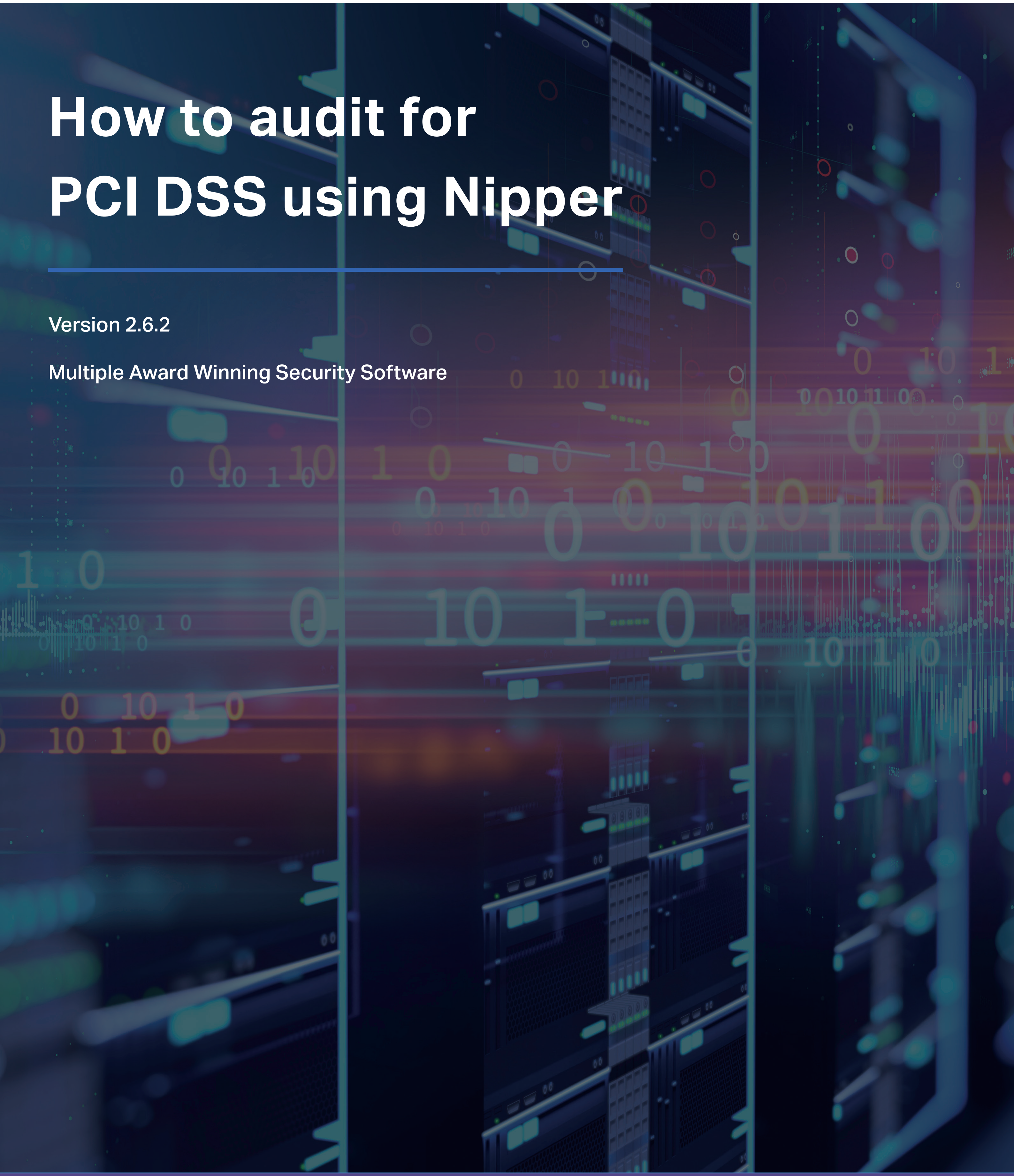
TITANIA NIPPER



How to audit for PCI DSS using Nipper

Version 2.6.2

Multiple Award Winning Security Software

Published November 2019

This document is intended to provide advice and assistance for the installation and running of Nipper software. While Titania takes care to ensure that all the information included in this document is accurate and relevant, customers are advised to seek further assistance from our support staff if required.

The use of Nipper software is subject to the acceptance of the license agreement.

Titania Limited
Security House
Barbourne Road
Worcester
WR1 1RS

Telephone: **(+44)1905 888 785**
Technical Support: Support@titania.com
Licensing: Enquiries@titania.com
Nipper Support: www.titania.com/support/nipper-support

Contents

Running a PCI DSS report with Nipper

Automate the auditing of your most critical PCI DSS (Payment Card Industry Data Security Standard) checks with Titania Nipper. You can easily, accurately and quickly assess your firewalls, switches and routers and cover many aspects of the PCI DSS compliance requirements.

