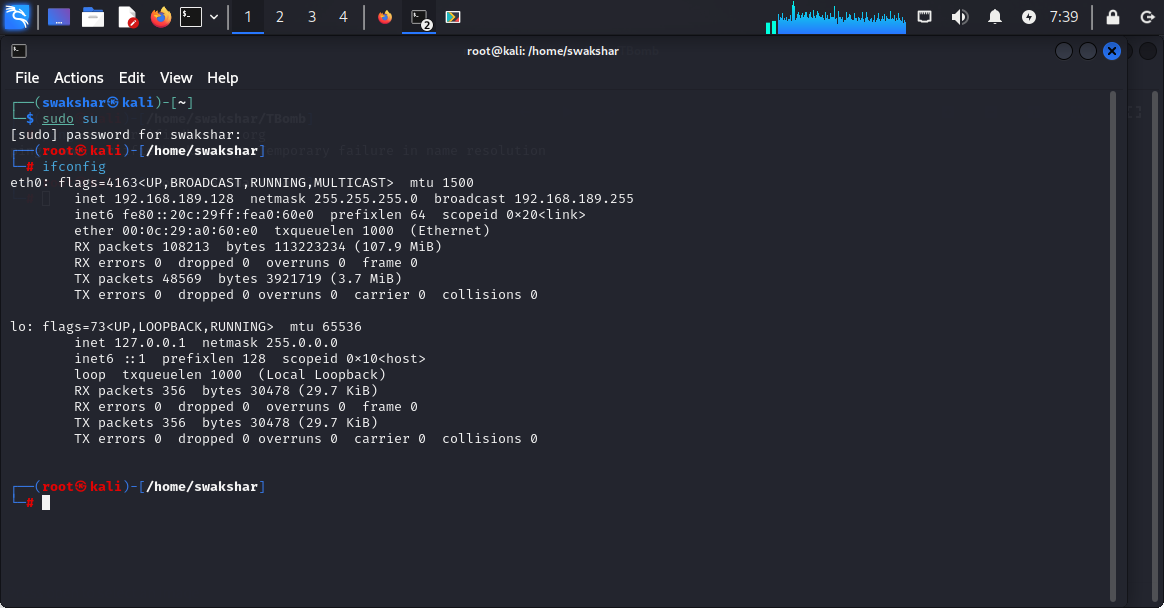
USING PING COMMAND FOR HOST DISCOVERY:

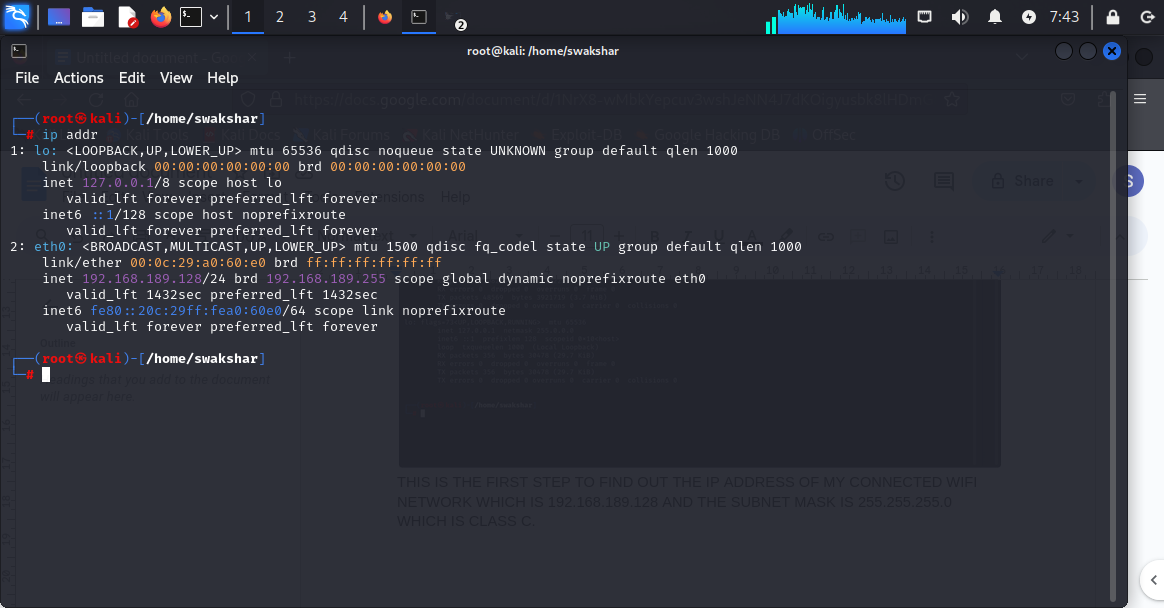
Host discovery is one of the important things in cyber security and ethical hacking because if we do not know that which remote port is open or filtered or closed to give us a response we will not be able to know what target we should attack for finding out vulnerability.

One of the most used command for that will be ping command and i will be using kali linux tool to exhibit different application of ping command and also without using ping in how many ways we can track the responses and find out open host .

**1. Without using ping how to do host discovery: there is command known as nmap and after that if we write scanme.nmap.org and it will automatically give you the open ports available out of all the existing ports.**



THIS IS THE FIRST STEP TO FIND OUT THE IP ADDRESS OF MY CONNECTED WIFI NETWORK WHICH IS 192.168.189.128 AND THE SUBNET MASK IS 255.255.255.0 WHICH IS CLASS C.

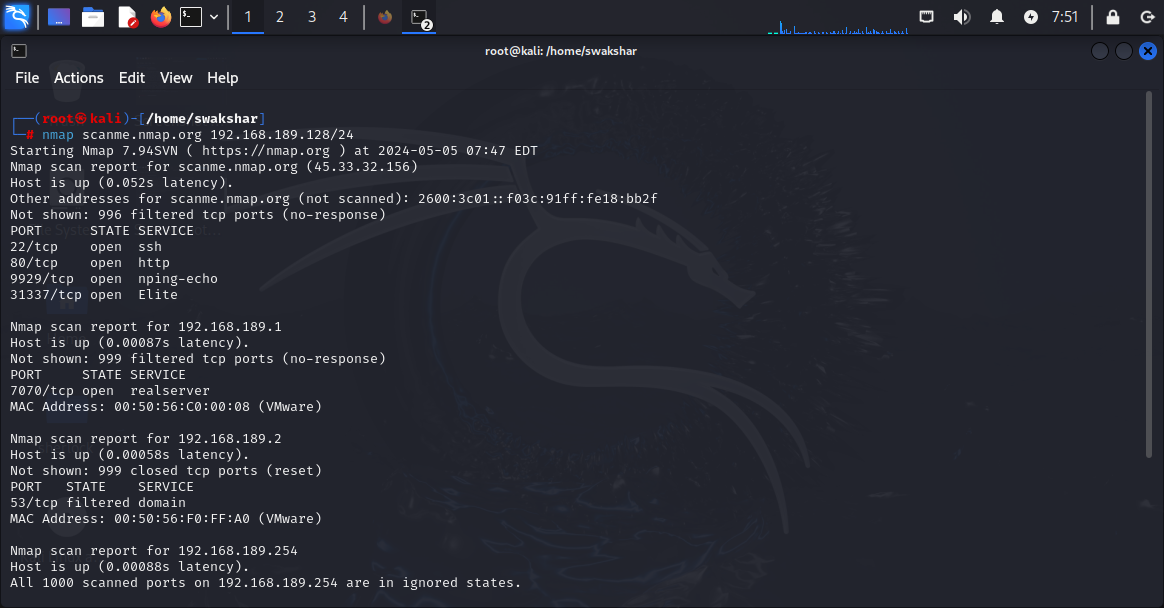


THIS IS THE SECOND WAY OF FINDING OUT THE IP ADDRESS OF MY CONNECTED WIFI ROUTER WHICH IS IN PURPLE 192.168.189.128/24 .

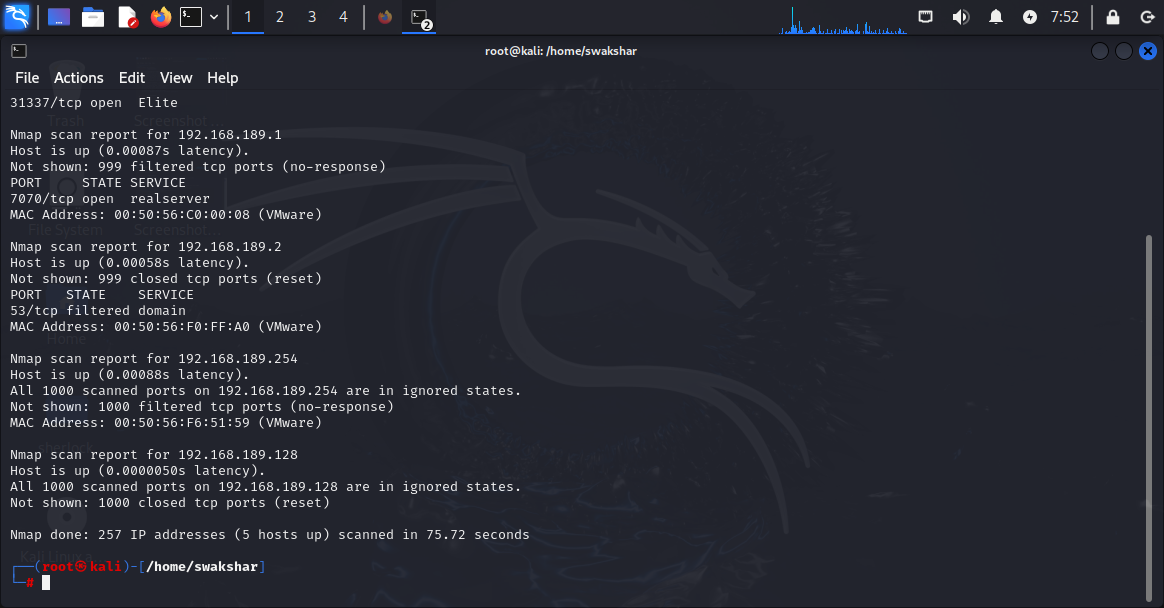
**BOTH THE COMMANDS WITH BE:**

**1.ipconfig**

**2.ip addr**

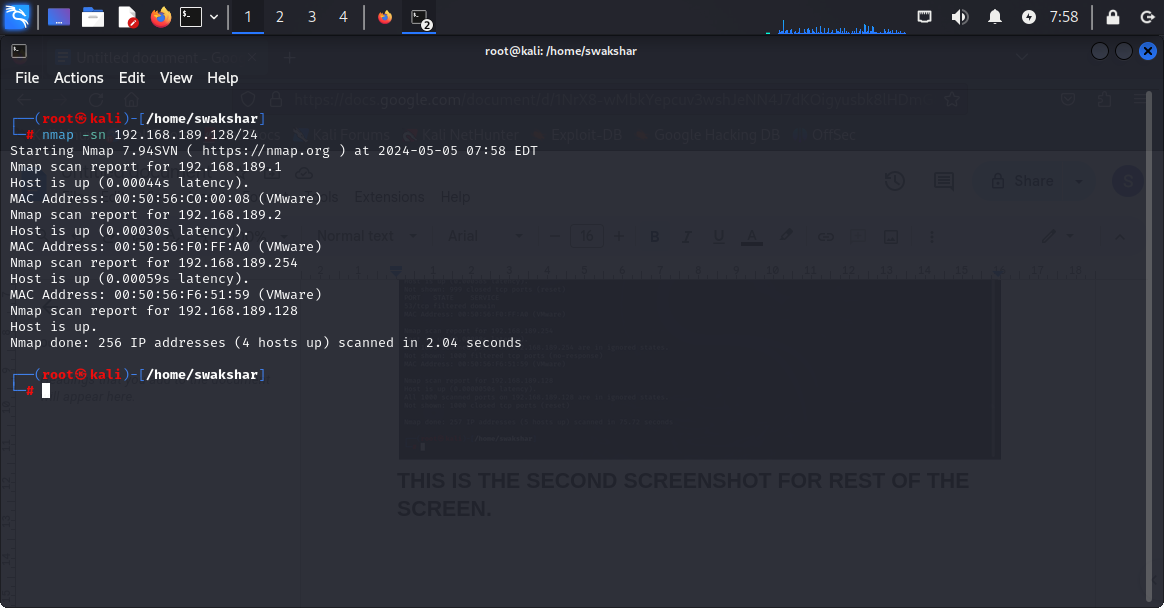
****

**HERE WE CAN SEE THAT BY USING THE COMMAND nmap scanme.nmap.org 192.168.189.128/24 we have got all the reports of all possible ports either they are open or closed or filtered for the ip 192.168.189.128/24 and this is one of the application of using nmap and to do the host discovery without using “ping” command.**

****

**THIS IS THE SECOND SCREENSHOT FOR REST OF THE SCREEN.**

**2. The second command is called “sn” command which is used just to do a host discovery without a port scan or we caall it “PING SWEEP SCAN” where we get to know all the possible hosts whether they are “up” or they are “down”.**

****

**AS WE CAN SEE THAT WE HAVE USED THE COMMAND nmap -sn 192.168.189.128/24 and here we have the reports for the hosts which are up that means we can perform an attack or scan the vulnerability for them.**

**As per the report the available up hosts are**

1. **192.168.189.1**
2. **192.168.189.2**
3. **192.168.189.128**
4. **192.168.189.254**

**Apart from that all the other hosts are down or not responsive AND that is why there are no other responses.**

**WE CAN USE PING COMMAND IN KALI LINUX TO KNOW ABOUT THE CLIENT NETWORK WHETHER IT IS RESPONSIVE OR NOT AND IT IS REACHABLE OR NOT**

**1.ping** [**www.certifiedhacker.com**](http://www.certifiedhacker.com) **-c 5**

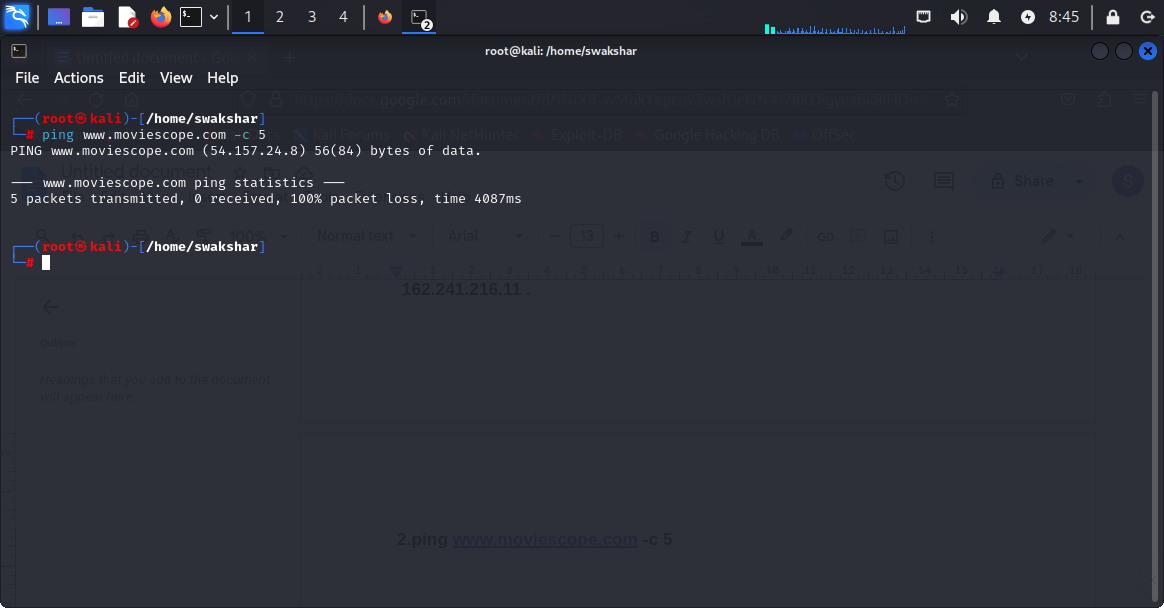
**It means that we are sending 5 packets to** [**www.certifiedhacker.com**](http://www.certifiedhacker.com) **domain to check whether the domain is up or responsive or reachable**

