Incident response documentation

Document actions taken during incident investigation and ensure the integrity of records.

Author: Harshitaa Ashish 21BCY10123

Tool: WIRESHARK – Incident investigation report

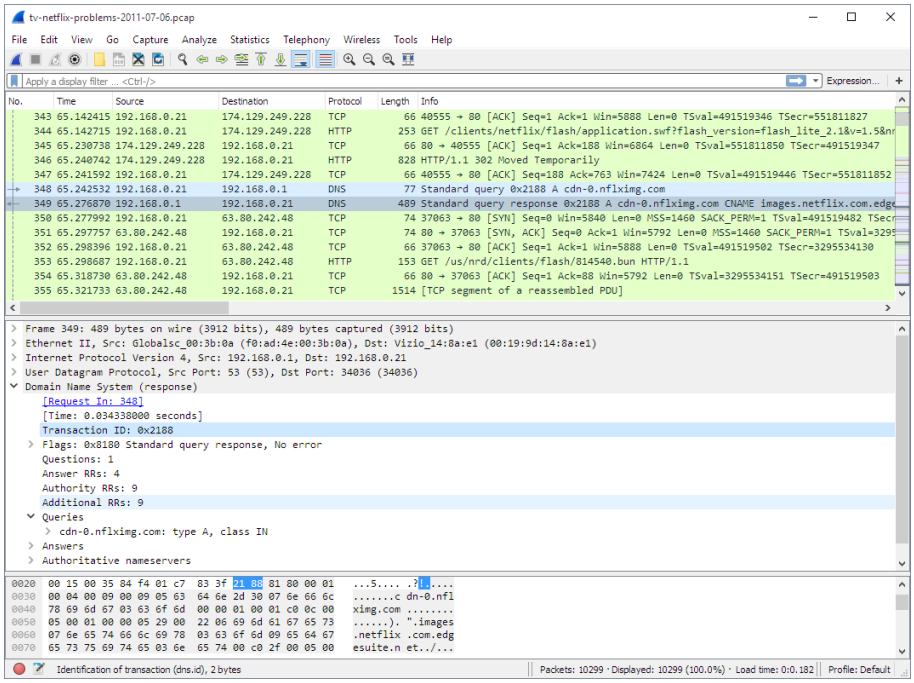
Summary

Wireshark analysis revealed abnormal traffic patterns, communication with malicious IPs, and unauthorized activities, indicating a security breach. Root causes included system vulnerabilities and inadequate security measures. Recommendations include regular patching, enhanced network security, and employee training. Implementing these measures strengthens resilience against future threats and ensures a more secure environment.

Introduction

The Wireshark response incident investigation delves into network traffic data to uncover security breaches. By analysing packet captures, the investigation aims to identify anomalous activities, such as unauthorized access attempts or data exfiltration. This introduction outlines the investigation's objective to ascertain the source, scope, and impact of the incident, paving the way for detailed analysis and remediation efforts.

