ESL Pro Security Report

Generated on: 2025-09-10 00:02:29

Executive Summary

AI Analysis: Okay, let's break down this scan report and assess the risk, recommend fixes, and predict potential threats.

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 4 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. This is a complex situation with multiple layers of concern. **1. Overall Risk Assessment: High** This scan presents a **high-risk** scenario due to several overlapping vulnerabilities and behaviors. The presence of multiple open ports, combined with the identified vulnerabilities and the suspicious traffic patterns, strongly suggest a potential compromise or reconnaissance activity. **2. Detailed Vulnerability Analysis & Identified Issues** * **Open Ports & Services:** * **Port 21 (FTP):** Open and running. FTP is notoriously insecure due to unencrypted data transmission. It?s a major vulnerability. * **Port 135 (msrpc):** Open - Microsoft RPC. Vulnerable to attacks if not properly secured and patched. This is often a gateway for malware. * **Port 445 (microsoft-ds):** Open - Microsoft Directory Services (Active Directory). This is *extremely* critical. Exploitation of vulnerabilities in Active Directory can lead to complete system compromise, user account takeover, and data exfiltration. It?s a prime target for ransomware and advanced persistent threats (APTs). * **Port 5000 (http):** Open - Running a web server (Werkzeug). This could be a basic web application, but it also presents a potential entry point for web-based attacks. * **Port 23570:** Open - Often used for Remote Desktop Protocol (RDP) if misconfigured, allowing unauthorized access to the system. * **ScanStats Details:** The scan report itself indicates that the target machine is responding to probes. This suggests someone is actively trying to connect to it, which is a key indicator of malicious activity. * **Traffic Analysis (Crucially Important):** * `Ether / IP / TCP 192.168.50.42:44350 > 3.168.73.51:https A / Raw`: This suggests outbound traffic to an external host (3.168.73.51) over HTTPS. While HTTPS encrypts the data, it doesn't protect against the *source* of the connection, nor does it prevent malicious code from being downloaded. The "A" designation indicates an A record DNS lookup - meaning this connection is likely attempting to resolve the external host. * `Ether / IP / TCP 150.171.27.11:https > 192.168.50.42:23570 A`: This shows inbound traffic, possibly a user attempting to access the system via RDP. **3. Threat Prediction & Potential Attack Vectors** Based on this scan, here's what could be happening, and what *could* happen: * **Reconnaissance:** The most likely scenario is that an attacker is performing reconnaissance, mapping out the target's network and identifying open ports and services. They?re likely gathering information to plan a more sophisticated attack. * **Exploitation of Active Directory Vulnerabilities:** The open 445 port immediately raises serious concerns. Exploits for Active Directory vulnerabilities (Kerberos, SMB) are widespread and frequently target organizations with outdated systems or unpatched s [Analysis truncated for report length]

Risk Assessment

Overall Risk Level: LOW - System appears secure