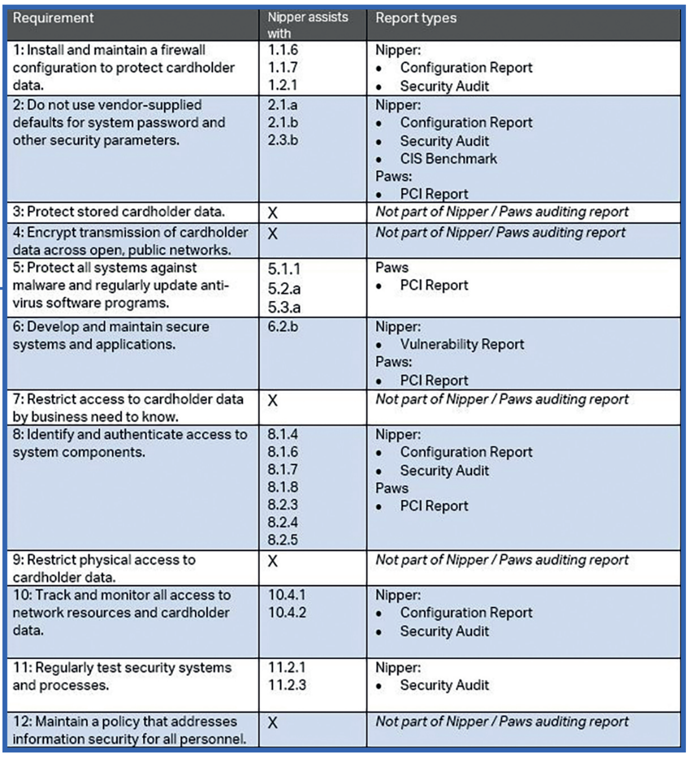
This PCI DSS ‘How to’ guide has been designed to demonstrate how Nipper software can help simplify meeting the requirements of PCI DSS.

The guide gives a simple step-by-step process in running the relevant audits to produce an easy-to-read, comprehensive report from which you can choose the most relevant information to report and evidence the PCI DSS requirements.

The report will prioritize risks found and offer remediation advice for each, that you can action to then be able to meet the respective PCI DSS requirements.

These reports assist you in addressing the aspects of the PCI DSS Compliance as shown in the table.

By the end of the guide you will be able to run the necessary audits to cover these requirements, which you can use to demonstrate how you cover them off and what measures you have in place to mitigate potential risks.



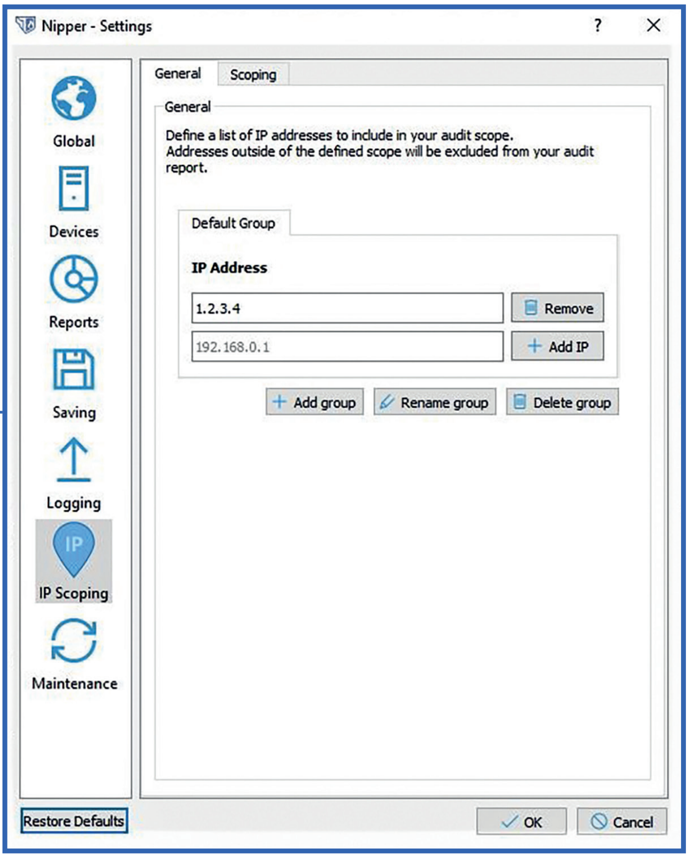
Requirement	Nipper assists with	Report types
1: Install and maintain a firewall configuration to protect cardholder data.	1.1.6 1.1.7 1.2.1	Nipper: • Configuration Report • Security Audit
2: Do not use vendor-supplied defaults for system password and other security parameters.	2.1.a 2.1.b 2.3.b	Nipper: • Configuration Report • Security Audit • CIS Benchmark Paws: • PCI Report
3: Protect stored cardholder data.	X	*Not part of Nipper / Paws auditing report*
4: Encrypt transmission of cardholder data across open, public networks.	X	*Not part of Nipper/ Paws auditing report*
5: Protect all systems against malware and regularly update anti-virus software programs.	5.1.1 5.2.a 5.3.a	Paws • PCI Report
6: Develop and maintain secure systems and applications.	6.2.b	Nipper: • Vulnerability Report Paws: • PCI Report
7: Restrict access to cardholder data by business need to know.	X	*Not part of Nipper / Paws auditing report*
8: Identify and authenticate access to system components.	8.1.4 8.1.6 8.1.7 8.1.8 8.2.3 8.2.4 8.2.5	Nipper: • Configuration Report • Security Audit Paws • PCI Report
9: Restrict physical access to cardholder data.	X	*Not part of Nipper / Paws auditing report*
10: Track and monitor all access to network resources and cardholder data.	10.4.1 10.4.2	Nipper: • Configuration Report • Security Audit
11: Regularly test security systems and processes.	11.2.1 11.2.3	Nipper: • Security Audit
12: Maintain a policy that addresses information security for all personnel.	X	*Not part of Nipper / Paws auditing report*

Scoping the report

Nipper includes an IP scoping feature which allows you to reduce the scope of your audit to specific sets or ranges of IP addresses; allowing you to define your Cardholder Data Environment (CDE) by IP address, CIDRs or IP ranges.

