsižvelgia į ....?

Teisingas atsakymas yra: Informacijos: vientisumą, konfidencionalumą, pasiekiamumą..

**8**. Kas nėra atakos požymiu?

Yra:

• Kai kurių įvykių **pasikartojimas**.

• **Neteisingos** komandos arba einamos situacijos neatitinkančios komandos.

• **Pažeidžiamumų** išnaudojimas.

• Netinkami tinklo srauto **parametrai**.

• Nenumatyti **atributai**.

• **Nepaaiškinamos** problemos.

Pavyzdžiai:

– Vartotojas eilę kartų bando įvesti neteisingą slaptažodį.

– Bandoma prisijungti prie eilės prievadų nedideliame laiko intervale.

– Atsiunčiami tendencingai blogi parametrai.

– Pažeidžiama normali pagal tam tikrą protokolą numatyta veiksmų seka.

**9**. Kada galima teigti, kad įvykių pasikartojimas rodo atakos požymius?

Teisingas atsakymas yra: Kai jie viršija tam tikras slenkstines reikšmes.

**10**. Vykstant TCP susijungimui, pirmu paketu turi būti SYN paketas, tačiau atsiunčiamas FIN paketas. Koks tai būtų atakos požymis?

FIN flood / FIN skenavimas

**11**. Kas kelias sekundes fiksuojamas prisijungimo bandymas į įvairius kompiuterio prievadus. Koks tai atakos požymis?

Teisingas atsakymas yra: Kai kurių įvykių pasikartojimas..

**12**. Iš tinklo išorės į ugniasienę ateina paketai, kurių gavėjo adresais nurodyti vidiniam tinkle nenaudojami IP adresai. Koks tai atakos požymis?

„IP spoofing“ – tai aukšto lygio interneto ataka. Yra dvi rūšys: „aklas“ ir „neaklas“ „spoofing“. „Neaklas“ – tai, kai pro tavo kabelį keliauja IP paketai (pvz., LAN). Jis daug paprastesnis nei „aklas“ „spoofing“, todėl jo neaptarinėsime.

**13**. Kuriose iš išvardytų situacijų reiktų įtarti, kad vyksta ataka?

Teisingas atsakymas: Autentifikuotas vartotojas įvedinėja vis kitokį neteisingą slaptažodį.

Teisingas atsakymas yra: Vartotojas bando prisijungti administratoriumi ir įvedinėja vis kitokį neteisingą slaptažodį..

**14**. Kuriose iš išvardytų situacijų reiktų įtarti, kad vyksta ataka?

Teisingas atsakymas: Autentifikuotas vartotojas įvedinėja vis kitokį neteisingą slaptažodį.

Teisingas atsakymas yra: Vartotojas bando prisijungti administratoriumi ir įvedinėja vis kitokį neteisingą slaptažodį..

**15**. Kas tai yra grėsmė?

**Grėsmė** -tai galimų, tendencingai kenksmingų veiksmų potencialas.

**Grėsmių sukėlėjai** – žmonės, žmonių grupės, gamtos, politiniai, ekonominiai ir socialiniai reiškiniai, galintys kelti grėsmę informacinių vertybių saugumui.

**16**. Kas sąlygoja atakas ir jų sėkmę?

Teisingas atsakymas yra: Motyvacija, aplinkybės, ištekliai., Atakuotojo turimi įrankiai., Palanki situacija.

**17**. Žmogus rado Internete atakai skirtą programą ir pabandė ja pasinaudoti. Kuriai atakuotojų kategorijai jį priskirtume?

**Smalsuolis**

*Kategorijos: Smalsuolis (bando), Megejas (kelia kvalifikacija), Profesionalas (kvalifikuotas)*

**18**. Kurios iš išvardytų priemonių tiesiogiai negalima priskirti prie priemonių, nukreiptų prieš atakas?

Teisingas atsakymas yra: Maršrutizatoriai.

**19**. Kokio tipo IDS galės fiksuoti ataką, jei staiga nebelieka vietos serverio diske?

Teisingas atsakymas yra: Aptinkančios anomaliją

**20**. Kokio tipo IDS galės fiksuoti ataką, jei staiga nebelieka vietos serverio diske?

Tas pats kl. 19

**21**. Kuriuos veiksmus realizuoja ne visos IDS?

Atlikti tyrimo neįsikišus žmogui

*Dauguma IDS automatiškai reaguoja į atakas, tačiau norint visapusiškai jas išnagrinėti (ypač naujas atakas), reikia administratoriaus*

**22**. Atpažinti naują ataką gali..... IDS?

Teisingas atsakymas yra: Aptinkančios anomaliją.

