**Network Penetration Testing Assignment**

**Password Attacks**

**Student Name: Aslam Patel**

**Student Number: 00520874**

**Summary of task:**

* Use different tools that are covered (or not covered) in this module to demonstrate a range of password attacks.
* Attack different network services such as http, ftp, ssh, rdp, etc

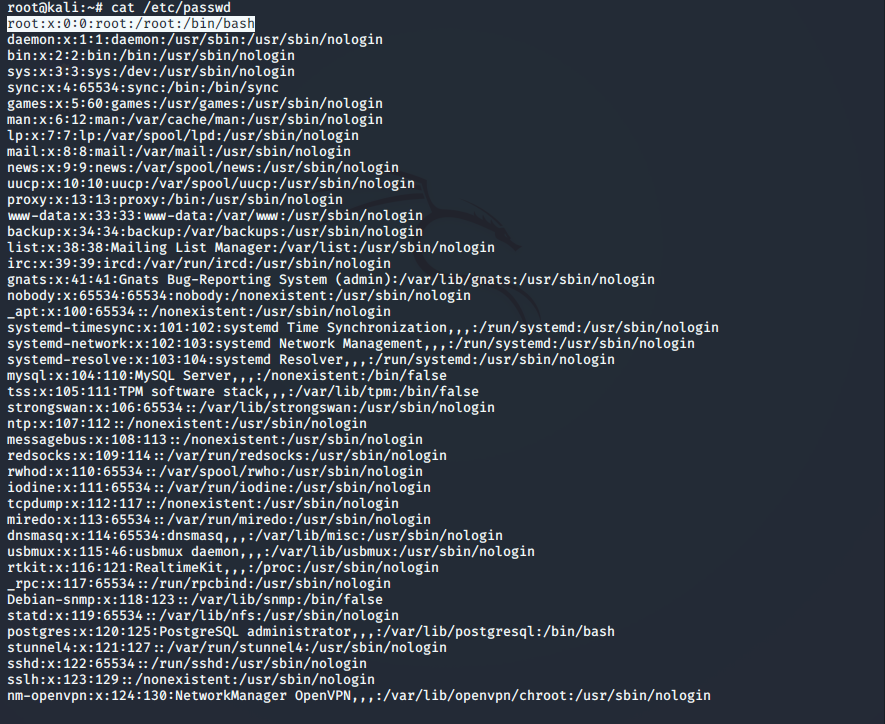
**Password Attack Report**

A password attack is merely when a hacker trys to steal your password. As nearly all passwords can only contain letters and numbers passwords can be deemed as unsafe. An attacker will know there can be a chance of lazy passwords to make them easier to remember for a user hence making passwords attacks a commion tool for date breach.

