

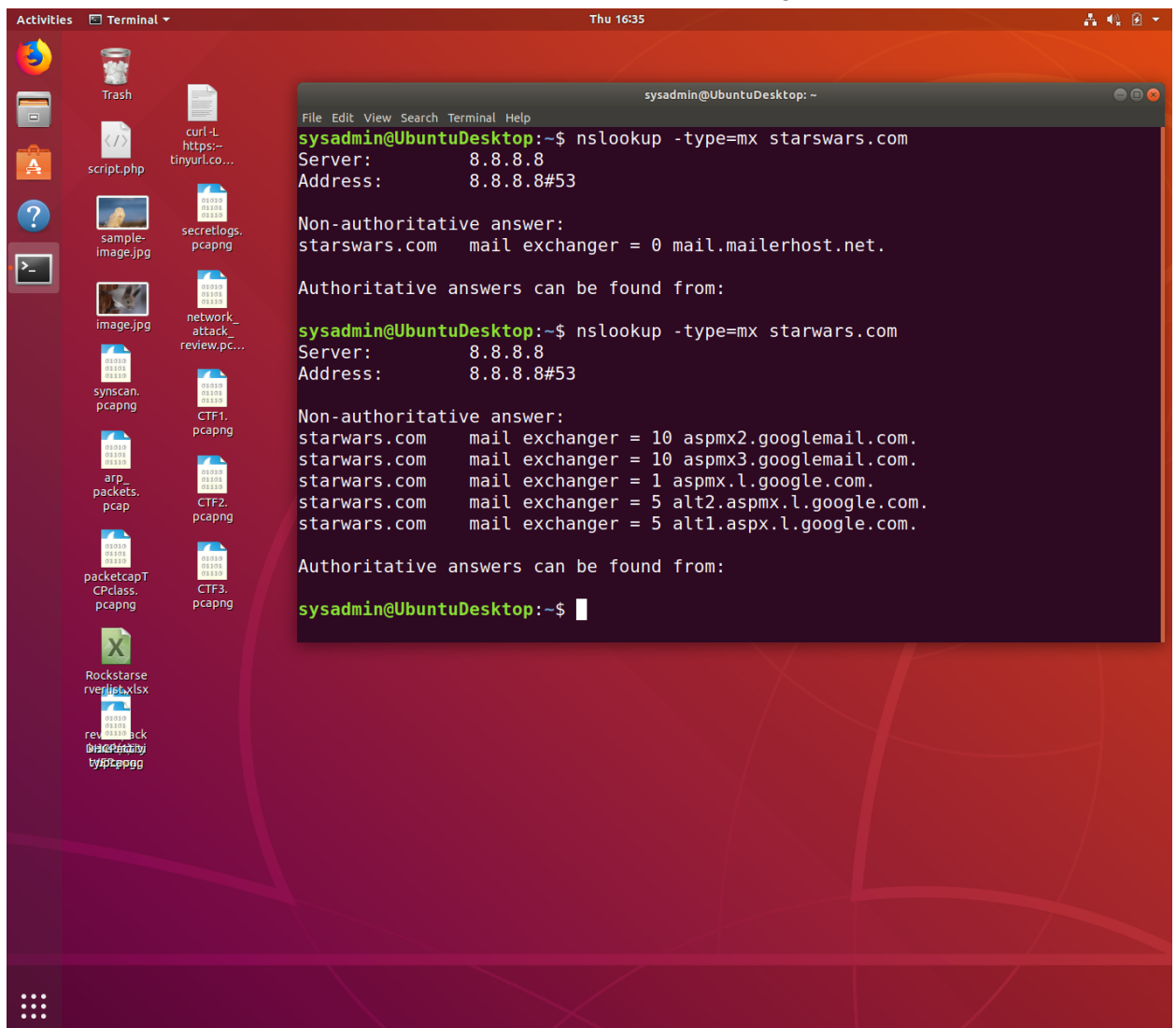
Mission 1

Issue: Due to the DoS attack, the Empire took down the Resistance's DNS and primary email servers.

- The Resistance's network team was able to build and deploy a new DNS server and mail server.
- The new primary mail server is asltx.l.google.com and the secondary should be asltx.2.google.com.
- The Resistance (starwars.com) is able to send emails but unable to receive any.

