



secure auditor

Audit Report

Top 20 Vulnerabilities

Report Generated Time: 9/27/2011 At 3:04:45PM

Audit Name: : CiscoAudit(Sep 27 2011 2:55PM)

Description: : Cisco Audit Report

IP Count : 1

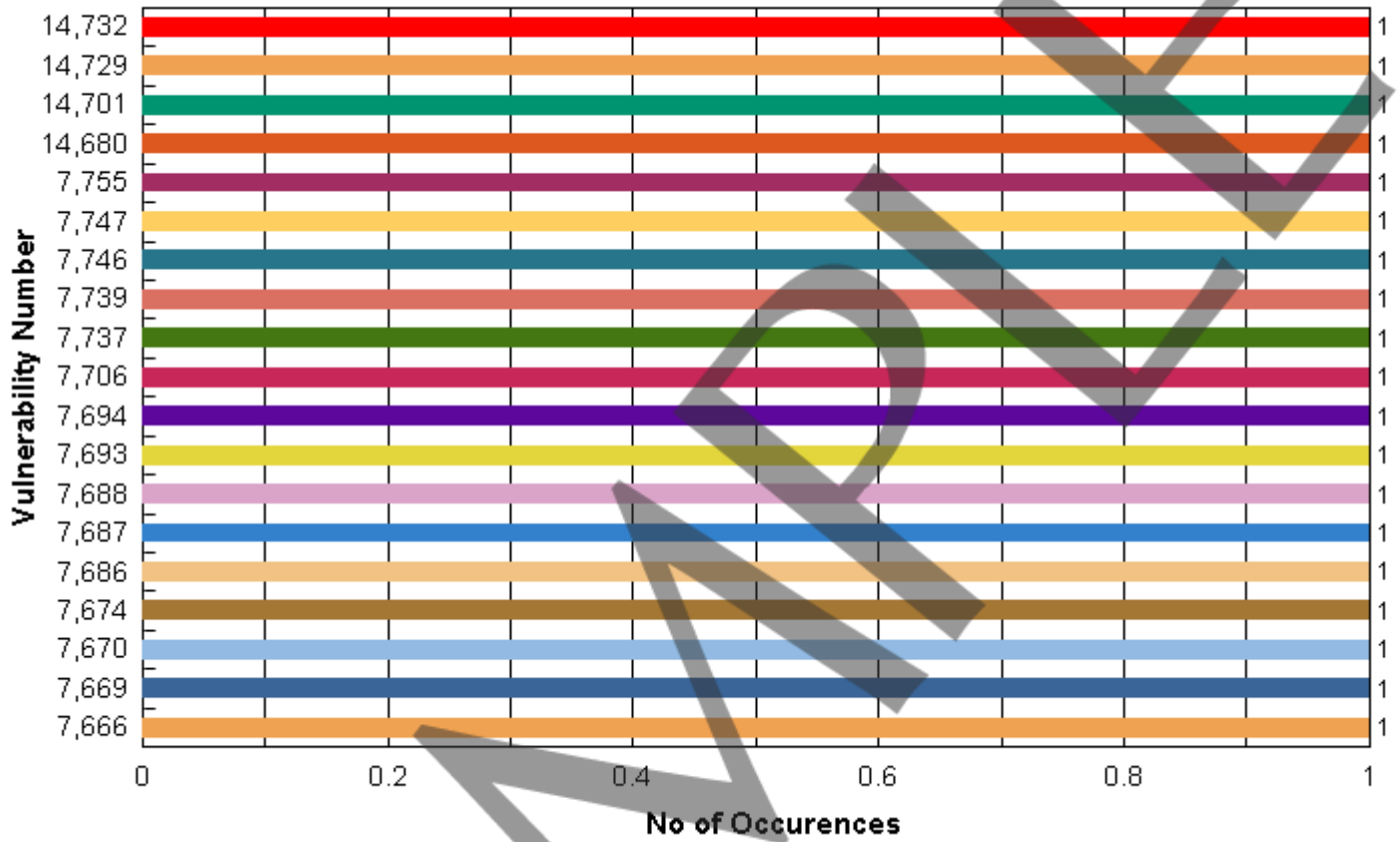
IP(s): : 192.168.68.203



Top 20 Vulnerabilities

Report generated on 27-Sep-2011 at 3:04:45PM

Top 20 Vulnerabilities



SAMPLE



Top 20 Vulnerabilities

Report generated on 27-Sep-2011 at 3:04:45PM

Audit performed on: CiscoAudit(Sep 27 2011 2:55PM)

Machine : 192.168.68.203

Vulnerability Name TCP Synwait Time is not configured.

Vulnerability Number 7,666 **RiskLevel** High

No. of Vulnerabilities : 1

Vulnerability Name Network Time Protocol (NTP) is enabled.

Vulnerability Number 7,669 **RiskLevel** High

No. of Vulnerabilities : 1

Vulnerability Name Cisco Discovery Protocol (CDP) is enabled.

Vulnerability Number 7,670 **RiskLevel** High

No. of Vulnerabilities : 1

Vulnerability Name Minimum Password Length is not configured.

Vulnerability Number 7,674 **RiskLevel** High

No. of Vulnerabilities : 1

Vulnerability Name Default private SNMP community is configured.

Vulnerability Number 7,686 **RiskLevel** High

No. of Vulnerabilities : 1

Vulnerability Name Default public SNMP community is configured.

Vulnerability Number 7,687 **RiskLevel** High

No. of Vulnerabilities : 1

Vulnerability Name Unicast RPF is enabled on required Interface.

Vulnerability Number 7,688 **RiskLevel** High

No. of Vulnerabilities : 1

Vulnerability Name Secure Copy (SCP) is not enabled.

Vulnerability Number 7,693 **RiskLevel** High

No. of Vulnerabilities : 1

