

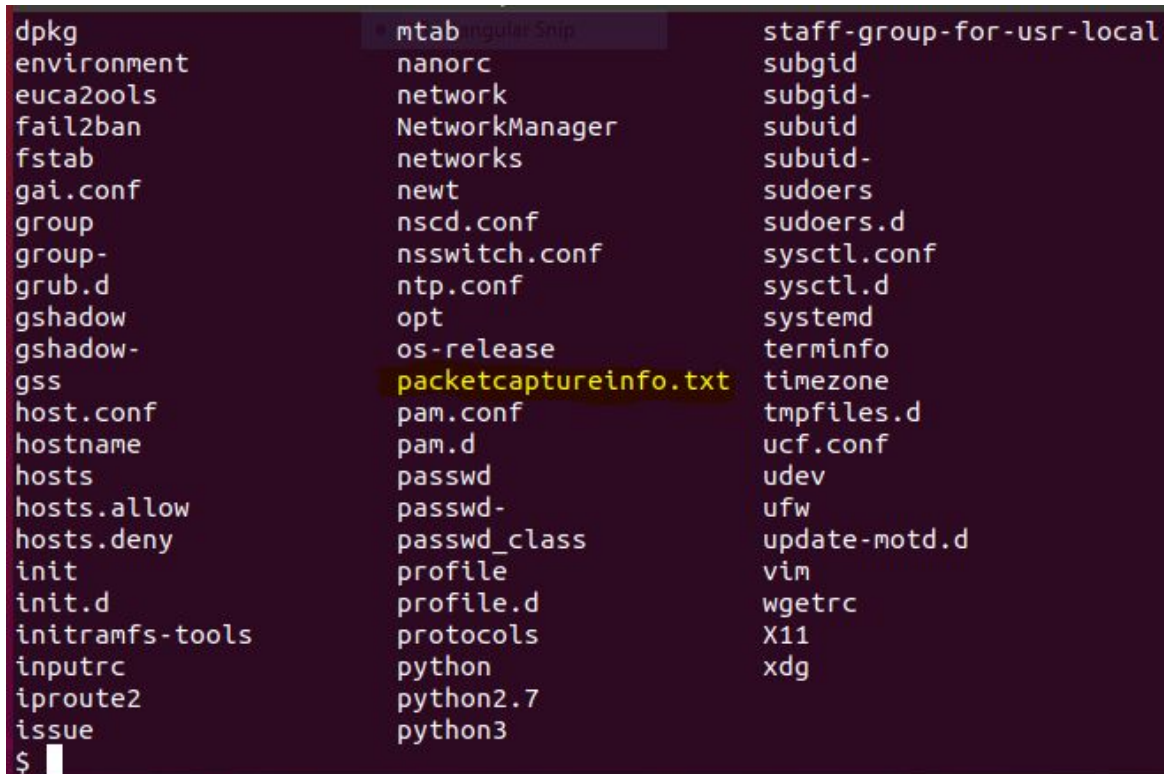
Phase 4: "ShARP Dressed Man"

Solution:

View the file the hacker left to find where to recover the packet captures.

```
$ cd /etc
```

```
$ ls
```



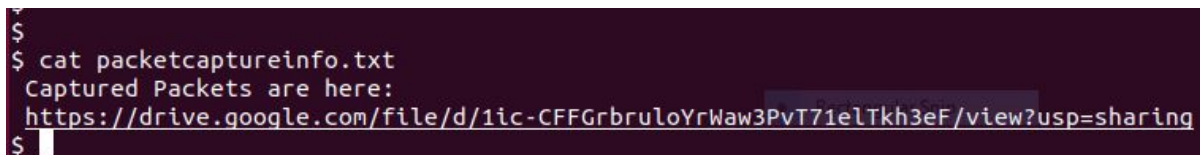
```
dpkg
environment
euca2ools
fail2ban
fstab
gai.conf
group
group-
grub.d
gshadow
gshadow-
gss
host.conf
hostname
hosts
hosts.allow
hosts.deny
init
init.d
initramfs-tools
inputrc
iproute2
issue
$
```

angular Snip

```
mtab
nanorc
network
NetworkManager
networks
newt
nscd.conf
nsswitch.conf
ntp.conf
opt
os-release
packetcaptureinfo.txt
pam.conf
pam.d
passwd
passwd-
passwd_class
profile
profile.d
protocols
python
python2.7
python3
```

```
staff-group-for-usr-local
subgid
subgid-
subuid
subuid-
sudoers
sudoers.d
sysctl.conf
sysctl.d
systemd
terminfo
timezone
tmpfiles.d
ucf.conf
udev
ufw
update-motd.d
vim
wgetrc
X11
xdg
```

