WEB SAYTLARDA MA'LUMOTLAR XAVFSIZLIGINI TA'MINLOVCHI DASTURLAR TAHLILI

To'ychiyev Xurshidbek Muxamatvali o'g'li
O'zbekiston xalqaro islom akademiyasi
xurshidbek7797@gmail.com

ANNOTATSIYA

Ushbu maqolada web saytlar va onlayn internet portallarining xavfsizligini ta'minlovchi dasturlar tahlil qilingan.

Kalit so'zlar: *Kerio Connect, NMAP, WinRouter, portlarni skaynerlash, UserGate, tarmoq xavfsizligi.*

ABSTRACT

This article analyzes programs that ensure the security of websites and online internet portals.

Keywords: *Kerio Connect, NMAP, WinRouter, port scanning, UserGate, network security.*

KIRISH

Hozirgi kunda ko'pgina korxonalar o'z tashkilotining muhim ma'lumotlarini (ko'p hollarda mijozlar va mijozlarning shaxsiy va moliyaviy ma'lumotlarini o'z ichiga oladi) saqlash va asosiy operatsiyalarini boshqarish uchun shaxsiy kompyuterlar, tarmoqlar va serverlardan foydalanmoqda. Bu esa yaxshi va ishonchli xavfsizlik tizimi juda muhimligini ta'kidlaydi.

Ilg'or texnologiyalarning paydo bo'lishi bilan kiberjinoyatchilar ham ko'plab tashkilotlar tizimiga kirishning ko'proq usullarini topdilar. Ko'proq korxonalar o'zlarining muhim operatsiyalarini dasturiy mahsulotlarga tayanayotganligi sababli, dasturiy ta'minot xavfsizligini ta'minlashning ahamiyatiga har qachongidan ham jiddiyroq munosabatda bo'lish kerak. Axborot texnologiyalari xavfsizlik dasturlari kabi ishonchli himoyaga ega bo'lish hisoblash muhiti va ma'lumotlaringizni himoya qilish uchun juda muhimdir.

Kiber tahdidlar qurboniga nafaqat hukumat yoki yirik korporatsiyalar aylanmaydi. Darhaqiqat, kichik va o'rta biznes so'nggi yillarda tobora ko'proq kiberjinoyatlar nishoniga aylangan. Kichik biznes korxonalari, shuningdek, kiberjinoyatchilar tomonidan to'g'ridan-to'g'ri va bilvosita biznes aloqalaridan foydalangan holda yirik korxonalarga kirish uchun shlyuz sifatida ishlatiladi. AQSh

Qimmatli qog‘ozlar va birjalar komissiyasi ma’lumotlariga ko‘ra, kichik biznesning yarmi kiberhujumlardan aziyat chekmoqda, buning natijasida biznes olti oy ichida yopiladi. Quyida ko‘rib turganingizdak, bu biznes uchun ancha qimmatga tushishi mumkin. Demak, kiberxavfsizlik butun biznes hamjamiyatiga

Web saytlar ma’lumotlarining xavfsizligini ta’minlash uchun bir nechta dasturiy komplekslar mavjud. Xavfsizlik komplekslarining himoyalash darajasi dastlabki barcha muhim xavfsizlik masalalarni hal etishda muhimdir. Ularning effektivligi web saytning xavfsizligi va hujumlar bilan bog‘liq ravishda ko‘rsatuvchi faktorlar bilan bog‘liq bo‘ladi. Web saytning muhim ma’lumotlarini va infrastrukturani himoyalashga imkon beruvchi yuqori darajadagi xavfsizlik komplekslari qo‘llanilishi tavsiya etiladi. Quyida web saytlar axborot xavfsizligini ta’minlovchi dasturiy komplekslarning eng keng tarqalgan turlari haqida ma’lumot keltirilgan.

