

1. Biznes aloqalarini qo'llab-quvvatlaydigan va bulutli provayderlar xizmatlaridan foydalanadigan shaxs yoki tashkilot.

Bulutli iste'molchi (Cloud Consumer)

Bulutli provayder (Cloud Provider)

Bulutli auditor (Cloud Auditor)

Bulutli broker (Cloud Broker)

2. Bulutli xizmatni bulutli iste'molchilarga taqdim etish uchun mas'ul shaxs, tashkilot yoki yuridik shaxs.

Bulutli provayder (Cloud Provider)

Bulutli auditor (Cloud Auditor)

Bulutli broker (Cloud Broker)

Bulutli iste'molchi (Cloud Consumer)

3. Bulutli xizmatlarni mustaqil baholash (baholash), axborot tizimlariga texnik xizmat ko'rsatish, bulutni amalga oshirish samaradorligi va xavfsizligini amalga oshiradigan ishtirokchi.

Bulutli auditor (Cloud Auditor)

Bulutli broker (Cloud Broker)

Bulutli iste'molchi (Cloud Consumer)

Bulutli provayder (Cloud Provider)

4. Bulutli xizmatlardan foydalanish, unumdorlik va yetkazib berishni boshqaradigan hamda bulutli provayderlar va bulutli iste'molchilar o'rtasida aloqalarni o'rnatuvchi tashkilot.

Bulutli broker (Cloud Broker)

Bulutli iste'molchi (Cloud Consumer)

Bulutli provayder (Cloud Provider)

Bulutli tashuvchi (Cloud Carrier)

5. Bulutli provayderlardan bulutli iste'molchilarga bulut xizmatlarini ulash va transport (aloqa xizmatlari) bilan ta'minlovchi vositachi.

Bulutli tashuvchi (Cloud Carrier)

Bulutli auditor (Cloud Auditor)

Bulutli broker (Cloud Broker)

Bulutli iste'molchi (Cloud Consumer)

6. Bulutli texnologiyalarda malumot himoyasini ta'minlashda asosiy metodlar

Huquqiy, Tashkiliy va texnik, Iqtisodiy

Ijtimoiy, Siyosiy

Geografik, Ijtimoiy

Texnik

7. Suqilib kirish turlari nechta

3

4

5

6

8. IDPS nima uchun kerak?

IDPS “chuqurlik” himoya tamoyili bo'yicha qo'shimcha tarmoq xavfsizligini ta'minlaydi

IDPS faqat tarmoq tezligini oshirish uchun ishlatiladi.

IDPS ma'lumotlarni siqish va uzatish uchun foydalaniladi.

IDPS faqat tarmoqdagi foydalanuvchilarni kuzatish uchun mo'ljallangan.

9. Quyidagilardan qaysi biri IDPS (Intrusion Detection and Prevention System)ning funksiyalari hisoblanadi?

Tarmoqdagi shubhali faollikni aniqlash va oldini olish.

Tarmoqdagi foydalanuvchilar sonini ko'paytirish.

Tarmoqdagi ma'lumotlarni shifrlash.

Tarmoq tezligini oshirish.

10. Quyidagilardan qaysi biri IDS (Intrusion Detection System)ning komponentlari hisoblanadi?

Tarmoq sensori, Tarmoq tezligini oshiruvchi tizim, Buyruq konsuli, Javob qaytaruvchi tizim, Hujum imzolari bazasi

Tarmoq sensori, Ogohlantirish tizimi, Buyruq konsuli, Ma'lumotlarni shifrlash tizimi

Tarmoq sensori, Ogohlantirish tizimi, Buyruq konsuli, Javob qaytaruvchi tizim

Tarmoq sensori, Ogohlantirish tizimi, Buyruq konsuli, Tarmoq foydalanuvchilarini kuzatuvchi tizim

11. Bu maxsus dasturiy ta'minot yoki apparat bo'lib, tarmoqni ikkiga bo'lish imkonini beruvchi ko'proq qismlar va belgilaydigan qoidalar to'plamini amalga oshirish tarmoq paketlarini bir qismdan ikkinchisiga o'tkazish shartlarini amalga oshiradi.