**23**. Tinklinės įsilaužimo aptikimo sistemos seka .....?

Teisingas atsakymas yra: Srautų charakteristikas

**24**. Tinklinės įsilaužimo aptikimo sistemos seka .....?

Tas pats kl. 23

**25**. Sistemos vientisumo tikrintojai seka ...?

Teisingas atsakymas yra: Pasikeitimus failų sistemose

**26**. Kokiam tikslui yra kaupiami log failų įrašai?  
Užpuolimo atveju, kad būtų galima atsekti užpuoliką ir kitą aktualią informaciją.

***Audito analize*** besiremiančios sistemos nagrinėja surinktus duomenis periodiškai arba realaus laiko režime ir gali:

•nustatyti sistemos būvį ir nuspręsti ar nevyksta įsilaužimas,

• identifikuoti kaip vyko ataka, identifikuoti atakuotoją.

**27**. IDS renka informaciją apie vykstančius įvykius sistemoje tikslu....?

Teisingas atsakymas yra: Identifikuoti įsilaužimą..

**28**. Kokia "medaus statinių" paskirtis?

Teisingas atsakymas yra: Įvilioti atakuotoją

**29**. IDS renka informaciją apie vykstančius įvykius sistemoje tikslu....? 27

**30**. Su kokiomis problemomis susiduria IDS, kurios remiasi audito analizės duomenimis?

Audito analizės problemos:

–Kokius duomenis kaupti,

–Saugojimo problema.

Jei sukaupta mažai duomenų, įsilaužimas gali likti neužfiksuotas.

**31**. Kokiu privalumu pasižymi IDS, kurios remiasi audito analizės duomenimis?

Teisingas atsakymas yra: Analizės galimybe po įsilaužimo.

**32**. IDS pagal taikomą atakų aptikimo metodą skirstomos į:

Teisingas atsakymas yra: Anomalijų aptikimo ir panaudojimo piktam aptikimo sistemas..

**33**. Anomalijas aptinkančių sistemų darbas remiasi....?

Sistemos ir vartotojiškais profiliais.

**34**. Kas nėra įtraukiama nusakant tipinių vartotojų darbo profilius?

Teisingas atsakymas yra: Vartotojų identifikaciniai duomenys..

**35**. Kas nėra įtraukiama į sistemos darbo profilį?

Teisingas atsakymas yra: Sistemos struktūra..

**36**. Anomalijos detektoriai pastoviai seka .....

Teisingas atsakymas yra: Elgsenos nukrypimus nuo normalaus profilio.

**37**. Anomalijos nustatymas naudojant neuroninius tinklus grindžiamas siekiu ....?

Teisingas atsakymas yra: Išmokyti nuspėti sekantį veiksmą ar komandą pagal n ankstesnių veiksmų ar komandų..

**38**. Dauguma komercinių IDS produktų yra pagrįsti ....?

Srauto analize ieškant gerai žinomų atakų pavyzdžių.

**39**. "Misuse detection" sistemos gali aptikti daugumą ar visas žinomas atakas, bet jos mažai tinka ....?

Naujoms ar nestandartinėms (mažai naudojamoms) atakoms aptikti?

**40**. IDS pagal saugomą objektą skirstomos į ....?

Teisingas atsakymas yra: Orientuotas į atskiro tinklo mazgo (hosto) apsaugą bei į tinklo apsaugą.

**41**. Kuris teiginys netinka HIDS sistemoms?

Teisingas atsakymas yra: HIDS analizuoja tinklo srautus..

