Suricata Network Security Incident Report

Generated on: 2025-12-01 20:18:48

[2025-11-26 16:29:52] WEB-ATTACK Directory Traversal Attempt

Source: 192.168.1.184 --> Destination: 3.170.103.6

Analysis: An attempt was detected to access files outside the web root folder (e.g., using '../').

Why it is Dangerous: CRITICAL. If successful, this allows attackers to read sensitive system files (like /etc/passwd) or configuration data.

Recommended Action: Immediate: Block Source IP. Check web logs to see if a 200 OK response was returned.

[2025-11-26 16:24:26] WEB-ATTACK Directory Traversal Attempt

Source: 192.168.1.184 --> Destination: 3.170.103.54

Analysis: An attempt was detected to access files outside the web root folder (e.g., using '../').

Why it is Dangerous: CRITICAL. If successful, this allows attackers to read sensitive system files (like /etc/passwd) or configuration data.

Recommended Action: Immediate: Block Source IP. Check web logs to see if a 200 OK response was returned.

[2025-11-26 16:20:19] WEB-ATTACK Directory Traversal Attempt

Source: 192.168.1.184 --> Destination: 3.170.103.11

Analysis: An attempt was detected to access files outside the web root folder (e.g., using '../').

Why it is Dangerous: CRITICAL. If successful, this allows attackers to read sensitive system files (like /etc/passwd) or configuration data.

Recommended Action: Immediate: Block Source IP. Check web logs to see if a 200 OK response was returned.

[2025-11-26 16:29:38] TELNET connection attempt

Source: 192.168.1.184 --> Destination: 192.168.1.181

Analysis: Unencrypted remote command-line connection attempt detected (Port 23).

Why it is Dangerous: HIGH. Telnet sends everything (including root passwords) in cleartext. Attackers can easily sniff credentials.

Recommended Action: Disable Telnet services immediately. Enforce SSH usage.

[2025-11-26 16:24:00] TELNET connection attempt

Source: 192.168.1.184 --> Destination: 192.168.1.181

Analysis: Unencrypted remote command-line connection attempt detected (Port 23).

Why it is Dangerous: HIGH. Telnet sends everything (including root passwords) in cleartext. Attackers can easily sniff credentials.

Recommended Action: Disable Telnet services immediately. Enforce SSH usage.

[2025-11-26 16:29:42] FTP connection attempt

Source: 192.168.1.184 --> Destination: 192.168.1.181

Analysis: File Transfer Protocol connection attempt detected (Port 21).

Why it is Dangerous: MEDIUM. FTP transmits data and credentials in cleartext. Vulnerable to Man-in-the-Middle attacks.

Recommended Action: Verify if transfer is authorized. Switch to SFTP or FTPS.

[2025-11-26 16:24:09] FTP connection attempt

Source: 192.168.1.184 --> Destination: 192.168.1.181

Analysis: File Transfer Protocol connection attempt detected (Port 21).

Why it is Dangerous: MEDIUM. FTP transmits data and credentials in cleartext. Vulnerable to Man-in-the-Middle attacks.

Recommended Action: Verify if transfer is authorized. Switch to SFTP or FTPS.

[2025-11-26 16:29:48] POLICY VIOLATION: Facebook Access

Source: 192.168.1.184 --> Destination: 192.168.1.254

Analysis: Traffic detected destined for social media (Facebook) domains.

Why it is Dangerous: LOW (Policy). Risks include productivity loss, tracking, and potential malware distribution vectors.

Recommended Action: Review corporate usage policy. Scan source host for unauthorized browser extensions.

[2025-11-26 16:29:48] POLICY VIOLATION: Facebook Access

Source: 192.168.1.184 --> Destination: 192.168.1.254

Analysis: Traffic detected destined for social media (Facebook) domains.

Why it is Dangerous: LOW (Policy). Risks include productivity loss, tracking, and potential malware distribution vectors.

Recommended Action: Review corporate usage policy. Scan source host for unauthorized browser extensions.