****

**As we see that all the 5 packets have been ssent successfully and all of them are received and there is 0% packet loss which confirms that there is no network traffic . the icmp stands for internet control message protocol which is the basic tool to send network packets to remote network to check its status. The ip address of the respective domain is**

**162.241.216.11 .**

**2.ping** [**www.moviescope.com**](http://www.moviescope.com) **-c 5**

****

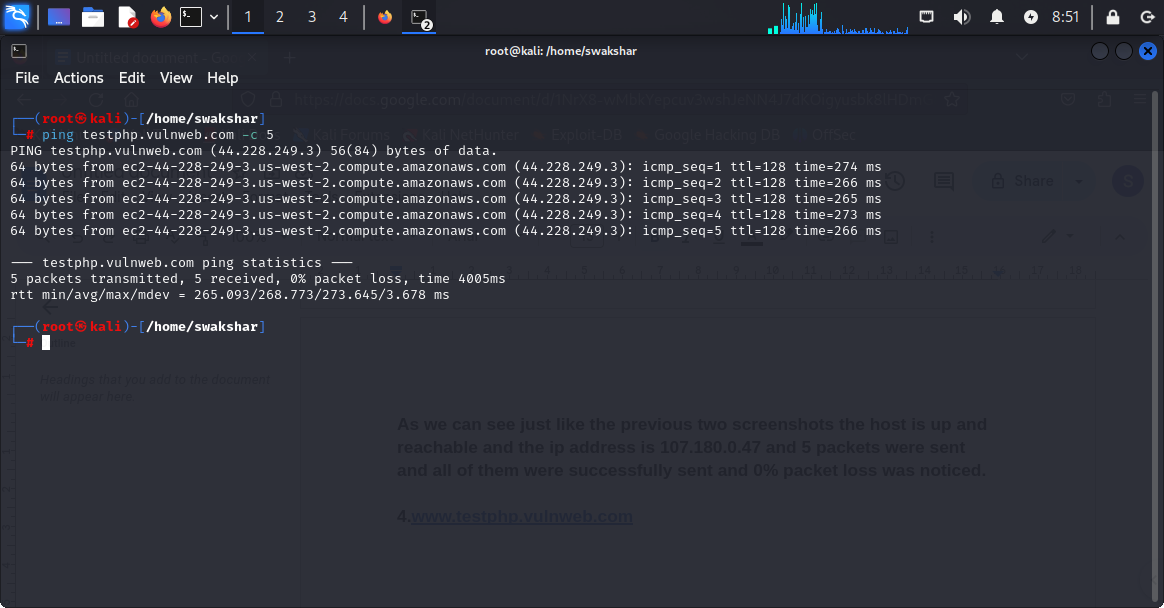
**As we can see that the domain** [**www.moviescope.com**](http://www.moviescope.com) **is not reachable and that is why we have sent 5 packets but it is showing 100% packet loss that means due to some reason the host is not reachable it may be firewall or filter or may be network traffic. The corresponding ip address of the domain is 54.157.24.8**

**3. ping** [**www.goodshopping.com**](http://www.goodshopping.com) **-c 5**

****

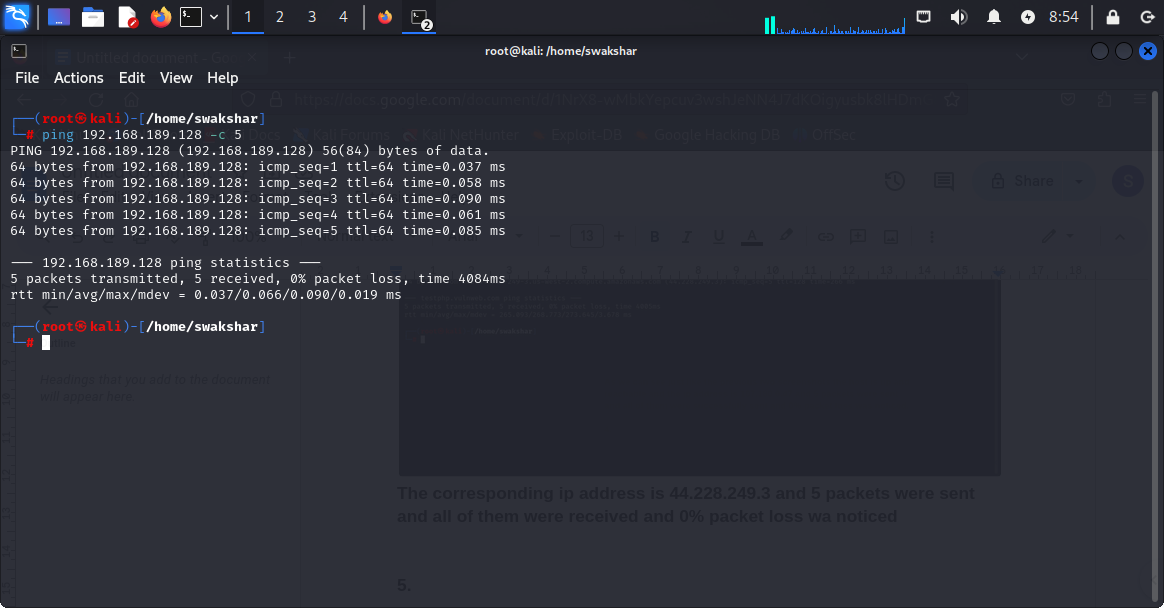
**As we can see just like the previous two screenshots the host is up and reachable and the ip address is 107.180.0.47 and 5 packets were sent and all of them were successfully sent and 0% packet loss was noticed.**

**4. ping** [**www.testphp.vulnweb.com**](http://www.testphp.vulnweb.com) **-c 5**

****

**The corresponding ip address is 44.228.249.3 and 5 packets were sent and all of them were received and 0% packet loss wa noticed**

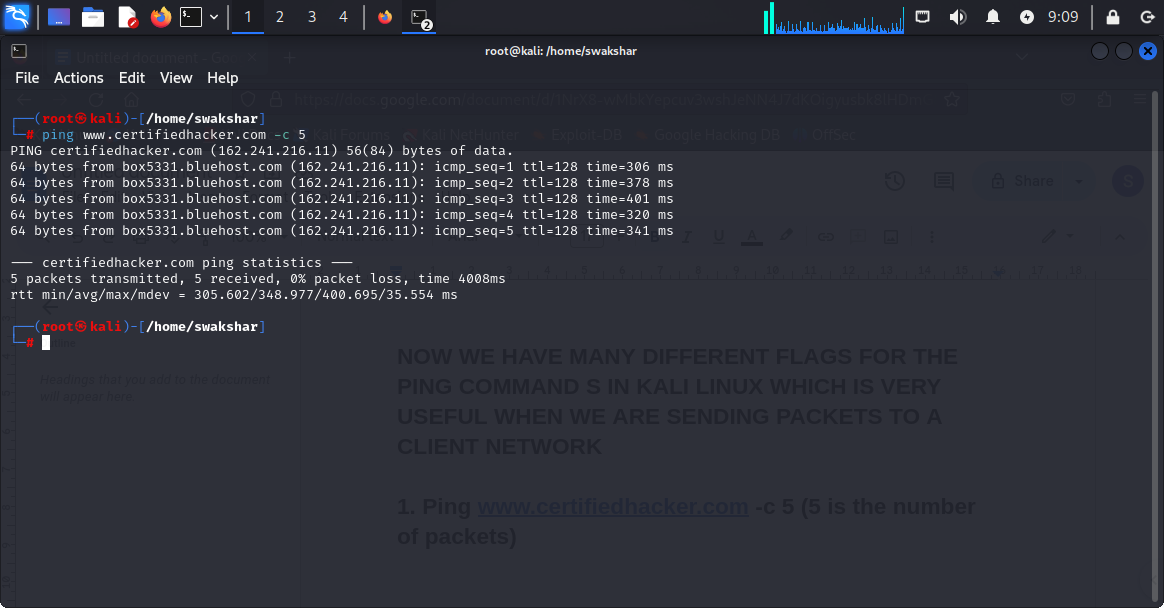
**5.ping 192.168.189.128 -c 5 (ip address of my network)**

****

**The same response because i have put my ip address of my connected wifi network so it will be “up” anyway.so all the packets were received and 0% packet loss was noticed.**

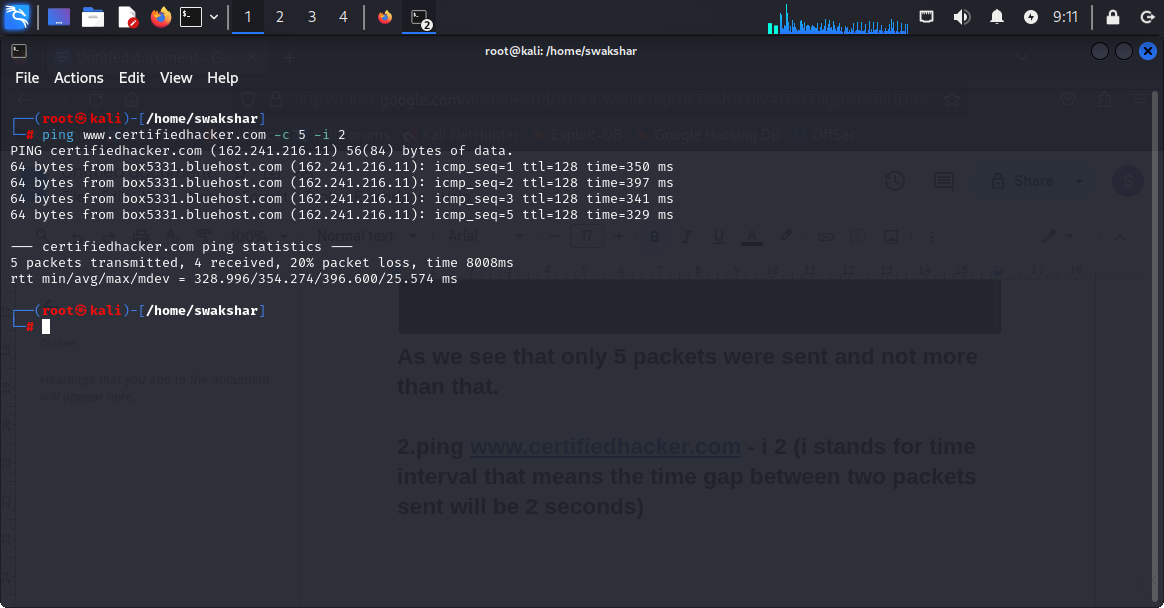
**NOW WE HAVE MANY DIFFERENT FLAGS FOR THE PING COMMAND S IN KALI LINUX WHICH IS VERY USEFUL WHEN WE ARE SENDING PACKETS TO A CLIENT NETWORK**

**1. Ping** [**www.certifiedhacker.com**](http://www.certifiedhacker.com) **-c 5 (5 is the number of packets)**

****

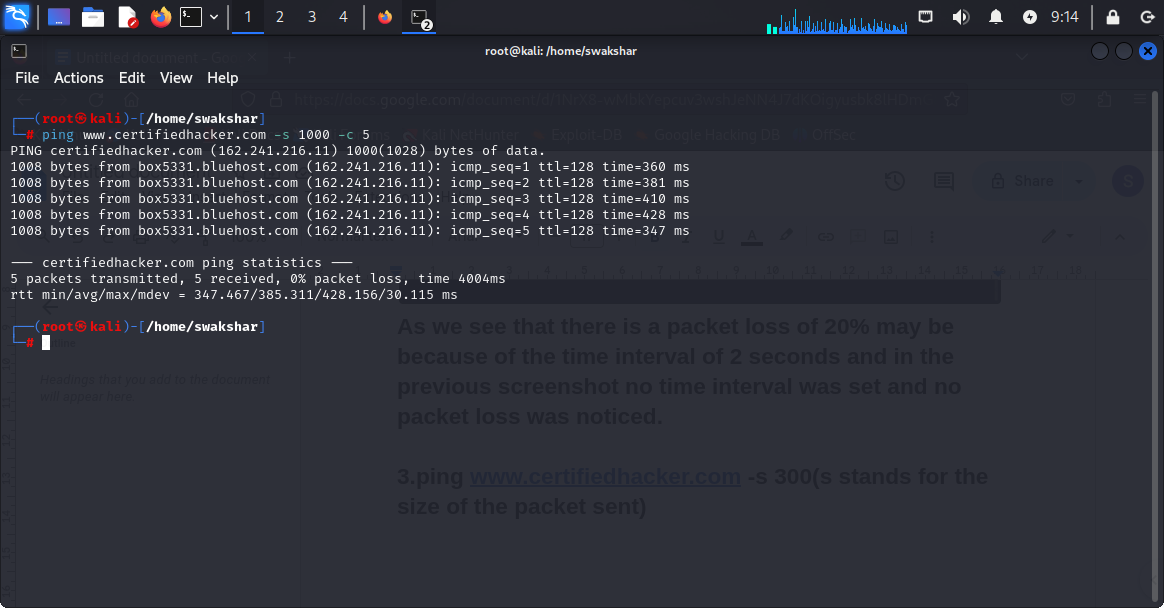
**As we see that only 5 packets were sent and not more than that.**

**2.ping** [**www.certifiedhacker.com**](http://www.certifiedhacker.com) **- i 2 (i stands for time interval that means the time gap between two packets sent will be 2 seconds)**

****

**As we see that there is a packet loss of 20% may be because of the time interval of 2 seconds and in the previous screenshot no time interval was set and no packet loss was noticed.**

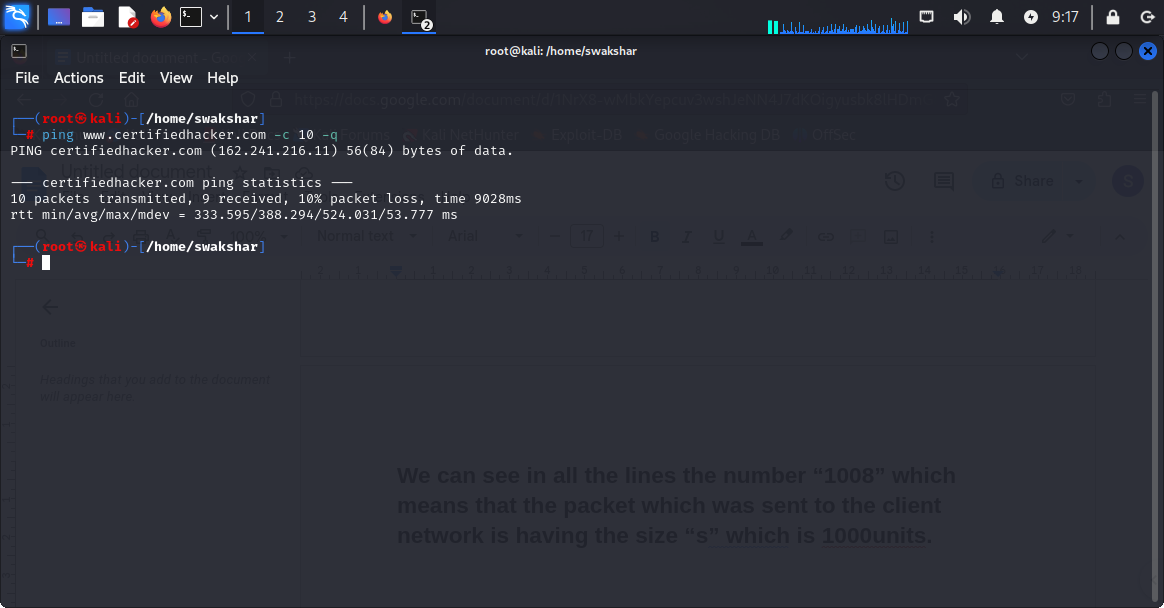
**3.ping** [**www.certifiedhacker.com**](http://www.certifiedhacker.com) **-s 300(s stands for the size of the packet sent)**

****

**We can see in all the lines the number “1008” which means that the packet which was sent to the client network is having the size “s” which is 1000units.**

**4.ping** [**www.certifiedhacker.com**](http://www.certifiedhacker.com) **-c 5 -q(q means just writing down the overall summary without showing**

**Each line)**

****

**As we can see that 10 packets were sent but the output is shown is one single line without showing 10 lines for each packet.**