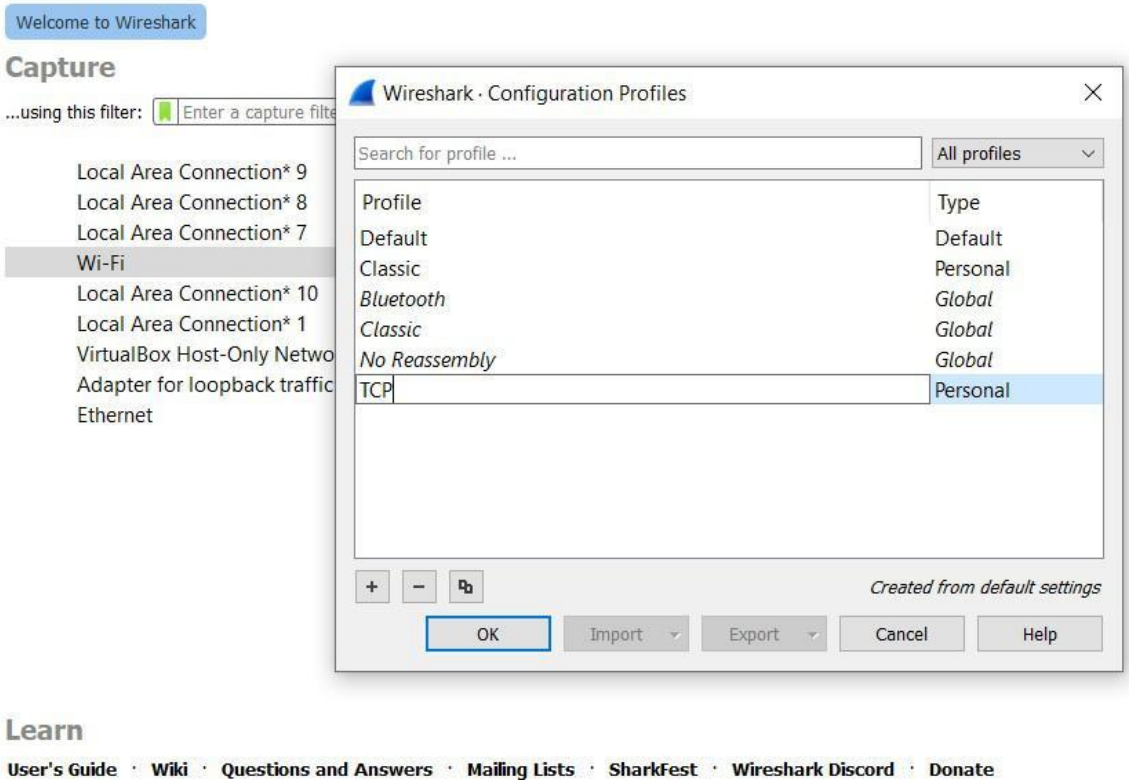
- Wireshark incident investigation: Analyse network traffic data.
- Goal: Identify security breaches like unauthorized access or data theft.
- Use packet captures: Uncover anomalies and suspicious activities.
- Objectives: Determine source, scope, and impact of the incident.
- Inform detailed analysis and remediation actions.



