CYBERMENT

VA-R2 - Vulnerabilities Summary Report

Azienda Srl

February 15, 2022

Vulnerability Assessment for 12 hosts

Severity	Confirmed	Information Gathered
5	62	0
4	133	0
3	99	69
2	65	121
1	9	727
Total	368	917

Cyberment Predictive Score

(version 2022.3.1.2)

81%

CRITICAL

Host List Summary

IP		SCAN MODE	TOTAL	CPS	V5	V4	V3	V2	V1
1.2.3.4		Wan scan	7	59%	0	0	2	4	1
1.2.3.5		Wan scan	0	0%	0	0	0	0	0
1.2.3.6		Wan scan	0	0%	0	0	0	0	0
192.168.1.24	PCLAB	Network	1	40%	0	0	0	1	0
192.168.1.24	PCLAB	Agent	140	100% E M	30	71	30	9	0
192.168.1.63		Network	0	0%	0	0	0	0	0
192.168.1.64	USER1	Network	6	43%	0	0	2	3	1
192.168.1.64	USER1	Agent	55	100% E	12	34	4	5	0
192.168.1.68		Network	0	0%	0	0	0	0	0
192.168.1.88		Network	13	46%	0	0	5	7	1
192.168.1.93	DESKTOP-ABCDEF	Network	1	40%	0	0	0	1	0
192.168.1.93	DESKTOP-ABCDEF	Agent	11	53%	0	2	5	4	0
192.168.1.101	SERVER	Network	46	100% E	0	2	28	12	4
192.168.1.101	SERVER	Agent	57	100% E M	18	21	11	7	0
192.168.1.150		Network	20	100%	2	1	8	7	2
192.168.1.156	SRVBACKUP	Network	1	40%	0	0	0	1	0
192.168.1.156	SRVBACKUP	Agent	7	50%	0	1	2	4	0

Top 10 vulnerabilities with exploit and malware associated

4	E	M	Microsoft Word and Office Web Apps Remote Code Execution Vulnerability (MS14-017) (121860) *192.168.1.24*
4	E	M	Oracle Java SE Critical Patch Update - July 2015 (123714) *192.168.1.101*
4		M	Microsoft Word Multiple Remote Code Execution Vulnerabilities (MS08-072) (110092) *192.168.1.24*
5	E		Microsoft Windows Security Update for August 2020 (91668) *192.168.1.24*
5	E		Oracle Java SE Critical Patch Update - January 2015 (123168) *192.168.1.101*
5	E		Microsoft Windows Security Update July 2017 (91393) *192.168.1.101*
5	E		Microsoft Windows TCP/IP Remote Code Execution Vulnerabilities (91738) *192.168.1.24*
5	E		Microsoft Windows Security Update for June 2020 (91646) *192.168.1.24*
5	E		Microsoft Windows Graphics Component Security Update (MS16-120) (91287) *192.168.1.64*
5	E		Microsoft MSHTML Remote Code Execution (RCE) Vulnerability (91814) *192.168.1.24*

Top 4 host with exploit and malware associated

33	192.168.1.24 (pclab.domain.local) | Windows 7 Professional 64 bit Edition Service Pack 1
21	192.168.1.64 (user1.domain.local) | Windows 10 Pro 64 bit Edition Version 21H1
12	192.168.1.101 (server.domain.local) | Windows Server 2012 R2 Standard 64 bit Edition AD
4	192.168.1.101 (server.domain.local) | Windows 2012 R2 Standard

DETAILED RESULTS

1.2.3.4 (Wan scan) (-) |

Total: 7 CPS: 59% Vulnerabilities: 0 0 2 4 1

Vulnerabilities (7) for 1.2.3.4

3	TCP Source Port Pass Firewall (34000)
3	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0) (38628) port 1026/tcp over ssl
2	SSL Certificate - Subject Common Name Does Not Match Server FQDN (38170) port 1026/tcp over ssl

2 SSL Certificate - Invalid Maximum Validity Date Detected (38685) port 1026/tcp over ssl

2 SSL Certificate - Signature Verification Failed Vulnerability (38173) port 1026/tcp over ssl

2 SSL Certificate - Self-Signed Certificate (38169) port 1026/tcp over ssl

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1) (38794) port 1026/tcp over ssl

Information Gathered for 1.2.3.4

3 Remote Access or Management Service Detected (42017)

1 ICMP Replies Received (82040)

1 Firewall Detected (34011)

1 SSL Session Caching Information (38291) port 1026/tcp

1 Host Scan Time (45038)

1 Traceroute (45006)

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods (38704) port 1026/tcp

1 Internet Service Provider (45005)

1 Target Network Information (45004)

1 Host Names Found (45039)

1 SSL Server Information Retrieval (38116) port 1026/tcp

1 Degree of Randomness of TCP Initial Sequence Numbers (82045)

1 TLS Secure Renegotiation Extension Support Information (42350) port 1026/tcp

1 DNS Host Name (6)

1 Scan Activity per Port (45426)

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties (38706) port 1026/tcp

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance (38597) port 1026/tcp

1 SSL/TLS Server supports TLS_FALLBACK_SCSV (38610) port 1026/tcp

1 Open UDP Services List (82004)

1 Open TCP Services List (82023)

1.2.3.5 (Wan scan) (-) | Linux 2.4 / Linux Based Firewall

Total: 0 CPS: 0% Vulnerabilities: 0 0 0 0 0

Vulnerabilities (0) for 1.2.3.5

Information Gathered for 1.2.3.5

1.2.3.6 (Wan scan) (-) | Linux 2.4 / Linux Based Firewall

Total: 0 CPS: 0% Vulnerabilities: 0 0 0 0 0

Vulnerabilities (0) for 1.2.3.6

Information Gathered for 1.2.3.6

192.168.1.24 (Network) (pclab.domain.local; PCLAB) | Windows 7 Service Pack 1

Total: 1 CPS: 40% Vulnerabilities: 0 0 0 1 0

Vulnerabilities (1) for 192.168.1.24

2		NetBIOS Name Accessible (70000)

Information Gathered for 192.168.1.24

3 NetBIOS Bindings Information (70004)	2 Open DCE-RPC / MS-RPC Services List (70022)	2 Operating System Detected (45017)
2 Windows Registry Pipe Access Level (90194)	2 Host Uptime Based on TCP TimeStamp Option (82063)	1 NetBIOS Host Name (82044)
1 Open TCP Services List (82023)	1 IP ID Values Randomness (82046)	1 Windows Authentication Not Attempted (105296)
1 Network Adapter MAC Address (43007)	1 DNS Host Name (6)	1 ICMP Replies Received (82040)
1 NetBIOS Workgroup Name Detected (82062)	1 Scan Activity per Port (45426)	1 Firewall Detected (34011)
1 SMB Version 2 or 3 Enabled (45262)	1 Host Names Found (45039)	1 Windows Authentication Method (70028)
1 Host Scan Time (45038)	1 SMB Version 1 Enabled (45261)	1 Degree of Randomness of TCP Initial Sequence Numbers (82045)
1 Traceroute (45006)	1 Open UDP Services List (82004)	

192.168.1.24 (Agent) (pclab.domain.local; PCLAB) | Windows 7 Professional 64 bit Edition Service Pack 1

Total: 140 CPS: 100% E M Vulnerabilities: 30 71 30 9 0

Vulnerabilities (140) for 192.168.1.24

5		EOL/Obsolete Software: Microsoft XML Parser and Microsoft XML Core Services (MSXML) 4.0 Detected (105576)
5	E	Microsoft Windows TCP/IP Remote Code Execution Vulnerabilities (91738)
5	E	Microsoft Internet Explorer Remote Code Execution Vulnerability (ADV200001) (100400)
5	E	Microsoft MSHTML Remote Code Execution (RCE) Vulnerability (91814)
5	E	Microsoft Windows Security Update for June 2020 (91646)
5		Microsoft Windows Security Update for July 2020 (91653)
5		EOL/Obsolete Software: Adobe Flash Player Detected (105943)
5	E	Microsoft Windows Security Update for March 2020 (91609)
5		EOL/Obsolete Operating System: Microsoft Windows 7 Detected (105793)
5		Microsoft Windows Security Update for January 2021 (91724)
5		EOL/Obsolete Software: Microsoft XML Core Services 4.0 Service Pack 2 (SP2) Detected (105458)
5		Microsoft Windows Security Update for June 2021 (91772)
5	E	Microsoft Office Remote Code Execution Vulnerabilities (MS16-070) (110273)
5	E	Microsoft Internet Explorer Cumulative Security Update (MS15-124) (100269)
5		Microsoft Windows Security Update for May 2021 (91762)
5	E	Microsoft Windows Security Update for August 2020 (91668)
5		EOL/Obsolete Software: Microsoft Office 2000 and 2003 Web Components (105579)
5		EOL/Obsolete Software: Microsoft Office 2007 Detected (105736)
5		Microsoft Windows Security Update for March 2021 (91749)
5		Microsoft Excel Could Allow Remote Code Execution Vulnerabilities (MS07-036) (110062)
5		Microsoft Office Compatibility Pack Service Pack 3 Not Installed (110200)
5	E	Microsoft PowerPoint Could Allow Remote Code Execution (MS08-051) (110083)
5		Microsoft Internet Explorer Security Update for March 2020 (100402)
5		Microsoft Active Template Library (ATL) for Microsoft Office Remote Code Execution Vulnerability (MS09-060) (90543)
5		EOL/Obsolete Software: Microsoft PowerPoint Viewer Detected (105910)
5		Microsoft .NET Framework Security Updates for August 2020 (91665)
5		Microsoft Office 2007 SP1 Not Installed (110066)
5		EOL/Obsolete Software: Microsoft Office 2007 RTM Detected (105348)

