Akm Imtahan Cavablar

1. Kompüter şəbəkəsi (network) anlayışını izah edin və onun əsas məqsədlərini real həyatdan nümunələrlə açıqlayın.

Kompüter şəbəkəsi məlumat və resursları paylaşmaq üçün iki və ya daha çox cihazın əlaqələndirilməsindən yaranan sistemdir. Əsas məqsədi aparat (məsələn, ofisdəki ortaq printer) və proqram təminatlarının ortaq istifadəsini təmin edərək xərclərə qənaət etməkdir. Bu sistem e-poçt və video zənglər kimi sürətli kommunikasiya üsulları ilə yanaşı, məsafədən səmərəli komanda işinə şərait yaradır. Həmçinin, məlumatların mərkəzi serverlərdə saxlanmasına və istifadəçilərin VPN vasitəsilə daxili resurslara uzaqdan təhlükəsiz girişinə imkan verir. Nəticədə, şəbəkədəki bütün cihazlar (*end devices* – noutbuk, smartfon və s.) tək bir nöqtədən qlobal internetə çıxış əldə edir.

2. LAN, MAN və WAN anlayışlarını izah edin və bu şəbəkə tiplərinin hansı hallarda istifadə olunduğunu müqayisə edin.

Lokal Şəbəkə (**LAN**) ev, ofis və ya məktəb kimi məhdud coğrafi ərazidə cihazların yüksək sürətli bağlantısını və resurs paylaşımını təmin edir. Şəhər Şəbəkəsi (**MAN**) bir şəhər daxilindəki xəstəxana, universitet və ya hökumət binaları kimi fərqli nöqtələri vahid mərkəzdə birləşdirmək üçün istifadə olunur. Qlobal Şəbəkə (**WAN**) isə ölkələri və qitələri əhatə edən, daxilində çoxsaylı LAN qovşaqlarını cəmləşdirən ən geniş infrastrukturdur. LAN məhdud ərazidə ən yüksək ötürmə sürətinə malik olduğu halda, WAN uzaq məsafəli kommunikasiya üçün ISP vasitəsilə əlaqə yaradır və sürəti nisbətən aşağıdır. Bu şəbəkə tiplərinin seçilməsi birbaşa tələb olunan coğrafi əhatə dairəsinə, infrastrukturun miqyasına və ötürmə effektivliyinə əsaslanır.

3. Şəbəkə təhlükəsizliyi (network security) nəyi əhatə edir və bu sahənin əhəmiyyəti nədir? Nümunə ilə izah edin.

Şəbəkə təhlükəsizliyi informasiya sistemlərini və ötürülən verilənləri kiber-təhdidlərdən qorumaq üçün tətbiq edilən tədbirlər toplusudur. Onun təməl məqsədi məlumatların məxfiliyini, bütövlüyünü və əlçatanlığını, yəni **CIA triadasını** təmin etməkdir. Mühafizə üçün **Firewall, IDS/IPS, şifrələmə** və **SIEM** kimi texnologiyalar vasitəsilə şəbəkə infrastrukturu davamlı monitorinq olunur. Bu sahə təşkilatları böyük maliyyə itkilərindən, məlumat sızmalarından və ransomware hücumlarından qorumaq üçün kritik əhəmiyyət kəsb edir. Məsələn, *Equifax* hadisəsində zəif yamaq idarəetməsi (*patch management*) səbəbindən 147 milyon insanın məxfi məlumatı oğurlanmış və şirkətə **1.4 milyard dollar** zərər dəymişdir.

4. End devices və intermediate devices anlayışlarını izah edin və onların şəbəkədə necə birlikdə işlədiyini nümunə ilə açıqlayın.

Son cihazlar (*end devices*) şəbəkənin uclarında yerləşən, məlumatın mənbəyi və ya hədəfi kimi çıxış edən istifadəçi avadanlıqlarıdır (məsələn, noutbuk, server). Aralıq cihazlar (*intermediate devices*) isə bu son cihazları əlaqələndirərək şəbəkədə məlumat axınını idarə edən infrastruktur elementləridir. Bu qrupa lokal şəbəkədə məlumatı yönləndirən **Switch**, şəbəkələrarası ən yaxşı yolu seçən **Router** və trafiki süzgəcdən keçirən **Firewall** daxildir. Nümunə olaraq, noutbukdan (*son cihaz*) veb-sayta daxil olarkən yaranan məlumat paketi məhz aralıq cihazların marşrutlaşdırma və təhlükəsizlik qaydaları vasitəsilə hədəf serverə çatdırılır. Xülasə, son cihazlar şəbəkədə məzmunu yaradır, aralıq cihazlar isə bu məlumatın təhlükəsiz və optimal yolla ünvanına çatmasını təmin edir.

5. Switch və Router cihazlarını müqayisə edin və məlumat ötürülməsində fərqlərini izah edin.

Switch lokal şəbəkə (LAN) daxilindəki cihazları birləşdirir və OSI modelinin Data Link (2-ci) qatında fəaliyyət göstərir. O, MAC ünvanlarından və CAM cədvəlindən istifadə edərək məlumat kadrlarını (*frames*) yalnız uyğun hədəf porta ünvanlayır. **Router** isə fərqli şəbəkələri əlaqələndirərək OSI modelinin Network (3-cü) qatında işləyir və paketlər üçün ən səmərəli yolu (*routing*) seçir. Bu cihaz məntiqi IP ünvanlarına və yönləndirmə cədvəlinə (*routing table*) əsasən məlumatın şəbəkələr arasında etibarlı ötürülməsini təmin edir. Xülasə olaraq, Switch eyni şəbəkə daxilində fiziki əlaqəni, Router isə fərqli infrastrukturlar arası məntiqi bağlantını və trafikin idarə olunmasını həyata keçirir.

6. Wireless Access Point (WAP) nədir və onun təhlükəsizlik baxımından yarada biləcəyi riskləri izah edin.

Wireless Access Point (WAP) simsiz cihazların naqilli şəbəkəyə qoşulmasını təmin edən və məlumatı radio dalğalarına çevirən körpü cihazıdır. Onun əsas təhlükəsizlik risklərinə kiber cinayətkarların qanuni şəbəkəni təqlid etdiyi **Evil Twin** və şəbəkəyə icazəsiz quraşdırılan **Rogue AP** hücumları aiddir. Həmçinin, şifrələnməmiş şəbəkələr məlumatların **packet sniffing** ilə asanlıqla ələ keçirilməsinə, radio maneələr isə **DoS** vəziyyətinin yaranmasına şərait yaradır. Bu təhdidlərdən qorunmaq üçün şəbəkənin siqnal gücü xüsusi xəritələr (*heatmaps*) vasitəsilə tənzimlənməli və kənara sızmanın qarşısı alınmalıdır. Eyni zamanda, ən müasir şifrələmə standartı olan **WPA3** protokoluna keçid edilməsi və avadanlıqların defolt parametrlərinin dəyişdirilməsi mütləqdir.