This restricts the audit report to just rules, services, issues etc. that only affect items included in the scope you have defined – saving you both time and effort by excluding irrelevant issues within the report.

For further information on how to set up IP Scoping, refer to the IP Scoping section found in the Nipper Beginner’s Guide, which is in the User Guides area of the website.



Define a list of IP addresses to include in your audit scope. Addresses outside of the defined scope will be excluded from your audit report.

Default Group

IP Address

1.2.3.4

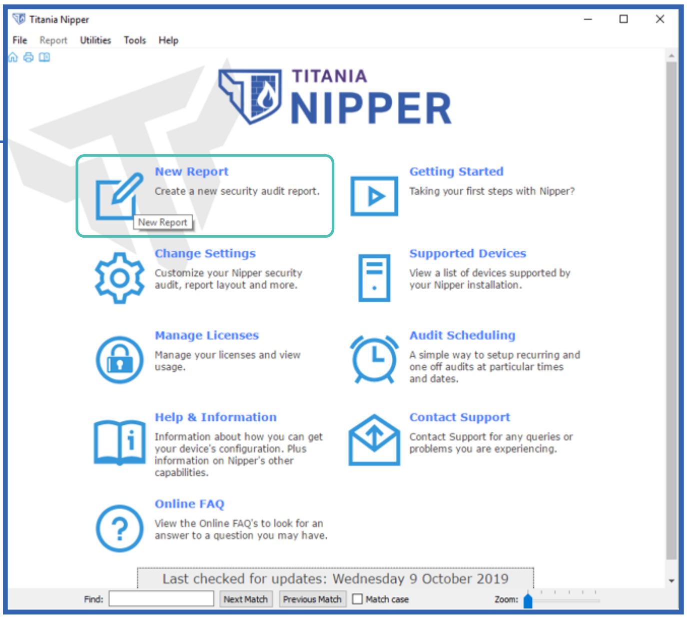
192.168.0.1

Step 1 – Installing Nipper and your license

- If you have Nipper already installed – Go to Step 2
- If you need to install Nipper:
  - Go to the 'Installing Nipper' section of the Nipper Beginner's Guide
- If you need to install your license:
  - Go to the 'Adding a license to Nipper' section of the Nipper Beginner's Guide
- The Nipper Beginner's Guide can be found in the user guides section of the website
- Go to Step 2

Step 2 – Create a new report

- Open Nipper and select 'New Report' on the Nipper homepage.



New Report
Create a new security audit report.

Getting Started
Taking your first steps with Nipper?

Change Settings
Customize your Nipper security audit, report layout and more.

Supported Devices
View a list of devices supported by your Nipper installation.

Manage Licenses
Manage your licenses and view usage.

Audit Scheduling
A simple way to setup recurring and one off audits at particular times and dates.

Help & Information
Information about how you can get your device's configuration. Plus information on Nipper's other capabilities.

Contact Support
Contact Support for any queries or problems you are experiencing.

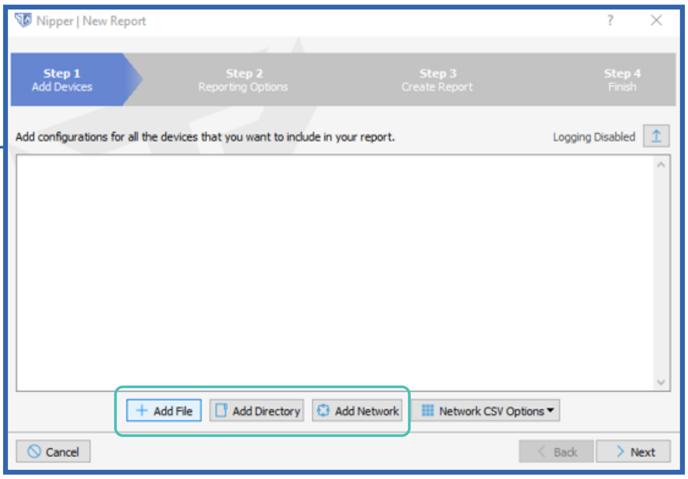
Online FAQ
View the Online FAQ's to look for an answer to a question you may have.

Last checked for updates: Wednesday 9 October 2019

Step 3 – Choose your devices to audit

Here you will see 3 options to;

- Add File (this is a single, manually exported device configuration file)
- Add Directory (containing one or more manually exported device configuration files
- Add Network (configuration files of supported devices)



Add configurations for all the devices that you want to include in your report.

You will need to navigate to where you have stored your files to be able to add them.

For further information on how to choose your devices refer to the 'Creating your first report with Nipper' section of the Nipper Beginner's Guide.

