AZƏRBAYCAN RESPUBLİKASI ELM və TƏHSİL NAZİRLİYİ
AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əlyazması hüququnda

MUSTAFAYEVA QUMRAL ABUBƏKİR qızı
NƏSİROV NURLAN SÜBHAN oğlu
VƏLİZADƏ YUSİF RASİM oğlu
MƏLİKMƏMMƏDOV ELTAC ELŞAD oğlu
MƏMMƏDZADƏ KƏRİM XƏLİYYƏDİN oğlu

AzTU-nun kompüter şəbəkəsində informasiya təhlükəsizliyinin qiymətləndirilməsi sisteminin işlənməsi

mövzusunda

MAGİSTRLİK DİSSERTASİYASI

İxtisas: 060631 " Kompüter mühəndisliyi"
İxtisaslaşma: "Biliklərin əldə edilməsi sistemləri"

Elmi rəhbər: t.f.d., dosent C. Məmmədov

BAKI – 2023

MÜNDƏRİCAT

İxtisarların siyahısı

LAN – Local Area Network

OSI - Open Systems Interconnection

PoE - Power over Ethernet

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

RHI – Route Health Injection

AFM – Advanced Firewall Manager

DDoS – Distributed Denial-Of-Service

WLAN – Wireless Local Area Network

WAP – Wireless Application Protocol (WAP)

WLC – Wireless LAN Controller

CAPWAP – Control and Provisioning of Wireless Access Points

BSS – Basic Service Set

LWAP – Lightweight Access Point

TKIP – Temporal Key Integrity Protocol

AES – Advanced Encryption Standard

DHCP – Dynamic Host Configuration Protocol

VPN – Virtual Private Network

GPRS – General Packet Radio Service

FTP – File Transfer Protocol

SMTP – Simple Mail Transfer Protocol

URL – Uniform Resource Locator

WWW – World Wide Web

WAF – Web Application Firewall

CSP – Content Security Policy

CSRF – Cross-site request forgery

ASAS – AzTUSecurity-Analyzer System

GİRİŞ

Mövzunun aktuallığı. Özəl və dövlət sektorlarında şəbəkə texnologiyalarına tələbat zaman keçdikcə artır. Müəssisələrdə istifadə edilən kompüterlər, printerlər, ip telefonlar və bu tipli cihazların hər birini idarə etmək üçün məqsədyönlü şəkildə mərkəzi bir tətbiq üsuluna ehtiyac duyulur. XX əsrin sonlarında texnologiyanın inkişafında güclü irəliləyişlər oldu. OSI şəbəkə modeli adlandırdığımız protokolun səviyyələrinin hər birində şəbəkədə istifadə edilən cihazların və onların parametrlərinin bölgüsü aparılmışdır. İlk zamanlar istifadə edilən cihazlar idarə edilmə qabiliyyəti və təhlükəsizliyi olmayan, yalnız bağlantıları qurmaq üçün istifadə edilən avadanlıqlar idi. Müasir dünyada bu cihazlara tələbat artdıqca, inkişaf baxımından mükəmməl işlərə imza atıldı. Artıq kiçik məkanlar üçün yox, müəssisələr, şəhərlər, hətta ölkələr arası güclü infrastruktur sayəsində yeni xidmətlər, yüksək sürətli internet, tətbiqlərin istifadəsi daha da asanlaşdı. Korporativ müəssisələrdə şəbəkənin rolu çox önəmlidir. Şəbəkədə istifadə edilən switch, router, hub və s. tipli cihazlar bağlantıların qurulması üçün istifadə edilən sistemdə mərkəzi rolu üstlənirlər. İnformasiyanın ötürülməsi, təhlükəsizliyi, saxlanılması kimi parametrlərin hər birini təmin edirlər.

Universitet üçün qurulan şəbəkəni bir neçə hissəyə bölmək olar. Rəhbərlik, müəllim heyəti, işçilər və tələbələr üçün daxili şəbəkədə bu qurğular vasitəsi ilə icazələr və qadağalar tətbiq edilir. Şəbəkə daxilində istifadəçinin internet xidmətinin olması, bəzi sənəd proqramlarının istifadəsi və bu kimi prosedurların icazəsi şəbəkə administratorları tərəfindən qoyulan təhlükəsizlik siyasətinə əsasən aparılır. Korporativ şəbəkələr də yalnız naqilli bağlantılarla deyil, həmçinin naqilsiz texnologiyanın tətbiqi də mühim rol oynayır. Wi-fi texnologiyası şəbəkə daxilində internetə qoşulmaq üçün istifadəçi sayının daha da çox olmasını təmin edir. Bu texnologiyanın tətbiqinin üstünlükləri olduğu kimi, müəyyən çatışmazlıqları da vardır. Wi-fi texnologiyası şəbəkədə şifrə vasitəsi ilə qoşulduqda və kontrollerdən icazə ilə istifadəçilərin xidmətinə verildikdə təhlükəsizlik tam təmin edilə bilir. Bu prosedurlar yerinə yetirilərkən, informasiya oğurluğu və itkisi kimi hadisələrə qarşı tədbir görülür.

Şəbəkə təhlükəsizliyi üçün istifadə edilən cihazların hər birində fərqli protokollar tətbiq edilir. Bu protokollar vasitəsi ilə korpusların hər birini ayrı-ayrılıqda lokal şəbəkələrə ayıraraq, təhlükəsizlik gücləndirilir və əlavə olaraq informasiya trafikinə nəzarət, ola biləcək təhdidlərə qarşı sürətli şəkildə müdaxilə üçün ümümi sistem qurulur.

İşin məqsədi. Azərbaycan Texniki Universitetində şəbəkə texnologiyasının tətbiq sahələrinin müəyyən edilməsi, şəbəkə təhlükəsizliyinin təmin edilməsi və bu prosedurların analizi aparılmışdır. Şəbəkənin təhlükəsizliyini təhdid edən hücumlara qarşı istifadə olunan proqram təminatları haqqında məlumat verilmişdir.

Tədqiqat obyekti. 1.“Azərbaycan Texniki Universiteti” – “İnformasiya Kommunikasiya Texnologiyaları” şöbəsi 2. “ NetTech MMC” – “Proqram təminatı” şöbəsi 3. “Avicom LLC” – “Texniki təminat və şəbəkə” şöbəsi

İşin elmi yeniliyi. Korporativ müəssisələrdə qurulan şəbəkənin universitet şəbəkəsi ilə bəzi parametrlər üzərindən fərqləndirilməsi aparılmışdır. İstifadəçilərin internetə çıxışını və universitet şəbəkəsində olan tətbiqlərin təhlükəsiz şəkildə istifadəsi nəzərdə tutulmuşdur. Təhlükəsizliyə təsir edə biləcək amillərin qarşısının alınması və onları necə analiz edə biləcəyimizin üsul və tətbiqlərinin təhlili aparılmışdır.

Tədqiqatın həqiqiliyi. Dissertasiya işi üzrə aparılmış tədqiqatlar və alınan nəticələr mövcud ədəbiyyatlarda olan informasiya ilə tamamilə uzlaşır.

İşin təcrübi əhəmiyyəti. Qeyd edilmiş hesabatların, nəticələrin analizi göstərir ki, tədqiqat prosesində əldə edilmiş nəticələr Azərbaycan Texniki Universitetinin kompüter şəbəkəsinin təhlükəsizliyi səviyyəsinin artırılması üçün istifadə oluna bilər.

İşin aprobasiyası. Elmin, təhsilin və cəmiyyətin müasir problemləri mövzusunda 19-21 iyun 2023-cü il tarixlərində keçirilən, IV Beynəlxalq Elmi-Praktik Distant Konfransında “Ali təhsil müəssisəsinin kompüter şəbəkəsinə edilən hücumların təhlili sistemi” adlı tezis ilə çıxış edilmişdir. Ukrayna, Kiyev.

İşin strukturu və həcmi. Dissertasiya işi girişdən, 5 fəsildən, nəticədən, 31 sayda ədəbiyyat siyahısından ibarətdir. İşin ümumi həcmi 133 səhifədir, burada 43 şəkildən, 1 cədvəldən istifadə olunmuşdur.

Girişdə dissertasiyasının işinin aktuallığı və məqsədi qeyd edilmişdir. İstifadə edilən metod və tətbiqlər, tədqiqat üsulları və digər prosedurlar göstərilmişdir. Bu sahə ilə əlaqəli olan bir sıra statistik informasiyalar qeyd edilmişdir. Praktiki informasiya, işin həcmi və ümumi struktur haqqında məlumat verilmişdir.

Birinci fəsildə korporativ şəbəkələrdə OSI modelinin layer 1, 2 və 3-ə aid avadanlıqları haqqında məlumat, işləmə prinsipi, parametrlər və digər qeydlər aparılmışdır.

İkinci fəsildə korporativ şəbəkələrdə wi-fi texnologiyasının arxitekturası, arxitekturanın funksional elementləri və onların işləmə prosesi, həmçinin Azərbaycan Texniki Universitetində istifadə edilən wi-fi texnologiyasının parametrləri analiz edilmişdir.

Üçüncü fəsildə Azərbaycan Texniki Universitetində şəbəkənin qurulması və onun təhlükəsizliyinin təmin edilməsi məsələlərin analizi aparılmışdır. İstifadə edilən cihazların və proqram təminatının şəbəkəni təhdid edən hücumlara qarşı təhlükəsizliyi yüksək səviyyədə təmin edilməsi prosesinin bu fəsildə analizi aparılmışdır.

Dördüncü fəsildə şəbəkəyə edilən veb hücumlar və bu hücumlardan mühafizə üsulları tədqiq edilmişdir. Veb hücumların sistemdə yarada biləcəyi zərərlər haqqında ümumi məlumat verilmişdir.

Beşinci fəsildə proqram təminatından istifadə edərək AzTUSecurity-Analyzer System (ASAS) mobil tətbiq proqramı qurulmuşdur. Bu proqram vasitəsinin köməyi ilə İKT şöbəsinin adminləri şəbəkəyə olan hücumlar və təhdidlərdən tez bir zamanda xəbərdar olur, onları analiz edərək qarşısını vaxtında almaq imkanı əldə edirlər.

AZƏRBAYCAN RESPUBLİKASI ELM və TƏHSİL NAZİRLİYİ

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əlyazması hüququnda

MUSTAFAYEVA QUMRAL ABUBƏKİR QIZI

AzTU-nun kompüter şəbəkəsində informasiya təhlükəsizliyinin qiymətləndirilməsi sisteminin işlənməsi

mövzusunda

MAGİSTRLİK DİSSERTASİYASI

İxtisas: 060631- " Kompüter mühəndisliyi"
İxtisaslaşma: "Biliklərin əldə edilməsi sistemləri"

Elmi rəhbər: **t.f.d., dosent C. Məmmədov**

BAKI – 2023

I FƏSİL. KORPORATİV ŞƏBƏKƏLƏRDƏ İSTİFADƏ EDİLƏN AVADANLIQLAR VƏ İNFORMASİYA TƏHLÜKƏSİZLİYİNİN QORUNMASI PRİNSİPLƏRİ

1.1. Korporativ şəbəkələrdə istifadə olunan Layer 1 və Layer 2 cihazların təsnifatı

Şəbəkə hubı məlumatı ona qoşulmuş hər bir kompüterə və ya Ethernet əsaslı cihaza ötürən qovşaqdır. Hub switchdən mürəkkəbliyi daha azdır. Şəbəkə hubları kiçik və sadə lokal şəbəkə (*LAN*) mühitləri üçün ən uyğundur. Hublar routing (marşrut) imkanlarını və ya digər xüsusi şəbəkə xidmətlərini təmin edə bilməz. Paketləri bütün portlar arasında fərq qoymadan, eyni üsul ilə ötürməklə işlədikləri üçün şəbəkə hubları bəzən *"lal switchlər" (eng dumb switches)* adlanır. Məhdud imkanları və aşağı ötürmə məsafəsi ilə şəbəkə hubları switchlərlə müqayisədə ilk növbədə bir rəqabət üstünlüyünə malik idi: aşağı qiymətlər.

2000-ci illərin əvvəllərində və ortalarında switch qiymətləri düşdükcə, hublar tədricən istifadədən çıxmağa başladı. Funksionallıq baxımından verdiyi xidmətlərə görə switchlərə üstünlük verildi. Bu gün hublar daha az yayılmışdır. Hublar ***Open Systems Interconnection (OSI)*** istinad modelində Layer 1 cihazları kimi təsnif edilir. Bu cihazlar bir neçə kompüteri birləşdirir, bir portda alınan məlumatları məhdudiyyət qoyulmadan bütün digər portlara ötürür. Hublar half-dupleks rejimdə işləyən cihazlardır. Bu üsul təhlükəsizlik və məxfiliklə bağlı narahatlıq doğurur, çünki trafiki qorumaq və ya nəzarət etmək mümkün deyildi. Huba qoşulan cihazlar şəbəkə kimi işləyir və collision domain (toqquşma domenini) paylaşır. Belə nəticə əldə olunur ki, huba qoşulmuş iki cihaz eyni vaxtda məlumat ötürdükdə paketlər toqquşaraq şəbəkənin işində problemlər yaradacaq. Bu problem idarə edilə bilən layer 2 və layer 3 cihazlarda görülmür. Hublara qoşulmuş

bütün cihazlar mövcud bant genişliyini bərabər şəkildə bölüşür. Hubdakı hər bir porta ayrılan bant genişliyinin (*eng bandwidth*) miqdarı switchdəki prosedurdan fərqlənir.

Hubların iki növü var: *aktiv və passiv.*

I. **Aktiv hublar** daxil olan ötürmələri təkrarlayır və gücləndirir. Onlara bəzən təkrarlayıcılar yəni *repeaters* da deyilir.

II. **Passiv hublar** isə heç bir əlavə xidməti olmadan, yalnız bağlantı nöqtəsi kimi istifadə edilir.

Ulduz topologiyasında bəzən hub və spoke adlanır, hər bir istifadəçi mərkəzi huba qoşulur; lakin hostlar bir-biri ilə birbaşa əlaqə saxlamırlar. Bu kontekstdə "hub" adətən switch rolunu oynayır. Hublar ip ünvanına ehtiyac duymur. Portların sayı seriyasından asılı olaraq 4 ilə 48 port arasında dəyişə bilər. Hubların çatışmazlıqlarını dedik də, ilk öncə köhnə texnologiya olduğunu qeyd edə bilərik. Qeyd olunan sürət itkiləri, məlumatların ötürülməsi və seçilmiş istifadəçilər baxımından çevikliyin olmaması ilə yanaşı, hub sistemi də təhlükəsizlik məsələlərinə nisbətən həssasdır [2].

Repeaters-lar OSI modelinin fiziki səviyyəsində işləyən şəbəkə cihazıdır və daxil olan siqnalı təkrar ötürməzdən əvvəl gücləndirir və ya bərpa edir. Onların əhatə dairəsini genişləndirmək üçün local şəbəkələrə daxil edilirlər. Repeaterslar həmçinin siqnal gücləndiriciləri kimi tanınırlar.

Təkrarlayıcılar niyə lazımdır? Elektrik siqnalı kanal vasitəsilə ötürüldükdə kanalın vəziyyətindən və ya texnologiyadan asılı olaraq zəifləyir. Bu prosedur, lokal şəbəkənin genişliyinə və ya mobil şəbəkələrin əhatə dairəsinə məhdudiyyət yaradır. Müəyyən edilmiş intervallarda təkrarlayıcıların quraşdırılması ilə yaranan problem aradan qaldırılır. Təkrarlayıcılar qəbul etdikləri zəifləmiş siqnalı gücləndirir və sonra yenidən siqnalı qarşı tərəfə ötürür.

Rəqəmsal təkrarlayıcılar (*eng Digital repeaters*) hətta ötürmə itkisi ilə təhrif olunan siqnalları yenidən qura bilər. Bu nümunədən belə nəticəyə gəlirik ki, təkrarlayıcılar iki lokal şəbəkə arasında əlaqə yaratmaq üçün zaman-zaman birləşdirilmişdir və beləliklə bu proses böyük bir lokal şəbəkə meydana gətirir.

Yenidən təmin etdikləri siqnal növlərinə görə təkrarlayıcıları iki kateqoriyaya bölmək olar:

➢ **Analog Repeaters (Analoq təkrarlayıcılar)** – Onlar yalnız analoq siqnalları gücləndirə bilər.

➢ **Digital Repeaters (Rəqəmsal təkrarlayıcılar)** – Onlar təhrif olunmuş siqnalı yenidən qura bilirlər.

Qoşulduqları şəbəkənin növlərinə görə də təkrarlayıcıları iki növə bölmək olar:

- **Wired Repeaters (Simli təkrarlayıcılar)** – Onlar kabel istifadə edilən lokal şəbəkələrdə istifadə olunur.
- **Wireless Repeaters (Simsiz Təkrarlayıcılar)** – Onlar simsiz LAN və mobil şəbəkələrdə tətbiq edilir.

Qoşduqları şəbəkələrin domeninə görə təkrarlayıcıları iki kateqoriyaya bölmək olar:

- *Local Repeaters (Yerli təkrarlayıcılar)* – Kiçik məsafə ilə ayrılmış şəbəkə seqmentlərini birləşdirir.
- *Remote Repeaters (Uzaqdan təkrarlayıcılar)* – Bir-birindən uzaq məsafədə olan lokal şəbəkələri birləşdirir.

Təkrarlayıcıların üstünlükləri kimi quraşdırılmasının sadə olması şəbəkəni genişləndirmək istərkən asanlıqla genişləndirilə bilməsidir. Qiymət baxımından effektivdir və heç bir emal yükü tələb etmir. Problem baş verərsə araşdırılması lazım olan yeganə vaxt performansın aşağı düşməsi halıdır. Müxtəlif növ kabellərdən istifadə edərək siqnalları birləşdirə bilərlər. Şəbəkənin məsafəsini genişləndirməkdə mühüm məqsədə xidmət etsələr də, onların bəzi çatışmazlıqları var:

- *Məhdud məsafə (Limited distance):* Təkrarlayıcıların məhdud diapazonu var və yalnız müəyyən məsafəyə qədər siqnalları bərpa edə bilər. Bu diapazondan kənarda siqnal pisləşə bilər ki, bu da şəbəkənin zəif işləməsi ilə nəticələnir.

- *Siqnal gecikməsi (Signal delay):* Təkrarlayıcılar siqnalı bərpa edərkən siqnal ötürülməsində gecikmə yaradır. Bu problem xüsusilə yüksək sürətli şəbəkələrdə daha yavaş şəbəkə performansı ilə nəticələnə bilər.
- *Artan şəbəkə mürəkkəbliyi (Increased network complexity):* Təkrarlayıcıların çoxlu şəkildə şəbəkədə istifadəsi şəbəkənin mürəkkəbliyini artıra bilər. Daha çox təkrarlayıcı əlavə olunduqca, şəbəkəni idarə etmək və problemləri həll etmək çətinləşə bilər.
- *Təhlükəsizlik problemləri (Security concerns):* Təkrarlayıcılar layer 1 səviyyədə istifadə edilən qurğu olduğu üçün, arzuolunmaz şəbəkə trafikini filtrləmir və ya bloklamır, bu da təkrarlayıcıları xidmətdən imtina hücumları və icazəsiz giriş kimi təhlükəsizlik təhdidlərinə qarşı həssas edir.

Lokal şəbəkələrdə istifadəsi görülsədə yeni texnologiyalarnan fərqləndirərək, onların əvəzlənməsi prosesi zaman-zaman daha da sürətlənir. Azərbaycan Texniki Univeristetində korpuslarda hublar və repeaterlara rast gəlinir. Əlbəttə ki, təhlükəsizliyin təminatı və təhdidlərdən qorunmaq üçün bu layer 1 texnologiyaların istifadəsi şəbəkədən çıxarılmalıdır [3].

Switchlər OSI modelinin 2-ci qatında və ya data-link səviyyəsində işləyən şəbəkə cihazlarıdır. Şəbəkədə cihazların bir-biriləri ilə əlaqə qurmasına xidmət edir, məlumat paketlərini və ya məlumat çərçivələrini şəbəkə üzərindən göndərmək, qəbul etmək, yönləndirmək üçün paket switchingdən istifadə edirlər. Məlumat çərçivəsi hər hansı bir portu çatdıqda, təyinat ünvanını yoxlayır, lazımi yoxlamaları həyata keçirir və çərçivəni təyin edilən müvafiq qurğuya(lara) göndərir. Unicast (bir-bir), multicast (bir-çox) və broadcast (bir-hamı) bağlantını dəstəkləyir. Cihaz əgər ilk dəfə qoşulubsa və digər portdakı kompüterə məlumat göndərirsə, switch tərəfindən ilk broadcast sorğular göndərilir. Switchin mac cədvəlinə ünvan qeyd edildikdən sonra məlumat unicast yəni, yalnız təyinat ünvanına göndərilir.

Switchlər yalnız layer 2 deyil, həmçinin layer 3 səviyyədə də xidmət göstərir. Layer 2 switch heç bir ip marşrutlaşdırma, NAT funksiyalarını yerinə yetirmir və şəbəkə

seqmentasiyası və vlan dəstəyi üçün istifadə olunur. Layer 2 switchlər üst səviyyə marşrutlaşdırma funksiyaları olmadan sürətli və güvənilir məlumat ötürülməsini tələb edən kiçik və orta ölçüdə şəbəkələr üçün ideal göstərilmişdir. Layer 3 switchi isə OSI modelinin network layerində işləyir və ip ünvanları istifadə edərək paketləri yönləndirə bilir. Bu switchlər həm layer 2, həm də layer 3 səviyyənin işini görə bilir. Məlumat paketlərinin təyinat yerinə çatması üçün ən yaxşı yolu müəyyən etmək üçün marşrut cədvəllərindən və protokollarından istifadə edir. Layer 2-dən fərqli olaraq daha mürəkkəb marşrutlaşdırma funksiyaları və çoxsaylı alt şəbəkələr üçün dəstək tələb edən daha böyük şəbəkələr üçün uyğundur. Korporataiv şəbəkələrdə, əsasən, distribution switch rolunda gedirlər. O, switch və marşrutlaşdırıcının funksionallığını birləşdirir və şəbəkə trafikinin daha səmərəli marşrutlaşdırılmasına imkan verir.

Switchləri bir çox xüsusiyyətlərinə görə qruplaşdırmaq olar:

1. *İdarə olunmayan* switch *(eng Unmanaged Switch):* İdarə olunmayan switch heç bir konfiqurasiya tələb olunmadan, sadəcə bir-biri ilə bağlantı qurmasına imkan verən switch növüdür. Onun istifadəçi interfeysi və ya hər hansı qabaqcıl xüsusiyyətləri yoxdur, bu prosedur switchi kiçik şəbəkələr üçün sadə və maddi cəhətdən sərfəli edir.

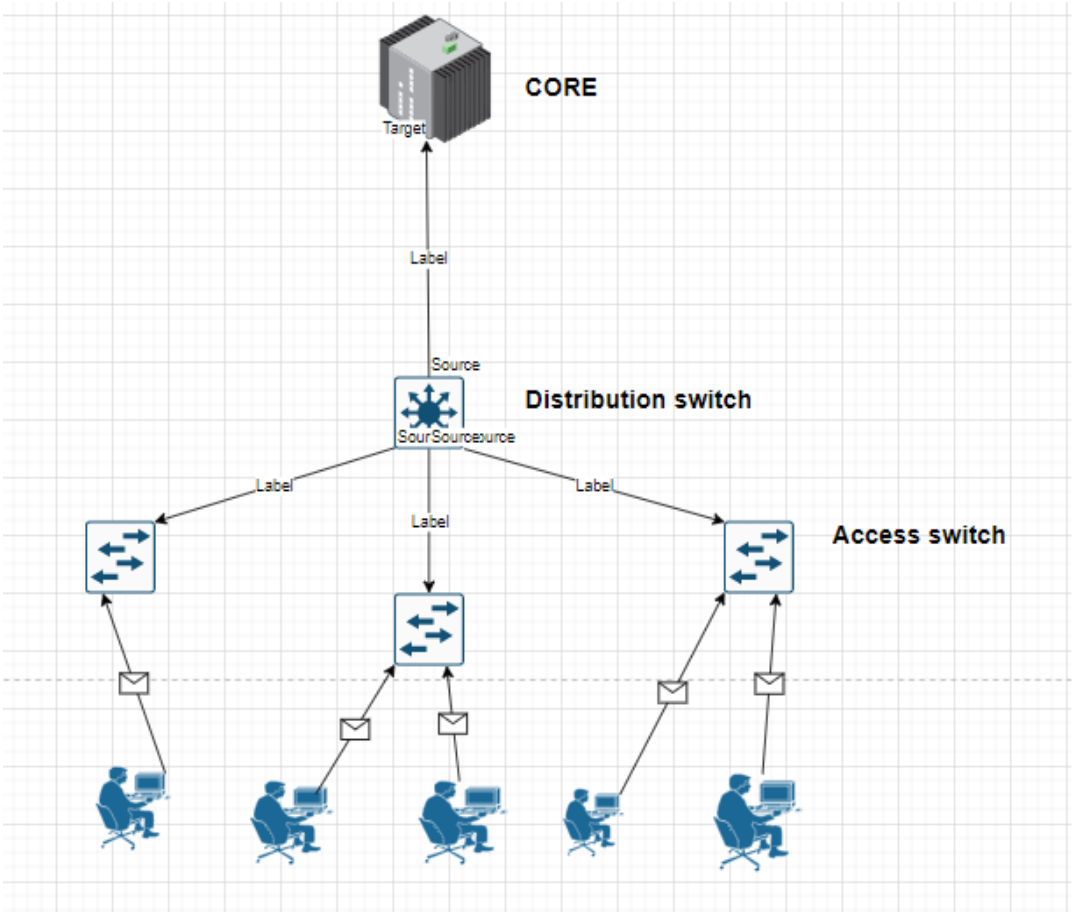
2. *İdarə olunan* switch *(eng Managed Switch):* İdarə olunan switch şəbəkə administratorlarına şəbəkə üzərində daha çox nəzarət etməyə imkan verən önəmli xüsusiyyətlər və konfiqurasiya seçimləri təmin edir. Vlan dəstəyi, Xidmət Keyfiyyəti (QoS) parametrləri və şəbəkə təhlükəsizliyi protokolları kimi funksiyaları təklif edir.

3. *PoE* switch *(PoE Switch):* **PoE (Power over Ethernet)** switchi həm məlumatın, həm də enerjinin Ethernet kabelləri üzərindən ötürülməsinə imkan verir. Bu switch fərqli elektrik kabellərinə ehtiyacı aradan qaldırır və adətən ip kameralar, telefonlar və simsiz giriş nöqtələri kimi cihazları şəbəkəyə əlavə etmək üçün istifadə olunur.

4. *Buludla idarə olunan* switch *(eng Cloud Managed Switch):* Buludla idarə olunan switch bulud əsaslı mərkəzi idarəetmə interfeysi vasitəsilə şəbəkənin hər hansı

bir nöqtədən idarə edilməsinə və monitorinqinə imkan verir. Switch bizə qabaqcıl funksiyalar təklif edir və daha geniş şəbəkələrdə istifadə edilir.

Switchlər vendor və seriyalarına görə də fərqlənir. Korporativ şəbəkələrdə istifadəçilər qoşulan switch adətən layer 2 səviyyədə istifadə edilən access switchlərdir. Access switchlər növbəti qoşulma nöqtəsi kimi distribution switchlərə qoşulurlar. Yəni mərkəzi nöqtə kimi distribution switchlər təyin edilir (şəkil 1.1). Core switchlər layer 3 səviyyədə aparılan protokolların, internetə çıxışın və digər əsas prosedurların ediliyi mərkəzi switch kimi qeyd edilir. Distribution switchlər də sonda core switchə bağlanırlar [8].



Şəkil 1. 1 Lokal şəbəkə

1.2 . Korporativ şəbəkələrdə istifadə olunan Layer 3 cihazların təsnifatı

Korporativ şəbəkələrdə Layer 3 qurğuları adətən müxtəlif alt şəbəkələr və vlanlar arasında marşrutlaşdırma, təhlükəsizlik və qarşılıqlı əlaqəni təmin etmək üçün istifadə edilir. OSI modelinin şəbəkə səviyyəsində işləyir və mürəkkəb marşrutlaşdırma funksiyalarını idarə etmə xüsusiyyəti, Xidmət Keyfiyyəti (QoS), təhlükəsizliyi və yüksək əlçatanlıq kimi qabaqcıl şəbəkə xüsusiyyətlərini təmin edə bilir. Korporativ şəbəkələrdə geniş istifadə olunan Layer 3 cihazlarının bəzi nümunələri daxildir:

Şəkil 1. 2 Router və Layer 3 switch

Routerlər: Müxtəlif şəbəkələr arasında Layer 3 marşrutlaşdırma funksiyalarını istifadə edərək, bağlantını təmin edən müstəqil şəbəkə cihazlarıdır. Korporativ şəbəkə daxilində müxtəlif alt şəbəkələrin bir-biriləri ilə əlaqə qurması üçün istifadə oluna bilər, həmçinin internet kimi xarici şəbəkələrə qoşulmanı təmin edir. Routerlər şəbəkədə təhlükəsizlik divarı və vpn bağlantısı kimi təhlükəsizlik xüsusiyyətlərini təmin edə bilər. Bəzi kiçik və orta şəbəkələrdə routerləri layer 3 switchlərlə əvəz edirlər (şəkil 1.2).

Firewall: Firewall paket filtrləmə, müdaxilənin qarşısının alınması və vpn bağlantısı kimi şəbəkə təhlükəsizliyi xüsusiyyətlərini təmin edən Layer 3 cihazıdır. Korporativ şəbəkəni xaricdən gələn təhdidlərdən qorumaq, həmçinin şəbəkə siyasəti və monitorinqini tətbiq etmək üçün istifadə edilə bilər [8].

Load Balancers (Yük balanslaşdırıcıları): Şəbəkə trafikini çoxsaylı serverlər və ya şəbəkədəki resurslar arasında paylayan Layer 3 cihazlarıdır. Şəbəkə performansını və əlçatanlığını yaxşılaşdırmaq, ehtiyat məsələləri və uğursuzluq imkanlarını təmin etmək üçün istifadə edilə bilər.

Firewall fəaliyyəti müxtəlif konfiqurasiyalara uyğun şəkildə tənzimlənir. Yerli təhlükəsizlik siyasətinə əsaslanan qaydalar təyin edilir və yalnız bu qaydalara uyğun olan trafik keçirilir. Buna əlavə olaraq, müxtəlif növ təhlükəsizlik siyasətlərini həyata keçirən fərqli növ firewall cihazlarından istifadə olunur. Bu sahədə, məqsədə uyğun olaraq fərqli cihazlar seçilərək ən effektiv təhlükəsizlik tədbirləri tətbiq edilir. Firewall cihazları iki əsas proqram (software) təminatı və aparat (hardware-based) təminatı adlı kateqoriyaya bölünür. Proqram təminatı firewall gələn və gedən trafiki monitorinq edərək təhlükəsizlik siyasətinə əsasən qaydalar tətbiq edir. Avadanlıq firewalları, şəbəkəniz və internet arasındakı fiziki avadanlıqlardır və avadanlığın içərisində lisenziyalardan istifadə edərək proqram əsaslı firewall aktiv edilir. Korporativ şəbəkələrdə virusla yoluxmuş faylların ötürülməsindən qorumaq üçün anti-virus proqramları ilə birlikdə işləyə bilər, lakin viruslara qarşı 100% təhlükəsizlik təmin etmək mümkün deyil. Firewallun əsas funksiyası, xüsusi protokolların və ya xüsusi portların ötürülməsini qadağan etməkdir. Virusların qarşısının alınması üçün, şəbəkədə anti-virus proqramlarının firewalla paralel şəkildə işləməsi vacibdir [16].

Firewall bəzi növlərindən paket filtrləmə, circuit-level gateway və s. tipli firewall haqqında qeyd edə bilərik.

Dövrə səviyyəli şlüz (*eng circuit-level gateway*), seans səviyyəsində şəbəkə trafikinə nəzarət təklif edən bir təhlükəsizlik divarıdır. Virtual dövrədə iki nəqliyyat səviyyəsi (*TCP və UDP*) arasında paketlər və əlaqə sorğularını yoxlayaraq təhlükəsizliyi təmin edir. Korporativ şəbəkədə istifadəçi təyinat serverlə bir TCP əlaqəsinin başlatmaq üçün müraciət etdiyində, dövrə səviyyəli şlüz üç şey edir:

1. Dövrə səviyyəli şlüz, istifadəçi tərəfindən TCP bağlantısı qurmaq üçün göndərilən sorğunu qəbul edir.
2. İstifadəçinin doğruluğunu və autentifikasiyası və avtorizasiyası təyin edir.
3. Əgər müştərinin autentifikasiyası və avtorizasiyası uğurla həyata keçirilərsə, istifadəçi üçün təyinat server üzərində ikinci bir TCP bağlantısı qurur. Əks təqdirdə, bağlantı rədd edilir.

Bağlantı qurulduqdan sonra, TCP seqmentlərini müştəri və təyinat server arasında ötürür. Gateway virtual dövrə cədvəlindəki girişlərə uyğunluqları monitorinq edir və əgər bağlantıların təsdiqlənməsi prosesində bir problem yoxdursa, hansı şəbəkə paketlərinin ötürülməsi üçün məlumatların olduğunu yoxlayır. Bu istifadə edilən cədvəl, şəbəkədə mövcud olan bəzi istifadəçilər və ya resurslar üçün istifadə edilən xüsusi məlumatlardan ibarətdir. Cədvəldəki girişlər üzərində edilən yoxlamalar, təhlükəsizlik qaydalarına uyğunluğu təmin edir [9].

F5 yük balanslaşdırıcıları layer 3 daxil olmaqla, OSI modelinin çoxsaylı qatlarında işləmək üçün nəzərdə tutulmuşdur. Əslində, F5 kritik şəbəkə xidmətləri üçün yüksək əlçatanlıq, genişlənmə və performans təmin etmək üçün nəzərdə tutulmuş layer 3 yük balanslaşdırma xüsusiyyətlərinin hərtərəfli dəstini təqdim edir. F5 həm firewall, həm də load balancer kimi şəbəkədə fəaliyyət göstərir. Balanslaşdırıcı rolunda aşağıdakı nümunələri görsətmək olar:

İP yük balansı (eng IP Load Balancing): F5 ip yük balansından istifadə edərək bir çox server və ya şəbəkə resurslar arasında şəbəkə trafikini paylaya bilər. Bu üsul serverin mövcudluğu, server tutumu və şəbəkə sıxlığı kimi amillər əsasında trafikin səmərəli paylanmasına icazə verir [17].

- *Route Health Injection (RHI):* F5 yük balanslaşdırıcıları şəbəkə resurslarının mövcudluğuna əsasən şəbəkə marşrutlaşdırma cədvəlinə dinamik marşrutlar yeridə bilər. Bu üsul trafikin həmişə sağlam resurslara yönəldilməsini təmin edir və şəbəkənin dayanıqlığını və əlçatanlığını yaxşılaşdıra bilər.
- *Virtual IP (VIP) ünvanı:* F5 yük balanslaşdırıcıları bir qrup server və ya şəbəkə avadanlıqları üçün vahid ip ünvanı təmin etmək üçün virtual ip ünvan üsulundan istifadə edə bilər. Bu üsul qüsursuz əvəzlənməyə və genişlənməyə imkan verir, həmçinin şəbəkənin idarə edilməsini sadələşdirir.

BIG-IP Advanced Firewall Manager (AFM) kimi tanınan F5-in firewallları şəbəkə təhlükəsizlik divarı, tətbiq səviyyəsinin təhlükəsizlik divarı və paylanmış xidmətdən imtina (DDoS) qorunması kimi bir sıra təhlükəsizlik xüsusiyyətlərini təmin

edir. BİG-İP AFM-in növbəti əsas xüsusiyyəti onun tətbiqi səviyyəli təhlükəsizlik divarı imkanlarıdır. Tətbiq səviyyəsində trafiki təhlil etmək üçün istifadə edilən bu siyasətlərin necə konfiqurasiya olunacağını əhatə edir. Bu prosedur trafikə daha çox nəzarət etməyə imkan verir və SQL injection və cross-site scripting (XSS) kimi hücumları aşkar etmək və qarşısını almaq üçün istifadə edilə bilər. BIG-IP AFM-ə real zaman rejimində DDoS hücumlarını aşkarlamağa və qarşısını almağa imkan verir, hətta hücum zamanı istifadə edilən tətbiqlərin və xidmətlərin əlçatan olmasını təmin edir [16].

1.3. Korporativ şəbəkələrdə texniki və proqram təminatının vasitəsi ilə təhlükəsizlik tədbirlərinin görülməsi

Təhlükəsizlik tədbirləri informasiyanın təsadüfi və ya düşünülmüş təbii və ya süni xarakterə malik təsirlərdən, məsələn, viruslardan, qəsdən xəsarət vurmaq cəhdi olan hakerlərdən, informasiya qaynağının mənfi təsirləri və s. kimi təhlükələrdən qorunmağı hədəfə qoyur. Bu təhlükəsizlik tədbirləri informasiyanın və informasiya obyektlərinin ziyan görməsini, informasiyanın istifadəsində saxlanılan məlumatların itirilməsini və ya silinməsini, informasiya istifadəçisinin və ya sahibinin məxfiliyinin pozulmasını və s. kimi problemləri önəmli dərəcədə azaldır.

