FINAL PROJECT CAPESTONE PROJECT

Submitted by: Navneet Kaur

Executive Summary:

Premium Lights Inc., an Ontario based lighting solution provider, recently experienced a significant cybersecurity incident in February 2022. The company fell victim to SYN Flood distributed denial-of-services DDOS attack, which severely impacted their network infrastructure and disrupted critical business operations and defamed the company's name for customer database and financial loss. This incident led to a significant loss of customer trust, financial resources, and the compromise of the organization's confidentiality, integrity, and availability. This attack methodology inundated the company's network infrastructure with an overwhelming volume of SYN packets, rendering critical systems unresponsive and causing significant disruption to their operations.

Upon immediate detection of the attack, Premium Lights Inc. activated their incident response plan. The company's dedicated incident response team, in collaboration with cybersecurity experts, swiftly enacted a series of measures to mitigate the attack and restore operational stability.

Incident Timeline:

a) Date of notification to the chief information security officer or department Information Security Representative(ISAC member) : **Feb 21st 2022 Monday at 10:00 AM UTC Received an email**

```
From: 4C484C@qq.com
To: support@premiumhouselights.com

Hello,

We will go right to the point. We are in possession of your database files, which include sensitive informatio

You wouldn't want this information to be out on the internet, would you? We will release this information on ht

              1JQqFLmAp5DQJbdD3ThgEiJGSmX8eaaBid

by Monday at 10:00AM UTC.

To demonstrate to you that we aren't just playing games, here is a snippet of your customer database table:

+------------------+-----------------+-------------+
| contactFirstName | contactLastName | phone       |
+------------------+-----------------+-------------+
| Carine           | Schmitt         | 40.32.2555  |
| Jean             | King            | 7025551838  |
| Peter            | Ferguson        | 03 9520 4555 |
| Janine           | Labrune         | 40.67.8555  |
| Jonas            | Bergulfsen      | 07-98 9555  |
+------------------+-----------------+-------------+

Now the ball is in your court to make the right decision and take action. There will be no negotiations on the

// The 4C484C Group
```

b) Date of incident occurred: **19-02-2022 at 21:57:39:244026**

c) Date of incident discovered: **19-02-2022 at 21:58:40:125288**

d) Incident location: **/var/www/html/uploads**

e) Was storage device encrypted? **NO**

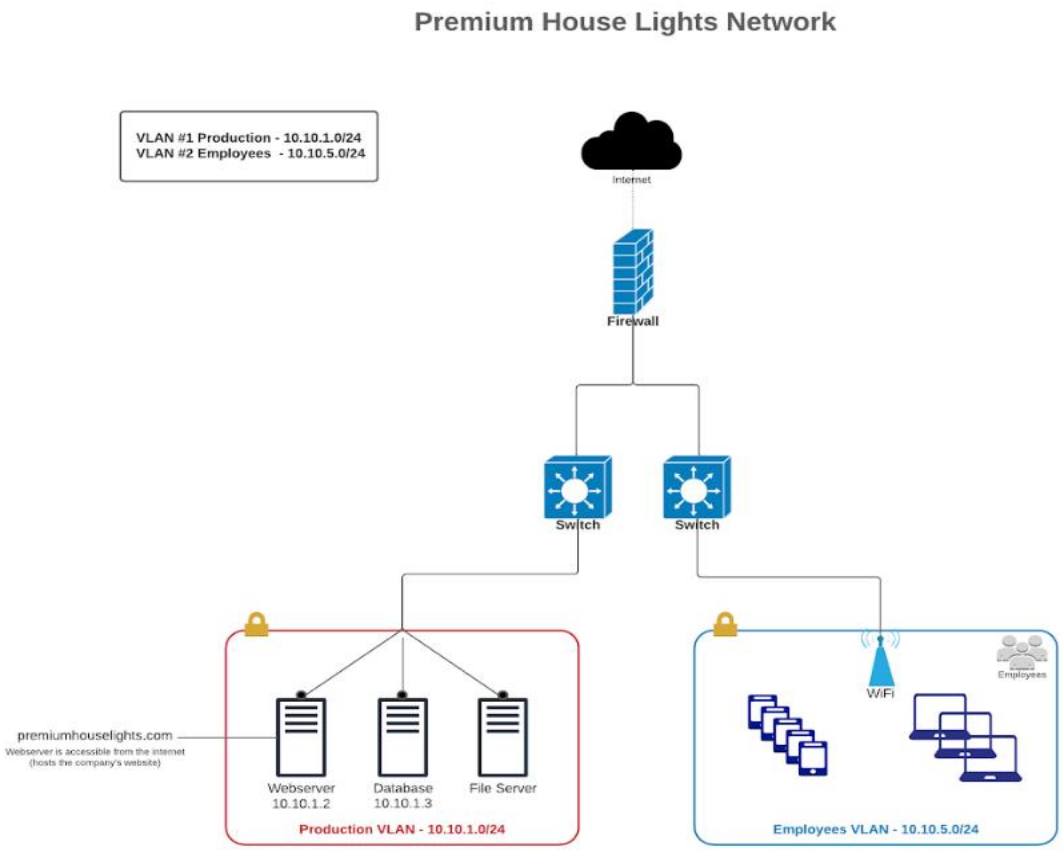
Because no password on database, default password on webserver and no encryption method used by company to encrypt the database.

(NOTE: Evidences are shown further in this report)

Technical analysis:

As a cyber security analyst, I'll analyze it in following steps:

- **Network topology analysis:**
  This is the network topology of Premium House Lights Inc.



Full scale mapping:

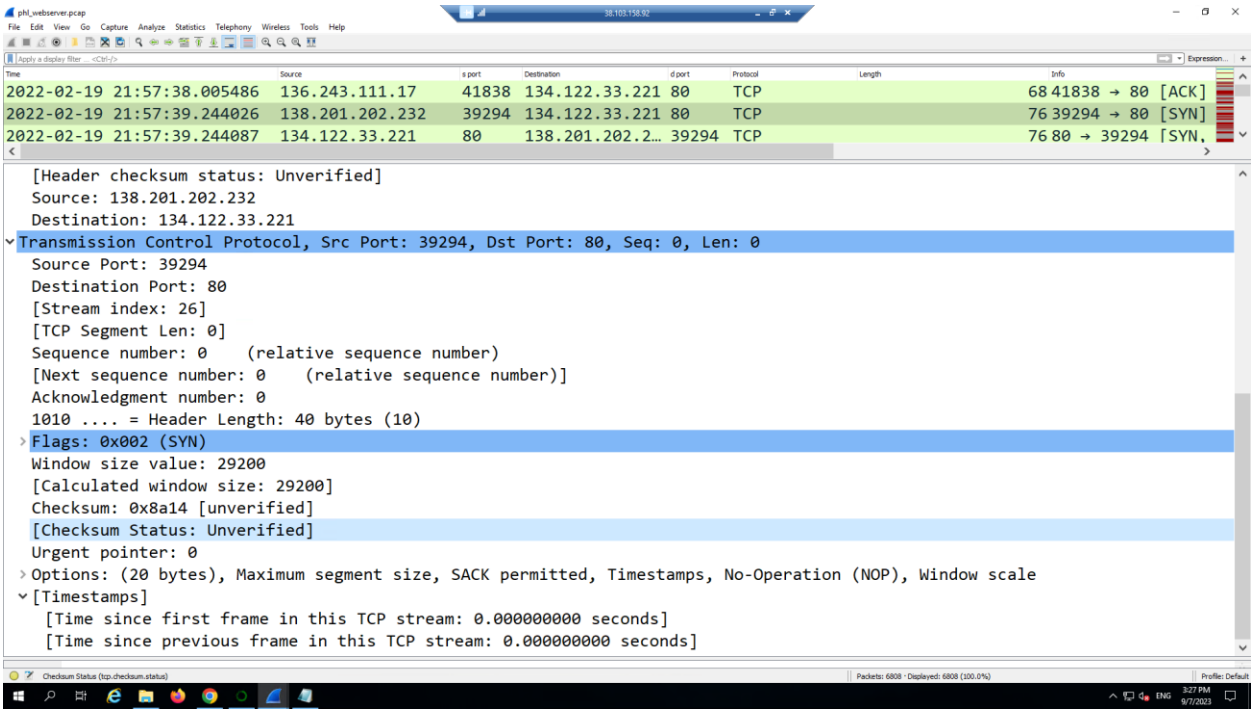
Endpoint	Current profile	Target profile	Security required	Security measures
Website	Basic security	Robust security	Protection against data breaches, DDOSs attacks, SQL injection attacks	-Web application firewall (WAF) to filter incoming traffic for malicious content -regular security patches and updates for website platform

Employee devices	Basic security, Single WIFI connectivity	Strengthened security	Protection against malware, unauthorized access and data leakage, secure WIFI	-updated and regularly patched Operating Systems and applications on all devices -Provide Guest network for BYOD(bring your own devices like mobile devices) in the network and separate very strong password with MFA security measures on employee laptops
Network infrastructure	Basic security	Improved security measures	Protection against unauthorized access and network attacks	-implementation of strong access controls with role based permission, -Least privileged access rule -zero trust rule Regular updates for routers, switches and firewalls Implementation of Intrusion detection system and Intrusion prevention system(IDS/IPS) to monitor network traffic -Network segmentation i.e there should be separate VLANs for file server, database and webserver and for employee devices.
Webserver, File server	Basic security	Strong security measures	Protection against sever breaches and data theft	-regular security patches and updates for sever OS and applications -proper configuration management and hardening guidelines -regular vulnerability scanning and assessment -implementation of MFA for servers access
Database	Basic security	Strong security measures	Protection of sensitive customer data from breaches and unauthorized access	-Strong encryption of stored customer data both at rest and in transit -Regular security audits and vulnerability assessments of the database -implementation of access controls bases on the principle of least privilege access -Regular monitoring of

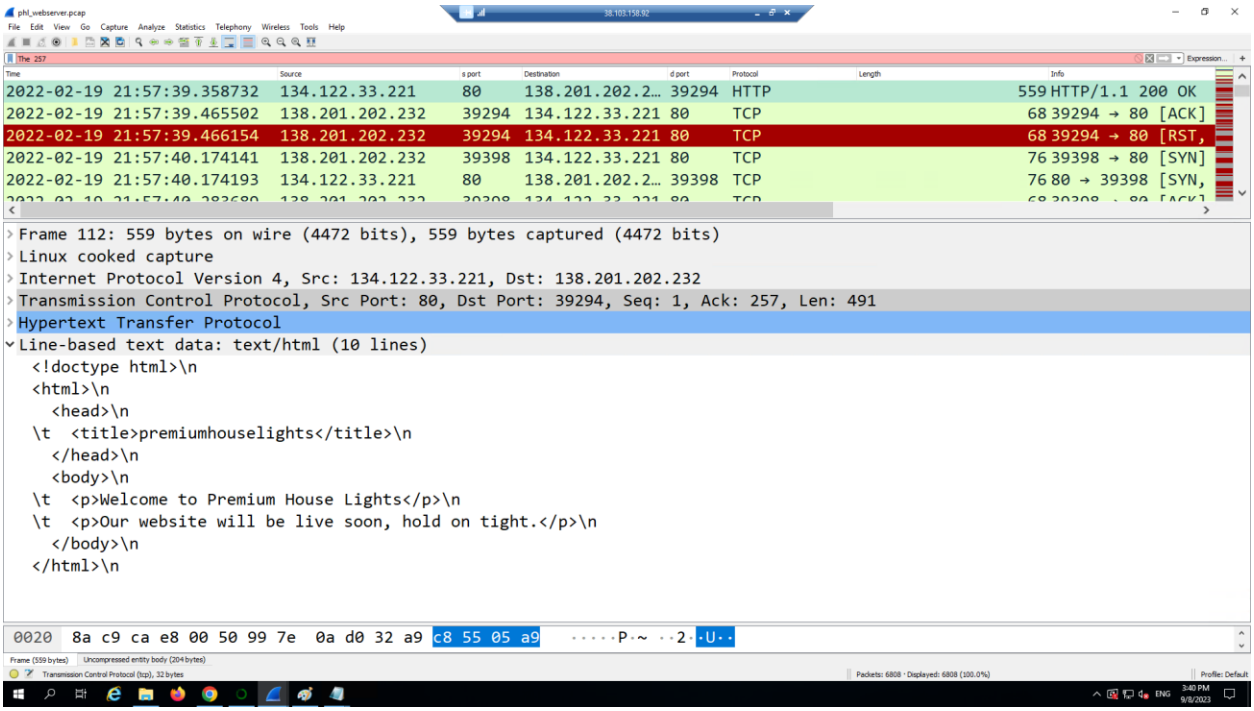
				database activity and access logs.

Attack origin and impact (with related evidence):

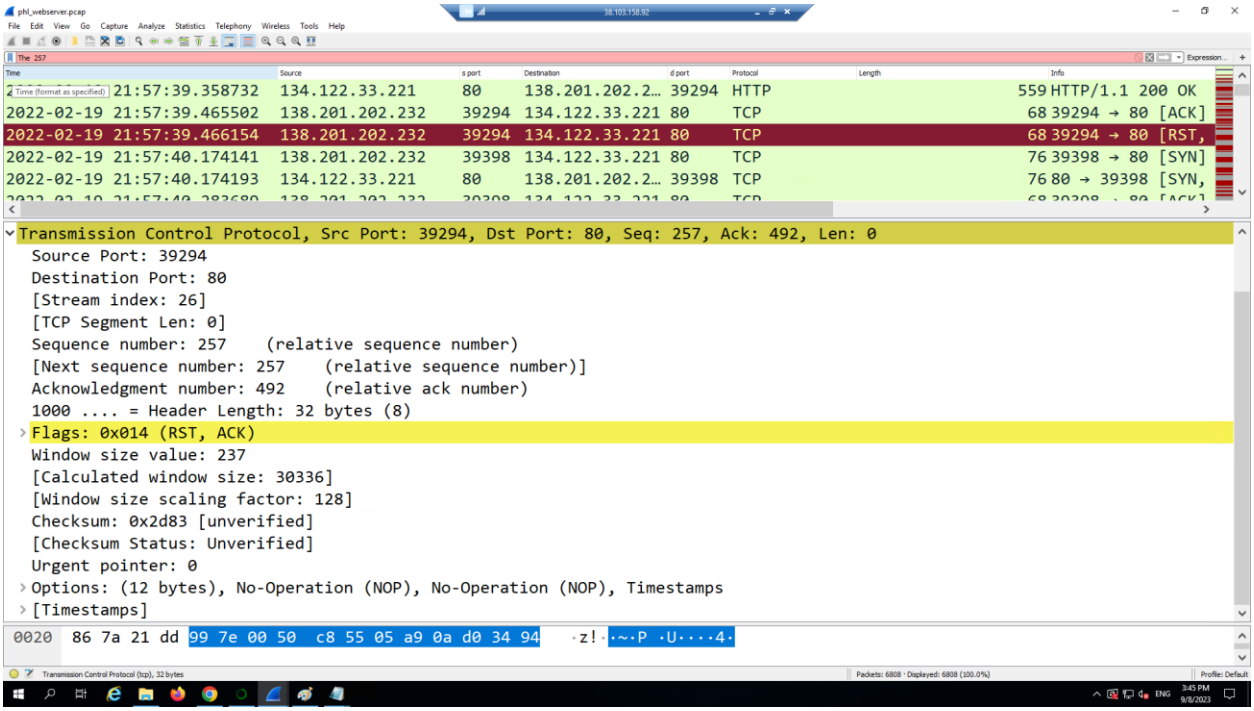
The very first time on 19-02-2022 at 21:57:39.244026 an unknown IP address 138.201.202.232 with port number 39294 was trying to make a connection with webserver IP address 134.122.33.221 at port 80 i.e. HTTP with 3 way handshaking method.

