NETWORK TRAFFIC PACKET ANALYSIS USING WIRESHARK

Group 5:

1. **Ivan Kasvan Opio**
2. **Austine Baraka**
3. **Barnice Wakiro Njoroge**
4. **Murungi Micheal Charles**
5. **Emmanuel Kofi Ansah-Anobah**
6. **Kitso Bantom**
7. **Emelda Adhiambo**
8. **Leon marienga**
9. **Buyondo Vale**

1. Introduction

In this assignment, we are tasked with investigating a potential security incident on a company web server. The SOC team detected unusual activity within the intranet and captured network traffic for further analysis. This captured pcap file that likely contained evidence of malicious behavior, including credential theft and service disruption.

Our goal was to analyze the provided pcap file to uncover critical details of the attack, such as compromised credentials, the server involved, and the specific attack methods used. By answering the questions posed, we gained deeper insight into the attacker's actions and this will help prevent future incidents.

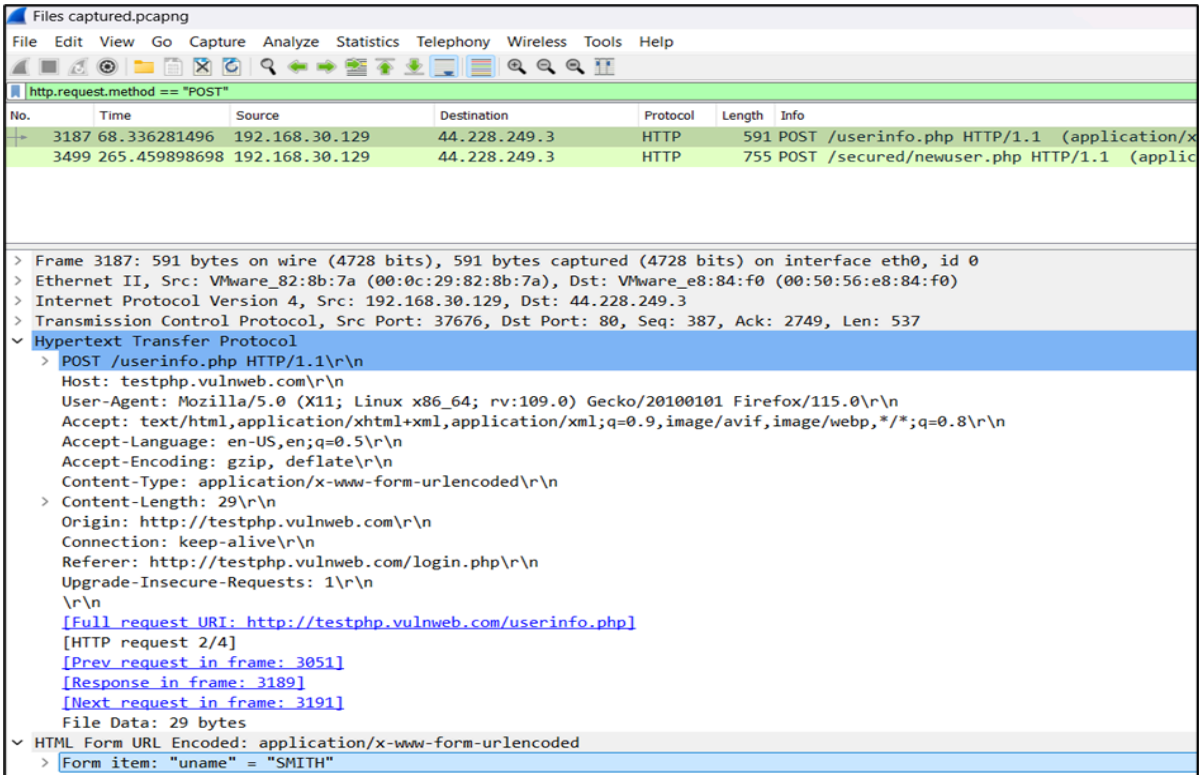
2. The Lab setup

For this assignment we dealt with a pcap file which is a data file used to store network packet data. This data is important as it can allow network administrators to analyze network traffic, troubleshoot network issues, and monitor network issues.In order to interact with these types of files there are specialized tools that are used including but not limited to Wireshark. Wireshark is a powerful, open source tool for Network traffic analysis that comes bundled with the Kali Linux operating system. Its wide range of filtering options for packet analysis and the ease of use are the reasons the group chose it for this challenge.

3. Packet Analysis

3.1 Username of the Victim

This information was found by inspecting the traffic, likely in a HTTP unencrypted protocol. The group filtered for authentication requests using: ***http.request.method* == *"POST"*.** The packet details interface in the HTTP packet the details of the form reveal the username as ***"SMITH".***


Files captured.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

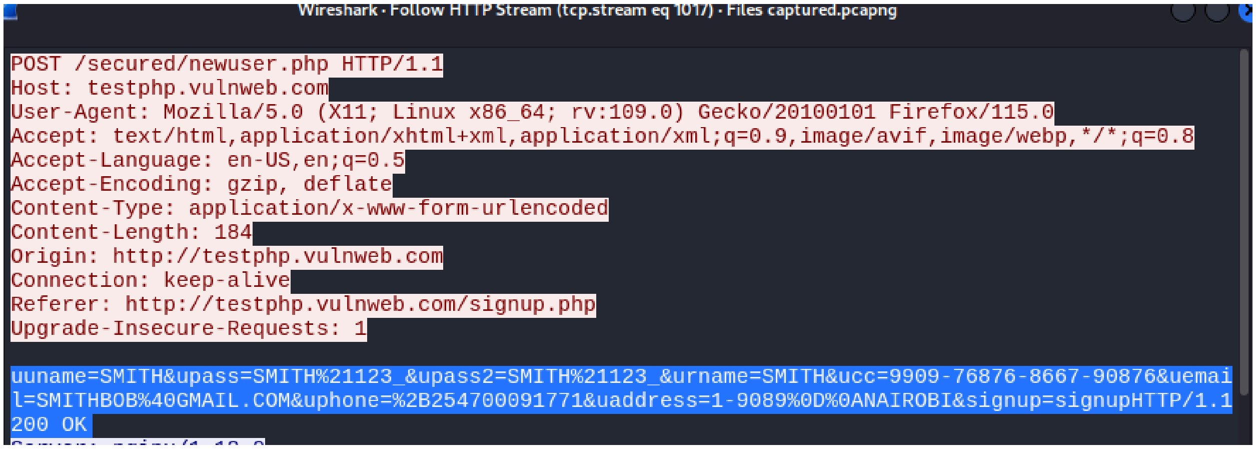
```
http.request.method == "POST"

No.    Time            Source           Destination    Protocol  Length Info
  3187 68.336281496    192.168.30.129   44.228.249.3   HTTP         591 POST /userinfo.php HTTP/1.1  (application/x
  3499 265.459898698   192.168.30.129   44.228.249.3   HTTP         755 POST /secured/newuser.php HTTP/1.1  (applic

> Frame 3187: 591 bytes on wire (4728 bits), 591 bytes captured (4728 bits) on interface eth0, id 0
> Ethernet II, Src: VMware_82:8b:7a (00:0c:29:82:8b:7a), Dst: VMware_e8:84:f0 (00:50:56:e8:84:f0)
> Internet Protocol Version 4, Src: 192.168.30.129, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 37676, Dst Port: 80, Seq: 387, Ack: 2749, Len: 537
v Hypertext Transfer Protocol
  > POST /userinfo.php HTTP/1.1\r\n
    Host: testphp.vulnweb.com\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
  > Content-Length: 29\r\n
    Origin: http://testphp.vulnweb.com\r\n
    Connection: keep-alive\r\n
    Referer: http://testphp.vulnweb.com/login.php\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://testphp.vulnweb.com/userinfo.php]
    [HTTP request 2/4]
    [Prev request in frame: 3051]
    [Response in frame: 3189]
    [Next request in frame: 3191]
    File Data: 29 bytes
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "uname" = "SMITH"
```

