a2

December 9, 2022

1 Task A2 - Identifying the attacker - (Computer Forensics, Packet Analysis)Points: 40

1.1 Problem Statement

Using the timestamp and IP address information from the VPN log, the FBI was able to identify a virtual server that the attacker used for staging their attack. They were able to obtain a warrant to search the server, but key files used in the attack were deleted.

Luckily, the company uses an intrusion detection system which stores packet logs. They were able to find an SSL session going to the staging server, and believe it may have been the attacker transferring over their tools.

The FBI hopes that these tools may provide a clue to the attacker's identity

Downloads:

- Files captured from root's home directory on the staging server (`root.tar.bz2`)
- PCAP file believed to be of the attacker downloading their tools (`session.pcap`)

1.2 What to do

What was the username of the account the attacker used when they built their tools?

1.3 My solution

1.3.1 Dependencies

- Wireshark

First, analyze the type of the given file, `session.pcap`.

[1]:
```
%%bash
file ./data/a2/session.pcap
```

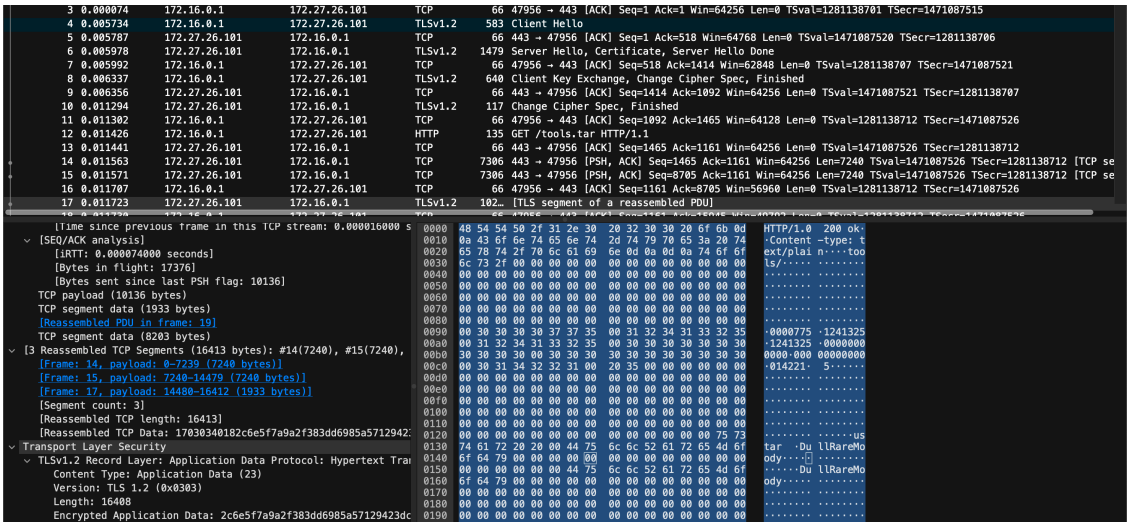
```
./data/a2/session.pcap: pcap capture file, microsecond ts (little-endian) -
version 2.4 (Ethernet, capture length 65535)
```

So, the file is a `pcap` file as the extension shows.

Next, open `pcap` using `Wireshark`.

After opening, use `.cert.pem` file to decrypt it. Go to `Preferences -> RSA keys -> Add new keyfile`, add `.cert.pem` as a key, and restart `Wireshark`.

You can find a weird string, `DullRareMoody` in `Client Hello` ,which is an answer.



You've got the flag.


I COMPLETED
TASK
A2
OF THE
CODEBREAKER
CHALLENGE
2022
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA