# **Network**

**Şəbəkə nədir?** - Şəbəkə, müxtəlif rabitə protokolları və texnologiyalarından istifadə edərək, istifadəçilər və ya sistemlər arasında məlumat mübadiləsini və əməkdaşlığı təmin edən məlumat və ya aparat kimi resursları əlaqələndirən və paylaşan bir-biri ilə əlaqəli cihazların məcmusudur.

**Şəbəkənin faydaları -** Şəbəkələr bir sıra üstünlüklər təklif edir, o cümlədən istifadəçilər arasında ünsiyyət və əməkdaşlığı asanlaşdırmaq, printerlər və fayllar kimi resurs mübadiləsini təmin etmək və resursların və xidmətlərin mərkəzləşdirilmiş idarə edilməsi və nəzarəti üçün platformanın təmin edilməsi, səmərəliliyin və məhsuldarlığın artmasına gətirib çıxarır.

**Şəbəkənin komponentləri? –**

**Switch:** Keçid şəbəkə daxilində birdən çox cihazı birləşdirir və məlumatları MAC ünvanları əsasında nəzərdə tutulan alıcıya ötürür, şəbəkənin səmərəliliyini artırır.

**Hub:** Hub açarların intellektinə malik olmayan, onlara qoşulmuş bütün cihazlara məlumatları yayımlayan əsas şəbəkə cihazlarıdır.

**Access Point:** Giriş nöqtəsi simsiz qurğulara simli və simsiz(wireless) bağlantılar arasında körpü rolunu oynayaraq simli şəbəkəyə qoşulmağa imkan verir.

**Router:** Router məlumat paketlərini müxtəlif şəbəkələr arasında yönləndirir, məlumat ötürülməsi üçün ən yaxşı yolu müəyyənləşdirir və təhlükəsizlik duvarları və şəbəkə ünvanının tərcüməsi (NAT) kimi xüsusiyyətlər vasitəsilə təhlükəsizliyi təmin edir.

**Şəbəkə İnterfeysi Kartı (NIC):** Şəbəkə İnterfeys Kartı (NIC) cihaz və Ethernet və ya Wi-Fi kimi şəbəkə mühiti arasında fiziki interfeys təmin etməklə cihazın şəbəkəyə qoşulmasına imkan verən aparat komponentidir. O, cihaz və şəbəkə arasında məlumatları tərcümə edir, məlumat paketlərini ötürmək və qəbul etməklə əlaqəni təmin edir. NIC-lər cihazların şəbəkə fəaliyyətlərində iştirak etməsi, internetə çıxış, fayl paylaşımı və şəbəkə daxilində cihazlar arasında əlaqə kimi tapşırıqları asanlaşdırmaq üçün vacibdir..

**CAT Kabel:** CAT kabelləri (Kateqoriya kabelləri) şəbəkə əlaqələri üçün istifadə edilən burulmuş cüt kabellərdir, CAT5 100 metrə qədər məsafələrdə 1000 Mbps (Gigabit Ethernet) sürətini dəstəkləyir, CAT6 isə 10 Gbps -a qədər sürəti dəstəkləyən daha yüksək performans və bant genişliyi təklif edir. Daha yaxşı səs-küyün azaldılması və çarpışmanın qarşısının alınması ilə eyni məsafədə Gbps.

**Repeater:** Səbəkənin əhatə dairəsini genişləndirmək üçün siqnalları gücləndirir və yenidən ötürür, əhatə dairəsini effektiv şəkildə artırır.

**Modem:** Rəqəmsal məlumatları kompüterdən telefon və ya kabel xətləri ilə ötürmək üçün analoq siqnallara çevirir və əksinə rəqəmsal cihazlar və analoq şəbəkələr arasında əlaqə yaratmağa imkan verir.

**Firewall:** Icazəsiz giriş və zərərli hücumlardan qoruyan, əvvəlcədən müəyyən edilmiş təhlükəsizlik qaydaları əsasında daxil olan və gedən şəbəkə trafikini izləyən və idarə edən şəbəkə təhlükəsizlik cihazı və ya proqram təminatıdır.

**Switch(Layer2,Layer3,Differences,Working Principle)** –

Layer 2 switches operate at the Data Link layer (Layer 2) of the OSI model and forward data packets based on MAC addresses, while Layer 3 switches operate at the Network layer (Layer 3) and can make routing decisions based on IP addresses, enabling inter-VLAN routing and more advanced network configurations.

Layer 3 switches integrate routing functions into their switching capabilities, allowing them to handle traffic at both Layer 2 and Layer 3, thus operating at OSI model Layer 3.

Switches work by examining the destination MAC address of incoming data packets and forwarding them to the appropriate port based on the MAC address table, ensuring efficient data transmission within a network.

**Network Topologies -** Şəbəkə topologiyaları şəbəkədəki bir-birinə bağlı cihazların quruluşunu və ya quruluşunu müəyyən edir.

**Bus:** Şin topologiyasında bütün qurğular verilənlər hər iki istiqamətdə ötürülən vahid rabitə xəttinə (avtobus) qoşulur. Bu sadə və ucuzdur, lakin toqquşmalar və məhdud miqyaslılıq kimi problemlərdən əziyyət çəkə bilər.

**Ring:** Halqa topologiyası cihazları qapalı dövrədə birləşdirir, burada məlumatlar halqanın ətrafında bir istiqamətdə hərəkət edir. Hər bir cihaz məlumatları qəbul edir və təyinat yerinə çatana qədər digərinə ötürür. O, avtobus topologiyasından daha yaxşı performans təklif etsə də və toqquşmalardan qaçsa da, bir uğursuzluq nöqtəsi bütün şəbəkəni poza bilər.

**Ulduz:** Ulduz topologiyasında bütün qurğular mərkəzi mərkəzə və ya keçidə qoşularaq ulduza bənzər bir quruluş yaradır. Məlumat mərkəzi hub vasitəsilə axır, toqquşmaları azaldır və problemlərin daha asan həllinə imkan verir. Bununla belə, mərkəzi hubın uğursuzluğu cihazları şəbəkədən təcrid edə bilər.

**Mesh:** Mesh topologiyası etibarlılığı və nasazlığa dözümlülüyünü artıraraq cihazlar arasında lazımsız yollar təmin edir. Hər bir cihaz çoxlu digər cihazlara qoşularaq yüksək dərəcədə bir-birinə bağlı şəbəkə yaradır. O, möhkəmlik təklif etsə də, onun həyata keçirilməsi mürəkkəbdir və daha çox kabel çəkilişi tələb olunur.

**OSI model -** OSI modeli şəbəkənin rabitə funksiyalarını standartlaşdırmaq və konseptuallaşdırmaq üçün istifadə olunur, şəbəkə protokollarını və texnologiyalarını başa düşmək və həyata keçirmək üçün çərçivə təmin edir. OSI modeli şəbəkə protokollarını və texnologiyalarını başa düşmək və həyata keçirmək, müxtəlif sistemlər və cihazlar arasında qarşılıqlı fəaliyyət və əlaqəni asanlaşdırmaq üçün standartlaşdırılmış çərçivə təmin edir.

OSI-də **inkapsulyasiya** və **dekapsulyasiya** məlumatların şəbəkə yığınından keçərkən hər bir təbəqədə protokol başlıqlarının əlavə edilməsini və silinməsini, məlumatların bütövlüyünü, marşrutlaşdırmasını və çatdırılmasını təmin edir. Şəbəkə prinsiplərinin daha praktik tətbiqi olan

**Physical səviyyə:** Cihazlar arasında fiziki əlaqələri idarə edir və rabitə kanalı üzərindən xam binar məlumatları ötürür. Protokollar: Ethernet, Wi-Fi.

**Data Link Layer:** Səhvlərin aşkarlanması və düzəldilməsi ilə məşğul olur və çərçivə, ünvanlama və xətaların idarə edilməsi üçün protokolları müəyyənləşdirir. Protokollar: MAC (Media Girişinə Nəzarət), ARP (Address resolution protocol).

**Network səviyyəsi:** Müxtəlif şəbəkələrdəki cihazlar arasında məlumat paketlərini istiqamətləndirir və məntiqi ünvanlamağı idarə edir. Protokollar: IP (Internet Protocol), ICMP (Internet Control Message Protocol).

**Transport Layeri:** Sistemlər arasında etibarlı məlumat çatdırılmasını təmin edir və axına nəzarəti və səhvlərin bərpasını idarə edir. Protokollar: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).

**TCP (Transmission Control Protocol)** şəbəkə üzərindən məlumat paketlərinin etibarlı, sifarişli və səhv yoxlanılmış çatdırılmasını təmin edən, internetə baxış və e-poçt kimi zəmanətli çatdırılma və məlumat bütövlüyü tələb edən proqramlar üçün uyğun olan əlaqə yönümlü protokoldur.

**UDP (User Datagram Protocol)**, digər tərəfdən, məlumat paketlərini minimum yüklə çatdıran, daha sürətli ötürmə sürətləri və daha az gecikmə müddəti təklif edən, lakin çatdırılma və ya səhvlərin yoxlanılmasına zəmanət verməyən, ümumiyyətlə axın mediası kimi real vaxt proqramları üçün istifadə olunan əlaqəsiz protokoldur. onlayn oyun.

**Session Layer:** Sinxronizasiya və yoxlama nöqtəsi daxil olmaqla proqramlar arasında əlaqə qurur, idarə edir və dayandırır. Protokollar: NetBIOS, RPC (Remote Procedure Call).

**Presentation Layeri:** Müxtəlif formatlar arasında məlumatları tərcümə edərək sistemlər arasında uyğunluğu təmin edir, şifrələmə və sıxılma ilə məşğul olur. Protokollar: SSL/TLS (Secure Sockets Layer/Transport Layer Security), JPEG, ASCII.

**Application Layeri:** E-poçt, internetə baxış və fayl ötürülməsi kimi istifadəçi proqramları və xidmətləri üçün interfeyslər təqdim edir. Protokollar: HTTP (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol), FTP (Fayl Transfer Protokolu).

**TCP/IP modeli** - dörd qatdan ibarətdir: Application, Transport, İnternet və Link, OSI modelinin üst qatları ilə sıx uyğunlaşır və real dünya tətbiqlərində şəbəkə rabitəsini və problemlərin aradan qaldırılmasını sadələşdirir.

**TCP Flags -** TCP (Transmission Control Protocol) rabitə seansının müxtəlif aspektlərini idarə etmək üçün başlıq daxilində bayraqlardan istifadə edir.

**SYN (Sinxronizasiya):** İki host arasında əlaqə yaratmaq üçün istifadə olunur.

**ACK (Acknowledgement):** Məlumatın qəbulunu təsdiq edir.

**FIN (Finish):** Bir tərəfdən məlumat ötürülməsinin sonunu göstərir.

**RST (Sıfırla):** adətən xətaya və ya gözlənilməz vəziyyətə cavab olaraq əlaqəni sıfırlayır.

**PSH (Push):** Qəbul edən TCP yığınına məlumatları buferləşdirmədən dərhal proqrama çatdırmaq üçün göstəriş verir.

**URG (Təcili):** Təcili məlumat göstərici sahəsinin əhəmiyyətli olduğunu göstərir.

**ECN (Explicit Congestion Notification):** Müasir TCP tətbiqlərində tıxaclara nəzarət üçün istifadə olunur.

**Three-way-handshake -** iki host arasında əlaqə yaratmaq üçün TCP-də (Transmission Control Protocol) istifadə edilən üsuldur.

