Metasploitable2 full walkthrough

This machine has several ways to get exploited. All ports are exploitable, also there will be various exploits which can be directly handled fro m metasploit and that’s why the name of machine is metasploitable.

Lets get into it

┌──(root💀kali)-[~]

└─# nmap -A -sC -sV 192.168.1.39

Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-24 03:04 EDT

Nmap scan report for 192.168.1.39

Host is up (0.0013s latency).

Not shown: 977 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

|\_ftp-anon: Anonymous FTP login allowed (FTP code 230)

| ftp-syst:

| STAT:

| FTP server status:

| Connected to 192.168.1.40

| 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

Now we can search for exploit vsftpd 2.3.4

$ searchsploit vsftpd 2.3.4

It will give result for 49757.py

You have to do some adjustments to run it with python3 like adding brackets after print( <content> )

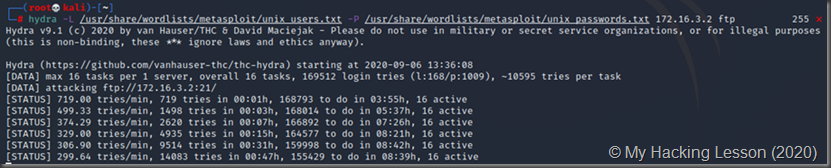
Now run it python3

$ python3 49757.py --help

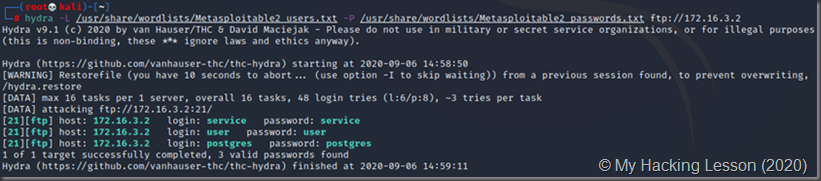
$ python3 49757.py 192.168.1.39

And you will get the shell

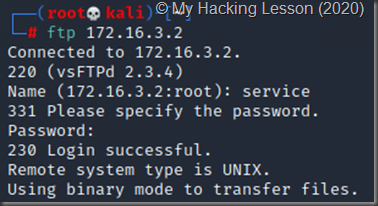
### Brute force FTP using Hydra

[](https://drive.google.com/uc?id=1ja1_IuTtCFLnfzLIipDo2h1boU8yVPoY)

This is an example of successful results using custom created wordlists:

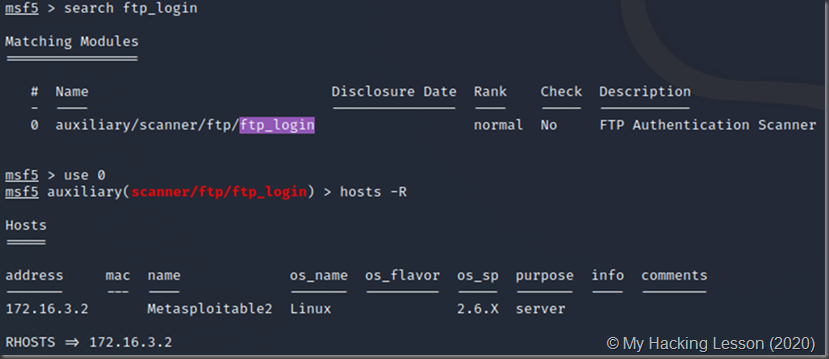
[](https://drive.google.com/uc?id=1IxGRAiiJQ4BGFyxauOlWfUDLXTyebLO4)

Once you have found a valid credential set, you can use it to login to the remote FTP server:

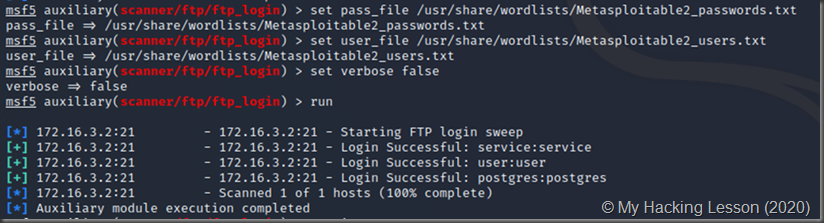
[](https://drive.google.com/uc?id=1iW2q7p8GnDBPi-A507johLarQ53sTD1d)

### Brute force FTP Metasploit

Metasploit has auxiliary modules that can be used to brute force passwords of FTP just like Hydra did.