5			Microsoft Foundation Class Library Remote Code Execution Vulnerability (MS11-025) (90698)
5			Microsoft Word and Office Web Apps Remote Code Execution Vulnerability (MS14-001) (110233)
4			Microsoft Internet Explorer Security Update for September 2020 (100410)
4			Microsoft .NET Framework Denial of Service Vulnerability - February 2021 (91733)
4	E		Microsoft Windows Security Update for October 2021 (91824)
4	E	M	Microsoft Word and Office Web Apps Remote Code Execution Vulnerability (MS14-017) (121860)
4			Microsoft Office 2007 SP2 Not Installed (110097)
4			Microsoft Windows Security Update - November 2021 (91832)
4	E		Intel Graphics Driver Type Confusion vulnerability in Content Protection HECI Service (INTEL-SA-00095) (370842)
4			Microsoft Internet Explorer Security Update for July 2020 (100408)
4			Microsoft Windows Security Update for August 2021 (91802)
4			Microsoft Internet Explorer Security Update for August 2020 (100409)
4			Microsoft Windows Security Update for December 2020 (91706)
4			Microsoft Windows Security Update for November 2020 (91691)
4	E		Microsoft Office Publisher 2007 Could Allow Remote Code Execution (MS07-037) (110056)
4			Microsoft .NET Framework Security Updates for May 2020 (91634)
4			Microsoft MSXML 4.0 Service Pack 3 Missing (90820)
4			Microsoft Windows Security Update for February 2021 (91739)
4			Microsoft Windows Security Update for September 2021 (91816)
4			Microsoft Office Dynamic Data Exchange (DDE) Vulnerability (KB 4053440) (ADV170021) (110307)
4	E		Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (Spectre/Meltdown Variant 4) (91462)
4			Microsoft Visual Studio Security Update for May 2021 (91763)
4			Microsoft Visual Studio Security Update for December 2020 (91703)
4			Microsoft Visual Basic for Applications Remote Code Execution Vulnerability (MS10-031) (110121)
4	E		Microsoft Office Excel Remote Code Execution Vulnerabilities (MS10-038) (110124)
4			Microsoft Excel Remote Code Execution Vulnerability (MS08-057) (110088)
4	E		Microsoft Excel Could Allow Remote Code Execution (MS08-043) (110084)
4			Microsoft .NET Framework Security Updates for October 2020 (91682)
4			Microsoft Windows Security Update for October 2020 (91683)
4	E		Microsoft Windows Security Update for February 2020 (91605)
4			Microsoft Internet Explorer Security Update for April 2020 (100403)
4			Microsoft Windows Security Update for September 2020 (91674)
4			Microsoft Visual Studio Security Update for June 2020 (91647)
4	E		Microsoft Visual Studio Security Update for July 2020 (91657)
4			Microsoft Windows Security Update for February 2022 (91857)
4			Microsoft Visual Studio Security Update for March 2020 (91611)
4			Microsoft Windows Security Update for April 2020 (91622)
4			Microsoft Internet Explorer Information Disclosure Vulnerability (September 2017) (100413)
4		M	Microsoft Word Multiple Remote Code Execution Vulnerabilities (MS08-072) (110092)
4			Microsoft Outlook S/MIME Certificate Metadata Information Disclosure Vulnerability (MS13-094) (110226)
4			Microsoft Windows Adobe Type Manager Library Remote Code Execution Vulnerability (ADV200006) (91617)
4	E		Microsoft .NET Framework And .NET Core Security Updates for July 2020 (91658)
4			Microsoft Visual Studio Security Update for August 2020 (91667)
4			Microsoft Visual Studio Security Update for January 2021 (91710)
4			Microsoft Excel Remote Code Execution Vulnerability (MS07-023) (110058)
4			Microsoft Visual Studio Security Update for May 2020 (91637)
4			Microsoft Visual Studio Security Update for April 2021 (91757)
4			Microsoft Visual Studio Security Update for September 2020 (91675)
4			Microsoft Word Multiple Remote Code Execution Vulnerabilities (MS13-086) (110222)

4		Microsoft Internet Explorer Security Update for February 2020 (100401)
4	E	Microsoft Office Word Remote Code Execution Vulnerability (MS10-056) (110129)
4	E	Microsoft Office Remote Code Execution Vulnerabilities (MS16-107) (110283)
4		Microsoft Windows Security Update for April 2021 (91758)
4	E	Microsoft Excel Remote Code Execution Vulnerability (MS09-009) (110093)
4		Microsoft Excel Multiple Remote Code Execution Vulnerabilities (MS08-074) (110090)
4		Windows Print Spooler Remote Code Execution Vulnerability (91796)
4		Microsoft XML Core Services Remote Code Execution Vulnerability (MS13-002) (90852)
4		Microsoft Internet Explorer Security Update for June 2020 (100407)
4	E	Microsoft Windows Print Spooler Remote Code Execution Vulnerability (PrintNightmare) (91785)
4		Microsoft Internet Explorer Security Update for November 2020 (100412)
4		Microsoft Windows Security Update for January 2022 (91851)
4		Microsoft Windows Security Update for December 2021 (91846)
4		Microsoft Visual Studio Security Update for April 2020 (91620)
4		Microsoft Visual Studio Security Update for March 2021 (91746)
4	E	Microsoft PowerPoint Remote Code Execution Vulnerability (MS11-022) (110148)
4		Microsoft Visual Studio Security Update for February 2021 (91729)
4		Microsoft Office Remote Code Execution Vulnerability (MS13-072) (110216)
4	E	Microsoft Windows Security Update for May 2020 (91636)
4		Microsoft Internet Explorer Security Update for May 2020 (100405)
4	E	Microsoft Office Remote Code Execution Vulnerabilities (MS16-029) (110266)
4		Microsoft Windows Security Update for July 2021 (91795)
4		Microsoft Visual Studio Security Update for November 2020 (91693)
4		Microsoft Windows Kernel Privilege Escalation Vulnerability (91690)
3		Windows Update For Credentials Protection and Management (Microsoft Security Advisory 2871997) (90954)
3		Microsoft Internet Explorer Security Update for March 2021 (100414)
3		Intel Graphics Driver Multiple Vulnerabilities(INTEL-SA-00166) (371263)
3		Microsoft Visual Studio Security Update for August 2021 (91809)
3	E	Ricoh Printer Drivers for Windows Local Privilege Escalation Vulnerability (372346)
3		Microsoft Windows Servicing Stack Security Update July 2020 (91655)
3	E	Microsoft Windows DHCPv6 Packets Remote Denial of Service Vulnerability - Zero Day (119518)
3		Microsoft XML Core Services XMLHttpRequest "SetCookie2" Header Information Disclosure Vulnerability - Zero Day (90482)
3		Microsoft Windows Elevation of Privilege Vulnerability (CVE-2021-43883) (91840)
3		Microsoft Windows Servicing Stack Security Update June 2020 (91643)
3		Microsoft Visual Studio Security Update for February 2022 (91858)
3	E	Microsoft Word 2007 WWLib.DLL Unspecified Document File Buffer Overflow Vulnerability - Zero Day (110057)
3	E	Microsoft Windows "ZwSetInformationProcess()" Local Denial of Service Vulnerability (90869)
3		Intel Graphics Driver Multiple Vulnerabilities(INTEL-SA-00189) (371696)
3		Microsoft Visual Studio Security Update for December 2021 (91843)
3		Microsoft WinHTTP support for TLS 1.1 and TLS 1.2 Missing (KB3140245) (91445)
3		Microsoft Internet Explorer Cumulative Security Update (KB5006671) for October 2021 (100416)
3		Microsoft Visual Studio Security Update for June 2021 (91769)
3		Microsoft Windows Gadgets Remote Code Execution Vulnerability (KB2719662) (90961)
3	E	NVIDIA Windows GPU Local Privilege Escalation Vulnerability (370263)
3		Microsoft Visual Studio Security Update for October 2021 (91822)
3		SMB Signing Disabled or SMB Signing Not Required (90043)
3		Microsoft Windows Servicing Stack Security Update May 2020 (91632)
3		Microsoft Office 2007 Service Pack 3 Not Installed (110171)
3	E	Microsoft Windows IcmpSendEcho2Ex Denial of Service Vulnerability - Zero Day (118425)

3	Microsoft .NET Framework Denial of Service (DoS) Vulnerability for January 2022 (91854)
3	Microsoft Internet Explorer Security Update for May 2021 (100415)
3	Microsoft Visual Studio Security Update for September 2021 (91815)
3	NVIDIA Display Driver Windows Privilege Impersonation Vulnerability (370301)
3	Built-in Guest Account Not Renamed at Windows Target System (105228)
2	Enabled Cached Logon Credential (90007)
2	Windows Explorer Autoplay Not Disabled for Default User (105171)
2	Microsoft Windows Servicing Stack Security Update April 2020 (91618)
2	Microsoft Windows Kerberos "Pass The Ticket" Replay Vulnerability (90630)
2	WinRAR Multiple Remote Code Execution (RCE) Vulnerability (375996)
2	Allowed Null Session (90044)
2	Microsoft Windows Servicing Stack Security Update February 2020 (91603)
2	Microsoft Windows Servicing Stack Security Update August 2020 (91670)
2	Microsoft Windows Explorer AutoPlay Not Disabled (105170)

Information Gathered for 192.168.1.24

- 3 Machine Security Group Membership Information (48116)
- 3 Microsoft Windows Socket Parameters, TCP/IP Hardening Guidelines (90127)
- 3 Administrator Group Members Enumerated (105231)
- 3 Microsoft Windows TCP Parameters, TCP/IP Hardening Guidelines (90128)
- 3 Antivirus Product Detected on Windows Host (105327)
- 3 Sticky Key's Enabled on System (124403)
- 3 Sophos Antivirus Scanner Detected (105000)
- 3 Microsoft Windows Link-Local Multicast Name Resolution (LLMNR) Not Disabled (45290)
- 3 Microsoft SQL Server Registry Key Security (105033)
- 3 Microsoft Windows Server Software SSL 3.0 Not Disabled (MSSA 3009008) (45230)
- 3 SAMR Pipe Permissions Enumerated (105237)
- 2 Windows Shares With Everyone Group Having Full Control (105316)
- 2 Last Successful User Login (105311)
- 2 Operating System Detected (45017)
- 2 Display BIOS Asset Tag - Chassis (45357)
- 2 Microsoft Windows File Security Check - C: System Files (105190)
- 2 Microsoft Windows Spectre Variant 2 Mitigation is Enabled (KB4078130) (91451)
- 2 Installed Applications Enumerated From Windows Installer (90235)
- 2 Microsoft Windows Effective Permission on Shares Enumerated (105185)
- 2 Windows Auto Reboot After Blue Screen Not Disabled (105172)
- 2 Detected a Modem (45106)
- 2 Microsoft .Net Framework Installed on Target Host (45178)
- 2 Administrator Group Members Enumerated Using SID (45302)
- 2 Security Permissions for Important CIFS Pipes (105244)
- 2 Microsoft Windows Folder Permission Check - Folders Under SystemRoot (105188)
- 2 Google Chrome Installed Extensions (45211)
- 2 Real Name of Built-in Guest Account Enumerated (90266)
- 2 Microsoft Windows Folder Permission Check - Folders Under System32 (105189)
- 2 Model Information from Devices (45304)
- 2 Windows Shares With Everyone Group Having Any Access (105317)
- 2 Microsoft XML parser (MSXML) Versions Detected (91228)
- 2 Antivirus Information Extracted Using WMI for Windows Desktop (105591)
- 1 Microsoft Windows Last Reboot Date and Time (90924)
- 1 Microsoft Active Directory Organizational Unit (OU) Information (48032)
- 1 File Access Permissions for Regedit.exe (105154)
- 1 Status of Remote Desktop/Terminal Service (45381)
- 1 Operating System's Install Date and Time (91074)
- 1 Processor Information for Windows Target System (43113)
- 1 Memory Information (115049)
- 1 Microsoft Windows 7 Operating System Detected (45340)
- 1 Git Installation Detected (45483)
- 1 Processor And BIOS Information Overview On Windows (43567)
- 1 Microsoft Windows System Hardware Enumeration: Serial, Parallel and USB Device Drivers (105060)
- 1 Windows WMI AuthenticationLevel Status (45456)
- 1 Enabled Display Last Username (90008)
- 1 Hotfix KB2264107 (DLL hijacking) Installed (90634)
- 1 SMB share list (78020)
- 1 Windows Services List (90065)
- 1 Windows Boot Method Detected (45309)
- 1 Adobe Flash Player Version Detected (45118)
- 1 Microsoft Office 2007 Installed (110164)
- 1 Local Firewall Status on Windows Detected (45506)
- 1 McAfee Data Loss Prevention Endpoint Agent not Installed (45272)
- 1 NTFS Settings Enumerated (45063)
- 1 Enumerate Windows shares that are readable by Everyone and count files (90635)
- 1 Internet Protocol version 6 (IPv6) Enabled on Target Host (45193)
- 1 System and BaseBoard Serial Numbers (45208)
- 1 Windows Forensics MRU Enumeration - WordPad Files (125018)
- 1 File Access Permissions for Regedt32.exe (105141)
- 1 Microsoft Windows Network Level Authentication Disabled (90788)
- 1 Message For Users Attempting To Logon To Windows System (105179)

