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:

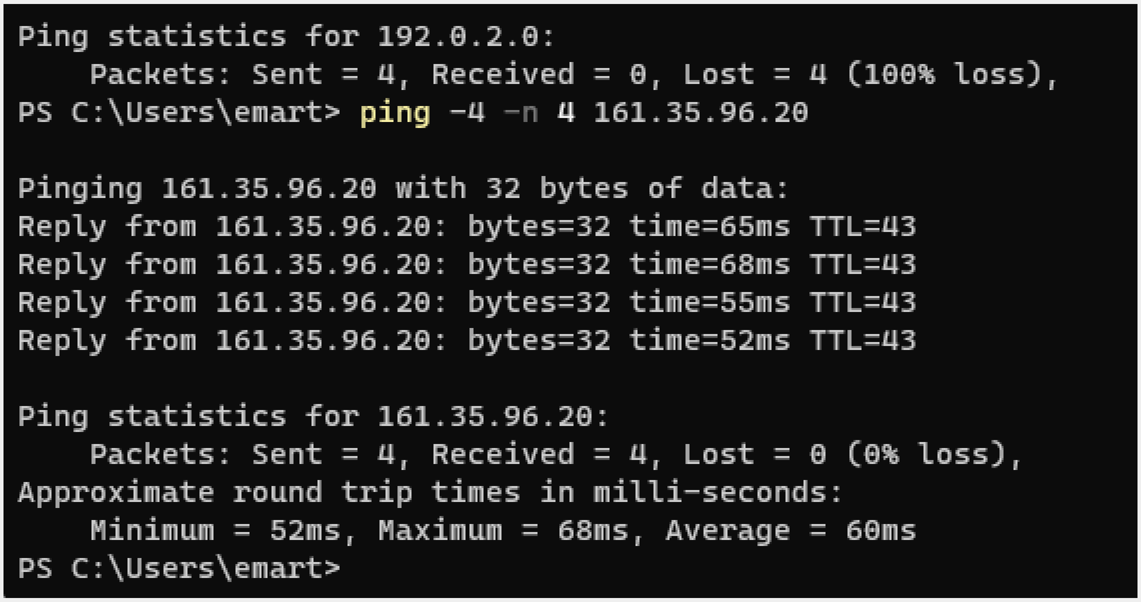
```
Ping 15.199.95.91
sping -4 -n 4 161.35.96.20
```

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

```
15.199.95.91 100% Loss; unreachable
15.199.94.91 100% Loss; unreachable
203.0.113.32 100% Loss; unreachable
161.35.96.20  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) is alive
192.0.2.0 100% Loss; unreachable
```

3. List of IPs responding to echo requests:

```
161.35.96.20  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss) is alive
```



```
Ping statistics for 192.0.2.0:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\emart> ping -4 -n 4 161.35.96.20

Pinging 161.35.96.20 with 32 bytes of data:
Reply from 161.35.96.20: bytes=32 time=65ms TTL=43
Reply from 161.35.96.20: bytes=32 time=68ms TTL=43
Reply from 161.35.96.20: bytes=32 time=55ms TTL=43
Reply from 161.35.96.20: bytes=32 time=52ms TTL=43

Ping statistics for 161.35.96.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 52ms, Maximum = 68ms, Average = 60ms
PS C:\Users\emart>
```

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

```
The ICPM Used for Pinging IP Addresses operates at the Network Layer of the
OSI model. Which is responsible for routing and forwarding data packets
between different network management and diagnostics, like, ping,
traceroute, and error reporting.
```

