

CTF: BDSec CTF 2023 - Networking



Hi! In this writeup, I'll explain how I solved the networking challenges from BDSec CTF 2023. If you're new to Wireshark or want to learn how to analyze network traffic, this guide is for you.

To follow along, you can download the challenge file attached below Download: [challenge.zip](#)

Challenge Description:

Nanomate Solutions, a dynamic startup software development company, has unfortunately experienced a recent security breach resulting in unauthorized access to their database. In response to this incident, the company's Incident Response team has obtained the network packet file and is seeking your expertise to investigate the evidence. Your skills are crucial in securing the company and resolving this matter effectively. Join forces with the Incident Response team to protect Nanomate Solutions and secure their confidence in their system's integrity.

N:B: This is a series of challenges, please use the same pcap file for all the challenges.

What is the server & attacker ip?

Flag format: BDSEC{serverip_attackerip}

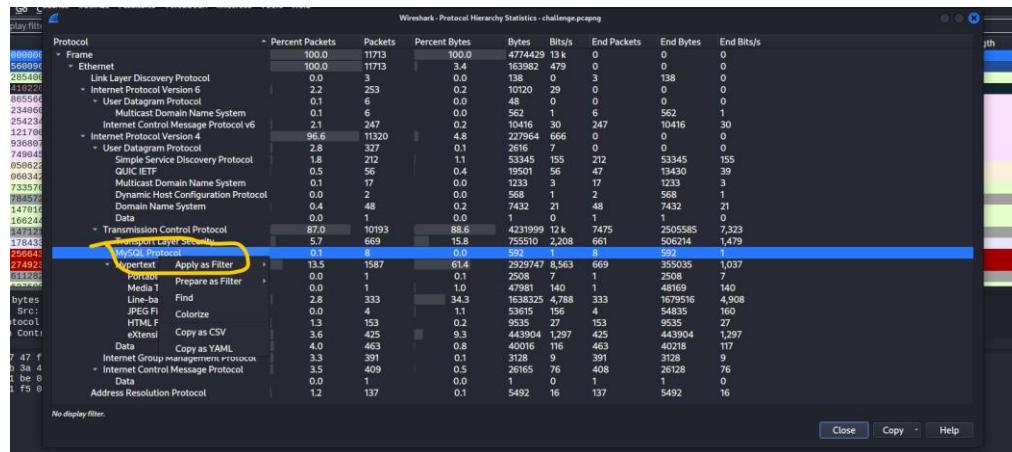
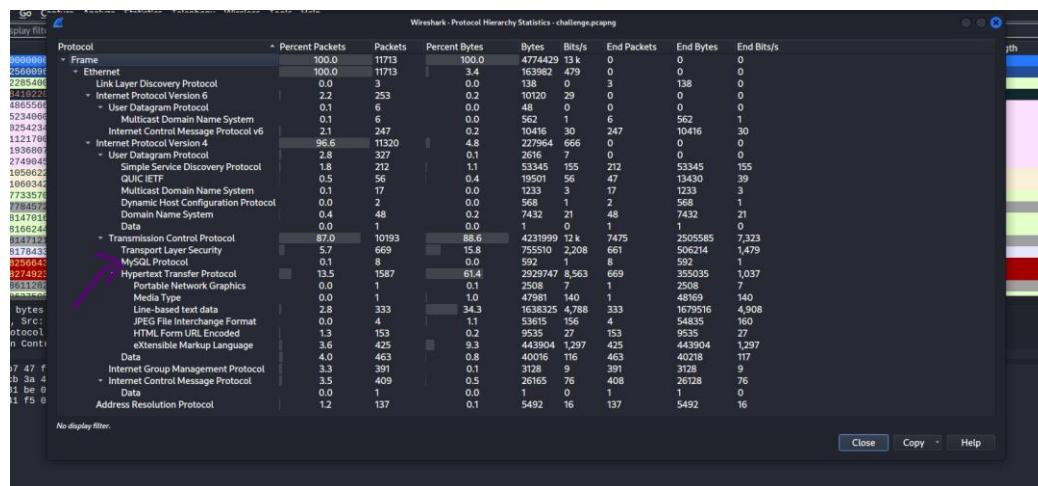
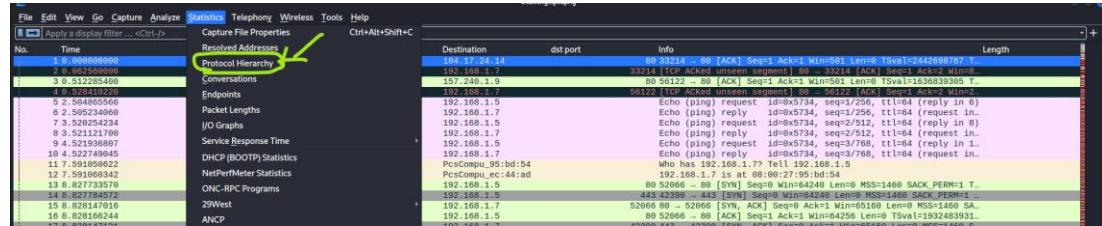
IP Addr