3.2 Password of the Victim:

The password was identified in the payload of HTTP POST requests. We used the filter ***http.request.method == "POST"*** and ***http.response.*** Following the HTTP stream the password is passed with one character encoded, and visible in the packet payload. **“SMITH!123”**



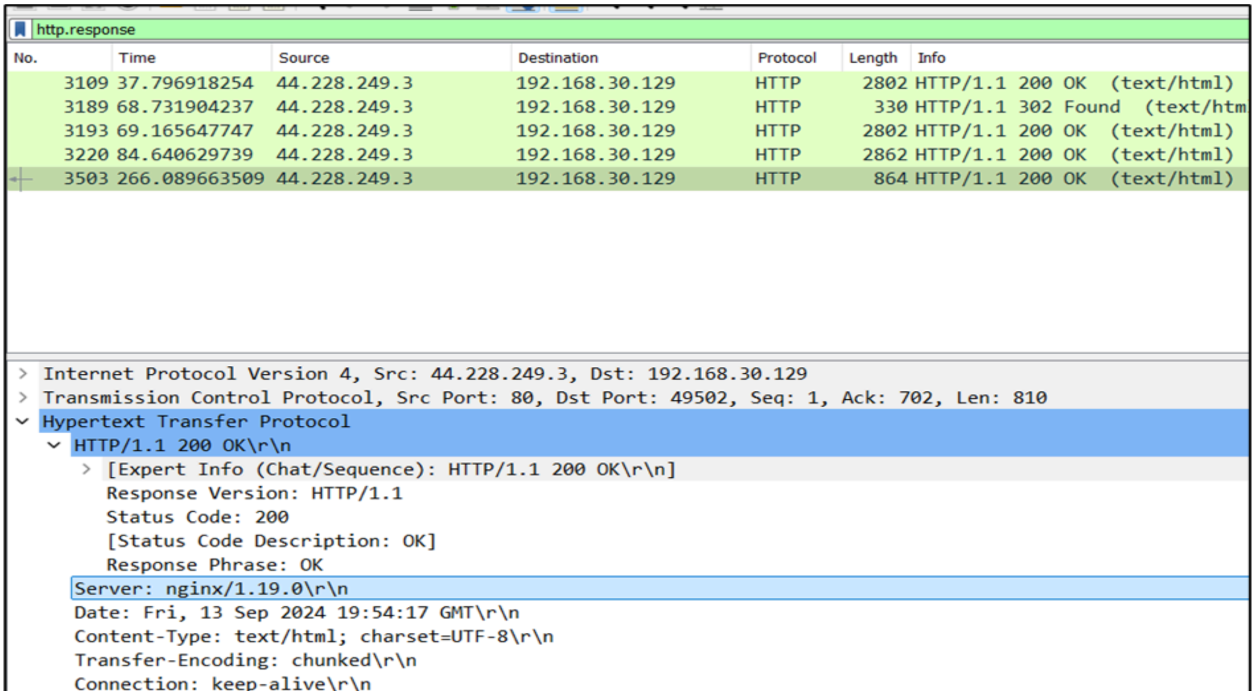
Wireshark · Follow HTTP Stream (tcp.stream eq 1017) · Files captured.pcapng

```
POST /secured/newuser.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 184
Origin: http://testphp.vulnweb.com
Connection: keep-alive
Referer: http://testphp.vulnweb.com/signup.php
Upgrade-Insecure-Requests: 1

uuname=SMITH&upass=SMITH%21123_&upass2=SMITH%21123_&urname=SMITH&ucc=9909-76876-8667-90876&uemai
l=SMITHBOB%40GMAIL.COM&uphone=%2B254700091771&uaddress=1-9089%0D%0ANAIROBI&signup=signupHTTP/1.1
200 OK
```

3.3 Server and Version Identification

The group Looked at the response headers of the HTTP traffic. HTTP headers often contain server details. We filtered using **http.response** and identified the server to be **nginx/1.19.0**



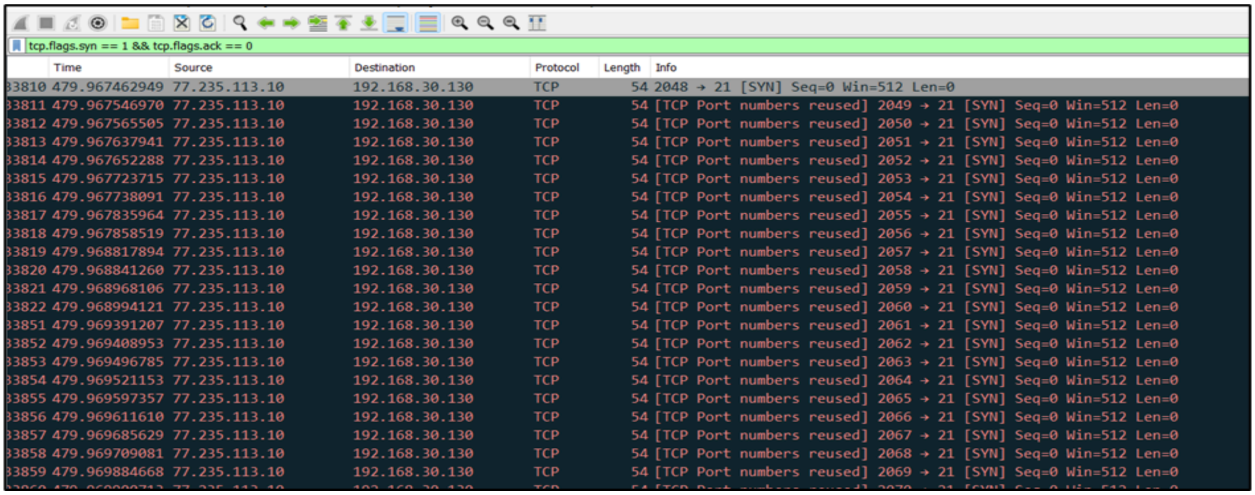
```
http.response
```

No.	Time	Source	Destination	Protocol	Length	Info
3109	37.796918254	44.228.249.3	192.168.30.129	HTTP	2802	HTTP/1.1 200 OK (text/html)
3189	68.731904237	44.228.249.3	192.168.30.129	HTTP	330	HTTP/1.1 302 Found (text/htm
3193	69.165647747	44.228.249.3	192.168.30.129	HTTP	2802	HTTP/1.1 200 OK (text/html)
3220	84.640629739	44.228.249.3	192.168.30.129	HTTP	2862	HTTP/1.1 200 OK (text/html)
3503	266.089663509	44.228.249.3	192.168.30.129	HTTP	864	HTTP/1.1 200 OK (text/html)