- Microsoft Windows ScForceOption Registry Key Detected (45425)
- Microsoft Windows Malicious Software Removal Tool Detected (121213)
- Microsoft Windows System EventLog Policy Parameters (105165)
- Java Enabled in the Internet Zone (100141)
- Internet Explorer Search Companion Setting (105291)
- Microsoft Windows Security EventLog Policy Parameters (105167)
- Enumerate Windows shares and shared directories readable by built-in groups (90978)
- Google Chrome Web Browser Detected (45105)
- IPSEC Policy Agent Service Status Detected (105256)
- SMB Version 2 or 3 Enabled (45262)
- Microsoft Windows System Hardware Enumeration, Networking Components (105059)
- Microsoft Visual C++ 2008 Redistributable Package Detected (45354)
- Windows Host Domain Role (45486)
- Host Names Found (45039)
- Interface Names and Assigned IP Address Enumerated from Registry (45099)
- Installed Software information enumerated from all users using HKU registry key (372899)
- Microsoft Revoked Digital Certificates Enumeration From Registry (90974)
- Microsoft System Center Configuration Manager Client (SCCM) Not Installed (105504)
- Enumerate Windows shares and shared directories readable by Everyone, Authenticated Users or Domain Users (90831)
- Microsoft Windows Print Spooler Service is running (45498)
- Access to File Share is Enabled (90331)
- Network Adapter MAC Address (43007)
- Secure Channel (Schannel) Secure Sockets Layer (SSL) and Transport Layer Security (TLS) Registry Keys Reporting (48039)
- Microsoft Windows System Hardware Enumeration, Sound Devices and Multimedia (105062)
- Microsoft Windows Hostname and Domain Name Information (45325)
- Possible Log Recording Issues (90014)
- Microsoft Windows System Hardware Enumeration: Connected USB Storage Devices (105322)
- Microsoft Defender Installed (105310)
- Windows CDROM Autorun Enabled (90012)
- Windows Forensics MRU Enumeration - Regedit.exe (125017)
- Windows Automatic Update Information (105008)
- Qualys Cloud Agent Detected (45421)
- Adobe Reader Version Detected (45116)
- Trusted Digitial Certificates Enumerated From Windows Registry (45231)
- Windows Internet Explorer Version (90295)
- Host Scan Time (45038)
- Report TimeZone Information (45366)
- Microsoft Windows System Hardware Enumeration, Display Devices (105056)
- Microsoft Internet Explorer 11 Detected (100274)
- Microsoft Windows Management Instrumentation Service (WMI) Is Running (45183)
- Windows Builtin User Group Membership Audit - Backup Operators (105239)
- Microsoft Windows Application EventLog Policy Parameters (105166)
- Microsoft Office Component Detected (110187)
- Windows Host Local Group and Their Respective Users Detected (48202)
- Windows Builtin User Group Membership Audit - Replicator (105240)
- Microsoft Windows User Access Control Enabled (45454)
- Enumerate Windows shares and shared directories readable by Everyone (90797)
- Windows Product Type (90107)
- Microsoft Visual C++ 2005 Redistributable Package Detected (45333)
- Disabled Clear Page File (90013)
- Microsoft Windows System Hardware Enumeration, CPU (105054)
- Windows Connected Printers Information Extracted Through WMI (48203)
- System Architecture Information for Windows and Unix Platform Detected (45501)
- Enabled Shutdown Without Logon (90009)
- Enabled Caching of Dial-up Password Feature (90015)
- Windows Running Service Permissions (45414)
- Installed Locale settings on Host (45382)
- Microsoft Windows User Last Logon Time (90925)
- Windows Host Domain Information (45265)
- Microsoft Outlook Version Detected on Target (124418)
- Group Policy Objects Processed By SecCli are Enumerated from History Log (105238)
- Microsoft Windows Audit Settings Enumerated From LSA (105063)
- SMB Version 1 Enabled (45261)
- Windows Registry Access Level (105025)
- Windows Builtin User Group Membership Audit - Network Configuration Operators (105241)
- MultiThreading is Enabled (45489)
- PowerShell Detected On Host (45254)
- Programs Launched At Startup Through The Registry (90074)
- BITS running on target (90346)
- Network Interface Information Extracted Through WMI (45232)
- System Management BIOS UUID Detected (45303)
- Microsoft Windows An Automatic Updater Of Revoked Certificates Is Installed (KB 2677070 or KB 2813430) (45225)
- Processor Microcode Revision Information Overview On Windows (43576)

192.168.1.63 (Network) (-) |

Total: 0 CPS: 0% Vulnerabilities: 0 0 0 0 0

Vulnerabilities (0) for 192.168.1.63

Information Gathered for 192.168.1.63

1 DNS Host Name (6)
1 Host Name Not Available (82056)
1 ICMP Replies Received (82040)
1 Host Scan Time (45038)
1 Firewall Detected (34011)
1 Traceroute (45006)

192.168.1.64 (Network) (user1.domain.local; USER1) | Windows 2016/2019/10

Total: 6 CPS: 43% Vulnerabilities: 0 0 2 3 1

Vulnerabilities (6) for 192.168.1.64

3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) (38657) port 3389/tcp over ssl
3 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0) (38628) port 3389/tcp over ssl
2 SSL Certificate - Subject Common Name Does Not Match Server FQDN (38170) port 3389/tcp over ssl
2 SSL Certificate - Signature Verification Failed Vulnerability (38173) port 3389/tcp over ssl
2 NetBIOS Name Accessible (70000)
1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1) (38794) port 3389/tcp over ssl

Information Gathered for 192.168.1.64

3 Remote Access or Management Service Detected (42017)
2 Windows Registry Pipe Access Level (90194)
1 Open TCP Services List (82023)
1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods (38704) port 3389/tcp
1 ICMP Replies Received (82040)
1 Firewall Detected (34011)
1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties (38706) port 3389/tcp
1 Host Scan Time (45038)
1 TLS Secure Renegotiation Extension Support Information (42350) port 3389/tcp
3 NetBIOS Bindings Information (70004)
2 Open DCE-RPC / MS-RPC Services List (70022)
1 File and Print Services Access Denied (70038)
1 IP ID Values Randomness (82046)
1 Network Adapter MAC Address (43007)
1 NetBIOS Workgroup Name Detected (82062)
1 SMB Version 2 or 3 Enabled (45262)
1 SSL Session Caching Information (38291) port 3389/tcp
1 SSL Server Information Retrieval (38116) port 3389/tcp
1 Degree of Randomness of TCP Initial Sequence Numbers (82045)
1 Open UDP Services List (82004)
2 Operating System Detected (45017)
1 NetBIOS Host Name (82044)
1 SSL Certificate - Information (86002) port 3389/tcp
1 Windows Authentication Not Attempted (105296)
1 DNS Host Name (6)
1 Scan Activity per Port (45426)
1 Host Names Found (45039)
1 Windows Authentication Method (70028)
1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance (38597) port 3389/tcp
1 Traceroute (45006)
1 SSL Certificate will expire within next six months (38600) port 3389/tcp

192.168.1.64 (Agent) (user1.domain.local; USER1) | Windows 10 Pro 64 bit Edition Version 21H1

Total: 55 CPS: 100% E Vulnerabilities: 12 34 4 5 0

CYBERMENT

Vulnerabilities (55) for 192.168.1.64

5	E	Microsoft Office Multiple Remote Code Execution Vulnerabilities (MS15-081) (110258)
5		Adobe Reader and Acrobat Multiple Vulnerabilities (APSB19-17) (371729)
5		Adobe Reader and Acrobat Multiple Vulnerabilities (APSB19-18) (371777)
5		Adobe Reader and Acrobat Multiple Security Vulnerabilities (APSB18-30) (371230)
5	E	Microsoft Graphics Component Remote Code Execution Vulnerabilities (MS16-097) (91263)
5		Microsoft Office Remote Code Execution Vulnerabilities (MS15-131) (110262)
5	E	Microsoft Windows Graphics Component Security Update (MS16-120) (91287)
5		EOL/Obsolete Software: Microsoft Office 2007 Detected (105736)
5	E	Microsoft Windows Graphics Component Security Update (MS16-039) (91204)
5		EOL/Obsolete Software: Microsoft PowerPoint Viewer Detected (105910)
5		Microsoft Office Remote Code Execution Vulnerabilities (MS16-004) (110263)
5	E	Microsoft Graphics Component Remote Code Execution Vulnerabilities (MS15-097) (91094)
4		Adobe Reader and Acrobat Multiple Security Vulnerabilities (APSB18-29) (371132)
4		Adobe Reader and Acrobat Multiple Security Vulnerabilities (APSB18-34) (371210)
4		Microsoft Office and Microsoft Office Services and Web Apps Security Update December 2018 (110327)
4		Microsoft Office and Microsoft Office Services and Web Apps Security Update July 2018 (110320)
4	E	Microsoft Office and Microsoft Office Services and Web Apps Security Update February 2019 (110330)
4	E	Adobe Security Update for Adobe Acrobat and Reader (APSB19-41) (372051)
4	E	Microsoft Office and Microsoft Office Services and Web Apps Security Update June 2017 (110299)
4		Adobe Reader and Acrobat Multiple Security Vulnerabilities (APSB19-07) (371638)
4	E	Adobe Reader and Acrobat Multiple Security Vulnerabilities (APSB18-09) (370948)
4		Adobe Reader and Acrobat Information Disclosure Vulnerability (APSB18-40) (371317)
4	E	Microsoft Office and Microsoft Office Services and Web Apps Security Update July 2017 (110300)
4		Microsoft Office and Microsoft Office Services and Web Apps Security Update February 2018 (110311)
4	E	Microsoft Office and Microsoft Office Services and Web Apps Security Update January 2018 (110310)
4	E	WinRAR Arbitrary Code Execution Vulnerability (371635)
4		Adobe Reader and Acrobat Multiple Security Vulnerabilities (APSB19-02) (371395)
4		Adobe Reader and Acrobat Multiple Security Vulnerabilities (APSB18-41) (371372)
4		Microsoft Office Remote Code Execution Vulnerabilities (MS16-148) (110292)
4	E	Microsoft Office and Microsoft Office Services and Web Apps Security Update April 2017 (110297)
4		Microsoft Office Remote Code Execution Vulnerabilities (MS16-015) (110265)
4	E	Microsoft Office Remote Code Execution Vulnerabilities (MS16-107) (110283)
4		Microsoft Office and Microsoft Office Services and Web Apps Security Update October 2018 (110324)
4	E	Microsoft Office and Microsoft Office Services and Web Apps Security Update September 2017 (110303)
4		Adobe Reader and Acrobat Multiple Security Vulnerabilities (APSB18-02) (370776)
4		Microsoft Office Remote Code Execution Vulnerabilities (MS15-116) (110261)
4	E	Microsoft Office Remote Code Execution Vulnerabilities (MS16-099) (110282)
4	E	Microsoft Office and Microsoft Office Services and Web Apps Security Update May 2017 (110298)
4		Microsoft Office and Microsoft Office Services and Web Apps Security Update November 2018 (110325)
4		Adobe Reader and Acrobat Multiple Vulnerabilities (APSB17-36) (370650)
4		Microsoft Office Remote Code Execution Vulnerability (MS13-072) (110216)
4		Adobe Reader and Acrobat Multiple Security Vulnerabilities (APSB18-21) (371060)
4		Adobe Reader and Acrobat Information Disclosure Vulnerability (APSB19-13) (371659)
4	E	Microsoft Office Remote Code Execution Vulnerabilities (MS15-022) (110251)
4	E	Microsoft Office and Microsoft Office Services and Web Apps Security Update September 2018 (110323)
4		Microsoft Office Remote Code Execution Vulnerabilities (MS15-046) (110255)
3	E	Microsoft Word 2007 WWLib.DLL Unspecified Document File Buffer Overflow Vulnerability - Zero Day (110057)
3	E	Ricoh Printer Drivers for Windows Local Privilege Escalation Vulnerability (372346)
3		SMB Signing Disabled or SMB Signing Not Required (90043)

