

Lab 07 Template – Ethan Roepke

1. Screenshot of properly configured DNS MX query

(5 points)

```
Last login: Mon Oct 16 15:37:41 2023 on ttys1  
cpre230@mail:~$ dig MX student126.230.com @199.100.16.100  
  
;; <>> DiG 9.18.12-0ubuntu0.22.04.3-Ubuntu <>> MX student126.230.com @199.100.16.100  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65438  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 1232  
; COOKIE: 08a30ed33e452e8401000000652d5e1e4cd63019dcbe3a1c (good)  
;; QUESTION SECTION:  
;student126.230.com. IN MX  
  
;; ANSWER SECTION:  
student126.230.com. 900 IN MX 10 mail.student126.230.com.  
  
;; Query time: 0 msec  
;; SERVER: 199.100.16.100#53(199.100.16.100) (UDP)  
;; WHEN: Mon Oct 16 16:00:20 UTC 2023  
;; MSG SIZE rcvd: 96
```

2. Screenshot of output from netstat -tnl

(5 points)

```
root@mail:/home/cpre230# netstat -tnl  
Active Internet connections (only servers)  
Proto Recv-Q Send-Q Local Address          Foreign Address        State  
tcp      0      0 0.0.0.0:143              0.0.0.0:*            LISTEN  
tcp      0      0 127.0.0.53:53             0.0.0.0:*            LISTEN  
tcp      0      0 0.0.0.0:22              0.0.0.0:*            LISTEN  
tcp      0      0 0.0.0.0:25              0.0.0.0:*            LISTEN  
tcp      0      0 0.0.0.0:110             0.0.0.0:*            LISTEN  
root@mail:/home/cpre230#
```

3. Screenshot of Sending mail from cpre230a --> cpre230b in terminal

(10 points)

```
cpre230@mail:~$ telnet mail.student126.230.com 25
Trying 192.168.1.204...
Connected to mail.student126.230.com.
Escape character is '^]'.
220 mail.student126.230.com ESMTP Postfix (Ubuntu)
he1o student126.230.com
250 mail.student126.230.com
mail from: <cpre230a@student126.230.com>
250 2.1.0 Ok
rcpt to: <cpre230b@student126.230.com>
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: You are a failure
Why did you get arrested.....
.
250 2.0.0 Ok: queued as 709673DB5
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

**4. Screenshot of reading the previously sent message in terminal
(10 points)**

```
cpre230@mail:~$ telnet mail.student126.230.com 110
Trying 192.168.1.204...
Connected to mail.student126.230.com.
Escape character is '^]'.
+OK Dovecot (Ubuntu) ready.
USER cpre230b
+OK
PASS cpre230
+OK Logged in.
LIST
+OK 2 messages:
1 542
2 550
.
RETR 2
+OK 550 octets
Return-Path: <cpre230a@student126.230.com>
X-Original-To: cpre230b@student126.230.com
Delivered-To: cpre230b@student126.230.com
Received: from student126.230.com (mail.student126.230.com [192.168.1.204])
    by mail.student126.230.com (Postfix) with SMTP id 709673DB5
    for <cpre230b@student126.230.com>; Thu, 12 Oct 2023 16:27:13 +0000 (UTC)
Subject: You are a failure
Message-Id: <20231012162741.709673DB5@mail.student126.230.com>
Date: Thu, 12 Oct 2023 16:27:13 +0000 (UTC)
From: cpre230a@student126.230.com

Why did you get arrested.....
.
QUIT
+OK Logging out.
Connection closed by foreign host.
cpre230@mail:~$
```

**5. Screenshot of Dovecot cert raw contents
(5 points)**

