



Kioptrix 1.2

Report generated by Nessus™

Sat, 06 Mar 2021 06:43:30 EST

TABLE OF CONTENTS

Hosts Executive Summary

• 192.168.103.144.....	4
------------------------	---

Nessus Essentials

Hosts Executive Summary

192.168.103.144



Vulnerabilities

Total: 57

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
HIGH	7.5	42424	CGI Generic SQL Injection (blind)
HIGH	7.5	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3)
MEDIUM	5.0	40984	Browsable Web Directories
MEDIUM	5.0	39467	CGI Generic Path Traversal
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	46803	PHP expose_php Information Disclosure
MEDIUM	5.0	57640	Web Application Information Disclosure
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
MEDIUM	4.3	85582	Web Application Potentially Vulnerable to Clickjacking
MEDIUM	4.3	51425	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6	26194	Web Server Transmits Cleartext Credentials
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	84574	Backported Security Patch Detection (PHP)
INFO	N/A	39520	Backported Security Patch Detection (SSH)

INFO	N/A	39521	Backported Security Patch Detection (WWW)
INFO	N/A	47830	CGI Generic Injectable Parameter
INFO	N/A	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	39470	CGI Generic Tests Timeout
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	132634	Deprecated SSLv2 Connection Attempts
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	49704	External URLs
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	14788	IP Protocols Scan
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	50345	Missing or Permissive X-Frame-Options HTTP Response Header
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	48243	PHP Version Detection
INFO	N/A	66334	Patch Report
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	22964	Service Detection
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	20094	VMware Virtual Machine Detection
INFO	N/A	100669	Web Application Cookies Are Expired
INFO	N/A	85601	Web Application Cookies Not Marked HttpOnly
INFO	N/A	85602	Web Application Cookies Not Marked Secure
INFO	N/A	91815	Web Application Sitemap
INFO	N/A	42057	Web Server Allows Password Auto-Completion
INFO	N/A	11032	Web Server Directory Enumeration
INFO	N/A	10662	Web mirroring
INFO	N/A	17219	phpMyAdmin Detection