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.

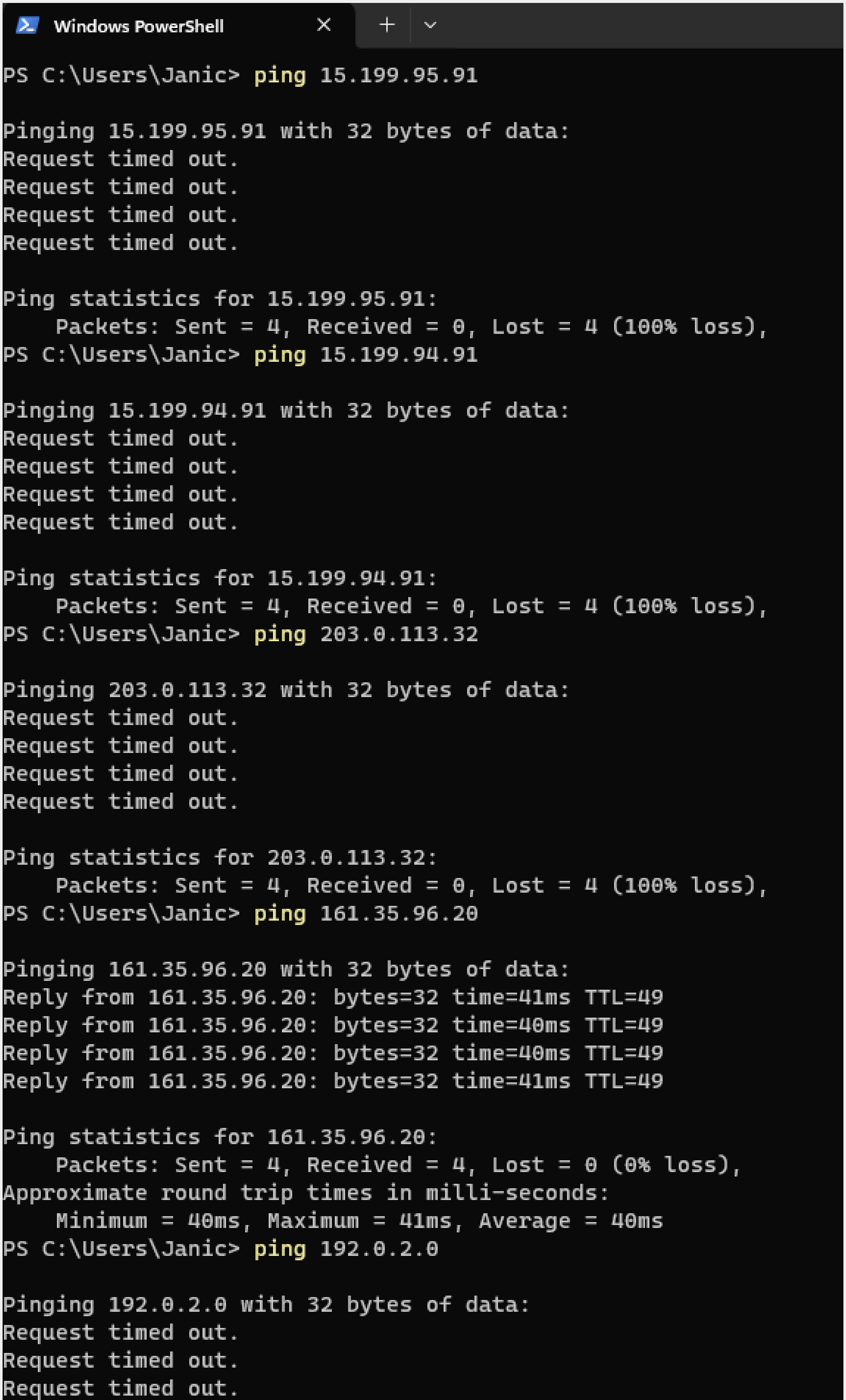
Phase 1: *"I'd like to Teach the World to `ping`"*

