**O‘ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALARI VAZIRLIGI**

**MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI**

**Ishlab chiqarish amaliyoti hisoboti**

**Guruh:** 051-20

**Topshirdi:** Alijonov Muhammadqodir

**Tekshirdi:** Shamsiyev A.S

Toshkent – 2024

Reja:

1. **Kirish**
2. Korxona bilan tanishish. Korxonaning asosiy maqsad va vazifalari.
3. **Asosiy qism**
4. Axborot xavfsizligi bilan tanishish.
5. Xavfsizlikni oshirish va muammolarni hal qilish.
6. Wi-Fi tizimi bo'yicha amaliyot.
7. Yangi optik tolali Wi-Fi tortish.
8. Server bilan tanishish
9. Server protokollari bo'yicha bilim olish
10. Serverning filiallar bilan aloqasi
11. Tizim monitoringi va xavfsizlik auditi
12. Ma'lumotlar bazasi boshqaruvi
13. Zaxira nusxa olish va tiklash jarayonlari
14. **Xulosa**

**Najot Ta'lim O'quv Markazidagi ishlab chiqarish amaliyoti hisoboti**

Men, Alijonov Muhammadqodir Bahodir o’g’li, Najot Ta'lim o'quv markazi Chilonzor filialida ishlab chiqarish amaliyoti doirasida quyidagi ishlarni amalga oshirdim.

**1. Axborot xavfsizligi bilan tanishish**

**O'quv markazining axborot xavfsizligi siyosati bilan tanishish**

Najot Ta'lim o'quv markazining axborot xavfsizligi siyosati bilan batafsil tanishdim. Bu siyosat tashkilotning barcha axborot resurslarini himoya qilish, ma'lumotlar maxfiyligini ta'minlash va ularning yaxlitligini saqlashga qaratilgan qoidalar, tartiblar va chora-tadbirlarni o'z ichiga oladi. Siyosatni tushunish uchun maxsus hujjatlar va ko'rsatmalar bilan tanishdim, shuningdek, axborot xavfsizligi bo'yicha ichki qo'llanmalarni o'rgandim.

**Axborot xavfsizligini ta'minlash bo'yicha zarur chora-tadbirlarni o'rganish**

Axborot xavfsizligini ta'minlash uchun qanday chora-tadbirlar ko'rilishi kerakligini o'rgandim. Bu chora-tadbirlar quyidagilarni o'z ichiga oladi:

* **Foydalanuvchilarni autentifikatsiya qilish va avtorizatsiya qilish**: Foydalanuvchilar tizimga kirishda identifikatsiyalash va ularga ruxsat berilgan ma'lumotlarga kirishni ta'minlash.
* **Shifrlash texnologiyalari**: Ma'lumotlarni uzatishda va saqlashda shifrlash usullaridan foydalanish.
* **Antivirus va zararli dasturlarga qarshi himoya**: Tizim va tarmoqlarni zararli dasturlardan himoya qilish uchun antivirus dasturlarini o'rnatish va muntazam yangilash.
* **Tizim yangilanishlari va yamalash**: Operatsion tizimlar va dasturiy ta'minotlarni muntazam ravishda yangilab turish va xavfsizlik yamoqlarini qo'llash.

**Ma'lumotlarni himoya qilish usullari va axborot xavfsizligi bo'yicha eng yaxshi amaliyotlar haqida ma'lumot olish**

Axborot xavfsizligi bo'yicha eng yaxshi amaliyotlar haqida batafsil ma'lumot oldim. Bu amaliyotlar quyidagilarni o'z ichiga oladi:

* **Parol siyosati**: Kuchli parollardan foydalanish, ularni muntazam ravishda o'zgartirish va boshqa foydalanuvchilar bilan almashmaslik.
* **Foydalanuvchilarni o'qitish va xabardorlikni oshirish**: Foydalanuvchilarga axborot xavfsizligi bo'yicha muntazam treninglar o'tkazish va ularni xavfsizlik tahdidlari haqida xabardor qilish.
* **Tizim va tarmoqlarni monitoring qilish**: Tizim va tarmoqlarda yuzaga keladigan har qanday shubhali faoliyatni aniqlash va kuzatish uchun monitoring vositalaridan foydalanish.
* **Zaxira nusxalarini olish**: Ma'lumotlarni yo'qotishdan himoya qilish uchun muntazam ravishda zaxira nusxalarini olish va ularni xavfsiz saqlash.
* **Voqea javob rejasi**: Axborot xavfsizligi hodisalari yuz berganda ularga tezkor va samarali javob berish uchun voqea javob rejalarini ishlab chiqish va amaliyotga joriy etish.

