Recommended Software for network analysis

Christopher Adam Craig

Several of you asked about software we may be using soon. For the network analysis assignment that will be assigned on Tuesday the following software could be useful (all of these are free):

Network analysis:

- tcpdump (linux, command line)
- wireshark (linux, GUI)
- NetworkMiner (Windows, GUI)

Object extraction:

- tcpflow (linux, command line)
- ChaosReader (linux, command line)
- wireshark (linux, GUI)
- NetworkMiner (Windows, GUI)

Metadata extraction:

- Suricata (linux)
- Bro (linux)
- nfcapd (linux)
- SiLK (linux)

You won't need all of these. If you want to learn a couple in depth you would probably get the most out of Suricata (because it can do metadata extraction and IDS signatures) and either Wireshark or NetworkMiner (because they can do full packet analysis, protocol decoding, and object extraction).

If you want to download a full VM that has stuff already configured, I would recommend SecurityOnion, which comes with Bro, Suricata, tcpdump, wireshark, and I think tcpflow already built in.

Search entries or author

Unread

Reply