**NAME : ADARSH M. MENDHE**

**Assignment Day 4**

**Question 1:**

Find out the mail servers of the following domain :

Ibm.com

Wipro.com

1. **Ibm.com**

**Open terminal**

**Command: sublist3r**

**\_\_\_\_ \_ \_ \_ \_ \_\_\_\_\_**

**/ \_\_\_| \_ \_| |\_\_ | (\_)\_\_\_| |\_|\_\_\_ / \_ \_\_**

**\\_\_\_ \| | | | '\_ \| | / \_\_| \_\_| |\_ \| '\_\_|**

**\_\_\_) | |\_| | |\_) | | \\_\_ \ |\_ \_\_\_) | |**

**|\_\_\_\_/ \\_\_,\_|\_.\_\_/|\_|\_|\_\_\_/\\_\_|\_\_\_\_/|\_|**

**Usage: python3 /usr/lib/python3/dist-packages/sublist3r.py [Options] use -h for help**

**Error: the following arguments are required: -d/--domain**

**root@kali:~# sublist3r -help**

**usage: sublist3r.py [-h] -d DOMAIN [-b [BRUTEFORCE]] [-p PORTS] [-v [VERBOSE]] [-t THREADS] [-e ENGINES] [-o OUTPUT] [-n]**

**OPTIONS:**

**-h, --help show this help message and exit**

**-d DOMAIN, --domain DOMAIN**

**Domain name to enumerate it's subdomains**

**-b [BRUTEFORCE], --bruteforce [BRUTEFORCE]**

**Enable the subbrute bruteforce module**

**-p PORTS, --ports PORTS**

**Scan the found subdomains against specified tcp ports**

**-v [VERBOSE], --verbose [VERBOSE]**

**Enable Verbosity and display results in realtime**

**-t THREADS, --threads THREADS**

**Number of threads to use for subbrute bruteforce**

**-e ENGINES, --engines ENGINES**

**Specify a comma-separated list of search engines**

**-o OUTPUT, --output OUTPUT**

**Save the results to text file**

**-n, --no-color Output without color**

**Example: python3 /usr/lib/python3/dist-packages/sublist3r.py -d google.com**

**root@kali:~# sublist3r -d ibm.com -e bing -t 2 -p 443**

**[-] Enumerating subdomains now for ibm.com**

**[-] Searching now in Bing..**

**[-] Total Unique Subdomains Found: 83**

**[-] Start port scan now for the following ports: 443**

**developer.ibm.com - Found open ports: 443**

**community.ibm.com - Found open ports: 443**

**my15.digitalexperience.ibm.com - Found open ports: 443**

**my13.digitalexperience.ibm.com - Found open ports: 443**

**service5.boulder.ibm.com - Found open ports: 443**

**publib.boulder.ibm.com - Found open ports: 443**

**publibz.boulder.ibm.com - Found open ports: 443**

**ibmdc.comprehend.ibm.com - Found open ports: 443**

**dtsc.dfw.ibm.com - Found open ports: 443**

**gbsjira.in.edst.ibm.com - Found open ports: 443**

**publib16.boulder.ibm.com - Found open ports: 443**

**csc.cn.ibm.com - Found open ports: 443**

**my12.digitalexperience.ibm.com - Found open ports: 443**

**public.dhe.ibm.com - Found open ports: 443**

**www.itc.de.ibm.com - Found open ports: 443**

**my14.digitalexperience.ibm.com - Found open ports: 443**

**my7.digitalexperience.ibm.com - Found open ports: 443**

**careers.ibm.com - Found open ports: 443**

**mediacenter-test.ibm.com - Found open ports: 443**

**render-prd-trops.events.ibm.com - Found open ports: 443**

**bcrs-portal.ibm.com - Found open ports: 443**

**pforg.ibm.com - Found open ports: 443**

**mysa.ibm.com - Found open ports: 443**

**dstuid-ww.dst.ibm.com - Found open ports: 443**

**optimizer.ibm.com - Found open ports: 443**

**watson.media.ibm.com - Found open ports: 443**

**cloud.ibm.com - Found open