Axborot xavfsizligi bo'yicha o'rganganlarim va amaliyotlarim menga o'quv markazidagi ma'lumotlarni xavfsiz saqlash va himoya qilish bo'yicha muhim ko'nikmalarni egallashimga yordam berdi. Bu bilimlar kelajakdagi faoliyatimda ham foydali bo'lishiga ishonaman.

**2. Xavfsizlikni oshirish va muammolarni hal qilish**

**Saytda yuzaga keladigan xavfsizlik muammolarini aniqlash va bartaraf etish**

Saytda yuzaga kelishi mumkin bo'lgan xavfsizlik muammolarini aniqlash va ularni bartaraf etish bo'yicha chuqur bilim oldim. Bu jarayon quyidagi bosqichlarni o'z ichiga oladi:

* **Tahdid tahlili**: Saytga tahdid solishi mumkin bo'lgan omillarni aniqlash va ularning tahlilini o'tkazish. Bu kiber hujumlar, zararli dasturlar va boshqa xavf-xatarlardan himoyalanish uchun zarur.
* **Zaifliklarni aniqlash**: Saytda mavjud bo'lgan zaifliklarni topish uchun muntazam skanerlash va tahlillar o'tkazish. Bu zaifliklarni aniqlash uchun maxsus dasturiy vositalardan foydalandim.
* **Xavfsizlik choralarini ko'rish**: Aniqlangan zaifliklarni bartaraf etish uchun zarur xavfsizlik choralarini ko'rish. Bu choralarga xavfsizlik yamog'ini o'rnatish, parol siyosatini yangilash va foydalanuvchilarga xavfsizlik bo'yicha ko'rsatmalar berish kiradi.

**Xavfsizlik tizimlarini samarali boshqarish**

Xavfsizlik tizimlarini qanday qilib samarali boshqarish mumkinligi haqida amaliyot o'tadim. Bunda quyidagi bosqichlar amalga oshirildi:

* **Xavfsizlik siyosati**: O'quv markazining xavfsizlik siyosatini ishlab chiqish va joriy etish. Bu siyosat foydalanuvchilarning tizimga kirishi, ma'lumotlarni boshqarish va xavfsizlik choralarini qamrab oladi.
* **Xavfsizlik protokollari**: Tizimda foydalaniladigan xavfsizlik protokollarini sozlash va boshqarish. Bu protokollar ma'lumotlarni himoya qilish, autentifikatsiya va avtorizatsiya jarayonlarini ta'minlash uchun zarur.
* **Foydalanuvchilarni boshqarish**: Foydalanuvchilarning tizimga kirish huquqlarini boshqarish, ularning faoliyatini kuzatish va zarur hollarda cheklash. Bu, ayniqsa, maxfiy ma'lumotlarga kirishni cheklash uchun muhimdir.

**Internet tarmog'ida xavfsizlikni ta'minlash uchun zarur dasturiy va apparat vositalari**

Internet tarmog'ida xavfsizlikni ta'minlash uchun zarur bo'lgan dasturiy ta'minot va apparat vositalari bilan tanishdim. Bunda quyidagi vositalar va texnologiyalar o'rganildi:

* **Firewall**: Internetdan keladigan va ketadigan trafikni nazorat qilish va xavfsizlik siyosatiga muvofiq filtrlash uchun ishlatiladigan dasturiy yoki apparat vositasi.
* **IDS/IPS tizimlari**: Intrusion Detection System (IDS) va Intrusion Prevention System (IPS) tizimlari yordamida tarmoqqa kiruvchi zararli faoliyatlarni aniqlash va oldini olish.
* **Antivirus dasturlari**: Kompyuter va tarmoqlarda zararli dasturlardan himoyalanish uchun foydalaniladigan dasturlar. Ushbu dasturlarni o'rnatish va muntazam yangilash orqali tizim xavfsizligini ta'minlash.
* **VPN (Virtual Private Network)**: Xavfsiz va maxfiy tarmoq ulanishini ta'minlash uchun ishlatiladigan texnologiya. VPN orqali foydalanuvchilar internetga xavfsiz ulanishlari mumkin.
* **Shifrlash**: Ma'lumotlarni shifrlash orqali ularning maxfiyligini va yaxlitligini ta'minlash. Shifrlash texnologiyalari, jumladan SSL/TLS protokollari, ma'lumotlarni uzatishda va saqlashda foydalaniladi.

