PowerShell Empire

Information Security Inc.

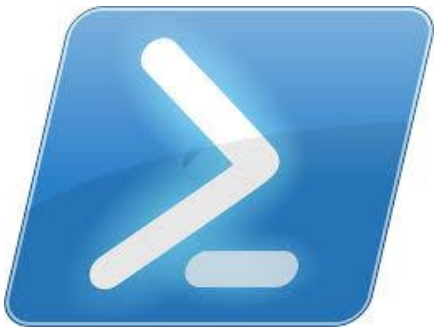
iSEC
information security inc.

Contents

- PowerShell
- PowerShell Offensive Frameworks
- What is Powershell Empire?
- PowerSploit to Empire
- Why PowerShell empire?
- Lab Setup, Empire installation, configuration and demo
- References

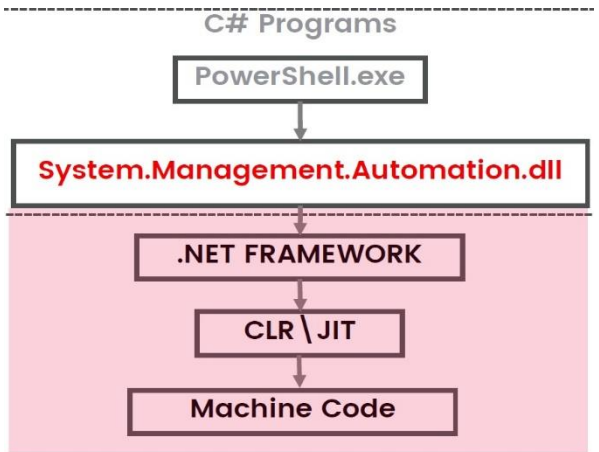
PowerShell

- Windows PowerShell is an interactive object-oriented command environment with scripting language features that utilizes small programs called cmdlets to simplify configuration, administration and management of hererogenous environments.



PowerShell

- Directly access globally cached .NET assemblies
- Reflectively load .NET assemblies which can load C-based Windows libraries
- Run scripts that are interpreted and executed as base64 strings



PowerShell

PowerShell is not the exploit itself, it's the enabler of further compromise.

PowerSploit

"That attack continued with **PowerSploit**, [...] and a second-stage malware payload taken from the efforts of others"
– *The Register*, ***June 2016***

PowerShell Empire

"The industry is [*facing*] years to come of attackers abusing PowerShell [...] tools like **PowerShell Empire** have all but assured that"
– *DarkReading.com*, ***Mar 2016***

PowerShell

"Windows PowerShell tied to more than a third of cyber attacks"
– *ComputerWeekly.com*, ***Mar 2016***

It is everywhere

Every modern Windows Operating System has PowerShell installed. But its not just Windows... Soon Linux