7. Defensive Security anlayışını izah edin və təşkilatlarda necə tətbiq olunduğunu nümunə ilə açıqlayın.

Defensive Security informasiya sistemlərini və məlumatları proaktiv və reaktiv tədbirlərlə kiber-təhdidlərdən qorumaq təcrübəsidir. Əsasən **Blue Team** və **SOC** tərəfindən idarə olunan bu sahənin məqsədi hücum səthini (*attack surface*) azaltmaq və **CIA triadasını** qorumaqdır. Təşkilatlarda bu mühafizə, hər bir aktivin

müstəqil qatlarla qorunduğu **Defence-in-Depth** strategiyasına əsaslanır. Təhlükəsizlik prosesi **Preventive** (Firewall, MFA), **Detective** (SIEM, IDS) və **Corrective** (backups, patch management) kontrollar vasitəsilə kompleks şəkildə həyata keçirilir. Bu tədbirlərin effektiv tətbiqi kütləvi məlumat sızmalarının və böyük maliyyə itkilərinin (məsələn, 1.4 milyard dollarlıq *Equifax* zərəri) qarşısını almaq üçün kritik əhəmiyyət daşıyır.

8. Red Team və Blue Team anlayışlarını izah edin və onların fərqli rollarını real ssenari ilə müqayisə edin.

Red Team (Hücumçu) sistemlərdəki zəiflikləri aşkarlamaq üçün real kiberhücumları, **penetration testing** və sosial mühəndislik ssenarilərini simulyasiya edir. **Blue Team** (Müdafiəçi) isə infrastrukturu qoruyur, **SIEM** vasitəsilə davamlı monitorinq aparır və aşkar edilən boşluqları yamaqlayaraq hücum səthini azaldır. Məsələn, bir bank ssenarisində **Red Team** yamaqlanmamış tətbiq boşluğundan istifadə edib məlumatları sızdırmağa çalışarkən, **Blue Team** bu anormal trafiki aşkarlayaraq serveri dərhal təcrid edir. Nəticə etibarilə, Red Team qorunma sistemindəki boşluqları tapmağa, Blue Team isə insidentləri aşkarlayıb həmin boşluqları bağlamağa köklənir. Bu qarşılıqlı strateji fəaliyyət təşkilatın real kiber-təhdidlərə qarşı hazırlığını və infrastrukturun dayanıqlığını maksimum səviyyəyə çatdırır.

9. Proactive və Reactive security yanaşmalarını izah edin və hər birinə nümunə verin.

Proaktiv təhlükəsizlik hər hansı kiber insident baş verməzdən əvvəl görülən profilaktik tədbirlərdir, **reaktiv təhlükəsizlik** isə hücum anında və ya sonrasında işə düşən aşkarlama və bərpa prosesidir. Proaktiv yanaşmanın əsas məqsədi hücum səthini azaltmaqdır və bura **Firewall, MFA, şifrələmə, patch management** və nüfuz etmə testləri (*penetration testing*) daxildir. Reaktiv yanaşma isə zərəri minimuma endirməyə fokuslanır və əsas alətləri **IDS, SIEM, insidentə cavab (IR)**

planları və ehtiyat nüsxələrdən (*backup*) bərpadır. Proaktiv müdafiədə işçilərə keçirilən təlimlərlə (*security awareness*) insan faktoru riski azaldılırsa, reaktiv tərəfdə yoluxmuş sistemlərin karantinə alınması əsas yer tutur. Müasir **Defence-in-Depth** strategiyasında bu iki yanaşma birgə tətbiq edilərək informasiya sistemlərinin dayanıqlığını və **CIA triadasını** təmin edir.

10. CIA Triad (Confidentiality, Integrity, Availability) nədir? Hər bir komponenti izah edin və nümunə ilə açıqlayın.

CIA üçbucağı informasiya təhlükəsizliyinin təməl modeli olub, üç əsas komponentdən ibarətdir. **Məxfilik (Confidentiality)** məlumatın yalnız səlahiyyətli şəxslər tərəfindən əldə olunmasını təmin edir; AES-256 və ya TLS kimi şifrələmə üsulları ilə qorunur (məs. *Equifax* məlumat sızması). **Bütövlük (Integrity)** verilənlərin icazəsiz dəyişdirilməsinin qarşısını alaraq dəqiqliyi qoruyur və SHA-256 kimi heşləmə alqoritmləri ilə yoxlanılır (məs. *Stuxnet* hücumu). **Əlçatanlıq (Availability)** isə sistemlərin ehtiyac duyulduğu an işlək olmasını zəmanət altına alır və DDoS qorunması, ehtiyat nüsxələrlə (*backups*) təmin edilir (məs. *Colonial Pipeline* dayanması).

11. Confidentiality prinsipi pozulduqda hansı nəticələr yaranır? Nümunə ilə izah edin.

Məxfiliyin (Confidentiality) pozulması kiber təhlükəsizlikdə məlumat sızması (disclosure) adlanır. Bu hadisə həm insidentin araşdırılması kimi birbaşa, həm də rəqabət üstünlüyünün itirilməsi kimi dolayı maliyyə zərərlərinə (Financial Risk) yol açır. Reputasiya zərəri müştəri etibarının sarsılmasına, Compliance Risk isə GDPR yaxud HIPAA tərəfindən tətbiq olunan ağır hüquqi cərimələrə səbəb olur. Şəxsi identifikasiya məlumatlarının (PII) ifşası fərdlər üçün kütləvi kimlik oğurluğu **təhlükəsi** yaradır, əqli mülkiyyətin (IP) sızması isə strateji risklərlə nəticələnir. Real nümunə kimi, Equifax hadisəsində 147 milyon insanın məlumatının sızması şirkətə 1.4 milyard dollar zərər vurmuş və rəhbərliyin istefasına səbəb olmuşdur.