**SYN:** Başlayan host, əlaqə yaratmaq üçün qəbul edən hosta SYN (sinxronizasiya) paketi göndərir.

**SYN-ACK:** Qəbul edən host SYN-ACK (sinxronizasiya-təsdiq) paketi ilə cavab verir ki, o, SYN paketini qəbul edib və əlaqə yaratmağa hazırdır.

**ACK:** Nəhayət, təşəbbüskar host SYN-ACK paketinin alınmasını təsdiq edən ACK (təsdiq) paketini qəbul edən hosta geri göndərir.

**Port and Protocol -**

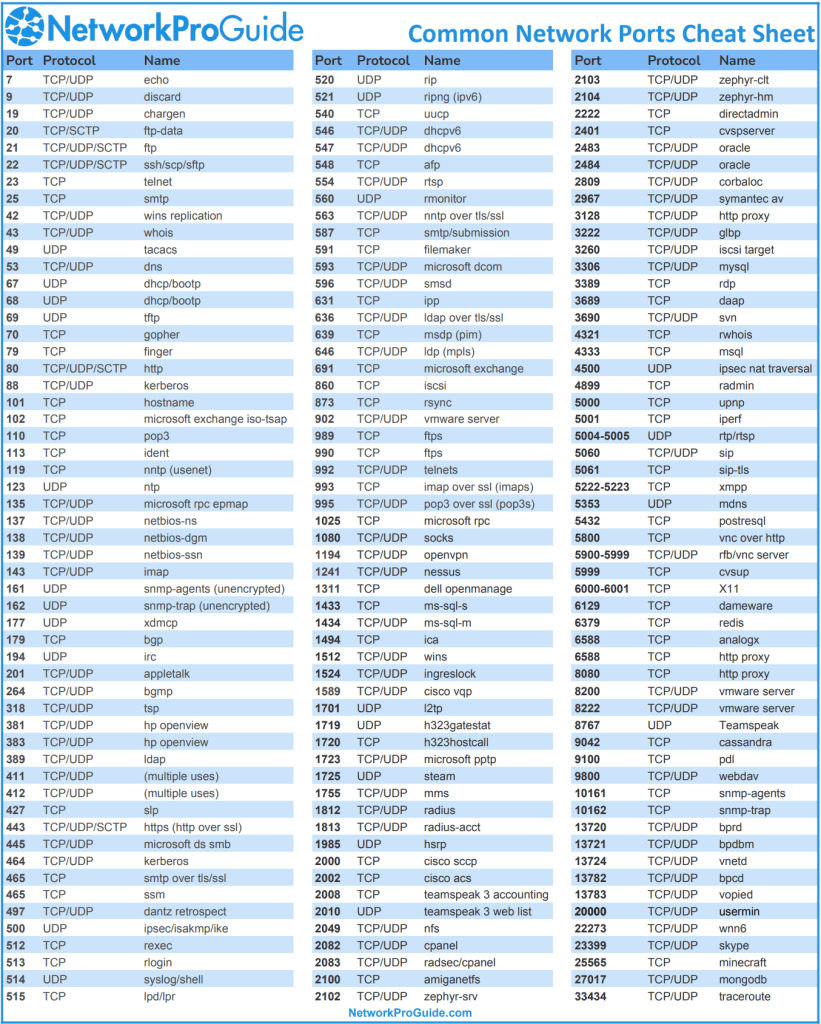
**Port:** Port şəbəkədə ünsiyyət üçün son nöqtə kimi çıxış edən məntiqi quruluşdur. Bu, məlumatların cihaza daxil olub-olmamasına imkan verən qapı və ya şlüz kimidir. Portlar 0-dan 65535-ə qədər olan nömrələrlə müəyyən edilir və xüsusi proqramlar və ya xidmətlərlə əlaqələndirilir.

Virtual portlar, serverlərə gedən bağlantılar yaratmaq üçün müştəri proqramları tərəfindən istifadə edilən müvəqqəti port nömrələridir. Bizə virtual portlar lazımdır, çünki onlar bir müştəri cihazına müxtəlif serverlərlə eyni vaxtda çoxsaylı əlaqə yaratmağa imkan verir. Hər bir əlaqə düzgün marşrutlaşdırma və məlumat paketlərinin eyniləşdirilməsini təmin etmək üçün mənbə IP ünvanı, mənbə portu, təyinat IP ünvanı və təyinat portunun unikal birləşməsini tələb edir.

65535 port diapazonu 16 bitlik ikili say sistemindən əldə edilmişdir. TCP/IP şəbəkəsində port nömrələri 16 bitlik işarəsiz tam ədədlər kimi təmsil olunur, yəni onlar 0-dan 65535-ə (2^16 - 1) qədər dəyişə bilər.

**Protokol:** Protokol şəbəkədəki cihazlar arasında məlumatların necə ötürüldüyünü və qəbul edildiyini tənzimləyən qaydalar və ya standartlar toplusudur. O, məlumat paketlərinin formatını, ardıcıllığını və xətaların idarə olunmasını müəyyən edir.

Xülasə, portlar bir cihazda işləyən çoxsaylı xidmətlər arasında fərq qoymağı təmin edir, protokollar isə şəbəkədəki cihazlar arasında əlaqə üçün qayda və prosedurları müəyyən edir.



**Difference between SSH and Telnet -** SSH (Secure Shell) və Telnet hər ikisi terminala uzaqdan daxil olmaq üçün istifadə olunan protokollardır, lakin SSH məlumat ötürülməsini şifrələyir, təhlükəsiz olmayan şəbəkə üzərindən təhlükəsiz rabitə təmin edir, Telnet isə məlumatları açıq mətndə göndərərək onu ələ keçirməyə və icazəsiz girişə qarşı həssas edir.

**Difference between SSH and RDP -** SSH (Secure Shell) Unix əsaslı sistemlərə təhlükəsiz uzaqdan daxil olmaq üçün istifadə edilən protokoldur, şifrəli rabitə və komanda xəttinə girişi təmin edir, RDP (Remote Desktop Protocol) isə Windows əsaslı sistemlərin qrafik istifadəçi interfeyslərinə daxil olmaq üçün istifadə olunur. uzaq iş masası mühiti ilə sanki maşında fiziki olaraq mövcudmuş kimi qarşılıqlı əlaqədə olmaq.

**What is ARP protocol** – Address resolution Protocol (ARP) cihazların bir-biri ilə əlaqə saxlamasına imkan verən IP ünvanlarını yerli şəbəkədəki MAC ünvanlarına uyğunlaşdırmaq üçün istifadə olunur. ARP qurğular üçün şəbəkədəki digər cihazların aparat ünvanlarını tapmaq üçün lazımdır, onlar arasında məlumat paketlərinin ötürülməsini təmin edir.

**What is OSPF protocol -** OSPF (Open Shortest Path First) marşrutlaşdırma məlumatlarını səmərəli şəkildə mübadilə etmək və məlumat ötürülməsi üçün ən yaxşı yolları hesablamaq üçün IP şəbəkələrində istifadə olunan marşrutlaşdırma protokoludur. Bu, dinamik marşrutlaşdırma üçün vacibdir, marşrutlaşdırıcılara şəbəkə dəyişikliklərinə uyğunlaşmağa və marşrutlaşdırma cədvəllərini avtomatik yeniləməyə imkan verir və optimallaşdırılmış şəbəkə performansına və etibarlılığına səbəb olur.

**DoH,DoT,Oblivious DoH -** DoH (HTTPS üzərindən DNS) və DoT (TLS üzərindən DNS) dinləmə və müdaxilənin qarşısını alaraq məxfiliyi və təhlükəsizliyi artırmaq üçün DNS sorğularını şifrələyən protokollardır. Oblivious DoH, DNS sorğularını istifadəçinin IP ünvanından ayıraraq, istifadəçi məxfiliyini daha da qoruyaraq və onlayn fəaliyyətlərin izlənilməsinin qarşısını alaraq əlavə məxfilik qatı əlavə edir.

**What is RARP protocol -** Reverse Address Resolution Protocol (RARP) MAC ünvanlarını IP ünvanlarına uyğunlaşdırmaq üçün, ilk növbədə cihazların öz IP ünvanlarını dinamik şəkildə əldə etməli olduğu disksiz iş stansiyası mühitlərində istifadə olunur. RARP bu cihazların IP ünvanlarının əl ilə konfiqurasiyasına ehtiyac olmadan şəbəkə üzərindən əlaqə saxlaması üçün vacibdir.

**DNS tunelləmə** - DNS sorğuları və cavabları daxilində qeyri-DNS trafikini əhatə etməklə şəbəkə təhlükəsizlik tədbirlərindən yan keçmək üçün istifadə edilən və DNS kanalları üzərində gizli əlaqə yaratmağa imkan verən bir texnikadır.

**Proksi** - serverlər müştərilər və serverlər arasında vasitəçi kimi çıxış edir, məxfiliyi, təhlükəsizliyi və performansı artırmaq üçün sorğuları və cavabları yönləndirir. Müştərilər və serverlər arasında yerləşdirilən əks proksilər veb trafik axınını optimallaşdırır, yük balansını təmin edir və serverləri internetə birbaşa məruz qalmadan qoruyur, təhlükəsizliyi və genişlənmə qabiliyyətini artırır.

**What is MAC and IP –**

MAC (Media Girişinə Nəzarət) **48 bit** ünvanları hardware səviyyəsində şəbəkə interfeyslərinə təyin edilmiş unikal identifikatorlardır və yerli şəbəkədəki cihazlar arasında əlaqəni asanlaşdırır.

IP (İnternet Protokolu) **32 bit** ünvanları isə şəbəkədəki cihazları müəyyən etmək və internet üzərindən qlobal olaraq onlar arasında məlumat paketlərini yönləndirmək üçün istifadə edilən məntiqi ünvanlardır.

**Binary to Decimal –** Ədədin üzərinə ( sağ tərəfdən ) 1 2 4 8 16 32 64 .... yazırıq və olanları toplayırıq.

**Decimal to Binary –** Ədədi 2 yə bölə- bölə 0 alınana qədər gedirik. Daha sona tərsinə son qisməti və qalıqları yazırıq.

**What is İCMP protocol -** ICMP (Internet Control Message Protocol) IP şəbəkələri daxilində səhv hesabatı və sınaq imkanlarını təmin etməklə şəbəkə bağlantısı problemlərinin diaqnostikası və həlli üçün vacibdir. (Ping)

**What is TRACERT -** Traceroute mənbə və təyinat arasında paketlərin keçdiyi marşrutu izləyən şəbəkə diaqnostikası vasitəsidir, paket itkisini və gecikmə problemlərini müəyyən etməyə kömək edir, bununla da əlaqə problemlərinin aradan qaldırılmasına və şəbəkə performansının optimallaşdırılmasına kömək edir.

**What is NetworkID , HostID –** Host ID və Network ID şəbəkə daxilində cihazları müəyyən etmək və müxtəlif şəbəkələri ayırd etmək üçün istifadə edilən IP ünvanının komponentləridir.

