



network scan

Report generated by Nessus™

Mon, 09 Oct 2023 14:40:29 EST

TABLE OF CONTENTS

Vulnerabilities by Host

• 192.168.0.1.....	4
• 192.168.0.15.....	6
• 192.168.0.19.....	7
• 192.168.0.20.....	8
• 192.168.0.100.....	9
• 192.168.0.101.....	11
• 192.168.0.104.....	12
• 192.168.0.108.....	15
• 192.168.0.109.....	16
• 192.168.0.127.....	18

Vulnerabilities by Host

192.168.0.1



Vulnerabilities

Total: 37

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
HIGH	7.5	-	35291	SSL Certificate Signed Using Weak Hashing Algorithm
HIGH	7.5	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	-	50686	IP Forwarding Enabled
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	5.9	-	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.3	-	134220	nginx < 1.17.7 Information Disclosure
LOW	3.3*	-	10663	DHCP Server Detection
LOW	3.3*	-	11197	Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)
LOW	N/A	-	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10028	DNS Server BIND version Directive Remote Version Detection
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	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11387	L2TP Network Server Detection
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	66334	Patch Report
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	-	62563	SSL Compression Methods 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	-	10287	Traceroute Information
INFO	N/A	-	106375	nginx HTTP Server Detection

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

192.168.0.15



Vulnerabilities

Total: 15

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	50686	IP Forwarding Enabled
MEDIUM	5.3	-	12217	DNS Server Cache Snooping Remote Information Disclosure
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	-	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	-	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

192.168.0.19



Vulnerabilities

Total: 17

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	50686	IP Forwarding Enabled
MEDIUM	5.3	-	134220	nginx < 1.17.7 Information Disclosure
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	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	10195	HTTP Proxy Open Relay Detection
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	66334	Patch Report
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	106375	nginx HTTP Server Detection

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

192.168.0.20



Vulnerabilities

Total: 14

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	50686	IP Forwarding Enabled
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	11002	DNS Server Detection
INFO	N/A	-	35371	DNS Server hostname.bind Map Hostname Disclosure
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	-	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

192.168.0.100



Vulnerabilities

Total: 22

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
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	-	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	-	56984	SSL / TLS Versions Supported
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	-	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	-	35712	Web Server UPnP Detection
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

192.168.0.101



Vulnerabilities

Total: 5

SEVERITY	CVSS V3.0	VPR 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	-	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

192.168.0.104



Vulnerabilities

Total: 48

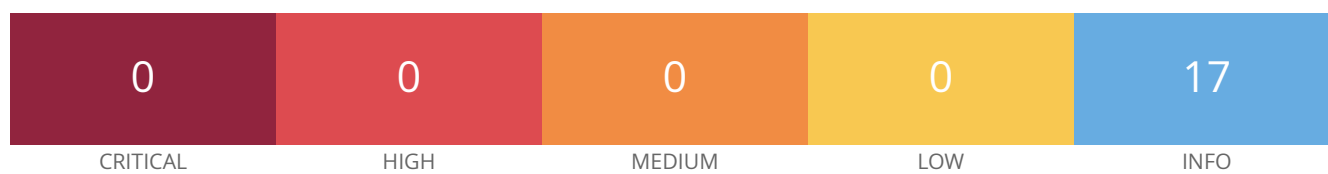
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
INFO	N/A	-	141394	Apache HTTP Server Installed (Linux)
INFO	N/A	-	142640	Apache HTTP Server Site Enumeration
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	55472	Device Hostname
INFO	N/A	-	54615	Device Type
INFO	N/A	-	25203	Enumerate IPv4 Interfaces via SSH
INFO	N/A	-	25202	Enumerate IPv6 Interfaces via SSH
INFO	N/A	-	33276	Enumerate MAC Addresses via SSH
INFO	N/A	-	170170	Enumerate the Network Interface configuration via SSH
INFO	N/A	-	179200	Enumerate the Network Routing configuration via SSH
INFO	N/A	-	168980	Enumerate the PATH Variables
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	-	171410	IP Assignment Method Detection
INFO	N/A	-	147817	Java Detection and Identification (Linux / Unix)
INFO	N/A	-	151883	Libgcrypt Installed (Linux/UNIX)

INFO	N/A	-	157358	Linux Mounted Devices
INFO	N/A	-	95928	Linux User List Enumeration
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10147	Nessus Server Detection
INFO	N/A	-	64582	Netstat Connection Information
INFO	N/A	-	14272	Netstat Portscanner (SSH)
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	-	117887	OS Security Patch Assessment Available
INFO	N/A	-	148373	OpenJDK Java Detection (Linux / Unix)
INFO	N/A	-	168007	OpenSSL Installed (Linux)
INFO	N/A	-	130024	PostgreSQL Client/Server Installed (Linux)
INFO	N/A	-	45405	Reachable IPv6 address
INFO	N/A	-	174788	SQLite Local Detection (Linux)
INFO	N/A	-	56984	SSL / TLS Versions Supported
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	-	22869	Software Enumeration (SSH)
INFO	N/A	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	110095	Target Credential Issues by Authentication Protocol - No Issues Found
INFO	N/A	-	141118	Target Credential Status by Authentication Protocol - Valid Credentials Provided

INFO	N/A	-	163326	Tenable Nessus Installed (Linux)
INFO	N/A	-	56468	Time of Last System Startup
INFO	N/A	-	110483	Unix / Linux Running Processes Information
INFO	N/A	-	152742	Unix Software Discovery Commands Available
INFO	N/A	-	136340	nginx Installed (Linux/UNIX)

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

192.168.0.108



Vulnerabilities

Total: 17

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	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
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	-	11936	OS Identification
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	-	10287	Traceroute Information
INFO	N/A	-	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	-	35712	Web Server UPnP Detection
INFO	N/A	-	66717	mDNS Detection (Local Network)

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

192.168.0.109



Vulnerabilities

Total: 33

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	50686	IP Forwarding Enabled
MEDIUM	5.3	-	57608	SMB Signing not required
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
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	-	10107	HTTP Server Type and Version
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	-	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	-	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	10395	Microsoft Windows SMB Shares Enumeration
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	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	10919	Open Port Re-check
INFO	N/A	-	10860	SMB Use Host SID to Enumerate Local Users
INFO	N/A	-	25240	Samba Server Detection
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	10386	Web Server No 404 Error Code Check
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

192.168.0.127



Vulnerabilities

Total: 26

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	5.3	-	57608	SMB Signing not required
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	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
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	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	43815	NetBIOS Multiple IP Address Enumeration
INFO	N/A	-	11936	OS Identification

INFO	N/A	-	22964	Service Detection
INFO	N/A	-	11153	Service Detection (HELP Request)
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	-	135860	WMI Not Available
INFO	N/A	-	35712	Web Server UPnP Detection
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