ESL Pro Security Report

Generated on: 2025-09-09 23:44:48

Executive Summary

AI Analysis: ?O?k?a?y?,? ?l?e?t?'?s? ?b?r?e?a?k? ?d?o?w?n? ?t?h?i?s? ?s?c?a?n? ?r?e?p?o?r?t? ?a?n?d? ?a?s?s?e?s?s? ?t?h?e? ?r?i?s?k?,? ?r?e?c?o?m?m?e?n?d? ?f?i?x?e?s?,? ?a?n?d? ?p?r?e?d?i?c?t? ?p?o?t?e?n?t?i?a?l? ?t?h?r?e?a?t?s?.? ? ?*?*?1?.? ?S?c?a?n? ?S?u?m?m?a?r?y? ?&? ?R?i?s?k? ?A?s?s?e?s?s?m?e?n?t?:?*?*?

Antivirus Status

{'C:\\Windows\\Temp': '', 'C:\\Users\\leaw0\\Downloads': ''}

Firewall Status

Domain Profile Settings:

State   ON

Firewall Policy   BlockInbound,AllowOutbound

LocalFirewallRules   N/A (GPO-store only)

LocalConSecRules   N/A (GPO-store only)

InboundUserNotification   Enable

RemoteManagement   Disable

UnicastResponseToMulticast Enable

Logging:

LogAllowedConnections   Disable

LogDroppedConnections	Disable
FileName	%systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize	4096

Private Profile Settings:

State	ON
Firewall Policy	BlockInbound,AllowOutbound
LocalFirewallRules	N/A (GPO-store only)
LocalConSecRules	N/... [truncated]

Network Status

{'nmap': {'command_line': 'nmap -oX - -sV 127.0.0.1', 'scaninfo': {'tcp': {'method': 'syn', 'services': '1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,280,301,306,311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,500,512-515,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,646,648,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,843,873,880,888,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-1011,1021-1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-1132,1137-1138,1141,1145,1147-1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187,1192,1198-1199,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-1501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,1666,1687-1688,1700,171... [truncated]

Network Traffic Analysis

Analyzed 4 network connections

AI Security Recommendations

Detailed Analysis & Recommendations

?O?k?a?y?,? ?l?e?t?'?s? ?b?r?e?a?k? ?d?o?w?n? ?t?h?i?s? ?s?c?a?n? ?r?e?p?o?r?t?,? ?a?s?s?e?s?s? ?t?h?e? ?r?i?s?k?s?,? ?a?n?d? ?r?e?c?o?m?m?e?n?d? ?a?c?t?i?o?n?s?.? ?*?*?O?v?e?r?a?l?l? ?A?s?s?e?s?s?m?e?n?t?:? ?H?i?g?h? ?R?i?s?k?*?*? ?T?h?i?s? ?s?c?a?n? ?r?e?v?e?a?l?s? ?a? ?s?i?g?n?i?f?i?c?a?n?t? ?n?u?m?b?e?r? ?o?f? ?v?u?l?n?e?r?a?b?i?l?i?t?i?e?s? ?a?n?d? ?p?o?t?e?n?t?i?a?l? ?a?t?t?a?c?k? ?v?e?c?t?o?r?s?.? ?T?h?e? ?c?o?m?b?i?n?a?t?i?o?n? ?o?f? ?o?p?e?n? ?p?o?r?t?s?,? ?i?d?e?n?t?i?f?i?e?d? ?s?e?r?v?i?c?e?s?,? ?a?n?d? ?t?h?e? ?r?e?p?o?r?t?e?d? ?t?h?r?e?a?t? ?i?n?t?e?l?l?i?g?e?n?c?e? ?m?a?k?e?s? ?t?h?i?s? ?a? ?*?*?h?i?g?h?-?r?i?s?k?*?*? ?s?i?t?u?a?t?i?o?n?.? ?*?*?D?e?t?a?i?l?e?d? ?B?r?e?a?k?d?o?w?n? ?&? ?R?i?s?k? ?A?s?s?e?s?s?m?e?n?t?*?*? ?1?.? ?*?*?V?u?l?n?e?r?a?b?l?e? ?S?e?r?v?i?c?e?s? ?&? ?O?p?e?n? ?P?o?r?t?s?:?*?*? ? ? ? ?*? ?*?*?F?T?P? ?(?2?2?1?)?:?*?*?*? ?O?p?e?n? ?F?T?P? ?i?s? ?a? ?*?*?m?a?j?o?r?*? ?v?u?l?n?e?r?a?b?i?l?i?t?y?.? ?F?T?P? ?t?r?a?n?s?m?i?t?s? ?u?s?e?r?n?a?m?e?s? ?a?n?d? ?p?a?s?s?w?o?r?d?s? ?i?n? ?p?l?a?i?n?t?e?x?t?,? ?m?a?k?i?n?g? ?a?c?c?o?u?n?t?s? ?e?x?t?r?e?m?e?l?y? ?s?u?s?c?e?p?t?i?b?l?e? ?t?o? ?c?o?m?p?r?o?m?i?s?e?.? ?l?t?'?s? ?a? ?s?t?a?n?d?a?r?d? ?t?a?r?g?e?t? ?f?o?r? ?b?r?u?t?e?-?f?o?r?c?e? ?a?t?t?a?c?k?s? ?a?n?d? ?c?r?e?d?e?n?t?i?a?l? ?t?h?e?f?t?.? ? ? ? ?*? ?*?*?M?i?c?r?o?s?o?f?t? ?R?P?C? ?(?1?3?5?)?:?*?*?*? ?O?p?e?n? ?R?P?C? ?i?s? ?o?f?t?e?n? ?a? ?c?o?n?d?u?i?t? ?f?o?r? ?a?t?t?a?c?k?s? ?l?i?k?e? ?W?a?n?n?a?C?r?y? ?a?n?d? ?o?t?h?e?r? ?m?a?l?w?a?r?e?.? ?l?t???s? ?f?r?e?q?u?e?n?t?l?y? ?e?x?p?l?o?i?t?e?d? ?d?u?e? ?t?o? ?m?i?s?c?o?n?f?i?g?u?r?a?t?i?o?n?s?.? ? ? ? ?*? ?*?*?M?i?c?r?o?s?o?f?t? ?D?i?r?e?c?t?o?r?y? ?S?e?r?v?i?c?e?s? ?(?4?4?5?)?:?*?*? ?T?h?i?s? ?p?o?r?t? ?e?x?p?o?s?e?s? ?t?h?e? ?S?e?r?v?e?r? ?M?e?s?s?a?g?e? ?B?l?o?c?k? ?(?S?M?B?)? ?p?r?o?t?o?c?o?l?,? ?t?h?e? ?f?o?u?n?d?a?t?i?o?n? ?f?o?r? ?W?i?n?d?o?w?s? ?f?i?l?e? ?s?h?a?r?i?n?g? ?a?n?d? ?p?r?i?n?t?i?n?g?.? ?l?t?'?s? ?c?o?n?s?i?s?t?e?n?t?l?y? ?t?a?r?g?e?t?e?d? ?b?y? ?r?a?n?s?o?m?w?a?r?e? ?a?n?d? ?o?t?h?e?r? ?m?a?l?i?c?i?o?u?s? ?a?c?t?o?r?s?.? ? ? ? ?*? ?*?*?H?T?T?P? ?(?8?0?)?:?*?*? ?T?h?e? ?p?r?e?s?e?n?c?e? ?o?f? ?a?n? ?H?T?T?P? ?s?e?r?v?i?c?e? ?i?n?d?i?c?a?t?e?s? ?a? ?w?e?b? ?s?e?r?v?e?r? ?i?s? ?r?u?n?n?i?n?g?.? ?T?h?i?s? ?c?o?u?l?d? ?b?e? ?v?u?l?n?e?r?a?b?l?e? ?t?o? ?w?e?b? ?a?p?p?l?i?c?a?t?i?o?n? ?a?t?t?a?c?k?s? ?(?S?Q?L? ?i?n?j?e?c?t?i?o?n?,? ?c?r?o?s?s?-?s?i?t?e? ?s?c?r?i?p?t?i?n?g?,? ?e?t?c?.?)? ?i?f? ?n?o?t? ?p?r?o?p?e?r?l?y? ?s?e?c?u?r?e?d?.? ? ? ? ?*? ?*?*?N?u?m?e?r?o?u?s? ?O?t?h?e?r? ?P?o?r?t?s?:?*?*? ?T?h?e? ?s?c?a?n? ?i?d?e?n?t?i?f?i?e?d? ?v?a?r?i?o?u?s? ?o?t?h?e?r?

