Nessus Scan Report

01/May/2015:17:15:27

Table Of Contents

204.88.135.50

204.88.135.80

204.88.135.81

204.88.137.4

204.88.137.6

204.88.137.14

204.88.137.25

204.88.137.26

204.88.137.39

204.88.138.33

204.88.138.59

204.88.138.65

204.88.138.68

204.88.138.73

204.88.138.76

204.88.138.80

204.88.138.81

204.88.138.82

204.88.138.84

204.88.138.89

204.88.138.97

204.88.138.99

204.88.138.101

204.88.138.102

204.88.138.111

204.88.138.122

204.88.138.123

204.88.138.124

204.88.138.125

204.88.140.62

204.88.141.10

204.88.141.205

204.88.142.3

204.88.142.7

204.88.142.17

204.88.142.32

204.88.142.44

204.88.142.45

204.88.142.48

204.88.142.54

204.88.142.63

204.88.142.66

204.88.142.72

204.88.142.90

204.88.142.92

204.88.142.94

204.88.142.100

204.88.142.101

204.88.142.102

204.88.142.105

204.88.142.106

204.88.142.112

204.88.142.116

204.88.142.117

204.88.142.126

204.88.142.127

204.88.142.129

204.88.142.155

204.88.142.159

204.88.142.161

204.88.142.162

204.88.142.163

204.88.142.179

204.88.142.180

204.88.142.185

204.88.142.186

204.88.142.190

204.88.142.197

204.88.142.202

204.88.142.208

204.88.142.212

204.88.142.213

204.88.142.216

204.88.142.221

204.88.142.222

204.88.142.226

204.88.142.228

204.88.142.232

204.88.142.235

204.88.142.246

204.88.142.249

204.88.143.213

204.88.144.1

204.88.144.3

204.88.144.4

204.88.144.5

204.88.144.65

204.88.144.67

204.88.144.68

204.88.144.80

204.88.144.153

204.88.144.161

204.88.144.177

204.88.144.189

204.88.144.225

204.88.145.1

204.88.145.2

204.88.145.3

204.88.145.4

204.88.145.5

204.88.145.6

204.88.145.7

204.88.145.19

204.88.145.20

204.88.145.25

204.88.145.33

204.88.145.61

204.88.145.62

204.88.145.65

204.88.145.83

204.88.145.94

204.88.145.129

204.88.145.130

204.88.145.131

204.88.145.132

204.88.145.140

204.88.146.1

204.88.146.2

204.88.146.4

204.88.146.29

204.88.146.169

204.88.146.173

204.88.147.1

204.88.147.6

204.88.147.7

204.88.147.10

204.88.147.17

204.88.147.22

204.88.147.33

204.88.147.65

204.88.147.70

204.88.147.97

204.88.147.100

204.88.147.105

204.88.147.129

204.88.147.134

204.88.147.137

204.88.147.138

204.88.147.145

204.88.147.148

204.88.147.161

204.88.147.193

204.88.147.196

204.88.147.225

204.88.147.226

204.88.147.230

204.88.147.234

204.88.147.235

204.88.147.236

204.88.147.237

- 204.88.147.238
- 204.88.147.241
- 204.88.147.242
- 204.88.147.249
- 204.88.148.13
- 204.88.148.49
- 204.88.148.50
- 204.88.148.53
- 204.88.148.62
- 204.88.148.65
- 204.88.148.66
- 204.88.148.75
- 204.88.148.97
- 204.88.148.105
- 204.88.148.129
- 204.88.148.137
- 204.88.148.138
- 204.88.148.140
- 204.88.157.1
- 204.88.157.2
- 204.88.157.5
- 204.88.157.6
- 204.88.157.13
- 204.88.157.14
- 204.88.157.17
- 204.88.157.18
- 204.88.157.21
- 204.88.157.22
- 204.88.157.33
- 204.88.157.34
- 204.88.157.37
- 204.88.157.38
- 204.88.157.41
- 204.88.157.42
- 204.88.157.49
- 204.88.157.50
- 204.88.157.57
- 204.88.157.58
- 204.88.157.61
- 204.88.157.62
- 204.88.157.65
- 204.88.157.66
- 204.88.157.69
- 204.88.157.70
- 204.88.157.73
- 204.88.157.74
- 204.88.157.77
- 204.88.157.78
- 204.88.157.89
- 204.88.157.90
- 204.88.157.97