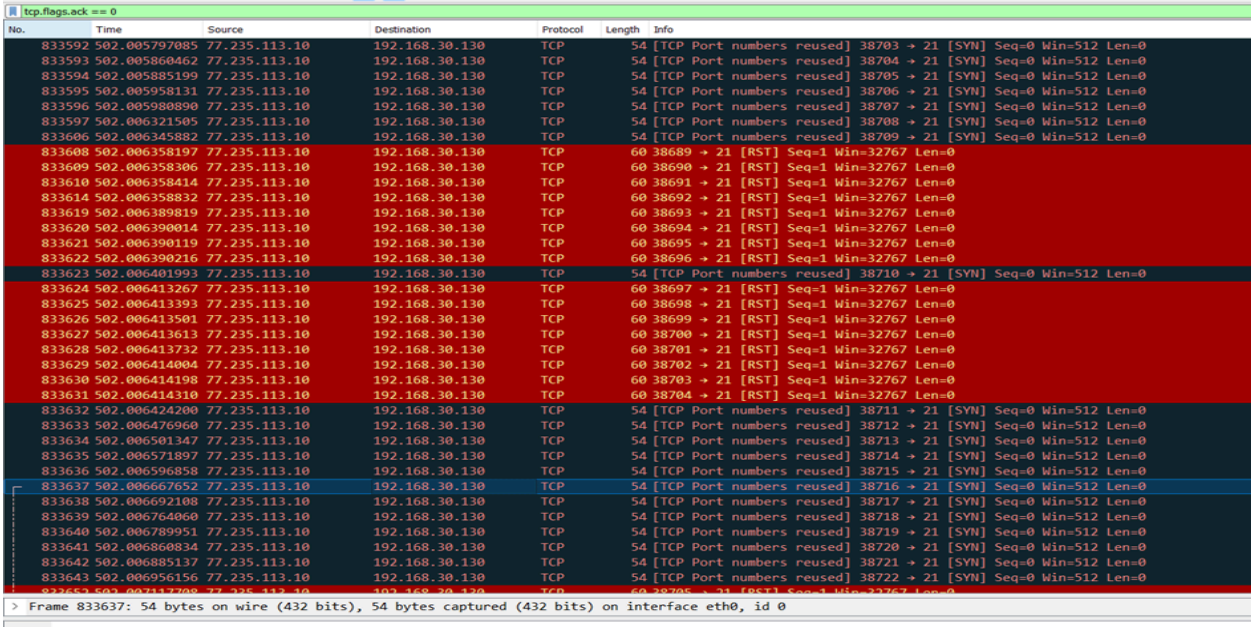
```
> Internet Protocol Version 4, Src: 44.228.249.3, Dst: 192.168.30.129
> Transmission Control Protocol, Src Port: 80, Dst Port: 49502, Seq: 1, Ack: 702, Len: 810
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Server: nginx/1.19.0\r\n
    Date: Fri, 13 Sep 2024 19:54:17 GMT\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    Transfer-Encoding: chunked\r\n
    Connection: keep-alive\r\n
```

3.4 Attack carried out

To identify the type of attack carried out by the attacker, the group looked for signs of abnormal traffic. We used the filters **tcp.flags.syn == 1 and tcp.flags ack == 0** to see if there's a large number of SYN requests without responses**.** These filters specifically targetted where the SYN flag was activated. We identified numerous SYN packets being sent within seconds of each other from two source ips **77.235.113.10** to a possible FTP server **192.168.30.130** using port **21** to overwhelm the server suggesting a **Denial of Service attack** using **: SYN Flooding .**



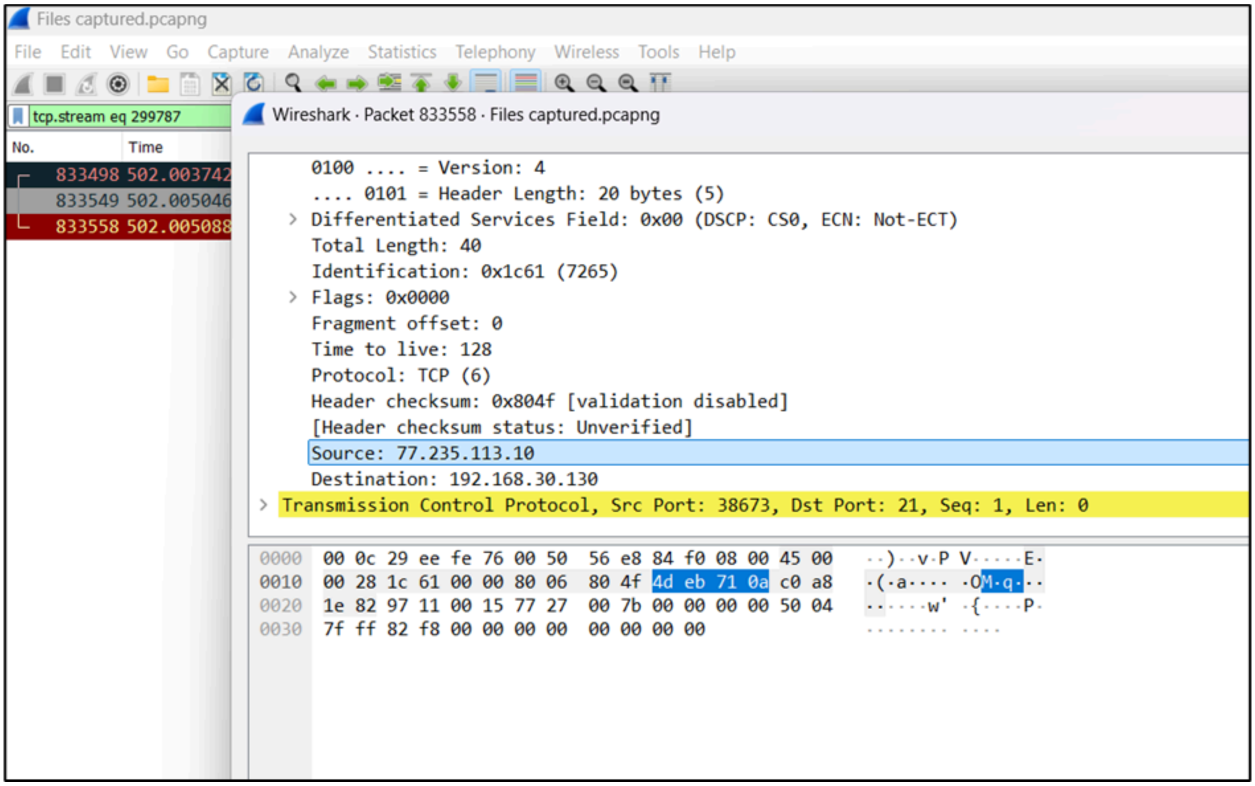
```
tcp.flags.syn == 1 && tcp.flags.ack == 0
      Time          Source          Destination     Protocol  Length  Info
33810 479.967462949 77.235.113.10   192.168.30.130  TCP       54 2048 → 21 [SYN] Seq=0 Win=512 Len=0
33811 479.967546970 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 2049 → 21 [SYN] Seq=0 Win=512 Len=0
33812 479.967565505 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 2050 → 21 [SYN] Seq=0 Win=512 Len=0
33813 479.967637941 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 2051 → 21 [SYN] Seq=0 Win=512 Len=0
33814 479.967652288 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 2052 → 21 [SYN] Seq=0 Win=512 Len=0
33815 479.967723715 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 2053 → 21 [SYN] Seq=0 Win=512 Len=0
33816 479.967738091 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 2054 → 21 [SYN] Seq=0 Win=512 Len=0
33817 479.967835964 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 2055 → 21 [SYN] Seq=0 Win=512 Len=0
33818 479.967858519 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 2056 → 21 [SYN] Seq=0 Win=512 Len=0
33819 479.968817894 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 2057 → 21 [SYN] Seq=0 Win=512 Len=0
33820 479.968841260 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 2058 → 21 [SYN] Seq=0 Win=512 Len=0
33821 479.968968106 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 2059 → 21 [SYN] Seq=0 Win=512 Len=0
33822 479.968994121 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 2060 → 21 [SYN] Seq=0 Win=512 Len=0
33851 479.969391207 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 2061 → 21 [SYN] Seq=0 Win=512 Len=0
33852 479.969408953 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 2062 → 21 [SYN] Seq=0 Win=512 Len=0
33853 479.969496785 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 2063 → 21 [SYN] Seq=0 Win=512 Len=0
33854 479.969521153 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 2064 → 21 [SYN] Seq=0 Win=512 Len=0
33855 479.969597357 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 2065 → 21 [SYN] Seq=0 Win=512 Len=0
33856 479.969611610 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 2066 → 21 [SYN] Seq=0 Win=512 Len=0
33857 479.969685629 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 2067 → 21 [SYN] Seq=0 Win=512 Len=0
33858 479.969709081 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 2068 → 21 [SYN] Seq=0 Win=512 Len=0
33859 479.969884668 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 2069 → 21 [SYN] Seq=0 Win=512 Len=0
```



```
tcp.flags.ack == 0
No.     Time           Source          Destination     Protocol  Length  Info
 833592 502.005797085 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 38703 → 21 [SYN] Seq=0 Win=512 Len=0
 833593 502.005860462 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 38704 → 21 [SYN] Seq=0 Win=512 Len=0
 833594 502.005885199 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 38705 → 21 [SYN] Seq=0 Win=512 Len=0
 833595 502.005958131 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 38706 → 21 [SYN] Seq=0 Win=512 Len=0
 833596 502.005980890 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 38707 → 21 [SYN] Seq=0 Win=512 Len=0
 833597 502.006321505 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 38708 → 21 [SYN] Seq=0 Win=512 Len=0
 833606 502.006345882 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 38709 → 21 [SYN] Seq=0 Win=512 Len=0
 833608 502.006358197 77.235.113.10   192.168.30.130  TCP       60 38689 → 21 [RST] Seq=1 Win=32767 Len=0
 833609 502.006358306 77.235.113.10   192.168.30.130  TCP       60 38690 → 21 [RST] Seq=1 Win=32767 Len=0
 833610 502.006358414 77.235.113.10   192.168.30.130  TCP       60 38691 → 21 [RST] Seq=1 Win=32767 Len=0
 833614 502.006358832 77.235.113.10   192.168.30.130  TCP       60 38692 → 21 [RST] Seq=1 Win=32767 Len=0
 833619 502.006389819 77.235.113.10   192.168.30.130  TCP       60 38693 → 21 [RST] Seq=1 Win=32767 Len=0
 833620 502.006390014 77.235.113.10   192.168.30.130  TCP       60 38694 → 21 [RST] Seq=1 Win=32767 Len=0
 833621 502.006390119 77.235.113.10   192.168.30.130  TCP       60 38695 → 21 [RST] Seq=1 Win=32767 Len=0
 833622 502.006390216 77.235.113.10   192.168.30.130  TCP       60 38696 → 21 [RST] Seq=1 Win=32767 Len=0
 833623 502.006401993 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 38710 → 21 [SYN] Seq=0 Win=512 Len=0
 833624 502.006413267 77.235.113.10   192.168.30.130  TCP       60 38697 → 21 [RST] Seq=1 Win=32767 Len=0
 833625 502.006413393 77.235.113.10   192.168.30.130  TCP       60 38698 → 21 [RST] Seq=1 Win=32767 Len=0
 833626 502.006413501 77.235.113.10   192.168.30.130  TCP       60 38699 → 21 [RST] Seq=1 Win=32767 Len=0
 833627 502.006413613 77.235.113.10   192.168.30.130  TCP       60 38700 → 21 [RST] Seq=1 Win=32767 Len=0
 833628 502.006413732 77.235.113.10   192.168.30.130  TCP       60 38701 → 21 [RST] Seq=1 Win=32767 Len=0
 833629 502.006414004 77.235.113.10   192.168.30.130  TCP       60 38702 → 21 [RST] Seq=1 Win=32767 Len=0
 833630 502.006414198 77.235.113.10   192.168.30.130  TCP       60 38703 → 21 [RST] Seq=1 Win=32767 Len=0
 833631 502.006414310 77.235.113.10   192.168.30.130  TCP       60 38704 → 21 [RST] Seq=1 Win=32767 Len=0
 833632 502.006424200 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 38711 → 21 [SYN] Seq=0 Win=512 Len=0
 833633 502.006476960 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 38712 → 21 [SYN] Seq=0 Win=512 Len=0
 833634 502.006501347 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 38713 → 21 [SYN] Seq=0 Win=512 Len=0
 833635 502.006571897 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 38714 → 21 [SYN] Seq=0 Win=512 Len=0
 833636 502.006596858 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 38715 → 21 [SYN] Seq=0 Win=512 Len=0
 833637 502.006667652 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 38716 → 21 [SYN] Seq=0 Win=512 Len=0
 833638 502.006692108 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 38717 → 21 [SYN] Seq=0 Win=512 Len=0
 833639 502.006764060 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 38718 → 21 [SYN] Seq=0 Win=512 Len=0
 833640 502.006789951 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 38719 → 21 [SYN] Seq=0 Win=512 Len=0
 833641 502.006860834 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 38720 → 21 [SYN] Seq=0 Win=512 Len=0
 833642 502.006885137 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 38721 → 21 [SYN] Seq=0 Win=512 Len=0
 833643 502.006956156 77.235.113.10   192.168.30.130  TCP       54 [TCP Port numbers reused] 38722 → 21 [SYN] Seq=0 Win=512 Len=0
> Frame 833637: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
```

3.5 Source IP of the Attacker

The group identified the ip of the attacker by examining the source IP address of the malicious traffic involved in the DoS attack.Following the tcp stream we identified the ip to be **77.235.113.10**

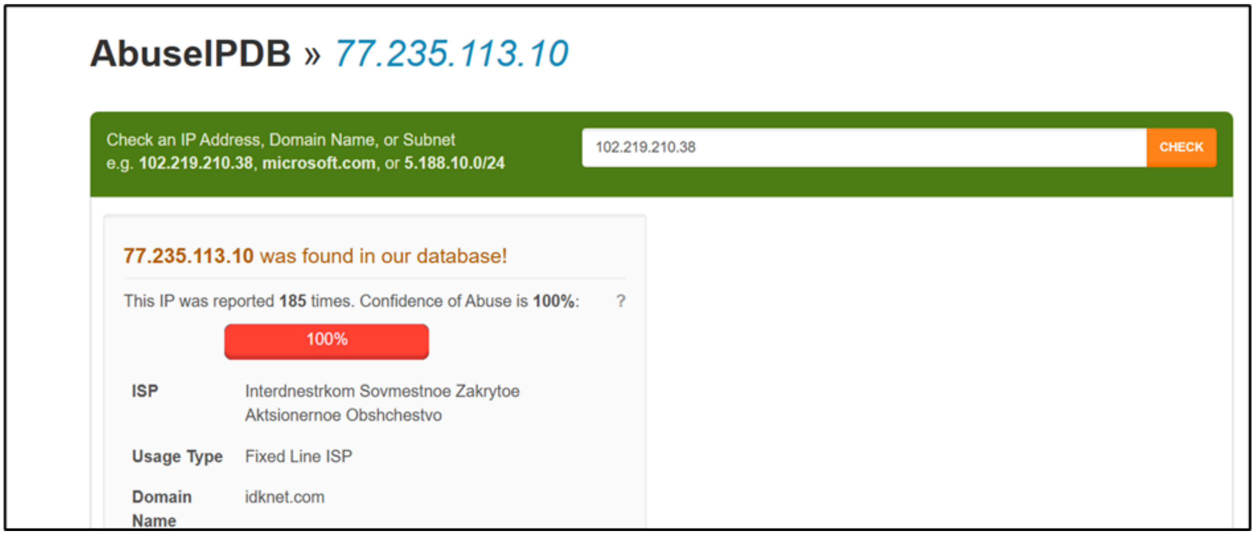

Files captured.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 299787
Wireshark · Packet 833558 · Files captured.pcapng

```
No.     Time
833498 502.003742
833549 502.005046
833558 502.005088
```

```
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x1c61 (7265)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x804f [validation disabled]
    [Header checksum status: Unverified]
    Source: 77.235.113.10
    Destination: 192.168.30.130
> Transmission Control Protocol, Src Port: 38673, Dst Port: 21, Seq: 1, Len: 0
```

```
0000  00 0c 29 ee fe 76 00 50  56 e8 84 f0 08 00 45 00   ··)··v·P V·····E·
0010  00 28 1c 61 00 00 80 06  80 4f 4d eb 71 0a c0 a8   ·(·a···· ·OM·q···
0020  1e 82 97 11 00 15 77 27  00 7b 00 00 00 00 50 04   ······w' ·{····P·
0030  7f ff 82 f8 00 00 00 00  00 00 00 00               ········ ····
```

Further analysis using **IPABUSE DB,** an ip blacklisting site used to report and find IP addresses that have been associated with malicious activity online.The IP **77.235.113.10** confidence of abuse is 100% having been reported 186 times.



AbuseIPDB » *77.235.113.10*

Check an IP Address, Domain Name, or Subnet
e.g. **102.219.210.38**, **microsoft.com**, or **5.188.10.0/24**

102.219.210.38

77.235.113.10 was found in our database!

This IP was reported **185** times. Confidence of Abuse is **100%**: ?

ISP	Interdnestrkom Sovmestnoe Zakrytoe Aktsionernoe Obshchestvo
Usage Type	Fixed Line ISP
Domain Name	idknet.com

3.6 Country of the Attacker

The group used MaxMind GeoLite2 database for geolocation in wireshark and VirusTotal, an online service that analyzes suspicious files, domains, IPs and URLs to detect malware and other breaches, and automatically share them with the security community.

Setting up Maxmind GeoIP

To use Maxmind Geoip databases in Wireshark we performed the following steps.

1.Download the MaxMind GeoIP Database

We created accounts on Maxmind and signed up for a free account to download the GeoLite2 database.
We downloaded the **GeoLite2 Country,**,**GeoLite2 City** and **GeoLite2 ASN** (Autonomous System Number) databases in `.mmdb` format.

2. Extract the Database Files

- After downloading the `.tar.gz` file for each database, we extracted it using an extraction tool to a preferred directory

3. Configure Wireshark to Use the GeoIP Database

- Open **Wireshark**.
- Go to **Edit** > **Preferences**.

4. Set GeoIP Database Paths

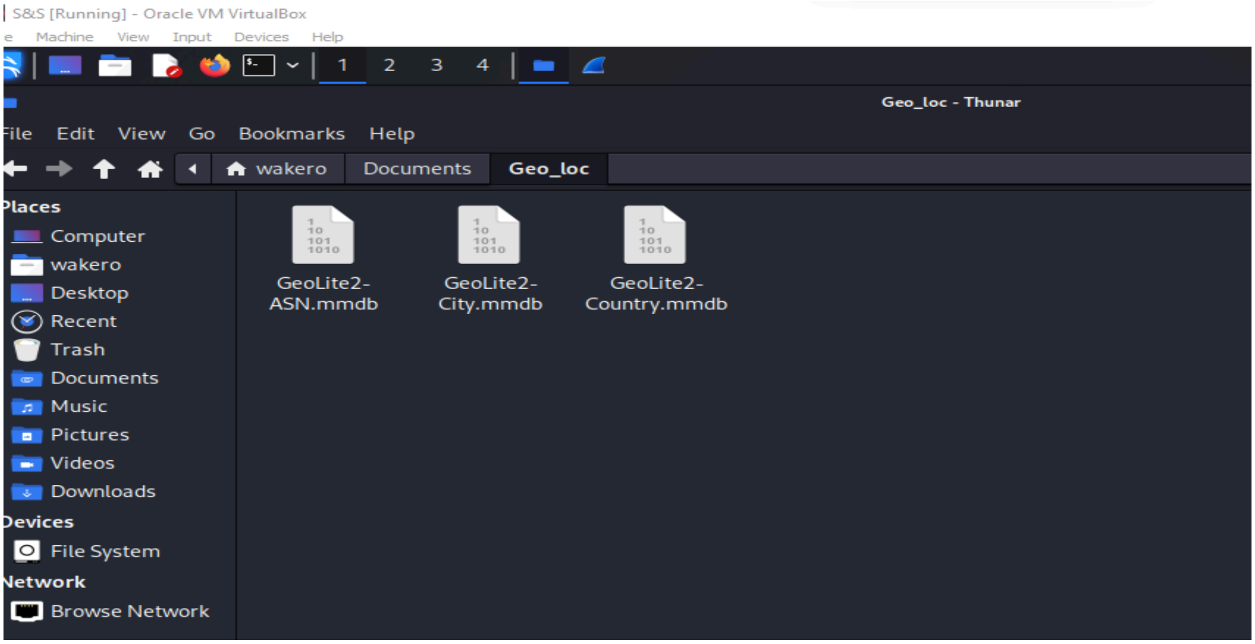
- In the Preferences window, expand the **Name Resolution** section from the left-side menu.
- Click on **GeoIP database directories**.
- Add the path to the folder where the extracted `.mmdb` files are located.

5. Enable Name Resolution

- Still within the **Preferences** window, ensure the following options are enabled under **Name Resolution**:
  - **Resolve IP addresses** (this will enable Wireshark to use the GeoIP database to resolve IPs to locations).
  - **Use GeoIP Lookup** -this is necessary to display geographic data.

6. Restart Wireshark

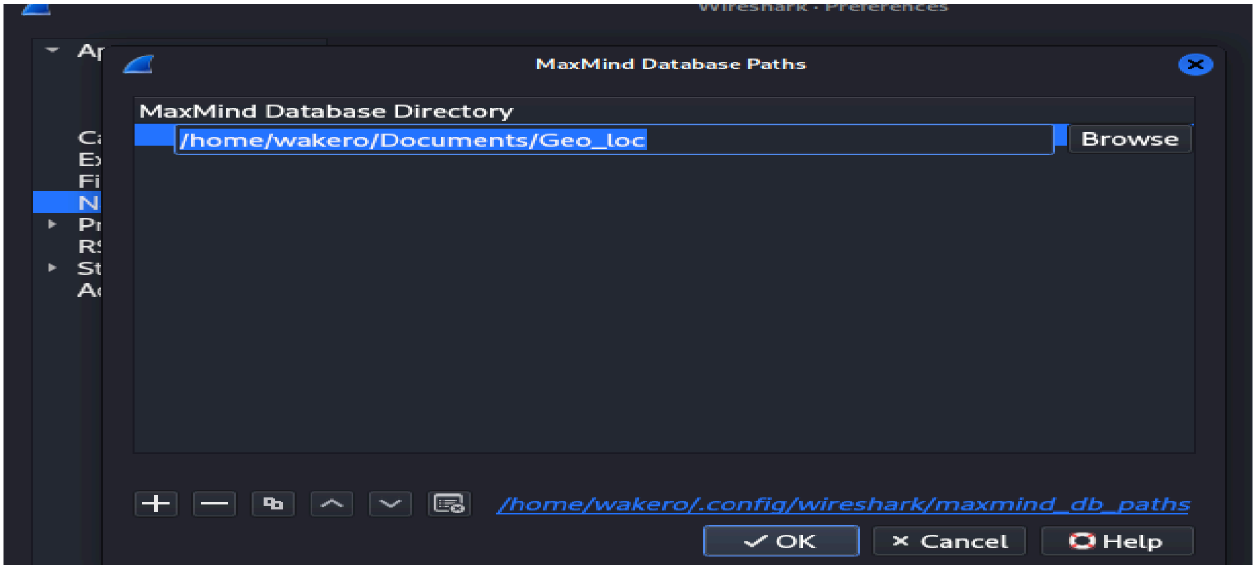
- After configuring the database paths and enabling IP resolution, restart Wireshark to
- Apply the changes.



GeoLite2-ASN.mmdb

GeoLite2-City.mmdb

GeoLite2-Country.mmdb

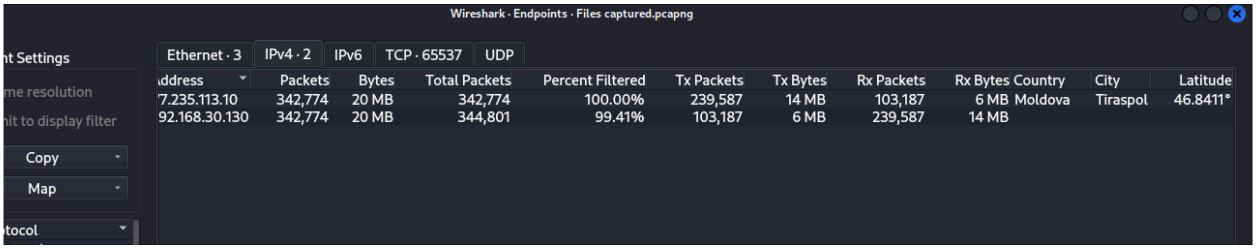


MaxMind Database Directory

/home/wakero/Documents/Geo_loc

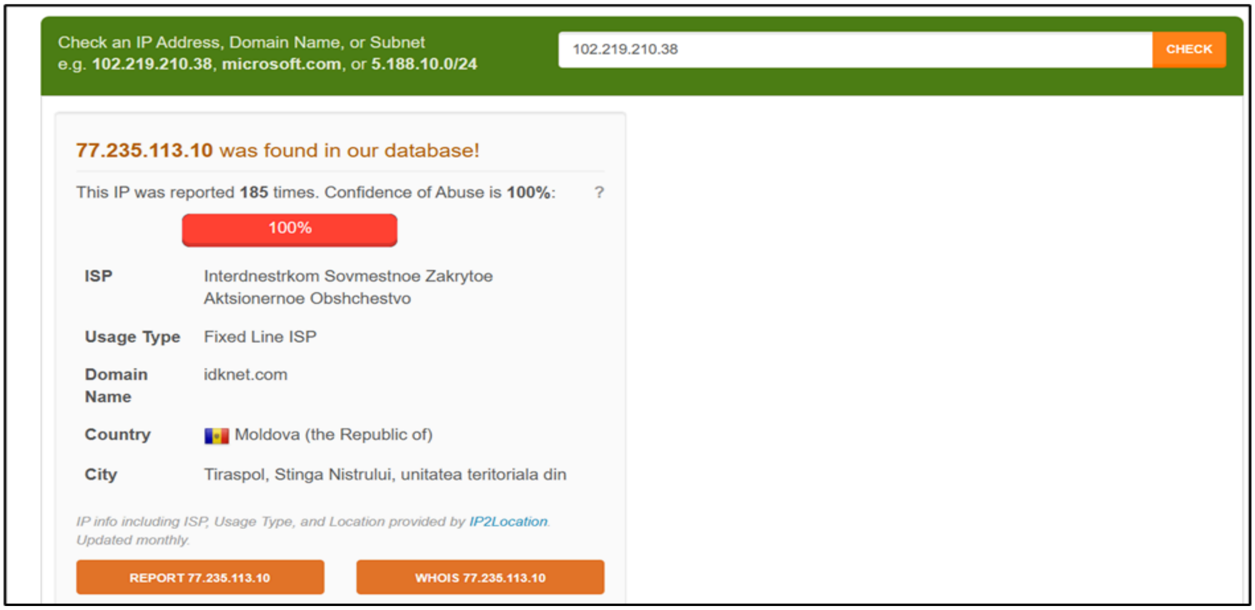
/home/wakero/.config/wireshark/maxmind_db_paths

The attacker's IP address **77.235.113.10** country of origin resolves to Moldova



ddress	Packets	Bytes	Total Packets	Percent Filtered	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude
7.235.113.10	342,774	20 MB	342,774	100.00%	239,587	14 MB	103,187	6 MB	Moldova	Tiraspol	46.8411°
92.168.30.130	342,774	20 MB	344,801	99.41%	103,187	6 MB	239,587	14 MB			

Using **VirusTotal** Whois lookup feature and **AbuseIPDB** the country still resolves to Moldova..



Check an IP Address, Domain Name, or Subnet
e.g. **102.219.210.38**, **microsoft.com**, or **5.188.10.0/24**

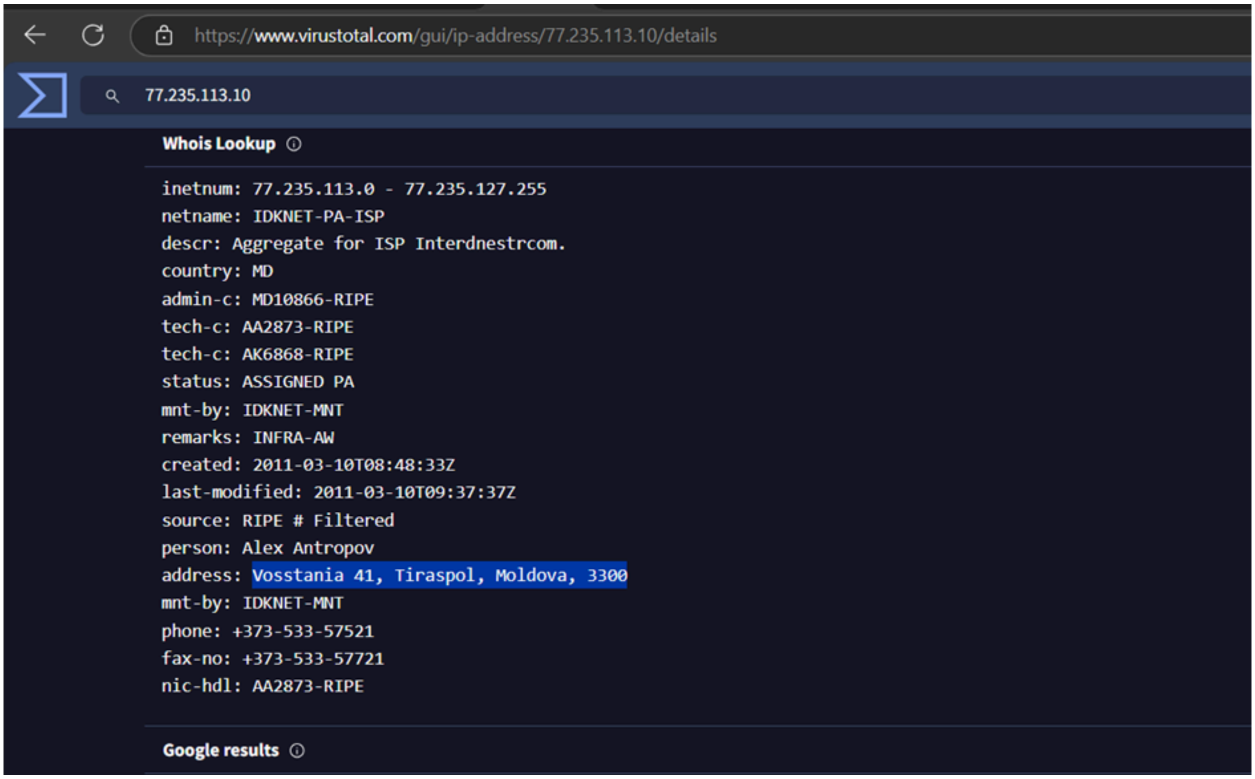
102.219.210.38

77.235.113.10 was found in our database!

This IP was reported **185** times. Confidence of Abuse is **100%**: ?

ISP	Interdnestrkom Sovmestnoe Zakrytoe Aktsionernoe Obshchestvo
Usage Type	Fixed Line ISP
Domain Name	idknet.com
Country	Moldova (the Republic of)
City	Tiraspol, Stinga Nistrului, unitatea teritoriala din

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.



https://www.virustotal.com/gui/ip-address/77.235.113.10/details

77.235.113.10

Whois Lookup

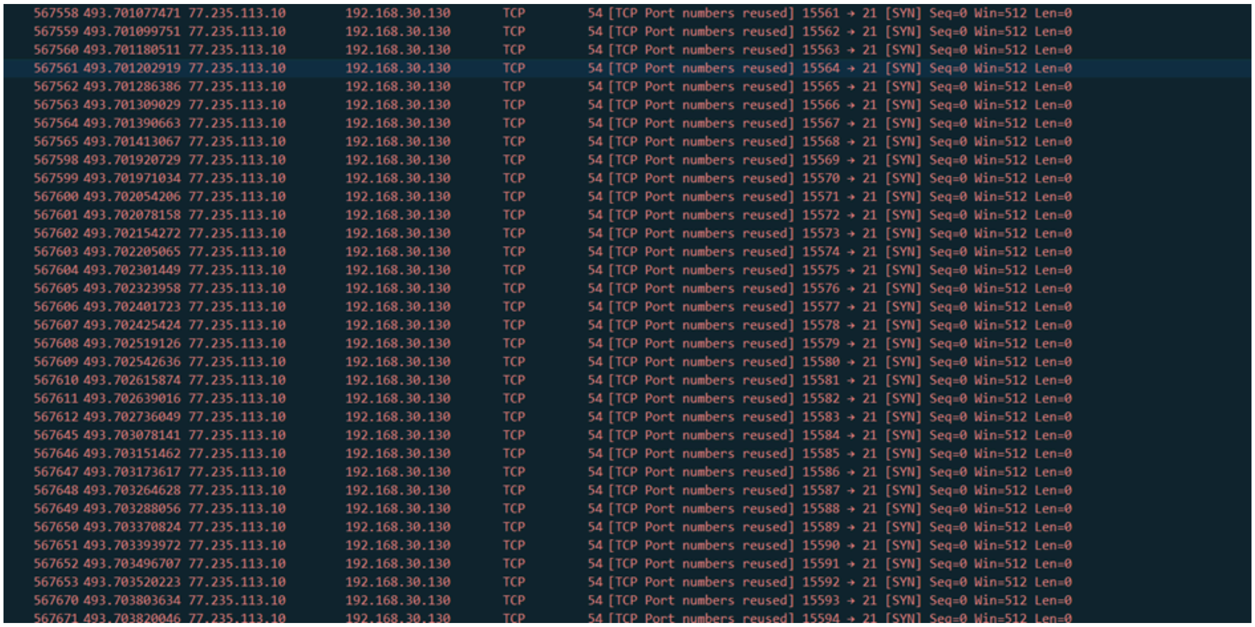
```
inetnum: 77.235.113.0 - 77.235.127.255
netname: IDKNET-PA-ISP
descr: Aggregate for ISP Interdnestrcom.
country: MD
admin-c: MD10866-RIPE
tech-c: AA2873-RIPE
tech-c: AK6868-RIPE
status: ASSIGNED PA
mnt-by: IDKNET-MNT
remarks: INFRA-AW
created: 2011-03-10T08:48:33Z
last-modified: 2011-03-10T09:37:37Z
source: RIPE # Filtered
person: Alex Antropov
address: Vosstania 41, Tiraspol, Moldova, 3300
mnt-by: IDKNET-MNT
phone: +373-533-57521
fax-no: +373-533-57721
nic-hdl: AA2873-RIPE
```

Google results

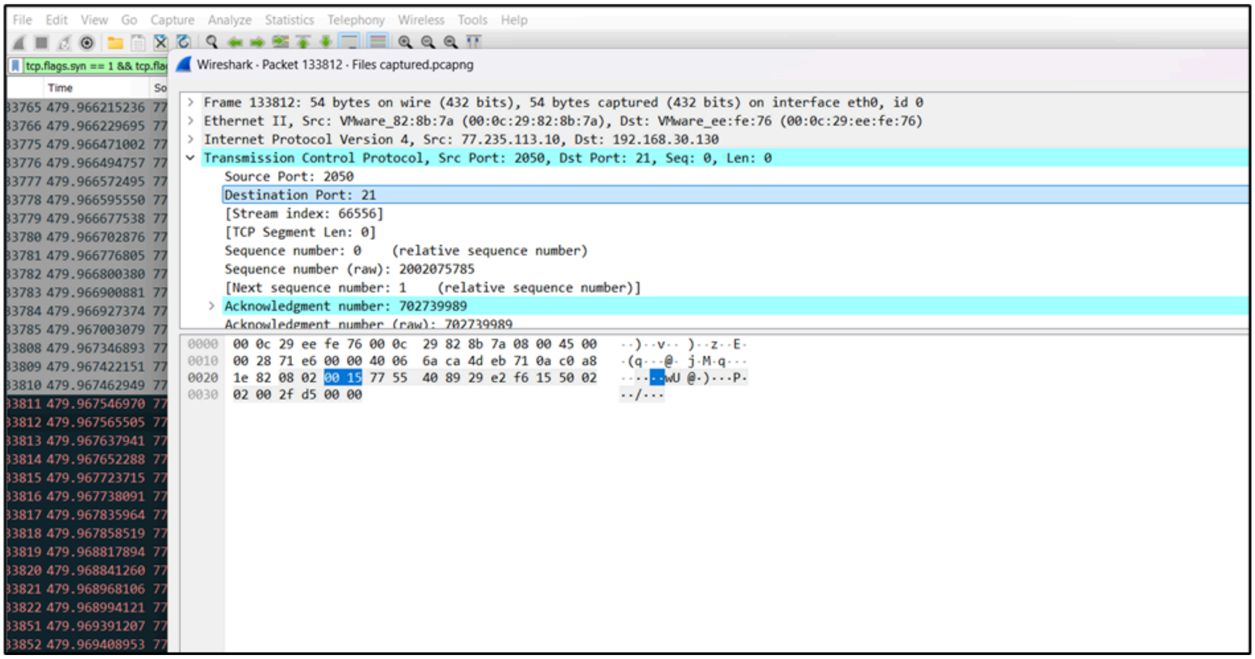
3.7 Service denied to users

After identifying the type of attack to be a denial of service: SYN Flood attack. The group checked for disrupted services by analyzing **port 21** which was target by the attack.The group identified the service being denied to the users to be :