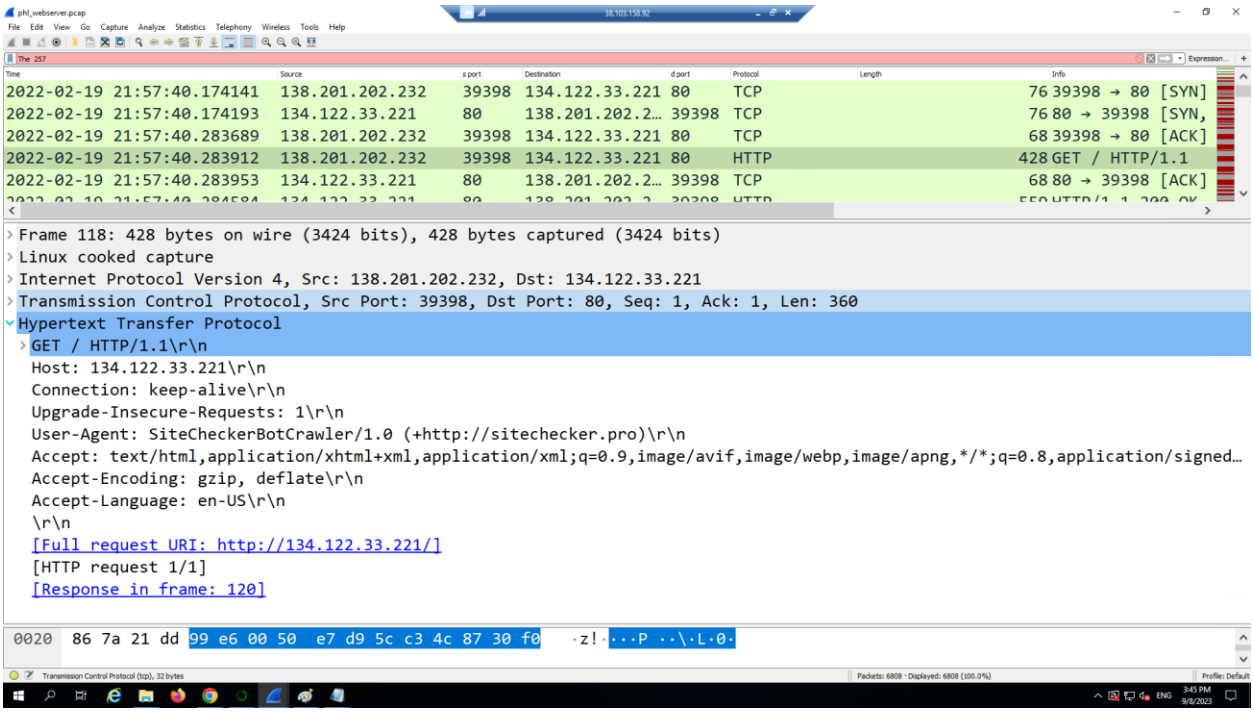


After that webserver 134.122.33.221 acknowledged it and then attacker 138.201.202.232 send a GET request to webserver 134.122.33.221 and webserver send a message with Premium lights Inc, page to attacker saying your request was successful and returning the requested data to source in this case source is attacker IP address 138.201.202.232.

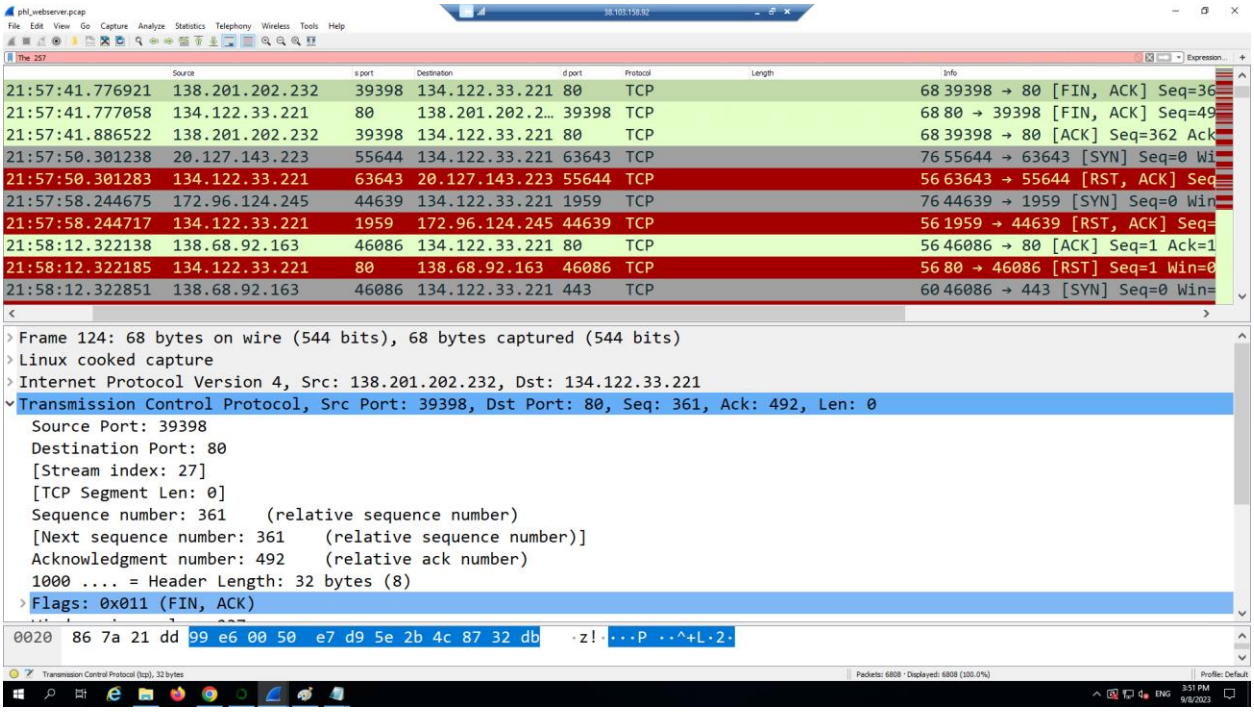


After that attacker IP 138.201.202.232 terminate the established connection abruptly and trying to make another connection using different port number 39398.

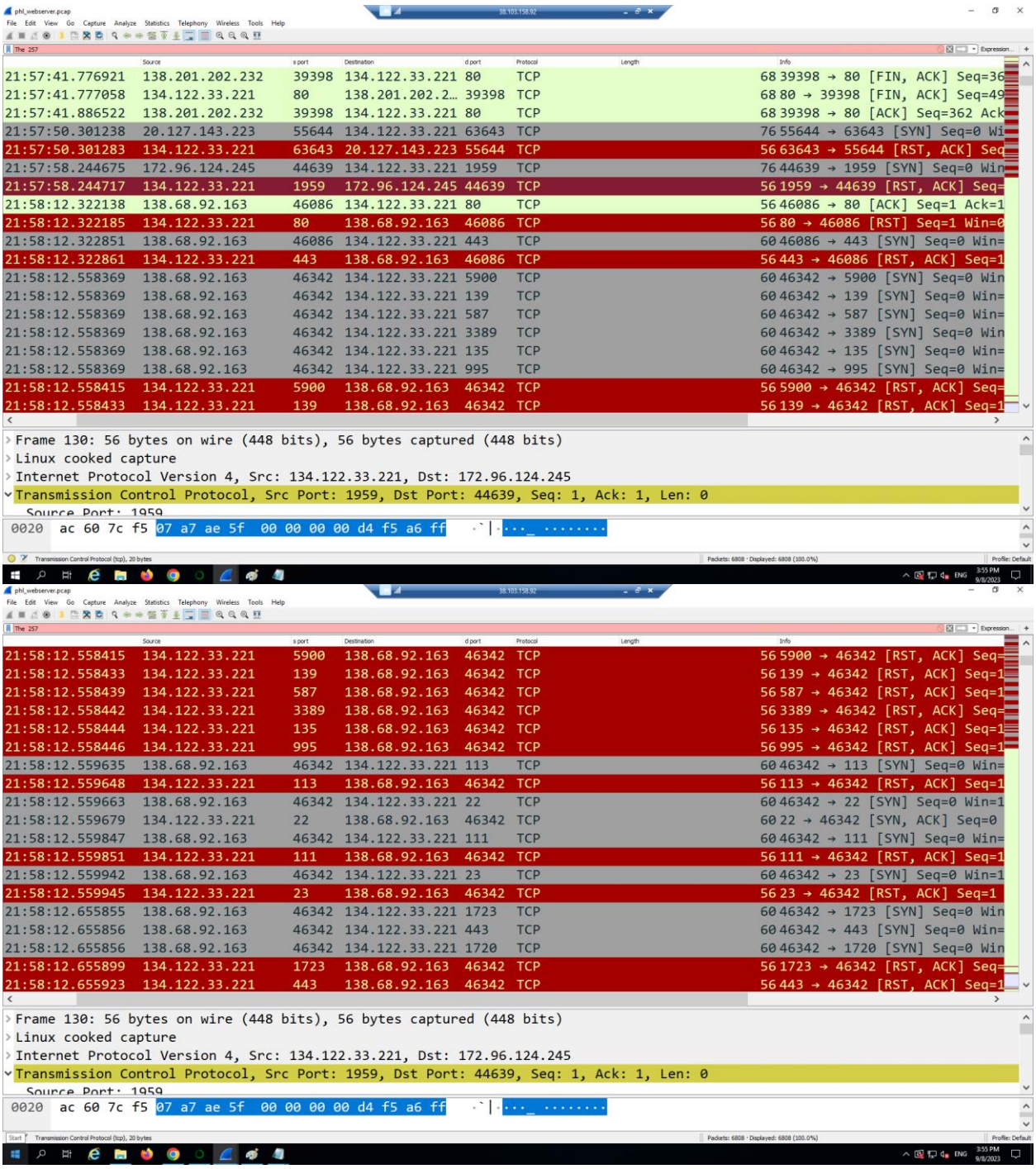




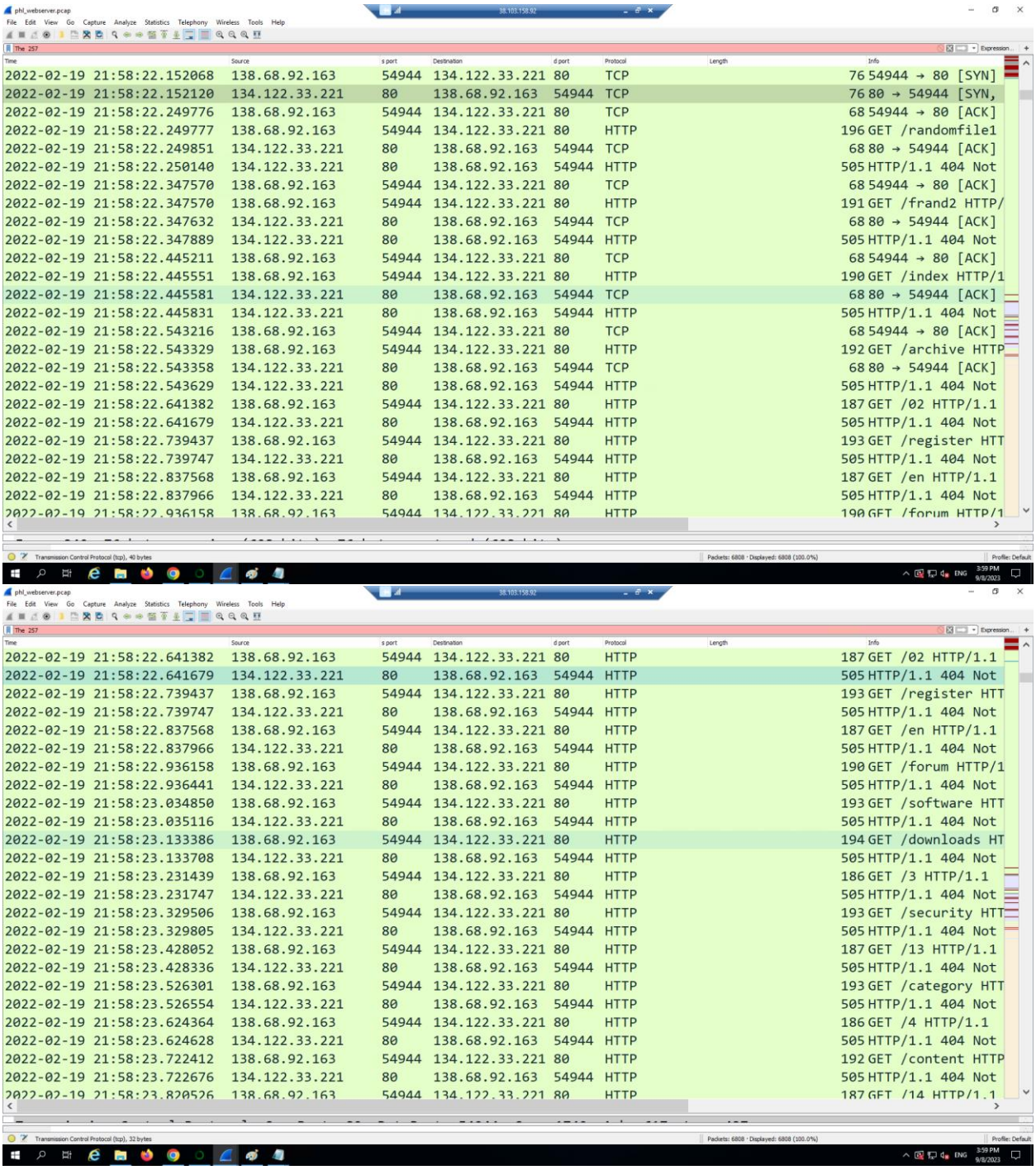
Again, Ip address 138.201.202.232 requested with intention to close the connection with webserver 134.122.33.221



This way attacker IP address 138.201.202.232 trying to make multiple connection with different port number and webserver 134.122.33.221 is terminating the connection again and again as firewall is not letting the attacker into the system, however attacker keep send the SYN request to webserver which crashed the webserver with DOS attack with SYN flood attack. In the given below captures we can see that multiple attempts by attacker and denied by webserver.



