**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,**

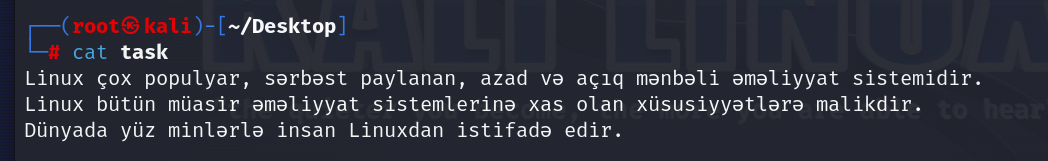
**wc document2.txt**

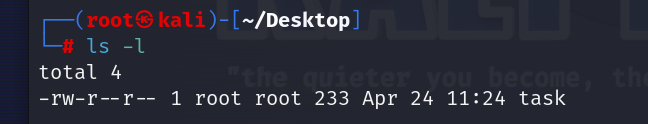
**wc -l document2.txt (yalnız sətirlərin sayını göstərir)**

**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**

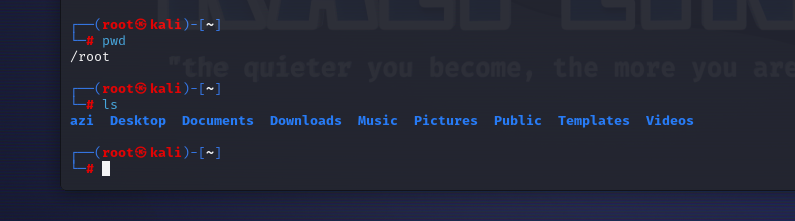
**echo “Red Team” >> t8**

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.**

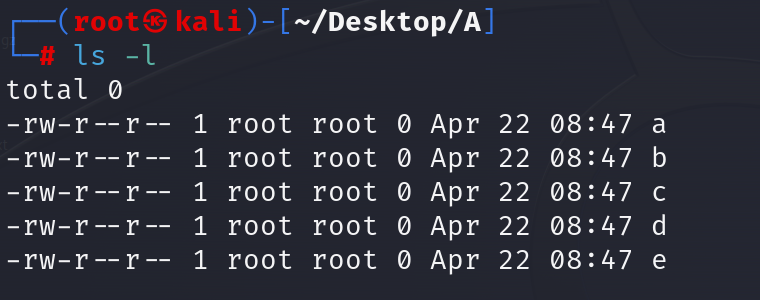
**Qovluqda vyz,vvv və z7 faylları qaldı.**

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:**

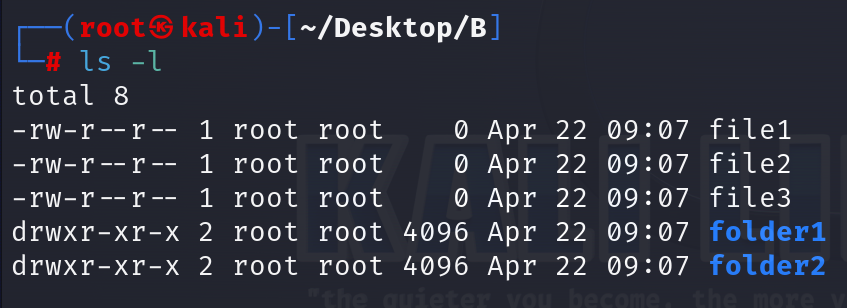
**Nəticə olaraq d faylında faylın sahibinə yazmaq,oxumaq və icra etmək icazəsi veriləcək.Qrup üzvlərinin və digərlərinin fayla girişə icazəsi yoxdur.**

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:**

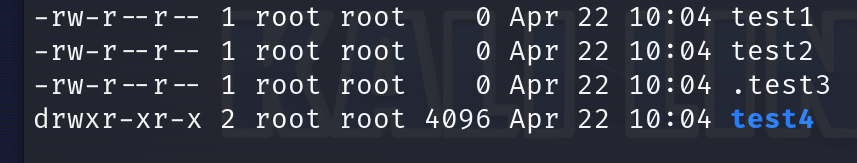
**Nəticə olaraq folder2 qovluğunda qrup üzvlərinin oxuma və icra etmə icazələri silinəcək.Son vəziyyətdə qovluğun sahibinə oxuma,yazma və icra etmə icazəsi,qrup üzvlərinin fayla girişə icazəsi yoxdur,digərləri isə oxuma və icra etmə icazəsinə malik olacaqlar.**

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:**

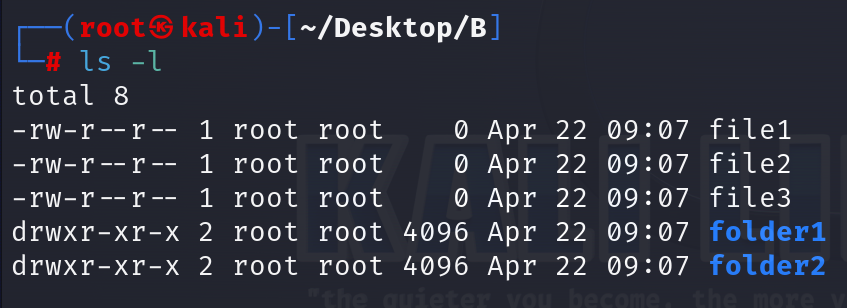
**chmod u=rw .test3 test2**

**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 : -rwx-rw-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,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:**

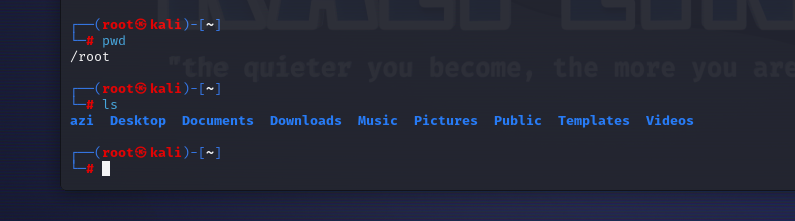
**Hashcat -m 0 -a 3 hash.txt wordlist.txt**

**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.

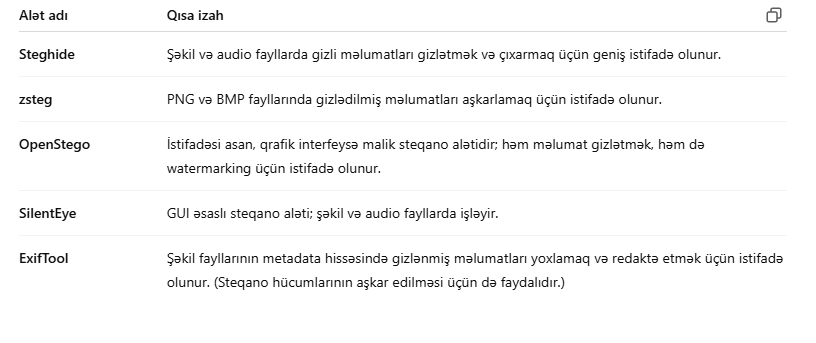
**Cavab:**

**steghide extract -sf aztu.jpg**

**mv aztu.txt gizli.txt**

1. Steqanoqrafiya sahəsində başqa hansı alətləri tanıyırsınız?

**Cavab:**

****

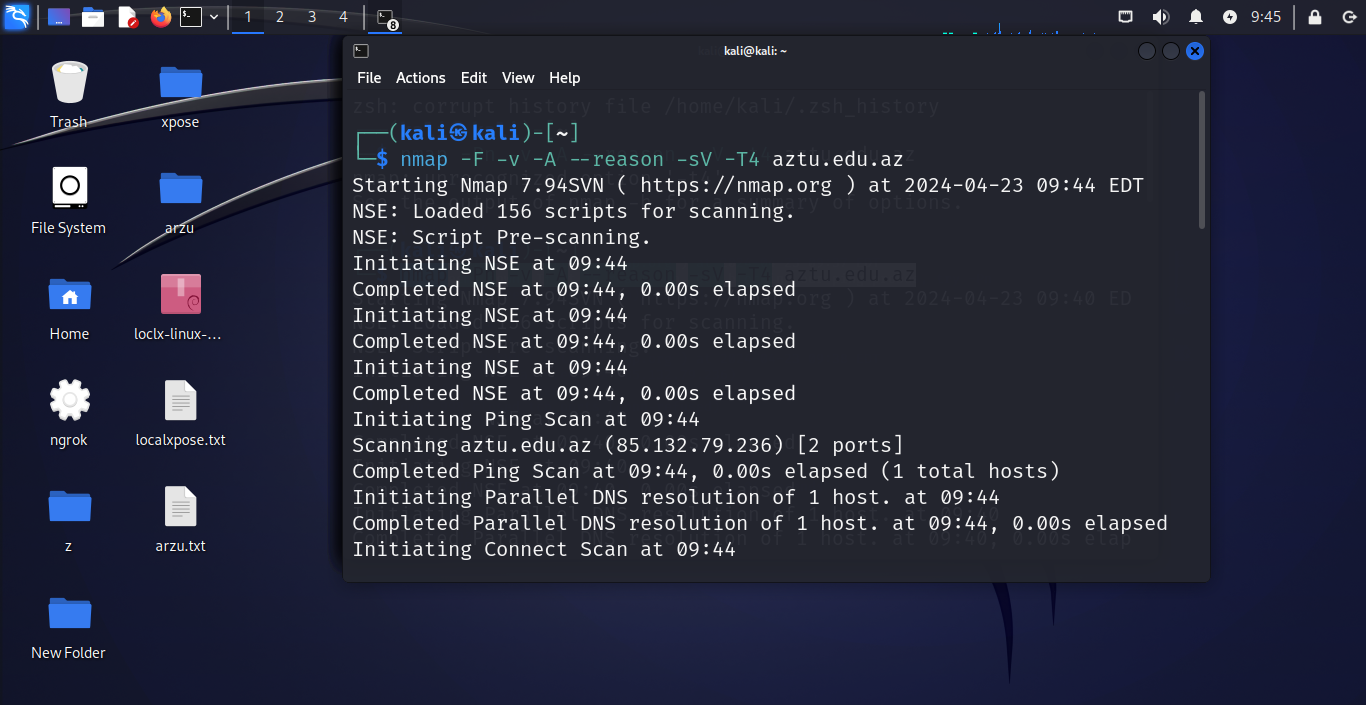
**21. Aşağıdakı sosial mühəndislik hücumları üzrə uyğunluğu müəyyən edin:**