Kerio Connect. Kerio Connect, bir tarmoq pochta serveri va birlikdagi boshqa kommunikatsiya xizmatlarini (kalendaring, kontaktlar, vazifalar) ta’min etuvchi dasturiy ta’minotdir. U korporativ tashkilotlarga tarmoq pochta va kommunikatsiya imkoniyatlarini taklif etish uchun ishlatiladi. Quyidagi xarakteristikalar Kerio Connect dasturiy ta’minotiga tegishli:

Tarmoq Pochta: Kerio Connect foydalanuvchilariga tarmoq pochta xizmatini taqdim etadi. Bu, foydalanuvchilarga elektron pochta xabarlarni jo‘natish, qabul qilish va boshqalar bilan pochta almashish imkoniyatlarini beradi.

Kontaktlar: Kerio Connect orqali, foydalanuvchilar shaxsiy va jamoatchilik kontaktlarini saqlayish, boshqarish va ularga kirish imkoniyatiga ega bo‘ladi. Bu, foydalanuvchilarga ma’lumotlarni to‘plab turish va ularga tezroq murojaat qilish imkoniyatini beradi.

Vazifalar: Kerio Connect, foydalanuvchilarga vazifalarni boshqarish va ularga murojaat qilish imkoniyatlarini taklif etadi. Bu, o‘z vaqtida vazifalarni belgilash, vazifalarni bajarishni nazorat qilish va ularga alohida vazifalar berish imkonini beradi.

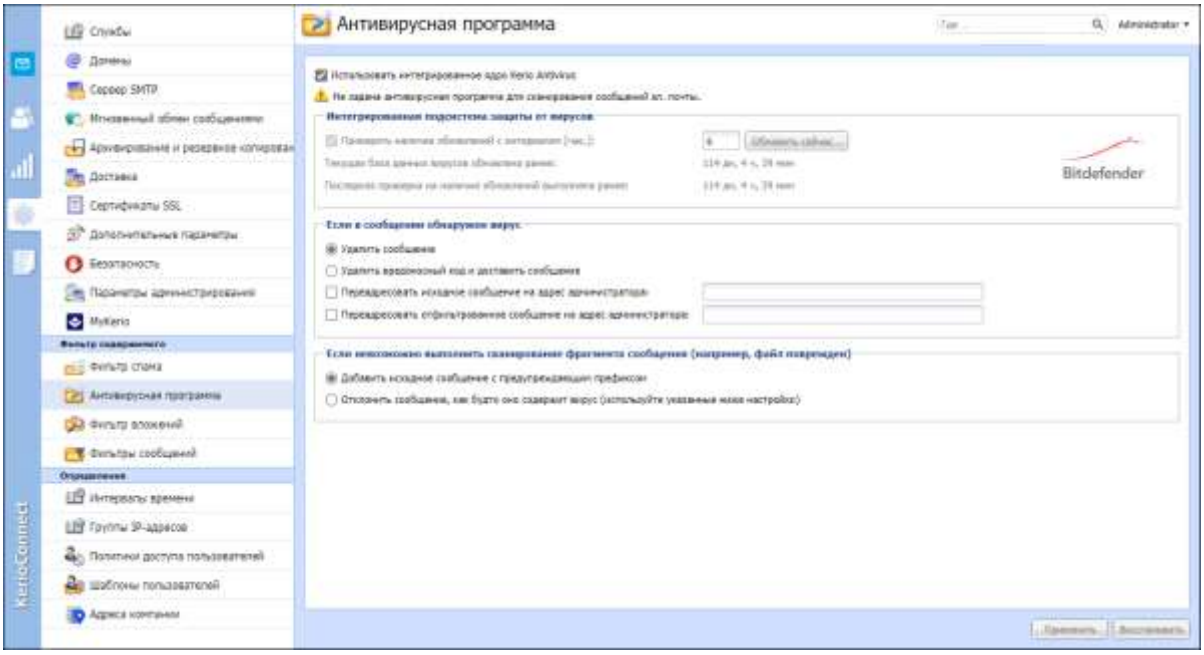
Xavfsizlik: Kerio Connect xavfsizlik tizimlari bilan muhofaza qilinadi. U, elektron pochta xabarlari, kalendaring ma’lumotlari, kontaktlar va boshqa ma’lumotlarni shifrlab turish, antivirustan o‘tkazib yuborish va saytdagi xavfsizlik uchun shifrlash protokollari bilan taminlash imkoniyatiga ega.

