

## Homework 2

Ans 1).

Stream cipher:

Cipher Text:

```
\xd7\x9a\xa6Q\x02fqy\x7f\x1d\xe8z\xa6\xe1\xc3\x13H\x83\x1a\x05z9\xc4\x12\xf2\x15(\x07
+\x03\x90\xffh\x17\xff\xdb_7\x9a\x7f\x86n/\xd5\xbb\x9b\xc93?\xbc\x90\x95\xc6
```

```
''
```

```
'''
```

Those algorithms work on a byte-by-byte basis. The block size is always one byte.

Two algorithms are supported by pycrypto: ARC4 and XOR.

Only one mode is available: ECB.

Let's look at an example with the algorithm ARC4 using the key '01234567'.

```
'''
```

```
from Crypto.Cipher import ARC4
```

```
obj1 = ARC4.new('01234567')
```

```
obj2 = ARC4.new('01234567')
```

```
text = 'FOUNDATIONS TO COMPUTER SECURITY IS A COURSE AT IIITD'
```

```
cipher_text = obj1.encrypt(text)
```

```
print( cipher_text )
```

```
print( obj2.decrypt(cipher_text) )
```

```
''
```

Block cipher:

Cipher Text:

```
*\xec\xec\xbe\x84\x8b\xf206\x11\xd6\xc3.\xec\xce\xf2U\xeaX\xd3\x8a\x88\xce\xf0E\xdc6\x91\x03$\x05\x1eB\x9c\x1aoX\xde\x80:\x04\xf1\xd4\xdd\xf5l\xb5\x17aE\xb7\xf7\x17\n#  
“”
```

```
from Crypto.Cipher import DES
```

```
key = '12345678'
```

```
des = DES.new(key, DES.MODE_ECB)
```

```
plain_text = "FOUNDATIONS TO COMPUTER SECURITY IS A COURSE AT IIITD "
```

```
#encryption
```

```
cipher_text = des.encrypt(plain_text)
```

```
#decryption
```

```
decrypted_pt = des.decrypt(cipher_text)
```

```
print( cipher_text )
```

```
print( decrypted_pt )
```

```
“”
```

Ans 2).

## Firewall On:

- `nmap -sA 192.168.1.104`

Starting Nmap 7.30 ( <https://nmap.org> ) at 2016-10-08 17:49 India Standard Time

Nmap scan report for 192.168.1.104

Host is up (0.0017s latency).

Not shown: 997 filtered ports

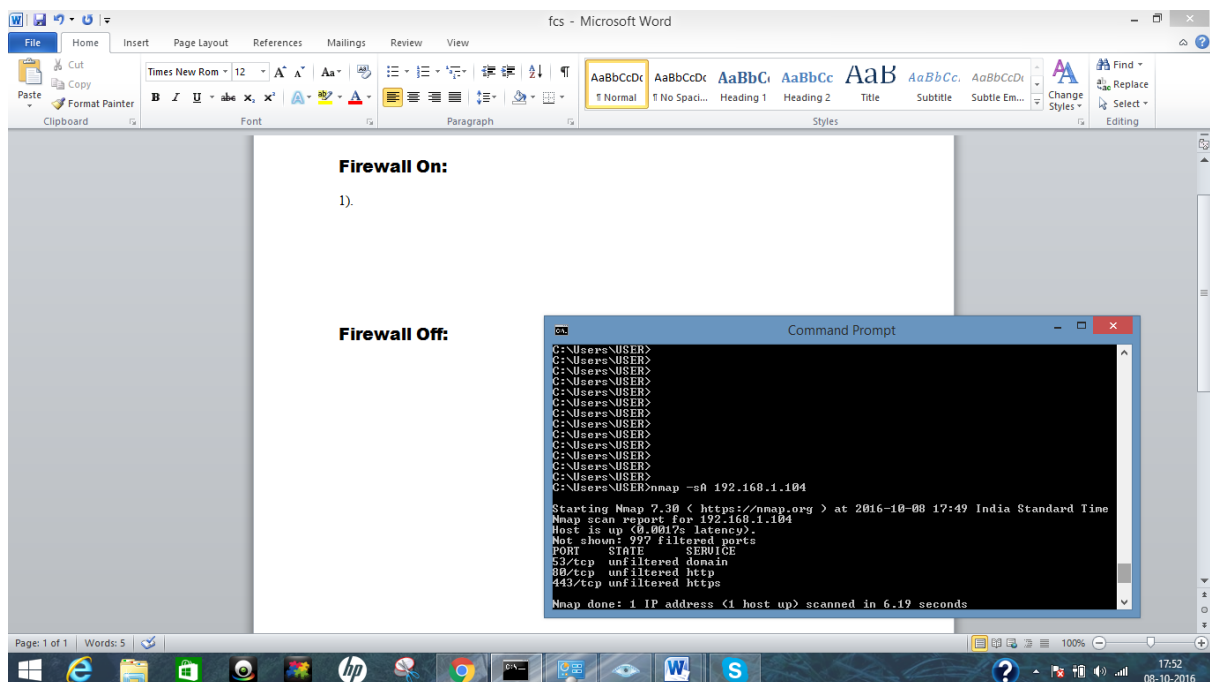
PORT STATE SERVICE

53/tcp unfiltered domain

80/tcp unfiltered http

443/tcp unfiltered https

Nmap done: 1 IP address (1 host up) scanned in 6.19 seconds



- `nmap -sW 192.168.1.104`

Starting Nmap 7.30 ( <https://nmap.org> ) at 2016-10-08 18:04 India Standard Time

Nmap scan report for 192.168.1.104

Host is up (0.0014s latency).