12. Integrity prinsipi nədir və məlumatın dəyişdirilməsi hansı risklərə səbəb olur? Nümunə ilə açıqlayın.

Bütövlük (Integrity) məlumatların və sistemlərin həm qəsdən, həm də təsadüfən icazəsiz dəyişdirilməsinin (**alteration**) qarşısını alaraq onların dəqiqliyini və tamlığını təmin edir. Bu prinsipin pozulması maliyyə fırıldaqçılığına, vebsaytların təhqir olunmasına (**defacement**) və ya tibbi qeydlərdəki yanlışlıqlar kimi operativ risklərə yol açır. Tarixi **Stuxnet** hücumunda sənaye idarəetmə kodlarının gizlicə manipulyasiyası və **Man-in-the-Middle (MitM)** hücumları zamanı əmrlərin yolda dəyişdirilməsi bu sahədəki əsas təhdidlərdəndir. Risklər yalnız kiberhücumlarla məhdudlaşmır; elektrik gərginliyi nəticəsində yaranan **bit flip** xətaları və mexaniki yazı səhvləri də məlumatın bütövlüyünü korlaya bilər. Texniki mühafizə məqsədilə **SHA-256** kimi heşləmə alqoritmləri, rəqəmsal imzalar və fayl bütövlüyünün izlənməsi (**FIM**) alətləri tətbiq olunur.

13. Availability prinsipi nədir və bu prinsip pozulduqda sistemlərə təsiri nə olur? Nümunə ilə izah edin.

Əlçatanlıq (Availability) prinsipi informasiya və sistemlərin ehtiyac duyulduğu an səlahiyyətli istifadəçilər üçün hazır və işlək olmasını təmin edir. Bu prinsipin pozulması xidmətlərin dayanmasına, biznesin iflicinə və ciddi **maliyyə itkilərinə** yol açır. Əsas təhdidlər resursları tükədən **DDoS** hücumları, məlumatı bloklayan **ransomware** (məs. *WannaCry*) və tək uğursuzluq nöqtəsi (*single point of failure*) kimi kritik texniki xətalardır. Yanğın və zəlzələ kimi təbii fəlakətlər, eləcə də proqram təminatındakı resurs sızmaları (*memory leaks*) sistemlərin əlçatanlığını həm fiziki, həm də məntiqi olaraq poza bilər. Mühafizə üçün **redundancy (artıqlıq), failover, load balancing** və ehtiyat nüsxələr (*backups*) tətbiq edilərək infrastrukturun dayanıqlığı təmin olunur.

14. Encryption və Hashing anlayışlarını izah edin və onların fərqini nümunə ilə açıqlayın.

Şifrələmə (Encryption) riyazi alqoritmlər və açarlar vasitəsilə məlumatı oxunmaz formaya salan iki tərəfli (**reversible**) prosesdir; əsas məqsədi məxfiliyi (**confidentiality**) qorumaqdır. **Hashing** verilənləri sabit uzunluqlu unikal rəqəmsal barmaq izinə çevirən bir tərəfli (**one-way**) funksiyadır və məlumatın bütövlüyünü (**integrity**) təmin edir. Şifrələmə simmetrik (məs. **AES**) və asimmetrik (məs. **RSA**) olmaqla iki qrupa bölünür; müvafiq deşifrə açarı ilə orijinal məlumatı bərpa etmək mümkündür. Heş funksiyalarında orijinal veriləni geri qaytarmaq qeyri-mümkündür və daxil edilən datada bir bitlik dəyişiklik tamamilə fərqli çıxış dəyəri yaradır. Praktikada şifrələmə faylların və e-poçtların gizlədilməsi, hashing isə parolların (**SHA-256**) və kod bütövlüyünün yoxlanılması üçün tətbiq edilir. Nümunə olaraq, bank sənədinin həm gizliliyini, həm də modifikasiya olunmadığını zəmanət altına almaq üçün o, eyni zamanda həm şifrələnir, həm də heşlənir.

15. Defence-in-Depth nədir və niyə bir qatlı təhlükəsizlik kifayət etmir? Real sistem üzərində izah edin.

Defence-in-Depth aktivi qorumaq üçün müxtəlif müstəqil təhlükəsizlik laylarından istifadə edən çoxsəviyyəli strategiyadır. Tək qatlı mühafizə texniki boşluqlar yaxud konfiqurasiya xətaları səbəbindən kifayət etmir; buna görə də bir nəzarət mexanizmi uğursuz olduqda digərləri qorunmanı təmin etməlidir. Strategiya fiziki təhlükəsizlikdən (CCTV, kilidlər) başlayaraq, **Firewall**, VPN və DMZ kimi şəbəkə perimetri nəzarətlərini əhatə edir. Host səviyyəsində **EDR** və yamaq idarəetməsi (**patch management**), tətbiq qatında isə **WAF** və giriş yoxlamaları kimi müdafiə baryerləri qurulur. Ən daxili qatda məlumatların **məxfiliyini** və **əlçatanlığını** qorumaq üçün şifrələmə, **DLP** və ehtiyat nüsxələr tətbiq edilir. Hücumçunun uğur qazanması üçün bütün layları ardıcıllıqla keçməsi tələb olunduğundan, bu yanaşma sistemin kiber-davamlılığını maksimuma çatdırır.

16. Security Controls anlayışını izah edin və risklərin azaldılmasında rolunu açıqlayın.

Təhlükəsizlik nəzarətləri (Security Controls) təşkilatın aktivlərini və CIA triadasını qorumaq üçün tətbiq edilən xüsusi tədbirlər və alətlərdir; əsas məqsədi riskləri qəbul edilə bilən səviyyəyə endirməkdir (*mitigation*). Tətbiq üsuluna görə bu nəzarətlər texniki (*firewall*), inzibati (təhlükəsizlik siyasətləri) və fiziki (CCTV kameralar) olaraq üç əsas qrupa bölünür. Funksional baxımdan isə insidentləri önləyən (*preventive*), aşkar edən (*detective*), zərəri bərpa edən (*corrective*) və hücumçunu çəkindirən (*deterrent*) növləri mövcuddur. **Defence-in-Depth** strategiyası çərçivəsində bu nəzarətlərin çoxqatlı və balanslı tətbiqi sistemin tam kiber-davamlılığını təmin edir.

17. Preventive, Detective və Corrective controls anlayışlarını izah edin və hər birinə nümunə verin.

Təhlükəsizlik nəzarətləri funksional məqsədlərinə görə proaktiv və reaktiv tədbirləri əhatə edən üç əsas növə bölünür. **Preventive (Profilaktik)** nəzarətlər təhdidləri baş verməzdən əvvəl dayandırmağa çalışır; **Firewall**, şifrələmə, **MFA**, şəbəkə seqmentasiyası və yamaq idarəetməsi (**patch management**) bu qrupa daxildir. **Detective (Aşkaredici)** nəzarətlər baş verməkdə olan və ya bitmiş insidentləri müəyyən edir; texniki vasitələrə **IDS**, **SIEM**, **Honeypot** və fayl bütövlüyünün izlənməsi (**FIM**) nümunədir. **Corrective (Düzəldici)** nəzarətlər hadisədən sonra zərəri minimuma endirərək sistemi bərpa edir; bura **ehtiyat nüsxələr (backups)**, **Incident Response** planları və yoluxmuş sistemlərin karantinə alınması aiddir. Bu mexanizmlərin vəhdəti sistemin kiber-dayanıqlığını təmin etmək üçün **Defence-in-Depth** strategiyası çərçivəsində tətbiq olunur.