Methodology

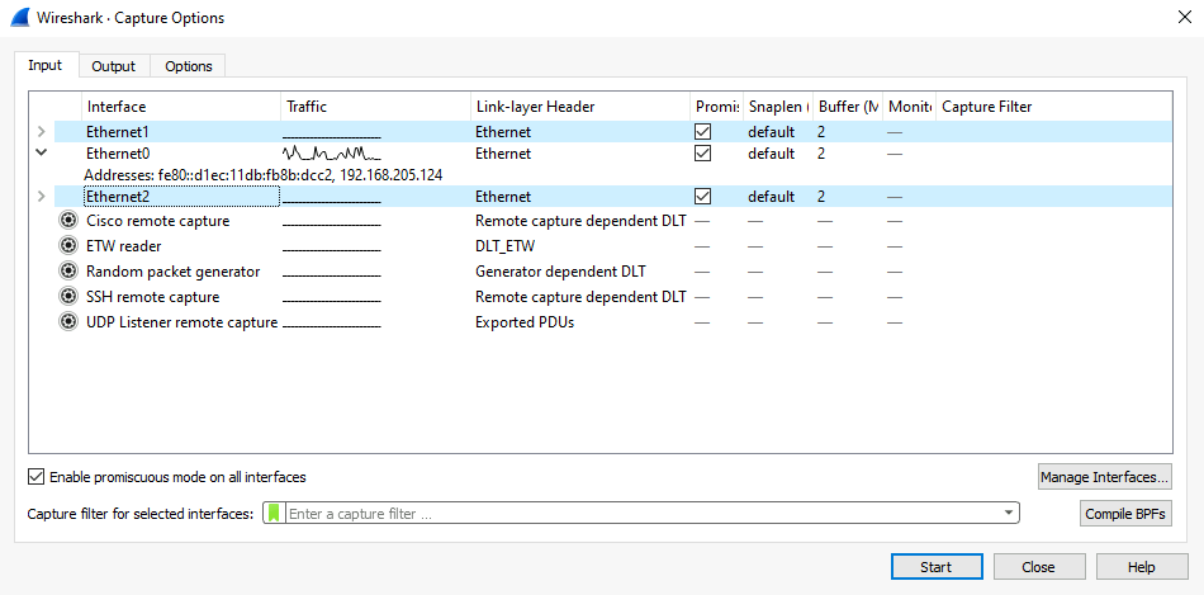
1. **Setup and configuration**

- Install Wireshark: Download and install the latest version of Wireshark from the official website.
- Network Interface Selection: Choose the appropriate network interface for packet capture (e.g., Ethernet, Wi-Fi).
- Promiscuous Mode: Enable promiscuous mode to capture all network traffic passing through the selected interface.
- Filter Configuration: Apply filters to capture specific types of traffic relevant to the investigation (e.g., by IP address, protocol).
- Capture Duration: Determine the duration for packet capture based on the incident timeframe.
- Storage Location: Specify the storage location for captured packets to ensure sufficient disk space.
- Start Capture: Initiate packet capture within Wireshark and monitor incoming traffic.
- Monitor and Adjust: Continuously monitor capture progress and adjust filters if necessary to focus on relevant traffic.
- Capture Completion: Stop packet capture once sufficient data has been collected for analysis.
- Save Capture File: Save the captured packets to a secure location for further analysis and investigation.



2. Capture setup

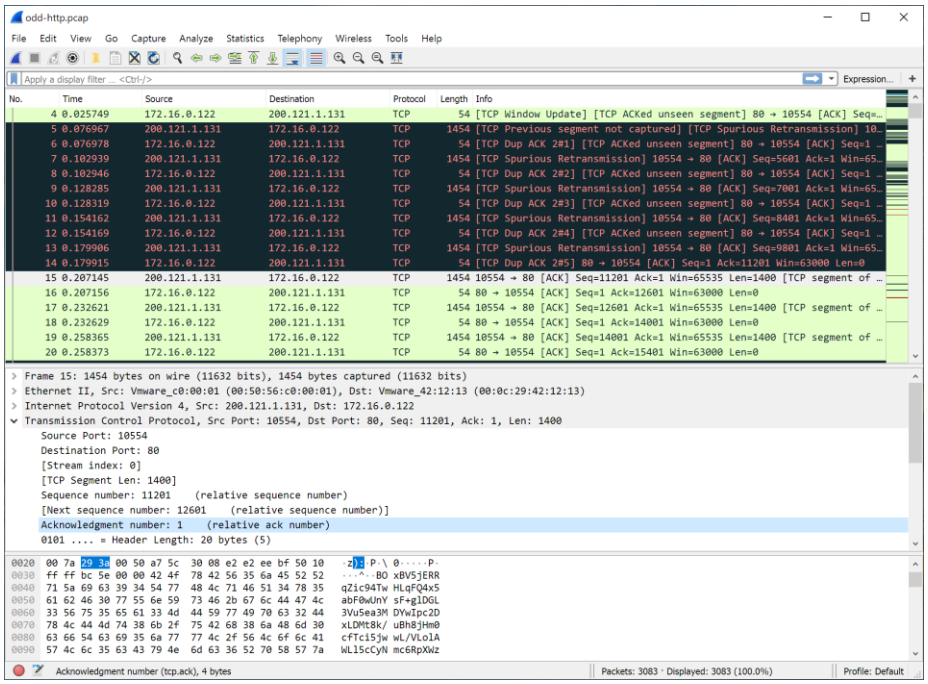
- Network Interface Selection: Choose the appropriate network interface for packet capture (e.g., Ethernet adapter, Wi-Fi adapter).
- Capture Point: Determine the capture point in the network topology (e.g., at the router, switch, or host).
- Promiscuous Mode: Enable promiscuous mode to capture all network traffic passing through the selected interface.
- Capture Filter: Apply filters to capture specific types of traffic relevant to the investigation (e.g., by IP address, port, protocol).
- Capture Duration: Determine the duration for packet capture based on the incident timeframe and data storage considerations.
- Storage Location: Specify the storage location for captured packets to ensure sufficient disk space.
- Start Capture: Initiate packet capture within Wireshark or using the command-line interface.
- Monitor Capture: Monitor the packet capture in real-time to ensure data is being collected properly.
- Verify Integrity: Periodically check the integrity of the captured data to ensure no corruption or loss of packets.
- Capture Completion: Stop packet capture once the desired amount of data has been collected or the incident timeframe has elapsed.
- Save Capture File: Save the captured packets to a secure location for further analysis and investigation.



