Cybersecurity

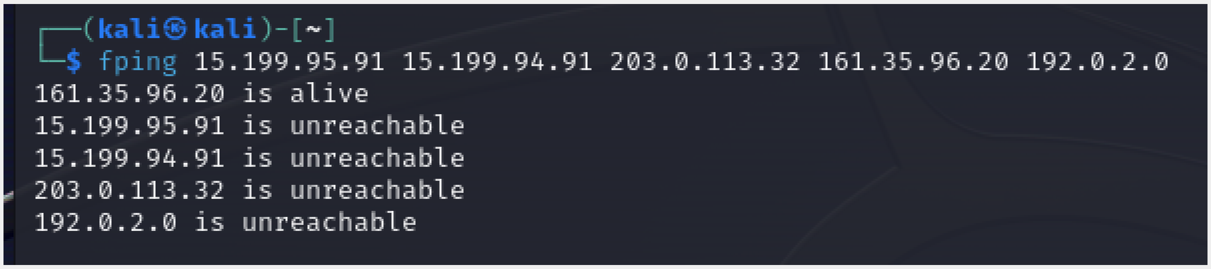
Networking Challenge Submission File

Networking Fundamentals: Rocking your Network

Make a copy of this document to work in. For each phase, add the solution below the prompt. Save and submit this completed file as your Challenge deliverable.

Phase 1: *“I’d like to Teach the World to `ping`”*

1. Command(s) used to run `ping` against the IP ranges:



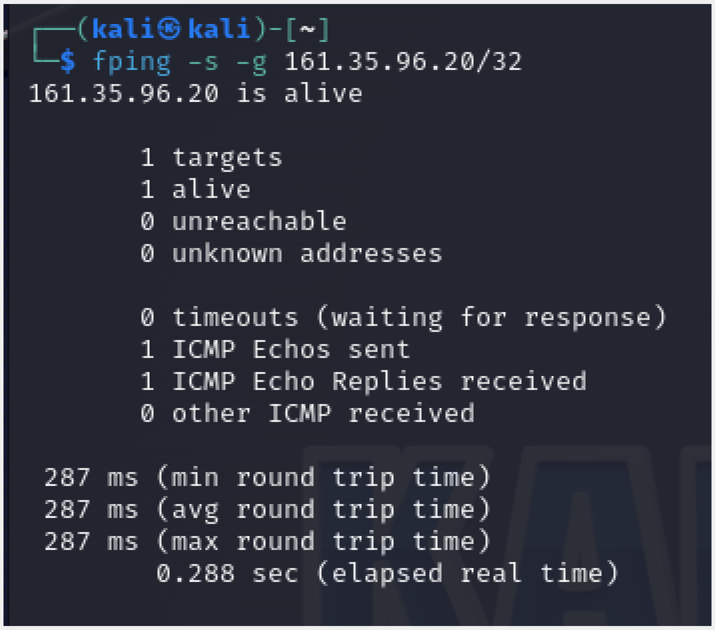
```
┌──(kali㉿kali)-[~]
└─$ fping 15.199.95.91 15.199.94.91 203.0.113.32 161.35.96.20 192.0.2.0
161.35.96.20 is alive
15.199.95.91 is unreachable
15.199.94.91 is unreachable
203.0.113.32 is unreachable
192.0.2.0 is unreachable
```

```
fping 15.199.95.91 15.199.94.91 203.0.113.32 161.35.96.20 192.0.2.0
```

2. Summarize the results of the `ping` command(s):

```
After running the fping command, we are able to conclude that only one ip
host is active which is 161.35.96.20
```

3. List of IPs responding to echo requests:



```
┌──(kali㉿kali)-[~]
└─$ fping -s -g 161.35.96.20/32
161.35.96.20 is alive

       1 targets
       1 alive
       0 unreachable
       0 unknown addresses

       0 timeouts (waiting for response)
       1 ICMP Echos sent
       1 ICMP Echo Replies received
       0 other ICMP received

 287 ms (min round trip time)
 287 ms (avg round trip time)
 287 ms (max round trip time)
        0.288 sec (elapsed real time)
```

```
fping -s -g 161.35.96.20/32

(IP Host 161.35.96.20 is still alive)
```