18. Firewall nədir və şəbəkədə necə işləyir? Nümunə ilə izah edin.

Firewall daxil olan və çıxan trafiki əvvəlcədən təyin edilmiş qaydalara (ACL) əsasən filtrdən keçirən, etibarlı daxili şəbəkə ilə qlobal internet arasında sədd

rolunu oynayan sistemdir. O, paketlərin başlıqlarına baxan sadə *stateless* rejimdən tutmuş, sessiya və tətbiq kontekstini anlayan müasir Növbəti Nəsil Firewall (*NGFW*) modellərinə qədər fərqli səviyyələrdə işləyir. Məsələn, veb-server üçün yalnız 80-ci (HTTP) və 443-cü (HTTPS) portları açıb, verilənlər bazasına (3306) icazəsiz giriş cəhdlərini dərhal bloklayır. Qısaca, şəbəkəni DMZ (ictimai zona) və daxili seqmentlərə bölərək tətbiq edilən ən təməl önləyici (*preventive*) təhlükəsizlik mexanizmidir.

19. IDS və IPS sistemlərini izah edin və onların fərqini nümunə ilə açıqlayın.

Müdaxilə Aşkarlama Sistemləri (IDS) şəbəkə trafikini passiv rejimdə monitorinq edərək şübhəli fəaliyyətlər barədə xəbərdarlıq (**alert**) yaradır, lakin orijinal trafik axınına müdaxilə etmir. **Müdaxilə Qarşısınıalma Sistemləri (IPS)** isə trafik yolunun üzərində (**in-line**) yerləşərək zərərli paketləri avtomatik bloklayır, bağlantını kəsir yaxud hücum edən IP ünvanını məhdudlaşdırır. Hər iki texnologiya təhdidləri məlum rəqəmsal imzalarla (**signature-based**) yaxud normal davranışdan kənarlaşmaları izləyən anomaliya analizi (**anomaly-based**) vasitəsilə müəyyən edir. IPS üçün ən böyük texniki risk qanuni trafikin səhvən bloklanması olan **false positive** halıdır ki, bu da infrastrukturun dayanmasına (**outage**) səbəb ola bilər. Funksional baxımdan IDS binadakı alarm sistemi kimi yalnız hadisəni bildirir, IPS isə girişdəki mühafizəçi kimi təhlükənin daxil olmasını real vaxtda dayandırır. Beləliklə, IDS monitorinq və aşkarlama, IPS isə aktiv müdafiə və preventiv nəzarət funksiyasını yerinə yetirir.

20. Multi-Factor Authentication (MFA) nədir və niyə daha təhlükəsiz hesab olunur? Nümunə ilə izah edin.

Multi-Factor Authentication (MFA) istifadəçinin şəxsiyyətini təsdiqləmək üçün ən azı iki fərqli kateqoriyadan olan yoxlama amilindən istifadə edən təhlükəsizlik sistemidir. Bu faktorlara bildiyiniz (*parol*), sahib olduğunuz (*telefon/OTP token*), olduğunuz (*biometrik barmaq izi*), harada olduğunuz (*lokasiya*) və etdiyiniz (*davranış analizi*) aiddir. Məsələn, bank tətbiqinə girərkən həm şifrə yazmaq, həm

də telefona gələn SMS kodunu daxil etmək hakerin yalnız şifrəni tapmaqla hesabı ələ keçirməsinin qarşısını alır. Həqiqi təhlükəsizlik üçün bu faktorlar mütləq fərqli qruplardan seçilməlidir ki, *brute-force* və ya şifrə oğurluğu kimi hücumların uğur qazanma ehtimalı 99.9% azalsın.

21. Patch management nədir və niyə təhlükəsizlik baxımından vacibdir? Nümunə ilə açıqlayın.

Patch management (Yamaq idarəetməsi) sistemlərdəki məlum təhlükəsizlik boşluqlarını (*vulnerabilities*) aradan qaldırmaq üçün tətbiq olunan mütəmadi proqram yenilənməsi prosesidir. Bu proses hücum səthini və kiber cinayətkarların sistemə sızmaq imkanını minimuma endirən ən əsas profilaktik (*preventive*) tədbirlərdən biridir. Yamaqlanmamış sistemlər təşkilatı kütləvi məlumat sızmalarına və fidyə yazılımlarına (*ransomware*) qarşı müdafiəsiz qoyur. Məsələn, 2017-ci ildə *Equifax* şirkəti məlum bir veb zəifliyini vaxtında yeniləmədiyi üçün 147 milyon insanın məxfi məlumatı oğurlanmış və şirkətə 1.4 milyard dollar ziyan dəymişdir.

22. Network segmentation nədir və hücumların yayılmasının qarşısını necə alır? Nümunə ilə izah edin.

Şəbəkə seqmentasiyası vahid şəbəkənin funksiya və təhlükəsizlik səviyyəsinə görə təcrid olunmuş kiçik alt şəbəkələrə (məs. *VLAN*) bölünməsidir. Əsas məqsədi hücumçunun şəbəkə daxilində sərbəst hərəkətini (*lateral movement*) məhdudlaşdıraraq mümkün zərərin miqyasını azaltmaqdır. Seqmentlər arasında quraşdırılan Firewall və qaydalar (ACL) yalnız icazə verilən spesifik trafikin keçidinə imkan yaradır. Məsələn, zəif qorunan IoT kameraları xüsusi ayrı seqmentdə saxlanıldıqda, onlara sızan haker şirkətin kritik məlumat bazasına və ya işçi kompüterlərinə birbaşa keçid edə bilmir.

