



Scan2

Report generated by Nessus™

Fri, 04 Aug 2023 16:47:51 Central Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

• 192.168.1.1.....	4
• 192.168.1.15.....	6
• 192.168.1.104.....	8
• 192.168.1.110.....	9
• 192.168.1.129.....	10
• 192.168.1.187.....	11
• 192.168.1.211.....	12
• 192.168.1.217.....	13
• 192.168.1.227.....	14
• 192.168.1.252.....	15

Nessus Essentials

Vulnerabilities by Host

192.168.1.1



Vulnerabilities

Total: 37

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	4.0	50686	IP Forwarding Enabled
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
LOW	3.3*	-	10663	DHCP Server Detection
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	72779	DNS Server Version 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	-	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	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information

INFO	N/A	-	11936	OS Identification
INFO	N/A	-	50845	OpenSSL Detection
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	-	94761	SSL Root Certification Authority Certificate Information
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	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	-	10386	Web Server No 404 Error Code Check
INFO	N/A	-	35712	Web Server UPnP Detection

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

192.168.1.15



Vulnerabilities

Total: 18

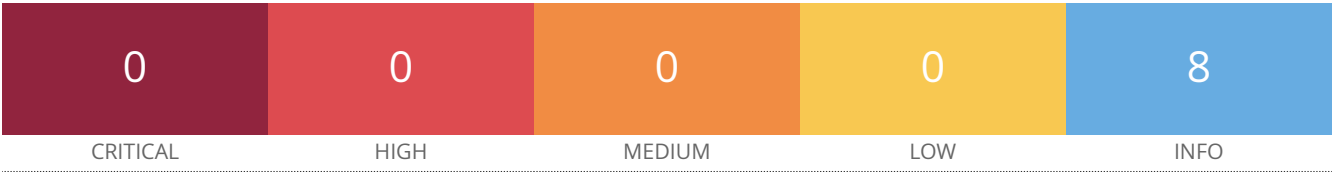
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	5.3	-	57608	SMB Signing not required
INFO	N/A	-	12634	Authenticated Check : OS Name and Installed Package Enumeration
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10736	DCE Services Enumeration
INFO	N/A	-	54615	Device Type
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
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 (remote check)
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	97993	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
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

192.168.1.104

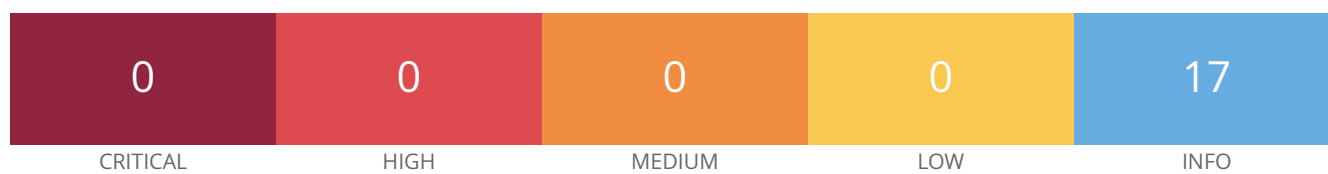


Vulnerabilities Total: 8

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	54615	Device Type
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
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

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

192.168.1.110



Vulnerabilities

Total: 17

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	19689	Embedded Web Server Detection
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	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
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	-	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	-	35712	Web Server UPnP Detection

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

192.168.1.129



Vulnerabilities

Total: 5

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
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

192.168.1.187



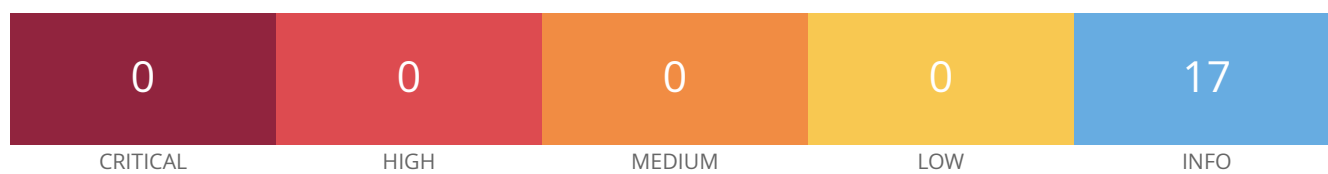
Vulnerabilities

Total: 4

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	11933	Do not scan printers
INFO	N/A	-	14274	Nessus SNMP Scanner
INFO	N/A	-	19506	Nessus Scan Information
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

192.168.1.211



Vulnerabilities

Total: 17

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	54615	Device Type
INFO	N/A	-	19689	Embedded Web Server Detection
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	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
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	-	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	-	10386	Web Server No 404 Error Code Check
INFO	N/A	-	35712	Web Server UPnP Detection

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

192.168.1.217



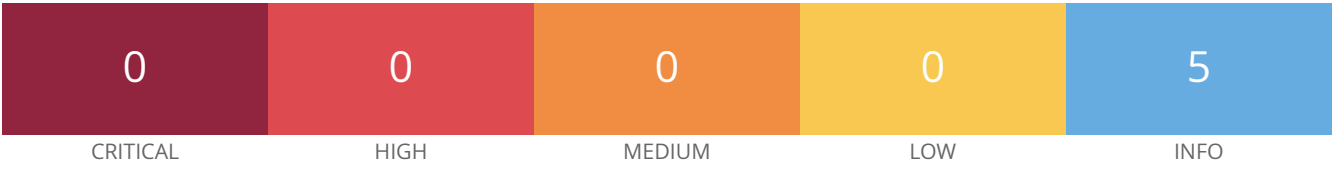
Vulnerabilities

Total: 9

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
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	-	11936	OS Identification
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	35711	Universal Plug and Play (UPnP) Protocol Detection

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

192.168.1.227

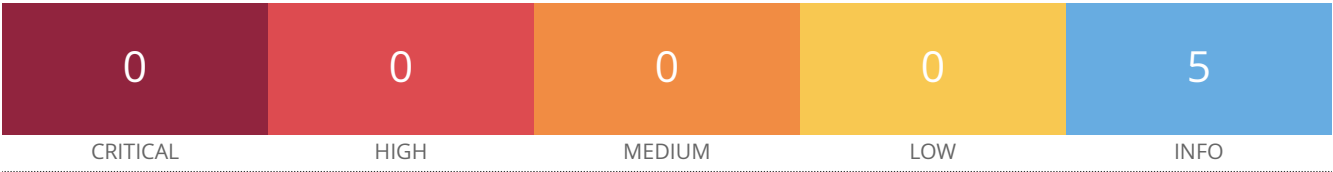


Vulnerabilities Total: 5

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	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

192.168.1.252



Vulnerabilities Total: 5

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
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