My Basic Network Scan

Vulnerabilities by Host

Vulnerabilities by Host

192.168.0.1

1	0	1	4	27
CRITICAL	HIGH	MEDIUM	LOW	INFO
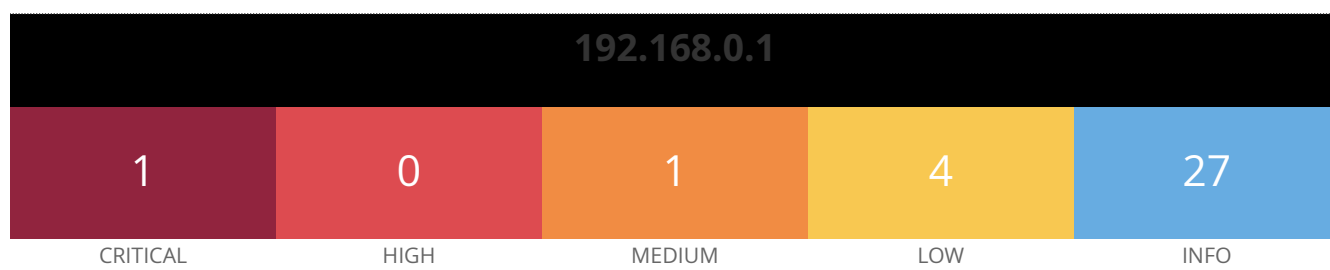
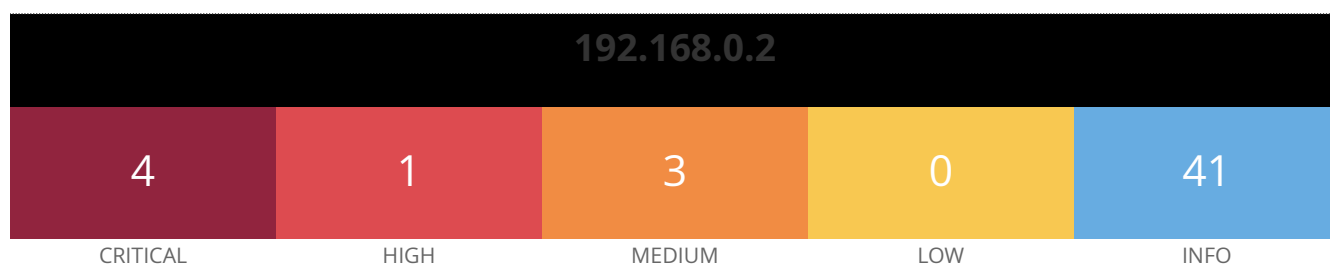Vulnerabilities   Total: 33

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	93650	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
MEDIUM	5.0*	70545	Dropbear SSH Server < 2013.59 Multiple Vulnerabilities
LOW	3.7	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.3*	10663	DHCP Server Detection
LOW	2.6*	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	71049	SSH Weak MAC Algorithms Enabled
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	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	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	73125	NAT-PMP Detection (local network)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information

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	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	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	35712	Web Server UPnP Detection

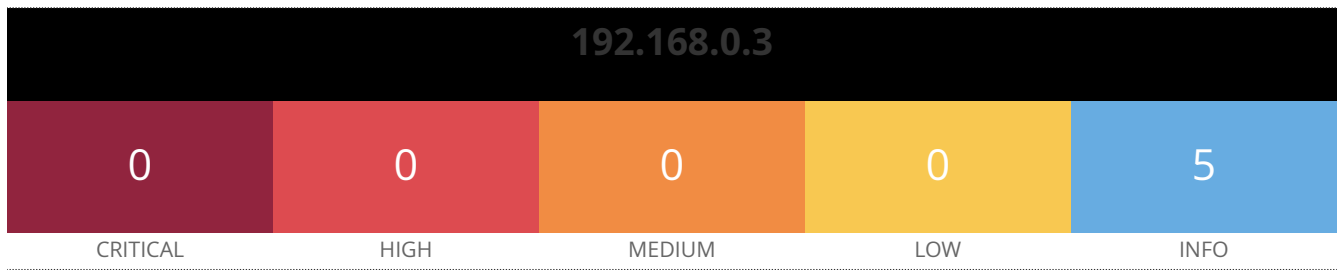* indicates the v3.0 score was not available; the v2.0 score is shown