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

```
ping 15.199.95.91
ping 15.199.94.91
ping 203.0.113.32
ping 161.35.96.20
ping 192.0.2.0
```

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

```
All IPs except for one did not accept the connection and timed out. IP
161.35.96.20 generated a reply.
```



```
PS C:\Users\Janic> ping 15.199.95.91

Pinging 15.199.95.91 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 15.199.95.91:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\Janic> ping 15.199.94.91

Pinging 15.199.94.91 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 15.199.94.91:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\Janic> ping 203.0.113.32

Pinging 203.0.113.32 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 203.0.113.32:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\Janic> ping 161.35.96.20

Pinging 161.35.96.20 with 32 bytes of data:
Reply from 161.35.96.20: bytes=32 time=41ms TTL=49
Reply from 161.35.96.20: bytes=32 time=40ms TTL=49
Reply from 161.35.96.20: bytes=32 time=40ms TTL=49
Reply from 161.35.96.20: bytes=32 time=41ms TTL=49

Ping statistics for 161.35.96.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum = 41ms, Average = 40ms
PS C:\Users\Janic> ping 192.0.2.0

Pinging 192.0.2.0 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
```

3. List of IPs responding to echo requests:

```
161.35.96.20
```

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

```
Because the setting to allow/disallow a response is likely set by/in the
firewall &/or at the router, this would involve layer 3 (Network).
```

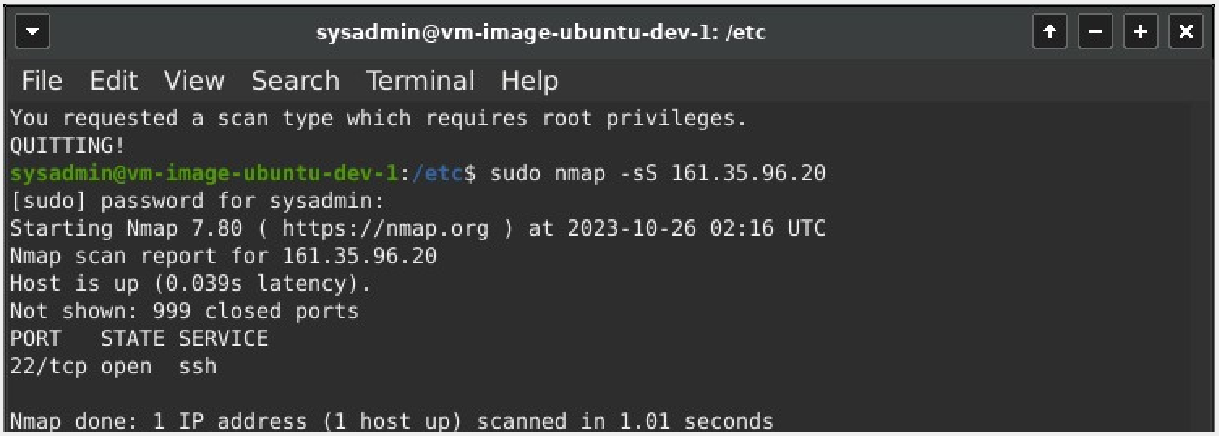
5. Mitigation recommendations (if needed):

```
The firewall should be configured to disable the ping response for the IP
161.35.96.20. Windows has a toggle for this in their Firewall. For linux, if
a csf firewall is installed, update the csf.conf file from ICMP_IN = “1” to
ICMP_IN = “0”. Alternaively, you could edit /etc/sysctl.conf to include the
following: “net.ipv4.icmp_echo_ignore_all = 1”.
```

Phase 2: *“Some SYN for Nothin’”*

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

```
Port 22 (ssh)
```


sysadmin@vm-image-ubuntu-dev-1: /etc
File Edit View Search Terminal Help

```
You requested a scan type which requires root privileges.
QUITTING!
sysadmin@vm-image-ubuntu-dev-1:/etc$ sudo nmap -sS 161.35.96.20
[sudo] password for sysadmin:
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-26 02:16 UTC
Nmap scan report for 161.35.96.20
Host is up (0.039s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 1.01 seconds
```