**5.ping** [**www.certifiedhacker.com**](http://www.certifiedhacker.com) **-w 10(it means it will stop printing after 10 liness)**

****

**As we can see that by writing -w 10 it automatically sends 10 packets and not more than that.**

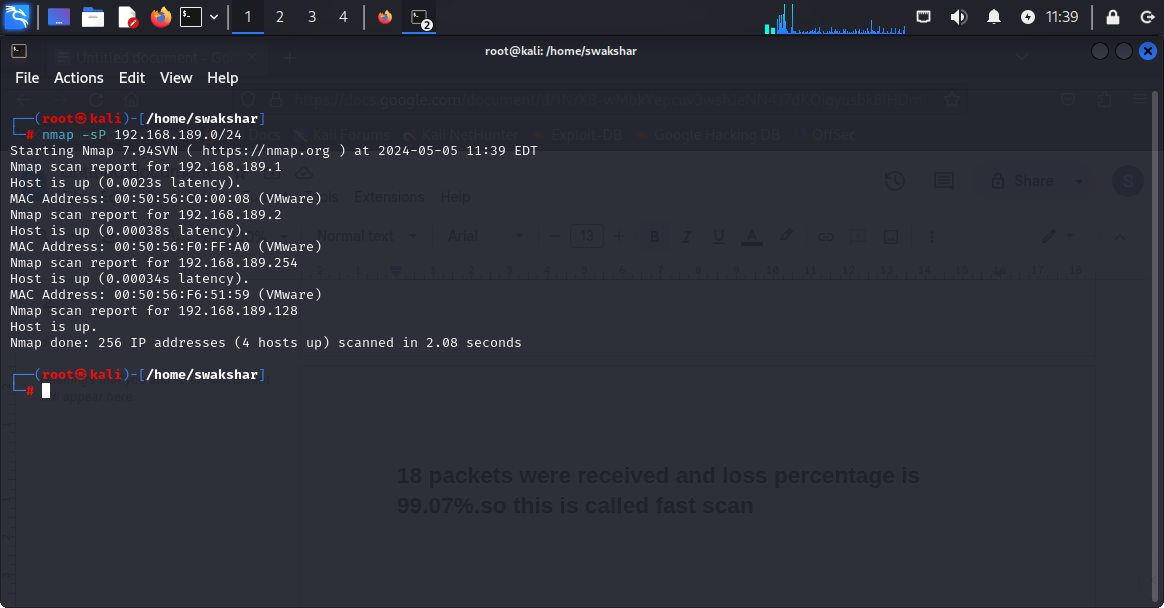
**6.ping** [**www.certifiedhacker.com**](http://www.certifiedhacker.com) **-f (f stands for fast scan)**

****

**As we can see that we have typed -f without mentioning any specific packet size or packet number or time interval but still it is able to send 1952 packets but only 18 packets were received and loss percentage is 99.07%.so this is called fast scan**

**There are one more command which does not do any port scan but just let us know about the hosts which are up and reachable as a target**

**The command is : nmap -sP 192.168.189.0/24 where 192.168.189.128 is my wifi ip address with a subnet mask of class C.**

****

**As we can see that there is no active port scan but all the available hosts reports are shown on the system.**

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*END OF HOST DISCOVERY\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

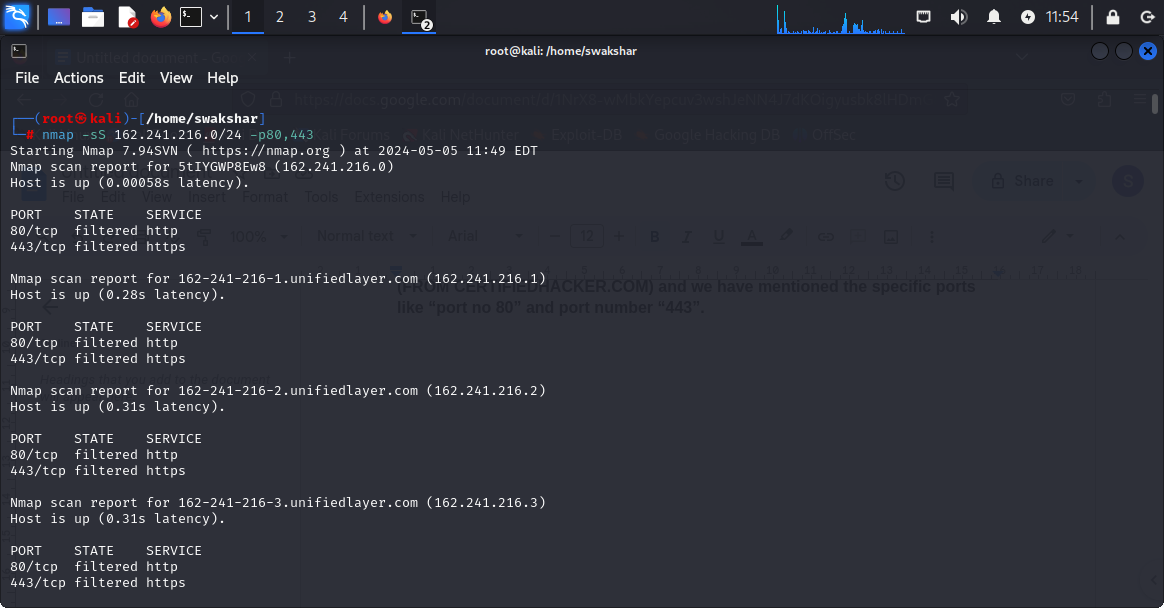
**COMPREHENSIVE PORT SCANNING \\ACTIVE PORT SCANNING USING nmap TOOL in KALI LINUX:**

**AS WE NEED TO BE AWARE OF THE SECURITY PROTOCOLS AND BECAUSE THIS IS AN ACTIVE SCANNING SO WE WILL BE USING SPECIFIC IP ADDRESSES OF THE DOMAINS MENTIONED IN THE ASSIGNMENT FOR EXAMPLE** [**WWW.CERTIFIEDHACKER.COM**](http://www.certifiedhacker.com) **,** [**WWW.MOVIESCOPE.COM**](http://www.moviescope.com) **ETC.**

**BEFORE WE USE DIFFERENT WAYS OF USING nmap COMMAND WE NEED TO USE HOW MANY DIFFERENT WAYS WE CAN WRITE THE SAME COMMAND TO PERFORM PORT SCAN.**

**1.nmap -sS 162.241.216.0/24 -p80,443**

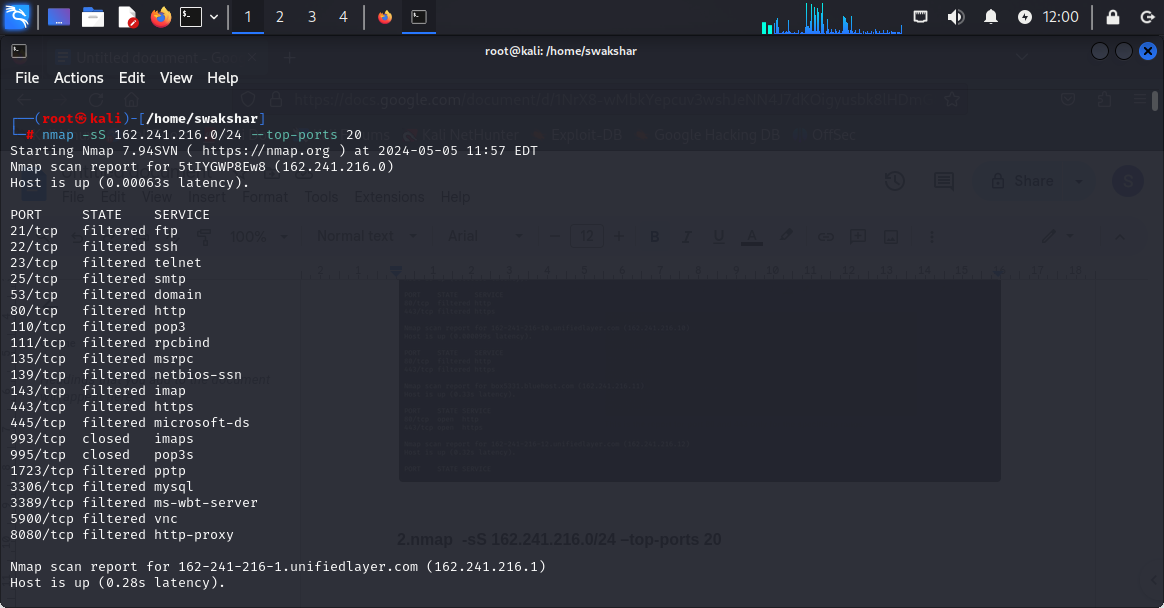
**In this case we have performed a stealth scan or syn scan for the ip address (FROM CERTIFIEDHACKER.COM) and we have mentioned the specific ports like “port no 80” and port number “443”.**

****

**This is the report for port 80 and 443 only for the specific ip range.**

****

**2.nmap -sS 162.241.216.0/24 –top-ports 20 ( double dash top-ports number of ports)**

****

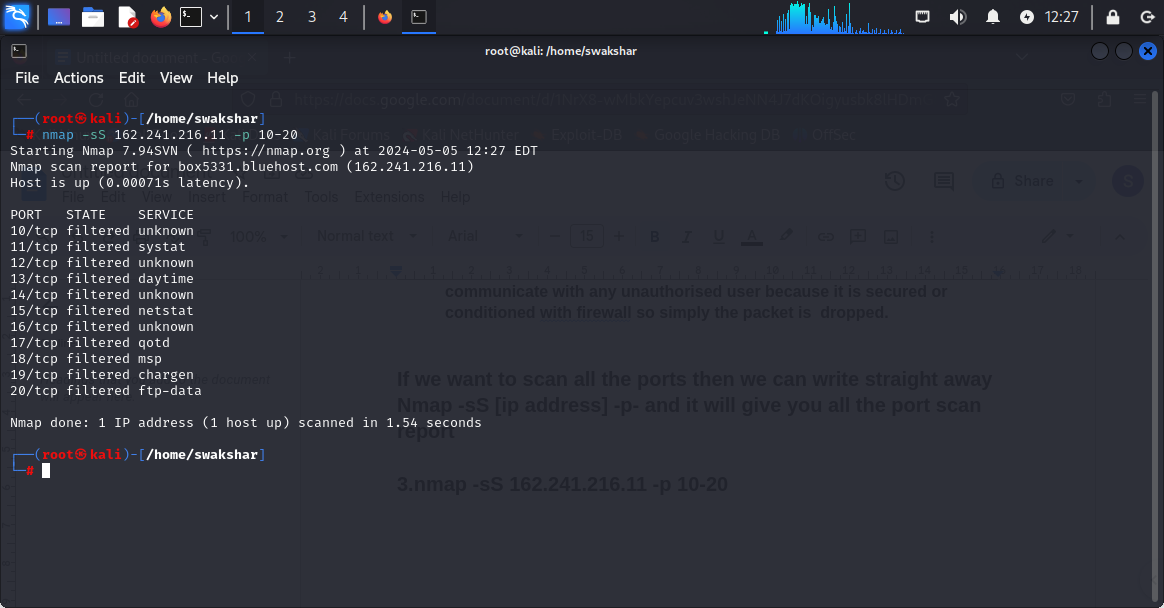
**So as we can see that there are the reports for top 20 ports for the following ip range and the port status has been mentioned.**

1. **Open stands for service is running and we can communicate**
2. **Closed means the port is not reachable or responsive for any sort of communication or it can not be concluded what is going on with that specific port.**
3. **Filtered means the service is running but the port is not willing to communicate with any unauthorised user because it is secured or conditioned with firewall so simply the packet is dropped.**

**If we want to scan all the ports then we can write straight away**

**Nmap -sS [ip address] -p- and it will give you all the port scan report**

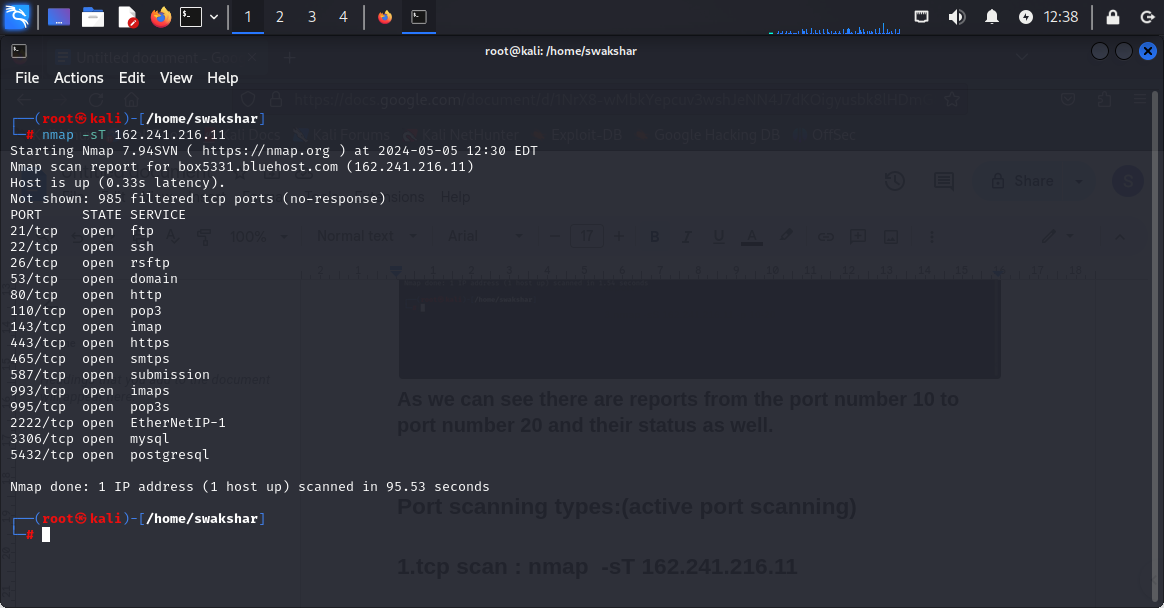
**3.nmap -sS 162.241.216.11 -p 10-20**

****

**As we can see there are reports from the port number 10 to port number 20 and their status as well.**

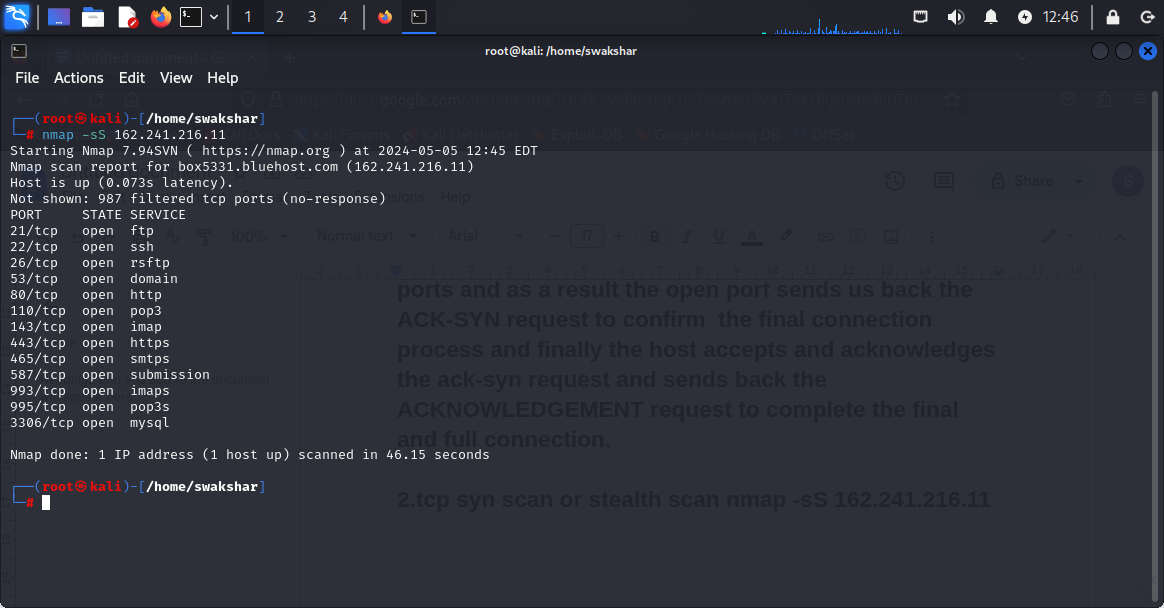
**Port scanning types:(active port scanning)**