ports, indicating the system is likely running a range of services that require appropriate configuration and security updates.

2. **Threat Intelligence & Attack Vectors:**

*   **"us.i.posthog.com."**

    *   **DNS Query:** The scan reported DNS queries to `us.i.posthog.com`. Posthog is a product analytics platform. While legitimate, this could be a potential indicator of data exfiltration if compromised. It's crucial to verify the integrity of this connection.

    *   **Network Traffic Analysis:** The traffic reported, specifically the connections to `us.i.posthog.com` and the various internal connections, suggests data is being transmitted. The scan confirms active communication, further intensifying the risk if vulnerabilities are exploited.

3. **Scan Results & Technical Details:**

*   **`elapsed': '6.43'`:** The scan took approximately 6 minutes and 43 seconds to complete. This suggests a fairly complex system.

*   **`uphosts': '21'`:** One host was successfully scanned (likely the target server itself).

*   **`downhosts': '0'`:** No hosts were found to be down.

*   **Predicted Threats:**

    *   **Ransomware:** The open SMB port and the identified Microsoft services make this system highly vulnerable to ransomware attacks.

    *   **Credential Theft:** Exploitation of FTP or SMB vulnerabilities can lead to stolen credentials, allowing attackers to gain full control of the system.

    *   **Data Exfiltration:** The DNS queries to Posthog raise concerns about potential data theft if the

?s?y?s?t?e?m? ?i?s? ?c?o?m?p?r?o?m?i?s?e?d?.? ?*? ?*?*?L?a?t?e?r?a?l? ?M?o?v?e?m?e?n?t?:?*?*? ? ?I?f? ?t?h?e? ?i?n?i?t?i?a?l? ?b?r?e?a?c?h? ?o?c?c?u?r?s?,?? ?t?h?e? ?a?t?t?a?c?k?e?r? ?c?a?n? ?l?i?k?e?l?y? ?u?s?e? ?t?h?i?s? ?c?o?m?p?r?o?m?i?s?e?d? ?s?y?s?t?e?m? ?t?o? ?a?t?t?a?c?k? ?o?t?h?e?r? ?s?y?s?t?e?m?s? ?o?n? ?t?h?e? ?n?e?t?w?o?r?k?.?? ?*? ?*?*?M?a?l?w?a?r?e? ?I?n?f?e?c?t?i?o?n?:?*?*? ?T?h?e? ?n?u?m?e?r?o?u?s? ?o?p?e?n? ?p?o? ? ?[?A?n?a?l?y?s?i?s? ?t?r?u?n?c?a?t?e?d? ?f?o?r? ?r?e?p?o?r?t? ?l?e?n?g?t?h?]?

Risk Assessment

Overall Risk Level: LOW - System appears secure