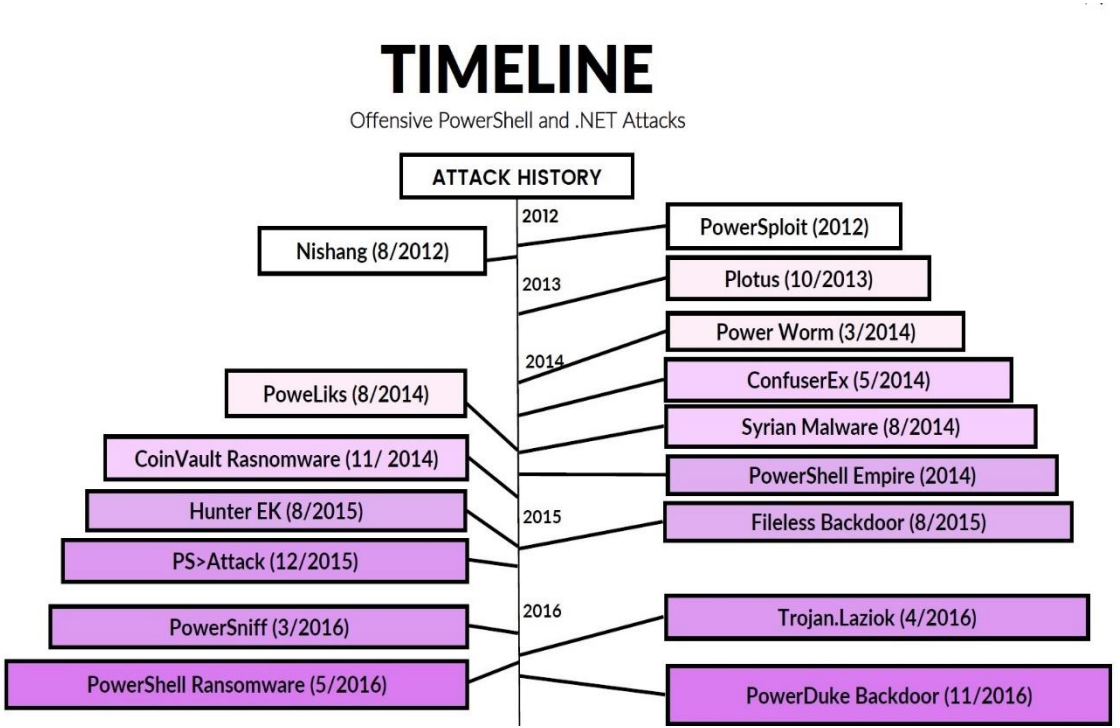
PowerShell is Legitimate

System Administrators use PowerShell for their day jobs. Some Windows Servers don't even have GUIs

Logging isn't Turned on

Most organizations probably don't have the logs required to detect PowerShell because they aren't turned on by default OR they are running an old version of PowerShell

PowerShell



PowerShell Offensive Frameworks

POWERSPLOIT

NISHANG

PS>ATTACK

POWERSHELL EMPIRE

Useful for automating attacks and post-exploitation routines

Collection of scripts to automate tasks such as:

- analysis evasion
- remote execution
- privilege escalation
- lateral movement
- exfiltration

Command to reflectively load and execute a PE binary into memory

Improve and propagate these PowerShell offensive techniques

What is PowerShell Empire?

• Empire is a pure PowerShell post-exploitation agent built on cryptologically-secure communications and a flexible architecture. Empire implements the ability to run PowerShell agents without needing powershell.exe

PowerSploit to Empire

PowerShell Attack Tool Evolution: PowerSploit to Empire

PowerSploit: [github.com/mattifestation/PowerSploit]

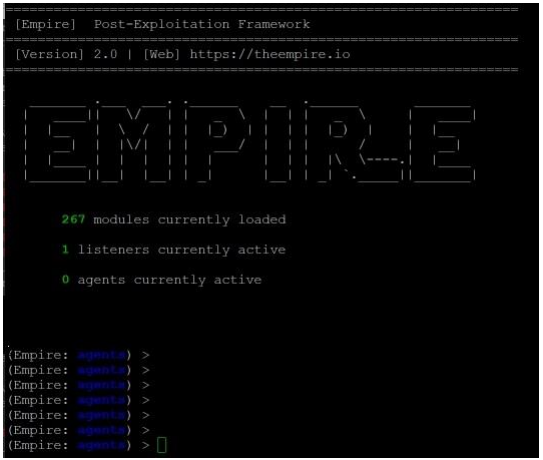
- Invoke-Shellcode
- Invoke-TokenManipulation
- Invoke-Mimikatz
- Get-GPPPassword
- Add-Persistence

Empire: [PowerShellEmpire.com]

- Pure PowerShell agent with secure comms
- Run PowerShell code without using PowerShell.exe
- Wraps functionality of the most popular attack PS tools
- Empire server leverages Python

Why PowerShell Empire?