Not shown: 997 filtered ports

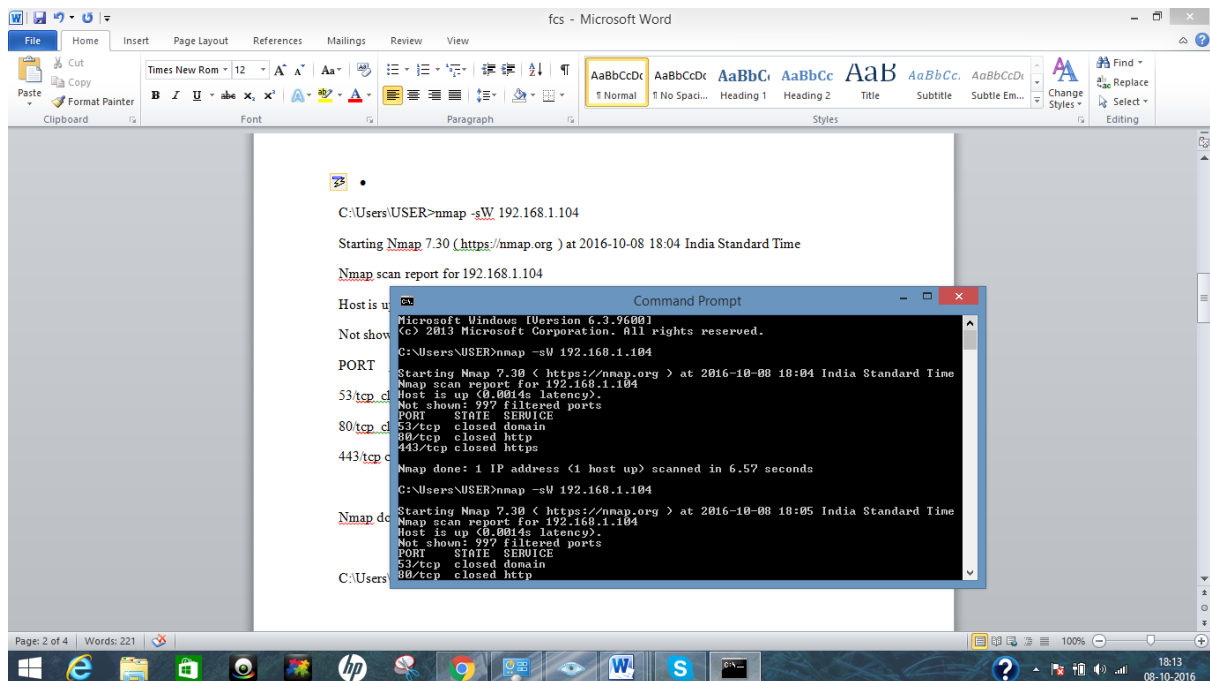
PORT STATE SERVICE

53/tcp closed domain

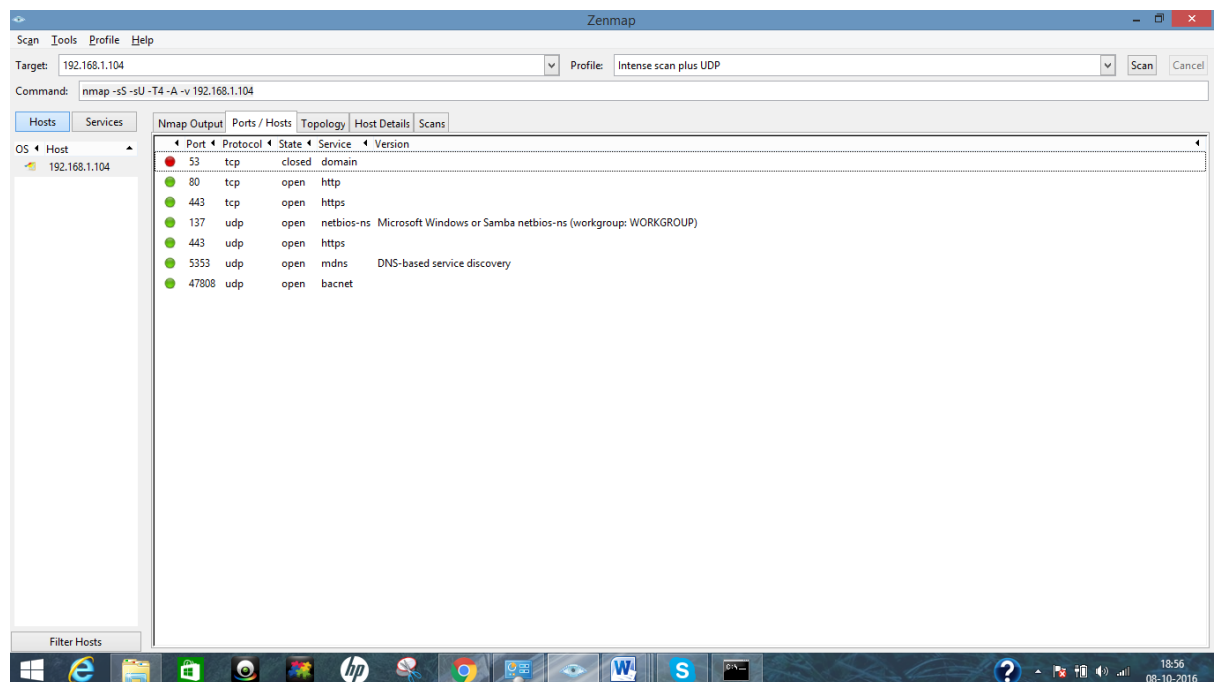
80/tcp closed http

443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 6.57 seconds



- nmap -sS -sU -T4 -A -v 192.168.1.104



Starting Nmap 7.30 ( https://nmap.org ) at 2016-10-08 18:50 India Standard Time

NSE: Loaded 142 scripts for scanning.

Completed NSE at 18:50, 0.00s elapsed

Initiating Parallel DNS resolution of 1 host. at 18:50

Completed Parallel DNS resolution of 1 host. at 18:50, 0.33s elapsed

Initiating SYN Stealth Scan at 18:50

Scanning 192.168.1.104 [1000 ports]

Discovered open port 80/tcp on 192.168.1.104

Discovered open port 443/tcp on 192.168.1.104

Completed SYN Stealth Scan at 18:50, 5.16s elapsed (1000 total ports)

Initiating UDP Scan at 18:50

Scanning 192.168.1.104 [1000 ports]

Discovered open port 443/udp on 192.168.1.104

Completed UDP Scan at 18:50, 4.33s elapsed (1000 total ports)

Initiating Service scan at 18:50

Scanning 1002 services on 192.168.1.104

Service scan Timing: About 0.40% done

Discovered open port 137/udp on 192.168.1.104

Discovered open|filtered port 137/udp on 192.168.1.104 is actually open

Discovered open port 5353/udp on 192.168.1.104

Discovered open|filtered port 5353/udp on 192.168.1.104 is actually open

Completed Service scan at 18:55, 275.88s elapsed (1002 services on 1 host)

Initiating OS detection (try #1) against 192.168.1.104

Retrying OS detection (try #2) against 192.168.1.104

NSE: Script scanning 192.168.1.104.

Discovered open port 47808/udp on 192.168.1.104

Completed NSE at 18:56, 6.73s elapsed

Nmap scan report for 192.168.1.104

NSOCK ERROR [308.6830s] mksock\_bind\_addr(): Bind to 0.0.0.0:500 failed (IOD #107):  
An attempt was made to access a socket in a way forbidden by its access permissions.  
(10013)

Host is up (0.00s latency).

Not shown: 997 filtered ports, 996 open|filtered ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

53/tcp closed domain

80/tcp open http

443/tcp open https

|\_ Supported Methods: GET

137/udp open netbios-ns Microsoft Windows or Samba netbios-ns (workgroup: WORKGROUP)

5353/udp open mdns DNS-based service discovery

47808/udp open bacnet

3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at <https://nmap.org/cgi-bin/submit.cgi?new-service>

IP ID Sequence Generation: Incremental

Service Info: Host: HP

Host script results:

| nbstat: NetBIOS name: HP, NetBIOS user: <unknown>, NetBIOS MAC: 38:b1:db:f2:bb:2b (Hon Hai Precision Ind.)

NSE: Script Post-scanning.

Initiating NSE at 18:56

Completed NSE at 18:56, 0.00s elapsed

Initiating NSE at 18:56

Completed NSE at 18:56, 0.00s elapsed

Nmap done: 1 IP address (1 host up) scanned in 327.75 seconds

Raw packets sent: 4081 (153.183KB) | Rcvd: 4227 (162.258KB)

## Firewall Off:

- nmap -sA 192.168.1.104

Starting Nmap 7.30 ( <https://nmap.org> ) at 2016-10-08 17:50 India Standard Time

Nmap scan report for 192.168.1.104

Host is up (0.0062s latency).