Tarmoqlararo ekran (firewall)

VPN (Virtual Private Network)

IDS (Intrusion Detection System)

IPS (Intrusion Prevention System)

12. Tarmoqlararo ekran (firewall)ning asosiy maqsadi nima?

xavfsizlik siyosatini amalga oshirish, axborot almashinuvi masalalarida tashkilotda qabul qilingan tashqi dunyo bilan xavfsiz ma'lumot almashinuvini joriy etishdir.

Xavfsizlik siyosatini amalga oshirish, axborot almashinuvi masalalarida tashkilotda qabul qilingan tashqi dunyo bilan xavfsiz ma'lumot almashinuvini joriy etishdir.

Tarmoqdagi barcha ma'lumotlarni shifrlash.

Tarmoq tezligini oshirish.

Tarmoq foydalanuvchilarini kuzatish

13. TE (Tarmoqlararo ekran) perimetr xavfsizlik tizimi sifatida nechta darajaga bo'linadi?

3 darajaga

5 darajaga

7 darajaga

4 darajaga

14. Virtual xususiy tarmoqlar (VPN) nima maqsadda ishlab chiqilgan?

Umumiy tarmoqlar orqali xavfsiz aloqani ta'minlash uchun.

Foydalanuvchilar sonini ko'paytirish uchun.

Tarmoq tezligini oshirish uchun.

Tarmoqdagi ma'lumotlarni shifrlash uchun.

15. IP manzil translyatsiyasining qaysi turlari mavjud?

Statik va dinamik

Statik va o'zgaruvchan

Dinamik va doimiy

O'zgaruvchan va doimiy

16. Quyidagilardan qaysi biri manzil translyatsiyasining kamchiliklari hisoblanadi?

Ishlash tezligining tushishi, Tashqi tomondan ichki tugunni aniqlash qiyinligi, SNMP va DNS bilan bog'liq muammolar, Ba'zilarini ilovalarni ishga tushirish bilan bog'liq muammolar, Noto'g'ri murojaat qilish ehtimolini oshirish

Tashqi tomondan ichki tugunni aniqlash osonligi, SNMP va DNS bilan bog'liq muammolar, Ba'zilarini ilovalarni ishga tushirish bilan bog'liq muammolar, Noto'g'ri murojaat qilish ehtimolini oshirish, Ishlash tezligining tushishi

SNMP va DNS bilan bog'liq muammolar, Ba'zilarini ilovalarni ishga tushirish bilan bog'liq muammolar, Noto'g'ri murojaat qilish ehtimolini oshirish, Ishlash tezligining oshishi, Tashqi tomondan ichki tugunni aniqlash qiyinligi

Ba'zilarini ilovalarni ishga tushirish bilan bog'liq muammolar, Noto'g'ri murojaat qilish ehtimolini oshirish, Ishlash tezligining oshishi, Tashqi tomondan ichki tugunni aniqlash osonligi, SNMP va DNS bilan bog'liq muammolar

17. Quyidagilardan qaysi biri tarmoqlararo ekran (firewall) turlari hisoblanadi?

Paket filtri yoki ekranlovchi router, Bog'lanish sathi shlyuzi, Ilova sath shlyuzi

Paket filtri yoki ekranlovchi router, DNS server, Ilova sath shlyuzi

Paket filtri yoki ekranlovchi router, Bog'lanish sathi shlyuzi, SNMP agenti

Paket filtri yoki ekranlovchi router, DHCP server, Ilova sath shlyuzi

18. Paketlarni filtrlash quyidagi qaysi ma'lumotlarga asoslanadi?

TCP/UDP - jo'natuvchi va qabul qiluvchi port, Yuboruvchi va qabul qiluvchining IP manzili

