Workshop 5

Internet Protocol Analysis

Sponsored by:

accenture

Internet Protocol Analysis

- Use of Packet analyzers to to capture, view and understand internet protocols

- Internet Protocol
  - Conceptual model and communication protocol used by the Internet
  - Commonly known as the TCP/IP

Aim

- Gathering raw data from the network

Result

- Understanding who is talking to who
- Types of traffic in the network
- Statistical Analysis

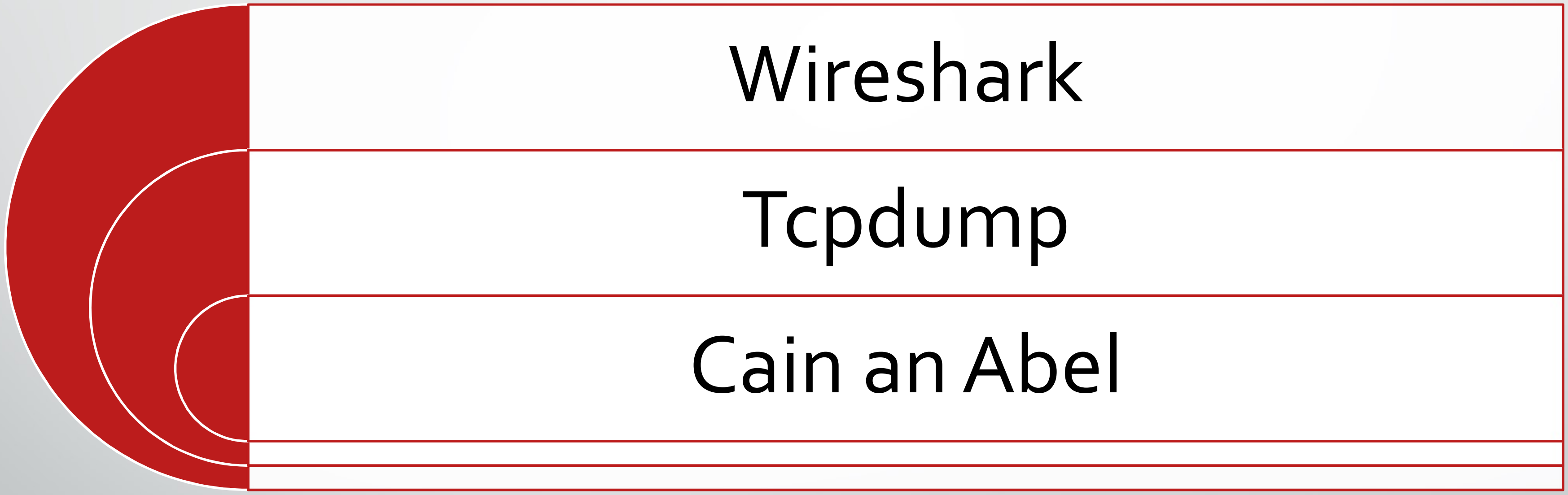
Usage

- Troubleshooting and capacity management
- Passive nature allows to monitor without detection

Packet Analyzers

- Also known as packet/network sniffers
- Intercepts and logs traffic on a network
- Data is stored as ‘Packets’

