ESL Pro Security Report

Generated on: 2025-09-17 10:54:58 ADT

Executive Summary

The system exhibits a medium security risk level due to the presence of several non-digitally signed processes and unusual locations of system processes. While the antivirus and firewall are active, the system requires immediate investigation of the identified suspicious processes. A proactive approach to process monitoring and security updates is recommended.

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': '2025-09-17T10:54:58.037576', 'total_processes': 258, 'suspicious_processes': 5, 'high_resource_processes': 0, 'network_processes': 40, 'processes': [{'pid': 272, 'name': 'Registry', 'exe_path': 'Registry', 'cmdline': '', 'cpu_percent': 0.0, 'memory_percent': 0.06485775881874425, 'create_time': '2025-09-17T09:47:29.565886', 'username': None, 'status': 'running', 'num_threads': 4, 'network_connections': 0, 'listening_ports': []}, {'pid': 436, 'name': 'python.exe', 'exe_path': 'C:\\Users\\leaw0\\AppData\\Local\\Programs\\Python\\Python310\\python.exe', 'cmdline': 'C:\\Users\\leaw0\\AppData\\Local\\Programs\\Python\\Python310\\python.exe main.py', 'cpu_percent': 14.3, 'memory_percent': 0.4328860567079065, 'create_time': '2025-09-17T10:37:42.067656', 'username': 'DESKTOP-DUQ7M23\\leaw0', 'status': 'running', 'num_threads': 31, 'network_connections': 0, 'listening_ports': [], 'file_size': 103192, 'file_modified': '2023-04-05T01:47:54', 'file_created': '2023-04-05T01:47:54', 'f... [truncated]

Vulnerability Scan Results

[OK] No vulnerabilities detected in the scanned directories.

OSV Scanner Details

OSV Results: No output from scanner

Network Traffic Analysis

Analyzed 22 network connections

Process Security Analysis

Scanned 258 processes, found 5 suspicious processes. Process security risk level: MEDIUM

Key Process Findings:

Found 5 potentially suspicious processes

Susp

AI Security Recommendations

Detailed Analysis & Recommendations

1. **Immediate Investigation of Suspicious Processes:** Prioritize investigating notepad++.exe (PID: 1408) and WidgetService.exe (PID: 13760) immediately. Use process monitoring tools to understand their activity and confirm whether they are legitimate or malicious. 2. **Verify System Process Locations:** Confirm the legitimacy of explorer.exe (PID: 9336) running from the `c:\windows\explorer.exe` location. A misdirection could indicate a compromise. Ensure all system processes execute from their intended locations. 3. **Full Antivirus Scan & Malware Removal:** Conduct a full system scan with the active antivirus software, focusing on the suspicious processes identified. Implement malware removal if any threats are detected. 4. **Enable and Configure Windows Defender (or equivalent):** If Windows Defender isnt already enabled, activate it immediately. Configure it for real-time protection and automatic updates. 5. **Implement Process Monitoring & Alerting:** Set up system monitoring to track key processes and generate alerts for any unusual activity, such as processes running from unexpected locations or consuming excessive resources. This provides early warning signs of potential threats.

Risk Assessment

Overall Risk Level: LOW - System appears secure