Korporativ şəbəkələrdə informasiya təhlükəsizliyini təmin etmək üçün bir çox müxtəlif üsullar və texnologiyalar mövcuddur.

I. Təhlükəsizlik tədbirlərinin texniki təminat vasitəsilə qarşısının alınması
II. Təhlükəsizlik tədbirlərinin proqram təminatı vasitəsilə qarşısının alınması

Məkanın fiziki olaraq qorunmasi üçün istifadə edilən fiziki təhlükəsizlik metodu korporativ şəbəkələrdə daxili və xarici təhlükəsizlik tədbirlərinin nəzərə alınmasında müəyyən bir rol oynayır. Fiziki təhlükəsizliyin əsas məqsədi, giriş nöqtələrinin və məkanın daxili hissələrinin güclü bir şəkildə qorunmasıdır. Fiziki təhlükəsizliyin əsas tədbirlərinə daxildir:

Giriş nöqtələrinin qorunması: Korporativ şəbəkəyə qoşulmaq istəyən şəxslər məkanın İT servis otaqlarına daxil olmaq üçün giriş nöqtələrindən istifadə edirlər. Fiziki

qorunma üçün bu nöqtələr vacibdir. Əsasən qapılar məxfi koda malik kartlar və ya biometrik məlumatların istifadəsi ilə qoruna bilər. Biometrik texnologiya, bəzi insanların fərdi və təkrarlana bilməyən fiziki və ya davranış atributlarından istifadə edir. Fərqli tətbiqlərdə çeşitli biometrik parametrlər istifadə edilir. Hər bir biometrik parametrin qüsursuz və çatışmayan tərəfləri mövcuddur və onların seçimi tətbiqdən asılıdır.

Barmaq izləri: İnsanın şəxsiyyətini yoxlamaq üçün ən etibarlı və ən çox yayılmış üsullardan biri, barmaq izinin identifikasiya texnologiyasıdır. Bu metod, hər bir insanın əl barmaqlarındakı naxışların unikal olmasına əsaslanır. Barmaq izi papilyar xətlər tərəfindən yaradılır ki, bunu xətlər, qövs, ilgək və spiral kimi mürəkkəb naxışlar təşkil edir. Bu üsul, DNT analizindən sonra dəqiqlik baxımından ikinci yer tutur. Bu biometrik üsul, ümumi şəkildə yüksək təhlükəsizlik və ümumi qorunma üsulu kimi hesab olunur. Barmaq izinin bir sıra üstünlükləri vardır:

- Barmaq izlərini itirmək və ya yaddan çıxarmaq olmaz və onlar həmişə insanın yanındadır. Bu, barmaq izi biometrikasının istifadəsi üçün mühüm bir faydadır, çünki parollar və ya kartlar kimi digər kimlik təsdiq vasitələri itirilə bilər və ya unutulduqda mənfi nəticələrə səbəb ola bilər.
- Barmaq izlərini saxtalaşdırmaq çətindir, parollardan daha təhlükəsizdir. Bu, barmaq izi biometrikasının istifadəsinin bir başqa böyük faydasıdır. Hər kəsin barmaq izi fərqli olduğundan, başqasının kimliyini təsdiq etmək üçün onun barmaq izi müvafiq şəkildə skan edilməlidir.
- Barmaq izi nümunələri təxmin edilə bilməz və ötürülə bilməz. Bu, barmaq izi biometrikasının təhlükəsizliyini artıran bir başqa faktordur. Bir dəfə skan edildikdən sonra barmaq izi nümunəsi yalnız təsdiq məqsədləri üçün saxlanılır və heç bir hallarda ötürülmür.

Üzün tanınması: Biometrik identifikatorlar arasında, üzün tanınması insanlar arasında populyar olan bir tanıma metodudur. Bu, insanların vizuallaşdırma yolu ilə tanınmasından ibarətdir. Üzün tanınması, tələb olunan xüsusi avadanlıqların bahalılığı

olmadan asanlıqla həyata keçirilir. Adi videomüşahidə kamerası, sifətin tanınması ilə birlikdə, başqa bir çox funksiyaların da yerinə yetirilməsinə kömək edir.

Üzün tanınması, oxuma qurğusu ilə fiziki təmas, nəyəsə toxunmaq, müəyyən vəziyyəti almaq və ya hər hansı bir frazanı tələffüz etmək kimi məsuliyyətli bir təcrübə tələb etmir. Bu tanıma prosesi təbii bir şəkildə baş verir və bəzi hallarda tanınma işləri identifikasiya edilənə hiss etdirilmədən yerinə yetirilir. Bu səbəbdən, sifət cəmiyyətdə ən yaxşı qəbul edilən biometrik identifikatorlardan biridir. Üz tanınması üçün fərqli yanaşmaların mövcud olduğu və 1990-cı illərin sonlarına doğru xüsusiyyət əsaslı yanaşmaların səmərəli olduğu bilinirdi. Bu zaman Christoph von der Malsburg və Bochum Universitetindəki tədqiqat qrupu üz xüsusiyyətlərini qeyd etmək üçün Gabor filtrindən istifadə etdilər. Ayrıca, Bochum sistemi, üz strukturunun şəbəkəsini hesablayaraq xüsusiyyətləri əlaqələndirir. Elastik Bunch Graph Matching proqramı, dəri seqmentasiyasından istifadə edərək görüntüdən üzü çıxarmaq üçün inkişaf etdirildi və Christoph von der Malsburg bu işdə rol oynadı.

Səsin tanınması: Biometrik səsin tanınması, bir fərdin autentifikasiyası üçün bioloji xüsusiyyətlərin tətbiq edildiyi bir autentifikasiya metodudur. Parol və ya işarələrlə müqayisədə, bu metod fiziki daxiletməyə ehtiyac qoymadan, insanın unikal səsi ilə fərdin identifikasiyasını təmin edir.

Kamera nəzarəti: Məkanın fərqli yerlərində quraşdırılan kamera sistemləri hansısa bir şübhəli fəaliyyəti izləmək və müdafiə etmək üçün istifadə edilir (şək.1.3).

Təhlükəsizlik sistemlərinin icazəsiz istifadəçiləri tanıma və giriş əldə etməyə çalışanları məhdudlamaq kimi əsas vəzifələri var. Ancaq, bu proseslər zaman zaman səlahiyyətli şəxslər üçün də məşğul edici ola bilər. Bu, yanlış yükləmələr, xəbərdarlıqlar və ya başqa səbəblərə görə baş verə bilər. Bu kimi hallarda, təhlükəsizlik sistemləri əvvəlcədən təyin edilmiş səlahiyyətli istifadəçilərin kimliyini tanıya bilən bir mühafizə mexanizmi ilə təchiz edilə bilər. Bu, sistemə giriş etmək üçün etibarlı bir yol yarada bilər və yanlış mənfi nəticələrin minimalizə edilməsinə kömək edə bilər (şəkil 1.3).

Şəkil 1. 3 Kamera sistemləri təhlükəsizliyi

Antivirus proqramı, kompüterlərdə və ya digər cihazlarda virus, malware, spyware, trojan və s. kimi zərərli proqramların aşkarlanmasına və silinməsinə kömək edən bir proqramdır. Antivirus proqramları, cihazları bir viruslardan qoruyan, faylların və şəxsi məlumatların qorunmasına yardım edən bir təhlükəsizlik layihəsidir. Korporativ şəbəkələrdə müxtəlif viruslar təhlükəsizlik problemi yaradır. Bu viruslar şəbəkəni yoluxdurmaq, işləri dayandırmaq və ya məxfilik məlumatlarını əldə etmək üçün istifadə edilə bilər. Bu səbəbdən, antiviruslar korporativ şəbəkələrin təhlükəsizliyini təmin etmək üçün mühüm bir vasitədir.

Korporativ şəbəkələrdə istifadə edilən antiviruslar, hər hansı bir virus təhlükəsinə qarşı qorunmaq üçün müəyyən proqramlar təklif edir. Bu proqramlar, yeni viruslara qarşı qorunmaq üçün müvafiq güncəlləmələr və ya *"imza (eng sign)"* adı verilən xüsusi kodlar təqdim edir. Bu imzalar sayəsində antiviruslar, müxtəlif virusların və köhnəlmiş virusların təhlükəsizliyini təmin edir. Antivirusların əsas funksiyaları arasında köhnə virusların silinməsi, yeni virusların aşkarlanması və yoluxma riskinə qarşı təhlükəsizliyin təmin edilməsi var. Həmçinin, antivruslar istifadəçilərə müxtəlif təhlükəsizlik məlumatları təqdim edir və şəbəkəni monitorinq edir. Bu nəzərdə tutulur

ki, şəbəkədəki bütün fəaliyyətlər müvafiq bir şəkildə izlənir və şəbəkədəki xətalara vaxtında müdaxilə edilir.

Antivirus proqramlarının əsas məqsədi şəbəkəni viruslardan və müxtəlif təhlükəsizlik problemindən qorumaqdır. Bu proqramların müvafiq quraşdırılması və hər hansı bir virus təhlükəsinə qarşı güncəllənməsi, korporativ şəbəkələrin fəaliyyətini müvafiq şəkildə davam etdirməklə yanaşı, istifadəçilərin məxfilik məlumatlarının qorunması və mənimsənməsinin qarşısını almaq üçün vacibdir [1].

Windows 10 istifadəçilərinin diqqətini cəlb edən antivirus proqramlarının sayı bir neçə dəfə artmışdır. Çoxballı qiymətləndirmə şkalası əsasında, aşağıdakı antivirus proqramlarından bir çox uğurlu nəticələr əldə edilmişdir. Korporativ şəbəkələrdə tətbiq edilən Windows 10 əməliyyat sistemi üçün ən yaxşı antivirus proqramları bunlardır:

1. Norton Antivirus Plus: Windows 10 üçün bir çox əlavə xüsusiyyətlər təklif edən antivirusdur. Windows təhlükəsizliyi üçün ən etibarlı adlar arasında yer alır.

2. TotalAV: TotalAV qoruma səviyyəsi üçün ən yaxşı qiymətləndirmələrə malik olan antivirus proqramlarından biridir. Bir çox müstəqil antivirus test laboratoriyaları tərəfindən daima yüksək qiymətləndirilmişdir.

3. McAfee Total Protection Plus: Windows 10 üçün çox sayda paket seçimi olan məşhur bir antivirus proqramıdır.

4. VIPRE Advanced Security: İstifadəçi dostu interfeysi (istifadəçilərin məhsulu rahat və asanlıqla istifadə etməsini təmin edəcək bir şəkildə dizayn olunması) olan və mütləq lazım olan xüsusiyyətləri olan bir antivirus proqramıdır.

5. Bitdefender Antivirus Plus: Windows 10 üçün çox sayda təhlükəsizlik ehtiyacını əhatə edən əla bir seçimdir.

6. Kaspersky Internet Security: Unikal bir yanaşma ilə işləyən güclü antivirus proqramıdır. Kaspersky Internet Security antivirusunun unikal olma səbəbi onun "Behavior Detection" texnologiyasıdır. Bu texnologiya, potensial təhlükəli davranışları təyin edərək yeni təhlükəli tətbiqlərin və proqramların müdafiəsini təmin edir.

7. Panda Antivirus: Panda Antivirus bir antivirus proqramıdır və reytinqlərdə ən yüksək nəticələrə sahib olan real vaxt virus skanerini təklif edir. Bu proqram, təhlükəli faylları avtomatik olaraq təyin edərək hər hansı bir təhlükəli faylın açılmasını və ya yüklənməsini dayandırır.

8. AVG : Çoxistifadəçili (bir çox insanın yaşadığı və birgə internet və ya kompüterlərdən istifadəsi) ən yaxşı seçimlərdən biri olan antivirus proqramıdır.

9. ESET : Bu antivirus proqramı maddi olaraq (qiymət-məhsul keyfiyyəti nisbəti) münasib bir antivirus proqramı olaraq qiymətləndirilir.

Norton antivirus - Norton 360 antivirus, güclü bir anti-malware olmaqla, geniş bir internet təhlükəsizliyi alətləri seçimi, intutitiv bir onlayn idarə paneli və çox sayda rəqiblərindən daha yaxşı qiymət ilə müştəri dəstəyi təklif edir.

Bu proqram zərərli proqramları təyin etmək və problemləri həll etmək üçün qabaqcıl, səmərəli bir üsuldan və müxtəlif zərərli proqramların əsas funksiyalarını və davranışlarını tanımaq üçün istifadə etdiyi bir verilənlər bazasından istifadə edir. Bu kataloq sadə virus və troyanlardan başlayıb, casus proqramlar, ransomware və kripto-jakerlər kimi qabaqcıl zərərli proqramlara qədər əhatə edir. Sınaq müddəti zamanı, Norton-un tam skanı və real vaxt qorunması hər bir zərərli proqram faylını minimum sistem yavaşlaması və heç bir yanlış xəta olmadan aşkar edə bildi. Norton-da həmçinin digər antiviruslar kimi bir çox xarakteristikalar mövcuddur. Bunalara firewall, vpn, parol meneceri, cihazın optimallaşdırılması və bulud ehtiya nüsxəsi kimi üsullar aiddir.

Norton 360, digər anti-viruslardan daha çox təhlükəsizlik xüsusiyyətləri təqdim edir. Ən ucuz təhlükəsizlik proqramında belə, faydalı olan əlavə xüsusiyyətlər verir: firewall, fişinq əleyhinə müdafiə, parol meneceri, 2 GB bulud ehtiyatı və s.

Norton'un ən yaxşı versiyası olan Norton 360 Deluxe təkmilləşdirməklə, limitsiz bir VPN, dark veb (qaranlıq veb- internetin gizli və anonim hissəsi) nəzarəti, veb kamerası qorunması, gizlilik monitoru və 50 GB-a qədər bulud saxlama mümkündür. ABŞ istifadəçiləri Norton LifeLock planlarının bir hissəsi kimi 250 GB-a qədər bulud saxlama və şəxsi məlumatların, əlaqə məlumatlarının, maliyyə məlumatlarının və digər

gizli məlumatların qanunsuz şəkildə əldə edilməsindən və istifadəsindən qorunmaq üçün tədbirlərdən istifadə edə bilir. Malware skanerinin ən yaxşılarından biri olan Norton antivirusun, real vaxt qorunması da təsirli hesab edilir. Nortonun tam skanını sınadıqdan sonra, real vaxt təhlükəsizliyi aktivləşdirib eyni 997-fayllı malware verilən bazasını sadə fayllar, zipped fayllar və hətta şifrələnmiş fayllar formasında yükləməyə çalışdıqda, kompüter yüklənməyə başlamadan öncə bütün sadə faylları blokladı. Həmçinin korporativ şəbəkələrdə sınaq müddəti zamanı anti-fişinq mühafizəsi yüksək dərəcə göstərdi [20].

Bu fəsildə, korporativ şəbəkələrdə informasiya təhlükəsizliyinin qorunması üçün istifadə edilən avadanlıqlar və prinsipləri təhlil edilir.

1-ci fəslin fərqli hissələrində istifadə olunan Layer-1, Layer-2 və Layer-3 cihazlar ayrı-ayrı təsnif olunur. Bu cihazlar şəbəkədə müxtəlif funksiyaları icra edir və informasiya təhlükəsizliyi üçün əhəmiyyətli rol oynayır. 1-ci fəsildə bu cihazların nə olduqları, funksiyaları və təhlükəsizliklə bağlı nələrə diqqət etmək lazım olduğu aydın şəkildə açıqlanır.

Həmçinin, korporativ şəbəkələrdə istifadə olunan texniki və proqram təminat vasitəsilə təhlükəsizlik tədbirlərinin həyata keçirilməsi burada öz əksini tapır. Bu, qüvvədə olan təhlükəsizlik standartları, firewall və IDS/IPS sistemləri, şifrələmə alqoritmləri və digər mühafizə vasitələri haqqında məlumatlardan ibarətdir. Bu texniki və proqram təminatlarının düzgün tətbiqi və idarə olunması, korporativ şəbəkələrdə informasiya təhlükəsizliyinin qorunmasında əhəmiyyətli bir rola malikdir.

AZƏRBAYCAN RESPUBLİKASI ELM və TƏHSİL NAZİRLİYİ
AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əlyazması hüququnda

NƏSİROV NURLAN SÜBHAN oğlu

AzTU-nun kompüter şəbəkəsində informasiya təhlükəsizliyinin qiymətləndirilməsi sisteminin işlənməsi

mövzusunda

MAGİSTRLİK DİSSERTASİYASI

İxtisas: 060631- " Kompüter mühəndisliyi"
İxtisaslaşma: "Biliklərin əldə edilməsi sistemləri"

Elmi rəhbər: t.f.d., dosent C. Məmmədov

BAKI –2023

II FƏSİL . WİRELESS TEXNOLOGİYALARININ İSTİFADƏSİ ZAMANI İNFORMASİYA TƏHLÜKƏSİZLİYİNİN QORUNMASI VƏZİYYƏTİNİN TƏDQİQİ

2.1. Korporativ şəbəkələrdə istifadə olunan Wireless texnlogiyalarının arxitekturası və tətbiqi prinsipi

Simsiz texnologiya, iki cihazın (və ya obyektin) bir-biriləri ilə kabellər və ya digər fiziki bağlantılar olmadan əlaqə yaratmasına imkan verən bir növ əlaqədir. Bu texnologiyalar, böyük məsafələrdə yerləşən obyektlər arasında məlumat ötürməyə imkan verir. Simsiz şəbəkə texnologiyası XX əsrin əvvəllərində yüksək sürətlə yayılmışdır və bu texnologiyaların diqqət çəkən xüsusiyyəti, kabellərdən istifadə etməməsidir. Simsiz şəbəkənin əsas məqsədi, əksər zamanlar insanların və ya cihazların bir-birilərinə məlumat ötürməsinə imkan verməkdir. Bu cür şəbəkələr, naviqasiya, mobil əlaqələr, internet və bir çox başqa texnologiyada istifadə olunur.

Simsiz rabitə haqqında danışarkən, 1888-cu ildə *Heinrich Hertz* tərəfindən radio dalğalarının kəşf edilməsini bu sahənin əsaslarından hesab etmək olar. Həmin dövrdə qısa bir məsafədə yerləşən iki nöqtə arasında elektromaqnit dalğalarından istifadə edərək simsiz ötürmə aparmaq mümkün olmuşdu. İlk simsiz ötürücülər XX əsrin əvvəllərində radioteleqrafiya vasitəsilə, yəni Morze kodu və ya digər kodlu siqnallar istifadə edərək əlaqə yaratmaqla əldə edildi. Modulyasiya vasitəsi ilə səs və musiqi kabelsiz şəkildə ötürülməsinə imkan yarandıqdan sonra, medium radio adlanmağa başlandı. Simsiz ötürücülər, səs, məlumat, video və ya siqnalların əlaqə yolu ilə daşımaq üçün elektromaqnit dalğalarından istifadə edir.

Radio tezliyə əsasında formalaşan simsiz müasir şəbəkənin əsası, 1970-ci illərdə *Havay* Universitetinin *ALOHANET* tədqiqat layihəsinə aiddir. Texniki olaraq geniş ərazili şəbəkə (WAN) adlanırdı və məkanlar arasında məlumatların yayılması üçün ultra-yüksək tezlikli siqnallardan istifadə edir. ALOHANET-in əsasında olan

texnologiya, 1973-cü ildə Ethernet-in yaradılmasına töhfə verdi və 802.11, ilk simsiz standartın inkişafında əhəmiyyətli bir rol oynadı. Simsiz rabitə yüz ildən artıq mövcud olmasına baxmayaraq, son 15 ildə xüsusilə 802.11ac və 4G standartlarının təsdiqindən sonra texnologiya geniş müəssisə , əhatəli tətbiqlərin və xidmətlərin inkişafına imkan verəcək qədər təkamül etdi.

Simsiz şəbəkə - Simsiz şəbəkə verilənlərin radiotezliklər vasitəsilə bir neçə cihazın qruplaşması üzərində göndərilməsi və qəbul edilməsidir. Simsiz şəbəkələr adətən elektromaqnit dalğalar spektrində müəyyən bir aralığ üzərində radiotransmissiya vasitəsi ilə məlumat göndərmək və qəbul etmək üçün istifadə olunur. Verilənlərin simsiz şəbəkə üzərində göndərilməsi əsasən, bir cihazda yerləşdirilmiş antena vasitəsi ilə aparılır. Fərqli simsiz şəbəkələr müxtəlif frekans aralıqlarını istifadə edir.

Simsiz şəbəkələrin növləri :

Simsiz LAN. *(eng. WLAN- Wireless Local Area Network)* - WLAN, şəbəkədəki qurğular arasında bağlantı yaratmaq üçün, naqilli bağlantı əvəzində radio texnologiyasından istifadə edir. IEEE tərəfindən təyin olunmuş standartlardan istifadə edərək Wi-Fi, qurğular arasında əlaqə yaratmağa imkan verən simsiz giriş nöqtələri *(eng. WAP)* vasitəsilə WLAN üzərindən ötürmə vasitəsi olaraq istifadə olunur.

WLAN - iki fərqli üsulla konfiqurasiya edilə bilər:

1. *İnfrastruktur rejimi:* Bu rejimdə ev və ya ofis Wi-Fi şəbəkəsi bir WLAN-ın infrastruktur rejimində qurulur. Şəbəkədə olan qurğuların hamısı baza stansiyası vasitəsilə bir-biri ilə və ya internetlə əlaqələrini təmin edir. Baza stansiyası, yəni Wi-Fi router, WLAN-a qoşulan bütün qurğularla əlaqə quraraq, hər bir cihaza internetə çıxış imkanı verir.

2. *Ad hoc*: Ad hoc şəbəkəsi qurularkən Wlan baza stansiyası istifadə etmədən kompüter və mobil qurğular kimi nöqtələri əlaqələndirir. Ad hoc simsiz şəbəkələr üçün Wi-Fi Direct texnologiyası tətbiq olunur. Ad hoc WLAN quraşdırılması asandır və əsas peer-to-peer (P2P) bağlantısını təmin edir.

WLAN - Wireless Local Area Network arxitekturası korporativ şəbəkələrdə wlan arxitekturası mobillik və çevik iş mühitlərinə artan tələbat səbəbindən şəbəkənin önəmli hissəsinə çevrilmişdir. Müəssisədə WLAN-lar arasında müxtəlif istifadəçilərə, cihazlara, tətbiqlərə və məkanlara xidmət etməli və təhlükəsizlik, etibarlılıq və yüksək performans baxımından əlaqəni təmin etməlidir. Haqqında məlumat verilən tələblər, məhdudiyyətlər və təcrübələr nəzərə alaraq yaxşı dizayn edilmiş WLAN arxitekturasını istinad edir.

Tövsiyə olunan *WLAN* arxitekturası üç səviyyədən ibarətdir:

1. Simsiz Giriş Layeri (*eng Wireless Access Layer*)
2. Paylama Layeri (*eng the Distribution Layer*)
3. Əsas Layer. (*eng the Core Layer*)

Korporativ şəbəkələrdə wireless Access Layer noutbuklar, smartfonlar və tətbiqlər kimi istifadəçi cihazlarına simsiz qoşulma prosedurunu təmin etmək üçün istifadə edilən səviyyədir. Şəbəkənin əhatə dairəsində yerləşdirilən giriş nöqtələrindən (AP) ibarətdir.

Distribution Layer, Access Layer və Core Layer arasında şəbəkədə istifadə edilən trafikə nəzarət etmək və idarə etmək üçün cavabdehdir. Məqsəd hər bir acces-pointlərin mərkəzləşdirilmiş idarə edilməsini və onlara nəzarətini təmin edən simsiz LAN nəzarətçilərindən (*WLC*) ibarətdir. Core Layer şəbəkədə *WLAN*-ın əsasını təşkil edir və İnternet, məlumat mərkəzləri və digər uzaq yerlər kimi digər şəbəkələrə qoşulma prosedurunu təmin edir.

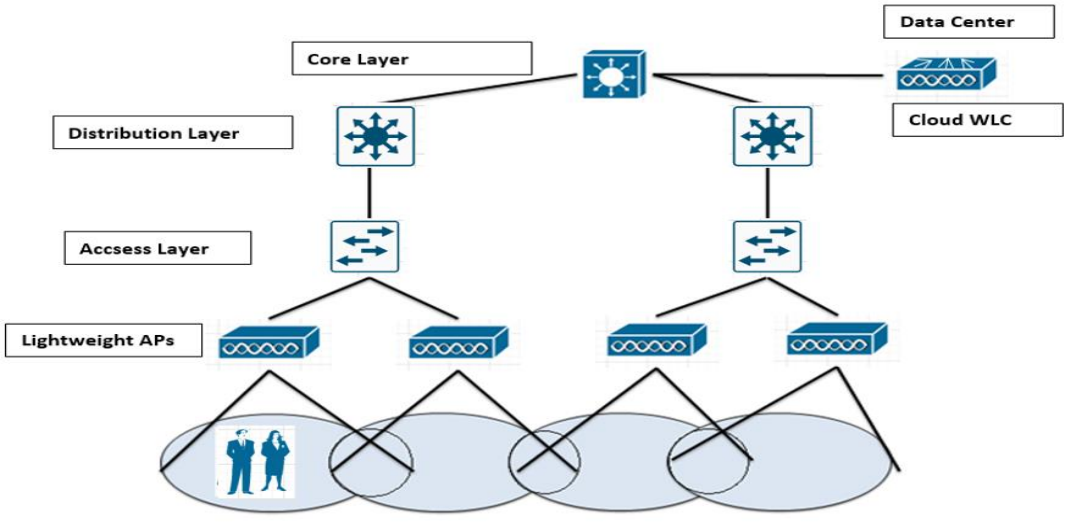
Simsiz Giriş Layeri istifadəçi cihazlarına simsiz qoşulmanı təmin edən həm fiziki, həm də məntiqi komponentlərdən ibarətdir. Fiziki komponentlərə access-pointlər, antenalar, kabellər və enerji mənbələri daxildir. Məntiqi komponentlər bölməsinə wireless protokollar, təhlükəsizlik mexanizmləri və xidmət keyfiyyəti (QoS) parametrləri aid edilir. AP-lər *autonomous, cloud-managed və controller-based* (nəzarətçi əsaslı) kimi müxtəlif konfiqurasiyalarda yerləşdirilir.

Distribution səviyyəsi access-pointlərin mərkəzləşdirilmiş şəkildə idarə edilməsini və nəzarətini təmin edən WLC-lərdən ibarətdir. WLC-lər radiotezlik (RF) mühitinin

idarə edilməsinə, təhlükəsizlik protokollarının həyata keçirilməsinə və yüksək performansın göstərilməsinə cavabdehdir. Controller yük balansı, qüsursuz rouminq və istifadəçi autentifikasiyası kimi funksiyaları tətbiq edirlər. WLC-lər *mərkəzi (eng central), yerləşdirilmiş (eng embedded), Mobility Express WLC və bulud əsaslı (eng cloud-based)* kimi müxtəlif konfiqurasiyalarda istifadə edilə bilər.

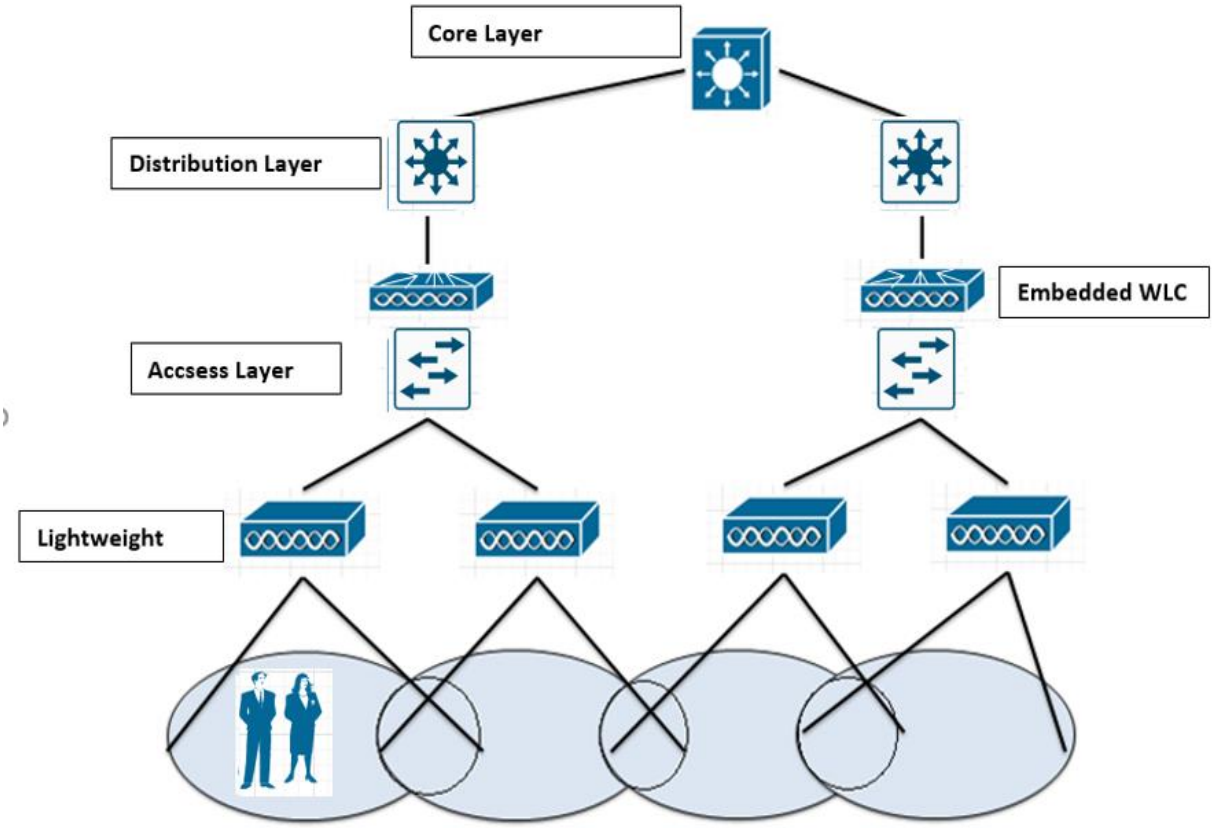
Mərkəzi yerləşdirmə bütün AP-ləri idarə edən tək WLC-dir, ona qoşulmuş access-pointlərin sayını maksimuma çatdıra biləsiniz. İstifadəçilərin əldə etməli olduğu resursların əksəriyyətinin məlumat mərkəzi və ya internet kimi mərkəzi bir yerdə yerləşdiyi arxitekturaya tətbiq etməyə meyllidir. Mərkəzləşdirilmiş controller istifadəçilərə təsir göstərən təhlükəsizlik protokollarını tətbiq etmək üçün əlverişli yer təmin edir. Korporativ şəbəkəsinin access səviyyəsinə qoşulmuş yüzlərlə AP ola bilər. Bu controller də 6000 access-point dəstəkləyə bilər. Əgər korporativ şəbəkədə bu say keçərsə, əlavə WLC istifadə edilməlidir.

Cloud-based WLC fiziki cihaz kimi deyil, virtual maşın kimi istifadə edilir. Bulud əsaslı xidmətdən istifadə edərək, adətən 3000-ə qədər AP-ni dəstəkləyə bilər. Simsiz şəbəkəniz dahada genişlərsə, əlavə WLC-lər daha çox virtual maşın kimi istifadə edilə bilər (şəkil 2.1).



Şəkil 2. 1. Bulud əsaslı yerləşdirmədə WLC Yeri

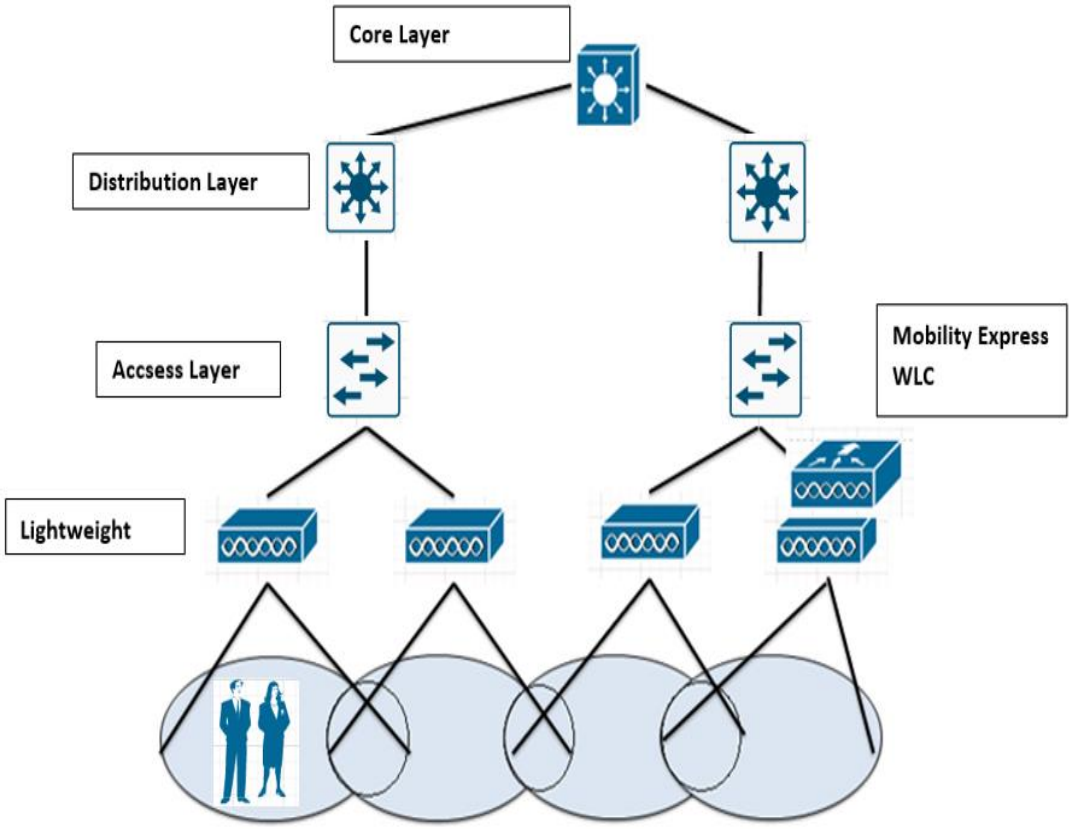
AP-lərin sayı əvvəlkilərdən nisbətən az olan kiçik şirkətlər və ya filial yerləri üçün, WLC şəkil 2. 2 - də göstərildiyi kimi switchlərlə stack formada birlikdə yerləşdirilə bilər. Xüsusilə məhdud büdcələri və daha az istifadəçi nöqtələri olan kiçik yerləşdirmələr üçün ilk haqqında məlumat verilən mərkəzləşdirilmiş simsiz arxitekturaya sərfəli bir alternativdir. Tipik cisco quraşdırılmış WLC-lər 200-ə qədər ap dəstəkləyə bilər. Access-pointlərin mütləq controllerə ilə birlikdə olan switchlərə qoşulmasına ehtiyac yoxdur, fərqli məkanlardakı digər switchlərə qoşulmuş access pointlərdə yerləşdirilmiş (*eng embedded*) WLC-yə qoşula bilər.



Şəkil 2. 2. Daxili Yerləşdirmədə WLC Yeri

Korporativ şəbəkələrdə kiçik, orta miqyaslı məkanlarda, xüsusi WLC-lərə rəhbərlik tərəfindən investisiya etmək istənməyə bilinər. WLC funksiyası kiçik müəssisələrdə quraşdırılmış AP ilə birgə qoyula bilər. Şəkil 2.3-də göstərildiyi kimi

Cisco Mobility Express WLC yerləşdirilməsi kimi tanınır. WLC-yə ev sahibliyi edən AP eyni nöqtədədəki hər hansısa bir AP-lə birlikdə WLC ilə *CAPWAP tunelini* tətbiq edə bilər. Mobility Express controlleri 100-ə qədər AP-ni dəstəkləyə bilər.



