**Azərbaycan Texniki Universiteti**

**2024/2025-ci Tədris İli**

**İmtahan Sualları**

**Fənn: Kibertəhlükəsizliyin Əsasları**

**6424a2**

**Nəzəri suallar:**

1.Kibertəhlükəsizliyin əsas anlayışları. Kibertəhlükəsizliyin təmin edilməsi metodları (Mövzu-1)

**Cavab:**

**Kibertəhlükəsizlik informasiya texnologiyaları sahəsində sistemlərin, şəbəkələrin və verilənlərin icazəsiz girişlərdən, hücumlardan, zərərli proqramlardan və digər təhlükələrdən qorunması prosesidir. Bu sahə sürətlə inkişaf edən texnologiya ilə birlikdə daha da aktuallaşır. Kibertəhlükəsizliyin əsas məqsədi məxfiliyi, bütövlüyü və əlçatanlığı təmin etməkdir – bu üç anlayış CIA triadası adlanır. Məxfilik o deməkdir ki, məlumatlar yalnız icazəli şəxslər tərəfindən əldə edilə bilər. Bütövlük – məlumatların dəyişdirilmədən saxlanılması və düzgünlüyüdür. Əlçatanlıq isə sistemlərin və məlumatların lazım olan vaxtda istifadə üçün hazır olmasıdır.**

**Kibertəhlükəsizlik yalnız texniki tədbirlərlə deyil, həm də inzibati və hüquqi yanaşmalarla həyata keçirilir. Təhlükənin qarşısını almaq üçün ən çox istifadə olunan metodlardan biri şifrləmə (encryption) texnologiyasıdır. Bu zaman məlumatlar yalnız açar vasitəsilə oxuna biləcək formaya çevrilir. Antivirus proqramları, firewall-lar və intrusion detection sistemləri (IDS) də sistemləri hücumlardan qorumaqda əsas rol oynayır. Giriş nəzarəti (access control) ilə istifadəçilərin hüquqları məhdudlaşdırılır və yalnız ehtiyacı olan məlumatlara çıxış verilir. İki mərhələli autentifikasiya kimi metodlarla istifadəçi identifikasiyası daha təhlükəsiz olur.**

**İnsan faktorunu nəzərə alaraq kibertəhlükəsizlik üzrə maarifləndirmə də mühüm yer tutur. Çünki bir çox kibertəhlükələr istifadəçilərin ehtiyatsızlığı nəticəsində baş verir. Sosial mühəndislik hücumları buna nümunədir – istifadəçiləri aldatmaqla onlardan gizli məlumatlar əldə olunur. Sistemlərin və proqram təminatlarının daim yenilənməsi, mövcud zəifliklərin aradan qaldırılması üçün vacibdir. Eyni zamanda, ehtiyat nüsxələrin (backup) mütəmadi alınması məlumat itkisinin qarşısını almağa kömək edir.**

**Kibertəhlükəsizliyin təminində həm də qanunvericilik, standartlar və siyasətlər önəmlidir. Məsələn, ISO/IEC 27001 informasiya təhlükəsizliyinin idarə olunması üzrə beynəlxalq standartdır. Müəssisələr bu standartlara uyğun fəaliyyət göstərməklə öz sistemlərini daha təhlükəsiz edə bilərlər. Kibertəhlükəsizlik həm fərdi istifadəçiləri, həm də korporativ və dövlət qurumlarını əhatə edir. Bu səbəbdən hər səviyyədə tədbirlər görülməli və risklərə qarşı hazırlıqlı olunmalıdır.**

2.GNU-Linux əməliyyat sistemi. Kali Linux və əsas linux komandaları (Mövzu-2)

**Cavab:**

**GNU/Linux açıq mənbəli və sərbəst paylanan əməliyyat sistemi nüvəsi olan Linux kernel-ə əsaslanır. GNU isə bu sistemdə istifadə olunan alət və proqramların ümumi adıdır. Bu əməliyyat sistemi əsasən sabitlik, təhlükəsizlik və azadlıq baxımından çox önəmlidir. Açıq mənbəli olması ona istifadəçi tərəfindən dəyişdirilmək və istəyə uyğunlaşdırılmaq imkanı verir. Bu xüsusiyyətləri sayəsində Linux, həm fərdi istifadəçilər, həm də təşkilatlar tərəfindən geniş istifadə olunur. Linux-un müxtəlif versiyaları mövcuddur və bunlara distribütivlər (distrolar) deyilir, məsələn: Ubuntu, Debian, Fedora, CentOS və s.**

**Kali Linux isə xüsusi olaraq kibertəhlükəsizlik, etik hacking, penetrasiya testləri üçün hazırlanmış bir Linux distribütividir. Kali Linux, Offensive Security şirkəti tərəfindən hazırlanmışdır və yüzlərlə təhlükəsizlik alətini özündə birləşdirir. Buraya Nmap, Wireshark, Metasploit, Aircrack-ng, Burp Suite və digər analiz və test proqramları daxildir. Kali Linux həm təcrübəli mütəxəssislər, həm də yeni başlayanlar üçün öyrənmək baxımından əlverişlidir.**

**Linux əməliyyat sistemində əsas funksiyalar çox zaman komanda sətri (terminal) vasitəsilə yerinə yetirilir. Əsas Linux komandalarından biri ls komandasıdır, bu komanda qovluqdakı faylları göstərir. cd komandası ilə qovluqlar arasında keçid etmək mümkündür. pwd istifadəçinin hansı qovluqda olduğunu göstərir. mkdir yeni qovluq yaratmaq üçün, rm isə fayl və ya qovluğu silmək üçün istifadə olunur. cp faylların surətini çıxarmaq, mv isə onları köçürmək üçün tətbiq olunur.**

**sudo komandası inzibati hüquqlarla əmr icra etmək üçündür və təhlükəsizlik baxımından çox önəmlidir. ifconfig və ip a komandaları şəbəkə interfeyslərini göstərmək üçün istifadə olunur. ping, netstat, nmap və traceroute kimi şəbəkə diaqnostika komandaları da sistemin və şəbəkənin vəziyyətini təhlil etmək üçün vacibdir. top və htop prosessor və yaddaş istifadəsini real vaxtda göstərir. Fayl məzmununa baxmaq üçün cat, less, more, nano və vim kimi mətn redaktorları mövcuddur.**

**Linux sistemlərində istifadəçi və hüquq idarəsi də önəmli yer tutur. adduser, usermod, chmod, chown kimi komandalarla istifadəçi və fayl hüquqları tənzimlənir. Bu komandaların düzgün istifadəsi sistemin təhlükəsizliyi üçün vacibdir. Ümumilikdə, Linux sistemləri açıq, çevik və güclü təhlükəsizlik alətləri ilə təchiz olunduğu üçün kibertəhlükəsizlik sahəsində geniş istifadə olunur.**

3.Kali Linux-da fayla giriş icazələri. chmod komandası ilə fayl icazələrin dəyişdirilməsi (Mövzu-2)

**Cavab:**

**Kali Linux və ümumilikdə bütün Linux sistemlərində fayl və qovluqların icazələri sistemin təhlükəsizliyini təmin etmək üçün vacib rol oynayır. Hər bir fayl və qovluq üzərində üç əsas tip icazə mövcuddur: oxuma (read – r), yazma (write – w) və icra (execute – x). Bu icazələr üç əsas istifadəçi qrupu üçün təyin olunur: fayl sahibi (owner), qrup (group), və digər istifadəçilər (others). Məsələn, bir faylda “rwxr-xr--” icazəsi varsa, bu o deməkdir ki, sahibi oxuya, yaza və icra edə bilər; qrupa daxil olan istifadəçilər oxuya və icra edə bilər; digər istifadəçilər isə yalnız oxuya bilər.**

**Linux-da fayl icazələrinə baxmaq üçün ls -l komandası istifadə olunur. Bu komanda fayl və ya qovluğun yanındakı icazə simvollarını və digər məlumatları göstərir. Hər bir icazənin ədədi qarşılığı da vardır: r = 4, w = 2, x = 1. Bu ədədlər cəmlənərək müəyyən bir icazə vəziyyəti yaradılır. Məsələn, chmod 755 fayl.txt komandasını icra etdikdə faylın sahibi üçün rwx (7), qrup üçün rx (5), və digərləri üçün də rx (5) icazəsi təyin olunur.**

**chmod (change mode) komandası bu icazələri dəyişmək üçün istifadə olunur. Bu komanda iki formada işləyə bilər: ədədi (numeric) və simvolik (symbolic). Ədədi formada biz yuxarıda göstərilən rəqəmlərlə icazələri təyin edirik. Simvolik formada isə chmod u+x fayl.sh kimi yazaraq, fayl sahibinə (u) icra icazəsi (+x) əlavə edə bilərik. Burada u – owner, g – group, o – others, a – all deməkdir. + icazə əlavə etmək, - icazəni silmək, = isə tam olaraq təyin etmək üçündür.**

**Qovluqlar üçün x icazəsi xüsusilə vacibdir, çünki bir qovluğa daxil olmaq üçün istifadəçidə execute hüququ olmalıdır. Əgər bir istifadəçidə oxuma icazəsi var, lakin icra icazəsi yoxdursa, o zaman həmin qovluğun içindəkiləri görə bilər, lakin ora daxil ola bilməz. Sistem administratorları təhlükəsizlik məqsədilə çox vaxt yalnız zəruri icazələri verirlər, çünki artıq icazələr sistemin zəif nöqtəsinə çevrilə bilər.**

**chmod komandası ilə yanaşı, chown (fayl sahibini dəyişmək) və chgrp (qrup dəyişmək) komandaları da fayl icazələrinin idarə olunmasında mühüm rol oynayır. Fayl sistemində düzgün icazələrin verilməsi həm istifadəçilərin sərbəst işləməsini təmin edir, həm də sistemin səlahiyyətsiz girişlərdən qorunmasına kömək edir. Kali Linux kimi təhlükəsizlik yönümlü sistemlərdə bu cür icazə mexanizmləri xüsusilə önəmlidir, çünki test edilən sistemlərdə maksimum nəzarət tələb olunur.**

**Yekun olaraq, chmod komandası Linux-un sadə amma güclü təhlükəsizlik vasitələrindən biridir. Bu komanda vasitəsilə hər bir fayl və qovluğun kimlər tərəfindən necə istifadə olunacağını dəqiq şəkildə tənzimləmək mümkündür.**

4.Sızma testi metodologiyası. Sızma testi standartları (Mövzu-3)

**Cavab:**

**Sızma testi (Penetration Testing), kompüter sistemlərinin, şəbəkələrin və tətbiqlərin zəifliklərini aşkar etmək və onlardan necə istifadə oluna biləcəyini müəyyən etmək məqsədilə simulyasiya olunmuş hücum prosesidir. Bu test kibertəhlükəsizlik sahəsində vacib yer tutur və təşkilatlara öz müdafiə sistemlərini real hücumlara qarşı necə dayanıqlı olduğunu öyrənmək imkanı verir. Sızma testi adətən etik hakerlər və ya təhlükəsizlik analitikləri tərəfindən həyata keçirilir. Bu proses sistemdə olan zəiflikləri vaxtında tapmaq və onları aradan qaldırmaq məqsədi daşıyır.**

**Sızma testi metodologiyası əsasən bir neçə mərhələdən ibarətdir. Birinci mərhələ məlumat toplama (reconnaissance) mərhələsidir. Bu mərhələdə hədəf sistem haqqında mümkün qədər çox məlumat toplanır. İkinci mərhələ skanlama və zəiflik analizidir – bu zaman açıq portlar, işləyən xidmətlər və istifadə olunan proqram təminatı müəyyən edilir. Daha sonra zəifliklərə əsaslanan istismar mərhələsi (exploitation) gəlir. Bu mərhələdə tapılan zəifliklər vasitəsilə sistemə sızmağa çalışılır. Əgər hücum uğurlu olarsa, post-exploitation mərhələsi başlayır – burada sistem daxilində hansı məlumatlara çıxış əldə olunduğu, hüquqların artırılması və s. yoxlanılır. Sonuncu mərhələ isə hesabatlandırma (reporting) mərhələsidir – bu mərhələdə tapılmış zəifliklər və onların necə istismar edildiyi ətraflı sənədləşdirilir.**

**Sızma testləri zamanı istifadə olunan metodologiyalar və standartlar testin keyfiyyətini və uyğunluğunu müəyyən edir. Ən tanınmış sızma testi standartlarından biri OSSTMM (Open Source Security Testing Methodology Manual) – açıq mənbəli təhlükəsizlik testi metodologiyasıdır. Bu metodologiya sistematik və obyektiv şəkildə test aparmağa imkan verir. Digər bir məşhur standart isə OWASP Testing Guide-dır – bu veb tətbiqlər üzərində sızma testlərinin necə aparılmalı olduğunu izah edir. Bundan əlavə, NIST SP 800-115 sızma testlərinin planlaşdırılması, aparılması və hesabatlandırılması üçün federal səviyyəli təlimat verir.**

**Daha bir praktiki yanaşma isə PTES (Penetration Testing Execution Standard) metodologiyasıdır. PTES sızma testlərini daha standartlaşdırılmış və strukturlaşdırılmış şəkildə aparmağı təmin edir. MITRE ATT&CK çərçivəsi də təcavüzkarların istifadə etdiyi taktikaları və texnikaları təsvir etməklə, sızma testlərində istifadə oluna bilər. Bu cür standart və metodologiyalar testin effektivliyini artırmaqla yanaşı, təşkilatlara təhlükələrin daha yaxşı başa düşülməsi və prioritetləşdirilməsi üçün kömək edir.**

**Sızma testləri mütəmadi aparılmalı və sistemdə dəyişikliklər olduqda yenilənməlidir. Bu testlər yalnız texniki deyil, həm də sosial mühəndislik və fiziki təhlükəsizlik aspektlərini əhatə edə bilər. Mühüm olan odur ki, sızma testi nəzarətli mühitdə, yazılı icazə ilə və etik prinsiplər daxilində həyata keçirilməlidir. Beləliklə, sızma testləri təşkilatların real hücumlara qarşı hazırlıqlı olmasına, zəiflikləri vaxtında aşkarlamasına və ümumi kibertəhlükəsizlik səviyyəsini artırmasına xidmət edir.**

5.Kəşfiyyat və məlumat toplanması (Mövzu-4)

**Cavab:**

**Kəşfiyyat və məlumat toplanması (reconnaissance and information gathering) sızma testinin və ya etik hacking prosesinin ilkin mərhələsidir. Bu mərhələnin əsas məqsədi hədəf sistem, şəbəkə və ya təşkilat haqqında mümkün qədər çox məlumat toplamaqdır. Toplanan bu məlumatlar daha sonra sistemdəki zəifliklərin müəyyən olunması və istismar olunması üçün istifadə olunur. Kəşfiyyat mərhələsi həm passiv, həm də aktiv ola bilər. Passiv kəşfiyyat zamanı hədəf sistemə birbaşa toxunulmur, yəni heç bir iz qoyulmur. Bu üsulda açıq mənbələrdən (məsələn, internet saytları, sosial media, WHOIS məlumatları və s.) istifadə olunur.**

**Aktiv kəşfiyyat isə sistemə qarşı birbaşa əlaqə qurularaq həyata keçirilir və bu zaman iz qoyulma riski daha yüksək olur. Aktiv üsullara port skanlaması, xidmətlərin müəyyən edilməsi və digər şəbəkə əsaslı əməliyyatlar daxildir. Kəşfiyyat mərhələsində istifadə olunan əsas vasitələrdən biri WHOIS analizidir – bu vasitə ilə domen adları, IP ünvan sahibləri və əlaqə məlumatları müəyyən edilə bilər. NSLookup və ya dig kimi DNS analiz vasitələri də hədəf haqqında əlavə məlumat almaq üçün istifadə olunur.**

**Google dorking və OSINT (Open Source Intelligence) texnikaları vasitəsilə açıq internet üzərindən çoxlu sayda faydalı informasiya əldə edilə bilər. Məsələn, şirkətin istifadə etdiyi texnologiyalar, proqram təminatları, email strukturları və hətta işçilərin adları kimi məlumatlar toplanır. Shodan kimi axtarış mühərrikləri isə internetə açıq olan cihazları və onların açıq portlarını tapmaq üçün istifadə olunur.**

**Aktiv kəşfiyyat mərhələsində Nmap, Netcat, Masscan, WhatWeb və Recon-ng kimi alətlərdən istifadə olunur. Nmap açıq portları və işləyən xidmətləri təyin etmək üçün ən çox istifadə olunan vasitələrdən biridir. WhatWeb və Wappalyzer veb saytların arxa planda hansı texnologiyalardan istifadə etdiyini aşkar edə bilər. Bu məlumatlar hücum planlamasında hücumçulara ciddi üstünlük verir. Məsələn, istifadə olunan Apache versiyası və ya köhnəlmiş CMS sistemləri zəifliklərə yol aça bilər.**

**Kəşfiyyat mərhələsi sızma testinin ən vacib mərhələlərindən biridir, çünki bu mərhələdə düzgün və dəqiq məlumat toplamaq bütün testin uğurunu müəyyən edə bilər. Bu mərhələ həmçinin sosial mühəndislik hücumları üçün də zəmin yarada bilər, çünki insan faktoru ilə bağlı zəifliklər bu mərhələdə aşkarlanır. Yekunda toplanan məlumatlar analiz olunur və növbəti mərhələlərdə (zəiflik analizi, istismar və s.) istifadə edilir. Düzgün aparılmış kəşfiyyat hücum edənə böyük üstünlük verir, müdafiə tərəfinə isə zəif yerlərini tanımaq fürsəti yaradır.**

6.Şəbəkənin daranması. Darama metodologiyası (Mövzu-5)

**Cavab:**

**Şəbəkənin daranması (network scanning) kibertəhlükəsizlik və sızma testlərinin vacib mərhələlərindən biridir. Bu mərhələnin əsas məqsədi hədəf şəbəkədə hansı qurğuların, portların və xidmətlərin açıq olduğunu müəyyən etməkdir. Darama (skanlama) nəticəsində əldə olunan məlumatlar hücum planlamasında və zəifliklərin analizində mühüm rol oynayır. Bu mərhələdə həm canlı cihazlar, həm də onların şəbəkə xidmətləri təyin edilir. Darama eyni zamanda sistemlərin identifikasiyasını, əməliyyat sisteminin təxminini və portların vəziyyətini ortaya çıxarır.**

**Darama prosesi bir neçə növə ayrılır: port daranması, şəbəkə qurğularının aşkarlanması, xidmət skanlaması və əməliyyat sisteminin təyini. Port daranması zamanı açıq TCP və UDP portlar təyin olunur. Bu portlar vasitəsilə sistemdə hansı xidmətlərin çalışdığı öyrənilir. Məsələn, port 80 açıqdırsa, çox güman ki, HTTP xidmətinə çıxış mövcuddur. Port 22 açıqsa, bu SSH xidmətini göstərir. Açıq portlar və xidmətlər zəifliklərin qapısı ola bilər.**