**What is SubnetMask –** Subnet mask ünvanın şəbəkə və host hissələrini müəyyən etmək üçün IP ünvanı ilə birlikdə istifadə edilən 32 bitlik nömrədir və cihazlara IP ünvanının hansı hissəsinin şəbəkəni və hansı hissəsinin hostu təmsil etdiyini müəyyən etməyə imkan verir. Subnet mask böyük şəbəkəni daha kiçik, daha idarə olunan alt şəbəkələrə bölmək, şəbəkə performansını və idarəetməni təkmilləşdirməklə IP ünvanlarından səmərəli istifadə etməyə imkan verən alt şəbəkə üçün vacibdir.

**Classes of IP :**

A klass İP addressləri 1-126 arası

B klass İP addressləri 128-191 arası

C klass İP addressləri 192-223 arası

D klass İP addressləri 224-239 arası 🡪 Multicast yayınlar üçün ayrılmışdır.

E klass İP addressləri 240-254 arasıdır 🡪 Test məqsədli olaraq istifadə olunurlar.

**Subnet Maska gore Classlari téyin etmek olar.**

**Şəbəkədə xəbərləşmə,danışma prosesinin növləri:**

Unicast – 1 cihazdan digər 1 cihazla arasında olan əlaqə

Multicast – 1 cihazdan müəyyən bir qrup cihaz arasında olan əlaqə

Broadcast – 1 cihazdan digər bütün cihazlar arasında olan əlaqə

ŞƏBƏKƏDƏKİ SON HOST İP-si .255 broadcast üçün istifadə olunur.

**What is DNS, DHCP , NAT –**

DNS (Domain Name System) internetdə resursların naviqasiyasını və əlçatanlığını asanlaşdırmaqla insan tərəfindən oxuna bilən domen adlarını IP ünvanlarına çevirir.

DHCP (Dinamik Host Konfiqurasiya Protokolu) dinamik şəkildə IP ünvanlarını və şəbəkə konfiqurasiya parametrlərini şəbəkədəki cihazlara təyin edir, şəbəkənin idarə edilməsini və idarə edilməsini sadələşdirir.

A table with numbers and a few letters

Description automatically generated with medium confidenceNAT (Network Address Translation ) Bir şəbəkə 2 cür İP addressi var:

**Private İP addressi :** Bu LAN-da işlədilən İP addressidir.LAN-a aiddirlər.Daxili İP-lərdir.

**Public İP addressi:** Bu WAN-da işlədilən İP addressidir.İnternetə aiddirlər.Çöl,xarici İP-lərdir.

**NAT** bu iki İP addressləri, yəni Private və Public İP addressləri arasında çevirmə işini görür.

Public(WAN) və Private(LAN) şəbəkələrinin bir birləri ilə danışmaqlarını,əlaqəsini təmin edir..

**DNS Records -**

**A** - qeydləri domen adlarını IPv4 ünvanları ilə əlaqələndirir,

**AAAA** - qeydləri onları IPv6 ünvanları ilə əlaqələndirir

**MX** - qeydləri domen üçün poçt serverlərini təyin edir

**NS** - qeydləri nüfuzlu ad serverlərini müəyyənləşdirir

**SOA** - qeydləri domenin zonası və əsas DNS serveri

**SPF** - qeydləri haqqında məlumatları ehtiva edir, e-poçt göndərənlərə icazə verir

**TXT** - qeydləri ixtiyari mətn məlumatlarını təmin edir

**PTI** - qeydləri domen sahibliyini təsdiqləyir

**DCIM** - qeydləri məlumat mərkəzi infrastrukturu haqqında məlumatları saxlayır

**DMARC** - qeydləri domen idarəçiliyi, e-poçt çatdırılması, DNS həlli və şəbəkə üçün birlikdə vacib olan e-poçt identifikasiyası və siyasətin tətbiqini müəyyənləşdirir təhlükəsizlik.

**Forward , Reverse lookup zone –**

**Forward lookup zone** domen adlarını IP ünvanlarına uyğunlaşdırır, ada görə resurslara daxil olmaq üçün DNS həllini asanlaşdırır

**Reverse lookup zone** isə əks DNS axtarışlarına icazə verməklə şəbəkə problemlərinin həllinə və identifikasiyasına kömək edərək IP ünvanlarını domen adlarına uyğunlaşdırır. Bu zonalar səmərəli və etibarlı DNS xidmətlərinin saxlanması, şəbəkələr arasında problemsiz rabitə və resurs girişinin təmin edilməsi üçün vacibdir.

Top, second , third level domains –

Top səviyyəli domenlər (TLD) .com və ya .org kimi domen adlandırma sistemində ən yüksək səviyyədir.

Second səviyyəli domenlər (SLD) "example.com"dakı "nümunə" kimi növbəti səviyyədir və tez-tez brendinq və ya identifikasiya üçün istifadə olunur.

Third səviyyəli domenlər (TLD) "blog.example.com" saytındakı "bloq" kimi, domen daxilində təşkilati strukturu və ya fərqləndirməni təmin edən əlavə bölmələrdir. Onlar internetdə veb-saytları təşkil etməyə və təsnif etməyə kömək edir.

**DNS Requests -**

1. Recursive (Client-Server) : Yəni bizlər Clientlar DNS Serverə sorğu göndərəndə bu Recursive sorğu olur
2. İterative ( Server-Server ) : DNS Serverin başqa DNS Serverə sorğu göndərməsi İterative sorğu olur.

**DNS Resolver:**

* Resolver servisi tərəfindən yadda saxlanılmış sorğuları görmək üçün terminalda bu əmri işlətmək lazımdır:

ipconfig /displaydns

* Yadda saxlanılmış sorğuları silmək üçün isə terminalda bu əmri işlətmək lazımdır:

ipconfig /flushdns

**DNS Logs -**

Linux-da DNS qeydləri adətən **/var/log/** kataloqunda yerləşdirilir, mesajlar və ya DNS ilə əlaqəli girişlər də daxil olmaqla ümumi sistem mesajlarını ehtiva edən syslog kimi fayl adları ilə. **C:\Windows\System32\drivers\etc-DNS HOST LOG**

Windows-da DNS qeydləri Applications and Services Logs > Microsoft > Windows > DNS Client Events or DNS Server bölməsində tapıla bilər.

**What is FQDN -** FQDN (Fully Qualified Domain Name) host adı və subdomenlər və yüksək səviyyəli domen kimi bütün yüksək səviyyəli domenlər daxil olmaqla, konkret host üçün tam domen adını təmsil edir.

FQDN-lər internetdə və ya şəbəkə daxilində resursların unikal şəkildə müəyyən edilməsi və ünvanlanması, cihazlar və xidmətlər arasında dəqiq və etibarlı əlaqə yaratmaq üçün vacibdir.

**DHCP working Principle (DORA) –**

Cihazlar İP addresslərini avtomatik almaq üçün ətrafdakı DHCP serveri bilməlidirlər

Bunuda şəbəkəyə broadcast yayın edərək öyrənirlər.Proses bu şəkildə baş verir:

**DHCP Discover** - İlk dəfə İP alacaq client cihaz broadcast yayın edir şəbəkədə. Bu yayın, DHCP DISCOVER adlanır. Client cihaz həmçinin bu yayın zamanı,MAC ünvanınıda əlavə edərək göndərir.

**DHCP Offer** – Yayını qəbul edən DHCP Serveri şəbəkədə DHCP Offer mesajını yayınlayır.Bu mesajda broadcastdır.Bütün cihazlara gedir,amma ki,mesajın içində MAC addressi mövcud olduğu üçün mesajı yalnız və yalnız MAC addressinə sahib olan cihaz qəbul edir.

**DHCP Request** – Cihaz DHCP-dən gələn təklifi qəbul edərsə bu zaman DHCP Request adlı bir Yayın göndərir şəbəkəyə.Bu mesaj,yayında broadcastdır.

**DHCP Acknowledgement** – DHCP Server istəyi qəbul etdiyini DHCP ACK mesajı ilə şəbəkəyə Broadcast yayın ilə göndərir və artıq Client həmin verilən İP-ni qəbul etmiş olur.

**What is APIPA** - APİPA (Automatic Private IP Addressing) :

Discover yayınında DHCP Serverdən cavab ala bilməyən cihaz şəbəkədə İP ala bilmir

Amma ki, cihaz Özü Özünə bir İP addressi verir. Bunada APİPA deyilir.

APİPA İP-si 169.254.0.0 şəklindədir və 169.254.255.254 İP aralığını əhatə edir.Subnetmaskı isə 255.255.0.0-dır. APİPA İP-si almış digər cihazlar ilə danışa,əlaqə qura bilər.

**What is ISP** - İSP ( İnternet Provider Service ) tərəfindən modemə bir İP verilir.Bu İP PUBLİC İP addressidir. NAT Clientin PRİVATE İP addressini modemin PUBLİC İP addressi ilə dəyişdirərək,çevirmə işi apararaq bizi Hədəfə göndərir.Və beləliklə fərqli şəbəkələr arasında xəbərləşə bilirik. Bu proses tərsidə olur.Yəni PUBLİC-dən PRİVATE-yədə çevirmə işini NAT görür.

**What is Virtualization –**

Virtuallaşdırma, birdən çox virtual mühitin vahid fiziki sistemdə işləməsinə imkan verən serverlər, yaddaş və ya şəbəkələr kimi hesablama resurslarının virtual nümunələrinin yaradılması prosesidir.

VMware vSphere və Microsoft Hyper-V kimi 1-ci tip hipervizorlar bilavasitə host aparatında işləyir,

VMware Workstation və Oracle VirtualBox kimi Tip 2 hipervizorlar isə host əməliyyat sisteminin üstündə işləyir.

Virtuallaşdırma resurs istifadəsini optimallaşdırır, miqyaslılığı artırır və iş yükünün təcrid olunmasını asanlaşdırır, bu da onu infrastrukturun səmərəli idarə edilməsi və tətbiqlərin yerləşdirilməsi üçün vacib edir.

**What is Docker –**

Docker, yüngül, portativ konteynerlərdə tətbiqlər hazırlamaq, göndərmək və işə salmaq üçün platformadır. O, proqram təminatının inkişafı və müxtəlif sistemlərdə yerləşdirilməsi üçün ardıcıl mühit təmin edir, tətbiqlərin qurulması, paylanması və idarə edilməsi prosesini sadələşdirir, nəticədə proqram təminatının hazırlanması və yerləşdirilməsi iş axınlarında səmərəliliyi və miqyaslılığı artırır.

# **Windows**

**WSUS -** WSUS (Windows Server Update Services) idarəçilərə təşkilat şəbəkəsi daxilində Windows əməliyyat sistemləri və digər Microsoft məhsulları üçün yeniləmələri, yamaqları və düzəlişləri idarə etməyə və yaymağa imkan verən Microsoft alətidir.

**Program Files 64x Vs 86x –**

"Proqram Faylları" kataloqu adətən 64 bitlik Windows sistemində 64 bit proqramlar üçün, "Proqram Faylları (x86)" isə 32 bit proqramlar üçün istifadə olunur.

**CMD vs Powersehell –**

CMD (Command Prompt) Windows-da köhnə command line interpreterdir, əsasən məhdud funksiyaları və skript imkanları olan əmrləri və skriptləri yerinə yetirmək üçün istifadə olunur.