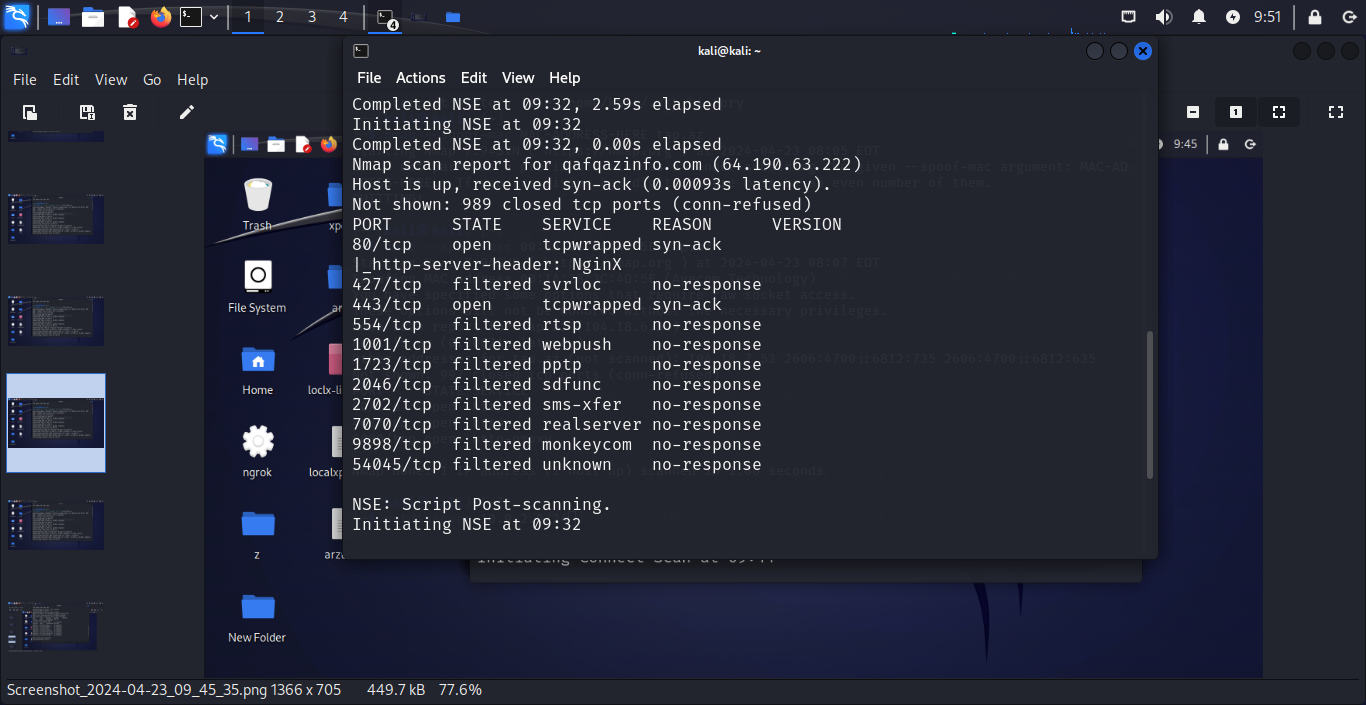
1. Bu tip hücumlarda bədniyyətli şirkət işçilərindən birinin giriş kartını əldə edərək binaya daxil olmağa çalışır.
2. Bədniyyətli özünü önəmli biri kimi təqdim edərək hədəf şəxslə ünsiyyət qurur. Bu əlaqə vasitəsilə hədəfin şəxsi məlumatlarının ələ keçirilməsi planlaşdırılır. Bu hücumlar, əsasən sosial 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**

