Nessus Report

Nessus Scan Report

Wed, 03 May 2017 03:25:30 EDT

Table Of Contents

Hosts Summary (Executive)

192.168.52.137

Summary

Critical	High	Medium	Low	Info	Total
6	3	14	3	64	90

Details

Severity	Plugin Id	Name
Critical (10.0)	10203	rexecd Service Detection
Critical (10.0)	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
Critical (10.0)	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
Critical (10.0)	33850	Unix Operating System Unsupported Version Detection
Critical (10.0)	51988	Rogue Shell Backdoor Detection
Critical (10.0)	61708	VNC Server 'password' Password
High (9.4)	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
High (7.5)	10205	rlogin Service Detection
High (7.5)	34460	Unsupported Web Server Detection
Medium (6.8)	90509	Samba Badlock Vulnerability
Medium (6.4)	11356	NFS Exported Share Information Disclosure
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.8)	42263	Unencrypted Telnet Server
Medium (5.0)	11213	HTTP TRACE / TRACK Methods Allowed
Medium (5.0)	12217	DNS Server Cache Snooping Remote Information Disclosure
Medium (5.0)	15901	SSL Certificate Expiry
Medium (5.0)	42256	NFS Shares World Readable
Medium (5.0)	45411	SSL Certificate with Wrong Hostname
Medium (5.0)	57608	SMB Signing Disabled
Medium (4.3)	57792	Apache HTTP Server httpOnly Cookie Information Disclosure
Medium (4.3)	90317	SSH Weak Algorithms Supported
Medium (4.0)	52611	SMTP Service STARTTLS Plaintext Command Injection
Low (2.6)	10407	X Server Detection
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled

Low (2.6)	71049	SSH Weak MAC Algorithms Enabled
Info	10028	DNS Server BIND version Directive Remote Version Detection
Info	10092	FTP Server Detection
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10223	RPC portmapper Service Detection
Info	10263	SMTP Server Detection
Info	10267	SSH Server Type and Version Information
Info	10281	Telnet Server Detection
Info	10287	Traceroute Information
Info	10342	VNC Software Detection
Info	10394	Microsoft Windows SMB Log In Possible
Info	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
Info	10437	NFS Share Export List
Info	10719	MySQL Server Detection
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10863	SSL Certificate Information
Info	10881	SSH Protocol Versions Supported
Info	11002	DNS Server Detection
Info	11011	Microsoft Windows SMB Service Detection
Info	11111	RPC Services Enumeration
Info	11153	Service Detection (HELP Request)
Info	11154	Unknown Service Detection: Banner Retrieval
Info	11156	IRC Daemon Version Detection
Info	11219	Nessus SYN scanner
Info	11422	Web Server Unconfigured - Default Install Page Present
Info	11424	WebDAV Detection
Info	11819	TFTP Daemon Detection
Info	11936	OS Identification
Info	17975	Service Detection (GET request)

Info	18261	Apache Banner Linux Distribution Disclosure
Info	19288	VNC Server Security Type Detection
Info	19506	Nessus Scan Information
Info	20094	VMware Virtual Machine Detection
Info	20108	Web Server / Application favicon.ico Vendor Fingerprinting
Info	21186	AJP Connector Detection
Info	22227	RMI Registry Detection
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	25240	Samba Server Detection
Info	26024	PostgreSQL Server Detection
Info	35371	DNS Server hostname.bind Map Hostname Disclosure
Info	35716	Ethernet Card Manufacturer Detection
Info	39446	Apache Tomcat Default Error Page Version Detection
Info	39519	Backported Security Patch Detection (FTP)
Info	39520	Backported Security Patch Detection (SSH)
Info	39521	Backported Security Patch Detection (WWW)
Info	42088	SMTP Service STARTTLS Command Support
Info	45410	SSL Certificate commonName Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	48243	PHP Version
Info	50845	OpenSSL Detection
Info	52703	vsftpd Detection
Info	53335	RPC portmapper (TCP)
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	62563	SSL Compression Methods Supported
Info	65792	VNC Server Unencrypted Communication Detection
Info	66334	Patch Report
Info	70657	SSH Algorithms and Languages Supported

Info	72779	DNS Server Version Detection
Info	84574	Backported Security Patch Detection (PHP)
Info	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)