**1.tcp scan : nmap -sT 162.241.216.11**

****

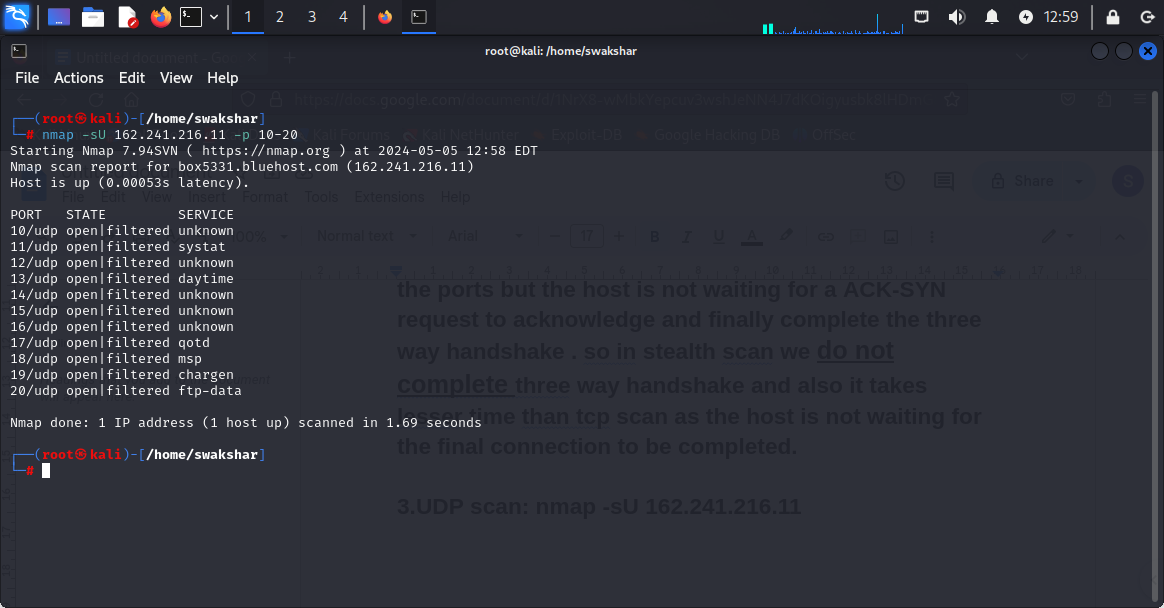
**The tcp scan is basically based on the three way handshake process where we send a SYNCHRONISATION request to the respective open ports and as a result the ports sends us back the ACK-SYN request to confirm the final connection process and finally the host accepts and acknowledges the ack-syn request and sends back the ACKNOWLEDGEMENT request to complete the final and full connection.**

**2.tcp syn scan or stealth scan nmap -sS 162.241.216.11**

****

**As we can see that this is called a tcp syn scan or stealth scan where we send synchronisation request to the ports but the host is not waiting for a ACK-SYN request to acknowledge and finally complete the three way handshake . so in stealth scan we do not complete three way handshake and also it takes lesser time than tcp scan as the host is not waiting for the final connection to be completed.**

**3.UDP scan: nmap -sU 162.241.216.11**

****

**Udp scan is also called the “stateless”scan and it is even stealthier than syn scan because in this type of scan we send the network packets to the client network without hoping whether the packet has been received or not. It is mostly showing open|filtered because the services are running but they are all firewalled or secured with safety protocols so most of the times the packets are dropped by the server.**

**Non -intrusive port scan is also called the passive scan where we do not need any access to the client network system in order to perform the scanning as we do not have any intention to disrupt the target system service or perform any sort of harm or malfunctioning . by using this type of scanning we get to know the hardware vulnerability , software aging amd any possible malware threat about the target network without any system disruption.**

**Scanning beyond firewall and ids:**

**In order to perform any scanning to avoid the firewall or advanced ids we need to find out what possibly the firewall can not catch or judge and it will let the network packet pass through it or do not even recognise that it is a network packet.**

**1.Fragmentation: The word fragmentation means the packet we will be sending we will fragment that specific packet into tiny small packets so it will be harder for the firewall to identify and resist the entire packet properly and we can evade the intrusion detection.**

**We will be using the ip addresses of the corresponding websites mentioned in the hands-on**

**1.**[**www.certifiedhacker.com**](http://www.certifiedhacker.com)

**2.**[**www.moviescope.com**](http://www.moviescope.com)

**3.**[**www.goodshopping.com**](http://www.goodshopping.com)

**4.T**[**estphp.vulnweb.com**](http://www.testphp.vulnweb.com)

**Ip address of the correspondings are**

**1.162.241.216.11**

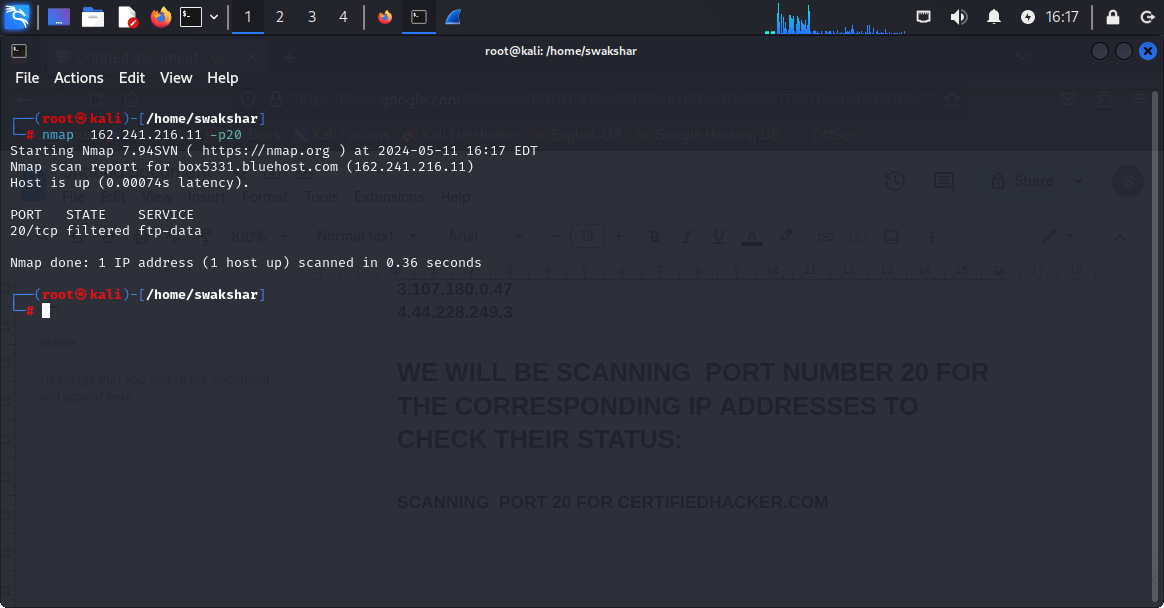
**2.54.157.24.8**

**3.107.180.0.47**

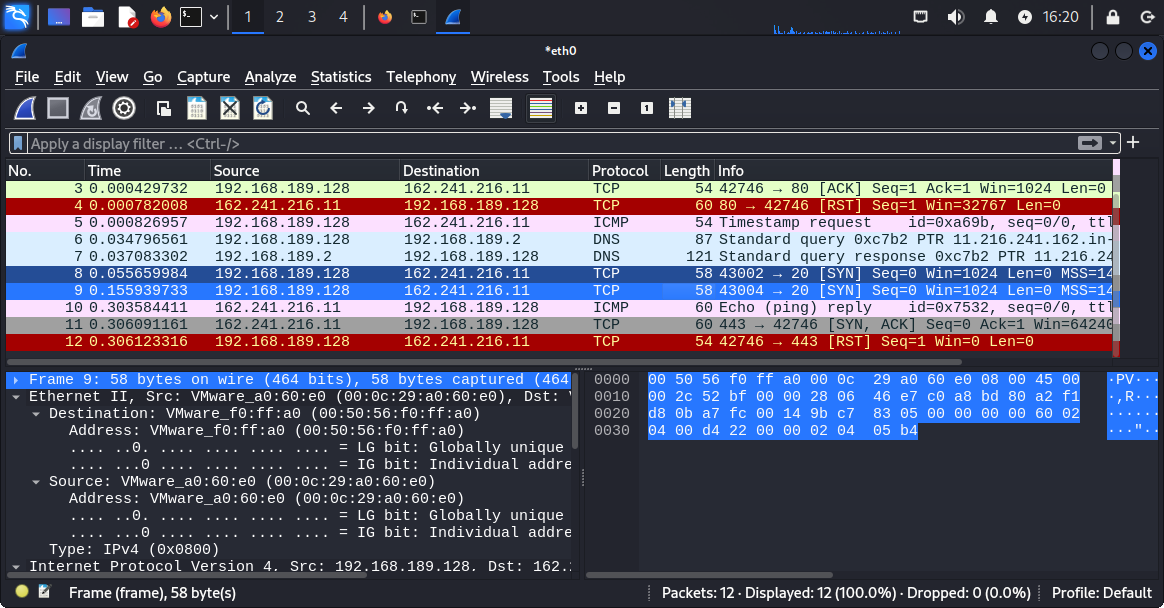
**4.44.228.249.3**

**WE WILL BE SCANNING PORT NUMBER 20 FOR THE CORRESPONDING IP ADDRESSES TO CHECK THEIR STATUS:**

**SCANNING PORT 20 FOR CERTIFIEDHACKER.COM**

****

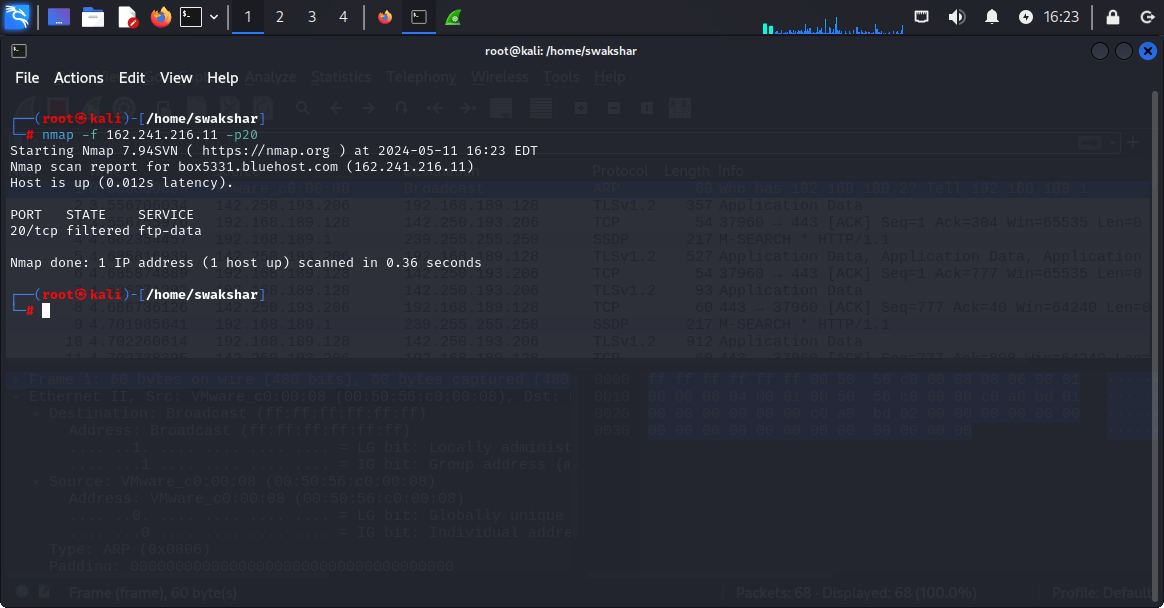
**AS WE CAN SEE THAT THE PORT STATUS IS filtered which means we can not say certainly the port is open or closed because for “open” we should receive [ack,syn] and for closed we should receive [rst,ack] but for filtered we do not receive any response.**

****

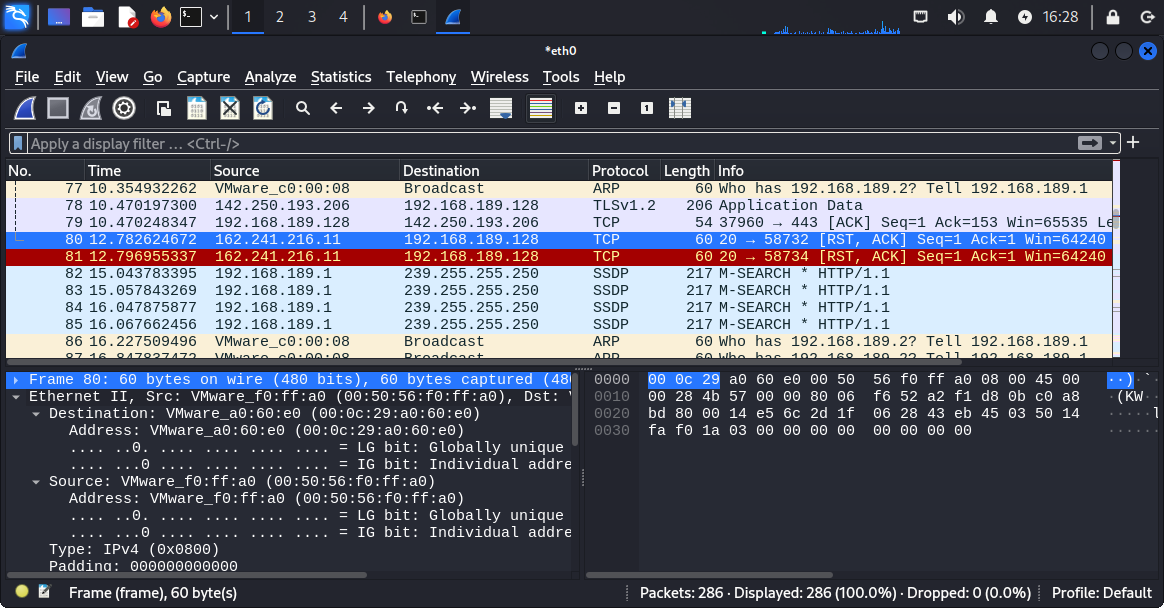
**As we can see that in packet number 8 and 9 two [SYN] requests were sent to port number 20 but no response was received.**

**Now we will be using packet fragmentation technique to evade the firewall that is not allowing us to know the exact port status.**