23. OSI Model nədir və niyə şəbəkə anlayışını izah etmək üçün istifadə olunur?

OSI (Open Systems Interconnection) modeli iki cihaz arasındakı şəbəkə rabitəsini 7 universal qata bölən məntiqi istinad çərçivəsidir. O, mürəkkəb şəbəkə proseslərini kiçik hissələrə bölməklə fərqli cihazların və protokolların birgə necə işlədiyini anlamağa kömək edir. Eyni zamanda texniki problemlərin tapılmasını asanlaşdırır; məsələn, "1-ci qat problemi" deyiləndə dərhal kabellərdə və ya fiziki bağlantıda nasazlıq olduğu müəyyən edilir. Kiber təhlükəsizlikdə isə çoxqatlı müdafiə (*Defence-in-Depth*) strategiyasının qurulması və xüsusi nəzarətlərin hansı səviyyədə tətbiq ediləcəyini göstərən təməl yol xəritəsidir.

24. OSI modelinin qatlarını izah edin və hər bir qatın funksiyasını nümunə ilə açıqlayın.

OSI modelinin 7 qatı məlumatın daşınmasında fərqli mərhələləri icra edir. **Physical (1)** qat məlumatı fiziki siqnallara (kabel, Wi-Fi) çevirir, **Data Link (2)** isə MAC ünvanları vasitəsilə lokal şəbəkə (*switch*) əlaqəsini qurur. **Network (3)** qatı məntiqi IP ünvanlama və marşrutlaşdırmaya (*router*), **Transport (4)** isə paketlərin etibarlı çatdırılmasına (*TCP/UDP*) cavabdehdir. Yuxarı qatlarda **Session (5)** əlaqələrin idarə edilməsini, **Presentation (6)** məlumatın şifrələnməsi və formatlanmasını (*SSL/TLS*), ən üst lay olan **Application (7)** isə istifadəçi proqramları (*HTTP, DNS*) ilə şəbəkə arasındakı interfeysi təmin edir.

25. Physical Layer nədir və məlumat ötürülməsində hansı rolu oynayır?

Physical Layer (Fiziki Qat) OSI modelinin ən aşağı qatı olub, rəqəmsal verilənləri (0 və 1-ləri) fiziki siqnallara çevirərək ötürür. Bu səviyyədə məlumatlar elektrik siqnalları (mis kabel), işıq impulsları (fiber-optik) və ya radio dalğaları (*Wi-Fi*) vasitəsilə daşınır, alıcı tərəfdə isə yenidən rəqəmsal formaya qaytarılır. Əsasən kabellər, şəbəkə kartları (NIC), *hub* və *repeater* kimi avadanlıqlar məhz bu qatda fəaliyyət göstərir. Onun yeganə məqsədi xam bit axınının mühit üzərindən hədəf cihaza etibarlı fiziki çatdırılmasını təmin etməkdir.

26. Physical layer attacks nədir və necə baş verir? Nümunə ilə izah edin.

Fiziki qat hücumları OSI modelinin birinci səviyyəsini, yəni kabellər, şəbəkə avadanlıqları və simsiz siqnallar kimi infrastrukturun maddi hissəsini hədəf alır. Bu hücumlar qorunan əraziyə icazəsiz daxil olmaqla, cihazlara birbaşa toxunmaqla (*casus USB taxılması*) və ya rabitə sahəsinə yaxınlaşmaqla həyata keçirilir. Əsas nümunələrə şəbəkə kabellərini kəsməklə yaradılan *Physical DoS*, simsiz əlaqəni kəsən *jamming* və keçid kartlarının kopyalandığı *RFID cloning* daxildir. Bu təhdidlərdən qorunmaq üçün *Defence-in-Depth* strategiyasının ilk qatı olan hasarlar, biometrik kilidlər və CCTV kameralar kimi fiziki təhlükəsizlik nəzarətləri tətbiq olunmalıdır.

27. MAC address və IP address anlayışlarını izah edin və fərqlərini nümunə ilə açıqlayın.

MAC ünvanı istehsalçı tərəfindən şəbəkə kartına təyin edilən dəyişməz fiziki ünvandır, OSI-nin 2-ci qatında işləyir və lokal şəbəkə (*LAN*) daxilində cihazların tanınmasını təmin edir. **IP ünvanı** isə proqram təminatı səviyyəsində verilən, şəbəkəyə görə dəyişə bilən məntiqi ünvandır və 3-cü qatda fərqli şəbəkələr arası yönləndirmə (*routing*) üçün istifadə olunur. Analoji olaraq, MAC ünvanı sizin dəyişməz şəxsiyyət vəsiqəniz, IP isə yerləşdiyiniz məkana görə dəyişən poçt ünvanınız kimidir. Praktikada ofis daxilində məlumat ötürülərkən *Switch* MAC ünvanına, internet üzərindən sorğu göndərilərkən isə *Router* IP ünvanına əsasən fəaliyyət göstərir.

28. TCP və UDP protokollarını izah edin və hansı hallarda hansının istifadə olunduğunu əsaslandırın.

TCP və UDP OSI modelinin *Transport* (4-cü) qatında fəaliyyət göstərən, məlumatın ötürülmə üsulunu müəyyən edən təməl protokollardır. **TCP** "üçtərəfli əl sıxma" (*3-way handshake*) metodundan istifadə edərək məlumatın tam, ardıcıl və xətasız çatdırılmasına zəmanət verən etibarlı protokoldur. **UDP** isə paketlərin çatmasını

yoxlamadan (*connectionless*) işlədiyi üçün etibarsız, lakin TCP-dən qat-qat sürətlidir. Məlumatın dəqiqliyi vacib olduqda (veb brauzinq, e-poçt, fayl köçürmə) TCP, sürət və aşağı gecikmə (*latency*) tələb olunduqda (video zənglər, onlayn oyunlar, DNS) isə UDP protokolu istifadə edilir.

29. TCP Three-way Handshake prosesini izah edin və hər mərhələnin məqsədini açıqlayın.

TCP Three-way Handshake iki cihaz arasında etibarlı və təsdiqlənmiş rabitə yaratmaq üçün istifadə olunan 3 addımlı sinxronizasiya prosesidir. İlk olaraq müştəri əlaqəni başlatmaq üçün `SYN` paketi, server isə ona cavab olaraq `SYN-ACK` təsdiq paketi göndərir. Müştəri sonuncu `ACK` paketini göndərdikdə əlaqə rəsmən qurulur (*ESTABLISHED*) və məlumatların xətasız ötürülməsi başlayır. Təhlükəsizlik baxımından kiber cinayətkarlar sonuncu addımı qəsdən icra etməyərək serverin yaddaş resurslarını tükədən *SYN Flood* (DoS) hücumları həyata keçirə bilərlər.

