TENABLE NETWORK SECURITY INC., COPYRIGHT © 2012

TENABLE NETWORK SECURITY

CIS Cisco Firewall Auditing

March 13, 2012 at 8:25pm CDT
Dave Breslin [dbreslin]

Confidential: The following report contains confidential information. Do not distribute, email, fax, or transfer via any electronic mechanism unless it has been approved by the recipient company's security policy. All copies and backups of this document should be saved on protected storage at all times. Do not share any of the information contained within this report with anyone unless they are authorized to view the information. Violating any of the previous instructions is grounds for termination.

TENABLE
Network Security®

Table of Contents

TENABLE NETWORK SECURITY INC., COPYRIGHT © 2012

Configuration Audit Summary

Compliance Checks. Info = Pass, Medium = Couldn't Execute, High = Fail

IP Address	DNS Name	Info	Med.	High
10.0.4.200	fw5.itsdept.com	96	0	5
10.0.3.200	fw4.itsdept.com	92	0	9
10.0.2.200	fw3.itsdept.com	95	0	6
10.0.1.200	fw2.itsdept.com	95	0	6
10.0.0.200	fw1.itsdept.com	97	0	4

Cisco Plugins Summary

Cisco Plugins. CVSS Ranges; Low = 0.1 - 3.9, Medium = 4.0 - 6.9, High = 7.0 - 9.9, Critical = 10

IP Address	DNS Name	Info	Low	Med.	High	Crit.
10.0.4.200	fw5.itsdept.com	0	0	0	3	0
10.0.3.200	fw4.itsdept.com	0	0	0	3	0
10.0.2.200	fw3.itsdept.com	0	0	0	3	0
10.0.1.200	fw2.itsdept.com	0	0	0	3	0
10.0.0.200	fw1.itsdept.com	0	0	0	3	0

Configuration Audit Details - Fails and Couldn't Execute

10.0.4.200

DNS Name: fw5.itsdept.com
Last Scan: Feb 10, 2012 @ 10:36AM

Configuration Audit Details. Medium = Couldn't Execute, High = Fail

Severity	Plugin Name
High	1.1.1.1 Require AAA Authentication for Enable Mode
High	1.1.2.3 Require SSHv2 for Remote Management Access (ssh ip_address subnet_mask interface)
High	1.1.2.3 Require SSHv2 for Remote Management Access (ssh version 2)
High	1.1.2.4 Require Timeout for Login Sessions (ssh timeout)
High	1.2.1.3 Require Summer Time Clock When Using Local Time Zone (clock timezone)

10.0.3.200

DNS Name: fw4.itsdept.com
Last Scan: Feb 10, 2012 @ 10:36AM

Configuration Audit Details. Medium = Couldn't Execute, High = Fail

Severity	Plugin Name
High	1.1.2.5 Require SSH Access Control
High	1.1.3.1 Require EXEC Banner
High	1.1.3.2 Require Login Banner
High	1.1.3.3 Require MOTD Banner
High	1.1.3.4 Require ASDM Banner
High	1.1.5.3 Require SNMP Trap Server When SNMP is Used (snmp-server host)
High	1.1.5.4 Require Authorized Read SNMP Community Strings and Access Control (snmp-server community)
High	1.1.5.4 Require Authorized Read SNMP Community Strings and Access Control (snmp-server host)
High	1.2.2.2 Forbid ASDM Service If Not Used

10.0.2.200

DNS Name: fw3.itsdept.com
Last Scan: Feb 10, 2012 @ 10:36AM

Configuration Audit Details. Medium = Couldn't Execute, High = Fail

Severity	Plugin Name
High	1.2.4.1 Require Primary NTP Server
High	1.2.4.2 Require NTP Authentication (ntp authentication-key)
High	1.2.4.2 Require NTP Authentication (ntp authenticate)
High	1.2.4.2 Require NTP Authentication (ntp trusted-key)
High	1.2.4.2 Require NTP Authentication (ntp server)
High	1.3.1.3 Require TranslationSlot Timeout

10.0.1.200

DNS Name: fw2.itsdept.com
Last Scan: Feb 10, 2012 @ 10:36AM

Configuration Audit Details. Medium = Couldn't Execute, High = Fail

Severity	Plugin Name
High	1.2.3.5 Require Logging to Syslog Server
High	1.2.3.6 Require logging Trap Severity Level (6/information or 7/ debugging)
High	1.2.3.7 Require System Logging
High	1.2.3.8 Require Timestamp in Log Messages
High	1.2.3.9 Require NetFlow Secure Event Logging (flow-export event-type)
High	1.3.1.2 Require Connection Timeout

