



Cybersecurity

Module 8 Challenge Submission File

Networking Fundamentals: Rocking your Network

Make a copy of this document to work in, and then 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 `fping` against the IP ranges:

```
fping 15.199.95.91 15.199.94.91 11.199.158.91 161.35.96.20 11.199.141.91
```

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

Determined after running that 161.35.96.20 is alive while the others are all unreachable

```
sysadmin@UbuntuDesktop:~$ fping 15.199.95.91 15.199.94.91 11.199.158.91 161.35.96.20 11.199.141.91
161.35.96.20 is alive
15.199.95.91 is unreachable
15.199.94.91 is unreachable
11.199.158.91 is unreachable
11.199.141.91 is unreachable
sysadmin@UbuntuDesktop:~$
```

Figure 1.

3. List of IPs responding to echo requests:

Ip address: 161.35.96.20

```
sysadmin@UbuntuDesktop:~$ fping -s 15.199.95.91 15.199.94.91 11.199.158.91 161.3
5.96.20 11.199.141.91
161.35.96.20 is alive
15.199.95.91 is unreachable
15.199.94.91 is unreachable
11.199.158.91 is unreachable
11.199.141.91 is unreachable

    5 targets
    1 alive
    4 unreachable
    0 unknown addresses

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

    52.4 ms (min round trip time)
    52.4 ms (avg round trip time)
    52.4 ms (max round trip time)
    4.129 sec (elapsed real time)

sysadmin@UbuntuDesktop:~$
```

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

For the reason that we are using ping, it is the network layer 3.

5. Mitigation recommendations (if needed):

Recommend to restrict ICMP privileges for 161.35.96.20 because that is a vulnerable entry point.

Phase 2: “Some SYN for Nothin`”

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

Port 22 is open, the ssh port

```
sysadmin@UbuntuDesktop:~$ sudo nmap -sS 161.35.96.20

Starting Nmap 7.60 ( https://nmap.org ) at 2022-11-02 23:51 EDT
Nmap scan report for 161.35.96.20
Host is up (0.0029s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 17.63 seconds
sysadmin@UbuntuDesktop:~$
```

2. Which OSI layer do SYN scans run on?

a. OSI Layer:

Layer 4 - Transport Layer

b. Explain how you determined which layer:

Because SYN is scanning ports, when scanning ports, ports are located in the transport layer of the OSI model, it determines which ports are open.

3. Mitigation suggestions (if needed):

Recommend closing the ssh port, as because it is open attackers can easily enter through.

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:

```
Within ssh jimi@161.35.96.20 -22:
Cd /etc
Nano hosts
98.137.246.8 rollingstone.com
```

Within my own system:

```
sysadmin@UbuntuDesktop:~$ nslookup rollingsstone.com
Server:      8.8.8.8
Address:     8.8.8.8#53

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

sysadmin@UbuntuDesktop:~$ nslookup 98.137.246.8
8.246.137.98.in-addr.arpa      name = unknown.yahoo.com.

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~$
```

When using nslookup, we can see that in the Rockstar corp server, the domain name is mapped to a different ip address to where the actual domain server for rollingsstone.com is located.

2. Command used to query Domain Name System records:

```
Nslookup -type=ns rollingsstone.com
```

Ns = specifies dns name server for named zone

3. Domain name findings:

```
sysadmin@UbuntuDesktop:~$ nslookup -type=ns rollingsstone.com
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
rollingsstone.com      nameserver = ns-1426.awsdns-50.org.
rollingsstone.com      nameserver = ns-2007.awsdns-58.co.uk.
rollingsstone.com      nameserver = ns-416.awsdns-52.com.
rollingsstone.com      nameserver = ns-718.awsdns-25.net.

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~$
```

4. Explain what OSI layer DNS runs on:

DNS runs on the Application layer 7 because it runs parallel to HTTP. It is called upon within the layer to aid HTTP in delivering the correct domain to address.