PowerShell, Windows mühitlərində sistem idarəçiliyi və idarə edilməsi üçün daha geniş funksiyalar spektrini təmin edən təkmilləşdirilmiş avtomatlaşdırma, tapşırıqların idarə edilməsi və .NET çərçivəsi ilə inteqrasiya təklif edən daha təkmil komanda xətti qabığı və skript dilidir.

**Task sheduler , Event viewer –**

Task Scheduler, müəyyən vaxtlarda və ya hadisələrdə tapşırıqların, proqramların və ya skriptlərin icrasını avtomatlaşdırmaq üçün istifadə olunan Windows yardım proqramıdır, əl müdaxiləsi olmadan adi əməliyyatların və texniki xidmət tapşırıqlarının sadələşdirilmiş idarə edilməsini asanlaşdırır.

Event Viewer sistem, təhlükəsizlik və tətbiq hadisələrini qeyd edən və göstərən, nasazlıqların aradan qaldırılmasına, sistemin sağlamlığının monitorinqinə və sistem fəaliyyətləri, xətalar və xəbərdarlıqlar haqqında ətraflı məlumat verməklə problemlərin diaqnostikasına kömək edən Windows alətidir.

**Log-** Loglar əməliyyat sistemləri, proqramlar və ya cihazlar tərəfindən yaradılan hadisələrin, hərəkətlərin və ya əməliyyatların qeydləridir, sistem fəaliyyətlərinin xronoloji tarixini və problemlərin aradan qaldırılması, audit və təhlil məqsədləri üçün səhvləri təmin edir.’

**Sysmon –** Sysmon potensial təhlükəsizlik təhdidlərini aşkar etmək və araşdırmaq üçün sistem fəaliyyətinə nəzarət edən, təkmilləşdirilmiş təhlükənin aşkarlanması və cavab tədbirləri üçün ətraflı məlumat verən Windows yardım proqramıdır.

**Event ID :**

* 4624: Successful account logon.
* 4625: Failed account logon.
* 4657: A handle to an object was requested.
* 4688: A new process has been created.
* 4689: A process has exited.
* 4698: Scheduled task created.
* 4702: Scheduled task updated.
* 4719: System audit policy changed.
* 4720: User account created.
* 4723: An attempt was made to change an account's password.
* 4724: An attempt was made to reset an account's password.
* 4725: User account disabled.
* 1102: Windows auditing cleared.

**Logon Types:**

* Logon Type 2: Interactive logon, typically via console or Remote Desktop.
* Logon Type 3: Network logon, accessing resources over the network.
* Logon Type 5: Service logon, used by services running under a user account.
* Logon Type 7: Unlock workstation, occurs when a locked workstation is unlocked.
* Logon Type 10: Remote desktop logon, using Remote Desktop Protocol (RDP) to access a system.
* Logon Type 11: Cached interactive logon, occurs when a user logs on to a system with cached credentials.

**Batch files –** Batch files (".bat") Windows-da command line interpreter yerinə yetiriləcək bir sıra əmr və ya təlimatları ehtiva edən skript fayllarıdır. Onlar təkrarlanan tapşırıqların avtomatlaşdırılması, bir neçə əmrin ardıcıl olaraq yerinə yetirilməsi və Windows mühitlərində mürəkkəb əməliyyatların sadələşdirilməsi üçün istifadə olunur.

**What is SMB -** SMB (Server Message Block) adətən Windows əsaslı sistemlərlə əlaqəli şəbəkədəki cihazlar arasında faylları, printerləri və digər resursları paylaşmaq üçün istifadə edilən şəbəkə rabitə protokoludur. O, həm yerli, həm də paylanmış mühitlərdə problemsiz fayl paylaşımına və resurs girişinə imkan yaradaraq, şəbəkəyə qoşulmuş cihazlar arasında səmərəli məlumat ötürülməsini və əməkdaşlığı asanlaşdırır.

**File Sysetms –**

FAT: Simple file system for older Windows versions and small devices.

FAT32: Extension of FAT with larger file size support.

NTFS: Advanced file system with improved reliability and security.

exFAT: Optimized for flash drives and large file support.

XFS: High-performance file system for Unix-like systems.

HFS: macOS file system for organizing files.

EXT4: Default Linux file system with improved performance.

ReFS: Microsoft's file system focusing on data integrity.

**Permissions -** Windows-da icazələr fayl, qovluq və resurslara girişi tənzimləyir, istifadəçilərin və ya qrupların oxumaq, yazmaq və ya icra etmək kimi onlarda hansı hərəkətləri yerinə yetirə biləcəyini müəyyən edir.

Advanced icazələr administratorlara əsas oxumaq, yazmaq və icra etmək icazələrindən kənarda təfərrüatlı icazələri müəyyən etməyə imkan verməklə, sistem daxilində təhlükəsizlik və giriş səviyyələrinin daha dəqiq idarə edilməsinə imkan verməklə, giriş hüquqları üzərində daha incə nəzarət təklif edir.

**EFS vs BitLocker –**

EFS (Encrypting File System) diskdə saxlanılan həssas məlumatları qorumaq üçün fayl və qovluqları şifrələyən Windows funksiyasıdır. O, simmetrik və asimmetrik şifrələmənin birləşməsindən istifadə etməklə işləyir, burada hər bir fayl unikal fayl şifrələmə açarı ilə şifrələnir, daha sonra istifadəçinin açıq açarı ilə şifrələnir.

BitLocker, istirahətdə olan məlumatları qorumaq üçün bütün diski şifrələyən Windows-da tam disk şifrələmə xüsusiyyətidir. BitLocker və EFS arasındakı əsas fərq onların əhatə dairəsidir: BitLocker bütün diskləri şifrələyir, EFS isə fərdi faylları və ya qovluqları şifrələyir.

**What is Redit -** Regedit, konfiqurasiya parametrlərini, sistem məlumatlarını və istifadəçi seçimlərini saxlayan Windows Reyestrinə baxmaq və dəyişdirmək üçün alət olan Windows Qeydiyyat Redaktorudur. Qeyd dəftəri **HKEY\_CLASSES\_ROOT,** **HKEY\_CURRENT\_USER, HKEY\_LOCAL\_MACHINE, HKEY\_USERS və HKEY\_CURRENT\_CONFIG** daxil olmaqla iyerarxik açarlar şəklində təşkil olunub, hər biri sistemin işləməsi və fərdiləşdirilməsi üçün vacib olan parametrləri və məlumatları ehtiva edir..

**What is Services -** Windows-da xidmətlər şəbəkə idarəçiliyindən tutmuş aparat nəzarətinə qədər tapşırıqların idarə edilməsi, sistemin işləməsi və proqram funksionallığı üçün vacib olan fon prosesləridir.

**What is GPOs –** Group Policy Objects (GPO) administratorlara kompüterlər şəbəkəsində sistem parametrlərini, təhlükəsizlik siyasətlərini və istifadəçi seçimlərini idarə etməyə və tətbiq etməyə imkan verən Windows mühitlərində konfiqurasiya parametrləridir. Onlar idarəetmənin mərkəzləşdirilməsi, ardıcıllığın təmin edilməsi və təşkilatda bir çox maşın arasında təhlükəsizlik tədbirlərinin tətbiqi üçün vacibdir.

**What is Applocker -** AppLocker, istifadəçilərin hansı proqramları işə sala biləcəyinə nəzarət edən, proqram təminatının icazəsiz icrasının qarşısını almağa və sistem təhlükəsizliyini gücləndirməyə kömək edən Windows təhlükəsizlik funksiyasıdır.

**Deleting vs Destroying,ciphers –**

Windows-da faylın silinməsi adətən onun istinadını fayl sistemindən çıxarır, yeni məlumatlar üçün yer hazırlayır, lakin faylın üzərinə yazılana qədər bərpa oluna bilər.

Faylın məhv edilməsi bərpa olunmasının qarşısını almaq üçün onun məlumatlarının təhlükəsiz şəkildə üzərinə yazılmasını nəzərdə tutur. Bu, adətən silinmiş fayl sahəsini təsadüfi məlumat və ya sıfırlarla əvəz edən **CIPHER** kimi yardım proqramlarından istifadə etməklə həyata keçirilir, həssas məlumatların icazəsiz istifadəçilər tərəfindən bərpa olunmamasını təmin etməklə məlumatların məxfiliyini və təhlükəsizliyini artırır.

**32bit vs 64 bit OS -** 32-bit və 64-bit əməliyyat sistemləri arasındakı əsas fərq onların yaddaş ünvanlama imkanlarındadır, 64-bit sistemlər 32-bit sistemlərdən daha böyük həcmdə yaddaşa daxil ola bilir. Artan yaddaş tutumundan, təkmilləşdirilmiş performansdan və müasir aparat və proqram təminatı tətbiqləri ilə uyğunluqdan istifadə etmək üçün bizə 64-bit əməliyyat sistemləri lazımdır ki, bu da daha səmərəli çoxlu tapşırıqları yerinə yetirməyə və böyük verilənlər toplusunu idarə etməyə imkan verir.

**UEFI , BIOS , MBR , GBT –**

**UEFI** (Unified Extensible Firmware Interface) **BIOS**-u (Basic Input/Output System) əvəz edən, təhlükəsiz yükləmə, daha sürətli yükləmə vaxtları və daha böyük yaddaş qurğuları üçün dəstək kimi təkmilləşdirilmiş xüsusiyyətləri təklif edən müasir proqram təminatı interfeysidir.

**GPT** (GUID Partition Table) və **MBR** (Master Boot Record) saxlama cihazlarında məlumatların təşkili üçün fərqli bölmə sxemləridir, GPT MBR ilə müqayisədə daha böyük disk ölçülərini, daha çox bölmələri və təkmilləşdirilmiş məlumat bütövlüyü xüsusiyyətlərini dəstəkləyir.

Təkmilləşdirilmiş sistemin işə salınması və idarə edilməsi üçün bizə UEFI lazımdır, GPT isə müasir yaddaş qurğuları və daha yüksək tutumlu disklər üçün daha yaxşı dəstək verir, məlumatların səmərəli təşkilini və sistemin işini təmin edir.

## **AD**

**Domain Controller**- AD nin yuklendiyi server. Domain Controller istifadəçi hesablarının və resurslarının mərkəzləşdirilmiş idarə olunmasını təmin edərək, Windows domenində şəbəkə təhlükəsizliyini, autentifikasiyanı və giriş nəzarətini idarə edir.

**DNS serverləri** domen adlarını IP ünvanlarına həll edir, insan tərəfindən oxuna bilən ünvanları maşın tərəfindən oxuna bilən ünvanlara çevirərək internet və şəbəkə rabitəsini təmin edir. **DHCP serverləri** şəbəkədəki cihazlara IP ünvanlarının və şəbəkə konfiqurasiya parametrlərinin təyin edilməsini avtomatlaşdırır, şəbəkənin idarə edilməsini və resursların idarə edilməsini sadələşdirir.

**Fayl serverləri** faylları və qovluqları saxlayır və idarə edir, mərkəzləşdirilmiş məlumatların saxlanmasını, girişə nəzarəti və şəbəkə üzrə paylaşılmasını asanlaşdırır.

**IIS serverləri** Windows sistemlərində veb-saytları və veb proqramları yerləşdirir və idarə edir, veb hostinq, inkişaf və yerləşdirmə üçün platforma təmin edir.

