Network Traffic Analysis Using Wireshark

By Youssef Ahmed Hany

**Uneeq Interns – Cyber Security Internship**

Network traffic analysis is a critical aspect of both cybersecurity and network management. Wireshark, a widely-used network protocol analyzer, allows users to capture and inspect data packets moving through a network in real time.

A blue and white fin

Description automatically generated

Once packet capture is underway, Wireshark's robust filtering capabilities enable users to focus on specific traffic types. The display filter bar, located at the top of the interface, allows users to narrow down the data by applying filters. For example, users can filter traffic by IP addresses, protocols (e.g., HTTP, TCP), or port numbers. Entering a command like "ip.addr == 10.0.2.5" will display only the traffic associated with the specified IP address, streamlining the analysis procA screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

When suspicious IP addresses are detected, it’s essential to verify their legitimacy. Tools like VirusTotal or Talos can help in this process. By entering an IP address into VirusTotal’s search bar, users can check it against a vast database of threat intelligence sources. The results indicate whether the IP address has been linked to malicious activity, helping to guide further security actions.

A screenshot of a computer

Description automatically generated

Suspicious network activity refers to any unusual or abnormal behavior within a network that may signal a potential security threat. This includes unauthorized access attempts, unexpected data transfers, communication with known malicious IP addresses, or deviations from typical network behavior. Such activities may precede cyber threats like malware infections, data breaches, or network intrusions. Therefore, organizations need strong cybersecurity measures to detect and respond to these anomalies quickly.

Security tools like intrusion detection systems (IDS) and firewalls constantly monitor network traffic for irregularities, generating alerts when suspicious activity is detected. Investigating these alerts promptly is essential for identifying and mitigating security breaches before they escalate.

**Examples of Suspicious Activities:**

1.*Malicious Database Activity:*

Unauthorized changes to databases, such as modifying user permissions or content, may indicate suspicious activity.

2.*Account Abuse:*

Privileged account misuse is a key sign of insider threats. Red flags include altered audit trails, shared accounts, and unauthorized access to sensitive information.

3.*Unusual User Access:*

Unexpected changes in user access patterns, such as off-hours logins or failed login attempts, may suggest compromised credentials or external threats.

4.*Configuration Changes:*

Unauthorized changes to file configurations—such as modifications, additions, or deletions—could indicate a data breach or a hacker operating covertly within the system.

5.*Abrupt Network Changes:*

Unexplained changes in network traffic, such as unusual traffic origins, erratic performance, or unauthorized scans, may signal a security threat.

6. *End-User Detection:*

In smaller organizations with fewer security controls, end users might first notice suspicious activity, such as increased pop-ups, slow network performance, or unfamiliar toolbars.

**Preventing Suspicious Network Activity:**

1. *Understand Your Data:*

Begin by mapping out what data you have, where it’s stored, how it’s accessed, and who owns it. Classify the data based on its sensitivity and value, and apply appropriate security measures to protect it.

2. *Monitor Activity:*

Continuously monitor network logs and activity using security tools that aggregate and analyze data. Set up alerts to flag abnormal events for timely investigation and response.

3. *Implement Security Measures:*

Protect data in transit and at rest using encryption, firewalls, VPNs, and network segmentation. Use multi-factor authentication and role-based access controls to prevent unauthorized access.

4. *Update Policies:*

Regularly review and update data governance and security policies to match current business and regulatory requirements. Ensure organization-wide compliance through regular training.

5. *Audit for Compliance:*

Periodic audits of your network and data security practices, conducted by internal or external teams, can help identify gaps and areas for improvement. Use these audits to refine your security posture.

6. *Leverage Experience:*

Stay informed on emerging security trends and threats. Learn from past experiences, best practices, and research to continuously improve your network security measures. Implement feedback loops and update strategies as needed to adapt to the evolving cybersecurity landscape.

**By applying these methods, organizations can effectively protect their networks, mitigate risks, and respond to potential threats in a timely manner.**