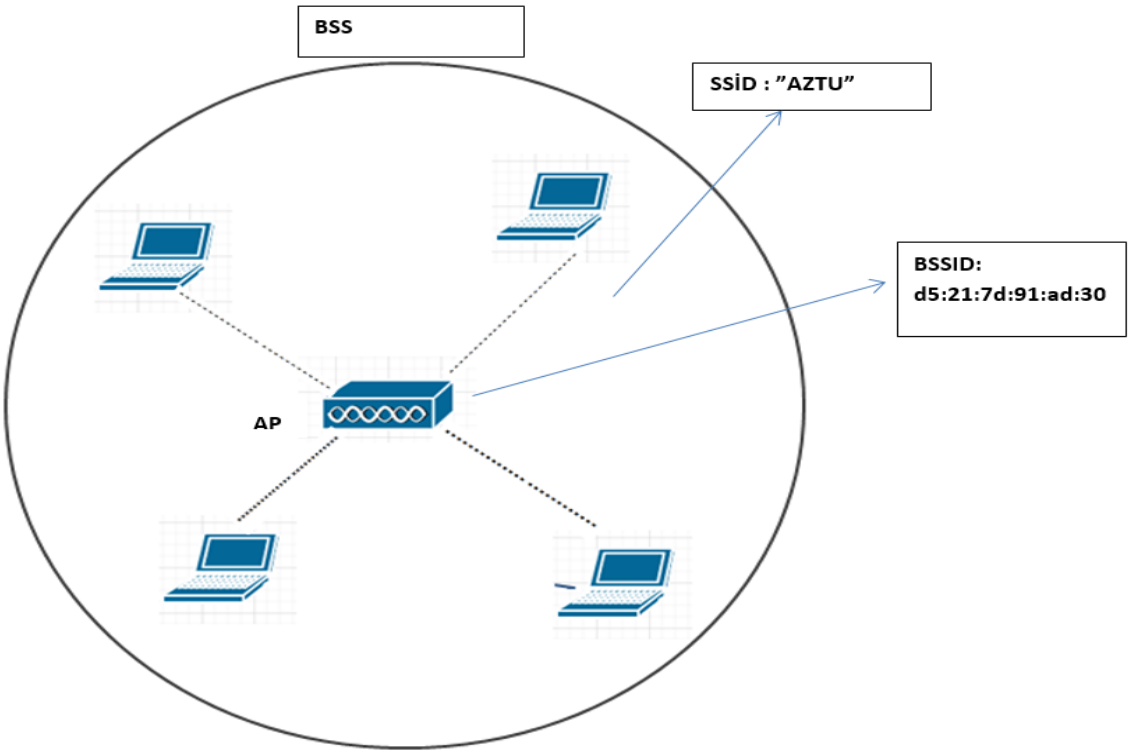
Şəkil 2. 3. Mobility Express Yerləşdirmədə WLC nöqtəsi

Cədvəl 2. 1. Summary of WLC Deployment Models (WLC Yerləşdirmə Modellərinin xülasəsi)

Deployment Model (*Yerləşdirmə modeli*)	***WLC Location (DC, Access,Central,AP (WLC vəziyyəti)***	***Aps Supported* (*AP-lər dəstəklədiyi say)***	***Clients Supported (Müştərilər Dəstəklədiyi say)***	***Typical Use (Tipik istifadə)***
Unified	Central	6000	64,000	Large enterprise
Cloud	DC	3000	32,000	Private cloud
Embedded	Access	200	4000	Small campus
Mobility Express	Ocher	100	2000	Branch location
Autonomous	N/A	N/A	N/A	N/A

1. *Basic Service Set -Əsas Xidmət Dəsti* (eng. BSS- Basic Service Set)

Hər bir simsiz xidmət sahəsini sabit cihaz ətrafında formalaşan qapalı mobil qurğular qrupuna çevirməkdir; cihaz iştirak etməzdən əvvəl öz məlumatlarını daxil etməli və sonra qoşulmaq üçün icazə almalıdır. 802.11 standartı bunu əsas xidmət dəsti (BSS) adlandırır. Hər bir BSS-nin mərkəzində şəkil 2.4-də göstərildiyi kimi simsiz giriş nöqtəsi (AP) yerləşir.

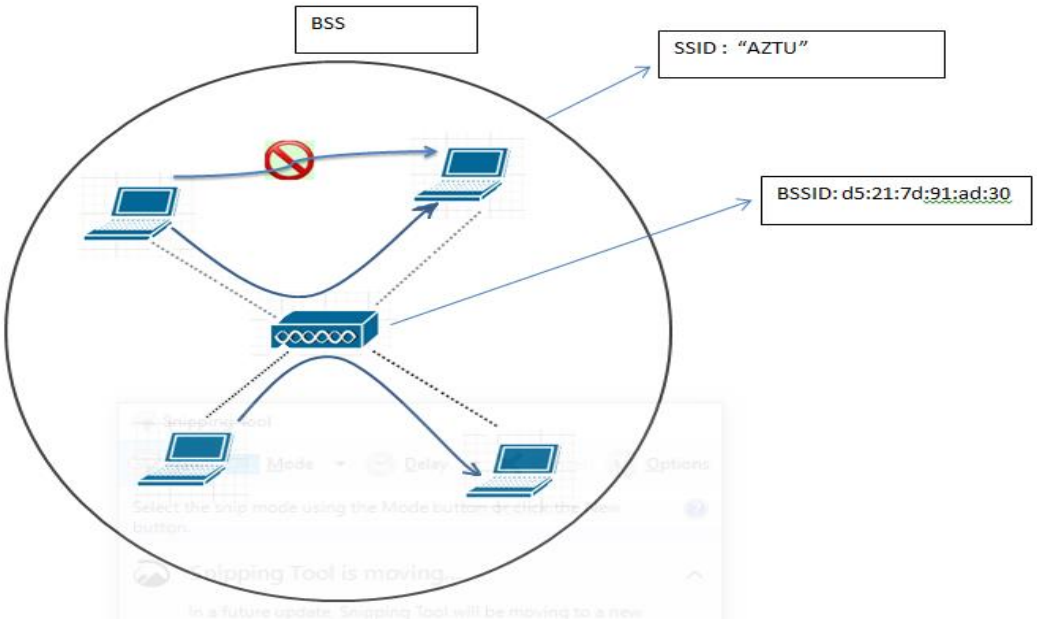


Şəkil 2. 4. 802.11 Basic Service Set

Burada AP *infrastruktur* rejimində işləyir, yəni istifadəçiyə simsiz şəbəkənin infrastrukturunu formalaşdırmaq üçün lazım olan xidmətləri təklif edir. Şəbəkədə AP öz BSS-ni tək simsiz kanal üzərində qurur. AP və BSS üzvləri doğru bağlantı qurmaq üçün hamısı eyni kanaldan istifadə etməlidirlər. BSS-nin işləmə proseduru AP-dən asılı olduğundan, BSS yalnız AP-nin siqnalının əhatə edə biləcəyi sahə ilə məhdudlaşır. Bu əsas xidmət sahəsi (*eng BSA- basic service area*) tanınır. Şəkil 2.4-də, BSA AP-nin ətrafında mərkəzləşən sadə kölgəli dairəvi sahə kimi göstərilir.

AP-yə qoşulan antenadan və siqnallarına təsir göstərə biləcək fiziki mühitdən asılı olaraq BSA başqa formalara da malik ola bilər. Bundan əlavə, AP simsiz şəbəkəni məntiqi adı ehtiva edən mətn sətri olan **Service Set Identifier (SSID)** ilə reklam edir. SSID istifadəçilərin cihazlarında wi-fi şəbəkəsinə qoşulmaq üçün istifadə elədiyi bir servisdir. BSSID-ni BSS cihazını (AP) unikal şəkildə təyin edən maşın tərəfindən oxuna bilən ad etiketi və SSID-ni simsiz xidməti qeyri-adi formada müəyyən edən, insan

tərəfindən oxuna bilən ad etiketi adlandıra bilərik. BSS-ə qrupuna üzvlük *assosiasiya* adlanır. Simsiz cihaz AP-yə assosiasiya sorğusu göndərməlidir və bu prosedurdan sonra AP sorğunu ya verməli, ya da rədd etməlidir. İcazədən sonra cihaz BSS-nin istifadəçisi və ya 802.11 stansiyası (*802.11 station STA*) olur. Növbəti prosedurda access-point BSS ilə əlaqəli olaraq qaldığı müddətcə istifadəçiyə və ondan gələn əlaqələrin əksəriyyəti şəkil 2.5-də göstərildiyi kimi AP-dən keçməlidir. BSSID-dən mənbə və ya təyinat ünvanı kimi istifadə etməklə, informasiyanı AP-ə və növbəti addımda ondan cihaza ötürülə bilər (şəkil 2.5).



Şəkil 2. 5. BSS daxilində trafik axınları

Simsiz giriş nöqtəsi (eng. Wireless Access Point) - Simsiz giriş nöqtəsi (WAP), simsiz şəbəkələrdə istifadə edilən bir şəbəkə qurğusudur və simsiz qurğuların şəbəkəyə qoşulması üçün bir giriş nöqtəsi təmin edir. Simsiz qurğular (məsələn, telefonlar, tablet kompüterlər, noutbuklar və s.) bu qurğu vasitəsi ilə simsiz şəkildə şəbəkəyə qoşula bilər. Həmçinin Simsiz giriş nöqtəsi (WAP) - hər hansı bir şəbəkənin əhatəsini genişləndirmək üçün istifadə edilən bir qurğudur.

Simsiz şəbəkə qurmaq üçün WAP istifadə etməyin üstünlükləri:

- Simsiz giriş nöqtəsi (WAP) vasitəsi ilə , hər hansı bir simli şəbəkənin daxilində simsiz şəbəkə qurmaq mümkündür. Bununla da, simsiz qurğuların şəbəkədə istifadəsi üçün şərait yaradır.
- Simsiz giriş nöqtəsi (WAP) vasitəsilə əhatə dairəsinin genişləndirilməsi, xüsusilə daha böyük ofis məkanlarında və ya binalarda təsir zonasının xaricində olan siqnalların çatmadığı yerlərdən xilas olmaq üçün simsiz şəbəkənin siqnal diapazonu və gücünün artırılması üçün istifadə edilə bilər.
- Simsiz giriş nöqtəsi (WAP) bir çox müasir mobil telefon və şəbəkə qurğuları tərəfindən dəstəklənir.
- Simsiz giriş nöqtələrinin uyğun qiyməti, sadə quraşdırılması, tənzimlənməsi və idarə olunması çox rahatdır. Belə ki, hər bir simsiz giriş nöqtəsi (WAP) ilə bir çox xüsusiyyətlər təmin edilir, istifadəçilərə sadəcə lazım olan xüsusiyyətləri seçmək və şəbəkəni tənzimləmək imkanını verir.
- Simsiz giriş nöqtələri (WAP), yeni Wi-Fi 6 (802.11ax) standartına uyğun olaraq hazırlanmışdır və günümüzdə sayı artmaqda olan əşyaların interneti (İoT) qurğularının idarə edilməsi üçün genişləndirilə bilən, təhlükəsiz və etibarlı simsiz şəbəkə yaratmağa kömək edir.

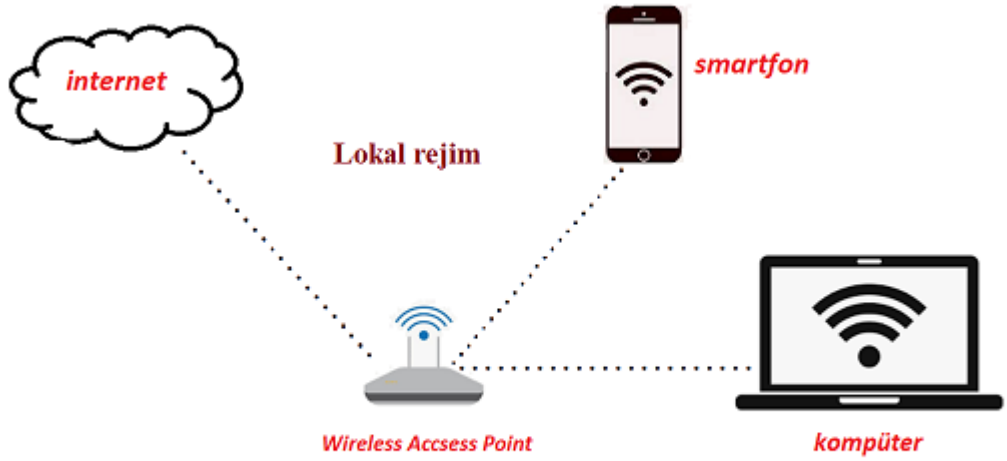
Access-point rejimləri

Hər bir **"yüngül" AP (Lightweight Access Point - LWAP)** bir neçə fərqli AP rejimində fəaliyyət göstərmək üçün konfiqurasiya edilir. Korporativ şəbəkələrdə bəzi rejimlərdə AP müştərilərə şəbəkədə bağlantı imkanı yaradaraq internet və ya digər şəbəkə xidmətlərinin istifadəsinə imkan verən şəbəkə xidməti təqdim edir, bəzilərində isə AP xüsusi şəbəkə idarəetmə vasitəsi kimi istifadə olunur.

Lokal rejim *(eng. Local Mode)*

Lokal rejim (Local Mode) standart rejimdir. Lokal rejimdəki bir AP, bütün WLAN-ların istifadəçi trafikini, *CAPWAP* (Control and Provisioning of Wireless Access Points- Simsiz Giriş Nöqtələrinə Nəzarət və Təminat) şəbəkə protokolu vasitəsilə

verilənləri paketlər şəklində təhlükəsiz bir şəkildə ötürür. AP modellərinin hamısı Lokal rejimdə işləyə bilər (şəkil 2.6).

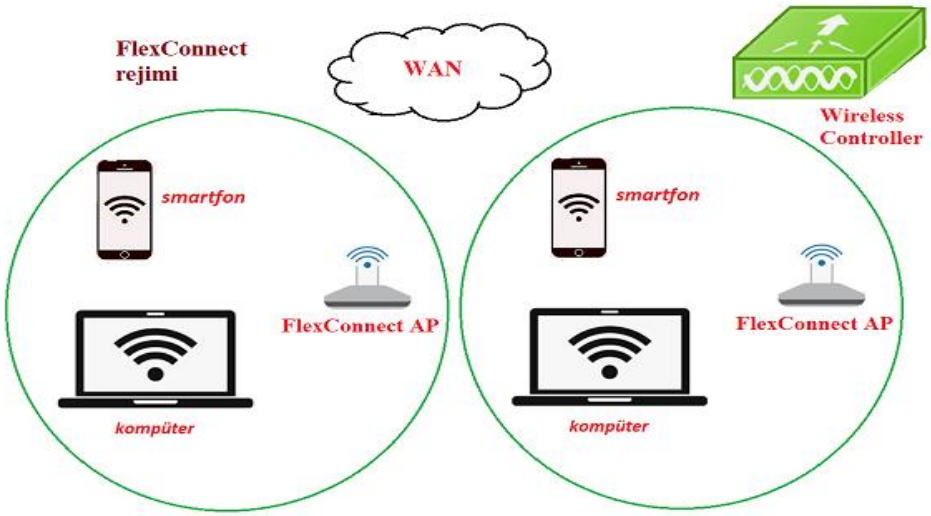


Şəkil 2. 6. Lokal rejim

FlexConnect rejimi *(eng. FlexConnect Mode)*

FlexConnect rejimində *WLAN (Wireless Local Area Network)* konfiqurasiyasına bağlı olaraq ya *CAPWAP (Control and Provisioning of Wireless Access Points)* protokolu vasitəsilə AP-dən gələn istifadəçi trafikləri təhlükəsiz bir şəkildə WLC-ə (Wireless LAN Controller) göndərə bilərik, ya da AP-dən gələn istifadəçi trafikləri, WLC-yə getmədən öncə yerli şəbəkədəki digər qurğulara (switch və ya router kimi) ötürülə bilər.

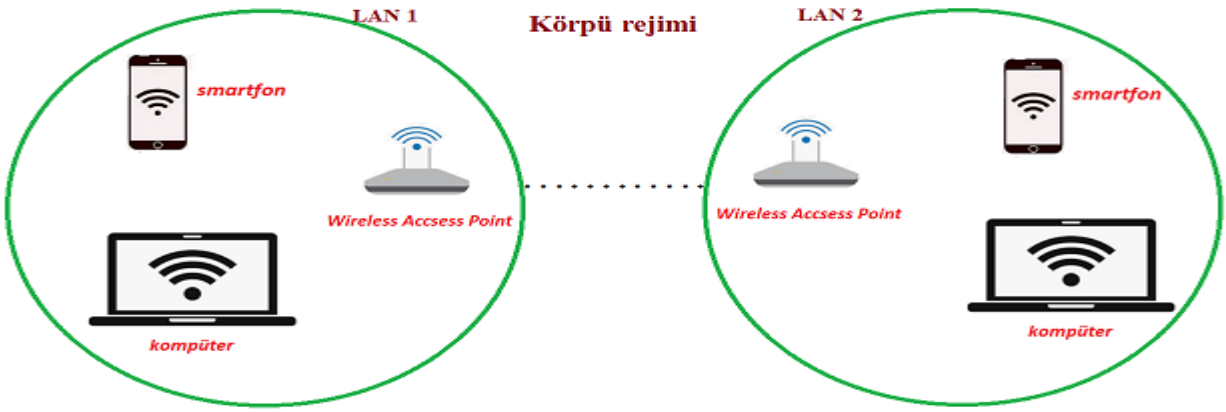
Bütün modellər FlexConnect rejimini dəstəkləyir lakin, bu rejimdəki AP-lər mesh əməliyyatını dəstəkləmir. Mesh əməliyyatları, bir şəbəkədə əlavə AP-lərin məhz tətbiqi yolu ilə şəbəkənin özünün qurulmasına imkan verir. Bu əməliyyatla, bir-birinə çox yaxın olmayan AP-lər bir-biriləri ilə əlaqə yaratmaq üçün istifadə edilə bilər. FlexConnect rejimi AP-ləri isə, yalnız istifadəçi trafiklərini idarə etmək üçün hazırlanmışdır və mesh əməliyyatlarını dəstəkləmir (şəkil 2.7).



Şəkil 2.7. FlexConnect rejim

Körpü rejimi *(eng. Bridge Mode)*

Körpü rejimi xarici Access Pointlərdə (daxili Access Pointlərdə də dəstəklənir) təyin edilmiş rejimidir. Giriş nöqtələrinin bu rejimində iki şəbəkəni birləşdirmək üçün istifadə olunur, burada AP şəbəkələr arasında köprü kimi hərəkət edir. AP-lər və WLC(Wireless LAN Controller) arasında kabel əlaqəsi olmadan istifadə edilən bu rejim, ayrı-ayrı şəbəkələrin təmin edilməsi üçün ən optimal yoldur, lakin bütün AP modelləri bu rejimi dəstəkləmir (şəkil 2.8).



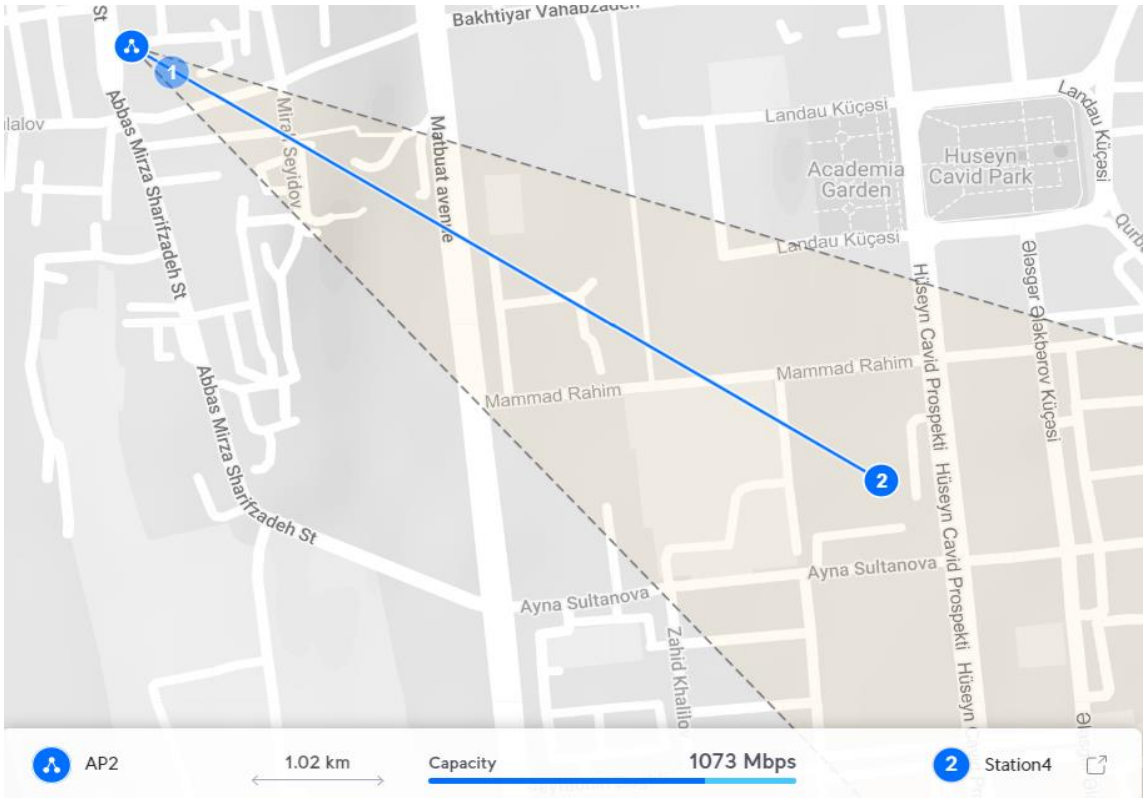
Şəkil 2. 8. Körpü rejimi

Flex + Körpü rejimi *(eng. Flex + Bridge Mode)*

Flex + Bridge AP rejimi, FlexConnect və Körpü AP rejiminin hər ikisinin birlikdə istifadə olunduğu rejimdir. Bu xüsusiyyət, şəbəkə qurğularının mesh dəstəyinə malik olduğu zaman əlavə edilir və bu, daha böyük və əvvəlcədən planlanlaşdırılmamış məkanlarda tətbiq edilə bilən bir şəbəkə arxitekturasıdır. Məsələn, böyük bir binada və ya stadionda kabel çəkmək mümkün olmadığı üçün bu tip bir şəbəkə arxitekturasına ehtiyac ola bilər [7].

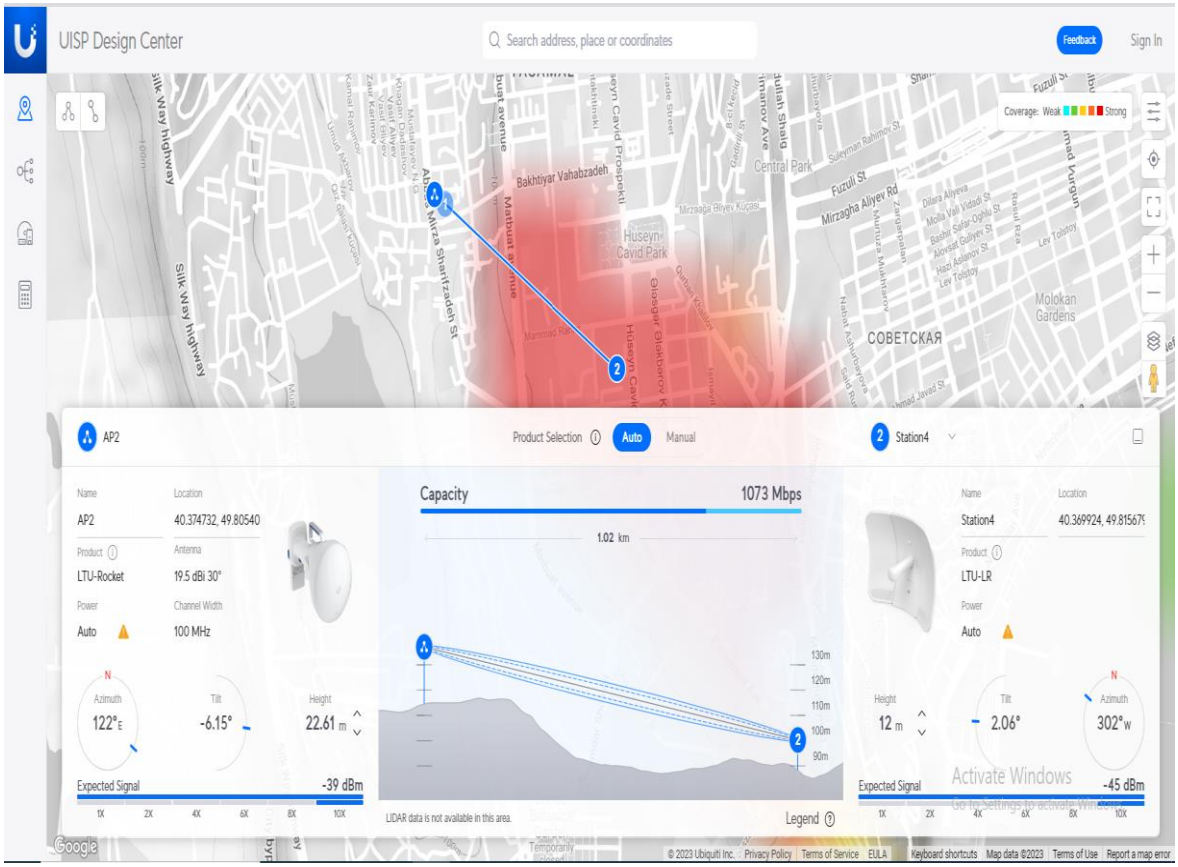
2.2. Azərbaycan Texniki Universitetinin kompüter şəbəkəsində Wireless texnologiyasının təhlükəsiz tətbiqi mexanizmləri

Azərbaycan Texniki Universitetində wi-fi texnologiyası şəbəkədə tətbiq edilmişdir. Korporativ şəbəkələrdə wireless texnologiya yalnız access-pointlərlə deyil, həm də antenlərin, controllerlərin və s. kimi cihazların istifadəsi ilə tamamlanır. Anten istifadəsi, əsasən, böyük şəbəkələrə malik müəssisələrdə tətbiq edilir. Bu texnologiyanın istifadəsi bəzi məqamlarda öz üstünlüyünü göstərir. Belə ki, relyefindən asılı olmayaraq optika xətti istifadə edilməyən ərazilərdə antenin tətbiqi bizlərə üstünlük verir. Uyğun qiymətə antenlərdən istifadə edərək, əlavə xərclərin qarşısı alınır. Antenlərin məsafə ölçüsü 20-30 km arası dəyişə bilər. Texniki universitetdə antenlərdən istifadə edilməsə də, gələcəkdə bu texnologiya tətbiq edilə bilər. Məsələn, anten texnologiyasını univeristet və yataqxana arasındakı məsafədə tətbiq edək. Hər iki ərazi arasında məsafə çox olmadığından, 2 ədəd anten istifadə edilir.



Şəkil 2. 9. Anten monitorinq

Şəkil 2.9-dan göründüyü kimi anten 1 yataqxana, anten 2 universitet ərazisində qoyulub. Hər birinə access switchdən bir port ayrılır. Bu portlar həm access, həmdə trunk vəziyyətində ötürülə bilər. Hər iki anten arası 1073 Mbps trafik ötürülə bilər. Məsafə 1 km şəklində təsvir edilmişdir.



Şəkil 2. 10 . Anten arası trafikin analizi

Şəkil 2.10-dən isə antenlər arası məsafədə problemin və əgər problemlə qarşılaşarıqsa trafikə necə təsir edəcəyini göstərir [21].

Azərbaycan Texniki Universiteti şəbəkəsində wireless texnologiyadan yalnız access-pointlərdən və controllerdən istifadə edilir. Access point anlayışını fəsil 2.1-də haqqında məlumat verilmişdir. Access-pointlər 2 növdə tətbiq edilə bilər:

1. *Autonomous Access Points*
2. *Lightweight Access Points*

Avtonom access pointlər şəbəkədə tətbiq edilməmişdir. Avtonom adından da göründüyü kimi, controller tək bir cihaza istənilən dəstəkdən əlavə müstəqil şəkildə trafiki idarə etməyə imkan verir. Avtonom access point simsiz əlaqədə bir nəfərlik ordudur. Siz ona istək daxilində cihazlar qoşa bilərsiniz (cihazların dizaynı çərçivəsində). Trafik üçün əlavə dəstəyə ehtiyacınız varsa və şəbəkəni genişləndirmək istəyirsinizsə, yeni konfiqurasiya edilmiş avtonom access-pointləri əlavə edə bilərsiniz.

Avtonom access-pointlər müstəqildir; həm naqilli, həm də simsiz avadanlıqla təchiz edilmişdir ki, istifadəçi assosiasiyaları AP-də yerli olaraq simli əlaqə ilə bağlantıları əlaqələndirə bilsin.

Lightweight access-pointləri avtonom nöqtələrə bir qədər əks olaraq hazırlanmışdır. "Lightweight" termini bu cihazların müstəqil və yalnız işləyə bilməyəcəyini ifadə edir. Lightweight access pointləri xarici simsiz LAN nəzarətçisinə (WLC) etibar edirlər. Controller vasitəsilə bir çox lightweight access pointləri eyni şəbəkədə işləmək üçün konfiqurasiya edilə bilər. Bu dizayn wireless şəbəkənin genişləndirilməsini asanlaşdırmaq üçün nəzərdə tutulub. Asılı lightweight cihazlar öz konfiqurasiyalarını WLC-dən götürürlər. Şəbəkəyə əlavə edilərkən controllerdə access pointin adı qeyd edilir, amma ip ünvanı, mask və digər konfiqurasiyalar avtomatik olaraq controller tərəfindən təyin edilir. Bura protokollar, təhlükəsizlik və konfiqurasiya ilə əlaqəli hər şey daxildir.

Hər iki tipi fərqləndirmək vacibdir. Lightweight access pointlər WLC vasitəsilə problemsiz əlaqə qura bilsə də, sistem avtonom access-pointləri tərəfindən istifadə edilən fərqli protokolda işləyir. Bu o deməkdir ki, avtonom AP-lər və lightweight AP-lər əhəmiyyətli həll yolları istifadə edilmədən eyni şəbəkədə birlikdə işləyə bilməz. Avtonom və lightweight rejimlər arasında keçid həmişə sadə proses olmayacaq. Bu proses istehsalçıdan və istifadə olunan modeldən asılı olacaq.

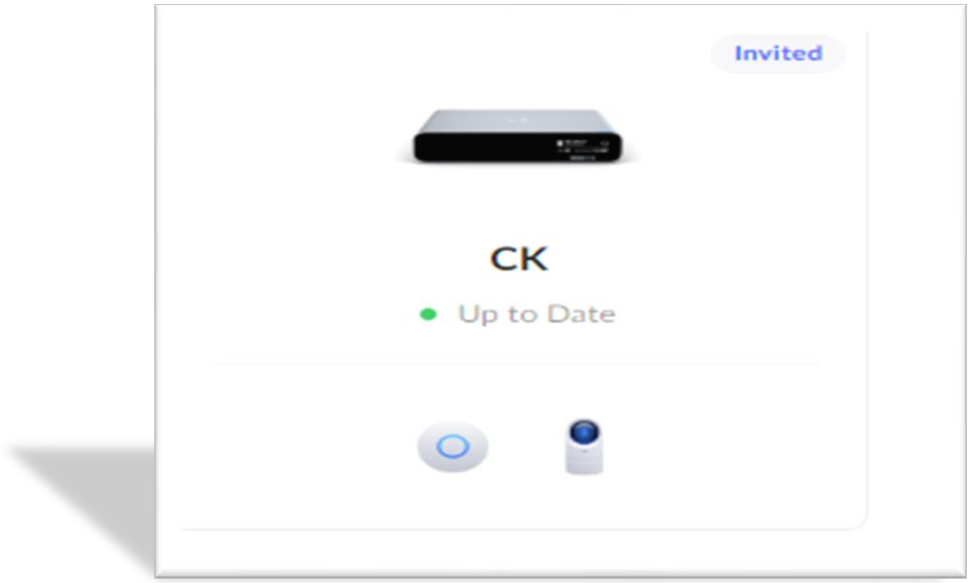
Texniki universitetin şəbəkəsində istifadə edilən access pointlər lightweight rejimdə işləyir. Zamanla universitetdə access-pointlərin sayını artıraraq, həm korpuslarda, həm də universitet həyətində wi-fi istifadəsini əlverişli etmək olar.

Lightweight Access Point Protocol (LWAPP) və Control and Provisioning of Wireless Access Points (CAPWAP) kimi lightweight access-pointləri protokolları simsiz Giriş Nöqtələrinin (AP) idarə edilməsini asanlaşdırmaq üçün tez-tez istifadə olunur. Bu protokollar AP-lərə controller ilə qarşılıqlı əlaqə yaratmağa imkan verir. Təhlükəsizlik baxımından həm AP-lər, həm də WLC arasında bağlantı qurarkən istifadə olunan protokollar vacibdir.

LWAPP və CAPWAP təhlükəsiz əlaqəni təmin etmək üçün öz təhlükəsizlik mexanizmlərindən istifadə edir. Bu mexanizmlərə *AES (Advanced Encryption Standard) və ya TKIP (Temporal Key Integrity Protocol)* kimi güclü şifrələmə alqoritmləri daxildir. Bu prosedurdan əlavə, *802.1X autentifikasiyası və TACACS* serverləri kimi digər təklif olunan təhlükəsizlik tədbirləri də istifadə edilə bilər.

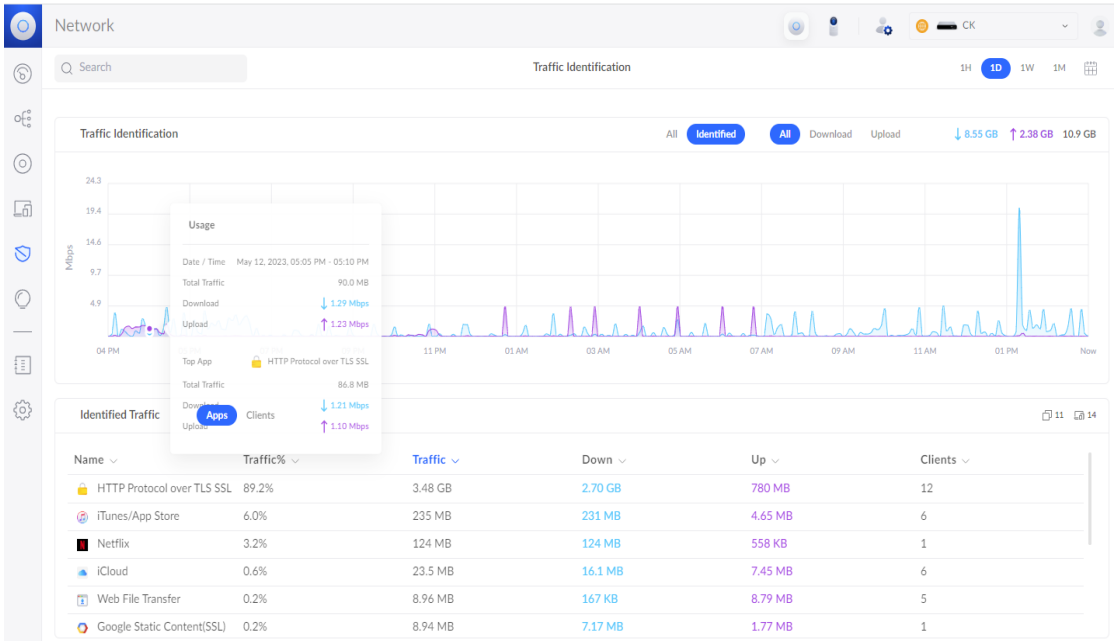
Tətbiq kontekstindən və xüsusi istənilən tələblərdən asılı olaraq müxtəlif təhlükəsizlik protokolları istifadə oluna bilər. Məsələn, CAPWAP istifadə edərək, access pointlər WLC-yə qoşulmazdan əvvəl sertifikatın yoxlanılması prosedurunu həyata keçirmək üçün hazırlana bilər. Access pointlərə yalnız səlahiyyəti olan cihazların WLC-yə bağlanmasına icazə verməklə şəbəkənin təhlükəsizliyini artıra bilərik. Ən yaxşı təcrübə təhlükəsizlik üsulları üçün IEEE 802.11i düzəlişi hələ hazırlanarkən Wi-Fi Alliance ilk nəsil WPA sertifikatını (WPA1 deyil, sadəcə WPA kimi tanınır) təqdim etdi. WPA 802.11i protokoluna əsaslanırdı və 802.1x autentifikasiyası, TKIP və dinamik şifrələmə açarının idarə edilməsi metodunu istinad edirdi. 802.11i ratifikasiya olunduqdan sonra Wi-Fi Alliance onu tam şəkildə WPA versiya 2 (WPA2) sertifikatına daxil etdi. WPA2 WPA-dan köhnəlmiş TKIP autentifikasiya əvəzinə, üstün şifrələmə AES CCMP alqoritmlərinə əsaslanır. WPA2 WPA-nı əvəz etmək üçün nəzərdə tutulmuşdur [7]. Texniki universitetin şəbəkəsində WPA2 autentifikasiya üsulundan istifadə edir. Qoşulduğumuz SSID **“AzTU”** adlanır və password kimi *“AztuİT@1950”* təyin edirik.

Azərbaycan Texniki Universitetində isitifadə edilən vendor **UniFi Design Center** texnologiyasıdır. UniFi access-pointlər korpuslarda müəyyən məsafə aralıqları ilə şəbəkəyə qoşulmuşdur. UniFi controllerdən istifadə edərək access-pointləri idarə edə bilərik (şəkil 2.11).



