Nessus Scan Report

02/Dec/2013:14:07:21

Table Of Contents

192.168.1.240

192.168.1.248

192.168.1.249

192.168.1.250

Vulnerabilities By Host

[-] Collapse All

[+] Expand All

192.168.1.1

Scan Information

Start time:	Mon Dec 2 14:07:21 2013
End time:	Mon Dec 2 14:36:44 2013

Host Information

DNS Name:	Wireless_Broadband_Router.home
IP:	192.168.1.1
MAC Address:	00:7f:28:eb:30:d0

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	7	3	0	10

Results Details

0/tcp

12213 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS	[-/+]
56283 - Linux Kernel TCP Sequence Number Generation Security Weakness	[-/+]

443/tcp

35291 - SSL Certificate Signed using Weak Hashing Algorithm	[-/+]
42880 - SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	[-/+]

992/tcp

35291 - SSL Certificate Signed using Weak Hashing Algorithm	[-/+]
42880 - SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	[-/+]

2555/tcp

64588 - Microsoft ASP.NET MS-DOS Device Name DoS [-/+]

2556/tcp

64588 - Microsoft ASP.NET MS-DOS Device Name DoS [-/+]

8443/tcp

35291 - SSL Certificate Signed using Weak Hashing Algorithm [-/+]

42880 - SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection [-/+]

192.168.1.10

Scan Information

Start time:	Mon Dec 2 14:07:21 2013
End time:	Mon Dec 2 14:23:31 2013

Host Information

IP:	192.168.1.10
MAC Address:	00:00:24:c9:55:21
OS:	Linux Kernel 2.6 on Debian 5.0 (lenny)

Results Summary

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

Results Details

0/tcp

12213 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS [-/+]

56283 - Linux Kernel TCP Sequence Number Generation Security Weakness [-/+]

53/tcp

10595 - DNS Server Zone Transfer Information Disclosure (AXFR) [-/+]

192.168.1.16

Scan Information

Start time:	Mon Dec 2 14:07:21 2013
End time:	Mon Dec 2 14:21:44 2013

Host Information

Netbios Name:	HANZO

IP: 192.168.1.16

MAC Address: 08:60:6e:73:11:ed

OS: Microsoft Windows 7 Professional

Results Summary

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

Results Details

445/tcp

10394 - Microsoft Windows SMB Log In Possible [-/+]

3389/tcp

18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness [-/+]

192.168.1.17

Scan Information

Start time: Mon Dec 2 14:07:21 2013

End time: Mon Dec 2 14:21:13 2013

Host Information

Netbios Name: COHIBA

IP: 192.168.1.17

MAC Address: 00:22:19:dc:a7:a9

OS: Microsoft Windows 7 Professional

Results Summary

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

Results Details

445/tcp

10394 - Microsoft Windows SMB Log In Possible [-/+]

3389/tcp

18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness [-/+]

192.168.1.20

Scan Information

Start time: Mon Dec 2 14:07:21 2013

End time: Mon Dec 2 14:18:56 2013

Host Information

IP: 192.168.1.20

MAC Address: 24:a4:3c:08:25:68

Results Summary

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

Results Details

0/tcp

12213 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS [-/+]

56283 - Linux Kernel TCP Sequence Number Generation Security Weakness [-/+]

22/tcp

70545 - Dropbear SSH Server < 2013.59 Multiple Vulnerabilities [-/+]

192.168.1.21

Scan Information

Start time: Mon Dec 2 14:07:21 2013

End time: Mon Dec 2 14:18:54 2013

Host Information

IP: 192.168.1.21

MAC Address: 24:a4:3c:08:27:5f

Results Summary

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

Results Details

0/tcp

12213 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS [-/+]

56283 - Linux Kernel TCP Sequence Number Generation Security Weakness [-/+]

22/tcp

70545 - Dropbear SSH Server < 2013.59 Multiple Vulnerabilities [-/+]

