ESL Pro Security Report

Generated on: 2025-09-10 16:24:17 ADT

Executive Summary

AI Analysis: Okay, let's analyze this scan report and formulate a comprehensive response.

1. RISK ASSESSMENT:

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

Okay, let's break down this scan report and formulate a response. **1. RISK ASSESSMENT:** **Overall Risk Level: High** **Justification:** This scan reveals multiple open connections and several potentially vulnerable services running on the host. The presence of FTP, RPC, and HTTP services, combined with the ?open? states of these connections, immediately elevates the risk. While no explicit vulnerabilities are highlighted in the provided scan output, the open connections represent a significant opportunity for malicious actors. The lack of detailed vulnerability information doesn?t mitigate the inherent risk - it simply masks it. This host likely requires immediate attention. **2. PRIORITY ACTIONS:** 1. **Immediate Investigation:** The most critical action is to immediately investigate *why* these connections are open. Are legitimate processes using them? Are they compromised? 2. **Isolate the Host (If Possible):** If there's any suspicion of compromise, isolate the host from the network to prevent further spread of potential attacks. 3. **Review System Logs:** Examine system logs (event logs on Windows, syslog on Linux) for unusual activity, connection attempts, or errors. 4. **Terminate Unnecessary Connections:** If legitimate services aren?t using these connections, terminate them immediately. **3. VULNERABILITY REMEDIATION:** * **Open FTP (Port 21):** FTP is notoriously insecure. * **Remedy:** *Immediately* disable FTP. This is a critical vulnerability. If it's absolutely necessary, migrate to a secure protocol like SFTP or FTPS (which uses TLS encryption). * **Open RPC (Port 135):** Microsoft RPC is often a target for exploitation. * **Remedy:** Review and restrict access to the RPC service. Ensure it?s only accessed by authorized processes. Investigate if the service is needed and if it?s running with unnecessary privileges. * **Open HTTP (Port 80):** Although HTTPS should be used, the HTTP service is exposed. * **Remedy:** Migrate to HTTPS - this is essential for any web-facing service. Implement a valid SSL/TLS certificate. * **General:** Regardless of the specific service, ensure that all software running on the host is up to date with the latest security patches. **4. SECURITY IMPROVEMENTS:** * **Firewall Rules:** Implement strict firewall rules to limit access to the host based on the principle of least privilege. Only allow connections from authorized sources. * **Intrusion Detection/Prevention System (IDS/IPS):** Deploy an IDS/IPS to monitor network traffic for suspicious activity. * **Regular Security Audits:** Conduct regular security audits to identify and address potential vulnerabilities. * **Principle of Least Privilege:** All user accounts and services should operate with the minimum necessary permissions. * **Disable Unnecessary Services:** Turn off any services that are not actively being used. * **Implement Multi-Factor Authentication (MFA):** If the host or any services accessed through it require [Analysis truncated for report length]

Risk Assessment

Overall Risk Level: LOW - System appears secure