metasploitable3_ubuntu_basicScan

Report generated by Nessus™ Mon, 27 Feb 2023 11:24:25 EET

Vulnerabilities by Host

Vulnerabilities by Host

192.168.56.104

Vulnerabilities Total: 69

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	9.8	84215	ProFTPD mod_copy Information Disclosure
CRITICAL	10.0*	92626	Drupal Coder Module Deserialization RCE
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5*	78515	Drupal Database Abstraction API SQLi
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
MEDIUM	5.3	10704	Apache Multiviews Arbitrary Directory Listing
MEDIUM	5.3	57608	SMB Signing not required
MEDIUM	4.3*	90317	SSH Weak Algorithms Supported
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	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	39519	Backported Security Patch Detection (FTP)
INFO	N/A	39520	Backported Security Patch Detection (SSH)

INFO	N/A	39521	Backported Security Patch Detection (WWW)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	18638	Drupal Software Detection
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	10092	FTP Server Detection
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	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	60119	Microsoft Windows SMB Share Permissions Enumeration
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	10719	MySQL 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	117886	OS Security Patch Assessment Not Available
INFO	N/A	66334	Patch Report
INFO	N/A	10860	SMB Use Host SID to Enumerate Local Users
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	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	25240	Samba Server Detection
INFO	N/A	104887	Samba Version
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
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	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	10287	Traceroute Information
INFO	N/A	66293	Unix Operating System on Extended Support
INFO	N/A	135860	WMI Not Available

INFO	N/A	20108	Web Server / Application favicon.ico Vendor Fingerprinting
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