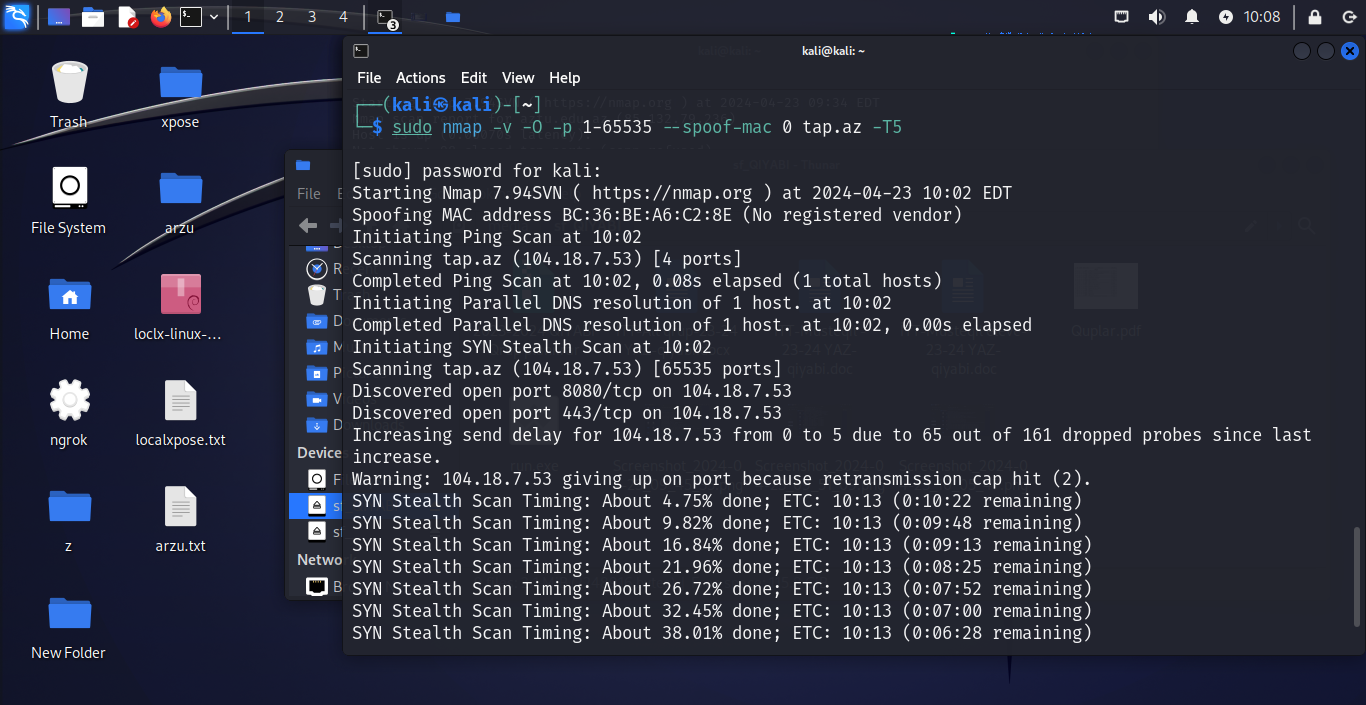
**Ping Scan(-sn)-hostun aktiv olub-olmadığını yoxlayır**