**42**. Kuris iš paminėtų privalumų nėra HIDS privalumas?

Teisingas atsakymas yra: Gali pastebėti tinklo skenavimo atakas, surištas su tinklo kompiuteriais

HIDS privalumai:

stebi įvykius, vykstančius konkrečiame kompiuteryje,

nustato, ar ataka sėkminga,

gali tirti šifruotą srautą,

Fiksuoja vartotojo prisijungimus, priėjimą prie failo, failų sistemos vientisumą

**43**. Kuris iš paminėtų teiginių nėra HIDS trūkumas?

Trūkumai:

negali aptikti tinklo skenavimo ar kitų pažeidimų

Įsilaužus į kompiuterį, visa surinkta informacija gali būti sugadinta

veikla gali sutrikti DoS atakų metu

mažina kompiuterio operacijų vykdymo spartą

**44**. Kuris teiginys, liečiantis NIDS nėra teisingas?

Privalumai:

Praneša apie įtartinus įvykius tinkle

galima tiksliau atpažinti anomalijas

reikia nedaug tinklo išteklių

identifikuoti įvairias adresų pakeitimo (spoofing) atakas

Sunkiai aptinkama įsilaužėlių

gali aptikti prievadų skenavimą, tikrinti, ar nekenksmingi paketai įvairiuose privaduose

**45**. Kuris nurodytas NIDS trūkumas nėra teisingas?

Trūkumai:

sunkiai valdo tinklus su perjungikliais (switches)

negali analizuoti šifruotų duomenų

negalinustatyti,ar ataka buvo sėkminga

nepajėgia tinkamai analizuoti fragmentuotų paketų

NIDS susiduria su sunkumais, kai srautas yra apsaugomas IPSec, SSL,SSH protokolais

**46**. Kuris teiginys, liečiantis papildomas priemones naudotinas kartu su IDS **nėra teisingas**?

**Teisingas teiginys**:

Papildomos apsaugos priemonės įdiegiamos į pačias taikomąsias programas.

**47**. Atakų atvejui turi būti numatyti tam tikri atsakai. Kuris iš nurodytų veiksmų nėra tiesiogiai susijęs su atakomis?

Teisingas atsakymas yra: Vietinio tinklo atjungimas nuo interneto.

**47.1**. Atakų atvejui turi būti numatyti tam tikri atsakai. Kuris iš nurodytų veiksmų NĖRA priskiriamas prie gerų gynybinių priemonių?

Teisingas atsakymas yra: Vietinio tinklo atjungimas nuo interneto.

**48**. Kodėl IDS dar vadinamos pasyviomis sistemomis?

Nes jos tik renka informaciją, bet nesiima veiksmų, veiksmų turi imtis sistemos administratorius atsižvelgdamas į gaunamus duomenis

**49**. Kuo skiriasi pasyvios ir aktyvios IDS?

Pasyviosios IDS aptinkaataką irskelbia aliarmą. Kai aptinkama atakos požymių, sukuriami aliarmo pranešimai ir siunčiami sistemos administratoriui ar vartotojui.

Aktyviosios IDS ne tik aptinka ataką ar netinkamą srautą ir praneša administratoriui, bet ir imasi veiksmų. Paprastai blokuojamas, nutraukiamas tinklinis srautas, ateinantis iš atakos šaltinio, IP adreso ar vartotojo

50. Kokiam tikslui yra kaupiami log failų įrašai IPS sistemose?

Teisingas atsakymas yra: Įsilaužimo pėdsakų aptikimui.

Kuo skiriasi pasyvios IDS ir IPS (aktyvios IDS) ?

Teisingas atsakymas yra: Aktyvios IDS (IPS) bando nutraukti ataką..

6. VPT

1. Pagrindiniai VPT tipai:

Nuotolinės prieigos VPT

Tarptinklinio sujungimo VPT

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

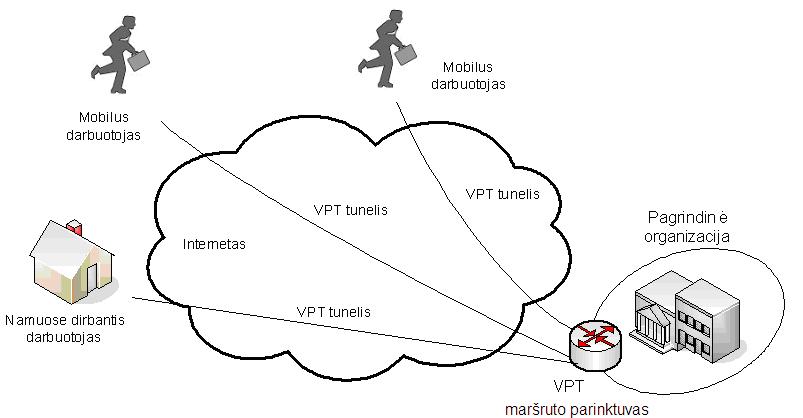
1. Kuri schema teisingiausiai pavaizduoja tarptinklinio sujungimo VPT:

Diagram

Description automatically generated

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Kuri schema teisingiausiai pavaizduoja nuotolinės prieigos VPT



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

4. VPT sujungimų režimai(-as):

Transporto režimas

Tuneliavimo režimas

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Kuri schema teisingai pavaizduoja duomenų įpakavimą naudojant transporto režimą?