Platformalar orasida integratsiya: Kerio Connect, Windows, Mac OS, Linux va mobil platformalar (iOS va Android) bilan integratsiya qilish imkonini beradi. Bu foydalanuvchilar uchun alohida qulaylik va o‘tish imkoniyatini beradi.

Bu faqat bir nechta xususiyatlarni o‘z ichiga olgan Kerio Connect dasturiy ta’minotining umumiy xarakteristikalaridir.

Dastur hozirda uni yangilashlar va qo‘shimchalarni qo‘llab-quvvatlash uchun ommaviy jamlanma tomonidan taqdim etiladi. To‘liq tafsilotlar va yangiliklar uchun,

Kerio Connect rasmiy veb-saytini va ularning tarqatuvchi tomonidan taqdim etilgan ma’lumotlarni ko‘rib chiqishingiz tavsiya etiladi.



1-rasm. Kerio Connect dasturiy kompleksining interfeysi[1]

Har qanday himoya mexanizmi tutilgan xabar bilan harakatlarni belgilashgacha sozlanishi mumkin.

Elektron pochta SSL/TLS, S/MIME shifrlash, spamga qarshi filtrlar, antivirus va ko‘p qatlamli tekshiruvlar yordamida xakerlik va hujumlardan himoyalangan. Zaxiradan qisman tiklash qobiliyatiga ega avtomatik zaxiralash, hatto jiddiy nosozlik bo‘lsa ham, ma’lumotlarni tezda tiklash imkonini beradi.

NMAP. Nmap ("Tarmoq xaritasi") tarmoqni aniqlash va xavfsizlik auditi uchun bepul va ochiq manbali yordamchi dasturdir.

Nmap (Network Mapper), bir xavfsizlik skanneri va tarmoq inventarizatsiya dasturi sifatida mashhur bo‘lgan ma’lumotlar to‘plamidir. U tarmoqdagi qurilmalarni skanlash va ularga bog‘liq portlar, xizmatlar, tarmoq topologiyasi va xavfsizlik tahlillarini bajarish imkonini beradi. Quyidagi xarakteristikalar Nmap dasturiy ta’minotiga tegishli.

Tarmoq inventarizatsiya: Nmap tarmoqda joylashgan qurilmalarni aniqlayish uchun qo‘llaniladi. U tarmoqdagi IP manzillarini va tizimlarni aniqlayadi, tarmoqni topologiyasini yaratishda yordam beradi.

Port skanlash: Nmap qurilmalardagi ochiq portlarni aniqlash va ularga bog‘liq xizmatlarni identifikatsiya qilish uchun ishlatiladi. Bu, tarmoqdagi qurilmalar va ularda ishlashda bo‘lgan portlar haqida ma’lumot olishga imkon beradi.

[1] https://gfi-software.ru/images/thumbs/KerioConnectA-1602360083-op.png

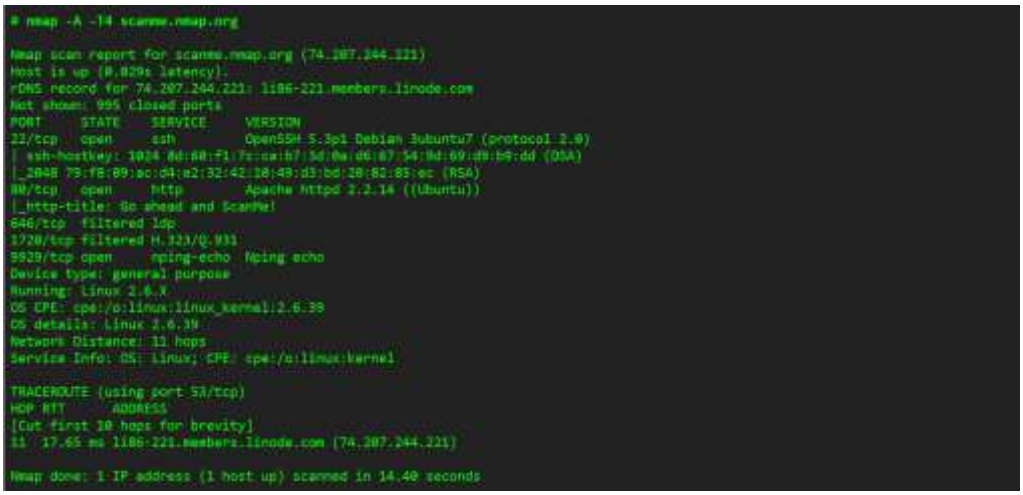
Xavfsizlik tahlillari: Nmap o‘rtasida xavfsizlik skanlari ham ishga tushirishi mumkin. U tarmoqdagi qurilmalar va ularga bog‘liq xizmatlarni xavfsizlik bo‘yicha tekshirib, potentsial xavfsizlik ko‘chalarni aniqlash imkonini beradi.