**Şəbəkənin daranmasında ən məşhur və geniş istifadə olunan alətlərdən biri Nmap-dır. Nmap həm host aşkarlama, həm port skanlama, həm də xidmət və versiya aşkarlama üçün istifadə olunur. nmap -sS TCP SYN skanlaması, nmap -sU isə UDP port skanlaması üçün istifadə edilir. nmap -O komutu ilə əməliyyat sistemi təxmin edilir. nmap -sV isə açıq portlardakı xidmətlərin versiyalarını göstərir. Bu məlumatlar zəifliklərin identifikasiyasında köməkçi olur.**

**Masscan aləti isə çox sürətli port skanlama üçün istifadə olunur. Minlərlə hostu çox qısa zamanda skanlaya bilir. Netdiscover və ARP-scan kimi vasitələr yerli şəbəkədəki aktiv qurğuları tapmaq üçün istifadə olunur. Bundan əlavə, Zenmap – Nmap-in qrafik interfeysə malik versiyasıdır və istifadə üçün daha rahatdır. Darama zamanı firewall və intrusion detection system (IDS) kimi təhlükəsizlik sistemləri testçini bloklaya bilər, buna görə gizli skanlama üsullarından istifadə olunur (məsələn, TCP SYN, FIN, Xmas skanlama və s.).**

**Darama prosesində etik qaydalara əməl etmək vacibdir. Əgər sızma testi real mühitdə həyata keçirilirsə, testçinin qarşısında olan sistemləri təsadüfən yükləməməsi və işinə mane olmaması üçün diqqətli olması tələb olunur. Darama zamanı əldə olunan nəticələr sızma testinin növbəti mərhələsi – zəifliklərin aşkarlanması və istismar mərhələsi üçün əsas yaradır.**

**Metodoloji baxımından daranma planlı şəkildə həyata keçirilməlidir. Əvvəlcə hədəf IP və ya domenlər müəyyənləşdirilir, sonra hostlar aşkarlanır, ardınca port və xidmətlər analiz olunur. Hər mərhələnin nəticələri sənədləşdirilməlidir ki, sonda tam və dəqiq hesabat təqdim oluna bilsin. Nəticə etibarilə, şəbəkənin daranması hücumçular üçün zəif nöqtələrin tapılması baxımından, müdafiə tərəfi üçünsə bu zəif nöqtələrin bağlanması baxımından olduqca vacib mərhələdir.**

7.Şəbəkənin inventarlaşdırılması. İnventarlaşdırma üsulları (Mövzu-5)

**Cavab:**

**Şəbəkənin inventarlaşdırılması (network inventory) – təşkilatın şəbəkəsində mövcud olan bütün cihazların, resursların, proqramların və xidmətlərin qeydiyyatının aparılması və izlənilməsidir. Bu proses təhlükəsizlik, idarəetmə və optimallaşdırma baxımından olduqca əhəmiyyətlidir. İnventarlaşdırma nəticəsində şəbəkədə hansı avadanlıqların, IP ünvanlarının, əməliyyat sistemlərinin, proqram təminatlarının və versiyalarının işlədiyi dəqiq şəkildə müəyyən olunur. Bu məlumatlar təhlükəsizlik boşluqlarının tapılması və profilaktik tədbirlərin görülməsi üçün əsas rol oynayır.**

**Şəbəkə inventarlaşdırması həm əl ilə, həm də avtomatlaşdırılmış vasitələrlə həyata keçirilə bilər. Əl ilə inventarlaşdırma zaman alır və insan səhvlərinə açıqdır. Bu səbəbdən, çox vaxt avtomatik inventarlaşdırma alətləri istifadə olunur. Bu alətlər şəbəkəni skanlayaraq cihazları, xidmətləri, əməliyyat sistemlərini, proqram versiyalarını və digər resursları avtomatik şəkildə müəyyən edir və hesabat yaradır. Məsələn, Nmap aləti ilə nmap -O -sV komutu vasitəsilə cihazlar və onların xidmətləri haqqında ətraflı məlumat toplamaq mümkündür.**

**İnventarlaşdırmada istifadə olunan alətlərə Spiceworks, Lansweeper, PRTG Network Monitor, Open-AudIT, SolarWinds Network Configuration Manager və GLPI kimi platformalar daxildir. Bu alətlər cihazların avtomatik aşkarlanması, tiplərinin təyini, proqram təminatlarının siyahısı, lisensiya izləmə və hətta zəifliklərin monitorinqi kimi funksiyaları dəstəkləyir.**

**İnventarlaşdırmanın əsas üsullarından biri SNMP (Simple Network Management Protocol) protokolundan istifadədir. Bu protokol vasitəsilə şəbəkə qurğularından status və informasiya alınır. Digər üsul isə agent-based monitoring üsuludur – burada hər bir cihazda xüsusi proqram agenti quraşdırılır və bu agentlər mütəmadi olaraq inventar məlumatlarını göndərirlər.**

**İnventarlaşdırma təkcə texniki inventar (hardware/software) deyil, həm də IP ünvanlarının idarə olunması (IPAM) və şəbəkə topologiyasının çıxarılması baxımından da həyata keçirilir. Bu, şəbəkə inzibatçılarına ümumi şəbəkə xəritəsini görmək və dəyişikliklərə nəzarət etmək imkanı verir. Yenilənmiş inventar sistemi vasitəsilə istifadə olunmayan, köhnəlmiş və ya təhlükəli sistemlər vaxtında aşkarlanaraq şəbəkədən çıxarıla bilər.**

**Eyni zamanda inventarlaşdırma aktiv və passiv üsullarla da həyata keçirilə bilər. Aktiv üsullarda skanlamalar və sorğular göndərilir, passiv üsullarda isə şəbəkə trafiki müşahidə olunur. Şəbəkənin effektiv inventarlaşdırılması nəticəsində həm təhlükəsizlik tədbirləri gücləndirilir, həm də şəbəkənin idarəolunması asanlaşır.**

**Şəbəkənin inventarlaşdırılması (network inventory) zamanı müxtəlif protokolların rolu böyükdür. Məsələn, SNMP (Simple Network Management Protocol) şəbəkə cihazlarından, məsələn, routerlər, switchlər, printerlər və serverlərdən məlumat toplamaq üçün geniş istifadə olunur. SNMP vasitəsilə cihazların vəziyyəti, işləmə statistikası və konfiqurasiya məlumatları sorğu ilə alınır. Bu, inventarlaşdırma prosesini avtomatlaşdırmağa və real vaxt monitorinqi təmin etməyə imkan verir.**

**Digər tərəfdən, SMTP (Simple Mail Transfer Protocol) e-poçt sistemlərinin işləməsi üçün istifadə olunur, lakin şəbəkə inventarlaşdırmasında e-poçt serverlərinin tapılması və monitorinqi üçün əhəmiyyət kəsb edir. SMTP xidmətləri aktiv olan serverlər müəyyən edilərək, onların təhlükəsizlik səviyyəsi yoxlanılır.**

**FTP (File Transfer Protocol) isə şəbəkədə fayl ötürmə xidməti göstərən serverlərin aşkarlanmasında istifadə olunur. Inventarlaşdırma zamanı FTP serverləri aşkar edilərək onların icazələri və təhlükəsizlik parametrləri qiymətləndirilir. Bu da şəbəkə təhlükəsizliyi üçün vacibdir, çünki zəif konfiqurasiya edilmiş FTP xidmətləri hücumçular üçün giriş nöqtəsi ola bilər.**

**Bu protokolların aktiv olub-olmaması və hansı versiyaların istifadə edilməsi sızma testləri və təhlükəsizlik auditləri zamanı önəmli məqamdır. Məsələn, köhnə və təhlükəsiz olmayan FTP versiyaları və ya SMTP serverləri sistemin zəif tərəflərindən biri ola bilər.**

**İnventarlaşdırma prosesində port skanlama vasitəsilə (məsələn, Nmap ilə) şəbəkədə bu protokolların işlədiyi portlar aşkar edilir: SMTP üçün 25 nömrəli port, FTP üçün 21 nömrəli port, SNMP üçün isə 161 nömrəli port əsasdır. Bu məlumatlar əsasında hansı xidmətlərin aktiv olduğu və onların təhlükəsizlik vəziyyəti təhlil olunur.**

8.Boşluqların idarə edilməsinin həyat dövrü mərhələləri. Boşluqlar üzrə məlumat mənbələri (Mövzu-6)

**Cavab:**

**Boşluqların idarə edilməsi (Vulnerability Management) – təşkilatın sistemlərində, proqram təminatında və infrastrukturunda olan zəifliklərin aşkar edilməsi, qiymətləndirilməsi, aradan qaldırılması və izlənməsi prosesidir. Bu idarəetmə, kibertəhlükəsizliyin effektivliyini artırmaq və potensial hücumları önləmək üçün vacibdir. Boşluqların idarə edilməsinin bir neçə əsas həyat dövrü mərhələsi mövcuddur.**

**Birinci mərhələ kəşfiyyat və aşkarlamadır. Bu mərhələdə müxtəlif avtomatlaşdırılmış alətlər və metodlar vasitəsilə şəbəkə, sistem və proqram təminatında mövcud olan boşluqlar müəyyən edilir. Ən çox istifadə olunan vasitələrə Nessus, OpenVAS, Qualys və Rapid7 Nexpose kimi skaner proqramları daxildir.**

**İkinci mərhələ təhlil və qiymətləndirmədir. Bu mərhələdə aşkar edilmiş boşluqların təhlükə səviyyəsi və potensial təsiri müəyyən edilir. CVSS (Common Vulnerability Scoring System) kimi standart ballandırma sistemləri istifadə olunaraq boşluqlar prioritetləşdirilir. Bu, resursların düzgün istiqamətləndirilməsi üçün vacibdir.**

**Üçüncü mərhələ tədbirlərin planlaşdırılması və tətbiqidir. Burada müəyyən edilmiş boşluqların aradan qaldırılması üçün tədbirlər görülür. Bu, proqram təminatının yenilənməsi, konfiqurasiya dəyişiklikləri, firewall qaydalarının tənzimlənməsi və ya digər müdafiə tədbirlərini əhatə edə bilər.**

**Dördüncü mərhələ izləmə və təkrarlamadır. Boşluqların idarə edilməsi davamlı proses olduğundan, sistemlərdə yenilənmələr və dəyişikliklər olduqca yenidən skanlama aparılır və nəticələr izlənilir. Bu mərhələ təhlükəsizlik vəziyyətinin sabit saxlanması üçün vacibdir.**

**Boşluqlar üzrə məlumat mənbələri müxtəlif formalarda ola bilər. Ən geniş istifadə olunan mənbələrdən biri Milli Təhlükəsizlik Məlumat Mərkəzləri (məsələn, NVD – National Vulnerability Database) və digər açıq təhlükəsizlik bazalarıdır. Bu bazalarda CVE (Common Vulnerabilities and Exposures) kimi unikal identifikatorlarla zəifliklər toplanır və təsnif edilir.**

**Digər məlumat mənbələrinə təhlükəsizlik xəbər saytları, təhlükəsizlik forumları, İT şirkətlərinin təhlükəsizlik məsləhətləri və təhlükəsizlik konfranslarının hesabatları daxildir. Mütəxəssislər həmçinin bug bounty proqramlarından və etik hakerlərin hesabatlarından məlumat əldə edirlər.**

**Boşluqların idarə edilməsində əsas məqsəd onların vaxtında aşkarlanması və aradan qaldırılmasıdır ki, bu da təşkilatın informasiya təhlükəsizliyini təmin edir. Bu prosesin düzgün aparılması kibertəhlükəsizlik strategiyasının əsasını təşkil edir və təşkilatı mümkün hücumlardan qoruyur.**

1. Boşluqların tezaurusu üzrə baza (CVE). Boşluqların skorinqi sistemi (CVSS) (Mövzu-6)

**Cavab:**

**Boşluqların tezaurusu üzrə baza, yəni CVE (Common Vulnerabilities and Exposures), kiber təhlükəsizlik sahəsində tanınmış zəifliklərin standartlaşdırılmış siyahısıdır. CVE, hər bir təhlükəsizlik boşluğu üçün unikal identifikator (məsələn, CVE-2023-12345) təqdim edir. Bu identifikatorlar vasitəsilə müxtəlif təhlükəsizlik vasitələri, məlumat bazaları və mütəxəssislər eyni boşluq barədə vahid şəkildə danışa bilir. CVE bazası təhlükəsizlik tədqiqatçıları, proqram təminatı istehsalçıları və sistem administratorları üçün əsas məlumat mənbəyidir.**

**CVE bazası, Milli Təhlükəsizlik Məlumat Mərkəzi (NVD - National Vulnerability Database) tərəfindən idarə olunur və açıqdır. Bu baza vasitəsilə istifadəçilər zəifliklərin təsviri, təsir sahəsi və həll yolları haqqında məlumat əldə edə bilirlər. CVE-lər dünyada geniş qəbul edilmiş standart olduğu üçün təhlükəsizlik analizlərinin əsasında dayanır.**

**Digər tərəfdən, CVSS (Common Vulnerability Scoring System) boşluqların təhlükə səviyyəsini qiymətləndirmək üçün istifadə olunan standart ballandırma sistemidir. CVSS skoru boşluğun ciddiliyini 0.0-dan 10.0-a qədər qiymətləndirir, burada 10 ən yüksək risk səviyyəsini göstərir. Bu skor, təhlükəsizlik komandalarına hansı boşluqların təcili aradan qaldırılmasını prioritetləşdirməyə kömək edir.**

**CVSS skoru üç əsas komponentdən ibarətdir: əsas baza skor, vaxtaşırı skor və çevrə skor. Əsas baza skor boşluğun texniki təsirini, hücumun çətinliyini və təsirlənən sistemin xüsusiyyətlərini nəzərə alır. Vaxtaşırı skor boşluğun həlli və ya təhlükə dərəcəsi dəyişdikdə yenilənir. Çevrə skor isə spesifik istifadəçi mühiti və biznes təsirlərini əhatə edir.**

**CVE və CVSS birlikdə təhlükəsizlik menecerlərinə, etik hakerlərə və sistem administratorlarına boşluqları effektiv şəkildə idarə etmək üçün zəruri vasitələr təqdim edir. CVE identifikatorları ilə boşluqlar müəyyən edilir, CVSS isə onların prioritetini göstərir.**

**Bu sistemlərdən istifadə etmək boşluqların vaxtında aşkarlanması, təsirinin düzgün qiymətləndirilməsi və uyğun müdafiə tədbirlərinin görülməsinə imkan verir. Beləliklə, təşkilatlar təhlükəsizlik risklərini daha səmərəli idarə edə bilir və mümkün hücumların qarşısını ala bilir.**

10.Sistemin hakinqi metodologiyası. Parolların sındırılması (Mövzu-7)

**Cavab:**

**Sistemin hakinqi metodologiyası kompüter sistemlərinə və şəbəkələrə qanunsuz və ya etik məqsədlə girmək üçün istifadə olunan addımlar və strategiyaların toplusudur. Bu metodologiya adətən bir neçə mərhələdən ibarətdir və məqsəd hədəf sistemin zəif nöqtələrini tapıb onlardan istifadə etməkdir. Bu mərhələlərə öncəliklə kəşfiyyat (reconnaissance), zəifliklərin aşkarlanması (vulnerability assessment), sızma testi (penetration testing), istismar (exploitation), sistemdə qalmaq (maintaining access) və izlərin gizlədilməsi (covering tracks) daxildir.**

**Birinci mərhələ olan kəşfiyyat zamanı hədəf haqqında məlumat toplanır. Bu məlumatlar arasında IP ünvanları, domenlər, şəbəkə arxitekturası, açıq portlar və xidmətlər olur. İkinci mərhələ zəifliklərin aşkarlanmasıdır, burada sistemdə olan proqram təminatı, konfiqurasiya və xidmətlərdə olan boşluqlar tapılır. Üçüncü mərhələ istismardır, yəni aşkarlanmış boşluqlardan istifadə edərək sistemə giriş əldə edilir.**

**Parolların sındırılması sistem hakinqinin ən geniş yayılmış metodlarından biridir və hədəf sistemin giriş şifrələrini tapmaq məqsədi daşıyır. Parollar müxtəlif üsullarla sındırıla bilər: sözlük hücumları (dictionary attacks), güc hücumları (brute force attacks), karma (hash) analizi, sosial mühəndislik və s.**

**Sözlük hücumu zamanı əvvəlcədən hazırlanmış sözlük fayllarında olan sözlər sistemin parol girişində sınanır. Bu metod güclü parollar üçün effektiv olmaya bilər, amma zəif parollarda çox faydalıdır. Güc hücumu isə bütün mümkün kombinasyonları sınayır və zaman tələb edən üsuldur.**

**Parolların sındırılması üçün çox vaxt parol məlumatlarının saxlanıldığı hash funksiyalarından istifadə edilir. Hücumçular hash-ləri əldə etdikdən sonra onları açmağa çalışırlar. Bunu etmək üçün onlar rainbow tables, salted hashes və digər texnikalardan istifadə edirlər.**

**Müasir təhlükəsizlikdə parolların sındırılması qarşısını almaq üçün iki faktorlu autentifikasiya (2FA), parol siyasətləri, şifrləmə və güclü hash funksiyaları tətbiq olunur. Eyni zamanda parolların tez-tez dəyişdirilməsi və istifadəçilərin maarifləndirilməsi də önəmlidir.**

**Sistemin hakinqi metodologiyasının və parolların sındırılması texnikalarının anlaşılması təhlükəsizlik mütəxəssislərinə hücumları qabaqcadan görmək və müdafiə tədbirləri hazırlamaq imkanı verir. Bu biliklər etik hakerlər üçün də vacibdir, çünki onlar sistemləri yoxlamaq və zəiflikləri aşkar etmək üçün bu metodlardan istifadə edir.**

11.İmtiyazların genişləndirilməsi. Tətbiqlərin icra edilməsi. Rutkitlər (Mövzu-7)

**Cavab:**

**İmtiyazların genişləndirilməsi (privilege escalation) kibertəhlükəsizlikdə hücumçunun sistemdə ilkin məhdud giriş hüququndan daha yüksək səviyyəli imtiyazlara keçid əldə etməsini ifadə edir. Bu, hücumçunun sistemdə daha çox nəzarət və idarəetmə imkanı qazanmasına səbəb olur. İmtiyazların genişləndirilməsi iki əsas növə bölünür: şaquli (vertical) və şaquli olmayan (horizontal) genişləndirmə.**

**Şaquli genişləndirmə zamanı istifadəçi aşağı səviyyəli icazələrdən idarəçi və ya kök (root) səviyyəli icazələrə keçid edir. Bu, sistemin tam nəzarətini əldə etmək deməkdir. Şaquli olmayan genişləndirmə isə istifadəçinin öz səviyyəsində digər istifadəçilərin resurslarına giriş əldə etməsidir.**

**İmtiyazların genişləndirilməsi üçün hücumçular sistem zəifliklərindən, konfiqurasiya səhvlərindən, proqram xətalarından və ya zəif təhlükəsizlik siyasətlərindən istifadə edirlər. Məsələn, köhnəlmiş proqram təminatı, icazələrin düzgün qurulmaması və ya zəif təhlükəsizlik parametrləri imtiyazların genişləndirilməsinə səbəb ola bilər.**