```

root@mail:/usr/share/dovecot# cd /etc/dovecot/ssl
root@mail:/etc/dovecot/ssl# sudo cat dovecot.pem
-----BEGIN CERTIFICATE-----
MIID3DCCAsSgAwIBAgIUCyExE/ynYYPeA7P+JqKETSwvxwowDQYJKoZIhvNAQEL
BQAwgZAxHDAAgNVBAoMEORvdmVjb3QgbWFpbCBzZJ22XIxDaEbgNVBAAsMF21h
aHwuc3R1ZGVudDEyNi4yMzAuY29tMSAwHgYDVQQDDBdTYWlsLnN0dWR1bnQxMjYu
MjMwLmNvbTEsMCogCSqGSIB3DQEJARYdcG9zdG1hc3R1ckBzdHVkZW50MTI2LjIz
MC5jb20wHhcNMjMxMDEyMTYzODAzWhcNMjQxMDExMTYzODAzWjCBkDEcMB0GA1UE
CgwTRG92ZWNvdCBtYWlsIHN1cnZlcJegMB4GA1UECwwXbWFpbC5zdHVkZW50MTI2
LjIzMC5jb20xIDAeBgNVBAMMF21haHwuc3R1ZGVudDEyNi4yMzAuY29tMSwwKgYJ
KoZIhvNAQKBFh1wb3N0bWFzdGVyQHNOdWR1bnQxMjYuMjMwLmNvbTCCASiwDQYJ
KoZIhvNAQEBBQA DggEPADCCAQoCggEBAJ6UvWXst2tYdmt/Wh9mA3ArPKVJz1B8
bnDYYm9Y8LyYnLyypKXNvnKyDIKrqUhfyS1bK1Y9E/vTFWa7RMqXws1ounehVu+
Hx1jEWTaPNhKroPP6gCKRKHL01L/EeoF1+PxQ6a2gKXUKv1ftnc1WTgSsEmJ2pop
51IUZ6ABivTEJfVG0AHjnHeMdpggm/fke2EC5B+aYU0A90f2i/Bm/9yg2G8KTH0t
RsG1yaptScUnIXodu wYirdI0BqVhy03yCv9yt0DIVxhvFrNCs8KyyTq91JisA+io
i8W2y whole certificate omitted ...
-----END CERTIFICATE-----
root@mail:/etc/dovecot/ssl#

```

6. Screenshot of Dovecot cert parsed as X.509 (5 points)

```

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      71:81:31:fc:a7:61:83:de:03:b3:fe:26:a2:84:4d:2c:2f:c7:0a
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: O = Dovecot mail server, OU = mail.student126.230.com, CN = mail.student126.230.com,
             emailAddress = postmaster@student126.230.com
    Validity
      Not Before: Oct 12 16:38:03 2023 GMT
      Not After : Oct 11 16:38:03 2024 GMT
    Subject: O = Dovecot mail server, OU = mail.student126.230.com, CN = mail.student126.230.com
             , emailAddress = postmaster@student126.230.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
        Modulus:
          00:9e:94:bd:65:ec:b7:6b:58:76:6b:7f:5a:1f:66:
          03:70:2b:3e:45:49:cf:50:7c:6e:70:d8:62:f6:58:
          f0:bc:98:ca:72:f2:ca:92:97:36:f9:ca:c8:32:0a:
          ae:a5:21:c9:f4:b5:6c:ad:58:f4:4f:ef:4c:55:9a:
          ed:13:2a:5f:0b:25:a2:e9:de:85:5b:be:1f:id:63:
          11:64:da:3c:08:4a:ae:83:cf:ea:00:8a:44:a1:cb:
          d2:52:ff:11:e3:9f:97:e3:f1:43:a6:b6:80:a5:d4:
          2a:f9:5f:b6:77:25:59:38:12:b0:49:89:66:9a:29:
          e7:s2:14:cf:a0:01:8a:f4:c4:25:f5:46:38:01:e3:
          9c:77:8c:76:98:20:9b:f7:e4:79:91:02:e4:1f:9a:
          61:4d:00:f7:47:d9:8b:f0:66:ff:dc:a0:08:6f:0a:
          4c:7d:2d:46:c1:b5:c9:aa:6d:49:c5:27:21:7a:1d:
          bb:06:22:ad:d2:34:06:a5:61:c8:ed:f2:0a:ff:72:
          b7:40:c8:57:18:6f:16:b3:42:b3:c2:b2:c9:3a:bd:
          d4:98:ac:03:e8:a8:8b:c5:b6:ca:9b:93:2c:f0:0c:
          30:d6:58:45:d7:37:b4:32:20:a4:09:70:a9:53:01:
          b2:a2:fe:b7:09:59:f0:d6:3b:75:89:0f:1b:d3:43:
          e8:6b
        Exponent: 65537 (0x10001)
:

```