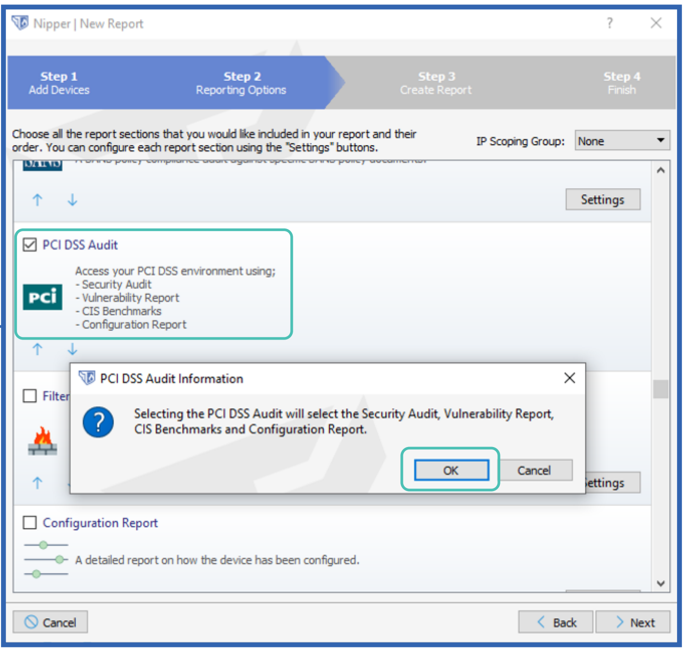
Once you have chosen your devices, click on **'Next'.**

Step 4 – Choose your reporting options

- The reporting options screen will appear
- Scroll down the screen and check the box next to PCI DSS Audit
- By clicking on this, the following will automatically be chosen:
  - Configuration Report
  - Security Audit
  - Vulnerability Audit
  - *CIS Benchmarks

- Click **'Next'** and a notification regarding the relevant reports selected will appear
- Click **'OK'**

**The CIS Benchmarks audit will run if you include CISCO ASA, IOS12 or IOS15 devices in your PCI audit.*



Nipper | New Report

Step 1 Add Devices · Step 2 Reporting Options · Step 3 Create Report · Step 4 Finish

Choose all the report sections that you would like included in your report and their order. You can configure each report section using the "Settings" buttons.

IP Scoping Group: None

☑ PCI DSS Audit

Access your PCI DSS environment using;
- Security Audit
- Vulnerability Report
- CIS Benchmarks
- Configuration Report

PCI DSS Audit Information

Selecting the PCI DSS Audit will select the Security Audit, Vulnerability Report, CIS Benchmarks and Configuration Report.

☐ Configuration Report

A detailed report on how the device has been configured.

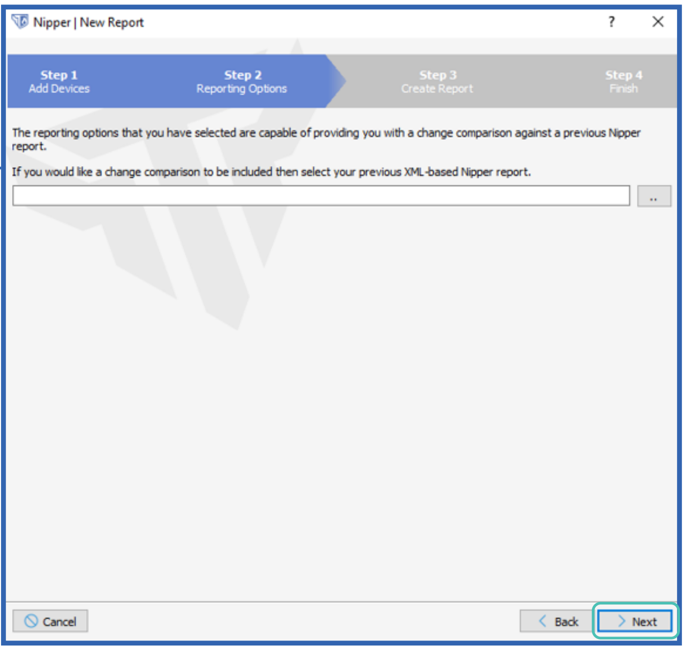
Step 5 – Compare the results with a previous report

- The next screen will give you the option to compare against a previous report. Instructions on how to do this can be found in the Nipper's Beginner's Guide
- If not required simply select **'Next'**

The report will be generated, taking only a few moments to appear.

Note: At this stage if you have selected CISCO ASA, IOS 12 or IOS15 devices to audit, you will see additional boxes appear:

- *CIS Settings*
  - *Click **'OK'***
- *Interface Definitions*
  - *Click **'OK'***

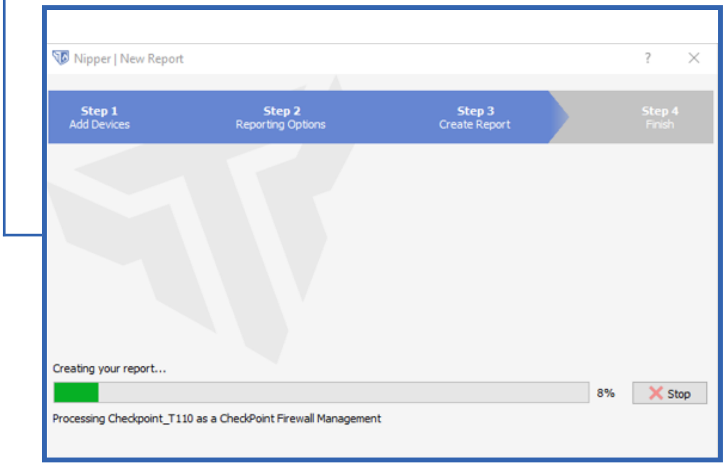


Nipper | New Report

Step 1 Add Devices · Step 2 Reporting Options · Step 3 Create Report · Step 4 Finish

The reporting options that you have selected are capable of providing you with a change comparison against a previous Nipper report.

