|  |
| --- |
| Tarmoq xavfsizligi. Yakuniy savollari  Birinchi variant to’g’ri! |
| “Intellektual mulkni obro’sizlantirilishi” tahdidi turi uchun tahdid namunasini tanlang. |
| Dasturiy ta’minot mahsuloti litsenziyalanmagan yoki mualliflik huquqini buzilgan |
| Yong’inlar, toshqinlar yoki zilzilalar tufayli ma’lumotlarni yo’q qilish yoki yo’qotish |
| Mahsulot ishlab chiqarish jadvalini o’g’irlash |
| Pochta xodimi tomonidan xatlarni noqonuniy o’qish |
| Sabotaj tahdidi turi uchun tahdid namunasini tanlang. |
| Buzg’unchi fayllarni o’chirib tashlaydigan qurtni o’rnatadi |
| Dastur xatosi yoki undagi xatolar |
| Dastur operatsion tizimning yangi versiyasi bilan ishlay olmaydi |
| Xodim tomonidan kompyuter o’g’irlanishi |
| "Inson xatosi" tahdidi turi uchun tahdid namunasini tanlang. |
| Xodim tashkilotning noutbukini to’xtash joyiga to’satdan tashlab yuboradi |
| Xavfsizlik devori barcha tarmoq trafigini bloklashi mumkin |
| Virus, qurt yoki DOS hujumi dasturiy ta’minot yoki apparatni yo’q qiladi |
| Barcha tizimlarning to’satdan to’xtashi, saqlangan ma’lumotlar yo’q |
| “Dasturiy hujumlar” tahdid turi uchun tahdid namunasini tanlang. |
| Virus, qurt yoki DOS hujumi dasturiy ta’minot yoki apparatni yo’q qiladi |
| Dasturiy ta’minot mahsuloti litsenziyalanmagan yoki mualliflik huquqini buzadi |
| Dastur xatosi yoki undagi xatolar |
| Dastur operatsion tizimning yangi versiyasi bilan ishlay olmaydi |
| Quyidagi misol uchun zaifliklarning ta’sirini (darajasini) aniqlang: Backdoor orqali tashkilot mahsulotini ishlab chiqish texnologiyasi va ilmiy asoslarini o’g’irlash |
| Muhim (Major) |
| Kichik ta’sir (Small impact) |
| Oʻrta (Significant) |
| O’ta muhim (Catastrophic) |
| Quyidagi misol uchun zaifliklarning ta’sirini (darajasini) aniqlang: Tarmoqda zararli dastur o’rnatilgan |
| Oʻrta (Significant) |
| Muhim (Major) |
| Kichik ta’sir (Small impact) |
| O’ta muhim (Catastrophic) |
| Quyidagi misol uchun zaifliklarning ta’sirini (darajasini) aniqlang: Qattiq diskning ma’lum bir turi ishlashi uchun qo’shimcha drayverlar yoki testlash talab qilinishi mumkin. |
| Kichik ta’sir (Small impact) |
| Oʻrta (Significant) |
| Muhim (Major) |
| O’ta muhim (Catastrophic) |
| Tashkilotni operatsiyalarni to’xtatishga yoki jiddiy uzilishlarga olib keladigan tanqidiy toifaga kiruvchi zaifliklarning ta’sirini (darajasini) aniqlang. |
| O’ta muhim (Catastrophic) |
| Kichik ta’sir (Small impact) |
| Oʻrta (Significant) |
| Muhim (Major) |
| Xavfsizlik siyosatiga nima uchun ehtiyoj bor? |
| Har xil zaifliklar keltirib chiqaradigan xavfsizlik tahdidlariga qarshi kurashish va ma’lumotlarni yo’qotishdan himoya qilish |
| Tashkilotning barcha funksiyalarini ishonchsiz bajarish uchun |
| Kompaniyaning tashqi axborot tahdidlariga ta’sirini oshirish |
| Tahdidlarni yuzaga kelishidan oldin bashorat qilish va zaifliklarni aniqlash orqali xavfsizlikni buzish ehtimolini oshirish. |
| Xavfsizlik siyosati nima uchun kerak? |
| Qurilmalardan foydalanish va ma’lumotlar transferining monitoringlanishi va nazoratlanishi |
| muammolarga tezda javob berish va ishlamay qolishi uchun tarmoqning yomon ishlashi uchun |
| boshqaruv stressini kamaytirish xarajatlarni oshiradi |
| ma’lumotlar va tarmoq xavfsizligini kamaytirish va xavflarni oshirish |
| Tashkilot tarmoq xavfsizligi uchun qonuniy va ichki talablarni qanday ishlab chiqadi? |
| siyosatlar yordamida |
| protseduralar orqali |
| qonunlar yordamida |
| ko’rsatmalar bilan |
| Tashkilot siyosatini amalga oshirish jarayonini amalga oshiradigan ketma-ket qadamlar majmui qanday nomlanadi? |
| Muolajalar |
| Standartlar |
| Umumiy qoidalar |
| Qonunlar |
| Internetdagi elektron pochta manzili belgilangan: user\_name@tuit.uz. Yuqori darajadagi domen nomini aniqlang? |
| uz |
| tuit.uz |
| user\_name @ tuit..uz \_ \_ |
| o’qish |
| Xavfsizlik siyosatini amalga oshirish usullarini qanday tavsiflash mumkin? |
| standartlar |
| ko’rsatmalar |
| protseduralar |
| normativ hujjatlar |
| Xodimlar tomonidan qonunlarga rioya qilishning kafolati nima? |
| Normativ hujjatlar |
| Ko’rsatmalar |
| Protseduralar |
| Qonunlar |
| Xavfsizlik siyosati ierarxiyasining qaysi bo’limi xavfsizlik bosqichlari, xavfsizlik tartib-qoidalari, ish jarayonlari va hujjatlar bilan bog’liq? |
| Siyosat tavsifi |
| Xavfsizlik talablari |
| Elementlarni joylashtirish arxitekturasi |
| Harakat xavfsizligi tushunchasi |
| Odatdagi siyosat mazmuni 5 ta asosiy elementdan iborat. Siyosat nima uchun tuzilganligi haqida batafsil tushuntirishni ifodalovchi elementni ko’rsating? |
| Maqsad |
| Harakat sohasi |
| Qoidalar va javobgarliklar |
| Sanksiyalar va buzilishlar |
| Odatdagi siyosat mazmuni 5 ta asosiy elementdan iborat. Kim va nimani qamrab olishi haqida ma’lumotni o’z ichiga olgan elementni belgilang? |
| Harakat sohasi |
| Kontaktlar |
| Qoidalar va javobgarliklar |
| Sanksiyalar va buzilishlar |
| Odatdagi siyosat mazmuni 5 ta asosiy elementdan iborat. Xodimlar va boshqaruv uchun mo’ljallangan elementni belgilang |
| Qoidalar va javobgarliklar |
| Sanksiyalar va buzilishlar |
| Harakat sohasi |
| Kontaktlar |