**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:**

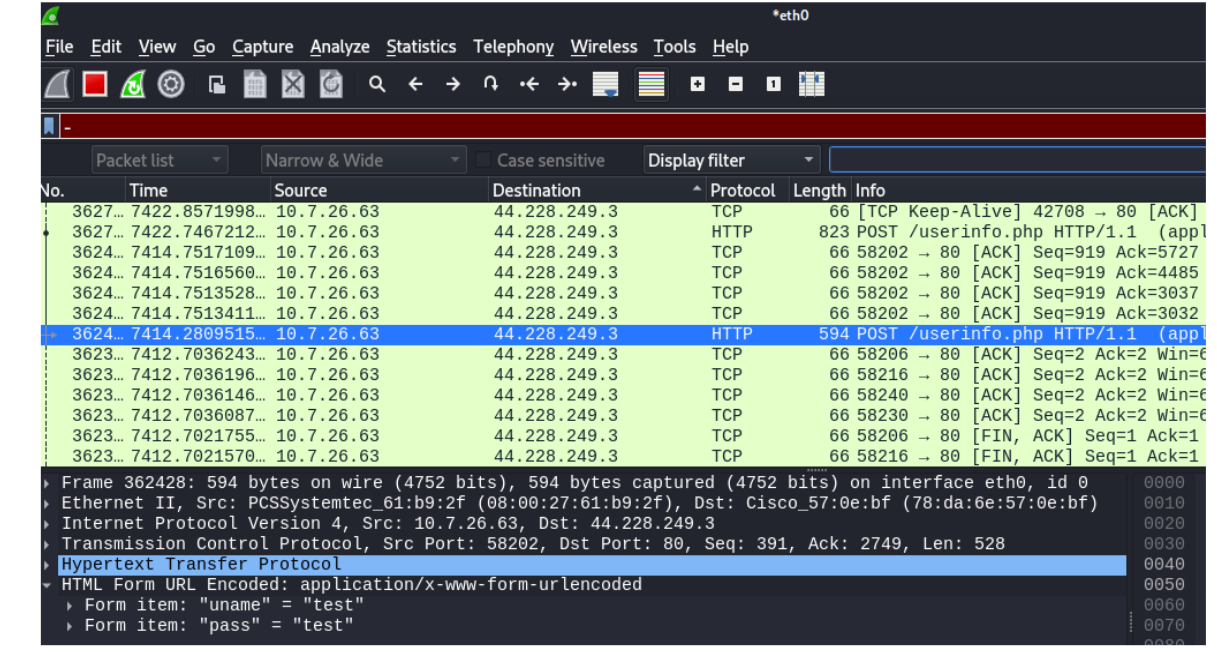
**site:test.com intitle:"Welcome"**

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**

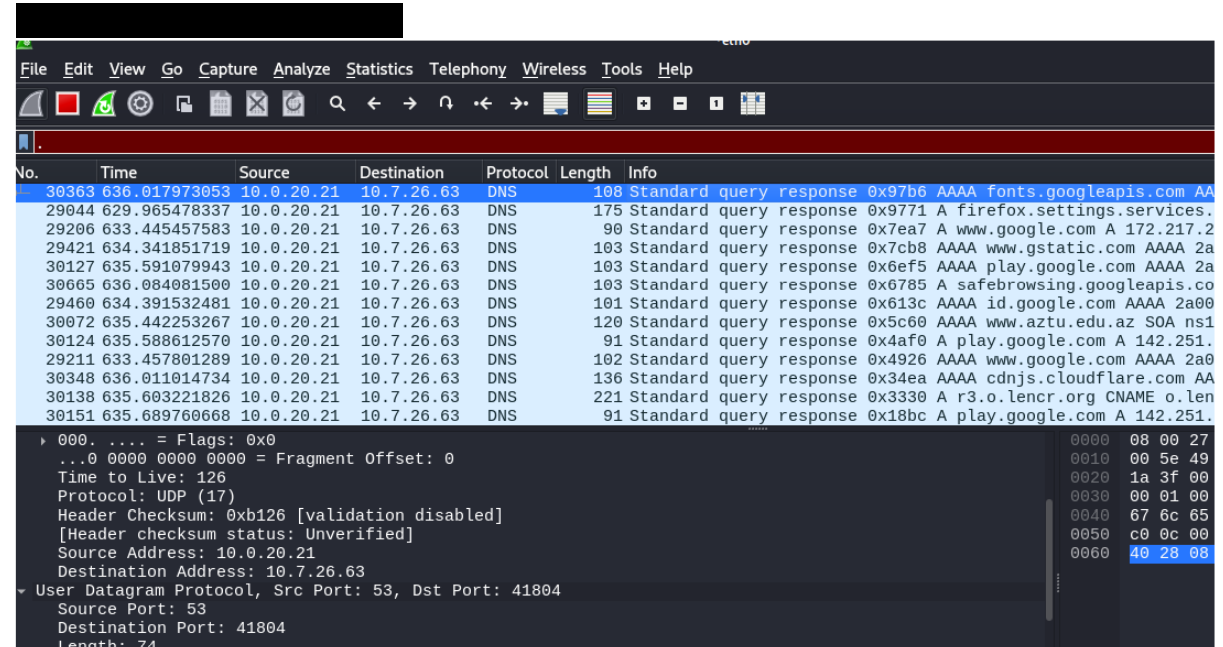
**bu komanda 10.7.26.63 İP ünvanına görə bütün http sorğularını və cavablarını göstərəcək.**

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.**

1. Kibertəhlükəsizlik anlayışı və təmin üsulları

Kibertəhlükəsizlik – sistemlərin və verilənlərin icazəsiz girişlərdən, hücumlardan və zərərli proqramlardan qorunması prosesidir. Əsas məqsədlər:

Məxfilik – yalnız icazəli şəxslər məlumatlara çıxış əldə edə bilər

Bütövlük – məlumatların dəyişdirilmədən saxlanması

Əlçatanlıq – məlumatların lazım olan vaxtda istifadəyə hazır olması

Əsas metodlar:

Şifrləmə (encryption)

Firewall, antivirus və IDS

Giriş nəzarəti, autentifikasiya (2FA)

Sistem yeniləmələri və ehtiyat nüsxələr (backup)

Hüquqi və inzibati tədbirlər (ISO/IEC 27001 və s.)

