Tests

Report generated by Nessus™ Mon, 16 Apr 2018 17:00:29 FLE Standard Time

TABLE OF CONTENTS

Hosts Executive Summary

Hosts Executive Summary

192.168.234.130

Vulnerabilities Total: 63

SEVERITY	CVSS	PLUGIN	NAME
HIGH	8.5	107219	PHP 7.2.x < 7.2.3 Stack Buffer Overflow
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	11229	Web Server info.php / phpinfo.php Detection
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	40984	Browsable Web Directories
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	46803	PHP expose_php Information Disclosure
MEDIUM	5.0	57608	SMB Signing Disabled
MEDIUM	5.0	108758	Apache 2.4.x < 2.4.30 Multiple Vulnerabilities
LOW	2.6	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
INFO	N/A	10092	FTP Server Detection
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	10287	Traceroute Information
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10662	Web mirroring

INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	11032	Web Server Directory Enumeration
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	11419	Web Server Office File Inventory
INFO	N/A	11936	OS Identification
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	14788	IP Protocols Scan
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	22964	Service Detection
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	43815	NetBIOS Multiple IP Address Enumeration
INFO	N/A	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	46215	Inconsistent Hostname and IP Address

INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	48243	PHP Version Detection
INFO	N/A	49704	External URLs
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	50845	OpenSSL Detection
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	57323	OpenSSL Version Detection
INFO	N/A	66334	Patch Report
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	84502	HSTS Missing From HTTPS Server
INFO	N/A	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	91634	HyperText Transfer Protocol (HTTP) Redirect Information
INFO	N/A	91815	Web Application Sitemap
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	104743	TLS Version 1.0 Protocol Detection
INFO	N/A	106658	JQuery Detection
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)

192.168.234.131

Vulnerabilities Total: 105

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
HIGH	8.3	59088	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution
HIGH	7.8	55976	Apache HTTP Server Byte Range DoS
HIGH	7.5	19704	TWiki 'rev' Parameter Arbitrary Command Execution
HIGH	7.5	36171	phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)
HIGH	7.5	39465	CGI Generic Command Execution
HIGH	7.5	39469	CGI Generic Remote File Inclusion
HIGH	7.5	42424	CGI Generic SQL Injection (blind)
HIGH	7.5	70728	Apache PHP-CGI Remote Code Execution
MEDIUM	6.8	42872	CGI Generic Local File Inclusion (2nd pass)
MEDIUM	6.8	90509	Samba Badlock Vulnerability
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	11229	Web Server info.php / phpinfo.php Detection
MEDIUM	5.0	11411	Backup Files Disclosure
MEDIUM	5.0	36083	phpMyAdmin file_path Parameter Vulnerabilities (PMASA-2009-1)
MEDIUM	5.0	39467	CGI Generic Path Traversal
MEDIUM	5.0	40984	Browsable Web Directories

MEDIUM	5.0	42256	NFS Shares World Readable
MEDIUM	5.0	46195	CGI Generic Path Traversal (extended test)
MEDIUM	5.0	46803	PHP expose_php Information Disclosure
MEDIUM	5.0	57608	SMB Signing Disabled
MEDIUM	5.0	57640	Web Application Information Disclosure
MEDIUM	4.3	39466	CGI Generic XSS (quick test)
MEDIUM	4.3	44136	CGI Generic Cookie Injection Scripting
MEDIUM	4.3	47831	CGI Generic XSS (comprehensive test)
MEDIUM	4.3	49067	CGI Generic HTML Injections (quick test)
MEDIUM	4.3	49142	phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)
MEDIUM	4.3	51425	phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)
MEDIUM	4.3	55903	CGI Generic XSS (extended patterns)
MEDIUM	4.3	57792	Apache HTTP Server httpOnly Cookie Information Disclosure
MEDIUM	4.3	85582	Web Application Potentially Vulnerable to Clickjacking
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
LOW	2.6	10407	X Server Detection
LOW	2.6	26194	Web Server Transmits Cleartext Credentials
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled
INFO	N/A	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	10092	FTP Server Detection
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	10223	RPC portmapper Service Detection

INFO	N/A	10263	SMTP Server Detection
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	10287	Traceroute Information
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	10437	NFS Share Export List
INFO	N/A	10662	Web mirroring
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	11002	DNS Server Detection
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	11032	Web Server Directory Enumeration
INFO	N/A	11111	RPC Services Enumeration
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	11419	Web Server Office File Inventory
INFO	N/A	11424	WebDAV Detection
INFO	N/A	11819	TFTP Daemon Detection
INFO	N/A	11936	OS Identification
INFO	N/A	14788	IP Protocols Scan
INFO	N/A	17219	phpMyAdmin Detection
INFO	N/A	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	19941	TWiki Detection
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	22964	Service Detection

INFO	N/A	24004	WebDAV Directory Enumeration
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	25240	Samba Server Detection
INFO	N/A	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	39470	CGI Generic Tests Timeout
INFO	N/A	39520	Backported Security Patch Detection (SSH)
INFO	N/A	39521	Backported Security Patch Detection (WWW)
INFO	N/A	40773	Web Application Potentially Sensitive CGI Parameter Detection
INFO	N/A	42057	Web Server Allows Password Auto-Completion
INFO	N/A	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	47830	CGI Generic Injectable Parameter
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	48243	PHP Version Detection
INFO	N/A	49704	External URLs
INFO	N/A	49705	Web Server Harvested Email Addresses
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	52703	vsftpd Detection
INFO	N/A	53335	RPC portmapper (TCP)

INFO	N/A	66334	Patch Report
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	72779	DNS Server Version Detection
INFO	N/A	84574	Backported Security Patch Detection (PHP)
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	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	100669	Web Application Cookies Are Expired
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	104887	Samba Version
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)