4. Explain which OSI layer(s) your findings involve:

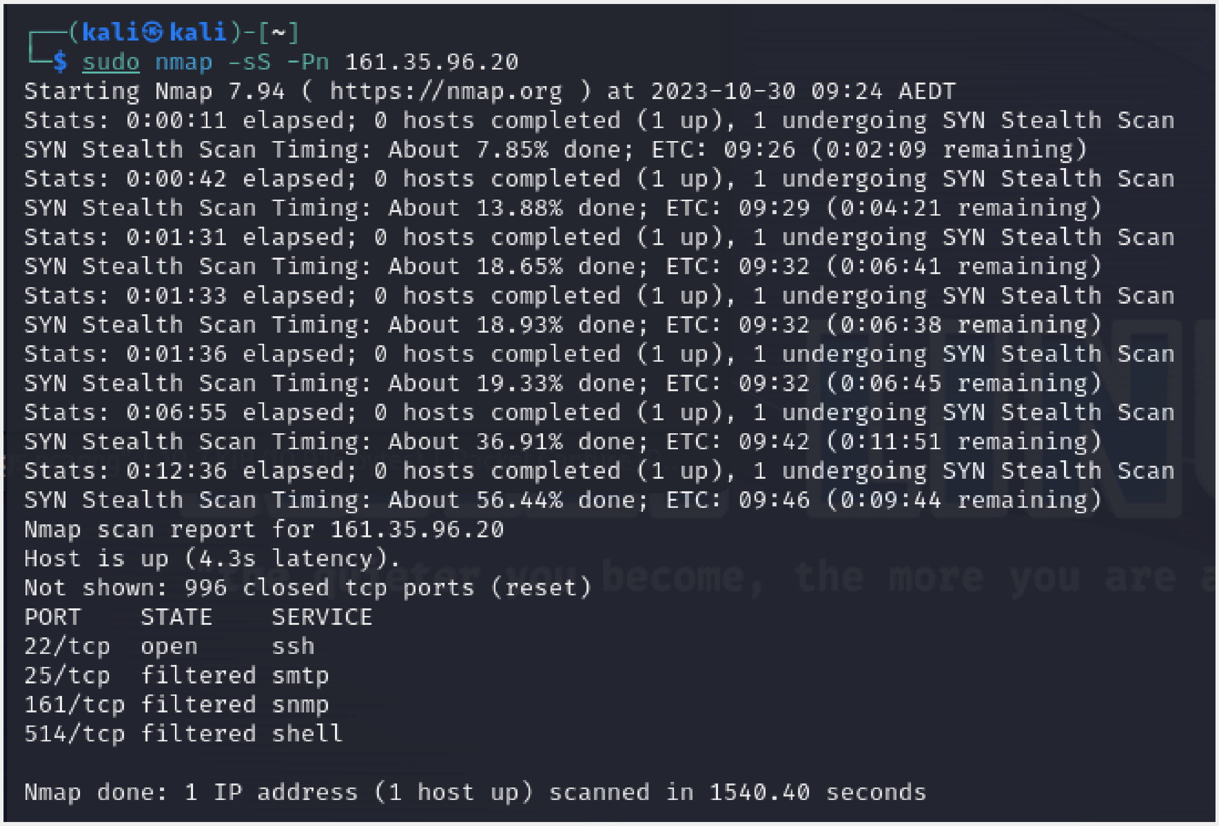
```
Layer 3 - The Networking Layer
```

5. Mitigation recommendations (if needed):

```
Since I was able to ping 161.35.96.20. Rockstar will need to adjust their
firewall configuration to ensure that that IP does not respond to ping
requests by blocking ICMP Echo Requests.
```

Phase 2: *“Some SYN for Nothin’”*

1. Which ports are open on the RockStar Corp server?



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -Pn 161.35.96.20
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-30 09:24 AEDT
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 7.85% done; ETC: 09:26 (0:02:09 remaining)
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 13.88% done; ETC: 09:29 (0:04:21 remaining)
Stats: 0:01:31 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 18.65% done; ETC: 09:32 (0:06:41 remaining)
Stats: 0:01:33 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 18.93% done; ETC: 09:32 (0:06:38 remaining)
Stats: 0:01:36 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 19.33% done; ETC: 09:32 (0:06:45 remaining)
Stats: 0:06:55 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 36.91% done; ETC: 09:42 (0:11:51 remaining)
Stats: 0:12:36 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 56.44% done; ETC: 09:46 (0:09:44 remaining)
Nmap scan report for 161.35.96.20
Host is up (4.3s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE    SERVICE
22/tcp  open     ssh
25/tcp  filtered smtp
161/tcp filtered snmp
514/tcp filtered shell