3	Built-in Guest Account Not Renamed at Windows Target System (105228)
2	Windows Explorer Autoplay Not Disabled for Default User (105171)
2	Enabled Cached Logon Credential (90007)
2	WinRAR Multiple Remote Code Execution (RCE) Vulnerability (375996)
2	Allowed Null Session (90044)
2	Microsoft Windows Explorer AutoPlay Not Disabled (105170)

Information Gathered for 192.168.1.64

3 BHOs Detected (90139)
3 Microsoft Windows Socket Parameters, TCP/IP Hardening Guidelines (90127)
3 Antivirus Product Detected on Windows Host (105327)
3 Microsoft Windows Link-Local Multicast Name Resolution (LLMNR) Not Disabled (45290)
2 Installed Applications Enumerated From Windows Installer (90235)
2 Security Permissions for Important CIFS Pipes (105244)
2 Microsoft Windows Folder Permission Check - Folders Under SystemRoot (105188)
2 Antivirus Information Extracted Using WMI for Windows Desktop (105591)
1 File Access Permissions for Regedit.exe (105154)
1 Processor Information for Windows Target System (43113)
1 Processor And BIOS Information Overview On Windows (43567)
1 Windows Services List (90065)
1 McAfee Data Loss Prevention Endpoint Agent not Installed (45272)
1 Access to File Share is Enabled (90331)
1 Message For Users Attempting To Logon To Windows System (105179)
1 Java Enabled in the Internet Zone (100141)
1 Windows Boot Method Detected (45309)
1 Microsoft Windows Security EventLog Policy Parameters (105167)
1 Network Adapter MAC Address (43007)
1 Microsoft Defender Installed (105310)
1 Windows Connected Printers Information Extracted Through WMI (48203)

3 Machine Security Group Membership Information (48116)
3 Administrator Group Members Enumerated (105231)
3 Sticky Key's Enabled on System (124403)
3 SAMR Pipe Permissions Enumerated (105237)
2 Last Successful User Login (105311)
2 Microsoft Windows Effective Permission on Shares Enumerated (105185)
2 Windows Auto Reboot After Blue Screen Not Disabled (105172)
2 Model Information from Devices (45304)
2 Real Name of Built-in Guest Account Enumerated (90266)
1 Microsoft Windows Last Reboot Date and Time (90924)
1 Status of Remote Desktop/Terminal Service (45381)
1 Memory Information (115049)
1 Adobe Acrobat Version Detected (45117)
1 Enabled Display Last Username (90008)
1 Windows Forensics MRU Enumeration - WordPad Files (125018)
1 NTFS Settings Enumerated (45063)
1 Internet Protocol version 6 (IPv6) Enabled on Target Host (45193)
1 Windows Builtin User Group Membership Audit - Replicator (105240)
1 Microsoft Windows ScForceOption Registry Key Detected (45425)
1 Microsoft Visual C++ 2005 Redistributable Package Detected (45333)
1 Microsoft Windows Hostname and Domain Name Information (45325)
1 Possible Log Recording Issues (90014)
1 Microsoft Windows User Access Control Enabled (45454)
1 Enabled Shutdown Without Logon (90009)
1 Windows CDROM Autorun Enabled (90012)
1 SMB Version 2 or 3 Enabled (45262)

3 Microsoft Windows Defender is Deactivated (121345)
3 Microsoft Windows TCP Parameters, TCP/IP Hardening Guidelines (90128)
3 Sophos Antivirus Scanner Detected (105000)
2 Operating System Detected (45017)
2 Microsoft Windows File Security Check - C: System Files (105190)
2 Microsoft .Net Framework Installed on Target Host (45178)
2 Administrator Group Members Enumerated Using SID (45302)
2 Microsoft Windows Folder Permission Check - Folders Under System32 (105189)
2 Google Chrome Installed Extensions (45211)
2 Microsoft XML parser (MSXML) Versions Detected (91228)
1 Microsoft Active Directory Organizational Unit (OU) Information (48032)
1 Operating System's Install Date and Time (91074)
1 Git Installation Detected (45483)
1 Windows WMI AuthenticationLevel Status (45456)
1 SMB share list (78020)
1 Microsoft Office 2007 Installed (110164)
1 Local Firewall Status on Windows Detected (45506)
1 Bitlocker Encryption Status Information (45437)
1 Microsoft Windows Malicious Software Removal Tool Detected (121213)
1 File Access Permissions for Regedt32.exe (105141)
1 Microsoft Windows Network Level Authentication Disabled (90788)
1 Microsoft Windows Print Spooler Service is running (45498)
1 Windows Host Local Group and Their Respective Users Detected (48202)
1 Internet Explorer Search Companion Setting (105291)
1 System and BaseBoard Serial Numbers (45208)
1 Disabled Clear Page File (90013)
1 Microsoft Windows System Hardware Enumeration, CPU (105054)
1 Microsoft Windows System EventLog Policy Parameters (105165)
1 Windows Product Type (90107)
1 IPSEC Policy Agent Service Status Detected (105256)
1 Enabled Caching of Dial-up Password Feature (90015)
1 System Architecture Information for Windows and Unix

1 Google Chrome Web Browser Detected (45105)
1 Microsoft Windows System Hardware Enumeration, Networking Components (105059)
1 Microsoft Windows Audit Settings Enumerated From LSA (105063)
1 Windows Builtin User Group Membership Audit - Network Configuration Operators (105241)
1 Microsoft Windows Sense agent Detected (45453)
1 Group Policy Objects Processed By SecCli are Enumerated from History Log (105238)
1 Host Names Found (45039)
1 Host Scan Time (45038)
1 Report TimeZone Information (45366)
1 Microsoft OneDrive Software Detected (45428)
1 Network Interface Information Extracted Through WMI (45232)
1 System Management BIOS UUID Detected (45303)
1 Windows Forensics MRU Enumeration - Regedit.exe (125017)
1 Microsoft Windows 10 Operating System Detected (45342)
1 Qualys Cloud Agent Detected (45421)
1 Windows Registry Access Level (105025)
1 Installed Software information enumerated from all users using HKU registry key (372899)
1 Microsoft Visual C++ 2008 Redistributable Package Detected (45354)
1 Microsoft Windows Fast Startup Feature Is Enabled (45445)
1 PowerShell Detected On Host (45254)
1 SMB Version 1 Enabled (45261)
1 Microsoft Windows Management Instrumentation Service (WMI) Is Running (45183)
1 Microsoft Windows An Automatic Updater Of Revoked Certificates Is Installed (KB 2677070 or KB 2813430) (45225)
1 Microsoft System Center Configuration Manager Client (SCCM) Not Installed (105504)
Platform Detected (45501)
1 Windows Running Service Permissions (45414)
1 Installed Locale settings on Host (45382)
1 Microsoft Windows User Last Logon Time (90925)
1 Windows Host Domain Information (45265)
1 Microsoft Windows System Hardware Enumeration, Display Devices (105056)
1 Microsoft Internet Explorer 11 Detected (100274)
1 MultiThreading is Enabled (45489)
1 Microsoft Outlook Version Detected on Target (124418)
1 Trusted Digitial Certificates Enumerated From Windows Registry (45231)
1 Windows Host Domain Role (45486)
1 Windows Internet Explorer Version (90295)
1 Programs Launched At Startup Through The Registry (90074)
1 Interface Names and Assigned IP Address Enumerated from Registry (45099)
1 Windows Builtin User Group Membership Audit - Backup Operators (105239)
1 Microsoft Office Component Detected (110187)
1 Processor Microcode Revision Information Overview On Windows (43576)
1 Microsoft Windows Application EventLog Policy Parameters (105166)

192.168.1.68 (Network) (-) |

Total: 0 CPS: 0% Vulnerabilities: 0 0 0 0 0

Vulnerabilities (0) for 192.168.1.68

Information Gathered for 192.168.1.68

192.168.1.88 (Network) (-) | Axis Network Camera / Axis Network Camera / Alpine Linux / HP Envy Photo Printer / Avocent / Dell iDRAC

Total: 13 CPS: 46% Vulnerabilities: 0 0 5 7 1

Vulnerabilities (13) for 192.168.1.88

3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) (38657) port 443/tcp over ssl
3 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher 4 (RC4/ARC4/ARCFOUR) (38601) port 443/tcp over ssl

3 UDP Source Port Pass Firewall (34020)

3 SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST) (42366) port 443/tcp over ssl

3 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0) (38628) port 443/tcp over ssl

2 SSL Certificate - Subject Common Name Does Not Match Server FQDN (38170) port 443/tcp over ssl

2 SSL Certificate - Invalid Maximum Validity Date Detected (38685) port 443/tcp over ssl

2 HTTP Security Header Not Detected (11827) port 443/tcp

2 HTTP Security Header Not Detected (11827) port 80/tcp

2 SSL Certificate - Self-Signed Certificate (38169) port 443/tcp over ssl

2 SSL Certificate - Improper Usage Vulnerability (38172) port 443/tcp over ssl

2 SSL Certificate - Signature Verification Failed Vulnerability (38173) port 443/tcp over ssl

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1) (38794) port 443/tcp over ssl

Information Gathered for 192.168.1.88

3 Content-Security-Policy HTTP Security Header Not Detected (48001) port 443/tcp

3 Content-Security-Policy HTTP Security Header Not Detected (48001) port 80/tcp

3 Remote Access or Management Service Detected (42017)

2 Web Server HTTP Protocol Versions (45266) port 80/tcp

2 Operating System Detected (45017)

2 Web Server HTTP Protocol Versions (45266) port 443/tcp

2 Host Uptime Based on TCP TimeStamp Option (82063)

1 HTTP Public-Key-Pins Security Header Not Detected (48002) port 443/tcp

1 SSL Server default Diffie-Hellman prime information (38609) port 443/tcp

1 Open TCP Services List (82023)

1 SSL Certificate - Information (86002) port 443/tcp

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods (38704) port 443/tcp

1 Referrer-Policy HTTP Security Header Not Detected (48131) port 443/tcp

1 Referrer-Policy HTTP Security Header Not Detected (48131) port 80/tcp

1 IP ID Values Randomness (82046)

1 HTTP Methods Returned by OPTIONS Request (45056) port 443/tcp

1 HTTP Methods Returned by OPTIONS Request (45056) port 80/tcp

1 SSH Banner (38050) port 22/tcp

1 HTTP Service Unavailable Replies Received (86383) port 443/tcp

1 HTTP Service Unavailable Replies Received (86383) port 80/tcp

1 Default Web Page (Follow HTTP Redirection) (13910) port 443/tcp

1 Default Web Page (Follow HTTP Redirection) (13910) port 80/tcp

1 Web Server Supports HTTP Request Pipelining (86565) port 443/tcp

1 Web Server Supports HTTP Request Pipelining (86565) port 80/tcp

1 DNS Host Name (6)

1 ICMP Replies Received (82040)

1 List of Web Directories (86672) port 443/tcp

1 List of Web Directories (86672) port 80/tcp

1 HTTP Response Method and Header Information Collected (48118) port 443/tcp

1 HTTP Response Method and Header Information Collected (48118) port 80/tcp

1 Scan Activity per Port (45426)

1 Firewall Detected (34011)

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties (38706) port 443/tcp

1 Host Name Not Available (82056)

1 SSL Session Caching Information (38291) port 443/tcp

1 SSL Server Information Retrieval (38116) port 443/tcp

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance (38597) port 443/tcp

1 Host Scan Time (45038)

1 Degree of Randomness of TCP Initial Sequence Numbers (82045)

1 SSL/TLS Server supports TLS_FALLBACK_SCSV (38610) port 443/tcp

1 Admin interface detected (48144) port 443/tcp

1 Admin interface detected (48144) port 80/tcp

1 Traceroute (45006)

1 SSH daemon information retrieving (38047) port 22/tcp

1 Default Web Page (12230) port 443/tcp

1 Default Web Page (12230) port 80/tcp

1 TLS Secure Renegotiation Extension Support Information (42350) port 443/tcp

1 Open UDP Services List (82004)

192.168.1.93 (Network) (desktop-abcdef.domain.local; DESKTOP-ABCDEF) | Windows 2016/2019/10