192.168.1.22

Scan Information

Start time:	Mon Dec 2 14:07:21 2013
End time:	Mon Dec 2 14:23:29 2013

Host Information

IP:	192.168.1.22
MAC Address:	24:a4:3c:08:24:bc

Results Summary

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

Results Details

0/tcp

12213 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS	[-/+]
56283 - Linux Kernel TCP Sequence Number Generation Security Weakness	[-/+]

22/tcp

70545 - Dropbear SSH Server < 2013.59 Multiple Vulnerabilities	[-/+]

192.168.1.25

Scan Information

Start time:	Mon Dec 2 14:07:21 2013
End time:	Mon Dec 2 14:18:51 2013

Host Information

IP:	192.168.1.25
MAC Address:	c8:d7:19:bd:2e:f2

Results Summary

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

Results Details

0/tcp

12213 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS	[-/+]
56283 - Linux Kernel TCP Sequence Number Generation Security Weakness	[-/+]

80/tcp

10815 - Web Server Generic XSS	[-/+]

192.168.1.30

Scan Information

Start time: Mon Dec 2 14:07:21 2013

Host Information

Netbios Name: NAS-BASEMENT

IP: 192.168.1.30

MAC Address: 00:0d:a2:01:83:fb

Results Summary

Critical	High	Medium	Low	Info	Total
1	7	12	1	1	22

Results Details

0/tcp

12213 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS	[-/+]
56283 - Linux Kernel TCP Sequence Number Generation Security Weakness	[-/+]

80/tcp

11213 - HTTP TRACE / TRACK Methods Allowed	[-/+]

443/tcp

35291 - SSL Certificate Signed using Weak Hashing Algorithm	[-/+]
58751 - SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability	[-/+]

445/tcp

58662 - Samba 3.x < 3.6.4 / 3.5.14 / 3.4.16 RPC Multiple Buffer Overflows	[-/+]
47036 - Samba 3.x < 3.3.13 SMB1 Packet Chaining Memory Corruption	[-/+]
45047 - Samba 'CAP_DAC_OVERRIDE' File Permission Security Bypass	[-/+]
26919 - Microsoft Windows SMB Guest Account Local User Access	[-/+]
41970 - Samba < 3.0.37 / 3.2.15 / 3.3.8 / 3.4.2 Multiple Vulnerabilities	[-/+]
64459 - Samba < 3.5.21 / 3.6.12 / 4.0.2 SWAT Multiple	[-/+]

Vulnerabilities

69276 - Samba 3.x < 3.5.22 / 3.6.x < 3.6.17 / 4.0.x < 4.0.8 read_nttrans_ea_lis DoS [-/+]

55733 - Samba 3.x < 3.3.16 / 3.4.14 / 3.5.10 Multiple Vulnerabilities [-/+]

39502 - Samba < 3.0.35 / 3.2.13 / 3.3.6 Multiple Vulnerabilities [-/+]

10394 - Microsoft Windows SMB Log In Possible [-/+]

631/tcp

47683 - CUPS < 1.4.4 Multiple Vulnerabilities [-/+]

36183 - CUPS < 1.3.10 Multiple Vulnerabilities [-/+]

45554 - CUPS < 1.4.3 Multiple Vulnerabilities [-/+]

65970 - CUPS < 1.6.2 Multiple Vulnerabilities [-/+]

34385 - CUPS < 1.3.9 Multiple Vulnerabilities [-/+]

42468 - CUPS < 1.4.2 kerberos Parameter XSS [-/+]

2049/udp

11356 - NFS Exported Share Information Disclosure [-/+]

192.168.1.81

Scan Information

Start time:	Mon Dec 2 14:07:36 2013
End time:	Mon Dec 2 14:35:33 2013

Host Information

IP:	192.168.1.81
MAC Address:	00:11:d9:31:8e:0b
OS:	Linux Kernel 2.6, PelcoLinux

Results Summary

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

Results Details

0/tcp

12213 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS [-/+]

