



Vulnerability scan -task1

Report generated by Tenable Nessus™

Sun, 08 Jun 2025 08:08:55 BST

TABLE OF CONTENTS

Vulnerabilities by Host

- 20.84.67.45..... 4

Nessus Essentials

Vulnerabilities by Host

20.84.67.45



Vulnerabilities

Total: 23

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
MEDIUM	6.5	-	-	18405	Remote Desktop Protocol Server Man-in-the-Middle Weakness
INFO	N/A	-	-	48204	Apache HTTP Server Version
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	-	-	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	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	181418	OpenSSH Detection
INFO	N/A	-	-	10940	Remote Desktop Protocol Service Detection
INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
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	-	-	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