What is the server & attacker ip?

Download the challenge.zip and unzip this in your directory unzip challenge.zip and open challenge.pcapng with wireshark using wireshark challenge.pcapng .

We need to find the attacker's IP address that tried to connect to the database server. To do that, we'll filter the packets that use the database protocol.

Go to **Statistics > Protocol Hierarchy > My SQL Protocol** and apply as selected filter



click on any packet and as you can see server's response to connecting host, 192.168.1.7 is our attacker's ip

No.	Time	src port	Source	Destination	dst port	Info
2648	9.039846195	3306	192.168.1.5	192.168.1.7		59496 Server Greeting Error 1138
2105	21.099131518	3306	192.168.1.5	192.168.1.7		47376 Server Greeting Error 1138
2106	21.099131518	3306	192.168.1.5	192.168.1.7		47377 Server Greeting Error 1138
3173	21.529931865	3306	192.168.1.5	192.168.1.7		47482 Server Greeting Error 1138
3207	21.532040552	3306	192.168.1.5	192.168.1.7		47416 Server Greeting Error 1138
3235	21.535721289	3306	192.168.1.5	192.168.1.7		47432 Server Greeting Error 1138
3247	21.536665747	3306	192.168.1.5	192.168.1.7		47436 Server Greeting Error 1138
3274	21.537985289	3306	192.168.1.5	192.168.1.7		47442 Server Greeting Error 1138


```

MySQL Protocol
Packet Length: 70
Packet Number: 0
Error Code: 1138
Error message: Host '192.168.1.7' is not allowed to connect to this MariaDB server

```

Another approach is:

Using this command in terminal which is **tshark -r challenge.pcapng -T fields -e ip.src -e ip.dst | sort | uniq -c | sort -nr**. It displays all unique (source IP, destination IP) pairs in the capture file

[(kali㉿kali)-[~/Documents]]	
\$ tshark -r challenge.pcapng -T fields -e ip.src -e ip.dst sort uniq -c sort -nr	4811 192.168.1.7 192.168.1.5
	4548 192.168.1.5 192.168.1.7
	520 34.240.117.4 192.168.1.7
	473 192.168.1.7 34.240.117.4
	393
	189 192.168.1.4 239.255.255.250
	120 192.168.1.1 239.255.255.250
	103 192.168.1.1 224.0.0.1
	97 192.168.1.5 224.0.0.251
	91 192.168.1.4 224.0.0.252
	33 192.168.1.7 54.78.169.94
	32 54.78.169.94 192.168.1.7
	31 157.240.1.9 192.168.1.7
	30 192.168.1.7 157.240.1.9
	24 45.125.222.187 192.168.1.7
	24 192.168.1.7 45.125.222.187
	20 34.117.65.55 192.168.1.7
	19 192.168.1.2 224.0.0.251
	18 192.168.1.7 34.117.237.239
	15 34.117.237.239 192.168.1.7
	14 34.242.205.151 192.168.1.7
	13 192.168.1.7 34.242.205.151
	12 54.192.150.110 192.168.1.7
	12 192.168.1.7 54.192.150.110
	12 192.168.1.7 34.117.65.55
	11 31.13.64.35 192.168.1.7
	11 192.168.1.7 104.17.24.14

The attacker IP 192.168.1.7 communicated extensively (4,811 times) with internal IP 192.168.1.5. This was the most active session in the capture file. So I think this is flag bcz of their Suspicious behavior.