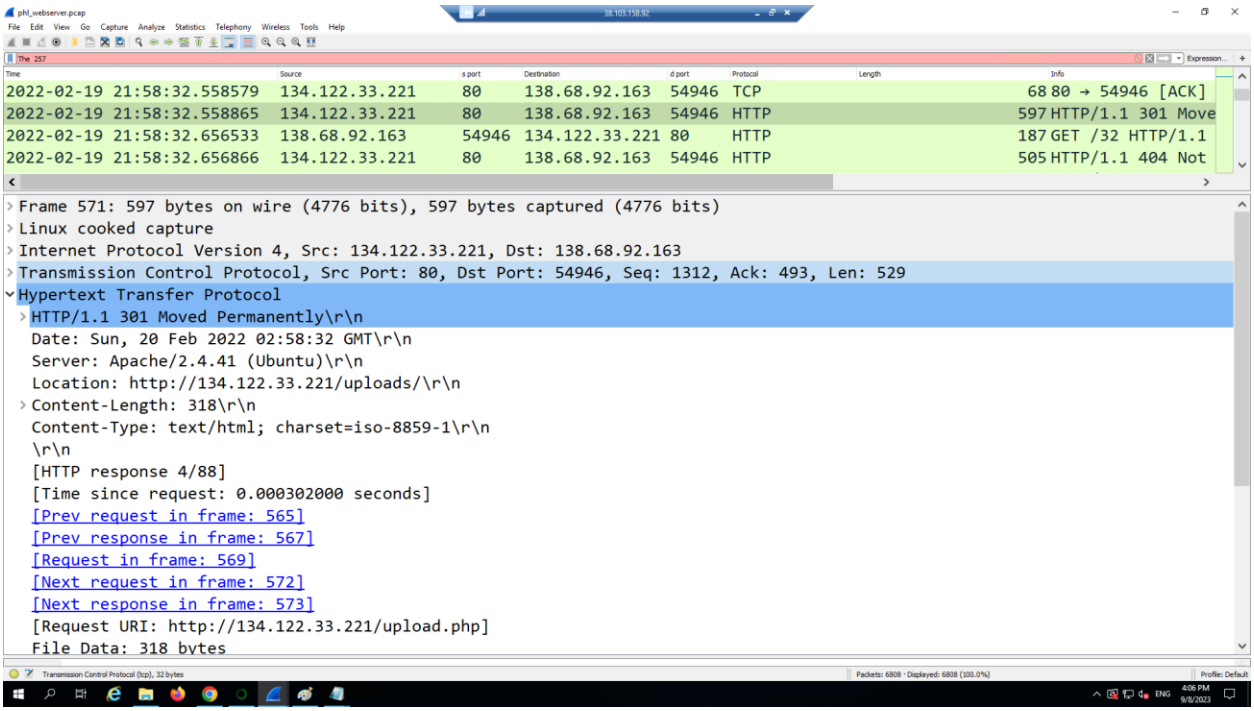
After this Attacker 138.68.92.163 with new port number 54944 trying to gain access of webserver by trying to make a connection with random file names in webserver multiple time and webserver keep replying that file not found until the system crashed with flood of SYN request. We can see this in the screenshot:



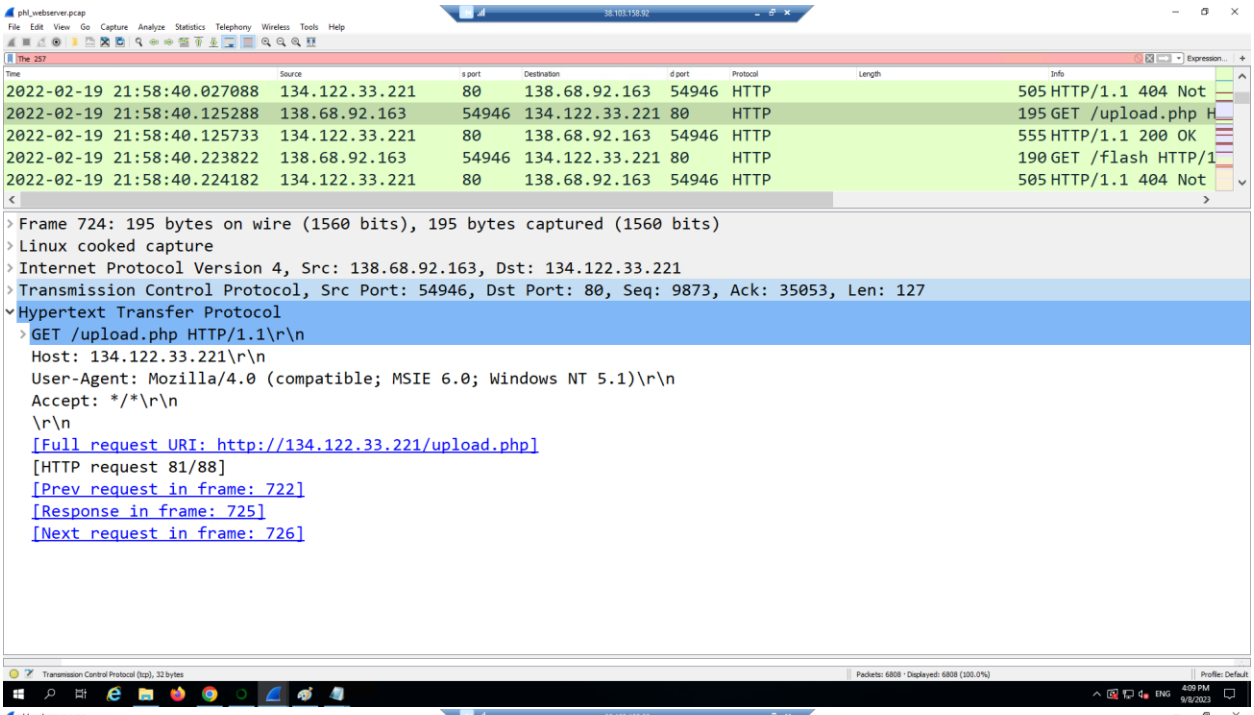
Time	Source	s port	Destination	d port	Protocol	Length	Info
2022-02-19 21:58:22.152068	138.68.92.163	54944	134.122.33.221	80	TCP	76	54944 → 80 [SYN]
2022-02-19 21:58:22.152120	134.122.33.221	80	138.68.92.163	54944	TCP	76	80 → 54944 [SYN,
2022-02-19 21:58:22.249776	138.68.92.163	54944	134.122.33.221	80	TCP	68	54944 → 80 [ACK]
2022-02-19 21:58:22.249777	138.68.92.163	54944	134.122.33.221	80	HTTP	196	GET /randomfile1
2022-02-19 21:58:22.249851	134.122.33.221	80	138.68.92.163	54944	TCP	68	80 → 54944 [ACK]
2022-02-19 21:58:22.250140	134.122.33.221	80	138.68.92.163	54944	HTTP	505	HTTP/1.1 404 Not
2022-02-19 21:58:22.347570	138.68.92.163	54944	134.122.33.221	80	TCP	68	54944 → 80 [ACK]
2022-02-19 21:58:22.347570	138.68.92.163	54944	134.122.33.221	80	HTTP	191	GET /frand2 HTTP/
2022-02-19 21:58:22.347632	134.122.33.221	80	138.68.92.163	54944	TCP	68	80 → 54944 [ACK]
2022-02-19 21:58:22.347889	134.122.33.221	80	138.68.92.163	54944	HTTP	505	HTTP/1.1 404 Not
2022-02-19 21:58:22.445211	138.68.92.163	54944	134.122.33.221	80	TCP	68	54944 → 80 [ACK]
2022-02-19 21:58:22.445551	138.68.92.163	54944	134.122.33.221	80	HTTP	190	GET /index HTTP/1
2022-02-19 21:58:22.445581	134.122.33.221	80	138.68.92.163	54944	TCP	68	80 → 54944 [ACK]
2022-02-19 21:58:22.445831	134.122.33.221	80	138.68.92.163	54944	HTTP	505	HTTP/1.1 404 Not
2022-02-19 21:58:22.543216	138.68.92.163	54944	134.122.33.221	80	TCP	68	54944 → 80 [ACK]
2022-02-19 21:58:22.543329	138.68.92.163	54944	134.122.33.221	80	HTTP	192	GET /archive HTTP
2022-02-19 21:58:22.543358	134.122.33.221	80	138.68.92.163	54944	TCP	68	80 → 54944 [ACK]
2022-02-19 21:58:22.543629	134.122.33.221	80	138.68.92.163	54944	HTTP	505	HTTP/1.1 404 Not
2022-02-19 21:58:22.641382	138.68.92.163	54944	134.122.33.221	80	HTTP	187	GET /02 HTTP/1.1
2022-02-19 21:58:22.641679	134.122.33.221	80	138.68.92.163	54944	HTTP	505	HTTP/1.1 404 Not
2022-02-19 21:58:22.739437	138.68.92.163	54944	134.122.33.221	80	HTTP	193	GET /register HTT
2022-02-19 21:58:22.739747	134.122.33.221	80	138.68.92.163	54944	HTTP	505	HTTP/1.1 404 Not
2022-02-19 21:58:22.837568	138.68.92.163	54944	134.122.33.221	80	HTTP	187	GET /en HTTP/1.1
2022-02-19 21:58:22.837966	134.122.33.221	80	138.68.92.163	54944	HTTP	505	HTTP/1.1 404 Not
2022-02-19 21:58:22.936158	138.68.92.163	54944	134.122.33.221	80	HTTP	190	GET /forum HTTP/1

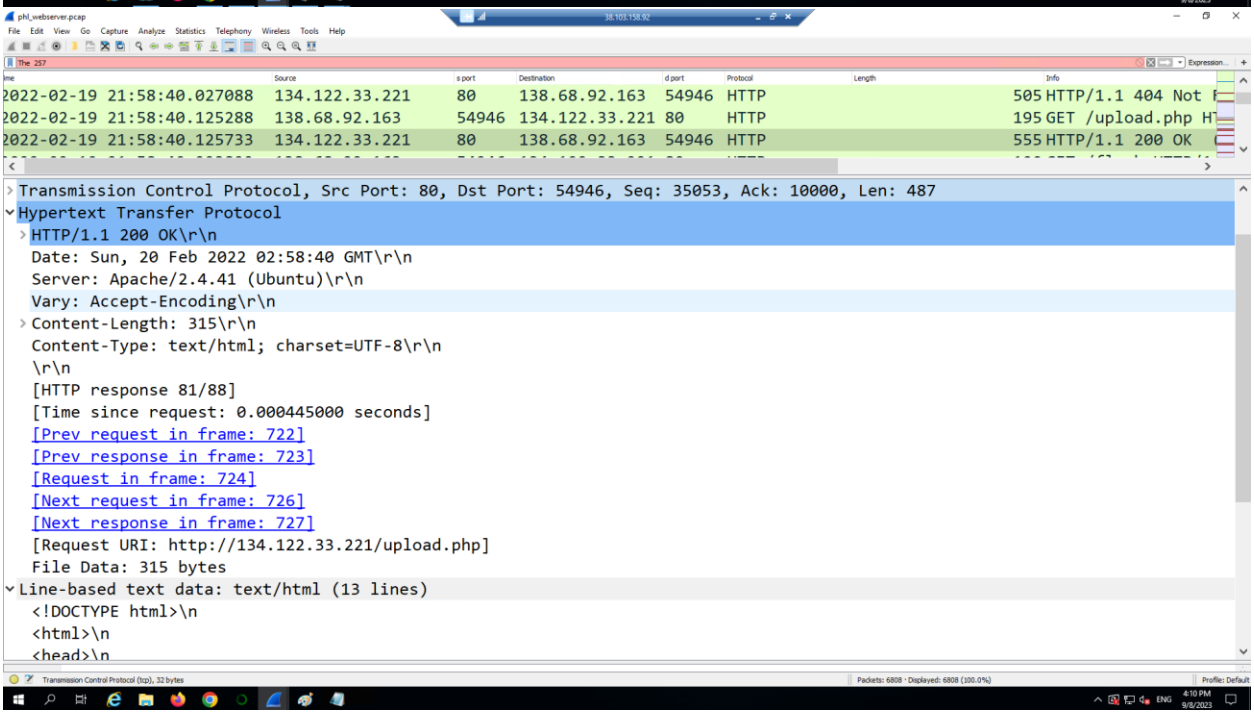
Time	Source	s port	Destination	d port	Protocol	Length	Info
2022-02-19 21:58:22.641382	138.68.92.163	54944	134.122.33.221	80	HTTP	187	GET /02 HTTP/1.1
2022-02-19 21:58:22.641679	134.122.33.221	80	138.68.92.163	54944	HTTP	505	HTTP/1.1 404 Not
2022-02-19 21:58:22.739437	138.68.92.163	54944	134.122.33.221	80	HTTP	193	GET /register HTT
2022-02-19 21:58:22.739747	134.122.33.221	80	138.68.92.163	54944	HTTP	505	HTTP/1.1 404 Not
2022-02-19 21:58:22.837568	138.68.92.163	54944	134.122.33.221	80	HTTP	187	GET /en HTTP/1.1
2022-02-19 21:58:22.837966	134.122.33.221	80	138.68.92.163	54944	HTTP	505	HTTP/1.1 404 Not
2022-02-19 21:58:22.936158	138.68.92.163	54944	134.122.33.221	80	HTTP	190	GET /forum HTTP/1
2022-02-19 21:58:22.936441	134.122.33.221	80	138.68.92.163	54944	HTTP	505	HTTP/1.1 404 Not
2022-02-19 21:58:23.034850	138.68.92.163	54944	134.122.33.221	80	HTTP	193	GET /software HTT
2022-02-19 21:58:23.035116	134.122.33.221	80	138.68.92.163	54944	HTTP	505	HTTP/1.1 404 Not
2022-02-19 21:58:23.133386	138.68.92.163	54944	134.122.33.221	80	HTTP	194	GET /downloads HT
2022-02-19 21:58:23.133708	134.122.33.221	80	138.68.92.163	54944	HTTP	505	HTTP/1.1 404 Not
2022-02-19 21:58:23.231439	138.68.92.163	54944	134.122.33.221	80	HTTP	186	GET /3 HTTP/1.1
2022-02-19 21:58:23.231747	134.122.33.221	80	138.68.92.163	54944	HTTP	505	HTTP/1.1 404 Not
2022-02-19 21:58:23.329506	138.68.92.163	54944	134.122.33.221	80	HTTP	193	GET /security HTT
2022-02-19 21:58:23.329805	134.122.33.221	80	138.68.92.163	54944	HTTP	505	HTTP/1.1 404 Not
2022-02-19 21:58:23.428052	138.68.92.163	54944	134.122.33.221	80	HTTP	187	GET /13 HTTP/1.1
2022-02-19 21:58:23.428336	134.122.33.221	80	138.68.92.163	54944	HTTP	505	HTTP/1.1 404 Not
2022-02-19 21:58:23.526301	138.68.92.163	54944	134.122.33.221	80	HTTP	193	GET /category HTT
2022-02-19 21:58:23.526554	134.122.33.221	80	138.68.92.163	54944	HTTP	505	HTTP/1.1 404 Not
2022-02-19 21:58:23.624364	138.68.92.163	54944	134.122.33.221	80	HTTP	186	GET /4 HTTP/1.1
2022-02-19 21:58:23.624628	134.122.33.221	80	138.68.92.163	54944	HTTP	505	HTTP/1.1 404 Not
2022-02-19 21:58:23.722412	138.68.92.163	54944	134.122.33.221	80	HTTP	192	GET /content HTTP
2022-02-19 21:58:23.722676	134.122.33.221	80	138.68.92.163	54944	HTTP	505	HTTP/1.1 404 Not
2022-02-19 21:58:23.820526	138.68.92.163	54944	134.122.33.221	80	HTTP	187	GET /14 HTTP/1.1