İstifadəçilərin maarifləndirilməsi

---

2. GNU/Linux və Kali Linux

Linux – açıq mənbəli, sərbəst dəyişdirilə bilən və təhlükəsiz əməliyyat sistemidir.

Kali Linux – sızma testləri, etik hacking üçün hazırlanmış xüsusi Linux distributividir. Burada Nmap, Wireshark, Metasploit kimi yüzlərlə təhlükəsizlik alətləri mövcuddur.

Əsas komandalar:

ls, cd, pwd, mkdir, rm – fayl sistemi üçün

sudo – inzibati icra

ping, netstat, nmap – şəbəkə diaqnostikası

top, htop – sistemin resurs istifadəsi

nano, vim, cat, less – fayl məzmununa baxış

chmod, chown, adduser – hüquq və istifadəçi idarəsi

---

3. Fayl icazələri və chmod

Linux sistemlərində fayl və qovluqlara read (r), write (w), execute (x) icazələri təyin olunur.

Bu icazələr 3 istifadəçi qrupu üçün verilir: owner (u), group (g), others (o).

Məsələn: rwxr-xr--

Sahib: oxu, yaz, icra

Qrup: oxu, icra

Digərləri: yalnız oxu

chmod komandası ilə bu icazələr dəyişdirilir:

Ədədi üsul: chmod 755 fayl.txt

Simvolik üsul: chmod u+x fayl.sh (sahibə icra icazəsi əlavə edir)

Əlavə komandalar:

ls -l – icazələri göstərir

chown – sahibi dəyişir

chgrp – qrupu dəyişir

---

4. Sızma testləri və metodologiyası

Sızma testi – sistemin zəifliklərini aşkarlamaq və istismar imkanlarını yoxlamaq üçün aparılan hücum simulyasiyasıdır.

Mərhələlər:

1. Məlumat toplama (Reconnaissance)

2. Skanlama və zəiflik analizi

3. İstismar (Exploitation)

4. Post-Exploitation – sistemdə səlahiyyət artırmaq, məlumatlara çıxış

5. Hesabatlandırma – zəifliklər və istismar yolları sənədləşdirilir

Standartlar:

OSSTMM – təhlükəsizlik test metodologiyası

OWASP Testing Guide – veb tətbiqlər üçün

NIST SP 800-115 – dövlət səviyyəsində

PTES – penetrasiya testləri üçün icra standartı

---

5. Kəşfiyyat və məlumat toplama

Sızma testinin ilk mərhələsi. Məqsəd – sistem haqqında maksimum məlumat toplamaqdır.

İki üsul var:

Passiv – hədəfə toxunulmadan (WHOIS, sosial media, Google dorking, Shodan)

Aktiv – hədəflə birbaşa əlaqə (port skanları, DNS analiz)

Əsas alətlər:

WHOIS, NSLookup, dig – domen, DNS məlumatları

Nmap, WhatWeb, Wappalyzer – texnologiya və port aşkarlama

Recon-ng, Maltego – geniş OSINT toplama vasitələri

**6. Şəbəkənin daranması və metodologiyası**

**Şəbəkə daranması – hədəf şəbəkədəki aktiv cihazlar, açıq portlar və işləyən xidmətlərin müəyyən edilməsidir. Bu proses hücumun planlanması üçün vacibdir.**

**Əsas növləri:**

**Port skanlaması – TCP/UDP portların yoxlanması**

**Host aşkarlanması – şəbəkədəki aktiv cihazlar**

**Xidmət skanlaması və versiya aşkarlanması**

**Əməliyyat sistemi təyini**

**Əsas alətlər:**

**Nmap – -sS, -sU, -O, -sV**

**Masscan – çox sürətli port skanlama**

**Netdiscover, ARP-scan – yerli şəbəkədə cihaz aşkarlama**

**Zenmap – Nmap-in qrafik interfeysi**

**Darama zamanı ehtiyatlı olmaq vacibdir, çünki firewall və IDS-lər testçini bloklaya bilər.**

**---**

**7. Şəbəkənin inventarlaşdırılması və üsulları**

**Şəbəkənin inventarlaşdırılması – mövcud cihazların, proqramların və xidmətlərin siyahıya alınması və izlənməsidir.**

**Əsas məqsədlər:**

**Aktiv avadanlıqları, IP-ləri və sistem versiyalarını bilmək**

**Təhlükəli, köhnəlmiş və icazəsiz qurğuları aşkar etmək**

**Resurs idarəsini və təhlükəsizlik nəzarətini gücləndirmək**

**İnventarlaşdırma üsulları:**

**Əl ilə və avtomatlaşdırılmış (əksər hallarda avtomatik)**

**Aktiv (sorgu və skanlamalar) və passiv (trafik müşahidəsi)**

**Protokollar və vasitələr:**

**SNMP – cihazlardan məlumat almaq üçün**

**Nmap, Spiceworks, Lansweeper, PRTG, Open-AudIT**

**FTP (port 21), SMTP (port 25), SNMP (port 161) kimi protokolların aşkarlanması**

**---**

**8. Boşluqların idarə olunması və məlumat mənbələri**

**Boşluqların idarə olunması – zəifliklərin aşkarlanması, qiymətləndirilməsi, aradan qaldırılması və izlənməsi prosesidir.**