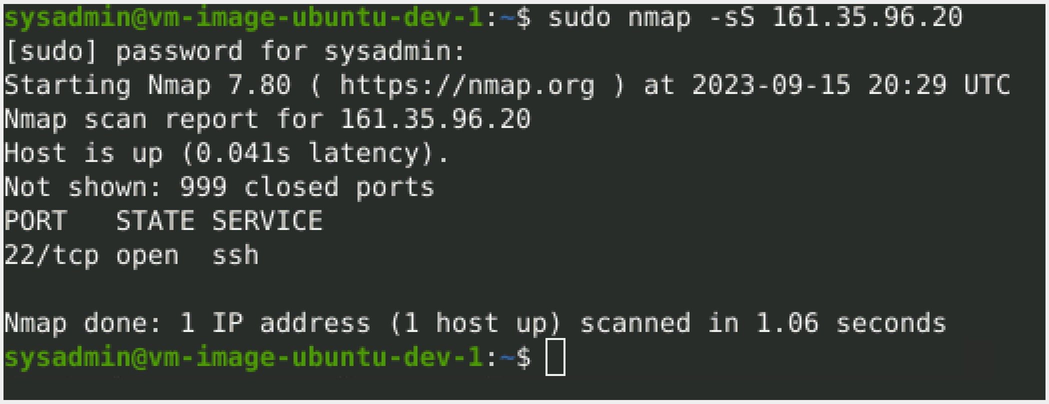
5. Mitigation recommendations (if needed):

```
To prevent an IP address from responding to a ping request, you can
implement firewall rules: by blocking ICMP requests packets; or the settings
of the nodes associated with that IP address.
```

Phase 2: *“Some SYN for Nothin’”*

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

```
Port 22 is the only one open.
```



```
sysadmin@vm-image-ubuntu-dev-1:~$ sudo nmap -sS 161.35.96.20
[sudo] password for sysadmin:
Starting Nmap 7.80 ( https://nmap.org ) at 2023-09-15 20:29 UTC
Nmap scan report for 161.35.96.20
Host is up (0.041s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 1.06 seconds
sysadmin@vm-image-ubuntu-dev-1:~$
```

2. Which OSI layer do SYN scans run on?

    a. OSI layer:

Transport Layer(layer 4). Responsible for determining which ports on a target system are open or closed.

    b. Explain how you determined which layer:

In a syn scan, the scanner sends TCP SYN packets to various ports on the target system. The behavior of the target system in response to these SYN packets helps the scanner identify which port is open and which are closed. This TCP protocol Operates at the Transport layer.

3. Mitigation suggestions (if needed):

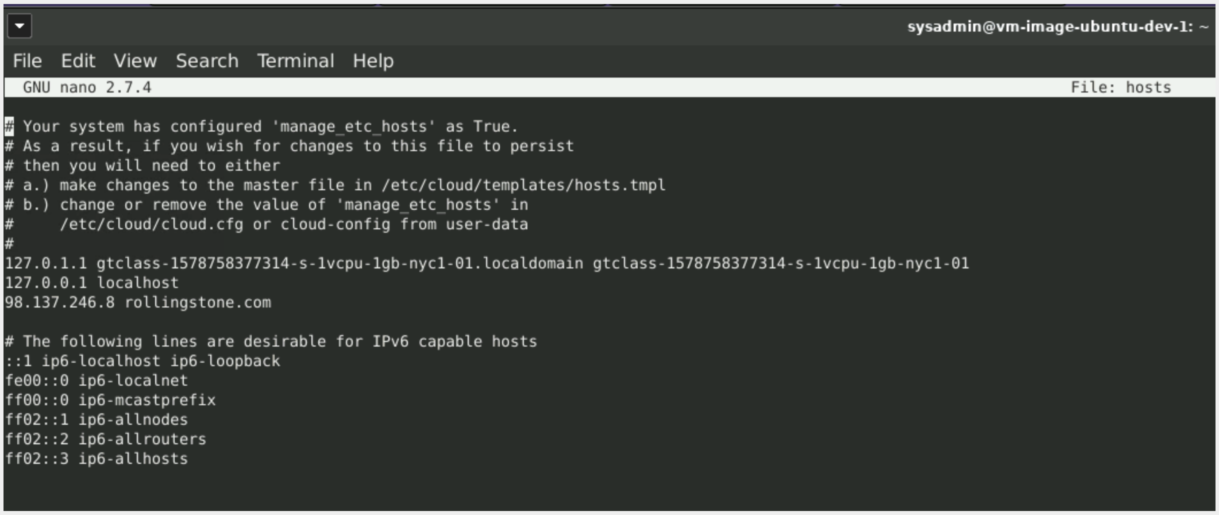
If the port is not in use,I Recommend to Disable traffic on ssh port 22, by adjusting the firewall rules. Or we can add an extra layer of security like multifactor authentication to avoid malicious characters.

```
On Linux with iptables: iptables -D
INPUT -p tcp —dport22 -j
ACCEPT to remove the ssh rule.
```