Open the file:

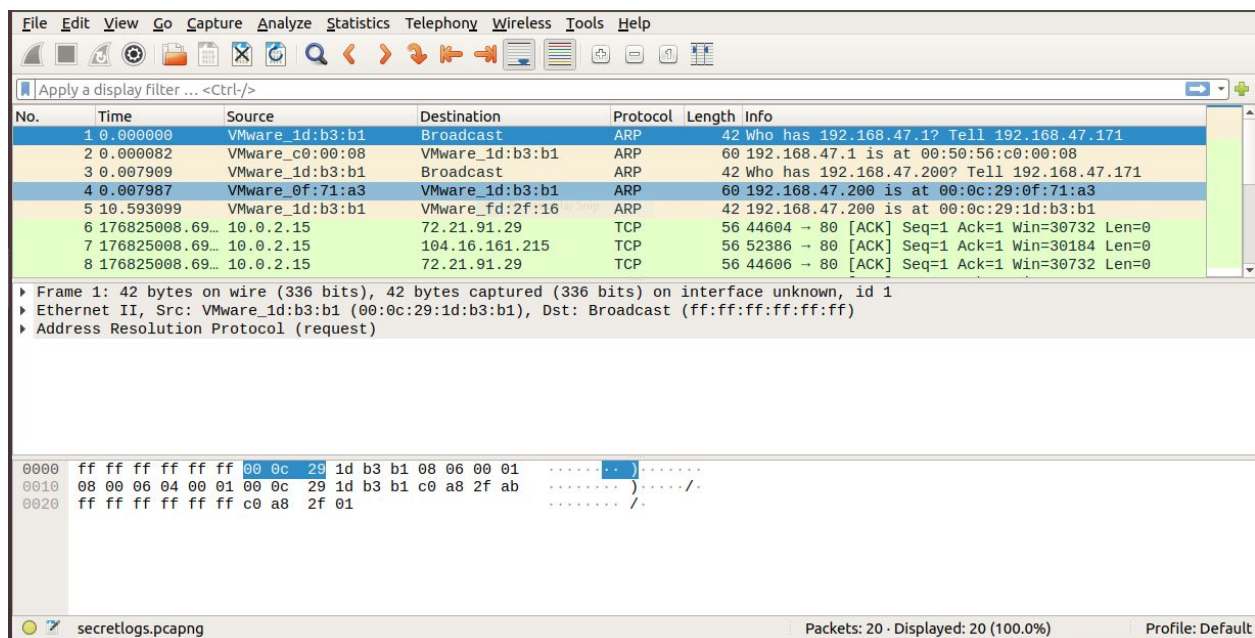


```
$
$ cat packetcaptureinfo.txt
Captured Packets are here:
https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71eITkh3eF/view?usp=sharing
$
```

Browse the URL:



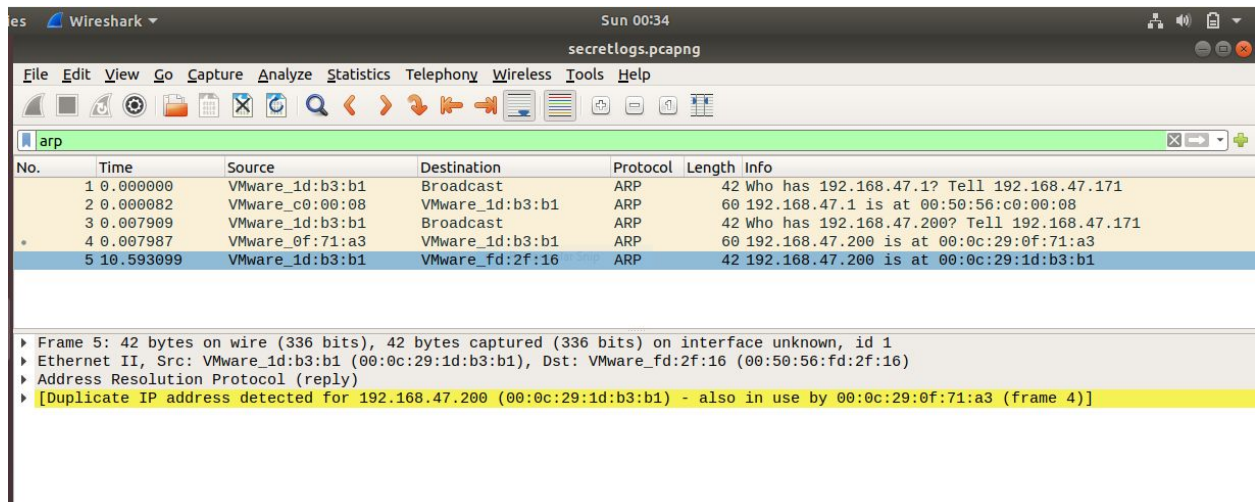
Open the secrelogs.pcapng with Wireshark:



Checking for arp spoofing:

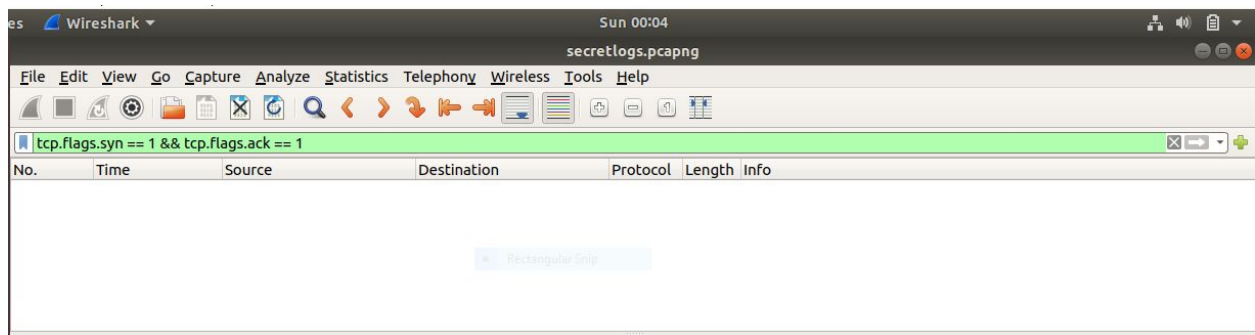
The hacker used spoof ARP message to the LAN, directing all traffic intended for host 192.168.47.200 (mac address - 00:0c:29:0f:71:a3) to it mac address - 00:0c:29:1d:b3:b1.

The OSI layer of the findings is DataLink layer (layer 2).



Checking for open ports.

Port 80 (HTTP)



Wireshark - Conversations - secretlogs.pcapng

Ethernet · 4		IPv4 · 5		IPv6		TCP · 10		UDP			
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
10.0.2.15	58610	104.18.127.89	80	4	2,271	2	1,605	2	6665825013.3841	1.8538	
10.0.2.15	33546	104.18.126.89	80	2	2,296	1	1,876	1	4205825119.7805	0.6913	
10.0.2.15	52482	104.16.161.215	80	2	4,339	1	684	1	3,6555825120.5111	0.1128	
10.0.2.15	44604	72.21.91.29	80	1	56	1	56	0	05825008.6952	0.0000	
10.0.2.15	52386	104.16.161.215	80	1	56	1	56	0	05825008.6954	0.0000	
10.0.2.15	44606	72.21.91.29	80	1	56	1	56	0	05825008.6955	0.0000	
10.0.2.15	57750	74.125.136.95	80	1	56	1	56	0	05825008.6955	0.0000	
10.0.2.15	57752	74.125.136.95	80	1	56	1	56	0	05825008.6956	0.0000	
10.0.2.15	52398	104.16.161.215	80	1	56	1	56	0	05825008.6956	0.0000	
10.0.2.15	52486	104.16.161.215	80	1	598	1	598	0	05825120.6665	0.0000	

The SYN scan shows that port 80 has 4 packets which indicated that the hacker closed it. We recommend it to be open immediately, since users need to communicate with the server.

The OSI layer these findings fall into is Transport layer (layer 4).