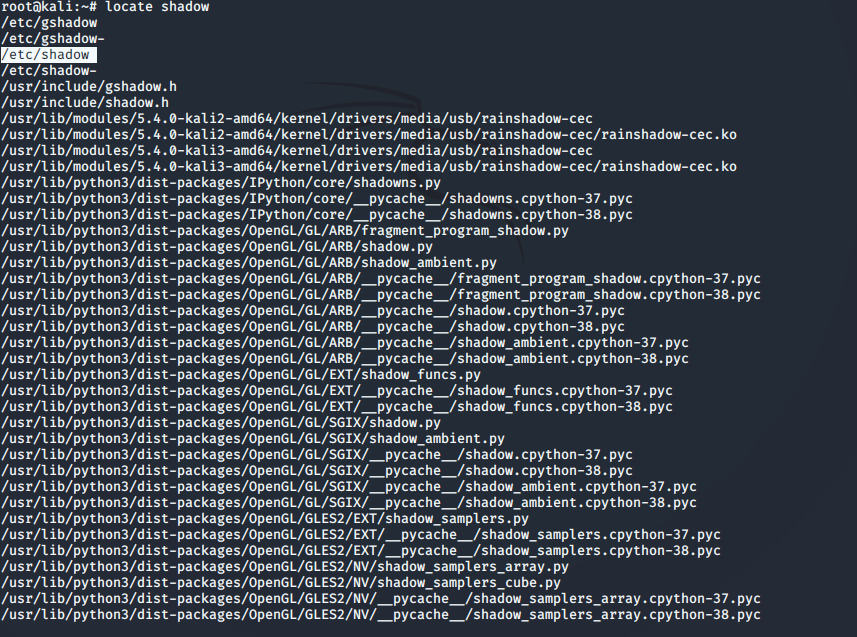
**Offline Attacks:**

**My own Kali Password Attack**

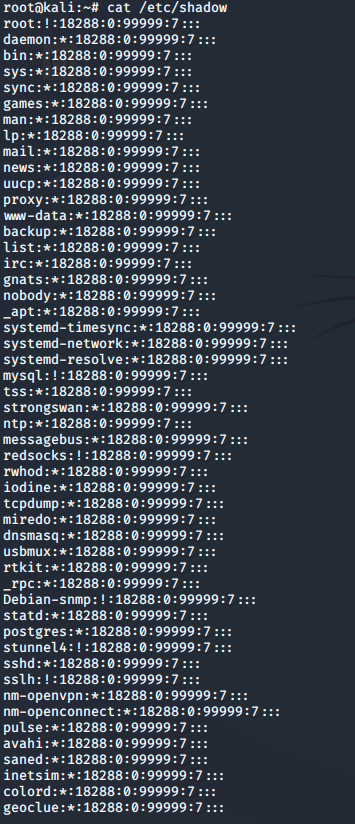
I started by locating the path In which my kali password is and displays all users of kali (for different tools)



Shadow files are where password files are stored.



After running cat etc/shadow I can see the users as empty, but I am only looking for my user.

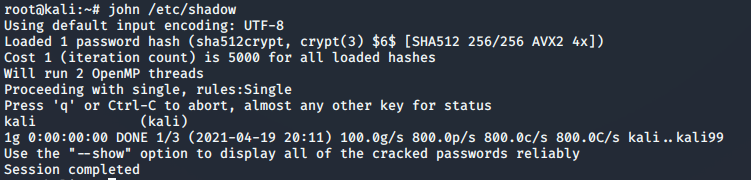


The $6 donates the version of hash used.



A password cracker such as John can be used to ‘hack’ this password.

I gave John the path of the file.

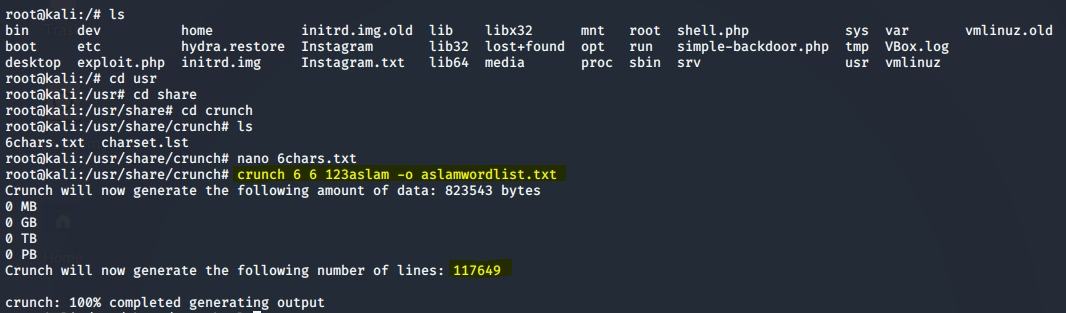


John has cracked the password very easily as it is weak password.