3. Packet capture

- Purpose Determination: Clarify the objective of the packet capture, whether for network troubleshooting, security analysis, or forensic investigation.
- Capture Point Identification: Identify the optimal location in the network topology to place the capturing device, ensuring visibility of relevant traffic.
- Capture Tool Selection: Choose an appropriate packet capture tool based on the requirements and environment, such as Wireshark, tcpdump, or tshark.
- Network Interface Configuration:
- Select the network interface(s) to capture traffic from, considering factors like network segment, bandwidth, and connectivity.
- Ensure the selected interface supports promiscuous mode for capturing all packets, including those not addressed to the capturing device.
- Filter Configuration:
- Apply filters to capture specific types of traffic relevant to the investigation, such as by IP address, port number, protocol, or packet content.
- Use both capture filters (for real-time capture) and display filters (for post-capture analysis) to focus on relevant packets.
- Capture Duration and Timing:
- Determine the duration of the capture based on the incident timeframe, network activity patterns, and available storage capacity.
- Schedule captures during periods of expected network activity or suspected security incidents for optimal data collection.
- Storage Considerations:
- Allocate sufficient storage space for storing captured packets, considering the expected volume of traffic and duration of the capture.
- Choose a storage location with appropriate access controls and data protection measures to ensure the integrity and confidentiality of captured data.
- Capture Execution:

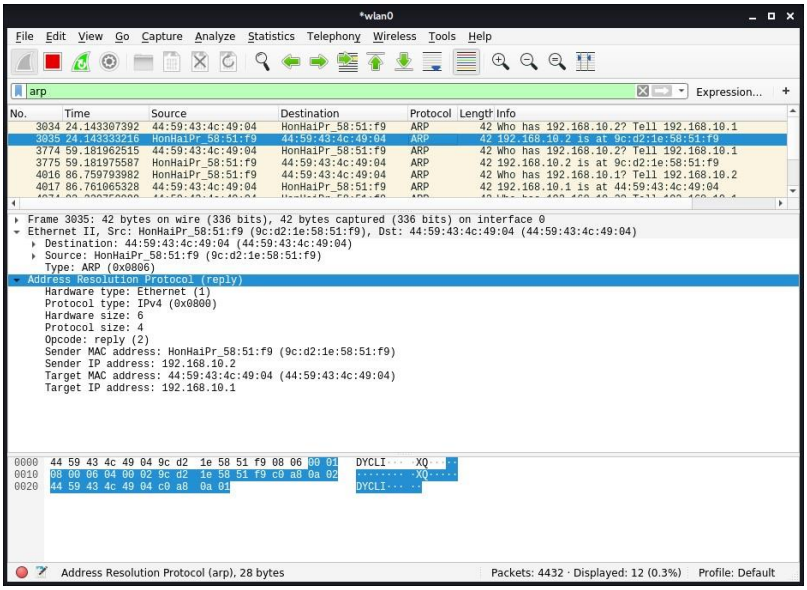
- Start the packet capture process on the selected network interface(s) using the chosen capture tool.
- Monitor the capture process to ensure packets are being captured correctly and without errors.
- Verify that the captured data meets the defined criteria and objectives of the investigation.
- Capture Validation:
- Periodically validate the integrity and completeness of captured packets to ensure accurate representation of network activity.
- Check for any dropped packets, capture errors, or hardware/software issues that may affect data quality.
- Capture Completion:
- Stop the packet capture process once the desired amount of data has been collected or the incident timeframe has elapsed.
- Save the captured packets to a secure location for further analysis and investigation, using standardized file formats like PCAP or PCAPNG.