The default location for IIS server logs in Windows is typically:

%SystemDrive%\inetpub\logs\LogFiles

**Logic Structure:**

1. Forest- Butun komputerler Foresti emele getirir
2. Tree- serverin butun computerleri (1ci DC olur- Root domain-global catalogue(butun userlerin melumatlarini saxlayir))
3. OU – Organizational unit (Computers, users, printers, groups)
4. Domain- millisec.local

**Physical Structure:**

1. Sites- Filiallar
2. DC-Domain Controller

**Member Server** – AD rolu yuklenmiyen amma AD ya bagli olan serverler.

**FSMO rules(Flexible Single Master Operations):**

1. Forest Wide

* **Schema Master**- Updatelere, deyisikliklere nezaret edir(default gelmir),Sesnsitivedi
* **Domain Naming Master**-Iki eyni domain olmamasina nezaret edir

1. Domain Wide

* **RID Master**- iki eyni adli user, group olmamamsina nezaret edir. Userler SID-lere gore ferqlenir(128 bit key)
* **PDC Emulator** – Password , time-a nezaret edir
* **Infrastructure Master** – Umumi infrastruktura nezaret edir

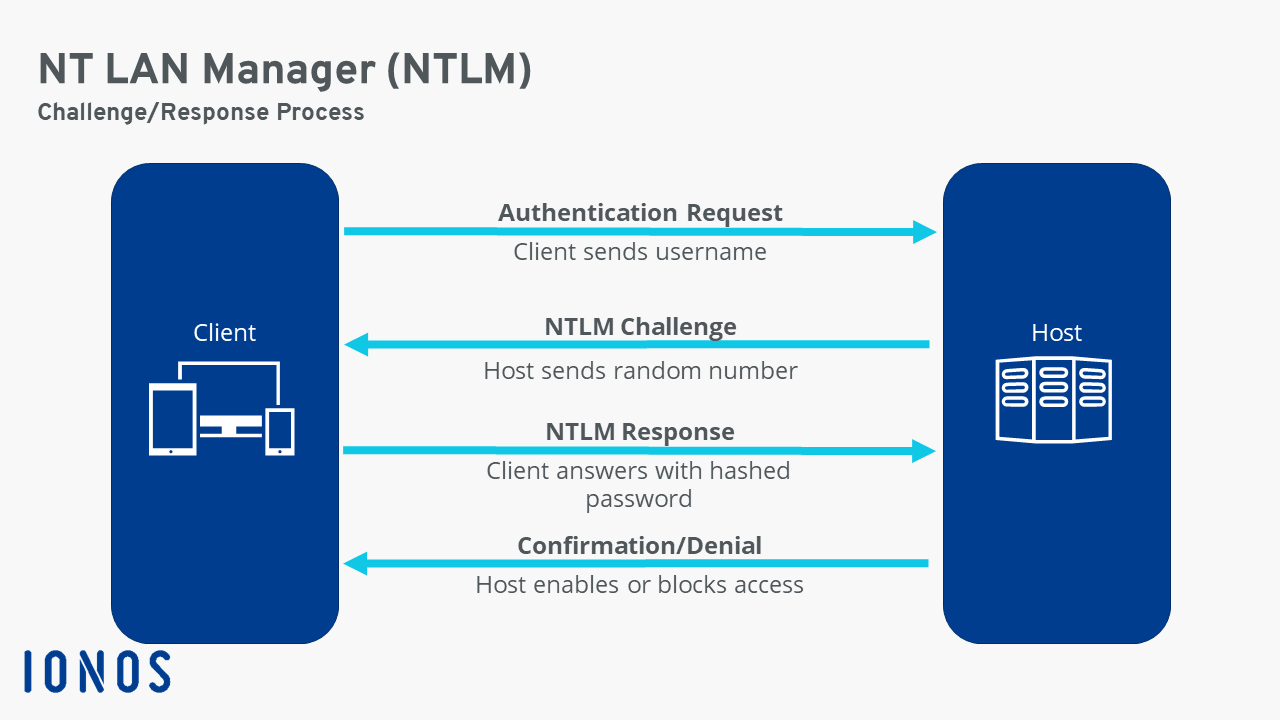
**Trust-Relationships**

1. **One-way trust:** If A domain trusts B domain then B can access resources of A domain, users can verify themselves

**Outgoing/Incoming trust->**If A trusts B then A is outgoing , B is incoming

1. **Two-way trust:** If A domain trusts B domain and wise verse. And both domains can access their resources
2. **Transitive trust:** If A domain trusts B domain and B domain trusts C domain then A domain trusts C domain.(must be two way trust between domains) A=B B=C => A=C
3. **Non-Transitive:** If A domain trusts B domain and B domain trusts C domain then *A domain do not trusts C domain*.(must be two way trust between domains) A=B B=C => A!=C
4. **Parent-Child trust:** It is default trust, If millisec.org is DC and it have baki.millisec.org child domain trust between them called parent-child trust.
5. **Tree-Root trust:** If root domain trusts tree domain domain
6. **Shortcut trust:** If millisec.local wants trust ygunesli.yusif.com. (don’t need other trust(parent , tree-root)
7. **Realm trust:** If one domain is linux another one is Windows (Kerberos v5 needed)
8. **Forest trust:** If you have a.com and b.com and you want to combine them. If they are in different countries you need to use Site-to-site VPN)
9. **External trust:** Windows<=>Windows NT

**NTLM**



1. User authentication ucun baglanmaq istediyi servere oz username-in gonderir
2. Host bu useri ferqlendirmek ucun ona random number verir(NTLM challenge)
3. Challenge hissesi ile hashi gonderir server eve o da oz databasesinde yoxlayir(response)
4. Access or Block

**LDAP (Lightweight Data Access Protocol)**

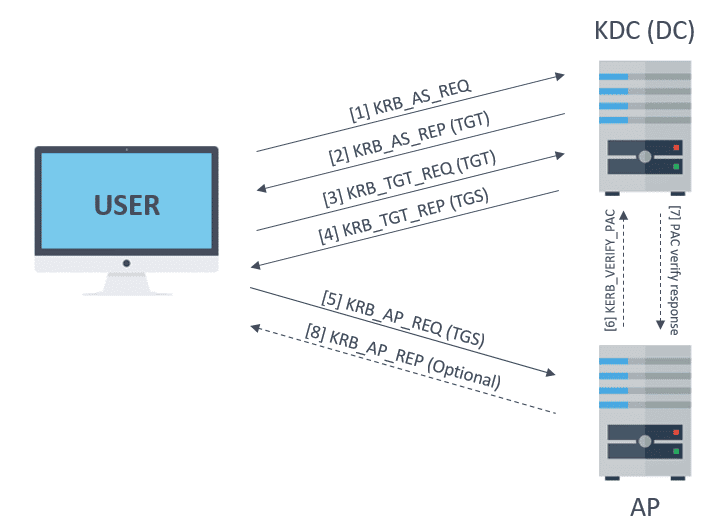
1. Authenticasiya ucun istifade olunur
2. Research Sharing ucun istifade olunur

LDAP->389 port

LDAP over SSL(secure)->636 port

NTLM kimidir

**KERBEROS (88,464)**



**KDC-**Key Distribution Center

**TGT-**Ticket Granted Ticket

**TGS-**Ticket Granting Service

**UPN-**User Principal Name(whoami /upn) -Domain adinin login olanda ferqli gorsenmesi ucun. millisec.org->millisec.platform

**AD Notes**

Windowsda fayl paylasmaq olmur, qovlugu paylasmaq olur

**Group Policy** – OUlara verilir

**Delegation-** One of the nice things you can do in AD is to give specific users some control over some OUs. This process is known as **delegation** and allows you to grant users specific privileges to perform advanced tasks on OUs without needing a Domain Administrator to step in.

**SYSVOL**-GP-larin saxlandigi yer

# **Hardware**

**Intel vs AMD -** Intel və AMD kompüterlər üçün prosessorlar (CPU) istehsal edən iki rəqib şirkətdir. Onlar arxitektura, performans, enerji istehlakı və qiymət baxımından fərqlənir, istifadəçilərə xüsusi ehtiyacları və üstünlükləri əsasında müxtəlif platformalar arasında seçim təklif edir.

**SSD vs HDD -** SSD (Solid State Drive) və HDD (Hard Disk Drive) texnologiya və performans baxımından fərqlənən saxlama cihazlarıdır. SSD-lər fırlanan maqnit disklərdən istifadə edən HDD-lərlə müqayisədə daha sürətli məlumat əldə etmək, daha az enerji sərfiyyatı və artan dayanıqlıq təklif edərək yaddaş üçün fləş yaddaşdan istifadə edir. Daha sürətli yükləmə müddətləri, təkmilləşdirilmiş sistem reaksiyası və daha yaxşı ümumi performans üçün SSD-lərə ehtiyacımız var, HDD-lər isə gigabayt üçün daha aşağı qiymətə daha böyük yaddaş tutumları təklif edərək, onları toplu saxlama ehtiyacları üçün uyğun edir.

**Power Supply -** Enerji təchizatı, sabit və tənzimlənən gərginlik və cərəyan təmin edən bir mənbədən elektrik enerjisini elektron cihazlar üçün istifadə edilə bilən gücə çevirən bir cihazdır.

**LED vs OLED vs PLASMA -**

LED (Light Emitting Diode) və OLED (Organic Light Emitting Diode) işıq yayan mexanizmləri və materialları ilə fərqlənən ekran texnologiyalarıdır. LED maye kristal displey (LCD) panelinin arxasında arxa işıqdan istifadə edir, OLED isə birbaşa üzvi birləşmələrdən işıq saçır.

Plazma displeylər işıq yaymaq üçün yüklü qazlardan istifadə edir. Enerji səmərəliliyi və uzun ömür müddəti təklif edən LED, canlı rənglər və nazik forma faktorları təmin edən OLED və dərin qara rənglər və geniş baxış bucaqları təklif edən Plazma ilə müxtəlif tətbiqlər üçün bu ekran texnologiyalarına ehtiyacımız var.

# **Linux**

**What is Linux , Diff Windows -** Linux Unix-ə bənzər əməliyyat sistemi **nüvəsidir** və müxtəlif Linux paylamalarının əsasını təşkil edir və onu əməliyyat sistemlərinin əsas komponentinə çevirir.

Windows-dan fərqli olaraq, Linux open source , yəni onun mənbə kodu hər kəs üçün dəyişdirilə və paylaya bilər, bu, birgə inkişaf mühitini təşviq edir və istifadəçilərə daha çox nəzarət və fərdiləşdirmə seçimləri təklif edir.

**Client Linux** sistemlərinə misal olaraq Ubuntu Desktop, Fedora Workstation və Linux Mint daxildir.

**Server Linux** sistemləri üçün nümunələrə Ubuntu Server, CentOS və Debian Server daxildir.

**What is Alias** - Alias Linux-da başqa daha uzun və ya daha mürəkkəb komandaya təyin edilmiş stenoqrafiya ad və ya əmrdir. O, istifadəçilərə tez-tez istifadə olunan əmrlər üçün fərdi qısa yollar yaratmağa imkan verməklə, vaxta qənaət etməklə və yazma zamanı xəta riskini azaltmaqla iş axınını tənzimləməyə kömək edir.

