

# CSE3501-Information Security Analysis and Audit Lab

NAME- HRITIK DUBEY REG NO-19BIT0150 SLOT- L41+L42

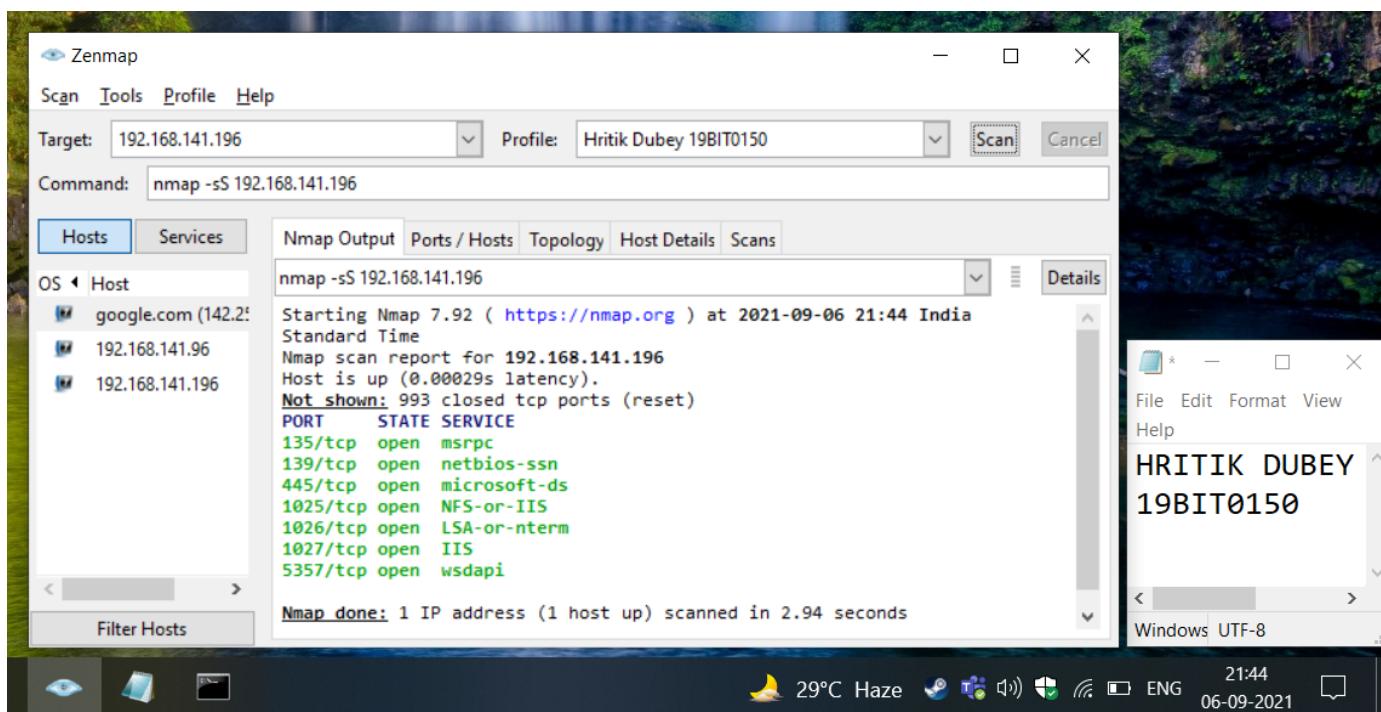
## DIGITAL ASSIGNMENT 1

Faculty : Dr. Priya V

**1. A security engineer of VIT- Vellore is attempting to map a company's internal network and he wants to perform the stealth scan. Which NMAP command would the security engineer use? Show the results**