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:

```
Upon inspection of the ssh port22, we can see that rollingstone.com ip
address has been tampered with, therefore the original destination is not
found.
```

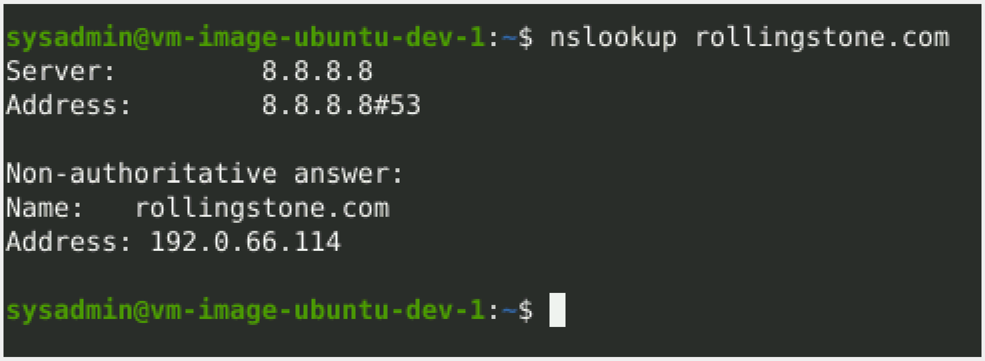


```
  GNU nano 2.7.4                                                          File: hosts

# 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
```

2. Command used to query Domain Name System records:

```
nslookup rollingstone.com
```

3. Domain name findings:



```
sysadmin@vm-image-ubuntu-dev-1:~$ nslookup rollingstone.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   rollingstone.com
Address: 192.0.66.114

sysadmin@vm-image-ubuntu-dev-1:~$ 
```

4. Explain what OSI layer DNS runs on:

```
DNS runs on layer 7 the Application Layer.
```

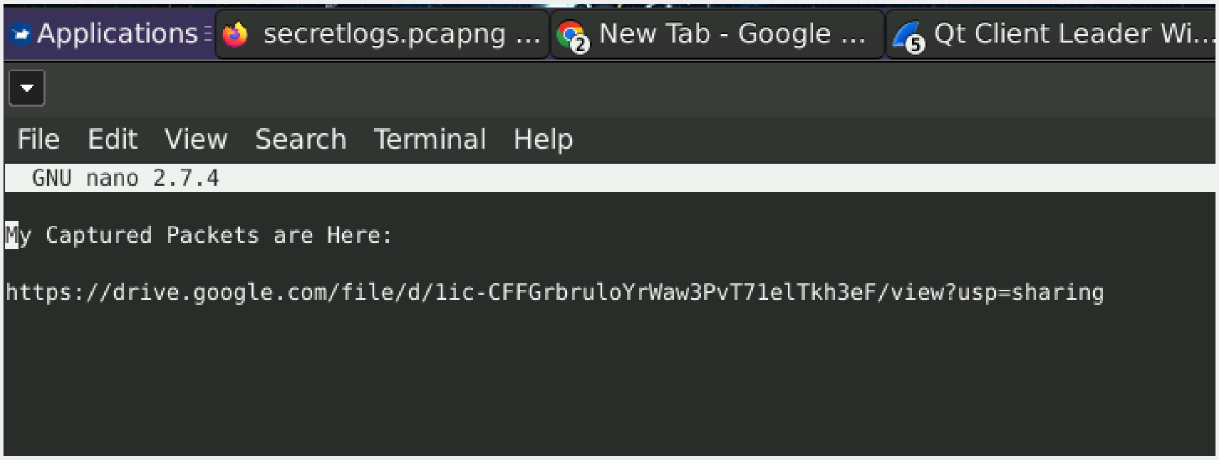
5. Mitigation suggestions (if needed):

```
Rockstar Corp should implement DNSSEC to add an additional layer of security
to DNS records, implement network traffic monitoring to detect any unusual
or malicious DNS queries or traffic patterns, Enable 2FA for your domain
registrar and DNS hosting accounts for extra security, limit access to DNS
settings by removing unnecessary users and restrict permissions to essential
personnel, educate staff for DNS security, phishing awareness and how to
recognize and report malicious activities, Regularly back up your DNS
settings and configurations so they can be readily available.
```

