ESL Pro Security Report

Generated on: 2025-09-11 14:57:54 ADT

Executive Summary

Okay, heres an analysis of the provided security scan data, structured as requested:

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': '1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-1

11,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,2

80,301,306,311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,5

00,512-515,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,646,648,6

66-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,8

43,873,880,888,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-10

11,1021-1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-1132,1137-11
38,1141,1145,1147-1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187,11
92,1198-1199,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,12
77,1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,14
61,1494,1500-1501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,1666,16
87-1688,1700,171... [truncated]

Process Security

{'scan_time': '2025-09-11T14:56:46.439698', 'total_processes': 293, 'suspicious_processes': 8, 'high_resource_processes': 0, 'network_processes': 41, 'processes': [{'pid': 272, 'name': 'Registry', 'exe_path': 'Registry', 'cmdline': '', 'cpu_percent': 0.0, 'memory_percent': 0.03520345358380748, 'create_time': '2025-09-10T16:43:08.567507', 'username': None, 'status': 'running', 'num_threads': 4, 'network_connections': 0, 'listening_ports': []}, {'pid': 412, 'name': 'python.exe', 'exe_path': 'H:\\Wael_AV\\venv\\Scripts\\python.exe', 'cmdline': 'python main.py', 'cpu_percent': 0.0, 'memory_percent': 0.004928865214431164, 'create_time': '2025-09-11T14:51:00.109870', 'username': 'DESKTOP-DUQ7M23\\leaw0', 'status': 'running', 'num_threads': 1, 'network_connections': 0, 'listening_ports': [], 'file_size': 268568, 'file_modified': '2025-09-08T15:07:26.468624', 'file_created': '2025-09-08T15:07:26.468624', 'file_hash_partial': '33b42fc0df380c055eb0cb6104b31a07', 'digitally_signed': True}, {'pid'... [truncated]

Vulnerability Scan Results

[OK] No vulnerabilities detected in the scanned directories.

OSV Scanner Details

[DATA] Total 6 packages affected by 27 known vulnerabilities (2 Critical, 10 High, 11 Medium, 2 Low, 2 Unknown) from 1 ecosystem.

[SCA

Mediu

Network Traffic Analysis

Analyzed 26 network connections

Process Security Analysis

Scanned 293 processes, found 8 suspicious processes. Process security risk level: HIGH

Key Process Findings:

Found 8 potentially suspicious processes

Susp

runni

c:\use

dcb0f

c:\use

dcb0f

AI Security Recommendations

Detailed Analysis & Recommendations

1. **Immediate Investigation of Suspicious Processes:** The scan identified a process executing from a temporary directory. Immediately investigate the origin of this file, verify its legitimacy, and ensure its removal or remediation. Utilize tools like Process Explorer or Task Manager to monitor and potentially terminate this process if it's deemed malicious. 2. **Enhanced Network Monitoring:** Implement more granular network monitoring around the Chrome process (PID: 9384). Increase the threshold for high network activity and consider using network traffic analysis tools (e.g., Wireshark) to examine the destination of the connections. Determine if the Chrome activity is legitimate or if it's being used for malicious purposes (e.g., data exfiltration). 3. **Strengthen Process Hygiene:** Enforce stricter controls on software installation and execution, particularly from temporary directories. Implement a software restriction policy to block execution from temporary locations. Utilize application whitelisting to only allow authorized applications to run. 4. **Antivirus/Anti-Malware Scan:** Run a full system scan with a reputable antivirus/anti-malware solution. Ensure definitions are up-to-date. 5. **Review System Logs:** Thoroughly review Windows Event Logs (Application, Security) for any related errors, warnings, or unusual activity during the scan period. ---

Risk Assessment

Overall Risk Level: LOW - System appears secure