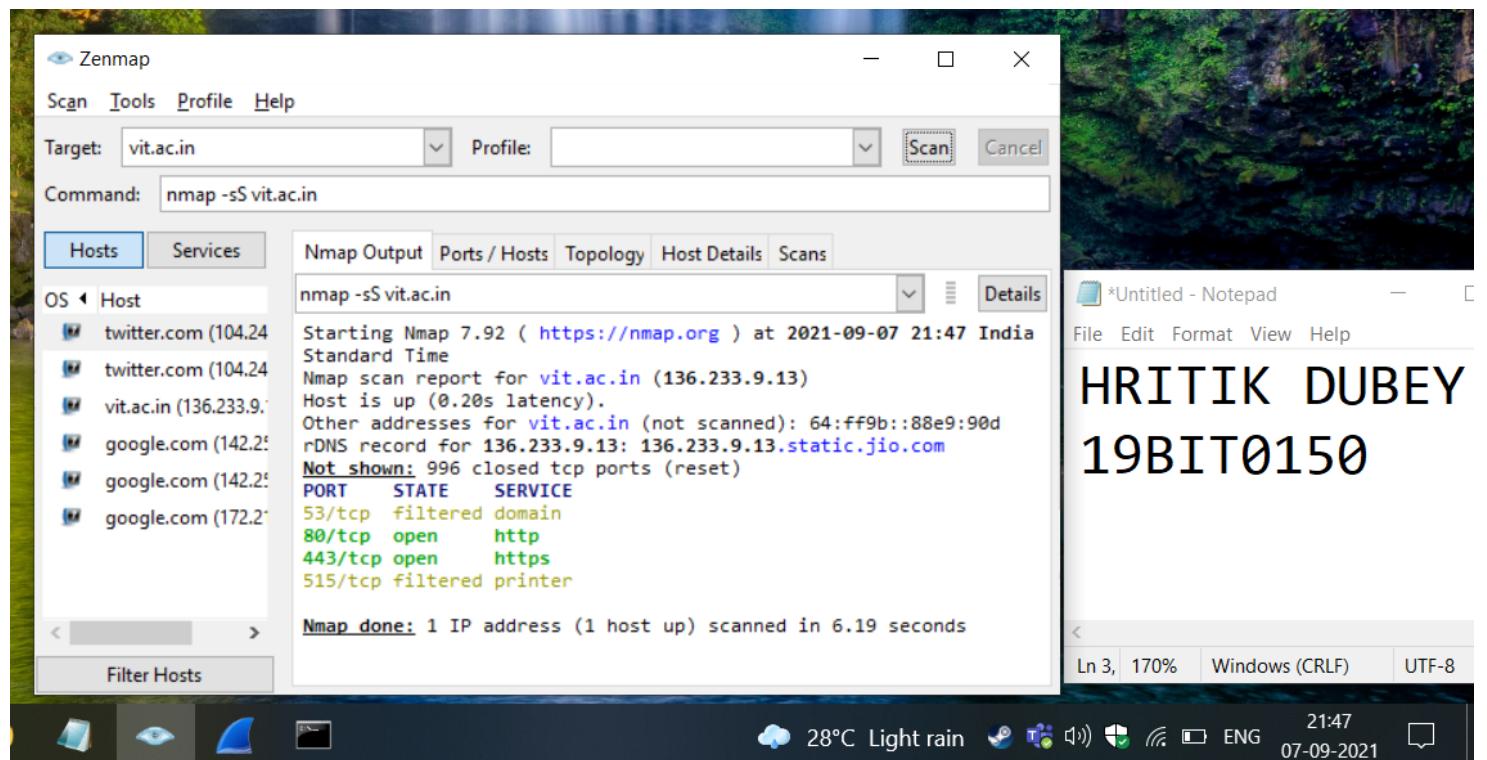
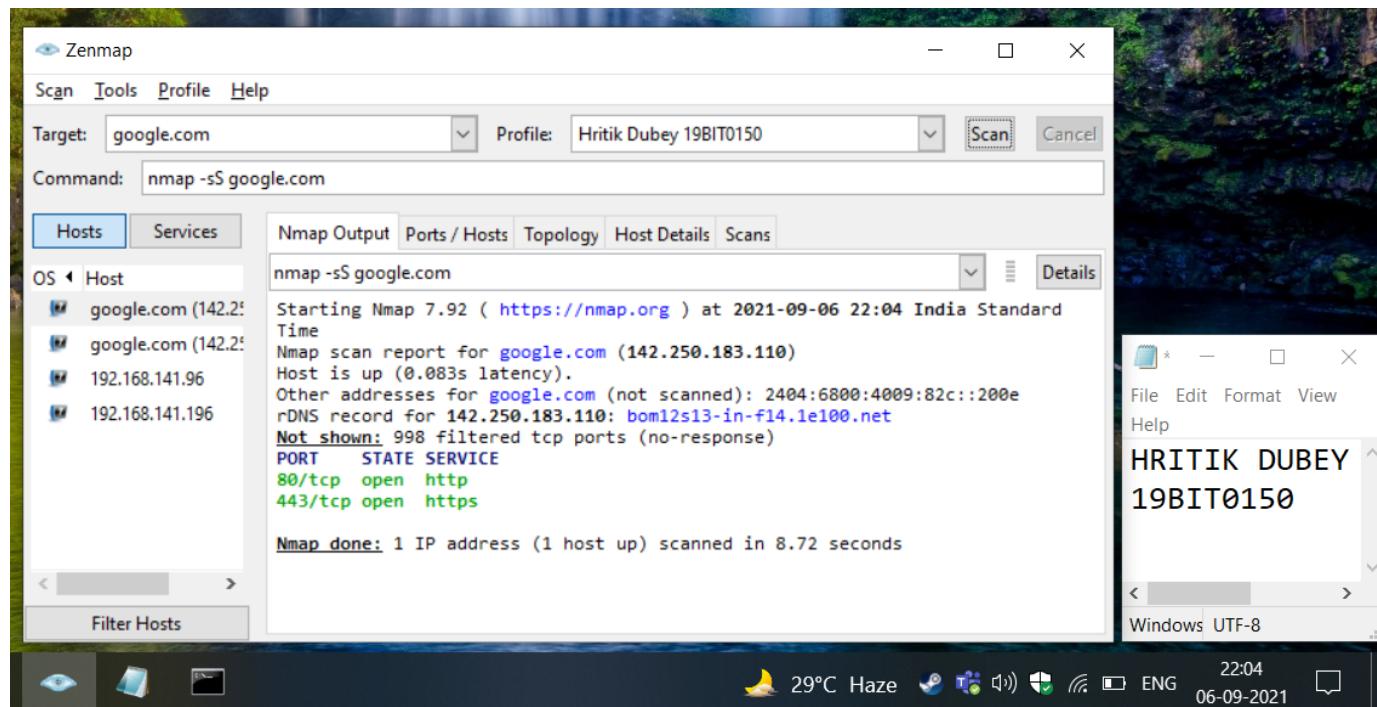
In order to perform a stealth scan we use Nmap -sS command in the format  
: Nmap -Ss IP address

Let's set the target ip as my own IP address.