[](https://drive.google.com/uc?id=16h64Swur1fmEHFkyFS9uFp6TgCil7zVo)

Using the custom wordlists

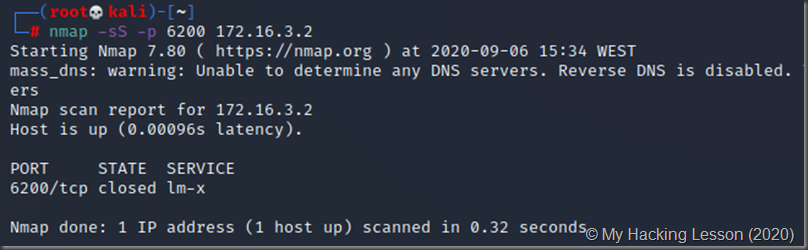
[](https://drive.google.com/uc?id=1gZizjXJ_pHb6AnMnjD4ISPQhEkgsVbF_)

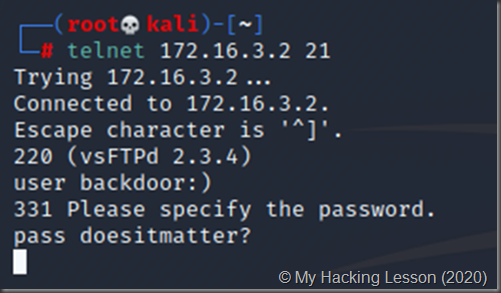
Metasploit has merits over Hydra since the credentials are automatically stored in the database:

[](https://drive.google.com/uc?id=1LMGnbC7zzpqXD5ZCDdf17mxd0T7bCQUw)

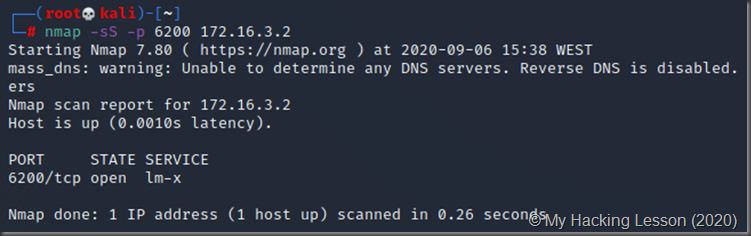
#### Open the backdoor manually vsFTPd 2.3.4 contained a backdoor that was smuggled into the server where the source code resides by an unknown person. Certain versions of vsFTPd included in the Metasploitable VM contain a vulnerability that opens a backdoor shell . This allows users to get a root shell, view and modify file contents. (Note that the login attempt does not have to be successful!)

* Opening backdoor  
  **To open** a backdoor on port 6200 **using vsFTP:**
* We begin by scanning the Metasploitable VM to show that port 6200 is closed:

[](https://drive.google.com/uc?id=1V2PjIOyajJmdV4jZRCWA19ttUsjGF3yK)

[](https://drive.google.com/uc?id=1gBoG7FjjnkUG0Z0fJF_K843xt09pbYmY)

