Hacking Articles

Raj Chandel's Blog

Credential Dumping: Applications

posted in RED TEAMING on APRIL 10, 2020 by RAJ CHANDEL

SHARE

This is a sixth article in the Credential Dumping series. In this article, we will learn about dumping the credentials from various applications such as **CoreFTP**, **FileZilla**, **WinSCP**, **Putty**, etc.

Table of Content:

- 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:

```
usemodule credentials/sessiongopher
execute
```

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

Core FTP server tool is made especially for windows. It lets you send and receive files over the network. For this transfer of files, it uses FTP protocol 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:

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

FTP Navigator: LaZagne

Just like Core FTP, the FTP navigator is the FTP client that makes transfers, editings, and renaming of files easily 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 all** 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/credetnials/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 FTP protocol. It is compatible with Windows, Linux, and macOS. It is used for transfer or editing or replacing the files in a network. We can dump its credentials using Metasploit and do so, type:

```
use post/multi/gather/filezilla_client_cred
set session 1
exploit
```

And so, we have successfully retrieved the credentials

HeidiSQL: Metasploit Framework

It is an open-source tool for managing MySQL, MsSQL, PostgreSQL, 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. Management of database is pretty easy if you are using this software. 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/creddtnitals/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 is developed by Nirsoft and is best suited for internal pentesting. Simple 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
execute
```

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 **lazagne.exe chat** command in LaZagne you can dump it's password as shown in the image below:

PST: PstPassword

Nirsoft provides a tool that lets you retrieve all the PST passwords from Outlook. You can download this tool from **here.** Simple launch the tool and you will have the passwords as shown below :

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 and to do so, type:

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

WinSCP: LaZagne

WinSCP is an FTP client which is based on 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 helps us to retrieve passwords. In LaZagne, use the command **lazagne.exe all** and it will dump the credentials as shown in the image below:

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.

Author: **Yashika Dhir** is a passionate Researcher and Technical Writer at Hacking Articles. She is a hacking enthusiast. contact **here**

ABOUT THE AUTHOR

RAJ CHANDEL

Raj Chandel is Founder and CEO of Hacking Articles. He is a renowned security evangelist. His works include researching new ways for both offensive and defensive security and has done illustrious research on computer Security, exploiting Linux and windows, wireless security, computer forensic, securing and exploiting web applications, penetration testing of networks. Being an infosec enthusiast himself, he nourishes and mentors anyone who seeks it.

PREVIOUS POST
← CREDENTIAL DUMPING: SAM

NEXT POST
WINDOWS PERSISTENCE USING WINLOGON →

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Notify me of follow-up comments by email.

Notify me of new posts by email.

POST COMMENT

Search

ENTER KEYWORD

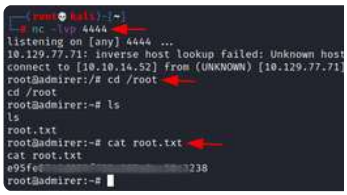
Subscribe to Blog via Email

Email Address

SUBSCRIBE

Join our Training Programs

Follow me on Twitter



Categories

- Password Cracking
- Penetration Testing
- Pentest Lab Setup
- Privilege Escalation
- Red Teaming
- Social Engineering Toolkit
- Uncategorized
- Website Hacking
- Window Password Hacking
- Wireless Hacking

Articles

Select Month