Yuboruvchi va qabul qiluvchining MAC manzili, Jo'natuvchi va qabul qiluvchi port

Yuboruvchi va qabul qiluvchining IP manzili, HTTP so'rovi turi

Yuboruvchi va qabul qiluvchining MAC manzili, DNS so'rovi turi

19. Paket filtrlarining afzalliklarini belgilang

Paket kechikishdagi vaqtning kichikligi, Arzon

Tarmoq xavfsizligi oshadi

Paket kechikishdagi vaqtning kattaligi

Ma'lumotlarning shifrlanishi

20. Paket filtrlarining kamchiliklarini belgilang:

Filtrlash qoidalarini tavsiflashda qiyinchilik, Ichki tarmoqning ochiqqligi

Yuqori narx

Xavfsizlik darajasi pastligi

Ma'lumotlar yo'qotilishi

21. .... bu TEda ishlaydigan vositachi dastur va u quyidagi funktsiyalarni bajaradi:

Proksi texnologiyasi

Qo'shimcha ma'lumotlarni saqlash

Tarmoq trafikini shifrlash

Ma'lumotlarni zaxiralash

22. Proksi texnologiyasining vazifalarini belgilang:

Mijozlarning so'rovlarini qabul qilish va tahlil qilish, So'rovlarni haqiqiy serverga yo'naltirish

Tarmoq xavfsizligini oshirish

Ma'lumotlarni siqish

Ma'lumotlarni zaxiralash

23. Ilova sathi shlyuzlari vazifasi nimalardan iborat?

Foydalanuvchi tarmoqlararo ekranda ishga tushirilgan xizmatga ulanishni o'rnatadi, kirish qoidalari xizmat nomi, foydalanuvchi nomi, ish vaqti va boshqalar asosida shakllantiriladi

Mijozlarning so'rovlarini qabul qilish va tahlil qilish, So'rovlarni haqiqiy serverga yo'naltirish

Tarmoq xavfsizligini oshirish

Ma'lumotlarni siqish

24. PROXY texnologiyalarining afzalliklarini belgilang:

Ichki tarmoqning yopiqligi, kuchli autentifikatsiya, oddiy filtrlash qoidalari

Tarmoq xavfsizligini oshirish

Ma'lumotlarni zaxiralash

Yuqori tezlik

25. PROXY texnologiyalarining kamchiliklarini belgilang:

Tashqariga chiqish va ichki tarmoqqa kirishning ikki bosqichli protsedurasi, unumdorlik darajasining pastligi, yuqori narx

Oddiy sozlash

Ma'lumotlarni siqish

Shifrlashning yo'qligi

26. Paket tarmoq sathida tutib olinadi, maxsus modul barcha sathlardagi axborotni tahlil qiladi, ma'lumotlar keyingi tahlil uchun saqlanadi va ishlatiladi. Jarayon qaysi texnologiyaga tegishli?

Stateful Inspection texnologiyasi

Proxy texnologiyasi

VPN texnologiyasi

Tarmoqli xavfsizlik devori

27. Himoya vositasi sifatida TEning kamchiliklari:

Avtorizatsiyadan o'tgan foydalanuvchilardan himoya qila olmaydi, TEni chetlab o'tish ulanishlaridan himoya qilmaydi

Foydalanuvchilarni autentifikatsiya qilmaydi

Ma'lumotlarni zaxiralashda qiyinchiliklar

Yuqori tezlikda ishlamaydi

28. .... mantiqiy tarmoq bo'lib, o'zidan yuqoridagi boshqa tarmoq, masalan, Internet asosida quriladi.

VPN

Proxy

Firewall

NAT

29. Bu tarmoqda kommunikatsiyalarda umumiy xavfsiz bo'lmagan tarmoq protokollaridan foydalanilishiga qaramay, shifrlashdan foydalangan holda, axborot almashinishda begonalarga berk bo'lgan kanallar tashkil qilinadi.

