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}

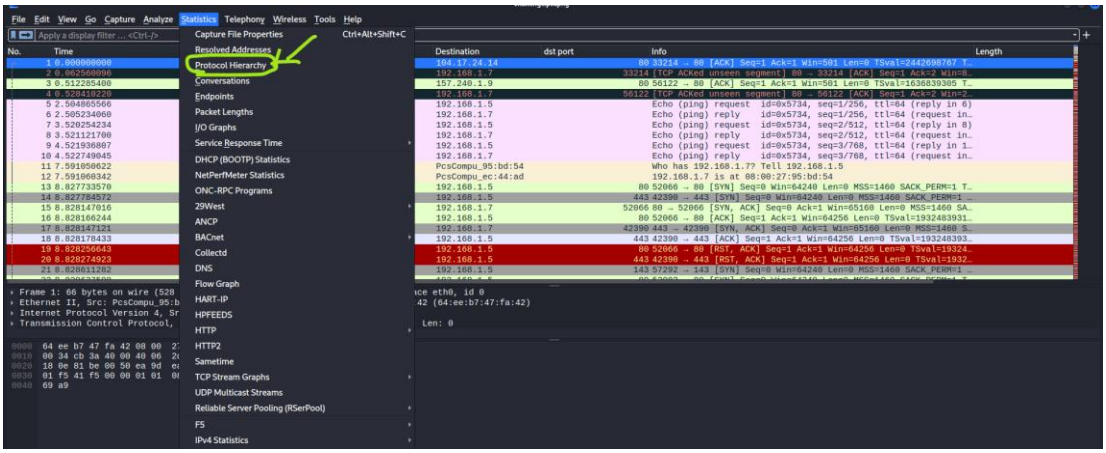
IP Addr

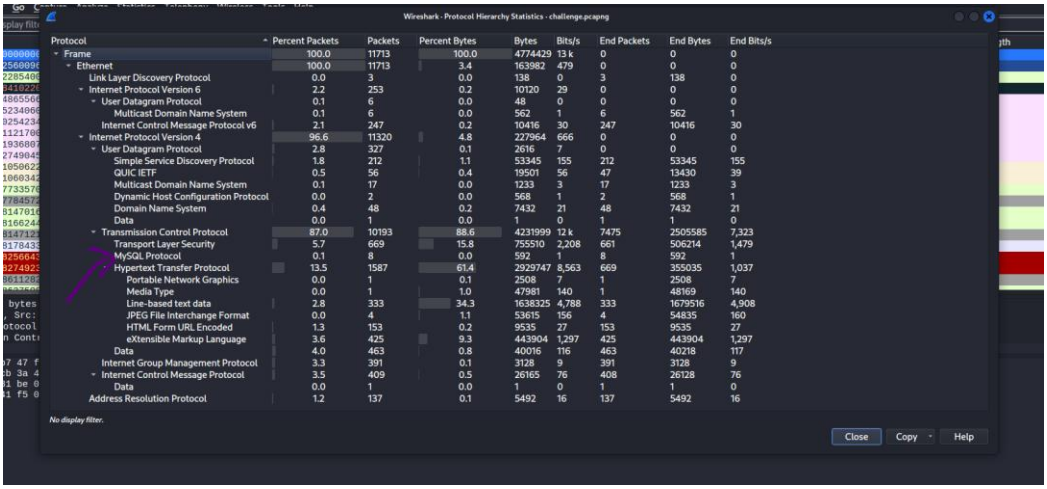
What is the server & attacker ip?