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

6. Kuri schema teisingai pavaizduoja duomenų įpakavimą naudojant tuneliavimo režimą?



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

7. Kurie teiginiai teisingi? (Apie tuneliavimo ir transporto režimus)

Naudojant tunelio režimą visas IP paketas yra užšifruojamas, naujam šifruotam paketui suteikiamos naujos antraštės atsižvelgiant į naudojamą šifravimo protokolą.

Pasirinkus šį režimą, speciali konfigūracija reikalinga tik šliuzų įrenginiams (galinių įrenginių papildomai konfigūruoti nereikia).

Numato plėtrą – galima pasirinkti labiau tinkamą įrenginį tunelio procesui vykdyti, neapkraunant kompiuterio procesoriaus nemažai išteklių reikalaujančiu apsaugos procesu.

Sudaro lankstaus darbo sąlygas – praplėsdamas VPT tinklą naujais įrenginiais, esančiais už VPT šliuzo, tad VPT perkonfigūruoti dažniausiai nereikia.

Slepia komunikacijas – esant šiam režimui, įsilaužėlis slapta nuskaitydamas paketus neturės galimybės išsiaiškinti tikrų duomenų perdavimo procese dalyvaujančių įrenginių IP adresus.

Naudoja privatų adresavimą – tikrieji, duomenų perdavimo metu dalyvaujantys įrenginiai, IP adresai gali būti ir viešieji, ir privatūs, nes IP paketai yra įdedami į kitus paketus, ir jiems suteikiama nauja IP antraštė.

Naudoja esamas saugumo priemones (Security Policies) – kadangi įrenginiai turi savo tikruosius IP adresus, nebūtina keisti užkardų įrenginiuose esamų saugumo priemonių.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

8. Kuris teiginys neteisingas (-i)? (Apie VPT naudojamus metodus ir technologijas)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

9. Kuris teiginys teisingas (-i)? (Apie VPT naudojamus metodus ir technologijas)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

10. Kuris teiginys teisingas (-i)? (Apie simetrinius ir asimetrinius raktus)

PEM šifravimui gali naudoti AES algoritmus, o siuntėjo autentifikacijai ir raktų valdymui – RSA

algoritmus. Pagrindiniai PEM naudojami elementai yra šie:

AES šifruoti pranešimai CBC reţimu.

Viešojo rakto valdymas naudojant RSA.

Sertifikato struktūros ir formato nustatymas taikant X.509 standartą.

PEM nebuvo naudojamas taip plačiai, kaip buvo suplanavę jo kūrėjai. Taip atsitiko todėl, kad PEM

Uzţikrina per daug struktūrų skirtingoms aplinkoms, o šioms reikia daugiau lankstumo saugios

komunikacijos infrastruktūroje. [7, 9, 10]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

12. Pažymėkite šifravimo algoritmus:

DES, 3DES, IDEA

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

13. Paketų autentiškumo nustatymas naudojamas:

Duomenų kilmės autentiškumui užtikrinti.,

Pažeistų, pakeistų paketų nustatymui.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

14. Kurie teiginiai teisingi (-as)? (Apie DH algoritmą)

Abu klientai apsikeičia bendra rakto kūrimo informacija (raktų dydžio informacija).

Kai jiems abiem rakto dydis yra žinomas, kiekvienas jų susikuria savo privatų

raktą ir pagal jį padaro viešąjį raktą.

Abu klientai apsikeičia savo viešaisiais raktais.

Kiekvienas klientas savo privačiam raktui ir iš kito kliento gautam viešajam raktui panaudoja DH algoritmą.

Kiekvienas klientas su gautu raktu galės užšifruoti savo informaciją ir iššifruoti gautą informaciją.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

15. Įrenginių autentiškumo nustatymui naudojami:

Daliniai (pre-shared) simetriniai raktai.

