

Key

I. Nmap Scan

- What is the total number of the "TCP Connect" scans?

```
tcp.flags.syn==1 and tcp.flags.ack==0 and tcp.window_size > 1024
```

Key: 1000

- Which scan type is used to scan the TCP port 80?

```
tcp.port == 80
```

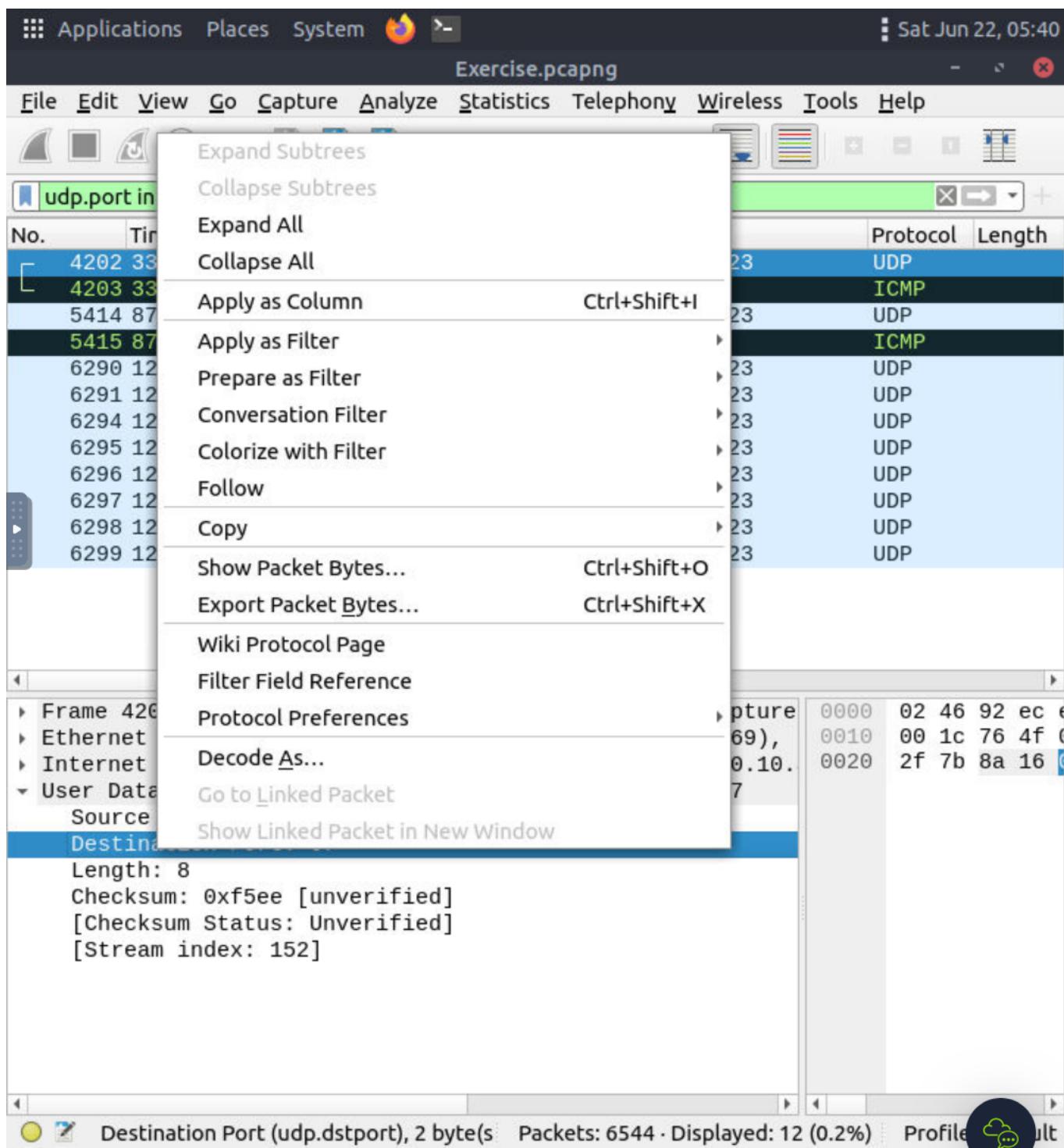
tcp.port == 80	
Destination Port	Info
42026 → 80	[SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 T...
80 → 42026	[SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SA...
42026 → 80	[ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=1438758499...
42026 → 80	[RST, ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=14387...
36044 → 80	[SYN] Seq=0 Win=1024 Len=0 MSS=1460
80 → 36044	[SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=8961
36044 → 80	[RST] Seq=1 Win=0 Len=0

- You can see result. It is TCP connect.