Nmap done: 1 IP address (1 host up) scanned in 1540.40 seconds
```

Port 22 is open

2. Which OSI layer do SYN scans run on?

   a. OSI layer:

Layer 4 - The Transport Layer

   b. Explain how you determined which layer:

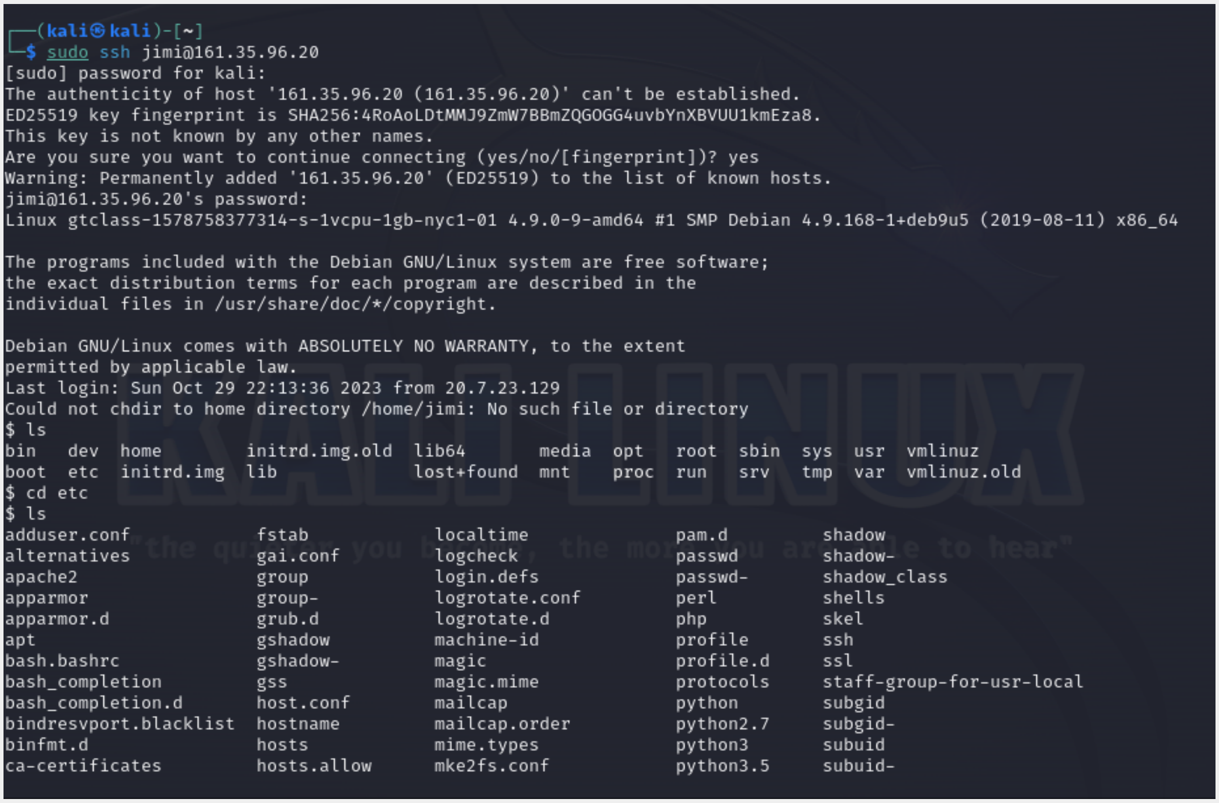
Layer 4 has protocols TCP and UDP and TCP makes a connection via the 3 way handshake (SYN/ACK)

3. Mitigation suggestions (if needed):

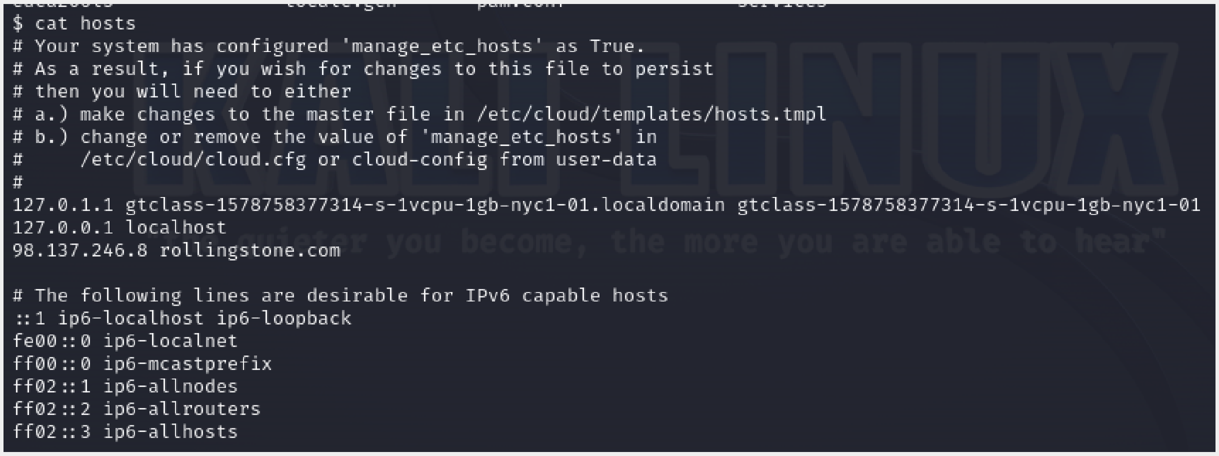
Close port 22 so no one can access the systems via ssh outside the network

Phase 3: *“I Feel a DNS Change Comin’ On”*

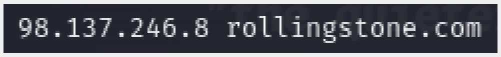
1. Summarize your findings about why access to rollingstone.com is not working as expected from the RockStar Corp Hollywood office:



```
┌──(kali㉿kali)-[~]
└─$ sudo ssh jimi@161.35.96.20
[sudo] password for kali:
The authenticity of host '161.35.96.20 (161.35.96.20)' can't be established.
ED25519 key fingerprint is SHA256:4RoAoLDtMMJ9ZmW7BBmZQGOGG4uvbYnXBVUU1kmEza8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '161.35.96.20' (ED25519) to the list of known hosts.
jimi@161.35.96.20's password:
Linux gtclass-1578758377314-s-1vcpu-1gb-nyc1-01 4.9.0-9-amd64 #1 SMP Debian 4.9.168-1+deb9u5 (2019-08-11) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Oct 29 22:13:36 2023 from 20.7.23.129
Could not chdir to home directory /home/jimi: No such file or directory
$ ls
bin   dev  home        initrd.img.old  lib64       media  opt   root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lib             lost+found  mnt    proc  run   srv   tmp  var  vmlinuz.old
$ cd etc
$ ls
adduser.conf             fstab          localtime          pam.d        shadow
alternatives             gai.conf       logcheck           passwd       shadow-
apache2                  group          login.defs         passwd-      shadow_class
apparmor                 group-         logrotate.conf     perl         shells
apparmor.d               grub.d         logrotate.d        php          skel
apt                      gshadow        machine-id         profile      ssh
bash.bashrc              gshadow-       magic              profile.d    ssl
bash_completion          gss            magic.mime         protocols    staff-group-for-usr-local
bash_completion.d        host.conf      mailcap            python       subgid
bindresvport.blacklist   hostname       mailcap.order      python2.7    subgid-
binfmt.d                 hosts          mime.types         python3      subuid
ca-certificates          hosts.allow    mke2fs.conf        python3.5    subuid-
```



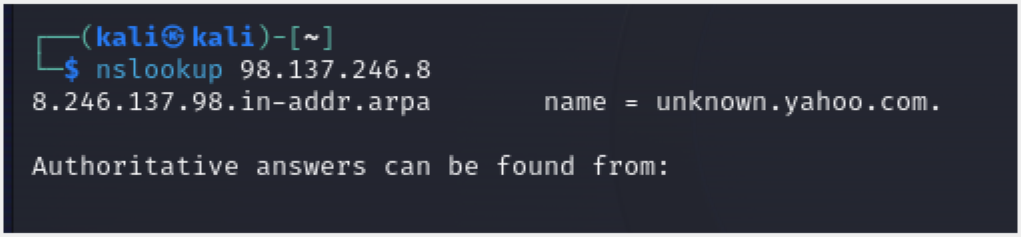
```
$ cat hosts
# Your system has configured 'manage_etc_hosts' as True.
# As a result, if you wish for changes to this file to persist
# then you will need to either
# a.) make changes to the master file in /etc/cloud/templates/hosts.tmpl
# b.) change or remove the value of 'manage_etc_hosts' in
#     /etc/cloud/cloud.cfg or cloud-config from user-data
#
127.0.1.1 gtclass-1578758377314-s-1vcpu-1gb-nyc1-01.localdomain gtclass-1578758377314-s-1vcpu-1gb-nyc1-01
127.0.0.1 localhost
98.137.246.8 rollingstone.com