Bu bilimlar va amaliyotlar xavfsizlik tizimlarini samarali boshqarish, internet tarmog'ida xavfsizlikni ta'minlash va sayt xavfsizligini oshirishda katta yordam berdi. Hisobotda keltirilgan tajribalar kelajakdagi xavfsizlik choralarini yanada rivojlantirish va mustahkamlashga zamin yaratadi.

**3. Wi-Fi tizimi bo'yicha amaliyot**

**Wi-Fi tizimini boshqarish**

O'quv markazining Wi-Fi tizimini boshqarish bo'yicha amaliyot o'tadim. Ushbu jarayonda tizimni sozlash, xavfsizlik choralarini amalga oshirish va ulanish jarayonlarini to'g'ri boshqarish usullarini o'rgandim.

* **Tarmoq sozlashlari**: Wi-Fi tarmog'ining SSID (Service Set Identifier) ni belgilash, parolni o'rnatish va tarmoqni yashirin qilish kabi asosiy sozlashlarni amalga oshirdim. Bu tarmoqning foydalanishga qulayligini oshiradi va xavfsizlikni ta'minlashga yordam beradi.
* **Xavfsizlik sozlamalari**: WPA3 (Wi-Fi Protected Access 3) xavfsizlik protokolini o'rnatish orqali Wi-Fi tarmog'ining xavfsizligini ta'minladim. Shuningdek, tarmoqga kirish ruxsatini autentifikatsiya qilish, MAC-manzil filtering va VPN orqali tarmoqni himoyalash usullarini qo'lladim.
* **Ulanish jarayonlari**: Foydalanuvchilarni Wi-Fi tarmog'iga ulanishda qo'llaniladigan protseduralar bilan tanishtirdim. Bu jarayon ulanish uchun zarur bo'lgan SSID va parolni taqdim etishni, shuningdek, muammolar yuzaga kelganda foydalanuvchilarga yordam ko'rsatishni o'z ichiga oladi.

**Wi-Fi tarmog'ida yuzaga keladigan muammolarni aniqlash va hal qilish**

Wi-Fi tarmog'ida yuzaga kelishi mumkin bo'lgan muammolarni aniqlash va bartaraf etish bo'yicha amaliy mashg'ulotlar o'tadim.

* **Signallarning sifati**: Wi-Fi signallarining kuchini o'lchash va kam quvvatli joylarni aniqlash uchun maxsus dasturiy ta'minotlardan foydalanish. Bu muammolarni hal qilish uchun qo'shimcha Access Point (AP) larni o'rnatish yoki mavjud AP larni qayta joylashtirish ishlari amalga oshirildi.
* **Interferensiya**: Wi-Fi tarmoqlarining interferensiyasini aniqlash va bartaraf etish. Bu uchun turli kanallarni sinab ko'rish va optimal kanalni tanlash usullaridan foydalandim.
* **Tarmoq uzilishlari**: Wi-Fi tarmog'ida yuzaga keladigan uzilishlarni aniqlash va bartaraf etish usullarini o'rgandim. Bu usullar routerni qayta yuklash, firware yangilash va tarmoq uskunalarini tekshirishni o'z ichiga oladi.

**4. Yangi optik tolali Wi-Fi tortish**

**Yangi optik tolali Wi-Fi tizimini o'rnatish**

O'quv markazining yangi xonalariga yangi optik tolali Wi-Fi tizimini o'rnatish jarayonida ishtirok etdim. Ushbu jarayonda optik tolali tarmoqlarni o'rnatish, sozlash va sinovdan o'tkazish bo'yicha amaliyot o'tadim.

* **Optik tolali kabellarni o'rnatish**: Optik tolali kabellarni o'rnatish jarayonida ishtirok etdim. Bu kabellar yuqori tezlik va katta hajmdagi ma'lumotlarni uzatish imkonini beradi. Kabellarni joylashtirish va ulanish nuqtalarini aniqlash bo'yicha bilim oldim.
* **Wi-Fi uskunalarini o'rnatish va sozlash**: Wi-Fi router va access pointlarni o'rnatish, ulanish sozlamalarini amalga oshirish va ularni tarmoq bilan bog'lash jarayonida ishtirok etdim.
* **Sinov va sozlash**: O'rnatilgan optik tolali Wi-Fi tizimini sinovdan o'tkazdim. Bu jarayonda tarmoqning ishlashini tekshirish, signallarni o'lchash va zarur hollarda sozlashlarni amalga oshirish bo'yicha amaliyot o'tadim.