5. Mitigation suggestions (if needed):

[Enter text here]

Phase 4: “*ShARP Dressed Man*”

1. Name of file containing packets:

```
Cd etc  
Cat packetcaptureinfo.txt  
Open in google  
file name : secretlogs.pcapng
```

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

In the first arp on line 1, it shows the actual ip address and mac address to the rollingstone.com address being requested.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
arp						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	VMware_1d:b3:b1	Broadcast	ARP	42	Who has 192.168.47.1? Tell 192.168.47.17
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 192.168.47.17
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
Frame 5: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface unknown, id 1						
Ethernet II, Src: VMware_1d:b3:b1 (00:0c:29:1d:b3:b1), Dst: VMware_fd:2f:16 (00:50:56:fd:2f:16)						
Destination: VMware_fd:2f:16 (00:50:56:fd:2f:16)						
Address: VMware_fd:2f:16 (00:50:56:fd:2f:16)						
.....0..... = LG bit: Globally unique address (factory default)						
.....0..... = IG bit: Individual address (unicast)						
Source: VMware_1d:b3:b1 (00:0c:29:1d:b3:b1)						
Address: VMware_1d:b3:b1 (00:0c:29:1d:b3:b1)						
.....0..... = LG bit: Globally unique address (factory default)						
.....0..... = IG bit: Individual address (unicast)						
Type: ARP (0x0806)						
Address Resolution Protocol (reply)						
Hardware type: Ethernet (1)						
Protocol type: IPv4 (0x0800)						
Hardware size: 6						
Protocol size: 4						
Opcode: reply (2)						
Sender MAC address: VMware_1d:b3:b1 (00:0c:29:1d:b3:b1)						
Sender IP address: 192.168.47.200						
Target MAC address: VMware_fd:2f:16 (00:50:56:fd:2f:16)						
Target IP address: 192.168.47.2						
[Duplicate IP address detected for 192.168.47.200 (00:0c:29:1d:b3:b1) - also in use by 00:0c:29:0f:71:a3 (frame 4)]						
[Frame showing earlier use of IP address: 4]						
[Expert Info (Warning/Sequence): Duplicate IP address configured (192.168.47.200)]						
[Seconds since earlier frame seen: 10]						
0000	00 50 56 fd 2f 16 00 0c 29 1d b3 b1 08 06 00 01	.PV./... }.....				
0010	08 00 06 04 00 02 00 0c 29 1d b3 b1 c0 a8 2f c0 }... ..				
0020	00 50 56 fd 2f 16 c0 a8 2f 02	.PV./... /.				
Source Hardware Address (eth.src), 6 bytes						
Packets: 20 · Displayed: 5 (25.0%)				Profile: Default		

In line 4 of the first arp, we can see that the response back to the one who requested the arp is the rollingingstone.com address, the mac and ip address originally linked to it.