VPN

Proxy

Firewall

NAT

30. Bu tarmoq tashkilotning bir necha ofislarini ular o'rtasida nazorat qilinmaydigan kanallardan foydalangan holda, yagona tarmoqqa birlashtirish imkonini beradi.

VPN

Proxy

Firewall

NAT

**Tekshirish moduli driver sifatida qanday funksiyalarni bajaradi**  
hamma javoblar to'g'ri

Manzil translyatsiyasi , Kirish nazorati

Audit

Mijoz autentifikatsiyasi, Seans autentifikatsiyasi

**Tekshirish modulida tarmoq adapter drayveri necha qisimdan tashkil to'pgan**

- 3
- 4
- 5
- 6

### **Proksi texnologiyasi qanday funksiyalarni bajaradi**

Mijozlarning so'rovlarini qabul qilish va tahlil qilish va serverga joylash

So'rovlarni haqiqiy serverga yo'naltirish

Mijozlarning so'rovlarini qabul qilishi yetarli bo'ladi

Filterlashdan iborat

### **Stateful Inspection texnologiyasining asosiy vazifasi nimadan iborat?**

Trafik paketlarini ulanish holatini kuzatib, xavfsizlikni ta'minlash

Faqat manzillarga asoslangan trafikni filtrlash

Shifrlangan ma'lumotlarni tahlil qilish

Foydalanuvchi faoliyatini kuzatish

### **Stateful Inspection texnologiyasining afzalliklaridan biri nima?**

Trafik paketlarining kontekstini tushunish

Ma'lumotlarni zaxira qilish

Tarmoqni kengaytirish

kirish imkoniyatini ta'minlash

### **IDPS klassifikatsiya necha turga bo'inadi**

- 2
- 3
- 4
- 5

### **IDS ni 1-funksiyasi nima?**

foydalanuvchi va tizim faoliyatini monitoring qilish

fayllar yaxlitligi baholash

hujum modeli

faoliyat izlarini dahlili

### **Tizimga suqulib kirish turlari to'g'ri berilgan qatorni belgilang**

Tizimdagi bo'shliqlar , Tizimni noodatiy ishlashi, Tizim dasturiy ta'minotini va konfiguratsiya

Qalbaki fayllar tasdiqlangan asosiy fayllar bilan mos kelmasligi

Yo'qolgan fayllar

Yo'qotib bo'lmaydigan fayl hajmi o'zgarishi

### **IPS signaturasi nima?**

Taniqli hujumlar yoki zararli harakatlarni aniqlash uchun mo'ljallangan oldindan belgilangan qoidalar to'plami

Tarmoq trafigini shifrlash usuli

Ma'lumotlarni saqlashning bir turi

Foydalanuvchilarni autentifikatsiya qilish usuli

**IPS signaturalarining asosiy vazifasi nimadan iborat?**

Hujum va zararli faoliyatlarni tarmoqda yuzaga kelishidan oldin aniqlash va oldini olish