```

cpred30_eroepke_mail To release your mouse press: Control-36
11:64:da:3c:d8:4a:ae:83:cf:ea:00:8a:44:a1:cb:
d2:52:ff:11:e3:9f:97:e3:f1:43:a6:b6:80:a5:d4:
2a:f9:5f:b6:77:25:59:38:12:b0:49:89:66:9a:29:
e7:52:14:cf:a0:01:8a:f4:c4:25:f5:46:38:01:e3:
9c:77:8c:76:98:20:9b:f7:e4:79:91:02:e4:1f:9a:
61:4d:00:f7:47:d9:8b:f0:66:ff:dc:a0:d8:6f:0a:
4c:7d:2d:46:c1:b5:c9:aa:6d:49:c5:27:21:7a:1d:
bb:06:22:ad:d2:34:06:a5:61:c8:ed:f2:0a:ff:72:
b7:40:c8:57:18:6f:16:b3:42:b3:c2:b2:c9:3a:bd:
d4:98:ac:03:e8:a8:b8:c5:b6:ca:9b:93:2c:f0:0c:
30:d6:58:45:07:37:b4:32:20:a4:09:70:a9:53:01:
b2:a2:fe:b7:09:59:f0:d6:3b:75:89:0f:1b:d3:43:
e8:6b
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
    CA:FALSE
X509v3 Subject Key Identifier:
    BE:81:88:17:85:4a:04:71:18:22:4E:40:D2:CA:4F:9B:D6:73:3D:75
Signature Algorithm: sha256WithRSAEncryption
Signature Value:
39:ac:93:db:25:8c:f9:fb:18:e8:ce:10:c1:35:c9:db:43:37:
fb:0c:b1:bf:32:3b:04:9d:34:81:ce:f2:84:c4:a3:ad:1e:66:
e3:8d:6c:c9:32:2d:ab:99:bc:49:8f:68:29:1f:20:b7:1f:88:
1c:85:fa:1b:da:a7:eb:82:99:28:67:e2:4c:bc:9f:ed:ce:24:
96:5e:2b:fb:b8:c0:1e:02:ec:a8:10:01:98:a5:67:01:17:51:
23:e9:2c:76:85:4b:ba:f3:ab:ed:2b:bc:2e:5d:1b:e5:5c:07:
9c:ee:89:fc:id:90:09:ff:88:a6:f1:14:33:6d:35:08:90:41:
23:38:73:6a:b9:fa:2b:69:00:9d:ae:8f:eb:cd:26:cd:87:67:
e6:94:de:dd:0a:a7:de:64:79:a5:77:5d:5d:c0:f0:06:6d:1e:
ef:46:59:c7:8e:51:02:6e:7e:1e:dd:04:de:fc:1f:e6:82:27:
82:5e:f0:98:97:54:c4:a4:84:98:d3:a2:2b:43:57:5f:02:4b:
48:03:af:55:5c:4e:9f:e9:7d:b9:39:42:f0:28:52:35:fd:5c:
b3:48:ff:f1:3b:15:94:fc:f1:fb:f6:9b:f1:e6:d1:f0:9e:33:
60:cc:66:3d:84:8a:63:cc:e9:b1:ab:0d:18:3e:18:27:c8:b4:
8e:6b:36:37
(END)

```

7. Screenshot of plaintext IMAP - Wireshark (5 points)

The screenshot shows a Wireshark capture of IMAP traffic. The timeline pane shows the sequence of packets, and the details and bytes panes provide a detailed view of the protocol exchange.

Protocol Details:

- Protocol: IMAP
- Length: 75 Request: 91 noop
- Length: 11 Response: 91 OK NOOP completed (0.001 + 0.000 secs).
- Length: 92 Request: 92 UID fetch 3:*(FLAGS)
- Length: 148 Response: 92 OK Fetch completed (0.001 + 0.000 secs).
- Length: 248 Request: 93 UID fetch 3 (UID RFC822.SIZE FLAGS BODY.PEEK[HEADER.FIELDS (F...]
- Length: 570 from: cpred30a <cpred30a@student126.230.com>, subject: Hello, (text/plain)
- Length: 112 Request: 94 UID fetch 3 (UID RFC822.SIZE BODY.PEEK[])
- Length: 928 from: cpred30a <cpred30a@student126.230.com>, subject: Hello, (text/plain)
- Length: 178 Request: 95 UID fetch 3 (UID BODY.PEEK[HEADER.FIELDS (Content-Type Content...
- Length: 358 (text/plain)
- Length: 75 Request: 96 IDLE
- Length: 76 Response: + idling
- Length: 72 Request: DONE

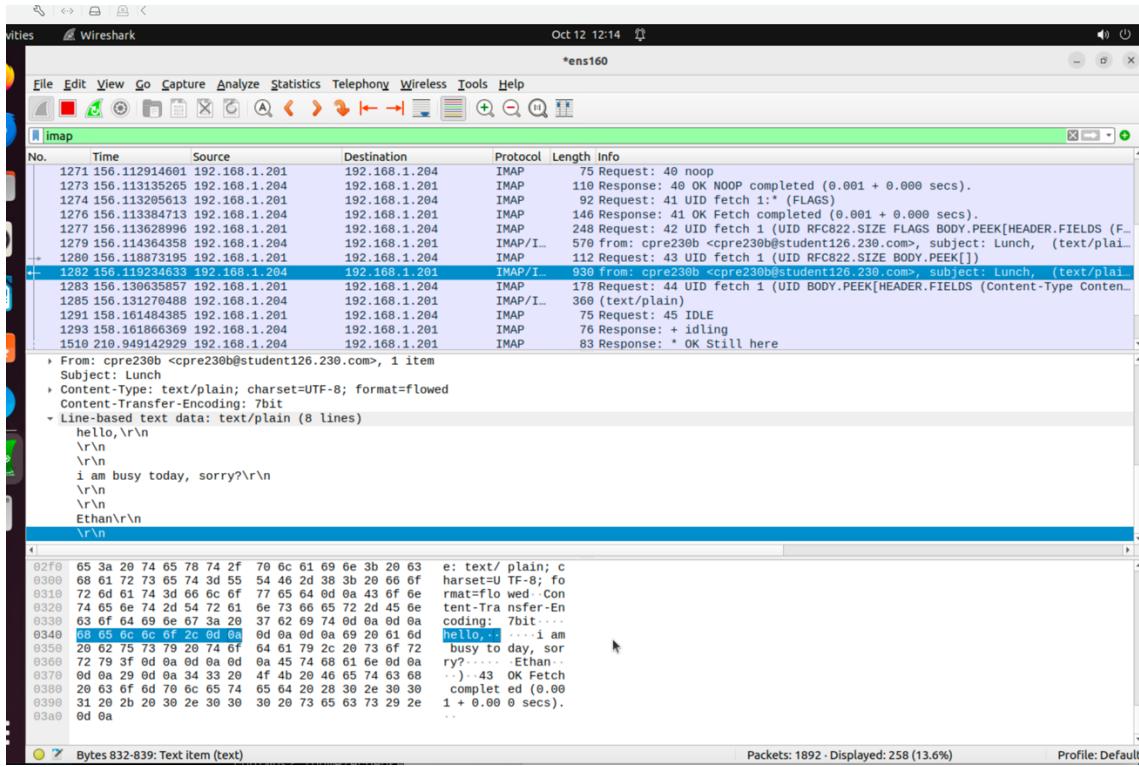
Message Body Content:

```

> To: cpred30b@student126.230.com, 1 item
> From: cpred30a <cpred30a@student126.230.com>, 1 item
Subject: Hello
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 7bit
Line-based text data: text/plain (8 lines)
Good morning,\r\n\r\n
lets get lunch\r\n
Ethan\r\n

```

Packets: 1836 · **Displayed:** 258 (14.1%) · **Profile:** Default



8. Screenshot of Base64 decode of password (10 points)

Decode from Base64 format

Simply enter your data then push the decode button.

```
AGNwcmUyMzBiAGNwcmUyMzA=
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

```
cpre230b@cpre230
```

Copy to clipboard

Decode files from Base64 format

9. Screenshot of plaintext SMTP - Wireshark (5 points)

The screenshot shows an SMTP session in Wireshark. The selected frame (index 574) contains the following message:

```
To: cpre230b@student126.230.com, 1 item
From: cpre230a <cpre230a@student126.230.com>, 1 item
Subject: Hello
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 7bit
Line-based text data: text/plain (8 lines)
Good morning,
lets get lunch
```

The message body is displayed in the hex and ASCII panes. The ASCII pane shows the raw text "Good morning,\r\nlets get lunch\r\n".

Frame (69 bytes) Reassembled SMTP (421 bytes)

smtp

No.	Time	Source	Destination	Protocol	Length	Info
1	1242 155.608955489	192.168.1.204	192.168.1.201	SMTP	100 S:	250 2.0.0 Ok: queued as 2D655312
2	876 181.266055301	192.168.1.204	192.168.1.201	SMTP	100 S:	250 2.0.0 Ok: queued as C9E70312
3	868 181.232252836	192.168.1.204	192.168.1.201	SMTP	80 S:	250 2.1.0 Ok
4	1234 155.588535494	192.168.1.204	192.168.1.201	SMTP	80 S:	250 2.1.0 Ok
5	870 181.241767251	192.168.1.204	192.168.1.201	SMTP	80 S:	250 2.1.5 Ok
6	1236 155.601000553	192.168.1.204	192.168.1.201	SMTP	80 S:	250 2.1.5 Ok