56283 - Linux Kernel TCP Sequence Number Generation Security [-/+]

Weakness

1413/tcp

35291 - SSL Certificate Signed using Weak Hashing Algorithm [-/+]

192.168.1.98

Scan Information

Start time:	Mon Dec 2 14:07:42 2013
End time:	Mon Dec 2 14:19:01 2013

Host Information

IP:	192.168.1.98
MAC Address:	00:1a:8c:12:2c:24

Results Summary

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

Results Details

0/tcp

12213 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS [-/+]

192.168.1.146

Scan Information

Start time:	Mon Dec 2 14:08:01 2013
End time:	Mon Dec 2 14:17:08 2013

Host Information

Netbios Name:	WINDOWS2000
IP:	192.168.1.146
MAC Address:	00:0c:29:f7:55:ea
OS:	Microsoft Windows 2000 Service Pack 4

Results Summary

Critical	High	Medium	Low	Info	Total
15	2	5	0	1	23

Results Details

0/tcp

12213 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS [-/+]

25/tcp

45517 - MS10-024: Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service (981832) (uncredentialed check)	[-/+]

80/tcp

10357 - Microsoft IIS MDAC RDS (msadcs.dll) Arbitrary Remote Command Execution	[-/+]
11161 - Microsoft Data Access Components RDS Data Stub Remote Overflow	[-/+]
11213 - HTTP TRACE / TRACK Methods Allowed	[-/+]

135/udp

11890 - MS03-043: Buffer Overrun in Messenger Service (828035) (uncredentialed check)	[-/+]

445/tcp

21193 - MS05-047: Plug and Play Remote Code Execution and Local Privilege Elevation (905749) (uncredentialed check)	[-/+]
22194 - MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)	[-/+]
19408 - MS05-039: Vulnerability in Plug and Play Service Could Allow Remote Code Execution (899588) (uncredentialed check)	[-/+]
35362 - MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)	[-/+]
12209 - MS04-011: Security Update for Microsoft Windows (835732) (uncredentialed check)	[-/+]
19407 - MS05-043: Vulnerability in Printer Spooler Service Could Allow Remote Code Execution (896423) (uncredentialed check)	[-/+]
11835 - MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (uncredentialed check)	[-/+]
12054 - MS04-007: ASN.1 Vulnerability Could Allow Code Execution (828028) (uncredentialed check) (NTLM)	[-/+]
11808 - MS03-026: Microsoft RPC Interface Buffer Overrun (823980) (uncredentialed check)	[-/+]
18502 - MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)	[-/+]
34477 - MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)	[-/+]
22034 - MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check)	[-/+]
56210 - Microsoft Windows SMB LsaQueryInformationPolicy	[-/+]

Function SID Enumeration Without Credentials

56211 - SMB Use Host SID to Enumerate Local Users Without Credentials [-/+]

10394 - Microsoft Windows SMB Log In Possible [-/+]

1025/tcp

13852 - MS04-022: Microsoft Windows Task Scheduler Remote Overflow (841873) (uncredentialed check) [-/+]

1086/tcp

21334 - MS06-018: Vulnerability in Microsoft Distributed Transaction Coordinator Could Allow DoS (913580) (uncredentialed check) [-/+]

192.168.1.200

Scan Information

Start time:	Mon Dec 2 14:08:17 2013
End time:	Mon Dec 2 14:22:06 2013

Host Information

Netbios Name:	PODCAST-1
IP:	192.168.1.200
MAC Address:	4c:72:b9:e2:09:cb
OS:	Microsoft Windows 7 Professional

Results Summary

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

Results Details

445/tcp

10394 - Microsoft Windows SMB Log In Possible [-/+]

3389/tcp

18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness [-/+]