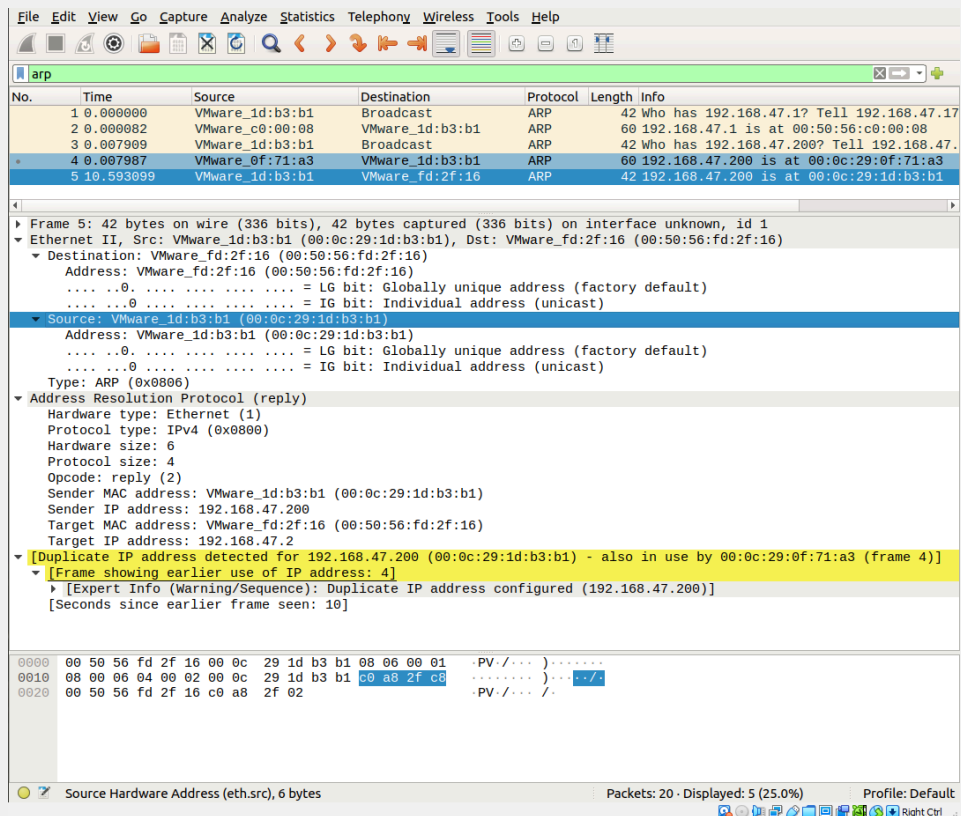
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
arp						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	VMware_id:b3:b1	Broadcast	ARP	42	Who has 192.168.47.1? Tell 192.168.47.17
2	0.000082	VMware_c0:00:08	VMware_id:b3:b1	ARP	60	192.168.47.1 is at 00:50:56:c0:00:08
3	0.007999	VMware_id:b3:b1	Broadcast	ARP	42	Who has 192.168.47.200? Tell 192.168.47.17
4	0.007987	VMware_0f:71:a3	VMware_id:b3:b1	ARP	60	192.168.47.200 is at 00:0c:29:0f:71:a3
5	10.593999	VMware_id:b3:b1	VMware_fd:2f:16	ARP	42	192.168.47.200 is at 00:0c:29:1d:b3:b1

Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface unknown, id 1	
Ethernet II, Src: VMware_0f:71:a3 (00:0c:29:0f:71:a3), Dst: VMware_id:b3:b1 (00:0c:29:1d:b3:b1)	
Destination: VMware_id:b3:b1 (00:0c:29:1d:b3:b1)	
Address: VMware_id:b3:b1 (00:0c:29:1d:b3:b1)	
...0. = LG bit: Globally unique address (factory default)	
...0. = IG bit: Individual address (unicast)	
Source: VMware_0f:71:a3 (00:0c:29:0f:71:a3)	
Address: VMware_0f:71:a3 (00:0c:29:0f:71:a3)	
...0. = LG bit: Globally unique address (factory default)	
...0. = IG bit: Individual address (unicast)	
Type: ARP (0x0806)	
Padding: 00000000000000000000000000000000	
Address Resolution Protocol (reply)	
Hardware type: Ethernet (1)	
Protocol type: IPv4 (0x0800)	
Hardware size: 6	
Protocol size: 4	
Opcode: reply (2)	
Sender MAC address: VMware_0f:71:a3 (00:0c:29:0f:71:a3)	
Sender IP address: 192.168.47.200	
Target MAC address: VMware_id:b3:b1 (00:0c:29:1d:b3:b1)	
Target IP address: 192.168.47.171	

0000	00 0c 29 1d b3 b1 00 0c 29 0f 71 a3 08 06 00 01	..).q...
0010	08 00 06 04 00 02 00 0c 29 0f 71 a3 c0 a8 2f c8}q.../
0020	00 0c 29 1d b3 b1 c0 a8 2f ab 00 00 00 00 00	..)...../.....
0030	00 00 00 00 00 00 00 00 00 00 00 00

Source Hardware Address (eth.src), 6 bytes Packets: 20 · Displayed: 5 (25.0%) Profile: Default

In line 5, that is where the hacker is spoofing their ip and mac address so that when you search rollingstone.com, you will end up on their site.