| Odatdagi siyosat mazmuni 5 ta asosiy elementdan iborat. Mijozlar va foydalanuvchilar rioya qilishi kerak bо’lgan ruxsat berish/ rad etish jarayonini belgilaydi? |
| Sanksiyalar va huquqbuzarliklar |
| Qo’llash doirasi |
| Kontaktlar |
| Qoidalar va javobgarliklar |
| Odatdagi siyosat mazmuni 5 ta asosiy elementdan iborat. Siyosat va/yoki boshqa qoidabuzarliklar sodir bo’lgan taqdirda kimga murojaat qilish kerakligi haqidagi ma’lumotni o’z ichiga olgan elementni belgilang |
| Kontaktlar |
| Sanksiyalar va huquqbuzarliklar |
| Qo’llash doirasi |
| Qoidalar va javobgarliklar |
| Foydalanishni cheklash yoki taqiqlash berilgan variantni ko’rsating |
| Tuhmat (sabotaj) materiallarini yaratish yoki uzatish |
| "Foyda olish" maqsadida biznesda qatnashishdan bosh tortish |
| Notijorat hujjatlarni chop etishni rad etish (ish jarayoniga aloqador bo’lmagan hujjatlar) |
| Internetdan foydalanish, faqat kompaniya faoliyati bilan bog’liq hollarda uskunalardan foydalanish |
| Foydalanishni cheklash yoki taqiqlash berilgan variantni ko’rsating |
| Qonun hujjatlarida yoki tashkilotning ichki qoidalarida belgilangan talablarga rioya qilmaslik |
| Internetdan foydalanish, faqat kompaniya faoliyati bilan bog’liq hollarda uskunalardan foydalanish |
| "Foyda olish" maqsadida biznesda qatnashishdan bosh tortish |
| Notijorat hujjatlarni chop etishni rad etish (ish jarayoniga aloqador bo’lmagan hujjatlar) |
| Foydalanishni cheklash yoki taqiqlash berilgan variantni ko’rsating |
| Qaysi serverda joylashishidan qat’iy nazar tashkilot faoliyati bilan bog’liq shaxsiy veb sahifalarni ochish va yuritish |
| Internetdan foydalanish, faqat kompaniya faoliyati bilan bog’liq hollarda uskunalardan foydalanish |
| "Foyda olish" maqsadida biznesda qatnashishdan bosh tortish |
| Notijorat hujjatlarni chop etishni rad etish (ish jarayoniga aloqador bo’lmagan hujjatlar) |
| “XAVFSIZLIK SHLYUZLARINI QО’LLAGAN HOLDA TARMOQLARARO XAVFSIZLIKNI TA’MINLASH UCHUN KOMMUNIKATSIYALAR” deb nomlanuvchi O’zR standarti roʻyxatini koʻrsatadigan variantni tanlang . |
| O’z DSt ISO/IEC 27033-4:2016 |
| O’z DSt ISO/IEC 27033-5:2016 |
| O’z DSt ISO/IEC 27033-3:2016 |
| O’z DSt ISO/IEC 27033-1:2016 |
| “ETALON TARMOQ SENARIYLARI. TAHDIDLAR, LOYIHALASHTIRISH USULLARI VA BOSHQARUV MASALALARI” deb nomlanuvchi O’zR standarti ro’yxatini ko’rsatadigan variantni tanlang . |
| O’z DSt ISO/IEC 27033-3:2016 |
| O’z DSt ISO/IEC 27033-4:2016 |
| O’z DSt ISO/IEC 27033-1:2016 |
| O’z DSt ISO/IEC 27033-2:2016 |
| “ХAVFSIZLIKNI TA’MINLASH USULLARI.TARMOQ XAVFSIZLIGI. 1-QISM.SHARH VA KONSEPSIYALAR” deb ataladigan O’zR standarti ro’yxati keltirilgan variantni tanlang . |
| O’z DSt ISO/IEC 27033-1:2016 |
| O’z DSt ISO/IEC 27033-3:2016 |
| O’z DSt ISO/IEC 27033-2:2016 |
| O’z DSt ISO/IEC 27033-4:2016 |
| “XAVFSIZLIK AMALIYOTLARI. TARMOQ XAVFSIZLIGI. TARMOQ XAVFSIZLIGINI LOYIHALASHTIRISH VA JORIY ETISH BО’YICHA RAXBARIY KО’RSATMALAR” deb nomlanuvchi O’zR standarti ro’yxati keltirilgan variantni tanlang . |
| O’z DSt ISO/IEC 27033-2:2016 |
| O’z DSt ISO/IEC 27033-4:2016 |
| O’z DSt ISO/IEC 27033-3:2016 |
| O’z DSt ISO/IEC 27033-1:2016 |
| “XAVFSIZLIK USULLARI. TARMOQ XAVFSIZLIGI. VIRTUAL HUSUSIY TARMOQLARNI QО’LLAGAN XOLDA TARMOQLARARO XAVFSIZLIKNI TA’MINLASH UCHUN KOMMUNIKATSIYALAR” deb nomlanuvchi OʻzR standarti berilgan variantni tanlang . |
| O’z DSt ISO/IEC 27033-5:2016 |
| O’z DSt ISO/IEC 27033-4:2016 |
| O’z DSt ISO/IEC 27033-2:2016 |
| O’z DSt ISO/IEC 27033-3:2016 |
| Foydalana olishlilikni boshqarish kabi xavfsizlik talabi uchun tarmoq xavfsizligi usuli qanday ta’minlanadi? |
| Kirish uchun ruxsatnomalar tizimi (identifikatsiya kartochkalari), ACL, majburiyatlarni taqsimlanishi |
| Soddalashtirilgan ro’yxatga olish / parol, raqamli sertifikatlar, elektron raqamli imzo, TLS 1.2 versiyasi, SSO, SNAR |
| Qayta yozish va zaxiralash, xavfsizlik devorlari, IDS / IPS ( DoS hujumlarini bloklash uchun), biznesning uzluksizligi, tarmoqni boshqarish va SLA bilan xizmatlarni boshqarish |
| IPSec / L2TP, shaxsiy havolalar, individual tarmoqlar |
| Qaysi variantda aloqa xavfsizligi kabi xavfsizlik talabi bilan tarmoq xavfsizligini ta’minlash usuliga misol keltirilgan? |
| IPSec/L2TP, xususiy aloqa liniyalari, moslashtirilgan tarmoqlar |
| Shifrlash, kirishni boshqarish ro’yxati, faylga kirish |
| Voqealarni yozib olish, rolga asoslangan boshqaruv va raqamli imzo |
| IPSec HMAC, davriy monitoring, antivirus dasturi |
| Autentifikatsiya qilish xavfsizlik talabi uchun tarmoq xavfsizligi usuli qanday amalga oshiriladi? |
| Tizimga kirishni soddalashtirilgan rо’yxatdan о’tkazish/parol, raqamli sertifikatlar, elektron raqamli imzo, TLS ning 1.2 versiyasi, SSO,CHAP |
| Voqealarni yozib olish, rolga asoslangan boshqaruv va raqamli imzo |
| Kirish avtorizatsiya tizimi (identifikatsiya kartalari), ACL, majburiyatlarni taqsimlash |
| IPSec HMAC, davriy monitoring, antivirus dasturi |
| Qaysi variant foydalana olishlilik xavfsizlik talabi bilan tarmoq xavfsizligini ta’minlash usuli amalga oshiriladi? |
| Rezerv nusxa olish, tarmoqlararo ekranlar, IDS/IPS (DoS hujumlarini blokirovka qilish uchun), biznesning uzluksizligi, tarmoq boshqaruvi va SLA bilan xizmatlarni boshqarish |