**The command: nmap -f [target ip address]**

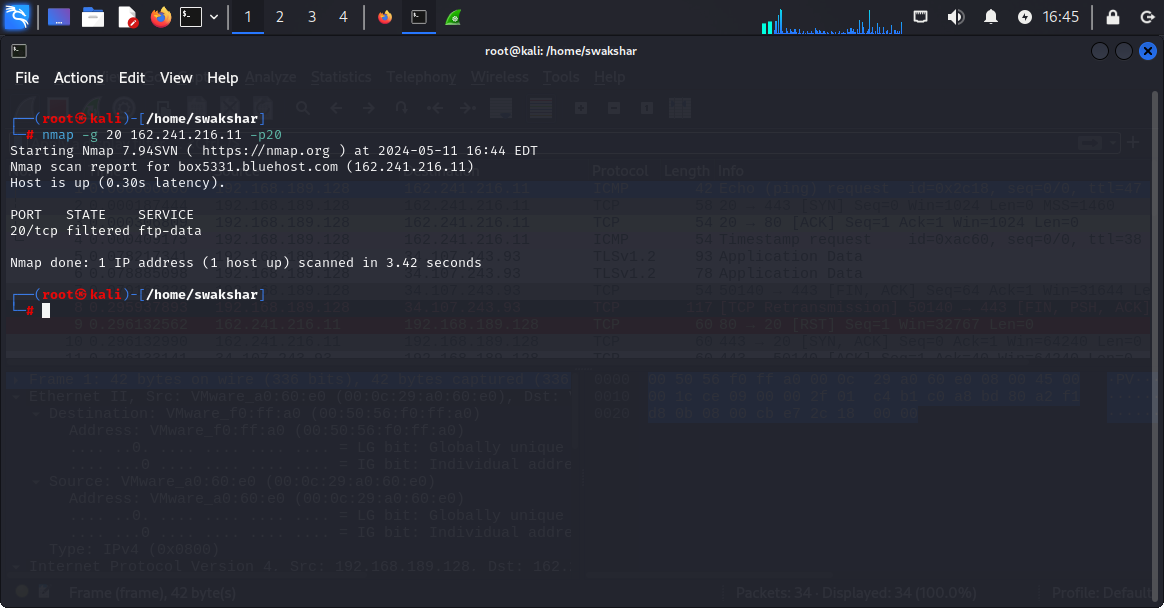
****

**We can still see the same output in kali linux but in wireshark there is something different**

****

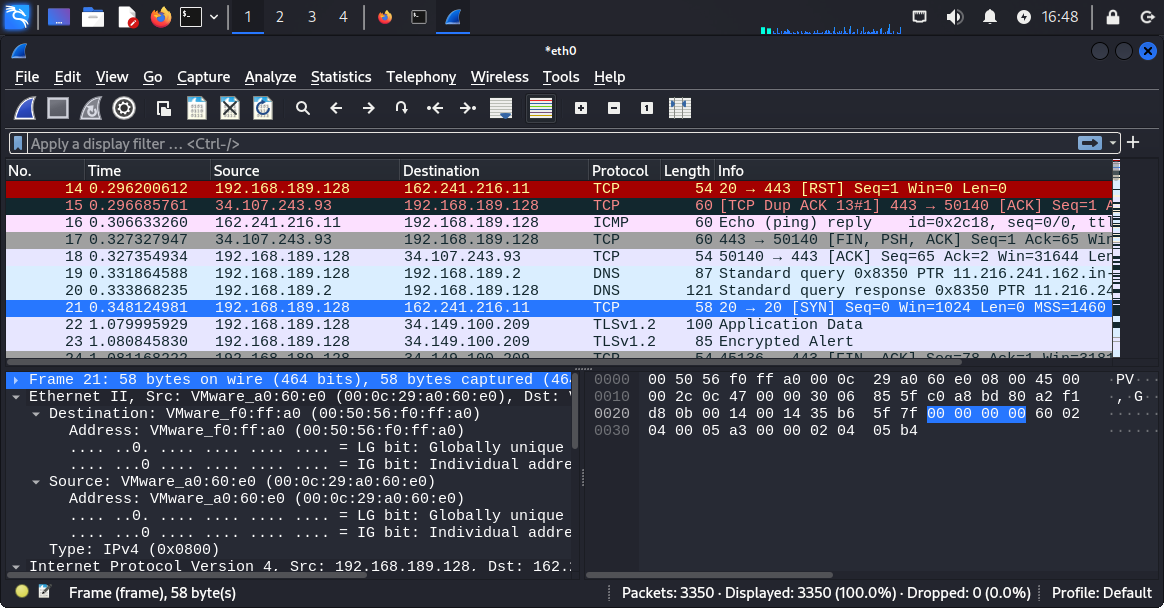
**Although we see that in kali linux it was showing as “FILTERED” but in wireshark we can see that from port 20 we have received[RST ,ACK] which means the port is closed .**

**2. Port manipulation: the command is nmap -g 80[port number] [target ip address] By using this command we are spoofing the port number just to confuse the firewall and reach the destination port.**

****

**As we can see that we are spoofing the port number and the spoofed port number is “20” and the result is still the same which is filtered.**

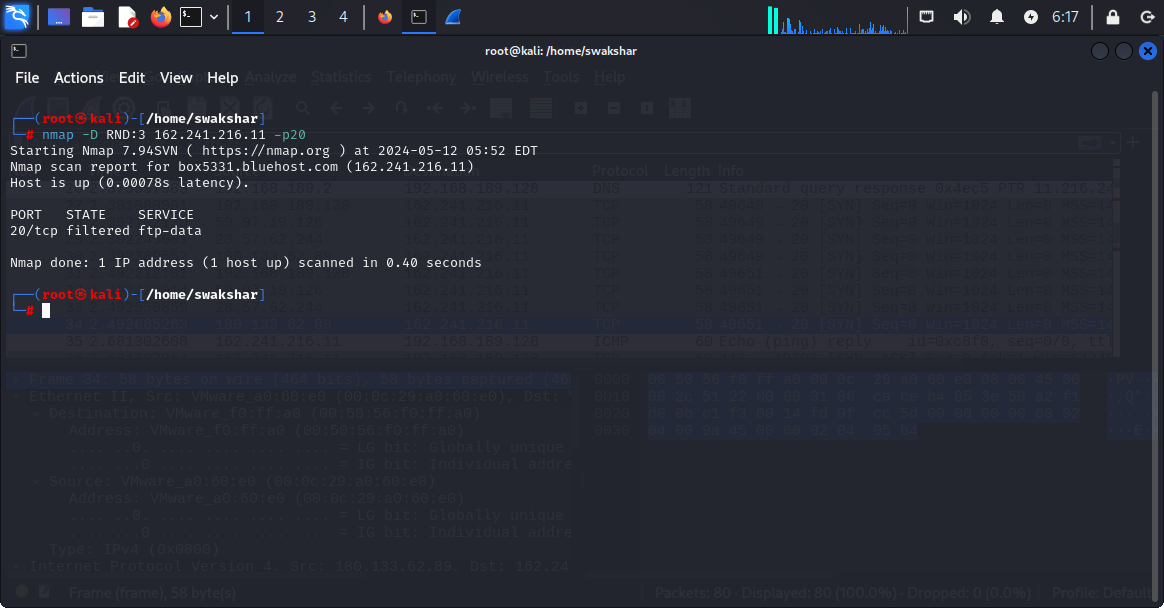
**Now we can see the wireshark report for that:**

****

**We can see that for packet number “21” from spoofed port number 20 we have sent the packet [SYN] to the original port 20 for the destination ip address 162.241.216.11 but in response there is no response. So port manipulation here is unable to evade the firewall unlike packet fragmentation.**

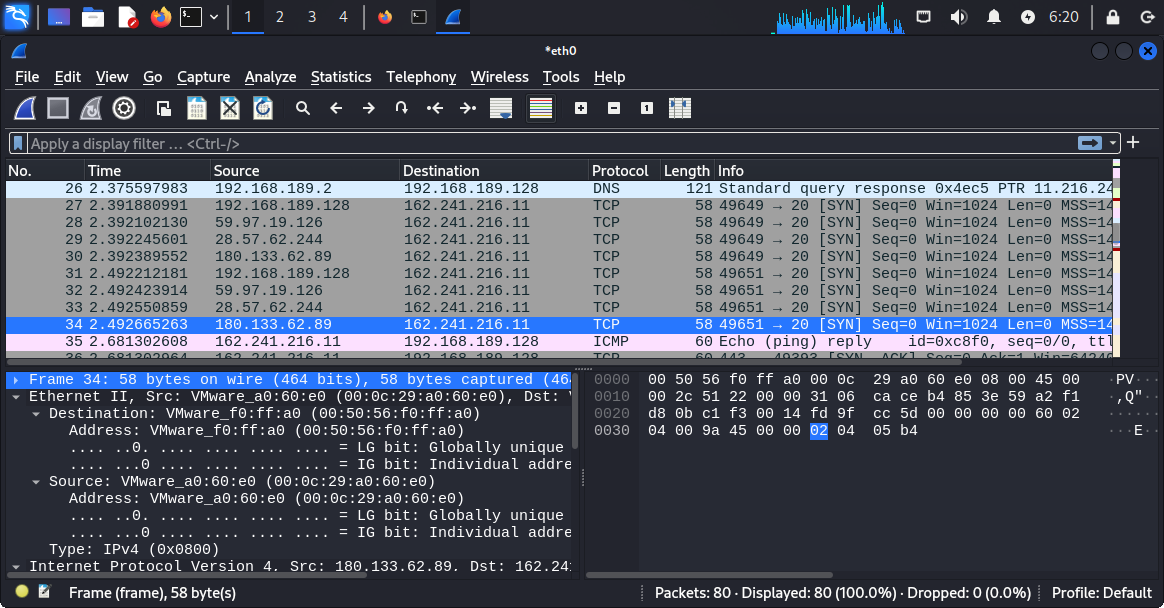
**3. Decoys: It means that we can use multiple ip addresses to hide our original ip address[192.168.189.128] and use random ip addresses to trick the firewall.**

**Command: nmap -D RND:3 162.241.216.11 -p20 , here 3 stands for number of random ip addresses .**

****

**As we can see that the result is still the same which is the port status is filtered .**

**Wireshark activity:**

****

**So we can see that our kali linux system has used 3 random ip addresses which are “59.97.19.126”[packet 28] , “28.57.62.244” [packet 29] , “180.133.62.89”[packet 30] along with the main kali linux ip address which is 192.168.189.128 but the whole motive is to evade the firewall that has been assigned to port “20” of the destination ip address.[SYN] request was sent by each of these ip addresses but no [RST] OR [ACK] packet was received.**

1. **Use Scanning timing to evade firewalls:**

**T0 : PARANOID**

**T1 : SNEAKY(THE BEST FOR FIREWALL EVASION)**

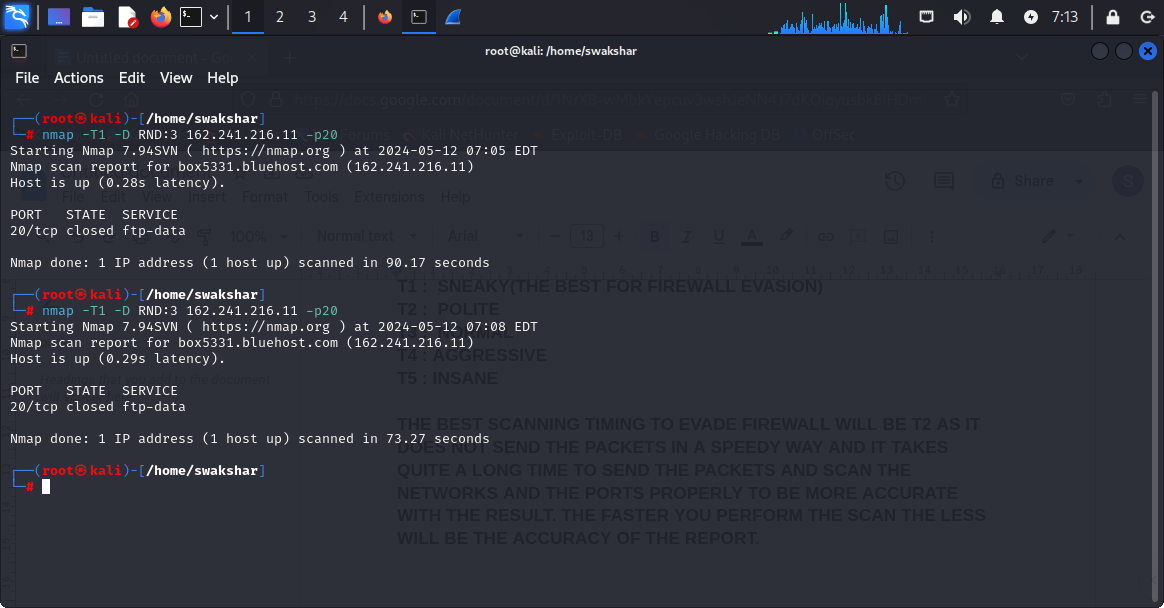
**T2 : POLITE**

**T3 : NORMAL**

**T4 : AGGRESSIVE**

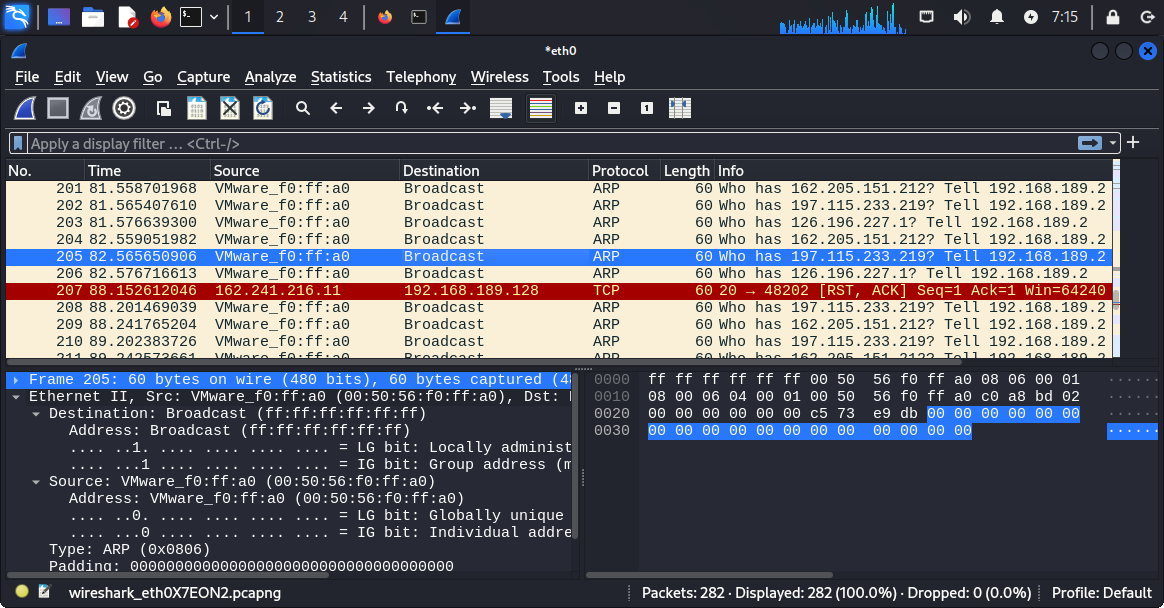
**T5 : INSANE**

**THE BEST SCANNING TIMING TO EVADE FIREWALL WILL BE T2 AS IT DOES NOT SEND THE PACKETS IN A SPEEDY WAY AND IT TAKES QUITE A LONG TIME TO SEND THE PACKETS AND SCAN THE NETWORKS AND THE PORTS PROPERLY TO BE MORE ACCURATE WITH THE RESULT. THE FASTER YOU PERFORM THE SCAN THE LESS WILL BE THE ACCURACY OF THE REPORT.**

****

**AS WE CAN SEE THAT IN THE PREVIOUS TECHNIQUES WE COULD NOT EVADE THE FIREWALL AND CONCLUDE THE PORT STATUS WHETHER IT IS OPEN OR CLOSED BUT HERE AS WE HAVE PERFORMED THE SCAN TIMING (-T1) ALONG WITH DECOYS SO THE RESULT IS CLEAR AND IT IS “CLOSED” NOT “FILTERED”**

**WIRESHARK REPORT:**

****

**AS WE CAN SEE THAT THE RED HIGHLIGHTED PACKET WHICH IS “207” WE HAVE RECEIVED THE [RST,ACK] FROM PORT NUMBER 20 FROM THE DESTINATION IP ADDRESS 162.241.216.11 SO THE PORT STATUS IS CONFIRMED AS “CLOSED” BY EVADING THE FIREWALL WITH SCANNING TIMING “SNEAKY” AND “DECOYS”.**