Your mission:

- Determine and document the mail servers for starwars.com using NSLOOKUP.



```
sysadmin@UbuntuDesktop: ~  
File Edit View Search Terminal Help  
sysadmin@UbuntuDesktop:~$ nslookup -type=mx starwars.com  
Server:      8.8.8.8  
Address:     8.8.8.8#53  
  
Non-authoritative answer:  
starwars.com mail exchanger = 0 mail.mailerhost.net.  
  
Authoritative answers can be found from:  
  
sysadmin@UbuntuDesktop:~$ nslookup -type=mx starwars.com  
Server:      8.8.8.8  
Address:     8.8.8.8#53  
  
Non-authoritative answer:  
starwars.com mail exchanger = 10 aspmx2.googlemail.com.  
starwars.com mail exchanger = 10 aspmx3.googlemail.com.  
starwars.com mail exchanger = 1 aspmx.l.google.com.  
starwars.com mail exchanger = 5 alt2.aspmx.l.google.com.  
starwars.com mail exchanger = 5 alt1.aspmx.l.google.com.  
  
Authoritative answers can be found from:  
  
sysadmin@UbuntuDesktop:~$
```

- Explain why the Resistance isn't receiving any emails.

The Resistance is not able to receive any emails because the primary mail addresses have been altered or deleted to different names. So any incoming mail sent to :asltx.1.google.com and asltx.2.google.com is now not being received by the server.

- Document what a corrected DNS record should be.
The corrected lines should read:
 - Starwars.com mail exchanger = 1 asltx.1.google.com
 - Starwars.com mail exchanger = 5 asltx.1.google.com