| Shifrlash, kirishni boshqarish ro’yxati, faylga kirish |
| Davriy nazorat, virusga qarshi dastur |
| Voqealarni yozib olish, rolga asoslangan boshqaruv va raqamli imzo |
| Qaysi variant konfidensiallik kabi xavfsizlik talabi bilan tarmoq xavfsizligini ta’minlash usuli amalga oshiriladi? |
| Shifrlash (3DES, AES, shuningdek O’z DSt 1105 da keltirilgan shifrlash algoritmlari), foydalana olishlilikni boshqarish rо’yxati, fayllardan foydalana olishlik huquqi |
| Voqealarni yozib olish, rolga asoslangan boshqaruv va raqamli imzo |
| Davriy nazorat, virusga qarshi dastur |
| Voqealarni yozib olish, rolga asoslangan boshqaruv va raqamli imzo |
| Qaysi variant yaxlitlik xavfsizlik talabi bilan tarmoq xavfsizligini ta’minlash usuli amalga oshiriladi? |
| IPSec HMAC (SHA-256), davriy monitoring, antivirus dasturi |
| Voqealarni yozib olish, rolga asoslangan boshqaruv va raqamli imzo |
| Soddalashtirilgan ro’yxatga olish / parol, raqamli sertifikatlar, elektron raqamli imzo, TLS 1.2 versiyasi, SSO, CHAP |
| IPSec / L2TP, shaxsiy havolalar, individual tarmoqlar |
| Rad etmaslik xavfsizlik talabi uchun tarmoq xavfsizligi usuli qanday amalga oshiriladi? |
| Hodisalarni rо’yxatga olish, rollar asosida foydalana olishlilikni boshqarish va elektron raqamli imzolar |
| Soddalashtirilgan ro’yxatga olish / parol, raqamli sertifikatlar, elektron raqamli imzo, TLS 1.2 versiyasi, SSO, SNAR |
| IPSec HMAC (SHA-256), davriy monitoring, antivirus dasturi |
| Qayta yozish va zaxiralash, xavfsizlik devorlari, IDS/IPS ( DoS hujumlarini bloklash uchun), tarmoqni boshqarish va SLA bilan xizmatlarni boshqarish |
| IPSec ulanishda ishtirok etuvchi qurilmalar o’rtasidagi IP-paketlarni himoyalash va autentifikatsiya qilish uchun protokollar stekining qaysi sathida ishlaydi? |
| tarmoq sathida |
| transport sathida |
| ilova sathida |
| taqdimot darajasida |
| DNS xizmatining asosiy maqsadi nima? |
| IP-manzillarda yoki TCP/IP tarmoqlarida domenlarning belgili nomlarini tashkil etish imkoniyatini beradigan domen nomi xizmati |
| tarmoq ishlashini qo’llab-quvvatlash |
| paket vaqtini sinxronlashtirish |
| javob vaqtini sinxronlashtirish |
| Quyidagilardan qaysi biri onlayn firibgarlik usuli emas? |
| Texnik qo’llab-quvvatlash |
| Karding |
| Fishing xabarlari |
| "Nigeriya" harflari |
| Kompyuterlarni lokal tarmoqqa ulash uchun asosan qaysi kabeldan foydalaniladi? |
| o’ralgan juftlik(utp) |
| koaksial kabel |
| optik tola |
| krossover kabel |
| WWW xizmatlaridan foydalanishning asosiy protokoli ... |
| HTTP |
| TELNET |
| FTP |
| SMTP |
| Ochiq tizimlarning o’zaro ta’sirining 7 darajali modeli nomini ko’rsating |
| OSI |
| TCP |
| IP |
| MAC |
| Fayl uzatish protokoli ko’rsatadigan variantni tanlang |
| FTP |
| SMTP |
| http |
| Telnet |
| Dastur operatsion tizimning yangi versiyasi bilan ishlashi mumkin emasligini tavsiflovchi tahdid turi berilgan variantni tanlang? |
| Texnik talablar jihatidan eskirish |
| Dastur xatosi yoki undagi xatolar |
| O’g’irlik |
| Sabotaj |
| 192.168.10.51 manzilining qaysi qismi standart tarmoq maskasi qo’llangan bo’lsa, tarmoq identifikatori (manzili) hisoblanadi? |
| 192.168.10 |
| 192.168 |
| 192 |
| 192.168.10.51 |
| 192.168.1.16 ning qaysi qismi standart tarmoq niqobi ishlatilgan deb hisoblasak, tarmoq identifikatori (manzili) hisoblanadi? |
| 192.168.1 |
| 192 |
| 192.168 |
| 192.168.1.16 |
| 192.168.3.36 ning qaysi qismi standart tarmoq niqobi ishlatilgan deb hisoblasak, tarmoq identifikatori (manzili) hisoblanadi? |
| 192.168.3 |
| 192.168 |
| 192.168.3.36 |
| 192 |
| 192.168.10.60 manzilining qaysi qismi standart tarmoq maskasi qo’llangan bo’lsa, tarmoq identifikatori (manzili) hisoblanadi? |
| 192.168.10 |
| 192.168 |
| 192 |
| 192.168.10.60 |
| Fayl arxivlarini o’z ichiga olgan internet-serverlar ... |
| kerakli fayllarni yuklab olish uchun ishlatiladi |
| elektron pochta xabarini olish uchun ishlatiladi |
| telekonferensiyalarda ishtirok etish ishlatiladi |
| video konferensiyalarni o’tkazish ishlatiladi |
| Kompyuter tarmog’ining umumlashtirilgan geometrik tavsifi ... |
| tarmoq topologiyasi |
| tarmoq qurilmalari |
| tarmoq serveri |
| tarmoq foydalanuvchilari |
| Kompyuter tarmog’i protokoli - bu... |
| tarmoqdagi ma’lumotlarni qabul qilish va uzatish, faollashtirishni tartibga soluvchi qoidalar |
| tarmoq trafigining xususiyatlari |
| tarmoq foydalanuvchilari harakatlarini qayd qilish uchun elektron jurnallar |
| audit jurnallari |
| Tarmoq sathida axborot almashinuvining asosiy birligi nima? |
| paket |
| bit |
| kanal |
| so’z |
| Mijozlarning fayllarga kirishini boshqaruvchi server qanday nomlanadi? |
| Fayl serveri |
| pochta serveri |
| Proksi-server |
| Mediatsiya serveri |
| Qaysi dastur antivirus emas? |
| Defrag |
| Norton Antivirus |
| Dr veb |
| AVP |
| Qaysi texnologiya taqsimlangan ishlov berish texnologiyasi bo’lib, unda umumiy hisoblash resurslari, dasturiy ta’minot va ma’lumotlar foydalanuvchilarga Internet orqali xizmat sifatida taqdim etiladi? |
| bulutli texnologiyalar |
| DBMS |
| blokcheyn |
| ADSL |
| MAC manzilining uzunligi necha baytga teng? |