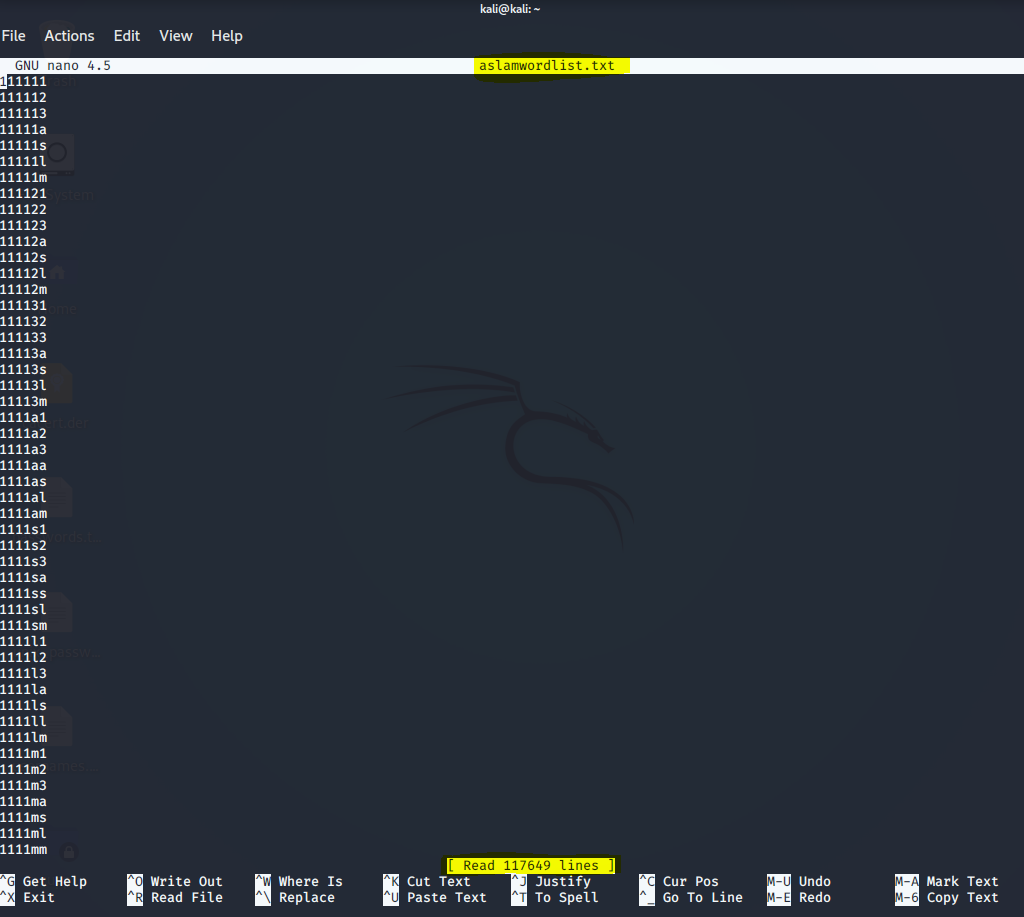
**Generating password wordlists**

**Crunch:**

Crunch is a wordlist generator where the user can stipulate a character set and it will produce all the potential combinations.



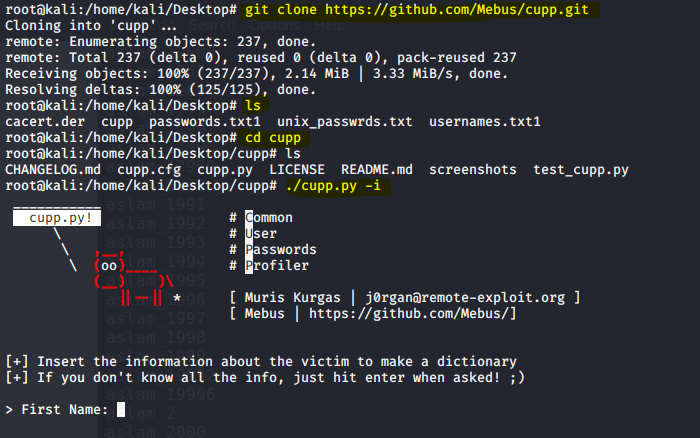
I generated a dictionary file which contained both words and letters with a minimum and maximum length of 6 characters. It used the characters ‘123aslam’ and saved it to a file I named ‘aslamwordlist.txt’



