Agentless Windows Vulnerability Assessment

Category: OS Profiling

Command: systeminfo
Summary: OS Profiling inspection completed.
Logic: OS version/build determines kernel exploit exposure.
NVD: []

Category: Hotfix Audit

Command: Get-HotFix; (New-Object -ComObject Microsoft.Update.Session).CreateUpdateSearcher().Search("IsInstalled=0").Updates
Summary: Hotfix Audit inspection completed.
Logic: Missing KBs correlate with Patch Tuesday RCE/LPE vulnerabilities.
NVD: []

Category: Software Inventory

Command: Get-Package; Get-WmiObject -Class Win32_Product; Get-Service | Where-Object {$_.Name -like "Sysmon"}
Summary: Software Inventory inspection completed.
Logic: Outdated or unmanaged software expands exploit surface.
NVD: []

Category: Service Status

Command: Get-Service | Where-Object {$_.Status -eq "Running"}; Get-CimInstance -Namespace root/subscription -ClassName __EventConsumer
Summary: Service Status inspection completed.
Logic: Running services and WMI consumers are common persistence vectors.
NVD: [{'cve_id': 'CVE-2000-0851', 'description': 'Buffer overflow in the Still Image Service in Windows 2000 allows local users to gain additional privileges via a long WM_USER message, aka the "Still Image Service Privilege Escalation" vulnerability.', 'severity': {}}, {'cve_id': 'CVE-2010-1886', 'description': 'Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 SP2 and R2, and Windows 7 allow local users to gain privileges by leveraging access to a process with NetworkService credentials, as demonstrated by TAPI Server, SQL Server, and IIS processes, and related to the Windows Service Isolation feature. NOTE: the vendor states that privilege escalation from NetworkService to LocalSystem does not cross a "security boundary."', 'severity': {}}, {'cve_id': 'CVE-2016-7381', 'description': 'For the NVIDIA Quadro, NVS, and GeForce products, NVIDIA Windows GPU Display Driver R340 before 342.00 and R375 before 375.63 contains a vulnerability

Category: EDR / AV Health

Command: Get-MpComputerStatus; Confirm-SecureBootUEFI
Summary: EDR / AV Health inspection completed.
Logic: Weak EDR or Secure Boot off enables BYOVD and bootkits.
NVD: []

Category: Audit Policy

Command: auditpol /get /category:*; Get-EventLog -List
Summary: Audit Policy inspection completed.
Logic: Low logging creates detection gaps.
NVD: No direct CVE – detection gap risk

Category: Firewall Rules

Command: Get-NetFirewallRule -Enabled True | Select DisplayName,Direction,Action
Summary: Firewall Rules inspection completed.
Logic: Inbound allow rules increase attack surface.
NVD: [{'cve_id': 'CVE-1999-1463', 'description': 'Windows NT 4.0 before SP3 allows remote attackers to bypass firewall restrictions or cause a denial of service (crash) by sending improperly fragmented IP packets without the first fragment, which the TCP/IP stack incorrectly reassembles into a valid session.', 'severity': {}}, {'cve_id': 'CVE-2004-2176', 'description': 'The Internet Connection Firewall (ICF) in Microsoft Windows XP SP2 is configured by default to trust sessmgr.exe, which allows local users to use sessmgr.exe to create a local listening port that bypasses the ICF access controls.', 'severity': {}}, {'cve_id': 'CVE-2006-1651', 'description': 'Microsoft ISA Server 2004 allows remote attackers to bypass certain filtering rules, including ones for (1) ICMP and (2) TCP, via IPv6 packets. NOTE: An established researcher has disputed this issue, saying that "Neither ISA Server 2004 nor Windows 2003 Basic Firewall support IPv6 filtering ... This is different network protocol.', 'se

Category: Neighbor Discovery

Command: Get-NetNeighbor; Get-NetRoute
Summary: Neighbor Discovery inspection completed.
Logic: ARP/IPv6 exposure enables MitM attacks.
NVD: [{'cve_id': 'CVE-2011-2393', 'description': 'The Neighbor Discovery (ND) protocol implementation in the IPv6 stack in FreeBSD, NetBSD, and possibly other BSD-based operating systems allows remote attackers to cause a denial of service (CPU consumption and device hang) by sending many Router Advertisement (RA) messages with different source addresses, a similar vulnerability to CVE-2010-4670.', 'severity': {}}, {'cve_id': 'CVE-2017-2315', 'description': 'On Juniper Networks EX Series Ethernet Switches running affected Junos OS versions, a vulnerability in IPv6 processing has been discovered that may allow a specially crafted IPv6 Neighbor Discovery (ND) packet destined to an EX Series Ethernet Switch to cause a slow memory leak. A malicious network-based packet flood of these crafted IPv6 NDP packets may eventually lead to resource exhaustion and a denial of service. The affected Junos OS versions are: 12.3 prior to 12.3R12-S4, 12.3R13; 13.3 prior to 13.3R10; 14.1 prior to 14.1R8-S3, 14