Amaliy hujumlar: Nmap amaliy hujumlar uchun ishlatilishi mumkin. U qurilmalar va ularga bog‘liq xizmatlarga qarshi hujumlar ko‘rish uchun imkoniyatlar taqdim etadi. Bu, tarmoqni xavfsizlikni oshirish va potentsial xavfsizlik masalalarini aniqlashga yordam beradi.

Skan natijalarini tahlil qilish: Nmap yordamida olingan skan natijalarini tahlil qilish va bu ma’lumotlarni bir faylda yig‘ish imkoniyati mavjud. Bu, tarmoq administratorlari va xavfsizlik mutaxassislarining tahlil qilish, ko‘rib chiqishlarini tuzish va ularga qarshi qadam atish imkonini beradi.

Nmap dasturiy ta’minoti o‘zida boshqa ko‘plab xususiyatlar ham o‘z ichiga oladi, ammo yuqoridagi xususiyatlarga asoslangan bo‘lib, tarmoqdagi inventarizatsiya, port skanlash, xizmat versiyasini aniqlash, xavfsizlik tahlillari va amaliy hujumlar bilan bog'liq vazifalarni bajarish imkoniyatlarini beradi.

2-rasm. NMAP dasturida tarmoqlarni skanerlash jarayoni[1]



Nmap (Network Mapper) dasturiy ta’minoting asosiy avzalliklari quyidagilardir:

Port skanlash: Nmap qurilmalardagi ochiq portlarni aniqlash uchun ishlatiladi. Bu, tarmoqdagi qurilmalar va ularda ishlaydigan xizmatlarni identifikatsiya qilishga imkon beradi.

Versiya aniqlash: Nmap qurilmalardagi xizmatlar versiyalarini aniqlash imkonini beradi. Bu, tarmoqdagi qurilmalar va ularda ishlashda bo‘lgan xizmatlarning yangilanishi, xavfsizlik yomonlashtirishlarini aniqlashga yordam beradi.

[1] https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQLyV3OzLSeywRRsBkVTX_tgb0yS4b4Bdx8ws0uwFgonZLA__Dvxg9o_I9uf3Vog6MEYwE&usqp=CAU

Tarmoq inventarizatsiya: Nmap tarmoqdagi IP manzillarini va ularda ishlashda bo‘lgan qurilmalarni aniqlayishda yordam beradi. Bu, tarmoqdagi tizimlarni topologiyasini yaratish va tarmoq xaritasi yaratish imkonini beradi.

Xavfsizlik skanlari: Nmap tarmoqdagi qurilmalarni xavfsizlik bo‘yicha tekshirishga imkon beradi. U potentsial xavfsizlik ko‘chalarni aniqlash va tarmoqdagi xavfsizlik holatini tahlil qilishga yordam beradi.

Amaliy hujumlar: Nmap amaliy hujumlar uchun ham ishlatiladi. U qurilmalarga hujum yuborish, tarmoqdagi xavfsizlik holatini sinovga olish va xavfsizlik masalalarini aniqlash imkonini beradi.

Scripting imkoniyatlari: Nmap, Lua skriptlash tilidan foydalanish imkonini beradi. Bu, foydalanuvchilarning xususiy talablari va tarmoqdagi xavfsizlikning boshqa asosiy muammolari uchun mos skriptlarni yozishga imkon beradi.