The hacker's MAC address is: 00:0c:29:1d:b3:b1

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

After looking through lines 12 - 15 the information looks normal and is what you would get from http request and response from the server.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
12	176825013.38	10.0.2.15	104.18.127.89	HTTP	784	GET /LoggingAgent/LoggingAgent?url=...
13	176825013.45	104.18.127.89	10.0.2.15	HTTP	333	HTTP/1.1 200 OK (application/x-jav...
14	176825015.20	10.0.2.15	104.18.127.89	HTTP	821	GET /LoggingAgent/LoggingAgent?url=...
15	176825015.23	104.18.127.89	10.0.2.15	HTTP	333	HTTP/1.1 200 OK (application/x-jav...
16	176825119.78	10.0.2.15	104.18.126.89	HTTP	1876	POST /formservice/en/3f64542cb2e34...
17	176825120.47	104.18.126.89	10.0.2.15	HTTP	420	HTTP/1.1 303 See Other

Frame 12: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface any, id 0

Linux cooked capture v1

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 104.18.127.89

Transmission Control Protocol, Src Port: 58610, Dst Port: 80, Seq: 1, Ack: 1, Len: 728

Hypertext Transfer Protocol

[truncated]GET /LoggingAgent/LoggingAgent?url=/www.gottheblues.yolasite.com/&pagename=index&siteid=6150f4b54616

[truncated]Expert Info (Chat/Sequence): GET /LoggingAgent/LoggingAgent?url=/www.gottheblues.yolasite.com/&pagename=index&siteid=6150f4b54616

Request Method: GET

Request URI [truncated]: /LoggingAgent/LoggingAgent?url=/www.gottheblues.yolasite.com/&pagename=index&siteid=6150f4b54616

Request Version: HTTP/1.1

Host: pixel.yola.com\r\n

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0\r\n

Accept: */*\r\n

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Referer: http://www.gottheblues.yolasite.com/\r\n

Cookie: cfduid=d8276a0af391153d2babc8fc7c64175b01565873955\r\n

0000 00 04 00 01 00 06 08 00 27 f8 42 a7 00 00 08 00B.....
 0010 45 00 03 00 cc e5 40 00 40 06 77 98 0a 00 02 0f E.....@.w.....
 0020 68 12 7f 59 e4 f2 00 50 9f 93 e0 1e 00 0b 6e b7 h..Y...P.....kn..
 0030 50 18 79 70 f6 0c 00 00 47 45 54 20 2f 4c 6f 67 P..y.l.. GET /Log..
 0040 67 69 6e 67 41 67 65 6e 74 2f 4c 6f 67 67 69 6e gAgent t/Loggin..
 0050 67 41 67 65 6e 74 3f 75 72 6c 3d 2f 2f 77 77 77 gAgent?u rl=/ww..
 0060 2e 67 6f 74 74 68 65 62 6c 75 65 73 2e 79 6f 6c .gottheb lues.yol..
 0070 61 73 69 74 65 2e 63 6f 6d 21 26 70 61 67 65 6e asite.co m/&pagen..
 0080 61 6d 65 3d 69 6e 64 65 78 26 73 69 74 65 69 64 ame=inde x&siteid..
 0090 3d 36 31 35 30 66 34 62 35 34 36 31 36 34 33 38 =6150f4b 54616438..
 00a0 64 62 30 31 65 62 38 37 37 32 39 36 34 35 33 dbb01eb8 77296d53..
 00b0 34 26 72 65 73 6f 6c 75 74 69 6f 6e 3d 31 33 36 &resolu tion=136..
 00c0 30 78 36 36 33 26 63 6f 6c 6f 72 44 65 70 74 68 0x663&co lorDepth..
 00d0 3d 32 34 26 66 6c 61 73 68 3d 30 26 6a 61 76 61 =24&flas h=&java..
 00e0 3d 30 26 73 69 74 65 72 65 66 65 72 65 72 3d 68 =0&siter eferer=h..
 00f0 74 74 70 25 33 41 2f 2f 77 77 77 2e 67 6f 74 74 ttp%3A// ww.w.gott..
 0100 68 65 62 6c 75 65 73 2e 79 6f 6c 61 73 69 74 65 heblues. yolasite..
 0110 2e 63 6f 6d 2f 26 76 69 73 69 74 6f 72 49 64 3d .com/&vi sitorId=