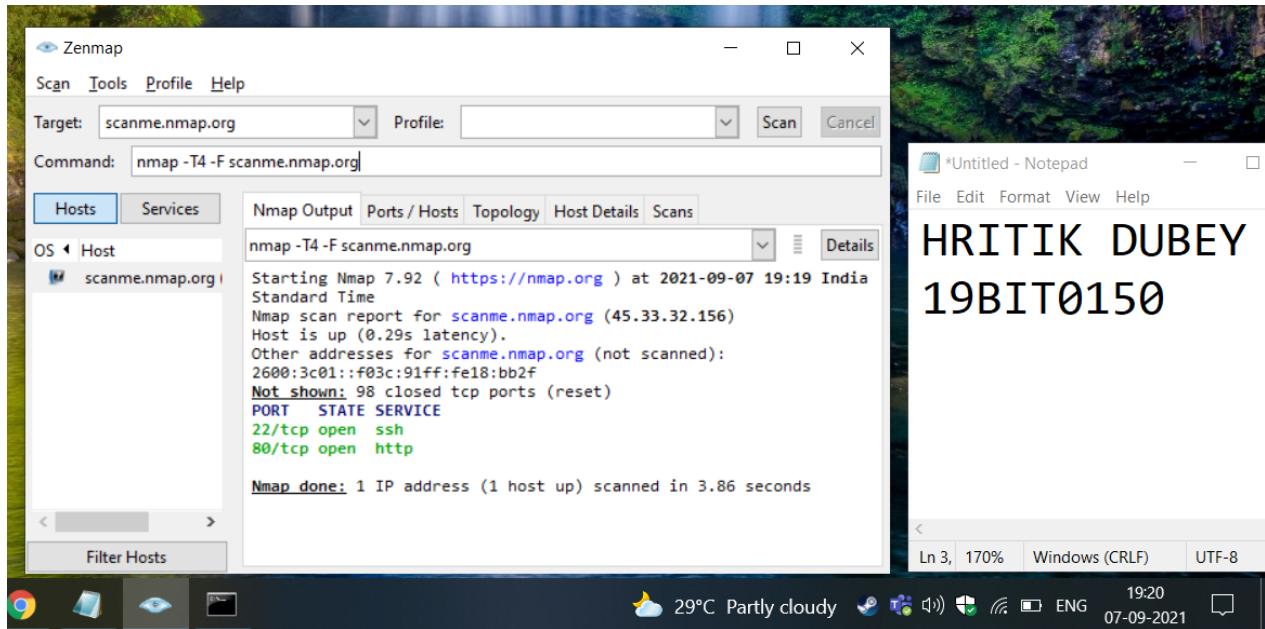
As we can see, Stealth search scan ip for port state service.

## Trying with google.com

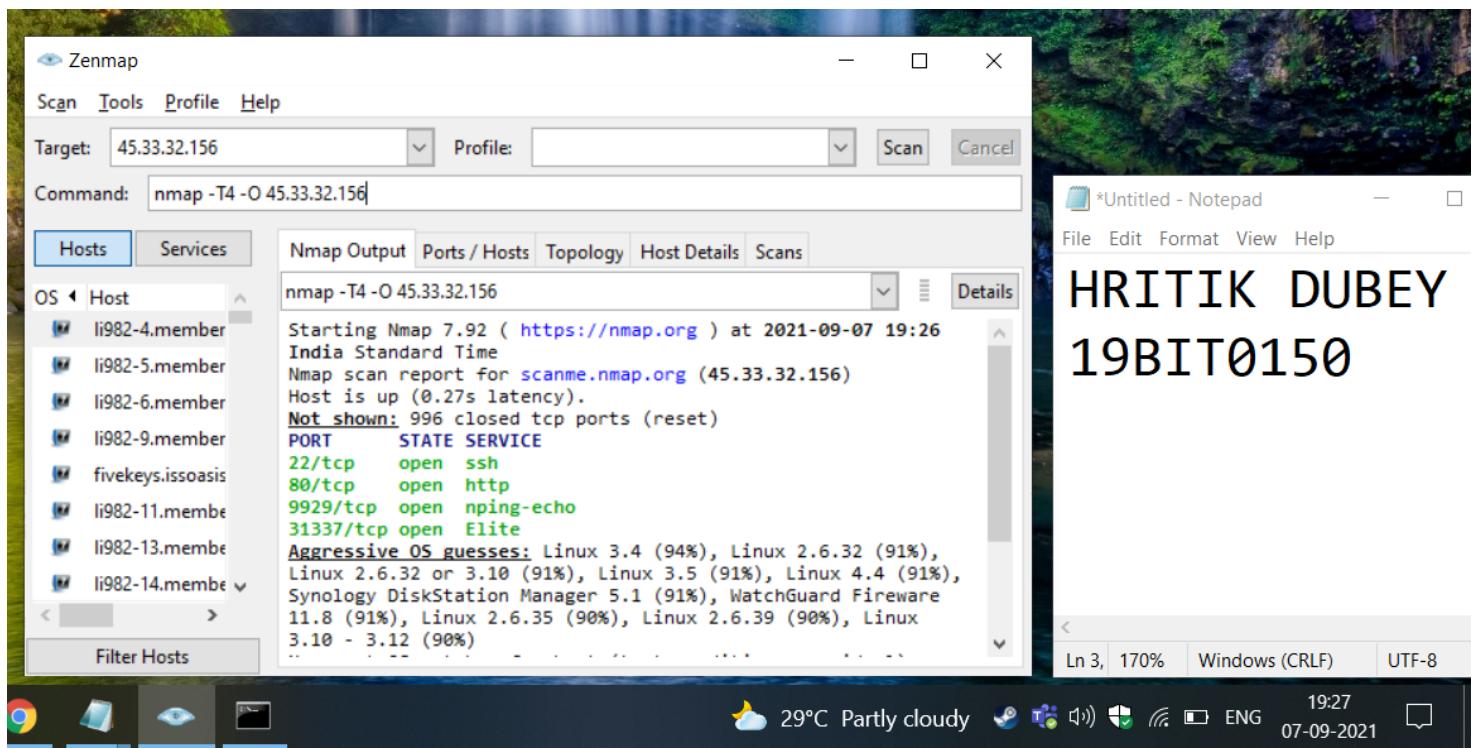


## 2. What is the best Nmap command to use when you want to list all devices in the same network quickly? Considering the server as scanme.nmap.org.

