Wireshark

IT EDUCATION CENTRE

Wireshark basics

Wireshark overview
L2-7 overview
Wireshark and Pcap library installation
Basic capture and filters
Layers dissection
UDP Specifications and Fragmentation capturing
Capture save options

Filters

Display filter language
Create filters to capture by MAC/IP/Application
Combine filters by using operators
Looking for bytes values
Detect applications and network protocols
Following streams and reassembling data
Normal UDP conversation
Normal TCP conversation
Basic capture filters
Colorize traffic

Statistics and Analysis

Statistics
Wireshark statistics view
Most active: IP addresses, conversations, endpoints, wireless statistics
I/O graph
Detect latency with combined statistics
HTTP and FTP conversation
TCP latency/duplicates ack/retransmit

IT EDUCATION CENTRE

Wireshark expert info

TCP retransmit
Previous segment lost
Ack lost
Segment not captured or not seen
Duplicate ack
Out of order segment
Windows full

Analysis

Traffic graph
Coloring and viewing basic I/O graphs
Use graphs to view trends
Special graphs: round trip times, throughput
TCP graph sequence numbers and windowing
Terms in network analysis
Latency, slowness, packet loss, dead time segment
Identify client server path delays(full analysis)
Attack detection

TCPDUMP and Deep conversation analysis

TCPDUMP
How to use
Syntax and filters
Smart optimization
Play with buffers
Ways to save capture files(ASCII, libcap format) with minimum overhead
tips and tricks

Deep conversations analysis

HTTP payload structure
HTTP full session analysis and troubleshooting
HTTPS full session analysis and troubleshooting
RTSP and RTP full session analysis and troubleshooting
Security, Capture filters and build dissector

IT EDUCATION CENTRE

Security

Hosts scan detection
Ports scan detection TCP and UDP
ICMP probe detection
Hands-on:
Scanning and discover it using NMAP and Wireshark

Detect denial of service attack (DOS and DDOS)

Analyzing suspicious traffic
Malformed packets
How to inject packets to network and simulate required scenario

Capture filter

LIBCAP capture filter syntax
Filter host, mac
Filter by payload
Combine filters to match TCP flags

Build dissector

How dissector works
Dissector language
Dissect new protocol “My Packet”
Add headers information

IT EDUCATION CENTRE