Daliniai (pre-shared) asimetriniai raktai

Skaitmeniniai sertifikatai

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

16. Pažymėkite VPT protokolus:

IPSec (Internet Protocol Security)

PPTP (Point-to-Point Tunneling Protocol )

L2TP (Layer 2 Tunneling Protocol )

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

17. IPSec teikia saugumą:

OSI modelio ryšio lygmenyje

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

18. IPSec pagrindiniai komponentai:

a. AH ir ESP protokolai.

c. Raktų valdymo protokolai.

d. Šifravimo ir autentifikacijos algoritmai \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

19. Kurie iš išvardintų rėžimų, nėra IPSec rėžimai?

Teisingas atsakymas yra: Agresyvus režimas., Greitas režimas.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

20. Orginali IP antraštė yra užšifruojama:

Transporto režime

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

21. Saugumo asociacijos (SA):

Apibrėžia, kokios saugumo paslaugos teikiamos kiekvienam vartotojui.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

22. Saugumo asociacijos (SA) naudojamos (-a) duomenų bazės (-ė):

SAD (Security Association Database )., SPD (Security Policy Database).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

23. Išrinkite teisingus teiginius: (apie ESP)

ESP (Encapsulating Security Payload) uţtikrina konfidencialumą, duomenų vientisumą, jų kilmės autentiškumą ir paketų nekartojimo paslaugas. Jeigu gavus ESP paketą jį pavyko sėkmingai atkoduoti, galima tvirtinti, kad paketas siuntimo metu nebuvo atkoduotas (su sąlyga, kad slaptasis seanso raktas yra ţinomas tik abiem bendraujančioms pusėms).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

24. Išrinkite teisingus teiginius: (apie AH)

AH (Authentication Header) teikia duomenų autentiškumo ir paketų nekartojimo paslaugą, bet neuţtikrina duomenų konfidencialumo. Jeigu paketas gautas ir kontrolinės sumos skaičiavimo operacija buvo sėkminga, tada galima tvirtinti, kad abi bendraujančios šalys naudoja tą patį slaptąjį raktą. Tai reiškia, kad paketas buvo siųstas reikiamo siuntėjo. AH kontrolinė suma yra skaičiuojama visam IP paketui.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

25. IKE yra:

Raktų valdymo protokolas

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

26. Kurie teiginiai teisingi? (Apie IKE)

IKE veikia dviem fazėmis. Pirmojoje IKE fazėje bendraujančios pusės viena kitą identifikuoja ir jungiasi į saugų IKE kanalą, skirtą SA uţmegzti. Toliau jos, kad raktai būtų saugūs, suderina šifravimo algoritmus, maišos funkcijas ir autentifikavimo metodus. Pirmosios fazės pabaigoje komunikuojančios pusės generuoja vienodus raktus

Antrosios IKE fazės metu yra uţmezgamas saugos ryšys, skirtas IPSec. Antroji fazė kartojama kas 4-5 minutes. Daţnas šifravimo raktų keitimas apsaugo nuo įsilauţėlių.

IKE protokolas gali veikti 4 reţimais:

1) Pagrindinis reţimas (Main Mode) patikrina ir uţtikrina bendraujančių pusių tapatybes. Šiuo reţimu bendraujančios pusės apsikeičia šešiais pranešimais:

a. du pirmieji pranešimai naudojami bendrai saugumo politikai nustatyti vykstant apsikeitimo procesui;

b. kitais dviem pranešimais apsikeičiama DH raktais ir einamuoju raktu;

c. du paskutiniai paketai reikalingi autentifikuoti komunikuojančias puses, naudojant parašus, kontrolines sumas (taip pat – ir sertifikatus).

2) Agresyvusis reţimas (Aggressive Mode) yra beveik toks pats kaip ir pagrindinis, tačiau apsikeičiama ne šešiais, o tik trimis pranešimais. Todėl šis metodas gerokai greitesnis negu pagrindinis reţimas. Abu šie reţimai priklauso pirmajai IKE fazei.

3) Greitasis reţimas (Quick Mode) priklauso antrajai IKE fazei. Jis naudojamas saugiam ryšiui suderinti su IPSec protokolu. Taip pat šis reţimas gali būti pasitelktas naujiems raktams generuoti.