If you would like a change comparison to be included then select your previous XML-based Nipper report.



Nipper | New Report

Step 1 Add Devices · Step 2 Reporting Options · Step 3 Create Report · Step 4 Finish

Creating your report...

8%

Processing Checkpoint_T110 as a CheckPoint Firewall Management

Step 6 – Once the report has run

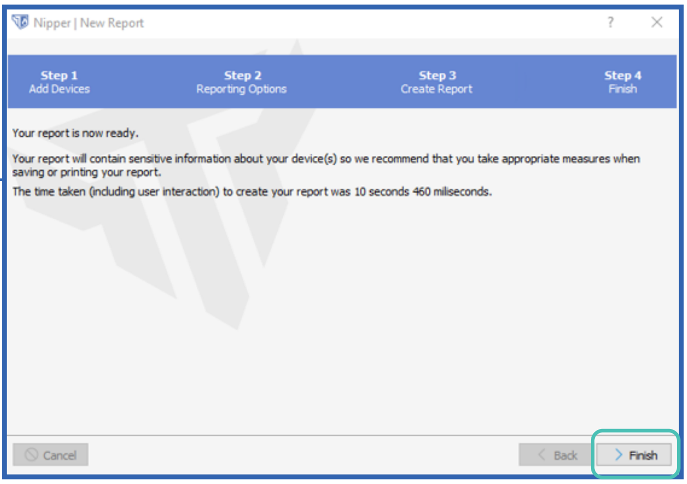
» When the report has finished running an advisory note, about handling the sensitive data contained, will appear.

» Click **'Finish'**

Your report will appear and give comprehensive detail. There is a summary at the top which is handy for a quick view of content and top-line reporting.

Note: The report does not save within the software. If you need to save, you will need to do this to an external file separate from the Nipper software. For further information on how to save a copy of your report please refer to 'Saving your reports' section in the [Nipper Beginner's Guide.]

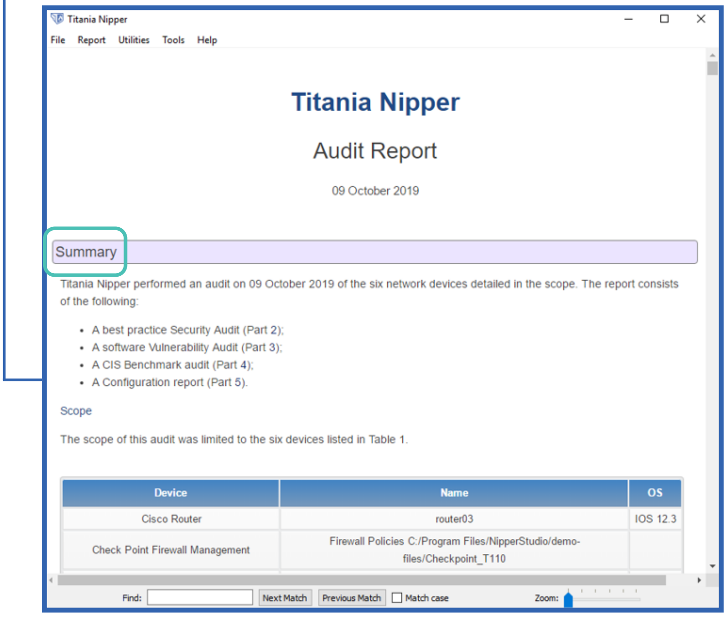
There are a number of options to 'save file as', however by saving as an html file will keep the links in the report live.



Your report is now ready.

Your report will contain sensitive information about your device(s) so we recommend that you take appropriate measures when saving or printing your report.

The time taken (including user interaction) to create your report was 10 seconds 460 miliseconds.



Titania Nipper

Audit Report

09 October 2019

Summary

Titania Nipper performed an audit on 09 October 2019 of the six network devices detailed in the scope. The report consists of the following:

- A best practice Security Audit (Part 2);
- A software Vulnerability Audit (Part 3);
- A CIS Benchmark audit (Part 4);
- A Configuration report (Part 5).

Scope

The scope of this audit was limited to the six devices listed in Table 1.