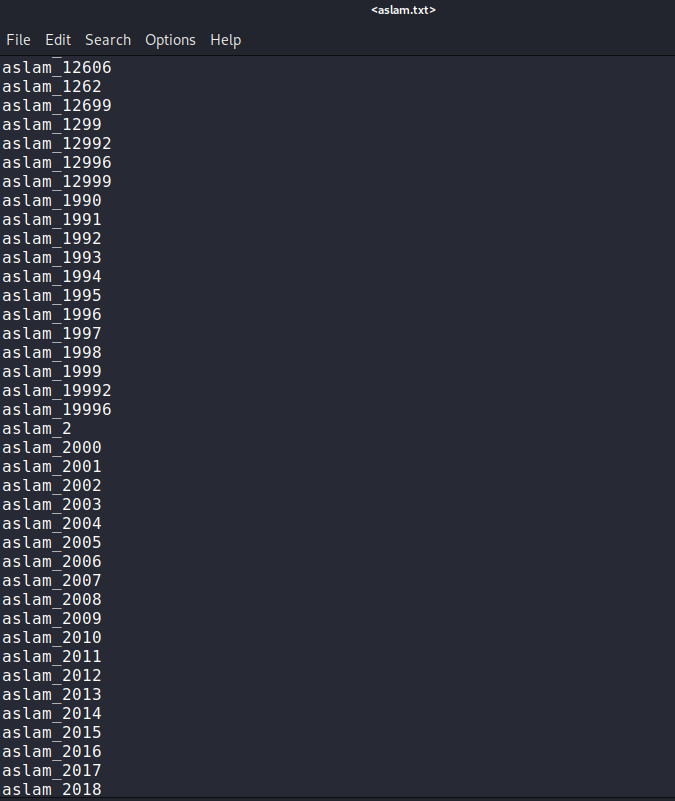
It gave me an output of 117,649 possible combinations.

There are many built password generators available on the web that can use information about a victim to generate a list of passwords

<https://github.com/Mebus/cupp.git> is one which I tested.

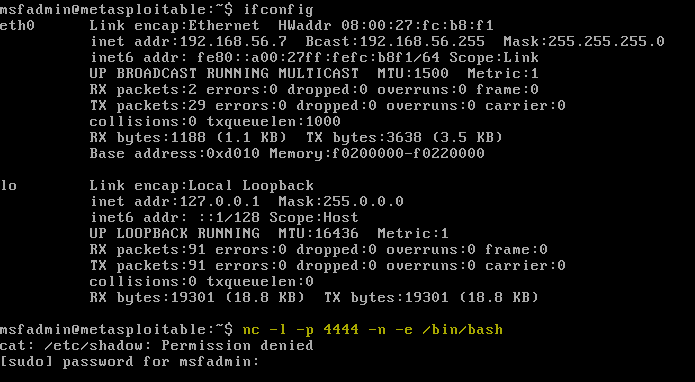


After inputting some details about myself which an attacker can do via some reconnaissance it generated over 10,000 possible passwords within seconds (would have done more if I did not cancel action) with an option for special characters and case sensitivity.



**Metasploitable VM using John**

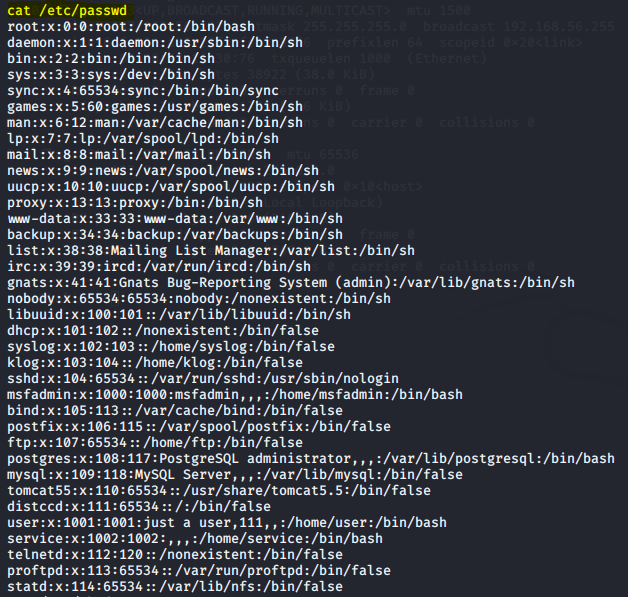
I used a VM Metasploitable to attempt to carry out a password attack using John.