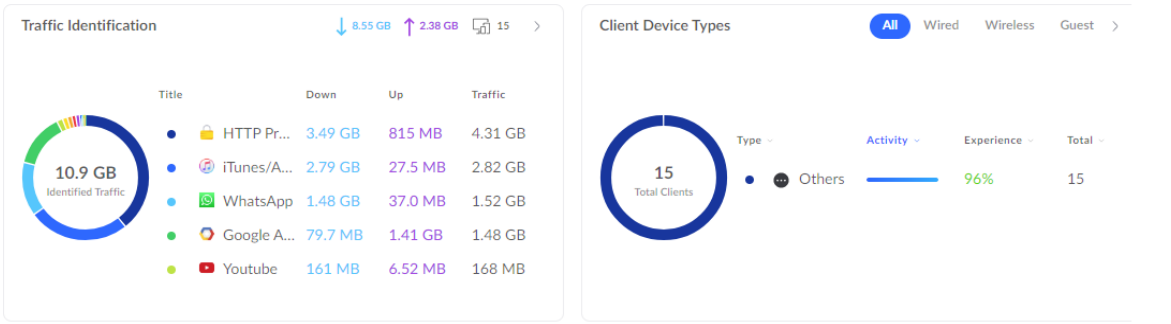
Şəkil 2. 11 . Controllerə giriş

Şəkil 2.12-də göründüyü kimi istifadə edilən trafikin həcmi və tətbiqlərin siyahısı göstərilmişdir. Trafikdə təhlükəsiz şəkildə 8.55 Gb informasiya yüklənmə, 2.38 GB isə göndərilmə prosesi olmuşdur. Biz bu trafik həcmini sol yuxarı hissədə göstərilən vaxta əsasən təyin edə bilərik və hesablanan cəmi 10.9 GB internet trafiki 1 gün ərzində istifadə edilmişdir.



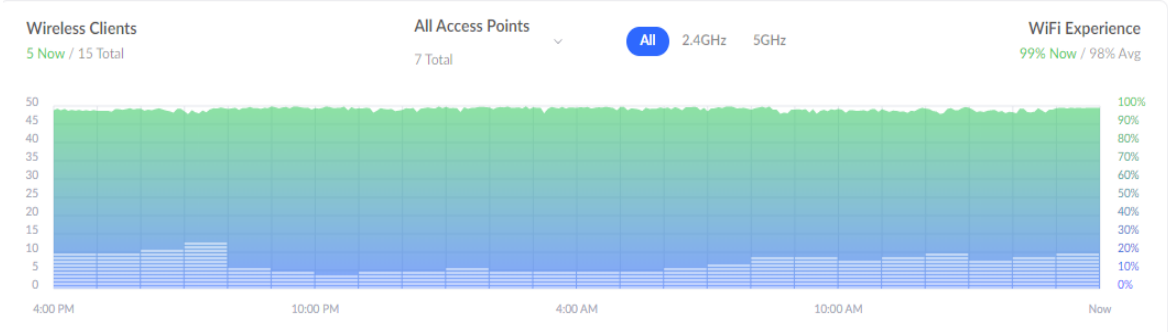
Şəkil 2. 12 . Controllerdə istifadə edilən trafik və tətbiqlər

Şəkil 2.13-də trafik istifadəsini daha aydın şəkildə göstərilmişdir. Əlavə olaraq, aktiv şəkildə qoşulan istifadəçi sayısı hesablanmışdır. Hal-hazırda 15 istifadəçi internetdən aktiv və problemsiz şəkildə istifadə edə bilir.



Şəkil 2. 13 . İstifadə edilən trafik və tətbiqlər , aktiv istifadəçi sayısı

Şəkil 2.14-də hazırda olduğu məkanda istifadə edilən 7 access point görəcəksiniz. Qrafik isə gün ərzində istifadə müddəti, dərəcəsi və göstərdiyi xidmətin keyfiyyətini izah edir. Təhlükəsizlik protokolları vasitəsi ilə gün ərzində ortalama trafik 98 % , hazırda isə 99 % internet təmin edə bilir.



Şəkil 2. 14 . Access pointlərin sayları və xidmət etmə dərəcəsi

Beləliklə, Wireless texnologiyalarının istifadəsi zamanı informasiya təhlükəsizliyi məsələsi əhəmiyyətli bir məsələdir və bu sahədə tədqiqatlar aparılır. Korporativ şəbəkələrdə istifadə olunan wireless texnologiyalarının arxitekturası və tətbiqi prinsipləri məqalədə əsas bir məzmun olaraq yer alır. Bu, korporativ şirkətlərin şəbəkə

infrastrukturunda istifadə etdikləri wireless sistemlərin təhlükəsiz və effektiv bir şəkildə fəaliyyət göstərməsinə imkan verən bir layihələməni əhatə edir [22].

Azərbaycan Texniki Universitetinin kompüter şəbəkəsində wireless texnologiyasının təhlükəsiz tətbiqi mexanizmləri isə konkret bir tədqiqat obyektidir. Bu fəsildə, universitetin kompüter şəbəkəsində istifadə olunan wireless texnologiyaların təhlükəsizliyini təmin etmək üçün hansı mexanizmlərin quraşdırıldığı, istifadə olunan protokollar və şifrələmə metodları ətraflı şəkildə müzakirə olunur. Bu tədqiqatlar, universitetin informasiya təhlükəsizliyini təmin etmək və potensial təhlükələrə qarşı qorunmaq məqsədi ilə aparılır.

AZƏRBAYCAN RESPUBLİKASI ELM və TƏHSİL NAZİRLİYİ
AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əlyazması hüququnda

VƏLİZADƏ YUSİF RASİM oğlu

AzTU-nun kompüter şəbəkəsində informasiya təhlükəsizliyinin qiymətləndirilməsi sisteminin işlənməsi

mövzusunda

MAGİSTRLİK DİSSERTASİYASI

İxtisas: 060631- " Kompüter mühəndisliyi"
İxtisaslaşma: "Biliklərin əldə edilməsi sistemləri"

Elmi rəhbər: **t.f.d., dosent C. Məmmədov**

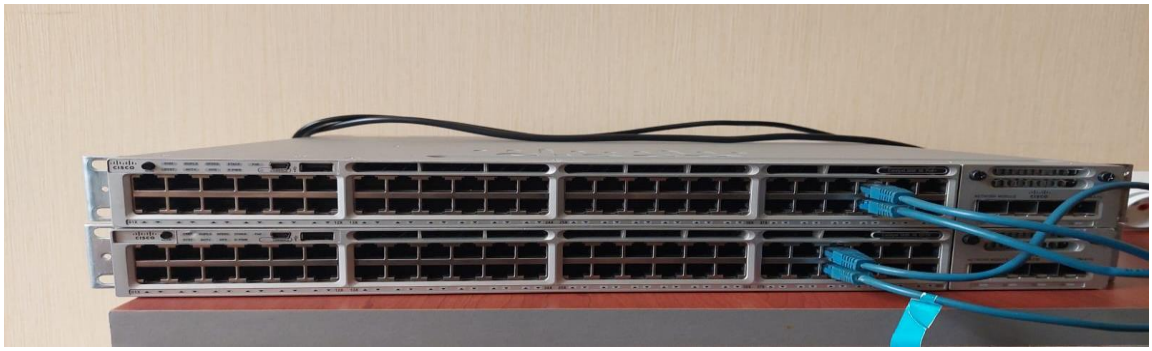
BAKI - 2023

III FƏSİL. AZƏRBAYCAN TEXNİKİ UNİVERSİTETİNİN KOMPÜTER ŞƏBƏKƏSİNDƏ İSTİFADƏ OLUNAN TƏHLÜKƏSİZLİK PROTOKOLLARININ ANALİZİ

3.1. AzTU kompüter şəbəkəsində layer 2 istifadə edilən təhlükəsizlik protokolları analizi və nəticələri

2023-cü il Azərbaycan Texniki universitetinin yeddi korpusunda şəbəkə texnologiyalarından istifadə edilmişdir. Hər biri yeni və köhnə texnologiyalardan ibarət olaraq universitet daxili kommunikasiya əlaqəsini və təhlükəsizliyini təmin edir.

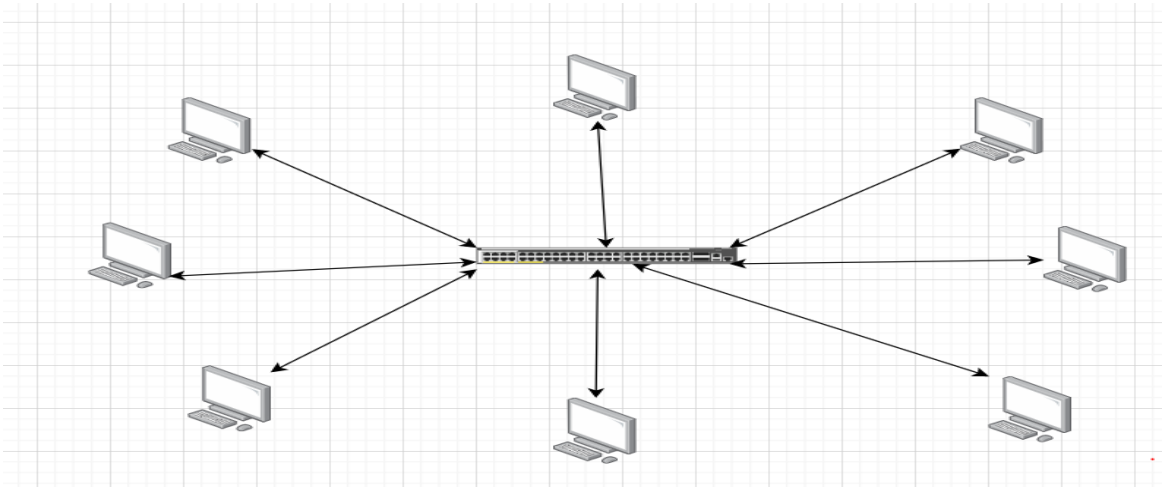
Azərbaycan Texniki universitetinin şəbəkəsində *Cisco, HP, Tp-Link* tipli şəbəkə cihazlarından istifadə edilir. Əsasən, digər korpuslara nəzərən üç, dörd və yeddinci korpuslarda istifadəsi az görülmüşdür. Hər korpusda layer 2 cisco, tp-link və layer 3 Cisco, HP switchlərdən istifadə edilmişdir. Həm layer 2, həm də layer 3 səviyyə də təhlükəsizlik təmin edilmişdir. Bu fəsildə layer iki və üç səviyyədə istifadə edilən protokollara nəzər yetirəciyik.



Şəkil 3. 1. Cisco stack switchlər

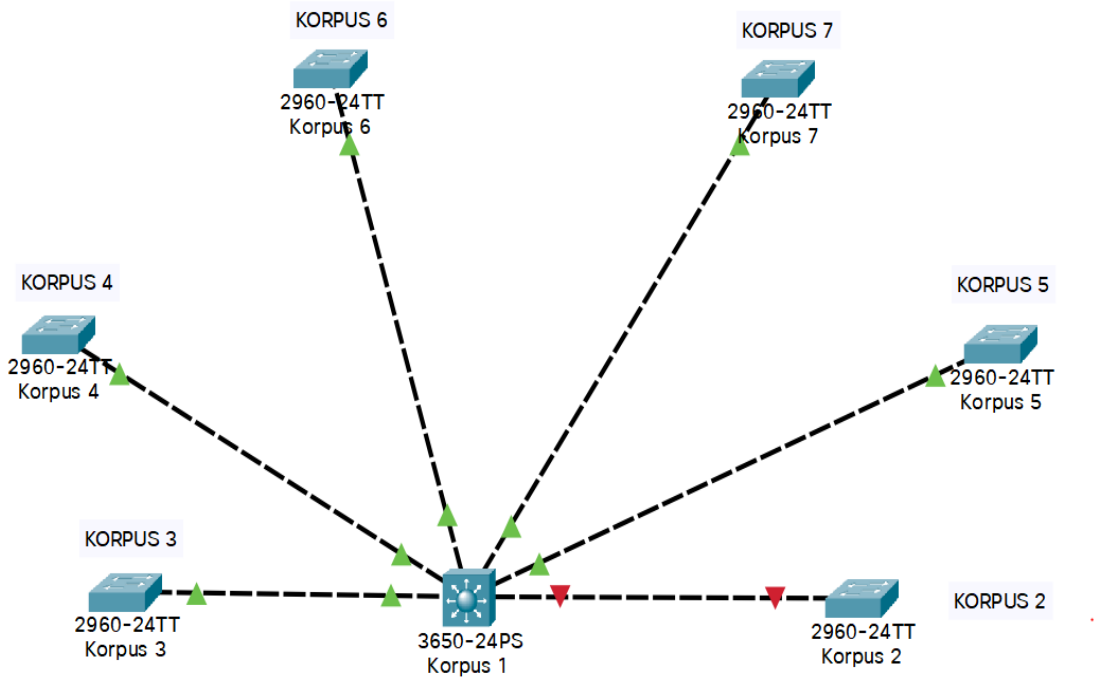
Korpuslar arası optika xəttlərinə üstünlük verilib. Hər bir korpusda yerləşən mərkəzi switchdə digər korpuslar ilə rezerv optika xətti var. Bütün korpuslar mərkəzi yəni, birinci korpusla əlaqəlidir. Universitetdə qurulan topologiya ulduz topologiyasına əsaslanıb. İstifadə edilən topologiya lokal şəbəkələrdə ən çox tətbiq edilən topologiya növlərindən biridir (şəkil 3.2). Ulduz topologiyasının üstün cəhətlərindən biridə odur ki,

şəbəkə daxilində hər hansı bir cihazda problem çıxarsa bu şəbəkənin qalan hissəsinə təsir göstərmiyəcək [3].



Şəkil 3. 2. Ulduz topologiyası

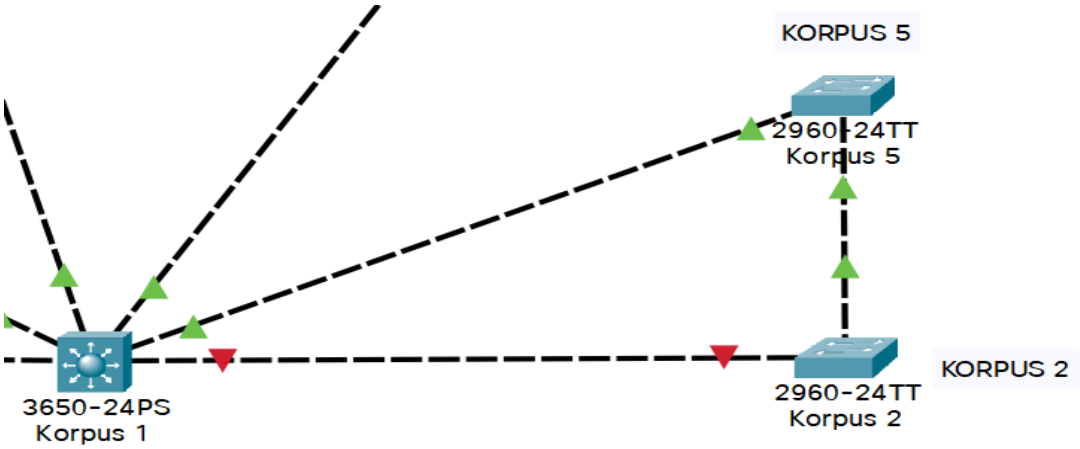
Nümunə kimi hər bir korpusun mərkəzi, yəni birinci korpusla əlaqə də olduğunu bilirik. İkinci korpusda baş verən problem artıq digər korpuslara təsir göstərmir və problem yalnız ikinci korpusun daxilində olan lokal şəbəkə də olur. Bir çox məsələyə görə bu problem ortaya çıxa bilər. Optika xəttinin qırılması, sfp modulda baş verən xətalar, switchin yanması, korpus daxilində enerji probleminin olması və s. kimi məsələlər bu problemi ortaya çıxara bilər. Şəkil 3.3-də göstərildiyi kimi ikinci korpusla bağlantı itsə də, digər korpuslarda şəbəkə aktiv şəkildədir. Belə bir məsələ ortaya çıxır, şəbəkə administratoru bu problemi və yaxud daxildə baş verə biləcək təhlükəsizlik məsələsini tez bir zamanda necə həll edə bilər?



Şəkil 3. 3. Korpuslar arası bağlantı

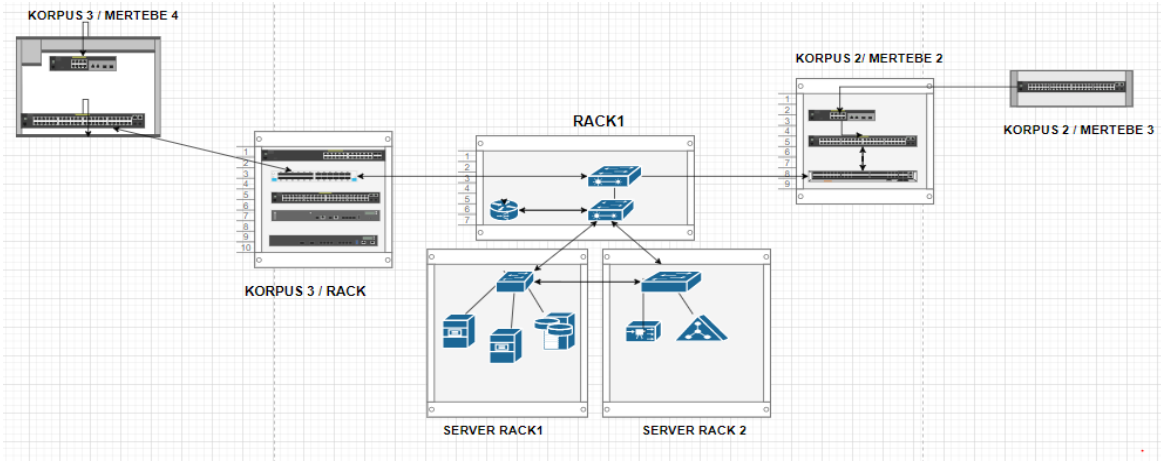
Belə ki, ikinci korpusda əgər optika problemi varsa rezerv optikadan yəni beşinci və ikinci korpuslar arası optika xəttindən istifadə edə bilərik (Şəkil 3.3). Bu proses şəbəkənin davamlı olaraq aktiv qalmasını təmin edir. Növbəti problemlərin həlli prosesi kimi enerji mənbəyi üçün UPS sistemlərdən, switchin əməliyyat sisteminin yanma prosesində stack switchlərdən istifadə edə bilərik. Stack switch anlayışı iki və ya daha çox stack ola biləcək switchlərin bir switch kimi idarə olunmasını təmin edən anlayışdır. Bu zamanda hər iki switchdən aktiv şəkildə istifadə görülür. Stack switchlərin birincisinə korpus 1-2 arası, ikinci switchdə isə korpus 2-5 arası optika xətti ilə təmin edilir və portları konfiqurasiya edilir. Şəkil 3.4-də göstərildiyi kimi bağlantının biri ilə problem yaşarkən, digəri aktiv şəkildə bağlantını saxlayır.

Bu prosesin həllini hər bir korpusda tətbiq edərək, şəbəkədə aktivlik prosesi təmin edilir. Lokal şəbəkə daxili əlçatanlıq və tamlıq 100 % təmin edilə bilir.



Şəkil 3. 4. Rezerv bağlantı və stack switch anlayışı

Korpuslar arası istifadə edilən optika single-modedir. İnternet xidməti provayderi *Delta Telecom LTD*-dir. Bu provayderə xidmət üçün müəyyən qədər məbləğ ödənilir və internetlə əlaqə, bəzi təhlükəsizlik prosesləri qorunub saxlanılır. Şəbəkə də ilkin təhlükəsizlik və bağlantıların təmin edilməsi məsələlərini ifadə etdiyimiz fikirlərlə izahı verildi. Növbəti təhlükəsizlik prosedurlarından şəbəkə avadanlıqlarının gözlə görünə biləcək açıqlıqda olmamasının təşkil edilməsidir. Nümunə kimi hər bir şəbəkə cihazının (switch, router, firewall..) rack adlanan şkaflarda yerləşdirilməsidir (şəkil 3.5). Racklərin hər biri açarla bağlanılır və əsasən rabitə otaqlarında saxlanılır.



Şəkil 3. 5. Rack

Şəbəkə cihazlarının ən aktiv istifadə ediləni, əsasən, switchdir. Əvvəlki illərdə hub istifadəsi çox olsada, zamanla şəbəkədə switch hubı əvəz etmişdir. Əsas səbəb kimi

switchin idarə edilə bilən olması və konfiqurasiya edə bildiyimiz üçün təhlükəsizliyi təmin etməyimizdir. Hub şəbəkəyə əlavə edildikdən sonra, hər bir portuna istənilən cihazı rahatlıqla qoşub, şəbəkəyə access əldə edə bilərik. Bu şəbəkə daxilində boşluqlar yaradır və təhlükəsizlik siyasəti pozulur.

Azərbaycan Texniki universitetində zamanla hublar switchlərlə əvəz edilir. Hal-hazırda korpuslarda bəzi mərtəbələrdə hubların istifadəsi görülsədə, il ərzində onların ləğvi prosesi davam edir. Universitet şəbəkəsində qeyd elədiyimiz kimi HP, Cisco, Tp-Link tipli switchlərdən istifadə edilir. Bu vendorların catalyst 2960, c1000, TL SX3008F, TL SG3452XP və s. kimi növlərindən istifadə edilir. Əsasən, cisconun switchlərinə üstünlük verilir.

Layer 2 səviyyədə lokal şəbəkədə bəzi təhlükəsizlik protokolları tətbiq edilə bilər. Layer 2 şəbəkəsinin təhlükəsiz həyata keçirilməsi, idarə edilməsi və saxlanılması üçün ən yaxşı təcrübə edilmiş siyahı təqdim olunur:

- Switchləri təhlükəsiz şəkildə idarə edin. Məsələn, ssh autentifikasiya mexanizmi, access list istifadə edin və imtiyaz səviyyələrini (privilege levels) təyin edin.
- Etibarsız şəbəkələrin snmp kimi idarəetmə interfeyslərindən və protokollarından istifadə edə bilməməsi üçün switchə idarəetmə icazəsini məhdudlaşdırın.
- Bütün trunk portlar üçün həmişə xüsusi VLAN ID-dən təyin edin.
- Yaradıcı olun; hər hansı bir şey üçün VLAN 1-dən istifadə etməyin. Nümunə kimi hər bir cihaz üçün ayrı vlanlar seçin. Telefon üçün vlan 10, kompüter üçün vlan 20, printerlər üçün isə vlan 30 seçə bilərik.
- Bütün trankinq olmayan giriş portlarında DTP-ni söndürün. Paralel olaraq mümkünsə CDP-ni söndürün.
- Portların dəyişdirilməsindən icazəsiz girişin qarşısını almaq üçün port təhlükəsizliyi funksiyasını (port security) istifadə edin.
- Mümkün olduqda MD5 autentifikasiyasından istifadə edin.

- İstifadə edilməmiş xidmətlər və protokolları deaktiv etməklə xidmətdən imtina hücumlarının (denial-of-service attacks) və digər təhlükələrin qarşısını alın.
- Switchdəki bütün istifadə olunmamış portları bağlayın və ya söndürün, onları normal əməliyyatlar üçün istifadə edilməyən VLAN-a qoyun.
- MAC flooding hücumundan müdafiəni təmin etmək üçün port security mexanizmlərindən istifadə edin.
- Mümkün olduqda DHCP Snooping, IP Source Guard və ARP təhlükəsizliyi kimi port səviyyəli təhlükəsizlik protokollarından istifadə edin.
- Spanning Tree Protocol xüsusiyyətlərini aktivləşdirin (məsələn, BPDU Guard, Loopguard və Root Guard) [2].

Tutaq ki , üçüncü korpus dördüncü mərtəbədə yerləşən 24 portlu Catalyst 2960 switchinin ilk 20 portu aktiv şəkildə istifadə edilib. İlkin olaraq mərkəzi switchdən bu switchə trunk port vasitəsi ilə managment və digər aktiv istifadə olunan vlanları ötürülür. Switch konfiqurasiya edilərkən telnet protokol deyil, təhlükəsizlik üçün ssh aktiv edilir. SSH bağlantı qurulduqdan sonra switchə qoşulub, istifadə edilməyən portlar söndürülür və istifadə etdiyimiz portlara isə port security protokolu tətbiq edilir. Bu switchin hər bir portuna sadəcə kompüter qoşulduğu üçün port security əmrində port üçün sadəcə bir mac ünvana icazə verilir. Aşağıdakı şəkildə tətbiqi göstərilmişdir:

```
interface FastEthernet0/3
 description DATA-MERTEBE 3
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/4
 description DATA-MERTEBE 3
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/5

KORPUS-3-MERTEBE-4#
```

Şəkil 3. 6. Port security əmri

Mərtəbə üçdə yerləşən kompüterlər üçün xüsusi portlar verilib və bu portlar yalnız portlara qoşulan ilk kompüterlərin mac ünvanlarını qeyd edəcək.

```
interface FastEthernet0/3
 description DATA-MERTEBE 3
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0006.2AAE.90D1
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/4
 description DATA-MERTEBE 3
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 0001.428D.B572
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/5

KORPUS-3-MERTEBE-4#
```

Şəkil 3. 7. Port security əmrinin tətbiq edilməsi

Əgər universitet şəbəkəsində istifadə edilən kompüteri deaktiv edib, hücum edən şəxs öz kompüterini ethernet kabellə şəbəkəyə qoşmaq istəsə, bu mümkün olmayacaq. Qeyd etdiyimiz kimi port security əmri tətbiq edilərkən yalnız bir mac ünvana icazəsi oldu (şəkil 3.7). Ümumiyyətlə, maximum *132 mac ünvan* bir interfeysin altına əlavə edilə bilər. Bu məsləhət edilən bir üsul deyil, amma switchin interfeysinə hub taxılıbsa, hubın portlarının sayı qədər mac ünvan icazəsi verə bilərik:

```
KORPUS-3-MERTEBE-4(config-if)#interface fa0/6
KORPUS-3-MERTEBE-4(config-if)#description MERTEBE 5-HUB
KORPUS-3-MERTEBE-4(config-if)#switchport port-security maximum 8
```

Cisco switchində üç növ port security rejimini konfiqurasiya edə bilərsiniz. Təhlükəsizlik pozuntusu mac ünvanlarının maksimum sayına çatdıqda və mac ünvanı mac ünvanı cədvəlində olmayan yeni cihaz interfeysə qoşulmağa cəhd etdikdə və ya interfeysdə öyrənilmiş mac ünvanı digər təhlükəsiz interfeysdə göründükdə baş verə bilər. Təhlükəsizlik pozuntusu baş verdikdə istifadə etmək istədiyimiz prosesdən asılı olaraq, switch portunu aşağıdakılardan birinə konfiqurasiya edə bilərsiniz:

- **Protect** – Təyin olunan mac ünvanlardan fərqli mac ünvanla gələn paketləri rədd edir. Şəbəkə administratorun bu barədə məlumatı olmur.
- **Restrict** – Təyin olunan mac ünvandan fərqli mac ünvanla gələn paketləri rədd edir və bu barədə SNMP serverə məlumat göndərir. Bu məlumatı biz switchlərdə show log əmrini qeyd edib, gələn mac ünvana nəzarət edə bilərik.
- **Shutdown** – Təyin olunan mac ünvandan fərqli mac ünvanla gələn paketləri həmin port üzərindən avtomatik olaraq err-disable edir və bu barədə SNMP serverə məlumat göndərir. Qeyd edim ki, bu əksər switchlərdə default seçimdir [8].

```
KORPUS3-MERTEBE3#Show log
May 27 16:12:41: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 7365.deef.a7d3 on port GigabitEthernet0/14.
May 27 16:13:11: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 7365.deef.a7d3 on port GigabitEthernet0/14.
May 27 16:13:41: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 7365.deef.a7d3 on port GigabitEthernet0/14.
```

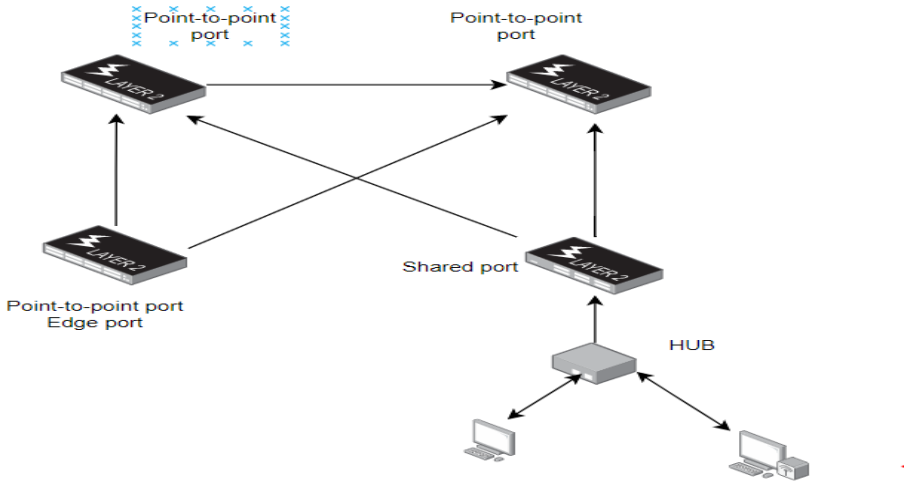
Layer 2 səviyyədə istifadə edilən əsas təhlükəsizlik prosedurlarından biridir. Lokal şəbəkədə switchlərdə istifadə edilməyən portlarda, interfeys altına shutdown əmri tətbiq edilərək daha bir təhlükəsizlik proseduru yerinə yetirilir.

Digər layer 2 səviyyədə istifadə edilən *Spanning Tree Protocol , Dynamic Host Configuration Protocol (DHCP) Snooping, IP Source Guard, Dynamic ARP Inspection (DAI)* kimi protokollar şəbəkədə tətbiq edilir.

PortFast switchə şəbəkəyə əlavə edilən qurğunu dərhal bloklamadan yönləndirməyə, dinləmə və öyrənmə vəziyyətlərindən kənar keçməyə imkan verir. Bununla belə, PortFast-ı etibarlı şəkildə aktiv edə biləcəyiniz yeganə portlar heç bir switchin və ya digər STP aktiv olan cihazların qoşulmadığını bildiyiniz portlardır. Əks halda, PortFast-dan istifadə, dinləmə və öyrənmə vəziyyətlərinin qarşısını almaq üçün

nəzərdə tutulan döngələr yaratmaq riski daşıyır. PortFast istifadəçi cihazlarına qoşulmaq üçün ən uyğun protokoldur. İstifadəçi cihazlarına qoşulmuş portlarda PortFast-ı aktiv etsəniz, istifadəçi kompüteri işə salındıqda switch portu STP yönləndirmə vəziyyətinə keçə və trafiki yönləndirə bilər. PortFast olmadan, keçid portun DP olduğunu təsdiq edənə qədər hər bir port gözləməlidir. Xüsusilə STP ilə (və RSTP deyil), switch trafiki ötürülmə vəziyyətinə keçməzdən əvvəl müvəqqəti dinləmə və öyrənmə vəziyyətlərində gözləyir. PortFast-ın yaxınlaşmanı sürətləndirdiyindən təxmin edə bildiyiniz kimi, RSTP-yə PortFast daxildir.

Şəkil 3.8 ətrafında RSTP port növlərinin, xüsusən də nöqtədən-nöqtə kənar port növlərinin qeyd edildiyini xatırlaya bilərsiniz.



Şəkil 3. 8. STP portfast və BPDU Guard

STP və RSTP LAN-ı bir neçə müxtəlif növ mümkün təhlükəsizlik risklərinə açır. Nümunə üçün:

■ Hücum edən şəxs switchi aşağı STP/RSTP prioritet dəyəri olan bu portlardan birinə qoşa və əsas (root) switch ola bilər.

■ Təcavüzkar bir neçə porta, birdən çox switchə qoşula, root switchə çevrilə və LAN-da trafikin böyük hissəsini yönləndirə bilər. Şəbəkə adminləri bunu anlamadan təcavüzkar LAN vasitəsilə göndərilən çoxlu sayda məlumat freymlərini göndərmək üçün LAN analizatorundan istifadə edə bilər.

■ İstifadəçilər ucuz istehlakçı LAN switchini (STP/RSTP istifadə etməyən) alıb qoşduqları zaman LAN-a istəmədən zərər verə bilərlər.

STP/RSTP funksiyası olmayan switch heç bir portu bloklamağı seçməyəcək və bu prosedur şəbəkədə dövrəyə səbəb ola bilər. BPDU Guard əmri portda hər hansı BPDU qəbul edildiyi təqdirdə portu söndürməklə bu cür problemlərin aradan qalxmasına kömək edir. Beləliklə, bu funksiya yalnız access portu kimi istifadə edilməli və heç vaxt başqa switchə qoşulmamalı olan portlarda xüsusilə faydalıdır (şəkil 3.6).

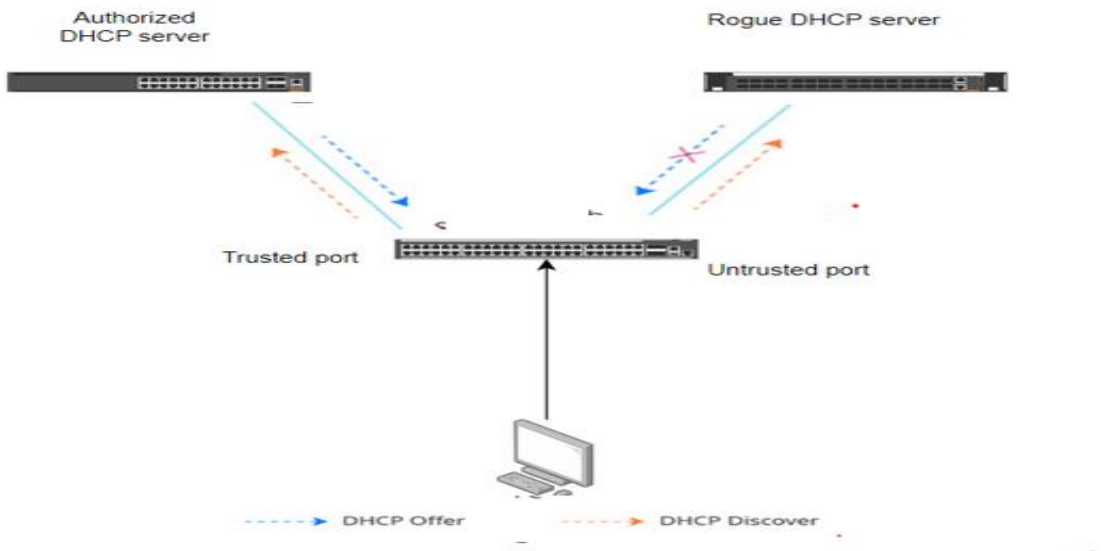
DHCP Spoofing hücum başlığı altında universitet şəbəkəsində görülən 2 hücum növü göstərilə bilər:

- **DHCP Starvation**: Hücum edən şəxs spoof edilmiş mənbə mac ünvanlar ilə DHCP serverə çoxlu DHCP request paketi göndərip DHCP serverin paylayacağı ip subneti qısa zamanda doldurur. Bu prosedur isə şəbəkəyə qoşulmaq istəyən digər istifadəçilərin ip ünvan əldə etməməsinə yol açır.
- **DHCP Spoofing**: Hücum edən şəxs özünü DHCP server kimi göstərərək istifadəçilərin onun qurduğu serverdən ip ünvanı almasını təmin edər.

DHCP snoopingin şəbəkədə istifadə məqsədi istifadəçinin təhlükəsizliyini və gizliliyini təhdid edə biləcək prosedura mane olmaq üçün Cisco cihazlar üzərində tətbiq edilən bir protokoldur. Texniki universitetin daxilində 1200-dən çox kompüter istifadəyə verilib. Hər bir kompüterə tək-tək statik olaraq ip ünvan verilə bilər, lakin bu həll yolu çox uzun və yorucudur. Şəbəkə administratoru rahat üsul kimi DHCP protokolundan istifadə edir. DHCP (Dinamik Host Konfiqurasiya Protokolu) avtomatik olaraq IP (İnternet Protokolu) ünvanını, subnet maskasını və DNS (Domain Name System) ünvan məlumatlarını istifadəçi cihazlarına paylayan protokoldur. Bu protokol vasitəsi ilə şəbəkədəki bütün kompüterlərə bir-bir məlumat daxil etməyə ehtiyac qalmır və ip konfliktləri kimi hallar aradan qaldırılır. İstifadəçilər DHCP serverdən lazımi məlumatları almaq üçün sorğular göndərir və DHCP serverdəki məlumatlardan istifadə edərək internetə daxil olmağa çalışırlar.

Şəbəkədə icazə olmadan DHCP serverini quran və istifadə edən şəxs eyni şəbəkədə DHCP sorğuları edən istifadəçi cihazlarına standart gateway ünvanları ilə DHCP cavabını qaytara bilər. İstifadəçi sorğunun cavabını alan kimi bu saxta ünvandan gateway ünvanı kimi istifadə etməyə başlayır və lokal şəbəkədən kənar ünvana yönəlmiş paketlər əvvəlcə hücum edən şəxsin cihazına yönəldilir. Hücum edən şəxs bu paketləri getmələri lazım olan doğru ünvanlara göndərərkən, bütün paketləri də izləmək imkanını əldə edir. Hücum edən şəxs saxta DHCP serveri şəbəkəyə əlavə etdikdən sonra, istifadəçinin daxil olmaq istədiyi internet ünvanlarının əvəzinə öz istədiyi internet ünvanlarına yönləndirmək imkanını əldə edir. Azərbaycan Texniki Universitetində şəbəkə təhlükəsizliyini təhdid edən bu prosesin qarşısını almaq üçün DHCP snooping funksiyası istifadə edilir.