30. Session Layer nədir və hansı funksiyanı yerinə yetirir? Nümunə ilə izah edin.

OSI modelinin 5-ci qatı olan **Session Layer** iki tətbiq arasındakı rabitə əlaqəsini (sessiyanı) açmaq, idarə etmək və iş bitdikdə səliqəli şəkildə bağlamaq funksiyasını daşıyır. Onun ən mühüm vəzifəsi məlumat axınına yoxlama nöqtələri (*checkpoints*) əlavə etməkdir; belə ki, 1 GB-lıq fayl yükləyərkən əlaqə kəsilərsə, proses tam başdan deyil, sonuncu uğurlu nöqtədən davam edir. RPC və SIP kimi protokolların çalışdığı bu səviyyə veb tətbiqlərdə istifadəçi sessiyalarının (*cookies*) idarə edilməsi ilə sıx bağlıdır. Təhlükəsizlik baxımından bu qatın ən böyük riski aktiv istifadəçi seansının haker tərəfindən ələ keçirildiyi *Session Hijacking* hücumlarıdır.

31. Session hijacking nədir və necə baş verir? Nümunə ilə açıqlayın.

Session hijacking (Sessiya oğurluğu) istifadəçinin veb-saytla qurduğu aktiv və autentifikasiya olunmuş əlaqənin (adətən *kuki* vasitəsilə) haker tərəfindən ələ keçirilməsidir. Bu hücum zamanı xaker şifrəni bilmədən belə, birbaşa sessiya nişanını oğurlayaraq sistemdə özünü qanuni istifadəçi kimi təqdim edir. Proses adətən şifrələnməmiş şəbəkələrdə trafik izləmə (*sniffing*) və ya zərərli skriptlərin icra edildiyi *XSS* hücumları vasitəsilə baş verir. Məsələn, *XSS* hücumunda istifadəçinin brauzeri zərərli kodu oxuduqda rəqəmsal sessiya kukisini dərhal hakerin serverinə göndərir və hesabın idarəsi tamamilə ələ keçirilir.

32. Packet nədir və niyə məlumat hissələrə bölünərək göndərilir?

Paket böyük həcmli məlumatların şəbəkə üzərindən sürətli və xətasız ötürülməsi üçün bölünmüş kiçik rəqəmsal verilənlər blokudur. Hər bir paket ünvan məlumatlarını daşıyan başlıqdan (*Header*), əsl veriləni saxlayan gövdədən (*Payload*) və xəta yoxlanışı üçün sonluqdan (*Trailer*) ibarətdir. Məlumatların *Transport* qatında bu cür hissələrə bölünməsi ötürmə səmərəliliyini artırır; çünki bir paket itərsə, bütün faylın deyil, yalnız həmin kiçik hissənin yenidən göndərilməsi kifayət edir. Paketlər şəbəkədə müxtəlif marşrutlarla hərəkət edərək hədəfə çatdıqda ardıcıllıq nömrələrinə əsasən yenidən vahid fayl şəklində birləşdirilir.

33. Routing nədir və məlumatın düzgün istiqamətə çatdırılmasında necə işləyir?

Routing (Marşrutlaşdırma) OSI modelinin *Network* (3-cü) qatında fəaliyyət göstərərək, məlumat paketlərinin mənbədən hədəfə çatdırılması üçün ən optimal yolun seçilməsi prosesidir. Bu əməliyyatı icra edən *Router* cihazı daxil olan paketlərin məntiqi IP ünvanlarını oxuyur və yönləndirmə cədvəlinə əsasən onları düzgün istiqamətə yola salır. Paketlər çıxış nöqtəsindən ayrılaraq hədəf serverə çatana qədər bir çox fərqli cihaz və keçid məntəqəsindən (*hop*) ötürülür. Eynilə rəqəmsal poçt xidməti kimi fəaliyyət göstərən bu sistem, fərqli şəbəkələrin (məsələn, lokal şəbəkə ilə qlobal internetin) bir-birinə etibarlı şəkildə bağlanmasını təmin edir.

34. DNS (Domain Name System) nədir və necə işləyir? Addım-addım izah edin.

DNS (Domain Name System) insanların rahat oxuya bildiyi domen adlarını (məsələn, *google.com*) kompüterlərin anladığı rəqəmsal IP ünvanlarına çevirən "internet telefon kitabçası"dır. Addım-addım baxsaq: istifadəçi sayt adını yazdıqda ilk olaraq brauzerin və ƏS-nin keşi yoxlanılır; əgər tapılmazsa, sorğu provayderin (*ISP*) DNS serverinə, oradan isə qlobal kök (*root*) serverlərə ötürülür. DNS daxilində domenləri IP-yə bağlayan *A*, ləqəblər yaradan *CNAME* və e-poçtları yönləndirən *MX* kimi vacib qeyd tipləri fəaliyyət göstərir. Saniyənin mində biri qədər qısa çəkən bu mürəkkəb axtarış prosesi bitdikdə əldə edilən IP ünvanı vasitəsilə cihazlar bir-biri ilə birbaşa əlaqə qurur.

35. DNS attacks nədir və hansı risklər yaradır? Nümunə verin.

DNS hücumları domen adlarını IP ünvanlarına çevirən sistemin zəifliklərindən istifadə edərək trafiki manipulyasiya etmək və ya şəbəkəni çökdürmək məqsədi daşıyır. Ən geniş yayılmış növlərinə istifadəçiləri saxta saytlara yönləndirən *DNS Poisoning*, sorğu həcmini süni böyüdən *Amplification DDoS* və səhv yazılmış domenlərin ələ keçirildiyi *Typosquatting* daxildir. Məsələn, zəhərlənmiş bir DNS qeydi (*Poisoning*) istifadəçini həqiqi bank saytı əvəzinə vizual olaraq eyni olan saxta səhifəyə yönləndirib şifrələrini rahatlıqla oğurlaya bilər. Bu böyük risklərdən qorunmaq üçün qeydlərin doğruluğunu rəqəmsal imzalarla təsdiqləyən *DNSSEC* texnologiyası və zərərli domenləri bloklayan *DNS filtering* tətbiq edilməlidir.

36. HTTP nədir və necə işləyir?

HTTP (Hypertext Transfer Protocol) veb-saytların fəaliyyətini təmin edən və OSI modelinin *Application* (7-ci) qatında 80-ci port üzərindən işləyən təməl rabitə protokoludur. O, serverin hər bir sorğunu müstəqil qəbul etdiyi *stateless* (vəziyyətsiz) bir sistemdir və istifadəçilərin tanınması üçün yalnız *Cookie* texnologiyasından istifadə edir. Məlumat mübadiləsi serverdən məlumat alan `GET` və məlumat göndərən `POST` metodları vasitəsilə aparılır, server isə `200 OK` və ya `404 Not Found` kimi status kodları ilə cavab verir. Lakin, məlumatları şifrələnməmiş açıq

mətn formatında (*plaintext*) göndərdiyi üçün təhlükəsiz deyil və müasir internetdə onun TLS/SSL ilə şifrələnmiş versiyası olan **HTTPS** (port 443) tətbiq edilir.