7	866 181.223830293	192.168.1.204	192.168.1.201	SMTP	240 S:	250-mail.student126.230.com PIPELINING SIZE 10240000 VRFY ETRN...
8	1232 155.572508773	192.168.1.204	192.168.1.201	SMTP	240 S:	250-mail.student126.230.com PIPELINING SIZE 10240000 VRFY ETRN...
9	872 181.243228732	192.168.1.204	192.168.1.201	SMTP	103 S:	354 End data with <CR><LF>.<CR><LF>
10	1238 155.601474472	192.168.1.204	192.168.1.201	SMTP	103 S:	354 End data with <CR><LF>.<CR><LF>
11	874 181.244266463	192.168.1.204	192.168.1.204	SMTP/I...	69 from: cpre230a <cpre230a@student126.230.com>, subject: Hello, (text/plai...	
12	1240 155.602396227	192.168.1.201	192.168.1.204	SMTP/I...	69 from: cpre230b <cpre230b@student126.230.com>, subject: Lunch, (text/plai...	

```

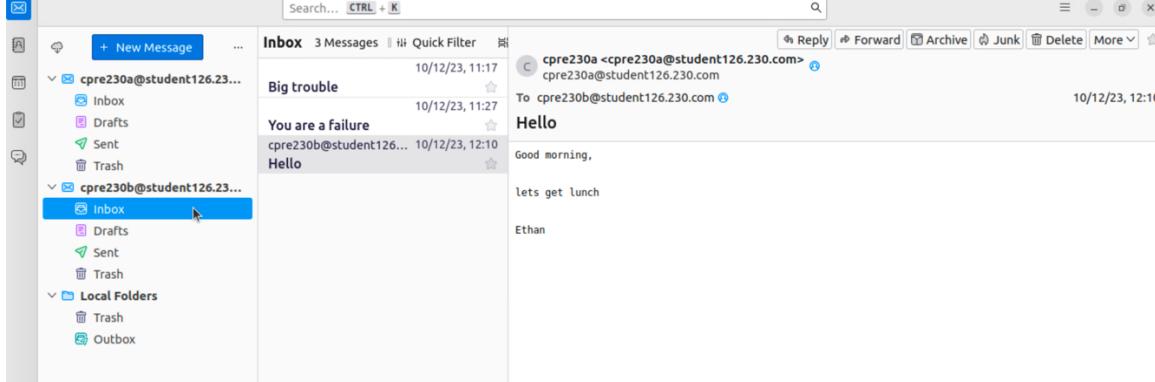
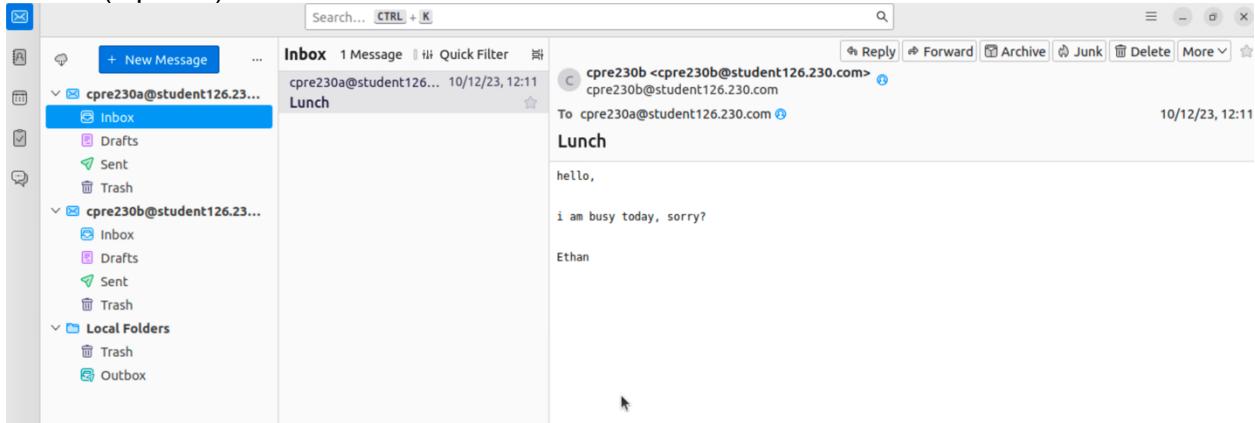
> To: cpre230a@student126.230.com, 1 item
> From: cpre230b <cpre230b@student126.230.com>, 1 item
Subject: Lunch
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 7bit
Line-based text data: text/plain (8 lines)
hello,\r\n
\r\n
\r\n
i am busy today, sorry?\r\n
\r\n
\r\n
Ethan\r\n
\r\n

0100 32 33 30 2e 63 6f 6d 3e 0d 0a 53 75 62 6a 65 63 230.com> ..Subje
0110 74 3a 20 4c 75 6e 63 68 0d 0a 43 6f 6e 74 65 6e t: Lunch ..Conten
0120 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 t-Type: text/pla
0130 69 6e 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d in; char set=UTF-
0140 38 3b 20 66 6f 72 6d 61 74 3d 66 6c 6f 77 65 64 8; forma t=flowed
0150 0d 0a 43 6f 6e 74 65 6e 74 2d 54 72 61 6e 73 66 ..Conten t=Transf
0160 65 72 2d 45 6e 63 6f 64 69 6e 67 3a 20 37 62 69 er-Encod ing: 7bi
0170 74 0d 0a 0d 0a 68 65 0c 6c 6f 2c 0d 0a 0d 0a 0d t... hel lo,....
0180 0a 69 20 61 0d 20 62 75 73 79 20 74 6f 64 61 79 .i am bu sy today
0190 2c 20 73 6f 72 72 79 3f 0d 0a 0d 0a 0d 0a 45 74 , sorry? .....Et
01a0 68 61 6e 0d 0a 0d 0a han...