**Tətbiqlərin icra edilməsi (code execution) isə hücumçunun sistemdə öz zərərli kodunu işlətməsi deməkdir. Bu mərhələ imtiyazların genişləndirilməsi ilə birgə istifadə olunur və sistemə tam nəzarət üçün vacibdir. Hücumçu zərərli proqram, skript və ya komanda sətri əmrləri vasitəsilə sistemdə istənilən əməliyyatları icra edə bilər.**

**Bu mərhələdə istifadə olunan üsullardan biri rutkitlərin (rootkits) tətbiqidir. Rutkitlər – sistemdə gizlənərək fəaliyyət göstərən və hücumçunun izlərini gizlətməyə imkan verən zərərli proqramlardır. Onlar sistemin nüvəsinə yaxın səviyyədə işləyə və faylları, prosesləri, şəbəkə əlaqələrini gizlədə bilirlər.**

**Rutkitlər çox təhlükəlidir, çünki onlar adi antivirus proqramlarından gizlənə bilir və sistemdə uzun müddət aşkar olunmadan fəaliyyət göstərə bilirlər. Onlar həmçinin imtiyazların genişləndirilməsi prosesində istifadə olunaraq hücumçunun sistemdə qalmasını təmin edir.**

**İmtiyazların genişləndirilməsi, tətbiqlərin icra edilməsi və rutkitlərin fəaliyyəti sistem təhlükəsizliyinə ciddi təhdid yaradır. Bu səbəbdən təhlükəsizlik komandaları sistemləri mütəmadi yoxlamalı, zəiflikləri aradan qaldırmalı və şübhəli fəaliyyətləri izləməlidirlər.**

**Təhlükəsizliyi artırmaq üçün əməliyyat sistemləri və proqram təminatı daimi olaraq yenilənməli, imtiyazların idarə olunması siyasətləri tətbiq edilməli və sistemdə şübhəli proqramlar üçün monitorinq aparılmalıdır.**

12.Faylların gizlədilməsi. Steqanoqrafiya (Mövzu-7)

**Cavab:**

**Faylların gizlədilməsi (file hiding) kibertəhlükəsizlikdə məlumatların və ya faylların aşkarlanmasının çətinləşdirilməsi üçün istifadə olunan texnikaları əhatə edir. Bu metodlar hücumçuların zərərli faylları, virusları və ya kritik məlumatları sistemdə gizlətməsi üçün geniş istifadə olunur. Faylların gizlədilməsi həmçinin sistem idarəçiləri tərəfindən məlumatların qorunması məqsədilə də tətbiq oluna bilər.**

**Faylların gizlədilməsi müxtəlif üsullarla həyata keçirilir. Məsələn, faylın atributlarını dəyişdirmək, onu görünməz etmək (hidden attribute), faylın adını dəyişdirərək diqqətdən yayınmaq və ya faylı sistemin xüsusi qovluqlarına yerləşdirmək kimi üsullar geniş yayılıb. Bəzi hallarda fayl adları simvollarla qarışdırılır ki, onları adi istifadəçilər və ya təhlükəsizlik proqramları tanıya bilməsin.**

**Digər bir inkişaf etmiş metod steqanoqrafiya (steganography) adlanır. Steqanoqrafiya məlumatları başqa fayl və ya media vasitələrinin daxilində gizlətmək sənətidir. Bu metodla, məsələn, mətn faylı, şəkil, səs və ya video faylı içərisində görünməyən şəkildə məlumat yerləşdirmək mümkündür.**

**Steqanoqrafiya ən çox rəqəmsal şəkillərdə istifadə olunur, çünki şəkil faylının piksellərində kiçik dəyişikliklər aparmaqla gizli məlumatlar yerləşdirilə bilər. Bu dəyişikliklər insan gözü ilə fərqləndirilməz, lakin xüsusi proqramlar vasitəsilə məlumatlar çıxarıla bilər.**

**Bu üsul, həm qanuni məqsədlərlə (məsələn, müəllif hüququ qorunması və ya gizli mesajların ötürülməsi), həm də zərərli məqsədlərlə (məsələn, zərərli proqramların gizlədilməsi və ya məlumat oğurluğu) istifadə oluna bilər.**

**Steqanoqrafiya alətləri məlumatların ötürülməsində və saxlamaqda əlavə gizlilik təmin edir. Məsələn, hücumçular zərərli kodu şəkil faylı içərisində gizlədərək antivirus proqramlarından qaça bilərlər.**

**Faylların gizlədilməsi və steqanoqrafiya üsullarına qarşı mübarizə üçün xüsusi analiz və aşkar etmə alətləri mövcuddur. Bu alətlər faylların içində gizlədilmiş məlumatları aşkar etmək üçün müxtəlif analitik metodlardan istifadə edir.**

**Nəticədə, faylların gizlədilməsi və steqanoqrafiya həm təhlükəsizlik riskləri, həm də müdafiə üsulları baxımından vacib sahələrdir. Bu texnikaların düzgün anlaşılması kibertəhlükəsizlik mütəxəssislərinə həm hücumların qarşısını almağa, həm də məlumatların qorunmasına kömək edir.**

13.Saytlararası skript (XSS) hücumları (Mövzu-7)

**Cavab:**

**Saytlararası skript (XSS) hücumları veb tətbiqlərinə yönəlmiş çox geniş yayılmış təhlükə növüdür. XSS hücumu zamanı hücumçu zərərli skript kodunu (adətən JavaScript) etibarlı veb saytın daxilində yerləşdirir. Bu skript kodu saytın digər istifadəçilərinin brauzerində icra olunur və onların sessiya məlumatlarını oğurlamaq, istifadəçi hesablarını ələ keçirmək və ya istifadəçiləri zərərli saytlara yönləndirmək kimi məqsədlərə xidmət edir.**

**XSS hücumları əsasən üç əsas növə bölünür: stored (saxlanmış), reflected (əks olunan) və DOM-based (DOM əsaslı) XSS.**

**Stored XSS zamanı zərərli skript saytın verilənlər bazasında saxlanılır və hər dəfə həmin səhifə istifadəçilər tərəfindən açıldıqda avtomatik işləyir. Bu növ hücum çox təhlükəlidir, çünki zərərli kod çoxlu sayda istifadəçiyə yayılır.**

**Reflected XSS isə zərərli kodun URL və ya istək parametrləri kimi göndərilməsi ilə icra olunur. Burada kod sayt serveri tərəfindən emal olunmadan istifadəçinin brauzerinə geri göndərilir. Bu növ hücum daha çox phishing və sosial mühəndislik üsulları ilə birgə istifadə olunur.**

**DOM-based XSS isə zərərli kodun veb səhifənin Document Object Model (DOM) strukturu içərisində, istifadəçi brauzerində işləməsi ilə bağlıdır. Bu tip hücum veb saytın serverindən asılı deyil və daha çox müasir veb tətbiqlərdə görülür.**

**XSS hücumlarının qarşısını almaq üçün veb tətbiq sahibləri giriş məlumatlarını düzgün təmizləməli (input validation), xüsusi simvolları (məsələn, <, >, &) əvəz etməli (output encoding) və məzmun təhlükəsizlik siyasəti (Content Security Policy - CSP) tətbiq etməlidirlər.**

**Bundan əlavə, istifadəçi sessiyalarının təhlükəsizliyi üçün HTTP-Only və Secure atributlu cookie-lərdən istifadə etmək vacibdir. Bu, brauzerdə zərərli JavaScript-in sessiya cookie-lərinə girişinin qarşısını alır.**

**XSS hücumları nəticəsində istifadəçi məlumatlarının oğurlanması, saytın reputasiyasının zədələnməsi və maliyyə itkiləri baş verə bilər. Buna görə də veb inkişaf etdiricilər və təhlükəsizlik mütəxəssisləri bu hücumlara qarşı ciddi tədbirlər görməlidirlər.**

**XSS testləri və skanerləri vasitəsilə veb tətbiqlərdə olan bu zəifliklər erkən mərhələdə aşkar edilə bilər. Mütəmadi təhlükəsizlik auditləri və kodun yoxlanılması da vacibdir.**

14.Sosial mühəndislik hücumları (Mövzu-8)

**Cavab:**

**Sosial mühəndislik hücumları insan psixologiyasından istifadə edərək insanları aldadıb gizli məlumatları və ya sistemlərə girişləri ələ keçirmə üsuludur. Bu hücum növü texniki zəifliklərdən daha çox insan faktoru üzərində qurulur. Hücumçular insanların etibarından, qorxu və tələsmə hissindən faydalanaraq onları istədikləri hərəkətə məcbur edə bilirlər.**

**Sosial mühəndislik müxtəlif üsullarla həyata keçirilə bilər: fırıldaqçılıq (phishing), telefon zəngləri (vishing), SMS mesajları (smishing), şəxsən görüşlər və ya sosial media vasitəsilə. Məsələn, phishing hücumunda istifadəçiyə rəsmi görünən, amma zərərli linklər və ya saxta formalar göndərilir.**

**Bu hücumlar istifadəçinin şifrəsini, kredit kartı məlumatlarını, şəxsi sənədlərini və ya korporativ məlumatları əldə etmək məqsədi daşıyır. Sosial mühəndislik hücumları çox vaxt insanları inandırmaq və təzyiq altında saxlamaq üçün manipulyasiya və emosional oyunlardan istifadə edir.**

**Pretexting adlı metodda hücumçu özünü etibarlı şəxs kimi təqdim edir və beləliklə istifadəçidən məlumat almağa çalışır. Baiting üsulunda isə istifadəçilərə maraqlı və ya pulsuz bir şey vəd edilərək məlumatların verilməsi təmin edilir.**

**Sosial mühəndislik hücumlarından qorunmaq üçün istifadəçilərin maarifləndirilməsi çox önəmlidir. İnsanlar tanımadıqları şəxslərdən gələn e-maillərə, linklərə və ya mesajlara diqqətli yanaşmalıdır. Güclü parollar və çoxfaktorlu autentifikasiya əlavə müdafiə təmin edir.**

**Təşkilatlar isə işçilər üçün davamlı təhlükəsizlik təlimləri keçirməli, phishing testləri aparmalı və istifadəçilərə real nümunələr əsasında məlumat verməlidir. Həmçinin, kritik məlumatların yalnız etibarlı şəxslərlə paylaşılması və məlumatların şifrələnməsi də tövsiyə olunur.**

**Sosial mühəndislik hücumlarının təsirli olması insanların psixoloji zəifliklərindən və diqqətsizliyindən istifadə etməsidir. Bu səbəbdən həm fərdi, həm də təşkilati səviyyədə diqqətli olmaq və təhlükəsizlik mədəniyyətini inkişaf etdirmək vacibdir.**

1. **Phishing (Fırıldaqçılıq)  
   İstifadəçilərə rəsmi və etibarlı görünən e-maillər, mesajlar və ya saytlar göndərilərək onları şəxsi məlumatları (şifrə, kart məlumatları və s.) daxil etməyə aldadılmasıdır.**
2. **Spear Phishing (Hədəfli Fırıldaqçılıq)  
   Phishing-in daha məqsədyönlü variantıdır. Hücumçu konkret şəxsi və ya şirkəti hədəf alır, onun haqqında əvvəlcədən məlumat toplayır və daha inandırıcı mesajlar göndərir.**
3. **Vishing (Səsli Fırıldaqçılıq)  
   Telefon zəngləri vasitəsilə insanları aldatmaqdır. Hücumçu özünü bank və ya rəsmi qurum nümayəndəsi kimi təqdim edərək, istifadəçidən məlumat almağa çalışır.**
4. **Smishing (SMS Fırıldaqçılığı)  
   Mobil telefonlara göndərilən zərərli link və ya mesajlar vasitəsilə məlumatların oğurlanmasıdır. Bu mesajlar istifadəçini linkə klikləməyə və ya zərərli proqram yükləməyə təşviq edir.**
5. **Pretexting (Ön Mətn Yaratma)  
   Hücumçu özünü etibarlı şəxs kimi təqdim edərək (məsələn, polis, bank əməkdaşı və ya IT dəstəyi), qurbanın məlumatlarını əldə etməyə çalışır.**
6. **Baiting (Tələ Qoyma)  
   Fiziki və ya rəqəmsal mühitdə maraqlı və ya pulsuz görünən obyektlər (məsələn, USB yaddaş kartı) vasitəsilə istifadəçini zərərli proqramı yaymağa təşviq etmək.**
7. **Tailgating (Arxadan İzləmə)  
   Fiziki girişin qorunmadığı yerlərdə, icazəsiz şəxs digərinin arxasınca girərək giriş icazəsi tələb etmədən məkanlara daxil olur.**
8. **Quid pro quo (Əvəzində Bir Şey Təklif Edilməsi)  
   Hücumçu istifadəçiyə bir fayda vəd edərək (məsələn, texniki yardım) onun şəxsi və ya sistem məlumatlarını əldə etməyə çalışır.**

15.DDoS hücumları və müdafiə üsulları (Mövzu-9)

**Cavab:**

**DDoS (Distributed Denial of Service) hücumu çoxsaylı kompromit edilmiş cihazlardan (botnetlərdən) təşkil olunmuş hücumdur. Bu hücumda hədəf server, şəbəkə və ya xidmətə qarşı çoxlu sayda sorğu göndərilir ki, resurslar tükənsin və xidmətin göstərilməsi mümkün olmasın. Məqsəd sistemin işini dayandırmaq, xidmətin əlçatanlığını itirmək və ya istifadəçilərin ona girişini məhdudlaşdırmaqdır.**

**DDoS hücumları müxtəlif növlərdə olur: trafik əsaslı (volumetric), protokol əsaslı və tətbiq səviyyəsində (application layer) hücumlar. Trafik əsaslı hücumlar hədəfi böyük miqdarda zərərli trafiklə yükləyir, protokol əsaslı hücumlar serverin və ya şəbəkənin resurslarını tükədir, tətbiq səviyyəsində hücumlar isə xüsusi tətbiq zəifliklərindən istifadə edir.**

**DDoS hücumlarının təsirli olması üçün çoxlu sayda fərqli cihazlar, bəzən dünya üzrə yayılan botnetlər istifadə olunur. Bu səbəbdən hücum mənbəyini tapmaq və bloklamaq çətinləşir.**

**DDoS hücumlarına qarşı müdafiə üçün bir neçə üsul tətbiq olunur. İlk olaraq, şəbəkə səviyyəsində trafik filtrlənməsi aparılır. Bu, firewall, router və ya xüsusi DDoS müdafiə cihazları vasitəsilə həyata keçirilir.**

**Digər müdafiə üsulu kimi trafik analiz və anomaliya aşkarlama sistemləri istifadə olunur. Bu sistemlər normal trafik nümunələrini öyrənərək, şübhəli trafiki təyin edir və onu bloklayır.**

**Load balancing (yük balanslaşdırma) də DDoS hücumlarının qarşısını almaqda kömək edir. Trafiki bir neçə serverə paylayaraq, hər bir serverin yüklənməsini azaldır və sistemin dayanıqlığını artırır.**

**Bundan əlavə, bulud əsaslı DDoS müdafiə xidmətləri hücumu tutmaq və zərərli trafiki əngəlləmək üçün geniş şəbəkə imkanlarından istifadə edir. Bu xidmətlər hücum zamanı trafikin böyük hissəsini öz üzərlərinə götürür.**

**Müdafiə üçün həmçinin rate limiting (sorğu limitlənməsi) tətbiq edilə bilər, yəni müəyyən IP-dən gələn sorğuların sayı məhdudlaşdırılır.**

**DDoS hücumlarının qarşısını almaq üçün qabaqcıl təhlükəsizlik siyasətləri və təlimatlar hazırlanmalıdır. Müntəzəm olaraq şəbəkə monitorinqi aparılmalı, zəif nöqtələr aradan qaldırılmalı və əməkdaşlıq əlaqələri qurulmalıdır.**

**Nəticədə, DDoS hücumları böyük zərər verə biləcək təhlükədir, amma düzgün tədbirlərlə onların təsirini minimuma endirmək mümkündür.**

16.Metasploit freymvorku. MSFCONSOLE komandaları (Mövzu-10)

**Cavab:**

**Metasploit freymvorku kibertəhlükəsizlik və sızma testi sahəsində geniş istifadə olunan açıq mənbəli platformadır. O, təhlükəsizlik mütəxəssislərinə sistemlərin zəifliklərini tapmaq, sınaqdan keçirmək və müdafiəni yoxlamaq üçün müxtəlif modullar və alətlər təqdim edir. Metasploit istifadəçilərə zərərli proqramlar yaratmaq, hücum senariləri tərtib etmək və təcrübələr aparmaq imkanı verir.**

**Freymvork çoxsaylı exploitlər, payloadlar, scannerlər və auxiliary modulllarla zəngindir. Bu, hücum səhnəsini real şəraitdə təqlid etmək və sistemlərin zəifliklərini tapmaq üçün geniş imkan yaradır. Metasploit həmçinin avtomatlaşdırılmış hücumların sınaqdan keçirilməsi və penetrasiya testləri üçün geniş istifadə olunur.**

**MSFCONSOLE Metasploit-in ən məşhur və geniş istifadə olunan istifadəçi interfeysidir. Bu konsol vasitəsilə istifadəçilər komandalar daxil etməklə modul seçə, konfiqurasiya edə və hücumları həyata keçirə bilərlər. MSFCONSOLE komandaları freymvorkun funksiyalarını idarə etmək üçün əsas vasitədir.**

**Əsas MSFCONSOLE komandalarına aşağıdakılar daxildir:**

* **search — mövcud modul və exploitləri axtarır.**
* **use — seçilmiş modulu aktivləşdirir.**
* **show options — modulun konfiqurasiya parametrlərini göstərir.**
* **set — modul parametrlərini təyin edir, məsələn, hədəf IP ünvanı.**
* **exploit və ya run — seçilmiş modulu işə salır və hücumu həyata keçirir.**
* **sessions — aktiv sessiyaları idarə edir və onların siyahısını göstərir.**
* **info — modullar haqqında ətraflı məlumat verir.**
* **exit — MSFCONSOLE-dan çıxır.**

**Bundan əlavə, background komandası ilə aktiv sessiyanı fon prosesinə göndərmək, jobs komandası ilə işləyən prosesləri idarə etmək mümkündür. help komandası bütün mövcud əmrlərin siyahısını göstərir.**

**Metasploit freymvorku həm yeni başlayanlar, həm də təcrübəli pentesterlər üçün çox faydalıdır. O, zəifliklərin aşkarlanması və sınaqdan keçirilməsi prosesini sadələşdirir və təhlükəsizlik testlərinin effektivliyini artırır.**

**Nəticədə, Metasploit və MSFCONSOLE komandaları kiber təhlükəsizlik sahəsində hücum və müdafiə bacarıqlarını inkişaf etdirmək üçün vacib vasitələrdir.**

17.Veb tətbiqlərin təhlükəsizliyi. OWASP yanaşması (Mövzu-11)

**Cavab:**

**Veb tətbiqlərin təhlükəsizliyi internet üzərindən xidmət göstərən proqramların və sistemlərin qorunmasıdır. Veb tətbiqlər hər gün milyardlarla istifadəçi tərəfindən işlədilir və bu səbəbdən onlar hücumçular üçün əsas hədəf sayılır. Təhlükəsiz veb tətbiqlər istifadəçi məlumatlarını qoruyur, məlumatların bütövlüyünü təmin edir və xidmətin dayanıqlığını saxlayır.**