Not shown: 997 filtered ports

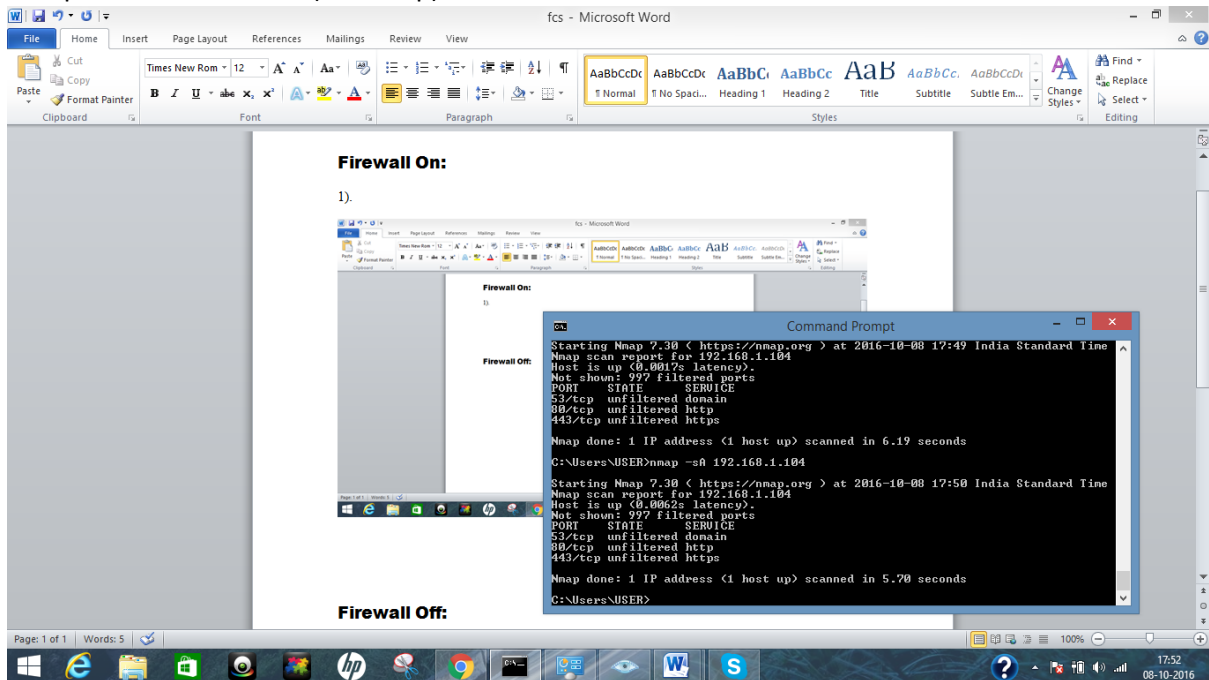
PORT STATE SERVICE

53/tcp unfiltered domain

80/tcp unfiltered http

443/tcp unfiltered https

Nmap done: 1 IP address (1 host up) scanned in 5.70 seconds



- nmap -sW 192.168.1.104

Starting Nmap 7.30 ( https://nmap.org ) at 2016-10-08 18:05 India Standard Time

Nmap scan report for 192.168.1.104

Host is up (0.0014s latency).

Not shown: 997 filtered ports

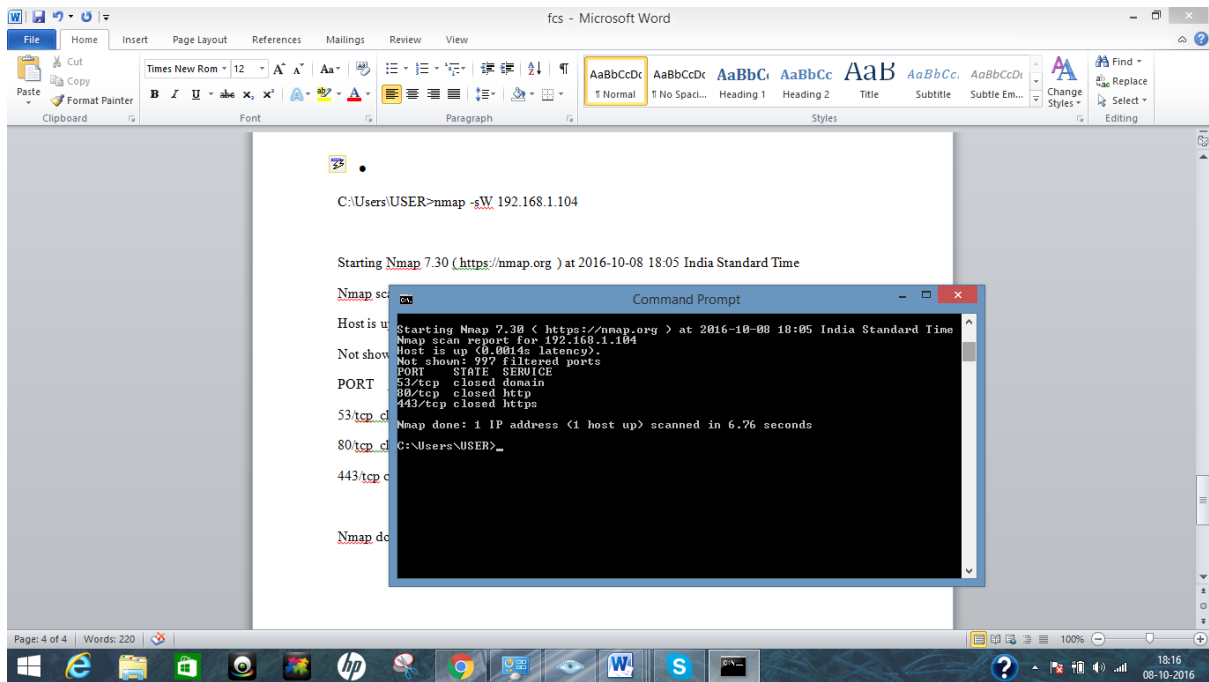
PORT STATE SERVICE

53/tcp closed domain

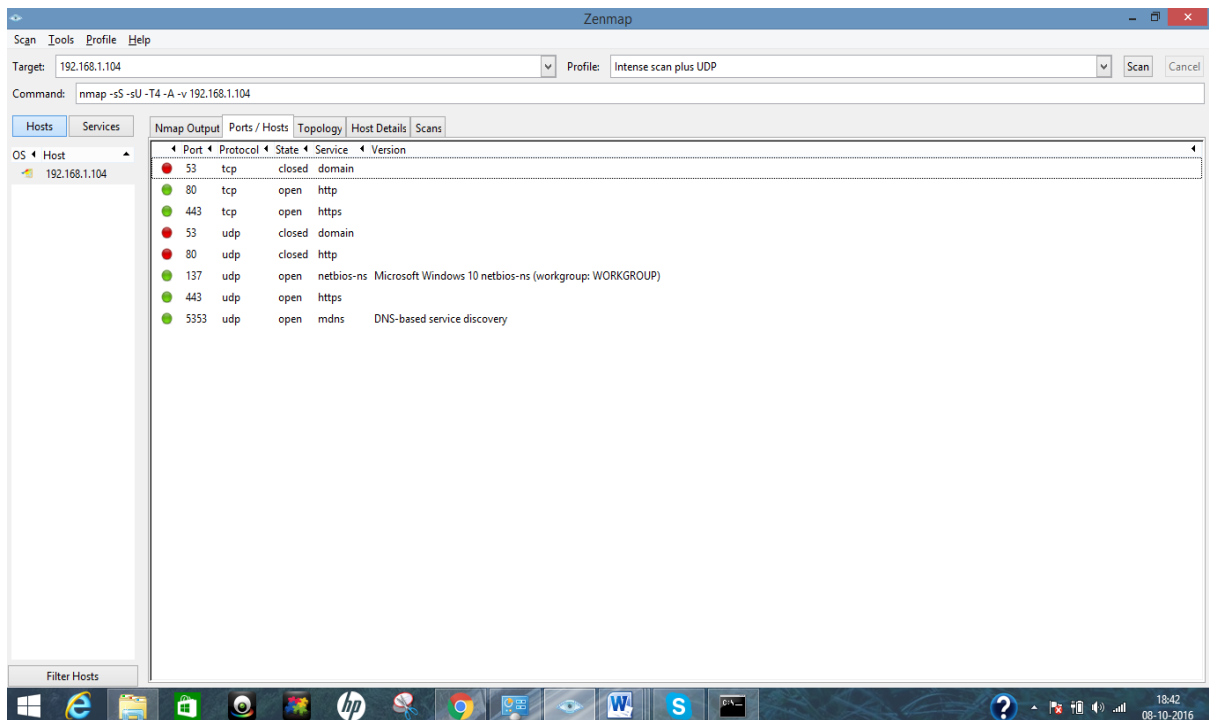
80/tcp closed http

443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 6.76 seconds



- `nmap -sS -sU -T4 -A -v 192.168.1.104`



Starting Nmap 7.30 ( <https://nmap.org> ) at 2016-10-08 18:32 India Standard Time

NSE: Loaded 142 scripts for scanning.