Nmap command - nmap -T4 -F will give us faster quick results. So it is the BEST COMMAND

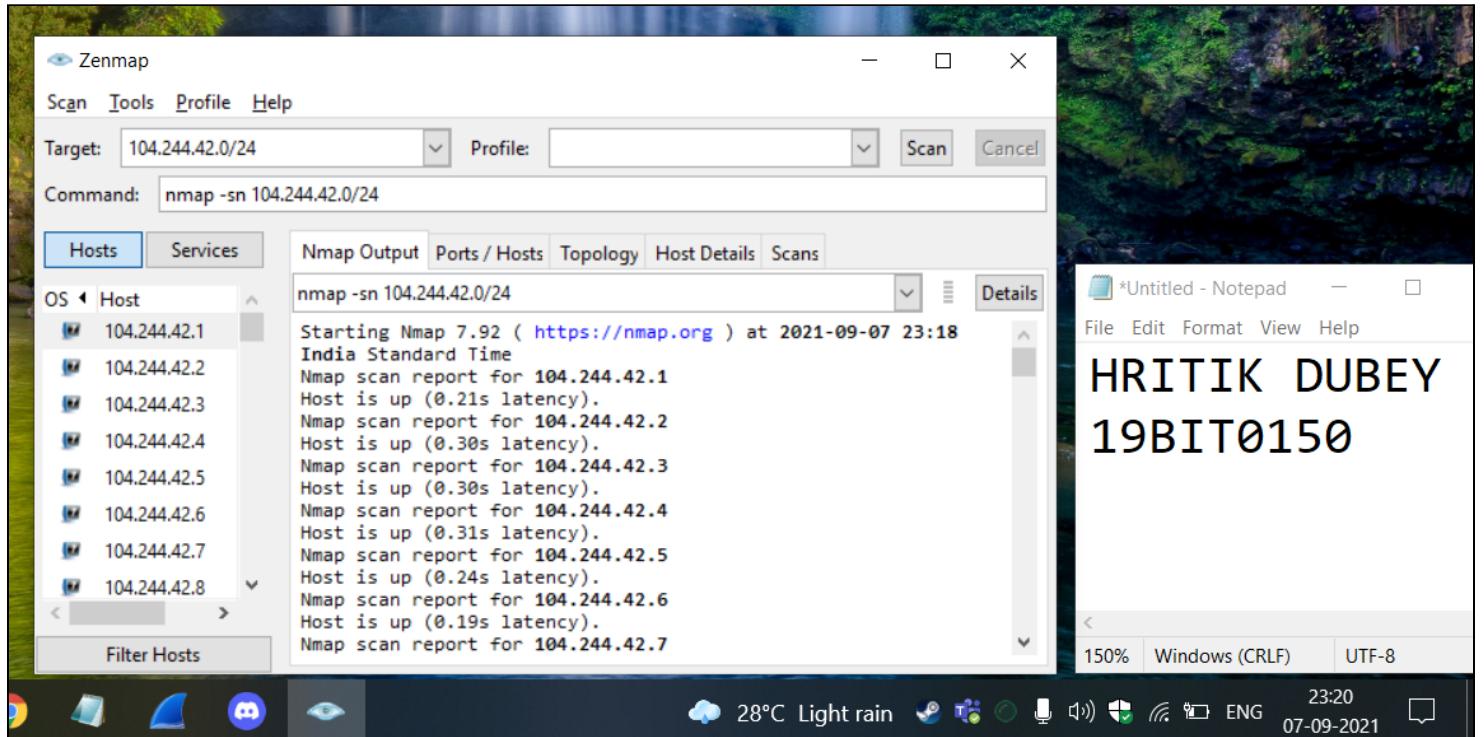


Trying with Nmap command - nmap -T4 -O IP Address - 45.33.32.156 .This gives more ports