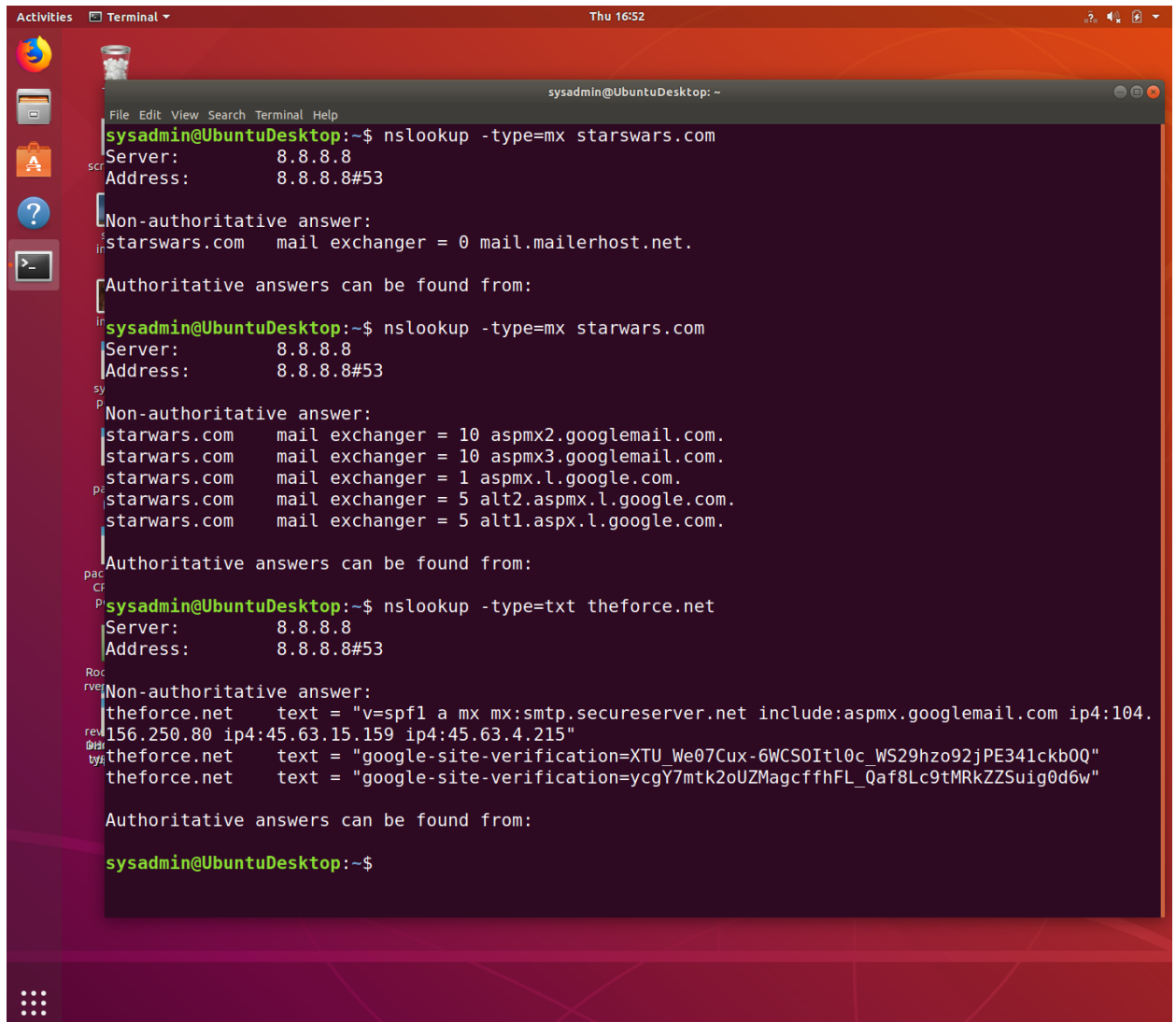
Mission 2

Issue: Now that you've addressed the mail servers, all emails are coming through. However, users are still reporting that they haven't received mail from the theforce.net alert bulletins.

- Many of the alert bulletins are being blocked or going into spam folders.
- This is probably due to the fact that theforce.net changed the IP address of their mail server to 45.23.176.21 while your network was down.
- These alerts are critical to identify pending attacks from the Empire.

Your mission:

- Determine and document the SPF for theforce.net using NSLOOKUP.



```
Activities Terminal Thu 16:52
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~$ nslookup -type=mx starwars.com
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
starwars.com mail exchanger = 0 mail.mailerhost.net.

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~$ nslookup -type=mx starwars.com
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
starwars.com mail exchanger = 10 aspmx2.googlemail.com.
starwars.com mail exchanger = 10 aspmx3.googlemail.com.
starwars.com mail exchanger = 1 aspmx.l.google.com.
starwars.com mail exchanger = 5 alt2.aspmx.l.google.com.
starwars.com mail exchanger = 5 alt1.aspmx.l.google.com.

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~$ nslookup -type=txt theforce.net
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
theforce.net text = "v=spf1 a mx mx:smtp.secureserver.net include:aspmx.googlemail.com ip4:104.156.250.80 ip4:45.63.15.159 ip4:45.63.4.215"
theforce.net text = "google-site-verification=XTU_We07Cux-6WCS0Itl0c_WS29hzo92jPE341ckb0Q"
theforce.net text = "google-site-verification=ycgY7mtk2oUZMagcffhFL_Qaf8Lc9tMRkZZSuig0d6w"

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~$
```

- Explain why the Force's emails are going to spam.
The cahnged Ip (45.23.176.21)for the email server has not been added to the list; so it is not quite lining up with the correct spf.
- Document what a corrected DNS record should be.
The corrected line should be:

```
theforce.net text = "v=spf1 a mx mx:smtp.secureserver.net
include:aspmx.googlemail.com include:45.23.176.21 ip4:104.156.250.80
ip4:45.63.15.159 ip4:45.63.4.215"
```

Mission 3

Issue: You have successfully resolved all email issues and the resistance can now receive alert bulletins. However, the Resistance is unable to easily read the details of alert bulletins online.

- They are supposed to be automatically redirected from their sub page of resistance.theforce.net to theforce.net.

Your mission:

- Document how a CNAME should look by viewing the CNAME of www.theforce.net using NSLOOKUP.

```

starwars.com      mail exchanger = 10 aspmx2.googlemail.com.
starwars.com      mail exchanger = 10 aspmx3.googlemail.com.
starwars.com      mail exchanger = 1 aspmx.l.google.com.
starwars.com      mail exchanger = 5 alt2.aspmx.l.google.com.
starwars.com      mail exchanger = 5 alt1.aspmx.l.google.com.

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~$ nslookup -type=txt theforce.net
Server:           8.8.8.8
Address:          8.8.8.8#53

Non-authoritative answer:
theforce.net      text = "v=spf1 a mx mx:smtp.secureserver.net include:aspmx.googlemail.com ip4:104.156.250.80 ip4:45.63.15.159 ip4:45.63.4.215"
theforce.net      text = "google-site-verification=XTU We07Cux-6WCS0Itl0c WS29hzo92jPE341ckb0Q"
theforce.net      text = "google-site-verification=ycgY7mtk2oUZMagcfffhFL_Qaf8Lc9tMRkZZSuig0d6w"

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~$ cybersecurity
cybersecurity: command not found

sysadmin@UbuntuDesktop:~$ nslookup 45.23.176.21
21.176.23.45.in-addr.arpa      name = 45-23-176-21.lightspeed.rcsntx.sbcglobal.net.

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~$ nslookup -type=cname www.theforce.net
Server:           8.8.8.8
Address:          8.8.8.8#53

Non-authoritative answer:
www.theforce.net      canonical name = theforce.net.

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~$

