TEST

Report generated by Tenable Nessus™ Wed, 27 Aug 2025 23:45:54 Taipei Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.9.1

Vulnerabilities Total: 72

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
HIGH	7.5*	-	0.9233	41028	SNMP Agent Default Community Name (public)
MEDIUM	6.5	-	0.7623	187201	OpenSSH < 9.6 Multiple Vulnerabilities
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	5.3	-	-	57608	SMB Signing not required
MEDIUM	5.3	-	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0*	-	0.0787	76474	SNMP 'GETBULK' Reflection DDoS
LOW	3.8	-	0.0001	234554	OpenSSH < 10.0 DisableForwarding
LOW	2.1*	-	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	42255	NFS Server Superfluous
INFO	N/A	-	-	10223	RPC portmapper Service Detection
INFO	N/A	-	-	46180	Additional DNS Hostnames
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution

INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remo check)
INFO	N/A	-	-	14274	Nessus SNMP Scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	103869	Open Network Video Interface Forum (ONVIF) Protocol Detect
INFO	N/A	-	-	181418	OpenSSH Detection
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	11111	RPC Services Enumeration
INFO	N/A	-	-	53335	RPC portmapper (TCP)
INFO	N/A	-	-	31097	RTMP Server Detection
INFO	N/A	-	-	10762	RTSP Server Type / Version Detection
INFO	N/A	-	-	35296	SNMP Protocol Version Detection
INFO	N/A	-	-	34022	SNMP Query Routing Information Disclosure
INFO	N/A	-	-	10550	SNMP Query Running Process List Disclosure
INFO	N/A	-	-	10800	SNMP Query System Information Disclosure
INFO	N/A	-	-	10551	SNMP Request Network Interfaces Enumeration

INFO	N/A	-	-	185519	SNMP Server Detection
INFO	N/A	-	-	40448	SNMP Supported Protocols Detection
INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	-	10863	SSL Certificate Information
INFO	N/A	-	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	72341	Synology DiskStation Manager (DSM) Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	-	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	-	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	-	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	-	135860	WMI Not Available
INFO	N/A	-	-	10386	Web Server No 404 Error Code Check
INFO	N/A	-	-	35712	Web Server UPnP Detection

INFO	N/A	-	-	10302	Web Server robots.txt Information Disclosure
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	-	66717	mDNS Detection (Local Network)
INFO	N/A	-	-	106375	nginx HTTP Server Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.2

Vulnerabilities Total: 3

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
INFO	N/A	-	-	11933	Do not scan printers
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.151

Vulnerabilities Total: 24

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
MEDIUM	5.3	-	-	57608	SMB Signing not required
INFO	N/A	-	-	46180	Additional DNS Hostnames
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10736	DCE Services Enumeration
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remo check)
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	43815	NetBIOS Multiple IP Address Enumeration
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available

INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	135860	WMI Not Available
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.154

Vulnerabilities Total: 6

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
MEDIUM	6.5	-	-	11901	TCP/IP Multicast Address Handling Remote DoS (spank.c)
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.157

Vulnerabilities Total: 19

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
INFO	N/A	-	-	127858	Apple AirPlay Web Detection
INFO	N/A	-	-	93741	Apple TV Version Detection
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	11002	DNS Server Detection
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	66717	mDNS Detection (Local Network)

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.160

Vulnerabilities Total: 7

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
LOW	2.1*	-	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.161

Vulnerabilities Total: 5

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	11834	Source Routed Packet Weakness
INFO	N/A	-	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.163

Vulnerabilities Total: 17

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
LOW	2.1*	-	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	10919	Open Port Re-check
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.164

Vulnerabilities Total: 16

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
INFO	N/A	-	-	11002	DNS Server Detection
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	66717	mDNS Detection (Local Network)

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.165

Vulnerabilities Total: 5

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
LOW	2.1*	-	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.166

Vulnerabilities Total: 8

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
LOW	2.1*	-	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	66717	mDNS Detection (Local Network)

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.167

Vulnerabilities Total: 15

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
LOW	2.1*	-	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	66717	mDNS Detection (Local Network)

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.169

Vulnerabilities Total: 17

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
MEDIUM	6.5	-	0.0596	50686	IP Forwarding Enabled
INFO	N/A	-	-	11002	DNS Server Detection
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	66717	mDNS Detection (Local Network)

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.170

Vulnerabilities Total: 5

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	11834	Source Routed Packet Weakness
INFO	N/A	-	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.174

Vulnerabilities Total: 5

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
LOW	2.1*	-	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.182