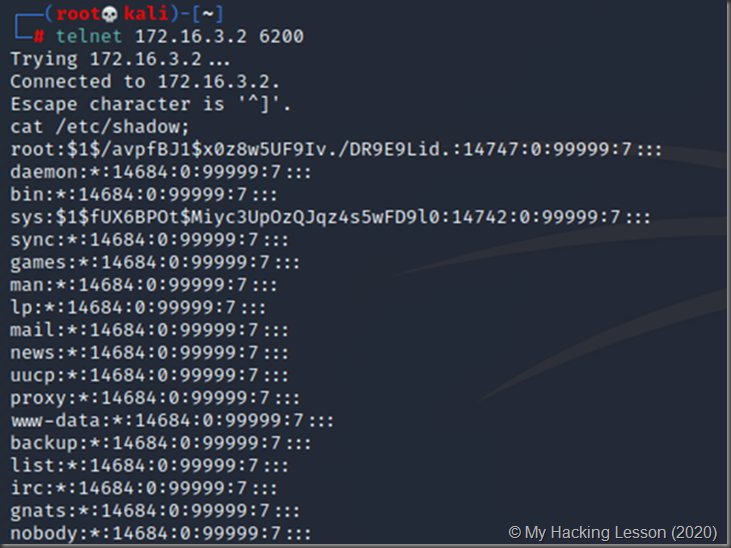
* You can close this window - you're done.
* Now check the same port 6200 with Nmap. It’s open!

[](https://drive.google.com/uc?id=1MJ_KL-dqz0gIxCCKqF8Gh-1HEF50C6xb)

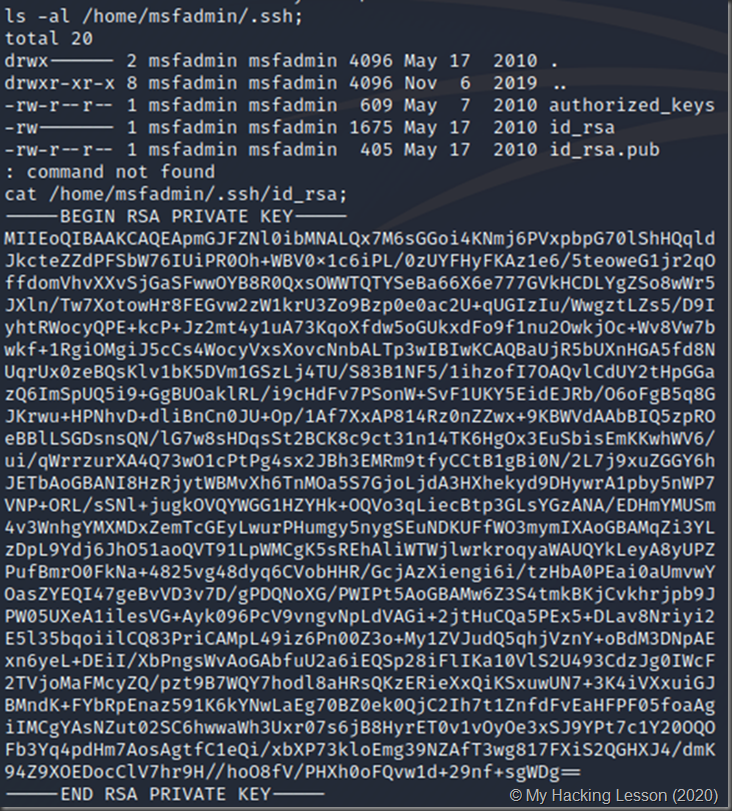
#### Exploiting the backdoor

Connect on port 6200 with Telnet client. There ,execute normal shell commands:

**E.g. command\_name args; (** to dump the contents of the /etc/shadow file)

[](https://drive.google.com/uc?id=1zHnq0rdrno4KKH_dwJXaq928CcLKXCe2)

* You can even grab SSH key information (authorized\_keys, known\_hosts, private and public keys)

[](https://drive.google.com/uc?id=1YmdBvFsxAxejyRTDMCQyJOTDkXtWAVSe)

**This** vsFTPd technique **always** opens a backdoor on port 6200, **making** it a convenient **way to connect to** and **execute** commands on **a** remote **victim's computer.** However, other connection techniques may be more **convenient. For** example, using SCP without a password to deliver a payload to the **victim's computer.**  
**When** you **disconnect** from the remote shell on port 6200, the port **is closed** again. You can always **resume** using the **methods** above.