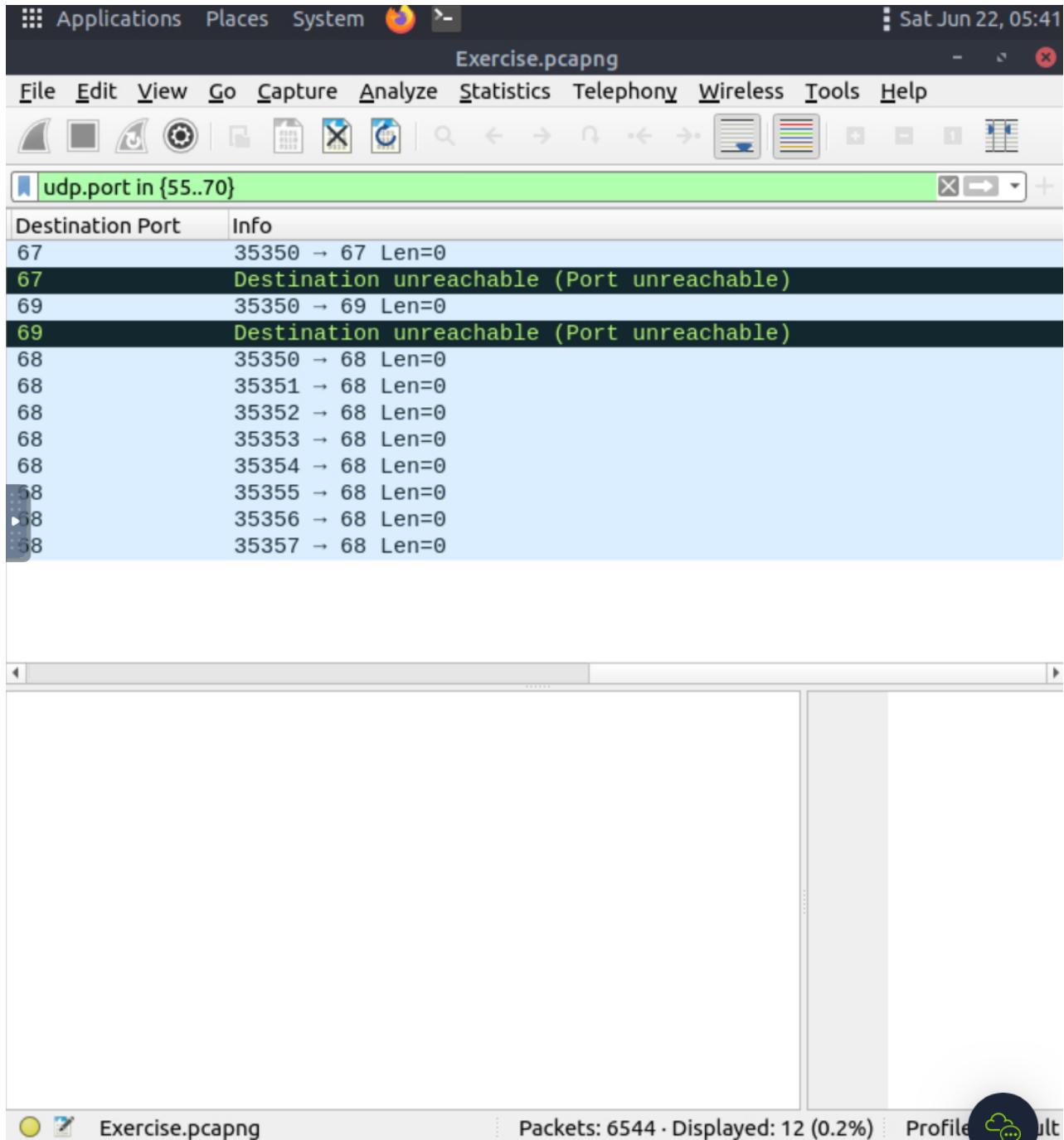
Key: TCP connect

- Which UDP port in the 55-70 port range is open?

```
udp.port in {55-70}
```



- Then choose *Apply as Column* for Destination port.



- As you can see, port 67 and 69 close. Port 68 open.

Key: 68

II. ARP Poisoning & Man In The Middle!

- What is the number of ARP requests crafted by the attacker?

- First find spoofing MAC address

```
arp.duplicate-address-detected or arp.duplicate-address-frame