NSE: Script Pre-scanning.

Completed NSE at 18:32, 0.00s elapsed

Initiating Parallel DNS resolution of 1 host. at 18:32

Completed Parallel DNS resolution of 1 host. at 18:32, 0.03s elapsed



Initiating SYN Stealth Scan at 18:32

Scanning 192.168.1.104 [1000 ports]

Discovered open port 443/tcp on 192.168.1.104

Discovered open port 80/tcp on 192.168.1.104

Completed SYN Stealth Scan at 18:32, 5.31s elapsed (1000 total ports)

Completed UDP Scan at 18:32, 4.50s elapsed (1000 total ports)

Initiating Service scan at 18:32

Scanning 1000 services on 192.168.1.104

Discovered open port 137/udp on 192.168.1.104

Discovered open|filtered port 137/udp on 192.168.1.104 is actually open

Service scan Timing: About 3.80% done; ETC: 18:46 (0:13:30 remaining)

Discovered open port 5353/udp on 192.168.1.104

Discovered open|filtered port 5353/udp on 192.168.1.104 is actually open

Service scan Timing: About 89.80% done; ETC: 18:40 (0:00:46 remaining)

Initiating OS detection (try #1) against 192.168.1.104

NSE: Script scanning 192.168.1.104.

Nmap scan report for 192.168.1.104

NSOCK ERROR [475.7240s] mksock\_bind\_addr(): Bind to 0.0.0.0:500 failed (IOD #75):  
An attempt was made to access a socket in a way forbidden by its access permissions.  
(10013)

Host is up (0.00030s latency).

Not shown: 997 filtered ports, 995 open|filtered ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

53/tcp	closed	domain	
--------	--------	--------	--

80/tcp	open	http	
--------	------	------	--

443/tcp	open	https	
---------	------	-------	--

| http-methods:

|\_ Supported Methods: GET

53/udp	closed	domain	
--------	--------	--------	--

80/udp	closed	http	
--------	--------	------	--

137/udp	open	netbios-ns	Microsoft Windows 10 netbios-ns (workgroup: WORKGROUP)
---------	------	------------	--

5353/udp open mdns DNS-based service discovery

| 47989/tcp nvstream

3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

OS details: Microsoft Windows 8.1

Uptime guess: 0.175 days (since Sat Oct 08 14:29:29 2016)

Network Distance: 0 hops

TCP Sequence Prediction: Difficulty=260 (Good luck!)

IP ID Sequence Generation: Incremental

Service Info: Host: HP; OS: Windows; CPE: cpe:/o:microsoft:windows\_10

Host script results:

| nbstat: NetBIOS name: HP, NetBIOS user: <unknown>, NetBIOS MAC: 38:b1:db:f2:bb:2b (Hon Hai Precision Ind.)

NSE: Script Post-scanning.

Completed NSE at 18:41, 0.00s elapsed

Initiating NSE at 18:41

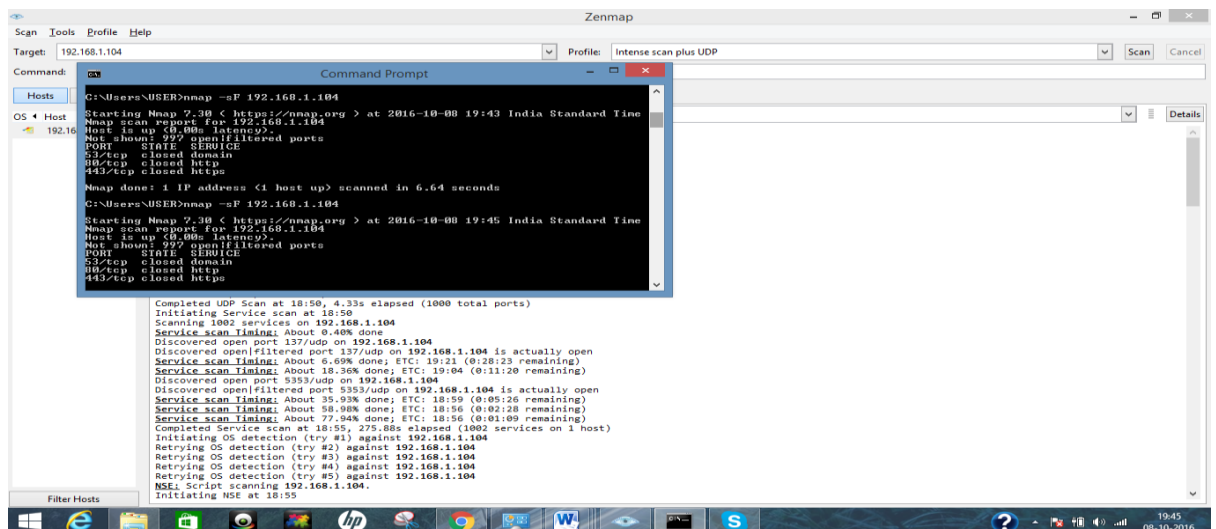
Completed NSE at 18:41, 0.00s elapsed

Nmap done: 1 IP address (1 host up) scanned in 510.19 seconds

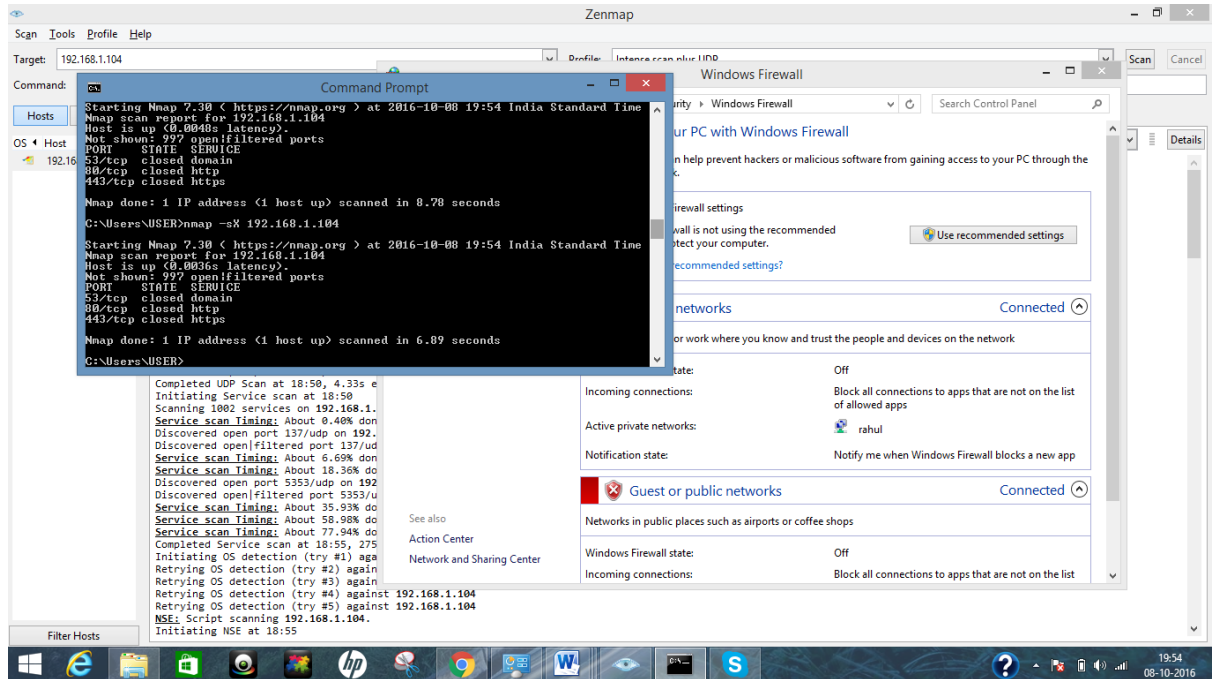
Raw packets sent: 4015 (147.159KB) | Rcvd: 8113 (299.074KB)