**File systems -** Linux-da fayl sistemlərinin iş prinsipi məlumatların nüvə tərəfindən idarə olunan və sistem zəngləri vasitəsilə əldə edilən fayl və qovluqlara təşkil edilməsini nəzərdə tutur.

Linux-da sistem faylları əsasən konfiqurasiya fayllarını ehtiva edən /etc qovluğunda yerləşir, /bin, /home, /lib, /tmp və /var kimi qovluqlar isə əsas ikili faylları, istifadəçi ev qovluqlarını, paylaşılan kitabxanaları saxlamaq kimi xüsusi məqsədlərə xidmət edir. , müvəqqəti fayllar və dəyişən məlumatlar.

**PAM Linux , SE Linux –**

Linux-da PAM (Pluggable Authentication Modules) inzibatçılara autentifikasiya siyasətlərini fərdiləşdirməyə və tətbiq etməyə imkan verən autentifikasiyaya çox yönlü yanaşma təklif edir.

SELinux (Security-Enhanced Linux) məcburi giriş nəzarətləri vasitəsilə sistemin təhlükəsizliyini gücləndirir, prosesləri əvvəlcədən müəyyən edilmiş siyasətlərə uyğun olaraq məhdudlaşdırır və ümumi sistemin dayanıqlığını gücləndirir.

**Commands in Linux -** Linux-da əmrlər adətən /bin, /sbin, /usr/bin, /usr/sbin və /usr/local/bin kimi sistemin PATH mühit dəyişənində müəyyən edilmiş kataloqlarda yerləşir.

The /bin directory in Linux contains essential system binaries that are crucial for basic system functionality and are accessible to all users. In contrast, the /sbin directory stores system binaries primarily used by administrators for system maintenance and management tasks, which typically require elevated privileges.

**Shell vs Kernel -** Kernel, hardware resurslarının idarə edilməsinə və tətbiqlərə əsas xidmətlərin təmin edilməsinə cavabdeh olan əməliyyat sisteminin əsas komponentidir. Bunun əksinə olaraq, shell istifadəçilərə əmrlər və skriptləri yerinə yetirməklə əməliyyat sistemi ilə qarşılıqlı əlaqə yaratmağa imkan verən komanda xətti tərcüməçisidir.

**Sudo command vs Sudo group** - "Sudo" əmri istifadəçilərə adətən autentifikasiya tələb edən yüksək imtiyazlara malik əmrləri yerinə yetirməyə imkan verir.

Bunun əksinə olaraq, "sudo" qrupu Linux sistemində üzvlərə "sudo" əmrindən istifadə etmək icazəsi verən qrupdur. Bizə həm təhlükəsiz, həm də idarə olunan giriş idarəetmə sistemini tətbiq etmək lazımdır ki, bu da müəyyən istifadəçilərə və ya qruplara sistemin bütövlüyünü qoruyarkən imtiyazlı əməliyyatlar həyata keçirməyə imkan verir.

**What is Regex -** Regex, müntəzəm ifadənin qısaldılması, mətni uyğunlaşdırmaq və manipulyasiya etmək üçün istifadə olunan axtarış modelini təyin edən simvollar ardıcıllığıdır. Mətn məlumatları ilə səmərəli işləmək üçün güclü və çevik alət təmin edən mətn emalı, nümunə uyğunluğu, məlumatların yoxlanılması və sətir manipulyasiyası kimi tapşırıqlar üçün regex lazımdır.

SUDO - /etc/sudoers

% -qrup

# **Red Team**

**Osi Model Attacks –**



**ATTACKS:**

**Brute Force:** Təcavüzkarların sistemə və ya hesaba icazəsiz giriş əldə etmək üçün simvol və ya parolların bütün mümkün kombinasiyalarını sınadığı üsul. O, adətən avtomatlaşdırılmışdır və çox vaxt apara bilər, lakin parollar zəif olduqda effektivdir.

**DoS (Xidmətdən imtina):** Təcavüzkarlar sistemə, serverə və ya şəbəkəyə onun resurslarını aşmaq üçün trafiklə dolur, bunun istifadəçilər üçün əlçatmaz olmasına səbəb olur. Buna həddindən artıq sorğu göndərmək və ya zəifliklərdən istifadə etmək kimi müxtəlif vasitələrlə nail olmaq olar.

**SQL injection:** Backend verilənlər bazasını manipulyasiya etmək üçün giriş sahələrinə SQL kodu daxil etməklə veb proqramlardakı zəifliklərdən istifadə etmək. Təcavüzkarlar məlumatları çıxara, dəyişdirə və ya silə, bəzi hallarda hətta serverdə ixtiyari əmrləri yerinə yetirə bilərlər.

**XSS (Cross-Site Scripting):** Təcavüzkarlar digər istifadəçilər tərəfindən baxılan veb səhifələrə zərərli skriptlər yeridirlər. Bu skriptlər kukilər, sessiya nişanları kimi həssas məlumatları oğurlaya və ya hətta istifadəçiləri fişinq saytlarına yönləndirə bilər.

**XML injection:** Zərərli kodu və ya obyektləri yeritmək üçün XML analizatorlarındakı boşluqlardan istifadə etmək, potensial olaraq məlumat sızmasına, xidmətdən imtinaya və ya arxa sistemlərə icazəsiz girişə gətirib çıxarır.

**JWT (JSON Veb Token):** Veb proqramları və ya API-lər daxilində icazəsiz giriş əldə etmək və ya imtiyazları artırmaq üçün tez-tez autentifikasiya üçün istifadə edilən JSON Veb Tokenlərini manipulyasiya etmək.

**SSRF (Server Side Request Forgery):** Daxili və ya xarici resurslara icazəsiz sorğular etmək üçün istifadəçi tərəfindən təmin edilən daxiletmədə serverin etibarından istifadə etmək. Bu, məlumatların oğurlanmasına, icazəsiz girişə və ya hətta server tərəfdən hücumlara səbəb ola bilər.

**CSRF (Cross-Site Request Forgery):** Doğrulanmış istifadəçiləri onların razılığı olmadan veb proqramında bilmədən hərəkətlər etməyə aldatmaq. Bu, hesabın ələ keçirilməsinə, məlumatların manipulyasiyasına və ya icazəsiz əməliyyatlara səbəb ola bilər.

**Clickjacking:** İstifadəçiləri veb-səhifədə gizli və ya maskalanmış elementlərə klikləməklə aldatmaq, onları gözlənilməz hərəkətlərə və ya həssas məlumatları aşkara çıxarmaq.

**Fişinq:** Təcavüzkarların istifadəçiləri parollar və ya maliyyə təfərrüatları kimi həssas məlumatları açıqlamaq üçün aldatmaq üçün qanuni şəxsləri təqlid etdiyi sosial mühəndislik hücumu.

**MITM (Man-in-the-Middle):** İki tərəf arasında onların xəbəri olmadan əlaqəni kəsmək və bəlkə də dəyişdirmək. Bu, həssas məlumatları dinləmək və ya tranzit zamanı məlumatlarla manipulyasiya etmək üçün istifadə edilə bilər.

**ARP zəhərlənməsi:** Saxta Ünvan Qəbul Protokolu (ARP) mesajları göndərməklə şəbəkə trafikinin yönləndirilməsi, ələ, modifikasiyaya və ya xidmət hücumlarının rədd edilməsinə səbəb olur.

**Golden/Silver/Diamond ticket attack:** Sistemlərə və ya xidmətlərə icazəsiz giriş əldə etmək üçün ticket verən biletləri (TGT) saxtalaşdırmaq və ya oğurlamaqla Kerberos autentifikasiya protokollarından istifadə etmək.

**LDAP pass back attcak:** identifikasiya sorğularını təcavüzkar tərəfindən idarə olunan serverlərə yönləndirmək üçün LDAP referallarından istifadə edərək, autentifikasiya məlumatlarının tutulmasına və ya manipulyasiyasına imkan verir.

**NTLM relay hücumu:** Şəbəkə resurslarına icazəsiz giriş əldə etmək və ya imtiyazları artırmaq üçün NTLM autentifikasiya sorğularının tutulması və ötürülməsi.

**Local / Remote File Inclusion :** LFI, proqram təcavüzkarın veb brauzer vasitəsilə serverə yerli fayl daxil etməsinə icazə verdikdə baş verir. Bu, ixtiyari kodun icrasına, həssas məlumatların açıqlanmasına və ya hətta tam server kompromislərinə səbəb ola bilər.

RFI, digər tərəfdən, təcavüzkarlara xarici serverdən uzaq faylları daxil etməyə imkan verir. Bu, uzaq serverdə yerləşdirilən zərərli skriptləri icra etmək üçün istifadə edilə bilər ki, bu da LFI kimi oxşar nəticələrə, o cümlədən uzaqdan kodun icrası və server güzəştinə gətirib çıxarır.

**Path Traversal:** Veb serverin kök kataloqundan kənar fayllara və ya qovluqlara daxil olmaq üçün girişin doğrulanması zəifliklərindən istifadə, potensial olaraq məlumat sızmasına və ya uzaqdan kod icrasına gətirib çıxarır.

**DNS zəhərlənməsi:** İstifadəçiləri zərərli və ya saxta veb-saytlara yönləndirmək, kommunikasiyalara müdaxilə etmək və ya şəbəkə xidmətlərini pozmaq üçün DNS qeydlərinə müdaxilə.

**DHCP starvation:** Çoxlu IP ünvanları tələb etməklə DHCP ünvan hovuzlarının tükənməsi, şəbəkəyə qoşulmağa cəhd edən qanuni cihazların xidmətdən imtinasına gətirib çıxarır.

**Active recon:** Port skanerləri, şəbəkə xəritəçiləri və ya zəiflik skanerləri kimi alətlərdən istifadə edərək hədəf şəbəkə və ya sistem haqqında aktiv şəkildə araşdırma və məlumat toplamaq.

**Passiv recon:** Hədəf şəbəkəsi və ya sistemlə birbaşa əlaqə yaratmadan, çox vaxt sosial media, forumlar və ya axtarış motorları kimi açıq mənbələr vasitəsilə məlumat toplamaq.

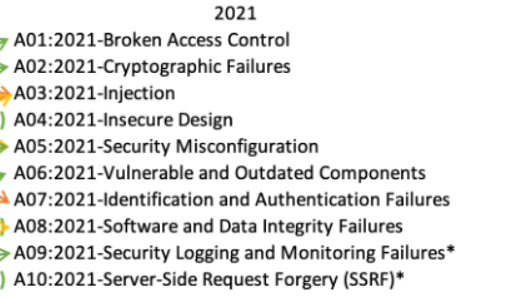
**Spoofing:** Sistemləri və ya istifadəçiləri aldatmaq üçün tez-tez şəbəkə hücumlarında istifadə olunan başqa bir qurumun timsalında məlumat və ya şəxsiyyətin saxtalaşdırılması.

**Sniffing:** Parollar, sessiya işarələri və ya məxfi məlumatlar kimi həssas məlumatları ələ keçirmək üçün şəbəkə trafikinin tutulması və təhlili.

**Path the Hash**: Plain text parollarına ehtiyacdan yan keçərək, başqa mənbədən əldə edilmiş hashed etimadnaməsini istifadə edərək sistemə autentifikasiya.