Files Transfer - series of these SYN packets from the same source IP (77.235.113.10) in a short time frame, especially without receiving **SYN-ACK** responses from the server, strongly suggests a SYN flood attack targeting the FTP service on port 21.



```
567558 493.701077471 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15561 → 21 [SYN] Seq=0 Win=512 Len=0
567559 493.701099751 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15562 → 21 [SYN] Seq=0 Win=512 Len=0
567560 493.701180511 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15563 → 21 [SYN] Seq=0 Win=512 Len=0
567561 493.701202919 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15564 → 21 [SYN] Seq=0 Win=512 Len=0
567562 493.701286386 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15565 → 21 [SYN] Seq=0 Win=512 Len=0
567563 493.701309029 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15566 → 21 [SYN] Seq=0 Win=512 Len=0
567564 493.701390663 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15567 → 21 [SYN] Seq=0 Win=512 Len=0
567565 493.701413067 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15568 → 21 [SYN] Seq=0 Win=512 Len=0
567598 493.701920729 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15569 → 21 [SYN] Seq=0 Win=512 Len=0
567599 493.701971034 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15570 → 21 [SYN] Seq=0 Win=512 Len=0
567600 493.702054206 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15571 → 21 [SYN] Seq=0 Win=512 Len=0
567601 493.702078158 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15572 → 21 [SYN] Seq=0 Win=512 Len=0
567602 493.702154272 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15573 → 21 [SYN] Seq=0 Win=512 Len=0
567603 493.702205065 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15574 → 21 [SYN] Seq=0 Win=512 Len=0
567604 493.702301449 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15575 → 21 [SYN] Seq=0 Win=512 Len=0
567605 493.702323958 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15576 → 21 [SYN] Seq=0 Win=512 Len=0
567606 493.702401723 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15577 → 21 [SYN] Seq=0 Win=512 Len=0
567607 493.702425424 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15578 → 21 [SYN] Seq=0 Win=512 Len=0
567608 493.702519126 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15579 → 21 [SYN] Seq=0 Win=512 Len=0
567609 493.702542636 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15580 → 21 [SYN] Seq=0 Win=512 Len=0
567610 493.702615874 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15581 → 21 [SYN] Seq=0 Win=512 Len=0
567611 493.702639016 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15582 → 21 [SYN] Seq=0 Win=512 Len=0
567612 493.702736049 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15583 → 21 [SYN] Seq=0 Win=512 Len=0
567645 493.703078141 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15584 → 21 [SYN] Seq=0 Win=512 Len=0
567646 493.703151462 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15585 → 21 [SYN] Seq=0 Win=512 Len=0
567647 493.703173617 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15586 → 21 [SYN] Seq=0 Win=512 Len=0
567648 493.703264628 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15587 → 21 [SYN] Seq=0 Win=512 Len=0
567649 493.703288056 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15588 → 21 [SYN] Seq=0 Win=512 Len=0
567650 493.703370824 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15589 → 21 [SYN] Seq=0 Win=512 Len=0
567651 493.703393972 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15590 → 21 [SYN] Seq=0 Win=512 Len=0
567652 493.703496707 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15591 → 21 [SYN] Seq=0 Win=512 Len=0
567653 493.703520223 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15592 → 21 [SYN] Seq=0 Win=512 Len=0
567670 493.703803634 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15593 → 21 [SYN] Seq=0 Win=512 Len=0
567671 493.703820046 77.235.113.10     192.168.30.130    TCP      54 [TCP Port numbers reused] 15594 → 21 [SYN] Seq=0 Win=512 Len=0
```



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.syn == 1 && tcp.flag

Wireshark · Packet 133812 · Files captured.pcapng

```
Time              So
33765 479.966215236 77
33766 479.966229695 77
33775 479.966471002 77
33776 479.966494757 77
33777 479.966572495 77
33778 479.966595550 77
33779 479.966677538 77
33780 479.966702876 77
33781 479.966776805 77
33782 479.966800380 77
33783 479.966900881 77
33784 479.966927374 77
33785 479.967003079 77
33808 479.967346893 77
33809 479.967422151 77
33810 479.967462949 77
33811 479.967546970 77
33812 479.967565505 77
33813 479.967637941 77
33814 479.967652288 77
33815 479.967723715 77
33816 479.967738091 77
33817 479.967835964 77
33818 479.967858519 77
33819 479.968817894 77
33820 479.968841260 77
33821 479.968968106 77
33822 479.968994121 77
33851 479.969391207 77
33852 479.969408953 77
```

```
> Frame 133812: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
> Ethernet II, Src: VMware_82:8b:7a (00:0c:29:82:8b:7a), Dst: VMware_ee:fe:76 (00:0c:29:ee:fe:76)
> Internet Protocol Version 4, Src: 77.235.113.10, Dst: 192.168.30.130
v Transmission Control Protocol, Src Port: 2050, Dst Port: 21, Seq: 0, Len: 0
    Source Port: 2050
    Destination Port: 21
    [Stream index: 66556]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
    Sequence number (raw): 2002075785
    [Next sequence number: 1    (relative sequence number)]
  > Acknowledgment number: 702739989
    Acknowledgment number (raw): 702739989

0000  00 0c 29 ee fe 76 00 0c  29 82 8b 7a 08 00 45 00   ··)··v·· )··z··E·
0010  00 28 71 e6 00 00 40 06  6a ca 4d eb 71 0a c0 a8   ·(q···@· j·M·q···
0020  1e 82 08 02 00 15 77 55  40 89 29 e2 f6 15 50 02   ······wU @·)···P·
0030  02 00 2f d5 00 00                                  ··/···
```

Conclusion

In this assignment, we successfully utilized Wireshark to analyze network traffic and investigate a potential security incident on a company web server. Our detailed analysis of the provided pcap file revealed several critical aspects of the attack:

1. Compromised Credentials: We identified the victim’s username and password through the use of HTTP POST request analysis.
2. Server Identification: The server involved in the incident was identified as nginx/1.19.0.
3. Attack Method: The attacker employed a Denial of Service (DoS) attack using SYN Flood, overwhelming the server with numerous SYN packets.
4. Attacker’s IP Address: The source IP of the attacker was determined to be 77.235.113.10, confirmed to be associated with malicious activity.
5. Geolocation: The attacker’s location was traced using the MaxMind GeoLite2 database and VirusTotal.

Recommendations

To prevent similar incidents in the future, we recommend the following measures:

1. Enhanced Security Protocols: Implement stronger authentication mechanisms, such as multi-factor authentication (MFA), to protect user credentials.
2. Regular Monitoring: Continuously monitor network traffic for unusual patterns and potential threats using tools like Wireshark.
3. Firewall and IDS/IPS: Deploy and configure firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) to detect and mitigate DoS attacks.
4. Employee Training: Educate employees on cybersecurity best practices to reduce the risk of credential theft and other social engineering attacks.
5. Regular Updates: Keep all software, including web servers, up to date with the latest security patches to minimize vulnerabilities.

By implementing these recommendations, the organization can enhance its security posture and better protect against future attacks. This assignment has provided valuable insights into the importance of network traffic analysis and the role it plays in maintaining cybersecurity.