Phase 4: *"ShARP Dressed Man"*

1. Name of file containing packets:

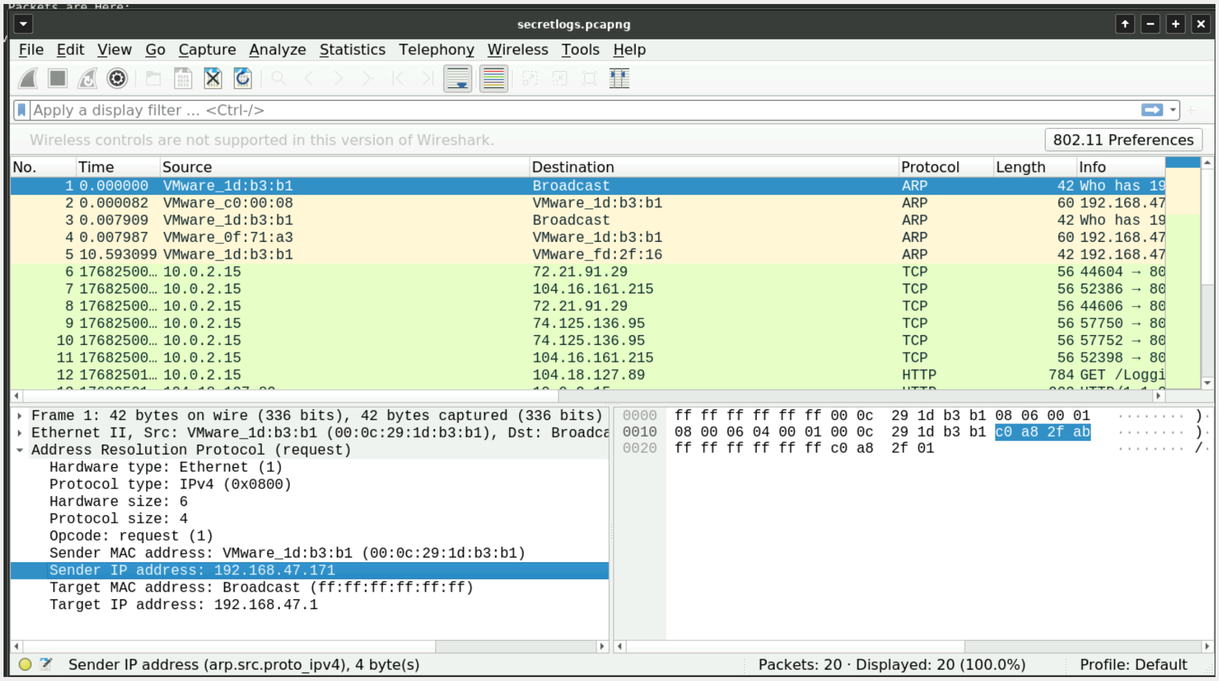
```
Packetcaptureinfo.txt
Inside ot the file there was a link to download the packets named
secretlogs.pcapng..
```



```
  GNU nano 2.7.4

My Captured Packets are Here:

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

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

```
Mac Address is 00:0c:29:1d:b3:b1
```



secretlogs.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Wireless controls are not supported in this version of Wireshark.
802.11 Preferences