4. Analysis phase

- Data Load: Load captured packet data into analysis tool.
- Initial Scan: Scan for immediate anomalies or irregularities.
- Traffic Overview: Profile network traffic to understand normal behavior.
- Focus Filters: Apply filters to isolate relevant traffic segments.
- Packet Inspection: Analyze packet contents for threats or anomalies.
- Pattern Recognition: Identify recurring patterns or suspicious sequences.
- Timeline Creation: Reconstruct a timeline of network events.
- Correlation: Link network data with other sources for context.
- Anomaly Detection: Flag deviations from normal network behavior.

- Evidence Collection: Document findings and collect supporting evidence.
- Reporting: Summarize findings in a clear and structured report.



5. Correlation context

- Data Integration: Collect and integrate network data with other relevant sources, such as system logs, security alerts, or threat intelligence feeds.
- Source Verification: Verify the reliability and integrity of external data sources to ensure accuracy in correlation efforts.
- Event Correlation: Correlate network events with external data sources to identify patterns, trends, or relationships that provide context to the incident.
- Temporal Correlation: Align timestamps of network events with related activities in other data sources to establish temporal relationships and sequence of events.
- Attribution Analysis: Analyse attribution details, such as IP addresses, user identities, or device information, to trace activities back to their origins.
- Behavioural Analysis: Assess the behaviour and characteristics of network traffic in comparison to known attack patterns or abnormal activities.
- Threat Intelligence Integration: Incorporate threat intelligence data to enrich analysis and identify potential indicators of compromise (IOCs) or malicious actors.
- Geospatial Correlation: Correlate network activity with geographic locations to identify potential sources of attacks or anomalies.
- Contextual Understanding: Develop a comprehensive understanding of the incident by considering contextual factors, such as organizational policies, network topology, and business operations.
- Holistic View: Combine correlated data points to form a holistic view of the incident, enabling deeper insights and more informed decision-making.
- Documentation: Document correlation efforts, including findings, observations, and contextual information, to support analysis and reporting processes.l