204.88.157.99

204.88.157.105

204.88.157.106

204.88.157.108

204.88.157.113

204.88.157.129

204.88.157.132

204.88.157.134

204.88.157.137

204.88.157.138

204.88.157.145

204.88.157.147

204.88.157.153

204.88.157.157

204.88.157.161

204.88.157.169

204.88.157.170

204.88.157.177

204.88.157.181

204.88.157.185

204.88.157.186

204.88.157.189

204.88.157.190

204.88.157.201

204.88.157.202

204.88.157.209

204.88.157.210

204.88.157.217

204.88.157.218

204.88.158.5

204.88.158.6

204.88.158.9

204.88.158.10

204.88.158.13

204.88.158.14

204.88.158.21

204.88.158.22

204.88.158.25

204.88.158.26

204.88.158.33

204.88.158.34

204.88.158.37

204.88.158.49

204.88.158.50

204.88.158.57

204.88.158.58

204.88.158.61

204.88.158.62

204.88.158.65

[204.88.158.66]
[204.88.158.69]
[204.88.158.70]
[204.88.158.73]
[204.88.158.74]
[204.88.158.77]
[204.88.158.78]
[204.88.158.93]
[204.88.158.94]
[204.88.158.121]
[204.88.158.122]
[204.88.158.125]
[204.88.158.126]
[204.88.158.141]
[204.88.158.142]
[204.88.158.165]
[204.88.158.166]
[204.88.158.169]
[204.88.158.170]
[204.88.158.173]
[204.88.158.174]
[204.88.158.181]
[204.88.158.182]
[204.88.158.209]
[204.88.158.210]
[204.88.158.213]
[204.88.158.214]
[204.88.158.217]
[204.88.158.218]
[204.88.158.219]
[204.88.158.225]
[204.88.158.226]
[204.88.158.241]
[204.88.158.254]
[204.88.159.9]
[204.88.159.10]
[204.88.159.17]
[204.88.159.18]
[204.88.159.19]
[204.88.159.21]
[204.88.159.23]
[204.88.159.33]
[204.88.159.41]
[204.88.159.42]
[204.88.159.50]
[204.88.159.65]
[204.88.159.66]
[204.88.159.77]
[204.88.159.78]
[204.88.159.81]

204.88.130.138

204.88.130.139

204.88.130.141

204.88.130.142

204.88.130.143

204.88.131.16

204.88.134.53

204.88.134.67

204.88.134.68

204.88.134.69

204.88.134.100

204.88.134.105

204.88.134.110

204.88.134.133

204.88.134.143

204.88.134.149

204.88.134.153

204.88.134.155

204.88.134.158

204.88.134.168

204.88.134.169

204.88.134.175

204.88.134.215

204.88.134.228

204.88.134.236

204.88.134.244

204.88.134.246

204.88.135.43

204.88.135.50

204.88.135.80

204.88.135.81

204.88.137.4

204.88.137.6

204.88.137.14

204.88.137.25

204.88.137.26

204.88.137.39

204.88.138.33

204.88.138.59

204.88.138.65

204.88.138.68

204.88.138.73

204.88.138.76

204.88.138.80

204.88.138.81

204.88.138.82

204.88.138.84

204.88.138.89

204.88.138.97

204.88.138.99

204.88.138.101

204.88.138.102

204.88.138.111

204.88.138.122

204.88.138.123

204.88.138.124

204.88.138.125

204.88.140.62

204.88.141.10

204.88.141.205

204.88.142.3

204.88.142.7

204.88.142.17

204.88.142.32

204.88.142.44

204.88.142.45

204.88.142.48

204.88.142.54

204.88.142.63

204.88.142.66

204.88.142.72

204.88.142.90

204.88.142.92

204.88.142.94

204.88.142.100

204.88.142.101

204.88.142.102

204.88.142.105

204.88.142.106

204.88.142.112

204.88.142.116

204.88.142.117

204.88.142.126

204.88.142.127

204.88.142.129

204.88.142.155

204.88.142.159

204.88.142.161

204.88.142.162

204.88.142.163

204.88.142.179

204.88.142.180

204.88.142.185

204.88.142.186

204.88.142.190

204.88.142.197

204.88.142.202

204.88.142.208

204.88.142.212

204.88.142.213

204.88.142.216

- 204.88.142.221
- 204.88.142.222
- 204.88.142.226
- 204.88.142.228
- 204.88.142.232
- 204.88.142.235
- 204.88.142.246
- 204.88.142.249
- 204.88.143.213
- 204.88.144.1
- 204.88.144.3
- 204.88.144.4
- 204.88.144.5
- 204.88.144.65
- 204.88.144.67
- 204.88.144.68
- 204.88.144.80
- 204.88.144.153
- 204.88.144.161
- 204.88.144.177
- 204.88.144.189
- 204.88.144.225
- 204.88.145.1
- 204.88.145.2
- 204.88.145.3
- 204.88.145.4
- 204.88.145.5
- 204.88.145.6
- 204.88.145.7
- 204.88.145.19
- 204.88.145.20
- 204.88.145.25
- 204.88.145.33
- 204.88.145.61
- 204.88.145.62
- 204.88.145.65
- 204.88.145.83
- 204.88.145.94
- 204.88.145.129
- 204.88.145.130
- 204.88.145.131
- 204.88.145.132
- 204.88.145.140
- 204.88.146.1
- 204.88.146.2
- 204.88.146.4
- 204.88.146.29
- 204.88.146.169
- 204.88.146.173
- 204.88.147.1