2. Which OSI layer do SYN scans run on?

   a. OSI layer:

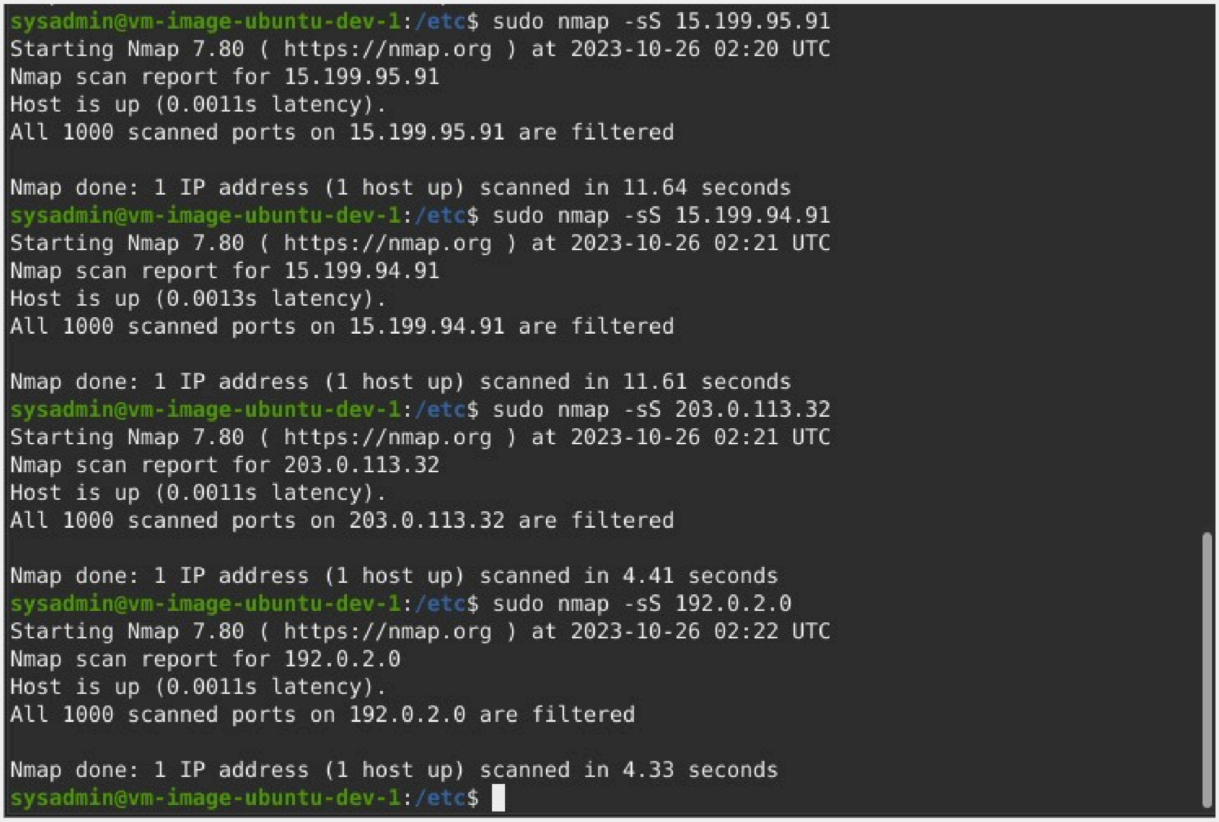
```
Layer 4 (Transport)
```

b. Explain how you determined which layer:

```
The transport layer is responsible for assigning source and destination
ports,so determining which port is open/available for connection would be
part of this layer.
```