Flag: BDSEC{192.168.1.5_192.168.1.7}

HostName

What is the host name of the web server?

At first we need to filter out all packets which are using http protocol

No.	Time	src port	Source	Destination	dst port	Info	Length
2217	21.114186884	60848	192.168.1.7	192.168.1.5	80	OPTIONS / HTTP/1.1	220
2218	21.114238801	60700	192.168.1.7	192.168.1.5	80	PROPFIND / HTTP/1.1	220
2220	21.114337194	60712	192.168.1.7	192.168.1.5	80	GET /robots.txt HTTP/1.1	220
2221	21.114437194	60714	192.168.1.7	192.168.1.5	80	PROPFIND / HTTP/1.1	220
2228	21.114567919	60740	192.168.1.7	192.168.1.5	80	GET / HTTP/1.0	220
2231	21.114619998	60754	192.168.1.7	192.168.1.5	80	OPTIONS / HTTP/1.1	220
2233	21.114637194	60762	192.168.1.7	192.168.1.5	80	GET /nmapowercheck1689717155 HTTP/1.1	220
2235	21.1146372024	60764	192.168.1.7	192.168.1.5	80	POST / HTTP/1.1	220
2459	21.229660423	60776	192.168.1.7	192.168.1.5	80	OPTIONS / HTTP/1.1	220
2520	21.240496894	60784	192.168.1.7	192.168.1.5	80	PROPFIND / HTTP/1.1	220
2521	21.240500930	60792	192.168.1.7	192.168.1.5	80	OPTIONS / HTTP/1.1	220
2522	21.240519950	60814	192.168.1.7	192.168.1.5	80	GET /dashboard/ HTTP/1.1	220
2523	21.240572642	60816	192.168.1.7	192.168.1.5	80	POST /sdk/ HTTP/1.1	220
2601	21.2405721997	60820	192.168.1.7	192.168.1.5	80	GET /nmap1 HTTP/1.1	220
2656	21.363369998	60836	192.168.1.7	192.168.1.5	80	OPTIONS / HTTP/1.1	220
2691	21.375437556	60848	192.168.1.7	192.168.1.5	80	GET / HTTP/1.1	220
2744	21.394435631	60860	192.168.1.7	192.168.1.5	80	OPTIONS / HTTP/1.1	220

Select any packet and then u can see the hostname in packet details section

No.	Time	src port	Source	Destination	dst port	Info	Length
2217	21.114186884	60692	192.168.1.7	192.168.1.5	80	OPTIONS / HTTP/1.1	220
2218	21.114238801	60700	192.168.1.7	192.168.1.5	80	PROPFIND / HTTP/1.1	220
2220	21.114337194	60712	192.168.1.7	192.168.1.5	80	GET /robots.txt HTTP/1.1	220
2221	21.114437194	60714	192.168.1.7	192.168.1.5	80	PROPFIND / HTTP/1.1	220
2228	21.114567919	60740	192.168.1.7	192.168.1.5	80	GET / HTTP/1.0	220
2231	21.114619998	60754	192.168.1.7	192.168.1.5	80	OPTIONS / HTTP/1.1	220
2233	21.114637194	60762	192.168.1.7	192.168.1.5	80	GET /nmapowercheck1689717155 HTTP/1.1	220
2235	21.1146372024	60764	192.168.1.7	192.168.1.5	80	POST / HTTP/1.1	220
2459	21.229660423	60776	192.168.1.7	192.168.1.5	80	OPTIONS / HTTP/1.1	220
2520	21.240496894	60784	192.168.1.7	192.168.1.5	80	PROPFIND / HTTP/1.1	220
2521	21.240500930	60792	192.168.1.7	192.168.1.5	80	OPTIONS / HTTP/1.1	220
2522	21.240519950	60814	192.168.1.7	192.168.1.5	80	GET /dashboard/ HTTP/1.1	220
2523	21.240572642	60816	192.168.1.7	192.168.1.5	80	POST /sdk/ HTTP/1.1	220
2601	21.2405721997	60820	192.168.1.7	192.168.1.5	80	GET /nmap1 HTTP/1.1	220
2656	21.363369998	60836	192.168.1.7	192.168.1.5	80	OPTIONS / HTTP/1.1	220
2691	21.375437556	60848	192.168.1.7	192.168.1.5	80	GET / HTTP/1.1	220
2744	21.394435631	60860	192.168.1.7	192.168.1.5	80	OPTIONS / HTTP/1.1	220

```

> Transmission Control Protocol, Src Port: 60848, Dst Port: 80, Seq: 1, Ack: 1
- Hypertext Transfer Protocol
  - GET / HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
      User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/nse.html)\r\n
      Host: nanomate-solutions.com\r\n
      Connection: close\r\n
    \r\n
0000  0d 0a 55 75 05 72 2d 41 07 85 6e 74 8a 20 40 0f  : User-Agent: Mo
0001  75 65 05 0c 05 21 25 2e 08 20 25 0f 8d 70 61  : noma5/... (compu
0002  74 60 02 06 05 3b 20 4e 0d 61 70 20 63 63 72 69  : table; N map Scrl
0003  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  : pting En gine; ht
0004  74 64 62 06 67 29 45 6e 67 69 6e 65 3b 20 68 74  : tps://nm ap.org/b
0005  74 64 62 06 67 29 45 6e 67 69 6e 65 3b 20 68 74  : ook/nse.html)\r\n
0006  6f 61 6b 2f 6e 73 65 2e 68 74 6d 6c 29 8d 6a 49  : oot/nse.html)\r\n
0007  6e 65 75 74 69 6f 6e 3a 20 63 6c 6f 73 65 6d 6a  : Lutinism.com Con
0008  6e 65 63 74 69 6f 6e 3a 20 63 6c 6f 73 65 6d 6a  : nection: close\r\n
0009  0d 0a

```

Another approach is:

Using this command in terminal which is **tshark -r challenge.pcapng -Y "http.host" -T fields -e http.host**. It displays all existing Host name.

Flag: BDSEC{nanomate-solutions.com}

Follow the Path

What is the path of the Admin endpoint?

At first we need to filter out all packets which are using http protocol .

No.	Time	src port	Source	Destination	ds
4319	110.087275861	44478	192.168.1.7	192.168.1.5	
4321	110.088348012	44478	192.168.1.7	192.168.1.5	
4323	110.089390336	44478	192.168.1.7	192.168.1.5	
4325	110.090227763	44478	192.168.1.7	192.168.1.5	
4335	118.216986484	59032	192.168.1.7	192.168.1.5	
4339	118.327390233	59032	192.168.1.7	192.168.1.5	
4355	137.849415727	57046	192.168.1.7	192.168.1.5	
4359	137.997699663	57046	192.168.1.7	192.168.1.5	
4397	154.335335540	32832	192.168.1.7	192.168.1.5	
4401	155.385534011	32832	192.168.1.7	192.168.1.5	
4410	163.438123402	47140	192.168.1.7	192.168.1.5	
4415	164.495961377	47140	192.168.1.7	192.168.1.5	
4418	164.616416139	47140	192.168.1.7	192.168.1.5	
4436	182.691920708	50679	192.168.1.4	239.255.255.250	
4437	183.692650614	50679	192.168.1.4	239.255.255.250	
4438	184.693727963	50679	192.168.1.4	239.255.255.250	
4439	185.694513730	50679	192.168.1.4	239.255.255.250	

Find out admin packet and then Select any one packet of admin.

The screenshot shows a NetworkMiner capture of network traffic. A single packet is selected, highlighted with a blue border. The selected packet is a POST request to '/app/admin_panel/process_login.php' with the following details:

- Frame 4397: 727 bytes on wire (5816 bits), 727 bytes captured (5816 bits) on interface eth0, id 0
- Ethernet II, Src: PcsCompu_95:bd:54 (08:00:27:95:bd:54), Dst: PcsCompu_ec:44:ad (08:00:27:ec:44:ad)
- Destination: PcsCompu_ec:44:ad (08:00:27:ec:44:ad)
- Address: PcsCompu_ec:44:ad (08:00:27:ec:44:ad)
-0..... = LG bit: Globally unique address (factory default)
-0..... = IG bit: Individual address (unicast)
- Source: PcsCompu_95:bd:54 (08:00:27:95:bd:54)
- Address: PcsCompu_95:bd:54 (08:00:27:95:bd:54)
-0..... = LG bit: Globally unique address (factory default)
-0..... = IG bit: Individual address (unicast)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.1.7, Dst: 192.168.1.5
- Transmission Control Protocol, Src Port: 32832, Dst Port: 80, Seq: 1, Ack: 1, Len: 661
- POST /app/admin_panel/process_login.php HTTP/1.1\r\n[Export I.F. (Chat/Sequence): POST /app/admin_panel/process_login.php HTTP/1.1\r\n]
- Request Method: POST
- Request URI: /app/admin_panel/process_login.php
- Request Version: HTTP/1.1