ports: 443**

**referrals.ibm.com - Found open ports: 443**

**www.research.ibm.com - Found open ports: 443**

**associate.comprehend.ibm.com - Found open ports: 443**

**dominoweb.draco.res.ibm.com - Found open ports: 443**

**ismnac.ibm.com - Found open ports: 443**

**learn.ibm.com - Found open ports: 443**

**pairs.res.ibm.com - Found open ports: 443**

**research.ibm.com - Found open ports: 443**

**www.redbooks.ibm.com - Found open ports: 443**

**newsroom.ibm.com - Found open ports: 443**

**mediacenter.ibm.com - Found open ports: 443**

**w3id.sso.ibm.com - Found open ports: 443**

**esls2.eu.smi.ibm.com - Found open ports: 443**

**portal.sec.ibm.com - Found open ports: 443**

**techsupport.services.ibm.com - Found open ports: 443**

**ism.smi.ibm.com - Found open ports: 443**

**digitaltwinexchange.ibm.com - Found open ports: 443**

**w3id.alpha.sso.ibm.com - Found open ports: 443**

**w3idprofile.sso.ibm.com - Found open ports: 443**

**iccve.uk.ibm.com - Found open ports: 443**

**video.ibm.com - Found open ports: 443**

**www-01.ibm.com - Found open ports: 443**

**www.vm.ibm.com - Found open ports: 443**

**www14.software.ibm.com - Found open ports: 443**

**domino.watson.ibm.com - Found open ports: 443**

**food.ibm.com - Found open ports: 443**

**researcher.watson.ibm.com - Found open ports: 443**

**www-07.ibm.com - Found open ports: 443**

**cmoc.m7.ism.br.ibm.com - Found open ports: 443**

**www-05.ibm.com - Found open ports: 443**

**www-03.ibm.com - Found open ports: 443**

**supportcontent.ibm.com - Found open ports: 443**

**www-356.ibm.com - Found open ports: 443**

**www-2000.ibm.com - Found open ports: 443**

**www-150.ibm.com - Found open ports: 443**

**www-903.ibm.com - Found open ports: 443**

**www-31.ibm.com - Found open ports: 443**

**www-750.ibm.com - Found open ports: 443**

**www-946.ibm.com - Found open ports: 443**

**www-912.ibm.com - Found open ports: 443**

**www.zurich.ibm.com - Found open ports: 443**

**links.spop.ibm.com - Found open ports: 443**

**yourlearning.ibm.com - Found open ports: 443**

**www-355.ibm.com - Found open ports: 443**

**www-945.ibm.com - Found open ports: 443**

**my.enterprisecloud.mgapp.ibm.com - Found open ports: 443**

**quantum-computing.ibm.com - Found open ports: 443**

**www-store.shop.ibm.com - Found open ports: 443**

**events.tools.ibm.com - Found open ports: 443**

**reg.tools.ibm.com - Found open ports: 443**

**2)Wipro.com**

**root@kali:~# sublist3r -d wipro.com -e bing -t 2 -p 443**

**\_\_\_\_ \_ \_ \_ \_ \_\_\_\_\_**

**/ \_\_\_| \_ \_| |\_\_ | (\_)\_\_\_| |\_|\_\_\_ / \_ \_\_**

**\\_\_\_ \| | | | '\_ \| | / \_\_| \_\_| |\_ \| '\_\_|**

**\_\_\_) | |\_| | |\_) | | \\_\_ \ |\_ \_\_\_) | |**

**|\_\_\_\_/ \\_\_,\_|\_.\_\_/|\_|\_|\_\_\_/\\_\_|\_\_\_\_/|\_|**

**[-] Enumerating subdomains now for wipro.com**

**[-] Searching now in Bing..