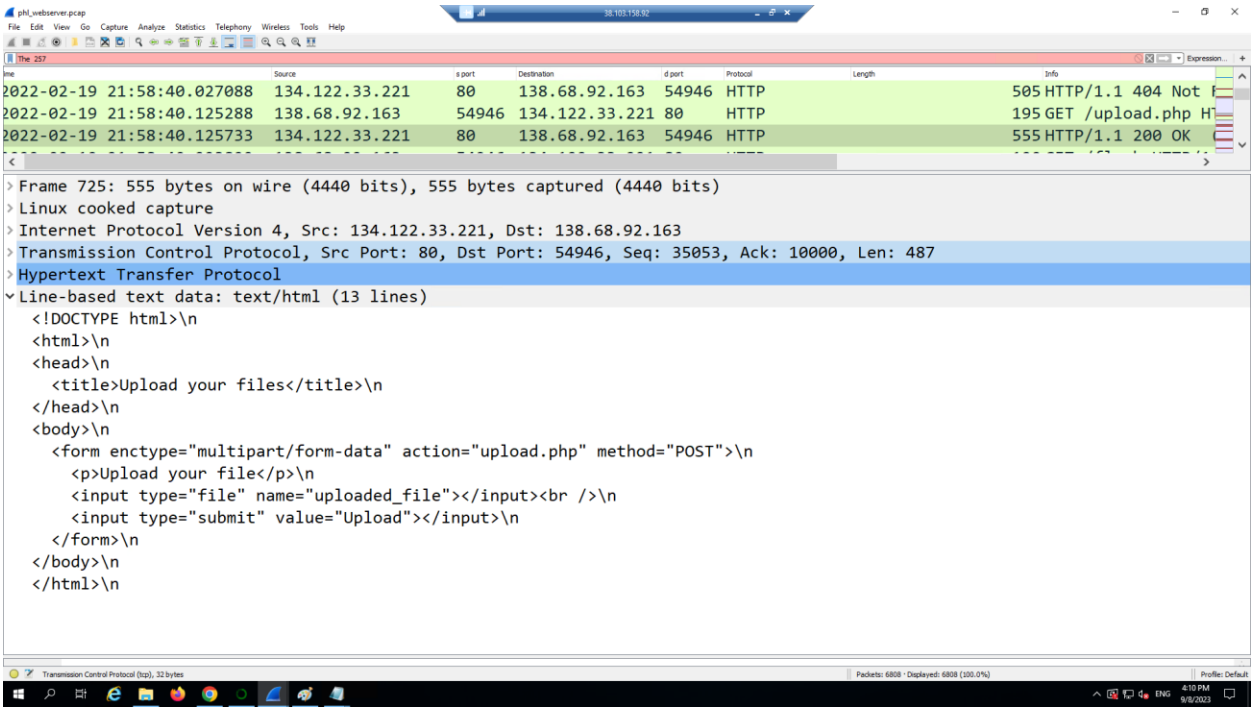
With all this DOS attack with SYN flood webserver redirected attacker to different URL location i.e. in uploads folder.



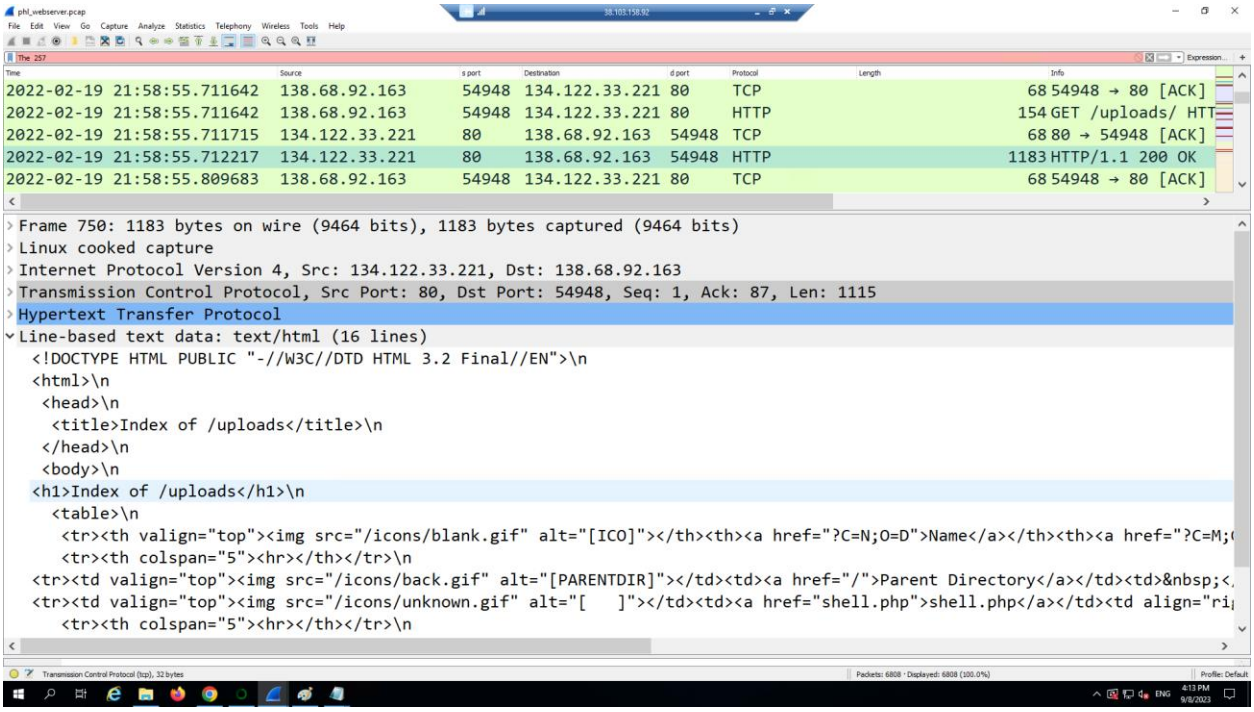
Now, attacker trying to gain access to webserver through new URL location in uploads but keep denied by webserver until it's totally crashed and then ip address 138.68.92.163 able to create a new file there as upload .php in uploads folder at 21:58:40.125288 with port number 54946 and webserver accepted the request to create a upload.php file.


phl_webserver.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Time Source s port Destination d port Protocol Length Info
2022-02-19 21:58:40.027088 134.122.33.221 80 138.68.92.163 54946 HTTP 505 HTTP/1.1 404 Not
2022-02-19 21:58:40.125288 138.68.92.163 54946 134.122.33.221 80 HTTP 195 GET /upload.php H
2022-02-19 21:58:40.125733 134.122.33.221 80 138.68.92.163 54946 HTTP 555 HTTP/1.1 200 OK
2022-02-19 21:58:40.223822 138.68.92.163 54946 134.122.33.221 80 HTTP 190 GET /flash HTTP/1
2022-02-19 21:58:40.224182 134.122.33.221 80 138.68.92.163 54946 HTTP 505 HTTP/1.1 404 Not
Frame 724: 195 bytes on wire (1560 bits), 195 bytes captured (1560 bits)
Linux cooked capture
Internet Protocol Version 4, Src: 138.68.92.163, Dst: 134.122.33.221
Transmission Control Protocol, Src Port: 54946, Dst Port: 80, Seq: 9873, Ack: 35053, Len: 127
Hypertext Transfer Protocol
GET /upload.php HTTP/1.1\r\n
Host: 134.122.33.221\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)\r\n
Accept: */*\r\n
\r\n
[Full request URI: http://134.122.33.221/upload.php]
[HTTP request 81/88]
[Prev request in frame: 722]
[Response in frame: 725]
[Next request in frame: 726]

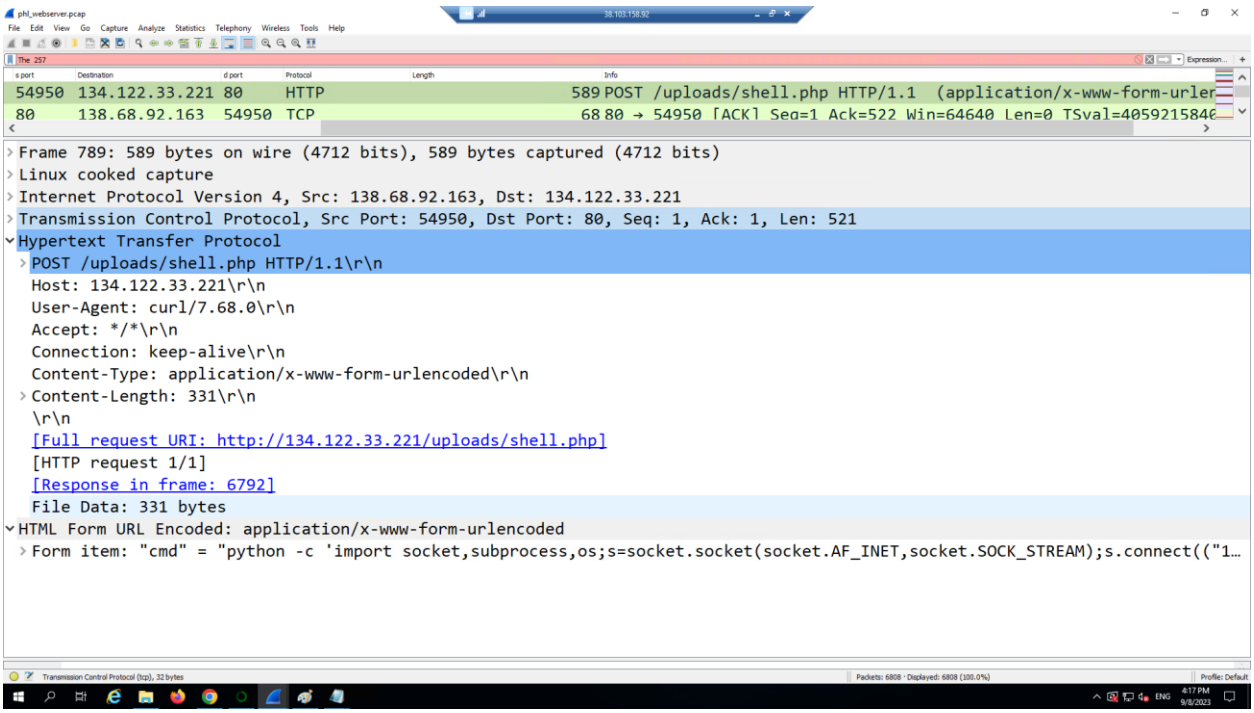

phl_webserver.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Source s port Destination d port Protocol Length Info
2022-02-19 21:58:40.027088 134.122.33.221 80 138.68.92.163 54946 HTTP 505 HTTP/1.1 404 Not
2022-02-19 21:58:40.125288 138.68.92.163 54946 134.122.33.221 80 HTTP 195 GET /upload.php HT
2022-02-19 21:58:40.125733 134.122.33.221 80 138.68.92.163 54946 HTTP 555 HTTP/1.1 200 OK
Transmission Control Protocol, Src Port: 80, Dst Port: 54946, Seq: 35053, Ack: 10000, Len: 487
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Sun, 20 Feb 2022 02:58:40 GMT\r\n
Server: Apache/2.4.41 (Ubuntu)\r\n
Vary: Accept-Encoding\r\n
Content-Length: 315\r\n
Content-Type: text/html; charset=UTF-8\r\n
\r\n
[HTTP response 81/88]
[Time since request: 0.000445000 seconds]
[Prev request in frame: 722]
[Prev response in frame: 723]
[Request in frame: 724]
[Next request in frame: 726]
[Next response in frame: 727]
[Request URI: http://134.122.33.221/upload.php]
File Data: 315 bytes
Line-based text data: text/html (13 lines)
<!DOCTYPE html>\n
<html>\n
<head>\n