**Path the Ticket:** İcazəsiz giriş əldə etmək və ya şəbəkə daxilində imtiyazları artırmaq üçün oğurlanmış Kerberos biletlərindən istifadə edərək sistemə autentifikasiya.

**LLMNR zəhərlənməsi:** Şəbəkə trafikini yönləndirmək üçün Link-Local Multicast Name Resolution (LLMNR) protokolundan istifadə, potensial olaraq ortadakı adam hücumlarına və ya məlumatın açıqlanmasına gətirib çıxarır.

****

**APT Groups -** APT (Advanced Persistent Threat) qrupları xüsusi hədəflərə qarşı mürəkkəb və uzunmüddətli hücumlar həyata keçirmək qabiliyyətinə və niyyətinə malik, çox vaxt dövlət tərəfindən maliyyələşdirilən təşkil edilmiş kibertəhlükə aktyorlarıdır. Hücumlarından effektiv müdafiə etmək üçün APT qruplarını başa düşməliyik, çünki onlar ənənəvi təhlükəsizlik tədbirlərindən yayına bilən və təşkilatlara və kritik infrastruktura əhəmiyyətli ziyan vura bilən qabaqcıl taktika, texnika və prosedurlardan (TTP) istifadə edirlər.

**VPN and Proxy -** VPN (Virtual Şəxsi Şəbəkə) internet trafikini şifrələyir və onu uzaq server vasitəsilə yönləndirir, istifadəçinin IP ünvanını maskalamaq və məlumat ötürülməsini şifrələməklə məxfilik və təhlükəsizliyi təmin edir.

Proksilər istifadəçilər və internet arasında vasitəçi kimi çıxış edərək, onlara məzmuna anonim daxil olmaq və geo məhdudiyyətləri keçmək imkanı verir, məxfiliyi və təhlükəsizliyi artırır, eyni zamanda internet sürətini və performansını artırır.

# **Blue Team**

**What is SOC-** Security Operations Center (SOC) kibertəhlükəsizlik insidentlərinin monitorinqi, aşkarlanması, təhlili və reaksiyasına cavabdeh olan mərkəzləşdirilmiş bölmədir. SOC-lar təhlükənin vaxtında aşkarlanması, insidentlərə cavab verilməsi və təsirlərin azaldılması səyləri üçün vacibdir. Tipik olaraq, SOC personalına security analysts, incident responders, threat intelligence analysts, and SOC managers daxildir.

**TOOLS:**

**SIEM:** Security Information and Event Management (SIEM) təhdidlərin aşkarlanması, insidentlərə reaksiya və uyğunluq hesabatı imkanlarını təmin etmək üçün müxtəlif mənbələrdən təhlükəsizlik hadisəsi məlumatlarını birləşdirən və təhlil edən proqram həllidir.

**XDR:** Extended Detection and Response (XDR) son nöqtələr, şəbəkələr və bulud mühitlərində mərkəzləşdirilmiş görünmə, aşkarlama və cavab imkanlarını təmin etmək üçün çoxsaylı təhlükəsizlik məhsullarını və texnologiyalarını birləşdirən təhlükəsizlik həllidir.

**EDR:** Endpoint Detection and Response (EDR) real vaxt rejimində kompüterlər, serverlər və mobil qurğular kimi son nöqtələrdə təhdidlərin aşkarlanması və azaldılmasına yönəlmiş kibertəhlükəsizlik texnologiyasıdır.

**MDR:** Managed Detection and Response ( (MDR) kibertəhlükəsizlik təchizatçıları tərəfindən təmin edilən xidmətdir və təşkilatlara davamlı monitorinq, təhlükənin aşkarlanması və insidentlərə reaksiya imkanları təklif edir, adətən üçüncü tərəf provayderinə verilir.

**SOAR:** Security Orchestration, Automation, and Response (SOAR) platformaları təhlükəsizlik qruplarına insidentlərə cavab, təhlükə kəşfiyyatı və iş axınının idarə edilməsi daxil olmaqla təhlükəsizlik əməliyyatlarını avtomatlaşdırmağa və sadələşdirməyə kömək edir.

**Firewall:** Firewall icazəsiz girişin qarşısını almaq və kibertəhlükələrdən qorunmaq üçün əvvəlcədən müəyyən edilmiş təhlükəsizlik qaydaları əsasında daxil olan və gedən şəbəkə trafikini izləyən və idarə edən şəbəkə təhlükəsizlik cihazı və ya proqram təminatıdır.

**Firewall növləri:** Firewallları müxtəlif növlərə bölmək olar, məsələn, Packet Filtering Firewalls, Stateful Inspection Firewalls, Proxy Firewalls, Next-Generation Firewalls, and Application Layer Firewalls, hər biri müxtəlif səviyyəli təhlükəsizlik və funksionallıq təklif edir.

**Paket Filtrləmə Firewallları** məlumat paketlərini şəbəkədən keçərkən yoxlayır və mənbə və təyinat IP ünvanları, port nömrələri və protokol növləri kimi əvvəlcədən müəyyən edilmiş meyarlar əsasında onlara icazə vermək və ya bloklamaq barədə qərarlar qəbul edir.

**Statefull firewall** aktiv əlaqələrin vəziyyətini izləyir və trafikin kontekstinə əsasən qərarlar qəbul edir, yalnız qanuni əlaqələrə icazə verir və icazəsiz girişin qarşısını alır.

**Proksi Firewalllar** müştərilər və serverlər arasında vasitəçi rolunu oynayır, müştəri adından şəbəkə trafikini ələ keçirir və süzür, daxili şəbəkə detallarını xarici mənbələrdən gizlətməklə əlavə təhlükəsizlik səviyyəsini təmin edir.

**Next Generation Firewalls** müdaxilənin qarşısının alınması, tətbiq məlumatlılığı və istifadəçinin identifikasiyası kimi qabaqcıl təhlükəsizlik xüsusiyyətlərini birləşdirir, ənənəvi paket filtrindən və vəziyyətlə bağlı yoxlamadan kənar təkmil təhlükə aşkarlama və təsirləri azaltma imkanları təklif edir.

**Application Layeri Firewallları** OSI modelinin tətbiqi səviyyəsində işləyir, xüsusi proqram protokolları və məzmunu əsasında trafiki yoxlayır və süzür, şəbəkə trafiki üzərində ətraflı nəzarəti təmin edir və tətbiq səviyyəli hücumlardan qoruyur.

**Antivirus**: Antivirus proqramı kompüter sistemləri və şəbəkələrindən viruslar, qurdlar, troyanlar və casus proqramlar kimi zərərli proqramları (zərərli proqramları) aşkar etmək, qarşısını almaq və aradan qaldırmaq üçün nəzərdə tutulmuşdur.

**DLP:** Data Loss Prevention (DLP) həssas məlumatları həm təşkilat daxilində, həm də ondan kənarda icazəsiz giriş, istifadə və ötürülmədən qorumaq üçün istifadə olunan alətlər və texnologiyalar toplusuna aiddir.

**DRP**: Disaster Recovery Plan (DRP) fəlakət və ya dağıdıcı insident zamanı İT infrastrukturunun və əməliyyatların bərpası və bərpası üçün prosedurları və strategiyaları əks etdirən sənədləşdirilmiş və strukturlaşdırılmış yanaşmadır.

**Ticket sistemi:** Bilet sistemi, xidmət sorğularını, insidentləri və tapşırıqları mərkəzləşdirilmiş qaydada idarə etmək və izləmək üçün İT və təhlükəsizlik qrupları tərəfindən istifadə olunan proqram təminatıdır və səmərəli iş axınının idarə edilməsini və kommunikasiyanı asanlaşdırır.

**IDS:** Intrusion Detection System (IDS) zərərli fəaliyyətlər və ya siyasət pozuntuları üçün şəbəkə və ya sistem fəaliyyətlərini izləyən və aşkar edilmiş təhdidlərə cavab olaraq xəbərdarlıqlar yaradan və ya digər tədbirlər görən təhlükəsizlik texnologiyasıdır.

**IPS:** Intrusion Prevention System (IPS) aşkar edilmiş təhdidlərin şəbəkə və ya sistemə zərər verməsini aktiv şəkildə bloklamaq və ya qarşısını almaqla IDS-in imkanlarından kənara çıxan təhlükəsizlik texnologiyasıdır.

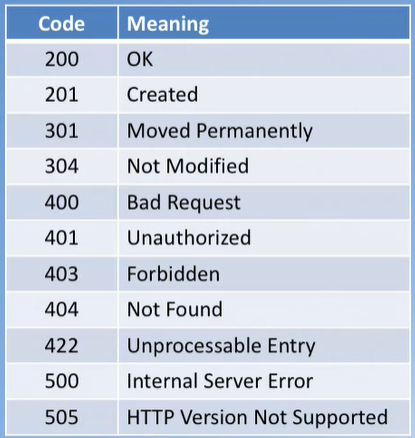
**HIDS:** Host-based Intrusion Detection System (HIDS) zərərli fəaliyyət əlamətləri və ya siyasət pozuntuları üçün fərdi hostlar və ya son nöqtələrdə fəaliyyətə nəzarət edən və təhlil edən müdaxilənin aşkarlanması sistemidir.

**NIDS:** Şəbəkəyə əsaslanan müdaxilənin aşkarlanması sistemi (NIDS), adətən şəbəkə infrastrukturunun strateji nöqtələrində yerləşdirilən şübhəli fəaliyyət və ya məlum hücum imzaları üçün şəbəkə trafikinə nəzarət edən müdaxilənin aşkarlanması sistemidir.

**İdentifikasiya, Avtorizasiya, Autentifikasiya arasındakı fərq:** İdentifikasiya şəxsiyyətin iddia edilməsi prosesidir, autentifikasiya iddia edilən şəxsiyyətin yoxlanılması prosesidir və avtorizasiya, təsdiqlənmiş şəxsiyyət əsasında giriş hüquq və imtiyazlarının verilməsi və ya rədd edilməsi prosesidir.

**SSL və TLS:** SSL (Secure Sockets Layer) və TLS (Nəqliyyat Layeri Təhlükəsizliyi) internet kimi kompüter şəbəkəsi üzərindən rabitənin təhlükəsizliyini təmin etmək üçün istifadə edilən kriptoqrafik protokollardır. TLS SSL-in varisidir və şəbəkə üzərindən ötürülən məlumatların məxfiliyini və bütövlüyünü təmin edərək müştərilər və serverlər arasında təhlükəsiz rabitə kanallarını təmin edir.

**Http status codes -**



**Types of VPN-**

**Remote Access VPN:** Fərdi istifadəçilərə adətən şifrələnmiş tunellər və autentifikasiya mexanizmlərindən istifadə edərək internet üzərindən uzaq bir yerdən şəxsi şəbəkəyə təhlükəsiz qoşulmağa imkan verir.

**Site-to-Site VPN:** Çoxlu fiziki yerlər və ya şəbəkələr arasında təhlükəsiz bağlantılar qurur və onlara internet kimi ictimai şəbəkələr üzərindən təhlükəsiz əlaqə saxlamağa imkan verir.

**Client-to-Site VPN:** Remote Access VPN-ə bənzəyir, lakin fərdi müştəri cihazlarının təhlükəsiz şəkildə korporativ şəbəkəyə qoşulmasını nəzərdə tutur, tez-tez uzaqdan işləyən və ya səyahət edən işçilər tərəfindən istifadə olunur.