[2025-11-26 16:24:18] POLICY VIOLATION: Facebook Access

Source: 192.168.1.184 --> Destination: 192.168.1.254

Analysis: Traffic detected destined for social media (Facebook) domains.

Why it is Dangerous: LOW (Policy). Risks include productivity loss, tracking, and potential malware distribution vectors.

Recommended Action: Review corporate usage policy. Scan source host for unauthorized browser extensions.

[2025-11-26 16:24:18] POLICY VIOLATION: Facebook Access

Source: 192.168.1.184 --> Destination: 192.168.1.254

Analysis: Traffic detected destined for social media (Facebook) domains.

Why it is Dangerous: LOW (Policy). Risks include productivity loss, tracking, and potential malware distribution vectors.

Recommended Action: Review corporate usage policy. Scan source host for unauthorized browser extensions.

[2025-11-26 16:29:28] ICMP Ping

Source: 192.168.1.184 --> Destination: 192.168.1.181

Analysis: ICMP Echo Request (Ping) packet detected.

Why it is Dangerous: INFO/LOW. Standard connectivity test, but can be used by attackers to map the network (Reconnaissance).

Recommended Action: Monitor for high-volume scanning patterns. Ignore if part of standard maintenance.

[2025-11-26 16:29:28] ICMP Ping

Source: 192.168.1.181 --> Destination: 192.168.1.184

Analysis: ICMP Echo Request (Ping) packet detected.

Why it is Dangerous: INFO/LOW. Standard connectivity test, but can be used by attackers to map the network (Reconnaissance).

Recommended Action: Monitor for high-volume scanning patterns. Ignore if part of standard maintenance.

[2025-11-26 16:23:47] ICMP Ping

Source: 192.168.1.184 --> Destination: 192.168.1.181

Analysis: ICMP Echo Request (Ping) packet detected.

Why it is Dangerous: INFO/LOW. Standard connectivity test, but can be used by attackers to map the network (Reconnaissance).

Recommended Action: Monitor for high-volume scanning patterns. Ignore if part of standard maintenance.

[2025-11-26 16:23:47] ICMP Ping

Source: 192.168.1.181 --> Destination: 192.168.1.184

Analysis: ICMP Echo Request (Ping) packet detected.

Why it is Dangerous: INFO/LOW. Standard connectivity test, but can be used by attackers to map the network (Reconnaissance).

Recommended Action: Monitor for high-volume scanning patterns. Ignore if part of standard maintenance.

[2025-11-26 16:23:16] ICMP Ping

Source: 192.168.1.254 --> Destination: 192.168.1.181

Analysis: ICMP Echo Request (Ping) packet detected.

Why it is Dangerous: INFO/LOW. Standard connectivity test, but can be used by attackers to map the network (Reconnaissance).

Recommended Action: Monitor for high-volume scanning patterns. Ignore if part of standard maintenance.

[2025-11-26 16:24:53] ET INFO Microsoft Connection Test

Source: 192.168.1.225 --> Destination: 23.215.15.185

Analysis: General network alert detected by Suricata.

Why it is Dangerous: Unknown. Requires manual investigation.

Recommended Action: Investigate raw logs.

[2025-11-26 16:24:09] SURICATA STREAM Packet with invalid timestamp

Source: 192.168.1.181 --> Destination: 192.168.1.184

Analysis: General network alert detected by Suricata.

Why it is Dangerous: Unknown. Requires manual investigation.

Recommended Action: Investigate raw logs.

[2025-11-26 16:16:41] ET INFO Spotify P2P Client

Source: 192.168.1.169 --> Destination: 192.168.1.255

Analysis: General network alert detected by Suricata.

Why it is Dangerous: Unknown. Requires manual investigation.

Recommended Action: Investigate raw logs.

[2025-11-26 16:16:35] TEST: Raw Content Found

Source: 192.168.1.184 --> Destination: 3.170.103.54

Analysis: General network alert detected by Suricata.

Why it is Dangerous: Unknown. Requires manual investigation.

Recommended Action: Investigate raw logs.