Tarmoq tezligini oshirish

Foydalanuvchilarga tarmoq manzillarini taqdim etish

Shifrlangan ma'lumotlarni dekodlash

**DHCP ning asosiy vazifasi nima?**

Avtomatik ravishda IP manzillarni ajratadi

Internetga kiradi

Mijoz-server balansini saqlaydi

IPv4 ni IPv6 ga o'zgartiradi

**Qaysi tarmoq topologiyasi mavjud emas?**

Jurnal

Yulduz

Shina

Halqa

**Kompyuterning IP manzilini bilish uchun qanday buyruq ishlatiladi?**

ipconfig

ifconfig

Ipconfig/aal

Show ip address

**Xostlar o'rtasida fayl va ma'lumotlarni almashish uchun qanday protokol ishlatiladi?**

FTP

IP

HTTP

IPX

**Ma'lumotlarni ishonchli yetkazib berilishini ta'minlaydigan transport qatlami protokoli qaysi?**

TCP

UDP

FTP

TFTP

**Global kompyuter tarmog'i:**

WAN

MAN

LAN

PAN

**HTTP protokolini kengaytmasi qaysi javobda to'g'ri keltirilgan?**

Hyper Text Transfer Protocol

High Terminal Transfer Protocol

High Text Tranzit Protocol

Hyper Terminal Tranzit Protocol



**ICMP protokolini kengaytmasi qaysi javobda to'g'ri keltirilgan?**

Internet Control Message Protocol

Intranet Control Message Protocol

Internet Connection Message Protocol

Illegal Control Mail Protocol

**ICMP protokolini kengaytmasi qaysi javobda to'g'ri keltirilgan?**

Internet Control Message Protocol

Intranet Control Message Protocol

Internet Connection Message Protocol

Illegal Control Mail Protocol

**Kompyuter tarmog'ining umumiy geometrik tavsifi:**

Tarmoq topologiyasi

Tarmoq qurilmasi

Tarmoq serveri

Foydalanuvchi tarmog'i

**Troubleshooting nima uchun ishlatiladi?**

Tarmoq xatoliklarini topish uchun

Tarmoqni sozlash uchun

Filtrlash uchun

Testlash uchun

**AAA serveri qaysi vazifalarni bajaradi?**

Authentication, Authorization, Accounting

Authentication, Authorization, Identification

Authentication, Identification, Accounting

Identification, Authorization, Accounting

**Quyidagilardan qaysi biri TACACS versiyasiga kirmaydi?**

TACACS#

TACACS

TACACS+

XTACACS

**Ish stoliga masofadan ruxsat olish protokoli qaysi javobda ko'rsatilgan?**

RDP

FTP

SMTP

HTTPS

**Tarmoqlararo ekran(firewall) – bu:**

avtorizatsiya qilingan ma'lumotlardan tashqari barcha trafikni blokirovka qilish uchun mo'ljallangan tarmoqqa kirishni boshqarish qurilmasi

vazifasi trafikni imkon qadar tezroq manzilga yetkazish bo'lgan qurilma

tarmoq trafigini keshlash qurilmasi

Tarmoq trafigini shifrlash qurilmasi

**Xodim kompyuterining o'g'irlanishi. Bu qanday tahdid turi?**

O'g'rilik

Dasturning buzilishi yoki undagi xatoliklar

Tabiiy ofatlar

Shpionaj

**OSI modelining qaysi qatlamidan boshlanadi?**

Fizik qatlam

Ma'lumotlar bog'lanish qatlam

Tarmoq qatlam

Transport qatlam

**Fizik qatlamdagi asosiy xavf-xatarlardan biri nima?**

Eavesdropping

Denial of Service (DoS)

Replay

Insertion

**Fizik muhit turlaridan qaysi biri simli tarmoq protokoliga kiradi?**

Magistral liniyalar

Simsiz tarmoqlar

Optik tolali tarmoqlar

Dinamik tarmoqlar

**Tarmoq xavfsizligini ta'minlashda qaysi usul dasturiy taroqlaro ekran bilan bog'liq?**

Zararli taroqlarni filtrlaydi

Fizik kanalni boshqaradi

Ma'lumotlarni shifrlaydi

Tarmoq trafikini boshqaradi

**DNS zararlash hujumi nima?**

DNS-serverni soxta ma'lumotlarni haqiqiy deb qabul qilishga aldash

Tarmoqdagi paketlarni o'g'irlash

Xakerlik orqali tizimga kirish

DoS hujumlarini amalga oshirish

**CMP hujumi qanday amalga oshiriladi?**

Xatolarni tekshirish xabarlarini yuborish orqali zaiflikdan foydalanish

DNS-serverni soxta ma'lumotlar bilan zaharlash

Tarmoqdagi paketlarni o'g'irlash

Foydalanuvchi parollarini o'g'irlash

**DoS hujumining asosiy maqsadi nima?**

Serverni soxta mijoz so'rovlari bilan to'ldirib, foydalanuvchilarga xizmat ko'rsatishni to'xtatish

