ESL Pro Security Report

Generated on: 2025-09-09 23:53:10

Executive Summary

AI Analysis: Okay, let's break down this vulnerability scan report, assess the risk, and provide actionable recommendations.

Executive Summary:

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 5 network connections

AI Security Recommendations

Detailed Analysis & Recommendations

Okay, let's break down this scan report and assess the risk, recommend fixes, and predict potential threats. **Overall Risk Assessment: High** This scan reveals a significant number of open ports and vulnerabilities, indicating a potentially high-risk environment. The presence of exposed services and a vulnerability scan suggests a system that?s not properly secured. The report shows a number of open ports, including FTP, RPC, HTTP, and DNS queries - all of which can be exploited if not properly configured and monitored. **Detailed Breakdown & Vulnerability Analysis** 1. **Open Ports and Services:** * **FTP (21):** This is a *major* red flag. FTP is inherently insecure, transmitting passwords and data in plaintext. It should *never* be exposed directly to the internet. It?s a prime target for attackers. * **Microsoft RPC (135):** RPC (Remote Procedure Call) can be vulnerable if not properly secured. It?s frequently targeted due to legacy implementations and misconfigurations. * **Microsoft Distributed Computing (445):** This port exposes Windows file sharing services, often a target for ransomware and other malware. * **HTTP (80):** While standard, the exposure here, coupled with the other vulnerabilities, elevates the risk. * **DNS Queries:** The repeated DNS queries to `us.i.posthog.com` indicate that this system is likely using Posthog for analytics. While Posthog itself isn't inherently vulnerable, the DNS queries could be a reconnaissance step by an attacker to map the network or gather information. 2. **Traffic Analysis:** * The traffic shown is indicative of network communication, and the Posthog queries are typical for systems using the analytics platform. This doesn't directly point to a vulnerability, but confirms the system is actively communicating with external services. 3. **Scanstats Details** *The scanstats information states that the source host is localhost. This likely suggests that the scan was conducted internally, potentially on a test or development system. The scan took 6.36 seconds, and there was one host that responded (localhost). **Recommended Fixes & Updates** 1. **Immediately Disable FTP (21):** This is the absolute priority. If FTP is absolutely necessary, it *must* be run over SSH tunnels or secured with TLS. 2. **Secure RPC (135):** * **Enable Authentication:** Ensure RPC uses strong authentication mechanisms (e.g., Kerberos). * **Restrict Access:** Limit access to RPC to only authorized users and services. * **Patch RPC Services:** Ensure the RPC services are running the latest patched versions to address known vulnerabilities. 3. **Secure File Sharing (445):** * **Enable Network Level Authentication (NLA):** NLA adds an extra layer of security by requiring users to authenticate before accessing file shares. * **Restrict File Share Permissions:** Implement the principle of least privilege - grant users only the minimum permissions th [Analysis truncated for report length]

Risk Assessment

Overall Risk Level: LOW - System appears secure