```
No.  Time        Source            Destination        Protocol  Length  Info
   1 0.000000    VMware_1d:b3:b1   Broadcast          ARP           42 Who has 19
   2 0.000082    VMware_c0:00:08   VMware_1d:b3:b1    ARP           60 192.168.47
   3 0.007909    VMware_1d:b3:b1   Broadcast          ARP           42 Who has 19
   4 0.007987    VMware_0f:71:a3   VMware_1d:b3:b1    ARP           60 192.168.47
   5 10.593099   VMware_1d:b3:b1   VMware_fd:2f:16    ARP           42 192.168.47
   6 17682500…   10.0.2.15         72.21.91.29        TCP           56 44604 → 80
   7 17682500…   10.0.2.15         104.16.161.215     TCP           56 52386 → 80
   8 17682500…   10.0.2.15         72.21.91.29        TCP           56 44606 → 80
   9 17682500…   10.0.2.15         74.125.136.95      TCP           56 57750 → 80
  10 17682500…   10.0.2.15         74.125.136.95      TCP           56 57752 → 80
  11 17682500…   10.0.2.15         104.16.161.215     TCP           56 52398 → 80
  12 17682501…   10.0.2.15         104.18.127.89      HTTP         784 GET /Loggi
```

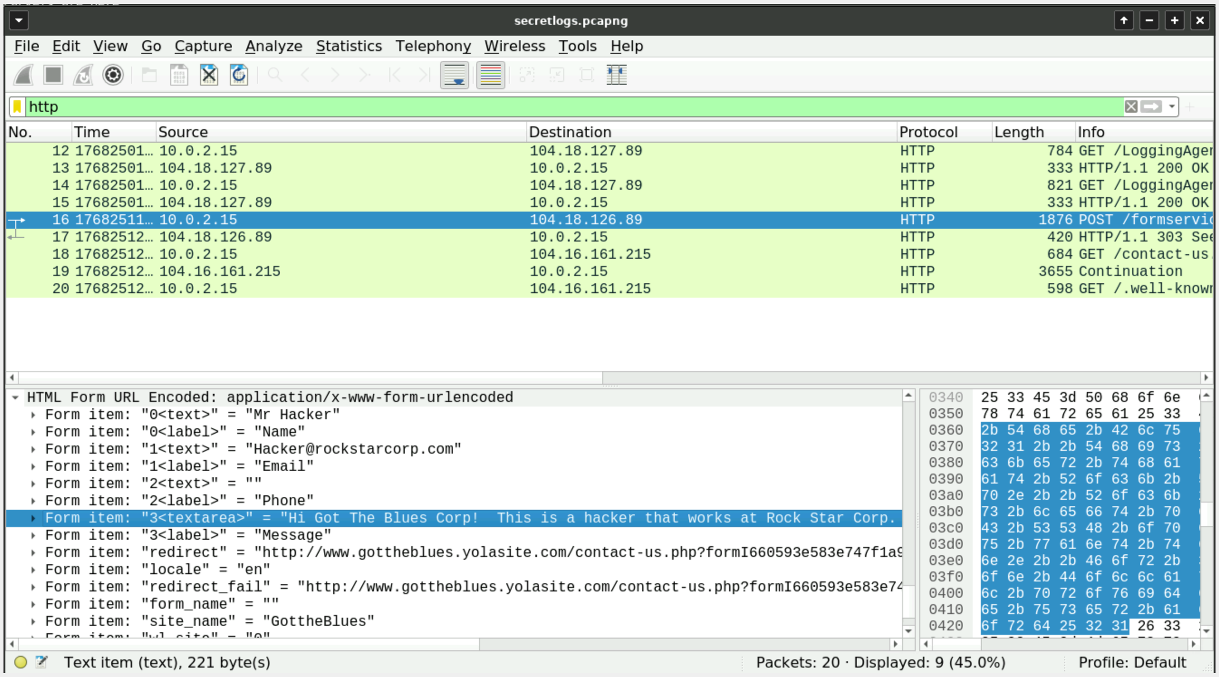
```
▸ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▸ Ethernet II, Src: VMware_1d:b3:b1 (00:0c:29:1d:b3:b1), Dst: Broadca
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: VMware_1d:b3:b1 (00:0c:29:1d:b3:b1)
    Sender IP address: 192.168.47.171
    Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
    Target IP address: 192.168.47.1
```