4) Naujos grupės reţimas (New Group Mode) reikalingas naujai grupei (charakteristikos, reikalingos DH algoritmui) suderinti. Ši grupė nepriklauso nei pirmajai, nei antrajai IKE fazei. Šis reţimas vyksta tarp pirmosios ir antrosios fazių

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

29. PPTP teikia saugumą:

OSI modelio ryšio lygmenyje

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

30. Kurie VPT protokolai veikia 2 OSI modelio lygmenyje?

PPTP, L2TP

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

31. Kurie teiginiai apie PPTP protokolą teisingi?

PPTP atlieka duomenų šifravimą ir glaudinimą., PPTP naudoja PAP autentifikavimo protokolą

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

32. Kurie iš išvardintų objektų yra PPTP komponentai?



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

33. L2TP teikia saugumą:

OSI modelio ryšio lygmenyje

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

34. Kurie iš išvardintų objektų yra L2TP komponentai?

Tinklo prieigos serveris (NAS), L2TP prieigos telktuvas (LAC), L2TP tinklo serveris (LNS)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

35. L2TP naudojami autentifikacijos protokolai:

IPSec standartu

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

36. Kurie teiginiai teisingi (-as)? (Apie PPTP)

PPTP atlieka duomenų šifravimą ir glaudinimą., PPTP naudoja PAP autentifikavimo protokolą

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

37. Kurie teiginiai apie saugumo grėsmes yra neteisingi?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

38. Diffie-Hellman algoritmas gali būti pažeidžiamas naudojant:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

39. Kas iš išvardintų yra PPTP pažeidžiamumai leidžiantys įsilaužėliui atakuoti PPTP protokolu veikiantį VPT tinklą?

GRE (Generic Routing Encapsulation)

Slaptažodžių apsikeitimas autentifikacijos proceso metu

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

40. Kuri iš išvardintų atakų yra efektyviausia naudoti prieš IPSec protokolu veikiantį VPT tinklą?

IPSec realizacijos atakos

Raktų valdymo atakos

Valdymo ir universaliųjų simbolių atakos

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

41. Kurie iš pateiktų pažeidžiamumų aprašymų yra teisingi?

IPSec gali būti pažeidžiamas naudojant tarpinio žmogaus ataką

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

42. VPT – tai:

virtualus privatus tinklas (angl.VPN)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

43. Kas yra VPN tinklas:

Virtual Private network (VPT)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

44. Pagrindiniai VPT tipai:

Nuotolinės prieigos VPT

Tarptinklinio sujungimo VPT

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

45. Kurie iš pateiktų pažeidžiamumų aprašymų yra teisingi?

IPSec gali būti pažeidžiamas naudojant tarpinio žmogaus ataką

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

46. VPT – tai

virtualus privatus tinklas (angl.VPN)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

47. L2TP teikia saugumą

OSI modelio ryšio lygmenyje

Kuri iš išvardintų atakų yra efektyviausia naudoti prieš IPSec protokolu veikiantį VPT tinklą?

Pasirinkite vieną:



a.

Grubios jėgos ataka.



b.

Tarpinio žmogaus ataka.



c.

Duomenų analizavimas.



d.

Paketų pakartojimo ataka.

#### **Grįžtamasis ryšys**

Teisingas atsakymas yra: Grubios jėgos ataka., Tarpinio žmogaus ataka.

## Klausimai iš paskutinės paskaitos “DDoS atakos prieš belaidžius tinklus” tik sausio mėn. Per egzamino testą

1. Koks yra kiekvieno čia pateikto standarto (802.11a, b, g, i, n) pagrindinis apibūdinimas?

2. Koks yra registravimosi į tinklą būsenų ryšys su valdymo kadrais? (Parinkti pavadinimus sunumeruotoms užklausoms)

3. Koks yra registravimosi į tinklą būsenų ryšys su valdymo kadrais? (Parinkti pavadinimą sunumeruotoms būsenoms)

4. Kaip vyksta CSMA/CA sistemos kadrinė komunikacija? (sunumeruokite pažingsniui)

5. Išvengimo lygis – atakos išvengimo arba neutralizavimo sudėtingumas. (Priskirkite išvengimo lygius apibudinimams)

6. Fizinio lygmens atakos veikia visus įrenginius, todėl sukelia daugiausiai žalos. KOKIE BŪNA ŠIŲ ATAKŲ IŠVENGIMAI? (PRISKIRKITE PAVADINIMUS APIBŪDINIMAMS)