Total: 1 CPS: 40% Vulnerabilities: 0 0 0 1 0

Vulnerabilities (1) for 192.168.1.93

2 NetBIOS Name Accessible (70000)

Information Gathered for 192.168.1.93

- 3 NetBIOS Bindings Information (70004)
- 2 Windows Registry Pipe Access Level (90194)
- 1 IP ID Values Randomness (82046)
- 1 DNS Host Name (6)
- 1 Scan Activity per Port (45426)
- 1 Host Names Found (45039)
- 1 Degree of Randomness of TCP Initial Sequence Numbers (82045)
- 2 Open DCE-RPC / MS-RPC Services List (70022)
- 1 NetBIOS Host Name (82044)
- 1 Windows Authentication Not Attempted (105296)
- 1 ICMP Replies Received (82040)
- 1 Firewall Detected (34011)
- 1 Windows Authentication Method (70028)
- 1 Traceroute (45006)
- 2 Operating System Detected (45017)
- 1 Open TCP Services List (82023)
- 1 Network Adapter MAC Address (43007)
- 1 NetBIOS Workgroup Name Detected (82062)
- 1 SMB Version 2 or 3 Enabled (45262)
- 1 Host Scan Time (45038)
- 1 Open UDP Services List (82004)

192.168.1.93 (Agent) (desktop-abcdef.domain.local; DESKTOP-ABCDEF) | Windows 10 Pro 64 bit Edition Version 2009

Total: 11 CPS: 53% Vulnerabilities: 0 2 5 4 0

Vulnerabilities (11) for 192.168.1.93

- 4 Microsoft Windows Security Update for February 2022 (91857)
- 4 Microsoft Office Security Update for February 2022 (110401)
- 3 NVIDIA GeForce Experience Privilege Escalation Vulnerability (375689)
- 3 NVIDIA GPU Display Driver Multiple Vulnerabilities (November 2021) (376042)
- 3 SMB Signing Disabled or SMB Signing Not Required (90043)
- 3 Google Chrome Prior to 98.0.4758.80 Multiple Vulnerabilities (376369)
- 3 Built-in Guest Account Not Renamed at Windows Target System (105228)
- 2 Microsoft Windows Explorer AutoPlay Not Disabled (105170)
- 2 Enabled Cached Logon Credential (90007)
- 2 Allowed Null Session (90044)
- 2 Windows Explorer Autoplay Not Disabled for Default User (105171)

Information Gathered for 192.168.1.93

- 3 BHOs Detected (90139)
- 3 Microsoft Windows Socket Parameters, TCP/IP Hardening Guidelines (90127)
- 3 Antivirus Product Detected on Windows Host (105327)
- 3 Sophos Antivirus Scanner Detected (105000)
- 2 Operating System Detected (45017)
- 2 Windows Auto Reboot After Blue Screen Not Disabled (105172)
- 2 Microsoft Windows File Security Check - C: System Files (105190)
- 2 Microsoft Windows Folder Permission Check - Folders Under System32 (105189)
- 3 Machine Security Group Membership Information (48116)
- 3 Administrator Group Members Enumerated (105231)
- 3 Sticky Key's Enabled on System (124403)
- 3 SAMR Pipe Permissions Enumerated (105237)
- 2 Installed Applications Enumerated From Windows Installer (90235)
- 2 Full Disk Encryption Software Detected (105325)
- 2 Microsoft .Net Framework Installed on Target Host (45178)
- 2 Microsoft Windows Folder Permission Check - Folders Under SystemRoot (105188)
- 2 Model Information from Devices (45304)
- 3 Microsoft Windows Defender is Deactivated (121345)
- 3 Microsoft Windows TCP Parameters, TCP/IP Hardening Guidelines (90128)
- 3 Microsoft Windows Link-Local Multicast Name Resolution (LLMNR) Not Disabled (45290)
- 2 Last Successful User Login (105311)
- 2 Microsoft Windows Effective Permission on Shares Enumerated (105185)
- 2 Security Permissions for Important CIFS Pipes (105244)
- 2 Administrator Group Members Enumerated Using SID (45302)
- 2 Google Chrome Installed Extensions (45211)
- 2 Real Name of Built-in Guest Account Enumerated (90266)
- 2 Antivirus Information Extracted Using WMI for Windows Desktop (105591)

- 2 Microsoft XML parser (MSXML) Versions Detected (91228)
- 1 Adobe Acrobat Version Detected (45117)
- 1 Microsoft Office Click-to-Run Installation Detected (110264)
- 1 File Access Permissions for Regedt32.exe (105141)
- 1 Microsoft Windows Print Spooler Service is running (45498)
- 1 File Access Permissions for Regedit.exe (105154)
- 1 Microsoft Windows Network Level Authentication Enabled (45379)
- 1 Local Firewall Status on Windows Detected (45506)
- 1 Internet Protocol version 6 (IPv6) Enabled on Target Host (45193)
- 1 Windows Product Type (90107)
- 1 Microsoft Windows Hostname and Domain Name Information (45325)
- 1 Microsoft Windows Security EventLog Policy Parameters (105167)
- 1 Microsoft Office 2019 Installed (45450)
- 1 IPSEC Policy Agent Service Status Detected (105256)
- 1 SMB Version 2 or 3 Enabled (45262)
- 1 Windows Running Service Permissions (45414)
- 1 Microsoft Windows 10 Operating System Detected (45342)
- 1 Windows Host Domain Information (45265)
- 1 Windows Builtin User Group Membership Audit - Network Configuration Operators (105241)
- 1 Microsoft Windows Sense agent Detected (45453)
- 1 Microsoft Windows Fast Startup Feature Is Enabled (45445)
- 1 Report TimeZone Information (45366)
- 1 Zoom Video Conferencing Software Detected (45427)
- 1 Microsoft Windows Application EventLog Policy Parameters (105166)
- 1 Git Installation Detected (45483)
- 1 Windows WMI AuthenticationLevel Status (45456)
- 1 SMB share list (78020)
- 1 Microsoft Windows Malicious Software Removal Tool Detected (121213)
- 1 Message For Users Attempting To Logon To Windows System (105179)
- 1 Windows Host Local Group and Their Respective Users Detected (48202)
- 1 Status of Remote Desktop/Terminal Service (45381)
- 1 Processor Information for Windows Target System (43113)
- 1 System and BaseBoard Serial Numbers (45208)
- 1 McAfee Data Loss Prevention Endpoint Agent not Installed (45272)
- 1 Microsoft Windows System EventLog Policy Parameters (105165)
- 1 Java Enabled in the Internet Zone (100141)
- 1 Disabled Clear Page File (90013)
- 1 Possible Log Recording Issues (90014)
- 1 Host Names Found (45039)
- 1 Microsoft Defender Installed (105310)
- 1 Windows CDROM Autorun Enabled (90012)
- 1 System Architecture Information for Windows and Unix Platform Detected (45501)
- 1 Installed Locale settings on Host (45382)
- 1 Microsoft Windows User Last Logon Time (90925)
- 1 Microsoft Windows Audit Settings Enumerated From LSA (105063)
- 1 Installed Software information enumerated from all users using HKU registry key (372899)
- 1 Trusted Digitial Certificates Enumerated From Windows Registry (45231)
- 1 Windows Host Domain Role (45486)
- 1 Host Scan Time (45038)
- 1 Microsoft Windows An Automatic Updater Of Revoked Certificates Is Installed (KB 2677070 or KB 2813430) (45225)
- 1 Network Interface Information Extracted Through WMI (45232)
- 1 System Management BIOS UUID Detected (45303)
- 1 Microsoft Windows Management Instrumentation Service (WMI) Is Running (45183)
- 1 Processor And BIOS Information Overview On Windows (43567)
- 1 Enabled Display Last Username (90008)
- 1 Windows Services List (90065)
- 1 Access to File Share is Enabled (90331)
- 1 Windows Builtin User Group Membership Audit - Replicator (105240)
- 1 Microsoft Windows ScForceOption Registry Key Detected (45425)
- 1 Microsoft Windows Last Reboot Date and Time (90924)
- 1 Microsoft Active Directory Organizational Unit (OU) Information (48032)
- 1 Operating System's Install Date and Time (91074)
- 1 Memory Information (115049)
- 1 Windows Boot Method Detected (45309)
- 1 NTFS Settings Enumerated (45063)
- 1 Bitlocker Encryption Status Information (45437)
- 1 Network Adapter MAC Address (43007)
- 1 Microsoft Windows User Access Control Enabled (45454)
- 1 Internet Explorer Search Companion Setting (105291)
- 1 Microsoft Windows System Hardware Enumeration, CPU (105054)
- 1 Microsoft Windows Secureboot Enabled (45319)
- 1 Windows Connected Printers Information Extracted Through WMI (48203)
- 1 Enabled Shutdown Without Logon (90009)
- 1 Enabled Caching of Dial-up Password Feature (90015)
- 1 Google Chrome Web Browser Detected (45105)
- 1 Trusted Platform Module (TPM) Detected on Windows (45321)
- 1 Microsoft Windows System Hardware Enumeration, Networking Components (105059)
- 1 Qualys Cloud Agent Detected (45421)
- 1 Windows Registry Access Level (105025)
- 1 Microsoft Windows System Hardware Enumeration, Display Devices (105056)
- 1 Microsoft Internet Explorer 11 Detected (100274)
- 1 MultiThreading is Enabled (45489)
- 1 Group Policy Objects Processed By SecCli are Enumerated from History Log (105238)
- 1 Windows Internet Explorer Version (90295)
- 1 Interface Names and Assigned IP Address Enumerated from Registry (45099)
- 1 Processor Microcode Revision Information Overview On Windows (43576)
- 1 Microsoft System Center Configuration Manager Client (SCCM) Not Installed (105504)
- 1 Microsoft Teams Software Detected (45440)
- 1 PowerShell Detected On Host (45254)
- 1 Programs Launched At Startup Through The Registry

(90074)

1 Windows Builtin User Group Membership Audit - Backup 1 BITS running on target (90346)

Operators (105239)