Other scans:

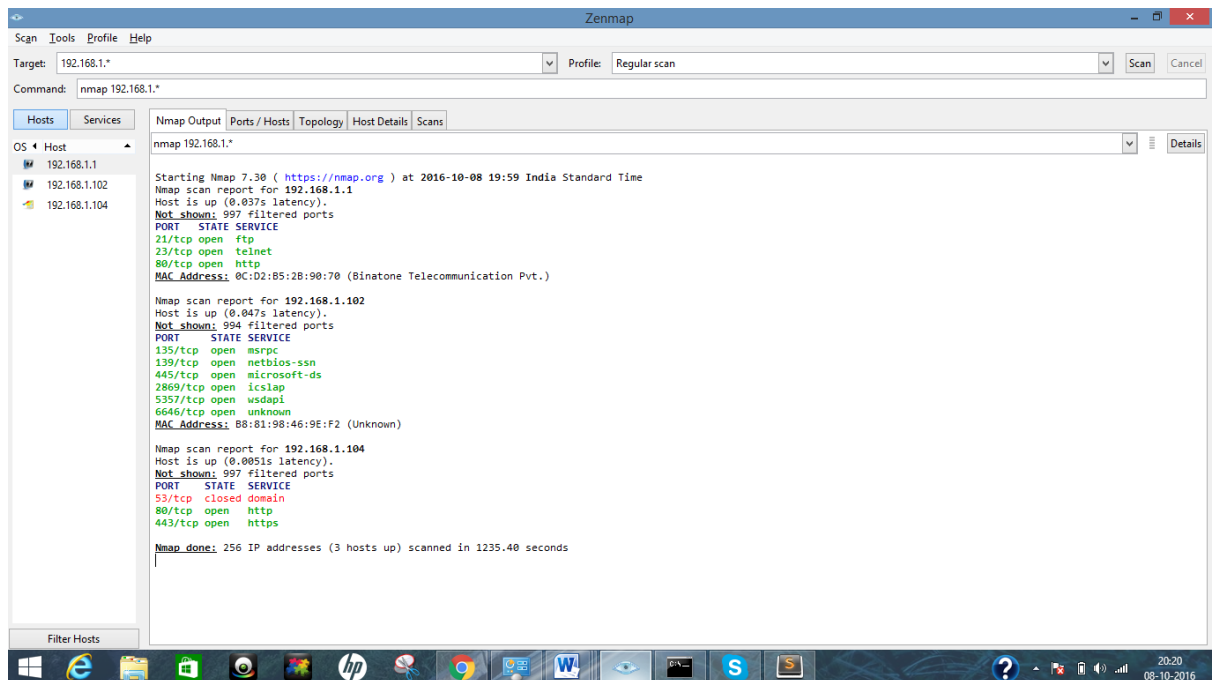
- fin scan:



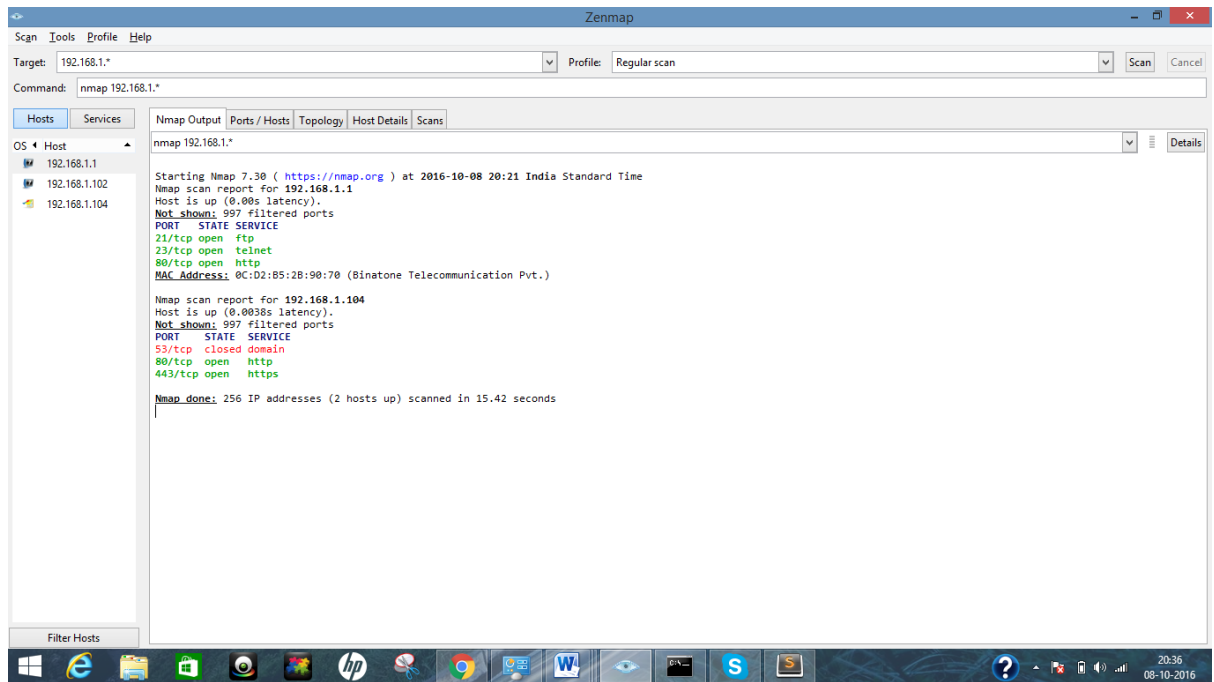
- Xmap scan:



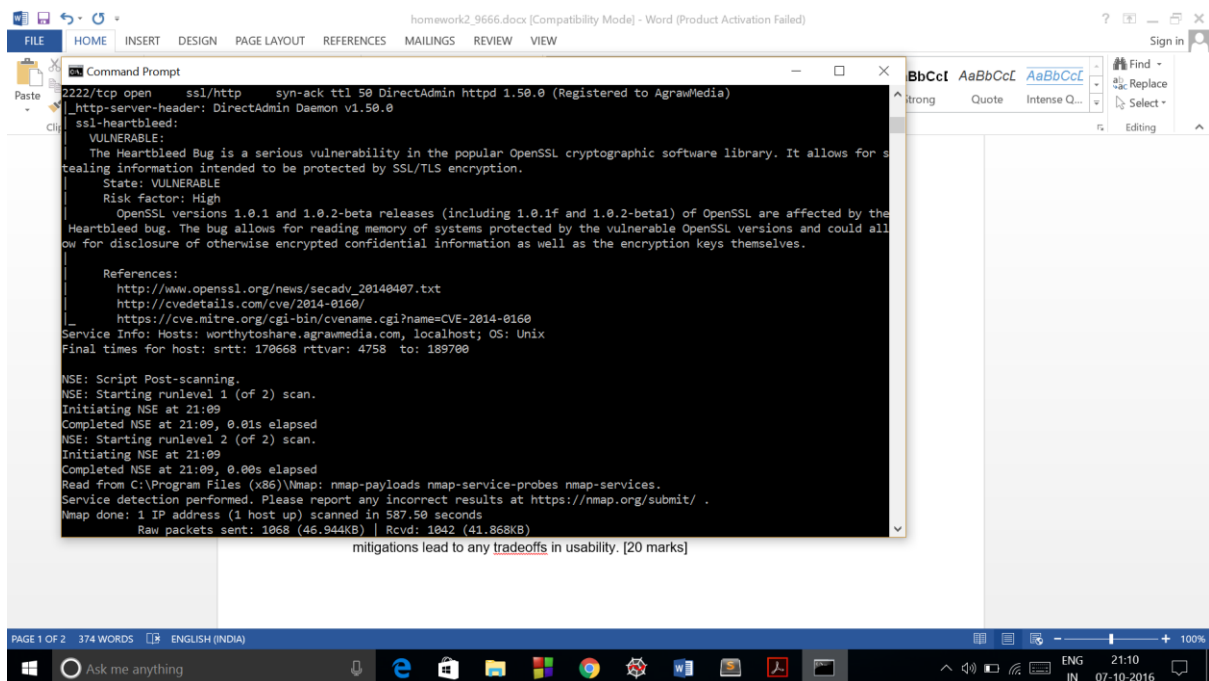
- Firewall off:



Firewall on:



Ans 3).



### A site vulnerable to heartbleed bug:

So, I first placed ssl-heratbleed.nse in scripts folder and then tls.lua in nselib folder of nmap.

```
C:\Users\lenovo>nmap -d --script ssl-heartbleed --script-args vulns.showall -sV  
www.worthytoSHARE.com
```

Starting Nmap 7.12 ( <https://nmap.org> ) at 2016-10-07 20:59 India Standard Time

PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)

Winpcap present, dynamic linked to: WinPcap version 4.1.3 (packet.dll version 4.1.0.2980),  
based on libpcap version 1.0 branch 1\_0\_rel0b (20091008)

----- Timing report -----

hostgroups: min 1, max 100000

rtt-timeouts: init 1000, min 100, max 10000

max-scan-delay: TCP 1000, UDP 1000, SCTP 1000

parallelism: min 0, max 0

max-retries: 10, host-timeout: 0

min-rate: 0, max-rate: 0

-----

NSE: Using Lua 5.2.

NSE: Arguments from CLI: vulns.showall

NSE: Arguments parsed: vulns.showall

NSE: Loaded 37 scripts for scanning.

NSE: Script Pre-scanning.

NSE: Starting runlevel 1 (of 2) scan.

Initiating NSE at 20:59

Completed NSE at 20:59, 0.00s elapsed

NSE: Starting runlevel 2 (of 2) scan.

Initiating NSE at 20:59

Completed NSE at 20:59, 0.00s elapsed

Initiating Ping Scan at 20:59

Scanning www.worthyto share.com (37.187.134.197) [4 ports]

Packet capture filter (device eth2): dst host 192.168.1.102 and (icmp or icmp6 or ((tcp or udp or sctp) and (src host 37.187.134.197)))

We got a TCP ping packet back from 37.187.134.197 port 443 (trynum = 0)

Completed Ping Scan at 20:59, 2.36s elapsed (1 total hosts)

Overall sending rates: 3.40 packets / s, 129.03 bytes / s.

mass\_rdns: Using DNS server 203.94.243.70

Initiating Parallel DNS resolution of 1 host. at 20:59

mass\_rdns: 13.43s 0/1 [#: 2, OK: 0, NX: 0, DR: 0, SF: 0, TR: 4]

Completed Parallel DNS resolution of 1 host. at 21:05, 380.71s elapsed

DNS resolution of 1 IPs took 381.15s. Mode: Async [#: 2, OK: 0, NX: 0, DR: 1, SF: 0, TR: 4, CN: 0]

Initiating SYN Stealth Scan at 21:05

Scanning www.worthyto share.com (37.187.134.197) [1000 ports]

Packet capture filter (device eth2): dst host 192.168.1.102 and (icmp or icmp6 or ((tcp or udp or sctp) and (src host 37.187.134.197)))

Discovered open port 80/tcp on 37.187.134.197

Discovered open port 143/tcp on 37.187.134.197

Increased max\_successful\_tryno for 37.187.134.197 to 1 (packet drop)

Discovered open port 465/tcp on 37.187.134.197

doAnyOutstandingRetransmits took 33ms

Increased max\_successful\_tryno for 37.187.134.197 to 2 (packet drop)

Completed SYN Stealth Scan at 21:06, 8.64s elapsed (1000 total ports)

Overall sending rates: 122.73 packets / s, 5400.02 bytes / s.

Initiating Service scan at 21:06

Scanning 12 services on www.worthyto share.com (37.187.134.197)

Completed Service scan at 21:06, 35.11s elapsed (12 services on 1 host)

NSE: Script scanning 37.187.134.197.

NSE: Starting runlevel 1 (of 2) scan.

Initiating NSE at 21:09

NSE: [ssl-heartbleed 37.187.134.197:587] we're done!

NSE: Finished http-server-header against www.worthyto share.com (37.187.134.197:2222).

NSE: Finished ssl-heartbleed against www.worthyto share.com (37.187.134.197:587).

NSE: Finished http-server-header against www.worthyto share.com (37.187.134.197:443).

Completed NSE at 21:09, 2.95s elapsed

NSE: Starting runlevel 2 (of 2) scan.

Initiating NSE at 21:09

Completed NSE at 21:09, 0.01s elapsed

Nmap scan report for www.worthyto share.com (37.187.134.197)

Host is up, received syn-ack ttl 50 (0.17s latency).

Scanned at 2016-10-07 20:59:31 India Standard Time for 586s

Not shown: 987 closed ports

Reason: 987 resets

PORT	STATE	SERVICE	REASON	VERSION
------	-------	---------	--------	---------

21/tcp	open	ftp	syn-ack ttl 51	ProFTPD 1.3.4b
--------	------	-----	----------------	----------------

| ssl-heartbleed:

| VULNERABLE:

| The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing information intended to be protected by SSL/TLS encryption. | State: VULNERABLE

| Risk factor: High

| OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading memory of systems protected by the vulnerable OpenSSL versions and could allow for disclosure of otherwise encrypted confidential information as well as the encryption keys themselves.

25/tcp open smtp syn-ack ttl 50 Exim smtpd 4.76

| ssl-heartbleed:

53/tcp open domain syn-ack ttl 50

80/tcp open http syn-ack ttl 51 Apache httpd 2

|\_http-server-header: Apache/2

110/tcp open pop3 syn-ack ttl 51 Dovecot DirectAdmin pop3d

| ssl-heartbleed

Service Info: Hosts: worthyto share.agrawmedia.com, localhost; OS: Unix

Final times for host: srtt: 170668 rttvar: 4758 to: 189700

NSE: Script Post-scanning.

NSE: Starting runlevel 1 (of 2) scan.

NSE: Starting runlevel 2 (of 2) scan.

Initiating NSE at 21:09

Completed NSE at 21:09, 0.00s elapsed

Read from C:\Program Files (x86)\Nmap: nmap-payloads nmap-service-probes nmap-services.

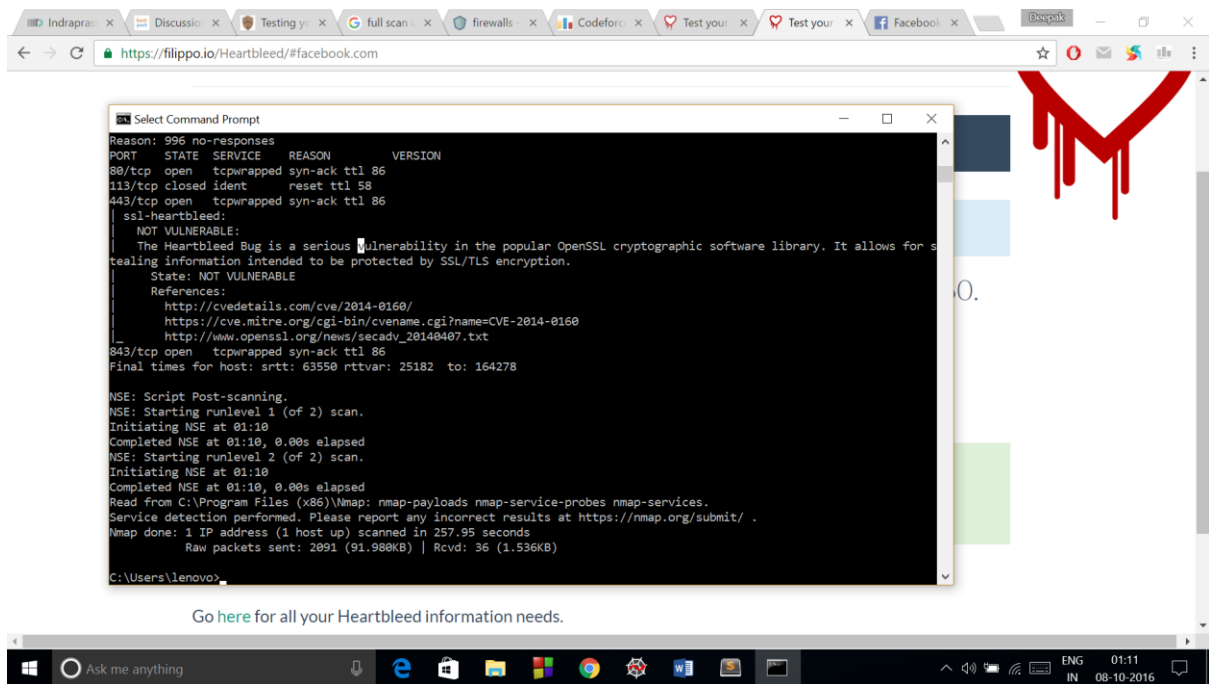
Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 587.50 seconds