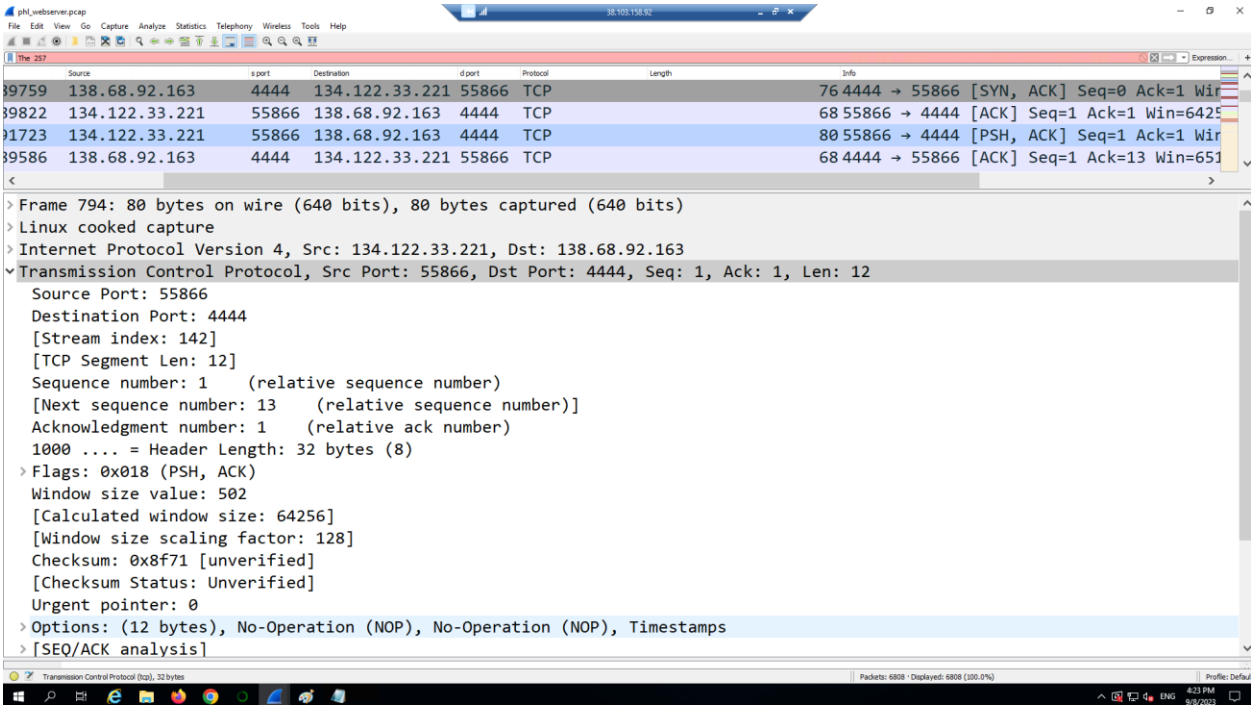
Here Attacker Ip address 138.68.92.163 again successful to gain the access to webserver files and gain access to parent directory by 3 way handshaking method.



Here in the given below capture, attacker is sending data to the webserver using POST, typically for the purpose of submitting a for or uploading a file. /uploads/shell.php is the path to the resource on the server; it's usually a file or a specific endpoint that the attacker is interacting with.



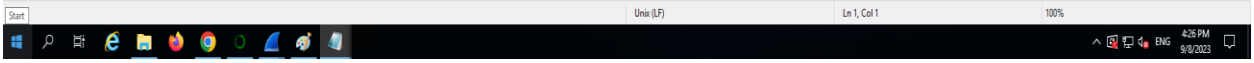
Furthermore, attacker keep delivering data to specific location with PUSH flag in TCP packet to indicate that the sending application should push all buffered data to the receiving application asap, rather than waiting for full buffer to accumulate by using telnet or chat programs.



Eventually, webserver become unavailable after this attack and attacker moved all the database into new folder phl.db and then removed the file after capturing all data to hide the tracks.
We can see this in artifacts of database file.

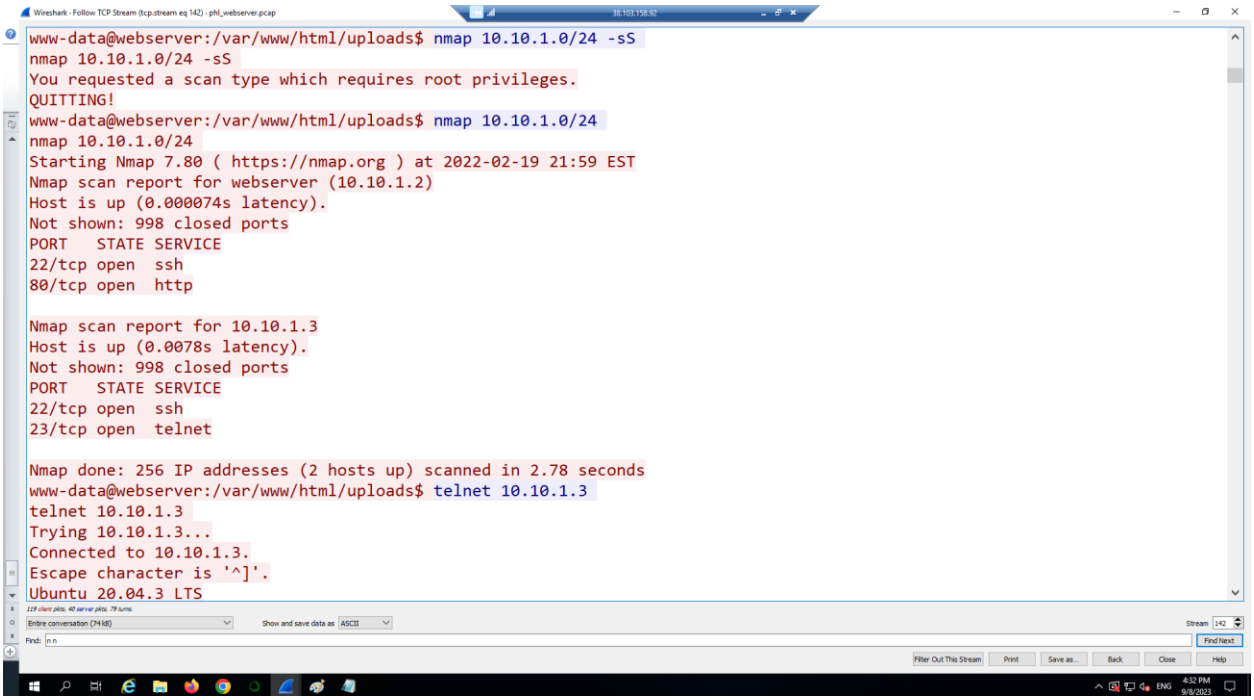
```
138.68.92.163 - - [19/Feb/2022:21:58:37 -0500] "GET /text HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:37 -0500] "GET /chat HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:37 -0500] "GET /39 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:38 -0500] "GET /nl HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:38 -0500] "GET /34 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:38 -0500] "GET /science HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:38 -0500] "GET /adview HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:38 -0500] "GET /intro HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:38 -0500] "GET /account HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:38 -0500] "GET /x HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:38 -0500] "GET /42 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:38 -0500] "GET /comment HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:38 -0500] "GET /privacypolicy HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:39 -0500] "GET /node HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:39 -0500] "GET /sponsors HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:39 -0500] "GET /uk HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:39 -0500] "GET /viewforum HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:39 -0500] "GET /dot HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:39 -0500] "GET /affiliates HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:39 -0500] "GET /testimonials HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:39 -0500] "GET /forms HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:39 -0500] "GET /corporate HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:39 -0500] "GET /donate HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /41 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /upload.php HTTP/1.1" 200 487 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /flash HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /48 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /portal HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /design HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /uploads/randomfile1 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /uploads/frand2 HTTP/1.1" 404 437 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:40 -0500] "GET /uploads/ HTTP/1.1" 200 1115 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
138.68.92.163 - - [19/Feb/2022:21:58:55 -0500] "GET /uploads/ HTTP/1.1" 200 1115 "-" "curl/7.68.0"
138.68.92.163 - - [19/Feb/2022:21:59:04 -0500] "POST /uploads/shell.php HTTP/1.1" 200 2655 "-" "curl/7.68.0"
```

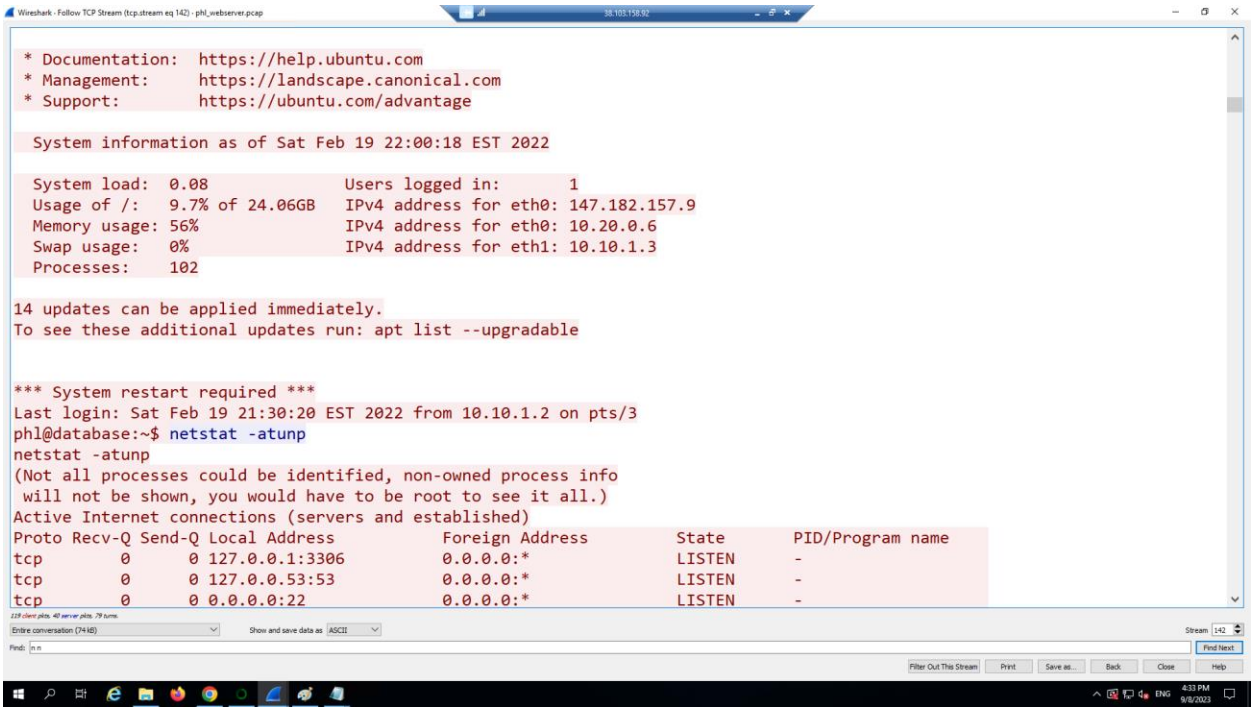
```
2022-02-20T03:01:02.455170Z        9 Field List       slave_relay_log_info
2022-02-20T03:01:02.455908Z        9 Field List       slave_worker_info
2022-02-20T03:01:02.456390Z        9 Field List       slow_log
2022-02-20T03:01:02.457875Z        9 Field List       tables_priv
2022-02-20T03:01:02.458175Z        9 Field List       time_zone
2022-02-20T03:01:02.458407Z        9 Field List       time_zone_leap_second
2022-02-20T03:01:02.458616Z        9 Field List       time_zone_name
2022-02-20T03:01:02.458783Z        9 Field List       time_zone_transition
2022-02-20T03:01:02.459017Z        9 Field List       time_zone_transition_type
2022-02-20T03:01:02.459358Z        9 Field List       user
2022-02-20T03:01:07.373140Z        9 Query     show tables
2022-02-20T03:01:10.167274Z        9 Query     SELECT * FROM user
2022-02-20T03:01:13.274571Z        9 Query     SELECT DATABASE()
2022-02-20T03:01:13.274934Z        9 Init DB   ph1
2022-02-20T03:01:13.275849Z        9 Query     show databases
2022-02-20T03:01:13.276443Z        9 Query     show tables
2022-02-20T03:01:13.277190Z        9 Field List       customers
2022-02-20T03:01:15.536553Z        9 Query     show tables
2022-02-20T03:01:21.694024Z        9 Query     SELECT * FROM customers
2022-02-20T03:01:31.159492Z        9 Query     SELECT * FROM customers LIMIT 5
2022-02-20T03:01:34.242985Z        9 Quit
2022-02-20T03:01:46.748188Z       10 Connect   root@localhost on  using Socket
2022-02-20T03:01:46.748326Z       10 Query     /*!40100 SET @@SQL_MODE='' */
2022-02-20T03:01:46.748435Z       10 Query     /*!40103 SET TIME_ZONE='+00:00' */
2022-02-20T03:01:46.748574Z       10 Query     /*!80000 SET SESSION information_schema_stats_expiry=0 */
2022-02-20T03:01:46.748680Z       10 Query     SET SESSION NET_READ_TIMEOUT= 86400, SESSION NET_WRITE_TIMEOUT= 86400
2022-02-20T03:01:46.748820Z       10 Query     SHOW VARIABLES LIKE 'gtid\_mode'
2022-02-20T03:01:46.753077Z       10 Query     SELECT LOGFILE_GROUP_NAME, FILE_NAME, TOTAL_EXTENTS, INITIAL_SIZE, ENGINE, EXTRA FROM INFORMATION_SCHEMA.FILES WHERE ENGINE = 'ndbcluster' AND FILE_TYPE = 'UNDO LOG' AND FILE_NAME IS NOT NU
2022-02-20T03:01:46.756231Z       10 Query     SELECT DISTINCT TABLESPACE_NAME, FILE_NAME, LOGFILE_GROUP_NAME, EXTENT_SIZE, INITIAL_SIZE, ENGINE FROM INFORMATION_SCHEMA.FILES WHERE FILE_TYPE = 'DATAFILE' AND TABLESPACE_NAME IN (SELECT D
2022-02-20T03:01:46.757327Z       10 Query     SHOW VARIABLES LIKE 'ndbinfo\_version'
2022-02-20T03:01:46.763600Z       10 Init DB   ph1
2022-02-20T03:01:46.763710Z       10 Query     show tables
2022-02-20T03:01:46.765171Z       10 Query     LOCK TABLES `customers` READ /*!32311 LOCAL */
2022-02-20T03:01:46.769709Z       10 Query     show table status like 'customers'
2022-02-20T03:01:46.772197Z       10 Query     SET SQL_QUOTE_SHOW_CREATE=1
2022-02-20T03:01:46.772305Z       10 Query     SET SESSION character_set_results = 'binary'
2022-02-20T03:01:46.772375Z       10 Query     show create table `customers`
2022-02-20T03:01:46.772772Z       10 Query     SET SESSION character_set_results = 'utf8mb4'
2022-02-20T03:01:46.772883Z       10 Query     show fields from `customers`
2022-02-20T03:01:46.774238Z       10 Query     show fields from `customers`
2022-02-20T03:01:46.775014Z       10 Query     SELECT /*!40001 SQL_NO_CACHE */ * FROM `customers`
2022-02-20T03:01:46.775651Z       10 Query     SET SESSION character_set_results = 'binary'
2022-02-20T03:01:46.775720Z       10 Query     use `ph1`
2022-02-20T03:01:46.775799Z       10 Query     select @@collation_database
2022-02-20T03:01:46.775886Z       10 Query     SHOW TRIGGERS LIKE 'customers'
2022-02-20T03:01:46.777051Z       10 Query     SET SESSION character_set_results = 'utf8mb4'
2022-02-20T03:01:46.777108Z       10 Query     SET SESSION character_set_results = 'binary'
2022-02-20T03:01:46.777571Z       10 Query     SELECT COLUMN_NAME,                    JSON_EXTRACT(HISTOGRAM, '$."number-of-buckets-specified"')                FROM information_schema.COLUMN_STATISTICS                WHERE SCHEMA_NAM
2022-02-20T03:01:46.778175Z       10 Query     SET SESSION character_set_results = 'utf8mb4'
2022-02-20T03:01:46.778230Z       10 Query     UNLOCK TABLES
2022-02-20T03:01:46.782060Z       10 Quit
```