```

Frame (69 bytes) Reassembled SMTP (423 bytes)

10. Screenshot of test messages in Thunderbird (5 points)



11. Screenshot of encrypted SMTP - Wireshark (5 points)

*ens160

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 587

No.	Time	Source	Destination	Protocol	Length	Info
467 19.732193465	192.168.1.201	192.168.1.204	TCP	74	57312 - 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=34065...	
468 19.732348648	192.168.1.204	192.168.1.201	TCP	74	587 - 57312 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 ...	
469 19.732370318	192.168.1.201	192.168.1.204	TCP	66	57312 - 587 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3406520068 TSecr=25...	
470 19.733361711	192.168.1.204	192.168.1.201	SMTP	118 S:	226 mail.student126.230.com ESMTP Postfix (Ubuntu)	
471 19.733372529	192.168.1.201	192.168.1.204	TCP	66	57312 - 587 [ACK] Seq=1 Ack=53 Win=64256 Len=0 TSval=3406520069 TSecr=25...	
472 19.740039179	192.168.1.201	192.168.1.204	SMTP	88 C:	EHLO [192.168.1.201]	
473 19.740111529	192.168.1.204	192.168.1.201	TCP	66	587 - 57312 [ACK] Seq=53 Ack=23 Win=65280 Len=0 TSval=2546503248 TSecr=3...	
474 19.740181433	192.168.1.204	192.168.1.201	SMTP	240 S:	250-mail.student126.230.com PIPELINING SIZE 10240000 VRFY ETR...	
475 19.767386694	192.168.1.201	192.168.1.204	SMTP	76 C:	STARTTLS	
476 19.767534312	192.168.1.204	192.168.1.201	SMTP	96 S:	220 2.0.0 Ready to start TLS	
477 19.771330794	192.168.1.201	192.168.1.204	TLSv1.3	583 Client Hello		
478 19.773345415	192.168.1.204	192.168.1.201	TLSv1.3	1598 Server Hello, Change Cipher Spec, Application Data, Application Data, Ap...		
479 19.773392608	192.168.1.201	192.168.1.204	TCP	66	57312 - 587 [ACK] Seq=556 Ack=1789 Win=62720 Len=0 TSval=3406520109 TSec...	
480 19.775383796	192.168.1.201	192.168.1.204	TLSv1.3	99 Application Data		
481 19.775434240	192.168.1.201	192.168.1.204	TCP	66	57312 - 587 [FIN, ACK] Seq=574 Ack=1789 Win=64128 Len=0 TSval=3406520111...	
482 19.776339929	192.168.1.204	192.168.1.201	TCP	66	587 - 57312 [FIN, ACK] Seq=1789 Ack=575 Win=64768 Len=0 TSval=2546503284...	
483 19.776341247	192.168.1.201	192.168.1.204	TCP	66	57312 - 587 [ACK] Seq=575 Ack=1790 Win=64128 Len=0 TSval=3406520112 TSec...	
484 19.539261312	192.168.1.201	192.168.1.204	TCP	74	51208 - 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=34065...	