4	1	3	0	41
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities

Total: 49

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	156860	Apache Log4j 1.x Multiple Vulnerabilities
CRITICAL	9.0	156057	Apache Log4j 2.x < 2.16.0 RCE
CRITICAL	10.0	155999	Apache Log4j < 2.15.0 Remote Code Execution (Nix)
CRITICAL	10.0	156032	Apache Log4j Unsupported Version Detection
HIGH	7.5	156103	Apache Log4j 1.2 JMSAppender Remote Code Execution (CVE-2021-4104)
MEDIUM	6.6	156327	Apache Log4j 2.0 < 2.3.2 / 2.4 < 2.12.4 / 2.13 < 2.17.1 RCE
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	5.9	156183	Apache Log4j 2.x < 2.17.0 DoS
INFO	N/A	141394	Apache HTTP Server Installed (Linux)
INFO	N/A	142640	Apache HTTP Server Site Enumeration
INFO	N/A	156000	Apache Log4j Installed (Linux / Unix)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	55472	Device Hostname
INFO	N/A	54615	Device Type
INFO	N/A	159273	Dockerfile Detection for Linux/UNIX
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	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	151883	Libgcrypt Installed (Linux/UNIX)
INFO	N/A	95928	Linux User List Enumeration
INFO	N/A	130626	MariaDB Client/Server Installed (Linux)
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	66334	Patch Report
INFO	N/A	130024	PostgreSQL Client/Server Installed (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	138330	TLS Version 1.3 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	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

192.168.0.3

0	0	0	0	5
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities

Total: 5

SEVERITY	CVSS V3.0	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

192.168.0.4

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	11
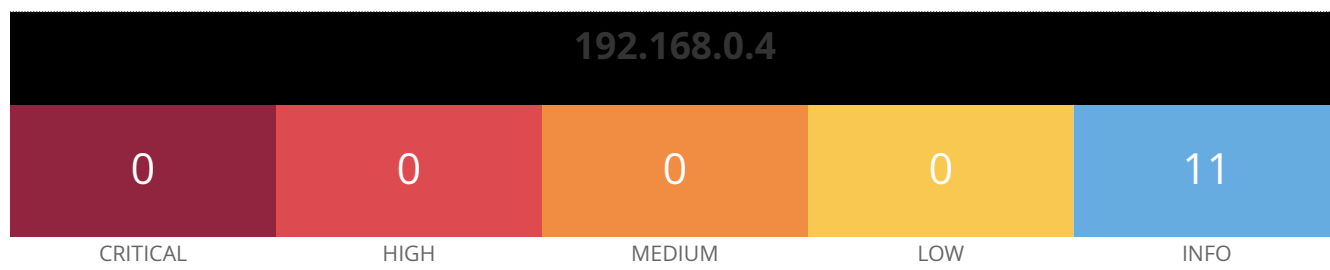
Vulnerabilities   Total: 11

SEVERITY	CVSS V3.0	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	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
INFO	N/A	11154	Unknown Service Detection: Banner Retrieval

