NetworkMiner

NetworkMiner is an open source Network Forensics & Analysis Tool (NFAT) for Windows (But also works in Linux, Mac, FreeBSD)

- can be used as a passive network sniffer/packet capturing tool to detect OS/sessions/hostnames/open ports etc. without putting any traffic on the network

- can parse PCAP files for offline analysis and to regenerate/reassemble transmitted files and certificates.

- Context of captured hosts like their IP, MAC, hostnames, OS
- List of potential attack indicators or anomalies like traffic spikes or port scans
- Used to perform the potential attack like nmap

Three main data types investigated:

- Live traffic
- Traffic captures
- Log Files

Traffic sniffing : It can intercept the traffic, sniff it, and collect and log packets that pass through ~~net w~~ the network

Parsing PCAP files : parse pcap files and show the content of the packets in detail

Protocol Analysis : identify the used protocol from the parsed pcap file

OS ~~fingerprint~~ fingerprinting : identify the used OS by reading the pcap file. This strongly relies on Satori and p0f

Satori and p0f : - They watch real traffic from the connection
- extracts "fingerprint features" from what they observe
- They compare those features to a signature database and output the closest match

- p0f focuses heavily on TCP/IP stack behavior (SYN/SYN-ACK, TTL, window size, MSS, TCP...)
- Satori can use more protocol clues (DHCP, HTTP, TLS)

File extraction : - extract images, HTML, files and emails from the parsed pcap file

Credential grabbing : - extract credential from the parsed pcap file.

Cleartext keyword parsing : - extract cleartext keywords and strings from the parsed pcap file.

Operating Modes:

- Sniffer Mode : (not recommended)
- Packet Parsing / Processing : parse traffic captures to have a quick overview and information on the investigated capture

Network Miner

Pros	Cons
- OS fingerprinting	- Not useful in active sniffing
- Easy file extraction	- Not useful for large pcap
- Credential grabbing	- Limited filtering
- Cleartext keyword parsing	- Not built for manual traffic investigation
- Overall overview	

NetworkMiner : Quick overview, traffic mapping, and data extraction

- have OS fingerprint feature
- doesn't have Analysis
- have host categorisation ~~filter~~ feature