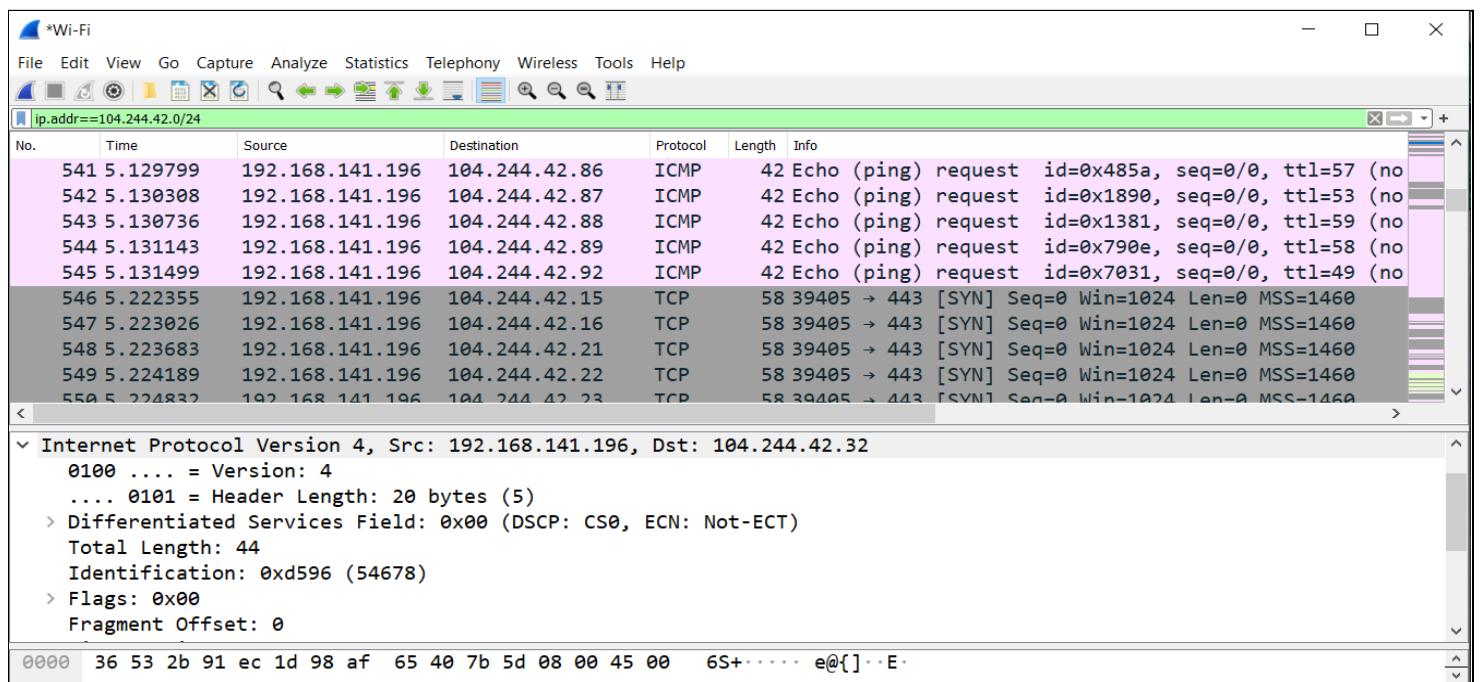


**3. A hacker is attempting to see which IP addresses are currently active on the “twitter” website. Which NMAP switch would the hacker use? In Wireshark, capture the packets that contain twitter and show the results**

Nmap -sp 104.244.42.0/24 Twitter.com Ip -104.244.42.129 from netcraft



Applying filter ip.addr==104.244.42.0/24 on wireshark to get packet containing twitter

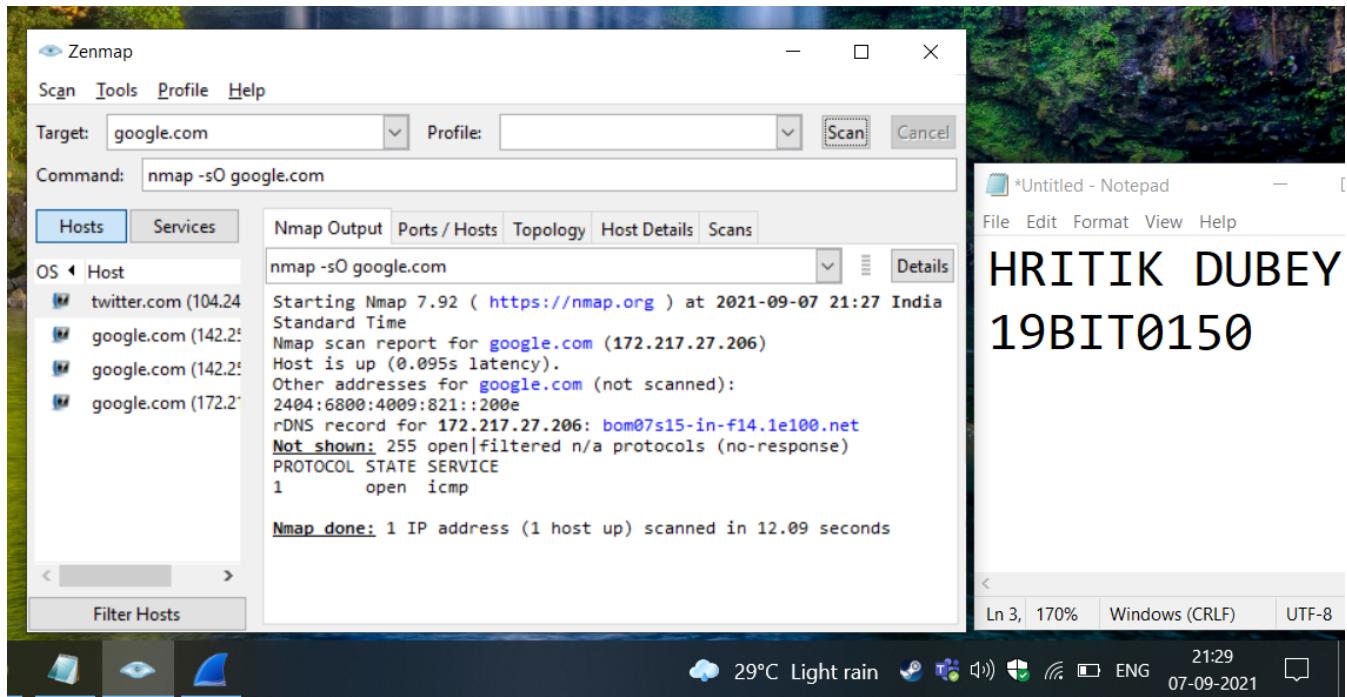


**4. A hacker is attempting to see which ports have been left open on a Google.com network. Which NMAP switch would the hacker use and how can the hacker filter using Wireshark and get the packets belonging to a specific protocol like HTTP, TCP, DNS and UDP and analyze the packet structure. Show the results**