DHCP snooping yalnız bilinən portlar üzərindən DHCP broadcasta (yayım) icazə verirki, bu portlar DHCP serverin switch ilə fiziki şəkildə qoşulduğu portlardır. Bu halda isə digər portlar bloklanır. Snooping istifadə ediliyi portları təhlükəsiz, digər portları isə təhlükəli kimi müəyyən edir. Güvənilir portlardan DHCP sorğulara cavab verilir və informasiyanın şəbəkə cihazları üzərindən göndərilməsinə icazə verilir. Bloklanan portlardan göndərilən DHCP sorğular cavabsız qalır [2].

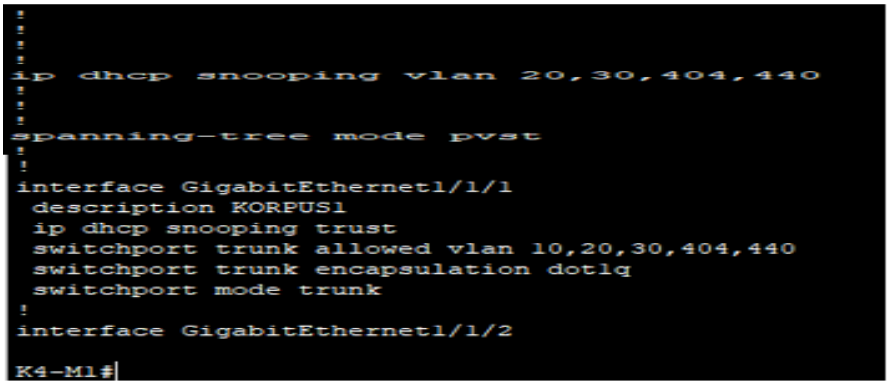


Şəkil 3. 9. DHCP Snooping

Switchlər üzərində DHCP snooping xüsusiyyəti başlanğıc konfiqurasiyada aktiv deyil. Swtch konfiqurasiyasında bu xüsusiyyətin aktiv vəziyyətə gətirilməsi lazımdır. Bu əməliyyat *ip dhcp snooping* əmri vasitəsi ilə yerinə yetirilir. Bu əmrdən sonra switch üzərində DHCP snooping əmri aktiv olur, ancaq switch hansı vlanlara və portlara güvənəcəyini bilməz.

Bunun üçün switchdə əlavə dhcp snooping əmrləri qeyd edilir. *İp dhcp snooping vlan* əmri ilə ip snoopingin hansı VLAN (virtual local area network - virtual local network connection) da prosesləri yerinə yetirəcəyi göstərilir. Sonra port seçilir və interfeys moduna keçilir. Bu əməliyyat üçün də *#ip dhcp snooping trust* əmri istifadə edilir.

Şəkil 3.9-da göstərildiyi kimi, Texniki universitetin şəbəkəsinə hücum edən şəxsin serveri sağdakı, universitetin həqiqi serveri isə soldakıdır. Universitetin serveri birinci port, hücum edən şəxsin serveri 27-ci port və birinci korpusda istifadə elədiyimiz kompüter isə səkkizini porta qoşulmuşdur. Əgər biz switchdə təhlükəsizlik protokollarında boşluq versək, kompüterimiz qoşulan serverdən ip alacaq və bu prosesdə göndərilən paketləri görmək imkanı olacaq. Şəbəkə administratoru olaraq, aşağıdakı şəkildə göstərildiyi kimi tətbiq etdikdən sonra təhlükəsizlik problemi aradan qalxacaq və kompüter ip ünvan məlumatlarını universitetin serverindən alaraq, şəbəkəyə aktiv və təhlükəsiz şəkildə qoşula biləcək.



Şəkil 3. 10. İP DHCP Snooping

(config)# ip dhcp snooping : Dhcp müdaxilənin qarşısını almaq üçün aktiv edilir. (config)# ip dhcp snooping vlan: DHCP müdaxilənin qarşısını almaq üçün hər hansı bir VLAN üzərində aktiv etmək üçün istifadə edilə bilir.
(config-if)# ip dhcp snooping trust : İstifadə edilən portda Dhcp müdaxilənin qarşısını almaq üçün aktiv edilir (şəkil 3.10).

Layer 2 üzrə universitetin şəbəkəsində Dynamic ARP Inspectionda tətbiq edilir. Layer 2 protokolu olan arp istifadəçilərin bir broadcast domain daxilində müraciət etmək istədiyi ip ünvanların hansı mac ünvanlarına bağlı olduğunu təyin edir. Nümunə kimi otaq 304-dəki kompüterlər bir-birinə məlumat göndərərkən mac ünvanlar tələb edilir. Bu proses arp üçün normal iş prinsipidir. Amma arp protokoluna məxsus olan *Gratuitous arp* təhlükəsizlik üçün müəyyən problemlər yarada bilər. Gratuitous arp şəbəkədəki istifadəçilərin arp məlumatlarını yeniləmək imkanına malikdir. Bu prosesdə hücum edən şəxsin ip və mac ünvanlarını əlaqələndirməklə özlərini gizlədiyi bu hücum növü, informasiyanın istifadəçilərin məlumatı olmadan izləmək və ya dəyişdirmək imkanı olur. Hücum edən şəxs yalnız spoofing hücumları ilə deyil, məlumatların oğurlanması və şəbəkənin çökməsinə səbəb olacaq mənfi prosedurlarada səbəb olur. Şəbəkə də olan bu boşluqlar *man in the middle attack, DDoS* kimi hücumlarla nəticələnə bilər.

Arp access-listin istifadəsi ilə standart olaraq, bu hücumların qarşısını almaq olar. Konfiqurasiya edərkən ip və mac ünvanlar bir-biriləri ilə bərabər qeyd edilir və mac ünvanlı kompüter əgər ip ünvanla qeyd edilibsə, şəbəkəyə qoşularkən yalnız həmin ip ünvanı alır.

```
KORPUS1/MERTEBE-3(config)# ip arp inspection
KORPUS1/MERTEBE-3 (config)# ip arp inspection validate
KORPUS1/MERTEBE-3 (config)# ip arp inspection vlan 404 (vlan 404-istifadəçi vlanı)
```

Trust Uplink Port:

```
KORPUS1/MERTEBE-3 (config)# interface range gigabitethernet 1/0/47-48
KORPUS1/MERTEBE-3 (config-if-range)# ip arp inspection trust
```

İP ünvana sahib cihazlar üçün arp list:

```
KORPUS1/MERTEBE-3 (config)# ip arp inspection list create USER-COMP
KORPUS1/MERTEBE-3 (config-arp-list)# ip 10.21.1.18 mac 0078.B7EA.AFE7
KORPUS1/MERTEBE-3 (config-arp-list)# ip 10.21.1.15 mac 7456.d0af.0fx6
KORPUS1/MERTEBE-3 (config-arp-list)# ip 10.21.1.13 mac 0033.B75A.C0A5
KORPUS1/MERTEBE-3 (config)# ip arp inspection list assign VLAN 404
```

Bu əmrləri yerinə yetirdikdən sonra İP Source Guard əmrini tətbiq edə bilərik. İp Source Guard DHCP Snooping verilənlər bazasından istifadə edərək, istifadəçilərin yalnız DHCP server tərəfindən təyin olunmuş ip ünvanlardan istifadə etməsini təmin edir və cihaz statik ip alıbsa, bu məlumatı əlavə olaraq konfiqurasiya əlavə edə bilərik. İp Source Guard funksiyasından istifadə etmək üçün switchdə DHCP Snooping aktiv şəkildə olmalıdır. Bu funksiya aktiv olanda DHCP snooping tərəfindən icazə veriləndən əlavə interfeyslərdəki ip trafiki bloklayır. İp Source Binding cədvəli statik verilən və dhcp server tərəfindən təyin olunan ip binding məlumatlarından ibarətdir. Bu cədvəldə ip ünvanlar, həmin ip ünvanlara uyğun mac ünvanlar və bu ünvanlar üçün vlan məlumatları daxildir [8].

Source Guard layer 2 səviyyəsində həm access, həm də trunk portlarda istifadə edilir. İnterfeysdə *ip verify source* əmri ip filtr funksiyasını aktivləşdirir. IP Source Guard yalnız layer 2 səviyyə olan portlarda (giriş və ya magistral) istifadə edilə bilər.

İnterfeys daxil edilərək yazılan ip source guard əmri ip ünvan filtrini aktivləşdirir. Trafik portdakı ip binding cədvələ və dhcp snooping bazasına baxaraq, sadəcə göstərilən mənbə ip ünvana icazə verəcək şəkildə data trafikini filtr edir. Bu proses istifadə edilən porta access list tətbiq etməklə yerinə yetirilir. Verilənlər bazasında edilmiş hər hansı bir dəyişiklikdə, portdakı access listin avtomatik olaraq dəyişilməsinə səbəb olur. Əgər ləğv olunarsa, access listdə ləğv olunacaq.

Bütün korpuslarda istifadə edilən access switchlərin istifadəçi portlarına ip verify source port-security əmri daxil edilərsə, ip və mac ünvanlar üçün filtrasiya aktiv olur. İp source binding cədvəlində olan ip və mac ünvanları uyğun olduqda port məlumatın

göndərilməsinə icazə verir. Bu funksiyalar aktivləşəndə trafik yoxlanılır və uyğunsuzluq aşkar edildiyi zaman isə bloklanır. Switclərdəki ip source guard konfiqurasiyasını tətbiq etdiyimiz zaman bəzi məqamlara diqqət etməliyik:

– Dhcp snooping, ip filtrasiyasının aktivləşdirilməsinin istəndiyi portlardakı access vlanda mütləq dhcp snoopingi aktiv etməliyik. Əgər ki, birdən çox vlan ötürülən trunk portlarda source guard tətbiq etmək istəyiriksə, dhcp snooping bütün vlanlarda aktiv olmalıdır. Universitetin şəbəkəsindəki access switchlərdə əmr istifadəçi portlarına tətbiq edilmişdir.

– İp və mac filtrləmə prosesi aktiv olacaqsa, portlarda dhcp snooping və port-security tətbiq edilməlidir. İp source guard əmrini etherchannel istifadə olunan portlarda bu əmri dəstəkləmədiyi üçün tətbiq edə bilmərik.

– İp source guard əmri *802.1x port əsaslı autentifikasiya* funksiyasının istifadə edildiyi portlarda istifadə edilə bilər [3].

Nümunə kimi ikinci korpusda istifadə edilən mərtəbə üç switchində bu konfiqurasiyanı görə bilərik:

```
KORPUS-2/MERTEBE-3#conf t
KORPUS-2/MERTEBE-3 (config)#interface range fa0/1-18
KORPUS-2/MERTEBE-3 (config-if)# ip verify source port-security
KORPUS-2/MERTEBE-3 (config-if)# exit
KORPUS-2/MERTEBE-3 (config)# ip source binding 0010.2131.4262 vlan 404
10.21.2.20 interface fa0/20
KORPUS-2/MERTEBE-3 (config)# ip source binding 3333.6543.AB4O vlan 404
10.21.2.19 interface fa0/19
KORPUS-2/MERTEBE-3 (config)# do write.
```

İp source binding əmri cihaza statik ip ünvan tətbiq olunarkən ip ünvan, vlan və interfeys qeyd edilir. Aşağıdakı şəkildə vlan 21-də olan porta arp attack olduğunu görürük. Gələn paketlər 19 dəfə blok edilmişdir, lakin bu dəfə arp acl-ə ehtiyac olmamışdır.

```
Jul 2 14:28:20.763: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Gi1/0/4,
vlan 21.([0200.2222.2222/172.16.2.108/0000.0000.0000/172.16.2.1/09:28:20 EST Thu Jul 2
2023])

KORPUS-3-MERTEBE-3# show ip arp inspection statistics

Vlan       Forwarded      Dropped      DHCP Drops    ACL Drops

----       ---------      -------      ----------    ---------

21         59              19          19             0
```

Şəkil 3. 11. Arp hücumdan sonra olan nəticə

Azərbaycan Texniki Universitetində access switchlərində arp sorğuların limitini müəyyən etmək üçün bu əmrlərdən istifadə edilib:

```
K-1-M1(config)#errdisable recovery cause dhcp-rate-limit
K-1-M1(config)#errdisable recovery cause arp-inspection
K-1-M1(config)#errdisable recovery interval 30
!
K-1-M1(config)#interface GigabitEthernet1/0/2
K-1-M1(config)#ip dhcp snooping limit rate 10
K-1-M1(config)#ip arp inspection limit rate 8
     !
K-1-M1(config)#interface GigabitEthernet1/0/3
K-1-M1(config)#ip dhcp snooping limit rate 2
K-1-M1(config)#ip arp inspection limit rate 8 burst interval 4
```

Şəkil 3.12-də konfiqurasiya parametrlərini təsdiq edən çıxışı sadalayır. Məsələn, qeyd edilən konfiqurasiyaya əsasən Gi1/0/2 portunu 1 saniyəlik hər standart partlayış (*eng. default burst*) üçün 8 mesaj dərəcəsi ilə konfiqurasiya yerinə yetirilir. Gi1/0/3 portunda 4 saniyə üçün 8 dərəcə ilə dəyəri təsdiqləyir. Nümunədəki digər iki interfeys bir saniyə ərzində 16 mesaj sürətinin standart parametrlərini göstərir [8].

```
K-1-M1# show ip arp inspection interfaces

Interface        Trust State     Rate (pps)     Burst Interval

---------------  -----------     ----------     --------------

Gi1/0/1          Untrusted       15                  1

Gi1/0/2          Trusted         8                   1

Gi1/0/3          Untrusted       8                   4
```

Şəkil 3. 12. ARP İnspection dərəcəsi limitlərinin təsdiqlənməsi.

3.2. AzTU kompüter şəbəkəsində layer 3 istifadə edilən təhlükəsizlik protokolları analizi və nəticələri

Şəbəkədə layer 3 səviyyəsində təhlükəsizliyin təmin edilməsi məsələləri - Texniki universitetin şəbəkəsində layer 3 səviyyəsində Ospf və statik routing protokollarından istifadə edilir. Əsasən, Ospf protokoluna üstünlük verilsədə, statik routingin istifadəsini bəzi korpuslarda görə bilərik. Korpuslar arası istifadə edilən layer 3 protokollar və texnologiyalar şəbəkədən şəbəkəyə kommunikasiya əlaqəsi qurmağa imkan verir.

Universitetin şəbəkəsində layer 2 cihazlar, protokollar və onların şəbəkənin təhlükəsizliyini təmin etmə prosedurunu, əvvəlki mövzularda tətbiqi prosesi göstərilib. Ospf protokolu hər bir korpusda tətbiq edilib. Nümunə olaraq korpuslarda istifadə edilən subnet aralığı ilkin olaraq təyin edilir. Switchlərin idarə edilməsi üçün, kompüterlərə, kameralara, access pointlər və server kimi cihazlara subnetlər ayırıb, ip ünvanlar təyin edilir. Ospf protokolu mərkəzi layer 3 switchlərdə təyin edildikdən sonra, digər arealarda olan cihazlar bir-birləri ilə qarşılıqlı şəkildə əlaqə qurur.

İlkin olaraq şəbəkədə ospf protokolu tətbiq edilərkən bir çox təhlükəsizlik qaydalarından istifadə edilir. Mərkəzi switchlərdə və routerlərda identifikasiyası, access

control, şifrələmə, trafikin monitorinqi, yenilənmə, areaların (sahə) ayrılması kimi mexanizmlər tətbiq edilir. Bu mexanizmlərin hər biri şəbəkədə ospf protokolunda istifadə olunur. Universitetdəki korpusların hər birini areaya bölmək əvəzinə area birdə korpus bir, iki və üç təyin edilir. Area iki daxilində dörd-yeddi arası korpusların qurğuları təyin edilir. Ospf böyük şəbəkələri arealara (sahələrə) bölür. Hər bir area şəbəkənin fərqli bir hissəsini təmsil edir. Bu sahələr bir-biri ilə əlaqələndirilə bilər və backbone sahəsi ilə birləşdirilir. Bu struktur şəbəkənin hər bir hissəsini daha kiçik və idarə oluna bilən bölmələrə bölərək, şəbəkə trafikini və marşrutlaşdırma cədvəllərini azaldır. Bundan əlavə, ospf şəbəkəsində fərqli yol variantları təyin etdikdə ən qısa yolu tapmaq üçün qabaqcıl marşrutlaşdırma alqoritmlərindən istifadə edilir. Öz növbəsində bu proses, şəbəkədə trafik axınını optimallaşdırır və şəbəkə bant genişliyindən daha yaxşı istifadə etməyə kömək edir. Nəticədə, ospfdən istifadə böyük şəbəkələrin idarə edilməsini asanlaşdırır, trafik axınını optimallaşdırır və marşrutlaşdırma səmərəliliyini artırır.

```
interface GigabitEthernet0/0.404
 description USER-COMP
 encapsulation dot1Q 404
 ip address 10.21.1.254 255.255.255.0
 ip helper-address 10.100.100.1
 ip helper-address 10.100.100.11
 ip ospf 1 area 0.0.0.1
 ip access-group USER-ACL in
!
interface GigabitEthernet0/0.440
 description USER-INTERNET
 encapsulation dot1Q 440
 ip address 10.101.1.254 255.255.255.0
 ip helper-address 10.100.100.1
 ip helper-address 10.100.100.11
 ip ospf 1 area 0.0.0.1
 ip access-group USER-INTERNET in
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 router-id 1.1.1.1
 no log-adjacency-changes
 area 0.0.0.1 nssa
 passive-interface GigabitEthernet0/0.404
 passive-interface GigabitEthernet0/0.440
!
ip classless

KORPUS-1--MERTEBE-1#
```

Şəkil 3. 13. Area 1 daxilində konfiqurasiya

Şəkil 3.13-də ospf protokolunun tətbiqi prosedurunun universitet şəbəkəsində dizaynı göstərilmişdir. Qeyd etdiyimiz kimi, area öz daxilində bir-birinə bağlıdır və digər arealarla yalnız müəyyən etdiyimiz routerlərlə əlaqa qurur. Bu şəbəkədə trafik axının məhdudlaşdırır və hücum edən şəxslərin bütün şəbəkəni ələ keçirməsinə və ya trafikə nəzarət etməyə icazə vermir. Ospf "area" strukturu bu səbəblərə görə şəbəkənin təhlükəsizliyini təmin etməyə kömək edir və şəbəkədə route (marşrut) məlumatlarının dəqiqliyini, məxfiliyini və təhlükəsizliyini artırır.

Ospf hər ospf mesajının autentifikasiyası üçün konfiqurasiya edilə bilər. Ospf autentifikasiyası mesajların istifadəçiyə qədər dəyişdirilmədiyini və etibarlı mənbədən

gəldiyini yoxlamaq üçün istifadə olunur. Bu proses saxta ospf mesajlarının şəbəkəyə daxil edilməsinin və ya mövcud olan olan ospf mesajlarının dəyişdirilməsinin qarşısını alır [8].

Ospf identifikasiyası üçün istifadə ediləcək iki əsas üsul var:

1. *Clear text authentication*
2. *MD5 authentication*

Clear text authentication üsulu ospf mesajlarının həqiqiliyini yoxlamaq üçün sadə paroldan istifadə edir və parol ospf mesajlarının saxta olub-olmadığını təyin edir. Bu üsulun istifadəsinə üstünlük verilmir , çünki asanlıqla sındırıla bilən parol istifadə etdiyi üçün təhlükəsizlik baxımından güclü deyil.

Kriptoqrafik autentifikasiya texniki universitetin şəbəkəsində istifadə edilən autentifikasiya növüdür. Bu üsul ospf mesajlarını yoxlamaq üçün daha güclü bir mexanizm kimi istifadə edilir. Mexanizmdə ospf mesajlarının *SHA-1* və ya *MD5* alqoritmləri ilə şifrələndiyi bir parol istifadə olunur. Təhlükəsizlik baxımından adminlər tərəfindən istifadə edilir. MD5 autentifikasiyası olan ospfdə hər bir router, hər bir OSPF paketi üçün *message digest (mesaj həzmini)* yaratmaq üçün istifadə edilən gizli açara malikdir. Message digest ospf paketlərinə daxildir və qəbul edən router tərəfindən paketin doğru olub-olmadığını yoxlamaq üçün istifadə olunur. Açar hər bir routerin ospf konfiqurasiyasına daxil edilir və ospf sahəsində iştirak edə bilən bütün routerlər arasında paylaşılır, router ospf paketlərini göndərdikdə, paketlər məzmununa və paylaşılan məxfi açara MD5 alqoritmini tətbiq etməklə message digest yaradır. Növbəti addımda message digest ospf paketlərinə daxil edilir. Növbəti əməliyyatda message digest prosesi uyğun gələrsə, paketlər etibarlı kimi qəbul edilir və prosedur işlənilir. Əgər uyğun gəlmirsə, paketlər bloklanır.

MD5 autentifikasiyası clear text autentifikasiyası ilə müqayisədə daha yüksək təhlükəsizlik səviyyəsini təmin edir, çünki gizli açar plain text (düz mətn) formatında ötürülmür. Hücum edən şəxsin autentifikasiya məlumatlarını ələ keçirməsini və oxumasını çətinləşdirir. Bununla belə, MD5-in bəzi zəif tərəfləri olduğu aşkar edilmişdir

və SHA-1 kimi daha yeni autentifikasiya üsulları indi OSPF şəbəkələrində istifadə üçün tövsiyə olunur.

Başqa bir təhlükəsizlik protkolu kimi access control listlərdən istifadə edilir. Şəkil 3.13-də göstərildiyi kimi interfeyslərin altına access listlər tətbiq edilmişdir. Azərbaycan Texniki Universiteti şəbəkəsində həm standart, həm də extended access-listlər tətbiq edilmişdir. Məsələn, şəbəkə daxilində 2 istifadəçi vlanı tətbiq edilmişdir: VLAN 404 və 440. Vlan 404-ün istifadə məqsədi yalnız lokal şəbəkədə istifadəsidir. Vlan 440 isə həm lokal, həmdə internetə çıxışı olan vlandır. Vlan 404 tətbiq edilən access list ümümi formada şəbəkədə olan bütün subnetlərə tətbiq edilir. Lakin internetə çıxışı olan kompüterlərdə bəzi məhdudiyyətlər olur. Bunlardan bəziləri qadağa qoyula portlar və ya həmin kompüterləri görə biləcək lokal subnet aralığıdır [7].

Access listlər tək interfeys altına yox, həmçinin başqa məqsədlər üçündə istifadə edilir. Kənardan şəbəkə cihazlarına qoşulmaq üçün istifadə etdiyimiz bəzi prosedurlar var. Bunlardan ssh, telnet qoşulma kimi protkolları göstərə bilərik. Router və switchlərin *line vty 0 4 və ya line vty 5 15* interfeyslərinin altında ssh, telnet protokollarını aktiv edərək qoşula bilərik. Məqsəd şəbəkə cihazlarına qoşulmaqdır, lakin qoşulma prosesindən əlavə olaraq, bu prosesin təhlükəsizliyini təmin etməkdir.

Bunun üçündə line vty interfeyslərinin altına access list tətbiq edilir. Şəbəkə administratorlarının istifadə elədiyi management subnet üçün access list yazılır və bu access list əmrlər şəklində line vty interfeysinin altında tətbiq edilir. Bu prosedurları tamamladıqdan sonra yalnız, adminlər üçün ayrılan subnet aralığından switch və routerlərə daxil olmaq olur.

```
ip access-list standard MANAGEMENT--ACL
 permit 10.1.1.0 0.0.0.255
 permit host 10.1.2.11
 permit host 10.1.2.12
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 access-class MANAGEMENT-ACL in
 password 7 082048430017544447
 login local
 transport input ssh
line vty 5 15
 access-class MANAGEMENT-ACL in
 login local
 transport input ssh
!
!

KORPUS-6/MERTEBE-2#
```

Şəkil 3. 14. Acces listin line vty interfeysinin altına tətbiq edilməsi

Şəkil 3.14-də görünən nəticəyə əsasən adminlərin istifadə elədiyi 10.1.1.0 subneti yalnız cihazlara girişi olacaq. Digər şəbəkədə olan istifadəçi kompüterləri şəbəkəyə cihazlarına qoşulma icazəsi olmayacaq. Əlavə olaraq, şəkil 3.14-də *line console* interfeysi altında heç bir əmr daxil edilmiyib. Bu vəziyyətlə əlaqədar bəzi əmrləri daxil edərək, təhlükəsizliyi qorumaq olar. Line console interfeysinin altına password daxil edərək təhlükəsizliyi bir qədərdə artırmaq olar (şəkil 3.15).

```
line con 0
 password 7 082048430017
!
line aux 0
!
line vty 0 4
 access-class MANAGEMENT-ACL in
 password 7 082048430017544447
 login local
 transport input ssh
line vty 5 15

KORPUS-6/MERTEBE-2#
```

Şəkil 3. 15. Konsol qoşulmada parolun istənilməsi

Ümumiyyətlə əvvəlki mövzularda qeyd elədiyimiz kimi, şəbəkə cihazlarının təhlükəsizliyi həm fiziki, həm də proqram tərəfdən çox önəmlidir. Ona görə də cihazlarda username və password təyin edilir. Həmçinin enable passwordda aktivləşdirilir. Daxil olarkən ilk öncə cihazın ip ünvanı, username və password daxil edilir, daha sonra console password və enable əmrini aktivləşdirdikdə enable password yazılır. Bununlada üç mərhələdən ibarət olan prosedur tamamlanır. Aşağıdakı əmr ardıcıllığını nümunə kimi göstərə bilərik:

```
KORPUS-6/MERTEBE-2(config)#enable pass
KORPUS-6/MERTEBE-2(config)#enable password ADMIN135
KORPUS-6/MERTEBE-2(config)#username ADMIN password ADMIN1357
KORPUS-6/MERTEBE-2(config)#ip domain-name aztu.edu.az
KORPUS-6/MERTEBE-2(config)#crypto key generate rsa
KORPUS-6/MERTEBE-2#exit
KORPUS-6/MERTEBE-2>ena
Password:
KORPUS-6/MERTEBE-2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
KORPUS-6/MERTEBE-2(config)#
KORPUS-6/MERTEBE-2#sh run
Building configuration...

Current configuration : 1135 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname KORPUS-6/MERTEBE-2
!
enable password 7 080068632037544447
```

```
!
username ADMIN password 7 080068632037544475C
!
KORPUS-6/MERTEBE-2#
```

Bu təhlükəsizlik protokollarından əlavə olaraq, OSI modelinin fərqli səviyyələrində tətbiq edilən *tacacs+ və ya radius* protokollarından istifadə eləmək olar. Bu protokolun istifadəsi şəbəkə də təhlükəsizliyi daha da artırır. Tacacs (Terminal Access Controller Access-Control System) şəbəkə cihazlarına (məsələn, routerlər və switchlər) girişə nəzarət üçün istifadə edilən şəbəkə identifikasiyası protokoludur. Tacacs əsasən Cisco şəbəkə avadanlığı tərəfindən istifadə edilir və şəbəkə admininə istifadəçi girişinə nəzarət etmək, onların hesablamalarına icazə vermək və idarə etmək imkanı verir. Bu protokolun əsas vəzifəsi autentifikasiya və girişə nəzarətdir. Bu o deməkdir ki, adminlər şəbəkə cihazlarına giriş icazəsi verilməzdən əvvəl autentifikasiya olunur. Tacacs protokolu istifadəçi məlumatlarını mərkəzi serverdə saxlamaqla təhlükəsizliyi təmin edir. Server adminlərə giriş icazələrini və səviyyələrini müəyyən edən verilənlər bazası saxlayır.

Tacacs protokolu şəbəkə administratorlarına bir sıra üstünlüklər təqdim edir:

1. Tacacs istifadəçilərin autentifikasiyası üçün təhlükəsiz üsul təqdim edir. Bu, hücum edən şəxslərin şəbəkəyə icazəsiz daxil olmasının qarşısını almağa kömək edir.

2. Tacacs şəbəkə administratorlarına mərkəzi yerdən giriş səviyyələrini və icazələri idarə etməyə imkan verir. Bu proses şəbəkə administratorlarına şəbəkəyə daxil olan istifadəçilərin giriş səviyyələrinə nəzarət etməyə və şəbəkədəki bütün cihazların təhlükəsizliyini artırmağa imkan verir.

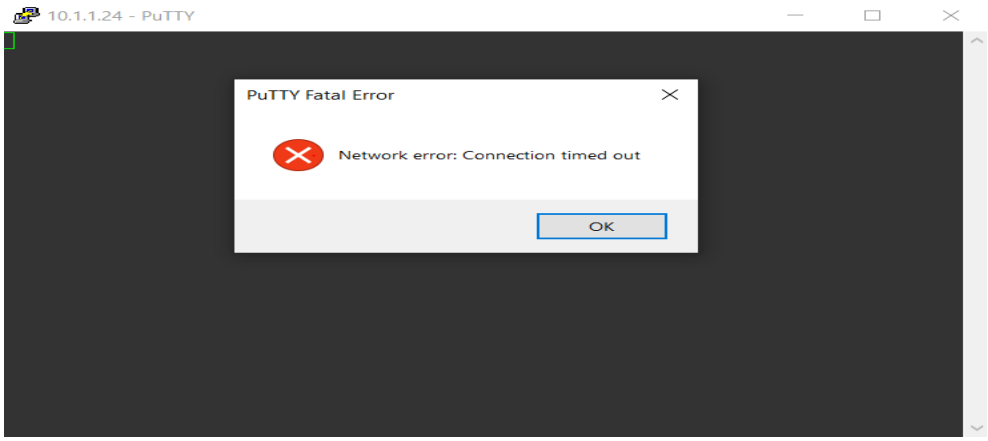
3. Şəbəkədəki cihazların idarə edilməsi üçün də istifadə edilə bilər. Cihazların konfiqurasiyası kimi əməliyyatlar Tacacs protokolu vasitəsilə həyata keçirilə bilər.

Switcdə istifadə edilən Tacacs əmr ardıcıllığını aşağıdakı nümunəyə əsasən nəzər yetirmək olar:

```
aaa new-model
```

```
!
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization config-commands
aaa authorization exec default group tacacs+ local
aaa authorization commands 0 default group tacacs+ local none
aaa authorization commands 15 default group tacacs+ local none
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 0 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
tacacs-server host 10.10.1.11 key 7 AAAA2YF411200LL1WD22
tacacs-server directed-request
```

Bu əmr ardıcıllığını yerinə yetirməklə switch və routerlərdə bizə ayrılan xüsusi username və passwordu istifadə edə bilərik . Yanlış daxil edilən məlumat cihazlara qoşulma prosesinə məhdudiyyət qoyacaq (şəkil 3.16).



Şəkil 3. 16. Yanlış məlumatların daxil edilməsi

Bu əmrlər əlavə edildikdən sonra cihaza daxil olarkən əvvəl qeyd elədiyimiz password və username istifadəsi mümkün olmayacaqdır [7,8].

Azərbaycan Texniki universitetində istifadə edilən firewall Cisco vendorunun ASA təhlükəsizlik cihazıdır. Cisco ASA texnologiyası istifadə edilmədiyi müddətdə, şəbəkədə NAT və digər prosedurlar routerlər tərəfindən edilirdi. Lakin routerlarda

təhlükəsizliyin təmin edilməsi bəzi hallarda qarşılana bilinmir. Bu problemə görə də, Texniki universitetin şəbəkəsində Cisco ASA texnologiyasından istifadə edilir. Əlbəttə hal-hazırda routerlərdə təhlükəsizlik üçün protokollar istifadə edilsə də, bəzi hallarda təhlükəsizlik yüksək şəkildə təmin edilə bilinmir. Cisco ASA-nın routerlərdən üstünlüklərini aşağıdakı kimi qeyd edilə bilər :

1. Firewall imkanları (Firewall Capabilities:): Routerlər ilk növbədə trafiki yönləndirmək və ötürmək üçün nəzərdə tutulmuşdur, amma ASA kimi firewallar şəbəkələr üçün hərtərəfli təhlükəsizlik həlli məsələlərini təmin edir. Firewallar vəziyyətə uyğun paket yoxlaması, tətbiq təbəqəsinin filtrasiyası və müdaxilənin qarşısının alınması imkanları kimi inkişaf etmiş təhlükəsizlik xüsusiyyətlərini təmin edir. Routerlər bəzi əsas access list kimi funksiyalara malik ola bilər, lakin onlar firewall ilə eyni səviyyəyə malik deyillər.

2. VPN Dəstəyi (*VPN Support*): ASA kənardan qoşulan istifadəçilərə şəbəkəyə təhlükəsiz qoşulmağa imkan verən vpn bağlantıları üçün daxili dəstəyi ehtiva edir. Routerlər VPN bağlantılarını da dəstəkləyə bilər, lakin ASA uzaqdan giriş VPN və saytdan sayta (*eng site-to-site*) kimi daha təkmil vpn xüsusiyyətləri təqdim edir.

3. Giriş nəzarəti (Access Control): Firewall-lar adətən routerlərdə olmayan qabaqcıl giriş nəzarəti (*eng advanced access control*) xüsusiyyətlərini təmin edir. ASA mənbə və təyinat ip ünvanları, portlar və protokollar kimi meyarlar əsasında trafiki süzgəcdən keçirə bilən girişə nəzarət siyahılarını (ACL) ehtiva edir. Firewall həmçinin routerlərdə istifadə edilməyən URL filtrasiyası və məzmunun filtrasiyası kimi qabaqcıl xüsusiyyətləri təmin edə bilər.

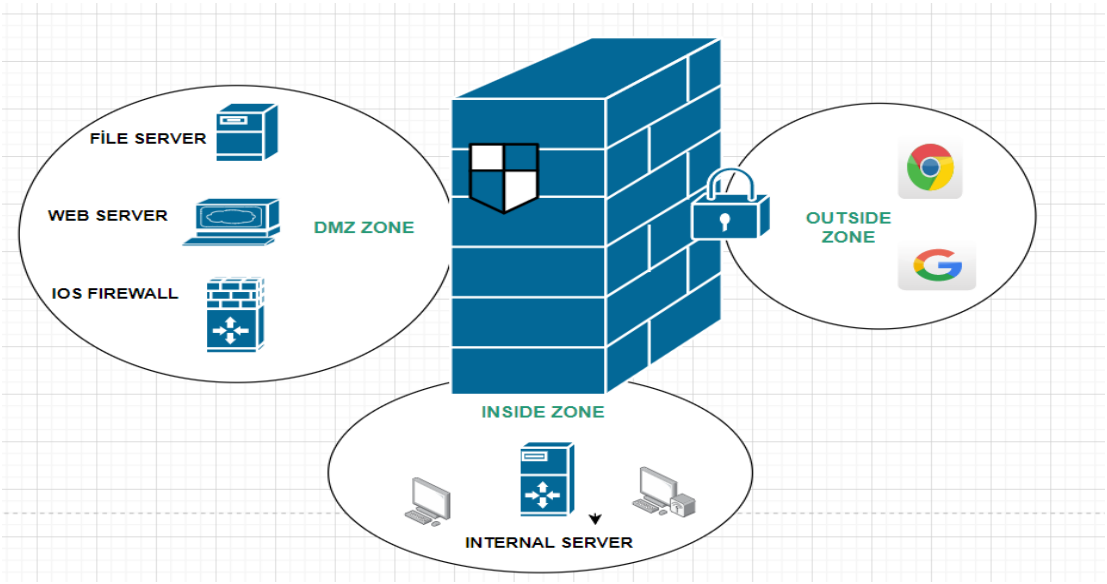
4. Təhlükədən Müdafiə (Threat Protection): ASA kimi firewall-lar müdaxilənin qarşısının alınması, zərərli proqram təminatının qorunması və URL filtri kimi qabaqcıl təhlükədən qorunma imkanlarını təmin edir. Bu xüsusiyyətlər şəbəkəni müxtəlif növ təhlükələrdən, o cümlədən viruslar və digər zərərli proqramlardan qorumağa kömək edir. Routerlər adətən firewall-lar ilə eyni səviyyədə təhlükədən qorunmur.

Firewall şəbəkədə bəzi policy və təhlükəsizlik zonaları yaradır. Zonalar daxili, xarici və DMZ qruplara bölünür:

1. **The outside zone :** Xarici zona ən az etibar edilən zonadır və public interneti təmsil edir. İnternetdən gələn bütün trafikin lokal şəbəkəyə daxil olduğu yerdir və buna görə də ASA tərəfindən ən məhdudlaşdırıcı təhlükəsizlik siyasətlərinə tabedir. Xarici zonadan gələn trafik adətən lokal şəbəkəyə icazəsiz girişi məhdudlaşdırmaq üçün firewall tərəfindən süzülür və yoxlanılır. Tətbiq oluna bilən təhlükəsizlik siyasətlərinin bəzi nümunələrinə müəyyən trafik növlərinin bloklanması (məsələn, P2P fayl paylaşımı) və ya xüsusi ayrılan ip ünvanlarına və ya subnetlərə girişin məhdudlaşdırılması daxildir.