3. Mitigation suggestions (if needed):

```
One could either close or filter the port. Based on scans of the other IPs
provided, it appears the business uses filtering in most instances.
```



```
sysadmin@vm-image-ubuntu-dev-1:/etc$ sudo nmap -sS 15.199.95.91
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-26 02:20 UTC
Nmap scan report for 15.199.95.91
Host is up (0.0011s latency).
All 1000 scanned ports on 15.199.95.91 are filtered

Nmap done: 1 IP address (1 host up) scanned in 11.64 seconds
sysadmin@vm-image-ubuntu-dev-1:/etc$ sudo nmap -sS 15.199.94.91
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-26 02:21 UTC
Nmap scan report for 15.199.94.91
Host is up (0.0013s latency).
All 1000 scanned ports on 15.199.94.91 are filtered

Nmap done: 1 IP address (1 host up) scanned in 11.61 seconds
sysadmin@vm-image-ubuntu-dev-1:/etc$ sudo nmap -sS 203.0.113.32
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-26 02:21 UTC
Nmap scan report for 203.0.113.32
Host is up (0.0011s latency).
All 1000 scanned ports on 203.0.113.32 are filtered

Nmap done: 1 IP address (1 host up) scanned in 4.41 seconds
sysadmin@vm-image-ubuntu-dev-1:/etc$ sudo nmap -sS 192.0.2.0
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-26 02:22 UTC
Nmap scan report for 192.0.2.0
Host is up (0.0011s latency).
All 1000 scanned ports on 192.0.2.0 are filtered

Nmap done: 1 IP address (1 host up) scanned in 4.33 seconds
sysadmin@vm-image-ubuntu-dev-1:/etc$
```

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:

```
/etc/hosts has been edited to include “98.137.246.8 rollingstone.com” which
will redirect any traffic aimed at rollingstone.com to the IP 98.137.246.8
```

2. Command used to query Domain Name System records:

```
Nslookup 98.137.246.8
```

3. Domain name findings:

```
unknown.yahoo.com
```

4. Explain what OSI layer DNS runs on:

```
DNS runs on layer 7 (application). The domain name that the user interacts
with in their browser is linked to the specific IP of the site using DNS.
DNS translates the domain name to the IP.
```

5. Mitigation suggestions (if needed):

```
Remove the edited line in the hosts configuration file. Scan for and remove
malware which may have been placed on the machine to replicate the edit. Set
up a DNS security extension to authenticate DNS entries.
```

Phase 4: *“ShARP Dressed Man”*

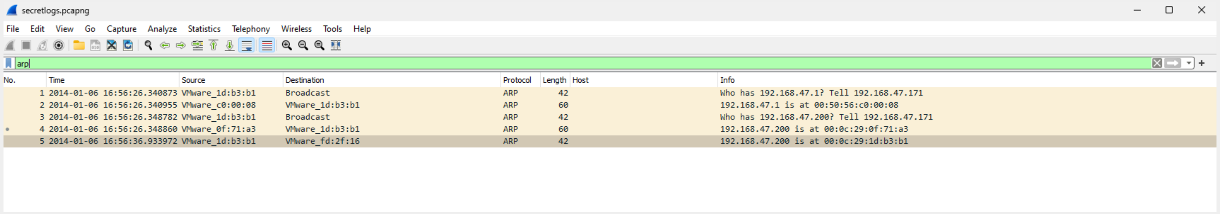
1. Name of file containing packets:

```
packetcaptureinfo.txt
Includes the link
https://drive.google.com/file/d/1ic-CFFGrbruloYrWaw3PvT71elTkh3eF/view?usp=s
haring

File: secretlogs.pcapng
```