6. Findings and conclusion

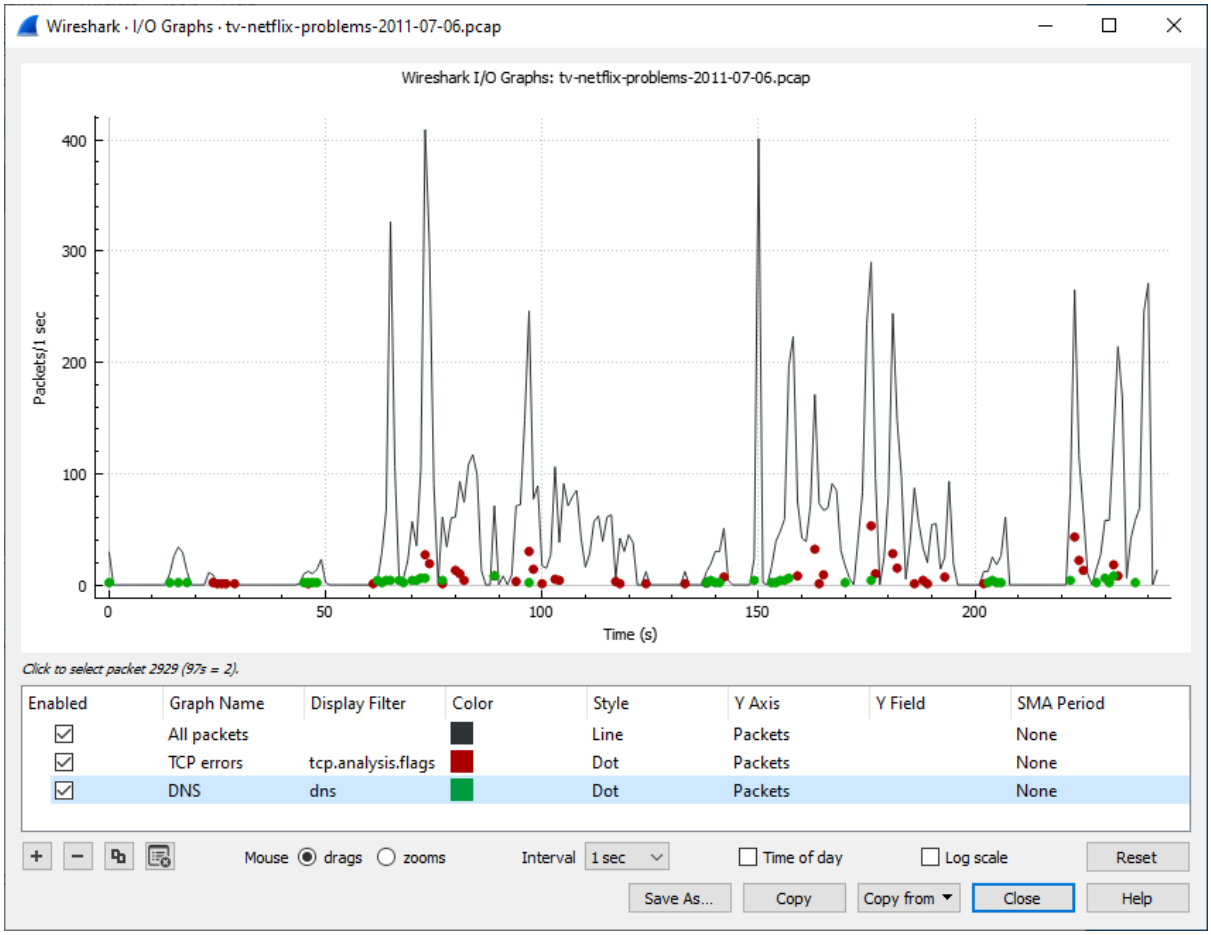
- Analysis Overview: Summarize key findings from Wireshark analysis, highlighting anomalies and security incidents.
- Incident Impact: Assess the impact of identified issues on network security, system integrity, and operational continuity.
- Root Cause Identification: Determine the underlying causes of security breaches or network anomalies uncovered during analysis.
- Attribution Analysis: If possible, attribute observed activities to specific sources or threat actors based on evidence from Wireshark data.
- Recommendations: Propose actionable steps to address identified vulnerabilities, enhance security controls, and prevent future incidents.
- Conclusion: Summarize overall findings, emphasizing the importance of continuous monitoring and proactive security measures in maintaining network resilience.

7. Record maintenance

- Documentation Standards: Establish standardized templates and procedures for documenting Wireshark incident response activities.
- Record Retention Policy: Define a record retention policy specifying the duration for storing captured packet data, analysis reports, and related documentation.
- Storage Infrastructure: Implement secure storage infrastructure with access controls and encryption mechanisms to safeguard captured packet data and sensitive information.
- Version Control: Maintain version control for documentation to track changes, updates, and revisions made throughout the incident response process.
- Timestamping: Ensure accurate timestamping of records to maintain chronological order and facilitate timeline reconstruction during investigations.
- Backup Procedures: Regularly backup captured packet data and analysis reports to prevent data loss and ensure availability for future reference or legal purposes.
- Access Logs: Maintain access logs and audit trails to track user interactions with stored records and ensure accountability for data management activities.