7. Kuriuose lygmenyse (pagal open system interconection - OSI modelį ) yra realizuotas 802.11 standartas ?

8. Kokių tipų kadrais operuoja loginė belaidžio tinklo duomenų mainų ir dialogų dedamoji?

9. Kokia valdymo kadrų paskirtis? (Parinkite tris atsakymus).

10. Koks teiginys nėra tinkamas valdymo kadrų paskirčiai apibūdinti?

11. Kokios yra pagrindinės kontrolės kadrų vėlevėlės naudojamos kontroliuoti duomenų kadrų perdavimą?

12. Kokius 3 pagrindinius parametrus nurodo stotis prieš inicijuodama RTS kontrolės kadro siuntimą?

13. Kokie funkciniai polygiai sudaro fizinį lygmenį? Kuris atsakymas yra neteisingas?

14. Fiziniame lygmenyje signalų šablonus apibrėžia polygis, kurios preambulės atributas SYNC sinchronizuoja įrenginius. O ką daro antraštės atributas SFD (start of frame delimiter)?

15. Kurios iš šių atakų priskiriamos prie Fizinio lygmens atsisakymo aptarnauti atakų?

16. Pagal ką skirstomos Fizinio lygmens atsisakymo aptarnauti atakos?

17. Pagal reikalingą energiją, veikimo trukmę ir veikimo sritį skirstomos:

18. Kas būdinga neribotų išteklių atakai?

19. Kokiais aspektais negalima palyginti atsisakymo aptarnauti atakų?

20. Kokiomis strategijomis remiasi kanalinio lygmens atsisakymo aptarnauti atakų išvengimas?

21. Kas būdinga priembulės atakai?

22. Kokio siganlo lygio užtenka preambulės atakai įvykdyti?

23. Kas būdinga konvergencijos žymos atakai?

24. Kokia ataka pavaizduota iliustracijoje? [Paveikslelis]

25. Kas būdinga reaktyviajai atakai?

26. Kokia ataka pavaizduota iliustracijoje? [Paveikslelis]

27. Kas būdinga atsitiktinio trukdžio atakai?

28. Kas būdinga monopolizavimo atakai?

29. Kuomet reaktyviosios atakos metu naudojamas atakos metodas (pvz. SFD ataka)?

30. Kurios iš šių atakų priskiriamos prie Kanalinio lygmens atsisakymo aptarnauti atakų? (Parinkite tris atsakymus).

31. Kokios atakas sudarytos siekiant taupyti atakuojančio įrenginio energiją bei apsunkinti jo radimą? (Parinkite du atsakymus).

32. Kuo remiasi Kanalinio lygmens atsisakymo aptarnauti atakos?

33. Kas būdinga Autentifikacijos (Asociacijos) tvindymo atakai?

34. Kokios yra fizinio lygmens atsisakymo aptarnauti atakos? (Parinkite tris atsakymus).

35. Kurios atakos yra įgyvendinamos dėl to, kad naudojamasi bendru eteriu? (Parinkite du atsakymus).

36. Kurios atsisakymo aptarnauti atakos energijos sąnaudos yra aukštos?

37. Kokios atakos priklauso kanalinio lygmens atsisakymo aptarnauti lygmeniui ?

38. Kas nebūdinga autentifikacijos (Asociacijos) tvindymo atakai?

39. Kas būdinga Deautentifikacijos ir deasociacijos atakai ?

40. Kas būdinga zondavimo tvindymo atakai ?

41. Kas nebūdinga siuntimo atidėjimo atakai ?

42. Kokia belaidžio tinklo standarto 802.11 sparta ?

43. Kas būdinga energijos taupymo režimo Nr.1 atakai ?

44. Kas būdinga energijos taupymo režimo Nr.2 atakai ?

45. Kas būdinga energijos taupymo režimo Nr.3 atakai ?

46. Energijos sąnaudos -...

47. Į kokias dvi strategijas skirtomas atakų išvengimas ?

48. Kuris teiginys teisingas ?

49. Kokiais aspektais galima palyginti atakas?

50. Preambulės atakos energijos sąnaudos ?

51. Koks konvergencijos žymos išvengimo lygis ?

52. Kokią spragą naudoja siuntimo atidėjimo ataka ?

53. Parinkti teisingą atsisakymo aptarnauti atakos apibrežimą.