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

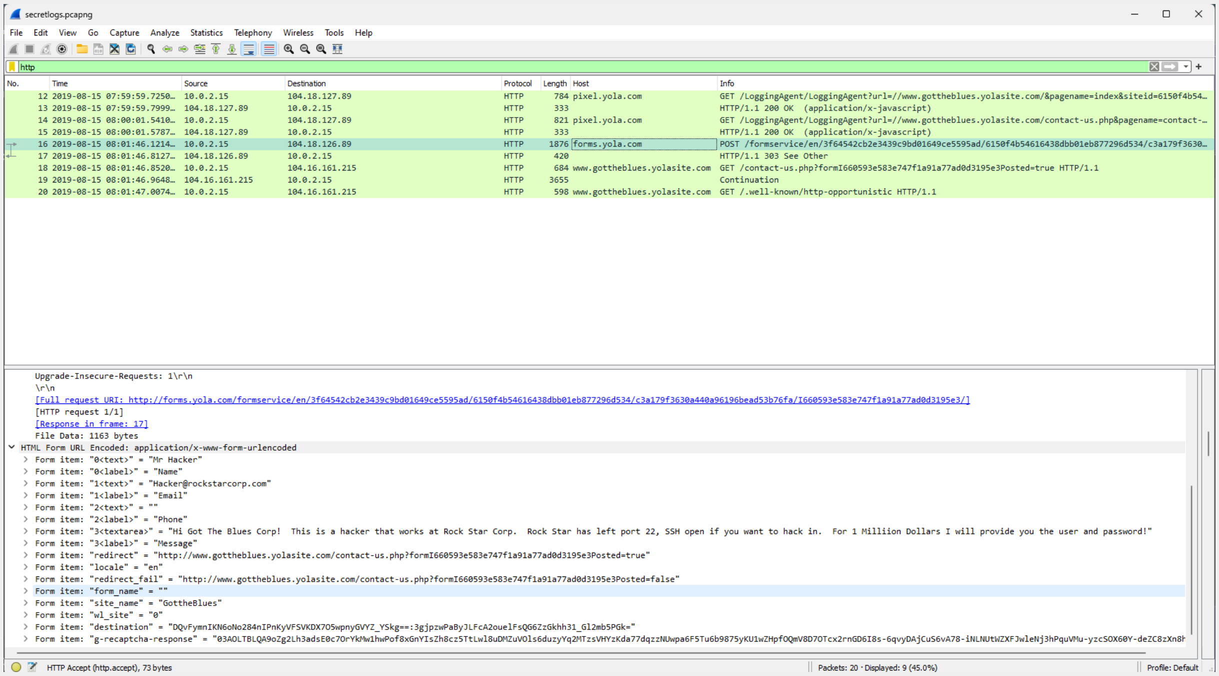
192.168.47.171


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

```
No.  Time                       Source            Destination       Protocol Length Host  Info
   1 2014-01-06 16:56:26.340873 VMware_1d:b3:b1   Broadcast         ARP      42           Who has 192.168.47.1? Tell 192.168.47.171
   2 2014-01-06 16:56:26.340955 VMware_c0:00:08   VMware_1d:b3:b1   ARP      60           192.168.47.1 is at 00:50:56:c0:00:08
   3 2014-01-06 16:56:26.348782 VMware_1d:b3:b1   Broadcast         ARP      42           Who has 192.168.47.200? Tell 192.168.47.171
   4 2014-01-06 16:56:26.348860 VMware_0f:71:a3   VMware_1d:b3:b1   ARP      60           192.168.47.200 is at 00:0c:29:0f:71:a3
   5 2014-01-06 16:56:36.933972 VMware_1d:b3:b1   VMware_fd:2f:16   ARP      42           192.168.47.200 is at 00:0c:29:1d:b3:b1
```