**Intranet VPN:** Bir təşkilatın şəxsi şəbəkəsinin çoxsaylı uzaq yerlərini və ya filiallarını təhlükəsiz şəkildə internet üzərindən birləşdirərək, problemsiz əlaqəni və paylaşılan resurslara çıxışı təmin edir.

**Extranet VPN:** Müxtəlif təşkilatlar arasında təhlükəsiz əməkdaşlığa və resurs mübadiləsinə imkan verən biznes tərəfdaşları, təchizatçılar və ya müştərilər kimi xarici tərəfləri daxil etmək üçün intranet VPN-in imkanlarını genişləndirir.

**Encryption and Cryptography –**

Şifrələmə, icazəsiz girişin qarşısını almaq üçün məlumatın koda çevrilməsi prosesidir, kriptoqrafiya isə təhlükəsiz ünsiyyət üçün üsulların öyrənilməsi və tətbiqidir. Həssas məlumatları qorumaq və rəqəmsal rabitə və əməliyyatlarda məxfiliyi və təhlükəsizliyi təmin etmək üçün ona ehtiyacımız var.

**True Positive :** Həyəcan siqnalı verməyə səbəb olan qanuni hücum.

Sizdə brute force xəbərdarlığı var və o, tetikler. Siz xəbərdarlığı araşdırırsınız və kiminsə həqiqətən də brute force metodları ilə sistemlərinizdən birinə daxil olmağa çalışdığını öyrənirsiniz.

**False Positive :** Hücum baş vermədikdə həyəcan siqnalı verən hadisə.

Siz bu brute force xəbərdarlıqlarından birini araşdırırsınız və bunun real hücum deyil, parolunu dəfələrlə səhv yazan bir istifadəçi olduğunu öyrənirsiniz.

**False Negative :** Hücum baş verdikdə həyəcan siqnalı verilmədikdə.

Kimsə sisteminizə daxil olmağa çalışırdı, lakin bunu sizin brute force hücumu məntiqinizin limitindən az etdi. Məsələn, siz qaydanızı bir dəqiqə ərzində on uğursuz giriş axtarmaq üçün təyin etdiniz və təcavüzkar yalnız 9-u etdi. Hücum baş verdi, lakin nəzarətiniz onu aşkar edə bilmədi.

**True Negative :** Heç bir hücumun baş vermədiyi və aşkarlanmadığı bir hadisə.

Heç bir hücum baş vermədi və sizin qaydanız triggerlənmədi.

**Encryption vs Hashing and Salting :**

**Şifrələmə:** Şifrələmə, şifrələmə alqoritmi və açardan istifadə edərək verilənlərin oxunmaz formata çevrildiyi geri çevrilən bir prosesdir. Şifrələmənin məqsədi verilənlərin məxfiliyini qorumaq, yalnız səlahiyyətli tərəflərin orijinal məlumatlara daxil ola bilməsini və deşifrə edə bilməsini təmin etməkdir.

**Hashing:** Hashing, verilənlərin hash funksiyasından istifadə edərək sabit ölçülü simvollar sətirinə çevrildiyi geri dönməz bir prosesdir. Nəticə hash giriş məlumatı üçün unikaldır, lakin orijinal məlumatları əldə etmək üçün geri qaytarıla bilməz. Hashing adətən məlumatların bütövlüyünün yoxlanılması, parolun saxlanması və rəqəmsal imza üçün istifadə olunur.

**Salting** təhlükəsizliyi artırmaq üçün hashing-də, xüsusən də parol saxlamasında istifadə olunan bir texnikadır. Hashing etməzdən əvvəl giriş məlumatlarına təsadüfi məlumatların ("duz" adlanır) əlavə edilməsini nəzərdə tutur. Bu, iki istifadəçi eyni parola malik olsa belə, hər parola əlavə edilən unikal duza görə onların heşlənmiş dəyərlərinin fərqli olacağını təmin edir. Salting, təcavüzkarların ümumi parollar üçün hashləri əvvəlcədən hesabladıqları göy qurşağı cədvəli hücumları kimi hücumlardan müdafiə edir.

**Symmetric vs Asymmetric Encryption:**

Simmetrik şifrələmə həm şifrələmə, həm də deşifrə üçün eyni açardan istifadə edir. Böyük həcmdə məlumat üçün effektivdir, lakin təhlükəsiz açar mübadiləsi tələb edir.

Asimmetrik şifrələmə bir cüt açardan istifadə edir: şifrələmə üçün açıq açar və şifrənin açılması üçün şəxsi açar. Bu, təhlükəsiz açar mübadiləsi ehtiyacını aradan qaldırır, lakin böyük həcmdə məlumat üçün daha yavaş ola bilər. O, adətən rəqəmsal imzalar və etibarsız şəbəkələr üzərindən təhlükəsiz rabitə kimi ssenarilərdə istifadə olunur.

Examples: Symmetric Encryption:

* AES (Advanced Encryption Standard)
* DES (Data Encryption Standard)
* Blowfish

Asymmetric Encryption:

* RSA (Rivest-Shamir-Adleman)
* DSA (Digital Signature Algorithm)
* Elliptic Curve Cryptography (ECC)

MD5 and SHA-1 are older hash functions vulnerable to collision attacks and should be avoided for new applications.

SHA-256 and SHA-512 are part of the SHA-2 family and offer significantly stronger security. SHA-512 provides stronger security due to its longer hash length and larger word size.

# **SOC**

**What is ISO 2700 -**

ISO 27000 ailəsi informasiya təhlükəsizliyi idarəetmə sistemləri (ISMS) üçün nəzərdə tutulmuş standartlar toplusudur. ISO 27001 təşkilatın ümumi biznes riskləri kontekstində İBS-nin yaradılması, həyata keçirilməsi, saxlanması və davamlı olaraq təkmilləşdirilməsi üçün tələbləri xüsusi olaraq təsvir edir.

**What is NIST, COBIT , Playbook –**

**NIST (Milli Standartlar və Texnologiya İnstitutu)** təşkilatlara kibertəhlükəsizlik risklərini effektiv şəkildə idarə etmək və azaltmaqda kömək etmək üçün kibertəhlükəsizlik çərçivələri və təlimatlar təqdim edir.

**COBIT (İnformasiya və Əlaqədar Texnologiyalar üçün Nəzarət Məqsədləri)** biznes məqsədlərinə və maraqlı tərəflərin ehtiyaclarına uyğunluğu təmin edən müəssisə İT-nin idarə edilməsi və idarə edilməsi üçün çərçivə təklif edir.

**Playbook -** kibertəhlükəsizlik qrupları tərəfindən təhlükəsizlik insidentlərinə səmərəli şəkildə cavab vermək və onlardan bərpa etmək, insidentlərin idarə edilməsinə strukturlaşdırılmış yanaşma təmin etmək və kibertəhlükələrin təsirini minimuma endirmək üçün istifadə olunan sənədləşdirilmiş prosedurlar və təlimatlar toplusudur.

**What is Incident Responce Plan –**

Insident Cavab Planı (IRP) təşkilat daxilində kibertəhlükəsizlik insidentlərinə cavab olaraq görüləcək prosedurları və tədbirləri təsvir edir. O, adətən, hazırlıq, aşkarlama, saxlama, məhv etmə, bərpa və öyrənilmiş dərslər kimi addımları əhatə edir. IRP təhlükəsizlik pozuntularının təsirini minimuma endirmək, bərpa müddətini azaltmaq və insidentlərə koordinasiyalı və effektiv reaksiyanı təmin etmək üçün vacibdir.

JOBS –

**Digital forensics-** kiber əlaqəli insidentləri və ya cinayətləri başa düşmək və yenidən qurmaq üçün rəqəmsal sübutların toplanması, qorunması, təhlili və təqdim edilməsini əhatə edir.

**Malware anaytics -** onun davranışını, funksionallığını və təsirini anlamaq üçün zərərli proqram təminatını araşdırır, kibertəhlükələrə qarşı müdafiə və əks tədbirlərin inkişafına kömək edir. Thread Hunter - zərər verməzdən əvvəl təhdidləri aşkar etmək və azaltmaq üçün təşkilatın şəbəkələri və sistemləri daxilində zərərli fəaliyyət əlamətlərini fəal şəkildə axtarırlar.

**SOC (Təhlükəsizlik Əməliyyatları Mərkəzi)** səviyyələri 1, 2 və 3 təhlükəsizlik komandası daxilində əsas insidentlərin monitorinqi və təhlilindən tutmuş qabaqcıl təhlükənin aşkarlanması və cavab reaksiyasına qədər müxtəlif təcrübə və məsuliyyət səviyyələrini təmsil edir. SOC meneceri

**SOC Manager -** Mərkəzinin əməliyyatlarına və işçi heyətinə nəzarət edir, təhlükəsizlik insidentlərinə effektiv koordinasiya və reaksiyanı təmin edir.

**Baş İnformasiya Təhlükəsizliyi Mütəxəssisi (CISO) -** informasiya aktivləri və texnologiyalarının kibertəhlükələrdən adekvat şəkildə qorunmasını təmin etmək, təhlükəsizlik təşəbbüslərini biznes məqsədləri və tənzimləyici tələblərlə uyğunlaşdırmaq üçün təşkilatın baxışını, strategiyasını və proqramlarını yaratmaq və saxlamaq üçün məsuliyyət daşıyır. Bu rollar kibertəhlükələrdən fəal şəkildə müdafiə etmək, təhlükəsizlik insidentlərini aşkar etmək və onlara cavab vermək və təşkilatın ümumi təhlükəsizlik vəziyyətini təmin etmək üçün vacibdir.

**Logs Collection –**

Log serverlər, şəbəkə cihazları və proqramlar kimi müxtəlif mənbələrdən toplanır və daha sonra SIEM (Təhlükəsizlik Məlumatı və Hadisə İdarəetmə) sisteminə göndərilməzdən əvvəl log kollektorları tərəfindən normallaşdırılır və birləşdirilir. SIEM sistemləri təhlükəsizlik hadisələrini müəyyən etmək, əlaqəli hadisələri əlaqələndirmək və potensial təhlükəsizlik insidentləri üçün xəbərdarlıqlar yaratmaq üçün qeydləri təhlil edir və təhlil edir, təşkilatlara onların təhlükəsizlik vəziyyəti haqqında məlumat verir və təhdidlərə vaxtında cavab verməyə imkan verir. Bu proses böyük həcmdə log məlumatlarının mərkəzləşdirilməsi və təhlili, proaktiv təhlükə aşkarlanmasının asanlaşdırılması və ümumi təhlükəsizliyin görünməsi və insidentlərə cavab imkanlarının artırılması üçün çox vacibdir.

**Malware analysis tools –**

Zərərli proqramların təhlili alətlərinə IDA Pro, OllyDbg və Wireshark kimi həm statik, həm də dinamik analiz alətləri daxildir ki, bu da analitiklərə zərərli proqram təminatının davranışını, funksionallığını və potensial təsirini anlamağa kömək edir.

**DLL and EXE -** DLL-lər çoxlu proqramlar arasında paylaşılan təkrar istifadə edilə bilən kodu ehtiva edir, EXE-lər isə proqramın icrasını başlatan müstəqil icra edilə bilən fayllardır.

/etc/ld.so.conf