Title: Hydra Hydra Brute Force Attack on Metasploitable 2 & 3
Name: Rafik Tarbari
Date: November 10, 2022

Hosts:

- Metasploitable 2: [redacted]
- Metasploitable 3: [redacted]

Adding New User Accounts:

In each of the metasploitable virtual machine, we add new user "cyberraf" with a weak (easy-to-guess) password "chloe"
The commands are the following:

sudo adduser cyberraf ← creates new user with username "cyberraf"

We are prompted to enter password, we type "chloe" (which is a password found in /usr/share/wordlists/rockyou.txt.gz)

SSH in Metasploitable 2 and Metasploitable 3

After solving the issues of ssh-ing in the VMs, we successfully get in each of them by ssh-ing.

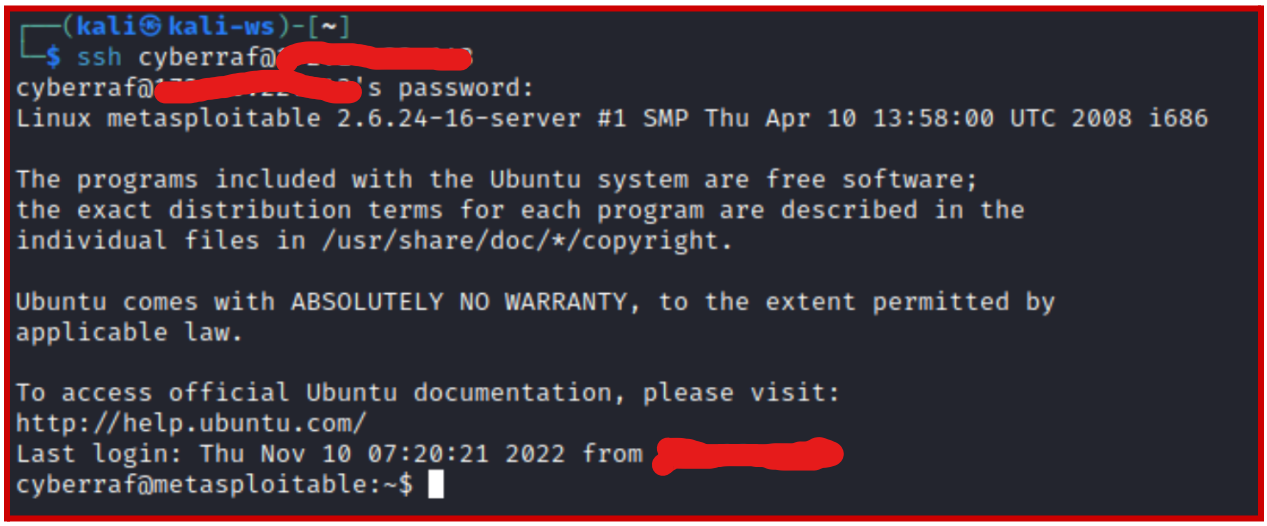

Fig1. ssh in metasploitable 2

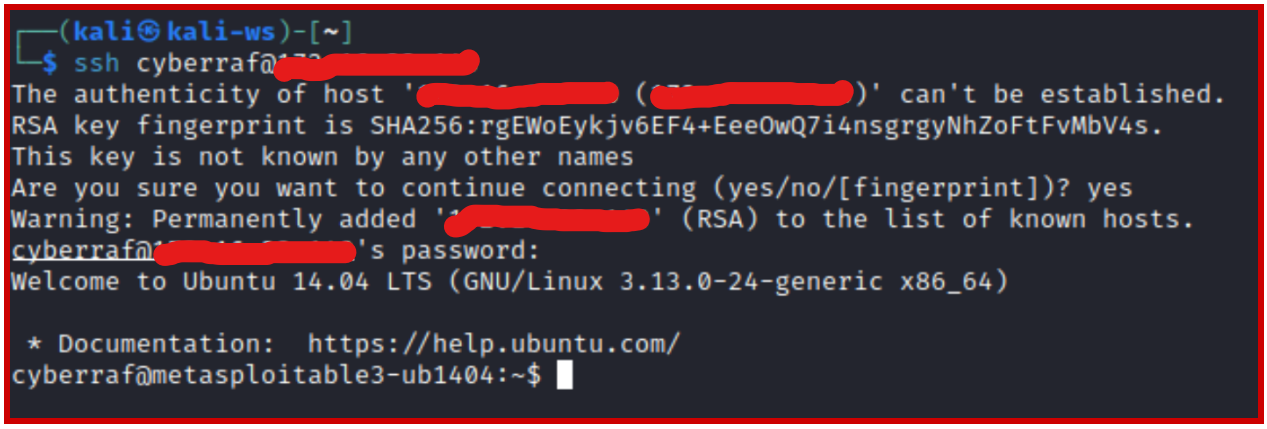

Fig. 2 ssh in metasploitable 3

Using Hydra Brute Force

Metasploitable 2:

As we can see in Fig. 3 below, running the following command launches the brute force attack on metasploitable 2.

sudo hydra -l cyberraf -P /usr/share/wordlists/rockyou.txt.gz -t 6 ssh://

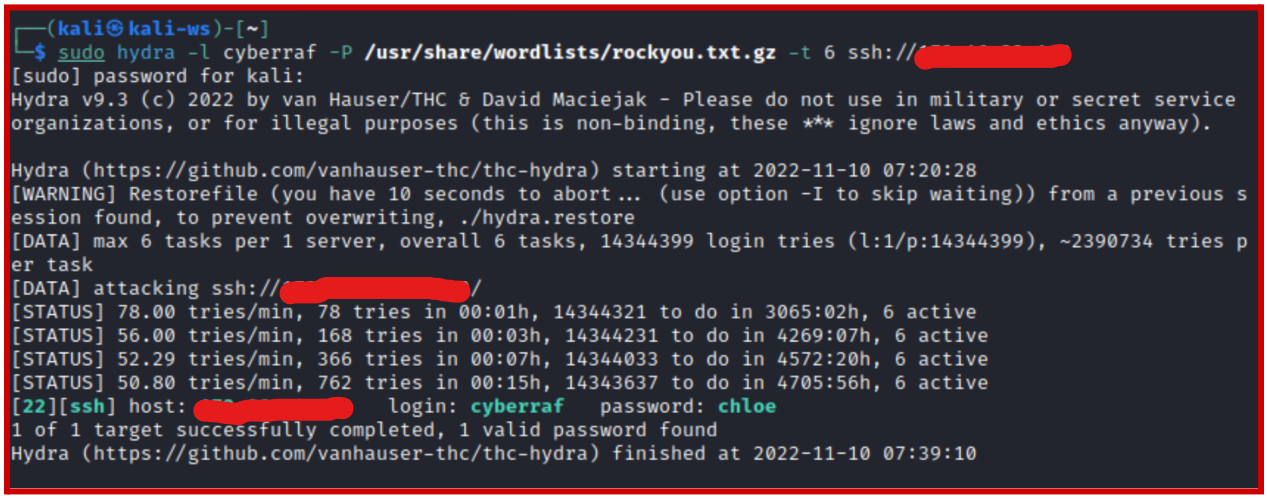

Fig. 3: metasploitable 2

The attack runs from 7:20:28 to 7:39:10 which is approximately **19 min.**

Metasploitable 3:

As we can see in Fig. 4 below, running the following command launches the brute force attack on metasploitable 3.

sudo hydra -l cyberraf -P /usr/share/wordlists/rockyou.txt.gz -t 6 ssh://

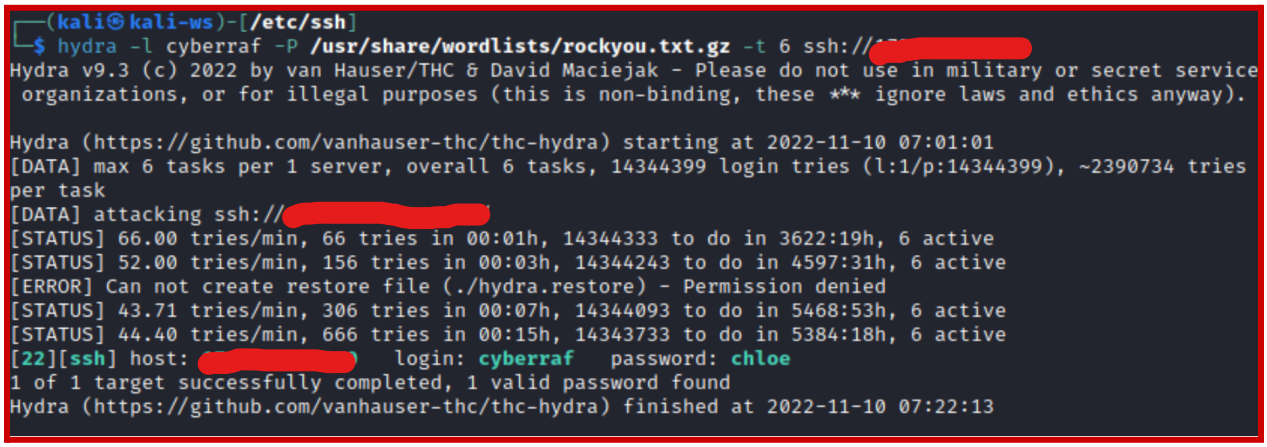

Fig. 4: metasploitable 3

The attack runs from 7:01:01 to 7:22:13 which is approximately **21 min.**

How to Accelerate the Speed of the Attack

We can accelerate or decelerate the speed of the attack by changing the flag -t.

