

Windows Endpoint Security: Traffic, Processes & Firewall Assessment

Project Type: Endpoint Security Assessment / SOC Analysis

Prepared by: Niknaz Sadehvandi

Role: Founder & Security Consultant

Organization: NS Cybersecurity

Date: December 2024

Objective

The objective of this assessment was to evaluate the security posture of a Windows endpoint by analyzing active network traffic, running processes, and firewall rule configurations. The goal was to identify potential indicators of compromise, unauthorized network exposure, or misconfigured firewall rules that could increase attack surface or enable malicious activity.

Tools & Technologies

- Windows Command Prompt (Administrator)
 - netstat -ano
 - Windows Task Manager (Details view)
 - Windows Defender Firewall with Advanced Security
 - Manual IP reputation and WHOIS lookups
-

Technical Steps Performed

1. Network Traffic Analysis

- Executed netstat -ano to enumerate all active TCP and UDP connections.
- Filtered results to review:
 - Listening ports
 - Established outbound connections
 - Common service ports (e.g., 443)
- Identified external IP addresses associated with active connections.

2. Process Correlation (PID Mapping)

- Mapped each Process ID (PID) from netstat output to running processes in Task Manager.
- Verified:
 - Executable names
 - User context
 - Application legitimacy
 - Publisher information where available
- Confirmed that all network-active processes corresponded to known and expected system or user applications.

3. Firewall Rule Review

- Reviewed inbound and outbound firewall rules using Windows Defender Firewall with Advanced Security.
 - Analyzed:
 - Enabled vs. disabled rules
 - Inbound allowances for third-party applications
 - Exposure of high-risk services and ports
 - Verified that no unnecessary inbound access was permitted.
-

Findings

Network Traffic Findings

- All outbound traffic was limited to legitimate services, including Google and Akamai CDN endpoints.

- No connections to suspicious, foreign, or blacklisted IP addresses were observed.
- No repeated failed connection attempts or abnormal traffic patterns were detected.
- Listening ports were associated with standard Windows networking services (e.g., mDNS, SSDP, LLMNR).

Process Integrity Findings

- All network-active processes were legitimate Windows system processes or trusted applications (e.g., browsers).
- No unknown, unsigned, or suspicious executables were identified.
- No evidence of persistence mechanisms or malware-style process behavior was observed.

Firewall Configuration Findings

- Firewall protection was enabled and functioning correctly.
- No high-risk inbound ports (RDP 3389, SMB 445, Telnet 23, FTP 21, SSH 22) were exposed.
- Inbound rules were limited to expected applications.
- Outbound rules aligned with normal system and application behavior.

Outcome

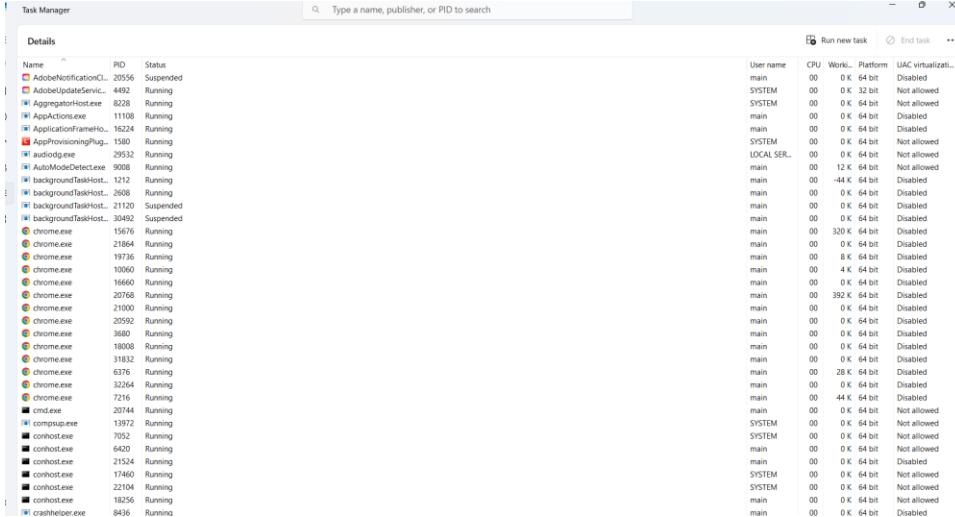
- Confirmed a low-risk endpoint security posture with no indicators of compromise.
- Established a baseline of normal network traffic and process behavior.
- Verified that firewall configurations do not expose the system to unnecessary inbound access.
- Produced a documented endpoint security assessment suitable for SOC triage, incident response baselining, and ongoing monitoring.