**Veb tətbiqlərdə olan zəifliklər hücumçulara məlumat oğurlamaq, sistemə zərərli kod yeritmək və ya xidmətləri dayandırmaq imkanı verir. Buna görə də veb tətbiqlərin təhlükəsizliyi həm inkişaf prosesində, həm də istifadə zamanı davamlı təmin olunmalıdır.**

**OWASP (Open Web Application Security Project) veb tətbiqlərin təhlükəsizliyi sahəsində ən nüfuzlu beynəlxalq təşkilatlardan biridir. OWASP təhlükəsizlik təcrübələrinin yayılması və veb tətbiqlərin ən çox rast gəlinən zəifliklərinin müəyyən edilməsi üçün resurslar yaradır.**

**OWASP-in məşhur Top 10 siyahısı veb tətbiqlərdə ən kritik zəiflikləri sıralayır. Bu siyahıya daxil olan zəifliklərə:**

* **Injection hücumları (məsələn, SQL injection),**
* **Broken Authentication (sındırılmış autentifikasiya),**
* **Sensitive Data Exposure (həssas məlumatların ifşası),**
* **XML External Entities (XXE),**
* **Broken Access Control (sındırılmış giriş nəzarəti),**
* **Security Misconfiguration (təhlükəsizlik səhvləri),**
* **Cross-Site Scripting (XSS),**
* **Insecure Deserialization (təhlükəsiz olmayan seriyalaşdırma),**
* **Using Components with Known Vulnerabilities (zəif komponentlərin istifadəsi),**
* **və Insufficient Logging & Monitoring (qeyri-kafi loglama və monitorinq) daxildir.**

**OWASP yanaşması tətbiq təhlükəsizliyinin inkişaf mərhələlərində tətbiq olunmasını tövsiyə edir. Bu, təhlükəsizlik dizaynı, kodun təhlükəsiz yazılması, testlərin aparılması və tətbiqin istismarı zamanı monitorinqi əhatə edir.**

**Veb tətbiqlərin təhlükəsizliyində autentifikasiya və avtorizasiya proseslərinin düzgün qurulması vacibdir. Güclü şifrə siyasəti, çoxfaktorlu autentifikasiya və sessiya idarəsi tətbiq edilməlidir. Məlumatların ötürülməsi zamanı SSL/TLS kimi şifrələmə protokollarından istifadə zəruridir.**

**İstifadəçi daxil olan məlumatların təmizlənməsi (input validation) və təhlükəsiz çıxış (output encoding) hücumların qarşısını almaqda əsas rol oynayır. Ayrıca, veb tətbiqlər mütəmadi olaraq təhlükəsizlik skanerləri ilə yoxlanmalı və zəifliklər aradan qaldırılmalıdır.**

**OWASP həmçinin veb tətbiqlərin inkişafında təhlükəsizlik testlərini avtomatlaşdırmaq üçün müxtəlif alətlər təklif edir. Bunlar proqram təminatında zəiflikləri aşkarlamaq və aradan qaldırmaq üçün əhəmiyyətlidir.**

**Nəticədə, veb tətbiqlərin təhlükəsizliyi həm texniki, həm də inzibati tədbirlərin kompleks tətbiqini tələb edir. OWASP yanaşması bu prosesdə rəhbər kimi çıxış edir və təhlükəsizlik səviyyəsini artırmaq üçün geniş imkanlar təqdim edir.**

18.Veb sistemlərə hücumların əsas sinifləri (Mövzu-11)

**Cavab:**

**Veb sistemlərə hücumlar müxtəlif üsullar və texnikalarla həyata keçirilir və əsasən bu hücumların sinifləri onların məqsədinə, texnikasına və təsir sahəsinə görə fərqlənir. Hücumların əsas siniflərini bilmək veb sistemlərin qorunmasını gücləndirməyə kömək edir.**

**Birinci sinif Injection hücumlarıdır. Bunlar SQL, OS, LDAP kimi sorğu dilinə zərərli kod yerləşdirməklə məlumatların oğurlanması və ya dəyişdirilməsi məqsədi daşıyır. SQL Injection ən çox rast gəlinən və təhlükəli hücum növüdür.**

**İkinci sinif Cross-Site Scripting (XSS) hücumlarıdır. Burada hücumçu veb səhifəyə zərərli skript kodu yerləşdirir və həmin kod istifadəçinin brauzerində işləyir. Bu, sessiya oğurluğu, məlumatların manipulyasiyası və ya phishing hücumları üçün istifadə olunur.**

**Üçüncü sinif Cross-Site Request Forgery (CSRF) hücumlarıdır. Bu hücumda istifadəçi etibar etdiyi sayta qarşı öz xəbəri olmadan zərərli sorğu göndərir və bu yolla sistemdə icazəsiz əməliyyatlar həyata keçirilir.**

**Dördüncü sinif Denial of Service (DoS) və Distributed Denial of Service (DDoS) hücumlarıdır. Bu hücumlarda server və ya şəbəkə çoxlu sayda sorğu ilə yüklənir və xidmətlərin dayandırılması məqsədi güdülür.**

**Beşinci sinif Authentication və Authorization hücumlarıdır. Burada istifadəçinin identifikasiyası və icazələrinin sındırılması məqsədi ilə parol oğurluğu, brute force, və ya session hijacking kimi üsullar tətbiq edilir.**

**Altıncı sinif Directory Traversal və Path Traversal hücumlarıdır. Bu hücumlarda hücumçu serverin fayl sistemində icazəsiz girişi təmin etmək üçün zəifliklərdən istifadə edir.**

**Yeddinci sinif File Inclusion hücumlarıdır. Burada hücumçu zərərli faylları serverə daxil etməklə təhlükəsizlik zəifliklərini istismar edir, məsələn, Remote File Inclusion (RFI) və Local File Inclusion (LFI).**

**Səkkizinci sinif \*\*Security Misconfiguration (Təhlükəsizlik səhvləri)\*\*dır. Yanlış konfiqurasiya edilmiş serverlər, proqramlar və şəbəkə qurğuları hücumçular üçün asan giriş imkanları yaradır.**

**Doqquzuncu sinif \*\*Sensitive Data Exposure (Həssas məlumatların açıqlanması)\*\*dır. Bu, zəif şifrələmə, məlumatların açıq saxlanması və ya icazəsiz giriş nəticəsində şəxsi məlumatların oğurlanmasıdır.**

**Onuncu sinif Insufficient Logging və Monitoring-dir. Bu, hadisələrin qeydə alınmaması və ya vaxtında aşkarlanması olmaması səbəbindən hücumların müəyyən edilə və qarşısı alınmağının çətinləşməsidir.**

**Bu siniflər veb sistemlərə edilən hücumların ən çox yayılmış və kritik kateqoriyalarını əhatə edir. Təhlükəsizliyin təminatı üçün bu hücum növlərinin hər birinə qarşı tədbirlər görülməlidir.**

19.SQL inyeksiyası metodologiyası. SQL inyeksiyasının növləri (Mövzu-11)

**Cavab:**

**SQL inyeksiyası (SQL Injection) veb tətbiqlərdə ən çox rast gəlinən və təhlükəli zəifliklərdən biridir. Bu hücum üsulunda hücumçu istifadəçi daxil etdiyi məlumatları (məsələn, formalar, URL-lər) manipulyasiya edərək, zərərli SQL kodunu sorğuya daxil edir. Nəticədə, verilənlər bazasına icazəsiz giriş əldə edilir və məlumatlar oğurlana, dəyişdirilə və ya silinə bilər.**

**SQL inyeksiyasının əsas məqsədi verilənlər bazasının idarəetmə sistemini aldatmaq və hücumçuya istədiyi əməliyyatları yerinə yetirmək üçün imkan yaratmaqdır. Bu, istifadəçinin daxil etdiyi məlumatın düzgün yoxlanılmaması və təmizlənməməsi səbəbindən baş verir.**

**SQL inyeksiyasının metodologiyası adətən bir neçə mərhələdən ibarətdir: əvvəlcə hücumçu zəif tətbiqləri müəyyən edir, sonra məlumat toplamaq üçün sorğular göndərir, sonda isə verilənlər bazasına zərərli əmrlər yeridir.**

**Bu hücumun müxtəlif növləri mövcuddur:**

* **Error-based SQL Injection: Hücumçu verilənlər bazasının səhv mesajlarından istifadə edərək məlumat toplayır.**
* **Union-based SQL Injection: Bu metodda iki və ya daha çox SQL sorğusu birləşdirilərək əlavə məlumatlar əldə edilir.**
* **Blind SQL Injection: Hücumçu verilənlər bazasından məlumatları birbaşa ala bilmir, amma bəli/xeyr cavabları ilə məlumatı mərhələli şəkildə çıxarır. Bu növ Boolean-based və Time-based olaraq iki yerə bölünür.**
* **Out-of-Band SQL Injection: Bu nadir növdə hücumçu məlumatı serverdən başqa kanallar vasitəsilə əldə edir, məsələn DNS sorğuları.**

**SQL inyeksiyasına qarşı müdafiə üsullarına daxil olan ən vacib addımlar: parametrli sorğulardan (prepared statements) istifadə etmək, istifadəçi daxil olan məlumatları düzgün yoxlamaq və təmizləmək (input validation), verilənlər bazasının səhvlərini gizlətmək, və ən əsası tətbiqin və verilənlər bazasının təhlükəsizlik yeniləmələrini vaxtında etməkdir.**

**Müasir veb tətbiq təhlükəsizliyi üçün SQL inyeksiyasının qarşısının alınması mühüm yer tutur. Bu zəiflikdən qorunmaq üçün proqramçılar və təhlükəsizlik mütəxəssisləri müxtəlif test və analizlər aparmalıdırlar.**

**Nəticədə, SQL inyeksiyası ciddi təhlükədir, amma düzgün tədbirlər və müasir metodlarla effektiv şəkildə qarşısı alınır.**

20.Naqilsiz şəbəkə konsepsiyası (Mühazirə-12)

**Cavab:**

**Naqilsiz şəbəkə (Wireless Network) anlayışı, məlumatların ötürülməsi üçün fiziki kabel və naqillərin istifadə edilmədiyi şəbəkə növüdür. Bu şəbəkələrdə məlumatlar elektromaqnit dalğaları, adətən radio dalğaları və ya infraqırmızı siqnallar vasitəsilə ötürülür. Naqilsiz şəbəkələr istifadəçilərə mobil və sərbəst əlaqə imkanı yaradır, çünki onlar kabelsiz və sərhədsizdir.**

**Naqilsiz şəbəkələrin əsas komponentləri arasında access point (AP), istifadəçi cihazları (məsələn, laptoplar, smartfonlar) və naqilsiz routerlər yer alır. Bu cihazlar şəbəkə daxilində əlaqə yaradır və məlumat mübadiləsini təmin edir.**

**Naqilsiz şəbəkələr müxtəlif növlərdə olur:**

* **Wi-Fi ən çox istifadə olunan naqilsiz şəbəkə texnologiyasıdır, evlərdə, ofislərdə və ictimai yerlərdə geniş tətbiq olunur.**
* **Bluetooth daha qısa məsafələr üçün nəzərdə tutulub və əsasən cihazlar arasında əlaqə üçün istifadə edilir.**
* **Mobil şəbəkələr (3G, 4G, 5G) mobil rabitə üçün naqilsiz şəbəkə kimi çıxış edir.**

**Naqilsiz şəbəkələrin üstünlüklərinə sərbəst hərəkət etmək imkanı, quraşdırmanın asanlığı, fiziki məhdudiyyətlərin olmaması daxildir. Bu, xüsusilə ofis, təhsil və ictimai yerlərdə çox önəmlidir.**

**Amma naqilsiz şəbəkələrdə təhlükəsizlik məsələləri də önəmlidir. Siqnallar açıq havada yayıldığı üçün, hücumçular bu şəbəkələrə müdaxilə edə, məlumatları ələ keçirə və ya xidmətləri poza bilərlər.**

**Naqilsiz şəbəkələrin təhlükəsizliyi üçün WPA, WPA2 və WPA3 kimi şifrələmə protokolları istifadə olunur. Bunlar məlumatların şifrələnməsi və şəbəkəyə icazəsiz girişin qarşısını almaq üçün vacibdir.**

**Bundan əlavə, təhlükəsiz əlaqə üçün güclü şifrə siyasəti, MAC ünvanlarının filtrlənməsi, VPN istifadəsi və müntəzəm şəbəkə monitorinqi tövsiyə olunur.**

**Naqilsiz şəbəkələrin idarə olunması üçün xüsusi proqram və alətlər mövcuddur. Bunlar şəbəkə performansını izləmək, istifadəçiləri idarə etmək və təhlükəsizlik tədbirlərini həyata keçirməkdə kömək edir.**

**Son illərdə IoT (Internet of Things) texnologiyalarının inkişafı ilə naqilsiz şəbəkələrin rolu daha da artmışdır. Çünki çoxsaylı cihazlar simsiz şəbəkələr vasitəsilə bir-biri ilə əlaqə yaradır.**

**Nəticədə, naqilsiz şəbəkələr müasir dövrdə əvəzolunmaz texnologiyadır. Onlar yüksək çeviklik və rahatlıq təqdim etsələr də, təhlükəsizlik və idarəetmə məsələləri diqqətlə nəzərə alınmalıdır.**

**Praktiki suallar:**

**1. Aşağıdakı tapşırıqları yerinə yetirmək üçün Linux əmrlərini yazın:**

1. Desktop-da **EXAM** adlı yeni bir gizli qovluq yaratmaq üçün uyğun əmri daxil edin. **EXAM** qovluğunun daxilində **“exam1.txt” , “exam2.txt”, “exam3.txt”** adlı üç yeni fayl yaradın və aşağıdakı mətni **exam2.txt** adlı faylın daxilinə qeyd edin:

*“Cybersecurity is the practice of protecting systems, networks and programs from digital attacks”.*

**Cavab:**

**cd Desktop**

**mkdir .EXAM**

**touch exam1.txt exam2.txt exam3.txt**

**echo “Cybersecurity is the practice of protecting systems, networks and programs from digital attacks” > exam2.txt**

1. **exam2.txt** faylının məzmununa baxın və **exam1.txt** faylını isə silin.

**Cavab:**

**cat exam2.txt**

**rm exam1.txt**

1. **EXAM** qovluğunu gizli rejimdən çıxararaq adını **EXAM2** olaraq dəyişdirin.

**Cavab:**

**mv ~/Desktop/.EXAM ~/Desktop/EXAM2**

1. **exam2.txt** faylını Desktopa köçürün və adını **document2.txt** olaraq dəyişdirin.

**Cavab:**

**mv ~/Desktop/EXAM2/exam2.txt ~/Desktop/document2.txt**

1. **exam3.txt** faylının icazələri aşağıda qeyd olunmuşdur. İcazələri izah edin və faylın **group (g)** icazələrini dəyişdirərək **write (w)** və **execute (x)** icazələrini əlavə etmək üçün uyğun əmr kombinasiyasını daxil edin.

***-rw-r--r-- 1 root root 0 Apr 19 03:45 exam3.txt***

**Cavab:**

**cd ~/Desktop/EXAM2**

**chmod 674 exam3.txt**

**2. Aşağıda verilmiş Linux əmrlərinin məqsəd və mahiyyətini nümunələrlə izah edin:**

1. **alias** və **unalias** əmrləri.

**Cavab: alias əmri standart olaraq təyin edilmiş komandaların adını dəyişdirmək üçün istifadə olunur.Məsələn,**

**alias c=’clear’**

**bu komandadan sonra biz terminalı təmizləmək üçün clear əmrindən deyil c əmrindən istifadə etməyimiz kifayətdir.**

**unalias əmri isə təyin olunmuş aliasları silmək üçündür.Məsələn,**

**unalias c**

**bu komanda artıq bu təyinetməni aradan qaldıracaq və clear əmri öz qaydasında işləyəcək.**

1. **grep, find, locate** əmrləri.

**Cavab:**

**grep komandası faylların mətn daxilində müəyyən söz və ya ifadəni axtarmaq üçün istifadə olunur.Məsələn,**

**grep “Cybersecurity” document2.txt**

**find komandası fayl və qovluqları fayl sistemində kriteriyalara görə tapmaq üçün istifadə olunur.Məsələn,**

**find /home/user -name "\*.txt"**

**bu zaman bütün .txt faylları ekrana çıxacaq.**

**locate komandası fayl adlarına görə sürətli axtarış üçün istifadə olunur.İndeksdən istifadə edir.Məsələn,**

**locate aztu.pdf**

1. **cat, less** əmrləri.

**Cavab:**

**cat komandası faylın məzmununu terminalda birdəfəlik göstərmək üçün istifadə olunur.Məsələn,**

**cat exam2.txt**

**cat -n exam2.txt (Sətirləri nömrələyərək göstərir)**

**cat -b exam2.txt (yalnız boş olmayan sətirləri nömrələyir)**

**less komandası böyük faylların məzmununu səhifələyərək (scroll) oxumağa imkan verir.Məsələn,**

**less test.txt**

1. **cd** əmri və parametrləri.

**Cavab:**

**cd əmri cari işçi qovluğu dəyişdirmək üçün istifadə olunur.Məsələn,**

**cd Desktop**

**cd .. bir səviyyə yuxarı qovluğa keçir.**

**cd ~ istifadəçinin ev qovluğuna keçir.**

**cd - əvvəlki qovluğa qayıdır.**

1. **wc** əmri və parametrləri.

**Cavab:**

**wc əmri fayldakı sətir, söz və simvolların sayını göstərir.Məsələn,**

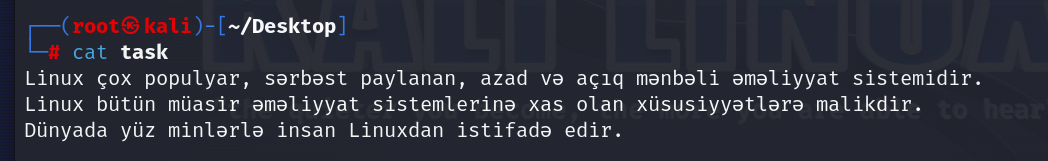
**wc document2.txt**

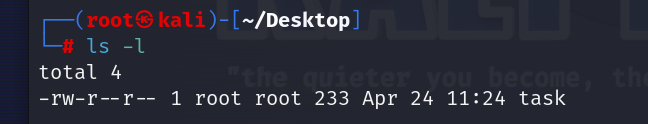
**wc -l document2.txt (yalnız sətirlərin sayını göstərir)**

**wc -c document2.txt (yalnız simvolların sayını göstərir)**

**wc -w document2.txt (yalnız sözlərin sayını göstərir)**

**3. Aşağıdakı tapşırıqları yerinə yetirmək üçün Linux əmrlərini yazın:**





1. **chmod 731 task** əmr kombinasiyasının nəticəsini qeyd edin.

**Cavab:**

**731**

**7- rwx**

**3-wx**

**1-x**

**Nəticə: -rwx-wx—x 1 root root 233 apr 24 11:24 task**

1. **cat –n task** əmrinin nəticəsi nə olacaqdır?