Category: Interface Statistics

Command: Get-NetAdapterStatistics; Get-DnsClientServerAddress
Summary: Interface Statistics inspection completed.
Logic: DNS hijacking can redirect traffic to malicious resolvers.
NVD: [{'cve_id': 'CVE-2011-0657', 'description': 'DNSAPI.dll in the DNS client in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly process DNS queries, which allows remote attackers to execute arbitrary code via (1) a crafted LLMNR broadcast query or (2) a crafted application, aka "DNS Query Vulnerability."', 'severity': {'source': '134c704f-9b21-4f2e-91b3-4a467353bcc0', 'type': 'Secondary', 'cvssData': {'version': '3.1', 'vectorString': 'CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H', 'baseScore': 9.8, 'baseSeverity': 'CRITICAL', 'attackVector': 'NETWORK', 'attackComplexity': 'LOW', 'privilegesRequired': 'NONE',

'userInteraction': 'NONE', 'scope': 'UNCHANGED', 'confidentialityImpact': 'HIGH', 'integrityImpact': 'HIGH', 'availabilityImpact': 'HIGH'}, 'exploitabilityScore': 3.9, 'impactScore': 5.9}}, {'cve_id': 'CVE-2017-0057', 'description': 'DNS client in Microsof

Category: Infrastructure Link

Command: Get-ADComputer -Identity $env:COMPUTERNAME -Properties *; (Get-CimInstance Win32_BIOS).Version
Summary: Infrastructure Link inspection completed.
Logic: Outdated BIOS/UEFI firmware enables bootkits.
NVD: [{'cve_id': 'CVE-2019-1736', 'description': 'A vulnerability in the firmware of the Cisco UCS C-Series Rack Servers could allow an authenticated, physical attacker to bypass Unified Extensible Firmware Interface (UEFI) Secure Boot validation checks and load a compromised software image on an affected device. The vulnerability is due to improper validation of the server firmware upgrade images. An attacker could exploit this vulnerability by installing a server firmware version that would allow the attacker to disable UEFI Secure Boot. A successful exploit could allow the attacker to bypass the signature validation checks that are done by UEFI Secure Boot technology and load a compromised software image on the affected device. A compromised software image is any software image that has not been digitally signed by Cisco.', 'severity': {'source': 'nvd@nist.gov', 'type': 'Primary', 'cvssData': {'version': '3.1', 'vectorString': 'CVSS:3.1/AV:P/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H', 'baseScore':

Category: Persistence Mechanisms

Command: Get-ScheduledTask; Get-ItemProperty HKCU:\Software\Microsoft\Windows\CurrentVersion\Run
Summary: Persistence Mechanisms inspection completed.
Logic: Startup tasks and run keys allow malware persistence.
NVD: []

Category: User / Group Audit

Command: Get-LocalGroupMember -Group "Administrators"
Summary: User / Group Audit inspection completed.
Logic: Admin sprawl enables privilege escalation chaining.
NVD: [{'cve_id': 'CVE-2000-0851', 'description': 'Buffer overflow in the Still Image Service in Windows 2000 allows local users to gain additional privileges via a long WM_USER message, aka the "Still Image Service Privilege Escalation" vulnerability.', 'severity': {}}, {'cve_id': 'CVE-2006-6308', 'description': 'Symantec LiveState 7.1 Agent for Windows allows local users to gain privileges by stopping the shstart.exe process and open "Web Self-Service" from the system tray icon, which will open a browser window running with elevated privileges. NOTE: several third-party researchers have noted that administrator privileges may be necessary to terminate shstart.exe. If this is the case, then no privilege escalation occurs, and this is not a vulnerability', 'severity': {}}, {'cve_id': 'CVE-2010-1886', 'description': 'Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 SP2 and R2, and Windows 7 allow local users to gain privileges by lever

Category: Active Connections

Command: Get-NetTCPConnection -State Listen
Summary: Active Connections inspection completed.
Logic: Unexpected listeners may indicate backdoors.

NVD: [{'cve_id': 'CVE-2016-0183', 'description': 'The Windows font library in Microsoft Office 2010 SP2, Word 2010 SP2, Word Automation Services on SharePoint Server 2010 SP2, and Office Web Apps 2010 SP2 allows remote attackers to execute arbitrary code via a crafted embedded font, aka "Microsoft Office Graphics RCE Vulnerability."', 'severity': {}}, {'cve_id': 'CVE-2024-7033', 'description': "In version 0.3.8 of open-webui/open-webui, an arbitrary file write vulnerability exists in the download_model endpoint. When deployed on Windows, the application improperly handles file paths, allowing an attacker to manipulate the file path to write files to arbitrary locations on the server's filesystem. This can result in overwriting critical system or application files, causing denial of service, or potentially achieving remote code execution (RCE). RCE can allow an attacker to execute malicious code with the privileges of the user running the application, leading to a full system compromise.", '