Tarmoqdagi paketlarni o'g'irlash

DNS-serverni zaharlash

Ma'lumotlarni shifrlash

**Port skaneri nima uchun ishlatiladi?**

Nishondagi tizimdagi portlarni skanerlash uchun

Tarmoqdagi paketlarni o'g'irlash uchun

DoS hujumlarini amalga oshirish uchun

DNS zararlash hujumlarini amalga oshirish uchun

**VPN tarmog'ining paydo bo'lishi qachon boshlandi?**

1967-yilda

1969-yilda

1970-yilda

1975-yilda

**VPN tarmog'ining asosiy komponentlaridan biri qaysi?**

Tunneling kommutatori

IP-manzillar

DNS-serverlar

DHCP serverlar

**VPN tarmog'ida autentifikatsiya qanday amalga oshiriladi?**

Taraflarni autentifikatsiyalash orqali

IP-manzillarni tahlil qilish orqali

Ma'lumotlarni shifrlash orqali

Trafikni monitor qilish orqali

**VPN qurishda foydalaniladigan asosiy usul qaysi?**

Marshrutizatorlardan foydalanish

DNS-serverlarni sozlash

Fayl serverlarni konfiguratsiya qilish

DHCP serverlarni sozlash

**OSI modelining ilova sathida ishlaydigan protokollardan qaysi biri to'g'ri keltirilgan?**

HTTP

Physical

Network

Data Link

**Ilova sathining asosiy vazifasi nimani ta'minlaydi?**

Foydalanuvchi darajasidagi dasturiy vositalar bilan ishlashni ta'minlaydi

Fizik darajada paketlarni uzatadi

Tarmoq manzillarini taqsimlaydi

Ma'lumotlarni kodlaydi

**TACACS protokoli qaysi sathda ishlaydi?**

Ilova

Transport

Ma'lumotlar bog'lanishi

Taqdimot

**Ilova sathidagi xavfsizlikka oid muammolardan biri qaysi?**

Ko'pchilik ilova sathi protokollari autentifikatsiyani qo'llab-quvvatlamaydi

Fizik sathdagi paketlarning buzilishi

Tarmoq manzillarini noto'g'ri taqsimlash

O'rta sathda paketlar yo'qotilishi

**ISO OSI modelining qaysi qatlami kanal sathi qatlamidir?**

2-qatlam

3-qatlam

4-qatlam

5-qatlam

**Qaysi protokollar kanal sathi protokollariga kiradi?**

SLIP va PPP

HTTP va FTP

TCP va UDP

ICMP va IP

**Qaysi protokol SLIP zaifliklaridan biri hisoblanadi?**

Authentication

Data Encryption

Firewall Integration

VPN Support

**MAC (Media Access Control) nima bilan shug'ullanadi?**

Uzatishni boshqarish va tarmoq manzilini boshqarish

Ma'lumotlarni kodlash

Qulaylikni oshirish

Ma'lumotlarni saqlash

**OSI modelida fizik sathning asosiy vazifasi nima?**

Jismoniy ommaviy axborot vositalari bilan to'g'ridan-to'g'ri aloqa o'rnatish

Ma'lumotlarni shifrlash va shifrni ochish

Tarmoq topologiyasini boshqarish

Multimediya ma'lumotlarini ishlov berish

**Quyidagilardan qaysi biri fizik muhit turiga kirmaydi?**

Tarmoq to'r (mesh) topologiyasi

Magistral liniyalar

Simli tarmoqlar

Simsiz tarmoqlar

**Fizik sath xavfsizligida ko'p uchraydigan tahdidlardan qaysi biri emas?**

Zararli dasturlar hujumlari

Ma'lumotlarni yoppasiga olish (sniffing)