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```



```
98.137.246.8 rollingstone.com
```

The hacker had changed the IP address hence you cannot access rollingstone.com

2. Command used to query Domain Name System records:



```
┌──(kali㉿kali)-[~]
└─$ nslookup 98.137.246.8
8.246.137.98.in-addr.arpa       name = unknown.yahoo.com.

Authoritative answers can be found from:
```

```
nslookup 98.137.246.8
```

3. Domain name findings:

```
unknown.yahoo.com
```

4. Explain what OSI layer DNS runs on:

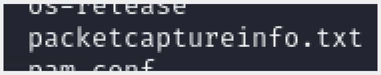
```
Layer 7 - The application layer
```

5. Mitigation suggestions (if needed):

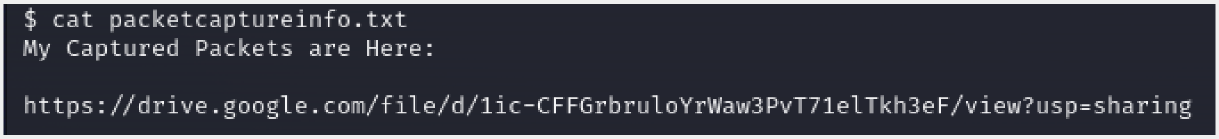
```
  1. Change the IP address back
  2. Close Port 22 to disallow access to SSH from outside the network
```

Phase 4: *"ShARP Dressed Man"*

1. Name of file containing packets:



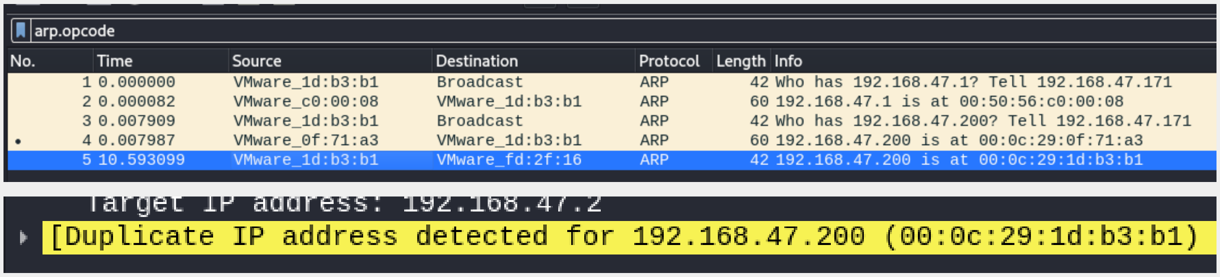
```
os-release
packetcaptureinfo.txt
pam.conf
```



```
$ cat packetcaptureinfo.txt
My Captured Packets are Here:

https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=sharing
```

```
https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view
secretlogs.pcapng
```

