

Nessus Report

Report

21/Mar/2012:09:07:06 GMT

Table Of Contents

Hosts Summary (Executive).....	3
•192.168.1.1.....	4
•192.168.1.10.....	5
•192.168.1.13.....	6
•192.168.1.16.....	7
•192.168.1.30.....	9
•192.168.1.78.....	11
•192.168.1.79.....	12
•192.168.1.80.....	13
•192.168.1.81.....	14
•192.168.1.85.....	15
•192.168.1.200.....	16
•192.168.1.208.....	17
•192.168.1.211.....	18
•192.168.1.213.....	19
•192.168.1.231.....	20
•192.168.1.245.....	21
•192.168.1.248.....	22

Hosts Summary (Executive)

192.168.1.1**Summary**

Critical	High	Medium	Low	Info	Total
0	0	0	0	15	15

Details

Severity	Plugin Id	Name
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10881	SSH Protocol Versions Supported
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	39520	Backported Security Patch Detection (SSH)
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

192.168.1.10

Summary

Critical	High	Medium	Low	Info	Total
1	0	2	0	17	20

Details

Severity	Plugin Id	Name
Critical (10.0)	33850	Unsupported Unix Operating System
Medium (5.0)	10595	DNS Server Zone Transfer Information Disclosure (AXFR)
Medium (5.0)	12217	DNS Server Cache Snooping Remote Information Disclosure
Info	10028	DNS Server BIND version Directive Remote Version Disclosure
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10881	SSH Protocol Versions Supported
Info	11002	DNS Server Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported
Info	35371	DNS Server hostname.bind Map Hostname Disclosure
Info	35373	DNS Server DNSSEC Aware Resolver
Info	35716	Ethernet Card Manufacturer Detection
Info	39520	Backported Security Patch Detection (SSH)
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

192.168.1.13

Summary

Critical	High	Medium	Low	Info	Total
0	0	2	1	19	22

Details

Severity	Plugin Id	Name
Medium (5.0)	12218	mDNS Detection
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Low (2.6)	53491	SSL / TLS Renegotiation DoS
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10223	RPC portmapper Service Detection
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10881	SSH Protocol Versions Supported
Info	11111	RPC Services Enumeration
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	39520	Backported Security Patch Detection (SSH)
Info	45590	Common Platform Enumeration (CPE)
Info	46212	PVS Proxy Detection
Info	53335	RPC portmapper (TCP)
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported

192.168.1.16

Summary

Critical	High	Medium	Low	Info	Total
0	0	3	1	21	25

Details

Severity	Plugin Id	Name
Medium (5.1)	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
Medium (5.0)	57608	SMB Signing Disabled
Medium (4.3)	57690	Terminal Services Encryption Level is Medium or Low
Low (2.6)	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10940	Windows Terminal Services Enabled
Info	11011	Microsoft Windows SMB Service Detection
Info	11153	Service Detection (HELP Request)
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20301	VMware ESX/GSX Server detection
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
Info	35716	Ethernet Card Manufacturer Detection
Info	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
Info	45590	Common Platform Enumeration (CPE)
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection

Info

54615

Device Type

192.168.1.30

Summary

Critical	High	Medium	Low	Info	Total
0	0	6	0	28	34

Details

Severity	Plugin Id	Name
Medium (5.0)	12218	mDNS Detection
Medium (5.0)	26919	Microsoft Windows SMB Guest Account Local User Access
Medium (5.0)	42256	NFS Shares World Readable
Medium (5.0)	45374	AFP Server Directory Traversal
Medium (5.0)	57608	SMB Signing Disabled
Medium (4.3)	57792	Apache HTTP Server httpOnly Cookie Information Disclosure
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	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10395	Microsoft Windows SMB Shares Enumeration
Info	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
Info	10437	NFS Share Export List
Info	10666	Apple Filing Protocol Server Detection
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
Info	10860	SMB Use Host SID to Enumerate Local Users
Info	11011	Microsoft Windows SMB Service Detection
Info	11111	RPC Services Enumeration
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	17651	Microsoft Windows SMB : Obtains the Password Policy
Info	19506	Nessus Scan Information

Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	25240	Samba Server Detection
Info	35716	Ethernet Card Manufacturer Detection
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	53335	RPC portmapper (TCP)
Info	54615	Device Type

192.168.1.78

Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	17	18

Details

Severity	Plugin Id	Name
Medium (5.0)	12217	DNS Server Cache Snooping Remote Information Disclosure
Info	10028	DNS Server BIND version Directive Remote Version Disclosure
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	10386	Web Server No 404 Error Code Check
Info	11002	DNS Server Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35371	DNS Server hostname.bind Map Hostname Disclosure
Info	35373	DNS Server DNSSEC Aware Resolver
Info	35716	Ethernet Card Manufacturer Detection
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

192.168.1.79

Summary

Critical	High	Medium	Low	Info	Total
0	0	2	0	15	17

Details

Severity	Plugin Id	Name
Medium (5.0)	10595	DNS Server Zone Transfer Information Disclosure (AXFR)
Medium (5.0)	12217	DNS Server Cache Snooping Remote Information Disclosure
Info	10028	DNS Server BIND version Directive Remote Version Disclosure
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	11002	DNS Server Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35371	DNS Server hostname.bind Map Hostname Disclosure
Info	35373	DNS Server DNSSEC Aware Resolver
Info	35716	Ethernet Card Manufacturer Detection
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