```

- We find `00:0c:29:e2:18:b4` is duplicated more time.
- Find arp request crafted by the attacker:

```
((arp) && (arp.opcode == 1)) && (arp.src.hw_mac ==  
00:0c:29:e2:18:b4)
```

Key 284

2. What is the number of HTTP packets received by the attacker?

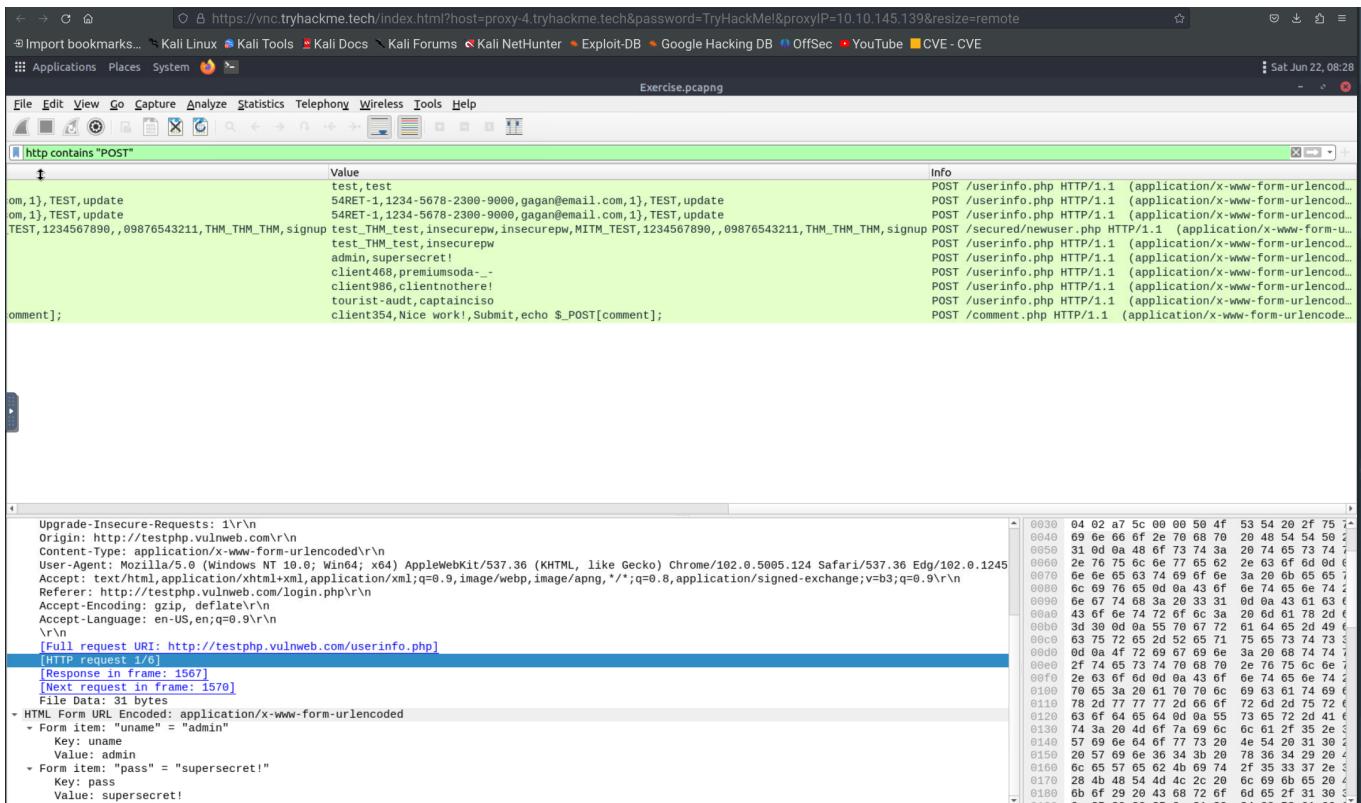
- Find anonymous ip of attacker and website.

```
http and ip.addr == 44.228.249.3 and ip.addr == 192.168.1.12
```