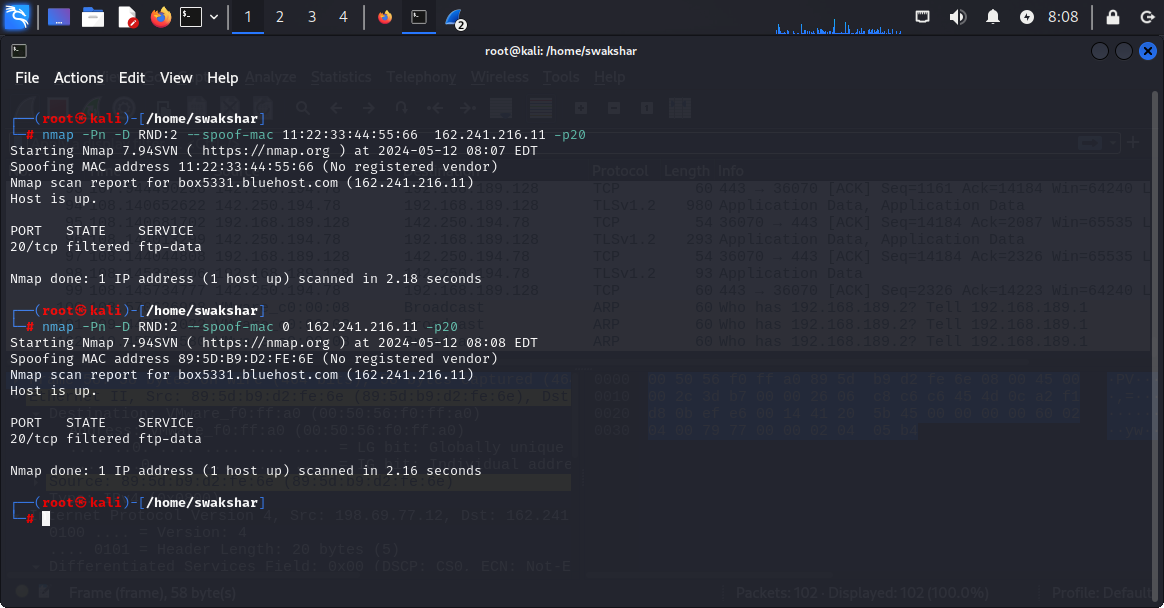
**5.using spoofing of MAC address to evade firewall**

**Command: nmap - - spoof-mac 0 [target ip address]**

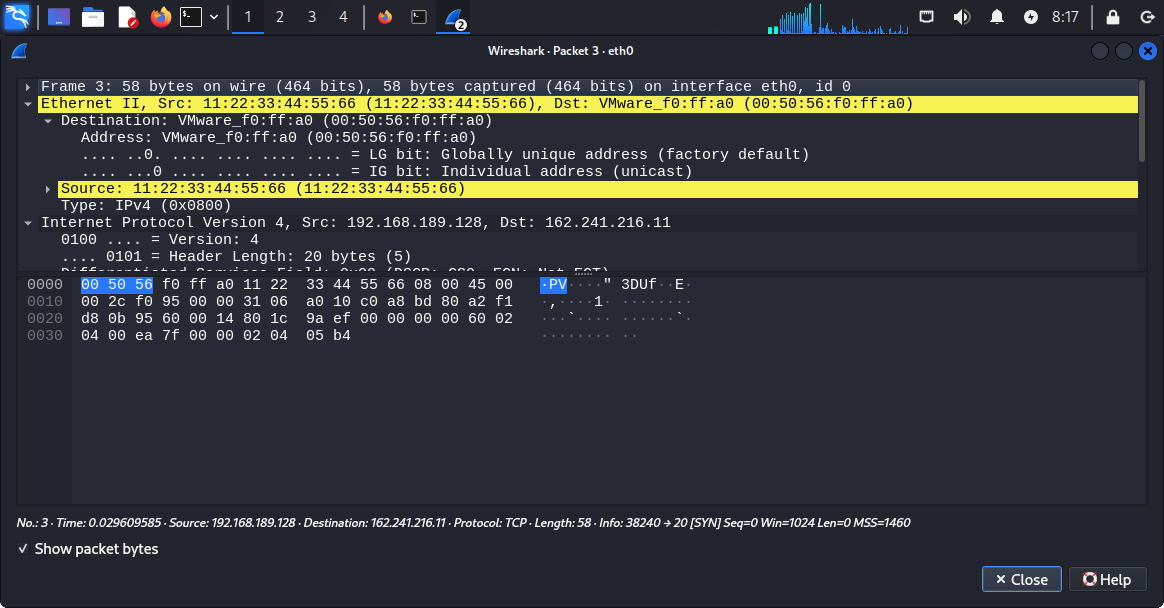
**Nmap - - spoof-mac 11:22:33:44:55:66[target ip address]**

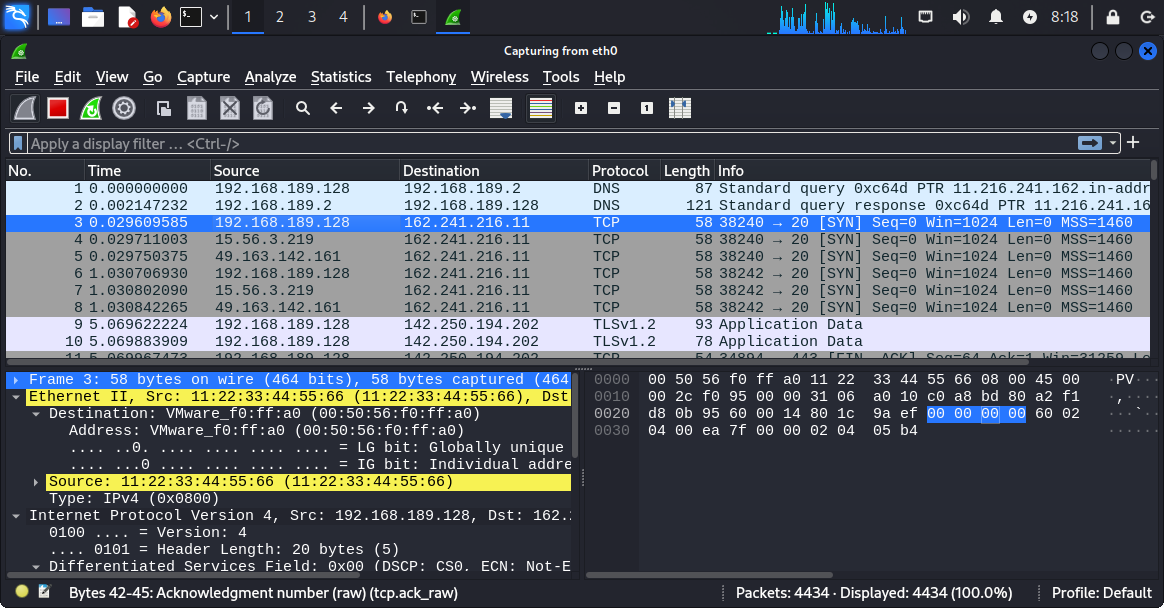
**Nmap - - spoof-mac dell [target ip address]**

**There are many ways of writing the spoof mac command where we are puting the mac address manually or it is taken randomly from no registered vendor or we put a company name like”dell” and the mac of dell is being used to evade firewall**

****

**As we can see that we have performed spoof mac where we have put 0 for random mac which is “ 89:5d:b9:d2:fe:6e” and in the other part we have used a manual mac which is “11:22:33:44:55:66”**

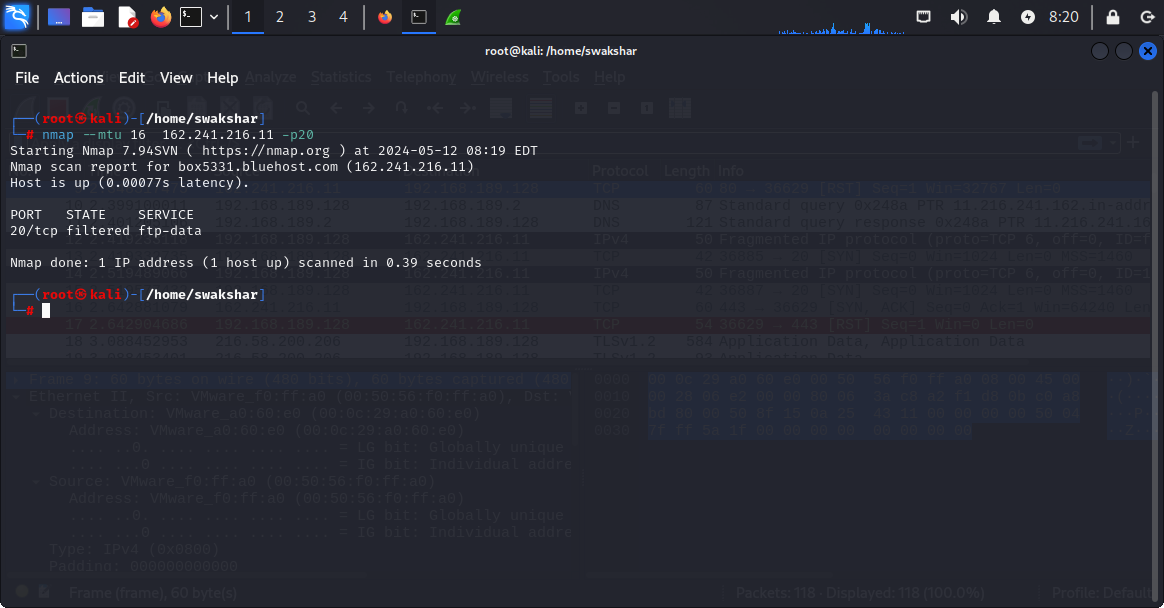
****

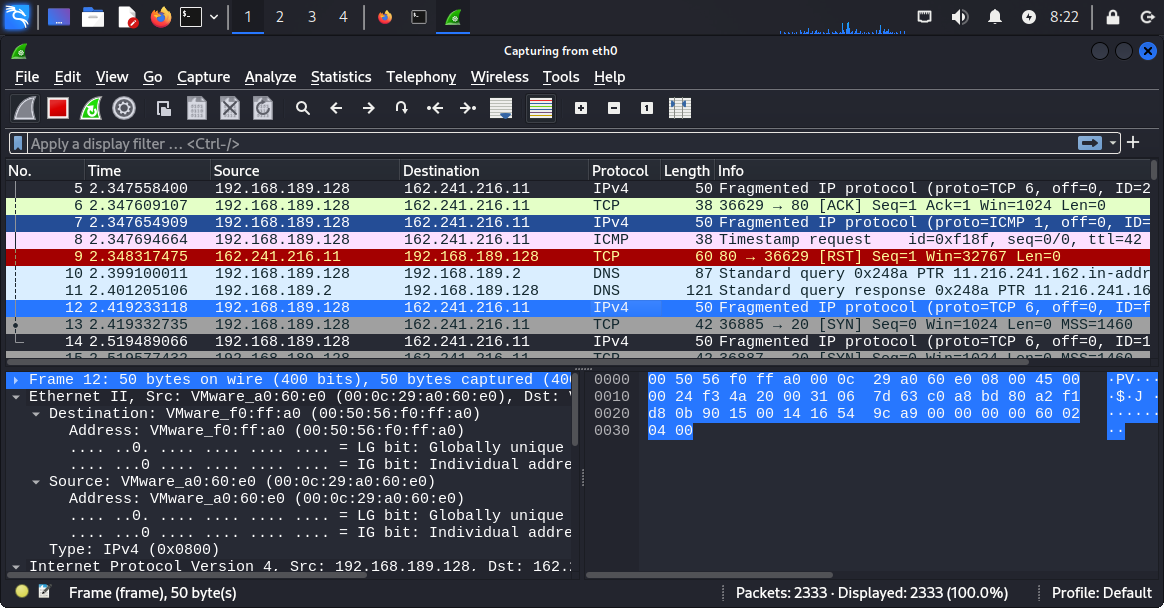
****

**Here we can see that the result is still “unfiltered” and we have not got any reset flag from the destination port and destination ip address .**

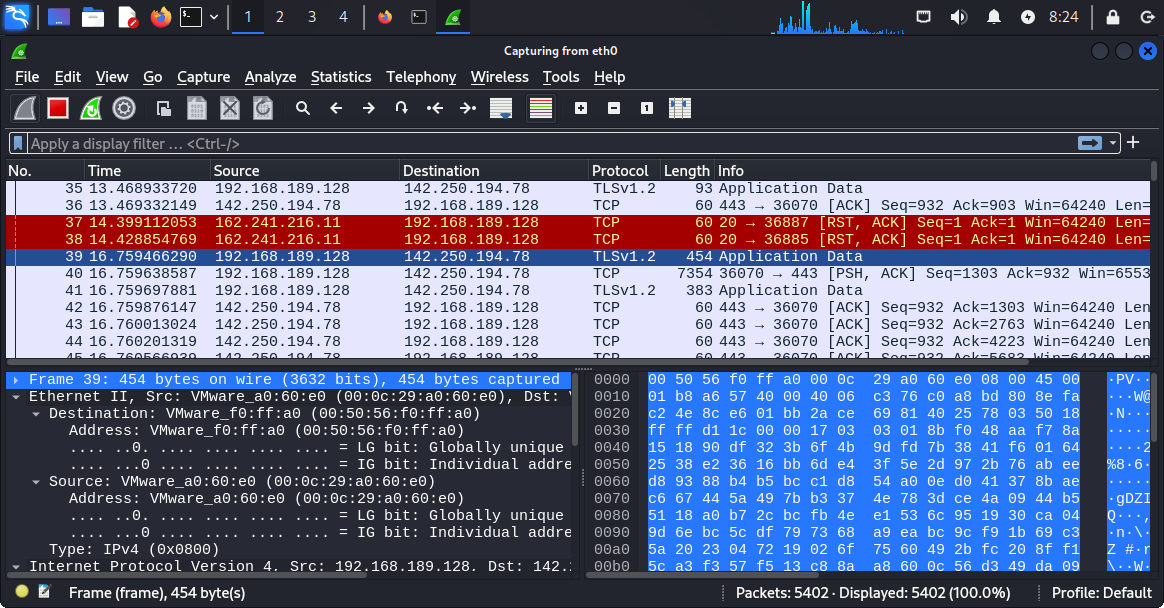
**6.packet fragmentation using - -mtu [multiple of 8]**

**Command: nmap - - mtu 16 162.241.216.11 -p20**

****

****

**We can see that in the packet number “12” 50 fragmented ip protocol packets were sent to port number 20 which was a [SYN] request .**

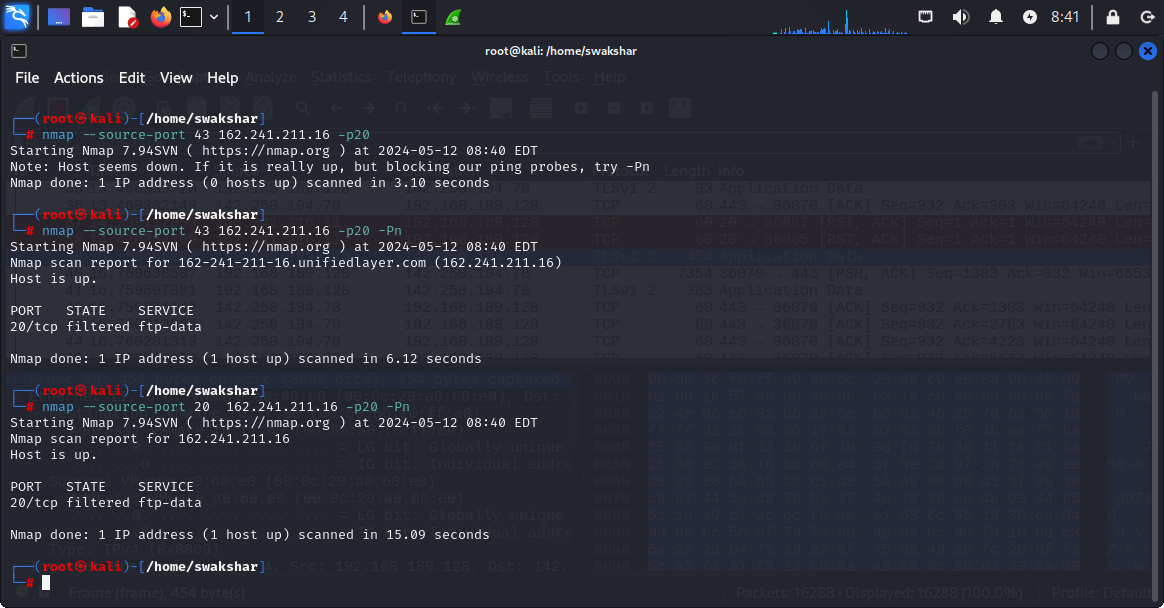
****

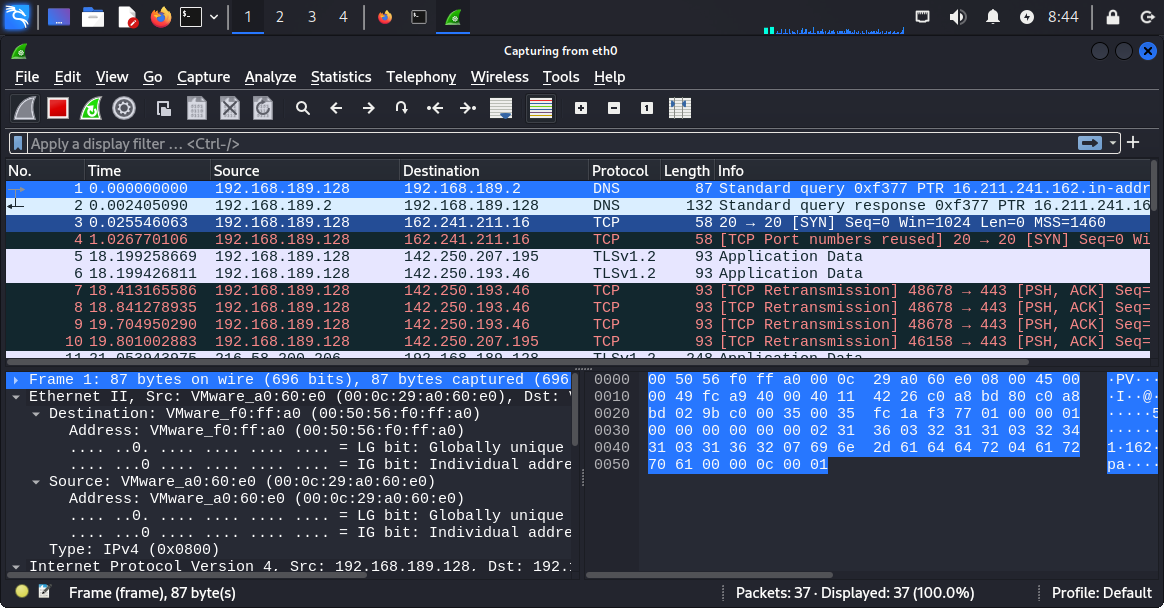
**Although in kali linux we have got the result which is “filtered” but in wireshark in packet number “37” and packet number “38” we have received the [RST , ACK] PACKET from port number “20” which again reconfirmed that the port 20 is closed.**

