Cybersecurity
Progress. Protected.

Kennisbank > Diagnostics > Using tcpdump on a MacOS

Using tcpdump on a MacOS

Steef | ESET Nederland - 2023-03-08 - Reacties (0) - Diagnostics

When troubleshooting network related issues on MacOS, tcpdump is the linux equivalent of wireshark. Tcpdump is available by default on MacOS.

Use the following command in Terminal to capture and save the packets in a file:

```
sudo tcpdump  -vv -w  FILENAME.pcap -i any
```

Fill in the password.
Reproduce the issue, so it is captured in the tcpdump log.

To cancel the capture press:

```
Ctrl + c
```

To compress the output file:

```
tar -cvzf FILENAME.tar.gz FILENAME.pcap
```

Please send the compressed output file FILENAME.tar.gz to ESET Support via Techcenter.

Gerelateerde inhoud

- Create a full memory dump of a VMware virtual machine
- How do I generate a memory dump manually?
- How to create a Wireshark log
- Run the Info_get.command on a Linux machine and send the logs to ESET Technical Support
- How do I use ESET Log Collector?