192.168.1.101 (Network) (server.domain.local; SERVER) | Windows 2012 R2 Standard

Total: 46 CPS: 100% E Vulnerabilities: 0 2 28 12 4

Vulnerabilities (46) for 192.168.1.101

4 SSL Server Allows Anonymous Authentication Vulnerability (38142) port 2161/tcp over ssl

4 SSL Server Allows Anonymous Authentication Vulnerability (38142) port 2260/tcp over ssl

3 SSL Server May Be Forced to Use Weak Encryption Vulnerability (38141) port 2161/tcp over ssl

3 SSL Server May Be Forced to Use Weak Encryption Vulnerability (38141) port 2260/tcp over ssl

3 SSL Server Supports Weak Encryption Vulnerability (38140) port 2161/tcp over ssl

3 SSL Server Supports Weak Encryption Vulnerability (38140) port 2260/tcp over ssl

3 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher 4 (RC4/ARC4/ARCFOUR) (38601) port 1433/tcp over ssl

3 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher 4 (RC4/ARC4/ARCFOUR) (38601) port 1434/tcp over ssl

3 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher 4 (RC4/ARC4/ARCFOUR) (38601) port 2161/tcp over ssl

3 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher 4 (RC4/ARC4/ARCFOUR) (38601) port 2260/tcp over ssl

3 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Use of Weak Cipher Rivest Cipher 4 (RC4/ARC4/ARCFOUR) (38601) port 3389/tcp over ssl

3 Windows Remote Desktop Protocol Weak Encryption Method Allowed (90882) port 3389/tcp

3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) (38657) port 1433/tcp over ssl

3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) (38657) port 1434/tcp over ssl

3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) (38657) port 2161/tcp over ssl

3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) (38657) port 2260/tcp over ssl

3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) (38657) port 3389/tcp over ssl

3 SSL Server Has SSLv3 Enabled Vulnerability (38606) port 1433/tcp over ssl

3 SSL Server Has SSLv3 Enabled Vulnerability (38606) port 1434/tcp over ssl

3 SSL Server Has SSLv3 Enabled Vulnerability (38606) port 2161/tcp over ssl

3 SSL Server Has SSLv3 Enabled Vulnerability (38606) port 2260/tcp over ssl

3 E SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE) (38603) port 1433/tcp over ssl

3 E SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE) (38603) port 1434/tcp over ssl

3 E SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE) (38603) port 2161/tcp over ssl

3 E SSLv3 Padding Oracle Attack Information Disclosure Vulnerability (POODLE) (38603) port 2260/tcp over ssl

3 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0) (38628) port 1433/tcp over ssl

3 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0) (38628) port 1434/tcp over ssl

3 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0) (38628) port 2161/tcp over ssl

3 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0) (38628) port 2260/tcp over ssl

3 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0) (38628) port 3389/tcp over ssl

2 SSL Certificate - Subject Common Name Does Not Match Server FQDN (38170) port 2161/tcp over ssl

2 SSL Certificate - Subject Common Name Does Not Match Server FQDN (38170) port 3389/tcp over ssl

2 SSL Certificate - Invalid Maximum Validity Date Detected (38685) port 1433/tcp over ssl

2 SSL Certificate - Invalid Maximum Validity Date Detected (38685) port 1434/tcp over ssl

2 SSL Certificate - Signature Verification Failed Vulnerability (38173) port 1433/tcp over ssl

2 SSL Certificate - Signature Verification Failed Vulnerability (38173) port 1434/tcp over ssl

2 SSL Certificate - Signature Verification Failed Vulnerability (38173) port 2161/tcp over ssl

2 SSL Certificate - Signature Verification Failed Vulnerability (38173) port 3389/tcp over ssl

2 NetBIOS Name Accessible (70000)

2 SSL Certificate - Self-Signed Certificate (38169) port 1433/tcp over ssl

2 SSL Certificate - Self-Signed Certificate (38169) port 1434/tcp over ssl

2 SSL Certificate - Self-Signed Certificate (38169) port 2161/tcp over ssl

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1) (38794) port 1434/tcp over ssl

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1) (38794) port 2161/tcp over ssl

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1) (38794) port 2260/tcp over ssl

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1) (38794) port 3389/tcp over ssl

Information Gathered for 192.168.1.101

3 Remote Access or Management Service Detected (42017)

2 Information Gathered from DHCP/Bootp Server (45021)

2 Windows Registry Pipe Access Level (90194)

2 Host Uptime Based on TCP TimeStamp Option (82063)

1 ICMP Replies Received (82040)

3 NetBIOS Bindings Information (70004)

2 Open DCE-RPC / MS-RPC Services List (70022)

2 Web Server HTTP Protocol Versions (45266) port 5053/tcp

1 Network Adapter MAC Address (43007)

1 Microsoft SQL Server Cluster Presence Check (19101) port 1434/udp

2 Microsoft SQL Server Version Information Gathered (90087)

2 Operating System Detected (45017)

2 Web Server HTTP Protocol Versions (45266) port 80/tcp

1 DNS Host Name (6)

1 NetBIOS Workgroup Name Detected (82062)

1 HTTP Response Method and Header Information Collected (48118) port 5053/tcp

1 HTTP Response Method and Header Information Collected (48118) port 80/tcp

1 Scan Activity per Port (45426)

1 SMB Version 2 or 3 Enabled (45262)

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties (38706) port 1434/tcp

1 Firewall Detected (34011)

1 Host Names Found (45039)

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties (38706) port 2161/tcp

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties (38706) port 1433/tcp

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties (38706) port 2260/tcp

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties (38706) port 3389/tcp

1 SSL Session Caching Information (38291) port 1433/tcp

1 SSL Session Caching Information (38291) port 1434/tcp

1 SSL Session Caching Information (38291) port 2161/tcp

1 SSL Session Caching Information (38291) port 2260/tcp

1 SSL Session Caching Information (38291) port 3389/tcp

1 Windows Authentication Method (70028)

1 SSL Server Information Retrieval (38116) port 1433/tcp

1 SSL Server Information Retrieval (38116) port 1434/tcp

1 SSL Server Information Retrieval (38116) port 2161/tcp

1 SSL Server Information Retrieval (38116) port 2260/tcp

1 SSL Server Information Retrieval (38116) port 3389/tcp

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance (38597) port 1433/tcp

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance (38597) port 1434/tcp

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance (38597) port 2161/tcp

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance (38597) port 2260/tcp

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance (38597) port 3389/tcp

1 Host Scan Time (45038)

1 Degree of Randomness of TCP Initial Sequence Numbers (82045)

1 Traceroute (45006)

1 SMB Version 1 Enabled (45261)

1 NetBIOS Host Name (82044)

1 SSL Server default Diffie-Hellman prime information (38609) port 1433/tcp

1 SSL Server default Diffie-Hellman prime information (38609) port 1434/tcp

1 SSL Server default Diffie-Hellman prime information (38609) port 2260/tcp

1 SSL Server default Diffie-Hellman prime information (38609) port 3389/tcp

1 LDAP Information Gathering (45016)

1 Microsoft SQL Server Instances Enumerated (19145)

1 Default Web Page (12230) port 5053/tcp

1 Default Web Page (12230) port 80/tcp

1 SSL Certificate will expire within next six months (38600)

1 SSL Certificate will expire within next six months (38600) port 3389/tcp
1 TLS Secure Renegotiation Extension Support Information (42350) port 1433/tcp
1 TLS Secure Renegotiation Extension Support Information (42350) port 1434/tcp
1 TLS Secure Renegotiation Extension Support Information (42350) port 2161/tcp
1 TLS Secure Renegotiation Extension Support Information (42350) port 2260/tcp
1 TLS Secure Renegotiation Extension Support Information (42350) port 3389/tcp
1 Open UDP Services List (82004)
1 IP ID Values Randomness (82046)
1 Web Server Version (86000) port 5053/tcp
1 Microsoft Windows Active Directory / Domain Controller Present (45022) port 389/tcp
1 Windows Authentication Not Attempted (105296)
1 Default Web Page (Follow HTTP Redirection) (13910) port 5053/tcp
1 Default Web Page (Follow HTTP Redirection) (13910) port 80/tcp
1 Microsoft Windows Network Level Authentication Disabled (90788)
1 Open TCP Services List (82023)
1 SSL Certificate - Information (86002) port 1433/tcp
1 SSL Certificate - Information (86002) port 1434/tcp
1 SSL Certificate - Information (86002) port 2161/tcp
1 SSL Certificate - Information (86002) port 3389/tcp
1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods (38704) port 1433/tcp
1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods (38704) port 1434/tcp
1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods (38704) port 2161/tcp
1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods (38704) port 2260/tcp
1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods (38704) port 3389/tcp

192.168.1.101 (Agent) (server.domain.local; SERVER) | Windows Server 2012 R2 Standard 64 bit Edition AD

Total: 57 CPS: 100% E M Vulnerabilities: 18 21 11 7 0

Vulnerabilities (57) for 192.168.1.101

5 Oracle Java SE Critical Patch Update - January 2018 (370727)
5 Oracle Java SE Critical Patch Update - July 2017 (370469)
5 Oracle Java SE Critical Patch Update - October 2018 (371265)
5 EOL/Obsolete Software: Microsoft SQL Server 2012 Service Pack 3 (SP3) Detected (105802)
5 E Microsoft Windows Security Update July 2017 (91393)
5 Oracle Java SE Critical Patch Update - April 2018 (370887)
5 E Oracle Java SE Critical Patch Update - October 2017 (370610)
5 EOL/Obsolete Software: Microsoft Visual Studio 2008 Detected (105759)
5 Oracle Java SE Critical Patch Update - October 2016 (370161)
5 EOL/Obsolete Software: Microsoft SQL Server Compact 3.5 Detected (105764)
5 E Microsoft Internet Explorer Cumulative Security Update (MS15-124) (100269)
5 Oracle Java SE Critical Patch Update - July 2018 (371079)
5 E Oracle Java SE Critical Patch Update - January 2015 (123168)
5 Oracle Java SE Critical Patch Update - October 2014 (122741)
5 EOL/Obsolete Software: Microsoft SQL Server 2008 R2 Service Pack 2 (SP2) Detected (105640)
5 E Oracle Java SE Critical Patch Update - January 2017 (370280)
5 Oracle Java SE Critical Patch Update - April 2017 (370371)
5 Microsoft Sync Framework Service Pack 1 Not Installed (105489)
4 Microsoft .NET Framework Security Update January 2018 (91427)
4 Detected LanMan/NTLMv1 Authentication method (90019)
4 Oracle Java SE Critical Patch Update - July 2016 (370087)
4 E Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (Spectre/Meltdown Variant 4) (91462)
4 Oracle Java SE Critical Patch Update - April 2016 (124882)
4 Oracle Java SE Critical Patch Update - April 2020 (372508)
4 E M Oracle Java SE Critical Patch Update - July 2015 (123714)