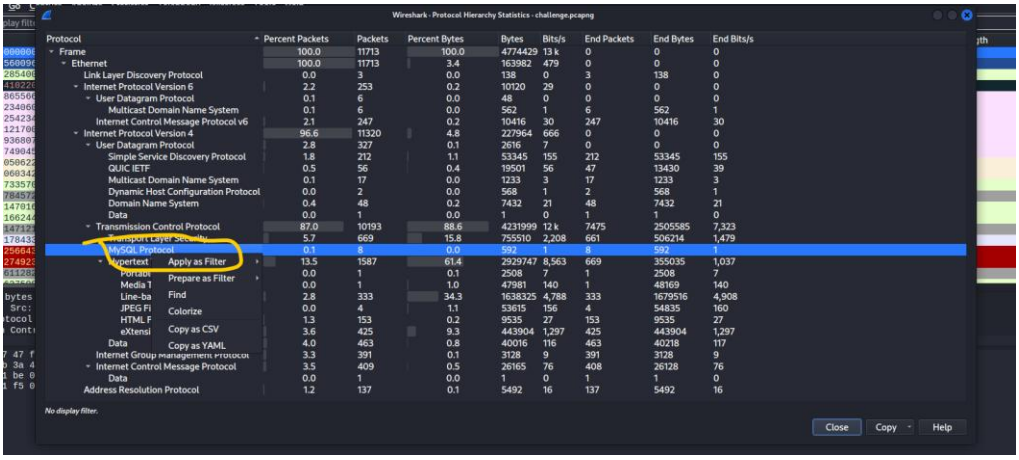
Download the challenge.zip and unzip this in your directory unzip challenge.zip and open challenge.pcapng with wireshark using wireshark challenge.pcapng .

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.

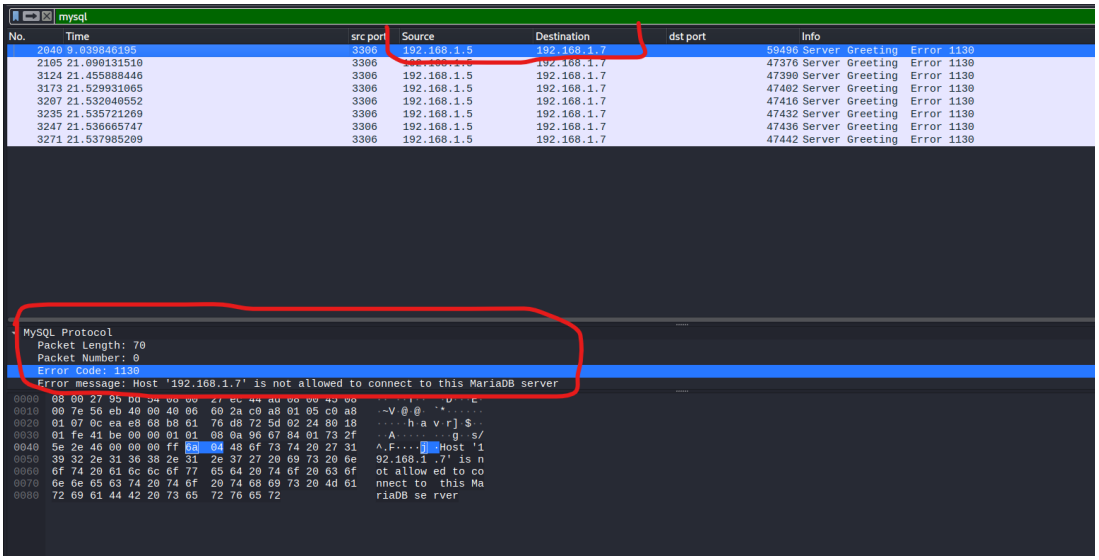
Go to **Statistics > Protocol Hierarchy > My SQL Protocol** and apply as selected filter