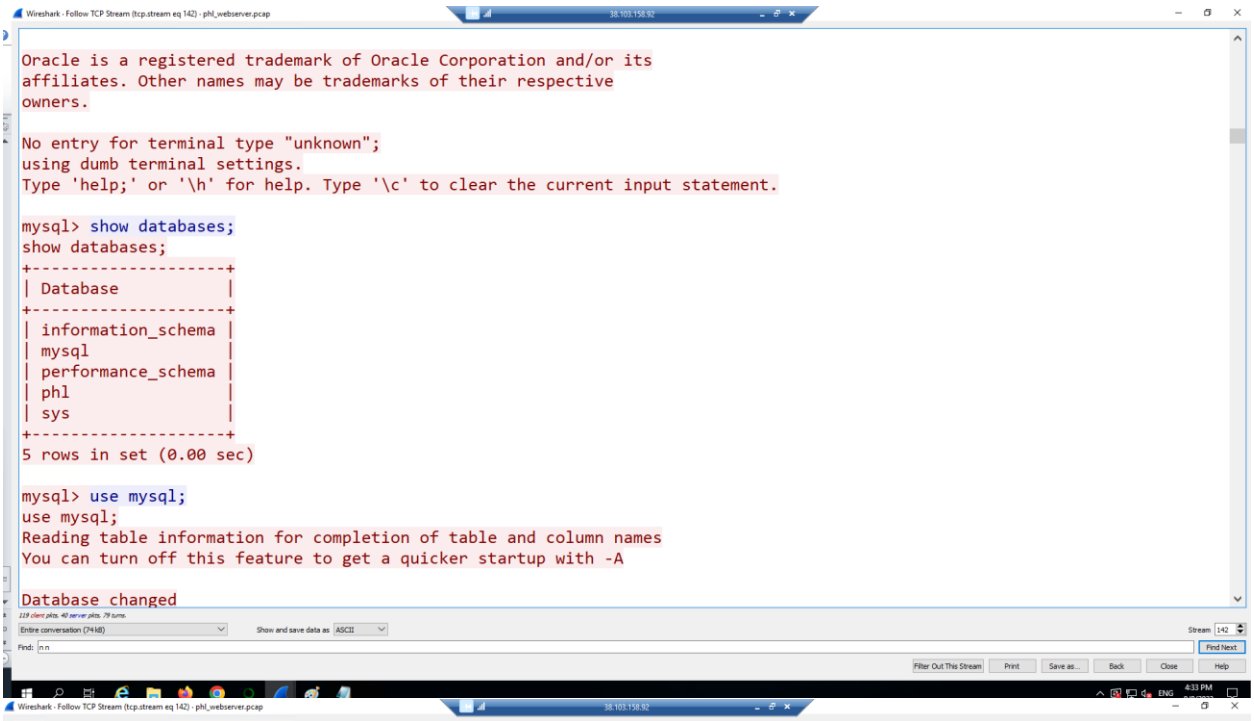
After analysing all the pcap file, we got to know that attacker firstly find what port are open on webserver and then attacked accordingly also adding to it there is a default password on Ubuntu Operating system as username = “admin” and password = “admin” which was very easy to crack and there was no password on the database, hence attacker coped all the database into new file and then removed the file from the system. The most important thing what I have noticed that there was write permission given to everyone modify the database. We can see this all information in given below captures that I got after analysing the reverse shell opened TCP stream.

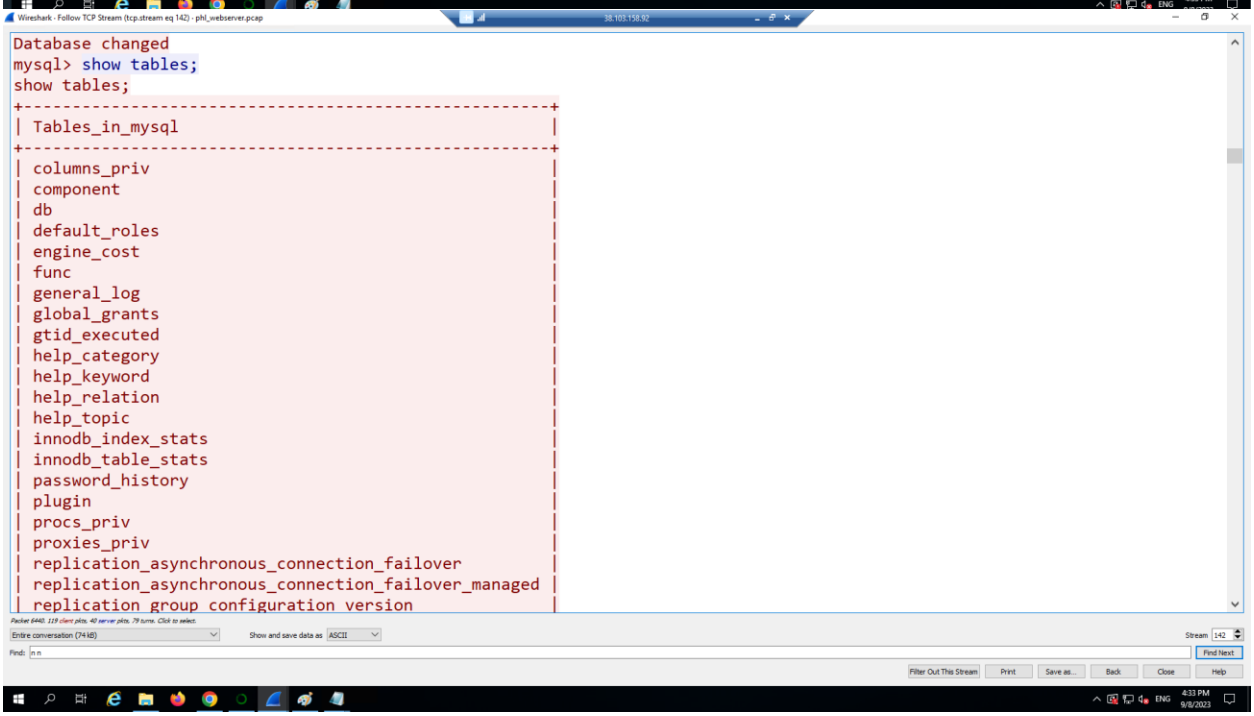
Checking what ports are open by using nmap command.

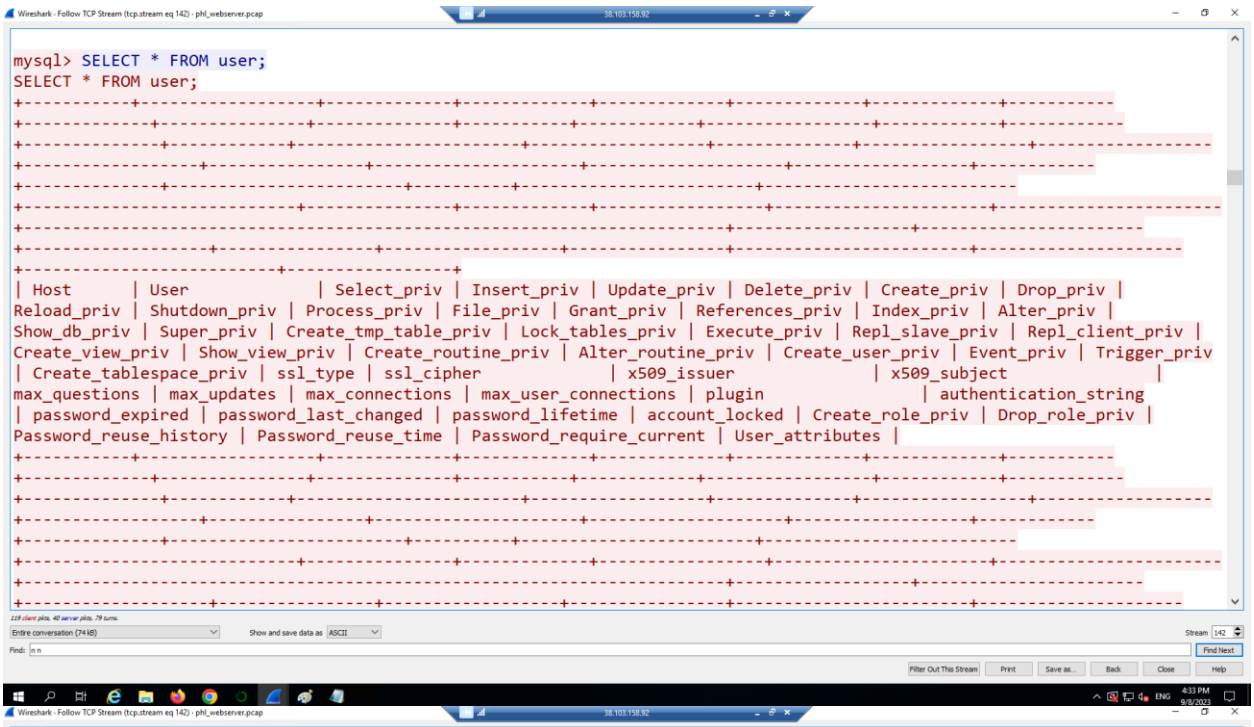


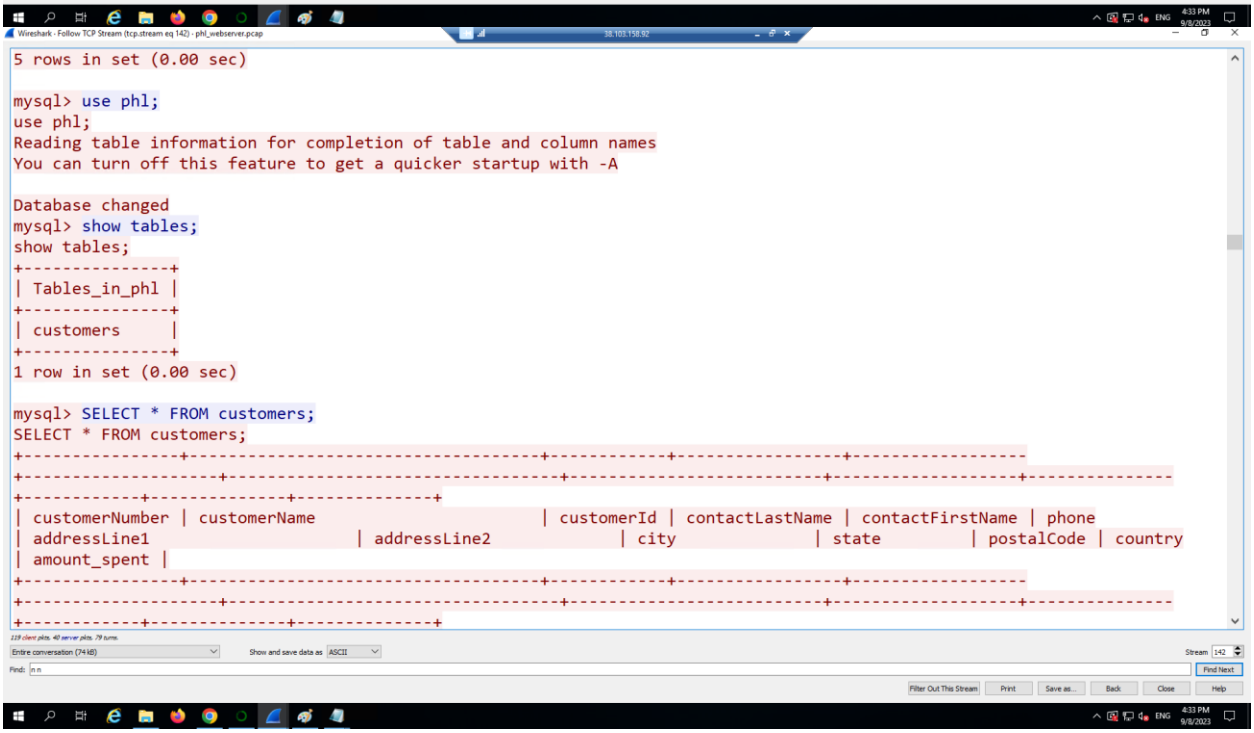


Accessing mySQL database ny attacker given below:

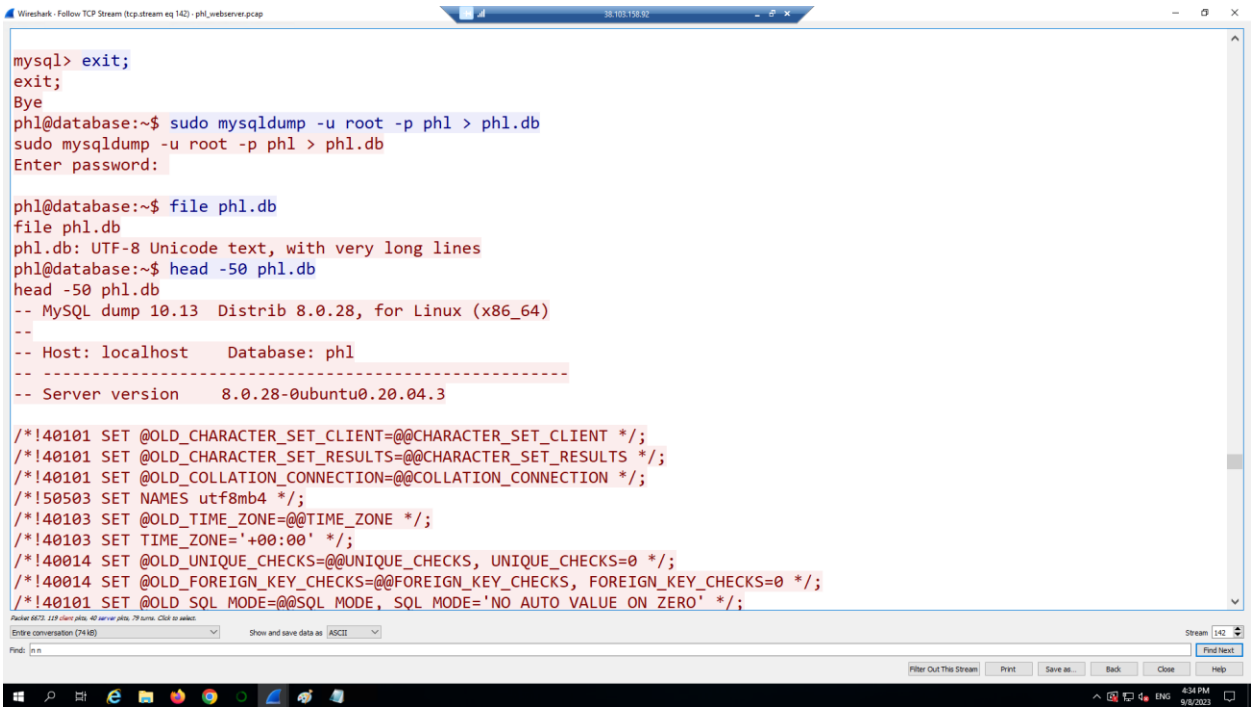

Wireshark · Follow TCP Stream (tcp.stream eq 142) · phl_webserver.pcap
38.103.158.92
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
No entry for terminal type "unknown";
using dumb terminal settings.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
mysql> show databases;
show databases;
+--------------------+
| Database |
+--------------------+
| information_schema |
| mysql |
| performance_schema |
| phl |
| sys |
+--------------------+
5 rows in set (0.00 sec)
mysql> use mysql;
use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
Entire conversation (74 kB)
Show and save data as
ASCII
Stream
142
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help


Wireshark · Follow TCP Stream (tcp.stream eq 142) · phl_webserver.pcap
38.103.158.92
Database changed
mysql> show tables;
show tables;
+---+
| Tables_in_mysql |
+---+
| columns_priv |
| component |
| db |
| default_roles |
| engine_cost |
| func |
| general_log |
| global_grants |
| gtid_executed |
| help_category |
| help_keyword |
| help_relation |
| help_topic |
| innodb_index_stats |
| innodb_table_stats |
| password_history |
| plugin |
| procs_priv |
| proxies_priv |
| replication_asynchronous_connection_failover |
| replication_asynchronous_connection_failover_managed |
| replication_group_configuration_version |
Entire conversation (74 kB)
Show and save data as
ASCII
Stream
142
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
4:33 PM
9/8/2023

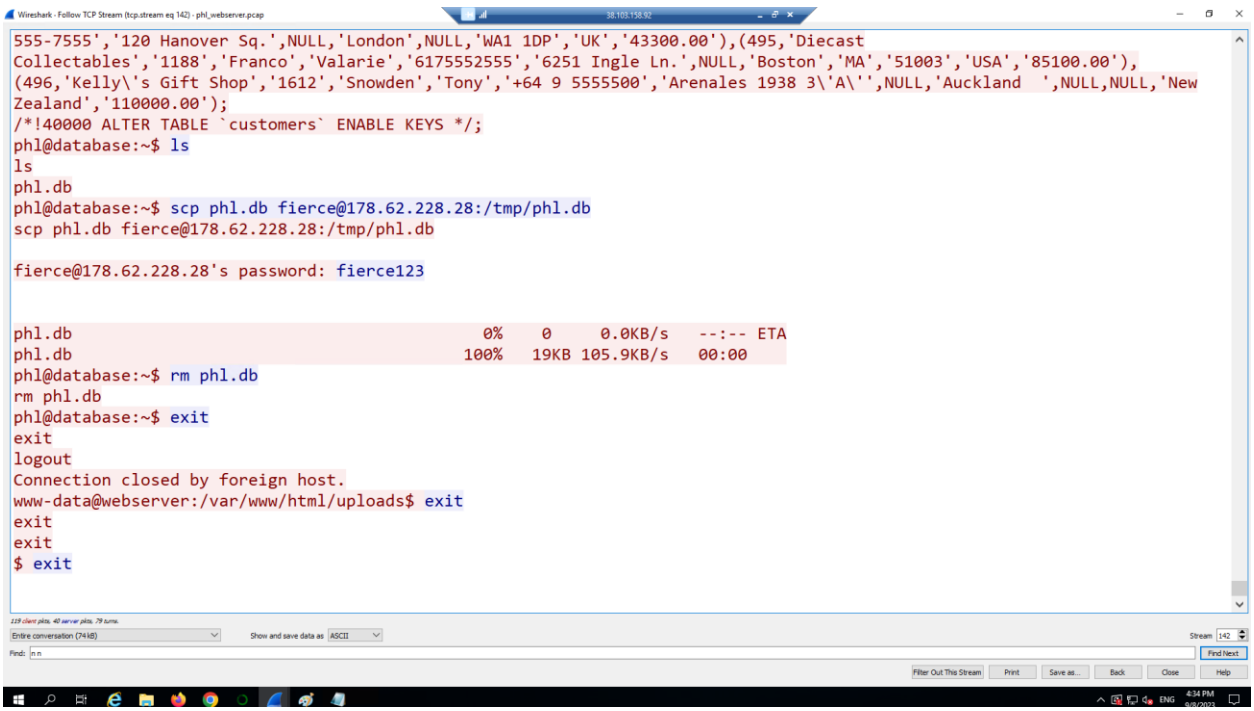




Created file **phl.db** to transfer all the data into new file.



Here in given below capture, file had been removed from the system to hide the tracks.



Risk tolerance

As we discussed earlier the network topology and its full scale mapping, we came to know that risk tolerance of the company is very low because of that impact of attack is high. Following are several critical issues that need immediate action:

- **Insufficient Security Measures**: The Company's current security setup is inadequate, particularly for an organization that handles sensitive data. The lack of proper monitoring and detection tools like IDS/IPS makes them vulnerable to cyber threats.

- **Flat Network Architecture**: A flat network without segmentation or proper access controls can allow attackers to move laterally within the network once they gain initial access, as was the case here. Here, Webserver, file server and database are all in same network segment which is highly at risk.

- **Data Sensitivity**: The type of data stored by the company (employee and customer information) is highly sensitive. This makes them an attractive target for cybercriminals. There is no encryption methods are used to protect the data and also no firewall is installed in network for employee devices and for database and fileserver.

- **Inadequate Incident Response Plan**: The Company doesn't have an incident response team or a plan in place to handle security breaches. This lack of preparedness could have severe consequences in the event of a breach.

- **Unauthorized Access and Data Manipulation**: The attacker successfully gained access to the database, exfiltrated data, and even manipulated it. These shows a significant security lapse as there is no password on database and default password on webserver operating system and also write permissions were given to everyone to make changes in database.

- **Lack of Backup Controls**: The fact that the attacker was able to create backups of the MySQL databases indicates a lack of proper access controls and monitoring. Because no encryption attacker used TELNET to transfer the plain text data.

Insight of attack happened on Premium Lights Inc.

A SYN flood is a type of Distributed Denial of Service (DDoS) attack that exploits the way TCP/IP protocol works. Here's how it worked:

TCP Handshake: When two devices want to establish a TCP connection (like when you visit a website), they go through a three-step process known as the "three-way handshake":

SYN (Synchronize): The client sends a SYN packet to the server, indicating its wish to start a connection.

SYN-ACK (Synchronize-Acknowledge): The server responds with a SYN-ACK packet, acknowledging the request.

ACK (Acknowledge): The client sends an ACK packet to acknowledge the server's response.

SYNC FLOOD attack:

In a SYN flood attack, the attacker sends a large number of SYN packets to the target server, but does not complete the handshake (i.e., does not send the final ACK packet). Since the server keeps waiting for the final ACK to complete the connection, it reserves resources for each incomplete connection.

Eventually, if the server is flooded with more SYN requests than it can handle, it may become overwhelmed and unable to process legitimate connection requests.

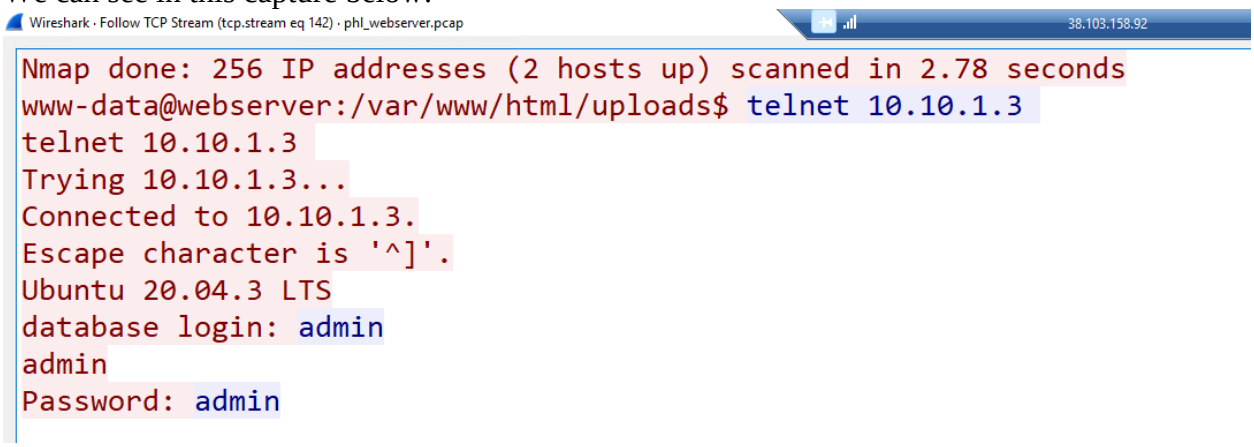
IMAPCT:

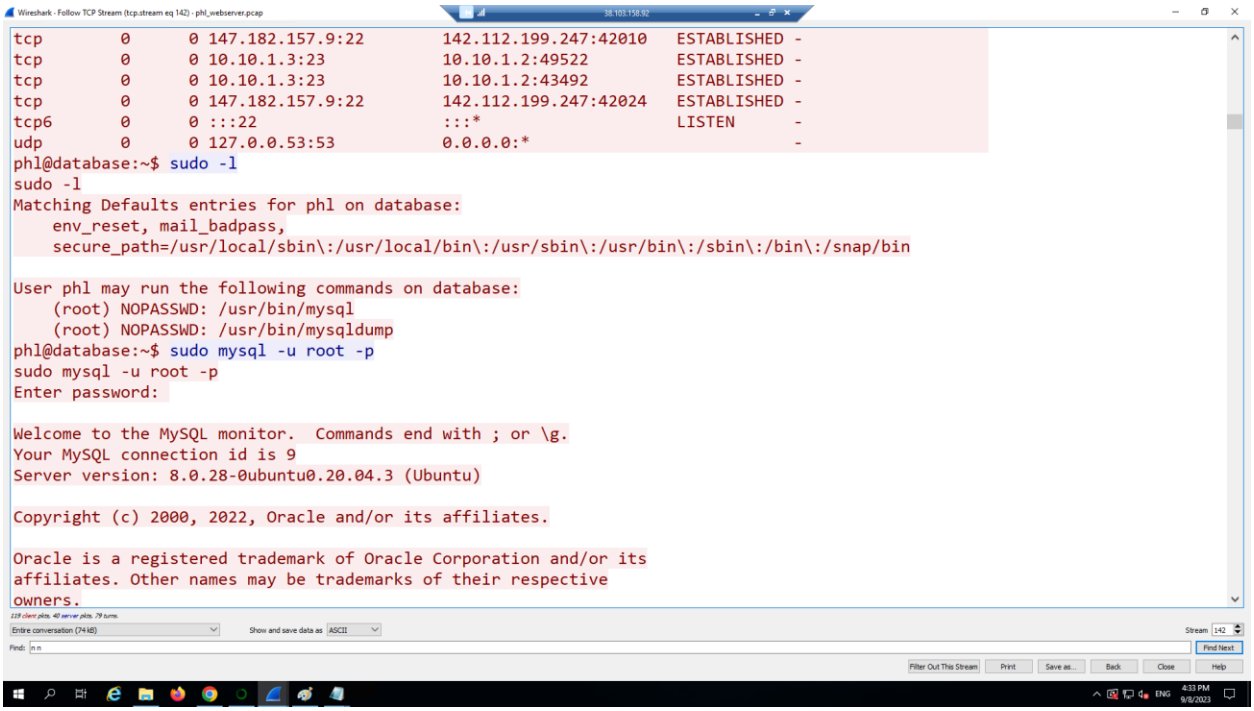
The targeted server's resources can be exhausted, causing it to slow down or even crash. Legitimate users may experience difficulty accessing the services provided by the server.