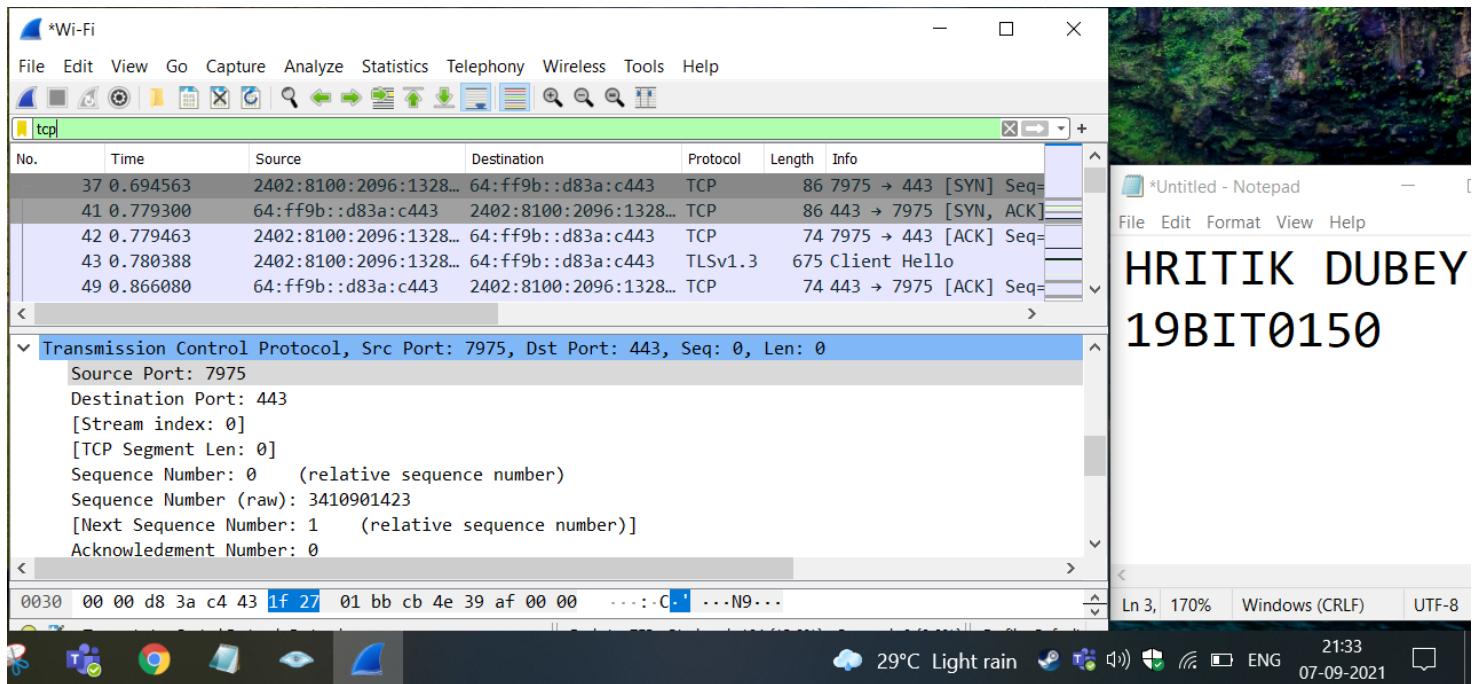
Nmap -sO command will be used to see which ports are open here. We will first use Nmap to find open ports. Getting IP from Netcraft.com as 74.125.193.101

The screenshot shows a Windows desktop environment with several windows open:

- Browser Window:** Displays the Netcraft site report for <http://google.com>. It provides detailed information about Google's infrastructure, including its domain (google.com), nameservers (ns1.google.com), and various Autonomous Systems (ASes) it is connected to.
- Zenmap Window:** An open terminal window titled "Zenmap" showing the command "nmap -sO 74.125.193.101". The output shows a single host, "di-in-f101.1e100.net" (74.125.193.101), which is up and has one open ICMP port.
- Notepad Window:** A text editor window titled "Untitled - Notepad" containing the text "HRITIK DUBEY" and "19BIT0150".
- Taskbar:** Shows the system tray with weather (28°C Light rain), battery level (ENG), and date/time (07-09-2021 23:30).