192.168.1.204

Scan Information

Start time:	Mon Dec 2 14:08:17 2013
End time:	Mon Dec 2 14:11:12 2013

Host Information

Netbios Name:	WINDOWS-XP-VM
IP:	192.168.1.204
MAC Address:	00:0c:29:d3:69:ed
OS:	Microsoft Windows XP Service Pack 2, Microsoft Windows XP Service Pack 3

Results Summary

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

Results Details

445/tcp

10394 - Microsoft Windows SMB Log In Possible [-/+]

192.168.1.207

Scan Information

Start time:	Mon Dec 2 14:08:20 2013
End time:	Mon Dec 2 14:31:13 2013

Host Information

IP:	192.168.1.207
MAC Address:	00:0d:4b:63:c8:ee
OS:	Cyber Switching ePower PDU

Results Summary

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

Results Details

0/tcp

12213 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS [-/+]

56283 - Linux Kernel TCP Sequence Number Generation Security Weakness [-/+]

192.168.1.212

Scan Information

Start time:	Mon Dec 2 14:08:22 2013
End time:	Mon Dec 2 14:22:18 2013

Host Information

Netbios Name:	BOXEEBOX
IP:	192.168.1.212
MAC Address:	74:f0:6d:9f:d0:2a
OS:	Linux Kernel 2.6, PelcoLinux

Results Summary

Critical	High	Medium	Low	Info	Total
1	1	6	0	1	9

Results Details

0/tcp

12213 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS	[-/+]
56283 - Linux Kernel TCP Sequence Number Generation Security Weakness	[-/+]

445/tcp

58662 - Samba 3.x < 3.6.4 / 3.5.14 / 3.4.16 RPC Multiple Buffer Overflows	[-/+]
47036 - Samba 3.x < 3.3.13 SMB1 Packet Chaining Memory Corruption	[-/+]
26919 - Microsoft Windows SMB Guest Account Local User Access	[-/+]
64459 - Samba < 3.5.21 / 3.6.12 / 4.0.2 SWAT Multiple Vulnerabilities	[-/+]
69276 - Samba 3.x < 3.5.22 / 3.6.x < 3.6.17 / 4.0.x < 4.0.8 read_nttrans_ea_lis DoS	[-/+]
55733 - Samba 3.x < 3.3.16 / 3.4.14 / 3.5.10 Multiple Vulnerabilities	[-/+]
10394 - Microsoft Windows SMB Log In Possible	[-/+]

192.168.1.216

Scan Information

Start time:	Mon Dec 2 14:08:22 2013
End time:	Mon Dec 2 14:14:31 2013

Host Information

IP:	192.168.1.216
MAC Address:	00:23:a2:47:d7:4c

Results Summary

Critical	High	Medium	Low	Info	Total

0	0	1	0	0	1

Results Details

0/tcp

12213 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS [-/+]

192.168.1.219

Scan Information

Start time: Mon Dec 2 14:08:22 2013

End time: Mon Dec 2 14:18:33 2013

Host Information

IP: 192.168.1.219

MAC Address: 00:0e:58:f1:48:bc

OS: KYOCERA Printer, Linux Kernel 2.6

Results Summary

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

Results Details

0/tcp

12213 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS [-/+]

56283 - Linux Kernel TCP Sequence Number Generation Security Weakness [-/+]

192.168.1.226

Scan Information

Start time: Mon Dec 2 14:08:27 2013

End time: Mon Dec 2 14:37:58 2013

Host Information

IP: 192.168.1.226

MAC Address: 00:0d:4b:ac:7c:59

OS: Cyber Switching ePower PDU

Results Summary

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

Results Details

0/tcp

12213 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS [-/+]

Synopsis

It may be possible to send spoofed RST packets to the remote system.

Description

The remote host might be affected by a sequence number approximation vulnerability that may allow an attacker to send spoofed RST packets to the remote host and close established connections. This may cause problems for some dedicated services (BGP, a VPN over TCP, etc).