204.88.147.6

204.88.147.7

204.88.147.10

204.88.147.17

204.88.147.22

204.88.147.33

204.88.147.65

204.88.147.70

204.88.147.97

204.88.147.100

204.88.147.105

204.88.147.129

204.88.147.134

204.88.147.137

204.88.147.138

204.88.147.145

204.88.147.148

204.88.147.161

204.88.147.193

204.88.147.196

204.88.147.225

204.88.147.226

204.88.147.230

204.88.147.234

204.88.147.235

204.88.147.236

204.88.147.237

204.88.147.238

204.88.147.241

204.88.147.242

204.88.147.249

204.88.148.13

204.88.148.49

204.88.148.50

204.88.148.53

204.88.148.62

204.88.148.65

204.88.148.66

204.88.148.75

204.88.148.97

204.88.148.105

204.88.148.129

204.88.148.137

204.88.148.138

204.88.148.140

204.88.157.1

204.88.157.2

204.88.157.5

204.88.157.6

204.88.157.13

204.88.157.14

204.88.157.17

204.88.157.18

204.88.157.21

204.88.157.22

204.88.157.33

204.88.157.34

204.88.157.37

204.88.157.38

204.88.157.41

204.88.157.42

204.88.157.49

204.88.157.50

204.88.157.57

204.88.157.58

204.88.157.61

204.88.157.62

204.88.157.65

204.88.157.66

204.88.157.69

204.88.157.70

204.88.157.73

204.88.157.74

204.88.157.77

204.88.157.78

204.88.157.89

204.88.157.90

204.88.157.97

204.88.157.99

204.88.157.105

204.88.157.106

204.88.157.108

204.88.157.113

204.88.157.129

204.88.157.132

204.88.157.134

204.88.157.137

204.88.157.138

204.88.157.145

204.88.157.147

204.88.157.153

204.88.157.157

204.88.157.161

204.88.157.169

204.88.157.170

204.88.157.177

204.88.157.181

204.88.157.185

204.88.157.186

204.88.157.189

204.88.157.190

204.88.157.201

204.88.157.202

204.88.157.209

204.88.157.210

204.88.157.217

204.88.157.218

204.88.158.5

204.88.158.6

204.88.158.9

204.88.158.10

204.88.158.13

204.88.158.14

204.88.158.21

204.88.158.22

204.88.158.25

204.88.158.26

204.88.158.33

204.88.158.34

204.88.158.37

204.88.158.49

204.88.158.50

204.88.158.57

204.88.158.58

204.88.158.61

204.88.158.62

204.88.158.65

204.88.158.66

204.88.158.69

204.88.158.70

204.88.158.73

204.88.158.74

204.88.158.77

204.88.158.78

204.88.158.93

204.88.158.94

204.88.158.121

204.88.158.122

204.88.158.125

204.88.158.126

204.88.158.141

204.88.158.142

204.88.158.165

204.88.158.166

204.88.158.169

204.88.158.170

204.88.158.173

204.88.158.174

204.88.158.181

204.88.158.182

204.88.158.209

204.88.158.210

204.88.158.213

204.88.158.214

204.88.158.217

204.88.158.218

204.88.158.219

204.88.158.225

204.88.158.226

204.88.158.241

204.88.158.254

204.88.159.9

204.88.159.10

204.88.159.17

204.88.159.18

204.88.159.19

204.88.159.21

204.88.159.23

204.88.159.33

204.88.159.41

204.88.159.42

204.88.159.50

204.88.159.65

204.88.159.66

204.88.159.77

204.88.159.78

204.88.159.81

204.88.159.82

204.88.159.89

204.88.159.93

204.88.159.94

204.88.159.105

204.88.159.106

204.88.159.113

204.88.159.114

204.88.159.117

204.88.159.118

204.88.159.129

204.88.159.130

204.88.159.141

204.88.159.142

204.88.159.153

204.88.159.154

204.88.159.169

204.88.159.170

204.88.159.173

204.88.159.189

204.88.159.190

204.88.159.193

204.88.159.194

204.88.159.197

67143 (2) - Tridium Niagara AX Web Server Directory Traversal 'config.bog' Disclosure Remote Compromise

67144 (2) - Tridium Niagara AX Web Server Multiple Vulnerabilities

17766 (1) - OpenSSL < 0.9.8p / 1.0.0b Buffer Overflow

17783 (1) - Cisco IOS Software Internet Group Management Protocol Denial of Service Vulnerability (cisco-sa-20100922-igmp)

17784 (1) - Cisco IOS Software Network Address Translation Vulnerabilities (cisco-sa-20100922-nat)

17791 (1) - Cisco IOS Line Printer Daemon (LPD) Stack Overflow

24739 (1) - Cisco IOS Intrusion Prevention System (IPS) Multiple Vulnerabilities (CSCsa53334, CSCsg15598)

24744 (1) - Cisco IOS TCP Listener Crafted Packets Remote DoS (CSCek37177)

36171 (1) - phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)

