



AV interno

Report generated by Nessus™

Tue, 24 Nov 2020 22:42:39 -05

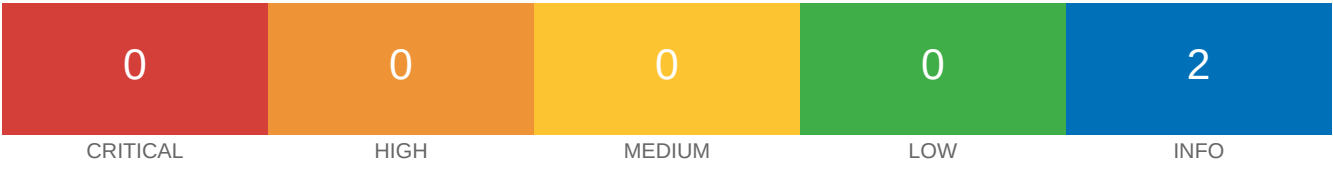
TABLE OF CONTENTS

Hosts Executive Summary

• 172.16.1.1.....	4
• 172.16.1.7.....	5
• 172.16.1.12.....	6
• 172.16.1.25.....	9
• 172.16.1.46.....	10
• 172.16.1.103.....	11
• 172.16.1.111.....	12
• 172.16.1.156.....	13
• 172.16.1.180.....	15
• 181.118.158.2.....	16

Hosts Executive Summary

172.16.1.1



Vulnerabilities Total: 2

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	19506	Nessus Scan Information

172.16.1.7

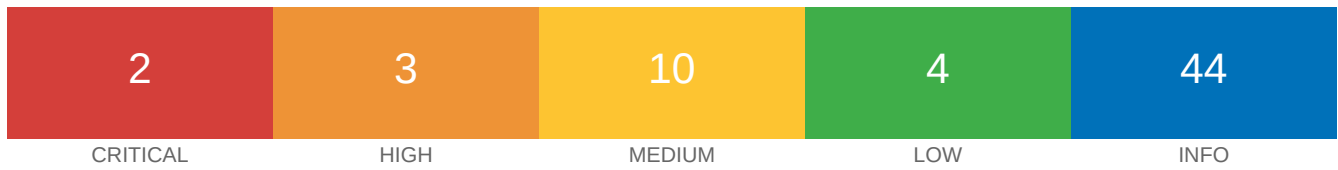


Vulnerabilities

Total: 14

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	4.3	87734	SMB Password Encryption Not Required
MEDIUM	4.3	10891	X Display Manager Control Protocol (XDMCP) Detection
INFO	N/A	10223	RPC portmapper Service Detection
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	10437	NFS Share Export List
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	43815	NetBIOS Multiple IP Address Enumeration
INFO	N/A	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	11111	RPC Services Enumeration
INFO	N/A	135860	WMI Not Available
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

172.16.1.12



Vulnerabilities

Total: 63

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0	10203	rexecd Service Detection
HIGH	7.5	69552	Oracle TNS Listener Remote Poisoning
HIGH	7.5	41028	SNMP Agent Default Community Name (public)
HIGH	7.1	20007	SSL Version 2 and 3 Protocol Detection
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	97861	Network Time Protocol (NTP) Mode 6 Scanner
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
MEDIUM	4.3	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	4.3	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.3	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
MEDIUM	4.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	2.6	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)

INFO	N/A	42255	NFS Server Superfluous
INFO	N/A	10223	RPC portmapper Service Detection
INFO	N/A	39520	Backported Security Patch Detection (SSH)
INFO	N/A	10833	CDE Subprocess Control Service (dtspcd) Detection
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10052	Daytime Service 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	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	117886	Local Checks Not Enabled (info)
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	110723	No Credentials Provided
INFO	N/A	11936	OS Identification
INFO	N/A	22073	Oracle Database Detection
INFO	N/A	10658	Oracle Database tnslnr Service Remote Version Disclosure
INFO	N/A	66334	Patch Report
INFO	N/A	11111	RPC Services Enumeration
INFO	N/A	53335	RPC portmapper (TCP)