Raw packets sent: 1068 (46.944KB) | Rcvd: 1042 (41.868KB)

**A site not vulnerable to heartbleed bug:**





```
C:\Users\lenovo>nmap -d --script ssl-heartbleed --script-args vulns.showall -sV  
www.facebook.com
```

Starting Nmap 7.12 ( <https://nmap.org> ) at 2016-10-08 01:06 India Standard Time

PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)

Winpcap present, dynamic linked to: WinPcap version 4.1.3 (packet.dll version 4.1.0.2980),  
based on libpcap version 1.0 branch 1\_0\_rel0b (20091008)

----- Timing report -----

hostgroups: min 1, max 100000

rtt-timeouts: init 1000, min 100, max 10000

max-scan-delay: TCP 1000, UDP 1000, SCTP 1000

parallelism: min 0, max 0

max-retries: 10, host-timeout: 0

min-rate: 0, max-rate: 0

NSE: Using Lua 5.2.

NSE: Arguments from CLI: vulns.showall

NSE: Arguments parsed: vulns.showall

NSE: Loaded 37 scripts for scanning.

NSE: Script Pre-scanning.

NSE: Starting runlevel 1 (of 2) scan.

Initiating NSE at 01:06

Completed NSE at 01:06, 0.00s elapsed

NSE: Starting runlevel 2 (of 2) scan.

Initiating NSE at 01:06

Completed NSE at 01:06, 0.00s elapsed

Initiating Ping Scan at 01:06

Scanning www.facebook.com (157.240.7.35) [4 ports]

Packet capture filter (device eth2): dst host 192.168.1.102 and (icmp or icmp6 or ((tcp or udp or sctp) and (src host 157.240.7.35)))

We got a TCP ping packet back from 157.240.7.35 port 443 (trynum = 0)

Completed Ping Scan at 01:06, 0.30s elapsed (1 total hosts)

Overall sending rates: 13.29 packets / s, 504.98 bytes / s.

mass\_rdns: Using DNS server 203.94.243.70

Initiating Parallel DNS resolution of 1 host. at 01:06

mass\_rdns: 0.56s 0/1 [#: 2, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]

Completed Parallel DNS resolution of 1 host. at 01:06, 0.11s elapsed

DNS resolution of 1 IPs took 0.56s. Mode: Async [#: 2, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]

Initiating SYN Stealth Scan at 01:06

Scanning www.facebook.com (157.240.7.35) [1000 ports]

Packet capture filter (device eth2): dst host 192.168.1.102 and (icmp or icmp6 or ((tcp or udp or sctp) and (src host 157.240.7.35)))

Discovered open port 443/tcp on 157.240.7.35

Discovered open port 80/tcp on 157.240.7.35

doAnyOutstandingRetransmits took 130ms

Discovered open port 843/tcp on 157.240.7.35

doAnyOutstandingRetransmits took 64ms

SYN Stealth Scan Timing: About 53.65% done; ETC: 01:07 (0:00:30 remaining)

doAnyOutstandingRetransmits took 34ms

Increasing send delay for 157.240.7.35 from 40 to 80 due to 11 out of 11 dropped probes since last increase.

doAnyOutstandingRetransmits took 65ms

Destroying timed-out global ping from 157.240.7.35.

Completed SYN Stealth Scan at 01:09, 187.14s elapsed (1000 total ports)

Overall sending rates: 11.15 packets / s, 490.71 bytes / s.

Initiating Service scan at 01:09

Scanning 3 services on www.facebook.com (157.240.7.35)

Got nsock CONNECT response with status TIMEOUT - aborting this service

Completed Service scan at 01:09, 5.00s elapsed (3 services on 1 host)

NSE: Script scanning 157.240.7.35.

NSE: Starting runlevel 1 (of 2) scan.

Initiating NSE at 01:09

NSE: Finished http-server-header against www.facebook.com (157.240.7.35:80).

NSE Timing: About 99.07% done; ETC: 01:10 (0:00:01 remaining)

NSE: Finished ssl-heartbleed against www.facebook.com (157.240.7.35:443).

Completed NSE at 01:10, 63.36s elapsed

NSE: Starting runlevel 2 (of 2) scan.

Initiating NSE at 01:10

Completed NSE at 01:10, 0.00s elapsed

Nmap scan report for www.facebook.com (157.240.7.35)

Host is up, received syn-ack ttl 86 (0.064s latency).

rDNS record for 157.240.7.35: edge-star-mini-shv-01-sin6.facebook.com

Scanned at 2016-10-08 01:06:42 India Standard Time for 256s

Not shown: 996 filtered ports

Reason: 996 no-responses

PORT	STATE	SERVICE	REASON	VERSION
------	-------	---------	--------	---------

80/tcp	open	tcpwrapped	syn-ack ttl 86	
--------	------	------------	----------------	--

113/tcp	closed	ident	reset ttl 58	
---------	--------	-------	--------------	--

443/tcp	open	tcpwrapped	syn-ack ttl 86	
---------	------	------------	----------------	--

| ssl-heartbleed:

| NOT VULNERABLE:

| The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing information intended to be protected by SSL/TLS encryption.

| State: NOT VULNERABLE

843/tcp open tcpwrapped syn-ack ttl 86

Final times for host: srtt: 63550 rttvar: 25182 to: 164278

NSE: Script Post-scanning.

NSE: Starting runlevel 1 (of 2) scan.

Initiating NSE at 01:10

Completed NSE at 01:10, 0.00s elapsed

NSE: Starting runlevel 2 (of 2) scan.

Initiating NSE at 01:10

Completed NSE at 01:10, 0.00s elapsed

Read from C:\Program Files (x86)\Nmap: nmap-payloads nmap-service-probes nmap-services.

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 257.95 seconds

Raw packets sent: 2091 (91.980KB) | Rcvd: 36 (1.536KB)

Ans 4).

•

IIIT-Delhi Library:

a). Threat: Default password provided by IIIT-Delhi Library is of the form: first three letters are the first three initial of the student's name and last three letters are last three letter of student's roll number.

So adversary over here can guess password of person and issue library book on behalf of other person.

Entry/exit point: library.iiitd.edu.in

Dread Analysis:

Damage Potential: Since if this vulnerability is exploited, it can lead to a security or privacy breach. A student may be booked for a book which he hasn't issued. Score: 8

Reproducibility: The attack will work most of the time, since it is quite easy to guess the password. Score: 7

Exploitability: This threat exploit security and privacy. Knowing ones password is a grave concern. Score: 7

Affected Users: All the students of IIIT-D. Score: 8

Discoverability: The vulnerability can be found quite easily as every student knows about it. Score: 7

Hence average threat rating of this threat is 7.4 which can be considered high.