41028 (1) - SNMP Agent Default Community Name (public)

44914 (1) - Multiple Vulnerabilities in Cisco ASA 5500 Series Adaptive Security Appliances (cisco-sa-20100217-asa)

48245 (1) - PHP 5.3 < 5.3.3 Multiple Vulnerabilities

48989 (1) - IOS Heap-based Overflow Vulnerability in System Timers - Cisco Systems

48994 (1) - DLSw Vulnerability - Cisco Systems

48999 (1) - SIP Packets Reload IOS Devices with support for SIP

49005 (1) - Multiple Vulnerabilities in Cisco IOS While Processing SSL Packets - Cisco Systems

49007 (1) - Voice Vulnerabilities in Cisco IOS and Cisco Unified Communications Manager - Cisco Systems

49010 (1) - Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS - Cisco Systems

49011 (1) - Cisco IOS User Datagram Protocol Delivery Issue For IPv4/IPv6 Dual-stack Routers - Cisco Systems

49012 (1) - Cisco IOS Multicast Virtual Private Network (MVPN) Data Leak - Cisco Systems

49019 (1) - Cisco IOS IPS Denial of Service Vulnerability - Cisco Systems

49023 (1) - Multiple Multicast Vulnerabilities in Cisco IOS Software - Cisco Systems

49025 (1) - Multiple Cisco IOS Session Initiation Protocol Denial of Service Vulnerabilities

49030 (1) - Cisco IOS Software Multiple Features IP Sockets Vulnerability

49031 (1) - Cisco IOS Software Mobile IP and Mobile IPv6 Vulnerabilities - Cisco Systems

49032 (1) - Cisco IOS Software Secure Copy Privilege Escalation Vulnerability - Cisco Systems

49035 (1) - Cisco IOS Software Multiple Features Crafted UDP Packet Vulnerability - Cisco Systems

49036 (1) - Cisco IOS Software WebVPN and SSLVPN Vulnerabilities - Cisco Systems

49038 (1) - TCP State Manipulation Denial of Service Vulnerabilities in Multiple Cisco Products - Cisco Systems

49040 (1) - Cisco IOS Software Authentication Proxy Vulnerability - Cisco Systems

49042 (1) - Cisco IOS Software H.323 Denial of Service Vulnerability - Cisco Systems

49048 (1) - Cisco IOS Software Tunnels Vulnerability - Cisco Systems

49049 (1) - Cisco Unified Communications Manager Express Denial of Service Vulnerabilities (cisco-sa-20100324-cucme)

49050 (1) - Cisco IOS Software H.323 Denial of Service Vulnerabilities (cisco-sa-20100324-h323)

49051 (1) - Cisco IOS Software IPsec Vulnerability (cisco-sa-20100324-ipsec)

49052 (1) - Cisco IOS Software Multiprotocol Label Switching Packet Vulnerability (cisco-sa-20100324-ldp)

49055 (1) - Cisco IOS Software Crafted TCP Packet Denial of Service Vulnerability (cisco-sa-20100324-tcp)

49648 (1) - Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerabilities (cisco-sa-20100922-sip)

51140 (1) - PHP 5.3 < 5.3.4 Multiple Vulnerabilities

55811 (1) - Adobe Flash Media Server < 3.5.7 / 4.0.3 Denial of Service (APSB11-20)

56314 (1) - Cisco IOS Software Data-Link Switching Vulnerability (cisco-sa-20110928-dlsw)

56318 (1) - Cisco IOS Software Network Address Translation Vulnerabilities (cisco-sa-20110928-nat)

57459 (1) - OpenSSL < 0.9.8s Multiple Vulnerabilities

58435 (1) - MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)

58566 (1) - Cisco IOS Internet Key Exchange Vulnerability (cisco-sa-20120328-ike)

58568 (1) - Cisco IOS Software Multicast Source Discovery Protocol Vulnerability (cisco-sa-20120328-msdp)

58570 (1) - Cisco IOS Software Command Authorization Bypass (cisco-sa-20120328-pai)

58799 (1) - OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption

59447 (1) - VMSA-2012-0009 : ESXi and ESX patches address critical security issues (uncredentialed check)

62372 (1) - Cisco IOS Software DHCP Denial of Service Vulnerability (cisco-sa-20120926-dhcp)

62373 (1) - Cisco IOS Software DHCP Version 6 Server Denial of Service Vulnerability (cisco-sa-20120926-dhcpv6)

62376 (1) - Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability (cisco-sa-20120926-sip)

65888 (1) - Cisco IOS Software Network Address Translation Vulnerability (cisco-sa-20130327-nat)

65889 (1) - Cisco IOS Software Protocol Translation Vulnerability (cisco-sa-20130327-pt)

67203 (1) - Cisco Unified Communications Manager Session Initiation Protocol Denial of Service Vulnerability (cisco-sa-20120926-cucm)

70316 (1) - Cisco IOS Software DHCP Denial of Service Vulnerability (cisco-sa-20130925-dhcp)