This project demonstrates hands-on experience performing endpoint network analysis, process validation, and firewall configuration reviews using SOC-relevant techniques and tooling.

Portfolio Status

Project Status: Completed

Deliverable: Windows_Endpoint_Security_Traffic_Process_and_Firewall_Assessment.pdf



The screenshot shows the Windows Task Manager interface. At the top, there is a search bar with the placeholder "Type a name, publisher, or PID to search". Below the search bar, there are two tabs: "Details" and "End task". The "Details" tab is selected, displaying a list of processes. The columns in the table are Name, PID, Status, User name, CPU, Work..., Platform, and UAC virtualizati... . The list includes numerous system processes like AdobeNotificationCL, AggregationHost.exe, ApplicationFrameHost.exe, AppProvicingHPlug.exe, AutoModeDetect.exe, backgroundTaskHost..., chrome.exe, cmd.exe, compupse.exe, connhostee..., and crashhelper.exe, along with several instances of chrome.exe and chrome.eve.

Name	PID	Status	User name	CPU	Work...	Platform	UAC virtualizati...
AdobeNotificationCL...	20556	Suspended	main	00	0 K	64 bit	Disabled
AggregationHost...	8228	Running	SYSTEM	00	0 K	64 bit	Not allowed
ApplicationFrameHo...	11108	Running	main	00	0 K	64 bit	Disabled
AppProvicingHPlug...	16224	Running	main	00	0 K	64 bit	Not allowed
AutoModeDetect.exe	9098	Running	SYSTEM	00	0 K	64 bit	Not allowed
backgroundTaskHost...	1212	Running	LOCAL SER...	00	0 K	64 bit	Not allowed
backgroundTaskHost...	266	Running	main	00	12 K	64 bit	Not allowed
backgroundTaskHost...	21120	Suspended	main	00	-44 K	64 bit	Disabled
backgroundTaskHost...	30404	Suspended	main	00	0 K	64 bit	Disabled
chrome.exe	21676	Running	main	00	320 K	64 bit	Disabled
chrome.exe	21664	Running	main	00	0 K	64 bit	Disabled
chrome.exe	19736	Running	main	00	8 K	64 bit	Disabled
chrome.exe	10060	Running	main	00	4 K	64 bit	Disabled
chrome.exe	16660	Running	main	00	0 K	64 bit	Disabled
chrome.exe	20768	Running	main	00	392 K	64 bit	Disabled
chrome.exe	21000	Running	main	00	0 K	64 bit	Disabled
chrome.exe	20592	Running	main	00	0 K	64 bit	Disabled
chrome.exe	368	Running	main	00	0 K	64 bit	Disabled
chrome.exe	18008	Running	main	00	0 K	64 bit	Disabled
chrome.exe	31832	Running	main	00	0 K	64 bit	Disabled
chrome.exe	63744	Running	main	00	28 K	64 bit	Disabled
chrome.exe	32264	Running	main	00	0 K	64 bit	Disabled
chrome.exe	7216	Running	main	00	44 K	64 bit	Disabled
cmd.exe	20744	Running	main	00	0 K	64 bit	Not allowed
compupse.exe	13972	Running	SYSTEM	00	0 K	64 bit	Not allowed
connhostee...	7052	Running	SYSTEM	00	0 K	64 bit	Not allowed
connhostee...	6420	Running	main	00	0 K	64 bit	Not allowed
connhostee...	21524	Running	main	00	0 K	64 bit	Disabled
connhostee...	17460	Running	SYSTEM	00	0 K	64 bit	Not allowed
connhostee...	22104	Running	SYSTEM	00	0 K	64 bit	Not allowed
connhostee...	18256	Running	main	00	0 K	64 bit	Not allowed
crashhelper.exe	8436	Running	main	00	0 K	64 bit	Disabled