**Cavab: Sətirləri nömrələyərək ekrana çıxaracaqdır.**

1. **task** faylında uyğun olaraq sətir sayı, söz sayı və simvol sayını müəyyən etmək üçün hansı əmr kombinasiyasını daxil etmək lazımdır?

**Cavab: wc əmrindən istifadə olunmalıdır.**

**wc task (sətir,söz və simvaol sayını göstərir)**

**wc -l task (yalnız sətirlərin sayını göstərir)**

**wc -c task (yalnız simvolların sayını göstərir)**

**wc -w task (yalnız sözlərin sayını göstərir)**

1. **mv** əmrini *“köçür”* ifadəsi ilə əvəz etmək üçün uyğun kod kombinasiyasını yazın.

**Cavab: alias köçür=’mv’**

**Qeyd: unalias köçür komandasını yazaraq əvvəlki vəziyyətinə qaytara bilərik.**

1. **task** faylının adını dəyişmək və gizli rejimə gətirmək üçün uyğun kod kombinasiyasını yazın.

**Cavab:**

**mv /root/Desktop/task /root/Desktop/.yeni-task**

**4. Aşağıdakı tapşırıqları yerinə yetirmək üçün Linux əmrlərini yazın:**

1. Desktopa keçid edin və **BOOK** adlı yeni bir **gizli qovluq** yaradın. **BOOK** qovluğunun daxilində **“book1.txt”, “book2.txt”** və **“book3.txt”** (gizli fayl)adlı üç yeni fayl yaradın və aşağıdakı mətni **book1.txt** adlı faylın daxilinə qeyd edin:

*Azərbaycan Texniki Universiteti*

*İTT fakültəsi*

*Kibertəhlükəsizlik ixtisası*

**Cavab:**

**cd Desktop**

**mkdir .BOOK**

**touch book1.txt book2.txt book3.txt**

**echo “Azərbaycan Texniki Universiteti” >> book1.txt**

**echo “İTT fakültəsi” >> book1.txt**

**echo “Kibertəhlükəsizlik ixtisası” >> book1.txt**

1. **book1.txt** faylının məzmununun ilk 2 sətrinə baxın və daha sonra sətir və simvol sayını ekrana çıxarmaq üçün olan kod kombinasiyasını yazın.

**Cavab:**

**head -n 2 book1.txt**

**wc -l -c book1.txt**

1. **clear** əmrini *“sil”* ifadəsi ilə əvəz edin və terminalı təmizləyin.

**Cavab:**

**alias sil=’clear’**

**sil**

**4**  **.book3.txt** faylının icazələri aşağıda qeyd edilmişdir. İcazələri izah edin və faylın **owner (u)** icazələrini dəyişdirərək **write (w)** icazəsini silin və **execute (x)** icazəsini əlavə edin.

***-rw-r--r-- 1 root root 0 Apr 19 03:45 .book3.txt***

**Cavab:**

***Hazırki vəziyyəti:-rw-r--r-- =644***

**chmod 544 book3.txt**

**5.BOOK** qovluğunu gizli rejimdən çıxarın və zip formatında sıxlaşdırın.

**Cavab:**

**mv ~/Desktop/.BOOK ~/Desktop/BOOK**

**zip book.zip BOOK**

**5. Aşağıdakı tapşırıqları yerinə yetirmək üçün Linux əmrlərini yazın:**

1. Desktopa keçid alın və **“b1” , “bcd” , “bbb” , “b6” , “b11” , “t8”** adlı 6 sayda boş yeni fayl yaradın və yeni bir qovluq yaradaraq bu faylları onun daxilinə kopyalayın.

**Cavab:**

**cd Desktop**

**touch b1 bcd bbb b6 b11 t8**

**mkdir Aztu**

**cp b1 bcd bbb b6 b11 t8 Aztu**

1. Yeni qovluğa keçid edin və **rm b?** əmr kombinasiyasının nəticəsini qeyd edin.

**Cavab:**

**cd Aztu**

**rm b?**

**nəticə: b1 və b6 faylı silindi.Çünki rm b? əmri 2 simvoldan ibarət b ilə başlayan faylları silir.**

1. **rm \*1** əmr kombinasiyasının nəticəsini qeyd edin. Qovluqda hansı fayllar qaldı?

**Cavab:**

**rm \*1**

**nəticə:b11 faylı silindi.Çünki rm \*1 əmri sonu 1 ilə bitən bütün faylları silir.**

**Qovluqda bcd,bbb və t8 faylları qaldı.**

1. Qovluqda qalan **b** simvolu ilə başlayan bütün faylları tək bir əmr kombinasiyası ilə silin. Hansı fayl(lar) qaldı?

**Cavab:**

**rm b\***

**qovluqda t8 faylı qaldı.**

1. Mövcud faylın daxilinə aşağıdakı mətni daxil edin:

***Cybersecurity***

***Offensive Security***

***Defensive Security***

***Kali Linux***

***Red Team***

**Cavab:**

**echo “Cybersecurity” >> t8**

**echo “Offensive Security” >> t8**

**echo “Defensive Security” >> t8**

**echo “Kali Linux” >> t8**

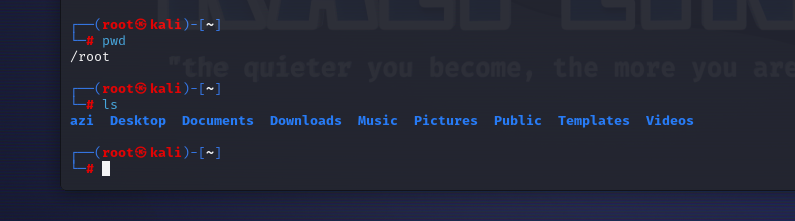
**echo “Red Team” >> t8**

1. Faylın məzmunun son 3 sətrini oxuyun.

**Cavab:**

**tail -n 3 t8**

**6. Aşağıdakı tapşırıqları yerinə yetirmək üçün Linux əmrlərini yazın:**



1. **Music** qovluğunda **“v1”, “vyz” , “vvv”, “v8”, “v22”, “z7”** adlı 6 sayda boş yeni fayl yaradın və **TASK** adlı yeni bir qovluq yaradaraq bu faylları onun daxilinə köçürün. Yeni qovluğa keçid edin.

**Cavab:**

**cd Music**

**touch v1 vyz vvv v8 v22 z7**

**mkdir TASK**

**cp v1 vyz vvv v8 v22 z7 TASK**

**cd TASK**

1. **pwd** əmri ilə vasitəsilə olduğunuz tam ünvanı yoxlayıb qeyd edin.

**Cavab:**

**pwd**

**/home/kali/Music/TASK**

1. **rm v?** əmr kombinasiyasının nəticəsini qeyd edin.

**Cavab:**

**rm v?**

**Nəticə: v1 və v8 faylı silindi.Çünki rm v? əmri adı v ilə başlayan 2 simvoldan ibarət olan faylları silir.**

1. **rm \*2** əmr kombinasiyasının nəticəsini qeyd edin. Qovluqda hansı fayllar qaldı?

**Cavab:**

**rm \*2**

**Nəticə:v22 faylı silindi.Çünki rm \*2 əmri adının sonu 2 ilə bitən bütün faylları silir.**

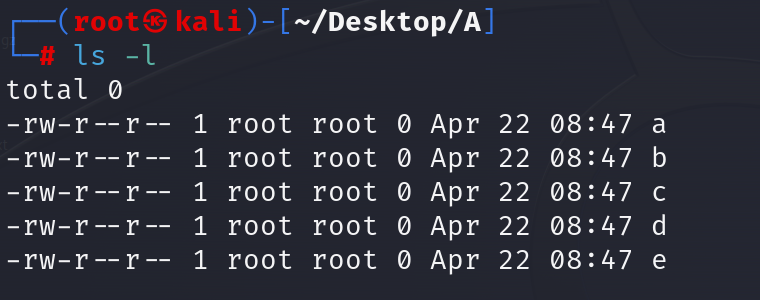
**Qovluqda vyz,vvv və z7 faylları qaldı.**

1. Qovluqda qalan **v** simvolu ilə başlayan bütün faylları tək bir əmr kombinasiyası ilə silin.

**Cavab:**

**rm v\***

**7. Şəkildə A qovluğu daxilindəki 5 faylın (a, b, c, d,e ) icazələri verilmişdir.**



**Aşağıdakı tapşırıqların nəticəsini izahlı şəkildə təsvir edin:**

1. chmod 777 a

**Cavab:**

**Nəticə olaraq a faylında faylın sahibinə,qrup üzvlərinə və digərlərinə yazmaq,oxumaq və icra etmək icazələri veriləcək.**

1. chmod 704 b

**Cavab:**

**Nəticə olaraq b faylında faylın sahibinə yazmaq,oxumaq və icra etmək icazəsi veriləcək,qrup üzvlərinə fayla girişə icazə yoxdur,digərlərinə oxumaq icazəsi veriləcək.**

1. chmod 612 c

**Cavab:**

**Nəticə olaraq c faylında faylın sahibinə yazmaq və oxumaq icazəsi,qrup üzvlərinə icra etmək icazəsi,digərlərinə isə yazmaq icazəsi veriləcək.**

1. chmod 700 d

**Cavab:**

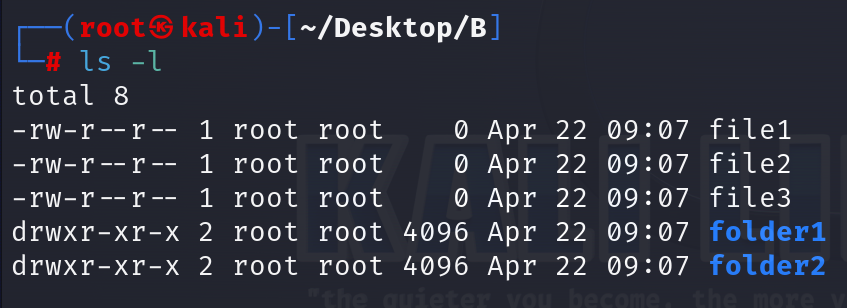
**Nəticə olaraq d faylında faylın sahibinə yazmaq,oxumaq və icra etmək icazəsi veriləcək.Qrup üzvlərinin və digərlərinin fayla girişə icazəsi yoxdur.**

1. chmod 523 e

**Cavab:**

**Nəticə olaraq e faylında faylın sahibinə oxumaq və icra etmək icazəsi,qrup üzvlərinə yazmaq icazəsi,digərlərinə isə yazmaq və icra etmək icazəsi veriləcəkdir.**

**8. Şəkildə B qovluğu daxilindəki 2 qovluq (folder1, folder2) və 3 faylın (file1, file2, file3) icazələri verilmişdir.**



**Aşağıdakı tapşırıqların nəticəsini izahlı şəkildə təsvir edin:**

1. chmod 755 folder1 folder2

**Cavab:**

**Nəticə olaraq folder1 və folder2 qovluğunda qovluqların sahibinə yazmaq,oxumaq və icra etmək icazəsi,qrup üzvlərinə oxumaq və icra etmək icazəsi,həmçinin digərlərinə oxumaq və icra etmək icazəsi veriləcəkdir.**

1. chmod g-r file2

**Cavab:**

**Nəticə olaraq file2 faylında qrup üzvlərinin oxumaq icazəsini siləcək.Son vəziyyətdə faylın sahibi oxuma və yazma icazəsinə sahib olacaq,qrup üzvlərinə fayla girişə icazə verilməyəcək,digərlərinə isə yalnız oxuma icazəsinə malik olacaqlar.**

1. chmod a=wrx file3

**Cavab:**

**Nəticə olaraq file3 faylında faylın sahibinə,qrup üzvlərinə və digərlərinə yazma,oxuma və icra etmə icazəsi veriləcək.**

1. chmod g-rx folder2

**Cavab:**

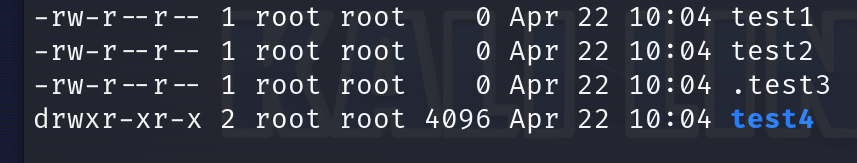
**Nəticə olaraq folder2 qovluğunda qrup üzvlərinin oxuma və icra etmə icazələri silinəcək.Son vəziyyətdə qovluğun sahibinə oxuma,yazma və icra etmə icazəsi,qrup üzvlərinin fayla girişə icazəsi yoxdur,digərləri isə oxuma və icra etmə icazəsinə malik olacaqlar.**

1. chmod o+w folder1

**Cavab:**

**Nəticə olaraq folder1 qovluğunda digərləri üçün yazmaq icazəsi əlavə edir.Son vəziyyətdə qovluğun sahibi yazma,oxuma və icra etmə icazəsinə,qrup üzvləri oxuma və icra etmə,digərləri isə yazma,oxuma və icra etmə icazəsinə malikdirlər.**

**9. Şəkildə C qovluğu daxilindəki 3 fayl və 1 qovluq üçün fayl icazələri təsvir edilmişdir. Şəkilə əsasən aşağıdakı tapşırıqları yerinə yetirin:**



1. **.test3** faylının icazələrini **- rwx-w- - wx** şəklində dəyişdirin.

**Cavab:**

**chmod 723 .test3**

1. **test4** qovluğunun icazələrini **drw-r-xr- -** şəklində dəyişdirin.

**Cavab:**

**chmod 645 test4**

1. **test1 faylının** qrup icazələrini dəyişdirərək **read (r)** icazəsini silin və digər icazələri əlavə edin.

**Cavab:**

**chmod g-r,g+wx test1**

1. **chmod 310 test2** əmrinin nəticəsini təsvir edin.

**Cavab:**

**--wx--x---**

1. **.test3** və **test2** fayllarının **sahib (u)** icazələrini bərabərləşdirin.

**Cavab:**

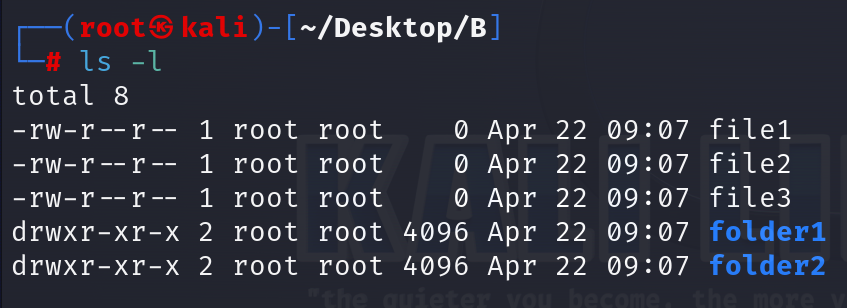
**chmod u=rw .test3 test2**

**6.C** qovluğunu zip formatında sıxlaşdırın.

**Cavab:**

**zip C-zipfayli.zip C**

**10. Şəkildə B qovluğu daxilindəki 2 qovluq (folder1, folder2) və 3 faylın (file1, file2, file3) icazələri verilmişdir.**



**Aşağıdakı tapşırıqların nəticəsini addım-addım təsvir edin:**

1. chmod 764 file1 file2

**Cavab:**

**File1 və file2 nəticəsi : -rwxrw-r—**

**Yəni faylın sahibinin yazma,oxuma və icra etmə,qrup üzvlərinin yazmaq və oxumaq,digərlərinin isə yalnız oxumaq icazəsi var.**

1. chmod 540 file3

**Cavab:**

**File3 nəticəsi -r-xr-----**

**Yəni bu faylda faylın sahibinin oxumaq və icra etmək,qrup üzvlərinin oxumaq icazəsi var.Digərləri fayla giriş edə bilməz.**

1. chmod a=wr folder1 folder2

**Cavab:**

**Folder1 və folder 2 nəticəsi : drw-rw-rw-**

**Yəni bu qovluqlar üçün sahibin,qrup üzvlərin və digərlərinin yazma və oxuma icazəsi var.**

1. chmod g-w folder2

**Cavab:**

**Folder2 nəticəsi: drw-r--rw-**

**(Burada icazələr 3-cü nəticədən sonraki halı götürülüb.)**

**Yəni bu qovluğun sahibin yazma və oxuma,qrup üzvlərinin oxumaq,digərlərinin isə yazma və oxuma icazələri var.**

1. ls –l > new.txt

**Cavab:**

**-rw-r--r—icazələri olan new.txt adlı fayl yaradır.Yəni sahibin oxuma və yazma,qrup üzvlərinin oxuma və yazma,digərlərinin isə yalnız oxuma icazəsi olan fayl yaradır.**

**11. Aşağıdakı tapşırıqları yerinə yetirin:**

1. Desktopa keçid edərək **crunch** aləti vasitəsilə 8 simvol uzunluğunda kiçik hərflərdən ibarət olan parol siyahısı yaradın və **task1.txt** adlı fayl daxilində saxlayın.

**Cavab:**

**cd Desktop**

**crunch 8 8 abcdefghijklmnopqrstuvwxyz -o task1.txt**

1. Uzunluğu minimum 5, maksimum isə 10 simvol olan rəqəmlərdən ibarət parol siyahısı yaradın və **task2.txt** adlı fayl daxilində saxlayın.

**Cavab:**

**Crunch 5 10 1234567890 -o task2.txt**

1. 10 simvol uzunluğunda random hərflərdən ibarət olan parol siyahısı yaradın və **task3.txt** adlı fayl daxilində saxlayın.

**Cavab:**

**Crunch 10 10 abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ -o task3.txt**

1. 10 simvoldan ibarət ***“aztu”*** ifadəsi ilə başlayan və davamı rəqəmlərdən ibarət spesifik parol siyahıları yaradın və **task4.txt** adlı fayl daxilində saxlayın.

**Cavab:**

**crunch 10 10 0123456789 -t aztu%%%% -o task4.txt**

1. Uzunluğu 5 simvoldan ibarət kiçik **“a”** hərfi ilə başlayan, ikinci simvolu böyük hərf olan, üçüncü simvolu rəqəm olan, dördüncüsü simvol olan, beşincisi isə kiçik hərf olan spesifik bir parol siyahısı yaradın və **task5.txt** adlı fayl daxilində saxlayın.

**Cavab:**

**crunch 5 5 -t a,%^@ -o task5.txt**

**@ → kicik hərflər**

**% → rəqəmlər**

**^ → simvollar (!"#$%&'()\*+,-./:;<=>?@[]^\_`{|}~)**

**, → boyuk hərflər**

1. **crunch 8 8 –t @t^c^%%y –o test.txt** əmr kombinasiyasının nəticəsini sözlərlə ifadə edin və bir neçə nümunə göstərin

**Cavab:**

**Bu əmrdə crunch aləti test.txt faylında uzunluğu 8 simvoldan ibarət olan sözlər toplusu(wordlist) yaradacaq.Burada ki sözlərin simvollarının necə olacağına baxaq:**

**1-ci simvol (@) = kicik hərif (A-Z)**

**2-ci simvol (t) = t hərfi**

**3-cü simvol (^) = simvollar (!”;%:?\*()/\*-+ və s.)**

**4-cü simvol (c) = c hərfi**

**5-ci simvol (^) = simvollar (!”;%:?\*()/\*-+ və s.)**

**6-cı simvol (%) = rəqəm (0123456789)**

**7-ci simvol (%) = rəqəm (0123456789)**

**8-ci simvol (y) = y hərfi**

**Nümunələr:**

**at!c@12y**

**bt$c#56y**

**zt#c^03y**

**kt@c!99y**

**12. Aşağıdakı tapşırıqları yerinə yetirin:**

1. Desktopa keçid edərək **crunch** aləti vasitəsilə 10 simvol uzunluğunda rəqəm və hərflərdən ibarət olan parol siyahısı yaradın və **kiber1.txt** adlı fayl daxilində saxlayın.

