



test 3

Report generated by Nessus™

Sun, 03 Mar 2024 18:06:41 CET

TABLE OF CONTENTS

Vulnerabilities by Host

• 192.168.1.246.....	4
----------------------	---

Nessus Essentials

Vulnerabilities by Host

192.168.1.246



Vulnerabilities

Total: 32

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	10.0	10.0	156056	Apache Log4Shell RCE detection via Raw Socket Logging (Direct Check)
CRITICAL	10.0	10.0	156197	Apache Log4Shell RCE detection via callback correlation (Direct Check NetBIOS)
CRITICAL	10.0	10.0	156232	Apache Log4Shell RCE detection via callback correlation (Direct Check SMB)
CRITICAL	10.0	-	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	7.3	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
HIGH	8.1	9.7	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (unauthenticated check)
MEDIUM	6.8	6.0	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (unauthenticated check)
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	-	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
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	-	24786	Nessus Windows Scan Not Performed with Admin Privileges
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	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
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	-	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