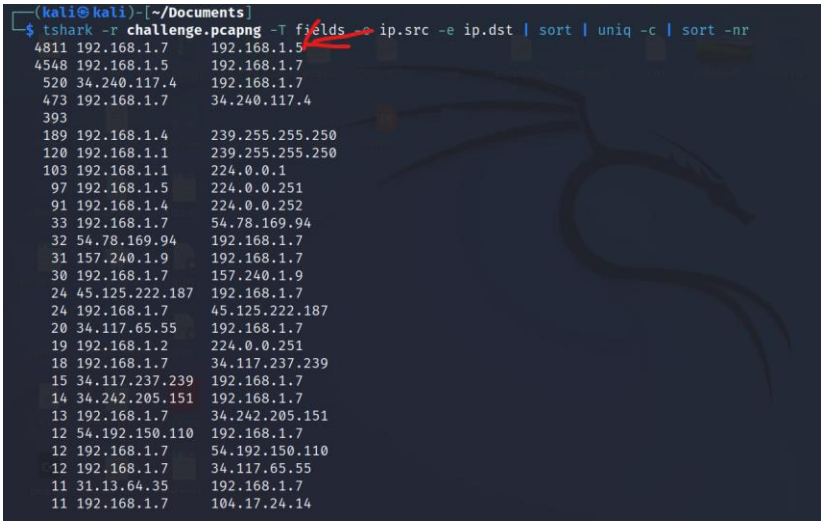


click on any packet and as you can see server's response to connecting host, 192.168.1.7 is our attacker's ip



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



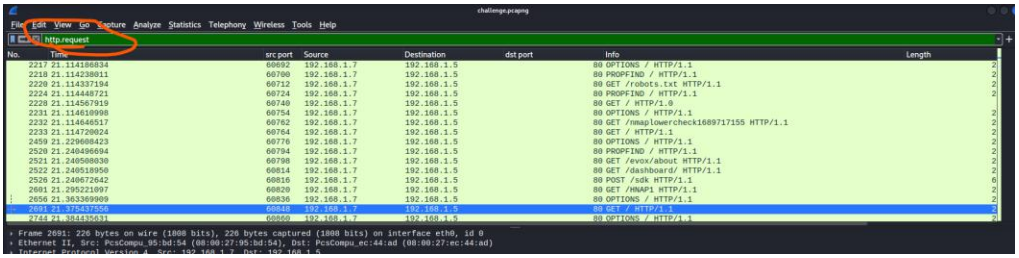
The attacker IP 192.168.1.7 communicated extensively (4,811 times) with internal IP 192.168.1.5. This was the most active session in the capture file.So I think this is flag bcz of their Suspicious behavior.