**Cavab:**

**cd Desktop**

**crunch 10 10 abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 -o kiber1.txt**

1. Uzunluğu minimum 6, maksimum isə 12 simvol olan sadəcə rəqəmlərdən ibarət parol siyahısı yaradın və **kiber2.txt** adlı fayl daxilində saxlayın.

**Cavab:**

**Crunch 6 12 0123456789 -o kiber2.txt**

1. 12 simvol uzunluğunda random hərflərdən ibarət olan parol siyahısı yaradın və **kiber3.txt** adlı fayl daxilində saxlayın.

**Cavab:**

**crunch 12 12 abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ -t -o kiber3.txt**

1. 9 simvoldan ibarət ***“kiber”*** ifadəsi ilə başlayan və davamı müxtəlif simvollardan ibarət spesifik parol siyahıları yaradın və **kiber4.txt** adlı fayl daxilində saxlayın.

**Cavab:**

**Crunch 9 9 -t kiber^^^^ -o kiber4.txt**

1. Uzunluğu 5 simvoldan böyük **“N”** hərfi ilə başlayan, ikinci simvolu kiçik hərf olan, üçüncü simvolu rəqəm olan, dördüncü və beşincisi isə simvollardan ibarət olan spesifik bir parol siyahısı yaradın və **kiber5.txt** adlı fayl daxilində saxlayın.

**Cavab:**

**crunch 5 5 -t N@%^^ -o kiber5.txt**

**13. Aşağıdakı tapşırıqları yerinə yetirin:**

1. 10 simvoldan ibarət ***“kiber”*** ifadəsi ilə başlayan və davamı müxtəlif *simvollardan* ibarət spesifik parol siyahıları yaradın və **kiber.txt** adlı fayl daxilində saxlayın.

**Cavab:**

**Crunch 10 10 –t kiber^^^^^ -o kiber.txt**

1. Uzunluğu 5 simvoldan ibarət böyük **“Z”** hərfi ilə başlayan, ikinci simvolu kiçik hərf olan, üçüncü simvolu rəqəm olan, dördüncü və beşincisi isə simvollardan ibarət olan spesifik bir parol siyahısı yaradın və **Z.txt** adlı fayl daxilində saxlayın.

**Cavab:**

**Crunch 5 5 –t Z,%^^ -o Z.txt**

1. **crunch 6 6 –t @51^%% –o test.txt** əmr kombinasiyasının nəticəsini sözlərlə ifadə edin və bir neçə nümunə göstərin.

**Cavab:**

**Bu əmr 6 simvoldan ibarət olan ilk hərfi kicik,2-ci simvolu 5,3-cü simvolu 1,4-cü simvolu hər hansı bir simvoldan,5-ci və 6-cı simvolları isə rəqəmlərdən ibarət olan test.txt spesifik parol siyahısı yaradır.**

1. **“task1.txt”** faylında saxlanılmış parollar siyahısından grep aləti ilə yalnız “abc” ardıcıllığını özündə saxlayan sətirləri süzgəcdən keçirin.

**Cavab:**

**Grep “abc” task1.txt**

1. ***“abc”*** ifadəsinin **sha1** alqoritmi üzrə heşini əldə etmək üçün uyğun kod kombinasiyasını yazın.

**Cavab:**

**Echo –n “abc” |sha1sum**

**14. Aşağıdakı tapşırıqları yerinə yetirin:**

1. ***“cybersecurity”***ifadəsinin md5 alqoritmi üzrə heşini əldə etmək üçün uyğun kod kombinasiyasını yazın və aldığınız heşi **hash.txt** adlı faylın daxilində saxlayın.

**Cavab:**

**echo -n "cybersecurity" | md5sum > hash.txt**

1. Heşin növünü müəyyən etmək üçün uyğun kod kombinasiyasını daxil edin.

***Cavab:***

***Hash-identifier***

**5d41402abc4b2a76b9719d911017c592**

**Bu alət vasitəsilə heşin növü müəyyən olunacaq.**

1. Heşlənmiş bir parolun dictionary hücumu və bruteforce hücumu ilə sındırılması arasındakı fərqi izah edin.

**Cavab:**

**Dictonary hücumunda Hücumçu əvvəldən hazırlanmış, çox vaxt istifadə olunan sözlərdən, ifadələrdən və ya parollardan ibarət olan sözlük (dictionary) faylı istifadə edir.Bu hücum insanların istifadə etdiyi parolları asanlıqla tapır.Həmçinin,çox sürətlidir.Brute-force hücumu isə hücumçu parol siyahısı yaradır və ya hazır parol siyahısından istifadə edərək parolları sınayır.Buna görədə brute-force hücumu çox vaxt alır və parolun qırılmasına tam zəmanət vermir.Lakin brute-force hücumu bütün parolları sındırmaq üçün istifadə olunur,dictonary hücumu isə nisbətən asan parolları sındırmaq üçün istifadə olunur.**

1. **John The Ripper** alətini yüklənilməsi kodunu yazın və bu alətin mahiyyətini izah edin.

***Cavab:***

***sudo apt install john***

***John The Ripper parolların sındırılması üçün nəzərdə tutulmuş kali linux alətidir.Bu alətdə əsasən heş parolların sındırılması nəzərdə tutulmuşdur.John The Ripper aləti dictionary və brute-force hücumlarını həyata keçirir.Güclü və çevik olduğu üçün etik hakerlər və peşəkar kibertəhlükəsizlik mütəxəsisləri tərəfindən istifadə olunur.***

1. **hash.txt** adlı faylda saxlanılan heşi sındırmaq məqsədi ilə John The Ripper alətinin işə salınması prosesini təsvir edin. Parolların sındırılması üçün istifadə edilən daha hansı alətləri tanıyırsınız?

***Cavab:***

***John –format=raw-md5 –wordlist=/usr/share/wordlists/rockyou.txt hash.txt***

***Başqa heşlərin və parolun sındırılması üçün hashcat,hash-buster,hydra və s. kimi alətləri misal göstərmək olar.***

**15. Aşağıdakı tapşırıqları yerinə yetirin:**

1. **“kitab”** ifadəsinin md5 alqoritmi üzrə heşini əldə etmək üçün uyğun kod kombinasiyasını yazın və aldığınız heşi **md5.txt** adlı faylın daxilində saxlayın

**Cavab:**

**Echo –n “kitab” | md5sum > md5.txt**

1. Heşin növünü necə müəyyən edə bilərik?

**Cavab:**

**Hash-identifier aləti vasitəsilə müəyyən edə bilərik.**

**Hash-identifier**

**5d41402abc4b2a76b9719d911017c592**

1. Heşlənmiş bir parolun dictionary hücumu və bruteforce hücumu ilə sındırılması arasındakı fərqi izah edin.

**Cavab:**

**Dictonary hücumunda Hücumçu əvvəldən hazırlanmış, çox vaxt istifadə olunan sözlərdən, ifadələrdən və ya parollardan ibarət olan sözlük (dictionary) faylı istifadə edir.Bu hücum insanların istifadə etdiyi parolları asanlıqla tapır.Həmçinin,çox sürətlidir.Brute-force hücumu isə hücumçu parol siyahısı yaradır və ya hazır parol siyahısından istifadə edərək parolları sınayır.Buna görədə brute-force hücumu çox vaxt alır və parolun qırılmasına tam zəmanət vermir.Lakin brute-force hücumu bütün parolları sındırmaq üçün istifadə olunur,dictonary hücumu isə nisbətən asan parolları sındırmaq üçün istifadə olunur.**

1. **md5.txt** adlı faylda saxlanılan heşi sındırmaq məqsədi ilə John The Ripper alətinin işə salınması prosesini təsvir edin.

**Cavab:**

**John –format=raw-md5 –wordlist=/usr/share/wordlists/rockyou.txt md5.txt**

1. Hash əldə edildikdən sonra, parolun təhlükəsizliyini artırmaq üçün hansı üsullar tətbiq oluna bilər? “Salt” və “Pepper” anlayışlarını izah edin.

***Cavab:***

***Parolun təhlükəsizliyini artırmaq üçün onu heşləmək ilkin prosesdir.Parol heşlənəndən sonra ona salt və pepper əlavə etmək lazımdır.İndi gəln bu anlayışları izah edək:***

***Salt- Parolun əvvəlinə və ya sonuna əlavə onunan məlumat parçasıdır.Burada hər istifadəçi üçün fərqli salt əlavə olunur və buda parolun təhlükəsizliyin nisbətən artırır.Salt parol ilə birlikdə hash olunur və serverdə saxlanılır.***

***Pepper- pepper salta bənzəyir lakin əlavə gizli məlumatdır.Pepper sistemin bir hissəsində gizli saxlanılır və istifadəçi belə bunu əldə edə bilmir.Bu gizli yer proqram kodu,ayrı server və s. ola bilər.Pepper bütün istifadəçilər üçün eyni ola bilər,lakin istifadəçidən gizli saxlanılır.Pepper-ə əlavə təhlükəsizlik qatı deyə bilərik.***

### 

### 16. Sual: Təsəvvür edin ki, universitetin server sistemində çalışan bir istifadəçi sistem administratoruna müraciət edir və deyir ki, onun şəxsi sənədləri yoxa çıxıb. Administrator sistemdə aşağıdakı fəaliyyətləri müşahidə edir:

* Sistemə kənar IP-dən gecə saatlarında daxil olunub.
* İstifadəçinin ev qovluğundakı sənədlər ZIP formatında sıxılıb.
* ZIP faylına parol qoyulub və orijinal sənədlər silinib.
* Fayl adının yanında README.txt adlı sənəd yerləşdirilib və orada ödəniş tələb olunur.

#### Tapşırıq:

1. Bu hadisə hansı kibertəhlükə növünə aiddir?

**Cavab:**

**Bu ransomware hücumudur.Burada hücum edən şəxs sənədləri şifrələyib və onların bərpası üçün müəyyən qədər pul tələb edir.**

1. Belə hücumların qarşısını almaq üçün hansı tədbirlər görülə bilər? Ən azı 3 tədbir yazın.

**Cavab:**

**Möhkəm parol siyasəti tətbiq edilməlidir.**

**Antivirus və anti-malware proqramları quraşdırılmalıdır.**

**Mütəmadi olaraq məlumatların ehtiyyat nüsxələri (buckup) çıxarılmalıdır.**

1. Belə hallarda İT təhlükəsizlik komandası ilkin olaraq hansı addımları atmalıdır? Ən azı 3 addım yazın.

**Cavab:**

**Zərəverici prosesi və ya sistemə girişi bloklamalıdır.**

**Hadisəni həll etmək üçün log fayllarını araşdırmalıdır.**

**Əlaqədar sistemləri şəbəkədən ayırmalıdır.**

1. Bu tip hücumların baş verməsində istifadəçi səhvləri rol oynaya bilərmi? Əgər bəli, misal verin.

**Cavab:**

**Bəli istifadəçi səhvləri rol oynaya bilər.Məsələn,fişinq e-poçtuna zərərli linkə klikləyə bilər.**

**Kompüterdə zəif təkrarlanan parollardan istifadə edə bilər.**

**Naməlum mənbədən proqram yükləyib quraşdıra bilər.**

**17. Aşağıdakı tapşırıqları yerinə yetirin:**

1. ***“Azərbaycan”*** ifadəsinin **md5** alqoritmi üzrə heşini əldə etmək üçün uyğun kod kombinasiyasını yazın və aldığınız heşi **hash.txt** adlı faylın daxilinə yazın.

***Cavab:***

**Echo -n “Azərbaycan” | md5sum >hash.txt**

1. Aldığımız heşin növünü necə müəyyən edə bilərik? Hash əldə edildikdən sonra, parolun təhlükəsizliyini artırmaq üçün hansı üsullar tətbiq oluna bilər? “Salt” və “Pepper” anlayışlarını izah edin.

**Cavab:**

**Aldığımız heşin növünü hash-identifier aləti vasitəsilə müəyyən etmək olar.Aşağıdakı addımları terminalda yerinə yetirməliyik.**

**Hash-identifier**

**4a13f3b5c5d92b87b0ed8637d0bf2e41**

**Burada heş kodu daxil edirik və o bizə növünü göstərir.**

***Parolun təhlükəsizliyini artırmaq üçün onu heşləmək ilkin prosesdir.Parol heşlənəndən sonra ona salt və pepper əlavə etmək lazımdır.İndi gəln bu anlayışları izah edək:***

***Salt- Parolun əvvəlinə və ya sonuna əlavə onunan məlumat parçasıdır.Burada hər istifadəçi üçün fərqli salt əlavə olunur və buda parolun təhlükəsizliyin nisbətən artırır.Salt parol ilə birlikdə hash olunur və serverdə saxlanılır.***

***Pepper- pepper salta bənzəyir lakin əlavə gizli məlumatdır.Pepper sistemin bir hissəsində gizli saxlanılır və istifadəçi belə bunu əldə edə bilmir.Bu gizli yer proqram kodu,ayrı server və s. ola bilər.Pepper bütün istifadəçilər üçün eyni ola bilər,lakin istifadəçidən gizli saxlanılır.Pepper-ə əlavə təhlükəsizlik qatı deyə bilərik.***

1. Hashcatalətinin yüklənilməsi üçün uyğun kod kombinasiyasını yazın.

**Cavab:**

**sudo apt install hashcat**

1. Hashcat alətinin mahiyyətini və 5 hücum rejimini qeyd edin.

**Cavab:**

**Hashcat aləti heş kodları qırmaq üçün nəzərdə tutulmuş kali linux alətidir.Bu alət vasitəsilə 5 hücum rejimində hücum həyata keçirmək mümkündür.**

**1.Dictonary attack**

**2.Combination attack**

**3.Brute-force attack**

**4.hybrid wordlist +mask**

**5.Hybrid mask+wordlist**

**6.Association**

**Hascat alətində brute-force hücumu nümunə:**

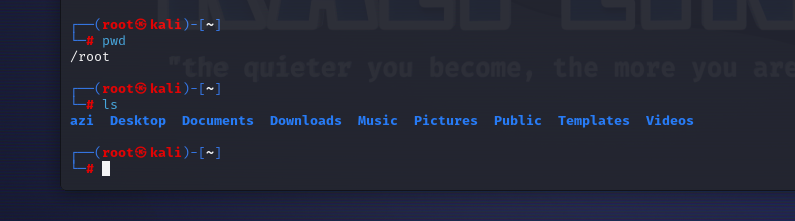
**Hashcat -m 0 -a 3 hash.txt wordlist.txt**

**5.**Hashcat alətini işə salın.

**Terminala hashcat yazmaqla bu aləti işə salmaq mümkündür.**

**Nümunə: Hashcat -m 0 -a 3 hash.txt wordlist.txt**

**Burada heş kod hash.txt adlı faylda yerləşdirilib.wordlist.txt faylı isə mümkün kombinasiyaları yoxlamaq üçün yaradılmış parol siyahısıdır.**

**18. Hashcat alətindən istifadə edərək heş-parolların sındırılması məsələsini yerinə yetirin:**

1. **Desktop** qovluğuna keçin və **Hashcat** alətinin sistemə yüklənməsi üçün uyğun **əmr kombinasiyasını** yazın.

**Cavab:**

**sudo apt install hashcat**

1. **“informasiya”** sözünün həm **SHA1**, həm də **MD5** alqoritmləri üzrə heşini hesablamaq üçün uyğun əmrləri yazın.

**Cavab:**

**Echo -n “informasiya” | md5sum**

**Echo -n “informasiya” | sha1sum**

1. **sha1.txt** və **md5.txt** adlı **iki boş fayl yaradın** və uyğun olaraq SHA1 və MD5 heşlərini bu fayllarda saxlayın.

**Cavab:**

**Echo -n “informasiya” | md5sum > md5.txt**

**Echo -n “informasiya” | sha1sum** **> sha1.txt**

1. **Hashcat** alətinin mahiyyətinin qısa şəkildə izah edin və onun **5 hücum rejimini** sadalayın.

**Cavab:**

**Hashcat aləti heş kodları qırmaq üçün nəzərdə tutulmuş kali linux alətidir.Bu alət vasitəsilə 5 hücum rejimində hücum həyata keçirmək mümkündür.**

**1.Dictonary attack**

**2.Combination attack**

**3.Brute-force attack**

**4.hybrid wordlist +mask**

**5.Hybrid mask+wordlist**

**6.Association**

**Hascat alətində brute-force hücumu nümunə:**

**Hashcat -m 0 -a 3 hash.txt wordlist.txt**

1. Əldə etdiyiniz **SHA1** və **MD5** heşlərini **Hashcat** vasitəsilə qırmaq üçün uyğun kod kombinasiyalarını yazın.

**Cavab:**

**hashcat -m 100 -a 3 sha1.txt wordlist.txt**

**hashcat -m 0 -a 3 md5.txt wordlist.txt**

**19. Steghide aləti istifadə edərək Kali Linux mühitində məlumatın steqanoqrafik şəkildə gizlədilməsi tapşırığını yerinə yetirin:**

1. Steqanoqrafiya nədir? Qısa şəkildə izah edin.

**Cavab:**

**Steqanoqrafiya — bir məlumatı gizli şəkildə başqa bir faylın (məsələn, şəkil, audio, video və s.) içərisində gizlətmək sənətidir. Məqsəd gizli məlumatın mövcudluğunu tamamilə gizlətmək və onu adi istifadəçidən görünməz etməkdir.**

1. **Steghide** alətinin Kali Linux mühitində yüklənilməsi üçün uyğun əmri yazın.

**Cavab:**

**sudo apt install steghide**

1. **gizli.txt** adlı bir fayl yaradın və daxilinə istənilən bir mətn daxil edin.

**Cavab:**

**touch gizli.txt**

**echo “Bu Gizli Metndir” >> gizli.txt**

1. Hazırladığınız **gizli.txt** faylını **gizli.jpg** adlı şəkil faylının daxilində **Steghide** aləti vasitəsilə gizlətmək üçün uyğun əmri yazın. Məlumat uğurla gizlədildikdən sonra **gizli.txt** faylını silin.

**Cavab:**

**Steghide embed -cf gizli.jpg -ef gizli.txt**

**rm gizli.txt**

1. Daha sonra həmin **gizli.jpg** faylından gizli məlumatı çıxararaq onu **yeni.txt** adlı faylda saxlayın.

**Cavab:**

**Steghide extract -sf gizli.jpg**

**mv gizli.txt yeni.txt**

1. **Steghide --info gizli.jpg** əmr kobninasiyası vasitəsilə hansı məlumatları əldə etmək mümkündür?