| 6 |
| 3 |
| 8 |
| 4 |
| IPv4 manzilining uzunligi necha bit? |
| 32 |
| 16 |
| 28 |
| 128 |
| IPv6 manzili uzunligida necha bit? |
| 128 |
| 64 |
| 32 |
| 8 |
| IPv4 manzilining uzunligi necha baytga teng? |
| 4 |
| 32 |
| 16 |
| 3 |
| TCP/IP protokoli stekining birinchi sathi ko’rsatadigan variantni tanlang |
| fizik |
| tarmoq |
| transport |
| qo’llaniladi |
| OSI modelining qaysi sathida ma’lumotlar freymlar sifatida ifodalanadi? |
| kanal |
| transport |
| tarmoq |
| ilova |
| Protokol nima? |
| kompyuter tarmog’i aloqa standarti |
| LAN qurilmasi |
| kompyuterning aloqa kanallari orqali fayllarni yuborish qobiliyati |
| elektron pochta orqali xabarlarni yuborish uchun standart |
| DHCP ning asosiy maqsadi nima? |
| avtomatik ravishda IP manzillarni ajratish |
| mijoz-server balansini saqlaydi |
| internetga kirish |
| IPv4 ni IPv6 ga aylantiradi |
| Qaysi tarmoq topologiyasi mavjud emas? |
| Jurnal |
| Yulduz |
| Shina |
| halqa |
| Elektron pochta protokollari ro’yxatini ko’rsatadigan variantni belgilang |
| SMTP, POP, IMAP |
| HTTP, HTTPS |
| DNS, BOOTP |
| DNS, DHCP |
| Optik kabelda ma’lumot qanday ko’rinadi? |
| nur |
| puls |
| chastota |
| harorat |
| Qaysi kabel odatdagi diametri 1 mm bo’lgan ikkita izolyatsiyalangan mis simlardan iborat? |
| o’ralgan juftlik(utp) |
| koaksial |
| optik tolali |
| MAREA |
| WAN tarmog’ini yaratish uchun marshrutizatorlarning minimal soni qancha? |
| 2 |
| 4 |
| 1 |
| 3 |
| WAN, MAN, LAN ni o’sish tartibida joylashtiring |
| LAN<MAN<WAN |
| WAN<LAN<MAN |
| WAN <LAN< WAN |
| MAN<LAN<WAN |
| OSI modelida 7-sathini belgilang? |
| ilova |
| taqdimot |
| seans |
| kanal |
| OSI modelida 6- sathini belgilang? |
| taqdimot |
| ilova |
| seans |
| kanal |
| OSI modelidagi 5- sathini belgilang? |
| seans |
| taqdimot |
| ilova |
| kanal |
| OSI modelidagi 4- sathini belgilang? |
| transport |
| taqdimot |
| ilova |
| taqdimot |
| OSI modelida 3- sathini belgilang? |
| tarmoq |
| taqdimot |
| transport |
| sessiya |
| OSI modelida 2- sathini belgilang? |
| havola |
| taqdimot |
| sessiya |
| dastur |
| OSI modelidagi 1- sathini belgilang? |
| fizik |
| taqdimot |
| dastur |
| sessiya |
| END DIVECES ga qaysi qurilmalar kiradi ? |
| kompyuter, noutbuk, server |
| kompyuter, server , router |
| router , switch , server |
| router , kalit , kompyuter |
| OSI modelida nechta qatlam mavjud? |
| 7 |
| 6 |
| 5 |
| 4 |
| DDoS hujumlari uchun qanday protokol ishlatiladi ? |
| ARP |
| http |
| HTTPS |
| POP3 |
| Windows buyruq satri orqali kompyuterning IP manzilini bilish uchun qanday buyruq ishlatiladi ? |
| ipconfig |
| ifconfig |
| ifconfig/all |
| show ip address |
| Kafolatlangan ma’lumotlarni yetkazib berishni ta’minlovchi protokol qanday nomlanadi? |
| TCP |
| POP3 |
| FTP |
| TFTP |
| Himoyalangan resurslar to’plamini belgilaydigan kirish qoidalari to’plami nima? |
| ACL |
| ASL |
| AVL |
| ACM |
| Tarmoq ichidagi tarmoq taqsimoti nomini ko’rsatilgan variantni tanlang? |
| qism tarmoq (subnet) |
| yuklama taqsimoti |
| resurslarni taqsimlash |
| to’liq tarmoq ( Fullnet ) |
| Qanday himoya usullari foydalanuvchi autentifikatsiya protseduralarini bajaradigan dasturiy va apparat vositalarini, ma’lumotlarni ruxsatsiz kirish va o’qishdan himoya qilishni, shuningdek, tarmoqlar orqali ma’lumotlarni xavfsiz uzatish vositalarini o’z ichiga oladi? |
| Texnik |
| Tashkiliy va huquqiy |
| Jismoniy |
| Huquqiy |
| Ilova sath protokollaridan ma’lumotlarni qabul qiluvchi va uni OSI modelidan foydalangan holda barcha kompyuterlar tushunadigan formatga aylantiruvchi sath qanday nomlanadi? |
| taqdimot |
| tarmoq |
| ilova |
| seans |
| Qaysi tashkilot OSI modelini ishlab chiqqan? |
| Xalqaro standartlashtirish tashkiloti |
| Xalqaro elektraloqa ittifoqi |
| Telefoniya va telegrafiya boʻyicha xalqaro maslahat qoʻmitasi |
| Yevropa kompyuter ishlab chiqaruvchilar uyushmasi |
| Qaysi protokol zamonaviy kriptografiyadan foydalangan holda xizmat protokollari va transport protokollari o’rtasidagi ma’lumotlarni himoya qiladi? |
| SSL |
| PPP |
| SET |
| IPSec |
| “Axborot xavfsizligi” tushunchasining uchta tarkibiy qismi nimalardan iborat? |
| Konfidensiallik, foydalanuvchanlik va butunlik |
| Konfidensiallik, foydalanuvchanlik va tekshirish imkoniyati |
| Konfidensiallik, tekshiriluvchanlik va yaxlitlik |
| Konfidensiallik, chidamlilik va mavjudlik |
| Mijoz so’ralgan serverga so’rov yuboradi va so’rovga javoban mijoz tomonidan olingan faylni yuboradigan ma’lumotni so’raydi. Ushbu jarayon uchun qaysi model xosdir? |
| mijoz-server |
| nuqta - nuqta(peer-to-peer) |
| MVC |
| MITM |
| Har bir oxirgi qurilma server yoki mijoz vazifasini bajarishi mumkin. Kompyuter bir ulanish uchun server va boshqa ulanish uchun mijoz vazifasini bajarishi mumkin. Bu qanday model? |
| nuqta – nuqta(peer-to-peer) |
| mijoz-server |
| MVC |
| MITM |
| POP3 va IMAP4 ma’lumotlarni xavfsiz yetkazib berish uchun qanday transport qatlami protokolidan foydalanadi? |
| TCP |
| IP |
| PPP |
| SMTP |
| Asosiy maqsadi fayllarni bir kompyuterdan ikkinchisiga o’tkazish yoki fayllarni serverlardan mijozlarga va mijozlardan serverlarga o’tkazish bo’lgan protokol nima? |