Notable Packet Analyzers

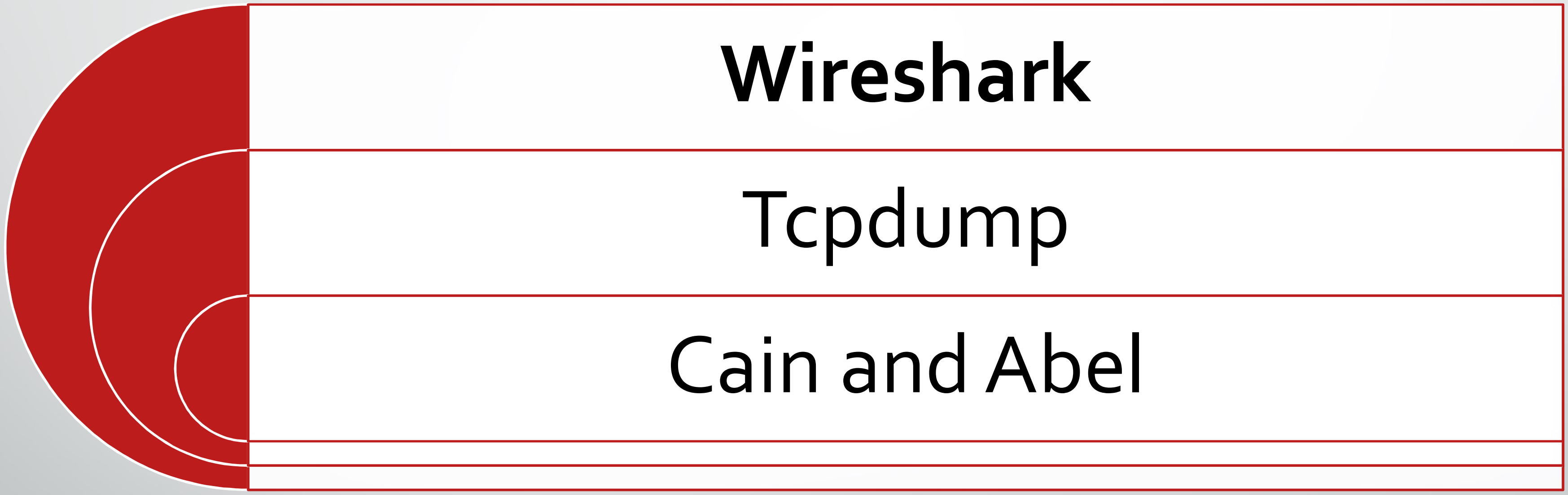


Wireshark

Tcpdump

Cain an Abel

Notable Packet Analyzers



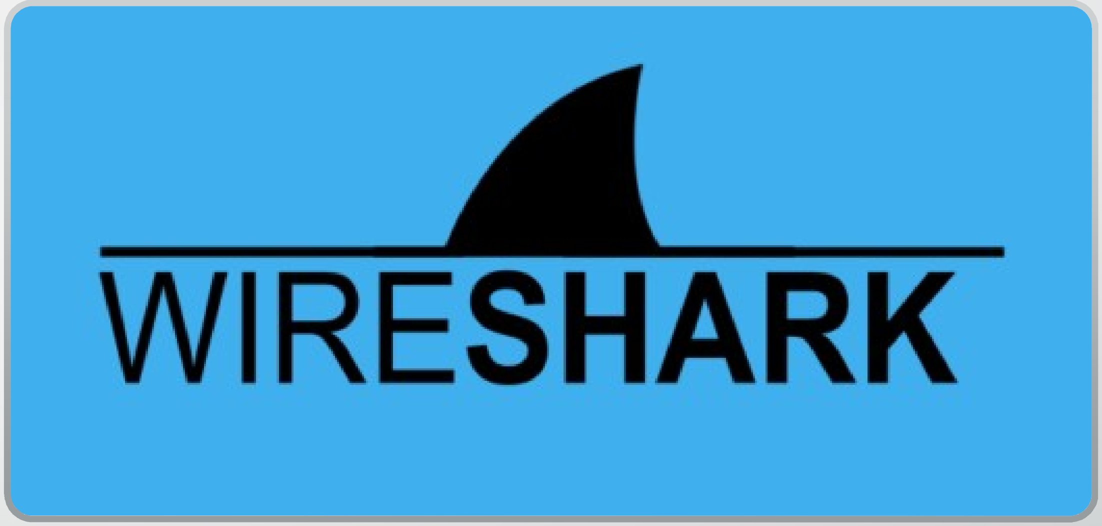
Wireshark

Tcpdump

Cain and Abel

Key Features:

- Deep Inspection of protocols
- Uses pcap
  - Data saved in ***.pcap*** format
- Can operate in Promiscuous mode



Wireshark Allows Us To:

- Capture live data from Ethernet, IEEE 802.11, PPP, loopback etc.
- VoIP calls can be detected and media can be played (Proper Encoding)
- Raw USB traffic can be captured

Promiscuous Mode

- Feature of a NIC or WNIC
- Allows to pass all traffic that takes place in a router or Network

Handy Resources

- Wikiversity – Internet Protocol Analysis
- Display Filters Cheat Sheet
  - http://packetlife.net/media/library/13/Wireshark_Display_Filters.pdf
- Top 15 Capture Filters:
  - https://www.cellstream.com/reference-reading/tipsandtricks/379-top-10-wireshark-filters-2
- Top Display Filters:
  - https://insights.profitap.com/14-powerful-wireshark-filters-to-use

Let the hacking begin!

Root-me.org – Network Challenges

Immersive Labs – Tools/ Packet Analysis Tools