Flag: BDSEC{192.168.1.5_192.168.1.7}

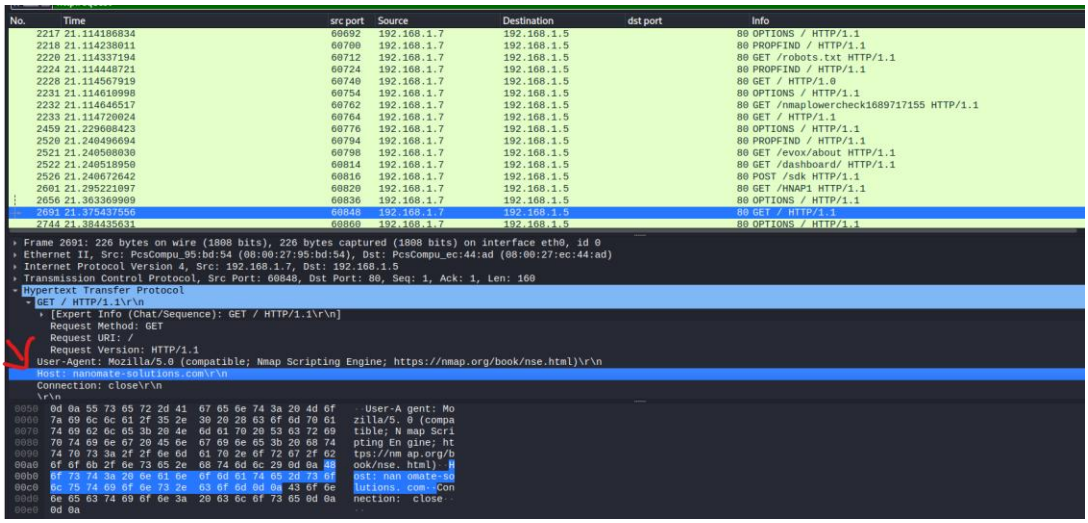
HostName

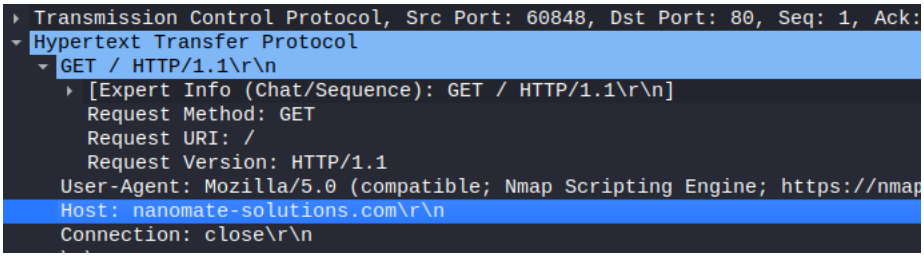
What is the host name of the web server?

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



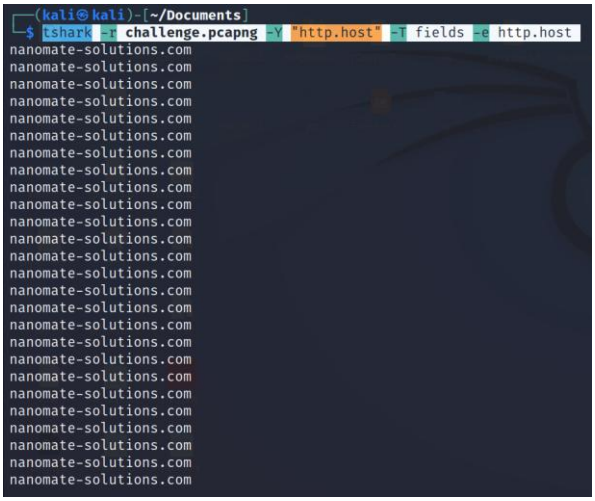
Select any packet and then u can see the hostname in packet details section





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.