**

**[-] Total Unique Subdomains Found: 29**

**[-] Start port scan now for the following ports: 443**

**basepdc.wipro.com - Found open ports: 443**

**mysupplierbuddy.wipro.com - Found open ports: 443**

**myfileshare.wipro.com - Found open ports: 443**

**shine.wipro.com - Found open ports: 443**

**sftp.wipro.com - Found open ports: 443**

**baseharmony.wipro.com - Found open ports: 443**

**itam.wipro.com - Found open ports: 443**

**crystalowafarm.wipro.com - Found open ports: 443**

**iverify.wipro.com - Found open ports: 443**

**feedback.wipro.com - Found open ports: 443**

**careers.wipro.com - Found open ports: 443**

**synergy.wipro.com - Found open ports: 443**

**securityintelligence.wipro.com - Found open ports: 443**

**talenttransformation.wipro.com - Found open ports: 443**

**topgear-app.wipro.com - Found open ports: 443**

**wipfs01.wipro.com - Found open ports: 443**

**wfm.wipro.com - Found open ports: 443**

**webmail.wipro.com - Found open ports: 443**

**wscloudapp.wipro.com - Found open ports: 443**

**catalyst.wipro.com - Found open ports: 443**

**go.wipro.com - Found open ports: 443**

**cloudapp.wipro.com - Found open ports: 443**

**crystalaz.wipro.com - Found open ports: 443**

**Question 3:**

Scan and find out port numbers open 203.163.246.23

Open terminal

Command:

root@kali:~# **nmap -Pn -sS -A -v 203.163.246.23**

Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 13:57 IST

NSE: Loaded 151 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 13:57

Completed NSE at 13:57, 0.00s elapsed

Initiating NSE at 13:57

Completed NSE at 13:57, 0.00s elapsed

Initiating NSE at 13:57

Completed NSE at 13:57, 0.00s elapsed

Initiating Parallel DNS resolution of 1 host. at 13:57

Completed Parallel DNS resolution of 1 host. at 13:57, 0.10s elapsed

Initiating SYN Stealth Scan at 13:57

Scanning 203.163.246.23 [1000 ports]

Discovered open port 110/tcp on 203.163.246.23

Increasing send delay for 203.163.246.23 from 0 to 5 due to 11 out of 14 dropped probes since last increase.

Increasing send delay for 203.163.246.23 from 5 to 10 due to 11 out of 11 dropped probes since last increase.

Completed SYN Stealth Scan at 13:58, 52.91s elapsed (1000 total ports)

Initiating Service scan at 13:58

Scanning 1 service on 203.163.246.23

Completed Service scan at 14:00, 156.36s elapsed (1 service on 1 host)

Initiating OS detection (try #1) against 203.163.246.23

Initiating Traceroute at 14:01

Completed Traceroute at 14:01, 0.03s elapsed

Initiating Parallel DNS resolution of 2 hosts. at 14:01

Completed Parallel DNS resolution of 2 hosts. at 14:01, 0.01s elapsed

NSE: Script scanning 203.163.246.23.

Initiating NSE at 14:01

Completed NSE at 14:01, 21.21s elapsed

Initiating NSE at 14:01

Completed NSE at 14:01, 21.03s elapsed

Initiating NSE at 14:01

Completed NSE at 14:01, 0.00s elapsed

Nmap scan report for 203.163.246.23

Host is up (0.0040s latency).

Not shown: 998 filtered ports

PORT STATE SERVICE VERSION

25 /tcp closed smtp

110 /tcp open pop3

Device type: general purpose

Running: Linux 2.4.X|3.X

OS CPE: cpe:/o:linux:linux\_kernel:2.4.37 cpe:/o:linux:linux\_kernel:3.2

OS details: DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2

Network Distance: 2 hops

TCP Sequence Prediction: Difficulty=256 (Good luck!)

IP ID Sequence Generation: Busy server or unknown class

TRACEROUTE (using port 25/tcp)

HOP RTT ADDRESS

1 1.86 ms 192.168.56.2

2 1.97 ms 203.163.246.23

NSE: Script Post-scanning.

I