Ma'lumotlarni takrorlash (replay) hujumlari

Xizmatdan mahrum qilish (DoS) hujumlari

**Fizik tarmoq segmentlarida uzilishlarning asosiy sabablari qaysilar?**

Elektr uzilishlari va uzilgan tarmoq kabellari

Zararli dasturlar hujumlari

Tarmoq qurilmalarining qayta ishlab chiqarilishi

Dasturiy ta'minotdagi xatolar

**PAN nima?**

Personal Area Network

Public Area Network

Private Area Network

Personal And Network

**Qaysi variantda tarmoq arxitekturasini ko'rsatilgan?**

Barchasi to'g'ri

Terminal arxitektura

Bir pog'onali arxitektura

Klent-server arxitektura

**Tarmoq topologiyasi nechta turga bo'linadi?**

4

6

7

10

**Tarmoq protokollarining TCP/IP modeli nechta sathda qo'llaniladi?**

4

5

3

2

**Tarmoqda zararlangan davlat korxonalari, zararlangan umumiy tashkilotlarning necha foizini tashkil qiladi?**

20%

35%

28%

38%

**Xavfli zaifliklar nechta turga bo'linadi?**

5 ta

7 ta

8 ta

10 ta

**Standart tarmoq portlari nechtaga bo'linadi?**

4 ta

3 ta

2 ta

5 ta

**Portning ishlash holatlari qaysilar?**

ochiq, yopiq va bloklangan

maxsus va umumiy

faqat ochiq

aktiv va passiv

**Xavfsizlik siyosati ierarxiyasi nechta pog'onadan iborat?**

7 ta

5 ta

9 ta

3 ta

**Tarmoq xavfsizligi siyosati qaysilar?**

Boshqaruvchi ko'rsatmalar va protseduralar

Standartlar va aloqalar

Portlar va kabellar

maqsad va harakat sohalari

**Qaysi variantda xavfsizlik siyosati afzalligiga kirmaydi?**

Tarmoq xatosi

Risklarni kamaytirish

Muammolarga tezkor javob berish

Xarajatlar kamayishi

**Xavfsizlik siyosati nimalarni qamrab oladi?**

Barchasi to'g'ri

Konfidensallik

Yaxlitlik

Foydalanuvchanlik

31. .... alohida tarmoq xususiyatlarini qamrab olgan, lekin bu tarmoq umumiy foydalanish tarmog'i, masalan, Internet orqali amalga oshiriladi.

VPN

Proxy

Firewall

NAT

32. Tunnelning asosiy komponentlari hisoblanadi qaysilar?

Tashabbuskor, marshrutlanuvchi tarmoq, tunnel kommutatori, bir yoki bir necha tunnel terminatorlari

Tashabbuskor, marshrutlanuvchi tarmoq, tunneling protokollari

Tashabbuskor, tunneling protokollari, firewall

Tashabbuskor, NAT, tunnel terminatorlari

33. Axborotni VPN tuneli bo'yicha uzatilishi jarayonidagi himoyalash quyidagi vazifalarni bajarishga asoslangan:

O'zaro aloqadagi taraflarni autentifikatsiyalash, Uzatiluvchi ma'lumotlarni kriptografik berkitish (shifrlash), Yetkaziladigan axborotning haqiqiylikini va yaxlitligini tekshirish

O'zaro aloqadagi taraflarni autentifikatsiyalash

Uzatiluvchi ma'lumotlarni kriptografik berkitish (shifrlash)

Axborotlarni zaxiralash

34. VPN qaysi xususiyatlariga ko'ra tavsiflanadi?

Amalga oshirish usuliga ko'ra, O'rnatilishiga ko'ra, Himoyalanganlik darajasiga ko'ra

Himoyalalanish darajasiga ko'ra

Tezlikka ko'ra

Foydalanuvchi soniga ko'ra

35. Hujumchilarning motivlarini belgilang:

Mafkura, shuxrat qozonish, pul, kuch qudrat

Professionallik

Tezlik

Xavfsizlik

36. ... bu bitta yoki kompyuter tarmog'iga qaratilgan zararli harakat. .. tajovuzkor foydalanayotgan kompyuterga ta'sir qilmaydi. Tajovuzkor kompyuter yoki tarmoqning xavfsizlik dasturlarida kompyuter yoki tizimga kirish uchun zaif nuqtalarni topadi.