Vulnerability Name Trivial File Transfer Protocol (TFTP) is enabled.

Vulnerability Number 7,694 **RiskLevel** High

No. of Vulnerabilities : 1

Vulnerability Name The Simple Network Management Protocol (SNMP) is enabled.

Vulnerability Number 7,706 **RiskLevel** High

No. of Vulnerabilities : 1

Vulnerability Name VTU exec-timeout is not configured.

Vulnerability Number 7,737 **RiskLevel** High

No. of Vulnerabilities : 1

Vulnerability Name Access Class is not configured on VTU.



Top 20 Vulnerabilities

Report generated on 27-Sep-2011 at 3:04:45PM

Audit performed on: CiscoAudit(Sep 27 2011 2:55PM)

Vulnerability Number 7,739 **RiskLevel** High

No. of Vulnerabilities : 1

Vulnerability Name Too many virtual terminals are configured.

Vulnerability Number 7,746 **RiskLevel** High

No. of Vulnerabilities : 1

Vulnerability Name HTTP Server is configured.

Vulnerability Number 7,747 **RiskLevel** High

No. of Vulnerabilities : 1

Vulnerability Name IP BOOTP Server Service is enabled.

Vulnerability Number 7,755 **RiskLevel** High

No. of Vulnerabilities : 1

Vulnerability Name Privilege level is not set for user accounts.

Vulnerability Number 14,680 **RiskLevel** High

No. of Vulnerabilities : 1

Vulnerability Name Rip Version 1 is configured on the device.

Vulnerability Number 14,701 **RiskLevel** High

No. of Vulnerabilities : 1

Vulnerability Name Authentication Retry settings are not configuration for SSH

Vulnerability Number 14,729 **RiskLevel** High

No. of Vulnerabilities : 1

Vulnerability Name User-based HTTP Authentication not configured.

Vulnerability Number 14,732 **RiskLevel** High

No. of Vulnerabilities : 1

Total Vulnerabilities : 19