Vulnerabilities Total: 32

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
MEDIUM	5.9	-	0.7623	187315	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)
LOW	2.1*	-	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	10223	RPC portmapper Service Detection
INFO	N/A	-	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	11919	HMAP Web Server Fingerprinting
INFO	N/A	-	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	181418	OpenSSH Detection

INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	11111	RPC Services Enumeration
INFO	N/A	-	-	53335	RPC portmapper (TCP)
INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	66717	mDNS Detection (Local Network)

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.184

Vulnerabilities Total: 26

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
HIGH	7.5*	-	0.9233	41028	SNMP Agent Default Community Name (public)
MEDIUM	6.1	-	0.2183	136929	JQuery 1.2 < 3.5.0 Multiple XSS
MEDIUM	5.0*	-	0.0787	76474	SNMP 'GETBULK' Reflection DDoS
LOW	2.1*	-	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	106658	JQuery Detection
INFO	N/A	-	-	14274	Nessus SNMP Scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	35296	SNMP Protocol Version Detection
INFO	N/A	-	-	34022	SNMP Query Routing Information Disclosure
INFO	N/A	-	-	10800	SNMP Query System Information Disclosure

INFO	N/A	-	-	10551	SNMP Request Network Interfaces Enumeration
INFO	N/A	-	-	185519	SNMP Server Detection
INFO	N/A	-	-	40448	SNMP Supported Protocols Detection
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	106628	lighttpd HTTP Server Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.185

Vulnerabilities Total: 5

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
LOW	2.1*	-	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.186

Vulnerabilities Total: 18

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
LOW	2.1*	-	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	11153	Service Detection (HELP Request)
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.187

Vulnerabilities Total: 8

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
LOW	2.1*	-	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	66717	mDNS Detection (Local Network)

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.193

Vulnerabilities Total: 17

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
LOW	2.1*	-	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	103869	Open Network Video Interface Forum (ONVIF) Protocol Detect
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.195

Vulnerabilities Total: 29

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
LOW	2.1*	-	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	10863	SSL Certificate Information

INFO	N/A	-	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.196

Vulnerabilities Total: 7

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	66717	mDNS Detection (Local Network)

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.198

Vulnerabilities Total: 12

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	66717	mDNS Detection (Local Network)

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.204

Vulnerabilities Total: 30

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
LOW	2.1*	-	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	185519	SNMP Server Detection
INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	56984	SSL / TLS Versions Supported

INFO	N/A	-	-	10863	SSL Certificate Information
INFO	N/A	-	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.227

Vulnerabilities Total: 38

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10736	DCE Services Enumeration
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	11919	HMAP Web Server Fingerprinting
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
INFO	N/A	-	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remo check)
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10147	Nessus Server Detection
INFO	N/A	-	-	64582	Netstat Connection Information

INFO	N/A	-	-	174736	Netstat Ingress Connections
INFO	N/A	-	-	14272	Netstat Portscanner (SSH)
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	97993	OS Identification and Installed Software Enumeration over SSH (Using New SSH Library)
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	-	10863	SSL Certificate Information
INFO	N/A	-	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	-	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	-	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	-	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	135860	WMI Not Available
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.237

Vulnerabilities Total: 5

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	11834	Source Routed Packet Weakness
INFO	N/A	-	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.239

Vulnerabilities Total: 3

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10287	Traceroute Information

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.253

Vulnerabilities Total: 24

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
MEDIUM	5.9	-	0.7623	187315	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)
LOW	2.1*	-	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	42823	Non-compliant Strict Transport Security (STS)
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	42822	Strict Transport Security (STS) Detection

INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.9.254

Vulnerabilities Total: 47

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
MEDIUM	6.5	-	0.0596	50686	IP Forwarding Enabled
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	157288	TLS Version 1.1 Deprecated Protocol
MEDIUM	5.9	-	0.7623	187315	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)
LOW	3.3*	-	-	10663	DHCP Server Detection
LOW	2.1*	-	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	106658	JQuery Detection
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available

INFO	N/A	-	-	181418	OpenSSH Detection
INFO	N/A	-	-	71495	Palo Alto Networks PAN-OS Firewall/Panorama Web UI Detect
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	83298	SSL Certificate Chain Contains Certificates Expiring Soon
INFO	N/A	-	-	42981	SSL Certificate Expiry - Future Expiry
INFO	N/A	-	-	10863	SSL Certificate Information
INFO	N/A	-	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	11153	Service Detection (HELP Request)
INFO	N/A	-	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	-	-	87242	TLS NPN Supported Protocol Enumeration
INFO	N/A	-	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	-	138330	TLS Version 1.3 Protocol Detection

INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	10302	Web Server robots.txt Information Disclosure

* indicates the v3.0 score was not available; the v2.0 score is shown