Key: 90

3. What is the number of sniffed username&password entries?

```
(http contain "POST") && (ip.addr == 192.168.1.12)
```



- Note `userinfo.php` and value. We can see username and pass but note 54RET.., it is not username and password. It logins using cookie so it is not user name and pass.

- After counteracting we find 6 username and password.

Key 6

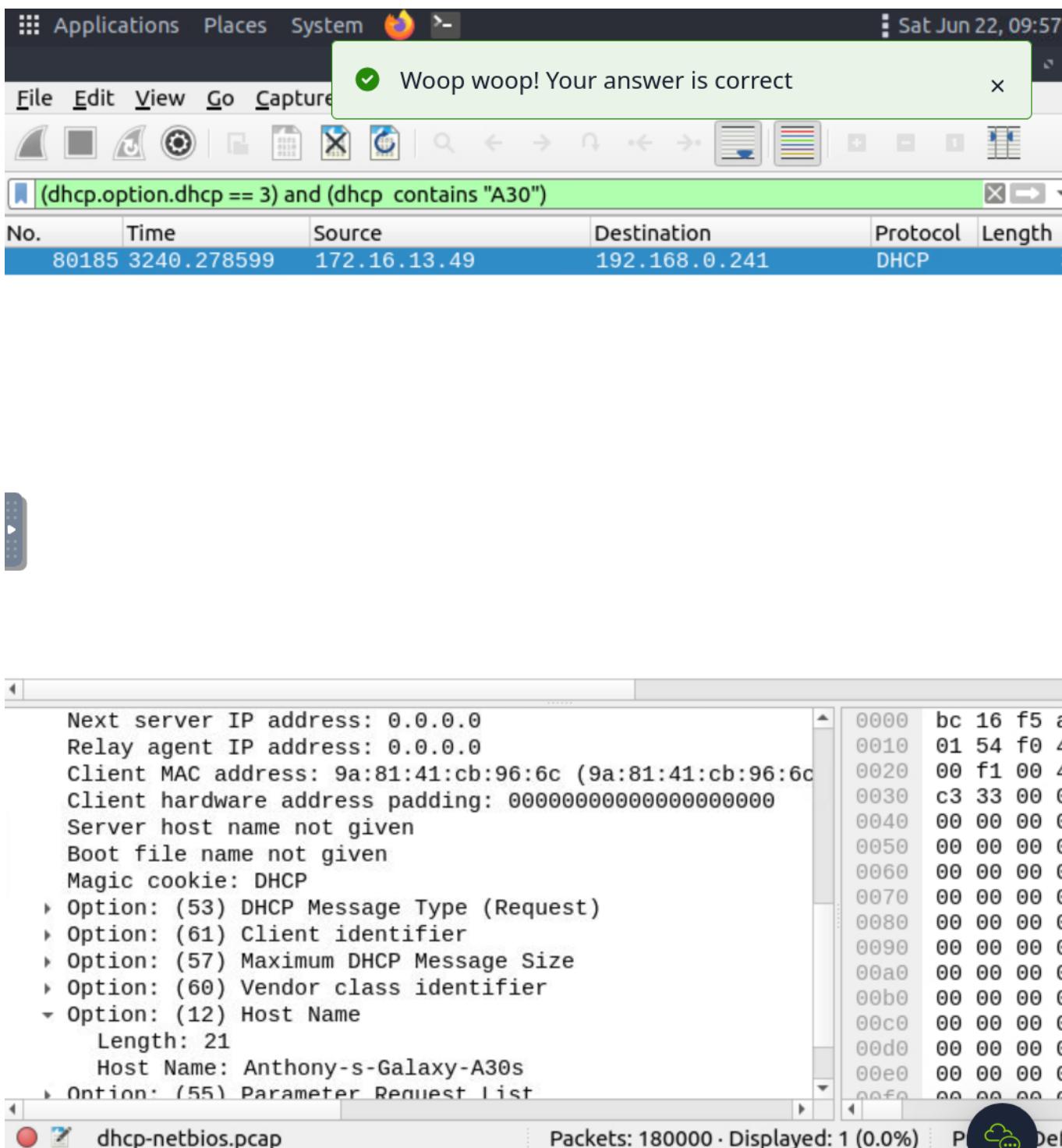
- See picture bellow to complete a rest of question.

