A-Ryan Security Report

Generated on: 2025-09-24 21:50:34 ADT

Executive Summary

Okay, here's an analysis of the provided security scan results, 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': '1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,280,301,306,311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,500,512-515,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,646,648,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,843,873,880,888,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-10

11,1021-1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-1132,1137-1138,1141,1145,1147-1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187,1192,1198-1199,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-1501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,1666,1687-1688,1700,171... [truncated]

Process Security

{'scan_time': '2025-09-24T21:48:05.777568', 'total_processes': 291, 'suspicious_processes': 13, 'high_resource_processes': 1, 'network_processes': 42, 'processes': [{'pid': 272, 'name': 'Registry', 'exe_path': 'Registry', 'cmdline': '', 'cpu_percent': 0.0, 'memory_percent': 0.060138835588277234, 'create_time': '2025-09-24T13:29:03.567301', 'username': None, 'status': 'running', 'num_threads': 4, 'network_connections': 0, 'listening_ports': []}, {'pid': 464, 'name': 'python.exe', 'exe_path': 'C:\\Python313\\python.exe', 'cmdline': 'C:\\Python313\\python.exe main.py', 'cpu_percent': 18.7, 'memory_percent': 0.6523613153075237, 'create_time': '2025-09-24T21:43:21.489705', 'username': 'DESKTOP-DUQ7M23\\leaw0', 'status': 'running', 'num_threads': 28, 'network_connections': 0, 'listening_ports': [], 'file_size': 105816, 'file_modified': '2025-08-14T15:33:40', 'file_created': '2025-08-14T15:33:40', 'file_hash_partial': '97c1a3bdc43e4648d754a97d2100d65a', 'digitally_signed': True}, {'pid': 848,... [truncated]

Vulnerability Scan Results

Vulnerability Summary

Total Vulnerabilities Found: 40

Vulnerabilities by Package:

aiohttp: 17 vulnerabilities (HIGH PRIORITY)

flask: 2 vulnerabilities (LOW PRIORITY)

lxml: 2 vulnerabilities (LOW PRIORITY)

requests: 4 vulnerabilities (MEDIUM PRIORITY)

torch: 10 vulnerabilities (HIGH PRIORITY)

werkzeug: 5 vulnerabilities (MEDIUM PRIORITY)

OSV Scanner Details

Network Traffic Analysis

Analyzed 4 network connections

Process Security Analysis

Scanned 291 processes, found 13 suspicious processes. Process security risk level: HIGH

Key Process Findings:

Found 13 potentially suspicious processes

Susp

AI Security Recommendations

Detailed Analysis & Recommendations

1. **Immediate Investigation of Suspicious Processes:** Prioritize investigation of all processes identified as suspicious (YouTube Music.exe, notepad++.exe, explorer.exe, and any others flagged as unusual). Utilize process monitoring tools to track their activity, network connections, and resource consumption. 2. **Verify Digital Signatures:** Conduct a thorough audit of all executable files on the system to ensure they are digitally signed by trusted vendors. Investigate the source of any unsigned executables and determine their legitimacy. Remove or quarantine any unsigned executables that cannot be verified. 3. **Review Process Locations:** Investigate the root cause of `explorer.exe` running from an unusual location (c:\\windows\\explorer.exe). This suggests possible compromise or a malicious modification. Confirm the validity of the executables origin and ensure its functioning as intended. 4. **Implement Enhanced Process Monitoring:** Deploy or refine existing process monitoring tools to provide real-time alerts for unusual process behavior, including: * Unexpected process creation * High CPU/Memory usage * Unusual network connections * Access to sensitive system resources 5. **Run a Full Antivirus Scan:** Execute a comprehensive antivirus scan utilizing a reputable antivirus solution to detect and remove any malware or malicious software. **Important Note:** This analysis is based solely on the provided security scan results. Further investigation and corroboration with other security tools and techniques are recommended to fully understand the scope and impact of the identified vulnerabilities. Continued monitoring is essential to ensure the system remains secure.

Risk Assessment

Overall Risk Level: MEDIUM - Review and address issues