Device	Name	OS
Cisco Router	router03	IOS 12.3
Check Point Firewall Management	Firewall Policies C:/Program Files/NipperStudio/demo-files/Checkpoint_T110	

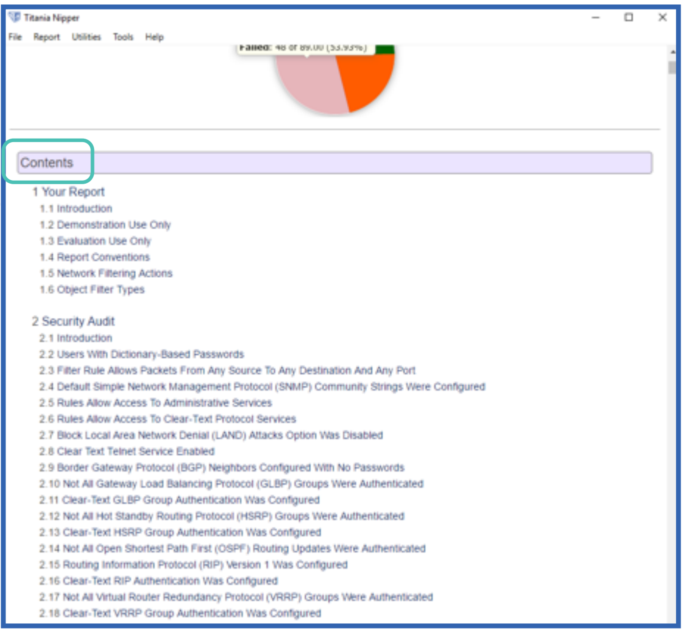
Step 7 - Navigating the report

» Below the summary is a Contents list

» Scroll up and down this list to find the section you want

» Click on the title to be taken to its relevant section

*Note: To return to the contents menu at any point, right click and click on **'Back'***


Titania Nipper
File Report Utilities Tools Help
Failed: 48 of 89.00 (53.93%)

Contents

1 Your Report
1.1 Introduction
1.2 Demonstration Use Only
1.3 Evaluation Use Only
1.4 Report Conventions
1.5 Network Filtering Actions
1.6 Object Filter Types

2 Security Audit
2.1 Introduction
2.2 Users With Dictionary-Based Passwords
2.3 Filter Rule Allows Packets From Any Source To Any Destination And Any Port
2.4 Default Simple Network Management Protocol (SNMP) Community Strings Were Configured
2.5 Rules Allow Access To Administrative Services
2.6 Rules Allow Access To Clear-Text Protocol Services
2.7 Block Local Area Network Denial (LAND) Attacks Option Was Disabled
2.8 Clear Text Telnet Service Enabled
2.9 Border Gateway Protocol (BGP) Neighbors Configured With No Passwords
2.10 Not All Gateway Load Balancing Protocol (GLBP) Groups Were Authenticated
2.11 Clear-Text GLBP Group Authentication Was Configured
2.12 Not All Hot Standby Routing Protocol (HSRP) Groups Were Authenticated
2.13 Clear-Text HSRP Group Authentication Was Configured
2.14 Not All Open Shortest Path First (OSPF) Routing Updates Were Authenticated
2.15 Routing Information Protocol (RIP) Version 1 Was Configured
2.16 Clear-Text RIP Authentication Was Configured
2.17 Not All Virtual Router Redundancy Protocol (VRRP) Groups Were Authenticated
2.18 Clear-Text VRRP Group Authentication Was Configured

Step 8 - Interpreting the report

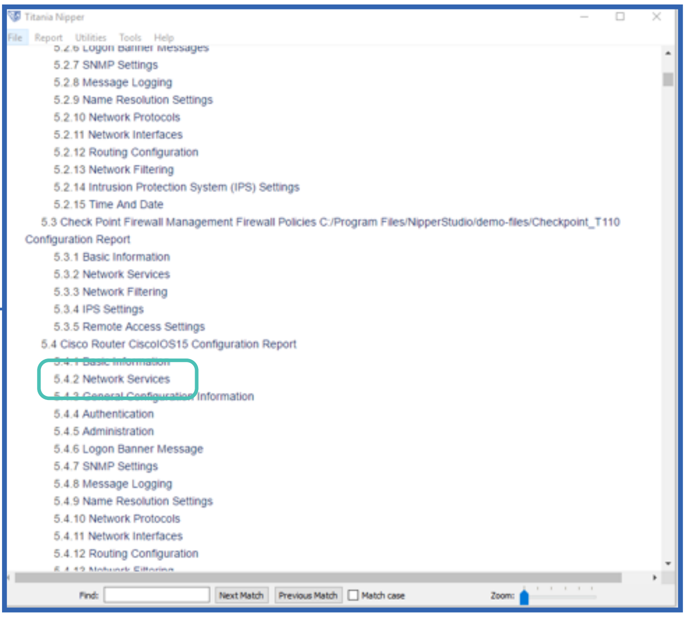
Requirement 1: Install and maintain a firewall configuration to protect card-holder data.

Nipper assists with: 1.1.6, 1.1.7 & 1.2.1 of this requirement.

The following parts are met by having run the **Configuration Report & Security Audit:**