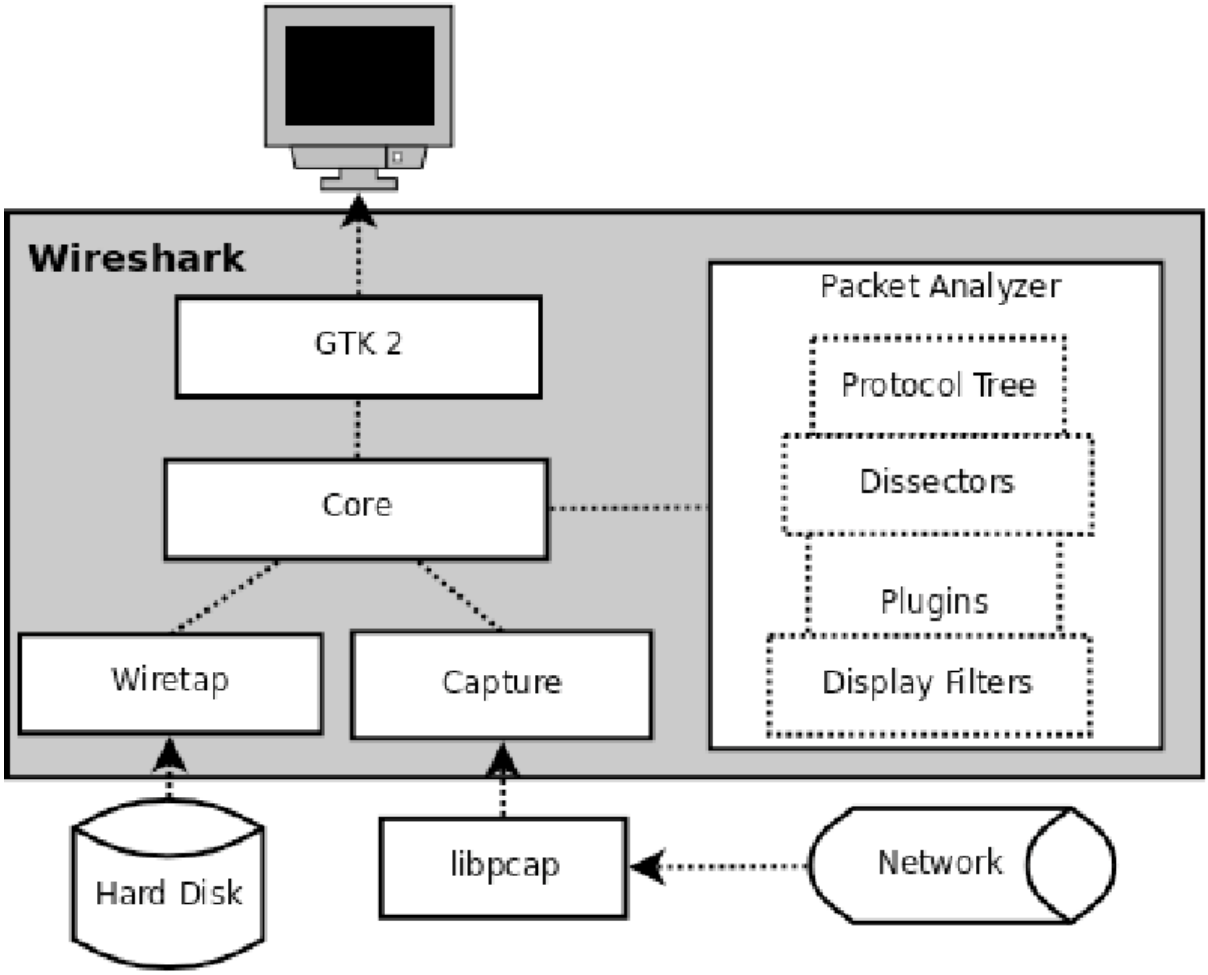
8. Review

Evaluate adherence to objectives, data integrity, technical accuracy, effectiveness of actions, timeliness, documentation completeness, lessons learned, feedback incorporation, compliance, and continuous improvement.



Timeline

- Capture: Initiate packet capture using Wireshark.
- Analysis: Analyse captured packets for anomalies and threats.
- Correlation: Correlate findings with other data sources.
- Attribution: Attribute activities to specific sources or actors.
- Mitigation: Implement remediation measures based on analysis.
- Documentation: Document findings, actions, and lessons learned.
- Reporting: Prepare and distribute incident reports.
- Review: Conduct post-incident review for process improvement.