**Optik tolali Wi-Fi tarmoqlarining afzalliklari va ulanish tezligini oshirish**

Optik tolali Wi-Fi tarmoqlarining afzalliklari va ulanish tezligini oshirish usullari bilan tanishdim.

* **Tezlik va ishonchlilik**: Optik tolali tarmoqlar yuqori tezlik va ishonchlilikni ta'minlaydi. Bu tarmoqlar katta hajmdagi ma'lumotlarni uzatishda, videokonferensiyalar va real vaqtda xizmatlarda juda samarali.
* **Keng qamrov**: Optik tolali tarmoqlar keng qamrovni ta'minlaydi va signal sifatini yaxshilaydi. Bu tarmoq orqali ko'plab foydalanuvchilar yuqori sifatli ulanishdan foydalanishi mumkin.
* **Xavfsizlik**: Optik tolali tarmoqlar yuqori xavfsizlikni ta'minlaydi, chunki ma'lumotlar tolali kabellar orqali uzatiladi va ularni sezish yoki soxta signal jo'natish deyarli imkonsiz.

Ushbu amaliyotlar menga o'quv markazining Wi-Fi tarmog'ini boshqarish va yangi optik tolali Wi-Fi tizimini o'rnatish bo'yicha muhim tajriba va bilimlarni berdi. Bu bilimlar va ko'nikmalar kelajakdagi texnik ishlarda va xavfsizlikni ta'minlashda juda foydali bo'lishiga ishonaman.

**5. Server bilan tanishish**

**Server arxitekturasi va komponentlari**

O'quv markazining serveri va uning arxitekturasi bilan tanishdim. Bu jarayonda serverning asosiy qismlari va ularning vazifalari haqida batafsil ma'lumot oldim:

* **Protsessor (CPU)**: Serverning asosiy hisoblash kuchini ta'minlaydi. Protsessor serverning samaradorligi va tezligini belgilaydi.
* **Operativ xotira (RAM)**: Ma'lumotlarni vaqtincha saqlash va tezkor ishlov berish uchun ishlatiladi. Ko'p yadroli protsessorlar bilan birgalikda katta hajmdagi RAM samarali ishlash uchun zarur.
* **Qattiq disklar (HDD/SSD)**: Doimiy ma'lumotlar saqlanadi. SSD disklari yuqori tezlik va ishonchlilikni ta'minlaydi.
* **Tarmoqqa ulanish (Network Interface Card - NIC)**: Serverni tarmoq bilan bog'lash uchun ishlatiladi. Gigabit va 10 Gigabit tarmoqli kartalar serverning tarmoqdan foydalanish imkoniyatlarini kengaytiradi.
* **Kiritish/chiqarish portlari**: Serverga tashqi qurilmalarni ulash uchun ishlatiladi.

**Serverning ishlash prinsiplari**

Serverning ishlash prinsiplari bo'yicha bilim oldim. Serverlar mijozlarga xizmat ko'rsatish uchun maxsus dasturiy ta'minotlar orqali ma'lumotlarni qayta ishlaydi va saqlaydi. Ular mijozlarning so'rovlarini qabul qilib, qayta ishlaydi va natijalarni qaytaradi. Serverlar quyidagi asosiy funksiyalarni bajaradi:

* **Mijoz-server modeli**: Serverlar mijozlardan kelgan so'rovlarni qabul qiladi, ularni qayta ishlaydi va natijalarni mijozlarga yuboradi.
* **Ma'lumotlar bazasi boshqaruvi**: Ma'lumotlarni saqlash va boshqarish uchun serverda ma'lumotlar bazalari o'rnatiladi va ularga so'rovlar yuboriladi.
* **Veb-serverlar**: Veb-sahifalarni mijozlarga yetkazib berish uchun veb-serverlar o'rnatiladi. Apache, Nginx kabi veb-server dasturlari keng qo'llaniladi.

**Serverni boshqarish va nazorat qilish**

Serverni boshqarish va nazorat qilish bo'yicha amaliy mashg'ulotlar o'tadim. Bu jarayonda quyidagi amallarni o'rgandim:

* **Tizim monitoringi**: Serverning ishlash holatini kuzatish uchun monitoring vositalaridan foydalanish. Bu vositalar CPU, RAM, disk va tarmoq yuklamalarini kuzatish imkonini beradi.
* **Zaxira nusxalarini olish**: Ma'lumotlarni yo'qotishdan himoya qilish uchun muntazam ravishda zaxira nusxalarini olish.
* **Xavfsizlik choralarini ko'rish**: Server xavfsizligini ta'minlash uchun firewall sozlash, foydalanuvchi ruxsatnomalarini boshqarish va xavfsizlik yangilanishlarini amalga oshirish.

**6. Server protokollari bo'yicha bilim olish**

**Serverning ishlash protokollari**

O'quv markazining serveri qaysi protokollarda ishlashi haqida ma'lumot oldim. Server asosiy protokollar orqali tarmoq bilan muloqot qiladi:

* **TCP (Transmission Control Protocol)**: Ma'lumotlarni uzatishda ishonchli aloqani ta'minlaydi. Bu protokol ma'lumotlarni paketlarga bo'lib yuboradi va ularni qabul qilishni nazorat qiladi.
* **HTTPS (HyperText Transfer Protocol Secure)**: Veb-saytlar va foydalanuvchilar o'rtasida xavfsiz aloqani ta'minlaydi. HTTPS SSL/TLS protokollari orqali ma'lumotlarni shifrlaydi.

**Protokollarni sozlash va xavfsizlikni ta'minlash**

Protokollarni sozlash, xavfsizlikni ta'minlash va tarmoq trafikini boshqarish bo'yicha amaliyot o'tadim:

* **TCP sozlash**: TCP ulanishlarini sozlash va optimallashtirish, ma'lumotlar uzatish tezligini oshirish va tarmoq samaradorligini yaxshilash.
* **HTTPS o'rnatish**: HTTPS protokolini sozlash va xavfsiz ulanishlarni ta'minlash uchun SSL/TLS sertifikatlarini o'rnatish. Bu foydalanuvchilar va server o'rtasidagi ma'lumotlarni himoya qiladi.
* **Firewall sozlash**: Tarmoq trafikini boshqarish va serverni zararli hujumlardan himoya qilish uchun firewall sozlash.

**Protokollar bo'yicha muammolarni aniqlash va bartaraf etish**

Protokollar bo'yicha kelib chiqadigan muammolarni aniqlash va bartaraf etish usullari bilan tanishdim:

* **Trafik tahlili**: Tarmoq trafikini tahlil qilish va muammolarni aniqlash uchun maxsus vositalardan foydalanish.
* **Tarmoq diagnostikasi**: Ping, traceroute kabi vositalar yordamida tarmoq muammolarini aniqlash.
* **Muammolarni bartaraf etish**: Aniqlangan muammolarni bartaraf etish uchun zarur choralarni ko'rish, konfiguratsiya sozlamalarini yangilash va kerakli yamoqlarni qo'llash.

Ushbu amaliyotlar va bilimlar server arxitekturasi, ishlash prinsiplari va protokollar bo'yicha keng ko'lamli tushunchalarni hosil qilishda katta yordam berdi. Bu tajribalar kelajakdagi texnik ishlarda muvaffaqiyatli bo'lishimga katta hissa qo'shadi.

**7. Serverning filiallar bilan aloqasi**

**Filiallar bilan aloqa**

O'quv markazining boshqa filiallari bilan serverning qanday aloqa qilishini o'rgandim. Serverlar tarmoqqa ulangan holda ma'lumot almashadi va filiallar o'rtasida ma'lumot uzatish va qabul qilish jarayonlari amalga oshiriladi. Bu jarayonlarda quyidagi asosiy komponentlar va protokollar ishlatiladi:

* **VPN (Virtual Private Network)**: Filiallar o'rtasida xavfsiz ma'lumot almashishni ta'minlash uchun VPN texnologiyasidan foydalaniladi. Bu texnologiya internet orqali xavfsiz va shifrlangan ulanishni ta'minlaydi.
* **LAN (Local Area Network) va WAN (Wide Area Network)**: Filiallar ichida LAN tarmog'i, filiallar o'rtasida esa WAN tarmog'i orqali ma'lumot uzatiladi.
* **Qo'shimcha xavfsizlik**: Firewall va boshqa xavfsizlik choralarini qo'llash orqali tarmoq xavfsizligini oshirish.

