

SPPU-BE-COMP-CONTENT - KSKA Git

Q1) What should I look for in a Wireshark Capture?

- ANS. When analyzing a Wireshark capture, you should look for the following:
- (1) Source and Destination IP Address
 - To identify who is communicating with whom.
 - Helps to detect unknown connection i.e. unknown source or destination.
 - (2) Protocols Used
 - Checks whether the traffic complies with TCP, UDP, ICMP, etc.
 - Suspicious protocols may indicate attacks.
 - (3) Port Numbers
 - Inspecting the open ports to identify unexpected traffic to the non-standard ports.
 - (4) Un-usual traffic Patterns
 - Sudden spikes, repeated re-transmission, or excessive broadcast packets can indicate attacks.
 - (5) Un-Encrypted Sensitive Data
 - Check if passwords, emails or personal data are being sent in plain-text, which would indicate MITM Attack.
 - (6) Suspicious Payloads
 - Inspecting packet content for malicious signatures can allow us to identify source of attack.

Q2) How do you Analyze Packet Captures?

ANS. Following are the steps to Analyze the Packet Captures:-

SPPU-BE-COMP-CONTENT - KSKA Git

(1) Open the Capture File.

- Load the .pcap or .pcapng File into Wireshark.
- It is good practice to stop capturing before beginning the Detailed Analysis.

(2) Check Overview Statistics.

- Use Statistics → Summary to look at total packets, duration, average packet size, etc.
- Break down traffic by protocol hierarchy which helps you understand what kind of traffic are in this capture.

(3) Identify the Key Conversation.

- Navigate to Statistics → Conversation/Endpoints to see which IP, MAC Address, or ports are communicating most.

(4) Examine Suspicious Packets.

- Click on individual packets to view packet list, details.
- Look for Anomalies like retransmission, suspicious Payloads.

(5) Document Findings:

- Note down the suspicious IP's, ports or Anomalies.
- Export Filtered packets captures for reporting on deeper Forensics Investigation.

CONCLUSION:-

→ Hence, We used Wireshark tool to perform packet Analysis and Vulnerability Assessment.