

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.

```
3 0.000074 172.16.0.1 172.27.26.101 TCP 66 47956 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1281138701 TSecr=1471087515
4 0.005734 172.16.0.1 172.27.26.101 TLSv1.2 583 Client Hello
5 0.005787 172.27.26.101 172.16.0.1 TCP 66 443 → 47956 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=1471087520 TSecr=1281138706
6 0.005978 172.27.26.101 172.16.0.1 TLSv1.2 1479 Server Hello, Certificate, Server Hello Done
7 0.005992 172.16.0.1 172.27.26.101 TCP 66 47956 → 443 [ACK] Seq=518 Ack=1414 Win=62848 Len=0 TSval=1281138707 TSecr=1471087521
8 0.006337 172.16.0.1 172.27.26.101 TLSv1.2 640 Client Key Exchange, Change Cipher Spec, Finished
9 0.006356 172.27.26.101 172.16.0.1 TCP 66 443 → 47956 [ACK] Seq=1414 Ack=1092 Win=64256 Len=0 TSval=1471087521 TSecr=1281138707
10 0.011294 172.27.26.101 172.16.0.1 TLSv1.2 117 Change Cipher Spec, Finished
11 0.011302 172.16.0.1 172.27.26.101 TCP 66 47956 → 443 [ACK] Seq=1092 Ack=1465 Win=64128 Len=0 TSval=1281138712 TSecr=1471087526
12 0.011426 172.16.0.1 172.27.26.101 HTTP 135 GET /tools.tar HTTP/1.1
13 0.011441 172.27.26.101 172.16.0.1 TCP 66 443 → 47956 [ACK] Seq=1465 Ack=1161 Win=64256 Len=0 TSval=1471087526 TSecr=1281138712
14 0.011563 172.27.26.101 172.16.0.1 TCP 7306 443 → 47956 [PSH, ACK] Seq=1465 Ack=1161 Win=64256 Len=7240 TSval=1471087526 TSecr=1281138712 [TCP se
15 0.011571 172.27.26.101 172.16.0.1 TCP 7306 443 → 47956 [PSH, ACK] Seq=8705 Ack=1161 Win=64256 Len=7240 TSval=1471087526 TSecr=1281138712 [TCP se
16 0.011707 172.16.0.1 172.27.26.101 TCP 66 47956 → 443 [ACK] Seq=1161 Ack=8705 Win=56960 Len=0 TSval=1281138712 TSecr=1471087526
17 0.011723 172.27.26.101 172.16.0.1 TLSv1.2 102. [TLS segment of a reassembled PDU]
18 0.011728 172.16.0.1 172.27.26.101 TCP 66 443 → 47956 [ACK] Seq=1465 Ack=1161 Win=64256 Len=0 TSval=1471087526 TSecr=1281138712 [TCP se

[Time since previous frame in this TCP stream: 0.000016000 s]
[SEQ/ACK analysis]
  [RIT: 0.000074000 seconds]
  [Bytes in flight: 17376]
  [Bytes sent since last PSH flag: 10136]
  TCP payload (10136 bytes)
  TCP segment data (1933 bytes)
  [Reassembled PDU in frame: 19]
  TCP segment data (6203 bytes)
  [3 Reassembled TCP Segments (16413 bytes): #14(7240), #15(7240),
  [Frame: 14, payload: 0-7239 (7240 bytes)]
  [Frame: 15, payload: 7240-14479 (7240 bytes)]
  [Frame: 17, payload: 14480-16412 (1933 bytes)]
  [Segment count: 3]
  [Reassembled TCP length: 16413]
  [Reassembled TCP Data: 17030340182c6e5f7a9a2f383dd6985a5712942dc]
  Transport Layer Security
    TLSv1.2 Record Layer: Application Data Protocol: Hypertext Tra
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 16488
    Encrypted Application Data: 2c6e5f7a9a2f383dd6985a5712942dc
```

You've got the flag.