70319 (1) - Cisco IOS Software IPv6 Virtual Fragmentation Reassembly Denial of Service Vulnerability (cisco-sa-20130925-ipv6vfr)

70322 (1) - Cisco IOS Software Multicast Network Time Protocol Denial of Service Vulnerability (cisco-sa-20130925-ntp)

73345 (1) - Cisco IOS Software Multiple Network Address Translation (NAT) Denial of Service Vulnerabilities (cisco-sa-20140326-nat)

74363 (1) - OpenSSL 0.9.8 < 0.9.8za Multiple Vulnerabilities

77086 (1) - OpenSSL 0.9.8 < 0.9.8zb Multiple Vulnerabilities

78912 (1) - Joomla! Unsupported Version Detection

82531 (1) - Visualware MyConnection Server Remote Agent Default Password

42263 (91) - Unencrypted Telnet Server

51192 (82) - SSL Certificate Cannot Be Trusted

20007 (57) - SSL Version 2 and 3 Protocol Detection

78479 (57) - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

65821 (51) - SSL RC4 Cipher Suites Supported

11213 (19) - HTTP TRACE / TRACK Methods Allowed

57582 (19) - SSL Self-Signed Certificate

46803 (16) - PHP expose_php Information Disclosure

42873 (15) - SSL Medium Strength Cipher Suites Supported

45411 (12) - SSL Certificate with Wrong Hostname

15901 (11) - SSL Certificate Expiry

80035 (10) - TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)

26928 (9) - SSL Weak Cipher Suites Supported

62694 (9) - Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key

81606 (9) - SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

35291 (8) - SSL Certificate Signed using Weak Hashing Algorithm

57792 (8) - Apache HTTP Server httpOnly Cookie Information Disclosure

71426 (7) - PHP 5.3.x < 5.3.28 Multiple OpenSSL Vulnerabilities

78554 (7) - OpenSSL 1.0.1 < 1.0.1j Multiple Vulnerabilities (POODLE)

80568 (7) - OpenSSL 1.0.1 < 1.0.1k Multiple Vulnerabilities

82032 (7) - OpenSSL 1.0.1 < 1.0.1m Multiple Vulnerabilities

42880 (6) - SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection

62565 (5) - Transport Layer Security (TLS) Protocol CRIME Vulnerability

10756 (4) - Apple Mac OS X Find-By-Content .DS_Store Web Directory Listing

10882 (4) - SSH Protocol Version 1 Session Key Retrieval

11411 (3) - Backup Files Disclosure

18405 (3) - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness

53896 (3) - Apache 2.2 < 2.2.18 APR apr_fnmatch DoS

56216 (3) - Apache 2.2 < 2.2.21 mod_proxy_ajp DoS

57690 (3) - Terminal Services Encryption Level is Medium or Low

57791 (3) - Apache 2.2 < 2.2.22 Multiple Vulnerabilities

62101 (3) - Apache 2.2 < 2.2.23 Multiple Vulnerabilities

64912 (3) - Apache 2.2 < 2.2.24 Multiple XSS Vulnerabilities

64992 (3) - PHP 5.3.x < 5.3.22 Multiple Vulnerabilities

66584 (3) - PHP 5.3.x < 5.3.23 Information Disclosure

68915 (3) - Apache 2.2 < 2.2.25 Multiple Vulnerabilities

73289 (3) - PHP PHP_RSHUTDOWN_FUNCTION Security Bypass

73405 (3) - Apache 2.2 < 2.2.27 Multiple Vulnerabilities

81126 (3) - Apache 2.4 < 2.4.12 Multiple Vulnerabilities

11714 (2) - Nonexistent Page (404) Physical Path Disclosure

12085 (2) - Apache Tomcat servlet/JSP container default files

17348 (2) - Jetty < 4.2.19 HTTP Server HttpRequest.java Content-Length Handling Remote Overflow DoS

25289 (2) - Tomcat Sample App hello.jsp test Parameter XSS

25525 (2) - Tomcat snoop.jsp URI XSS

26070 (2) - Tomcat Sample App cal2.jsp time Parameter XSS (CVE-2006-7196)

47696 (2) - Apache Tomcat Implicit Objects XSS

47708 (2) - Apache Tomcat JSP2 Examples XSS

48205 (2) - Apache 2.2 < 2.2.16 Multiple Vulnerabilities

50070 (2) - Apache 2.2 < 2.2.17 Multiple Vulnerabilities

51439 (2) - PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS

58453 (2) - Terminal Services Doesn't Use Network Level Authentication (NLA) Only

81574 (2) - Cisco ASA SSL VPN Remote Information Disclosure (CSCuq65542)