> Frame 473: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface ens160, id 0

> Ethernet II, Src: Intersof_04:7e:04 (00:02:30:04:7e:04), Dst: VMware_86:de:5e (00:50:56:86:de:5e)

> Internet Protocol Version 4, Src: 192.168.1.204, Dst: 192.168.1.201

> Transmission Control Protocol, Src Port: 587, Dst Port: 57312, Seq: 53, Ack: 23, Len: 0

0000	00	50	56	86	de	5e	00	02	30	04	7e	04	08	00	45	00	PV ..A.. 0 -.- E
0010	00	34	03	06	48	00	48	06	b2	d8	c8	a8	01	cc	c8	a8	.4 ..@ .. .
0020	01	c9	02	4b	df	e0	c8	59	7a	be	e4	8d	19	d4	88	10	..K ..Y z ..
0030	01	fe	84	02	00	00	01	01	08	0a	97	c8	8e	50	cb	0bP ..
0040	5f	0c															-

12. Screenshot of encrypted IMAP - Wireshark (5 points)

*ens160

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 993

No.	Time	Source	Destination	Protocol	Length	Info
449 9.788918831	192.168.1.204	192.168.1.201	TLSv1.3	604	Application Data	
450 9.8308001735	192.168.1.201	192.168.1.204	TCP	66	49740 - 993 [ACK] Seq=1209 Ack=4219 Win=64128 Len=0 TSval=3406510167 TSe...	
451 10.5798090614	192.168.1.201	192.168.1.204	TLSv1.3	97	Application Data	
452 10.579943257	192.168.1.204	192.168.1.201	TCP	66	49718 - 49718 [ACK] Seq=3057 Ack=922 Win=64640 Len=0 TSval=2546494087 TSec...	
453 10.588494301	192.168.1.204	192.168.1.201	TLSv1.3	98	Application Data	
454 10.5885052365	192.168.1.201	192.168.1.204	TCP	66	49718 - 993 [ACK] Seq=922 Ack=3089 Win=64128 Len=0 TSval=3406510916 TSec...	
455 10.987616164	192.168.1.201	192.168.1.204	TLSv1.3	97	Application Data	
456 10.987755099	192.168.1.204	192.168.1.201	TCP	66	4993 - 49722 [ACK] Seq=4221 Ack=1240 Win=64512 Len=0 TSval=2546494495 TSe...	
457 10.988140195	192.168.1.204	192.168.1.201	TLSv1.3	98	Application Data	
458 10.988147950	192.168.1.201	192.168.1.204	TCP	66	49722 - 993 [ACK] Seq=1240 Ack=4253 Win=64128 Len=0 TSval=3406511324 TSe...	
459 11.383786003	192.168.1.201	192.168.1.204	TLSv1.3	97	Application Data	
460 11.383928463	192.168.1.204	192.168.1.201	TCP	66	4993 - 49724 [ACK] Seq=3057 Ack=922 Win=64640 Len=0 TSval=2546494891 TSec...	
461 11.384396290	192.168.1.204	192.168.1.201	TLSv1.3	98	Application Data	
462 11.384404997	192.168.1.201	192.168.1.204	TCP	66	49724 - 993 [ACK] Seq=922 Ack=3089 Win=64128 Len=0 TSval=3406511720 TSec...	
463 11.796807832	192.168.1.201	192.168.1.204	TLSv1.3	98	Application Data	
464 11.796946520	192.168.1.204	192.168.1.201	TCP	66	4993 - 49740 [ACK] Seq=4219 Ack=1241 Win=64512 Len=0 TSval=2546495304 TSe...	
465 11.797353737	192.168.1.204	192.168.1.201	TLSv1.3	98	Application Data	
466 11.797361363	192.168.1.201	192.168.1.204	TCP	66	49740 - 993 [ACK] Seq=1241 Ack=4251 Win=64128 Len=0 TSval=3406512133 TSe...	