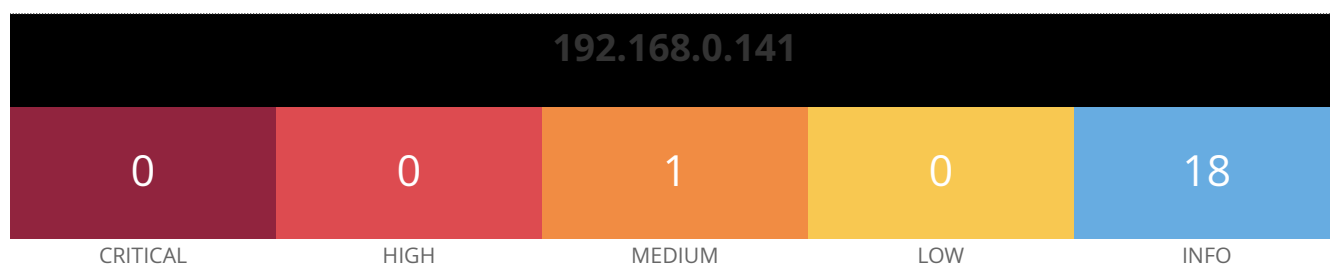* indicates the v3.0 score was not available; the v2.0 score is shown

192.168.0.126

0	0	0	3	17
CRITICAL	HIGH	MEDIUM	LOW	INFO
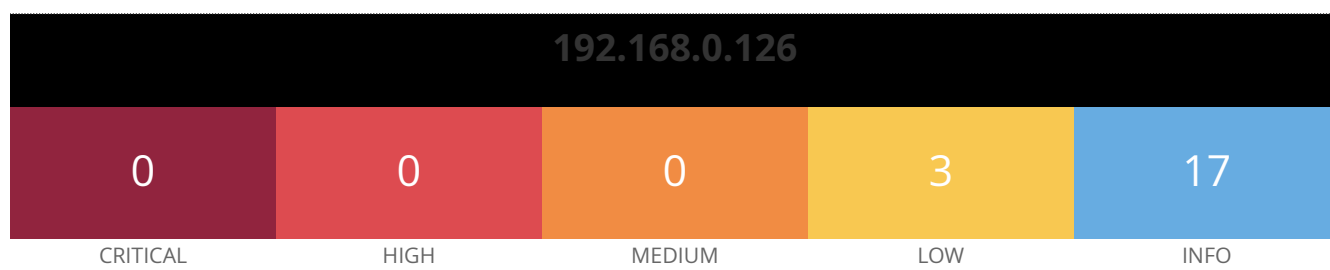
Vulnerabilities   Total: 20

SEVERITY	CVSS V3.0	PLUGIN	NAME
LOW	3.7	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	54615	Device Type
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	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	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 |

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

0	0	1	0	18
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities   Total: 19

SEVERITY	CVSS V3.0	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	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	11936	OS Identification
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	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

192.168.0.195

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	11
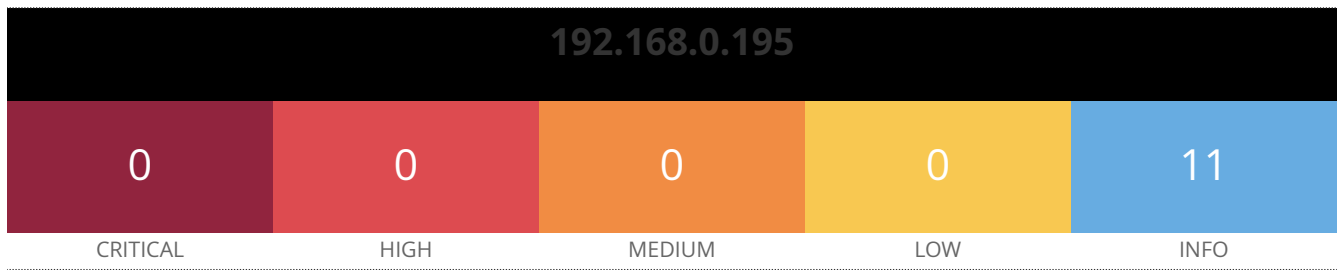
Vulnerabilities   Total: 11

SEVERITY	CVSS V3.0	PLUGIN	NAME
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	86420	Ethernet MAC Addresses
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	11936	OS Identification
INFO	N/A	26024	PostgreSQL Server Detection
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