10068 (1) - Finger Service Remote Information Disclosure

10815 (1) - Web Server Generic XSS

11229 (1) - Web Server info.php / phpinfo.php Detection

11658 (1) - Sun ONE Application Server Upper Case Request JSP Source Disclosure

11690 (1) - JBoss %00 Request JSP Source Disclosure

17767 (1) - OpenSSL < 0.9.8p / 1.0.0e Double Free Vulnerability

17790 (1) - Cisco Regular Expression Processing DoS

17792 (1) - Cisco VLAN Trunking Protocol Vulnerability

17795 (1) - Cisco IOS XSS and XSRF Vulnerabilities

24019 (1) - Cisco IOS Data-link Switching (DLSw) Capabilities Exchange Remote DoS (CSCsf28840)

33219 (1) - Lyris ListManager read/search/results words Parameter XSS

33821 (1) - .svn/entries Disclosed via Web Server

36083 (1) - phpMyAdmin file_path Parameter Vulnerabilities (PMASA-2009-1)

44921 (1) - PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities

45414 (1) - VMware ESX WebAccess Context Data XSS (VMSA-2010-0005)

49004 (1) - Vulnerability In Crypto Library - Cisco Systems

49017 (1) - Multiple Cisco Products Vulnerable to DNS Cache Poisoning Attacks

49028 (1) - Cisco IOS MPLS VPN May Leak Information - Cisco Systems

49142 (1) - phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)

51425 (1) - phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)

51892 (1) - OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue

57608 (1) - SMB Signing Required

58564 (1) - OpenSSL < 0.9.8u Multiple Vulnerabilities

59076 (1) - OpenSSL 0.9.8 < 0.9.8x DTLS CBC Denial of Service

63643 (1) - MS13-006: Vulnerability in Microsoft Windows Could Allow Security Feature Bypass (2785220) (uncredentialed check)

64532 (1) - OpenSSL < 0.9.8y Multiple Vulnerabilities

69377 (1) - OSPF LSA Manipulation Vulnerability in Cisco IOS (cisco-sa-20130801-lsaospf)

76474 (1) - SNMP 'GETBULK' Reflection DDoS

78552 (1) - OpenSSL 0.9.8 < 0.9.8zc Multiple Vulnerabilities (POODLE)

80566 (1) - OpenSSL 0.9.8 < 0.9.8zd Multiple Vulnerabilities

82030 (1) - OpenSSL 0.9.8 < 0.9.8zf Multiple Vulnerabilities

70658 (13) - SSH Server CBC Mode Ciphers Enabled

26194 (12) - Web Server Uses Plain Text Authentication Forms

71049 (12) - SSH Weak MAC Algorithms Enabled

[69551 (9) - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits]
[10759 (6) - Web Server HTTP Header Internal IP Disclosure]
[34850 (5) - Web Server Uses Basic Authentication Without HTTPS]
[34324 (4) - FTP Supports Clear Text Authentication]
[30218 (3) - Terminal Services Encryption Level is not FIPS-140 Compliant]
[10969 (1) - SNMP Request Cisco Router Information Disclosure]
[11219 (1100) - Nessus SYN scanner]
[22964 (411) - Service Detection]
[19506 (376) - Nessus Scan Information]
[12053 (356) - Host Fully Qualified Domain Name (FQDN) Resolution]
[11936 (261) - OS Identification]
[54615 (247) - Device Type]
[45590 (232) - Common Platform Enumeration (CPE)]
[46215 (184) - Inconsistent Hostname and IP Address]
[10107 (153) - HTTP Server Type and Version]
[24260 (142) - HyperText Transfer Protocol (HTTP) Information]
[25220 (113) - TCP/IP Timestamps Supported]
[10863 (93) - SSL Certificate Information]
[56984 (93) - SSL / TLS Versions Supported]
[62563 (92) - SSL Compression Methods Supported]
[21643 (87) - SSL Cipher Suites Supported]
[70544 (86) - SSL Cipher Block Chaining Cipher Suites Supported]
[46180 (80) - Additional DNS Hostnames]
[10281 (75) - Telnet Server Detection]
[43111 (74) - HTTP Methods Allowed (per directory)]
[11032 (60) - Web Server Directory Enumeration]
[51891 (57) - SSL Session Resume Supported]
[66334 (53) - Patch Report]
[49704 (51) - External URLs]
[45410 (45) - SSL Certificate commonName Mismatch]
[11154 (43) - Unknown Service Detection: Banner Retrieval]
[57041 (40) - SSL Perfect Forward Secrecy Cipher Suites Supported]
[10662 (38) - Web mirroring]
[50845 (35) - OpenSSL Detection]
[10302 (34) - Web Server robots.txt Information Disclosure]
[10386 (31) - Web Server No 404 Error Code Check]
[10092 (21) - FTP Server Detection]
[14274 (20) - Nessus SNMP Scanner]
[42057 (19) - Web Server Allows Password Auto-Completion]
[50350 (17) - OS Identification Failed]
[56471 (16) - SSL Certificate Chain Not Sorted]
[10267 (15) - SSH Server Type and Version Information]
[11933 (15) - Do not scan printers]
[31422 (15) - Reverse NAT/Intercepting Proxy Detection]
[48243 (15) - PHP Version]
[70657 (14) - SSH Algorithms and Languages Supported]
[11874 (13) - Microsoft IIS 404 Response Service Pack Signature]
[57323 (13) - OpenSSL Version Detection]
[21642 (12) - Session Initiation Protocol Detection]
[39521 (12) - Backported Security Patch Detection (WWW)]