2. **The inside zone :** Ən etibarlı zonadır və lokal şəbəkəni təmsil edir. Bu zonaya istifadəçilər tərəfindən istifadə olunan workstationlar, serverlər, printerlər və digər qurğular daxil ola bilər. Bu zonaya tətbiq edilən təhlükəsizlik prosedurları, xarici zonaya tətbiq ediləndən daha az məhdudlaşdırır, çünki daxildən gələn trafikə etibar edildiyi müəyyən edilir. Əlbəttə ki, daxildə baş verə biləcək təhlükələrin hər an qarşısını almaq üçün trafik izlənilməlidir. Bu hissədə tətbiq edilən təhlükəsizlik nümunələrinə müəyyən edilmiş veb-saytların və ya bəzi proqramların bloklanması (sosial media), baza resurslara (maliyyə qeydləri və s.) icazənin məhdudlaşdırılması daxildir.

3. **The DMZ (demilitarized zone)** : xarici və daxili zonalar arasında yerləşən aralıq zonadır. Veb serverlər, e-poçt və ya FTP serverləri kimi internetdən daxil olmaq lazım olan serverləri yerləşdirmək üçün istifadə olunur. DMZ zonaya tətbiq edilən məhdudiyyət inside zonaya tətbiq ediləndən daha çox, lakin outside zonadan isə daha azdır. Bu hissədən gələn trafikə həm outside, həm inside zonalarla əlaqə qurmağa icazə verilir, ancaq daxili şəbəkəyə (*eng internal network*) icazəsiz girişi məhdudlaşdırmaq üçün trafik filtrlənir və yoxlanılır. Tətbiq edilə bilən təhlükəsizlik qaydalarının bəzi nümunələrinə xüsusi portlara (HTTP , FTP , SMTP) giriş icazəsi və həssas məlumatlara icazənin məhdudlaşdırılması daxildir [10].



Şəkil 3. 17. Firewall təhlükəsizlik zonaları

Cisco ASA firewall istifadəsində lokal və kənar şəbəkələri ayırmaq üçün təhlükəsizlik səviyyələri qurar. Səviyyə nə qədər yüksək göstərilsə interfeys bir o qədər təhlükəsizdir. Təhlükəsizlik səviyyəsi nömrələri 0 (güvənilir olmayan) ilə 100 (çox güvənilir) arasında dəyişir. Təhlükəsizlik səviyyələrinə aid nümunələr aşağıdakı kimi təyin edilir:

I. **Təhlükəsizlik səviyyəsi 0 (*eng Security level 0*):** ASA-da mövcud olan ən aşağı təhlükəsizlik səviyyəsidir və standart olaraq "outside" interfeysə təyin edilir. Daha aşağı təhlükəsizlik səviyyəsi olmadığı üçün bu o deməkdir ki, adminlərin access list də icazə vermədiyi halda kənardan gələn trafik şəbəkənin hər hansı bir interfeysinə daxil ola bilməz.

II. **Təhlükəsizlik səviyyəsi 100 (*eng Security level 100*):** ASA da ən yüksək təhlükəsizlik səviyyəsidir və default olaraq "inside" interfeysə təyin edilir. Biz bunu adətən "LAN" üçün istifadə edirik və ən yüksək təhlükəsizlik səviyyəsi olduğundan, default olaraq bütün digər interfeyslərə çata bilər.

III. **Təhlükəsizlik səviyyəsi 1 – 99 (*eng Security level 1 – 99*):** İstənilən hər hansı bir təhlükəsizlik səviyyəsi yarada bilərik , nümunə olaraq, DMZ üçün 50 təhlükəsizlik səviyyəsi tətbiq edilir. Onu ifadə edir ki, lokal şəbəkədə DMZ-yə (təhlükəsizlik

səviyyəsi 100 -> 50) və həmçinin DMZ-dən xaricə (təhlükəsizlik səviyyəsi 50 -> 0) trafikə icazə verilir. DMZ-dən gələn trafik inside hissəyə (*eng without an access-list*) daxil ola bilməz, çünki təhlükəsizlik səviyyəsi 50-dən gələn trafikə təhlükəsizlik səviyyəsi 100-ə çatmağa icazə verilmir.

1. Mürəkkəblik (Complexity): Cisco ASA-nın əsas zəif cəhətlərindən biri onun mürəkkəbliyidir. Cihazın bir çox parametrləri var ki, bu parametrlər yeni istifadəçilər üçün çətin ola bilər. ASA-nın istifadə etdiyi konfiqurasiya dili də kifayət qədər texnikidir və bunu anlamaq üçün müəyyən müddət ərzində təlim və təcrübə tələb edilə bilər.

2. *Məhdud miqyaslılıq (Limited scalability):* Cisco ASA kiçik və orta təşkilatlar üçün istifadə oluna bilsə də, böyük müəssisələr üçün o qədər də uyğun olmaya bilər. Cihazın dəstəkləyə biləcəyi interfeyslərin və vlanların sayı baxımından bəzi məhdudiyyətlər var və istifadə prosesi müddətində böyük həcmdə trafiki idarə etməkdə çətinlik çəkə bilər.

3. *Məhdud Tətbiq Görünüşü və Nəzarət (Limited Application Visibility and Control):* Cisco ASA-nın tətbiqin görünməsi və nəzarəti (AVC) xüsusiyyətləri yeni nəsil firewall (NGFW) ilə müqayisədə məhduddur. O, yalnız məhdud sayda tətbiqləri və protokolları müəyyən edə və idarə edə bilər ki, bu da bütün növ təhlükəsizlik təhdidlərinin qarşısını almaq üçün kifayət etməyə bilər.

4. *Məhdud URL Filtrləmə İmkanları (Limited URL Filtering Capabilities):* Cisco ASA-nın URL filtrləmə imkanı məhduddur, bu prosedur onu izah edir ki, o, istifadəçilərin potensial zərərli ola biləcək bəzi veb-saytlara daxil olmasının qarşısını ala bilməyəcək. NGFW-lər isə adətən daha geniş növlərdə zərərli vebsaytlara girişi bloklaya bilən daha möhkəm URL filtrləmə imkanlarına malikdir.

5. *Məhdud Hesabat və Analitika (Limited Reporting and Analytics):* Cisco ASA şəbəkə trafiki və təhlükəsizlik prosesləri haqqında əsas hesabatı təqdim edə bilsə də, onun hesabat və analitik imkanları yeni nəsil firewallarla müqayisədə məhduddur.

Risklərin müəyyən edilməsi hallarını və təhlükəsizlik hadisələrinin araşdırılmasını çətinləşdirə bilər ki, məsələ həllində zaman itkisinə yol açır.

6. *Siyasətlərin yaradılmasında məhdud çeviklik (Limited Flexibility in Policy Creation:):* Cisco ASA-nın qaydaların yaradılması və idarə edilməsi mürəkkəb və daha yavaş ola bilər. Bu proses onu izah edir ki, dövlət orqanları və müəssisə kimi yerlər öz xüsusi təhlükəsizlik tələblərinə uyğun qaydalar yaratmaq və bunları tətbiq etməkdə çətinlik çəkə bilərlər.

7. *Bulud Mühitləri ilə Məhdud İnteqrasiya (Limited Integration with Cloud Environments):* Bulud texnologiyası ilə inteqrasiyası məhduddur və getdikcə çox yayılmış bulud əsaslı tətbiqlər üçün təhlükəsizliyin təmin edilməsini çətinləşdirir.

8. *Məhdud Təhdid Kəşfiyyatı İmkanları (Limited Threat Intelligence Capabilities):* Cisco ASA bəzi daxildə təhdid kəşfiyyatı imkanlarına malik olsa da, onlar NGFW-lərdə olanlar qədər inkişaf etmiş deyil. Bu o deməkdir ki, Cisco ASA sıfır gün hücumları (*eng zero-day attacks*) və ya inkişaf etmiş davamlı təhdidlər (*eng-APT advanced persistent threats*) kimi müəyyən növ qabaqcıl təhdidləri aşkarlaya və qarşısını ala bilməyəcək [11].

Hal-hazırda ASA-nın tətbiqi Azərbaycan Texniki Universiteti şəbəkəsində böyük problemlər yaratmasada, zamanla şəbəkənin inkişafı və genişlənməsi ilə bərabər NGFW-larla əvəzlənməsinə üstünlük verilməlidir. NGFW vendorları Palo Alto, Cisco Firepower, FortiGate, Sophos kimi növlərini bildirmək olar. Əlbəttə ki, onları hardware-based, software-based, cloud-based, open-source kimi xüsusi imkanlara malik olan tipləri vardır. Nümunə olaraq Palo Alto firewall-un vacib özəlliklərini qeyd edə bilərik:

I. *Advanced Threat Prevention:* Ən qabaqcıl və təhlükəsizlik protokollarından yayınan kiberhücumları aşkar etmək və qarşısını almaq üçün machine learning, davranış analitikası və fayl təhlili də daxil olmaqla bir sıra yeni təhlükənin qarşısının alınması üsullarından istifadə edir.

II. *Granular Visibility and Control:* Palo Alto firewalları proqramlar və istifadəçilər üçün şəbəkə trafiki üzərində ətraflı görünürlük və nəzarət təmin edərək,

istifadə edən təşkilatlara təhlükəsizlik qaydalarını ətraflı səviyyədə tətbiq etməyə imkan verir.

III. *İntegration and Automation:* Digər şəbəkə avadanlıqları ilə asanlıqla inteqrasiya oluna bilər. Təhlükəsizlik iş prosedurunu sadələşdirmək, əl ilə yazılan, vaxt aparan prosesləri azaltmaq üçün API və skript kimi bir sıra avtomatlaşdırma və qruplaşdırma imkanlarını dəstəkləyir.

IV. *Cloud-Native Security:* Bulud mühitlərinin təhlükəsizliyini təmin etmək üçün məqsədyönlü şəkildə qurulmuş bulud arxitekturaları ilə dizayn edilmişdir, o cümlədən Amazon Web Services, Microsoft Azure və Google Cloud Platform kimi public bulud provayderlərinə dəstək göstərə bilir [28].

AZƏRBAYCAN RESPUBLİKASI ELM və TƏHSİL NAZİRLİYİ
AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əlyazması hüququnda

MƏLİKMƏMMƏDOV ELTAC ELŞAD OĞLU

AzTU-nun kompüter şəbəkəsində informasiya təhlükəsizliyinin qiymətləndirilməsi sisteminin işlənməsi

mövzusunda

MAGİSTRLİK DİSSERTASİYASI

İxtisas: 060631- " Kompüter mühəndisliyi"
İxtisaslaşma: "Biliklərin əldə edilməsi sistemləri"

Elmi rəhbər: t.f.d., dosent C. Məmmədov

BAKI – 2023

IV FƏSİL. VEB HÜCUMLARI VƏ ONLARA QARŞI GÖRÜLƏN TƏHLÜKƏSİZLİK TƏDBİRLƏRİNİN TƏDQİQİ.

4.1. Şəbəkəyə veb hücumlar və təhlükəsizliyin təmin edilməsi.

İnternet və Ümumdünya Şəbəkəsinin (WWW) inkişafından bugünə veb proqramları çox populyarlaşdı və bu gün onlardan demək olar ki, hər bir mühitdə istifadə olunur. Bu onlayn tətbiqlər təşkilat, brend və məlumat üçün çoxlu faydalarla bərabərində riskləri də özü ilə birlikdə gətirdi. İnternetin (və hər hansı digər məlumat kommunikasiya şəbəkəsinin) əsas funksionallığı son sistemlərin əlaqə saxlamasına imkan verməkdir. Beləliklə, internet zərərli istifadəçilərin hakerlik, casusluq və s. məqsədləri üçün son sistemlərə icazəsiz giriş əldə etdiyi bir vasitə formalı hücumlar kimi xidmət etmişdir [14].

Kibertəhlükəsizlik və şəbəkə təhlükəsizliyi bu günlərdə iki əsas mövzudur, çünki hücumların hər gün artdığını nəzərə alaraq həyatımıza təsir edir. Kibertəhlükəsizlik şəbəkələri, kompüterləri, proqramları və məlumatları hücumdan, zədələnmədən və ya icazəsiz girişdən qorumaq üçün nəzərdə tutulmuş texnologiyalar, proseslər və təcrübələr məcmusudur. Şəbəkə təhlükəsizliyi internetdə mühüm narahatlıq doğurur. Şəbəkə təhlükəsizliyi kompüter şəbəkəsindəki fayllara və qovluqlara girişin hakerlikdən, sui-istifadədən və sistemdə icazəsiz dəyişikliklərdən qorunmasıdır

Kiberhücum icazəsiz giriş əldə etməyə, məlumatları oğurlamağa və ya kompüterlərə, kompüter şəbəkələrinə və ya digər hesablama sistemlərinə zərər vurmağa cəhd edən təhdid subyektləri tərəfindən görülən bir sıra tədbirlərdir. Kiberhücum istənilən yerdən həyata keçirilə bilər. Hücum bir və ya bir neçə taktika, texnika və prosedurdan istifadə edərək bir şəxs və ya qrup tərəfindən həyata keçirilə bilər. Şəbəkə hücumlarının iki əsas növü var:

Passiv: Təcavüzkarlar şəbəkəyə giriş əldə edir və həssas məlumatları izləyə və ya oğurlaya bilərlər, lakin heç bir dəyişiklik etmədən məlumatları toxunulmaz olaraq buraxırlar.

Aktiv: Təcavüzkarlar yalnız icazəsiz giriş əldə etmir, həm də məlumatları silməklə, şifrələməklə və ya başqa yolla zədələməklə onları dəyişdirirlər.

Veb hücumları mürəkkəblik və müxtəliflik baxımından sürətlə böyüdükcə, şəbəkə təhlükəsizliyi tədqiqatçıları dərin öyrənməyə əsaslanan yeni təhlükəsizlik texnologiyalarını fəal şəkildə araşdırırlar. Ənənəvi veb-hücum aşkarlama texnologiyaları böyük verilənlər mühitində zəif cəhətləri göstərsə də, dərin öyrənmənin yüksəlişi belə mühitlərdə təhlükəsizlik problemlərinə yeni həllər təqdim edir [26].

Müasir təşkilatlar ünsiyyət üçün internetdən istifadə edirlər və məxfi məlumatlar tez-tez şəbəkələr arasında mübadilə edilir. Müəssisələr öz aktivlərini getdikcə daha təkmilləşən kibertəhlükəsizliklərdən qorumaq üçün ən yüksək kibertəhlükəsizlik standartlarını, şəbəkə təhlükəsizliyi siyasətlərini və personalın təlimini təmin etməlidirlər.

Ən çox istifadə olunan şəbəkə hücumlarının ümumi növləri hansılardır?

Aşağıda təcavüzkarların şəbəkənizə nüfuz etmək üçün istifadə edə biləcəyi ümumi təhlükə vektorları verilmişdir.

1. *İcazəsiz giriş*

İcazəsiz giriş icazə almadan şəbəkəyə daxil olan təcavüzkarlara aiddir. İcazəsiz giriş hücumlarının səbəbləri arasında zəif parollar, sosial təhlükəsizlik qaydaların qorunmaması, əvvəllər oğurlanmış hesablar və daxili təhdidlər var.

2. *Man-in-the-middle Attacks*

Man-in-the-middle Attacks, şəbəkəniz və xarici saytlar arasında və ya şəbəkəniz daxilində hərəkət müdaxilə edən təcavüzkarları əhatə edir. Şəbəkə protokolları vasitəsi ilə qorunmursa və ya təcavüzkarlar bu təhlükəsizliyin qarşısını almaq üçün bir yol tapsalar, ötürülən məlumatları oğurlaya, istifadəçi etimadnaməsini əldə edə və sessiyalarını ələ keçirə bilərlər.

3. *Kod və SQL İnjection hücumları*

Bir çox veb-saytlar, istifadəçi daxiletmələrini qəbul edir və bu girişləri təsdiq edə və təmizləyə bilmir. Təcavüzkarlar daha sonra gözlənilən məlumat dəyərləri əvəzinə

zərərli kodu ötürərək formanı doldura və ya API çağırışı edə bilərlər. Kod serverdə icra olunur və təcavüzkarlara onu pozmağa imkan verir.

Yoxlanılmamış istifadəçi məlumatlar girişləri, korporativ şəbəkələri SQL injection hücum riskinə ata bilər. Şəbəkə hücumu metodunda kənar tərəflər gözlənilən məlumat dəyərləri əvəzinə zərərli kodlar göndərərək formaları dəyişdirirlər. Onlar şəbəkəni pozur və istifadəçi parolları kimi həssas məlumatlara giriş əldə edirlər.

Versiya və strukturu haqqında təfərrüatları əldə etmək üçün verilənlər bazalarını araşdırmaq və tətbiq səviyyəsində məntiqin təxribatı, məntiq ardıcıllığının və funksionallığın pozulması kimi müxtəlif SQL infeksiya növləri mövcuddur.

Şəbəkə təhlükəsizliyi adətən istifadəçi adı və parol, avtorizasiya ilə başlayır. Şəbəkə təhlükəsizliyi kompüter şəbəkəsinə və şəbəkə əlçatan resurslarına icazəsiz girişin, dəyişdirilməsinin, sui-istifadəsinin və ya rədd edilməsinin qarşısını almaq və nəzarət etmək üçün şəbəkə administratoru tərəfindən qəbul edilmiş müddəa və siyasətlərdən ibarətdir. Əsasən, şəbəkə təhlükəsizliyi şəbəkə administratoru tərəfindən idarə olunan şəbəkədəki məlumatlara daxil olmaq icazəsini əhatə edir [5].

Şəbəkəyə qoşulmuş kompüterlərdə təhlükəsizlik üçün ən yaxşı üsullardan bəzilərini aşağıdakı kimi ifadə edə bilərik:

● *Proxy Server vasitəsilə internetə çıxışı tənzimləyin*

Şəbəkə yoxlanılmadan istifadəçilərinin internetə daxil olmasına icazə verməyin. Bütün sorğuları şəffaf proxy vasitəsilə yönləndirin və istifadəçi davranışına nəzarət etmək və izləmək üçün ondan istifadə edin. Çıxan bağlantıların bot və ya digər avtomatlaşdırılmış mexanizm tərəfindən deyil, əslində insan tərəfindən edildiyinə əmin olun. Korporativ istifadəçilərin yalnız sizin açıq şəkildə təsdiqlədiyiniz veb saytlara daxil ola bilməsini təmin etmək üçün domenləri ağ siyahıya salın.

● *Təhlükəsizlik cihazlarını düzgün yerləşdirin*

Yalnız şəbəkənin kənarında deyil, şəbəkə zonalarının hər bir qovşağında bir firewall yerləşdirin. Tam hüquqlu firewall-ları hər yerdə yerləşdirə bilmirsinizsə, açarlarınızın daxili təhlükəsizlik divarı funksionallığından istifadə edin. Şəbəkənin

kənarında anti-DDoS cihazları və ya bulud xidmətləri yerləşdirin. Yük balanslaşdırıcıları kimi strateji cihazları hara yerləşdirmək barədə diqqətlə düşünün - əgər onlar Hərbiləşdirilmiş Zonadan (DMZ) kənardadırlarsa, onlar şəbəkə təhlükəsizlik cihazınız tərəfindən qorunmayacaq.

● *Network Address Translation istifadə edin*

NAT daxili IP ünvanlarını ictimai şəbəkələrdə əlçatan olan ünvanlara çevirmə etməyə imkan verir. Bir IP ünvanından istifadə edərək birdən çox kompüteri internetə qoşmaq üçün ondan istifadə edə bilərsiniz. Bu, əlavə təhlükəsizlik səviyyəsini təmin edir, çünki istənilən daxil olan və ya gedən yol NAT cihazından keçməlidir və daha az ip ünvanları var ki, bu da təcavüzkarların hansı hosta qoşulduqlarını anlamalarını çətinləşdirir.

● *Aldatma Texnologiyasından istifadə edin.*

Heç bir şəbəkə mühafizə tədbiri 100% uğurlu deyil və təcavüzkarlar nəhayət şəbəkənizi sındırmağı bacaracaqlar. Bunun olacağını bilib və şəbəkənizdə tələlər yaradan, təcavüzkarları onlara "hücum etməyə" təşviq edən və onların planlarını və üsullarını müşahidə etməyə imkan verən aldatma texnologiyasını tətbiq edin. Siz həyat dövrünün bütün mərhələlərində təhdidləri aşkar etmək üçün tələlərdən istifadə edə bilərsiniz: məlumat faylları, etimadnamələr və şəbəkə əlaqələri. [1]

4.2 Azərbaycan Texniki Universiteti şəbəkəsinə olan veb hücumlar və təhlükəsizliyinin təmin edilməsi

Universitetlər həm mədəniyyət, həm də texnologiya baxımından ən açıq və ekstrovert sektorlardan biridir. Bu, akademiklər arasında transsərhəd əməkdaşlığa imkan verərək asanlaşdırır və çox güman ki, onların uğurunun mühüm tərkib hissəsidir. Təəssüf ki, bu, təcavüzkarın işini asanlaşdırır. Universitetin veb-saytı kimi resurslardan istifadə edərək kimin hədəf alınacağını, onlara necə çatacağını müəyyən etmək və onlara yaxınlaşmaq üçün inandırıcı hekayə yaratmaq asandır. Bu bilik tez-tez fişinq

hücumlarını təmin etmək üçün açardır, burada yaxşı hazırlanmış mesaj bir işçini və ya tələbəni təcavüzkar üçün faydalı bir şey etmək, aldatmaq üçün istifadə olunur.

Kibertəhlükəsizlik xüsusilə pandemiyadan sonrakı dünyada kolleclər və universitetlər üçün əsas narahatlıq doğurur. Bununla pandemiyadan əvvəl ali təhsil müəssisələrində tələbələrdən və müəllimlərdən çoxlu məlumat toplamışdı. Bu, indi daha da böyükdür, çünki bir çox universitet hibrid və ya tamamilə uzaqdan kurikulum təklif edir. Kolleclər və universitetlər böyük həcmdə məlumat saxladıqları üçün onlar tez-tez hakerlərin və digər kibercinayətkarların hədəfinə çevrilirlər.

Lakin kiberhücumların yaratdığı risklər ali təhsil dünyası üçün maliyyə itkilərindən kənara çıxır. Həqiqətən də, kolleclər və universitetlər tələbələrin sosial təminat nömrələrindən tutmuş qiymətli əqli mülkiyyətə qədər böyük həcmdə həssas məlumatlara malikdirlər ki, bu da oğurlandıqda və ya ələ keçirildiyi təqdirdə, akademik mühitin hüdudlarından kənarda əhəmiyyətli zərərlərə səbəb ola bilər. Kiberhücumlar universitetin reputasiyasına və tələbələrinin təhlükəsizliyinə ciddi təhlükə yaradır, bəlkə də yuxarıda qeyd olunan potensial maliyyə itkilərindən daha vacibdir. Təhlükələr daim inkişaf etsə də, kolleclər və universitetlər gələcəkdə kibertəhlükəsizlik problemlərinə cavab vermək üçün lazım olan istedada və infrastruktura sərmayə qoymağa davam etməlidir.

Kolleclər və universitetlər rəqəmsal alətləri və interfeysləri qəbul etmək üçün hələ tez olduğundan (maliyyə və digər praktiki narahatlıqlar nəticəsində) bir çox ali təhsil müəssisələri hələ də hücuma xüsusilə həssas olan köhnə sistemlərə etibar edirlər. Sadəcə olaraq, kiberhücumçular bəzi hallarda təəssüf ki, köhnəlmiş və rəqibsiz olan universitet sistemlərindən faydalanmaq üçün ən son texnologiya və üsullardan istifadə edirlər. Hakerlər kiberhücumları həyata keçirərkən müxtəlif taktika və vasitələrdən istifadə edirlər. Ən çox yayılmış bu cür üsullar aşağıda təsvir edilmişdir. Bu siyahı heç bir halda kolleclər və universitetlər üçün unikal olmasa da, hakerlərin kibertəhlükəsizlik boşluqlarından necə tam istifadə etməyə çalışdıqlarını daha yaxşı başa düşməyə imkan

verəcək və gələcəkdə bu cür hücumların ən yaxşı şəkildə necə dayandırılacağını nəzərdən keçirməyə kömək edəcək [4].

SQL Enjeksiyonları:

"Veb proqramlarının üzləşdiyi ən ciddi problem kimi, SQL Enjeksiyonları (SQLi), sadə dillə desək, müəyyən proqramların əsas verilənlər bazalarından istifadə edərək parol mühafizəsini keçmək üçün nəzərdə tutulmuş hücumlardır. SQL (Standart Sorğu Dili) qısa olaraq ifadə etsək verilənlər bazalarını idarə edir və onlarla əlaqə qurur." SQL Enjeksiyonları giriş səhifələrində (məsələn, istifadəçi adı və parol giriş səhifələri) kodun zəif cəhətlərindən istifadə etməklə və xüsusi verilənlər bazasını zəif məlumatları qaytarmağa məcbur etməklə işləyir. Əsas verilənlər bazasının kodu zəifdirsə, bu SQL kodu əsas verilənlər bazasını dəyişdirə və verilənlər bazasının idarə etdiyi tətbiqi hakerlərin girişinə icazə verməyə məcbur edə bilər. Nə qədər ki, ali təhsil müəssisələri əsas verilənlər bazalarına yazılan boşluqlara malik olmaqda davam edəcək, SQL Enjeksiyonları çox güman ki, ümumi və hakerlərin istifadəsi üçün çox asan olacaq. Versiya və strukturu haqqında təfərrüatları əldə etmək üçün, verilənlər bazalarını araşdırmaq və tətbiq səviyyəsində məntiqin təxribatı, məntiq ardıcıllığının və funksionallığın pozulması kimi müxtəlif SQL Enjeksiyon növləri mövcuddur.

SQL Enjeksiyon hücumlarının qarşısını necə almaq olar?

SQL Enjeksiyonları kiberhücumların həyata keçirilməsinin ən asan və effektiv formalarından biridir. Digər tərəfdən, SQL enjeksiyonlarına qarşı müdafiə də nisbətən asandır. Veb tərtibatçıları yaxşı kodlaşdırması ilə SQL Enjeksiyon hücumlarının qarşısını ala bilərlər. Ancaq həssas məlumatlarınızı SQLi hücumlarından qorumaq üçün edə biləcəyiniz çox şey var.

- Məlumatlarınızı daxil etməzdən əvvəl vebsaytın təhlükəsiz olub-olmadığını yoxlayın və texniki təhlükəsizlik xəbərlərini izləyin ki, istifadə etdiyiniz vebsayt pozulduğu halda parolunuzu dəyişə biləsiniz. AVG BreachGuard, pozuntu halında məlumatlarınızın sızmasının qarşısını almağa kömək edə bilər.

- Ən azı 12 simvoldan ibarət unikal parollardan istifadə etmək kimi güclü parol vərdişlərinə yiyələnin.

- Məlumat bazası təhlükəsizliyini artırmaq, əlavə məlumatların daxil olmasını məhdudlaşdırmaq və istifadə ediləcək proqramların sınaq prosesindən keçirilməsi ən önəmli prosedurlardan biridir.

- Avast Hack Check ilə SQLi hücumu və ya digər pozuntu nəticəsində hesablarınızdan hər hansı birinin sızdığını yoxlayın. Təhlükəsizliyiniz pozulubsa, dərhal parolunuzu dəyişdirin.

- Veb tətbiqi təhlükəsizlik divarı (WAF) veb tətbiqi ilə internet arasında zərərli proqram və trafiki süzən bir maneədir. Müxtəlif növ SQL infeksiyalarından və digər təhlükəsizlik təhdidlərindən qorunmaq üçün veb tətbiqi quraşdırıla bilər.

- AVG Antivirus ilə təhdidlərdən və zəifliklərdən qorunmaq mümkündür. Şəbəkənizin təhlükəsizliyini təmin etmək, köhnəlmiş proqramı silmək və ya zərərli proqramları aradan qaldıraraq, onlayn təhlükələrin bütün aspektlərindan qorunmaq olar.

Phishing:

Phishing hücumları istifadəçiləri aldadaraq parollar və ya kredit kartı məlumatları kimi həssas məlumatları daxil etməsi üçün nəzərdə tutulmuş e-poçt və ya veb səhifələrlə müraciət edirlər. Texniki Universitetinin İnformasiya Təhlükəsizliyi İdarəsi bu tip hücumlara qarşılaşa bilirlər. Phishing hakerləri, ünvanları internetdəki ünvan kitabçalarından və internet saytlarından əldə etdikləri böyük bir qrup şəxsə e-poçt mesajı göndərirlər. Çox vaxt yaxşı hazırlanmış və rəsmi görünən mesajın bir maliyyə institutundan, bir xidmət sektorundan gəldiyi iddia edilir. Adətən, alıcıdan məlumat vermək üçün veb-sayt linkinə daxil olması xahiş olunur. Bununla belə, vebsayta keçid qanuni görünsə də, göstərilən linkin faktiki qanuni deyil və daxil olduğunuz zaman artıq sizin o təhlükəyə məruz qaldığınız görünməkdədir.

Phishing hücumları istifadəçi məlumatlarının oğurlanmasından tutmuş, maliyyə ödənişinin alınmasına qədər geniş məqsədlərə malik ola bilər. Bu hücumlar aşkar və qarşısını almaq asan görünsə də, araşdırmalar göstərdi ki, müəssisələrin, təşkilatların,

univeritetlerin əksəriyyəti phishing hücumlarının qurbanı olur. Phishing qarşısının alınması üçün bu istiqamətdə marifləndirici addımlar atmaq lazımdır [29].

Daxili texniki düzəlişlərlə edilə bilən SQL hücumlarının qarşısının alınmasından fərqli olaraq, phishing hücumlarının qarşısının alınması əsasən müəllimlər, işçilər və tələbələr kimi son istifadəçilərdən asılıdır. Bütün son istifadəçilərin oyaq qalmasını təmin etmək üçün kollec və universitetlərin atmalı olduğu bir neçə addım var:

- E-poçt filtrləri: İlk və sadə addım olaraq, kolleclər və universitetlər şübhəli qeyri-universitet e-poçtlarını istifadəçinin spam qovluğuna göndərən e-poçt filtrləri yaratmalıdır. Bu, mükəmməl bir düzəlişdən uzaq olsa da, zərərli e-poçtların təyinat yerinə çatmasının qarşısını ala biləcək vacib ilk addımdır.

- Universitetlər son istifadəçilərdən phishing-in nə olduğunu və onun necə tanınacağını əhatə edən təlim keçmələrini tələb etməlidir. Bu xidməti göstərməyə həsr olunmuş şirkətlər var və ali təhsil müəssisələri müəllim və işçi heyətini lazımi qaydada hazırlamaq üçün lazımi vaxt və resursları sərf etməyə hazır olmalıdırlar. Müəllim heyətinin və tələbələrin şəxsi parolları və digər məxfi informasiyanı bilinməyən e-poçta və ya saytlarda qeyd etməməsinin izahı verilməlidir [27].

Distributed Denial of Service (DDoS), DoS/DDoS hücumları

DDoS- "paylanmış xidmətdən imtina" kimi tərcümə olunur. Bu, bant genişliyini həddən artıq yükləməklə xidmətin (portal, vebsayt, onlayn mağaza və s.) fəaliyyətini pozan bir növ haker hücumudur. DoS hücumları, bir qayda olaraq, bir nöqtədən (bir cihazdan) gəlir, lakin DDoS hücumları isə daha böyükdür və eyni vaxtda çoxlu sayda fərqli nöqtədə yerləşən avadanlıqdan həyata keçirilir. Həm şəxsi serverlər, həm də botnetlər bu şəkildə hərəkət edə bilər.

Təcavüzkarların ilk və ən bariz məqsədi veb-resursların işləməsinin qarşısını almaq, istifadəçilərin onlardan istifadə etməsinə mane olmaqdır. Bəzən bu cür hücumlar diqqəti şirkətin daxili mühitinə sızmaq və məlumatların oğurlanması kimi digər zərərli fəaliyyətlərdən faydalanmaq üçün də istifadə olunur. Həmçinin şəbəkənizə və ya serverlərinizə saxta məlumat yönləndirmək üçün istifadə edirlər. DDoS şəbəkə

səviyyəsində, məsələn, serveri sıxışdıra bilən böyük həcmdə SYN/ACC paketləri göndərməklə və ya proqram səviyyəsində, məsələn, verilənlər bazasını diz çökdürən mürəkkəb SQL sorğularını yerinə yetirməklə baş verə bilər. Bu prosedurlar tətbiq edilərkən, istifadəçi internetə daxil olduğu müddətdə veb-sitelerinin ciddi şəkildə ağırlaşması, veb saytı və ya server xidmətlərində ki bağlantıların itməsi, bağlantıda uzun müddətli xidmət kəsintisi və s. kimi hallarla qarşılaşıla bilinər.

DoS/DDoS hücumlarının qarşısının alınması üsulları:

-Şəbəkə seqmentasiyası – Şəbəkələri daha kiçik, daha idarə oluna bilən hissələrə ayırmaq DoS hücumunun təsirini məhdudlaşdıra bilər. Bu, vlan-lar yaratmaqla edilə bilər və firewall-lar hücumun yayılmasını məhdudlaşdıra bilər.

-İP bloklanması - Məlum və ya şübhəli zərərli mənbələrdən gələn trafikin bloklanması DoS trafikinin təyinat yerinə çatmasının qarşısını ala bilər.

-Daxil olan və ya gedən şəbəkə xəttinə nəzarət edən və bir sıra təhlükəsizlik qaydaları əsasında məlumat paketlərinə icazə verən və ya bloklayan şəbəkə təhlükəsizliyi cihazı olar.

Universitet şəbəkəsində görülən bəzi DDoS hücum növlərini aşağıdakı kimi qeyd edə bilərik:

UDP FloodDDoS - Server tərəfdə olan portları bloklamaq üçün istifadə edilən hücum növüdür. Bu prosedurda, UDP paketlərini serverə göndərməklə xidmət göstərə bilməməsinə və portların bağlanmasına xidmət edir.

PingFlood: Serverə saysız-hesabsız minlərlə ip üzərindən ping göndərilməsi nəticəsində baş tutan hücum növüdür. Bu hücum növləri ilə birlikdə *Volume BasedDDoS (həcm mərkəzli hücum), Application LayerDDoS, Protocol BasedDDoS şəbəkədə görülə bilər* [26].

Cross-Site Scripting (Saytlararası Skriptləmə)

Cross-Site Scripting (qısaca XSS) hakerlərin, veb proqramlara gizli şəkildə girmək üçün istifadə etdiyi ən çox yayılmış tətbiq səviyyəli hücumlardan biridir. Saytlararası Skript, müştəri təfərrüatları oğurlandıqda və ya manipulyasiya edildikdə,

təhlükəsizliyin tamamilə pozulmasına səbəb ola biləcək xüsusi veb-saytın müştərilərinin məxfi məlumatlarına olan hücumdur. Bu hücum növvü əksər hücumlardan fərqli olaraq, XSS hücumu üç tərəfi – təcavüzkarı, müştərini və veb saytı əhatə edir. XSS hücumunun məqsədi müştəri məlumatlarını və ya müştərini vebsaytla müəyyən edə biləcək hər hansı digər həssas məlumatları oğurlamaqdır. Saytlararası skript hücumu həyata keçirən hakerlərin bir neçə hədəfi mövcuddur. Bunlara aşağıdakılardır:

-Sessiya identifikatorları kimi dataya giriş

-Hesabını sındırmaq üçün qurbanı təqlid edilməsi, şəxsi hesabın ələ keçirilməsi,

-Zərərli proqram/ Troya atının hücum proqramlarının quraşdırılması,

-Saytın davranışını manipulyasiya etmək və məzmunu dəyişdirmək,

-İstifadəçi fayllarının/məlumatlarının hərkəsə yayılması,

-Veb məzmun saxtakarlığı, zərərli yönləndirmələr,

Saytlararası skript(Cross-Site Scripting) aşkarlanması və düzəltməsi çətin olan mürəkkəb hücum vektorudur. Ən yaxşı təhlükəsizlik təcrübələrinə əməl etməklə məlumatlarınızı qoruya bilərsiniz. Aşağıda XSS hücumlarından qorunmaq üçün bəzi üsullar göstərilmişdir:

● Məzmun Təhlükəsizliyi Siyasəti (CSP) yaradın

Məzmun təhlükəsizliyi siyasətinin (CSP) yaradılması və tətbiqi Saytlararası Skript və digər zəifliklər azaltmaq üçün effektiv üsuldur. Brauzerlərin skriptləri yükləyə və işlədə bildiyi URL-ləri ağ siyahıya salmaqla XSS-in qarşısını alır.

● Çıxış Kodlaşdırmasından istifadə edin

Təcavüzkar məlumatı dəyişdirə bilər, yəni məlumatın tam olaraq istifadəçinin yazdığı kimi göstərildiyinə əmin olmaq üçün çıxış kodlaşdırmasından istifadə etməlisiniz. Bu, onun təsdiqlənmiş və aktiv məzmun kimi şərh edilməsinin və sonra veb səhifəyə əlavə edilməsinin qarşısını alır.

● Ağ siyahı və qara siyahı

OWASP, XSS hücumlarından qorunmaq üçün ağ siyahıya qarşı qara siyahıya doğrulama yanaşmasını qəbul etməyi tövsiyə edir. Ağ siyahı yalnız müəyyən ünvanların,

proqramların, vebsaytların və ya cihazların ("yaxşı" kimi təsdiqlədiyiniz) şəbəkələrinizə daxil olmasına icazə vermək deməkdir.