| FTP |
| TFTP |
| http |
| SMTP |
| Tarmoq sathidagi ma’lumotlar birligining nomi nima? |
| paket |
| trafik |
| protokol |
| stack |
| Ma’lumotlarni tinglash va uzatish jarayonidagi o’zgarishlar hujumi ko’rsatilgan variantni tanlang. |
| Eavesdropping |
| DDoS |
| Port scanning |
| Denial-of-service |
| Qaysi protokol tarmoq orqali uzatiladigan ma’lumotlarning maxfiyligini ta’minlaydi, ya’ni faqat jo’natuvchi va qabul qiluvchi ma’lumotlarning shaffofligini va paketlar autentifikatsiyasining ishlashini tushunishi mumkinmi? |
| IPsec |
| IP |
| PPP |
| IPX |
| ......yordamida tizim yoki tarmoq xavfsizlik siyosatini buzib kirishga harakat qilingan usul yoki vositalar aniqlanadi. Nuqtalar o’rniga to’g’ri javobni belgilang. |
| hujumlarni aniqlash tizimi |
| tarmoq skanerlaridan foydalanish |
| xavfsizlik devorlari |
| antivirusdan foydalanish |
| Elektron pochta xizmatlari sizga ....yuborish imkonini beradi. Nuqtalar o’rniga to’g’ri javobni belgilang. |
| xabarlar va undagi qo’shimcha ilovalar |
| faqat xabarlar |
| faqat fayllar |
| video tasvirlar |
| Aniqlangan foydalanuvchini jarayon yoki qurilmaga kiritilgan paroli haqiqiyligini tekshirish tartibi qanday nomlanadi? |
| autentifikatsiya |
| ruxsat |
| identifikatsiya |
| boshqaruv |
| Uning egasining haqiqiyligini aniqlash jarayonida axborot nazorati sifatida foydalaniladigan belgilar ketma-ketligi qanday nomlanadi? |
| parol |
| yaxlitligini tekshirish |
| shifrlangan matn |
| xabar dayjesti |
| TCP/IP protokoli stekida nechta sath mavjud? |
| 4 |
| 5 |
| 6 |
| 7 |
| 192.168.1.0 manziliga qaysi standart tarmoq niqobi mos keladi? |
| /24 |
| /32 |
| /16 |
| /sakkiz |
| TCP/IP protokoli stekidagi 1-sathini belgilang? |
| fizik |
| taqdimot |
| tarmoq |
| transport |
| OSI modelidagi qaysi sath IP manzillar bilan shug’ullanadi? |
| tarmoq |
| ilova |
| taqdimot |
| fizik |
| OSI modelidagi qaysi sath MAC manzillari bilan shug’ullanadi? |
| kanal |
| transport |
| ilova |
| taqdimot |
| 192.168.1.243 /24 uchun broadcast manzilini aniqlang. |
| 192.168.1.255 |
| 192.168.1.128 |
| 192.168.1.252 |
| 192.168.1.257 |
| 192.168.1.243 /24 IP manzilining tarmoq manzilini aniqlang |
| 192.168.1.0 |
| 192.168.1.128 |
| 192.168.1.255 |
| 192.168.1.252 |
| 11.192.168.1.243 /25 IP manzilining broadcast manzilini ko’rsating. |
| 192.168.1.255 |
| 192.168.1.128 |
| 192.168.1.0 |
| 192.168.1.252 |
| Qaysi sinf manzillari faqat tadqiqot maqsadlarida (faqat laboratoriyalarda) qo’llaniladi? |
| D |
| E |
| A |
| B |
| Qaysi texnologiya mahalliy IP manzilni global manzilga o’zgartiradi? |
| NAT |
| OSI |
| HMAC |
| IDS |
| Switch OSI modelining qaysi qatlamida ishlaydi ? |
| 2 |
| 3 |
| to’rtta |
| 1 |
| Hub OSI modelining qaysi qatlamida ishlaydi ? |
| 1 |
| 2 |
| 3 |
| to’rtta |
| 255.0.0.0 standart tarmoq maskasi qaysi sinfga tegishli? |
| A |
| B |
| C |
| D |
| 255.255.0.0 standart tarmoq maskasi qaysi sinfga tegishli? |
| B |
| C |
| D |
| A |
| 255.255.255.0 standart tarmoq maskasi qaysi sinfga tegishli? |
| C |
| A |
| B |
| D |
| 255.255.255.128 maskasida nechta IP manzil mavjud? |
| 128 |
| 256 |
| 64 |
| 32 |
| Marshrutlashning nechta turi mavjud? |
| 2 |
| 3 |
| 4 |
| 1 |
| E-mail jo’natish va qabul qilish vazifasini bajaradigan serverning nomi nima ? |
| Pochta serveri |
| Fayl serveri |
| Qabul qiluvchi-uzatuvchi server |
| Proksi-server |
| SSH protokolining funksiyasini belgilang. |
| masofaviy aloqani o’rnatadi |
| tashqi tahdidlardan himoya qilish uchun xizmat qiladi |
| IP manzili uchun domen nomi sifatida ishlaydi |
| DHCP kabi ishlaydi |
| BGP qanday protokol turi hisoblanadi? |
| marshrutlash protokollari |
| internet protokollari |
| pochta protokollari |
| fayl uzatish protokollari |
| OSPF protokoli qanday turdagi protokollardan iborat? |
| marshrutlash protokollari |
| internet protokollari |
| pochta protokollari |
| fayl uzatish protokollari |
| SNMPv3 protokolining qaysi ishlash holatida parollar ochiq ko’rinishda uzatiladi, ma’lumotlar konfidensialligi mavjud emas? |
| noAuthNoPriv |
| authNoPriv |
| authPriv |
| noAuthPriv |
| SNMPv3 protokolining qaysi ishlash holatida konfidensialliksiz autentifikatsiya amalga oshiriladi? |
| authNoPriv |
| authPriv |
| noAuthPriv |
| noAuthNoPriv |
| Bir bino yoki idora ichidagi tarmoq qanday nomlanadi? |
| LAN (Local Area Network) |
| PAN (Personal Area Network) |
| GAN (Global Area Network) |
| CAN (Campus Area Network) |
| OSI modelining 1-sathida ishlaydigan aloqa uchun tarmoqdagi qurilmalarni birlashtiruvchi tarmoq qurilmasini ko’rsating? |
| kontsentrator |
| komutator |
| marshrutizator |
| repiter |
| Tarmoq sathining protokollari qaysi qatorda keltirilgan? |
| IP, ARP, IPSec , ICMP, OSPF |
| TCP, ARP, UDP, ICMP, OSPF |
| UDP, ARP, IPSec , SIP, FTP |
| IP, ARP, PPP, ICMP, TCP |
| Kompyuter yordamida komutatorni sozlash imkonini beruvchi kabel turini belgilang |
| Konsol kabeli |
| Krossover kabel |
| Optik kabel |
| Ketma-ket kabel |
| Firewall butun tarmoq trafigini bloklab qо‘yishi xavfi qanday tahdid turi? |
| Apparat vositalarining buzilishi yoki ishlashidagi xatoliklar |