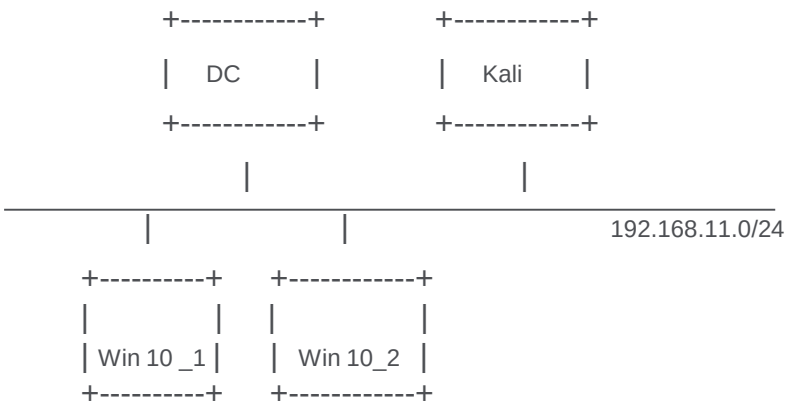
- Similar to Metasploit in user experience
- C2 functionality
- Second stage implant after the initial one
- Use extensively for lateral movement
- Rapid development



Lab Setup

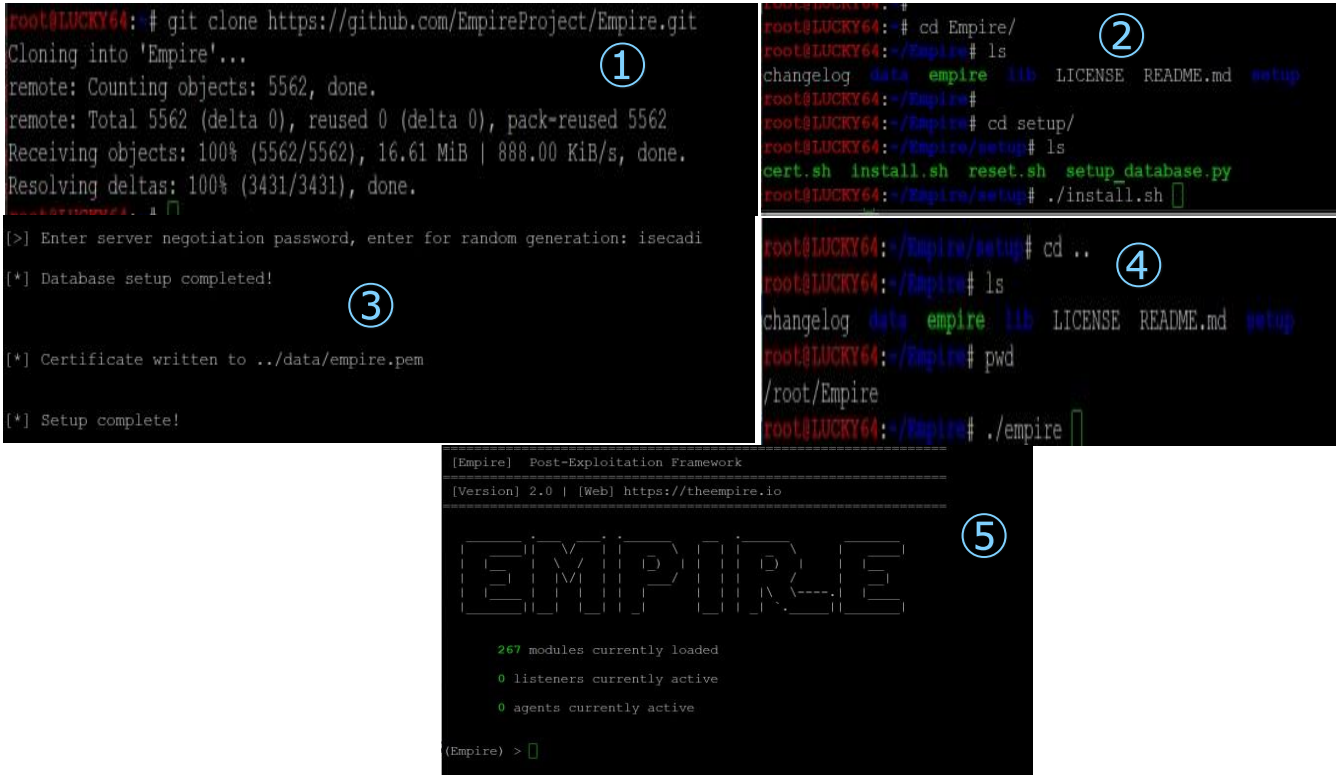
- Lab setup containing the following machines:

◎ Windows Server 2012 R2 Standard as DC (IP: 192.168.11.30)
◎ Windows 10 machine 1 as vulnerable host (IP: 192.168.11.32)
◎ Windows 10 machine 2 as vulnerable host (IP: 192.168.11.193)
◎ Kali Linux as the attack machine running PowerShell Empire (IP: 192.168.11.9)



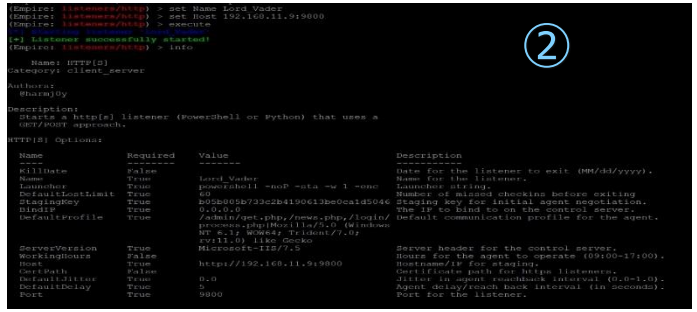
Empire installation

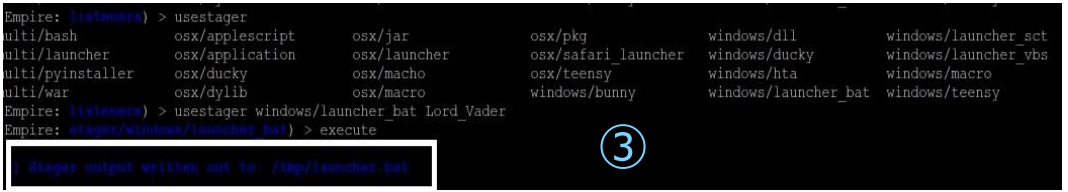
- Installing Empire Framework on the Kali Linux machine



Empire configuration and demo

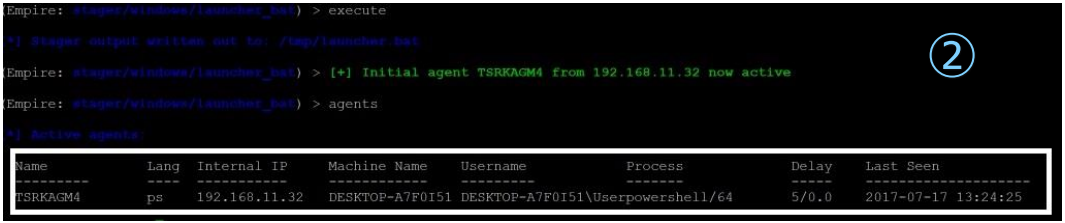
- Configure Empire Listeners,the reverse shell and stagers (payload)