37. HTTPS nədir və HTTP-dən fərqi nədir? Təhlükəsizlik baxımından izah edin.

HTTPS (HTTP Secure) məlumatların məxfiliyini və bütövlüyünü qorumaq üçün standart HTTP protokolunun *TLS/SSL* vasitəsilə şifrələnmiş təhlükəsiz versiyasıdır. Əsas fərq HTTP-nin məlumatı açıq mətnlə 80-ci portdan göndərməsi, HTTPS-in isə 443-cü port üzərindən şifrəli ötürmə apararaq araya girmə (*MitM*) hücumlarının qarşısını almasıdır. O, həmçinin rəqəmsal sertifikatlar vasitəsilə saytın kimliyini təsdiqləyir və *HSTS* mexanizmi ilə istifadəçiləri yalnız təhlükəsiz bağlantıya məcbur edir. Lakin unutmaq olmaz ki, brauzerdəki "kilid" işarəsi saytın mütləq zərərsiz olduğunu bildirmir; çünki kiber cinayətkarlar da fişinq saytları üçün asanlıqla HTTPS sertifikatı əldə edə bilərlər.

38. GET və POST metodlarını izah edin və təhlükəsizlik baxımından fərqlərini açıqlayın.

GET və POST veb-serverlə məlumat mübadiləsi üçün istifadə edilən iki əsas HTTP metodudur; `GET` məlumatı oxumaq, `POST` isə göndərmək və ya dəyişdirmək üçün istifadə olunur. Təhlükəsizlik baxımından ən böyük fərq `GET` metodunun parametrləri URL-də açıq göstərməsi (brauzer tarixçəsində qalması), `POST` metodunun isə verilənləri sorğunun gövdəsində (*body*) gizlədərək ötürməsidir. Buna görə də login şifrələri kimi məxfi məlumatlar heç vaxt `GET` ilə göndərilməməlidir, əks halda hakerlər URL parametrlərindən istifadə edərək *Reflected XSS* hücumları reallaşdıra bilərlər. Standart olaraq, həssas məlumatların ötürülməsində URL-də heç bir iz buraxmadığı üçün yalnız `POST` metoduna üstünlük verilməlidir.

39. Man-in-the-Middle (MitM) hücumu nədir və necə baş verir? Nümunə ilə izah

edin.

Man-in-the-Middle (MitM) və ya on-path hücumu, hakerin bir-biri ilə ünsiyyətdə olan iki tərəf arasına gizlicə sızaraq şəbəkə trafikini öz üzərindən keçirməsidir. Bu mövqeni ələ keçirən hücumçu məlumatları həm dinləyərək məxfiliyi, həm də hədəfə çatmazdan əvvəl dəyişdirərək bütövlüyü (məs. pul köçürməsində hesab nömrəsini dəyişərək) poza bilir. Hücumlar lokal şəbəkədə *ARP Spoofing*, şifrələməni ləğv edən *SSL Stripping* və ya ictimai məkanlarda saxta Wi-Fi yaradan *Evil Twin* metodları ilə həyata keçirilir. Məsələn, kafelərdə "Pulsuz Wi-Fi" kimi görünən saxta şəbəkəyə qoşulub bank hesabına daxil olan istifadəçi bütün şifrələrini bilmədən hakerə təhvil verir; bundan qorunmaq üçün mütləq VPN və HTTPS-dən istifadə edilməlidir.

40. DoS və DDoS hücumlarını izah edin və onların sistemə təsirini nümunə ilə açıqlayın.

DoS (Denial of Service) və DDoS (Distributed DoS) hücumları serverin resurslarını süni sorğularla doldurараq, qanuni istifadəçilərin xidmətlərə girişini (CIA triadasının *Availability* prinsipini) əngəlləyən kiber təhdidlərdir. Fərq ondadır ki, DoS tək bir cihazdan həyata keçirilir, DDoS isə minlərlə yoluxmuş cihazdan ibarət zombi şəbəkəsi (*botnet*) vasitəsilə idarəedilməz miqyasda zərbə vurur. Məsələn, saatda 1000 dollar gəlir gətirən bir onlayn mağazanın *SYN Flood* hücumu nəticəsində 3 saat dayanması, təşkilata həm birbaşa 3000 dollar maliyyə, həm də ciddi reputasiya zərəri vurur. Bu həcmli və ya protokol əsaslı hücumların qarşısını almaq üçün şəbəkə perimetrində Firewall, IPS cihazları və *Cloudflare* kimi xüsusi DDoS qorunma xidmətlərindən istifadə edilməlidir.

🛠️ Praktiki Tapşırıqlar Üçün Alətlər

Yoldaşlar, imtahandakı 5 praktiki sualda proqramlaşdırma və ya Kali Linux tələb olunmur. İnternet açıq olacağı üçün qarşınıza çıxa biləcək ssenariləri sadəcə aşağıdakı onlayn alətlərlə rahatlıqla həll edə bilərsiniz. Sualları görəndə panikaya düşməyin, sadəcə **növünü təyin edin və uyğun sayta girin.**

🔐 1. Kriptoqrafiya və Şifrə Sındırma (Decryption & Hashing)

Sualda sizə qəribə, oxunmayan bir mətn və ya kod veriləcək və onun əslini tapmaq tələb olunacaq.

- **CyberChef (cyberchef.io):** Ən çox istifadə edəcəyiniz saytdır. Növünü bilmirsinizsə: Sol menyudan "Magic" funksiyasını seçib sürükləyin, o avtomatik növünü tapıb sındırmağa çalışacaq.
- **Base64:** Əgər verilən kodun sonunda `=` və ya `==` işarələri varsa (məsələn: `QXpUVQ==`), bu böyük ehtimalla Base64-dür. Sol tərəfdən "From Base64" seçib həll edin.
- **Sezar/ROT13:** Əgər mənalı sözə oxşayır, amma hərflər sürüşübsə (məsələn, 'A' əvəzinə 'D' yazılıb), "ROT13" və ya "Caesar Cipher" funksiyasını istifadə edin.
- **CrackStation (crackstation.net) - Sırf Hash üçün:** Əgər sizə verilən çox uzun, içində rəqəm və hərflər olan qarışıq bir koddursa (məsələn: MD5, SHA-256), birbaşa bu sayta girin. Kodu yapışdırıb "Crack Hashes" düyməsini basın, saniyələr içində əsl sözü tapacaq.