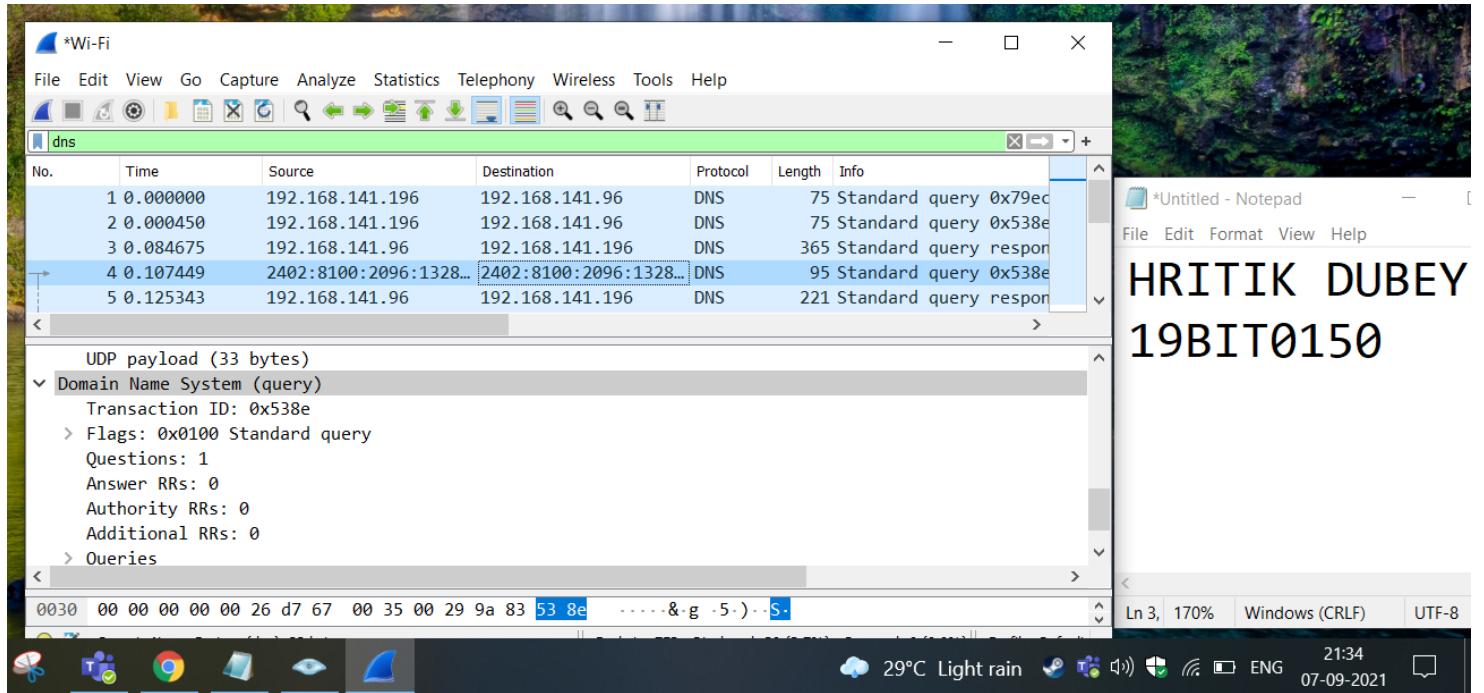


Now we will use Wire shark filter, TCP, UDP, DNS to filter the packets.

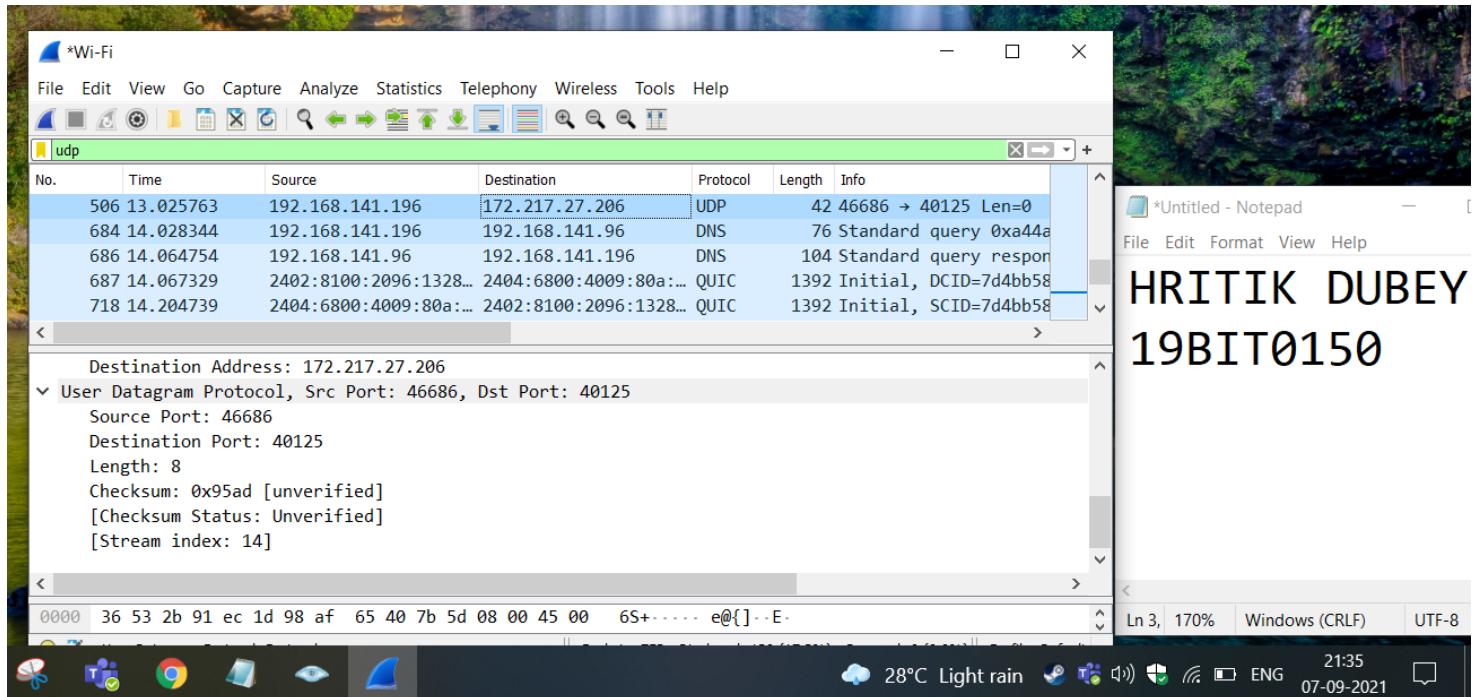


For the TCP protocol as we can see in the packet structure, Transmission control protocol section we are provided with source Port & Destination Port.