10881 (11) - SSH Protocol Versions Supported

10919 (11) - Open Port Re-check

11422 (11) - Web Server Unconfigured - Default Install Page Present

11153 (10) - Service Detection (HELP Request)

11424 (10) - WebDAV Detection

11935 (10) - IPSEC Internet Key Exchange (IKE) Version 1 Detection

15588 (9) - Web Server SSL Port HTTP Traffic Detection

39520 (9) - Backported Security Patch Detection (SSH)

40984 (9) - Browsable Web Directories

49705 (9) - Web Server Harvested Email Addresses

10736 (8) - DCE Services Enumeration

42981 (7) - SSL Certificate Expiry - Future Expiry

56472 (7) - SSL Certificate Chain Contains Unnecessary Certificates

11419 (6) - Web Server Office File Inventory

58768 (5) - SSL Resume With Different Cipher Issue

10622 (4) - PPTP Detection

20108 (4) - Web Server / Application favicon.ico Vendor Fingerprinting

39446 (4) - Apache Tomcat Default Error Page Version Detection

67142 (4) - Tridium Niagara AX Web Server Detection

10940 (3) - Windows Terminal Services Enabled

11819 (3) - TFTP Daemon Detection

17975 (3) - Service Detection (GET request)

18261 (3) - Apache Banner Linux Distribution Disclosure

24242 (3) - Microsoft .NET Handlers Enumeration

32318 (3) - Web Site Cross-Domain Policy File Detection

42796 (3) - CISCO ASA SSL VPN Detection

57396 (3) - VMware vSphere Detect

62695 (3) - IPSEC Internet Key Exchange (IKE) Version 2 Detection

66173 (3) - RDP Screenshot

10185 (2) - POP Server Detection

10263 (2) - SMTP Server Detection

10695 (2) - Microsoft IIS .IDA ISAPI Filter Enabled

11002 (2) - DNS Server Detection

11011 (2) - Microsoft Windows SMB Service Detection

11414 (2) - IMAP Service Banner Retrieval

17219 (2) - phpMyAdmin Detection

31097 (2) - RTMP Server Detection

35716 (2) - Ethernet Card Manufacturer Detection

39519 (2) - Backported Security Patch Detection (FTP)

51080 (2) - Web Server Uses Basic Authentication over HTTPS

52703 (2) - vsftpd Detection

64814 (2) - Terminal Services Use SSL/TLS

10150 (1) - Windows NetBIOS / SMB Remote Host Information Disclosure

10394 (1) - Microsoft Windows SMB Log In Possible

10551 (1) - SNMP Request Network Interfaces Enumeration

10666 (1) - Apple Filing Protocol Server Detection

10785 (1) - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

10800 (1) - SNMP Query System Information Disclosure

10829 (1) - UPnP Client Detection

10833 (1) - CDE Subprocess Control Service (dtspcd) Detection

Hosts Summary (Executive)

[-] Collapse All

[+] Expand All

204.88.128.1

Summary

Critical	High	Medium	Low	Info
0	0	0	0	7

Details

Severity	Plugin Id	Name
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	21642	Session Initiation Protocol Detection
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

204.88.128.2

Summary

Critical	High	Medium	Low	Info
0	0	0	0	2

Details

Severity	Plugin Id	Name
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information

204.88.128.5

Summary

Critical	High	Medium	Low	Info
0	0	0	0	3

Details

Severity	Plugin Id	Name
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	46215	Inconsistent Hostname and IP Address

204.88.128.7

Summary

Critical	High	Medium	Low	Info
0	0	1	0	13

Details

Severity	Plugin Id	Name
Medium (5.0)	10068	Finger Service Remote Information Disclosure
Info	10092	FTP Server Detection
Info	10833	CDE Subprocess Control Service (dtspcd) Detection
Info	11002	DNS Server Detection
Info	11154	Unknown Service Detection: Banner Retrieval
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
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	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

204.88.128.14

Summary

Critical	High	Medium	Low	Info
0	0	0	0	5

Details

Severity	Plugin Id	Name
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information

Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported

204.88.128.34

Summary

Critical	High	Medium	Low	Info
0	0	0	0	7

Details

Severity	Plugin Id	Name
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported
Info	46215	Inconsistent Hostname and IP Address

204.88.128.35

Summary

Critical	High	Medium	Low	Info
0	0	0	0	3

Details

Severity	Plugin Id	Name
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	46215	Inconsistent Hostname and IP Address

204.88.128.131

Summary

Critical	High	Medium	Low	Info
0	0	0	0	6

Details

Severity	Plugin Id	Name
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	21642	Session Initiation Protocol Detection
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