> Frame 466: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface ens160, id 0

> Ethernet II, Src: VMware_86:de:5e (00:50:56:86:de:5e), Dst: Intersof_04:7e:04 (00:02:30:04:7e:04)

> Internet Protocol Version 4, Src: 192.168.1.201, Dst: 192.168.1.204

> Transmission Control Protocol, Src Port: 49740, Dst Port: 993, Seq: 1241, Ack: 4251, Len: 0

0000	00	02	30	04	7e	04	00	50	56	86	de	5e	08	00	45	00	..0 ..- P V ..A.. E
0010	00	34	2c	6b	40	00	40	06	89	73	c0	a8	01	c9	c0	a8	.4 ..@ .. s ..
0020	01	cc	c2	4c	03	e1	42	19	4e	0c	b8	6e	4c	cc	80	10	..L ..B ..N ..L ..
0030	01	f5	65	0c	00	00	01	01	08	0a	cb	0b	40	05	97	c8	..I @ ..
0040	6f	49															oi

13. Screenshot of NAT rules (5 points)

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
Desktop - Nagios check										
<input type="checkbox"/>	✓  WAN	TCP	*	*	105.148.172.201	22 (SSH)	192.168.1.201	22 (SSH)	desktop1 - SSH check	  
NS2 - Nagios checks										
<input type="checkbox"/>	✓  WAN	TCP/UDP	37.56.23.100	*	105.148.172.199	53 (DNS)	192.168.1.200	53 (DNS)	ns2 - Nagios DNS for inside machines	  
ldap - nagios check										
<input type="checkbox"/>	✓  WAN	TCP	37.56.23.100	*	105.148.172.205	389 (LDAP)	192.168.1.205	389 (LDAP)	ldap - nagios check from outside network	  
mail - nagios check										
<input type="checkbox"/>	✓  WAN	TCP	37.56.23.100	*	105.148.172.204	25 (SMTP)	192.168.1.204	25 (SMTP)	mail - nagios secure SMTP	  
<input type="checkbox"/>	✓  WAN	TCP	37.56.23.100	*	105.148.172.204	993 (IMAP/S)	192.168.1.204	993 (IMAP/S)	mail - nagios secure imap login	  
<input type="checkbox"/>	✓  WAN	TCP	37.56.23.100	*	105.148.172.204	587 (SUBMISSION)	192.168.1.204	587 (SUBMISSION)	mail - nagios secure IMAP	  
<input type="checkbox"/>	✓  WAN	TCP	37.56.23.100	*	105.148.172.204	110 (POP3)	192.168.1.204	110 (POP3)	mail - nagios mail pop	  

14. Screenshot of Nagios queries with green indicated for all mail services (20 points)

www.student125.230.com	www http www https www login	  
www2.student125.230.com	www2 django www2 ssh	  

Student 126 (student126)		
Host	Services	Actions
desktop1.student126.230.com	desktop1 ssh	  
ldap.student126.230.com	ldap Bezos ldap Gates ldap Jobs ldap Musk ldap Zuckerberg ldap service	  
mail.student126.230.com	dns MX mail pop secure imap secure imap login secure smtp	  
ns1.student126.230.com	dns mail dns ns1 dns www dns www2 reverse dns mail reverse dns ns1 reverse dns www reverse dns www2	  
ns2.student126.230.com	dns desktop1 dns ldap dns ws reverse dns desktop1 reverse dns ldap reverse dns ws	  
www.student126.230.com	www http www https www login	  
www2.student126.230.com	www2 django www2 ssh	  

Student 127 (student127)		
Host	Services	Actions
desktop1.student127.230.com	desktop1 ssh	  