**7.source port \\source address spoofing:**

**Command: nmap - - source-port 43 162.241.211.16 -p20 -Pn**

**No ping probe and we are spoofing the original source port and we have given the port number 20 to evade the firewall for the destination port**

****

****

**As we can see that in packet number “3” in wireshark we have used the spoofed port number “20” to evade firewall in the destination ip address.**

**But no reset flag or ack flag were received so the status is still “filtered”**

**8. Sending custom UDP AND SYN packets by using hping3 to perform flood attacks or DOS attacks:**

**Command: hping3 - -count [no of packets] - - data [data size] - - win [window size] - -udp - - rand-source - - flood [target ip address] -p 20**

**By using these command we can put the firewalls in useless action of preventing or analysing superfluous requests of udp or syn packets without completing the three way handshake and therefore impacting their firewall service and using that as an advantage to evade the firewall and IDs.**

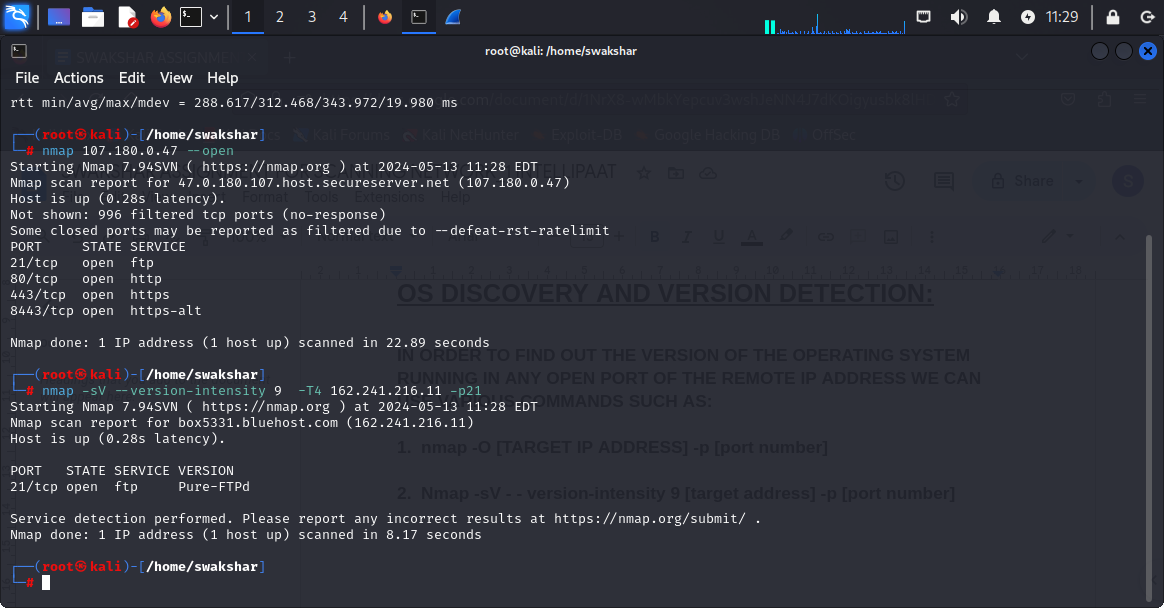
**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**OS DISCOVERY AND VERSION DETECTION:**

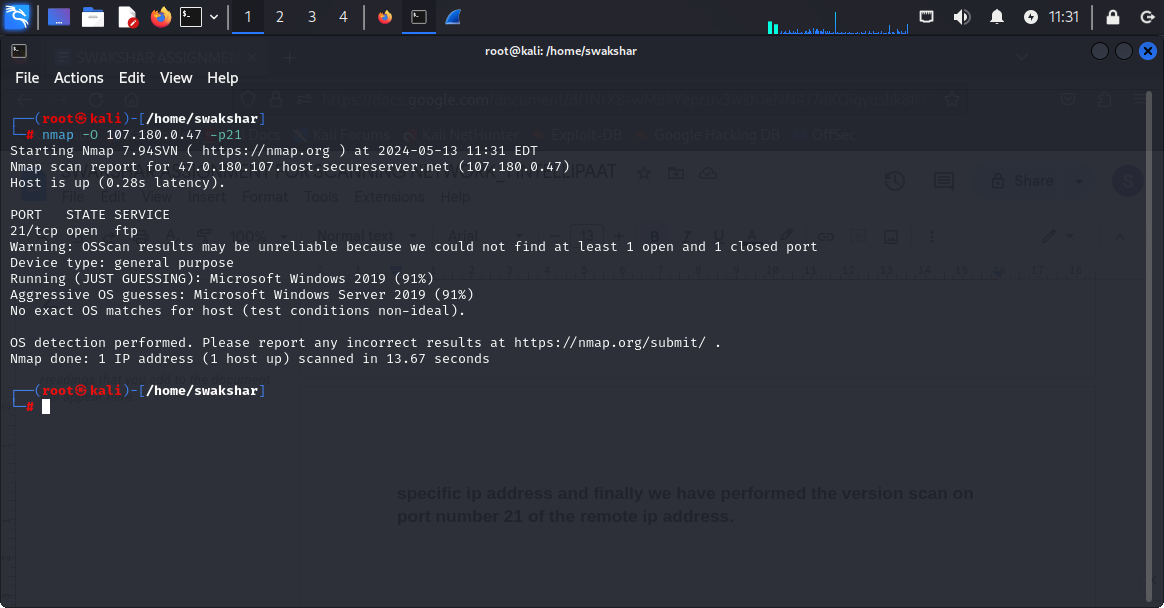
**IN ORDER TO FIND OUT THE VERSION OF THE OPERATING SYSTEM RUNNING IN ANY OPEN PORT OF THE REMOTE IP ADDRESS WE CAN USE VARIOUS COMMANDS SUCH AS:**

**1. nmap -O [TARGET IP ADDRESS] -p [port number]**

**2. Nmap -sV - - version-intensity 9 [target address] -p [port number]**

****

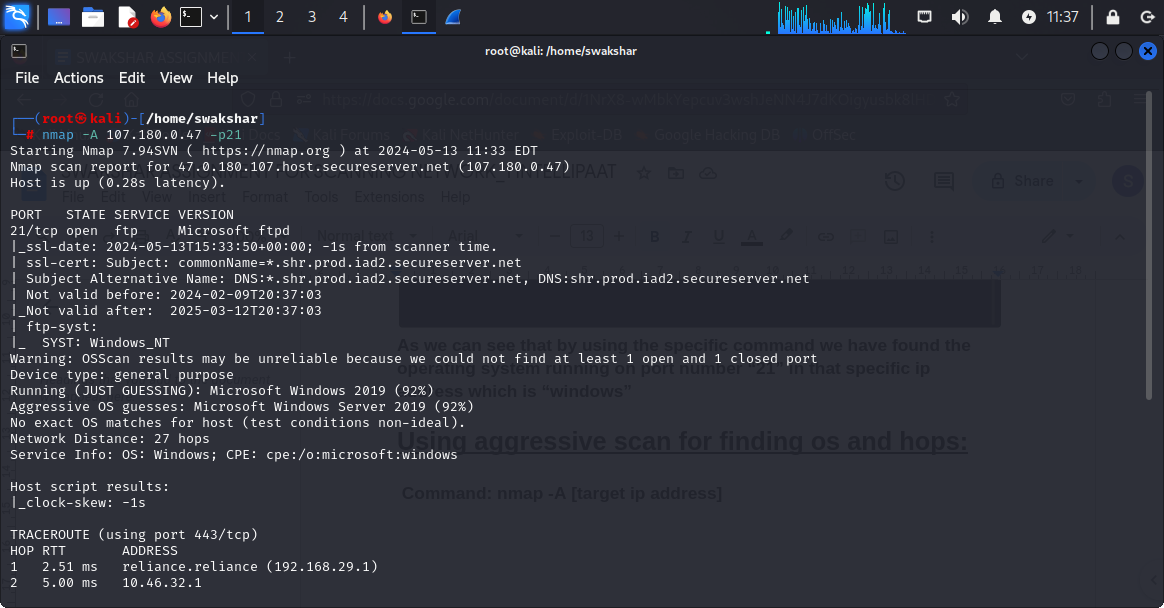
**As we can see that we are using the ip address of** [**www.goodshopping.com**](http://www.goodshopping.com) **and we have found the open ports of that specific ip address and finally we have performed the version scan on port number 21 of the remote ip address.**

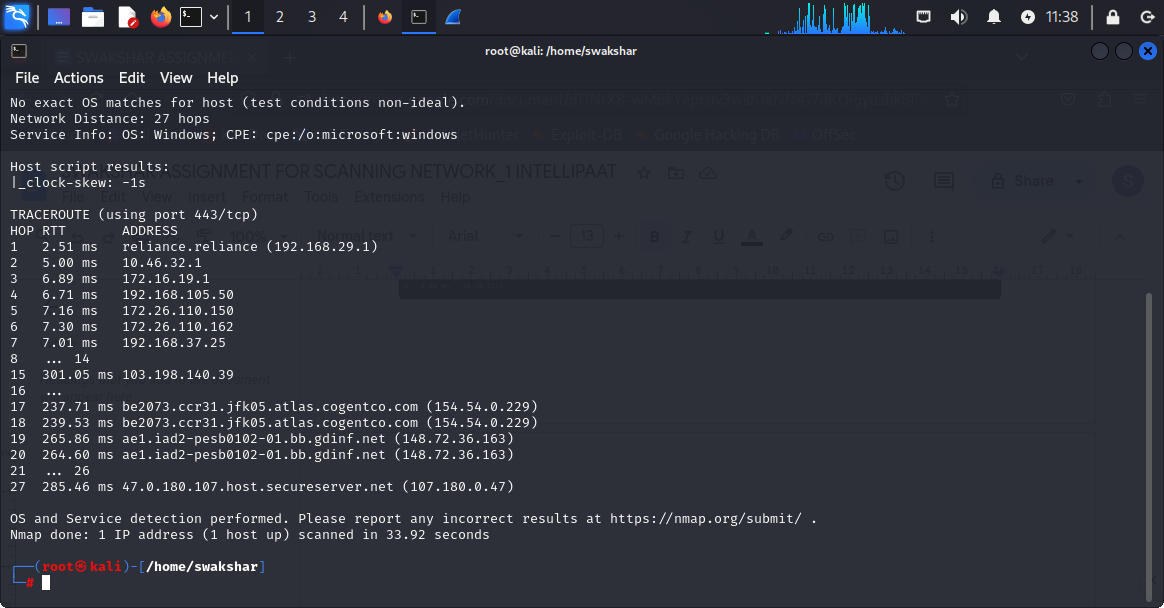
****

**As we can see that by using the specific command we have found the operating system running on port number “21” in that specific ip address which is “windows”**

**Using aggressive scan for finding os and hops:**

**Command: nmap -A [target ip address]**

****

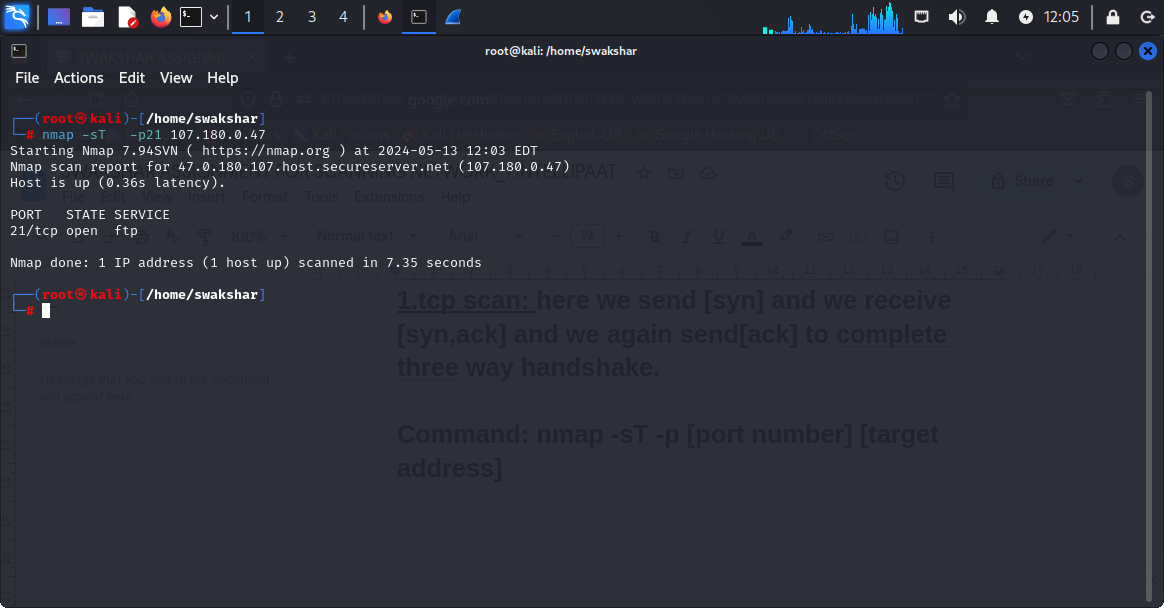
****

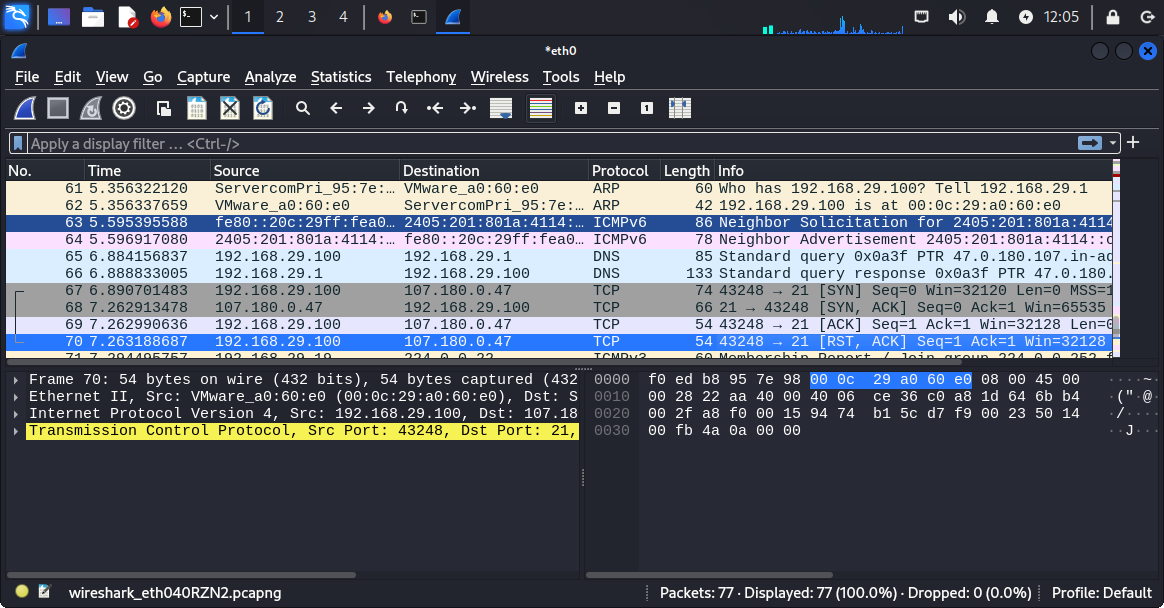
**We can see by doing the aggressive scanning we have found out the version and the number of hops as well for the corresponding port number for specific ip address.**