XSS hücumu necə işləyir? Ümumi olaraq, saytlararası skript hücumu belə işləyir:

Kibercinayətkarlar aşkar edirlər ki, istifadəçilərin tətbiq etdikləri veb səhifə XSS hücumlarına qarşı həssasdır. O, giriş formaları, şərh və axtarış qutuları vasitəsilə istifadəçilərdən daxil olan məlumatları qəbul edə bilər. Kibercinayətkar zərərli skript (faydalı yük) yaradır və onu bu prosesdən şübhələnməyən istifadəçiyə göndərir. Zərərli skripti fişinq linkinə əlavə edə və hədəflənən şəxsi onu klikləməyə inandıra bilər. Hədəf edilən şəxs zərərli linki kliklədikdə, bu zamana qədər etibar etdikləri təhlükəli veb səhifəyə yönləndirilir. Zərərli skripti təhlükəli veb səhifəyə enjekte edilir və kibercinayətkar tərəfindən hədəflənmiş şəxsin veb brauzeri ona qanuni mənbə kodu kimi yanaşır. Şübhə edilmir ki, istifadəçi bəzi saytlara daxil olmaq istədikdə və bu məlumatları onlara təqdim etdikdə, zərərli skript kibercinayətkarların əmrlərinə uyğun olaraq həyata keçirilir [30].

Cross-site request forgery (CSRF) (Saytlararası sorğu)

Ümumi struktur olaraq CSRF *(eng. Cross Site Request Forgery)* saytın zəifliyindən istifadə edərək, sayt istifadəçinin özüdür kimi rol oynayır. Uğurlu CSRF hücumunda, təcavüzkar qurban istifadəçinin qəsdən hərəkət etməsinə səbəb olur. Məsələn, bu, onun hesabındakı e-poçt ünvanının dəyişdirilməsi, parolunun dəyişdirilməsi və ya pul köçürməsi ola bilər. Hərəkətin xarakterindən asılı olaraq, təcavüzkar istifadəçinin hesabına tam nəzarət edə bilər. Təhlükəli istifadəçinin proqram daxilində imtiyazlı rolu varsa, təcavüzkar tətbiqin bütün məlumatlarına və funksiyalarına tam nəzarət edə bilər. Təcavüzkarın CSRF hücumunu həyata keçirməkdə məqsədi istifadəçini vəziyyət dəyişikliyi sorğusunu göndərməyə məcbur etməkdir. Nümunələr daxildir:

-Qeydin təqdim edilməsi və ya silinməsi,

-Əməliyyat təqdim ediməsi,

-Bir məhsul almaq,

-Parolun dəyişdirilməsi,

-Mesaj göndərmək kimi və s.

CSRF hücumlarının həm qarşısının alınması, həm də azaldılması üçün bir sıra effektiv üsullar mövcuddur. İstifadəçinin nöqteyi-nəzərindən, qarşısının alınması giriş etimadnaməsini qorumaq və icazəsiz aktyorların proqramlara girişini rədd etmək məsələsidir.

CSRF hücumları üçün ən çox istifadə edilən qarşısının alınması üsulu anti-CSRF token və ya mapper token kimi tanınır. CSRF hücumunu qarşısının alınması üçün tətbiqlərə HTTP sorğusunun tətbiqin istifadəçi interfeysi vasitəsilə qanuni şəkildə yaradılıb-yaratılmadığını müəyyən etmək üçün bir üsul lazımdır. Buna nail olmağın ən yaxşı yolu CSRF tokenindən istifadə etməkdir. CSRF tokeni CSRF hücumlarının qarşısını almaq üçün istifadə edilən təhlükəsiz təsadüfi nişandır [31].

Clickjacking attack (Klik hücumu)

Clickjacking hücumları, istifadəçinin hesab etdiyi hərəkətin üstündə görünməz səhifə elementi yaradaraq, veb istifadəçilərini istəmədikləri hərəkətləri etməsi üçün aldadan kiber hücum növüdür. Clickjacking hücumları adətən veb-saytın görünən interfeysini, qurbanın hücumdan xəbəri olmayan şəkildə redaktə etmək və ya manipulyasiya etməklə həyata keçirilir. Bu aldatma istifadəçiləri zərərli proqramları yükləmək, hədəf hesablara vəsait köçürmək, parol menecerlərində avtomatik doldurma funksiyalarından istifadə etmək və hətta qurbanın kompüterinə daxil olmaq kimi hərəkətlərə sövq edə bilər.

Riski azaltmaq üçün veb-tərtibatçılara və adminlərə vebsaytda klik oğurluğunun qarşısını almaq üçün aşağıdakı addımları atmağı tövsiyə edir:

- Çərçivə kimi fəaliyyət göstərməsi nəzərdə tutulmayan bütün veb səhifələrdə X-Frame-Options HTTP cavab başlığından istifadə edin.

- Təcavüzkarların vebsaytınıza zərərli məzmun yerləşdirməsinin qarşısını almaq üçün veb saytınızın SSL istifadə etdiyinə və HTTPS üzərindən xidmət göstərdiyinə əmin olun.

- Yeni versiyalar çıxan kimi məlum zəifliklər və boşluğu olan proqramlar (patch programs) üçün veb saytınızı müntəzəm olaraq skan edin.

- Klik-oğurluq cəhdlərini aşkar etmək və bloklamaq üçün veb tətbiqi təhlükəsizlik duvarından (WAF) istifadə edin [15].

Brute force attacks (Sərt güc hücumu)

Brute force attacks, sayta və ya serverə (və ya parolla qorunan hər hansı bir şeyə) daxil olmaq üçün ən sadə üsuldur. O, vebsayta daxil olmaq üçün müxtəlif parol birləşmələrini sınamaq üçün təkrar cəhdləri əhatə edən kibercinayətdir. Hakerlər bu cür hücumları həyata keçirmək üçün lazım olan gücü artırmaq üçün başqa kompüterlərə zərərli şəkildə quraşdırdıqları botlardan istifadə etməklə buna cəhd edirlər.

Hakerlər bir insanı təqlid etmək üçün sərt hücuma keçə bilərlər. Onlar şəxsi hesablardan istifadəçinin məlumatlarını, o cümlədən tibbi qeydlərini və maliyyə detallarını əldə edərək daha geniş hücumlara başlamaq üçün sui-istifadə edilə bilərlər. Həmçinin məxfi məlumatları oğurlamaq və ya məlumatları dəyişdirməklə şirkətin reputasiyasına xələl gətirmək üçün bu növ hücumlar təşkil edirlər.

Brute force attacks aşağıdakı şəkildə göründüyü kimi bəzi ehtiyat tədbirləri görərək bu hücumlarının qarşısını ala bilərsiniz:

● Şifrə uzunluğu və parolun mürəkkəbliyi - Brute force attacks qarşısını almaq üçün ilk addım daha uzun parol olmalıdır. Bu gün bir çox veb sayt və platformalar istifadəçilərini asanlıqla təxmin edilə bilməyəcək şəkildə müəyyən uzunluqda (8 – 16 simvol) parol yaratmağa məcbur edir. Digər vacib məsələ təhlükəsizlik zəifliklərini minimuma endirmək üçün kompleks parol yaratmaqdır. Parolunuz böyük və kiçik hərflərin birləşməsindən ibarət olmalıdır və onu daha mürəkkəb etmək üçün rəqəmlərdən və xüsusi simvollardan istifadə etmək lazımdır.

Giriş cəhdlərini məhdudlaşdırın - WordPress, admininizdə və ya hər hansı digər idarəetmə panelinizdə giriş cəhdlərini məhdudlaşdırmaq da saytınızı güclü hücumlardan qorumağa kömək edir. Məsələn, veb saytınız beş uğursuz giriş cəhdi alırsa, o, növbəti cəhdləri dayandırmaq üçün həmin İP-ni müəyyən müddətə bloklamalıdır [6].

File inclusion attacks (Fayl daxiletmə hücumları)

Fayl daxil edilməsi hücumu, istifadəçilərə istəmədən veb server daxilində və ya xaricində tələb olunan fayllara daxil olmağa və onları veb proqram tərəfindən icra etməyə imkan verən hücum növüdür. Fayl daxiletmə hücumlarının iki növü mümkündür: yerli fayl daxil edilməsi (LFI- Local File Inclusion) və ya uzaq fayl daxil edilməsi (RFI- Remote File Inclusion). Hər iki növ hücumunda zərərli şəxs vacib faylları oxuya, daha həssas məlumatlara daxil ola və ya ixtiyari əmrlər işlədə bilər. Fayl daxiletmə hücumlar infeksiya hücumlarının daha geniş sinifinin bir hissəsidir. Buraya SQL enjeksiyonları (SQLi), saytlar arası skript (XSS) və skript daxiletmə hücumları daxildir. Məzmun Təhlükəsizliyi Siyasəti (CSP) və Set-Cookie kimi HTTP cavab başlıqları WordPress veb saytınıza fayl daxil edilməsinə və digər inyeksiya hücumlarına qarşı müdafiə təmin edə bilər.

Fayl daxiletmə zəifliklərı riskini aradan qaldırmaq və ya minimuma endirmək üçün aşağıdakı addımlar tövsiyə olunur:

-Düzgün girişin yoxlanılması və təmizlənməsi

-Zəifliklər üçün proqramları müntəzəm olaraq skan edin.

-Qara siyahıya yanaşma: məlum olan təcavüzkarların və zərərli URL-lərin, həmçinin saytınıza və ya serverinizə sızmağa cəhd edənlərin müəyyən edilməsi və bloklanması.

-Kodda təhlükəsizlik boşluqlarını müəyyən etmək üçün kodun nəzərdən keçirilməsinə diqqət etmək lazımdır [18].

Content security policy - Məzmun Təhlükəsizliyi Siyasəti (CSP) veb proqramlarında istifadə olunan təhlükəsizlik mexanizmidir. Məqsədi veb-səhifələrin məzmununun dəqiqlik, etibarlılıq və təhlükəsizlik baxımından qorunmasını təmin etməkdir. CSP veb saytın və ya tətbiqin brauzerə ötürdüyü HTTP başlıq sahəsidir. Bu başlıq brauzerə səhifənin hansı mənbələrə daxil ola biləcəyini və hansı mənbələrdən yüklənməsinə icazə verilməli olduğunu bildirir. Resurslara JavaScript və CSS faylları, şəkillər, videolar, iframe-lər və xaricdən yüklənmiş digər məzmun daxil ola bilər. Əsas

məqsəd Cross-Site Scripting (XSS), clickjacking, məlumat itkisi kimi ümumi veb zəifliklərin qarşısını almaqdır. Bu cür boşluqlar zərər verən şəxsə veb-səhifənin məzmunundan istifadə etməyə və ya istifadəçinin brauzerində zərərli kod aktiv etməyə imkan verə bilər. Konfiqurasiyası veb proqramçıları tərəfindən edilir və sonra veb server tərəfindən brauzerə göndərilir. CSP siyasətlərinə müəyyən edilmiş mənbələr üçün icazələrin təyin olunması, məlumat yükləmələrinə nəzarət, eval () və daxili skriptlərin məhdudiyyət qoyulması kimi müxtəlif təhlükəsizlik prosedurları daxil edilə bilər. Məzmun Təhlükəsizliyi Siyasəti brauzerlərdə dəstəklənən təhlükəsizlik mexanizmlərindən biridir və müasir brauzerlər tərəfindən geniş formada dəstəklənir. Konfiqurasiya düzgün formada edilmiş CSP veb tətbiqinin təhlükəsizliyini artıra və ola biləcək hücumlara qarşı effektiv bir vasitə ola bilər (şəkil 4.1).

Şəkil 4. 1. Məzmun Təhlükəsizliyi Siyasəti

Aşağıda göstərilən idarəetmə sahələrində mənbə istifadəsini bloklaya və tənzimləyə bilərik.

- child-src: Deprecated olan frame-src yerinə tətbiq edilir. Veb-səhifəyə qoyulacaq frame-lərin əldə edə biləcəyi resurs dəyərlərini müəyyənləşdirir. Veb-səhifəni Frame Injection təhdidlərindən qorumaq üçün əlavə bir nümunə olaraq tətbiq edə bilərik.
- connect-src: XHR, VebSockets, EventSource ilə bağlı olan resursları bloklayır.
- font-src: Şriftlərin yüklənə resusrları təyin edir və təhdid olanda bloklayır.

- img-src: Şəkillərin yüklənə biləcəyi resusrları təyin edir və təhdid olanda bloklayır.
- media-src: Video və səsin yüklənə biləcəyi resusrları təyin edir və təhdid olanda bloklayır.
- report-uri: Məzmun Təhlükəsizliyi Siyasəti pozulduğu təqdirdə hesabat göndəriləcək ünvanı təyin edilir [13].

Beləliklə bu fəsildə veb hücumlarının şəbəkələrə təhlükə yarada biləcəyi və bu hücumlara qarşı hansı təhlükəsizlik tədbirlərinin gözləndiyini təhlil edir. Fəsilin fərqli hissələrində, veb hücumlarının şəbəkəyə təsirini və informasiya təhlükəsizliyinə olan təhlükələri əhatə edir. Bu hücumlar, şəbəkə infrastrukturlarında mövcud olan zəifliklərdən istifadə edərək məlumatların oğurlanması, şəbəkənin təxribat altına alınması və xidmətlərin mənimsənilməsi kimi təhlükələrə səbəb ola bilər.

Həmçinin bu fəsildə, Azərbaycan Texniki Universitetinin şəbəkəsinə olan veb hücumlarına və bu hücumlara qarşı təhlükəsizlik tədbirlərinin gözləndiyinə dair konkret nümunələr və tədqiqatlar təqdim olunur. Bu, universitetin informasiya təhlükəsizliyini təmin etmək üçün hansı tədbirlərin gözləndiyini, hücumları qarşılama və cəzalandırma strategiyalarını, güclü parol tələbləri və şifrələmə alqoritmlərini əhatə edir.

AZƏRBAYCAN RESPUBLİKASI ELM və TƏHSİL NAZİRLİYİ
AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əlyazması hüququnda

MƏMMƏDZADƏ KƏRİM XƏLİYƏDDİN oğlu

AzTU-nun kompüter şəbəkəsində informasiya təhlükəsizliyinin qiymətləndirilməsi sisteminin işlənməsi

mövzusunda

MAGİSTRLİK DİSSERTASİYASI

İxtisas: 060631- " Kompüter mühəndisliyi"
İxtisaslaşma: "Biliklərin əldə edilməsi sistemləri"

Elmi rəhbər: **t.f.d., dosent C. Məmmədov**

BAKI - 2023

V FƏSİL. AZTUSECURİTY-ANALYZER SYSTEM (ASAS) PROQRAMININ TƏTBİQİ VASİTƏSİLƏ ŞƏBƏKƏYƏ OLAN HÜCUMLARIN ANALİZİ VƏ İNFORMASİYA TƏHLÜKƏSİZLİYİNİN QİYMƏTLƏNDİRİLMƏSİ SİSTEMİNİN İŞLƏNMƏSİ

5.1. AzTUsecurity-analyzer system (ASAS) proqram təminatı və onun tətbiqi xüsusiyyətləri

AzTUSecurity-Analyzer System (ASAS) tətbiqi spesifik olaraq cari dissertasiya mövzusu üçün dizaynı verilmiş, strukturu qurulmuş,sıfırdan hazırlanmışdır. Tətbiqin əsas məqsədi dissertasiya işinin mövzusunu, nəticəsini, hədəflərini, məqsədlərini dəstəkləmək, reallaşdırma ehtiyacı duyularsa, gerçək məlumatlar və sistemlə əlaqələndirilərək həyata keçirməkdir.

ASAS tətbiqi Android platforması üçün Kotlin proqramlaşdırma dili və XML(Extensible Markup Language) dilindən istifadə edərək hazırlanmışdır.

Tətbiqin funksionallıqları aşağıdakılardır:

- Mail və şifrə ilə daxil olma;
- Biometrik vasitələrlə daxil olma(əgər cihaz dəstəkləyirsə göz və ya barmaq izi);
- Mail vasitəsilə şifrə yeniləmə;
- Tətbiq daxilində sistem işçiləri ilə əlaqə yaradaraq təhlükəsiz xəbərləşmə;
- Bu gündən keçmişə doğru sistemə qarşı baş vermiş və ya cəhd edilmiş hücumların qrafiki;
- Bu gündən keçmişə doğru sistemə qarşı baş vermiş və ya cəhd edilmiş hücumların təsviri;

- Bu gündən keçmişə doğru sistemə qarşı baş vermiş və ya cəhd edilmiş hücumların məlumatları;
- Cari anda sistemin vəziyyətinin təsviri;
- Cari anda baş verən və təyin oluna bilən hücumun təsviri;
- Cari anda baş verən və təyin oluna bilən hücumun məlumatları;
- Cari anda baş verən və təyin oluna bilən hücuma qarşı görülə biləcək tədbirlərin qısa yolla və mobil formada tətbiq olunması.

ASAS tətbiqetməsinin hazırlanmasında istifadə olunan texnologiyalar aşağıdakılardır:

- Kotlin Core -KTX(1.7.0) ;
- KOİN-Dependency İnjection;
- MVVM strukturu;
- Kotlin Navigation;
- Kotlin serialization;
- OkHTTP/Retrofit;
- Kotlin Coroutines/Flows.

ASAS tətbiqetməsinin platformu və yazılma dili haqqında - Kotlin, ənənəvi olaraq Android inkişafı üçün istifadə olunan bir dil olan Java-nın bəzi çatışmazlıqlarını aradan qaldırmaq üçün hazırlanmış müasir bir proqramlaşdırma dilidir. Kotlin Java-dan daha qısadır, yəni eyni funksiyanı yerinə yetirmək üçün daha az kod tələb olunur. Bu, inkişafı sürətləndirə və səhv ehtimalını azalda bilər. Bundan əlavə, Kotlin, sıfır göstərici istisnaları kimi ümumi proqramlaşdırma səhvlərinin qarşısını almağa kömək edə biləcək bir sıra təhlükəsizlik xüsusiyyətlərinə malikdir. Kotlin ayrıca Java ilə əla uyğunluğa malikdir, yəni heç bir problem olmadan Android layihələrində Java ilə birlikdə istifadə edilə bilər.

Android, smartfonlar, planşetlər və hətta bəzi televizorlar və geyilə bilən cihazlar da daxil olmaqla geniş çeşidli cihazlarda istifadə olunan Google tərəfindən hazırlanmış

açıq mənbəli əməliyyat sistemidir. Android, proqramçılara istifadəçi interfeysi elementləri, saxlama seçimləri və şəbəkə imkanları daxil olmaqla mobil tətbiqetmələr yaratmaq üçün tam bir vasitə və API (Application Package İnstaller) təqdim edir. Bundan əlavə, Android istifadəçi məlumatlarını və cihazlarını zərərli proqramlardan qorumağa kömək edən möhkəm bir təhlükəsizlik modeli təklif edir.Kotlin, JetBrains tərəfindən hazırlanmış və Java-dan daha qısa, ifadəli və təhlükəsiz olması üçün hazırlanmış bir proqramlaşdırma dilidir. Kotlin Java ilə tam uyğundur, yəni Android tətbiqetmələrini inkişaf etdirərkən Java ilə birlikdə istifadə edilə bilər. Android üçün inkişafın əsas üstünlüklərindən biri platformanın təklif etdiyi böyük auditoriyadır. Android dünyada milyardlarla insan tərəfindən istifadə olunur, yəni inkişaf etdirdiyiniz hər hansı bir tətbiq üçün böyük bir potensial bazar var. Bundan əlavə, açıq mənbəli Android, inkişaf etdiricilər üçün sənədlər, forumlar və kod nümunələri daxil olmaqla bir çox mənbənin olması deməkdir. Android, əsasən smartfonlar və planşetlər kimi mobil cihazlarda istifadə olunan Google tərəfindən hazırlanmış bir əməliyyat sistemidir. Android açıq mənbəli bir platformadır, yəni hər kəs mənbə koduna daxil ola və dəyişdirə bilər. Bu, Android üçün çox sayda tətbiq və vasitə yaradan inkişaf edən bir inkişaf Cəmiyyətinin yaranmasına səbəb oldu.

Nəticə olaraq Kotlin və Android-in mobil tətbiqetmələr yaratmaq üçün güclü bir birləşmə olduğunu söyləmək olar. Kotlin, yüksək keyfiyyətli Android tətbiqetmələri yaratmaq üçün Java ilə birlikdə istifadə edilə bilən müasir, qısa və təhlükəsiz bir proqramlaşdırma dili təklif edir. Bu vaxt Android, tətbiqinizi inkişaf etdirmək və geniş istifadəçi auditoriyasına yaymaq üçün hərtərəfli bir platforma təqdim edir. Mobil tətbiqetmələrin inkişafı ilə maraqlanırsınızsa, Kotlin və Android mütləq araşdırmağa dəyər [23].

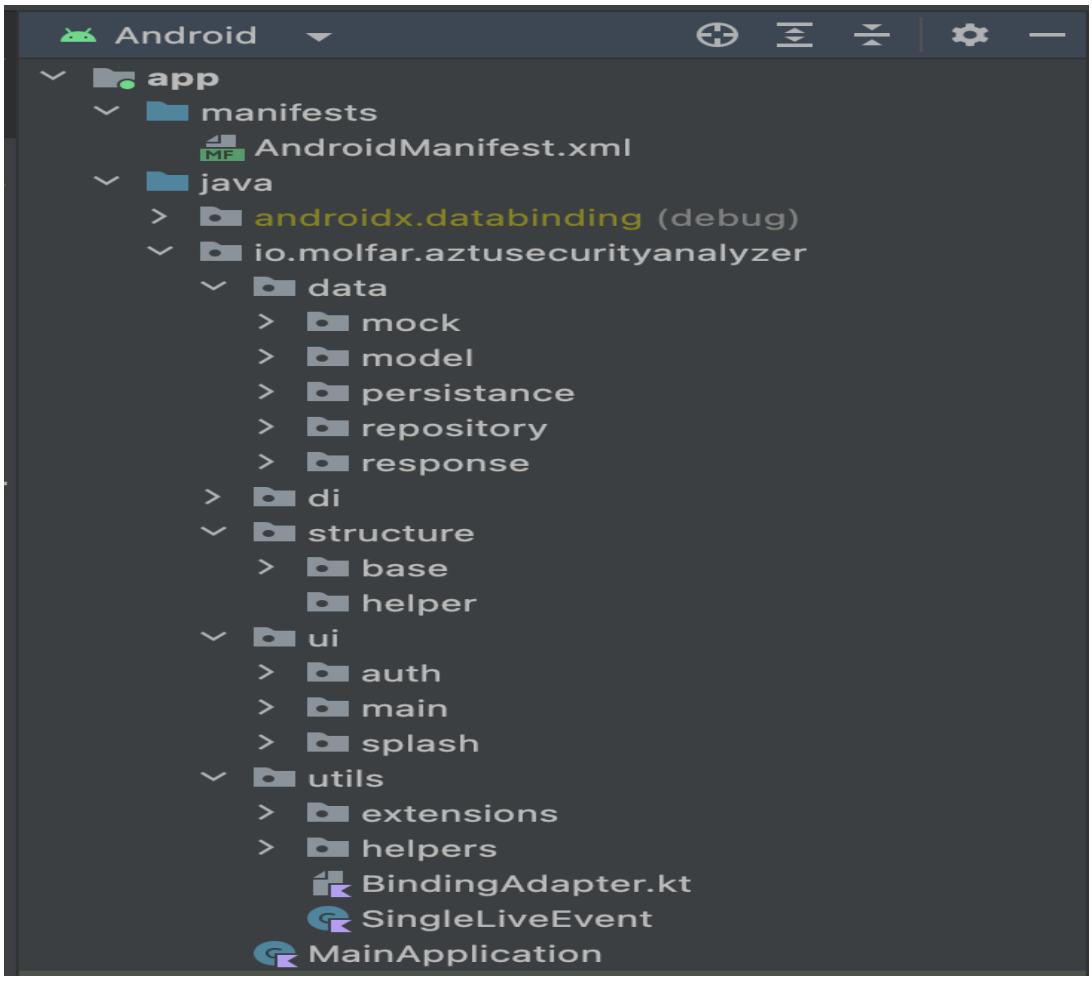
Kotlin və Android birlikdə yüksək keyfiyyətli mobil tətbiqetmələr yaratmaq üçün güclü bir birləşmədir. Qısa Kotlin sintaksisi və təhlükəsizlik xüsusiyyətləri təmiz kodu səhvsiz yazmağı asanlaşdırır, Android isə tətbiqinizi dünyada milyonlarla istifadəçiyə yaymaq və çatdırmaq üçün möhkəm platforma təqdim edir. Bir başlanğıc və ya təcrübəli

bir yazılımçı olmağınızdan asılı olmayaraq, Kotlin və Android, insanların həyatını dəyişdirə biləcək zəhmli mobil tətbiqetmələr yaratmaq üçün bir çox imkanlar təqdim edir.

ASAS tətbiqetməsinin kod dizayn strukturu MVVM- modern mobil tətbiq proyekti hazırlanmasında geniş istifadə olunan və Google tərəfindən məsləhət görülən bir design patterndir. Model-View-ViewModel təbəqələrindən ibarətdir. Tətbiq olunan model əlimizdə olan və yaxud əldə etmək istədiyimiz məlumatın,informasiyanın modelidir. View - istifadəçinin gördüyü, qarşılıqlı əlaqədə olduğu, tətbiqi istifadə etməsinə kömək edən interfeysin yansımasıdır. ViewModel - istifadəçi interfeysi və model arasında yerləşən təbəqədir. Əsasən, interfeys üçün idarəçi (controller) rolunu üstlənir. İnterfeys üçün bir istiqamətli məlumat axını, şərtlərin tətbiq olunması, əlavə etmələr - azaldılmalar bir başa və birmənalı şəkildə bu təbəqə vasitəsilə edilməlidir. Bu strukturun istifadəsinin ən önəmli müsbət cəhəti mobil cihazlarda qarşılaşdığımız ekran döndürmə və s. kimi sistem yenilənmələri və dəyişilmələri zamanı əldə olan cari məlumatın itməməsini təmin etməsidir. ASAS tətbiqetməsinin qovluq ayrılması, təbəqə bölünməsi şəkildəki kimidir.

5.2. Proqram təminatının mənbə kodu (source code) və izahı

Məlumat (data), interfeys (ui) kodlarının yerləşməsini və qovluğunu ayırmaq, habelə köməkçi kodların və əsas siniflərin fərqli yerləşdirilməsi təmiz və düzgün proyekt hazır edilməsi üçün zəruridir (şəkil 5.1) [24].



Şəkil 5. 1. Qovluq sturukturu

Proyektin giriş nöqtəsi- Main Application

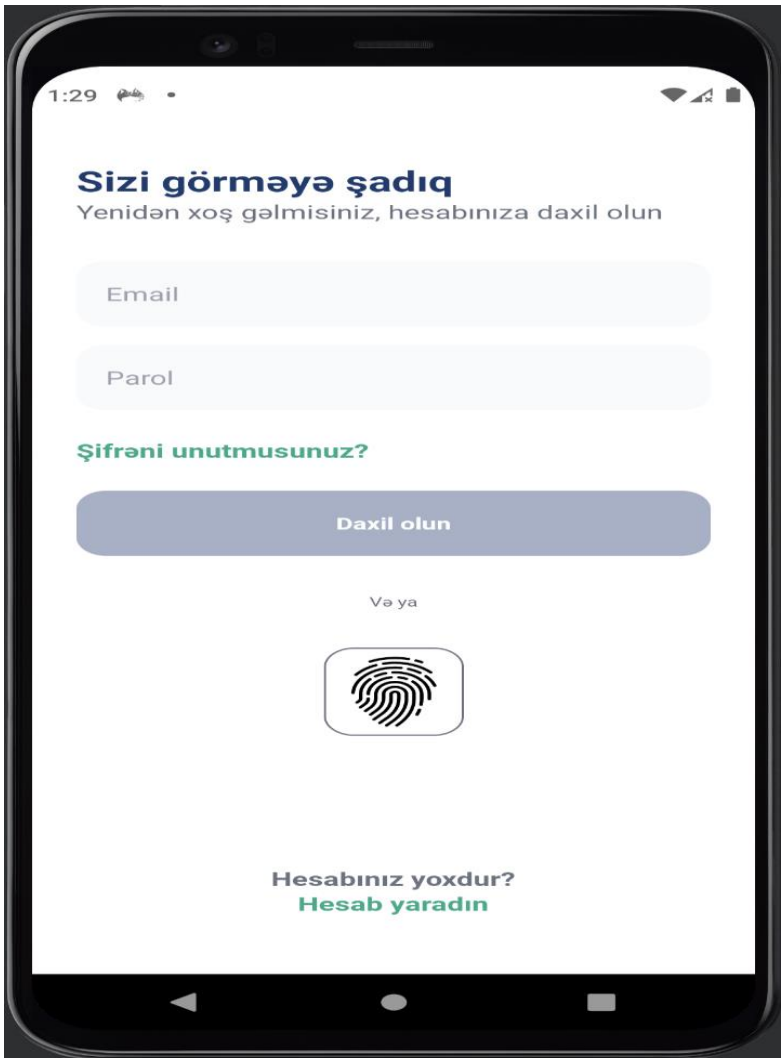
```
class MainApplication : Application() {
  override fun onCreate() {
        super.onCreate()
        startKoin {
            androidLogger(Level.DEBUG)
            androidContext(this@MainApplication)
            androidFileProperties()
            modules(listOf(AppModule.appModule))
        }
        val sharedPrefHelper = SharedPrefHelper(this)
        if (sharedPrefHelper.usersList == null) {
            sharedPrefHelper.usersList = Json.encodeToString(users)
```

```
        }
    }
```

Proyektin giriş nöqtəsi Application () sinifindən varislik alan MainApplication sinfidir. Bu proyekt yani tətbiqetmə işə düşdüyü zaman ilk işləyən kod parçasıdır. Ənənəyə sadiq qalaraq başlanğıcda Koin texnologiyası sistemə qoşulur, və lazımlı sinifləri öncədən hazırlayaraq, istifadəyə hazır formaya gətirir. SharedPreferHelper adlı sinif ASAS tətbiqetməsi üçün lokal keş məlumat qovluğu rolunu görür.

```
class SharedPrefHelper(context: Context) {
    companion object {
        private const val PREF_NAME = "asa_preferences"
        private const val IS_USER_LOGGED_IN = "is_user_logged_in"
        private const val LOGGED_USER_MAIL = "logged_user_mail"
        private const val USERS_LIST = "users_list"
    }
    private val sharedPreferences = context.getSharedPreferences(PREF_NAME, Context.MODE_PRIVATE)
    var isUserLoggedIn: Boolean
        get() = sharedPreferences.getBoolean(IS_USER_LOGGED_IN, false)
        set(value) = sharedPreferences.putBoolean(IS_USER_LOGGED_IN, value)
    var usersList:String?
        get() = sharedPreferences.getString(USERS_LIST, null)
        set(value) = sharedPreferences.putString(USERS_LIST, value)
    var loggedUserMail:String?
        get() = sharedPreferences.getString(LOGGED_USER_MAIL, null)
        set(value) = sharedPreferences.putString(LOGGED_USER_MAIL, value)
    fun clearSharedPref() = sharedPreferences.clearPreferences()
}
```

Tətbiqetmənin istifadəsi zamanı yadda saxlanılmalı olan və eyni zamanda internet əlaqəsinin qeyri-zəruri olduğu məlumatlar Android platforması tərəfindən istifadəyə verilən SharedPreferences adlı baza tərkibində saxlanılır.

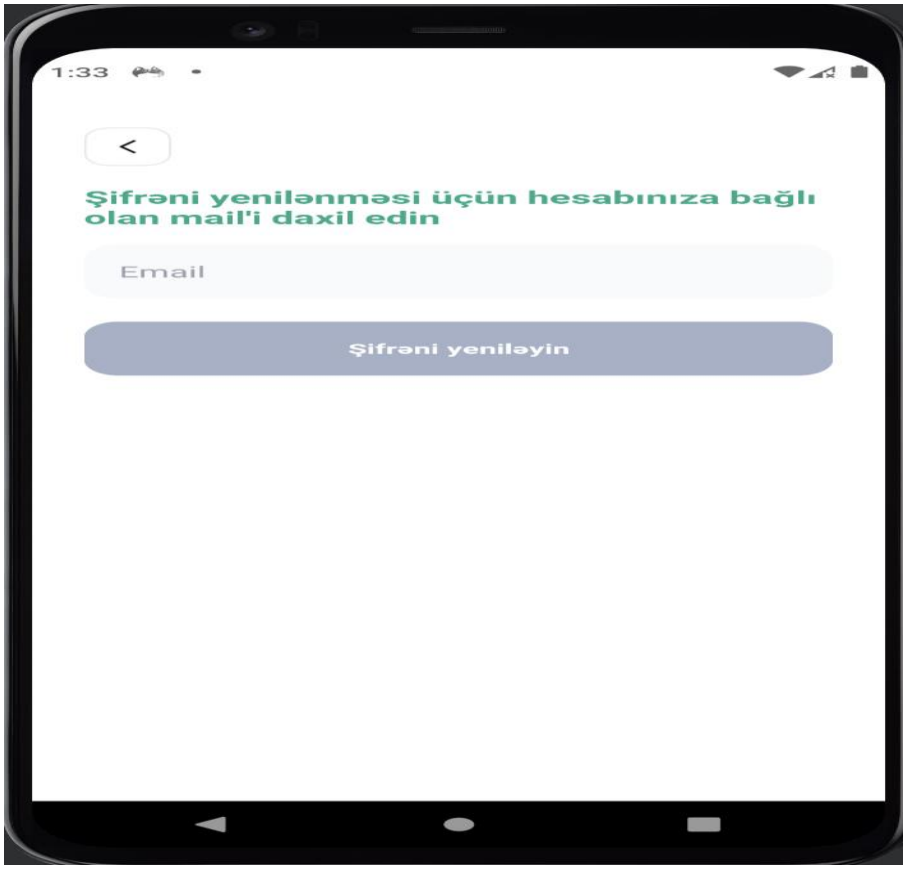


Şəkil 5. 2. Qarşılama interfeysi- Login fragment

ASAS tətbiqetməsinin istifadəçini qarşıladığı ilk interfeys LoginFragmentdir. Burada istifadəçinin sistemə və tətbiqə təhlükəsiz şəkildə daxil olması təmin olunur. Email və şifrəni daxil edərək sistemə daxil olma və ya biometrik vasitələrlə sistemə daxil olmaq imkanı mövcuddur. Şifrəni yeniləmək lazım olduqda ara interfeys olan şifrə yeniləmə interfeysinə keçid üçün tekst butonu yerləşdirilmişdir (şəkil 5.2) [25].

```
class LoginFragment : BaseFragment() {
    private val viewModel: LoginViewModel by viewModel()
    private val binding: FragmentLoginBinding by lazy {
        FragmentLoginBinding.inflate(layoutInflater).apply {
            lifecycleOwner = this@LoginFragment
            viewModel = this@LoginFragment.viewModel
            executePendingBindings()
        }
    }
    override fun onCreateView(
        inflater: LayoutInflater,
        container: ViewGroup?,
        savedInstanceState: Bundle?
    ): View {
        binding.forgotPasswordText.setOnClickListener {
            findNavController().navigate(
                LoginFragmentDirections.toForgotpassFragment(),
                getNavOptions()
            )
        }
        binding.signupLayout.setOnClickListener {
            findNavController().navigate(
                LoginFragmentDirections.toRegisterFragment(),
                getNavOptions()
            )
        }
        viewModel.successFullLogin.observe(viewLifecycleOwner) {
            val intent = Intent(requireActivity(),
MainActivity::class.java)
            intent.flags = Intent.FLAG_ACTIVITY_NEW_TASK or
Intent.FLAG_ACTIVITY_CLEAR_TASK
            startActivity(intent)
```

```
                requireActivity().finish()
            }
            viewModel.showError.observe(viewLifecycleOwner) {
                it?.let {
                    Toast.makeText(requireContext(), it,
Toast.LENGTH_SHORT).show()
                }
            }
            return binding.root
        }
    }
```



Şəkil 5. 3. Şifrə yeniləmə interfeysi

Cari interfeys vasitəsilə istifadəçi istəyərsə qeydiyyatda olan poçtuna yenilənmə üçün istək göndərə bilər (şəkil 5.3).

```
class ForgotPassFragment : BaseFragment() {
    private val viewModel: ForgotPassViewModel by viewModel()
```

```
        private val binding: FragmentForgotpassBinding by lazy {
            FragmentForgotpassBinding.inflate(layoutInflater).apply {
                lifecycleOwner = this@ForgotPassFragment
                viewModel = this@ForgotPassFragment.viewModel
                executePendingBindings()
            }
        }
        override fun onCreateView(
            inflater: LayoutInflater,
            container: ViewGroup?,
            savedInstanceState: Bundle?
        ): View {
            binding.backButton.setOnClickListener {
                findNavController().popBackStack()
            }
            viewModel.messageSent.observe(viewLifecycleOwner) {
                Toast.makeText(requireContext(),
getString(R.string.pass_recover), Toast.LENGTH_SHORT)
                    .show()
            }
            return binding.root
        }
```

Şifrə yeniləmə interfeysinin şərt və dəyişmələrini, məlumat göndərmə və çağırma funksiyalarını özündə saxlayan Controller sinfinin məlumatları bu formada tərtib edilir.