192.168.1.80

Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	14	15

Details

Severity	Plugin Id	Name
Medium (5.0)	18262	TFTP Traversal Arbitrary File Access
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	11026	Wireless Access Point Detection
Info	11219	Nessus SYN scanner
Info	11819	TFTP Daemon Detection
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	44318	HNAP Detection
Info	44391	Linksys Router Detection
Info	54615	Device Type

192.168.1.81

Summary

Critical	High	Medium	Low	Info	Total
0	0	4	1	17	22

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	12218	mDNS Detection
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Low (2.6)	42880	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20813	TiVo Detection
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	45590	Common Platform Enumeration (CPE)
Info	50845	OpenSSL Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported

192.168.1.85

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Details

Severity	Plugin Id	Name
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	19506	Nessus Scan Information
Info	35716	Ethernet Card Manufacturer Detection

192.168.1.200

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	10	10

Details

Severity	Plugin Id	Name
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	10919	Open Port Re-check
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	54615	Device Type

192.168.1.208

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	3	4

Details

Severity	Plugin Id	Name
Low (3.2)	50686	IP Forwarding Enabled
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	19506	Nessus Scan Information
Info	35716	Ethernet Card Manufacturer Detection

192.168.1.211

Summary

Critical	High	Medium	Low	Info	Total
0	0	2	0	11	13

Details

Severity	Plugin Id	Name
Medium (6.4)	43156	NTP ntpd Mode 7 Error Response Packet Loop Remote DoS
Medium (5.0)	12218	mDNS Detection
Info	10287	Traceroute Information
Info	10884	Network Time Protocol (NTP) Server Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	42825	Apple TV Detection
Info	54615	Device Type

192.168.1.213

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	12	12

Details

Severity	Plugin Id	Name
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	17975	Service Detection (GET request)
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported
Info	35712	Web Server UPnP Detection
Info	35716	Ethernet Card Manufacturer Detection
Info	54615	Device Type

Summary

Critical	High	Medium	Low	Info	Total
0	0	2	0	22	24

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Info	10107	HTTP Server Type and Version
Info	10147	Nessus Server Detection
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10267	SSH Server Type and Version Information
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	10881	SSH Protocol Versions Supported
Info	10884	Network Time Protocol (NTP) Server Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20108	Web Server / Application favicon.ico Vendor Fingerprinting
Info	20217	iTunes Music Sharing Enabled
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35716	Ethernet Card Manufacturer Detection
Info	39520	Backported Security Patch Detection (SSH)
Info	45590	Common Platform Enumeration (CPE)
Info	56693	Dropbox Software Detection (uncredentialed check)
Info	56984	SSL / TLS Versions Supported

192.168.1.245

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	2	2

Details

Severity	Plugin Id	Name
Info	11933	Do not scan printers
Info	19506	Nessus Scan Information

Summary

Critical	High	Medium	Low	Info	Total
11	43	25	2	12	93

Details

Severity	Plugin Id	Name
Critical (10.0)	55172	USN-1154-1 : openjdk-6, openjdk-6b18 vulnerabilities
Critical (10.0)	55407	USN-1149-1 : firefox, xulrunner-1.9.2 vulnerabilities
Critical (10.0)	55921	USN-1184-1 : firefox, xulrunner-1.9.2 vulnerabilities
Critical (10.0)	56330	USN-1210-1 : firefox, xulrunner-1.9.2 vulnerabilities
Critical (10.0)	56860	USN-1263-1 : icedtea-web, openjdk-6, openjdk-6b18 vulnerabilities
Critical (10.0)	57436	USN-1317-1 : ghostscript vulnerabilities
Critical (10.0)	57685	USN-1263-2 : openjdk-6, openjdk-6b18 regression
Critical (10.0)	57844	USN-1355-1 : firefox vulnerabilities
Critical (10.0)	57874	USN-1353-1 : xulrunner-1.9.2 vulnerabilities
Critical (10.0)	58069	USN-1370-1 : libvorbis vulnerability
Critical (10.0)	58130	USN-1373-1 : openjdk-6 vulnerabilities
High (9.3)	55168	USN-1153-1 : libxml2 vulnerability
High (9.3)	55858	USN-1191-1 : libxfont vulnerability
High (9.3)	56775	USN-1251-1 : firefox, xulrunner-1.9.2 vulnerabilities
High (9.3)	56870	USN-1267-1 : freetype vulnerabilities
High (9.3)	57449	USN-1320-1 : ffmpeg vulnerabilities
High (9.3)	57615	USN-1334-1 : libxml2 vulnerabilities
High (9.3)	57887	USN-1357-1 : openssl vulnerabilities
High (8.5)	58325	USN-1397-1 : mysql-5.1, mysql-dfsg-5.0, mysql-dfsg-5.1 vulnerabilities
High (7.8)	55976	Apache HTTP Server Byte Range DoS
High (7.8)	58146	USN-1377-1 : ruby1.8 vulnerabilities
High (7.6)	57616	USN-1335-1 : t1lib vulnerabilities
High (7.5)	55414	USN-1158-1 : curl vulnerabilities
High (7.5)	56236	USN-1209-1 : ffmpeg vulnerabilities
High (7.5)	56554	USN-1231-1 : php5 vulnerabilities
High (7.5)	57888	USN-1358-1 : php5 vulnerabilities