204.88.129.40

Summary

Critical	High	Medium	Low	Info
0	0	0	2	14

Details

Severity	Plugin Id	Name
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled
Info	10267	SSH Server Type and Version Information
	10881	

Info		SSH Protocol Versions Supported
Info	11154	Unknown Service Detection: Banner Retrieval
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported
Info	39520	Backported Security Patch Detection (SSH)
Info	45590	Common Platform Enumeration (CPE)
Info	46215	Inconsistent Hostname and IP Address
Info	54615	Device Type
Info	70657	SSH Algorithms and Languages Supported

204.88.129.54

Summary

Critical	High	Medium	Low	Info
0	0	0	2	14

Details

Severity	Plugin Id	Name
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled
Info	10267	SSH Server Type and Version Information
Info	10881	SSH Protocol Versions Supported
Info	11154	Unknown Service Detection: Banner Retrieval
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported
Info	39520	Backported Security Patch Detection (SSH)
Info	45590	Common Platform Enumeration (CPE)
Info	46215	Inconsistent Hostname and IP Address
Info	54615	Device Type
Info	70657	SSH Algorithms and Languages Supported

204.88.130.129

Summary

Critical	High	Medium	Low	Info
0	0	0	0	3

Details

Severity	Plugin Id	Name
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	46215	Inconsistent Hostname and IP Address

204.88.130.137

Summary

Critical	High	Medium	Low	Info
0	0	1	0	19

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Info	10107	HTTP Server Type and Version
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	42981	SSL Certificate Expiry - Future Expiry
Info	45410	SSL Certificate commonName Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	50845	OpenSSL Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

204.88.130.138

Summary

Critical	High	Medium	Low	Info
0	0	1	0	19

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Info	10107	HTTP Server Type and Version
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	42981	SSL Certificate Expiry - Future Expiry
Info	45410	SSL Certificate commonName Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	50845	OpenSSL Detection

Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

204.88.130.139

Summary

Critical	High	Medium	Low	Info
0	0	0	0	2

Details

Severity	Plugin Id	Name
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information

204.88.130.141

Summary

Critical	High	Medium	Low	Info
0	0	1	0	19

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Info	10107	HTTP Server Type and Version
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	42981	SSL Certificate Expiry - Future Expiry
Info	45410	SSL Certificate commonName Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	50845	OpenSSL Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

204.88.130.142

Summary

Critical	High	Medium	Low	Info
0	0	1	0	19

Details

Severity	Plugin Id	Name
	51192	

Medium (6.4)		SSL Certificate Cannot Be Trusted
Info	10107	HTTP Server Type and Version
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	42981	SSL Certificate Expiry - Future Expiry
Info	45410	SSL Certificate commonName Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	50845	OpenSSL Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

204.88.130.143

Summary

Critical	High	Medium	Low	Info
0	0	1	0	19

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Info	10107	HTTP Server Type and Version
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	42981	SSL Certificate Expiry - Future Expiry
Info	45410	SSL Certificate commonName Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	50845	OpenSSL Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported

Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

204.88.131.16

Summary

Critical	High	Medium	Low	Info
0	0	1	0	19

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Info	10107	HTTP Server Type and Version
Info	10302	Web Server robots.txt Information Disclosure
Info	10662	Web mirroring
Info	10863	SSL Certificate Information
Info	11032	Web Server Directory Enumeration
Info	11219	Nessus SYN scanner
Info	11419	Web Server Office File Inventory
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	43111	HTTP Methods Allowed (per directory)
Info	45410	SSL Certificate commonName Mismatch
Info	46180	Additional DNS Hostnames
Info	46215	Inconsistent Hostname and IP Address
Info	49704	External URLs
Info	50845	OpenSSL Detection
Info	56984	SSL / TLS Versions Supported
Info	62563	SSL Compression Methods Supported

204.88.134.53

Summary

Critical	High	Medium	Low	Info
0	0	4	0	23

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (4.3)	65821	SSL RC4 Cipher Suites Supported
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Info	10107	HTTP Server Type and Version
Info	10863	SSL Certificate Information
Info	11032	Web Server Directory Enumeration
Info	11219	Nessus SYN scanner
Info	11422	Web Server Unconfigured - Default Install Page Present
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
	21643	

Info		SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	43111	HTTP Methods Allowed (per directory)
Info	45590	Common Platform Enumeration (CPE)
Info	46180	Additional DNS Hostnames
Info	49704	External URLs
Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	66334	Patch Report
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported

204.88.134.67

Summary

Critical	High	Medium	Low	Info
0	0	6	0	20

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (5.0)	15901	SSL Certificate Expiry
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	45411	SSL Certificate with Wrong Hostname
Medium (4.3)	65821	SSL RC4 Cipher Suites Supported
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Info	10107	HTTP Server Type and Version
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	45410	SSL Certificate commonName Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	46180	Additional DNS Hostnames
Info	51891	SSL Session Resume Supported
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62563	SSL Compression Methods Supported
Info	66334	Patch Report