Val mailEtBackground = MutableLiveData<Drawable>(resourcesHelper.getDrawable(R.drawable.*unfilled_et_bg*)
)

```
        val mailEtText = MutableLiveData<String>()
        val isResetPassValid = MutableLiveData<Boolean>(false)
        val loadingState = MutableLiveData(false)
        val messageSent = SingleLiveEvent<Unit>()
```

```
        fun onMailTextChanged(it: Editable?) {
            mailEtText.value = it.toString()
            mailEtBackground.value =
                if (it?.isNotEmpty() == true &&
it.toString().isValidEmail()) {
                    resourcesHelper.getDrawable(R.drawable.filled_et_bg)
                } else {
                    resourcesHelper.getDrawable(R.drawable.unfilled_et_bg)
                }
            checkIfForgotPassValid()
        }
        private fun checkIfForgotPassValid() {
            isResetPassValid.value =
                (!mailEtText.value.isNullOrEmpty() &&
mailEtText.value.toString().isValidEmail())
        }
        fun onResetPassBtnClick() {
            if (isResetPassValid.value == true) {
                viewModelScope.launch {
                    loadingState.value = true
                    delay(2000)
                    loadingState.value = false
                    messageSent.value = Unit
                }
            }
        }
        private fun String?.isValidEmail() =
            !isNullOrEmpty() &&
Patterns.EMAIL_ADDRESS.matcher(this).matches()
    }
```

Əgər istifadəçinin hal hazırda qeydiyyatda olan bir profili yoxdursa,

qeydiyyatdan keçmə-registrasiya interfeysinə yönələrək özünə hesab yarada bilər (şəkil 5.4).

Şəkil 5. 4. Proqram təminatında istifadəçi hesabının yaradılması

```
class RegisterFragment : BaseFragment() {
    private val viewModel: RegisterViewModel by viewModel()
    private val binding: FragmentRegisterBinding by lazy {
        FragmentRegisterBinding.inflate(layoutInflater).apply {
            lifecycleOwner = this@RegisterFragment
            viewModel = this@RegisterFragment.viewModel
            executePendingBindings()
        }
    }

    override fun onCreateView(
        inflater: LayoutInflater,
        container: ViewGroup?,
        savedInstanceState: Bundle?
    ): View {
```

```
            binding.backButton.setOnClickListener {
                findNavController().popBackStack()
            }
            binding.signinLayout.setOnClickListener {
                findNavController().popBackStack()
            }
            viewModel.successFullLogin.observe(viewLifecycleOwner) {
                val intent = Intent(requireActivity(),
MainActivity::class.java)
                intent.flags = Intent.FLAG_ACTIVITY_NEW_TASK or
Intent.FLAG_ACTIVITY_CLEAR_TASK
                startActivity(intent)
                requireActivity().finish()
            }
            viewModel.showError.observe(viewLifecycleOwner) {
                it?.let {
                    Toast.makeText(requireContext(), it,
Toast.LENGTH_SHORT).show()
                }
            }
            return binding.root
        }
    }
```

Təmin edilən kodlar qeydiyyat interfeysinin, interfeyslə əlaqəli olan lazimi işləri görməsi üçün zəruri olan məntiqi əməliyyatlardır. Cari interfeysin controller isə aşağıdakı kimidir:

```
class RegisterViewModel(
        private val resourcesHelper: ResourcesHelper,
        private val repository: ProjectRepository
    ) : ViewModel() {
```

```
        val fullNameEtBackground =

MutableLiveData<Drawable>(resourcesHelper.getDrawable(R.drawable.unfilled_e
t_bg))
        val mailEtBackground =

MutableLiveData<Drawable>(resourcesHelper.getDrawable(R.drawable.unfilled_e
t_bg))
        val passwordEtBackground =

MutableLiveData<Drawable>(resourcesHelper.getDrawable(R.drawable.unfilled_e
t_bg))

        val fullNameEtText = MutableLiveData<String>()
        val mailEtText = MutableLiveData<String>()
        val passwordEtText = MutableLiveData<String>()
        val isRegisterValid = MutableLiveData<Boolean>(false)
        val successFullLogin = SingleLiveEvent<Unit>()
        val showError = SingleLiveEvent<String?>()
        val loadingState = MutableLiveData(false)

        fun onFullNameTextChanged(it: Editable?) {
            fullNameEtText.value = it.toString()
            fullNameEtBackground.value =
                if (it?.isNotEmpty() == true) {
                    resourcesHelper.getDrawable(R.drawable.filled_et_bg)
                } else {
                    resourcesHelper.getDrawable(R.drawable.unfilled_et_bg)
                }
            checkIfRegisterValid()
        }
```

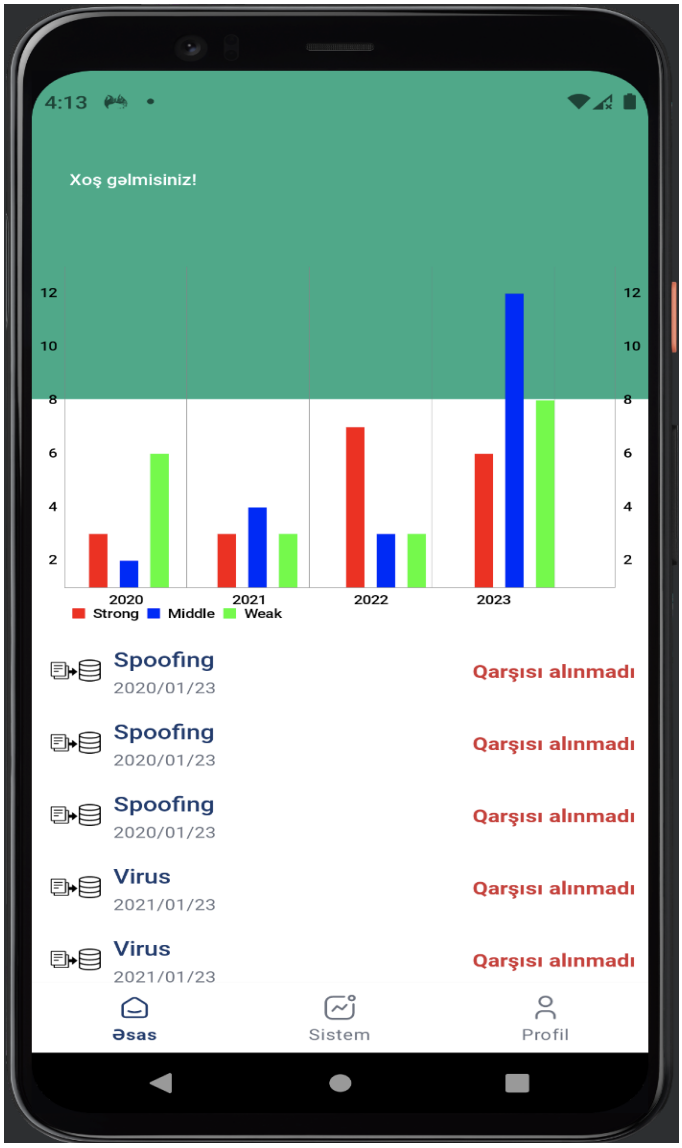
```
        fun onMailTextChanged(it: Editable?) {
            mailEtText.value = it.toString()
            mailEtBackground.value =
                if (it?.isNotEmpty() == true &&
it.toString().isValidEmail()) {
                    resourcesHelper.getDrawable(R.drawable.filled_et_bg)
                } else {
                    resourcesHelper.getDrawable(R.drawable.unfilled_et_bg)
                }
            checkIfRegisterValid()
        }
        fun onPasswordTextChanged(it: Editable?) {
            passwordEtText.value = it.toString()
            passwordEtBackground.value =
                if (it?.isNotEmpty() == true) {
                    resourcesHelper.getDrawable(R.drawable.filled_et_bg)
                } else {
                    resourcesHelper.getDrawable(R.drawable.unfilled_et_bg)
                }
            checkIfRegisterValid()
        }
        private fun checkIfRegisterValid() {
            isRegisterValid.value =
                (!passwordEtText.value.isNullOrEmpty() &&
!mailEtText.value.isNullOrEmpty() && mailEtText.value.toString()
                    .isValidEmail() &&
!fullNameEtText.value.isNullOrEmpty())
        }

        fun registerBtnClick() {
            if (isRegisterValid.value == true) {
                viewModelScope.launch {
```

```
                    loadingState.value = true
                    val registerModel =
                        RegisterModel(fullNameEtText.value,
mailEtText.value, passwordEtText.value)
                    val                 registerResponse                =
repository.registerUser(registerModel)
                    loadingState.value = false
                    if (registerResponse.data == null) {
                        showError.value = registerResponse.errorMessage
                    } else {
                        successFullLogin.value = Unit
                    }
                }
            }
        }
        private fun String?.isValidEmail() =
            !isNullOrEmpty()                                          &&
Patterns.EMAIL_ADDRESS.matcher(this).matches()
    }
```

Növbəti olaraq, uğurlu avtorizasiya əməliyyatının ardınca, tətbiqetmənin əsas səhifəsinə yönlənilir. Burada əsas səhifə,sistem səhifəsi və profil səhifəsi istifadəçini qarşılayır. Əsas səhifə bu gündən keçmişə doğru əldə olan hücumların, növü, adı, təfərrüatı, uğurlu və ya uğursuz olması, uğurlu və ya uğursuz olmasının səbəbi, tarixi, müddəti, hücumun gerçəkləşdirildiyi məkan və s. məlumatları göstərir. Eyni zamanda bu məlumatlarının toplamının, illərə və ciddiyət dərəcəsinə nəzərən, sayalara bölərək qrafik təsvirini verir.

Sistem səhifəsi cari anda baş verdiyinə ehtimal verilən və yaxud təyin olunan hücumun məlumatlarını, təfərrüatını, gerçəkləşdirilmə məkanını, adını, növünü və s. məlumatları göstərir. Əlavə olaraq bu cari hücum üçün əvvəlcədən hazırlanmış, əldə

olan sovuşdurma əməliyyatı üçün seçimlər də təsvir edir ki, onlar bir toxunma ilə məqsədlərinə çata bilirlər (şəkil 5.5).



Şəkil 5. 5. Əsas səhifənin interfeysi

Əsas səhifədə istifadə olunan hücumlar listi üçün Recyclerview komponentindən istifadə olunmuşdur. Bu komponentin düzgün işləməsi üçün Adapter modelindən istifadə olunur. Adapter modelinin işləmə prinsipi aşağıdakı kimidir. Əlaqəli Adapter sinfi təyin olunmuş tipdə məlumat və ya modelin listini qəbul edir.Qəbul etdiyi listi bəlirlənmiş interfeys üzrə dövr operatoru şəklində hər bir modeli sıra ilə ilk öncə interfeysə təyin edir sonrasında isə lazımı əməliyyatları, yani gələcəyə doğru gözlənməsi

ehtimal olunan əməliyyatları interfeyslə əlaqələndirir və bunu list şəklində interfeysdə əks etdirir. Adapter sinfinin işlənməsi üçün zəruri kodlar belədir:

```
class AttacksAdapter(private val clickListener: (Attack) -> Unit) :
    ListAdapter<Attack, AttacksAdapter.AttackViewHolder>(Companion) {
    companion object : DiffUtil.ItemCallback<Attack>() {
        override fun areItemsTheSame(
            oldItem: Attack,
            newItem: Attack,
        ): Boolean =
            oldItem == newItem

        override fun areContentsTheSame(
            oldItem: Attack,
            newItem: Attack,
        ): Boolean =
            oldItem == newItem
    }

    class AttackViewHolder(val binding: ListItemAttackBinding) :
        RecyclerView.ViewHolder(binding.root)
    override fun onCreateViewHolder(parent: ViewGroup, viewType: Int):
AttackViewHolder {
        val layoutInflater = LayoutInflater.from(parent.context)
        val  binding  =  ListItemAttackBinding.inflate(layoutInflater,
parent, false)
        return AttackViewHolder(binding)
    }
    override  fun  onBindViewHolder(holder:  AttackViewHolder,  position:
Int) {
        val model = getItem(position)
        holder.binding.model = model
```

```
            holder.binding.executePendingBindings()
            holder.binding.root.setOnClickListener {
                clickListener.invoke(model)
            }
        }
```

Əsas səhifə interfeysinin interfeyslə əlaqəli kodları, işləməsi, qrafikin çəkilməsi,hücumlar listinin düzgün əlaqəli və performans problemləri yaşamadan işləməsi üçün istifadə olunan kodlar bunlardır.

```
class HomeFragment : BaseFragment() {
    private val viewModel: HomeViewModel by viewModel()
    private val binding: FragmentHomeBinding by lazy {
        FragmentHomeBinding.inflate(layoutInflater).apply {
            lifecycleOwner = this@HomeFragment
            executePendingBindings()
        }
    }
    override fun onCreateView(
        inflater: LayoutInflater,
        container: ViewGroup?,
        savedInstanceState: Bundle?
    ): View {
        binding.attacksRv.bindRecyclerViewAdapter(viewModel.adapter)
        setBarChart()
        listenAttackClickEvents()
        return binding.root
    }

    private fun listenAttackClickEvents() {
        viewModel.showAttackDetail.observe(viewLifecycleOwner){
            showAttackDialog(it)
        }
```

```
        }

        private fun showAttackDialog(attack: Attack?) {
            val dialog = Dialog(requireActivity(), R.style.Theme_Dialog)
            dialog.requestWindowFeature(Window.FEATURE_NO_TITLE)
            val dialogBinding: DialogAttackInfoBinding =
                DataBindingUtil.inflate(
                    LayoutInflater.from(dialog.context),
                    R.layout.dialog_attack_info,
                    null,
                    false
                )
            dialogBinding.lifecycleOwner = this
            dialog.setContentView(dialogBinding.root)
            dialogBinding.model=attack
            dialog.show()

        }


        private fun setBarChart() {
            val data =
                BarData(getFirstMainTypeBarSet(),
getSecondMainTypeBarSet(), getThirdMainTypeBarSet())
            binding.chart.data = data
            data.barWidth = 0.15f
            binding.chart.setVisualProperties()
            val barSpace = 0.1f
            val groupSpace = 0.3f
            binding.chart.setVisibleXRangeMaximum(
                binding.chart.barData.getGroupWidth(
                    groupSpace,
```

```
                barSpace
            ) * 12
        )
        binding.chart.groupBars(0f, groupSpace, barSpace)
    }

    override fun onResume() {
        super.onResume()
        requireActivity().window.statusBarColor =
requireContext().getColor(R.color.splash_green)
    }

    private fun prepareFirstMainTypeDatas(): ArrayList<BarEntry> {
        val barEntries = ArrayList<BarEntry>()
        val firstYearCount = viewModel.firstTypeAttacks.count {
it.date.year == "2020" }
        val secondYearCount = viewModel.firstTypeAttacks.count {
it.date.year == "2021" }
        val thirdYearCount = viewModel.firstTypeAttacks.count {
it.date.year == "2022" }
        val fourthYearCount = viewModel.firstTypeAttacks.count {
it.date.year == "2023" }
        barEntries.add(BarEntry(1f, firstYearCount.toFloat()))
        barEntries.add(BarEntry(2f, secondYearCount.toFloat()))
        barEntries.add(BarEntry(3f, thirdYearCount.toFloat()))
        barEntries.add(BarEntry(4f, fourthYearCount.toFloat()))
        return barEntries
    }

    private fun prepareSeondMainTypeDatas(): ArrayList<BarEntry> {
        val barEntries = ArrayList<BarEntry>()
```

```
            val   firstYearCount   =   viewModel.secondTypeAttacks.count   {
it.date.year == "2020" }
            val   secondYearCount   =   viewModel.secondTypeAttacks.count   {
it.date.year == "2021" }
            val   thirdYearCount   =   viewModel.secondTypeAttacks.count   {
it.date.year == "2022" }
            val   fourthYearCount   =   viewModel.secondTypeAttacks.count   {
it.date.year == "2023" }
            barEntries.add(BarEntry(1f, firstYearCount.toFloat()))
            barEntries.add(BarEntry(2f, secondYearCount.toFloat()))
            barEntries.add(BarEntry(3f, thirdYearCount.toFloat()))
            barEntries.add(BarEntry(4f, fourthYearCount.toFloat()))
            return barEntries
        }

        private fun prepareThirdMainTypeDatas(): ArrayList<BarEntry> {
            val barEntries = ArrayList<BarEntry>()
            val   firstYearCount   =   viewModel.thirdTypeAttacks.count   {
it.date.year == "2020" }
            val   secondYearCount   =   viewModel.thirdTypeAttacks.count   {
it.date.year == "2021" }
            val   thirdYearCount   =   viewModel.thirdTypeAttacks.count   {
it.date.year == "2022" }
            val   fourthYearCount   =   viewModel.thirdTypeAttacks.count   {
it.date.year == "2023" }
            barEntries.add(BarEntry(1f, firstYearCount.toFloat()))
            barEntries.add(BarEntry(2f, secondYearCount.toFloat()))
            barEntries.add(BarEntry(3f, thirdYearCount.toFloat()))
            barEntries.add(BarEntry(4f, fourthYearCount.toFloat()))
            return barEntries
        }
        private fun getThirdMainTypeBarSet(): BarDataSet {
```

```
            val   barDataSet3   =   BarDataSet(prepareThirdMainTypeDatas(),
"Weak")
            barDataSet3.color = Color.GREEN
            barDataSet3.valueFormatter = object : ValueFormatter() {
                override fun getBarLabel(barEntry: BarEntry?): String {
                    return ""
                }
                override fun getAxisLabel(value: Float, axis: AxisBase?):
String {
                    axis?.typeface                                          =
ResourcesCompat.getFont(requireContext(), R.font.roboto_medium)
                    return super.getAxisLabel(value, axis)
                }
            }
            return barDataSet3
        }
        private fun getSecondMainTypeBarSet(): BarDataSet {
            val   barDataSet2   =   BarDataSet(prepareSeondMainTypeDatas(),
"Middle")
            barDataSet2.color = Color.BLUE
            barDataSet2.valueFormatter = object : ValueFormatter() {
                override fun getBarLabel(barEntry: BarEntry?): String {
                    return ""
                }
                override fun getAxisLabel(value: Float, axis: AxisBase?):
String {
                    axis?.typeface                                          =
ResourcesCompat.getFont(requireContext(), R.font.roboto_medium)
                    return super.getAxisLabel(value, axis)
                }
            }
            return barDataSet2
```

```
        }

        private fun getFirstMainTypeBarSet(): BarDataSet {
            val   barDataSet1   =   BarDataSet(prepareFirstMainTypeDatas(),
"Strong")
            barDataSet1.color = Color.RED
            barDataSet1.valueFormatter = object : ValueFormatter() {
                override fun getBarLabel(barEntry: BarEntry?): String {
                    return ""
                }

                override fun getAxisLabel(value: Float, axis: AxisBase?):
String {
                    axis?.typeface                                          =
ResourcesCompat.getFont(requireContext(), R.font.roboto_medium)
                    return super.getAxisLabel(value, axis)
                }
            }
            return barDataSet1
        }

        private val years = arrayOf("2020", "2021", "2022", "2023")

        private fun BarChart.setVisualProperties() {
            val  robotoMedium  =  ResourcesCompat.getFont(requireContext(),
R.font.roboto_medium)
            with(this) {
                axisLeft.setDrawGridLines(false);
                axisRight.setDrawGridLines(false);
                description.isEnabled = false
                setPinchZoom(false)
                isDragEnabled = false
```

```
                setVisibleXRangeMaximum(12f)
                setDrawGridBackground(false)
                with(xAxis) {
                    axisMinimum = 0f
                    valueFormatter = IndexAxisValueFormatter(years)
                    setCenterAxisLabels(true)
                    position = XAxis.XAxisPosition.BOTTOM
                    granularity = 1f
                    isGranularityEnabled = true
                    typeface = robotoMedium
                }
                axisLeft.typeface = robotoMedium
                axisRight.typeface = robotoMedium
                legend.typeface = robotoMedium
                moveViewToX(binding.chart.barData.xMax)
                animateY(2000)
            }
        }
    }
```

List formasında əks olunan hücumlar toplusunun istənilən birinə toxunduqda, əlavə interfeys açılır və seçilmiş hücum haqqında təfərrüatlı məlumat göstərilir

Vizuallaşdırma üçün lazım olan məlumatın əldə edilməsi üçün istifadə olunan metod REST APİ-dir (Representational Transfer Protocol). Json formatında məlumat götürülür və lazımı formada,uyğun gələn model və tiplərə nəzərən formatlanaraq düzgün növ əldə edilir. Bu əldə olunmuş model və məlumat qrafikə tətbiq olunur. Təqribi uyğun olan json formatı bu şəkildədir.

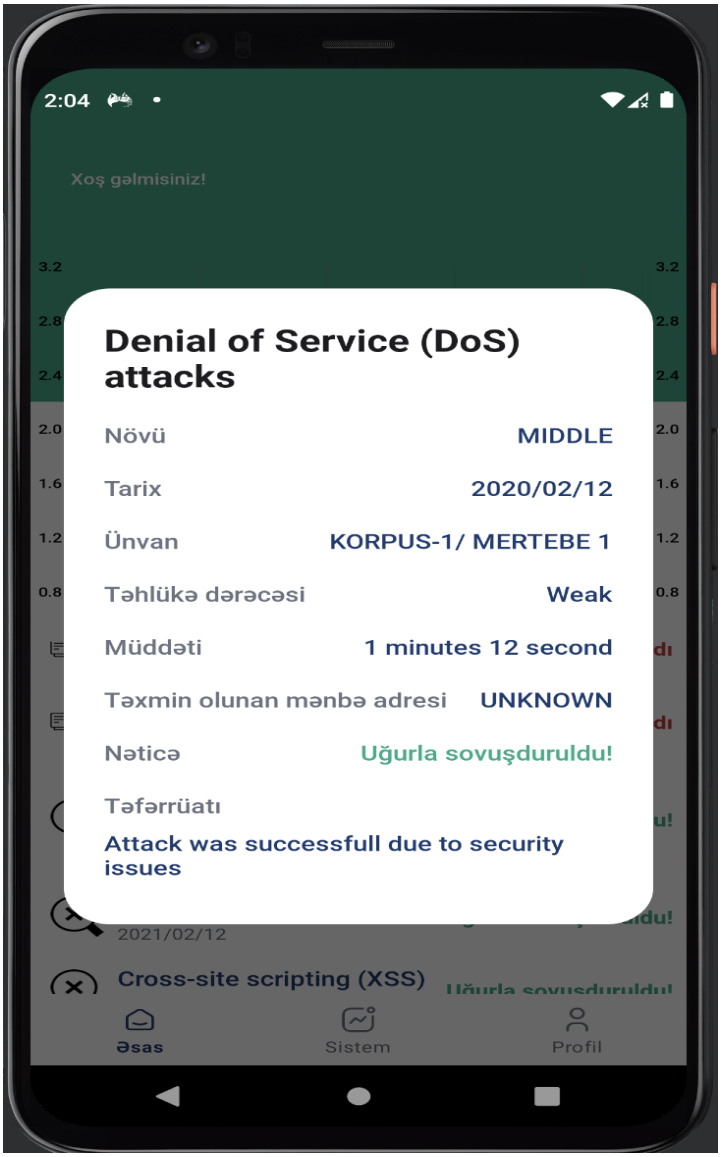
```
[
{
  "strongAttack": {
    "attackLocation": "KORPUS-3/ Mertebe-4",
    "date": {
```

```
            "day": "23",
            "month": "01",
            "year": "2020"
          },
          "duration": "3 minutes 43 second",
          "estimatedAttackLocation": "Zimbabve",
          "name": "Spoofing",
          "resultDescription": "Attack avoided by server firewall",
          "threatLevel": "Strong",
          "type": "STRONG",
          "wasSuccesfull": false
        }
      },
      {
        "middleAttack": {
          "attackLocation": "KORPUS-1/ MERTEBE 1",
          "date": {
            "day": "12",
            "month": "02",
            "year": "2020"
          },
          "duration": "1 minutes 12 second",
          "estimatedAttackLocation": "UNKNOWN",
          "name": "Denial of Service (DoS) attacks",
          "resultDescription": "Attack was successfull due to security
issues",
          "threatLevel": "Weak",
          "type": "MIDDLE",
          "wasSuccesfull": true
        }
      },
      {
```

```
  "weakAttack": {
    "attackLocation": "KORPUS-7/ MERTEBE 2",
    "date": {
      "day": "01",
      "month": "03",
      "year": "2020"
    },
    "duration": "1 minutes 12 second",
    "estimatedAttackLocation": "Moscow",
    "name": "Denial of Service (DoS) attacks",
    "resultDescription": "Attack avoided by server firewall",
    "threatLevel": "Weak",
    "type": "WEAK",
    "wasSuccesfull": false
  }
},
{
  "strongAttack": {
    "attackLocation": "KORPUS-2/ MERTEBE 6",
    "date": {
      "day": "23",
      "month": "01",
      "year": "2021"
    },
    "duration": "3 minutes 43 second",
    "estimatedAttackLocation": "Zimbabve",
    "name": "Virus",
    "resultDescription": "Attack avoided by server firewall",
    "threatLevel": "Strong",
    "type": "STRONG",
    "wasSuccesfull": false
  }
```

```
}]]
```

Məlumat verilən interfeys bu şəkildədir:



Şəkil 5. 6. Əks olunan hücum növü

Növbəti interfeys ehtimal olunan və ya təyin olunan cari hücumların əks olunduğu interfeysdir.

Şəkil 5. 7. Cari hücumlar

Cari interfeysin məntiqi və yaxud interfeyslə əlaqəli iş prinsipini təmin etmək üçün yazılmış kodlar belədir.

```
class ActivityFragment : BaseFragment() {
    private val viewModel: ActivityViewModel by viewModel()
    private val binding: FragmentActivityBinding by lazy {
        FragmentActivityBinding.inflate(layoutInflater).apply {
            lifecycleOwner = this@ActivityFragment
            executePendingBindings()
        }
    }
    override fun onCreateView(
        inflater: LayoutInflater,
        container: ViewGroup?,
        savedInstanceState: Bundle?
    ): View {
```

```
binding.currentAttacksRv.bindRecyclerViewAdapter(viewModel.adapter)
    listenClickEvents()
    return binding.root
}
private fun listenClickEvents() {
    viewModel.showAttackOptions.observe(viewLifecycleOwner) {
        showAttackOptionsDialog(it)
    }
}
private fun showAttackOptionsDialog(it: CurrentAttack?) {
    val dialog = Dialog(requireActivity(), R.style.Theme_Dialog)
    dialog.requestWindowFeature(Window.FEATURE_NO_TITLE)
    val dialogBinding: DialogCurrentAttackOptionsBinding =
        DataBindingUtil.inflate(
            LayoutInflater.from(dialog.context),
            R.layout.dialog_current_attack_options,
            null,
            false
        )
    dialogBinding.lifecycleOwner = this
    dialog.setContentView(dialogBinding.root)
    dialogBinding.model = it
    dialog.show()
    dialogBinding.shutButton.text = it?.options!![0].text
    dialogBinding.restartButton.text = it.options[1].text
    if (it.options.count() == 2) {
        dialogBinding.blockButton.visibility = View.GONE
    } else {
        dialogBinding.blockButton.text = it.options[2].text
    }
    dialogBinding.blockButton.setOnClickListener {
        dialog.cancel()
```

```
            }
            dialogBinding.restartButton.setOnClickListener {
                dialog.cancel()
            }
            dialogBinding.shutButton.setOnClickListener {
                dialog.cancel()
            }
        }
        override fun onResume() {
            super.onResume()
            requireActivity().window.statusBarColor =
requireContext().getColor(R.color.white)
        }
    }
```

Növbəti və son interfeys Profil interfeysidir. Sözügedən interfeys istifadəçi məlumatlarını, tətbiqetmənin müəyyən sazlamalarını, profildən çıxış funksionallığını, sistem daxilində əlaqə qurulmuş hesablarla təhlükəsiz xəbərləşmə funksionallığına keçid funksiyasını təmin edir [23].

Profil interfeysinin düzgün və problemsiz işləməsi üçün yazılan sinif belədir. class ProfileFragment : BaseFragment() {

```
    private val viewModel: ProfileViewModel by viewModel()
     private val binding: FragmentProfileBinding by lazy {
            FragmentProfileBinding.inflate(layoutInflater).apply {
                lifecycleOwner = this@ProfileFragment
                viewModel = this@ProfileFragment.viewModel
                executePendingBindings()
            }
        }
        override fun onCreateView(
            inflater: LayoutInflater,
            container: ViewGroup?,
```

```
            savedInstanceState: Bundle?
        ): View {
            viewModel.comingSoonEvent.observe(viewLifecycleOwner) {
                Toast.makeText(requireContext(),
getString(R.string.coming_soon), Toast.LENGTH_SHORT)
                    .show()
            }
            viewModel.logOutEvent.observe(viewLifecycleOwner) {
                val intent = Intent(requireActivity(),
AuthActivity::class.java)
                intent.flags = Intent.FLAG_ACTIVITY_NEW_TASK or
Intent.FLAG_ACTIVITY_CLEAR_TASK
                startActivity(intent)
                requireActivity().finish()
            }
            return binding.root
        }
        override fun onResume() {
            super.onResume()
            requireActivity().window.statusBarColor =
requireContext().getColor(R.color.white)
        }
```

Şəkil 5. 8. Profil interfeysi

ASAS tətbiqinin təyinatı.

AzTU Security Analyzer System - məqsədi, server-sistem-təhlükəsizlik 3-lüsü ilə daim əlaqədə olaraq, cari və keçmiş vəziyyəti istifadəçiyə çatdırmaq, çatdırdığı mövhum haqda ətraflı məlumat vermək, mümkün olduğu zaman verilə biləcək qərarları məsləhət görməkdir.

Bunlardan başqa tətbiq biometrik autentifikasiya metodları ilə işləyir və əlavə olaraq poçt və şifrə cütlüyü ilə də daxil olma metodu mümkündür. Gələcək və ya növbəti hədəflərdə tətbiq daxili təhlükəsiz mesajlaşma, mesajlaşmanın daxilinə şifrələnmiş səs, media (video-şəkil-fayl və s.) və digər əlavələrin artılırılması planlanır.

Tətbiqetmənin əsas məqsədi sistem və ya planlaşdırıldığı üzrə Azərbaycan Texniki Universitetində işləyən, server-təhlükəsizlik və bənzəri kimi vəzifəsi olan bir işçinin, habelə tabe olduğu şəxslərin və ya bu məlumata sahib olmaq istəyən personalın işini asanlaşdırmaqdır.

Cari anda baş verən potensial təhlükələri bir başa mobil cihaza bildiriş kimi göndərərək, kritik və təcili anlarda gecikmədən məlumat alma, vəziyyətdən xəbərdar olma, lazımı tədbiri görmək üçün yaradılmışdır.

NƏTİCƏ

1) Korporativ şəbəkələrdə istifadə edilən layer 1-3 avadanlıqlarının təhlili aparılmış və qeyd edilmişdir ki, uzaq və yaxud yaxın kommunikasiya əlaqələrinin qurulması üçün şəbəkənin planlaşdırılması mühüm və vacib prosedurdur, çünki planlaşdırma şəbəkədə olan xərclər, avadanlıqların yerləşmə nöqtələrinin optimallaşdırılması kimi parametrlərə böyük təsir edə bilər.

2) AzTU kompüter şəbəkəsində təhlükəsizliyi təmin edən protokolların real şəraitdə istifadəsi təhlil edilmiş, şəbəkədə yarana biləcək boşluqların aradan qaldırılması üsulları göstərilmişdir.

3) AzTU kompüter şəbəkəsində ola biləcək təhdidlərin təsnifatı aparılmış, bu təhdidlərin qarşısının alınması üçün müvafiq təhlükəsizlik tədbirləri müəyyən edilmişdir.

4) Azərbaycan Texniki Universitetində simsiz texnologiyanın tətbiqi və bu texnologiyanının təhlükəsizlik məsələləri təhlil edilmişdir. AzTU kompüter şəbəkəsində istifadə olunan UniFi vendorunun avadanlıqlarının yeni versiyalarının tətbiq olunması zəruri hesab edilmişdir.

5) Korpusları bir-birindən uzaq məsafədə olan universitetlər üçün simsiz anten texnologiyalarından istifadə etməklə alternativ kommunikasiya üsullarının tətbiq edilməsi təklif edilmişdir. AzTU-nun gələcəkdə yataqxana korpuslarının istifadəsində bu texnologiya müvəffəqiyyətlə tətbiq edilə bilər.

6) AzTU-nun kompüter şəbəkəsi üçün hücumların təhlili və xəbərdarlıq sistemi (ASAS) işlənilmişdir. Bu sistem kompüter şəbəkəsinin bölünməz hissəsi kimi şəbəkə ilə paralel işləməyi, personala və ya istifadəçiyə təhlükə haqqında məlumatı lazımi anda çatdırmağı bacarır. Bundan əlavə, ASAS əvvəl baş vermiş hücumları analiz etmək, həmçinin dəyərləndirmək üçün səmərəli şəkildə filtrləyərək istifadəçiyə təqdim edir. Hazırkı dövrdə respublikanın ali təhsil müəssəsilərinin kompüter şəbəkələri üçün belə bir sistem işlənməmişdir.

ƏDƏBİYYAT

1. İNFORMASİYA TƏHLÜKƏSİZLİYİ, Dərslik, Bakı, “İQTİSAD UNİVERSİTETİ“ nəşriyyatı, şəkilli, 2016 – 134-135, 141, 195, 209, 293

2. Cisco Ağ Teknolojileri Yönetimi by Todd Lammle 2.Basım

3. CCNA Dökümantasyon çalışması by Hayrullah KoluKısaoğlu

4. İhsan TUĞAL, Cengiz ALMAZ, Mehmet SEVİ. Üniversitelerdeki Siber Güvenlik Sorunları ve Farkındalık Eğitimleri; BİLİŞİM TEKNOLOJİLERİ DERGİSİ, CİLT: 14, SAYI: 3, 2021

5. A. Le, A. Markopoulou, M. Faloutsos, et al. Phishdef: Url names say it all. 2011 Proceedings IEEE INFOCOM. IEEE, 2011, pp. 191-195.

6. Bosnjak, L., Sres, J., & Brumen, B. Brute-force and dictionary attack on hashed real-world passwords. 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) 2018.

7. CCNA 200-301 Official Cert Guide, Volume 1 1st Edition by Wendell Odom (Author) 114-117, 129-135, 161-163, 189-195, 291-292, 379, 471, 475-482, 615-616, 622, 639, 643-647

8. CCNA 200-301 Official Cert Guide, Volume 2 1st Edition by Wendell Odom 2020, 35-38, 54-60, 71-79, 82-83, 88-103, 108-119, 124-132, 155-165, 292-294

9. CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide 1st Edition by Brad Edgeworth (Author), David Hucaby (Author), Ramiro Garza Rios (Author), Jason Gooley (Author)

10. "Cisco ASA Configuration" by Richard Deal

11. "Cisco ASA and PIX Firewall Handbook" by David Hucaby

12. CCNA Certification Study Guide , Volume 2 by Todd Lammle

13. Content Security Policy A Complete Guide - 2020 Edition Paperback – April 6, 2021by Gerardus Blokdyk (Author)

14. Chasaki, D., Wu, Q., & Wolf, T. (2011). Attacks on Network Infrastructure. 2011 Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN).

15. Clickjacking: Attacks and Defenses by Huang, Lin-Shung, et al. 2012

16. F5 Networks TMOS Administration Study Guide - Black and White Edition First Edition by Philip Jönsson (Author), Steven Iveson (Author)

17. "F5 Networks A Complete Guide" March 1, 2021 by Gerardus Blokdyk (Author)

18. Herley, C., & Florêncio, D. (n.d.). Protecting Financial Institutions from Brute-Force Attacks. IFIP – The International Federation for Information Processing, 681–685.2008.

19. How to Master CCNA 2002-2013 by René Molenaar

20. https://www.comparitech.com/antivirus/best-antivirus-windows-10/

21. https://help.ui.com/hc/en-us/articles/115005212927-UniFi-Network-AP-Antenna-Radiation-Patterns

22. https://www.adamintech.com/configuring-the-ubiquiti-unifi-network-controller/

23. https://kotlinlang.org/docs/home.html

24. https://insert-koin.io/docs/setup/koin/

25. https://developer.android.com/jetpack/getting-started

26. J. Liu, Y. Lai, and S. Zhang, “A detection and defense system for DDoS attack in SDN,” in Proceedings of the 2017 International Conference on Cryptography, Security and Privacy, pp. 107–111, Wuhan, China, March 2017.

27. Kaur, D., & Kaur, P. (2016). Empirical Analysis of Web Attacks. Procedia Computer Science, 78, 298–306.

28. "Mastering Palo Alto Networks" by Tom Piens, Basile P. Starynkevitch, and Aron H. Kaplan

29. Shabnam Sharma, Study on Phishing Attacks; International Journal of Computer Applications; December 2018 182(33):27-29

30. Vassilis Papaspirou, Leandros Maglaras, Mohamed Amine Ferrag; A Tutorial on Cross Site Scripting Attack - Defense; 2020

31. W. Zeller and E. Felten, “Cross-site request forgeries: Exploitation and prevention,” 2008.