**Həyat dövrü mərhələləri:**

**1. Aşkarlama – skanerlərlə (Nessus, OpenVAS və s.)**

**2. Qiymətləndirmə – təhlükə səviyyəsinin təyini (CVSS ilə)**

**3. Tədbir görmə – yeniləmələr, konfiqurasiya dəyişiklikləri**

**4. İzləmə – boşluqların davamlı təqibi və təkrar yoxlama**

**Əsas məlumat mənbələri:**

**NVD (National Vulnerability Database)**

**CVE (Common Vulnerabilities and Exposures)**

**Təhlükəsizlik forumları, bloglar, şirkət tövsiyələri**

**Bug bounty platformaları və etik haker hesabatları**

**---**

**9. CVE və CVSS sistemləri**

**CVE – tanınmış zəifliklər üçün unikal identifikatorlar (məs. CVE-2024-12345). Bu baza NVD tərəfindən idarə olunur və qlobal şəkildə qəbul edilir.**

**CVSS – zəifliklərin təhlükə dərəcəsini ölçən sistemdir.**

**Skor 0.0-dan 10.0-a qədərdir, 10 ən təhlükəlidir.**

**CVSS 3 əsas komponentə bölünür:**

**Base score – texniki təsir və istismar çətinliyi**

**Temporal score – zamanla dəyişən risklər**

**Environmental score – təşkilatın mühitinə görə risk səviyyəsi**

**Bu sistemlər təhlükəsizlik komandalarına zəifliklərin prioritetləşdirilməsində yardım edir.**

**---**

**10. Sistemin hakinqi və parolların sındırılması**

**Sistemin hakinqi – sistemə daxil olmaq və ya nəzarət əldə etmək üçün mərhələli hücum planıdır. Mərhələlər:**

**1. Məlumat toplama**

**2. Zəiflik analizi**

**3. İstismar (exploitation)**

**4. Sistemə daxil olma və qalmaq**

**5. İzinləri genişləndirmək**

**6. İzləri gizlətmək**

**Parolların sındırılması üsulları:**

**Dictionary attack – əvvəlcədən təyin edilmiş söz siyahısı ilə**

**Brute force – bütün mümkün kombinasiyaları yoxlamaq**

**Hash analiz – hash-ləri əldə edib deşifrə etmə cəhdi**

**Sosial mühəndislik – insanları aldadaraq parolu almaq**

**Müdafiə üsulları: güclü parol siyasəti, 2FA, şifrləmə, tez-tez parol dəyişdirmə.**

**11. İmtiyazların genişləndirilməsi və rutkitlər**

**İmtiyazların genişləndirilməsi – sistemə ilkin məhdud giriş əldə etmiş hücumçunun daha yüksək (məsələn, administrator/root) səlahiyyətlər əldə etməsidir.**

**İki əsas növ var:**

**Şaquli (Vertical) – adi istifadəçidən root-a keçid**

**Şaquli olmayan (Horizontal) – eyni səviyyədə başqasının hüquqlarını əldə etmək**

**Rutkitlər – sistemdə gizlənərək fəaliyyət göstərən və hücumçunun izlərini gizlədən zərərli proqramlardır. Antiviruslar onları aşkarlaya bilmir. Hücumçu rutkitlə sistemi tam nəzarətə ala bilər.**

**---**

**12. Faylların gizlədilməsi və steqanoqrafiya**

**Faylların gizlədilməsi – ad, atribut, yer dəyişdirməklə faylın görünməz edilməsi prosesidir.**

**Steqanoqrafiya – məlumatı başqa faylın (şəkil, audio, video) içinə gizlətməkdir.**

**Məsələn: bir .jpg faylın içində gizli mətn saxlamaq.**

**Bu texnikalar həm müdafiə, həm də hücum məqsədilə istifadə oluna bilər.**

**Aşkar etmək üçün xüsusi analiz alətləri mövcuddur.**

**---**

**13. XSS (Saytlararası Skript) hücumları**

**XSS hücumları – zərərli JavaScript kodlarının istifadəçinin brauzerində icra olunması ilə həyata keçirilir.**

**Növləri:**

**Stored XSS – kod saytın DB-sində saxlanır**

**Reflected XSS – URL vasitəsilə ötürülür**

**DOM-based XSS – brauzer tərəfində işləyir**

**Əsas məqsəd: sessiyaların oğurlanması, istifadəçinin aldadılması.**

**Qarşısı: giriş məlumatlarını təmizləmək (input validation), məzmun təhlükəsizlik siyasəti (CSP), HTTP-only cookie-lər.**