```

- Explain why the sub page of resistance.theforce.net isn't redirecting to theforce.net. In the record there is no mention of a redirect to resistance.theforce.net, so it is not redirecting.
- Document what a corrected DNS record should be. By adding a line for it, it can be added

www.theforce.net canonical name = theforce.net

resistance.theforce.net

canonical name = www.theforce.net

Mission 4

Issue: During the attack, it was determined that the Empire also took down the primary DNS server of princessleia.site.

- Fortunately, the DNS server for princessleia.site is backed up and functioning.
- However, the Resistance was unable to access this important site during the attacks and now they need you to prevent this from happening again.
- The Resistance's networking team provided you with a backup DNS server of: ns2.galaxybackup.com.

Your mission:

- Confirm the DNS records for princessleia.site.

```
Activities Terminal Thu 17:23
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
Address: 8.8.8.8#53
Non-authoritative answer:
theforce.net text = "v=spf1 a mx mx:smtp.secureserver.net include:aspmx.googlemail.com ip4:104.156.250.80 ip4:45.63.15.159 ip4:45.63.4.215"
theforce.net text = "google-site-verification=XTU_We07Cux-6WCS0Itl0c_WS29hzo92jPE341ckb0Q"
theforce.net text = "google-site-verification=ycgY7mtk2oUZMagcfffHFL_Qaf8Lc9tMRkZZSuig0d6w"
Authoritative answers can be found from:
sysadmin@UbuntuDesktop:~$ cybersecurity
cybersecurity: command not found
sysadmin@UbuntuDesktop:~$ nslookup 45.23.176.21
21.176.23.45.in-addr.arpa name = 45-23-176-21.lightspeed.rcsntx.sbcglobal.net.
Authoritative answers can be found from:
sysadmin@UbuntuDesktop:~$ nslookup -type=cname www.theforce.net
Server: 8.8.8.8
Address: 8.8.8.8#53
Non-authoritative answer:
www.theforce.net canonical name = theforce.net.
Authoritative answers can be found from:
sysadmin@UbuntuDesktop:~$ nslookup -type=ns princessleia.site
Server: 8.8.8.8
Address: 8.8.8.8#53
Non-authoritative answer:
princessleia.site nameserver = ns25.domaincontrol.com.
princessleia.site nameserver = ns26.domaincontrol.com.
Authoritative answers can be found from:
sysadmin@UbuntuDesktop:~$
```

- Document how you would fix the DNS record to prevent this issue from happening again. To be able to see the backup when the site is down, a reference needs to be added that it can find.

Princessleia.site nameserver = ns26.domaincontrol.com

Princessleia.site nameserver = ns25.domaincontrol.com

Princessleia.site nameserver = ns2.galaxybackup.com

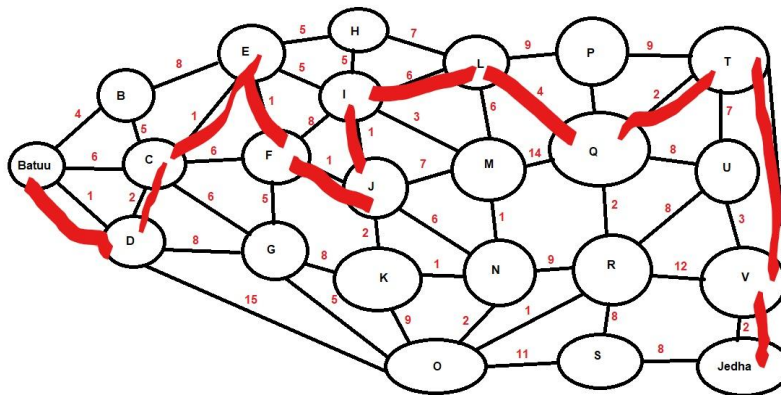
Mission 5

Issue: The network traffic from the planet of Batuu to the planet of Jedha is very slow.