4		Oracle Java SE Critical Patch Update - January 2019 (371528)
4		Oracle Java SE Critical Patch Update - January 2016 (124567)
4		Microsoft .NET Framework Security Update December 2018 (91489)
4	E	Oracle Java SE Critical Patch Update - April 2019 (371749)
4	E	Microsoft Windows Security Update for Windows Server (ADV180002) (Spectre/Meltdown) (91426)
4		Microsoft Windows Server Registry Key Configuration Missing (ADV190013) (91537)
4		Oracle Java SE Critical Patch Update - January 2020 (372333)
4	E	Oracle Java SE Critical Patch Update - October 2015 (124169)
4		Oracle Java SE Critical Patch Update - July 2019 (372013)
4		Oracle Java SE Critical Patch Update - October 2019 (372163)
4	E	Microsoft Security Update for SQL Server (ADV180002) (Spectre/Meltdown) (91424)
4		Oracle Java SE Critical Patch Update - July 2020(CPUJUL2020) (373156)
4		Oracle Java SE Critical Patch Update - April 2015 (123519)
4		Microsoft Internet Explorer Information Disclosure Vulnerability (September 2017) (100413)
3		Microsoft SQL Server 2008 R2 Service Pack 3 Not Installed (22000)
3		Oracle Java SE Critical Patch Update - October 2020 (CPUOCT2020) (373540)
3		Oracle Java SE Critical Patch Update - April 2021 (CPUAPR2021) (375477)
3		Oracle Java SE Critical Patch Update - July 2021 (CPUJUL2021) (375729)
3		Oracle Java SE Critical Patch Update - October 2021 (CPUOCT2021) (375964)
3		SMB Signing Disabled or SMB Signing Not Required (90043)
3		Oracle Java Standard Edition (SE) Critical Patch Update - January 2022 (CPUJAN2022) (376252)
3		Microsoft Windows DNS Resolver Addressing Spoofing Vulnerability (ADV200013) (91704)
3	E	Ricoh Printer Drivers for Windows Local Privilege Escalation Vulnerability (372346)
3		Oracle Java SE Critical Patch Update - January 2021 (CPUJAN2021) (374873)
3		Built-in Guest Account Not Renamed at Windows Target System (105228)
2		Enabled Cached Logon Credential (90007)
2		Windows Explorer Autoplay Not Disabled for Default User (105171)
2		VMware Tools Denial of Service Vulnerability (VMSA-2021-0011) (375639)
2		Microsoft Guidance for Enabling LDAP Signing Missing (ADV190023) (91565)
2		Allowed Null Session (90044)
2		Microsoft Guidance for LDAP Channel Binding Missing (ADV190023) (91564)
2		Microsoft Windows Explorer AutoPlay Not Disabled (105170)

Information Gathered for 192.168.1.101

3 BHOs Detected (90139)	3 Machine Security Group Membership Information (48116)	3 Internet Explorer Enhanced Security Configuration Disabled (123827)
3 Microsoft Windows Socket Parameters, TCP/IP Hardening Guidelines (90127)	3 Administrator Group Members Enumerated (105231)	3 Microsoft Windows TCP Parameters, TCP/IP Hardening Guidelines (90128)
3 Antivirus Product Detected on Windows Host (105327)	3 Microsoft DNS Server Parameters Information Gathering (15038)	3 Sticky Key's Enabled on System (124403)
		3 Sophos Antivirus Scanner Detected (105000)
3 Microsoft SQL Server Registry Key Security (105033)	3 Microsoft Windows Link-Local Multicast Name Resolution (LLMNR) Not Disabled (45290)	3 Microsoft Windows Server Software SSL 3.0 Not Disabled (MSSA 3009008) (45230)
3 SAMR Pipe Permissions Enumerated (105237)	2 Windows Shares With Everyone Group Having Full Control (105316)	2 Last Successful User Login (105311)
		2 Operating System Detected (45017)
2 Microsoft Windows Effective Permission on Shares Enumerated (105185)	2 Display BIOS Asset Tag - Chassis (45357)	2 Windows System-Wide Mandatory ASLR with Bottom-Up Randomization Not Enabled (45289)
2 Microsoft SQL Server Version Information Gathered (90087)	2 Microsoft .Net Framework Installed on Target Host (45178)	2 Administrator Group Members Enumerated Using SID (45302)
2 Security Permissions for Important CIFS Pipes (105244)	2 Microsoft Windows File Security Check - C: System Files (105190)	2 Installed Applications Enumerated From Windows Installer (90235)

2 Microsoft Windows Folder Permission Check - Folders Under SystemRoot (105188)
2 Model Information from Devices (45304)
2 Real Name of Built-in Guest Account Enumerated (90266)
2 Microsoft Windows Folder Permission Check - Folders Under System32 (105189)
2 Firewall Product Not Detected on Windows Host (105336)
2 Microsoft SQL Server Service Account Name (105034)
2 Microsoft XML parser (MSXML) Versions Detected (91228)
2 Google Chrome Installed Extensions (45211)
1 Git Installation Detected (45483)
1 Processor And BIOS Information Overview On Windows (43567)
1 Microsoft Silverlight Version (115635)
1 Java Development Kit (JDK) /Java Runtime Environment (JRE) 1.7 Installed (45188)
1 Windows Forensics MRU Enumeration - WordPad Files (125018)
1 Local Firewall Status on Windows Detected (45506)
1 McAfee Data Loss Prevention Endpoint Agent not Installed (45272)
1 Microsoft SQL Server Desktop Engine Installed (45163)
1 NTFS Settings Enumerated (45063)
1 Internet Protocol version 6 (IPv6) Enabled on Target Host (45193)
1 Microsoft Windows Malicious Software Removal Tool Detected (121213)
1 Windows Builtin User Group Membership Audit - Server Operators (105242)
1 Access to File Share is Enabled (90331)
1 Windows Builtin User Group Membership Audit - Replicator (105240)
1 Microsoft Windows System Hardware Enumeration, IDE Controllers (105055)
1 File Access Permissions for Regedt32.exe (105141)
1 Microsoft Windows Network Level Authentication Disabled (90788)
1 Message For Users Attempting To Logon To Windows System (105179)
1 Microsoft Windows Server 2012 R2 Operating System Detected (45348)
1 Microsoft Windows ScForceOption Registry Key Detected (45425)
1 Microsoft Windows Print Spooler Service is running (45498)
1 Windows Host Local Group and Their Respective Users Detected (48202)
1 Microsoft Windows System Hardware Enumeration: Serial, Parallel and USB Device Drivers (105060)
1 Windows WMI AuthenticationLevel Status (45456)
1 Enabled Display Last Username (90008)
1 SMB share list (78020)
1 Windows Services List (90065)
1 Windows Boot Method Detected (45309)
1 Sun Java Runtime Environment Installed (45095)
1 Internet Explorer Search Companion Setting (105291)
1 Microsoft Windows Last Reboot Date and Time (90924)
1 Microsoft Active Directory Organizational Unit (OU) Information (48032)
1 File Access Permissions for Regedit.exe (105154)
1 Status of Remote Desktop/Terminal Service (45381)
1 Operating System's Install Date and Time (91074)
1 Processor Information for Windows Target System (43113)
1 Memory Information (115049)
1 Microsoft Windows System EventLog Policy Parameters (105165)
1 Network Adapter MAC Address (43007)
1 Microsoft Windows User Access Control Enabled (45454)
1 Secure Channel (Schannel) Secure Sockets Layer (SSL) and Transport Layer Security (TLS) Registry Keys Reporting (48039)
1 Windows Product Type (90107)
1 Java Version Detected (45125)
1 Java Enabled in the Internet Zone (100141)
1 System and BaseBoard Serial Numbers (45208)
1 Microsoft Windows Hostname and Domain Name Information (45325)
1 Disabled Clear Page File (90013)
1 Microsoft Windows System Hardware Enumeration, CPU (105054)
1 Microsoft Windows Security EventLog Policy Parameters (105167)
1 Possible Log Recording Issues (90014)
1 Microsoft Defender Installed (105310)
1 Windows Builtin User Group Membership Audit - Account Operators (105243)
1 Microsoft Visual C++ 2008 Redistributable Package Detected (45354)
1 Host Names Found (45039)
1 Windows Connected Printers Information Extracted Through WMI (48203)
1 Windows CDROM Autorun Enabled (90012)
1 Enabled Caching of Dial-up Password Feature (90015)
1 Microsoft Windows System Hardware Enumeration, Input Devices (105058)
1 SMB Version 2 or 3 Enabled (45262)
1 System Architecture Information for Windows and Unix Platform Detected (45501)
1 Google Chrome Web Browser Detected (45105)
1 IPSEC Policy Agent Service Status Detected (105256)
1 Microsoft SQL Server Express Edition Installed (45156)
1 Symantec Endpoint Protection Software Detected (115832)
1 Microsoft Windows System Hardware Enumeration, Networking Components (105059)
1 Domain Controller Detection (90036)
1 Windows Automatic Update Information (105008)
1 Microsoft Windows User Last Logon Time (90925)
1 Qualys Cloud Agent Detected (45421)
1 Windows Host Domain Information (45265)
1 Microsoft Windows Audit Settings Enumerated From LSA (105063)
1 Trusted Digitial Certificates Enumerated From Windows Registry (45231)
1 Group Policy Objects Processed By SecCli are Enumerated from History Log (105238)
1 Windows Host Domain Role (45486)
1 Windows Internet Explorer Version (90295)
1 Host Scan Time (45038)
1 SMB Version 1 Enabled (45261)
1 Interface Names and Assigned IP Address Enumerated from Registry (45099)
1 Report TimeZone Information (45366)
1 Windows Registry Access Level (105025)
1 Microsoft Windows System Hardware Enumeration, Display
1 Windows Builtin User Group Membership Audit - Network
1 Installed Software information enumerated from all users

Devices (105056)

1 Microsoft Internet Explorer 11 Detected (100274)

1 Windows Running Service Permissions (45414)

1 PowerShell Detected On Host (45254)

1 Microsoft System Center Configuration Manager Client (SCCM) Not Installed (105504)

1 Processor Microcode Revision Information Overview On Windows (43576)

Configuration Operators (105241)

1 MultiThreading is Enabled (45489)

1 Installed Locale settings on Host (45382)

1 Programs Launched At Startup Through The Registry (90074)

1 Microsoft Windows Application EventLog Policy Parameters (105166)

1 Windows Builtin User Group Membership Audit - Backup Operators (105239)

using HKU registry key (372899)

1 Windows Forensics MRU Enumeration - Regedit.exe (125017)

1 Microsoft Windows Management Instrumentation Service (WMI) Is Running (45183)

1 Network Interface Information Extracted Through WMI (45232)

1 System Management BIOS UUID Detected (45303)

1 Microsoft Windows An Automatic Updater Of Revoked Certificates Is Installed (KB 2677070 or KB 2813430) (45225)

1 BITS running on target (90346)

192.168.1.150 (Network) (-) | Ricoh Printer

Total: 20 CPS: 100% Vulnerabilities: 2 1 8 7 2

Vulnerabilities (20) for 192.168.1.150

5 Bssaudio Soundweb London Default Credentials Detected (38853) port 21/tcp

5 EOL/Obsolete Software: SNMP Protocol Version Detected (105459)

4 Unauthenticated Access to FTP Server Allowed (27210) port 21/tcp

3 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0) (38628) port 443/tcp over ssl

3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32) (38657) port 443/tcp over ssl

3 Readable SNMP Information (78030) port 161/udp

3 Remote Management Service Accepting Unencrypted Credentials Detected (FTP) (48169)

3 TLS Padding Oracle Vulnerability (Zombie POODLE and GOLDENDOODLE) (38764) port 443/tcp over ssl

3 Remote Management Service Accepting Unencrypted Credentials Detected (Telnet) (48168)

3 FTP Server Does Not Support AUTH Command (27356) port 21/tcp

3 NFS Exported Filesystems List Vulnerability (66002)

2 SSL Certificate - Signature Verification Failed Vulnerability (38173) port 443/tcp over ssl

2 AutoComplete Attribute Not Disabled for Password in Form Based Authentication (86729) port 443/tcp

2 AutoComplete Attribute Not Disabled for Password in Form Based Authentication (86729) port 80/tcp

2 SSL Certificate - Invalid Maximum Validity Date Detected (38685) port 443/tcp over ssl

2 Hidden RPC Services (11)

2 SSL Certificate - Subject Common Name Does Not Match Server FQDN (38170) port 443/tcp over ssl

2 SSL Certificate - Self-Signed Certificate (38169) port 443/tcp over ssl

1 mountd RPC Daemon Discloses Exported Directories Accessed by Remote Hosts (66036)