Hypertext Transfer Protocol: Protocol

Packets: 20 · Displayed: 9 (45.0%) Profile: Default

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
12	176825013.38	10.0.2.15	104.18.127.89	HTTP	784	GET /LoggingAgent/LoggingAgent?url=/www.gottheblues.yolasite.com/&pagename=index&siteid=6150f4b54616
13	176825013.45	104.18.127.89	10.0.2.15	HTTP	333	HTTP/1.1 200 OK (application/x-javascript)
14	176825015.20	10.0.2.15	104.18.127.89	HTTP	821	GET /LoggingAgent/LoggingAgent?url=/www.gottheblues.yolasite.com/contact-us.php&page...
15	176825015.23	104.18.127.89	10.0.2.15	HTTP	333	HTTP/1.1 200 OK (application/x-javascript)
16	176825119.78	10.0.2.15	104.18.126.89	HTTP	1876	POST /formservice/en/3f64542cb2e3439c9bd01649ce5595ad/6150f4b54616438dbb01eb877296d53...
17	176825120.47	104.18.126.89	10.0.2.15	HTTP	420	HTTP/1.1 303 See Other
18	176825120.51	10.0.2.15	104.16.101.215	HTTP	684	GET /contact-us.php?form1660593e583e747f1a91a77ad8d3195e3Posted=true HTTP/1.1

Frame 15: 333 bytes on wire (2664 bits), 333 bytes captured (2664 bits) on interface any, id 0

Linux cooked capture v1

Internet Protocol Version 4, Src: 104.18.127.89, Dst: 10.0.2.15

Transmission Control Protocol, Src Port: 80, Dst Port: 58610, Seq: 278, Ack: 1494, Len: 277

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Date: Thu, 15 Aug 2019 13:00:01 GMT\r\n

Content-Type: application/x-javascript\r\n

Content-Length: 32\r\n

Connection: keep-alive\r\n

Content-Encoding: gzip\r\n

Expires: -1\r\n

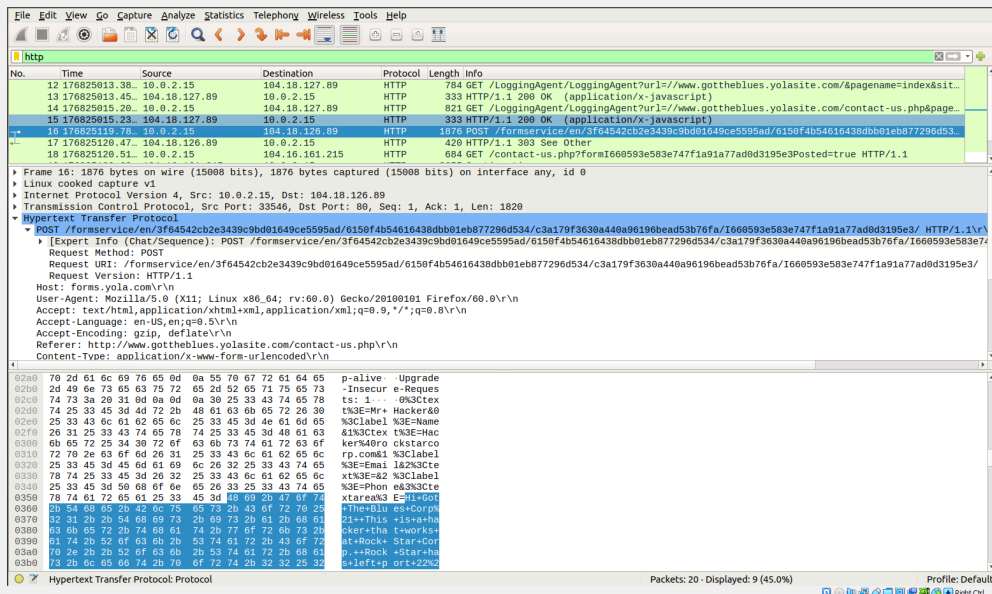
0000 00 00 00 01 00 06 52 54 00 12 35 02 00 00 00RT..S.....
 0010 45 00 01 3d 3f fe 00 00 40 06 46 43 68 12 7f 59 E...??...@.FCH..Y..
 0020 0a 00 02 0f 00 50 e4 f2 00 60 6f cc 9f 93 e5 f3P...ko.....
 0030 50 18 ff ff 3b 00 00 00 48 54 50 2f 31 2e 31 P...B... HTTP/1.1..
 0040 20 32 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 200 OK. Date: T..
 0050 68 75 2c 20 31 35 20 41 75 67 20 32 30 31 39 20 hu, 15 A ug 2019..
 0060 31 33 3a 30 30 3a 30 31 20 47 4d 54 6d 0a 43 6f 13:00:01 GMT. Co..
 0070 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c ntent-Ty pe: appl..
 0080 69 63 61 74 69 6f 6e 2f 70 2d 6a 61 76 61 73 63 ication/ x-javasc..
 0090 72 69 70 74 6d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 ript. Co ntent-Le..
 00a0 6e 67 74 60 3a 20 33 32 0d 0a 43 6f 6e 6e 65 63 nght: 32 .Connec..
 00b0 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 tion: ke ep-alive..
 00c0 0d 0a 43 6f 6e 74 65 6e 74 2d 45 6e 63 6f 64 69 .Conten t-Encodi..
 00d0 6e 67 3a 20 67 7a 69 70 0d 0a 45 70 69 72 65 ng: gzip .Expire..
 00e0 73 3a 20 2d 31 6d 0a 50 72 61 67 6d 61 3a 20 6e s: -1 P ragma: n..
 00f0 0f 2d 03 61 63 68 65 0d 0a 53 65 72 76 65 72 3a o-cache- Server:

Frame 333 bytes Uncompressed entity body (12 bytes)

Hypertext Transfer Protocol: Protocol

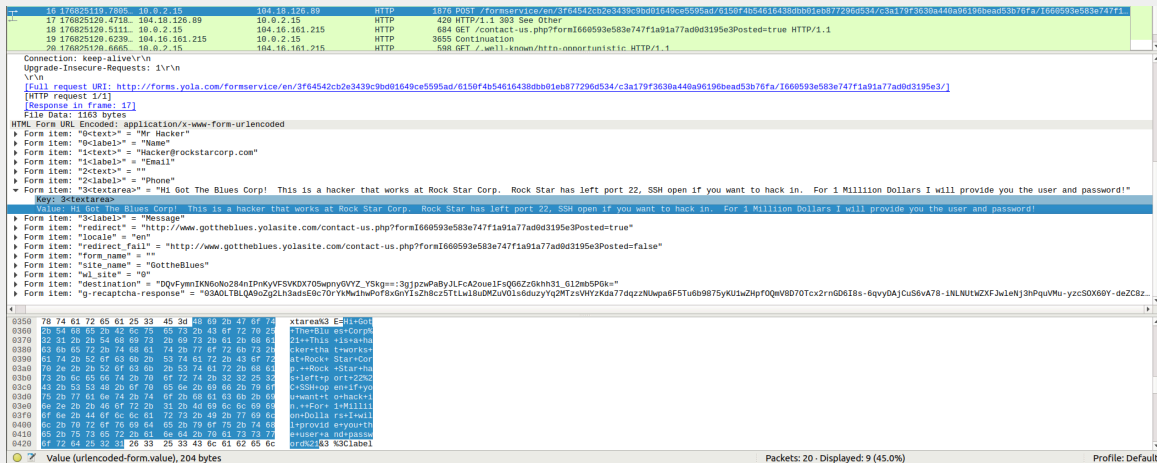
Packets: 20 · Displayed: 9 (45.0%) Profile: Default

At line 16, I can see that this is where the hacker has spoofed the ip so that when searching rollingstone.com, you end up on this site.



The hacker's message is:

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 Million Dollars I will provide you the user and password!



4. Explain the OSI layers for HTTP and ARP.

a. Layer used for HTTP:

HTTP uses the application layer 7 because the input to receive the information utilizes the application layer

b. Layer used for ARP:

ARP uses the data link layer 2 because it is used to map IP network addresses to the MAC address that is used by layer 2. MAC addresses are layer 2.

5. Mitigation suggestions (if needed):

Close port 22