Empire configuration and demo

- Copy the payload to the victim's machine and execute it



Empire configuration and demo

- Five seconds heartbeat between agents and server

```
13:40:07.250352 IP 192.168.11.32.49660 > 192.168.11.9.9800: Flags [P.], seq 1:204, ack 1, win 256, length 203
        0x0000:  000c 2969 6fee 000c 2972 5edb 0800 4500  ..)io...)r^...E.
        0x0010:  00f3 61f8 4000 8006 0093 c0a8 0b20 c0a8  ..a.@.........
        0x0020:  0b09 c1fc 2648 ed14 e452 8db9 5ca2 5018  ....&H...R..\.P.
        0x0030:  0100 8de3 0000 4745 5420 2f6e 6577 732e  ......GET./news.
        0x0040:  7068 7020 4854 5450 2f31 2e31 0d0a 436f  php.HTTP/1.1..Co
        0x0050:  6f6b 6965 3a20 7365 7373 696f 6e3d 6830  okie:.session=h0
        0x0060:  7556 5071 5a37 4a50 7667 762f 6165 6e5a  uVPqZ7JPvgv/aenZ
        0x0070:  4d71 6c76 3442 4433 633d 0d0a 5573 6572  Mqlv4BD3c=..User
        0x0080:  2d41 6765 6e74 3a20 4d6f 7a69 6c6c 612f  -Agent:.Mozilla/
        0x0090:  352e 3020 2857 696e 646f 7773 204e 5420  5.0.(Windows.NT.
        0x00a0:  362e 313b 2057 4f57 3634 3b20 5472 6964  6.1;.WOW64;.Trid
        0x00b0:  656e 742f 372e 303b 2072 763a 3131 2e30  ent/7.0;.rv:11.0
        0x00c0:  2920 6c69 6b65 2047 6563 6b6f 0d0a 486f  ).like.Gecko..Ho
        0x00d0:  7374 3a20 3139 322e 3136 382e 3131 2e39  st:.192.168.11.9
        0x00e0:  3a39 3830 300d 0a43 6f6e 6e65 6374 696f  :9800..Connectio
        0x00f0:  6e3a 204b 6565 702d 416c 6976 650d 0a0d  n:.Keep-Alive...
        0x0100:  0a                                       .
```

```
13:40:12.298372 IP 192.168.11.32.49661 > 192.168.11.9.9800: Flags [P.], seq 1:213, ack 1, win 256, length 212
        0x0000:  000c 2969 6fee 000c 2972 5edb 0800 4500  ..)io...)r^...E.
        0x0010:  00fc 61fd 4000 8006 0085 c0a8 0b20 c0a8  ..a.@.........
        0x0020:  0b09 c1fd 2648 5cf2 fe4c 5539 f010 5018  ....&H\..LU9..P.
        0x0030:  0100 f250 0000 4745 5420 2f6c 6f67 696e  ...P..GET./login
        0x0040:  2f70 726f 6365 7373 2e70 6870 2048 5454  /process.php.HTT
        0x0050:  502f 312e 310d 0a43 6f6f 6b69 653a 2073  P/1.1..Cookie:.s
        0x0060:  6573 7369 6f6e 3d6b 3779 3248 3748 7773  ession=k7y2H7Hws
        0x0070:  5663 712b 754b 7874 502f 6c4d 4761 4559  Vcq+uKxtP/lMGaEY
        0x0080:  4b73 3d0d 0a55 7365 722d 4167 656e 743a  Ks=..User-Agent:
        0x0090:  204d 6f7a 696c 6c61 2f35 2e30 2028 5769  .Mozilla/5.0.(Wi
        0x00a0:  6e64 6f77 7320 4e54 2036 2e31 3b20 574f  ndows.NT.6.1;.WO
        0x00b0:  5736 343b 2054 7269 6465 6e74 2f37 2e30  W64;.Trident/7.0
        0x00c0:  3b20 7276 3a31 312e 3029 206c 696b 6520  ;.rv:11.0).like.
        0x00d0:  4765 636b 6f0d 0a48 6f73 743a 2031 3932  Gecko..Host:.192
        0x00e0:  2e31 3638 2e31 312e 393a 3938 3030 0d0a  .168.11.9:9800..
        0x00f0:  436f 6e6e 6563 7469 6f6e 3a20 4b65 6570  Connection:.Keep
        0x0100:  2d41 6c69 7665 0d0a 0d0a                 -Alive....
```

References

- Powershell Empire website; github

https://www.powershellempire.com/
https://github.com/powershellempire/empire

- Metasploit

https://www.metasploit.com/

- Windows PowerShell

https://blogs.msdn.microsoft.com/powershell/2017/06/
http://www.exploit-monday.com/2012/08/Why-I-Choose-PowerShell.html

To be continued…