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	40448	SNMP Supported Protocols Detection
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	10881	SSH Protocol Versions Supported
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	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	51891	SSL Session Resume Supported
INFO	N/A	22964	Service Detection
INFO	N/A	17975	Service Detection (GET request)
INFO	N/A	11153	Service Detection (HELP Request)

172.16.1.25



Vulnerabilities

Total: 16

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	10223	RPC portmapper Service Detection
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
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	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	11936	OS Identification
INFO	N/A	11111	RPC Services Enumeration
INFO	N/A	104887	Samba Version
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	135860	WMI Not Available

172.16.1.46

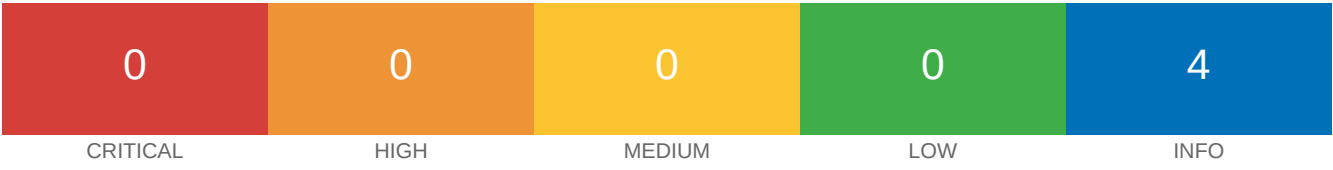


Vulnerabilities

Total: 4

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	4.3	10891	X Display Manager Control Protocol (XDMCP) Detection
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	23778	SLP Server Detection (UDP)

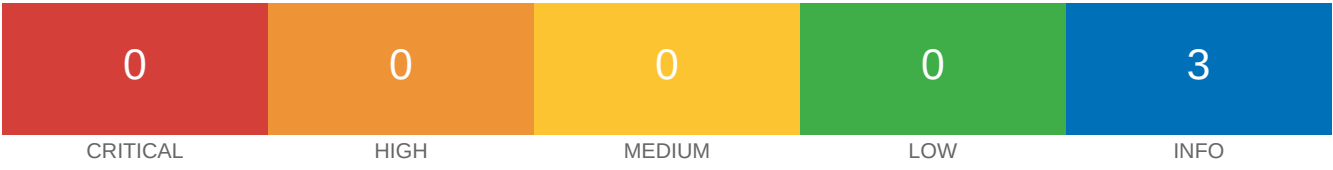
172.16.1.103



Vulnerabilities Total: 4

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	10223	RPC portmapper Service Detection
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11111	RPC Services Enumeration

172.16.1.111



Vulnerabilities Total: 3

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	10223	RPC portmapper Service Detection
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11111	RPC Services Enumeration

172.16.1.156



Vulnerabilities

Total: 20

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	5.0	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	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	117886	Local Checks Not Enabled (info)
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	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	110723	No Credentials Provided
INFO	N/A	11936	OS Identification
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	20094	VMware Virtual Machine Detection

INFO	N/A	135860	WMI Not Available
------	-----	--------	-------------------

INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
------	-----	-------	--

172.16.1.180



Vulnerabilities Total: 6

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	10223	RPC portmapper Service Detection
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	11111	RPC Services Enumeration
INFO	N/A	66717	mDNS Detection (Local Network)

181.118.158.2



Vulnerabilities

Total: 30

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	43111	HTTP Methods Allowed (per directory)
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	11936	OS Identification
INFO	N/A	31422	Reverse NAT/Intercepting Proxy Detection
INFO	N/A	18528	SMTP Server Connection Check
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	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	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	91815	Web Application Sitemap
INFO	N/A	11032	Web Server Directory Enumeration