**Cavab:**

**Bu əmr vasitəsilə gizli.jpg adlı içərisində əgər nəsə gizlədibsə onun adını göstərir.Lakin qeyd olunmalıdır ki,steghide aləti məlumatı gizlədərkən ona şifr təyin edir.Bu şifri biliriksə,gizlənmiş faylı tapa bilərik.Əlavə olaraq burada şifrələmə metodunu,gizlənmiş faylın ölçüsünü və faylın öz ölçüsünü görmək mümkündür.**

**20. Steghide aləti istifadə edərək Kali Linux mühitində məlumatın steqanoqrafik şəkildə gizlədilməsi tapşırığını yerinə yetirin:**

1. Steqanoqrafiya nədir? Qısa şəkildə izah edin.

**Cavab:**

**Steqanoqrafiya — bir məlumatı gizli şəkildə başqa bir faylın (məsələn, şəkil, audio, video və s.) içərisində gizlətmək sənətidir. Məqsəd gizli məlumatın mövcudluğunu tamamilə gizlətmək və onu adi istifadəçidən görünməz etməkdir.**

1. **Steghide** alətinin Kali Linux mühitində yüklənilməsi üçün uyğun əmri yazın.

**Cavab:**

**sudo apt install steghide**

1. **aztu.txt** adlı bir fayl yaradın və daxilinə *“Bu gizli informasiyadır!”* mətnini qeyd edin.

**touch aztu.txt**

**echo “Bu gizli informasiyadır!” >> aztu.txt**

1. Hazırladığınız **aztu.txt** faylını **aztu.jpg** adlı şəkil faylının daxilində **Steghide** aləti vasitəsilə gizlətmək üçün uyğun əmri yazın. Məlumat uğurla gizlədildikdən sonra **aztu.txt** faylını silin.

**Cavab:**

**steghide embed -cf aztu.jpg -ef aztu.txt**

**rm aztu.txt**

1. Daha sonra həmin **aztu.jpg** faylından gizli məlumatı çıxararaq onu **gizli.txt** adlı faylda saxlayın.

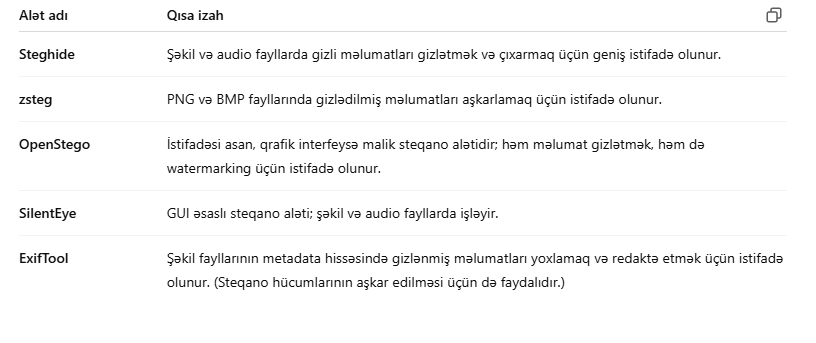
**Cavab:**

**steghide extract -sf aztu.jpg**

**mv aztu.txt gizli.txt**

1. Steqanoqrafiya sahəsində başqa hansı alətləri tanıyırsınız?

**Cavab:**

****

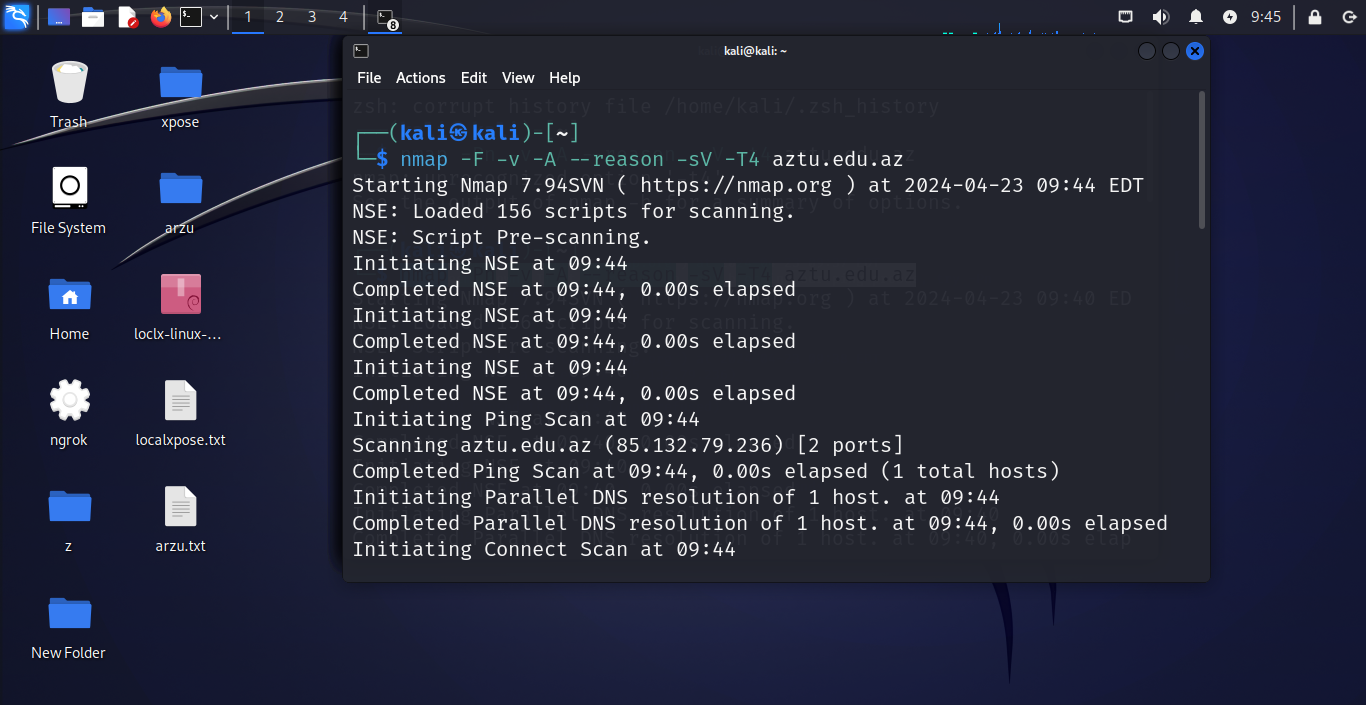
**21. Aşağıdakı sosial mühəndislik hücumları üzrə uyğunluğu müəyyən edin:**

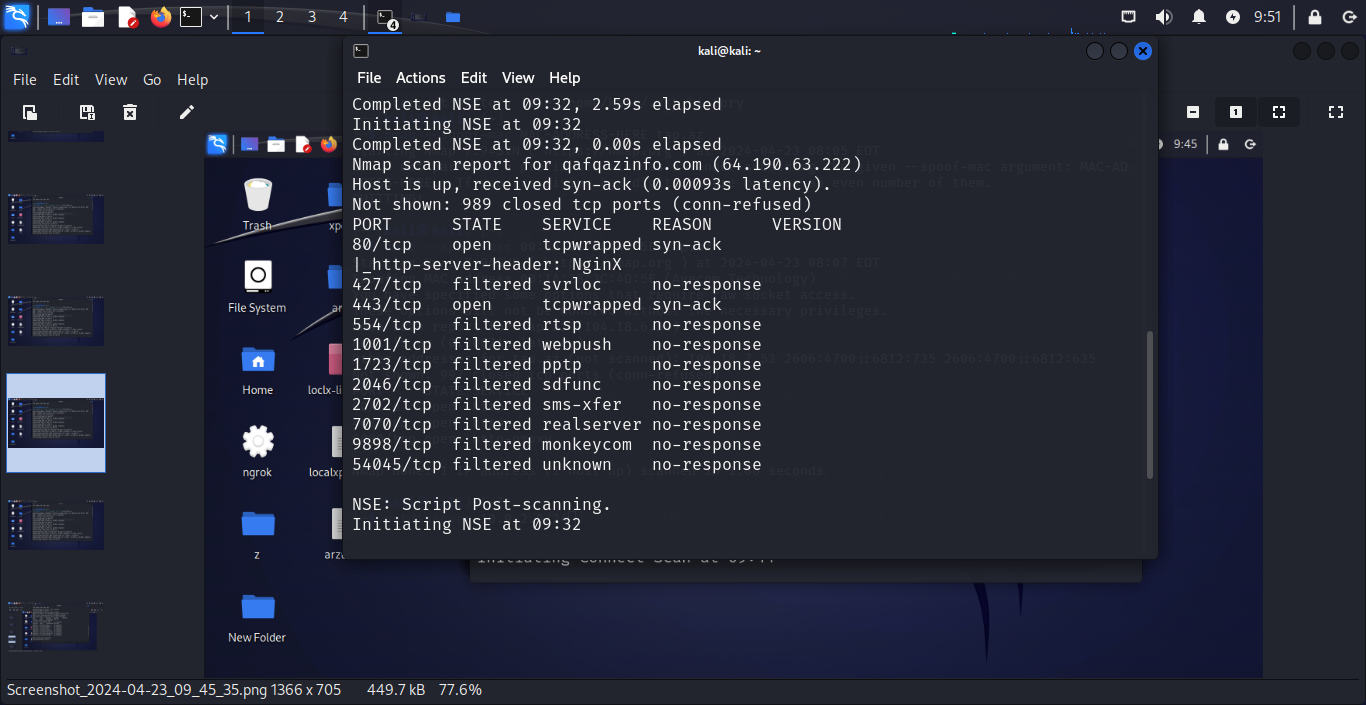
1. Bu tip hücumlarda bədniyyətli şirkət işçilərindən birinin giriş kartını əldə edərək binaya daxil olmağa çalışır.
2. Bədniyyətli özünü önəmli biri kimi təqdim edərək hədəf şəxslə ünsiyyət qurur. Bu əlaqə vasitəsilə hədəfin şəxsi məlumatlarının ələ keçirilməsi planlaşdırılır. Bu hücumlar, əsasən sosial media kanalları vasitəsilə həyata keçirilir.
3. Bədniyyətli texniki dəstək işçisi adı altında istifadəçi ilə əlaqə saxlayır. İstifadəçinin yaşadığı problemləri bəhanə edərək, istifadəçidən əlaqədar cihaz üçün giriş icazəsi tələb edir. İcazə əldə edildikdən sonra zərərli proqramı istifadəçi cihazına yerləşdirir.
4. Bədniyyətlilər hədəfləri tərəfindən geniş olaraq istifadə edilən veb saytları ələ keçirərək bu saytlara zərərli proqramlarını yerləşdirərək sayta giriş edən istifadəçiləri hədəf alırlar.
5. Bədniyyətlilər hədəf istifadəçi qruplarının maraqlarını və zəifliklərini istifadə edərək hücum təşkil edirlər. Misal üçün; içərisində zərərli proqram olan USB kartlar ictimai yerlərdə buraxılır və istifadəçinin USB kartını öz cihazına daxil edib içərisindəki zərərli faylı işə salması gözlənilir.
6. Bədniyyətli tanınmış şirkət adı altında saxta kimlik yaradır və bu İD-nin vasitəsilə hədəflə əlaqəyə keçir. Müəyyən bir müddətdən sonra şəxsi məlumatları, maliyyə bilgiləri, şifrələri və s. ələ keçirməyə çalışır.
7. Baiting Attack -- 5
8. Watering Hole -- 4
9. Honey Trap --2
10. Quid Quo Pro --3
11. Pretexting -- 6
12. Tailgating -- 1

**22. Aşağıdakı sosial mühəndislik hücumları üzrə uyğunluğu müəyyən edin:**

1. Bu tip hücumlarda bədniyyətli şirkət işçilərindən birinin giriş kartını əldə edərək binaya daxil olmağa çalışır.
2. Bədniyyətli texniki dəstək işçisi adı altında istifadəçi ilə əlaqə saxlayır. İstifadəçinin yaşadığı problemləri bəhanə edərək, istifadəçidən əlaqədar cihaz üçün giriş icazəsi tələb edir. İcazə əldə edildikdən sonra zərərli proqramı istifadəçi cihazına yerləşdirir.
3. Bədniyyətlilər hədəfləri tərəfindən geniş olaraq istifadə edilən veb saytları ələ keçirərək bu saytlara zərərli proqramlarını yerləşdirərək sayta giriş edən istifadəçiləri hədəf alırlar.
4. Bədniyyətlilər şirkətin/şəxsin ətrafındakı zibil qutularını qarışdıraraq vacib informasiyaları əldə etməyə çalışırlar.
5. Bədniyyətlilər karqo/nəqliyyat şirkətlərinin sistemlərinə daxil olur və müvafiq çatdırılmaların marşrutunu dəyişirlər. Beləliklə, göstərdikləri ünvanlara yönəldilmiş əşyaları ələ keçirirlər.
6. Bədniyyətlilər hədəf istifadəçi qruplarının maraqlarını və zəifliklərini istifadə edərək hücum təşkil edirlər. Misal üçün; içərisində zərərli proqram olan USB kartlar ictimai yerlərdə buraxılır və istifadəçinin USB kartını öz cihazına daxil edib içərisindəki zərərli faylı işə salması gözlənilir.
7. Dumster Diving -- 4
8. Divertion Theft -- 5
9. Quid Quo Pro -- 2
10. Watering hole -- 3
11. Baiting Attack -- 6
12. Tailgating -- 1

**23. aztu.edu.az saytının skan edilməsi üçün göstərilən bütün parametrləri və nmap alətindən əldə edilən nəticələri ətraflı şəkildə təsvir edin:**

****

****

1. İstifadə edilən **–F** parametri nəyi müəyyən edir?

**Cavab:**

**-F(Fast Scan) parametri sürətli skanlamaq üçün istifadə olunur.**

1. **–v** parametri nəyə xidmət edir?

**Cavab:**

**- v(verbose) parametri Nmap-in daha ətraflı məlumat verməsi üçün istifadə olunur.Yəni skan zamanı hansı mərhələdə olduğunu nə etdiyini göstərir.**

1. **–A** parametri nəyə xidmət edir?

**Cavab:**

**-A parametri vasitəsilə əməliyyat sistemlərini,versiya aşkarlanması,skriptlərin aşkarlanmasını,tracerouteni aşkalaya bilərik.**

1. **–reason** parametri nəyi göstərir?

**Cavab:**

**--reason parametri protların açıq və ya bağlı olduğunu aşkarlayan zaman nəyə görə aşkarladığını göstərir.Bir növ bayraqları göstərir.**

1. **–sV** parametri nəyə xidmət olur?

**Cavab:**

**-sV parametri açq portlarda çalışan xidmətlərin versiyasını müəyyən etməyə çalışır.**

1. **–T4** parametri nəyi göstərir?

**Cavab:**

**-T4 parametri bu skanlama sürətini müəyyən edir.Skanlama sürəti T0-T5 arasında ola bilər.T4 ən sürətli olmasada effektiv skanlama sürətidir.**

1. Verilənlərə əsasən, **aztu.edu.az** veb saytında açıq port(lar) hansı(lar)dır?

Əldə edilən digər nəticələri təsvir edin.

**Cavab:**

**Verilənlərə əsasən aztu.edu.az saytında 80 və 443 portları açıqdır.Http NGNİX serverindən istifadə edir.HTTPS isə müəyyən deyil.**

1. Nmap aləti ilə başqa hansı darama metodlarını tanıyırsınız?

**Cavab:**

**SYN Scan(-sS)-Stealth Scan ən çox istifadə olunan.**

**TCP Scan(-sT)-Sadə TCP bağlantısı ilə daranır.**

**UDP Scan(-sU)-UDP portlarını yoxlayır**

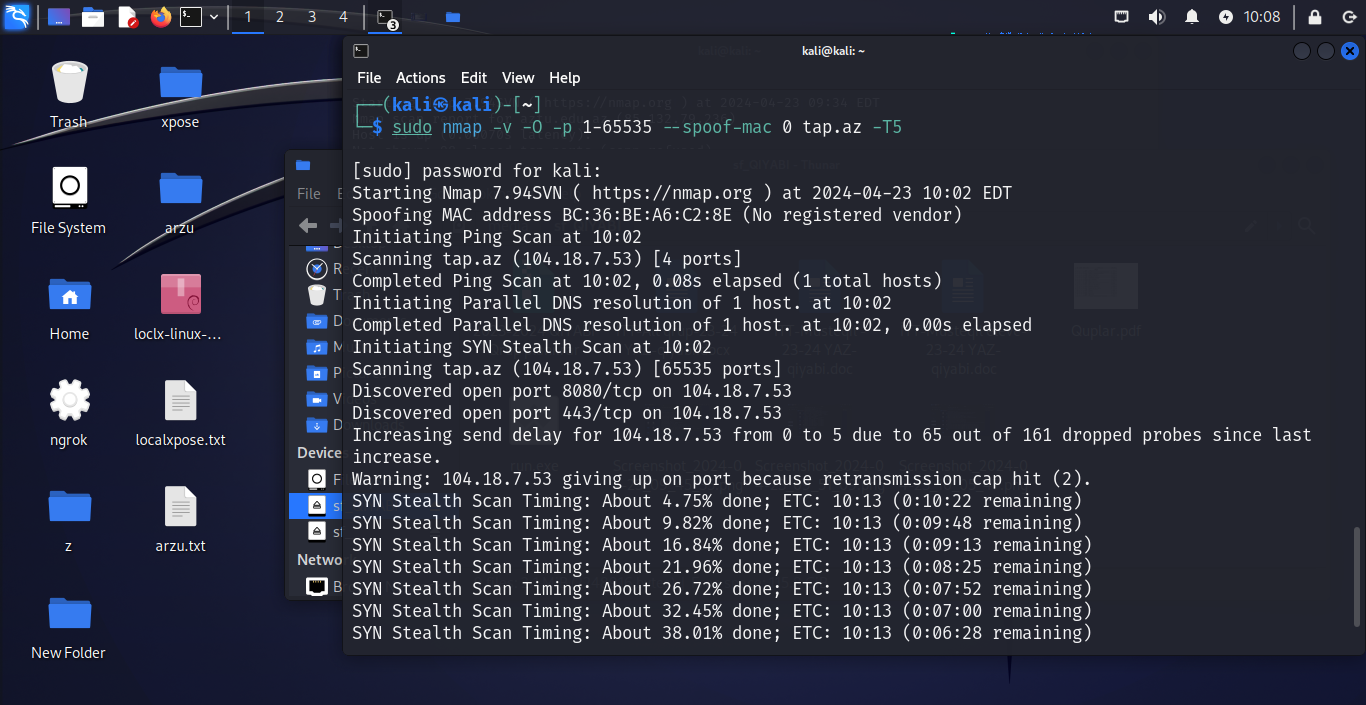
**Ping Scan(-sn)-hostun aktiv olub-olmadığını yoxlayır**

**Null Scan(-sN)-TCP bayraqları olmadan cavab göndərir**

**FİN Scan(-sF)-TCP FİN bayraqları ilə cavab göndərir**

**XMAS Scan(-sX) – TCP bayraqları ilə cavab göndərir.**

**24. Tap.az saytının skan edilməsi üçün göstərilən bütün parametrləri və nmap alətindən əldə edilən nəticələri ətraflı şəkildə təsvir edin:**



1. İstifadə edilən **–v** parametri nəyə xidmət edir?