**Uzilishlarni bartaraf etish**

Serverda uzilishlar bo'lsa, ularni qanday bartaraf etish kerakligi bo'yicha amaliy mashg'ulotlar o'tadim. Ushbu mashg'ulotlarda uzilishlarni aniqlash va tezda hal qilish usullarini o'rgandim:

* **Monitoring va diagnostika**: Uzilishlarni aniqlash uchun tarmoq monitoring vositalaridan foydalanish. Bu vositalar tarmoqning ishlash holatini kuzatish va uzilishlarni tezda aniqlash imkonini beradi.
* **Zaxira tizimlari**: Serverda uzilishlar yuzaga kelganda, zaxira tizimlar va replikatsiya orqali ma'lumotlarni tiklash. Bu ma'lumotlarning yo'qolishining oldini olish va xizmatlar davomiyligini ta'minlashda muhim rol o'ynaydi.
* **Qo'shimcha choralari**: Server va tarmoq uskunalarini muntazam ravishda yangilab turish, muammolarni bartaraf etish uchun o'z vaqtida zarur chora-tadbirlarni ko'rish.

**Tarmoqqa ulanish va uzatish jarayonlarini optimallashtirish**

Tarmoqqa ulanish va uzatish jarayonlarini optimallashtirish bo'yicha bilim oldim. Bu jarayonlar tarmoq samaradorligini oshirish va ma'lumot uzatish tezligini yaxshilash uchun muhimdir:

* **Qo'shimcha tarmoq uskunalari**: Qo'shimcha tarmoq uskunalari, masalan, router va switchlarni qo'shish orqali tarmoq samaradorligini oshirish.
* **Qo'shimcha kanallar**: Ma'lumot uzatish kanallarini kengaytirish va optimallashtirish. Bu tarmoq trafigini teng taqsimlash va uzilishlarni kamaytirishga yordam beradi.
* **Qo'shimcha sozlashlar**: Qo'shimcha tarmoq sozlamalari va protokollarini optimallashtirish. Bu jarayon ma'lumot uzatish tezligini oshirish va tarmoq samaradorligini yaxshilashga qaratilgan.

**8. Tizim monitoringi va xavfsizlik auditi**

**Tizim monitoringi**

Tizim monitoringi bo'yicha dasturlar va ularning ishlashini o'rgandim. Monitoring vositalari tizimning ishlash holatini kuzatish va muammolarni aniqlashda muhim rol o'ynaydi:

* **Nagios**: Tizim monitoringi uchun keng tarqalgan vositalardan biri. Nagios tarmoq uskunalari, serverlar, xizmatlar va boshqa komponentlarni kuzatish imkonini beradi.
* **Zabbix**: Yana bir keng tarqalgan monitoring vositasi. Zabbix tarmoq trafigi, xizmatlar va dasturlarni kuzatish uchun qulay interfeys va keng qamrovli funksiyalarni taqdim etadi.
* **Prometheus**: Monitoring va kuzatuv uchun ochiq manbali vosita. Prometheus real vaqtda tarmoq trafigi va tizim holatini kuzatish imkonini beradi.

**Xavfsizlik auditi**

Xavfsizlik auditi o'tkazish va tizimda yuzaga keladigan muammolarni aniqlash bo'yicha amaliy mashg'ulotlar o'tadim. Xavfsizlik auditi tizimning xavfsizlik holatini baholash va zaifliklarni aniqlashda muhim ahamiyatga ega:

* **Audit vositalari**: Xavfsizlik auditini o'tkazish uchun Nessus, OpenVAS kabi vositalardan foydalanish. Bu vositalar tizimdagi zaifliklarni aniqlash va xavfsizlik darajasini baholash imkonini beradi.
* **Xavfsizlik testlari**: Penetratsion testlar o'tkazish orqali tizimning zaif joylarini aniqlash. Bu testlar tizimning real hujumlarga qarshi chidamliligini baholashga yordam beradi.
* **Xavfsizlik siyosati**: Xavfsizlik siyosatini amalga oshirish va muntazam ravishda yangilash. Bu siyosat foydalanuvchilar ruxsatnomalari, ma'lumotlarni himoyalash va xavfsizlik choralari haqida qo'llanmalar taqdim etadi.