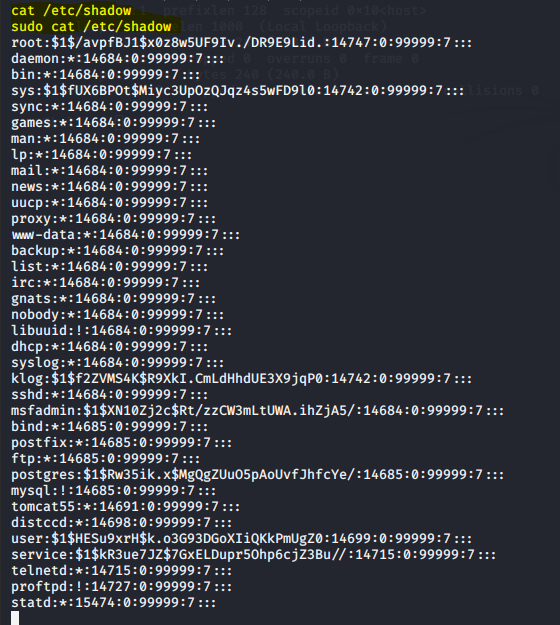
I set up nc -l -p 4444 -n -e /bin/bash



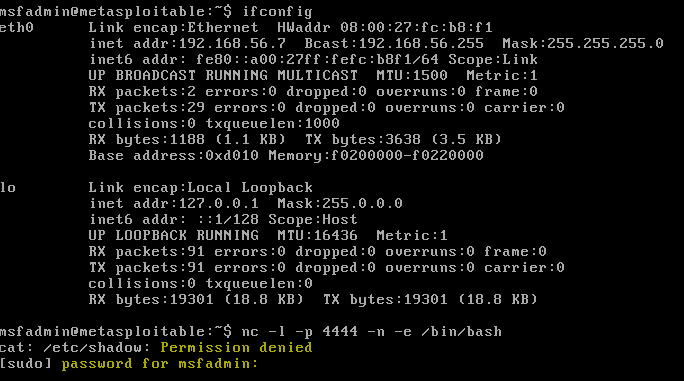
Tested connection from Kali VM



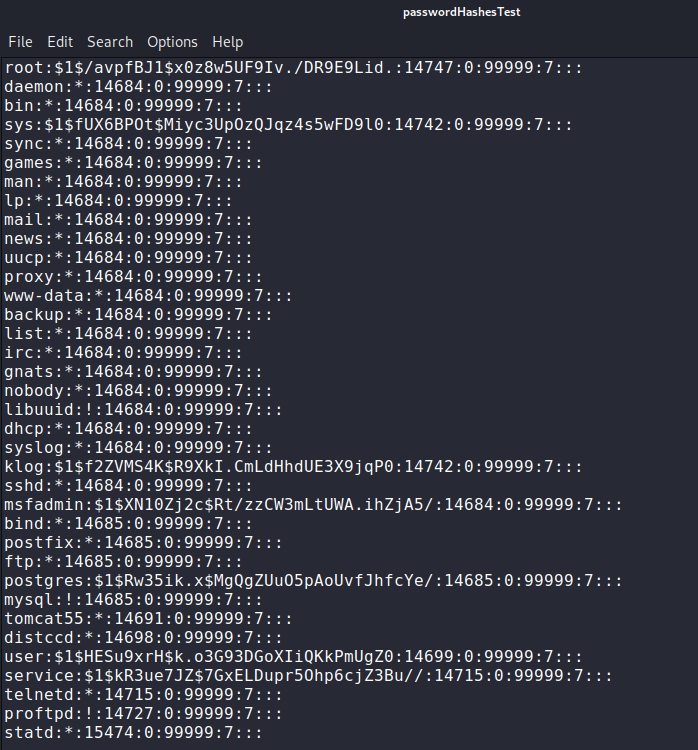
Here are all the password files available as users.



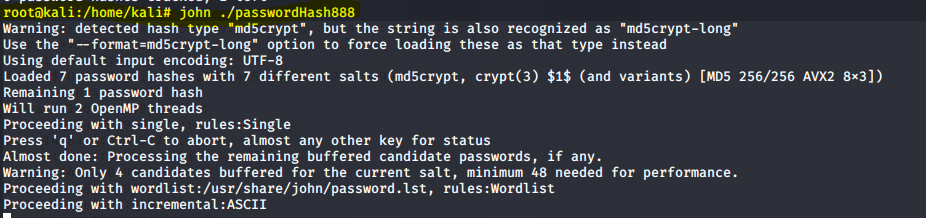
I attempted to use cat /etc/shadow however permission was denied so I had to use sudo. But the problem with that was I had to input the password of Metasploitable VM from its own machine now my Kali VM.



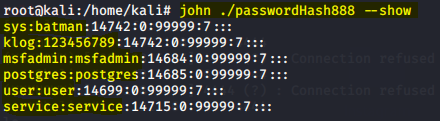
By using sudo -S cat /etc/shadow it does not ask for a password.