2. ARP findings identifying the hacker's MAC address:

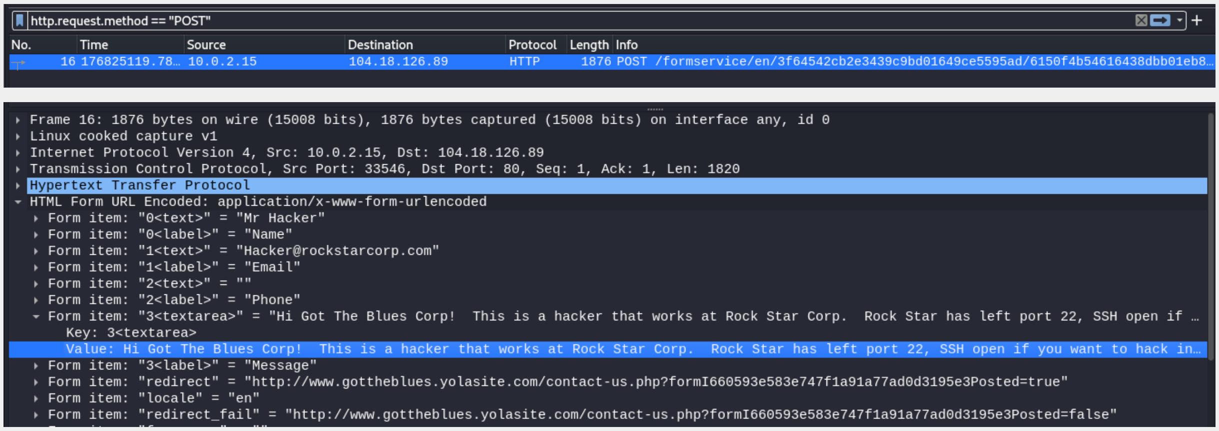


```
arp.opcode
No.   Time       Source            Destination       Protocol Length Info
    1 0.000000   VMware_1d:b3:b1   Broadcast         ARP          42 Who has 192.168.47.1? Tell 192.168.47.171
    2 0.000082   VMware_c0:00:08   VMware_1d:b3:b1   ARP          60 192.168.47.1 is at 00:50:56:c0:00:08
    3 0.007909   VMware_1d:b3:b1   Broadcast         ARP          42 Who has 192.168.47.200? Tell 192.168.47.171
•   4 0.007987   VMware_0f:71:a3   VMware_1d:b3:b1   ARP          60 192.168.47.200 is at 00:0c:29:0f:71:a3
    5 10.593099  VMware_1d:b3:b1   VMware_fd:2f:16   ARP          42 192.168.47.200 is at 00:0c:29:1d:b3:b1
```

```
    Target IP address: 192.168.47.2
  [Duplicate IP address detected for 192.168.47.200 (00:0c:29:1d:b3:b1)
```

```
00:0c:29:1d:b3:b1
```

3. HTTP findings, including the message from the hacker:



```
http.request.method == "POST"
No.  Time              Source     Destination    Protocol Length Info
  16 176825119.78…  10.0.2.15  104.18.126.89  HTTP       1876 POST /formservice/en/3f64542cb2e3439c9bd01649ce5595ad/6150f4b54616438dbb01eb8…
```

```
Frame 16: 1876 bytes on wire (15008 bits), 1876 bytes captured (15008 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 104.18.126.89
Transmission Control Protocol, Src Port: 33546, Dst Port: 80, Seq: 1, Ack: 1, Len: 1820
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "0<text>" = "Mr Hacker"
  Form item: "0<label>" = "Name"
  Form item: "1<text>" = "Hacker@rockstarcorp.com"
  Form item: "1<label>" = "Email"
  Form item: "2<text>" = ""
  Form item: "2<label>" = "Phone"
  Form item: "3<textarea>" = "Hi Got The Blues Corp!  This is a hacker that works at Rock Star Corp.  Rock Star has left port 22, SSH open if …
    Key: 3<textarea>
    Value: Hi Got The Blues Corp!  This is a hacker that works at Rock Star Corp.  Rock Star has left port 22, SSH open if you want to hack in…
  Form item: "3<label>" = "Message"
  Form item: "redirect" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=true"
  Form item: "locale" = "en"
  Form item: "redirect_fail" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=false"
```

```
"Hi Got The Blues Corp!  This is a hacker that works at Rock Star Corp.
Rock Star has left port 22, SSH open if you want to hack in.  For 1 Milliion
Dollars I will provide you the user and password!"
```

4. Explain the OSI layers for HTTP and ARP.

   a. Layer used for HTTP:

```
Layer 7 - The Application Layer
```

   b. Layer used for ARP:

```
Layer 2 - The Data Link Layer
```

5. Mitigation suggestions (if needed):

```
1. Close Port 22
2. Do not use your surname as your password aka Jimi Hendrix
3. No outside access unless via VPN
4. Create logs and ensure proper access and not a general admin like Jimi
```