Masofaviy hujum

Lokal hujum

Fizik hujum

Tarmoqli hujum

36. Bunda DNS-serverni soxta ma'lumotlarni haqiqiy va domen egasidan olingan deb qabul qilish uchun aldaydi. Noto'g'ri ma'lumotlar ma'lum vaqt davomida saqlanadi, bu esa

tajovuzkorga domenlar manzillarini so'ragan kompyuterlarga DNS javoblarini o'zgartirish imkonini beradi:

DNS Poisoning

DNS Hijacking

DNS Spoofing

DNS Flooding

37. Bu ma'lumotlar paketlarining kutilayotgan soni haqiqiy sonidan farq qilganda ishga tushadi. Kutilmagan paketlar tugatiladi. Xaker kerakli paketlarni aniq ketma-ket raqam bilan ta'minlaydi:

TCP Desynchronization

TCP Spoofing

TCP Flooding

TCP Hijacking

38. Server, kompyuter yoki tarmoqni foydalanuvchilari va mijozlari uchun soxta mijoz so'rovlari bilan to'ldirib, foydalanishning katta sur'atini taqlid qiladigan usul. Bu foydalanuvchilar o'rtasidagi aloqaga to'sqinlik qiladi, chunki server ko'p miqdorda kutilayotgan so'rovlar bilan band bo'lib qoladi:

DoS

MITM

DDoS

Phishing

39. DoS-hujumlar klassifikatsiyasi qaysilar?

Ping-flood, ICMP-flood, UDP-flood, SYN-flood

HTTP Flood, DNS Amplification, NTP Amplification

SQL Injection, XSS, CSRF

ARP Spoofing, DNS Spoofing, DHCP Spoofing

40. Tarmoqqa ulangan kompyuterlar tomonidan xatolarni tekshirish xabarlarini yuborish uchun foydalaniladigan Internet protokoli:

ICMP

TCP



UDP

HTTP

41. IP manzil bilan ko'rsatilgan portni skanerlash dasturi:

Port skaneri

Packet Sniffer

Vulnerability Scanner

IDS/IPS

42. Port skannerlovchi vositalarni belgilang:

CyberCop Scanner (Pullik), Secure Scanner (Pullik)

Nmap (Pullik), Metasploit (Pullik)

Wireshark (Pullik), tcpdump (Pullik)

Nessus (Pullik), Nikto (Pullik)

43. Kanal sathining Low-Level Protocollarni belgilang:

FDDI, LAPF, PPP, Carrier Sense Multiple Access/Collision Detection

ARP, RARP

STP, RSTP

OSPF, BGP

44. Kanal sathining Middle-Level Protocollarini belgilang:

MAC va LLC

IP, ICMP

TCP, UDP

HTTP, HTTPS

45. Kanal sathining High-Level Protocollarini belgilang:

AppleTalk Address Resolution Protocol (AARP) va the multilink protocol (MP)

DNS, DHCP

FTP, SMTP

POP3, IMAP

46. Tartibsiz rejim hujumlari qaysilar?

Plaintext, Reconnaissance, Hijacking, Detection

Smurf, Fraggle

Teardrop, Land

Ping of Death, SYN Flood

47. Qaysi yillar boshida Xalqaro standartlashtirish tashkilotlari – ISO va xalqaro elektraloqa ittifoqi - ITU-T tomonidan tarmoq rivojlanishida muhim o‘rin tutgan model ishlab chiqdilar?

1980

1970

1990

2000

48. OSI modeli nechta darajadan iborat?

7

5

6

8

49. TCP/IP modelining eng quyi pog'onasi qaysi?

Tarmoq pog'onasi

Ilova pog'onasi

Transport pog'onasi

Internet pog'onasi

50. OSI modelining 6- pog'onasini belgilang

Taqdimot pog'onasi

Tarmoq pog'onasi

Ilova pog'onasi

Transport pog'onasi