High (7.5)	57932	USN-1358-2 : php5 regression
High (7.5)	57934	USN-1360-1 : firefox vulnerability
High (7.5)	57998	USN-1367-1 : libpng vulnerabilities
High (7.5)	58034	USN-1367-2 : firefox vulnerability
High (7.5)	58036	USN-1367-4 : xulrunner-1.9.2 vulnerability
High (7.5)	58318	USN-1396-1 : eglibc, glibc vulnerabilities
High	56036	USN-1197-1 : firefox, xulrunner-1.9.2 vulnerability
High	56115	USN-1197-3 : firefox, xulrunner-1.9.2 vulnerability
High	56139	USN-1197-4 : nss vulnerability
High	56140	USN-1197-5 : ca-certificates vulnerability
High	56194	USN-1206-1 : libsvg vulnerability
High	56281	USN-1215-1 : apt vulnerabilities
High	56555	USN-1232-1 : xorg-server vulnerabilities
High	56563	USN-1232-2 : xorg-server regression
High	56580	USN-1232-3 : xorg-server vulnerability
High	56629	USN-1237-1 : pam vulnerabilities
High	56767	USN-1255-1 : libmodplug vulnerabilities
High	56970	USN-1283-1 : apt vulnerability
High	57315	USN-1308-1 : bzip2 vulnerability
High	57341	USN-1310-1 : libarchive vulnerabilities
High	57706	USN-1348-1 : icu vulnerability
High	57707	USN-1349-1 : xorg vulnerability
High	57997	USN-1284-2 : update-manager regression
High	58104	USN-1371-1 : cvs vulnerability
High	58144	USN-1375-1 : python-httplib2 vulnerability
High	58145	USN-1376-1 : libxml2 vulnerability
High	58168	USN-1378-1 : postgresql-8.3, postgresql-8.4, postgresql-9.1 vulnerabilities
High	58301	USN-1395-1 : python-pam vulnerability
Medium (6.9)	55102	USN-1140-1 : pam vulnerabilities
Medium (6.9)	55103	USN-1140-2 : pam regression
Medium (6.9)	55648	USN-1172-1 : logrotate vulnerabilities

Medium (6.8)	55114	USN-1148-1 : libmodplug vulnerabilities
Medium (6.8)	55689	USN-1174-1 : libsndfile vulnerability
Medium (6.8)	55699	USN-1175-1 : libpng vulnerabilities
Medium (6.8)	55957	USN-1194-1 : foomatic-filters vulnerabilities
Medium (6.8)	57357	USN-1315-1 : jasper vulnerabilities
Medium (6.8)	57370	USN-1316-1 : t1lib vulnerability
Medium (6.4)	57314	USN-1307-1 : php5 vulnerability
Medium (6.4)	57345	USN-1314-1 : python3.1, python3.2 vulnerabilities
Medium (5.1)	56206	USN-1207-1 : cups, cupsys vulnerabilities
Medium (5.0)	55101	USN-1139-1 : bind9 vulnerabilities
Medium (5.0)	55522	USN-1163-1 : bind9 vulnerability
Medium (5.0)	55731	USN-1181-1 : libsoup2.4 vulnerability
Medium (5.0)	56048	USN-1199-1 : apache2 vulnerability
Medium (5.0)	56506	USN-1229-1 : postgresql-8.3, postgresql-8.4 vulnerability
Medium (5.0)	56778	USN-1259-1 : apache2, apache2-mpm-itk vulnerabilities
Medium (5.0)	56861	USN-1264-1 : bind9 vulnerability
Medium (4.9)	52740	USN-1090-1 : linux vulnerabilities
Medium (4.6)	55700	USN-1176-1 : dbus vulnerability
Medium (4.6)	57999	USN-1368-1 : apache2 vulnerabilities
Medium (4.3)	55095	USN-1134-1 : apache2, apr vulnerabilities
Medium (4.3)	55097	USN-1136-1 : rdesktop vulnerability
Medium (4.3)	57792	Apache HTTP Server httpOnly Cookie Information Disclosure
Low (3.3)	56389	USN-1226-1 : samba vulnerabilities
Low (2.1)	55099	USN-1138-1 : dbus-glib vulnerability
Info	10107	HTTP Server Type and Version
Info	11936	OS Identification
Info	12634	Authenticated Check: OS Name and Installed Package Enumeration
Info	18261	Apache Banner Linux Distribution Disclosure
Info	19506	Nessus Scan Information
Info	22869	Software Enumeration (SSH)
Info	24260	HyperText Transfer Protocol (HTTP) Information

Info	39521	Backported Security Patch Detection (WWW)
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type
Info	55472	Device Hostname