See Also

https://downloads.avaya.com/elmodocs2/security/ASA-2006-217.htm

http://www.kb.cert.org/vuls/id/JARL-5ZQR4D

http://www-01.ibm.com/support/docview.wss?uid=isg1IY55949

http://www-01.ibm.com/support/docview.wss?uid=isg1IY55950

http://www-01.ibm.com/support/docview.wss?uid=isg1IY62006

http://www.juniper.net/support/security/alerts/niscc-236929.txt

http://technet.microsoft.com/en-us/security/bulletin/ms05-019

http://technet.microsoft.com/en-us/security/bulletin/ms06-064

http://www.kb.cert.org/vuls/id/JARL-5YGQ9G

http://www.kb.cert.org/vuls/id/JARL-5ZQR7H

http://www.kb.cert.org/vuls/id/JARL-5YGQAJ

http://www.nessus.org/u?9a548ae4

http://isc.sans.edu/diary.html?date=2004-04-20

Solution

Contact the vendor for a patch or mitigation advice.

Risk Factor

Medium

CVSS Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVSS Temporal Score

4.1 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

References

BID	10183
CVE	CVE-2004-0230

XREF	OSVDB:4030
XREF	CERT:415294
XREF	EDB-ID:276
XREF	EDB-ID:291

Plugin Information:

Publication date: 2004/04/25, Modification date: 2012/12/28

Ports

tcp/0

56283 - Linux Kernel TCP Sequence Number Generation Security Weakness [-/+]

192.168.1.228

Scan Information

Start time:	Mon Dec 2 14:08:27 2013
End time:	Mon Dec 2 15:06:27 2013

Host Information

Netbios Name:	WIN-52NMLK4OFS8
IP:	192.168.1.228
MAC Address:	00:0c:29:20:af:78
OS:	Microsoft Windows 7 Ultimate

Results Summary

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

Results Details

445/tcp

10394 - Microsoft Windows SMB Log In Possible [-/+]

192.168.1.240

Scan Information

Start time:	Mon Dec 2 14:08:44 2013
End time:	Mon Dec 2 14:17:34 2013

Host Information

IP: 192.168.1.240

MAC Address: 00:1a:4b:27:c4:e9

OS: Nortel Secure Router

Results Summary

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

Results Details

0/tcp

12213 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS [-/+]

192.168.1.248

Scan Information

Start time: Mon Dec 2 14:09:02 2013

End time: Mon Dec 2 14:26:19 2013

Host Information

IP: 192.168.1.248

MAC Address: 00:09:b0:c1:d2:ca

OS: EPSON Stylus Printer, Linksys Wireless Access Point, Oracle Integrated Lights Out Manager

Results Summary

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

Results Details

0/tcp

12213 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS [-/+]

56283 - Linux Kernel TCP Sequence Number Generation Security Weakness [-/+]

80/tcp

10815 - Web Server Generic XSS [-/+]

50600 - Apache Shiro URI Path Security Traversal Information Disclosure [-/+]

192.168.1.249

Scan Information

Start time: Mon Dec 2 14:09:02 2013

End time: Mon Dec 2 14:31:25 2013

Host Information

IP: 192.168.1.249

MAC Address: 00:0d:4b:4c:29:5e

OS: Cyber Switching ePower PDU

Results Summary

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

Results Details

0/tcp

12213 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS	[-/+]
56283 - Linux Kernel TCP Sequence Number Generation Security Weakness	[-/+]

192.168.1.250

Scan Information

Start time: Mon Dec 2 14:09:36 2013

End time: Mon Dec 2 14:18:17 2013

Host Information

IP: 192.168.1.250

MAC Address: 00:0e:58:1b:e9:c2

OS: Linux Kernel 2.4

Results Summary

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

Results Details

0/tcp

12213 - TCP/IP Sequence Prediction Blind Reset Spoofing DoS	[-/+]
56283 - Linux Kernel TCP Sequence Number Generation Security Weakness	[-/+]