For DNS we can see in the packet structure, Domain Name System containing queries.



For the UDP protocol in the packet structure User Datagram Protocol we are given Source/Dest Port



Hence for each protocol we have filtered the packets UDP,TCP & DNS while using -sO command on Nmap.

5. Choose any vulnerable website from “<http://www.vulnweb.com/>”. Create an account having the username with your name and register number. Grab the username and password in Wireshark.

First we will create a sign up form on <http://testphp.vulnweb.com/signup.php>. The Http protocol used here is using POST form method with less security hence it can be extracted in packet.

ISAA LAB DA 2 - Google Docs X signup X +

Not secure | testphp.vulnweb.com/signup.php

CodeTantra Teach... Gmail YouTube PDF Convert PPT files (P... Laptop Health Games JAVA DSA IT Resume Other bookmarks Reading list

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art  go

Browse categories

Browse artists

Your cart

Signup

Your profile

Our guestbook

AJAX Demo

Links

Security art

PHP scanner

PHP vuln help

Fractal Explorer

signup

Type here to search 28°C Haze ENG 00:14 07-09-2021

Now we will apply a filter on Wireshark to find http.request packet.

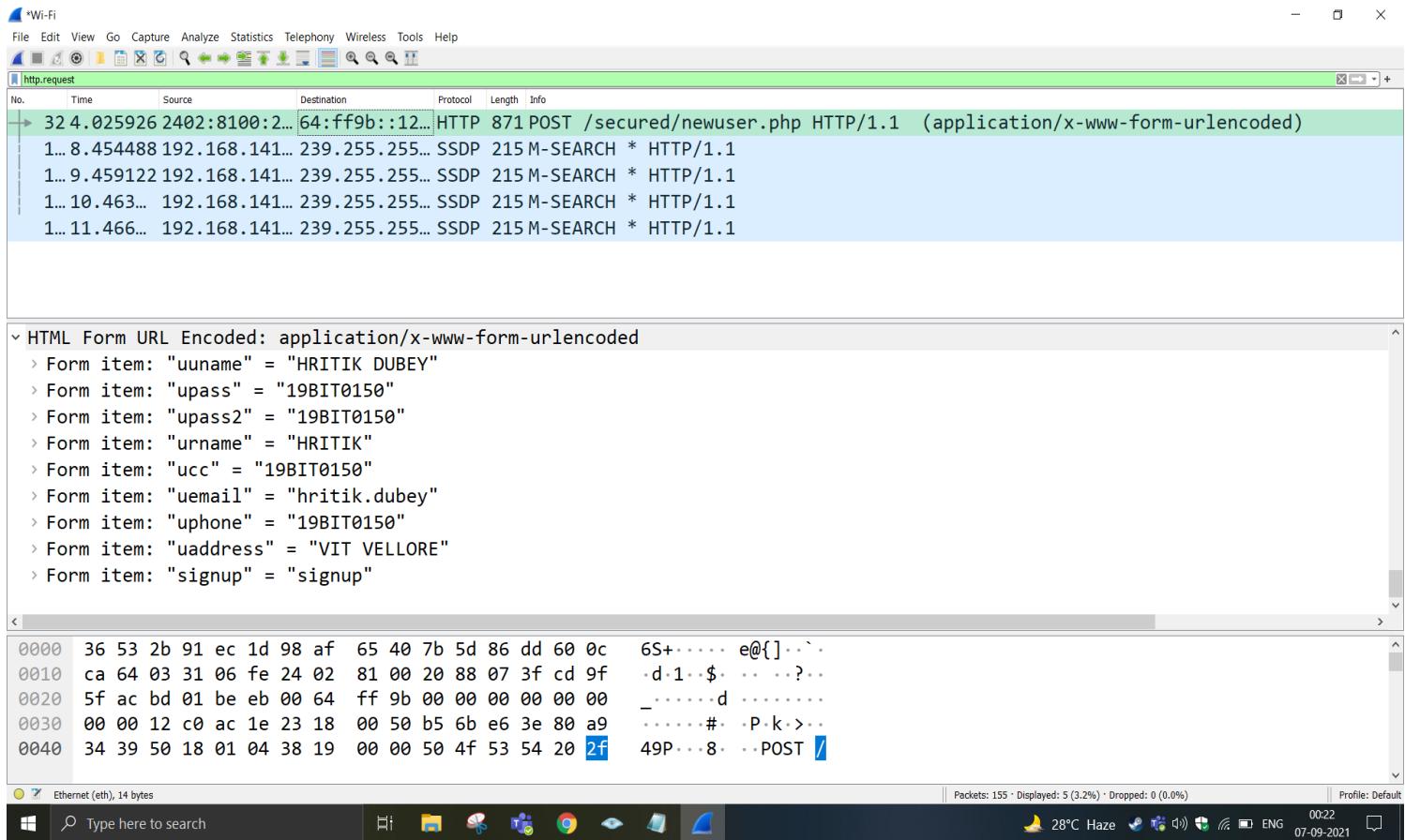
\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request

No.	Time	Source	Destination	Protocol
32	4.025926	2402:8100:2088:73...	64:ff9b::12c0:ac1e	HTTP

Now we will find the form data, in the HTML form URL Encoded section.



As we can see that the form data which we will fill can now be seen in Packet analysis through wire shark.