**Cavab:**

**-v(verbose) parametri Nmap-in daha ətraflı məlumat verməsi üçün istifadə olunur.Yəni skan zamanı hansı mərhələdə olduğunu nə etdiyini göstərir.**

1. **–O** parametri nəyi göstərir?

**Cavab:**

**-O (Operation System Detection) skanlama zamanı hədəf sistemin əməliyyat sistemini müəyyən edir.**

1. **–p** parametri nəyi göstərir? Hansı port kateqoriyaları və nömrələri var?

**-p parametri portları təyin etmək üçündür.buradaki şəkildə 65535 portun hamısını yoxlayıb.Məsələn, -p 80 yazsaydı http portunu göstərəcəkdi.**

**80 – HTTP açıqdır**

**443 – HTTPS açıqdır**

1. **--spoof-mac** parametrinin tətbiq edilməsi nə üçün önəmlidir?

**Cavab:**

**--spoof-mac MAC ünvanını yəni fiziki ünvanı dəyişmək üçün istifadə olunur.Bu gizli axtarış üçn lazımdır.**

1. **–T5** parametri nəyə xidmət edir?

**Cavab:**

**-T5 parametri ən aqressiv skanlama rejimidir.-T5 maksimum sürətlə skanlamanı həyata keçirir.**

1. Verilənlərə əsasən, **tap.az** veb saytında açıq port(lar) hansı(lar)dır? Əldə edilən digər nəticələri təsvir edin.

**Cavab:**

**Tap.az saytında 8080 və 443 portları açıqdır.Yəni HTTP və HTTPS.**

**Hədəf İP ünvanı: 104.18.7.53**

**Skan nəticəsində bəzi portlardan cavab alınmayıb.SYN Stealth Scan metodu istifadə olunub.**

1. Nmap aləti ilə başqa hansı darama metodlarını tanıyırsınız?

**Cavab:**

**SYN Scan(-sS)-Stealth Scan ən çox istifadə olunan.**

**TCP Scan(-sT)-Sadə TCP bağlantısı ilə daranır.**

**UDP Scan(-sU)-UDP portlarını yoxlayır**

**Ping Scan(-sn)-hostun aktiv olub-olmadığını yoxlayır**

**Null Scan(-sN)-TCP bayraqları olmadan cavab göndərir**

**FİN Scan(-sF)-TCP FİN bayraqları ilə cavab göndərir**

**XMAS Scan(-sX) – TCP bayraqları ilə cavab göndərir.**

**25. Aşağıdakı sorğuların nəticəsini təsvir edin:**

|  |
| --- |
| 1**. site**:aztu.edu.az **filetype**:pdf  **link:**aztu.edu.az  **Cavab:**  **Bu sorğuda aztu.edu.az saytından yalnız pdf tipli fayllar tapılacaq.Link:aztu.edu.az aztu saytına link verən səhifələri göstərmək üçün nəzərdə tutulub.** |
| 2. **site:**"wikipedia.org" **intext:**"yaşıl kitab"  [**site**:az **inurl**:admin](https://www.exploit-db.com/ghdb/8422) **intitle**:"kibertəhlükəsizlik"  **Cavab:**  **1-ci axtarışda wikipedia.org saytında məzmununda yaşıl kitab olan səhifələri göstərəcək.**  **2-ci axtarışda isə .az domenində olan saytlardan URL-də admin olan səhifələrdə kibertəhlükəsizlik başlığı olan hissələri göstərəcək.** |
| 3. **inurl**:"php.id?" **site**:tr  **filetype**:txt "username" "password" **site**:example.com  **Cavab:**  **1-ci axtarışda .tr domenində olan saytlardan URL-də php.id? olan səhifələri göstərəcək.**  **2-ci axtarışda example.com saytında txt fayllarını axtaracaqdır.Həmin faylın içərisində username və password sözləri olmalıdır.** |
| 4. **allintitle**:"tələbə" **site**:.edu  **allintext:**cyber threats  **Cavab:**  **1-ci sorğuda .edu domenli saytların başlıqlarında "tələbə" sözü olan səhifələr tapılacaq.**  **2-ci sorğuda cyber threats sözü bu ardıcıllıqda axtaracaq və tapılan səhifələrdə bu söz varsa onu göstərəcək.** |
| 1. **Başqa hansı axtarış operatorlarını tanıyırsınız?**   **Cavab:**  **Cache- google-un saxladığı saytın versiyasını göstərir**   * **-sözün çıxarılması(istisna)**   **“” – dəqiq ifadə axtarışı**  **OR – sözlərdən birini və ya digərini tapır.**  **\* vahid yer tutucu** |

**26. Uyğun Google təkmilləşdirilmiş axtarış operatorlarını yazın:**

1. example.com veb saytı üzərində yalnız *.ppt* fayllarını axtarın.

**Cavab:**

**Site:example.com filetype:ppt**

1. example.com veb saytında yalnız *“cyber”* ifadəsini təşkil edən səhifələri axtarın.

**Cavab:**

**Site:example.com “cyber”**

1. example.com saytında mətn daxilində *"login"* **və ya** *"signin"* ifadələrini axtarın.

**Cavab:**

**Site:example.com (“login” OR “signin”)**

1. example.com saytında yalnız *.doc* və *.docx* fayllarını axtarın.

**Cavab:**

**Site:example.com (filetype:doc OR filetype:docx)**

1. example.com saytında başlığı *"404 Not Found"* olan səhifələri axtarın.

**Cavab:**

**Site:example.com intitle:”404 Not Found”**

**27. Uyğun Google təkmilləşdirilmiş axtarış operatorlarını yazın:**

1. aztu.edu.az veb saytı üzərində “*security”* ifadəsini təşkil edən səhifələri axtarın.

**Cavab:**

**site:aztu.edu.az "security"**

1. yalnız .edu domainlərindəki səhifələrin başlıqlarında *"təqaüd"* sözünü axtarın.

**Cavab:**

**site:.edu intitle:”təqaüd”**

1. aztu.edu.az saytında yalnız .xls və .xlsx fayllarını axtarın.

**Cavab:**

**site:aztu.edu.az filetype:xls OR filetype:xlsx**

1. test.com saytında başlığı *"Welcome"* olan səhifələri axtarın.

**Cavab:**

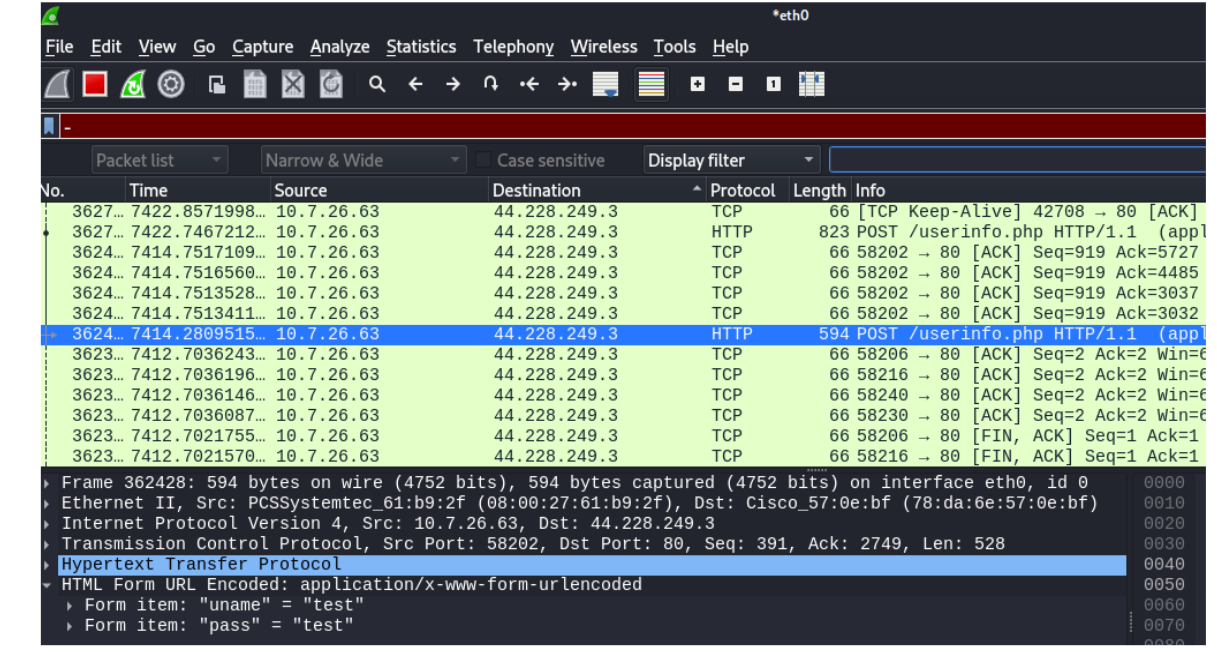
**site:test.com intitle:"Welcome"**

1. Test.com saytında URL-də *"news"* ifadəsini təşkil edən səhifələri axtarın.

**Cavab:**

**site:test.com inurl:news**

**28. Şəkildə Wireshark aləti vasitəsilə şəbəkə trafikinin analizinin nəticəsi göstərilmişdir. Aşağıdakı tapşırıqları təsvir edin:**

****

1. Mənbə İP ünvanını göstərin. **Cavab: 10.7.26.63**
2. Təyinat İP ünvanını göstərin. **Cavab: 44.228.249.3**
3. Yalnız HTTP sorğu və cavablarını necə axtarmaq olar?

**Cavab:**

**Yuxarı hissədə axtarış yerinə aşağıdakılar yazılmalıdır:**

**http – bütün http-ləri göstərir**

**http.request və ya http.flags.response == 0 -yalnız http sorğularını göstərəcək**

**http.flags.response == 1 -yalnız http cavablarını göstərəcək**

1. Müəyyən bir İP ünvanı üçün HTTP sorğu və cavabları necə axtarıla bilər?

**Cavab:**

**http && ip.addr == 10.7.26.63**

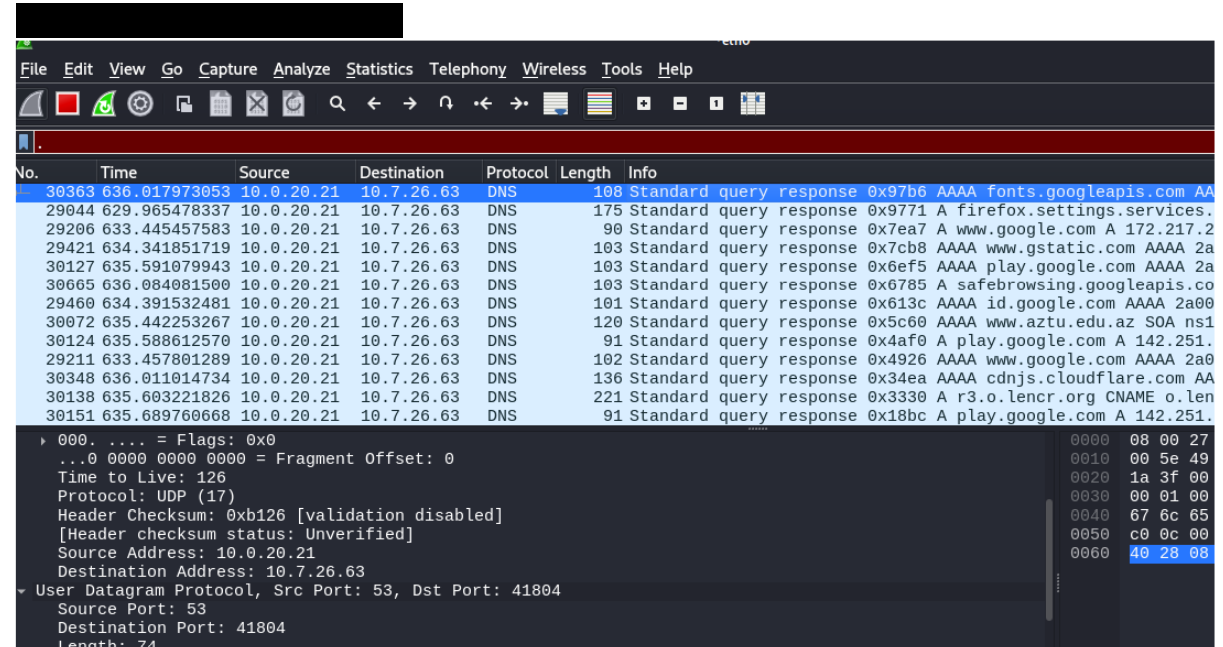
**bu komanda 10.7.26.63 İP ünvanına görə bütün http sorğularını və cavablarını göstərəcək.**

1. Şəkildə HTTP protokolunun təhlükəsiz olmadığını nə sübut edir?

**Cavab:**

**Burada gördüyünüz kimi - Form item: "uname" = "test" – və - Form item: "pass" = "test" – istifadəçi adı və parolu göstərir.Bu isə təhlükəli haldır,çünki bədniyyətli sizin məlumatlarınızı artıq ələ keçirmiş olur.Http protokolu məlumatları şifrləmir ona görədə təhlükəlidir.Əgər Bunun əvəzinə HTTPS protokolu olsaydı o təhlükəsiz olardı.Çünki https məlumatları şifrləyərək göndərir.**

**29. Şəkildə Wireshark aləti vasitəsilə şəbəkə trafikinin analizinin nəticəsi göstərilmişdir. Aşağıdakı tapşırıqları təsvir edin:**

****

1. Mənbə İP ünvanını göstərin.

**Cavab:**

**10.0.20.21**

1. Təyinat İP ünvanını göstərin.

**Cavab:**

**10.7.26.63**

1. Yalnız DNS sorğu və cavabları necə axtarıla bilər?

**Cavab:**

**Yuxarı hissəyə bu komandaları yazmaqla:**

**dns – bütün dns-ləri göstərəcək**

**dns.flags.response == 0 – yalnız dns sorğularını göstərəcək**

**dns.flags.response == 1 -yalnız dns cavablarını göstərəcək**

1. DNS sorğu və cavabı üçün A sorğu tipini görəcəksiniz, bu sorğu tipi nə deməkdir?

**Cavab:**

**A tipi dns sorğusu İPv4 ünvanı üçün edilir.yəni host adı İPv4 ünvanına çevrilir.məsələn google.com – 172.217.2.110**

1. DNS sorğu və cavabı üçün sorğu tipinin AAAA olduğunu görəcəksiniz, bu sorğu tipi nə deməkdir?

**Cavab:**

**AAAA tipi dns sorğusu İPv6 üçün edilir.Yəni host adı İPv6 ünvanına çevrilir.**

**Məsələn,google.com-** **2607:f8b0:4006:80d::200a**

**30. Aşağıdakı tapşırığı yerinə yetirin:**

1. Metasploit aləti hansı məqsəd(lər) üçün istifadə edilir?

**Cavab:**

**Metasploit aləti əsasən penetrasiya testləri və təhlükəsizlik zəifliklərinin yoxlanılması məqsədi ilə istifadə olunur.**

**Metasploit alətinin əsas məqsədləri:**

1. **Zəifliklərin istismarı (exploitation):  
   Mövcud zəiflikləri istismar edərək sistemə sızmaq üçün istifadə olunur. Məsələn, köhnə və yamalanmamış sistemlərdəki zəifliklərə qarşı exploit-lər işlədilir.**
2. **Penetrasiya testi (penetration testing):  
   Bir təşkilatın sistemlərindəki təhlükəsizlik boşluqlarını aşkarlamaq üçün istifadə olunur. Bu, etik hakerlik çərçivəsində həyata keçirilir.**
3. **Payload yaratmaq və inject etmək:  
   Sistemə daxil olduqdan sonra orada müxtəlif əmrlər icra etməyə imkan verən payload-lar hazırlanır və göndərilir (məsələn, meterpreter).**
4. **Təhlükəsizlik maarifləndirilməsi və təlim:  
   Təhlükəsizlik mütəxəssislərinin və tələbələrin real senarilərlə işləməsi üçün öyrədici mühit yaradır.**
5. **Post-exploitation əməliyyatları:  
   Sistemə sızıldıqdan sonra əlavə məlumat toplamaq, digər sistemlərə yayılmaq, istifadəçi hüquqlarını artırmaq kimi əməliyyatlar aparılır.**
6. Əsas **msfconsole** komandalarını göstərin.

**Cavab:**

**Help və ya ? - Kömək menyusunu açır**

**History - əvvəlki yazılan əmrləri ekrana çıxarır**

**Sessions – aktiv sessiyaları siyahiya alır**

**Exit – msfconsole-dən çıxır**

**Kill – müəyyən fon proseslərini dayandırır**

**Jobs – aktiv fon işlərini göstərir**

**Back - əvvəlki menyuya qayıdır**

**Show payloads – payloadları göstərir**

**Show exploits – exploitləri göstərir**

**Show auxiliary – Auxiliary modularını göstərir**

**İnfo – seçilmiş modul haqqında ətraflı məlumat verir**

**Use – hər-hansı prosesi işə salır(məsələn,use <modul>-seçilmiş modulu işə salır.**

**Seach -exploit,payload,modul və s. axtarmaq üçün istifadə olunur**

**Set – parametrlərin dəyərini təyin edir**

1. Metasploit aləti vasitəsilə PDF daxilinə troyan yerləşdirilməsi prosesini ətraflı təsvir edin.

**Cavab:**

**Kali linux-da terminalı açırıq və aşağıdakıları addım-addım yerinə yetiririk.**

**Terminala *msfconsole* yazırıq.**

**Sonraki addım: *use exploit/windows/fileformat***

**Burada exploitlər açılacaq.Biz burada *exploit/windows/fileformat/adobe\_pdf\_embedded\_exe* olan exploiti seçməliyik.Onu koplayayıb terminala yazmalıyıq.**

**Buraya keçdikdən sonra,*show options* komandasını yazaraq tələb olunan məlumatları göstərməsini istəyəciyik.**

**Burada 3 əsas tələb olunan məlumat çıxacaq:**

**1.Filename-çıxış faylının adı**

**2.İnfilename-giriş faylının adı**

**3.LPORT – port nömrəsi**

**Vacib məsələ odurki,aşağıda çıxan İP ünvanının doğru olduğunu yoxlamaq lazımdır.Bu funksiyanı digər sahədə terminala *ifconfig* komandası yazaraq həll etmək mümkündür.**

**Daha sonra set vasitəsilə parametrləri təyin etməliyik.**

**1.set LPORT – 2323 (Burada 1000-9999 arası istənilən rəqəm ola bilər)**

**2.set FİLENAME – virus.pdf (yaradılan istismar faylının adı)**

**3.set İNFİLENAME - /home/kali/Desktop/exam.pdf (Burada hansı pdfin içərisinə istismar olunacaqsa,o faylın yolu yazılmalıdır.**

**Son olaraq faylı görmək üçün Metasploit sizə fayl yolu verəcək.Bu fayl yolunu fayl sistemində axtarışa verərək,istismar olan faylı tapmaq olar.**