6. VPT

1. Pagrindiniai VPT tipai:

b. Nuotolinės prieigos

c. Tarptinklinio sujungimo

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

2. Kuri schema teisingiausiai pavaizduoja tarptinklinio sujungimo VPT:

1-oji

Diagram

Description automatically generated

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

3. Kuri schema teisingiausiai pavaizduoja nuotolinės prieigos VPT

2-oji

Diagram

Description automatically generated

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

4. VPT sujungimų režimai(-as):

Teisingas atsakymas yra: PPTP, IPSec, L2TP

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

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

2-oji

Diagram

Description automatically generated

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

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

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

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

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

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

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

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

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

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

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

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

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

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

11. Kuris teiginys teisingas? (Apie simetrinius ir asimetrinius raktus)

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

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

12. Pažymėkite šifravimo algoritmus:

Teisingas atsakymas yra: DES, 3DES, IDEA

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

13. Paketų autentiškumo nustatymas naudojamas:

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

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

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

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

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

15. Įrenginių autentiškumo nustatymui naudojami:

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

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

16. Pažymėkite VPT protokolus:

Teisingas atsakymas yra: PPTP, IPSec, L2TP

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

17. IPSec teikia saugumą:

Kokios apsaugos neteikia IPSec protokolas? Teisingas atsakymas yra: Apsaugos nuo paketo perėmimo

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

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

18. IPSec pagrindiniai komponentai:

Teisingas atsakymas yra:

a. AH ir ESP protokolai.

c. Raktų valdymo protokolai.

d. Šifravimo ir autentifikacijos algoritmai.

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

19. Kurie iš išvardintų rėžimų, nėra IPSec rėžimai?

YRA – transporto ir tuneliavimo

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

20. Orginali IP antraštė yra užšifruojama:

Tunelio režime

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

21. Saugumo asociacijos (SA):

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

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

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

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

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

23. Išrinkite teisingus teiginius: (apie ESP)

ESP – saugaus IP paketo apkrovos įpakavimo protokolą.

ESP protokolas uţtikrina duomenų vientisumą, konfidencialumą (taip pat ribotą srauto kontrolės konfidencialumą), apsaugo nuo seno paketo panaudojimo – tai reiškia, kad protokolas gali uţtikrinti IP paketo sekos numerio tikrumą, tačiau jis negali lemti paketų atėjimo tvarkos.

ESP transporto režime neautentifikuoja originalios IP antraštės laukų

ESP (*Encapsulating Security Payload*) uţtikrina konfidencialumą, duomenų vientisumą, jų kilmės autentiškumą ir paketų nekartojimo paslaugas.

Išrinkite teisingus teiginius:

ESP(Encapsulating Security Payload) suteikia paketų nepakartojamumo savybę

ESP(Encapsulating Security Payload) užtikrina konfidencialumą

ESP šifruoja perduodamą paketą. Kokią saugos charakteristiką tai užtikrina?

Teisingas atsakymas yra: Konfidencionalumą

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

24. Išrinkite teisingus teiginius: (apie AH)

AH protokolas autentifikuoja duomenų šaltinį, uţtikrina duomenų vientisumą, apsaugo nuo seno paketo atkartojimo, gali teikti „negalėjimo paneigti“ apsaugą. AH protokolas negarantuoja duomenų konfidencialumo.

AH – IP autentifikacinės antraštės protokolą,

AH neteikia duomenų konfidencionalumo paslaugos

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

25. IKE yra:

Teisingas atsakymas yra: PPTP, IPSec, L2TP

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

26. Kurie teiginiai teisingi? (Apie IKE)

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

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

27. Kurie teiginiai teisingi? (Apie IKE)

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

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

28. Kurie teiginiai neteisingi? (Apie IKE)

IKE – raktų apsikeitimo protokolą (Internet Key Exchange – IKE

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.

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

29. PPTP teikia saugumą:

PPTP atlieka duomenų šifravimą ir glaudinimą., PPTP naudoja PAP autentifikavimo protokolą

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.

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

30. Kurie VPT protokolai veikia 2 OSI modelio lygmenyje?

Teisingas atsakymas yra: PPTP, L2TP

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

31. Kurie teiginiai apie PPTP protokolą teisingi?

PPTP atlieka duomenų šifravimą ir glaudinimą., PPTP naudoja PAP autentifikavimo protokolą

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.