Hex dump of the selected packet:

0000	08 00 27 ec 44 ad 08 00 27 95 bd 54 08 00 45 00	.. 'D... 'T..E..
0010	02 c9 49 fd 40 00 40 06 6a d5 c0 a8 01 07 c0 a8	.I @ @. j
0020	01 05 80 40 00 50 85 49 38 47 29 37 e7 67 80 18	..@P I 8G)7 g..
0030	01 f6 86 18 00 00 01 01 08 0a 73 31 95 be 96 69s1 ..i

Flag: BDSEC{/app/admin_panel}

Root Access

How did the attacker got root access?

The terminal session shows the following steps to gain root access:

- Initial password entry: Password: tareq@manmate
- Authentication failure message: su: Authentication failure
- Switching to root shell: su -
- Running 'id' command: id
- Output of 'id': uid=0(root) gid=0(root) groups=0(root)
- Attempting to set terminal process group: bash: cannot set terminal process group (5821): Inappropriate ioctl for device
- Checking current working directory: pwd
- Listing files in the current directory: ls
- Changing directory to /home: cd /home
- Listing files in /home: ls
- Switching to root user: su -
- Running 'id' again to confirm root status: id

```
Password: tareqbnanomat
su: Authentication failure
[User@john-lab ~]$ /opt/lampp/htdocs/app$ sudo vim -c ':!/bin/sh'
[User@john-lab ~]$ vim -c ':!/bin/sh'
Vim: Warning: Output is not to a terminal
Vim: Warning: Input is not from a terminal
[?1849h,[22;0t,[~4;2m,[?1h.=,[?2004h,[1;24r,[?12h,[?12l,[22;2t,[22;1t,[27m,[29m,[m,[H,[23,[?251,[24;1m:[/bin/sh,[?2004l,[?2004l,[?1l.>,[?25h,[>4;m,[?1049l,[23;0;9t
[User@john-lab ~]$ root
[User@john-lab ~]$ whoami
root
[User@john-lab ~]$ id
uid=0(root) gid=0(root) groups=0(root)
[User@john-lab ~]$ /bin/bash
bash: warning: set terminal process group (5821): Inappropriate ioctl for device
bash: no job control in this shell
[User@john-lab ~]$ ./.root@john-lab: /opt/lampp/htdocs/app.root@john-lab:/opt/lampp/htdocs/app$ ls
admin.php
assets.php
dashboard.php
includes.php
index.php
login.php
notes.php
register.php
[User@john-lab ~]$ ./.root@john-lab: /opt/lampp/htdocs/app.root@john-lab:/opt/lampp/htdocs/app$ cd /home
[User@john-lab ~]$
```

Flag: BDSEC{sudo_vim_-c_':!/bin/sh'}

Root Flag

What is the root flag?

```
media
mnt
opt
proc
root
run
sbin
snap
srv
swapfile
sys
tmp
usr
var
[User@john-lab ~]$ ./.root@john-lab: /# cd /root
[User@john-lab ~]$ cd /root
[User@john-lab ~]$ ls
is
flag
snap
[User@john-lab ~]$ file flag
file flag
flag: ASCII text
[User@john-lab ~]$ cat flag
cat flag
You are supposed to get this flag at the end of this networking category. If you solved all the challenges, you
Here's a reward for you.
- Y0u_NaILeD_IT_HaCkEr
- Keep Hacking & Make System Safer
- See you in next event pal... :D

[User@john-lab ~]$ cd /opt
[User@john-lab ~]$ /opt.root@john-lab:/opt# cd /lampp/app
```

Flag: BDSEC{Y0u_NaILeD_IT_HaCkEr}