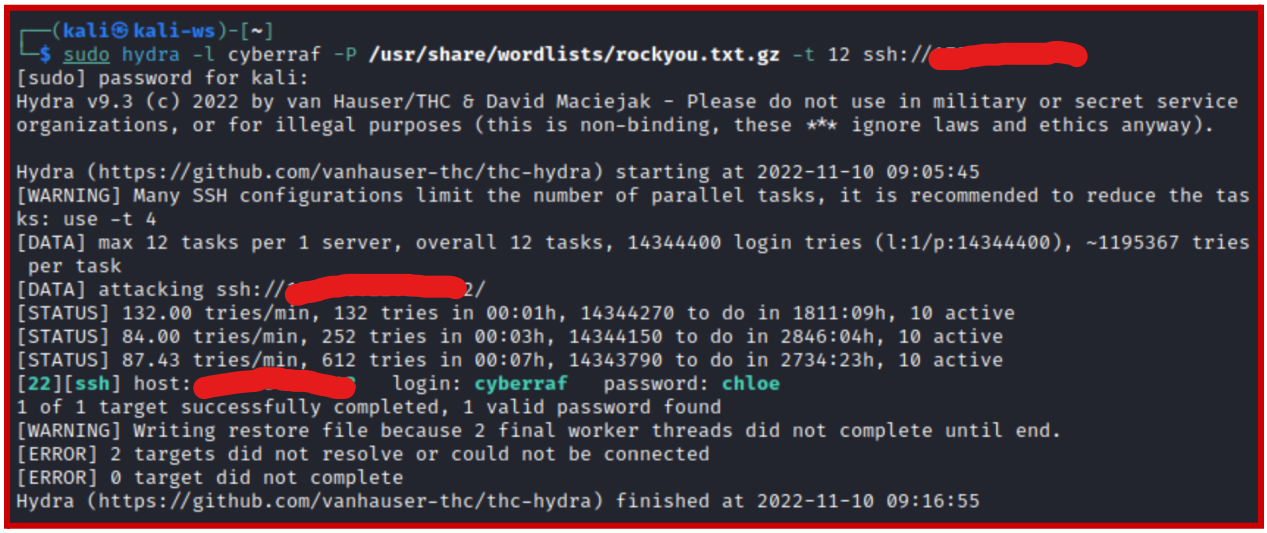

Fig. 5: metasploitable 2

The attack runs from 9:05:45 to 9:16:55 which is approximately **11 min.** So, increasing the value of the flag -t from **6** to **12** , reduced the run time of the attack from **19** min to **11** min.

Other Protocols other than SSH

- FTP
- FTPS

- TELNET
- SMTP: Simple Mail Transfer Protocol
- PostgreSQL
- HTTP → GET/HEAD/POST
- IMAP

- If I knew a common password, I can easily add it to the /usr/share/wordlists/rockyou.txt.gz file by using **vi (**Fig. 6).

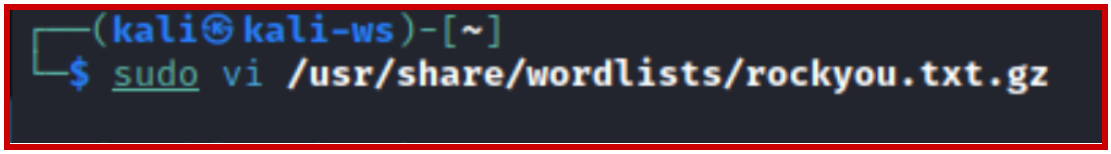

Fig. 6

In Fig. 7, we can see that the common password “rafik” has been added successfully.

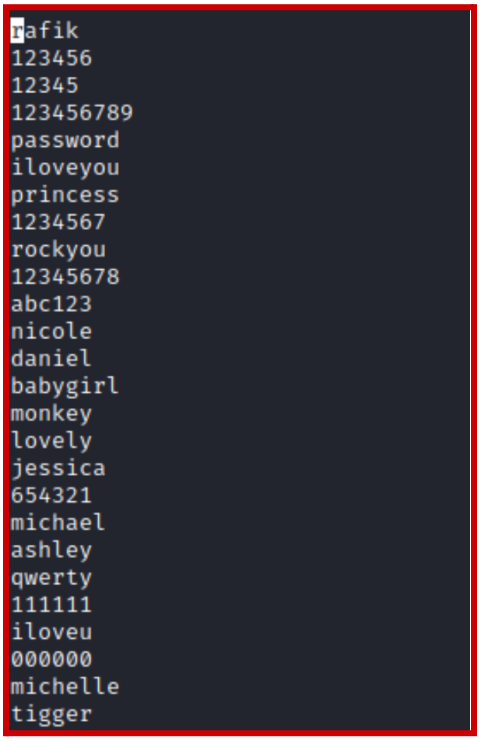

Fig. 7

To get the list of user names,

- If we have access to the system, we can look into the /etc/passwd file (Fig. 8)

Fig. 8: /etc/passwd

- If we do not have access to the system, we can use OSINTs like
  - checkusernames.com
  - Knowem.com
  - nameck.com

  Or check on company's website to find organization email directory