- You have been provided a network map with a list of planets connected between Batuu and Jedha.
- It has been determined that the slowness is due to the Empire attacking Planet N.

Your Mission:

- View the Galaxy Network Map and determine the OSPF shortest path from Batuu to Jedha.
BATUU-D-C-E-F-J-I-L-Q-T-V-JEDHA this is 23 hops $(1+2+1+1+1+1+6+4+2+2+2)=23$ hops
- Confirm your path doesn't include Planet N in its route.
-D-C-E-F-J-I-L-Q-T-V-
- Document this shortest path so it can be used by the Resistance to develop a static route to improve the traffic.



Mission 6

Issue: Due to all these attacks, the Resistance is determined to seek revenge for the damage the Empire has caused.

- You are tasked with gathering secret information from the Dark Side network servers that can be used to launch network attacks against the Empire.
- You have captured some of the Dark Side's encrypted wireless internet traffic in the following pcap: Darkside.pcap.

Your Mission:

- Figure out the Dark Side's secret wireless key by using Aircrack-ng.
 - Hint: This is a more challenging encrypted wireless traffic using WPA.

- In order to decrypt, you will need to use a wordlist (-w) such as rockyou.txt. Searched system for rockyou.txt, which was in /usr/share/wordlists. Then ran: aircrack-ng Darkside.pcap -w /usr/share/wordlists/rockyou.txt

```

sysadmin@UbuntuDesktop: ~/Desktop
File Edit View Search Terminal Help
network_attack_review.pcap
packetcapTCPclass.pcapng
'reviewpackets (1).pcapng'
Rockstarseverlist.xlsx
sample-image.jpg
script.php
secretlogs.pcapng
Stricklands_messages
Stricklands_messages.zip
synscan.pcapng
wireless2.pcapng
sysadmin@UbuntuDesktop:~/Desktop$ aircrack-ng Darkside.pcap -w /usr/share/wordli
sts/rockyou.txt
Opening Darkside.pcap
Read 586 packets.

# BSSID ESSID Encryption
1 00:0B:86:C2:A4:85 linksys WPA (1 handshake)

Choosing first network as target.

Opening Darkside.pcap
Reading packets, please wait...

Aircrack-ng 1.2 rc4

[00:00:00] 2280/7120714 keys tested (2786.09 k/s)

Time left: 42 minutes, 35 seconds 0.03%

KEY FOUND! [ dictionary ]

Master Key : 5D F9 20 B5 48 1E D7 05 38 DD 5F D0 24 23 D7 E2
52 22 05 FE EE BB 97 4C AD 08 A5 2B 56 13 ED E2

Transient Key : 1B 7B 26 96 03 F0 6C 6C D4 03 AA F6 AC E2 81 FC
55 15 9A AF BB 3B 5A A8 69 05 13 73 5C 1C EC E0
A2 15 4A E0 99 6F A9 5B 21 1D A1 8E 85 FD 96 49
5F B4 97 85 67 33 87 B9 DA 97 97 AA C7 82 8F 52

EAPOL HMAC : 6D 45 F3 53 8E AD 8E CA 55 98 C2 60 EE FE 6F 51
  
```

- Use the Dark Side's key to decrypt the wireless traffic in Wireshark.
 - Hint: The format for they key to decrypt wireless is <Wireless_key>:<SSID>.

Activities Wireshark Fri 17:22 sysadmin@UbuntuDesktop: ~/Desktop

File Edit View Search Terminal Help

script.php

Darkside.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Time	Source	Destination	Protocol	Length	Info
0.000000	IntelCor_55:98:ef	ArubaaHe_c2:a4:85	802.11	24	Null function (No data), SN=93
0.000265	IntelCor_55:98:ef	ArubaaHe_c2:a4:85	802.11	10	Acknowledgement, Flags=.....
0.028738	ArubaaHe_c2:a4:85	IntelCor_55:98:ef	802.11	37	Deauthentication, SN=0, FN=0
0.028747	IntelCor_55:98:ef	ArubaaHe_c2:a4:85	802.11	37	Deauthentication, SN=0, FN=0
0.030651	IntelCor_55:98:ef	ArubaaHe_c2:a4:85	802.11	10	Acknowledgement, Flags=.....
0.090780	IntelCor_55:98:ef	ArubaaHe_c2:a4:85	802.11	24	Null function (No data), SN=93
0.091084	IntelCor_55:98:ef	ArubaaHe_c2:a4:85	802.11	10	Acknowledgement, Flags=.....
0.092224	ArubaaHe_c2:a4:85	IntelCor_55:98:ef	802.11	26	Deauthentication, SN=4001, FN=
0.101482	ArubaaHe_c2:a4:85	Broadcast	802.11	111	Beacon frame, SN=4007, FN=0, F
0.113880	IntelCor_55:98:ef	Broadcast	802.11	49	Probe Request, SN=939, FN=0, F