**Xavfsizlik auditi natijalarini tahlil qilish**

Xavfsizlik auditi natijalarini tahlil qilish va muammolarni bartaraf etish rejalari tuzishni o'rgandim. Bu jarayon tizimning xavfsizlik holatini yaxshilash va zaifliklarni bartaraf etishga qaratilgan:

* **Natijalarni tahlil qilish**: Xavfsizlik auditi natijalarini batafsil tahlil qilish va zaifliklarni aniqlash. Bu jarayon zaifliklarning sabablarini aniqlash va ularni bartaraf etish rejasini tuzishda muhimdir.
* **Bartaraf etish rejalari**: Muammolarni bartaraf etish uchun rejalar tuzish. Bu rejalarda xavfsizlik choralarini ko'rish, yangilanishlarni amalga oshirish va foydalanuvchilarni xavfsizlik haqida xabardor qilish kabi tadbirlar kiritiladi.
* **Muntazam auditlar**: Xavfsizlik holatini muntazam ravishda tekshirish va yangi zaifliklarni aniqlash uchun auditlar o'tkazish. Bu tizimning xavfsizlik darajasini doimiy ravishda yuqori darajada saqlashga yordam beradi.

Ushbu amaliyotlar va bilimlar tizim monitoringi, xavfsizlik auditi va tarmoq boshqaruvi bo'yicha keng qamrovli tushunchalarni hosil qilishda katta yordam berdi. Bu tajribalar kelajakdagi texnik ishlarda muvaffaqiyatli bo'lishimga katta hissa qo'shadi.

**9. Ma'lumotlar bazasi boshqaruvi**

**Ma'lumotlar bazasi yaratish va boshqarish**

O'quv markazining ma'lumotlar bazasini boshqarish bo'yicha amaliyot o'tadim. Ushbu jarayonda ma'lumotlar bazasi yaratish, ma'lumotlarni kiritish, yangilash va o'chirish jarayonlari bilan tanishdim:

* **Ma'lumotlar bazasini yaratish**: Ma'lumotlar bazasini yaratish uchun zarur bo'lgan SQL buyruqlarini o'rgandim. Bu buyruqlar yordamida jadval va boshqa ob'ektlarni yaratish imkoniyatiga ega bo'ldim.
* **Ma'lumotlarni kiritish**: Ma'lumotlar bazasiga yangi ma'lumotlarni kiritish uchun INSERT buyruqlarini ishlatishni o'rgandim. Ushbu jarayon ma'lumotlarni tez va samarali kiritish uchun muhimdir.
* **Ma'lumotlarni yangilash**: Ma'lumotlar bazasidagi mavjud ma'lumotlarni yangilash uchun UPDATE buyruqlarini ishlatishni o'rgandim. Bu buyruqlar yordamida ma'lumotlarni o'zgartirish va yangilash imkoniyatiga ega bo'ldim.
* **Ma'lumotlarni o'chirish**: Ma'lumotlar bazasidan kerak bo'lmagan ma'lumotlarni o'chirish uchun DELETE buyruqlarini ishlatishni o'rgandim. Bu jarayon ma'lumotlar bazasini toza va tartibli saqlashda muhim ahamiyatga ega.

**Ma'lumotlar bazasi muammolarini aniqlash va hal qilish**

Ma'lumotlar bazasida yuzaga keladigan muammolarni aniqlash va hal qilish bo'yicha bilim oldim. Ushbu jarayonlar ma'lumotlar bazasining samarali va ishonchli ishlashini ta'minlash uchun muhimdir:

* **Muammolarni aniqlash**: Ma'lumotlar bazasida yuzaga keladigan muammolarni aniqlash uchun diagnostika vositalaridan foydalanish. Bu vositalar ma'lumotlar bazasining ishlash holatini kuzatish va muammolarni tezda aniqlash imkonini beradi.
* **Muammolarni hal qilish**: Aniqlangan muammolarni hal qilish uchun zarur choralarni ko'rish. Bu choralar orasida ma'lumotlarni tiklash, konfiguratsiya sozlamalarini yangilash va ma'lumotlarni optimallashtirish kabi amallar mavjud.
* **Zaxira nusxa olish**: Ma'lumotlar bazasining zaxira nusxasini muntazam ravishda olish va zarur paytda tiklash imkoniyatiga ega bo'lish. Bu jarayon ma'lumotlarni yo'qotishdan himoya qilish va uzluksiz ishlashni ta'minlashda muhimdir.