Incident analysis

1. Description of observed anomalies and suspicious activities

Identified abnormal traffic behaviours, such as unusual communication patterns, unexpected protocol usage, or unauthorized access attempts.

2. Analysis of network traffic patterns

Analysed network traffic patterns to identify trends, spikes in activity, or irregularities indicative of potential security incidents.

3. Identification of compromised systems or affected assets

Detected compromised systems or affected assets through analysis of communication logs, identifying sources and destinations of suspicious traffic.

4. Relation of incident and findings with threat intelligence

Correlated incident findings with threat intelligence feeds to identify known malicious IPs, signatures, or attack patterns associated with observed activities.

5. Assessment of impact on operations

Assessed the impact of the incident on operations, including disruptions to network services, data loss, or compromise of sensitive information, based on analysis findings and operational logs.

Root cause analysis

Vulnerability Identification: Identify vulnerabilities in systems or network configurations that allowed for exploitation or unauthorized access, based on analysis of captured traffic and system logs.

Misconfiguration Assessment: Evaluate misconfigurations in network devices, applications, or security controls that contributed to the incident, analysing packet headers and protocol behaviour for anomalies.

Human Error Examination: Investigate instances of human error, such as improper configuration changes or lapses in security protocols, by correlating user actions with network activity captured in Wireshark.

Weaknesses in Security Controls: Assess the effectiveness of existing security controls, such as firewalls, intrusion detection systems, or access controls, in preventing or detecting malicious activities, based on observed traffic patterns and packet contents.

External Factors Consideration: Consider external factors, such as third-party integrations, supply chain dependencies, or environmental conditions, that may have contributed to the incident, analysing communication logs for interactions with external entities.

Recommendations

Enhance Network Monitoring: Implement continuous network monitoring using Wireshark to detect and respond to security incidents in real-time.

Regular Training and Education: Provide regular training and education to staff on Wireshark usage, network security best practices, and incident response procedures to enhance incident detection and response capabilities.

Update Security Policies: Review and update security policies and procedures to include Wireshark as a primary tool for incident investigation and response.

Implement Intrusion Detection Systems: Deploy intrusion detection systems (IDS) and network intrusion prevention systems (IPS) to complement Wireshark analysis and automate threat detection and response processes.

Enhance Access Controls: Strengthen access controls and authentication mechanisms to prevent unauthorized access to network resources and sensitive data captured by Wireshark.

Regular Software Patching: Ensure timely software patching and updates for Wireshark and other network monitoring tools to address known vulnerabilities and improve overall security posture.

Incident Response Plan Review: Review and update the incident response plan to incorporate lessons learned from the Wireshark incident response investigation and improve incident response processes.

Collaboration with Threat Intelligence: Foster collaboration with threat intelligence providers to stay updated on emerging threats and incorporate threat intelligence feeds into Wireshark analysis for proactive threat detection.

Conclusion

In conclusion, the utilization of Wireshark in incident response investigations offers valuable insights into network activities, enabling effective detection, analysis, and mitigation of security incidents. Through meticulous packet analysis, anomaly detection, and root cause identification, Wireshark empowers organizations to strengthen their security posture and respond proactively to emerging threats. Moving forward, continuous improvement of incident response processes, collaboration with threat intelligence sources, and ongoing training on Wireshark usage are essential to enhance resilience against evolving cybersecurity challenges. By leveraging Wireshark as a cornerstone of incident response efforts, organizations can better protect their networks, data, and assets from malicious actors and cybersecurity risks.

References

https://www.infosecinstitute.com/resources/incident-response-resources/wireshark-for-incident-response-101/

https://cybersecurity.att.com/blogs/security-essentials/network-traffic-analysis-using-wireshark

https://www.infosecinstitute.com/resources/hacking/wireshark/

https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html