🌍 2. OSINT və Şəbəkə Məlumatları Toplama (Domain/DNS)

Sualda sizə hədəf bir sayt (məsələn: aztu.edu.az) veriləcək və onun arxa planındakı məlumatları tapmaq istəniləcək.

- **whois.com / centralops.net (Domain Məlumatları):** *Nə vaxt istifadə etməli:* "Bu sayt kim tərəfindən qeydiyyata alınıb?", "Nə vaxt yaradılıb?", "Qeydiyyat müddəti nə vaxt bitir?" kimi suallarda bu saytlara girib axtarış verin.
- **DNSdumpster (dnsdumpster.com) - IP və Subdomainlər:** *Nə vaxt istifadə etməli:* Saytın "A record" (IP ünvanı), gizli alt-domenləri (subdomains) və ya serverin harada yerləşdiyini tapmaq tələb olunsa, bu sayt sizə tam xəritə çıxaracaq.

🔒 3. Veb Təhlükəsizlik və SSL Sertifikatları

Brauzerin Özü (Heç bir sayta ehtiyac yoxdur): *Nə vaxt istifadə etməli:* Əgər "Bu saytın SSL sertifikatı etibarlıdırmı? Kim tərəfindən və nə vaxta qədər verilib?" sualı gəlsə...

- **Həlli:** Verilən saytı açın, yuxarıda linkin solundakı qıfıl (🔒) işarəsinə klikləyin. "Connection is secure" → "Certificate is valid" bölməsinə girin. Orada sertifikatı verən şirkəti (Issuer) və bitmə tarixini (Valid until) görəcəksiniz.

🪓 4. Zərərli Fayl, Link və Fişinq Analizi (Threat Intelligence)

Sualda sizə şübhəli bir link (məsələn: secure-bank-login.com) və ya e-poçt vasitəsilə gələn şübhəli bir fayl veriləcək. Onun zərərli (malware/phishing) və ya ransomware olub-olmadığını analiz etmək tələb olunacaq.

- **VirusTotal (virustotal.com):** Link və ya faylı bura yükləyin. 90-dan çox antivirus və təhlükəsizlik bazası ilə yoxlayıb onun fişinq və ya virus olub-olmadığını dərhal təyin edəcək.
- **Urlscan.io:** Şübhəli linkləri arxa planda təhlükəsiz şəkildə açaraq hansı real IP ünvanına bağlandığını və saytın vizual görünüşünü (skrinşotunu) sizə təqdim edəcək.

🔍 5. Server İnfrastrukturu və Açıq Portların Kəşfiyyatı (Network OSINT)

Sualda sizə bir IP ünvanı və ya şirkət adı veriləcək. "Bu serverdə hansı xidmətlər (HTTP, FTP, SSH) və portlar internetə açıqdır?", "Şirkətin xaricə açıq patch olunmamış zəiflikləri varmı?" soruşulacaq.

- **Shodan (shodan.io) / Censys (censys.io):** İnternetə bağlı olan bütün server, router və boşluqların qlobal axtarış motorudur. Bura IP və ya domen yazaraq, serverdə hansı köhnə proqram təminatının işlədiyini asanlıqla tapa bilərsiniz.

💻 6. Veb Tətbiq Texnologiyalarının Analizi (Web Stack OSINT)

Sualda sizə bir veb-sayt linki veriləcək və "Bu sayt hansı proqramlaşdırma dili, CMS sistemi (WordPress, Drupal) və ya veb server (Nginx/Apache) üzərində

işləyir?" soruşulacaq.

- **BuiltWith (builtwith.com) / Wappalyzer (wappalyzer.com):** Saytın ünvanını bura daxil edin. Saytın kod strukturuna girmədən, arxa planda işləyən bütün infrastrukturu, JavaScript kitabxanalarını və analitik alətləri sizə siyahı ilə verəcək.

📧 7. Sızmış Məlumatlar və E-poçt Yoxlanışı (Breach OSINT)

Şirkətdə əməkdaşların parollarının sızıb-sızmadığını və ya bir işçinin keçmiş qlobal sızıntılarda (LinkedIn, Canva və s.) hesabı olub-olmadığını yoxlamaq istənildikdə istifadə olunur.

- **HaveIBeenPwned (haveibeenpwned.com):** E-poçtu yazın. Əgər qırmızı ekran çıxarsa, bu e-poçtun keçmişdə hansı saytların sındırılması nəticəsində ələ keçdiyini və parollarının sızdığını göstərəcək.

💡 Qızıl Qayda: İmtahan Anında Nə Etməli?

Yoldaşlar, imtahanda internet açıq olduğu üçün əslində ən böyük silahınız Google və yuxarıdakı 7 fərqli ssenari alətidir. Qarşınıza tamamilə fərqli və naməlum bir tapşırıq çıxarsa, bu 3 addımlıq strategiyanı tətbiq edin:

1. **Axtarış Operatorlarından (Google Dorking) İstifadə Edin:** * Sırf gizli sənədlər tapmaq üçün: `site:saytadi.com filetype:pdf` (və ya docx, xlsx, txt).
    - Sırf idarəetmə və qovluq sızıntılarını tapmaq üçün: `site:saytadi.com intitle:"index of"` və ya `site:saytadi.com inurl:admin` yazın.
2. **Doğru Açar Sözlərlə Alət Axtarın:** * Əgər qarşınıza siyahıda olmayan spesifik bir fayl və ya şifrələmə çıxsa, Google-da ingiliscə bəsit axtarın. Məsələn: *"Online [fayl_adı] analyzer"*, *"Online [şifrə_növü] decoder"* və ya *"Online [data] parser"*. İlk 3 linkdən biri işinizi 100% həll edəcək.
3. **Hədəfi Dırnaq İçində Axtarın:** * Spesifik bir xəta mesajı və ya termin haqqında məlumat tələb olunursa, onu mütləq dırnaq arasında yazın: `"Xəta Mesajı"`. Bu, Google-un lazımsız və bənzər nəticələri silərək birbaşa hədəf nöqtəni tapmasını təmin edəcək.

Unutmayın, bu imtahan əzbəri yox, informasiyanı düzgün təyin edib, internetdəki açıq resurslardan (OSINT) sürətli şəkildə istifadə etmək bacarığınızı yoxlayır. Siyahını əlinizin altında saxlayın, növü təyin edin və uyğun alətə keçid edin. Hər kəsə uğurlar! 🚀