Mitigation: IIIT-D should make a unique and complex password difficult to break. This should be sent to the mail of the person so that he can login and the if he want to change he is allowed to do so.

There is tradeoff in usability as last password was quite easy but could be easily hacked. However, here there is a complex password but it is difficult to learn.

•

Threat: The back gate at 1<sup>st</sup> floor in IIITD is left open sometimes. So, adversary over here can enter the library and steal precious items of library.

Entry/exit point: Library building.

Dread Analysis:

Damage Potential: Since if this vulnerability is exploited, it can lead to a security. Property of IIITD is at risk over here. Score: 6

Reproducibility: The attack will work when the gate is left open and guard is not vigilant enough. Score: 6

Exploitability: This threat exploit security. Books, printer, desktop, etc are at risk over here. Score: 5

Affected: Items kept in IIIT-D. Score: 5

Discoverability: The vulnerability can be found by adversary upon proper investigation.

Score: 5

Hence average threat rating of this threat is 5.4 which can be considered as medium.

Mitigation: IIIT-D should keep the door closed for proper security.

There is tradeoff in usability as people can't use rear door which would lead them to hostel or metro station quickly.

b).

•

IIIT-Delhi ERP

Threat: Denial Of Service( DOS or DDOS ) attack can be done on [erp.iiitd.edu.in](http://erp.iiitd.edu.in). The website may be pinged in short duration such that it becomes unavailable temporarily at critical times when one has to pay the fees or apply for hostel.

Entry/exit point: [erp.iiitd.edu.in](http://erp.iiitd.edu.in)

DREAD Analysis:

Damage Potential: Since if this vulnerability is exploited, it can lead to many disastrous situation where person may not be able to pay fees, allot grades at times when required.

Score: 8

Reproducibility: The attack will work most of the time, since it is quite easy to perform DOS attacks. There are many online tutorials for this too. Score: 7

Exploitability: Adversary over here can easily exploit this discoverability. Score: 7

Affected users: All students and faculty of IIITD. Score: 9

Discoverability: If site becomes unresponsive then it is can be discovered. Score: 7

Average Score: 8 which is high.

Mitigation: IIIT-D should have routers or firewalls that prevent the unnecessary traffic.

There is tradeoff in usability as special routers and firewalls are much expensive as compared to previous one.

•

Threat: Brute force attack to detect password of a person can be performed on [erp](http://erp.iiitd.edu.in) as there is no count maintained for bad attempt in writing the password.

Entry/exit point: [erp.iiitd.edu.in](http://erp.iiitd.edu.in)

DREAD Analysis:

Damage Potential: Since if this vulnerability is exploited, it can lead to many disastrous situation, where person grades, personal information, etc will be known to everyone else.

Score: 6

Reproducibility: The attack will work if somebody guesses the password correctly.

Score: 5

Exploitability: Adversary over here can easily exploit this discoverability.

Score: 5

Affected users: All students and faculty of IIITD.

Score: 5

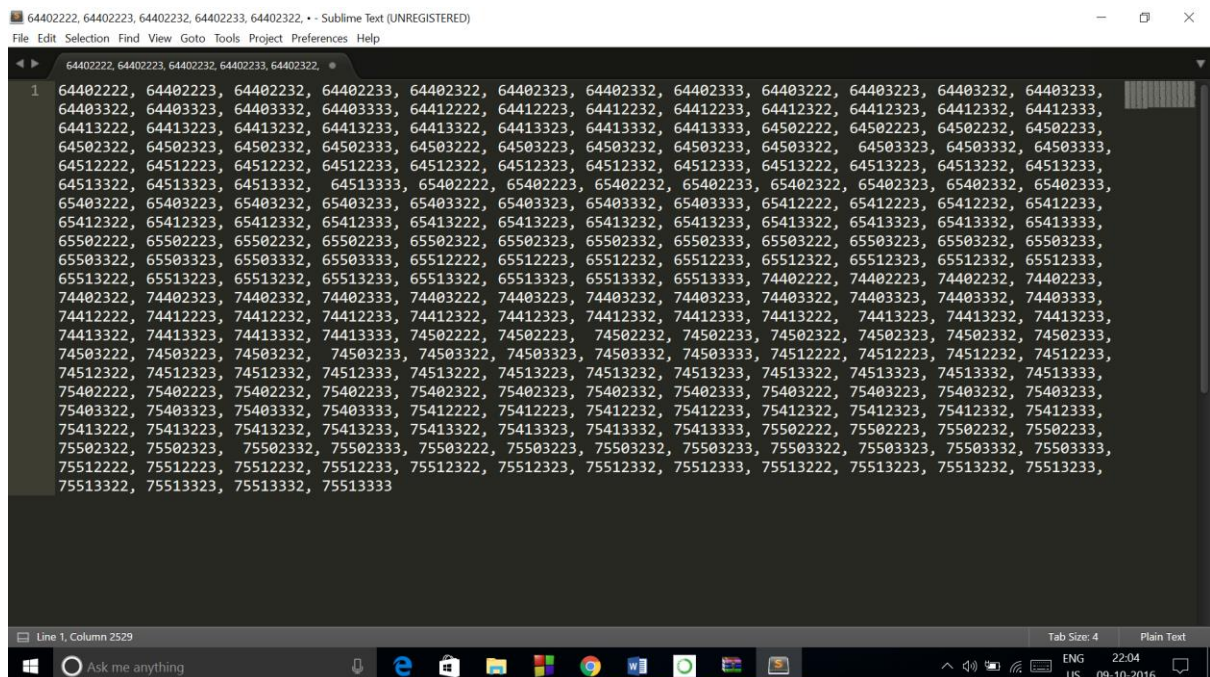
Discoverability: It can be found easily by person.

Score: 5

Average Score: 5.2 which is considered as medium.

Mitigation: There should be 1 min gap if one fail to enter correct password 3 times.

There is tradeoff in usability as in genuine case one person may find it extremely time taking.



Ans 5).

Code:

“”

```
from Crypto.Cipher import DES
```

```
quotes = ["" for x in range(10)]
```

```
quotes[0] = b'I can resist everything except temptation'
```

```

quotes[1] = b'We are all in the gutter but some of us are looking at the stars'
quotes[2] = b'Always forgive your enemies - nothing annoys them so much'
quotes[3] = b'Experience is simply the name we give our mistakes'
quotes[4] = b'What is a cynic A man who knows the price of everything and the value of
nothing'
quotes[5] = b'To live is the rarest thing in the world Most people exist that is all'
quotes[6] = b'Be yourself everyone else is already taken'
quotes[7] = b'There is only one thing in the world worse than being talked about and that is
not being talked about'
quotes[8] = b'To love oneself is the beginning of a lifelong romance'
quotes[9] = b'Some cause happiness wherever they go others whenever they go'

cipher_text =
b"\xc5\x81\x97~\xb4\x0b:U\x13^\x9c\xb2:\xedcC\xe5\n\xab\xb2\xbas\xbe/r\xa8\x00'\x87\x9
1Ch\xb8\x060\xfb\x8V\xf7)\x1d\xfb\x12\xe7\x16\xf0\x12\x1dQ\x99Gs`\xf5qZjQL\xe1\x1f\
xfd\x90E"

flag = 0

for i in range(0, 100000000):
    key = str( i )
    while( len(key)<8 ):
        key = '0' + key
    des = DES.new(key, DES.MODE_ECB)
    decrypted_pt = des.decrypt(cipher_text)
    for j in range(10):
        if quotes[j] in decrypted_pt:
            print(decrypted_pt)
            print(key)
            flag = 1
            break
    if( flag==1 ):
        break
    ''

```

(There are other keys too which satisfy the quote but I have mentioned only one).



So the quote is: We are all in the gutter but some of us are looking at the stars

Key is: 64402222