I then added the hashes to a file to run with John. I noticed the hashes are using version one so this should be simple to crack using John.



I ran the command, but I was unable to gain a screen capture as I cleared my terminal. I believe the reasoning behind this is John never outputs the same password more than once. On that screen msfadmin, postgres, service & user were cracked first implying they were the easiest as it was the same as the username.



Nevertheless, a simple command shows me the 6 out of 7 hashes that are cracked from Metasploitable.

In this case it showed me that the john first used ‘single crack mode’ where it uses passwords that are account based e.g., admin:admin

For the hash that was not cracked it was attempting to use Incremental mode however after waiting 30 mins for a result I discontinued it.

John can also use wordlists however I did not use this for john.

**Hydra ftp & ssh using wordlist**

Hydra is a pre-installed tool which is used to brute-force username and password to various services such as ftp, ssh etc.

I located a pre-existing wordlist from kali which had a total of 1010 passwords.

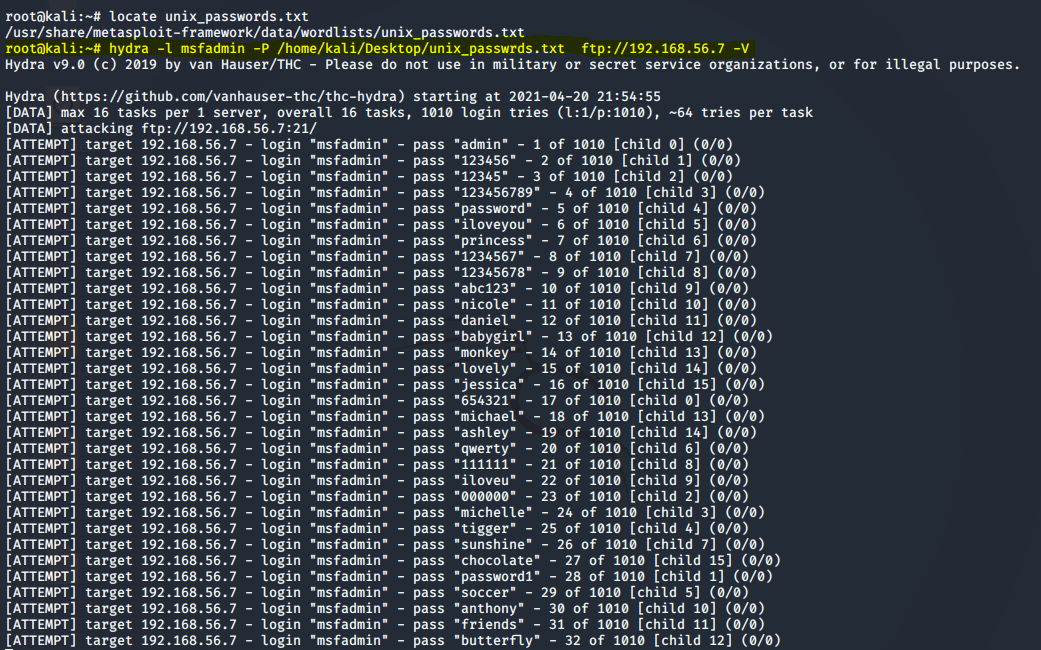


I ran hydra -l msfadmin -P /home/kali/Desktop/unix\_passwrds.txt ftp://192.168.56.7 -V

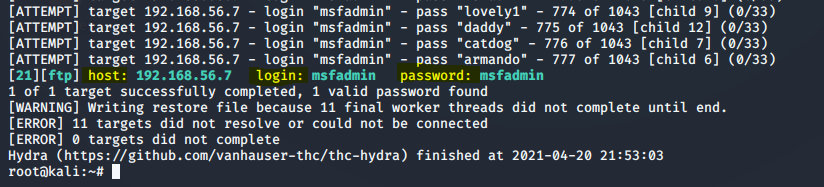
Where;