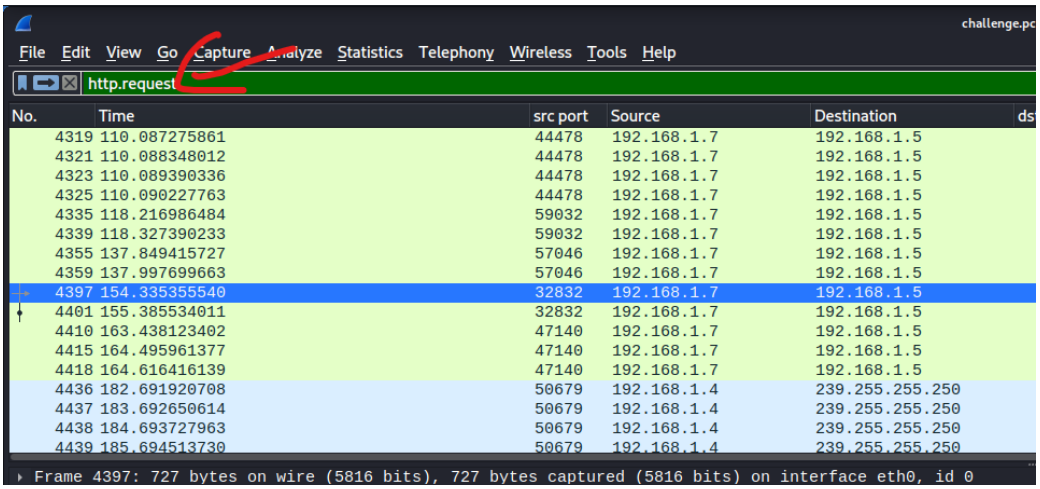


Flag: BDSEC{nanomate-solutions.com}

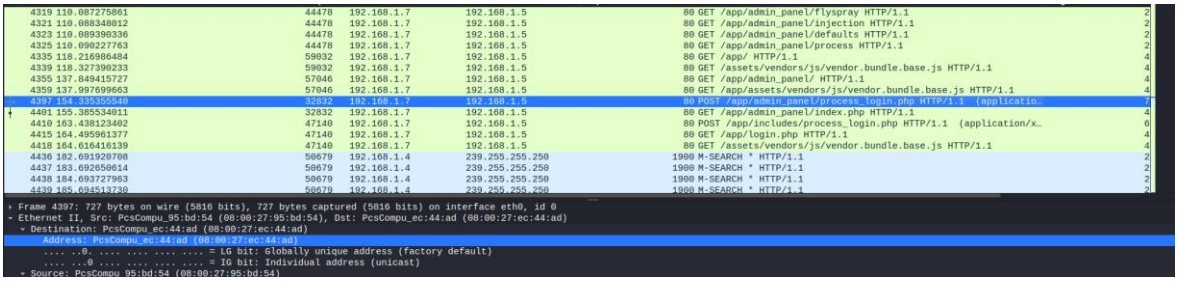
Follow the Path

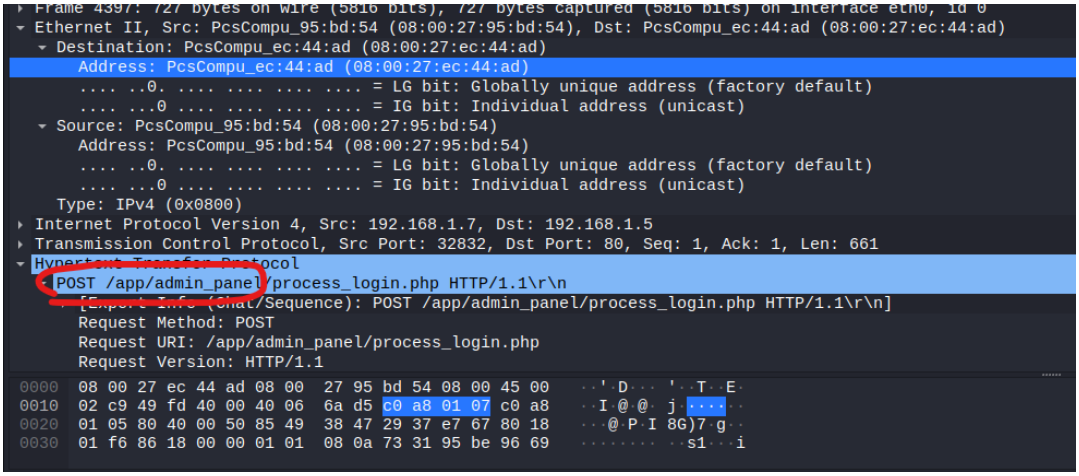
What is the path of the Admin endpoint?

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



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

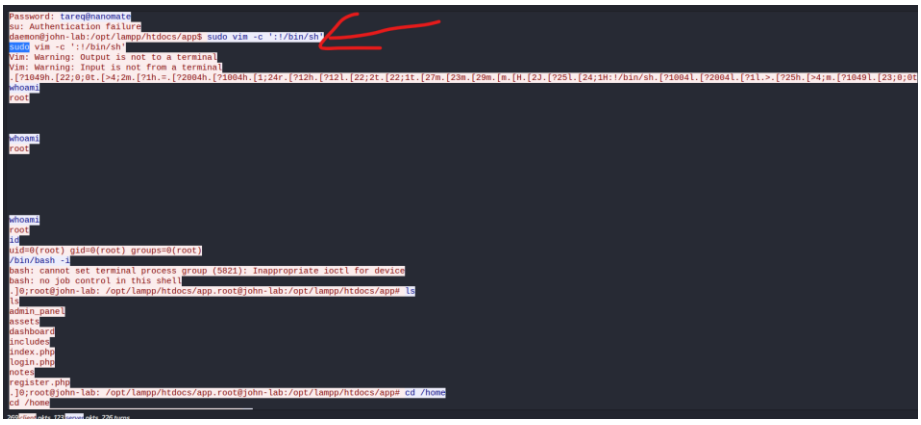




Flag: BDSEC{/app/admin_panel}

Root Access

How did the attacker got root access?



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

Root Flag

What is the root flag?

Flag: BDSEC{Y0u_NaILeD_IT_HaCkEr}