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

32. Kurie iš išvardintų objektų yra PPTP komponentai?

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

33. L2TP teikia saugumą:

Teisingas atsakymas yra: OSI modelio ryšio lygmenyje

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

34. Kurie iš išvardintų objektų yra L2TP komponentai?

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

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

35. L2TP naudojami autentifikacijos protokolai:

PAP

CHAP

MSCHAP

EAP

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

36. Kurie teiginiai teisingi (-as)? (Apie PPTP)

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

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

37. Kurie teiginiai apie saugumo grėsmes yra neteisingi?

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

38. Diffie-Hellman algoritmas gali būti pažeidžiamas naudojant:

MITM

Teisingas atsakymas :Tarpinio žmogaus ataką

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

39. 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

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

40. Kuri iš išvardintų atakų yra efektyviausia naudoti prieš IPSec protokolu veikiantį VPT tinklą?

paketo perėmimo.

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

41. Kurie iš pateiktų pažeidžiamumų aprašymų yra teisingi?

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

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

42. VPT – tai:

Pagal IETF (*Internet Engineering Task Force*) pateikiamą apibrėžimą virtualusis privatusis tinklas (VPT) (*Virtual Private Network –* VPN) yra platusis tinklas, kuriame naudojamos interneto technologijos ir duomenų perdavimo šifravimas tam tikrai grupei vartotojų atskirti. Jis yra privačiojo tinklo internetinis plėtinys, užtikrinantis apsaugotą nuo kitų vartotojų duomenų perdavimą tarp vartotojų.

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

43. Kas yra VPN tinklas:

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

44. Pagrindiniai VPT tipai:

Teisingas atsakymas yra: Nuotolinės prieigos, Tarptinklinio sujungimo

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

45. Kurie iš pateiktų pažeidžiamumų aprašymų yra teisingi?

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

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

46. VPT - tai

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

47. L2TP teikia saugumą

Teisingas atsakymas yra: OSI modelio ryšio lygmenyje

**-** Kokia komanda naudojama OpenVPN išinstaliavimui (pašalinimui)?

apt-get --purge remove openvpn

**-** Kokia komanda naudojama OpenVPN instaliavimui (įdiegimui)?

apt-get install openvpn

- Kokia komanda (programa) naudojama failo, kuriame yra kliento parametrai redagavimui?

Nano

- Kokia komanda naudojama failo client.conf perkopijavimui į vartotojo darbinį katalogą (kuriame yra vartotojas)?

Teisingas atsakymas yra:

cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf client.conf.

- Kokia komanda naudojama sertifikato prašymo K[5]\_client.csr generavimui?

./build-req K[?]\_client

- Kokia komanda naudojama OpenVPN kliento K[5]\_client paleidimui? Po paleidimo susijungia su OpenVPN serveriu ir sudaromas VPN tunelis.

Teisingas atsakymas yra:

openvpn --config /root/openvpn/client.conf.

- Ką reiškia kiekvienas konfigūraciniame faile client.conf atliktas pakeitimas?

dev tap # Bus naudojamas L2 VPN

;dev tun # Išjungiamas L3 VPN parametras

remote 192.168.0.[nr] 1194 # Nurodomas serverio IP adresas ir prievadas

ca /root/openvpn/ca\_K[nr].crt # Nurodomi reikiami atitinkami keliai iki

cert /root/openvpn/K[?]\_client.crt # reikiamų sertifikatų ir raktų

key /root/openvpn/K[?]\_client.key

tls-auth /root/openvpn/ta\_K[nr].key 1

- Kokios 4 komandos naudojamos OpenVPN ir susijusios konfigūracijos pašalinimui?

apt-get --purge remove openvpn : Išinstaliuoti OpenVPN

openvpn --rmtun --dev tap0 : Pašalinamas virtualus interfeisas

rm -r /root/openvpn : Ištrinami OpenVPN konfigūracijos katalogai

rm -r /root/secret : Ištrinami OpenVPN konfigūracijos katalogai

Kurie iš išvardintų režimų, nėra IPSec režimai?

Teisingas atsakymas yra: Agresyvus režimas., Greitas režimas.

L2TP naudojami autentifikacijos protokolai:

PAP

CHAP

MSCHAP

EAP

Originali IP antraštė yra užšifruojama:

Tunelio režime