| Dasturiy ta’minot hujumlari |
| Texnik talablar jihatdan eskirish |
| Josuslik |
| Ushbu usulda testlovchi testlanadigan tarmoq infrastrukturasi haqida hech qanday dastlabki bilimlarga ega bо‘lmaydi. Testlovchi real tajribalarni о‘tkazishdan oldin tizim va qurilmalarning turi va joylashuvini aniqlashi lozim. Bunda tashkilotga tashqaridan real hujumlarni imitatsiyalashga imkon beradi. Qaysi usul haqida gapiryapsiz? |
| Qora quti |
| Oq quti |
| Kulrang quti |
| Yashil quti |
| Ushbu usulda testlovchi testlanadigan tarmoq va tizim haqida tarmoq topologiyasi, IP-manzillar, hattoki foydalanuvchilar ilovalarining joriy kodlari kabi muhim malumotlarga ega bо‘ladi. Qaysi usul haqida gapiryapsiz? |
| Oq quti |
| Qora quti |
| Kulrang quti |
| Yashil quti |
| Yong’in, suv toshqini yoki zilzila ma’lumotlarni yo’q qilishi mumkin. Bu qanday tahdid? |
| tabiiy ofatlar |
| sabotaj |
| josuslik |
| antropogen omillar |
| Mahsulot ishlab chiqarish uchun ish jadvalini o’g’irlash qanday tahdid turiga bog’liq bo’lishi mumkin? |
| josuslik |
| tabiiy ofatlar |
| sabotaj |
| inson xatosi |
| Xodim tashkilotning noutbukini to’xtash joyiga to’satdan tushurib yuborishi. Bu qanday tahdid? |
| inson xatosi |
| sabotaj |
| tabiiy ofatlar |
| josuslik |
| Virus, qurt yoki DOS hujumi dasturiy yoki apparat taminotni buzadi? |
| Dasturiy hujumlari |
| O’g’irlik |
| inson xatosi |
| Sabotaj |
| Хatolik dasturning yuklanishiga tо’sqinlik qiladi qanday tahdid turi? |
| Dasturning buzilishi yoki undagi xatoliklar |
| O’g’irlik |
| inson xatosi |
| Sabotaj |
| Dasturning operatsion tizimning yangi versiyasi bilan ishlay olmasligi qanday turdagi tahdidlarga bog’liq bo’lishi mumkin? |
| Texnik talablar jihatidan eskirish |
| Dastur xatosi yoki undagi xatolar |
| O’g’irlik |
| Sabotaj |
| Xodimning kompyuterini noqonuniy va ruxsatsiz olib qo’yish qanday tahdidlarni tasniflash mumkin? |
| O’g’irlik |
| Dastur xatosi yoki undagi xatolar |
| inson xatosi |
| Josuslik |
| Qaysi topologiya tarmoq orqali uzatiladigan axborot oqimini aks ettiradi? |
| axborot |
| jismoniy |
| mavjud |
| mantiqiy |
| Qaysi topologiya fizik topologiyadagi signallarning harakatini aks ettiradi? |
| mantiqiy |
| jismoniy |
| axborot |
| strukturaviy |
| Xakerlar tomonidan amalga oshiriladigan skanerlashning qaysi turini ixtisoslashgan kompaniyalar tomonidan amalga oshiriladigan skanerdan ajratib bo’lmaydi? |
| zaifliklarni skanerlash |
| faylni kuzatish |
| Troyan otlarini skanerlash |
| yashirin skanerlash |
| Tarmoqqa kirish usullarini ko’rsating? |
| Ethernet , PPP, ADSL |
| IP, ICMP, ARP, DHCP |
| TCP, UDP |
| Telnet, SMTP, FTP, NNTP, HTTP, SNMP, DNS, SSH |
| Qaysi sath o’zaro aloqa qiluvchi ikkita xost o’rtasidagi aloqani o’rnatish, boshqarish va tugatish uchun javobgardir? |
| seans |
| taqdimot |
| tarmoq |
| ilova |
| Ma’lumotlar oqimidagi ma’lumotlarni segmentlash va qayta yig’ish funksiyasini qaysi sath bajaradi? |
| transport |
| Ilova |
| tarmoq |
| seans |
| Mantiqiy manzil asosida paketni marshrutlash uchun qaysi sath javobgar? |
| tarmoq |
| transport |
| ilova |
| seans |
| Ushbu usulda testlovchiga cheklangan miqdordagi ma’lumot taqdim etiladi. Qaysi usul haqida gapiryapsiz? |
| Kulrang quti |
| Qora quti |
| Oq quti |
| Yashil quti |
| Oxirgi tizimlar о’rtasida fizik kanal orqali strukturlanmagan bitlar potokini uzatadi. Bu qaysi sathning vazifasi? |
| fizik |
| taqdimot |
| transport |
| ilova |
| Tarmoqlararo ekran(firewall) bu : |
| ichki tarmoq foydalanuvchilarini tashqi tarmoq resurslaridan himoyalash, ichki tarmoq foydalanuvchilarini tashqi tarmoqqa bo’lgan murojaatlarini cheklash |
| vazifasi trafikni imkon qadar tezroq manzilga yetkazish bo’lgan qurilma |
| tarmoq trafigini keshlash qurilmasi |
| tarmoq trafigini xeshlash qurilmasi |
| Quyidagi protokollardan qaysi biri ilova sathini autentifikatsiya qilish protokoli sifatida ishlatiladi? |
| TACACS |
| DHCP |
| SSH |
| telnet |
| Tizim sozlamalarida masofaviy ulanish protokollarini belgilang? |
| SSH, Telnet |
| SSH, RTP |
| FTP, LDP |
| POP3, LDP |
| Masofaviy ish stoliga kirish uchun qanday protokol ishlatiladi? |
| RDP |
| FTP |
| SMTP |
| HTTPS |
| Quyidagilardan qaysi biri TACACS versiyasi emas? |
| TACACS# |
| TACACS |
| TACACS+ |
| XTACACS |
| Qaysi javobda to’g’ri SMTP protokoli nomi keltirilgan? |
| Simple Mail Transfer Protocol |
| Session Mail Transfer Protocol |
| Security Mail Transfer Protocol |
| Simple Massege Transfer Protocol |
| Qaysi javob to’g’ri HTTP protokoli nomini ko’rsatadi? |
| Hyper Text Transfer Protocol |
| High Terminal Transfer Protocol |
| High Text Tranzit Protocol |
| Hyper Terminal Tranzit Protocol |
| Qaysi javobda ICMP protokolining to’g’ri nomi ko’rsatilgan? |
| Internet Control Message Protocol |
| Intranet Control Message Protocol |
| Illegal Control Mail Protocol |
| Internet Connection Message Protocol |
| Xizmatni rad etish hujumini belgilang? |
| DoS |
| DHCP poisoning |
| Resource Attack |
| MiTM |
| O’rta hujumdagi odamni topingmi? |
| MiTM |
| Resource Attack |
| DDoS |
| DoS |