Identify all network services enabled on your scope

» Within the **Configuration Report**, > go to the Network Services section



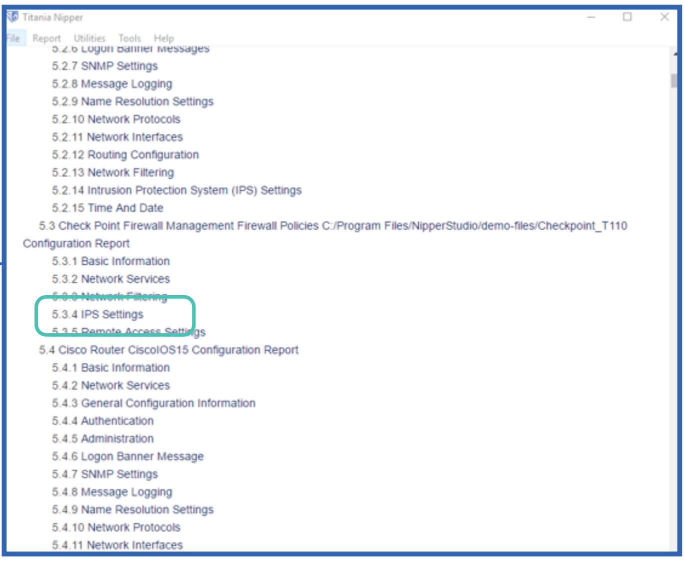
Titania Nipper

5.2.6 Logon Banner Messages
5.2.7 SNMP Settings
5.2.8 Message Logging
5.2.9 Name Resolution Settings
5.2.10 Network Protocols
5.2.11 Network Interfaces
5.2.12 Routing Configuration
5.2.13 Network Filtering
5.2.14 Intrusion Protection System (IPS) Settings
5.2.15 Time And Date
5.3 Check Point Firewall Management Firewall Policies C:/Program Files/NipperStudio/demo-files/Checkpoint_T110 Configuration Report
5.3.1 Basic Information
5.3.2 Network Services
5.3.3 Network Filtering
5.3.4 IPS Settings
5.3.5 Remote Access Settings
5.4 Cisco Router CiscoIOS15 Configuration Report
5.4.1 Basic Information
5.4.2 Network Services
5.4.3 General Configuration Information
5.4.4 Authentication
5.4.5 Administration
5.4.6 Logon Banner Message
5.4.7 SNMP Settings
5.4.8 Message Logging
5.4.9 Name Resolution Settings
5.4.10 Network Protocols
5.4.11 Network Interfaces
5.4.12 Routing Configuration
5.4.13 Network Filtering

Identify all firewall and router rule sets, highlight crucial information relating to permitted and denied network traffic

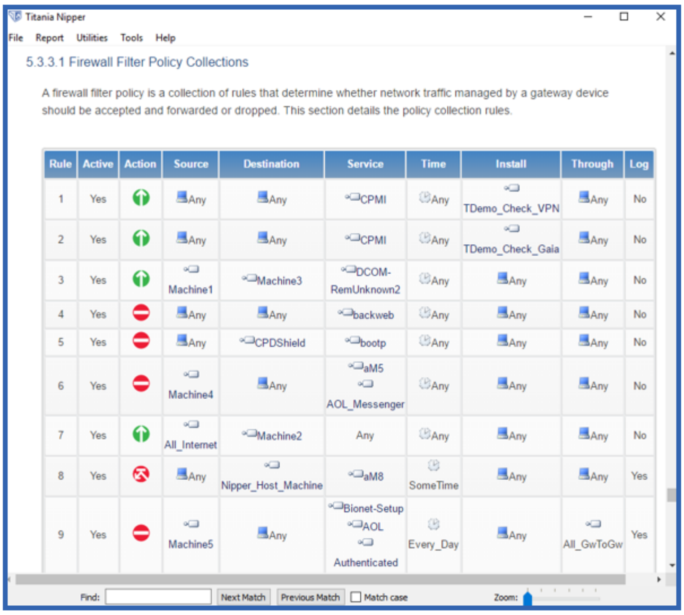
» Within the **Configuration Report**, > go to the Network Filtering section.

» The list of Rules will be listed and can be checked line-by-line for issues.



Titania Nipper

5.2.6 Logon Banner Messages
5.2.7 SNMP Settings
5.2.8 Message Logging
5.2.9 Name Resolution Settings
5.2.10 Network Protocols
5.2.11 Network Interfaces
5.2.12 Routing Configuration
5.2.13 Network Filtering
5.2.14 Intrusion Protection System (IPS) Settings
5.2.15 Time And Date
5.3 Check Point Firewall Management Firewall Policies C:/Program Files/NipperStudio/demo-files/Checkpoint_T110 Configuration Report
5.3.1 Basic Information
5.3.2 Network Services
5.3.3 Network Filtering
5.3.4 IPS Settings
5.3.5 Remote Access Settings
5.4 Cisco Router CiscoIOS15 Configuration Report
5.4.1 Basic Information
5.4.2 Network Services
5.4.3 General Configuration Information
5.4.4 Authentication
5.4.5 Administration
5.4.6 Logon Banner Message
5.4.7 SNMP Settings
5.4.8 Message Logging
5.4.9 Name Resolution Settings
5.4.10 Network Protocols
5.4.11 Network Interfaces



Titania Nipper

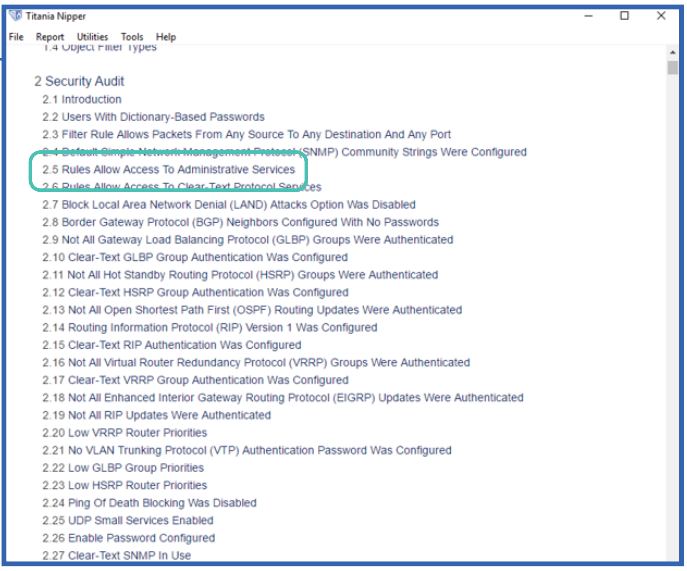
5.3.3.1 Firewall Filter Policy Collections