Platformalar orasida ishlov berish: Nmap Windows, Mac OS, Linux va boshqa bir nechta platformalar uchun mavjud bo‘lgan, shuningdek, mobil qurilmalar uchun ham imkoniyatlar taqdim etadi.

Nmap dasturiy ta’minoti ko‘p yo‘nalishlarda foydalaniladi va xavfsizlik mutaxassislarining va tarmoq administratorlarining tarmoqdagi qurilmalarni tekshirish, tahlil qilish va xavfsizlikni ta’minlashda qo‘llaniladi.

WinRouter. WinRouter, tarmoqning tuzilishi va boshqarilishi, tarmoq xizmatlarini ta’minlash va tarmoq xavfsizligini oshirish uchun ishlatiladigan dasturiy ta’minotdir. U quyidagi xususiyatlarga ega bo‘lishi mumkin:

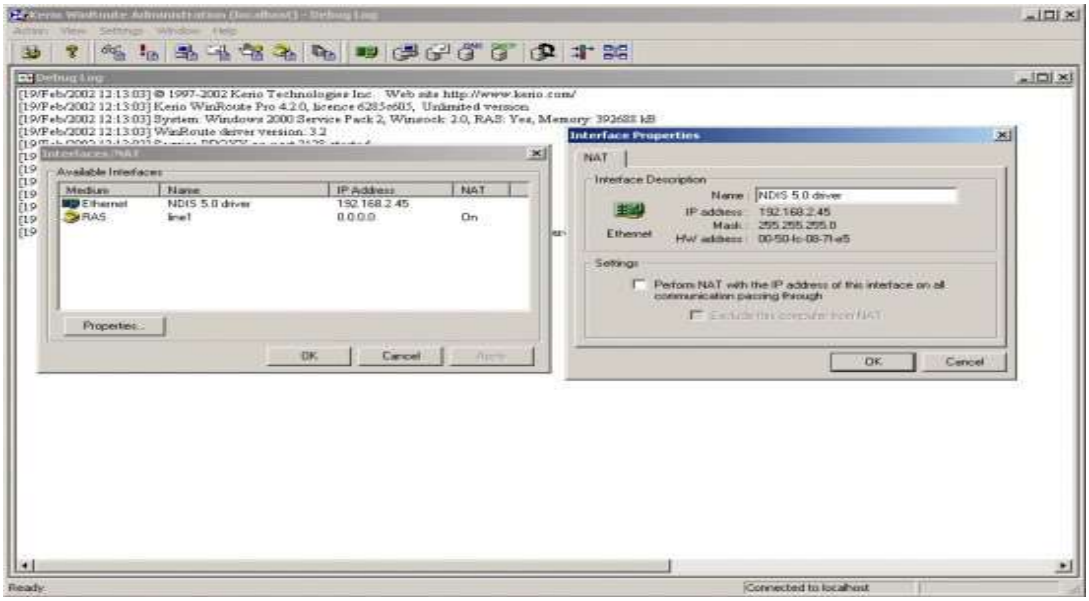
Tarmoqning boshqarilishi: WinRouter tarmoqni boshqarish imkoniyatlarini taqdim etadi. Bu tarmoqni tuzish, tuzatish, IP manzillarini boshqarish, ro‘yxatdan o‘tkazish va tarmoqdagi qurilmalarni boshqarishga imkon beradi.

Tarmoq xizmatlarini ta’minlash: Dastur tarmoqdagi xizmatlarni ta’minlash imkoniyatlarini beradi. Bu xizmatlar orasida tarmoq pochta, aloqa protokollari, VPN, kengaytirilgan tarmoq xavfsizligi va boshqalar bo‘lishi mumkin.

Xavfsizlik: WinRouter tarmoq xavfsizligini ta’minlash uchun xavfsizlik tahlillarini va xavfsizlik sozlamalarini o‘rnatish imkonini beradi. U veb-fayllarni filtrlash, portlar ustida monitorlik qilish, veb-saytlarni bloklash va xavfsizlik sozlamalari yaratish uchun qo‘llaniladi.