Frame 1: 24 bytes on wire (192 bits), 24 bytes captured (192 bits) on interface 0

IEEE 802.11 Null function (No data), Flags: ...PR...

WEP and WPA Decryption Keys

Key type	Key
wep	1F:1F:1F:1F:1F
wpa-pwd	Induction
wpa-pwd	dictionary.linksys

Invalid key format

Help

/home/sysadmin/config/wireshark/80211_keys

Copy from Cancel OK

Packets: 586 - Displayed: 586 (100.0%) Profile: Default

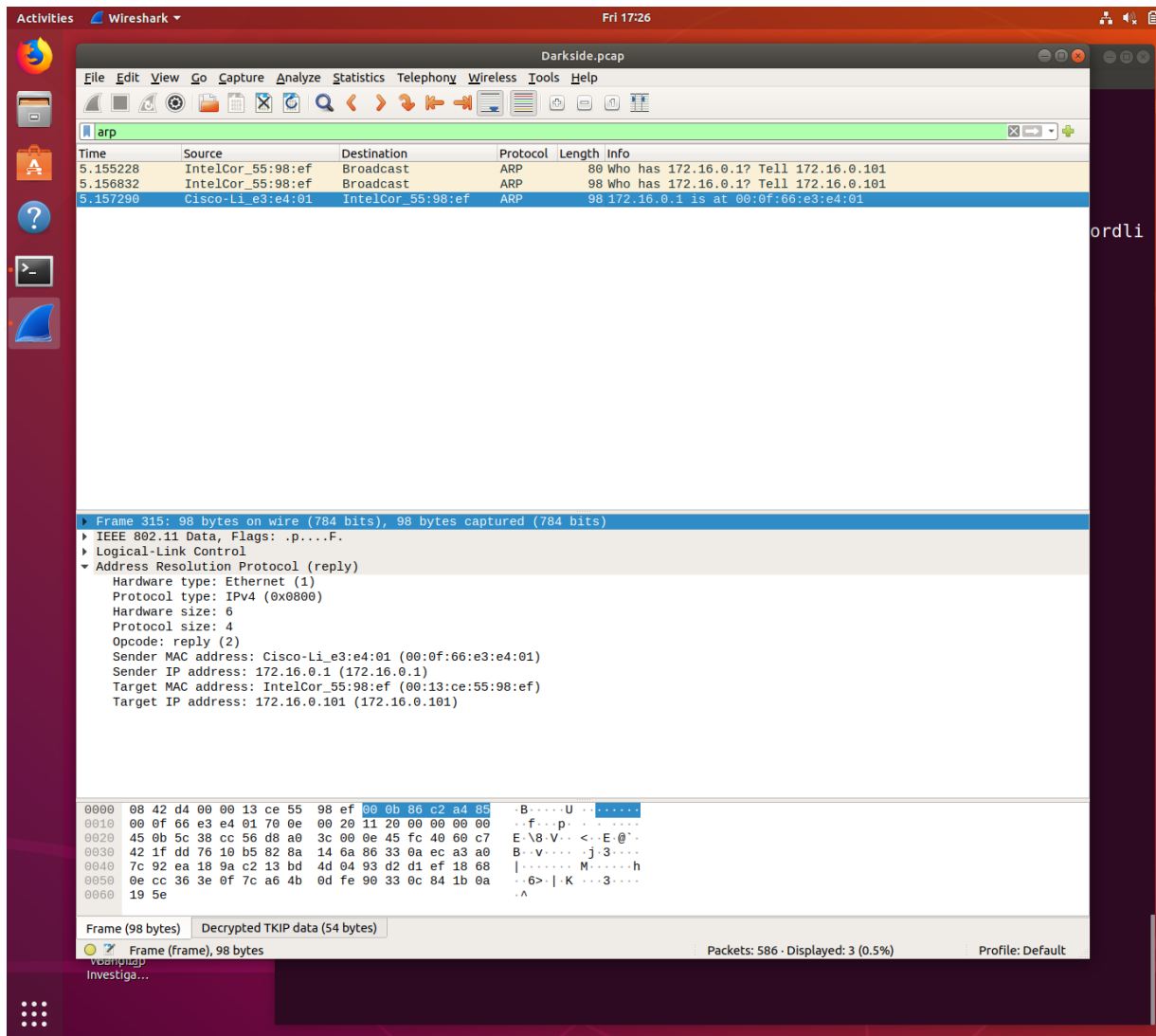
Transient Key : 1B 7B 26 96 03 F0 6C 6C D4 03 AA F6 AC E2 81 FC
55 15 9A AF BB 3B 5A A8 69 05 13 73 5C 1C EC E0
A2 15 4A E0 99 6F A9 5B 21 1D A1 8E 85 FD 96 49
5F B4 97 85 67 33 87 B9 DA 97 97 AA C7 82 8F 52