input login: -l

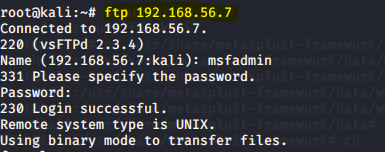
list of passwords: -P



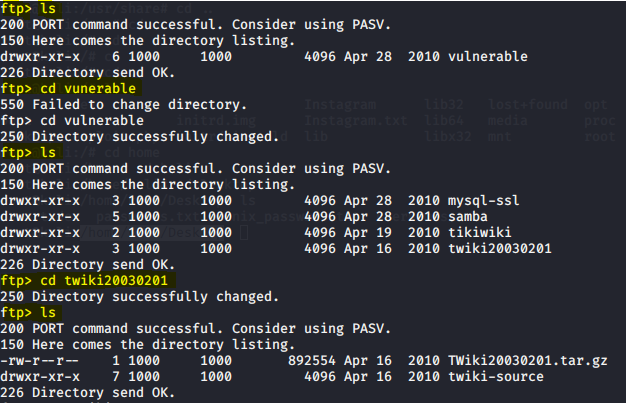
Hydra was able to find the password via ftp.



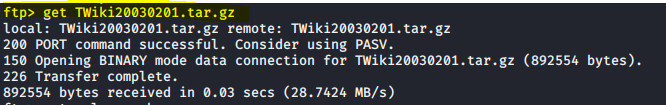
I ran ftp to my target machine



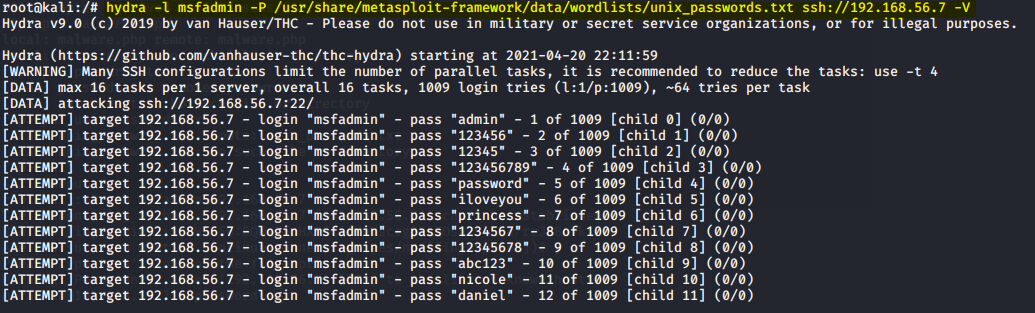
I could then browse through directories and files



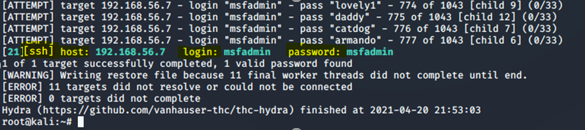
And download remote files to my own VM



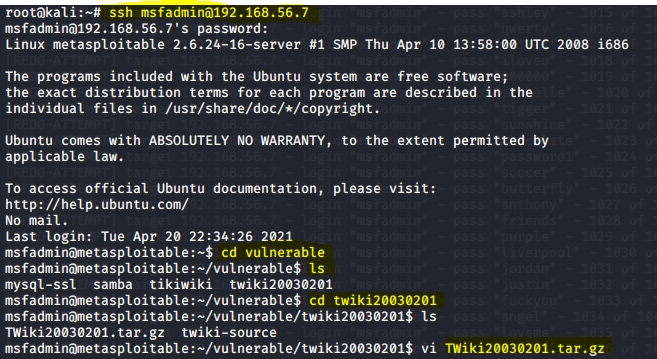
The same was attempted but this time using SSH



Again, the password was found.