**10. Zaxira nusxa olish va tiklash jarayonlari**

**Zaxira nusxa olish**

Server va ma'lumotlar bazasining zaxira nusxasini olish va tiklash jarayonlari bo'yicha amaliyot o'tadim. Ushbu jarayonlar ma'lumotlarni yo'qotishdan himoya qilish va uzluksiz ishlashni ta'minlash uchun muhimdir:

* **Zaxira nusxa olish usullari**: Zaxira nusxa olishning eng yaxshi usullarini o'rganib chiqdim. Bunga to'liq zaxira olish, inkremental zaxira olish va differentsial zaxira olish usullari kiradi. Har bir usulning afzalliklari va kamchiliklarini o'rganib, qaysi usulni qaysi holatda qo'llash kerakligini tushundim.
* **Avtomatlashtirilgan zaxira olish**: Zaxira olish jarayonlarini avtomatlashtirish uchun skriptlar va dasturlar yaratishni o'rgandim. Bu avtomatlashtirilgan jarayonlar zaxira olishni muntazam va ishonchli amalga oshirish imkonini beradi.
* **Zaxira nusxasini tekshirish**: Olingan zaxira nusxalarining yaxlitligini va to'liqligini tekshirish. Bu jarayon ma'lumotlarning to'liq va zarar ko'rmagan holda zaxiraga olinganligini ta'minlashda muhimdir.

**Zaxira nusxasini tiklash**

Zaxira nusxasini tiklash jarayonlarini o'rganib chiqdim. Ushbu jarayonlar ma'lumotlarni yo'qotishdan keyin tiklash va tizimni qayta tiklash uchun zarurdir:

* **Tiklash usullari**: Zaxira nusxasini tiklashning eng yaxshi usullarini o'rganib chiqdim. Bu usullar orasida to'liq tiklash, inkremental tiklash va differentsial tiklash kabi usullar mavjud. Har bir usulning afzalliklari va kamchiliklarini o'rganib, qaysi usulni qaysi holatda qo'llash kerakligini tushundim.
* **Tiklash jarayonlari**: Zaxira nusxasini tiklash jarayonlarini amaliyotda qo'llashni o'rgandim. Bu jarayonlar tizimni qayta tiklash va ma'lumotlarni yo'qotishning oldini olish uchun muhimdir.
* **Muammolarni bartaraf etish**: Zaxira nusxasini tiklash jarayonlarida yuzaga keladigan muammolarni aniqlash va bartaraf etish. Bu jarayonlar tiklash jarayonini muvaffaqiyatli yakunlash va tizimni uzluksiz ishlashini ta'minlash uchun muhimdir.

Ushbu amaliyotlar va bilimlar ma'lumotlar bazasi boshqaruvi, zaxira nusxa olish va tiklash jarayonlari bo'yicha keng qamrovli tushunchalarni hosil qilishda katta yordam berdi. Bu tajribalar kelajakdagi texnik ishlarda muvaffaqiyatli bo'lishimga katta hissa qo'shadi.

Xulosa

10.06.2024-20.07.2024 kunlari tashkilotning axborot xavfsizligini oshirish va IT infratuzilmasini mustahkamlash bo‘yicha amalga oshirilgan chora-tadbirlar muvaffaqiyatli yakunlandi. Dastlab, axborot xavfsizligi bilan tanishish jarayoni o‘tkazilib, mavjud xavf-xatarlar va ularni bartaraf etish usullari o‘rganildi. Bu jarayon axborot xavfsizligi madaniyatini oshirish va xodimlar tomonidan xavfsizlikka rioya qilishni kuchaytirishga yordam berdi.

Xavfsizlikni oshirish va muammolarni hal qilish doirasida xavfsizlik tizimlari yangilandi va muhim infratuzilma elementlari nazoratga olindi. Wi-Fi tarmog‘i bo‘yicha o‘tkazilgan amaliyotlar natijasida, yangi optik tolali Wi-Fi texnologiyasiga muvaffaqiyatli o'tildi, bu esa tarmoqning tezligini va barqarorligini oshirdi.

Server tizimlari bilan tanishish va server protokollari bo'yicha bilim olish tashkilotning IT infratuzilmasini yanada optimallashtirishga imkon berdi. Serverlarning filiallar bilan aloqasi tekshirilib, ularning o'zaro bog'liqligi mustahkamlandi. Shu bilan birga, tizim monitoringi va xavfsizlik auditi muntazam ravishda amalga oshirilib, tarmoq va server tizimlarining xavfsizligi ta'minlandi.

Ma'lumotlar bazasi boshqaruvi jarayonlari takomillashtirilib, ma'lumotlarning yaxlitligi va xavfsizligi ta'minlandi. Zaxira nusxa olish va tiklash jarayonlari muvaffaqiyatli tashkil etilib, tizimning doimiy ishlash qobiliyati kafolatlandi. Ushbu kompleks chora-tadbirlar natijasida tashkilotning axborot xavfsizligi darajasi sezilarli darajada oshdi va IT infratuzilmasi barqaror va samarali ishlashni davom ettirishi ta'minlandi.