**Exploring wireshark in scanning network:**

**1.tcp scan: here we send [syn] and we receive [syn,ack] and we again send[ack] to complete three way handshake.**

**Command: nmap -sT -p [port number] [target address]**

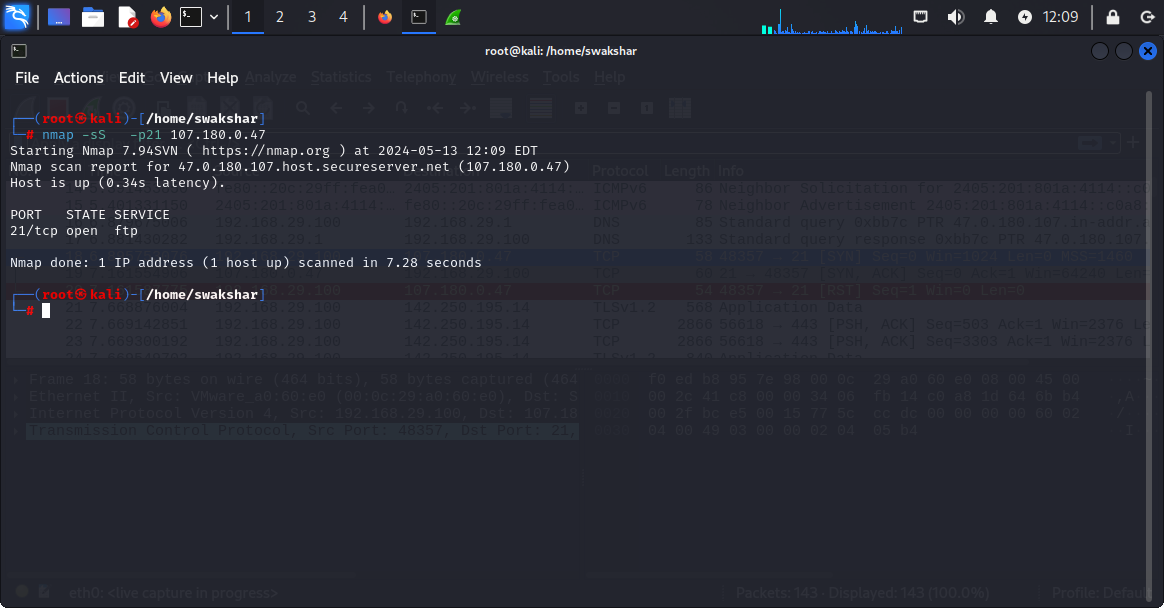
****

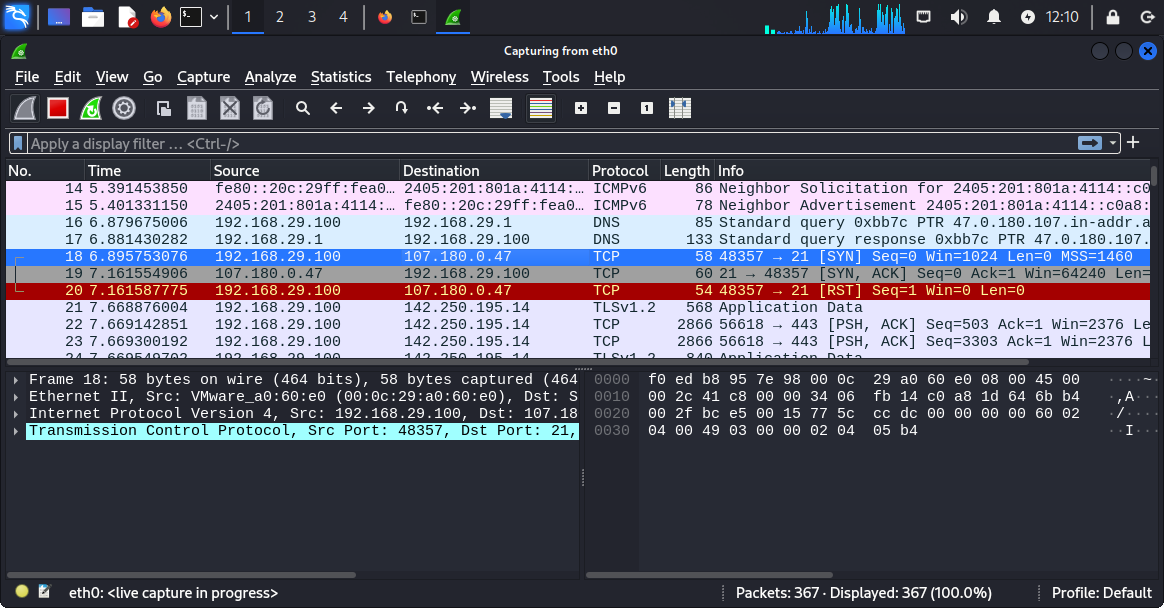
****

**WE CAN SEE THAT IN THE PACKET NUMBERS**

**“67” “68” AND “69” the three way handshake process is being followed.**

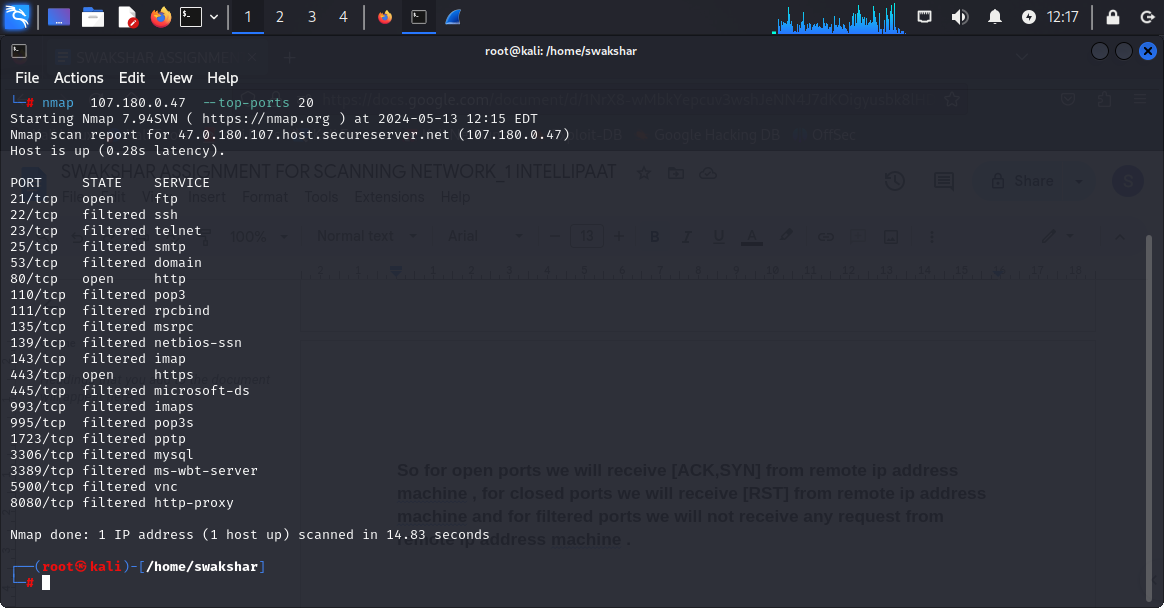
**2.STEALTH scan: in this case we send [syn] requests but as soon as we receive [ACK,SYN] we simply drop the request packet by sending [RST] because we do not want to complete the three way handshake process and acknowledge the ack packet. That is why it is also called the “half open scan”**

****

****

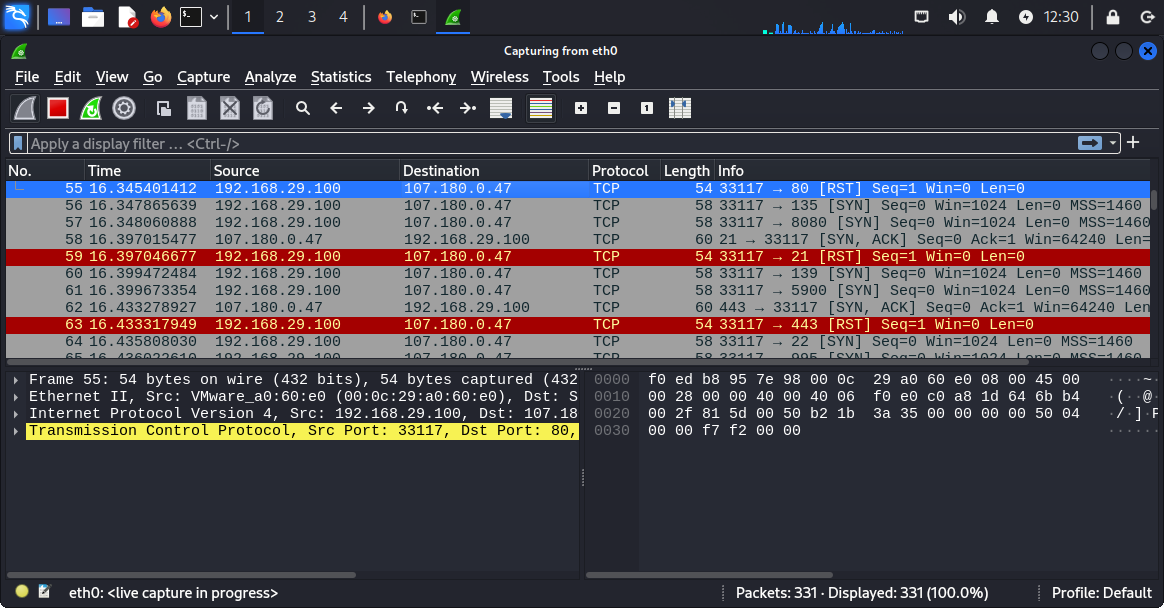
**AS WE CAN SEE THAT IN THE PACKET NUMBER “18” WE HAVE SENT THE [SYN] signal AND IN PACKET NUMBER 19 WE HAVE RECEIVED [ACK,SYN] SIGNAL BUT IN PACKET NUMBER “20” WE HAVE JUST DROPPED THE PACKET BY SENDING [RST].**

**So for open ports we will receive [ACK,SYN] from remote ip address machine , for closed ports we will receive [RST] from remote ip address machine and for filtered ports we will not receive any request from remote ip address machine .**

****

**Here we have scanned top 20 ports of the respective ip address.**

**Lets see the wireshark screenshot and analyse the packet results.**

****

**We can see the [SYN,ACK] request received by the source ip address and source port but there are no responses from the filtered ports just because the firewall just have dropped them.**

**GENERATING COMPREHENSIVE REPORT:**

**SO WE HAVE PERFORMED ALL SORTS OF SCANNING TECHNIQUES TO PERFORM HOST DISCOVERY, PORT STATUS SCANNING,FIREWALL AND IDs EVASION AND VERSION AND OS DISCOVERY ALONG WITH THEIR WIRESHARK ANALYSIS.**

**MOST IMPORTANT OBSERVATION FROM THE REPORT:**

**1. ONLY IF WE ARE PLANNING TO CONNECT TO OUR REMOTE IP THEN ONLY WE SHOULD DO TCP SCAN WHICH IS -sT WHERE WE ARE WAITING FOR [SYN,ACK]FROM THE REMOTE PORT SO WE CAN ACKNOWLEDGE.**

**2.WE SHOULD USE THE STEALTH SCAN OR SYN SCAN OR SHORT -sS TO DO THE SCANNING IN A FASTER WAY AND ALSO TO DO THE SCANNING FOR EFFICIENTLY AS WE ARE NOT PLANNING TO CONNECT TO OUR REMOTE HOST .SO AS SOON AS WE GET [ACK,SYN] WE JUST DROP THE PACKET.**

**3.WE SHOULD BE USING -Pn WHICH IS NO PING PROBE TO PERFORM HOST DISCOVERY MORE EFFICIENTLY.**

**4.SCANNING TIMING IS VERY IMPORTANT .THE FASTER WE SCAN THE LESS WILL BE THE ACCURACY AND THE SLOWER WE DO THE SCAN THE MORE WILL BE THE ACCURACY.SO TO EVADE THE FIREWALL THE MOST POPULAR SCANNING TECHNIQUE WILL BE -T1:WHICH IS SNEAKY OR -T0 WHICH IS PARANOID BUT TO PERFORM SCANNING FASTLY WE CAN USE -T4 WHICH IS AGGRESSIVE.**

**5.WE HAVE VARIOUS METHODS OF FIREWALL EVASION WHICH ARE SCANNING TIMING, SENDING EMPTY PACKET FOR EXAMPLE NULL SCAN -sN , FRAGMENTATION ALONG WITH SPECIFIED MAXIMUM TRANSMISSION UNIT -f mtu 16**

**PORT MANIPULATION WHICH IS -g [port number] , SOURCE PORT SPOOFING WHICH IS -- source-port[port number], SPOOFING IP ADDRESS OR DECOYS -D RND:[NUMBER OF RANDOM IPS] OR WE CAN USE SPOOF MAC WHICH IS - -spoof-mac [specified mac] OR WE CAN USE HPING3 AS WELL WHERE WE CAN SEND CUSTOM UDP OR SYN PACKETS TO PERFORM A DOS ATTACK OR FLOODING TO BRING DOWN THE FIREWALL VIGILANCE OR SERVICE SO WE CAN PERFORM SCANNING AND EVADE THEM.**

**6.JUST TO DISCOVER THE HOST WHETHER IT IS UP OR DOWN WE SHOULD USE -sn NO PORT SCAN ONLY HOST DISCOVERY.**

**7.WE CAN USE VARIOUS FLAGS WITH ping command like -c ,-i -w , -q , -s , - a , or –scan-delay to control our ping request.**

**8.WE HAVE MANY OTHER TYPES OF nmap SCANNING LIKE NULL SCAN,FIN SCAN,XMAS SCAN,ZOMBIE SCAN,WINDOW SCAN,TIMESTAMP SCAN TO EVADE FIREWALL IN DIFFERENT SCENARIOS.**

**9.WE CAN ALSO USE METASPLOIT-FRAMEWORK IN KALI LINUX TO EXPLOIT CERTAIN TARGET SYSTEM AND EVADE THE FIREWALL .IN THAT CASE WE NEED TO GO TO KALI LINUX AND TYPE >> service postgresql start>>msfconsole>>db\_status>>it must show connected>>search smb or grep exploit search smb(for example)>>use [the preferable exploitation tool]>>show option>>set RHOSTS[TARGET IP ADDRESS]>>EXPLOIT**

**10.THE ABOVEMENTIONED ARE ALL THE IMPORTANT OBSERVATION FROM SCANNING NETWORK ASSIGNMENT AND ALL THESE THINGS ARE NEEDED TO BE TAKEN INTO CONSIDERATION TO ENHANCE AND IMPROVE THE NETWORK SECURITY AND TO EXPAND THE EASE OF FINDING VULNERABILITY AND EXPLOIT THE TARGET NETWORK.**

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*end of assignment\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***