Weaknesses that allowed for this incident to occur:

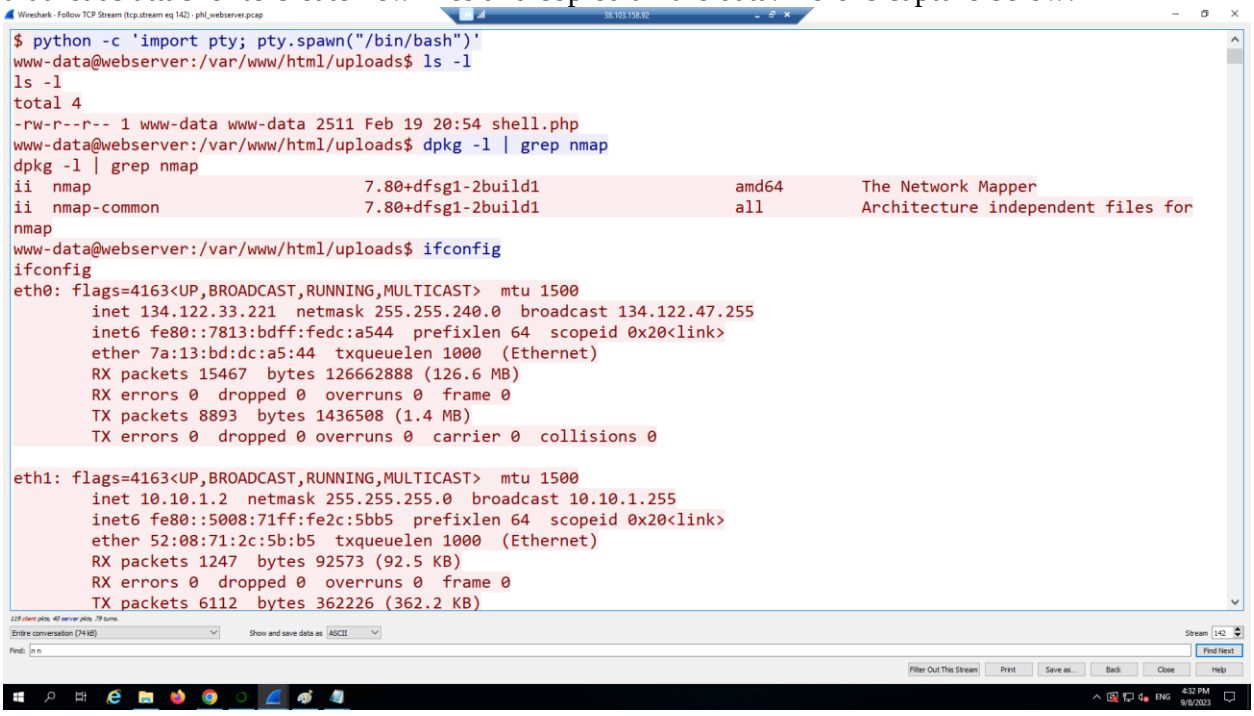
Cyberattacks on companies can occur due to a variety of vulnerabilities and weaknesses in their security posture. Identifying and addressing these vulnerabilities and weaknesses is crucial to improving overall cybersecurity. Here are some common factors that can contributed to attack on Premium Lights Inc:

- **Weak password and default Password:**
  Using weak passwords or default credentials makes it easier for attackers to gain unauthorized access to systems, especially if brute force or password spraying attacks are attempted. Here in this attack, default passwords were used on Ubuntu OS which was easily cracked by the attacker and also there was no password on SQL database.
  We can see in this capture below:





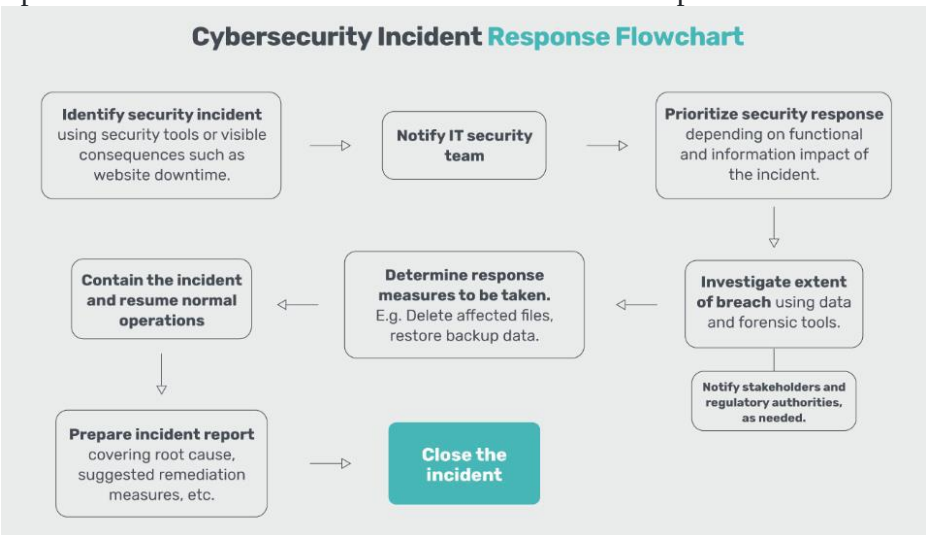
- **No Multi-factor authentication:**
  Not implementing MFA makes it easier for attackers to compromise user accounts, as it provides an additional layer of security beyond passwords.
- **Insufficient security updates**: Failed to restrict access to sensitive data and systems based on the principle of least privilege can allow attackers to move laterally within a network. There is write permission granted to everyone to make changes in the database that leads attacker to create new files and copied all the data. Here is capture below:

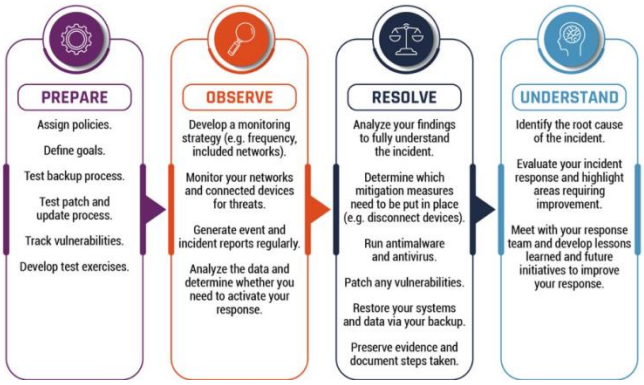


- **Port scanning:** In above capture, we can see that attacker scans the open ports on the system to check which ones are vulnerable. After identifying open ports, the attacker might conduct a service scan to determine which services are running on those ports.
- **Poorly Configured Firewalls and Security Devices:** Misconfigurations in firewall rules and security devices can create openings that attackers can exploit. Also, there is only one firewall in the organization that was very crucial security gap.
- **Poor network segmentation**: Flat network architecture without segmentation can allow attackers to easily move laterally across the network.
- **Inadequate logging and monitoring**: Without robust logging and monitoring solutions, suspicious activities and security incidents may go unnoticed.
- **No regular security audits and assessments:** Failing to conduct regular security audits, vulnerability assessments, and penetration testing can result in undiscovered weaknesses.
- **Physical security weakness:** Neglecting physical security measures, such as unauthorized access to server rooms, can lead to data breaches.
- **Missing security updates:** Failed to implement updated intrusion detection systems, antivirus software, and other security tools can render them ineffective against new threats.
- **Inadequate employee training:** Employees who are not well-informed about cybersecurity best practices can inadvertently open phishing emails or engage in risky behavior, leading to security breaches. Also, there is a common Wi-Fi for employee personal devices and company work devices which may exploit the weaknesses of the system.

Incident Response plan:

An incident playbook for an SYNC flood DDOS attack is crucial step in ensuring a swift and effective response to such an event. Given below is incident response checklist.





Preparation

Document Critical Assets: Identify and document critical systems, applications, and network infrastructure that need protection.
Baseline Traffic: Establish baseline traffic patterns for normal operations to aid in anomaly detection. **Incident Response Team (IRT)**: Assemble a dedicated incident response team with defined roles and responsibilities. **Team roles**: Incident manager, network, security, communication lead, legal/compliance representative, system administrators.
DDoS Mitigation Tools: Ensure you have the necessary DDoS mitigation tools or services in place (e.g., firewalls, load balancers, DDoS protection services).
Communication Plan: Establish a clear communication plan with internal stakeholders, including key contacts, and external parties (vendors, ISPs, etc.).
Detection

Monitor

Continuously monitor network traffic, server logs, and performance metrics for signs of abnormal behavior.
Detection: Identify the attack through monitoring tools, network traffic analysis, and alerts from security systems.
Triage:
Verify that it's a SYN flood DDoS attack.
Assess the severity and impact on network resources and services.

Identification

Confirm DDoS Attack: Validate the incident, ensuring it is indeed a DDoS attack and not a false positive.
Classify Attack Type: Determine the type of DDoS attack to inform mitigation strategy. In this case DDOS attack is SYNC flood attack.
Affected Services: Identify which services or systems are being affected and prioritize them based on criticality.

Containment

Traffic Diversion: Redirect traffic through DDoS mitigation tools or services.
Rate Limiting: Implement rate limiting rules on routers, firewalls to control incoming connection requests.

SYN cookies: enable SYN cookies to protect against SUN flood attacks.
Adjust firewall rules: Modify firewall rules to block or rate limit the suspicious traffic.

Eradication

Implement Filters: Apply filters to block or throttle malicious traffic at the perimeter.
Patch/Update: Identify and apply any necessary patches or updates to vulnerable systems that may have been exploited.

Recovery

Gradual Service Restoration: Gradually restore services, monitoring for signs of reoccurrence.
Performance Verification: Verify that the affected systems are operating at normal capacity and performance levels.

Lessons Learned

Post-Incident Analysis: Conduct a thorough post-incident analysis to understand what worked, what didn't, and what can be improved.

Documentation: Update the incident response playbook with any new information or lessons learned. **Training and Drills**: Provide additional training to the incident response team based on the incident's findings.

Communication and Reporting

Internal Communication: Notify relevant internal stakeholders about the incident, steps taken, and any ongoing concerns.
External Communication: If necessary, communicate with customers, partners, and regulatory bodies, while ensuring compliance with legal requirements.

Documentation and reporting:

Incident Report: Document the incident, including the timeline of events, actions taken, and lessons learned.
Forensic Analysis: Conduct a post-incident analysis to understand the attack vectors and vulnerabilities.

Post-Incident Review

Lessons Learned: Conduct a post-incident review to identify areas for improvement and update the incident response plan accordingly.
Documentation: Update incident reports with any additional information discovered during the post-incident review.

Follow-Up Actions

Implement Recommendations: Implement any recommendations from the post-incident review.
Training and Awareness: Conduct training sessions to educate team members on lessons learned.

Closure and Post-Incident Report

Closure: Declare the incident as resolved once normal operations are restored.
Post-Incident Report: Compile a final incident report summarizing the incident, response actions, and recommendations for future improvement.

Post-Incident Recommendations

After experiencing a SYN flood DDoS attack, it's crucial for the company to take proactive measures to enhance its security posture and protect against future attacks. Here are some post-incident recommendations and potential adjustments to the security policy:

1. **Implement DDoS Protection Solutions:** Invest in DDoS mitigation services or appliances to detect and mitigate attacks in real-time. These solutions can help absorb and filter malicious traffic.
2. **Enhance Network Security:**
   Intrusion Detection/Prevention Systems (IDS/IPS): Implement advanced IDS/IPS solutions to monitor network traffic for suspicious patterns and block malicious activity.
   Firewalls: Configure and manage firewalls to filter traffic and prevent unauthorized access. Consider next-generation firewalls for more advanced threat detection capabilities.
3. **Increase Bandwidth Capacity:** Ensure sufficient bandwidth capacity to handle sudden spikes in traffic. This can help absorb a portion of DDoS attacks.
4. **Implement Rate Limiting and Connection Throttling:** Configure network devices and systems to limit the rate of incoming connections to prevent overload during an attack.
5. **Enable SYN Cookies**: Enable SYN cookies at the network level to protect against SYN flood attacks. SYN cookies can help ensure that server resources are not tied up by incomplete connections.
6. **Deploy Load Balancers:** Use load balancing solutions to distribute traffic across multiple servers. This can help spread the load and minimize the impact of a DDoS attack.
7. **Regularly Update and Patch Systems:** Ensure all systems, applications, and network devices are up-to-date with the latest security patches and updates to mitigate known vulnerabilities.
8. **Conduct Security Audits and Penetration Testing:** Regularly assess the security of systems and networks through audits and penetration testing to
9. **Employee Training and Awareness:** Conduct regular security awareness training for employees to educate them about phishing, social engineering, and best practices for protecting sensitive information.
10. **Develop an Incident Response Plan for DDoS Attacks:** Create a detailed incident response plan specific to DDoS attacks, outlining roles, responsibilities, and response procedures.
11. **Engage with a Managed Security Service Provider (MSSP):** Consider outsourcing certain aspects of security monitoring and incident response to an MSSP that specializes in DDoS protection.

Recommended Adjustments to Security Policy

1. **DDoS Response Plan**: Include a dedicated section in the security policy outlining procedures for detecting, mitigating, and recovering from DDoS attacks.

2. **Multi**-Factor authentication: MFA policy should be must as security policy with least privilege rule.
3. **Network Security Measures**: Specify the configuration and management of firewalls, IDS/IPS systems, and other network security controls.
4. **Patch Management**: Define processes for timely and regular patching of systems, applications, and network devices to address known vulnerabilities.
5. **Employee Training and Awareness**: Emphasize the importance of ongoing security training and awareness programs for all employees.
6. **Third-Party Security Requirements**: Include clauses in contracts with third-party vendors or service providers, requiring them to adhere to specified security measures to protect against DDoS attacks.
7. **Incident Reporting and Escalation**: Detail reporting procedures for suspected or confirmed DDoS attacks, including escalation steps and communication protocols.
8. **Regular Security Audits and Testing**: Establish guidelines for conducting security audits, vulnerability assessments, and penetration tests to identify and mitigate risks.

Conclusion:

Premium Lights Inc. acknowledges the gravity of the incident and remains steadfast in their dedication to ensuring the security and resilience of their operations. Through an amalgamation of enhanced cybersecurity measures and strategic collaborations, the company aspires to emerge from this incident stronger, more resilient, and better poised to confront future challenges.

CITITATIONS:

- The CIS (Center for Internet Security) Controls: CIS Controls https://www.cisecurity.org/controls
- OWASP (Open Web Application Security Project) for web application security: OWASP https://owasp.org/
- NIST (National Institute of Standards and Technology) Cybersecurity Framework: NIST Cybersecurity Framework https://www.nist.gov/cyberframework
- Threat Scenario, 2023 https://cyber.compass.lighthouselabs.ca/p/2/days/w11d3/activities/3186
- NIST, 2020. Security and Privacy Controls for Information Systems and Organizations **https://doi.org/10.6028/NIST.SP.800-53r5**
- What is denial of services attack (DOS)? https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos
- Sniffing the reverse shell https://dev.to/kalaimani_solarc/sniffing-the-reverse-shell-2hnc
- Incidence Response https://www.incidentresponse.org/workflows/download/DDoS.pdf
- What is SYN flood? https://www.netscout.com/what-is-ddos/syn-flood-attacks
- How to Prevent DDoS Attacks: 7 Tried-and-Tested Methods https://phoenixnap.com/blog/prevent-ddos-attacks