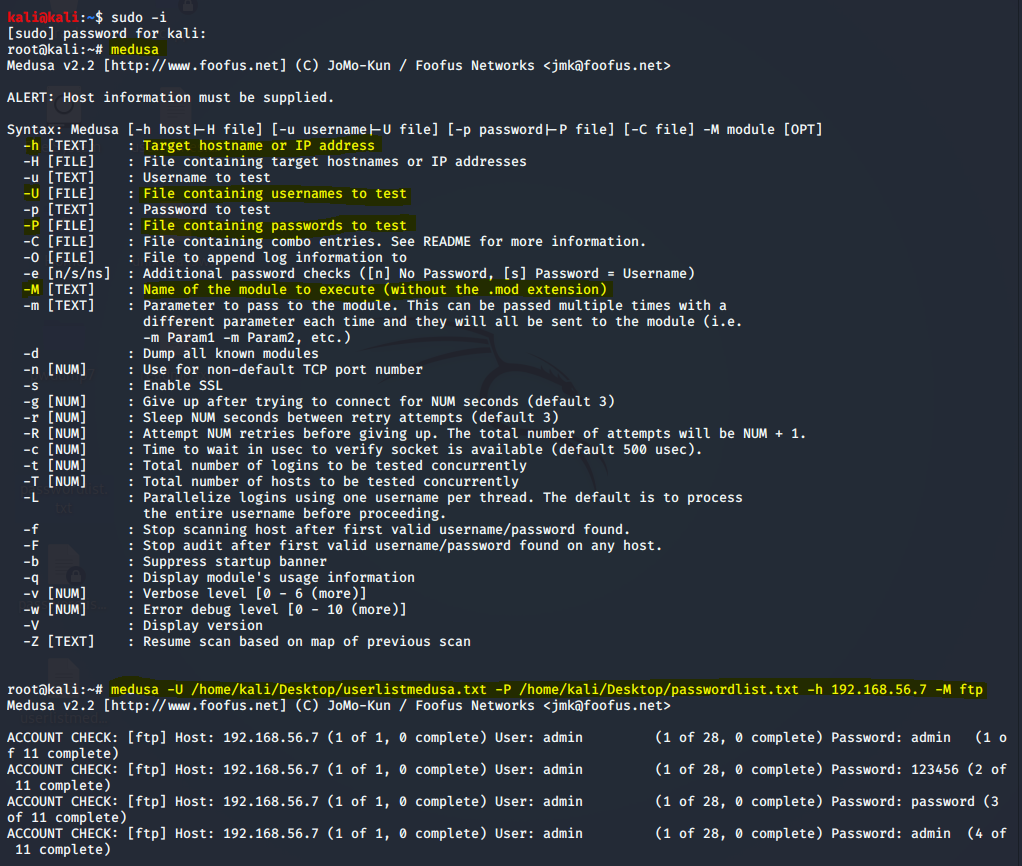
As it was with ftp, with ssh I can browse, move, copy files etc.



**Medusa attack on metasploitable using ftp**

Medusa is speedy login brute-forcer. It allows multiple hosts to be tested at one time and consists of a flexible user input.

I created two wordlists one for usernames and one for passwords.



medusa -U /home/kali/Desktop/userlistmedusa.txt -P /home/kali/Desktop/passwordlist.txt -h 192.168.56.7 -M ftp

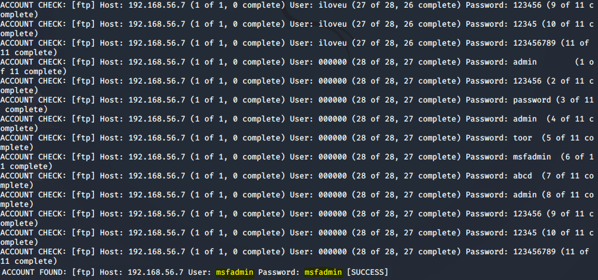
*where;*

-h: my target IP

-P: File containing passwords to test

-U: File containing usernames to test

-M: name of module to execute



Again, I can set up a connection to take information from target, plant information on target or even install malware onto the target.

**Conclusion:**

From this short this test it is easily detectable that weak passwords have a massive vulnerability aspect and shows the importance of designing complex passwords.

“58% of hackers’ passwords contained only the lower-case alphabet characters a-z. The most common lower-case letter is “a” and f, j, v, w, y, z was the least used.” (Smith, 2021)

This was proved in my small testing.

**References**

Smith, M., 2021. *Hackers use pathetic passwords just like everyone else*. [online] CSO Online. Available at: <https://www.csoonline.com/article/2362943/hackers-use-pathetic-passwords-just-like-everyone-else.html> [Accessed 20 April 2021].

WonderHowTo. 2021. *Password Cracking « Null Byte :: WonderHowTo*. [online] Available at: <https://null-byte.wonderhowto.com/how-to/password-cracking/> [Accessed 17 April 2021].

Dargahi, Dr.T. and Young, Dr.A., 2021. Presentation slides. Password Attacks. University of Salford, Greater Manchester.