Qo‘shimcha funktsiyalar: WinRouterning qo‘shimcha funktsiyalari o‘rnatish mumkin. Bu, VLAN, QoS (xizmat sifati), bandlik boshqarish, SNMP monitoringi, to‘plam manzillar va boshqalar kabi imkoniyatlarni oshirishni o‘z ichiga oladi.

Statistik ma’lumotlar: Dastur tarmoqdagi trafik statistikasini ko‘rsatish, ulardan tahlil olish va tarmoqdagi yuqori trafik yoki xato holatlarni aniqlash imkonini beradi.



3-rasm. WinRouter dasturiy ta’minoti interfeysi[1]

Monitoring va tanlov: WinRouter, tarmoqdagi qurilmalarni va ularda ishlashdagi xizmatlarni monitor qilish va ularga mos tanlovlar qilish imkonini beradi. Bu, tarmoqdagi xavfsizlik muammolarini aniqlash va ularga tezroq javob berishga yordam beradi.

Konfiguratsiya va barcha sozlamalar: Dastur, tarmoq sozlamalarini va konfiguratsiyalarini o‘rnatish, barcha sozlamalar va o‘zgarishlarni boshqarish imkonini beradi.

WinRouter dasturiy ta’minoti tarmoq administratorlari va tarmoq tuzishchilari tomonidan tarmoqni boshqarish, xavfsizlikni ta’minlash va tarmoq xizmatlarini optimallashtirish uchun qo‘llaniladi. U foydalanuvchilarga tarmoqdagi qurilmalarni tahlil qilish va boshqarishda yordam beradi. Shuningdek, dastur iste’mol qilishni oson va samarali qilishga intiladi.

UserGate. UserGate dasturiy ta’minoti, tarmoqdagi internet trafiklarini boshqarish va tarmoq xavfsizligini ta’minlash uchun ishlatiladigan dasturdir. U quyidagi xususiyatlarga egadir:

Tarmoqning boshqarilishi: UserGate tarmoqdagi internet trafikini boshqarish imkonini beradi. Bu tarmoqdagi tizimlarni va ularga kiradigan internet trafiklarini boshqarish, filtrlash, qosib olish, kirishni cheklash va chiqishni tartibga solishni o‘z ichiga oladi.

[1] https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRH7Kb_JFVuOdOWwJVQAA6iv3Yc0XV7BZLhwg&usqp=CAU

Internet xavfsizligi: Dastur tarmoqdagi xavfsizlikni ta’minlash uchun xavfsizlik sozlamalarini va tahlilini o‘rnatish imkonini beradi. U web saytlarni filtrlash, zararli fayllarni bloklash, DDoS hujumlariga qarshi himoya ta’minlash, veb-fayllar va elektron pochtalardagi viruslarni aniqlash va boshqalar kabi xavfsizlik imkoniyatlarini taqdim etishi mumkin.

Qo‘shimcha funktsiyalar: UserGate tarmoq boshqaruvini osonlashtirish uchun qo‘shimcha funktsiyalar taqdim etadi. Bu, VPN tarmoqlarini o‘rnatish, DNS-sorovlarni boshqarish, tarmoq monitoringini o‘rnatish, bandlik boshqarish va boshqalar kabi imkoniyatlarni oshirishni o‘z ichiga oladi.

Statistik ma’lumotlar: Dastur tarmoqdagi internet trafikining statistik ma’lumotlarini ko‘rsatish, ulardan tahlil olish va tarmoq holatini monitoring qilish imkonini beradi. Bu, tarmoq boshqaruvchilari uchun trafik yoki xato holatlarini tahlil qilishga yordam beradi.

Filtrlash va cheklash: UserGate tarmoqdagi internet trafikini filtrlash va cheklash imkonini beradi. Bu, tarmoq administratorlarining foydalanuvchilar uchun tarmoqdagi saytlar va xizmatlarga kirishni cheklash, foydalanuvchilarning faolligini nazorat qilish va tarmoqdagi zararli yoki nafaqatli saytlarni bloklashga yordam beradi.