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

The hacker visited gottheblues.com and submitted an email via their forums: "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 Host                        Info
  12 2019-08-15 07:59:59.7250… 10.0.2.15       104.18.127.89   HTTP     784 pixel.yola.com               GET /LoggingAgent/LoggingAgent?url=//www.gottheblues.yolasite.com/&pagename=index&siteid=6150f4b54…
  13 2019-08-15 07:59:59.7999… 104.18.127.89   10.0.2.15       HTTP     333                              HTTP/1.1 200 OK  (application/x-javascript)
  14 2019-08-15 08:00:01.5410… 10.0.2.15       104.18.127.89   HTTP     821 pixel.yola.com               GET /LoggingAgent/LoggingAgent?url=//www.gottheblues.yolasite.com/contact-us.php&pagename=contact-…
  15 2019-08-15 08:00:01.5787… 104.18.127.89   10.0.2.15       HTTP     333                              HTTP/1.1 200 OK  (application/x-javascript)
  16 2019-08-15 08:01:46.1214… 10.0.2.15       104.18.126.89   HTTP    1876 forms.yola.com               POST /formservice/en/3f64542cb2e3439c9bd01649ce5595ad/6150f4b54616438dbb01eb877296d534/c3a179f3630…
  17 2019-08-15 08:01:46.8127… 104.18.126.89   10.0.2.15       HTTP     420                              HTTP/1.1 303 See Other
  18 2019-08-15 08:01:46.8520… 10.0.2.15       104.16.161.215  HTTP     684 www.gottheblues.yolasite.com GET /contact-us.php?formI660593e583e747f1a91a77ad0d3195e3Posted=true HTTP/1.1
  19 2019-08-15 08:01:46.9648… 104.16.161.215  10.0.2.15       HTTP    3655                              Continuation
  20 2019-08-15 08:01:47.0074… 10.0.2.15       104.16.161.215  HTTP     598 www.gottheblues.yolasite.com GET /.well-known/http-opportunistic HTTP/1.1
```

```
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://forms.yola.com/formservice/en/3f64542cb2e3439c9bd01649ce5595ad/6150f4b54616438dbb01eb877296d534/c3a179f3630a440a96196bead53b76fa/I660593e583e747f1a91a77ad0d3195e3/]
    [HTTP request 1/1]
    [Response in frame: 17]
    File Data: 1163 bytes
⌄ 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 you want to hack in.  For 1 Milliion Dollars I will provide you the user and password!"
  > 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"
  > Form item: "form_name" = ""
  > Form item: "site_name" = "GottheBlues"
  > Form item: "wl_site" = "0"
  > Form item: "destination" = "DQvFymnIKN6oNo284nIPnKyVFSVKDX7O5wpnyGVYZ_YSkg==:3gjpzwPaByJLFcA2ouelFsQG6ZzGkhh31_Gl2mb5PGk="
  > Form item: "g-recaptcha-response" = "03AOLTBLQA9oZg2Lh3adsE0c7OrYkMw1hwPof8xGnYIsZh8cz5TtLwl8uDMZuVOls6duzyYq2MTzsVHYzKda77dqzzNUwpa6F5Tu6b9875yKU1wZHpfOQmV8D7OTcx2rnGD6I8s-6qvyDAjCuS6vA78-iNLNUtWZXFJwleNj3hPquVMu-yzcSOX60Y-deZC8zXn8h
```

```
HTTP Accept (http.accept), 73 bytes          Packets: 20 · Displayed: 9 (45.0%)          Profile: Default
```

4. Explain the OSI layers for HTTP and ARP.

    a. Layer used for HTTP:

Layer 7 (application) http transmits information to/from browsers, the end user interface.

    b. Layer used for ARP:

```
Layer 2 (data link) arp comes into play when establishing the connection to
identify the MAC address associated with the IP so that data can be routed
to the proper machine within a network.
```

5. Mitigation suggestions (if needed):

```
If the mitigation suggestions from the previous sections are followed, there
should be no additional mitigation required at this stage as the means of
ingress the hacker is specifying in their message will have already been
addressed.
```

Sources:
Configuring IP to not respond to ping request:
https://neoserver.site/help/disablingenabling-ping-response-windows-server-2012-and-2016
https://monovm.com/blog/how-to-disable-ping-in-linux/#How-to-Disable/Stop-Ping-in-Linux?
DNS spoofing mitigation:
https://www.pandasecurity.com/en/mediacenter/dns-spoofing/