| Qaysi hujum quyidagilar bilan tavsiflanadi: agar seans identifikatori shifrlanmagan bo’lsa, tajovuzkor seans identifikatorini sotib olib, sessiyani o’g’irlashi mumkin? |
| Session Hijacking |
| Man-in-the-Middle |
| Information Leakage |
| Blind Session Attacks |
| Quyidagi topologiyalardan qaysi biri yopiq zanjir hisoblanadi? |
| halqa |
| Shina |
| Yulduz |
| Yog’och |
| Hujumlarni aniqlash tizimining qisqartmasi ko’rsatilgan qatorni toping? |
| IDS |
| IPS |
| VPN |
| DPA |
| Hujumni bartaraf etish tizimining qisqartmasi ko’rsatilgan qatorni toping? |
| IPS |
| IDS |
| VPN |
| DPA |
| Jahon miqyosidagi global kompyuter tarmog’i bu... |
| www |
| Elektron pochta \_ |
| intranet |
| WEP |
| Kompyuter tarmog’ining umumiy geometrik tavsifi: |
| tarmoq topologiyasi |
| tarmoq qurilmasi |
| tarmoq foydalanuvchilari |
| tarmoq serveri |
| Quyidagilardan qaysi biri spam deb ataladi? |
| Siz ishtirok etmagan tanlovda g’olib bo’lganingiz haqida bildirishnomalar |
| Do’stingizdan xabar |
| Bankdan qarz haqida xat |
| Elektron pochta - jurnalni ular obuna bo’lgan nashrdan tarqatish |
| Qaysi jarayonni quyidagi buyruqlar yordamida sozlash mumkin?Qaysi jarayonni quyidagi buyruqlar yordamida sozlash mumkin?  S1( config )# line vty 0 15  S1( config -line)# parol cisco  S1( config -line)# login  S1( config -line)# end |
| telnet |
| SSH |
| Konsol |
| yoqish |
| Port security funksiyasi qaysi qurilmada sozlanadi ? |
| komutator |
| marshrutizator |
| server |
| kontsentrator |
| Qaysi buyruqni kiritishda MAC manzili noma’lum bo’lgan paketlar qabul qilinmaydi va xabar yaratilmaydi va port o’chirish rejimiga o’tmaydi? |
| protect |
| portsecurity |
| shutdown |
| restrict |
| Cisco routerlarida parolni olib tashlash uchun nima ishlatiladi ? |
| Konfiguratsiya registri |
| jurnal reestri |
| Xabarlar ro’yxati |
| Yozuvlar reestri |
| Qaysi qatorda rezervlash protokollar keltirilgan? |
| STP, RSTP |
| LACP, HTTP |
| SMTP, RSTP |
| POP, PAgP |
| Agregatlash protokollari qaysi qatorda keltirilgan? |
| LACP, PAgP |
| STP, RIP |
| POP, PAgP |
| SMTP, RSTP |
| Port securityni sozlash uchun qanday parametr ishlatiladi? |
| MAC manzili |
| IP manzili |
| uskunani identifikatsiya qilish raqami |
| broadcast manzili |
| Dinamik marshrutlash protokollari ro’yxatini ko’rsating? |
| RIP, EIGRP, OSPF, BGP |
| IP marshruti, EIGRP, OSPF, Telnet |
| HTTP, OSPF, POP |
| SSH, IGRP, OSPF, BGP |
| Manzil translatsiyalash uchun qanday texnologiya qo’llaniladi? |
| NAT |
| DHCP |
| DNS |
| ARP |
| Troubleshooting qilish nima uchun ishlatiladi ? |
| tarmoq ishlamay qolishini aniqlash uchun |
| tarmoqni sozlash uchun |
| trafikni filtrlash uchun |
| tarmoq sinovlari uchun |
| AAA serveri qanday vazifalarni bajaradi? |
| Authentication, Authorization, Accounting |
| Authentication, Authorization, Identification |
| Authentication, Identification, Accounting |
| Identification, Authorization, Accounting |
| Turli xil tarmoq segmentlarida joylashgan oxirgi tizimlar o’rtasida ma’lumotlarni uzatish imkonini beruvchi mexanizm qanday nomlanadi? |
| marshrutlash |
| ro’yxatga olish |
| shifrlash |
| standartlashtirish |
| Kompyuter tarmog’i (kompyuter tarmog’i) bu ... |
| hisoblash qurilmalari o’rtasida ma’lumot almashish tizimi |
| odam atrofida qurilgan tarmoq |
| virtual lokal tarmoq |
| bir nechta tarmoqlardan tashkil topgan yagona tashkilot tarmog’i |
| PAN tarmog’i bu... |
| inson tarmog’i |
| bir nechta tarmoqlardan tashkil topgan yagona tashkilot tarmog’i |
| virtual mahalliy tarmoq |
| hisoblash qurilmalari o’rtasida ma’lumot almashish tizimi |
| Zaiflikni baholash nima? |
| aktivlarga yetkazilgan zararni tizimli va uslubiy baholash |
| tashkilotning aktivlarini aniqlash |
| dastur xatosi yoki undagi xatolar |
| barcha tizimlarning to’satdan to’xtashi |
| Zaiflikni baholashning xarakteristikasini toping: Tasiri yо’q (No impact) |
| Ushbu zaiflik tashkilotning faoliyatiga hech qanday ta’sir ko’rsatmaydi. |
| Ish faoliyatning to’xtab qolishi oqibatida xodimlarning ish unumdorligini pasayishiga olib keluvchi tahdidlar |
| Tashkilotning ish faoliyatining to’xtab qolishigan yoki sezilarli darajada buzilishiga sabab bo’luvchi o’ta muhim turiga kiruvchi zaifliklar |
| Tashkilot daromadiga sezilarli darajada tasir ko’rsatuvchi zaifliklar |
| Zaiflikni baholashning xarakteristikasini toping: Muhim (Major) |
| Tashkilot daromadiga sezilarli darajada tasir ko’rsatuvchi zaifliklar |
| Ushbu zaiflik tashkilotning faoliyatiga hech qanday ta’sir ko’rsatmaydi. |
| Ish faoliyatning to’xtab qolishi oqibatida xodimlarning ish unumdorligini pasayishiga olib keluvchi tahdidlar |
| Tashkilotning ish faoliyatining to’xtab qolishigan yoki sezilarli darajada buzilishiga sabab bo’luvchi o’ta muhim turiga kiruvchi zaifliklar |
| Port security funksiyasi qanday vazifani bajaradi? |
| har qanday kommutator portini faqat ma’lum qurilmalar u orqali tarmoqqa kirishi uchun sozlash |
| ADCL marshrutizatorini sozlash |
| virtual tarmoqlarni yaratish |
| masofaviy kirishni oching |
| Komutator portiga ulanishga ruxsat berilgan qurilmalar ... orqali aniqlanadi. Nuqtalar o’rniga berilgan so’zni toping? |
| MAC manzillari |
| IP4 manzillari |
| IP6 manzillari |