**---**

**14. Sosial mühəndislik hücumları**

**Bu hücumlar insan psixologiyasından istifadə edərək istifadəçini aldatmaqla məlumat almağa yönəlir.**

**Əsas növləri:**

**Phishing – saxta email/link göndərmə**

**Spear Phishing – konkret şəxsi hədəf alma**

**Vishing – telefonla aldatma**

**Smishing – zərərli SMS göndərmə**

**Pretexting – saxta şəxsiyyətlə məlumat alma**

**Baiting – maraqlı "tələ" qoyma (məs. USB)**

**Tailgating – kiminsə arxasınca fiziki giriş**

**Quid pro quo – bir şey qarşılığında məlumat alma**

**Qarşısı: maarifləndirmə, 2FA, link və mesajlara diqqət.**

**---**

**15. DDoS hücumları və müdafiə üsulları**

**DDoS (Distributed Denial of Service) – sistemə çoxsaylı sorğular göndərilərək onu çökdürməkdir.**

**Növləri:**

**Trafik əsaslı – sistemin bant genişliyini doldurur**

**Protokol əsaslı – server resurslarını tükədir**

**Tətbiq səviyyəli – konkret veb xidmətləri hədəfləyir**

**Müdafiə üsulları:**

**Firewall və DDoS qoruma sistemləri**

**Trafik analiz sistemləri**

**Rate limiting (IP başına sorğu sayı)**

**Load balancing**

**Bulud əsaslı qoruma xidmətləri (Cloudflare və s.)**

**---**

**16. Metasploit və MSFCONSOLE komandaları**

**Metasploit Framework – zəifliklərin istismarı və sızma testləri üçün platformadır.**

**İstifadəçilər buradan exploitlər, payloadlar və skanerlərlə işləyə bilər.**

**Əsas MSFCONSOLE komandaları:**

**search – exploit axtar**

**use – exploit seç**

**set – parametrləri təyin et**

**show options – mövcud dəyişənləri göstər**

**exploit və ya run – hücumu icra et**

**sessions, background, info, help – əlavə əmrlər**

**---**

**17. Veb tətbiqlərin təhlükəsizliyi və OWASP**

**Veb tətbiqlər hücumların əsas hədəflərindən biridir.**

**OWASP Top 10 – vebdə ən çox rastlanan zəiflikləri göstərən siyahıdır:**

**Əsasları:**

**SQL injection**

**XSS**

**CSRF**

**Sındırılmış autentifikasiya**

**Səhv konfiqurasiya**

**Sensitive data exposure**

**Sındırılmış giriş nəzarəti və s.**

**Qarşısı: input validation, şifrələmə (SSL/TLS), güclü autentifikasiya, təhlükəsizlik testləri.**

**---**

**18. Veb hücumlarının əsas sinifləri**

**Əsas hücum növləri:**

**Injection (SQL, OS) – kod yeritmə**

**XSS – skript yeritmə**

**CSRF – istifadəçi xəbəri olmadan sorğu göndərmə**

**Auth bypass – login sisteminin sındırılması**

**DDoS/DoS – xidmətin dayandırılması**

**File Inclusion, Directory Traversal – fayl sisteminə icazəsiz çıxış**

**Sensitive Data Exposure – məlumatların ifşası**

**Logging & Monitoring zəifliyi**

**---**

**19. SQL inyeksiyası və növləri**

**SQL inyeksiyası – istifadəçinin daxil etdiyi məlumatlarla SQL sorğularına zərərli kod yeridilərək DB-ə müdaxilə edilməsidir.**

**Növləri:**

**Error-based – səhv mesajları ilə məlumat çıxarma**

**Union-based – əlavə nəticələr əlavə etmə**

**Blind – səhv mesajı olmadan məlumat alma (Boolean/Time-based)**

**Out-of-band – fərqli kanal (məsələn, DNS) ilə məlumat göndərmək**

**Qarşısı: parametrli sorğular (prepared statements), input validation, DB səhvlərinin gizlədilməsi.**

**---**

**20. Naqilsiz şəbəkə konsepsiyası**

**Naqilsiz şəbəkələr (Wi-Fi, Bluetooth, 4G/5G) – məlumatları fiziki kabel olmadan ötürən sistemlərdir.**

**Əsas komponentlər: access point, router, cihazlar.**

**Üstünlükləri: rahatlıq, hərəkət azadlığı.**

**Risklər: siqnalın açıq yayılması, müdaxilə və gizli dinləmə.**

**Müdafiə üsulları:**

**WPA2/WPA3 şifrələmə**

**MAC filtrasiya**

**Güclü parol**

**VPN istifadə**

**Şəbəkə monitorinqi**