1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1) (38794) port 443/tcp over ssl

Information Gathered for 192.168.1.150

3 Remote Access or Management Service Detected (42017)

2 Web Server HTTP Protocol Versions (45266) port 8080/tcp

1 List of devices available on this host (78009)

2 Open RPC Services List (9) port 111/tcp

2 Operating System Detected (45017)

1 Open TCP Services List (82023)

2 FTP Server Banner (27113) port 21/tcp

1 SSL Server default Diffie-Hellman prime information (38609) port 443/tcp

1 Web Server Not Scanned for Possible Vulnerabilities (86509) port 443/tcp

CYBERMENT

- 1 Web Server Not Scanned for Possible Vulnerabilities (86509) port 80/tcp
- 1 SSL Certificate - Information (86002) port 443/tcp
- 1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods (38704) port 443/tcp
- 1 List of storage devices connected to this host (78008)
- 1 Network Adapter MAC Address (43007)
- 1 DNS Host Name (6)
- 1 ICMP Replies Received (82040)
- 1 Interface list (78001)
- 1 UDP listening sockets (78006)
- 1 TCP listening sockets (78005)
- 1 Information about this host (78016)
- 1 HTTP Response Method and Header Information Collected (48118) port 8080/tcp
- 1 Scan Activity per Port (45426)
- 1 Firewall Detected (34011)
- 1 Network information (78017)
- 1 Host Names Found (45039)
- 1 Telnet Banner (38007) port 23/tcp
- 1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties (38706) port 443/tcp
- 1 SSL Session Caching Information (38291) port 443/tcp
- 1 SSL Server Information Retrieval (38116) port 443/tcp
- 1 Routing table (78003)
- 1 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance (38597) port 443/tcp
- 1 Host Scan Time (45038)
- 1 Degree of Randomness of TCP Initial Sequence Numbers (82045)
- 1 Traceroute (45006)
- 1 Default Web Page (12230) port 443/tcp
- 1 Default Web Page (12230) port 80/tcp
- 1 Default Web Page (12230) port 8080/tcp
- 1 ARP table (78004)
- 1 TLS Secure Renegotiation Extension Support Information (42350) port 443/tcp
- 1 Open UDP Services List (82004)
- 1 IP ID Values Randomness (82046)
- 1 General information about this host (78000)
- 1 Default Web Page (Follow HTTP Redirection) (13910) port 443/tcp
- 1 Default Web Page (Follow HTTP Redirection) (13910) port 80/tcp
- 1 Default Web Page (Follow HTTP Redirection) (13910) port 8080/tcp
- 1 IP addresses via SNMP (78002)

192.168.1.156 (Network) (srvbackup.domain.local; SRVBACKUP) | Windows 2016/2019/10

Total: 1 CPS: 40% Vulnerabilities: 0 0 0 1 0

Vulnerabilities (1) for 192.168.1.156

2 NetBIOS Name Accessible (70000)

Information Gathered for 192.168.1.156

- 3 Remote Access or Management Service Detected (42017)
- 3 NetBIOS Bindings Information (70004)
- 2 Operating System Detected (45017)
- 2 Windows Registry Pipe Access Level (90194)
- 2 Open DCE-RPC / MS-RPC Services List (70022)
- 1 NetBIOS Host Name (82044)
- 1 Open TCP Services List (82023)
- 1 File and Print Services Access Denied (70038)
- 1 IP ID Values Randomness (82046)
- 1 Windows Authentication Not Attempted (105296)
- 1 Network Adapter MAC Address (43007)
- 1 DNS Host Name (6)
- 1 ICMP Replies Received (82040)
- 1 NetBIOS Workgroup Name Detected (82062)
- 1 Scan Activity per Port (45426)
- 1 Firewall Detected (34011)
- 1 SMB Version 2 or 3 Enabled (45262)
- 1 Host Names Found (45039)
- 1 Windows Authentication Method (70028)
- 1 Host Scan Time (45038)
- 1 Degree of Randomness of TCP Initial Sequence Numbers (82045)
- 1 Traceroute (45006)
- 1 Open UDP Services List (82004)

192.168.1.156 (Agent) (srvbackup.domain.local; SRVBACKUP) | Windows 10 Pro 64 bit Edition Version 21H2

Total: 7 CPS: 50% Vulnerabilities: 0 1 2 4 0

Vulnerabilities (7) for 192.168.1.156

4 Microsoft Windows Codecs Library HEVC Video and VP9 Extensions Remote Code Execution (RCE) Vulnerability for February 2022 (91866)

3 SMB Signing Disabled or SMB Signing Not Required (90043)

3 Built-in Guest Account Not Renamed at Windows Target System (105228)

2 Microsoft Windows Explorer AutoPlay Not Disabled (105170)

2 Enabled Cached Logon Credential (90007)

2 Windows Explorer Autoplay Not Disabled for Default User (105171)

2 Allowed Null Session (90044)

Information Gathered for 192.168.1.156

3 BHOs Detected (90139)

3 Machine Security Group Membership Information (48116)

3 Microsoft Windows Defender is Deactivated (121345)

3 Microsoft Windows Socket Parameters, TCP/IP Hardening Guidelines (90127)

3 Administrator Group Members Enumerated (105231)

3 Microsoft Windows TCP Parameters, TCP/IP Hardening Guidelines (90128)

3 Sticky Key's Enabled on System (124403)

3 Microsoft Windows Link-Local Multicast Name Resolution (LLMNR) Not Disabled (45290)

3 SAMR Pipe Permissions Enumerated (105237)

2 Microsoft .Net Framework Installed on Target Host (45178)

2 Last Successful User Login (105311)

2 Operating System Detected (45017)

2 Microsoft Windows Effective Permission on Shares Enumerated (105185)

2 Installed Applications Enumerated From Windows Installer (90235)

2 Administrator Group Members Enumerated Using SID (45302)

2 Full Disk Encryption Software Detected (105325)

2 Microsoft Windows File Security Check - C: System Files (105190)

2 Windows Auto Reboot After Blue Screen Not Disabled (105172)

2 Security Permissions for Important CIFS Pipes (105244)

2 Microsoft Windows Folder Permission Check - Folders Under SystemRoot (105188)

2 Model Information from Devices (45304)

2 Microsoft Windows Folder Permission Check - Folders Under System32 (105189)

2 Real Name of Built-in Guest Account Enumerated (90266)

2 Google Chrome Installed Extensions (45211)

2 Antivirus Information Extracted Using WMI for Windows Desktop (105591)

2 Microsoft XML parser (MSXML) Versions Detected (91228)

1 Git Installation Detected (45483)

1 Processor And BIOS Information Overview On Windows (43567)

1 Windows WMI AuthenticationLevel Status (45456)

1 Enabled Display Last Username (90008)

1 SMB share list (78020)

1 Windows Services List (90065)

1 Local Firewall Status on Windows Detected (45506)

1 McAfee Data Loss Prevention Endpoint Agent not Installed (45272)

1 NTFS Settings Enumerated (45063)

1 Bitlocker Encryption Status Information (45437)

1 Internet Protocol version 6 (IPv6) Enabled on Target Host (45193)

1 Microsoft Windows Malicious Software Removal Tool Detected (121213)

1 Access to File Share is Enabled (90331)

1 Windows Builtin User Group Membership Audit - Replicator (105240)

1 File Access Permissions for Regedt32.exe (105141)

1 Message For Users Attempting To Logon To Windows System (105179)

1 Microsoft Windows ScForceOption Registry Key Detected (45425)

1 Microsoft Windows Print Spooler Service is running (45498)

1 Windows Host Local Group and Their Respective Users Detected (48202)

1 Microsoft Windows Last Reboot Date and Time (90924)

1 Microsoft Active Directory Organizational Unit (OU) Information (48032)

1 File Access Permissions for Regedit.exe (105154)

1 Status of Remote Desktop/Terminal Service (45381)

1 Operating System's Install Date and Time (91074)

1 Microsoft Windows Network Level Authentication Enabled (45379)

1 Processor Information for Windows Target System (43113)

1 Memory Information (115049)

1 Java Enabled in the Internet Zone (100141)

1 Microsoft Visual C++ 2005 Redistributable Package Detected (45333)

1 Internet Explorer Search Companion Setting (105291)

1 System and BaseBoard Serial Numbers (45208)

1 Windows Boot Method Detected (45309)

1 Microsoft Windows Hostname and Domain Name Information (45325)

1 Disabled Clear Page File (90013)

1 Microsoft Windows System Hardware Enumeration, CPU (105054)

1 Microsoft Windows Security EventLog Policy Parameters (105167)

1 Possible Log Recording Issues (90014)

1 Microsoft Windows System EventLog Policy Parameters (105165)

1 Network Adapter MAC Address (43007)

1 Microsoft Windows User Access Control Enabled (45454)

1 Windows Product Type (90107)

1 Microsoft Defender Installed (105310)

1 Enabled Shutdown Without Logon (90009)

1 IPSEC Policy Agent Service Status Detected (105256)

1 Host Names Found (45039)

1 Windows Connected Printers Information Extracted

1 Windows CDROM Autorun Enabled (90012)

- Through WMI (48203)
- Enabled Caching of Dial-up Password Feature (90015)
- SMB Version 2 or 3 Enabled (45262)
- System Architecture Information for Windows and Unix Platform Detected (45501)
- Google Chrome Web Browser Detected (45105)
- Trusted Platform Module (TPM) Detected on Windows (45321)
- Trusted Digitial Certificates Enumerated From Windows Registry (45231)
- Group Policy Objects Processed By SecCli are Enumerated from History Log (105238)
- Microsoft Windows Fast Startup Feature Is Enabled (45445)
- Windows Host Domain Role (45486)
- Windows Internet Explorer Version (90295)
- Host Scan Time (45038)
- Interface Names and Assigned IP Address Enumerated from Registry (45099)
- Report TimeZone Information (45366)
- Windows Running Service Permissions (45414)
- Installed Locale settings on Host (45382)
- Microsoft Windows System Hardware Enumeration, Networking Components (105059)
- Microsoft Windows 10 Operating System Detected (45342)
- Microsoft Windows User Last Logon Time (90925)
- Qualys Cloud Agent Detected (45421)
- Windows Host Domain Information (45265)
- Microsoft Windows Audit Settings Enumerated From LSA (105063)
- Windows Registry Access Level (105025)
- Microsoft Windows System Hardware Enumeration, Display Devices (105056)
- Windows Builtin User Group Membership Audit - Network Configuration Operators (105241)
- Installed Software information enumerated from all users using HKU registry key (372899)
- Microsoft Internet Explorer 11 Detected (100274)
- MultiThreading is Enabled (45489)
- Microsoft Windows Sense agent Detected (45453)
- PowerShell Detected On Host (45254)
- Programs Launched At Startup Through The Registry (90074)
- Microsoft Windows Management Instrumentation Service (WMI) Is Running (45183)
- Microsoft Windows An Automatic Updater Of Revoked Certificates Is Installed (KB 2677070 or KB 2813430) (45225)
- Processor Microcode Revision Information Overview On Windows (43576)
- Network Interface Information Extracted Through WMI (45232)
- Microsoft System Center Configuration Manager Client (SCCM) Not Installed (105504)
- Microsoft Windows Application EventLog Policy Parameters (105166)
- System Management BIOS UUID Detected (45303)
- Windows Builtin User Group Membership Audit - Backup Operators (105239)
- Microsoft OneDrive Software Detected (45428)