```
0000  ff ff ff ff ff ff 00 0c  29 1d b3 b1 08 06 00 01   ········ )·
0010  08 00 06 04 00 01 00 0c  29 1d b3 b1 c0 a8 2f ab   ········ )·
0020  ff ff ff ff ff ff c0 a8  2f 01                     ········ /·
```

Sender IP address (arp.src.proto_ipv4), 4 byte(s)   Packets: 20 · Displayed: 20 (100.0%)   Profile: Default

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

There was a message in the http: “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!”


secretlogs.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
```

```
No.   Time           Source          Destination      Protocol  Length Info
   12 17682501… 10.0.2.15       104.18.127.89    HTTP       784 GET /LoggingAger
   13 17682501… 104.18.127.89   10.0.2.15        HTTP       333 HTTP/1.1 200 OK
   14 17682501… 10.0.2.15       104.18.127.89    HTTP       821 GET /LoggingAger
   15 17682501… 104.18.127.89   10.0.2.15        HTTP       333 HTTP/1.1 200 OK
   16 17682511… 10.0.2.15       104.18.126.89    HTTP      1876 POST /formservic
   17 17682512… 104.18.126.89   10.0.2.15        HTTP       420 HTTP/1.1 303 See
   18 17682512… 10.0.2.15       104.16.161.215   HTTP       684 GET /contact-us.
   19 17682512… 104.16.161.215  10.0.2.15        HTTP      3655 Continuation
   20 17682512… 10.0.2.15       104.16.161.215   HTTP       598 GET /.well-known
```

```
▾ 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.
  ▸ Form item: "3<label>" = "Message"
  ▸ Form item: "redirect" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e747f1a9
  ▸ Form item: "locale" = "en"
  ▸ Form item: "redirect_fail" = "http://www.gottheblues.yolasite.com/contact-us.php?formI660593e583e74
  ▸ Form item: "form_name" = ""
  ▸ Form item: "site_name" = "GottheBlues"
```

```
0340  25 33 45 3d 50 68 6f 6e
0350  78 74 61 72 65 61 25 33
0360  2b 54 68 65 2b 42 6c 75
0370  32 31 2b 2b 54 68 69 73
0380  63 6b 65 72 2b 74 68 61
0390  61 74 2b 52 6f 63 6b 2b
03a0  70 2e 2b 2b 52 6f 63 6b
03b0  73 2b 6c 65 66 74 2b 70
03c0  43 2b 53 53 48 2b 6f 70
03d0  75 2b 77 61 6e 74 2b 74
03e0  6e 2e 2b 2b 46 6f 72 2b
03f0  6f 6e 2b 44 6f 6c 6c 61
0400  6c 2b 70 72 6f 76 69 64
0410  65 2b 75 73 65 72 2b 61
0420  6f 72 64 25 32 31 26 33
```

Text item (text), 221 byte(s)   Packets: 20 · Displayed: 9 (45.0%)   Profile: Default

4. Explain the OSI layers for HTTP and ARP.

   a. Layer used for HTTP:

```
Application Layer 7 Responsible for communication between web browsers and
web servers facilitating the transfer of web pages, txt, images and other
resources.
```

   b. Layer used for ARP:

```
Link Layer 2 ARP is used for mapping an IP address on a local network.
```

5. Mitigation suggestions (if needed):

```
For HTTP we can ensure to Use HTTPS to encrypt data in transit, Keep
security patches uptodate(regular updates), Web Application Firewall to
filter out malicious traffic and protect against multiple attacks.
For ARP we can implement Spoofing Detection mechanism like ARPwatch or IDS
to detect suspicious activity, Configure ARP static entries on critical
devices to prevent ARP poison attacks, and MAC filtering only allowed
authorized devices to communicate on the network.
```