EAPOL HMAC : 6D 45 F3 53 8E AD 8E CA 55 98 C2 60 EE FE 6F 51

sysadmin@UbuntuDesktop:~/Desktop\$

- Once you have decrypted the traffic, figure out the following Dark Side information:

- Host IP Addresses and MAC Addresses by looking at the decrypted ARP traffic.



- IP:172.16.0.1 MAC: 00:0f:66:e3:e4:01
- IP:172.16.0.101 MAC: 00:13:ce:55:98:ef
- Document these IP and MAC Addresses, as the resistance will use these IP addresses to launch a retaliatory attack.
Other IP/MAC seen:
- IP:172.16.0.09 MAC:00:14:bf:0f:03:30 Location: Location:
<http://172.16.0.9:5431/dyndev/uuid:0014-bf0f-0330000099dc\r\n>

Mission 7

As a thank you for saving the galaxy, the Resistance wants to send you a secret message!

Your Mission:

- View the DNS record from Mission #4.
- The Resistance provided you with a hidden message in the TXT record, with several steps to follow.

```

sysadmin@UbuntuDesktop: ~/Desktop
File Edit View Search Terminal Help
sysadmin@UbuntuDesktop:~/Desktop$ aircrack-ng Darkside.pcap -w /usr/share/wordlists/rockyou.txt
Opening Darkside.pcap
Read 586 packets.

# BSSID          ESSID          Encryption
1 00:0B:86:C2:A4:85 linksys        WPA (1 handshake)

Choosing first network as target.

Opening Darkside.pcap
Reading packets, please wait...

                                Aircrack-ng 1.2 rc4

[00:00:00] 2280/7120714 keys tested (2786.09 k/s)

Time left: 42 minutes, 35 seconds                                0.03%

                                KEY FOUND! [ dictionary ]

Master Key      : 5D F9 20 B5 48 1E D7 05 38 DD 5F D0 24 23 D7 E2
                  52 22 05 FE EE BB 97 4C AD 08 A5 2B 56 13 ED E2

Transient Key   : 1B 7B 26 96 03 F0 6C 6C D4 03 AA F6 AC E2 81 FC
                  55 15 9A AF BB 3B 5A A8 69 05 13 73 5C 1C EC E0
                  A2 15 4A E0 99 6F A9 5B 21 1D A1 8E 85 FD 96 49
                  5F B4 97 85 67 33 87 B9 DA 97 97 AA C7 82 8F 52

EAPOL HMAC     : 6D 45 F3 53 8E AD 8E CA 55 98 C2 60 EE FE 6F 51
sysadmin@UbuntuDesktop:~/Desktop$ nslookup -type=txt princessleia.site
Server:          8.8.8.8
Address:         8.8.8.8#53

Non-authoritative answer:
princessleia.site      text = "Run the following in a command line: telnet towe
l.blinkenlights.nl or as a backup access in a browser: www.asciimation.co.nz"

Authoritative answers can be found from:

sysadmin@UbuntuDesktop:~/Desktop$

```

- Follow the steps from the TXT record.
 - **Note:** A backup option is provided in the TXT record (as a website) in case the main telnet site is unavailable
- Take a screen shot of the results.