10.0.0.200

DNS Name: fw1.itsdept.com
Last Scan: Feb 10, 2012 @ 10:36AM

Configuration Audit Details. Medium = Couldn't Execute, High = Fail

Severity	Plugin Name
High	1.3.1.4 Require Intrusion Detection Actions (ip audit attack action)
High	1.3.1.8 Require Object Groups to Simplify Access Control Entries (port-object)
High	1.3.2.1 Forbid External Source Addresses on Outbound Traffic (access-list)
High	1.3.2.1 Forbid External Source Addresses on Outbound Traffic (access-group)

Cisco Plugin Details - Info Severity Excluded

10.0.4.200

DNS Name: fw5.itsdept.com
Last Scan: Feb 10, 2012 @ 10:36AM

Cisco Plugin Details. CVSS Ranges; Low = 0.1 - 3.9, Medium = 4.0 - 6.9, High = 7.0 - 9.9, Critical = 10

Plugin	Plugin Name	Severity	Port	Exploit?
52586	Cisco ASA 5500 Series Multiple Vulnerabilities (cisco-sa-20110223-asa)	High	0	Yes

Plugin	Plugin Name	Severity	Port	Exploit?
56045	Cisco ASA 5500 Series Multiple DoS Vulnerabilities (cisco-sa-20100804-asa)	High	0	Yes

Plugin	Plugin Name	Severity	Port	Exploit?
56631	Cisco ASA 5500 Series Multiple Vulnerabilities (cisco-sa-20111005-asa)	High	0	Yes

10.0.3.200

DNS Name: fw4.itsdept.com
Last Scan: Feb 10, 2012 @ 10:36AM

Cisco Plugin Details. CVSS Ranges; Low = 0.1 - 3.9, Medium = 4.0 - 6.9, High = 7.0 - 9.9, Critical = 10

Plugin	Plugin Name	Severity	Port	Exploit?
52586	Cisco ASA 5500 Series Multiple Vulnerabilities (cisco-sa-20110223-asa)	High	0	Yes

Plugin	Plugin Name	Severity	Port	Exploit?
56045	Cisco ASA 5500 Series Multiple DoS Vulnerabilities (cisco-sa-20100804-asa)	High	0	Yes

Plugin	Plugin Name	Severity	Port	Exploit?
56631	Cisco ASA 5500 Series Multiple Vulnerabilities (cisco-sa-20111005-asa)	High	0	Yes

10.0.2.200

DNS Name: fw3.itsdept.com
Last Scan: Feb 10, 2012 @ 10:36AM

Cisco Plugin Details. CVSS Ranges; Low = 0.1 - 3.9, Medium = 4.0 - 6.9, High = 7.0 - 9.9, Critical = 10

Plugin	Plugin Name	Severity	Port	Exploit?
52586	Cisco ASA 5500 Series Multiple Vulnerabilities (cisco-sa-20110223-asa)	High	0	Yes

Plugin	Plugin Name	Severity	Port	Exploit?
56045	Cisco ASA 5500 Series Multiple DoS Vulnerabilities (cisco-sa-20100804-asa)	High	0	Yes

Plugin	Plugin Name	Severity	Port	Exploit?
56631	Cisco ASA 5500 Series Multiple Vulnerabilities (cisco-sa-20111005-asa)	High	0	Yes

10.0.1.200

DNS Name: fw2.itsdept.com
Last Scan: Feb 10, 2012 @ 10:36AM

Cisco Plugin Details. CVSS Ranges; Low = 0.1 - 3.9, Medium = 4.0 - 6.9, High = 7.0 - 9.9, Critical = 10

Plugin	Plugin Name	Severity	Port	Exploit?
52586	Cisco ASA 5500 Series Multiple Vulnerabilities (cisco-sa-20110223-asa)	High	0	Yes

Plugin	Plugin Name	Severity	Port	Exploit?
56045	Cisco ASA 5500 Series Multiple DoS Vulnerabilities (cisco-sa-20100804-asa)	High	0	Yes

Plugin	Plugin Name	Severity	Port	Exploit?
56631	Cisco ASA 5500 Series Multiple Vulnerabilities (cisco-sa-20111005-asa)	High	0	Yes

10.0.0.200

DNS Name: fw1.itsdept.com
Last Scan: Feb 10, 2012 @ 10:36AM

Cisco Plugin Details. CVSS Ranges; Low = 0.1 - 3.9, Medium = 4.0 - 6.9, High = 7.0 - 9.9, Critical = 10

Plugin	Plugin Name	Severity	Port	Exploit?
52586	Cisco ASA 5500 Series Multiple Vulnerabilities (cisco-sa-20110223-asa)	High	0	Yes

Plugin	Plugin Name	Severity	Port	Exploit?
56045	Cisco ASA 5500 Series Multiple DoS Vulnerabilities (cisco-sa-20100804-asa)	High	0	Yes

Plugin	Plugin Name	Severity	Port	Exploit?
56631	Cisco ASA 5500 Series Multiple Vulnerabilities (cisco-sa-20111005-asa)	High	0	Yes