| kompyuter nomi |
| MAC manzillarini cheklashning nechta usuli bor? |
| 2 |
| 3 |
| 4 |
| 5 |
| Ushbu loglash darajasi darhol chora ko’rish zarurligi to'g'risida xabarlarni ko’rsatadi. Bu qaysi loglash darajasi? |
| 1 - Alets |
| 0 - Emergencies |
| 2 - Critical |
| 3 - Errors |
| Ushbu loglash darajasi Ogohlantirishlarni o'z ichiga olgan xabarlarni ko’rsatadi. Bu qaysi loglash darajasi? |
| 4 - Warnings |
| 0 - Emergencies |
| 2 - Critical |
| 3 - Errors |
| Windows tizimida Ethernet adapterining MAC manzili ... buyrug’i yordamida aniqlanishi mumkin. |
| ipconfig / all |
| cls |
| cmd |
| telnet |
| Kommutatorda MAC manzillar jadvalini ko’rish uchun qanday buyruqni ishlatiladi. |
| show mac-address-table |
| show macs |
| show address-table |
| show table |
| Konsol nima port ? |
| Cisco qurilmasini sozlash uchun tashqi kirishni ta’minlovchi boshqaruv porti |
| RFC 854 da yozilgan tarmoqdagi qurilmalarga kirish uchun tarmoq protokoli |
| virtual tarmoqlarni yaratish |
| har qanday kommutator portini faqat ma’lum qurilmalar u orqali tarmoqqa kirishi uchun sozlash |
| TELNET ....? |
| tarmoq bo’ylab qurilmalarga murojat qilish uchun mo’ljallangan tarmoq protokoli. Protokolning zamonaviy standarti RFC 854 da yozilgan. |
| Cisco qurilmasini sozlash uchun tashqi kirishni ta’minlovchi boshqaruv porti |
| virtual tarmoqlarni yaratish |
| har qanday kommutator portini sozlash |
| Secureshell (SSH) nima ? |
| bu masofaviy qurilmalarni boshqarish uchun xavfsiz (shifrlangan) ulanishni ta’minlovchi protokoldir |
| bu tarmoqdagi qurilmalarga kirish uchun tarmoq protokoli, RFC 854 standarti |
| virtual tarmoqlarni yaratishdir |
| Cisco qurilmasini sozlash uchun tashqi kirishni ta’minlovchi boshqaruv porti |
| STP protokoli...? |
| IEEE 802.1d standartiga asoslangan OSI kanal sathi protokoli |
| tarmoqdagi qurilmalarga kirish uchun tarmoq protokoli, RFC 854 da yozilgan protokol standarti |
| ADCL router konfiguratsiya protokoli |
| masofaviy qurilmalarni boshqarish uchun xavfsiz ulanish protokoli |
| Kommutatorni asosiy(root) komutator sifatida belgilash uchun qanday buyruq ishlatiladi? |
| spanning-tree vlan vlan-id root primary |
| spanning tree root primary |
| spanning-tree id root primary |
| spanning-tree vlan root private |
| Komutatorni zaxira(bridge) komutator sifatida belgilash uchun qanday buyruq ishlatiladi? |
| spanning-tree vlan vlan-id root secondary |
| spanning tree root secondary |
| spanning tree root primary primary2 |
| spanning-tree vlan vlan-id root |
| Root komutatorni ustuvorlik bilan belgilash uchun qaysi buyruq ishlatiladi? |
| spanning-tree vlan vlan-id priority value |
| spanning-tree vlan vlan-id root secondary |
| spanning-tree vlan vlan-id root primary |
| spanning-tree vlan vlan-id root |
| show spanning-tree buyrug’i nima uchun ishlatiladi? |
| komutatorni ustuvorligini ko’rish uchun |
| faqat STP protokoli bilan ishlaydigan faol interfeyslarni ko’rsatadi |
| port holati ma’lumotlarini ko’rsatadi |
| ildiz ko’prigining konfiguratsiyasi haqidagi ma’lumotlarni ko’rsatadi |
| show spanning-tree active buyrug’i nima uchun ishlatiladi? |
| faqat STP protokoli bilan ishlaydigan faol interfeyslarni ko’rsatadi |
| o’tish ko’prigi ustuvorligini ko’rish uchun ishlatiladi |
| port holati ma’lumotlarini ko’rsatadi |
| ildiz ko’prigining konfiguratsiyasi haqidagi ma’lumotlarni ko’rsatadi |
| show spanning-tree summary buyrug’i nima uchun ishlatiladi? |
| port holati ma’lumotlarini ko’rsatadi |
| faqat STP protokoli bilan ishlaydigan faol interfeyslarni ko’rsatadi |
| ildiz ko’prigining konfiguratsiyasi haqidagi ma’lumotlarni ko’rsatadi |
| o’tish ko’prigi ustuvorligini ko’rish uchun ishlatiladi |
| show spanning-tree root buyrug’i nima uchun ishlatiladi? |
| ildiz komutatorning konfiguratsiyasi haqidagi ma’lumotlarni ko’rsatadi |
| port holati ma’lumotlarini ko’rsatadi |
| o’tish ko’prigi ustuvorligini ko’rish uchun ishlatiladi |
| faqat STP protokoli bilan ishlaydigan faol interfeyslarni ko’rsatadi |
| SSL sertifikati nima? |
| mijoz va server o’rtasida almashinadigan ma’lumotlarni shifrlaydigan, shaxsiy ma’lumotlarni uzatishni himoya qiluvchi protokol |
| identifikatsiya qilish, avtorizatsiya qilish va autentifikatsiya qilish imkoniyatlarini ta’minlovchi amaliy qatlam protokoli |
| tarmoq diagnostikasi ma’lumotlarni uzatish va qabul qilish |
| elektron pochta xabarlarini yuborish uchun ishlatiladigan protokol |
| PPP va SLIPning asosiy xavflarini tanlang |
| autentifikatsiya, ikki tomonlama aloqa va foydalanuvchilarni o’qitish |
| ish stoliga masofaviy kirish imkoniyatini olish |
| signallar to’plami |
| aloqa seansini tashkil qilishda turli tarmoq muhitlarida ma’lumotlarni uzatish qoidalari va tartiblari |
| Router metric attacks... |
| marshrutlash metrik hujumi marshrutlash jadvalidagi dinamik ko’rsatkichlarni zaharlaydi |
| DoS yoki tizimni buzish shaklida yo’riqnomaga to’g’ridan-to’g’ri hujum |
| bir xil tarmoq manziliga ega ikkita xost mavjud bo’lsa, eng tez javob beradigan xost tarmoq ulanishini saqlab qolishi mumkin. |
| tarmoq protokollari tarmoq halqalarini aniqlash va oldini olishga harakat qilganda |