## Category:

Network Forensics

## Name:

To the “future” direction - 1

## Message:

Now you have received a PCAP file according to Mirai malware. The packets are taken from an infected host. Find the first packet related to the command & control server. The flag template is “CSG_FLAG{<IP>:<port>:<TCP sequence number in hex-big endian without ‘0x’>}”. Ex. If the command & control server is “10.192.0.18:3333” and the first TCP sequence number of the packet is “0xbeef1337” (be ef 13 37), the flag should be “CSG_FLAG{10.192.0.18:3333:beef1337}”. You can easily find a related source code from the Internet. Note that we assume the Mirai variant uses Mirai original protocol.

## Objective:

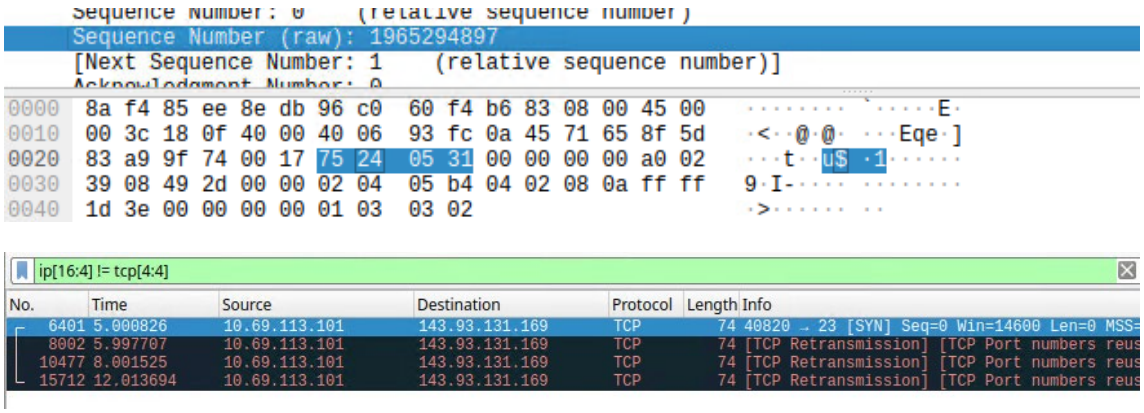
You can learn how you can use open-source information to network forensics.

## Instructions:

Your task is to reveal the command & control (C&C) server of a Mirai variant from packet capture. To conduct the analysis, you can check Mirai’s source code from GitHub (https://github.com/jgamblin/Mirai-Source-Code), or an article of its detailed analysis from many security blogs (such as https://medium.com/@cjbarker/mirai-ddos-source-code-review-57269c4a68f) and many academic papers (https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf) .

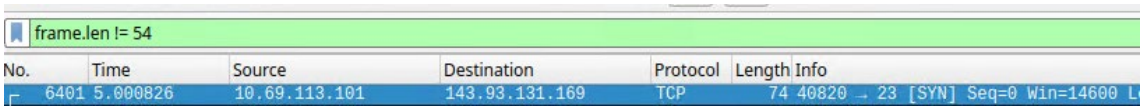
The communication packets to C&C server were hidden within an avalanche of scanning packets for virus outbreak. To get a flag, you need to check TCP stream number to get the flag. As many articles pointed out, every scanning packet from Mirai has a TCP sequence number which equal to the destination IP address. So, you can find the packets related to C&C communication by removing such packets. The 4-byte sequence of destination address is starting from offset 16 of its IP header, and the 4-byte TCP sequence number is starting from offset 4 of its IP header. So, using WireShark you can filter out if both are equal.

Its TCP sequence number is 0x75240531 (in big endian).




Then the flag is CSG_FLAG{143.93.131.169:23:75240531}

Different solution: You can find all of the SYN packet related to scan are 54 bytes. So, you can find anormal packets by filtering them out. But in actual case it is not the solution always.




## References:

Documents

Mirai-Source-Code https://github.com/jgamblin/Mirai-Source-Code

Mirai (DDoS) Source Code Review https://medium.com/@cjbarker/mirai-ddos-source-code-review-57269c4a68f

Understanding the Mirai Botnet

https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

Tools

WireShark https://www.wireshark.org/