III. Identifying Host: DHCP, NetBIOS, and Kerberos

1. What is the MAC address of the host "Galaxy A30"?

- **"DHCP Request"** packets contain the hostname information
- Filtering

(`dhcp.option.dhcp == 3`) and (`dhcp contains "A30"`)



2. How many NetBIOS registration requests does the "LIVALJM" workstation have?

- First, we can see queries name "LIVALJM". We start filter with "LIVALMJ"

```
nbns.name contains "LIVAJM"
```

- After filtering, we will see info column. It is not only containing opcode "Registration".

- Starting analysis. Go to a packet has opcode "Registration". We will see:

The screenshot shows two windows of Wireshark. On the left, a 'NetBIOS (NBNS) Analysis' pane displays information about NBNS, stating it's the technology for hosts to communicate. It includes sections for 'Global search.' and 'NBNS investigation in a nutshell'. The 'NBNS investigation in a nutshell' section contains a table with 'Notes' and a 'Wireshark Filter' column. The notes say 'Global search.' and the filter is set to 'nbns'. Below this, under 'NBNS' options, it says 'Queries: Query details.' and 'Query details could contain "name, Time to live (TTL) and IP address details"'. The right window shows a list of captured packets with a green highlight on the first few. A specific packet is selected, showing its details and bytes panes. The details pane shows a 'User Datagram Protocol, Src Port: 137, Dst Port: 137' with flags '0x2910'. The bytes pane shows the raw hex and ASCII data.

- Notice in Flags, we can see Opcode: Registration (5). Continuing filtering with command:

`nbns.name contains "LIVALJM" and nbns.flags.opcode == 5`

Key: 16

3. Which host requested the IP address "172.16.13.85"?

A challenge interface with a progress bar at 38%. It asks for the MAC address of the host "Galaxy A30?". A text input field contains "9a:81:41:cb:96:6c". Below it are 'Correct Answer' and 'Hint' buttons. Another question asks "How many NetBIOS registration requests does the "LIVALJM" workstation have?", with a text input field containing "16" and a 'Correct Answer' button. A third question asks "Which host requested the IP address "172.16.13.85?", with a text input field containing "Galaxy-A12" and a 'Correct Answer' button.

The screenshot shows a Wireshark capture window with a green highlight on a specific DHCP request packet. The details pane shows the packet number 72529, source 0.0.0.0, destination 255.255.255.255, and protocol DHCP. The bytes pane shows the raw hex and ASCII data. The packet is a DHCP request for option 54 (Requested IP Address), which is set to 172.16.13.85. A message box in the top right says "Woop woop! Your answer is correct".

4. What is the IP address of the user "u5"? (Enter the address in defanged format.)

Room progress (41%)

16 ✓ Correct Answer ✗ Hint

Which host requested the IP address "172.16.13.85"?

Galaxy-A12 ✓ Correct Answer

Use the "Desktop/exercise-pcaps/dhcp-netbios-kerberos/kerberos.pcap" file.
What is the IP address of the user "u5"? (Enter the address in defanged format.)

10[.]1[.]12[.]2 ✓ Correct Answer

What is the hostname of the available host in the Kerberos packets?

Answer format: *** ✗ Submit

Task 5 Tunneling Traffic: DNS and ICMP

Task 6 Cleartext Protocol Analysis: FTP

Task 7 Cleartext Protocol Analysis: HTTP

Task 8 Encrypted Protocol Analysis: Decrypting HTTPS

Task 9 Bonus: Hunt Cleartext Credentials!

Applications Places System Firefox Sat Jun 22, 10:50 kerberos.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

kerberos.CNameString contains "u5"

No.	Time	Source	Destination	Protocol	Length
19	72.033913	10.1.12.2	10.5.3.1	KRB5	1
20	72.033924	10.5.3.1	10.1.12.2	KRB5	1
22	72.115052	10.5.3.1	10.1.12.2	KRB5	1
23	73.140897	10.1.12.2	10.5.3.1	KRB5	1
24	73.140901	10.5.3.1	10.1.12.2	KRB5	1
25	73.166835	10.1.12.2	10.5.3.1	KRB5	1
26	73.166842	10.5.3.1	10.1.12.2	KRB5	1
27	73.494805	10.1.12.2	10.5.3.1	KRB5	1
28	73.494808	10.5.3.1	10.1.12.2	KRB5	1
29	73.732765	10.1.12.2	10.5.3.1	KRB5	1
30	73.732769	10.5.3.1	10.1.12.2	KRB5	1
31	74.030758	10.1.12.2	10.5.3.1	KRB5	1
32	74.030765	10.5.3.1	10.1.12.2	KRB5	1

req-body
Padding: 0
kdc-options: 40810010
cname
name-type: kRB5-NT-PRINCIPAL (1)
cname-string: 1 item CNameString: u5
realm: DENYDC
sname
name-type: kRB5-NT-SRV-INST (2)
sname-string: 2 items SNameString: krbtgt SNameString: DENYDC
till: 2027-09-13 02:48:05 (UTC)

CNameString (kerber...eString), 2 byte(s) Packets: 82 · Displayed: 13 (15.9%) Profile Result

Key: 10[.]1[.]12[.]2

5. What is the hostname of the available host in the Kerberos packets?

Room progress (44%)

Answer the questions below

Use the "Desktop/exercise-pcaps/dhcp-netbios-kerberos/dhcp-netbios.pcap" file.
What is the MAC address of the host "Galaxy A30"?

9a:81:41:cb:96:6c ✓ Correct Answer ✗ Hint

How many NetBIOS registration requests does the "LIVALJM" workstation have?

16 ✓ Correct Answer ✗ Hint

Which host requested the IP address "172.16.13.85"?

Galaxy-A12 ✓ Correct Answer

Use the "Desktop/exercise-pcaps/dhcp-netbios-kerberos/kerberos.pcap" file.
What is the IP address of the user "u5"? (Enter the address in defanged format.)

10[.]1[.]12[.]2 ✓ Correct Answer

What is the hostname of the available host in the Kerberos packets?

xp1\$ ✓ Correct Answer

Task 5 Tunneling Traffic: DNS and ICMP

Applications Places System Firefox Sat Jun 22, 10:50 kerberos.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

kerberos.CNameString contains "\$"

No.	Time	Source	Destination	Protocol	Length
8	0.653004	10.5.3.1	10.1.12.2	KRB5	1

User Datagram Protocol, Src Port: 88, Dst Port: 1065
Kerberos
tgs-rep
pvno: 5
msg-type: krb-tgs-rep (13)
realm: DENYDC.COM
cname
name-type: kRB5-NT-PRINCIPAL (1)
cname-string: 1 item CNameString: xp1\$
ticket
enc-part
etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
cipher: 61a5e49b6bb3b062e4be9f1262ecbeb20ad5d238c

CNameString (kerber...eString), 4 byte(s) Packets: 82 · Displayed: 1 (1.2%) Profile Result