

Name: Muhammad Nadeem
Roll no: 201980050
Section: B
Course: Information Security
Submitted to: Sir Aleem Awan

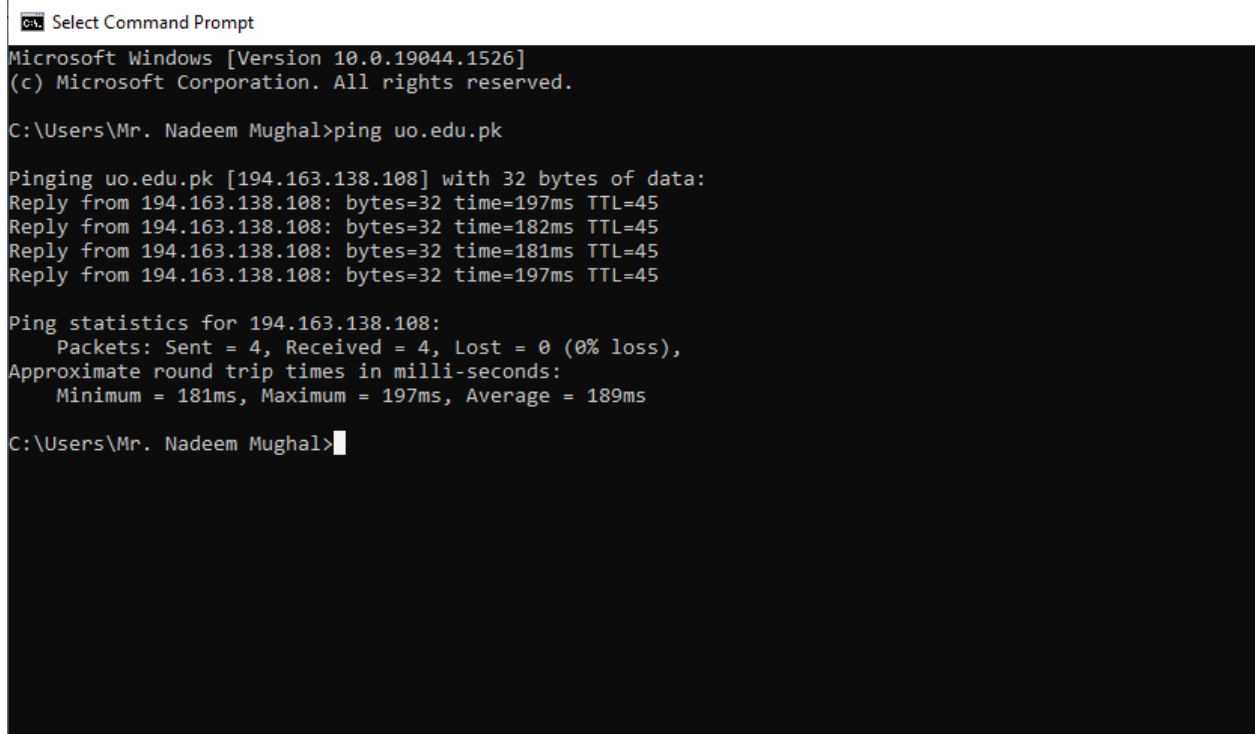
Targeted Website:

<https://www.uo.edu.pk>

Tool Name:

Zenmap

Find Ip address through cmd.



```

Select Command Prompt
Microsoft Windows [Version 10.0.19044.1526]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Mr. Nadeem Mughal>ping uo.edu.pk

Pinging uo.edu.pk [194.163.138.108] with 32 bytes of data:
Reply from 194.163.138.108: bytes=32 time=197ms TTL=45
Reply from 194.163.138.108: bytes=32 time=182ms TTL=45
Reply from 194.163.138.108: bytes=32 time=181ms TTL=45
Reply from 194.163.138.108: bytes=32 time=197ms TTL=45

Ping statistics for 194.163.138.108:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 181ms, Maximum = 197ms, Average = 189ms

C:\Users\Mr. Nadeem Mughal>
```

Ip address paste in Zenmap and scan it.

Zenmap

Scan Tools Profile Help

Target: 194.163.138.108 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 194.163.138.108

Hosts Services

OS Host

uodupk.uo.edu.pk

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v 194.163.138.108

Network Distance: 21 hops
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 22/tcp)

HOP	RTT	ADDRESS
1	3.00 ms	192.168.43.1
2	...	
3	33.00 ms	10.253.10.193
4	...	5
6	28.00 ms	10.253.10.1
7	42.00 ms	10.253.14.252
8	39.00 ms	10.253.0.186
9	44.00 ms	10.232.111.41
10	43.00 ms	static-host119-30-106-57.link.net.pk (119.30.106.57)
11	155.00 ms	tw249-static184.tw1.com (110.93.249.184)
12	54.00 ms	tw255-static26.tw1.com (110.93.255.26)
13	152.00 ms	110.93.252.190
14	142.00 ms	110.93.253.22
15	198.00 ms	be4932.agr21.mrs01.atlas.cogentco.com (149.14.125.89)
16	203.00 ms	be2345.ccr21.mrs01.atlas.cogentco.com (154.54.38.169)
17	196.00 ms	be2751.ccr31.mrs02.atlas.cogentco.com (154.54.37.250)
18	304.00 ms	ae-24.edge4.Marseille1.Level3.net (4.68.111.245)
19	208.00 ms	ae1.3107.edge6.Dusseldorf1.Level3.net (4.69.161.194)
20	209.00 ms	GIGA-HOSTIN.edge6.Dusseldorf1.Level3.net (62.67.22.194)
21	207.00 ms	uodupk.uo.edu.pk (194.163.138.108)

NSE: Script Post-scanning.
Initiating NSE at 09:11
Completed NSE at 09:11, 0.00s elapsed
Initiating NSE at 09:11
Completed NSE at 09:11, 0.00s elapsed
Initiating NSE at 09:11
Completed NSE at 09:11, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.
Nmap done: 1 IP address (1 host up) scanned in 309.17 seconds
Raw packets sent: 2098 (95.892KB) | Rcvd: 345 (31.283KB)

Zenmap

Scan Tools Profile Help

Target: 194.163.138.108 Profile: Intense scan Scan Cancel

Command: nmap -T4 -A -v 194.163.138.108

Hosts Services

OS Host

uodupk.uo.edu.pk

Nmap Output Ports / Hosts Topology Host Details Scans

Port	Protocol	State	Service	Version
20	tcp	closed	ftp-data	
21	tcp	open	ftp	Pure-FTPd
22	tcp	closed	ssh	
25	tcp	open	smtp	
53	tcp	open	domain	PowerDNS Authoritative Server 4.4.1
80	tcp	open	http	Apache httpd
110	tcp	open	pop3	Dovecot pop3d
143	tcp	open	imap	Dovecot imapd
443	tcp	open	http	Apache httpd
465	tcp	open	smtp	Exim smtpd 4.94.2
587	tcp	open	smtp	Exim smtpd 4.94.2
993	tcp	open	imaps	
995	tcp	open	pop3s	
8443	tcp	closed	https-alt	

