



# Ubuntu\_Vm\_\_Simple\_Vulnerability\_Scan

Report generated by Nessus™

Fri, 26 Apr 2024 18:41:25 EEST

---

## TABLE OF CONTENTS

---

### Vulnerabilities by Host

• 192.168.44.4.....	4
---------------------	---

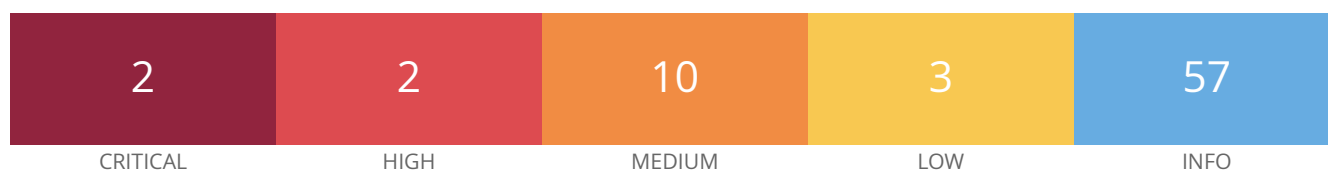
Nessus Essentials

---

## **Vulnerabilities by Host**

---

192.168.44.4



## Vulnerabilities

Total: 74

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	7.4	84215	ProFTPD mod_copy Information Disclosure
CRITICAL	10.0*	-	92626	Drupal Coder Module Deserialization RCE
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5*	7.4	78515	Drupal Database Abstraction API SQLi
MEDIUM	6.5	4.0	50686	IP Forwarding Enabled
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	5.9	6.7	187315	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)
MEDIUM	5.3	2.2	10704	Apache Multiviews Arbitrary Directory Listing
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	4.0	2.2	10114	ICMP Timestamp Request Remote Date Disclosure
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
LOW	3.7	3.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	48204	Apache HTTP Server Version

INFO	N/A	-	<a href="#">39519</a>	Backported Security Patch Detection (FTP)
INFO	N/A	-	<a href="#">39520</a>	Backported Security Patch Detection (SSH)
INFO	N/A	-	<a href="#">39521</a>	Backported Security Patch Detection (WWW)
INFO	N/A	-	<a href="#">45590</a>	Common Platform Enumeration (CPE)
INFO	N/A	-	<a href="#">54615</a>	Device Type
INFO	N/A	-	<a href="#">18638</a>	Drupal Software Detection
INFO	N/A	-	<a href="#">19689</a>	Embedded Web Server Detection
INFO	N/A	-	<a href="#">35716</a>	Ethernet Card Manufacturer Detection
INFO	N/A	-	<a href="#">86420</a>	Ethernet MAC Addresses
INFO	N/A	-	<a href="#">10092</a>	FTP Server Detection
INFO	N/A	-	<a href="#">43111</a>	HTTP Methods Allowed (per directory)
INFO	N/A	-	<a href="#">10107</a>	HTTP Server Type and Version
INFO	N/A	-	<a href="#">24260</a>	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	<a href="#">42410</a>	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
INFO	N/A	-	<a href="#">17651</a>	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	-	<a href="#">10859</a>	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	-	<a href="#">10785</a>	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	<a href="#">11011</a>	Microsoft Windows SMB Service Detection
INFO	N/A	-	<a href="#">60119</a>	Microsoft Windows SMB Share Permissions Enumeration
INFO	N/A	-	<a href="#">10395</a>	Microsoft Windows SMB Shares Enumeration
INFO	N/A	-	<a href="#">100871</a>	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	<a href="#">106716</a>	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	<a href="#">10719</a>	MySQL Server Detection

INFO	N/A	-	<a href="#">11219</a>	Nessus SYN scanner
INFO	N/A	-	<a href="#">19506</a>	Nessus Scan Information
INFO	N/A	-	<a href="#">11936</a>	OS Identification
INFO	N/A	-	<a href="#">117886</a>	OS Security Patch Assessment Not Available
INFO	N/A	-	<a href="#">181418</a>	OpenSSH Detection
INFO	N/A	-	<a href="#">66334</a>	Patch Report
INFO	N/A	-	<a href="#">10180</a>	Ping the remote host
INFO	N/A	-	<a href="#">10860</a>	SMB Use Host SID to Enumerate Local Users
INFO	N/A	-	<a href="#">70657</a>	SSH Algorithms and Languages Supported
INFO	N/A	-	<a href="#">149334</a>	SSH Password Authentication Accepted
INFO	N/A	-	<a href="#">10881</a>	SSH Protocol Versions Supported
INFO	N/A	-	<a href="#">153588</a>	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	<a href="#">10267</a>	SSH Server Type and Version Information
INFO	N/A	-	<a href="#">56984</a>	SSL / TLS Versions Supported
INFO	N/A	-	<a href="#">45410</a>	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	<a href="#">10863</a>	SSL Certificate Information
INFO	N/A	-	<a href="#">70544</a>	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	<a href="#">21643</a>	SSL Cipher Suites Supported
INFO	N/A	-	<a href="#">156899</a>	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	<a href="#">25240</a>	Samba Server Detection
INFO	N/A	-	<a href="#">104887</a>	Samba Version
INFO	N/A	-	<a href="#">96982</a>	Server Message Block (SMB) Protocol Version 1 Enabled (unauthenticated check)
INFO	N/A	-	<a href="#">22964</a>	Service Detection
INFO	N/A	-	<a href="#">17975</a>	Service Detection (GET request)
INFO	N/A	-	<a href="#">25220</a>	TCP/IP Timestamps Supported

INFO	N/A	-	<a href="#">121010</a>	TLS Version 1.1 Protocol Detection
INFO	N/A	-	<a href="#">110723</a>	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	<a href="#">10287</a>	Traceroute Information
INFO	N/A	-	<a href="#">66293</a>	Unix Operating System on Extended Support
INFO	N/A	-	<a href="#">135860</a>	WMI Not Available
INFO	N/A	-	<a href="#">20108</a>	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	-	<a href="#">10150</a>	Windows NetBIOS / SMB Remote Host Information Disclosure

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