A firewall filter policy is a collection of rules that determine whether network traffic managed by a gateway device should be accepted and forwarded or dropped. This section details the policy collection rules.

Rule	Active	Action	Source	Destination	Service	Time	Install	Through	Log
1	Yes	⬆	Any	Any	CPMI	Any	TDemo_Check_VPN	Any	No
2	Yes	⬆	Any	Any	CPMI	Any	TDemo_Check_Gaia	Any	No
3	Yes	⬆	Machine1	Machine3	DCOM-RemUnknown2	Any	Any	Any	No
4	Yes	⛔	Any	Any	backweb	Any	Any	Any	No
5	Yes	⛔	Any	CPDShield	bootp	Any	Any	Any	No
6	Yes	⛔	Machine4	Any	aM5 AOL_Messenger	Any	Any	Any	No
7	Yes	⬆	All_Internet	Machine2	Any	Any	Any	Any	No
8	Yes	⊗	Any	Nipper_Host_Machine	aM8	SomeTime	Any	Any	Yes
9	Yes	⛔	Machine5	Any	Bionet-Setup AOL Authenticated	Every_Day	Any	All_GwToGw	Yes

Review issues in the rule sets, such as Any-to-Any rules against the CVSS scoring system

» Go to the **Security Audit** section to review this.



1.4 Object Filter Types

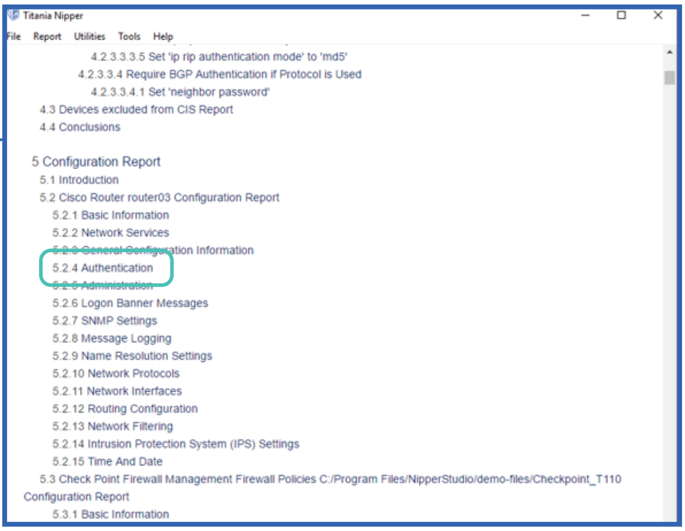
2 Security Audit
2.1 Introduction
2.2 Users With Dictionary-Based Passwords
2.3 Filter Rule Allows Packets From Any Source To Any Destination And Any Port
2.4 Default Simple Network Management Protocol (SNMP) Community Strings Were Configured
2.5 Rules Allow Access To Administrative Services
2.6 Rules Allow Access To Clear-Text Protocol Services
2.7 Block Local Area Network Denial (LAND) Attacks Option Was Disabled
2.8 Border Gateway Protocol (BGP) Neighbors Configured With No Passwords
2.9 Not All Gateway Load Balancing Protocol (GLBP) Groups Were Authenticated
2.10 Clear-Text GLBP Group Authentication Was Configured
2.11 Not All Hot Standby Routing Protocol (HSRP) Groups Were Authenticated
2.12 Clear-Text HSRP Group Authentication Was Configured
2.13 Not All Open Shortest Path First (OSPF) Routing Updates Were Authenticated
2.14 Routing Information Protocol (RIP) Version 1 Was Configured
2.15 Clear-Text RIP Authentication Was Configured
2.16 Not All Virtual Router Redundancy Protocol (VRRP) Groups Were Authenticated
2.17 Clear-Text VRRP Group Authentication Was Configured
2.18 Not All Enhanced Interior Gateway Routing Protocol (EIGRP) Updates Were Authenticated
2.19 Not All RIP Updates Were Authenticated
2.20 Low VRRP Router Priorities
2.21 No VLAN Trunking Protocol (VTP) Authentication Password Was Configured
2.22 Low GLBP Group Priorities
2.23 Low HSRP Router Priorities
2.24 Ping Of Death Blocking Was Disabled
2.25 UDP Small Services Enabled
2.26 Enable Password Configured
2.27 Clear-Text SNMP In Use

Requirement 2: Do not use vendor-supplied defaults for system password and other security parameters.

Nipper assists with: 2.1.a, 2.1.b & 2.3.b of this requirement.

Within the **Configuration Report**, > go to the Authentication section.

» Here you can review the listing of all user accounts and passwords (that are not encrypted) for unused accounts and security roles.

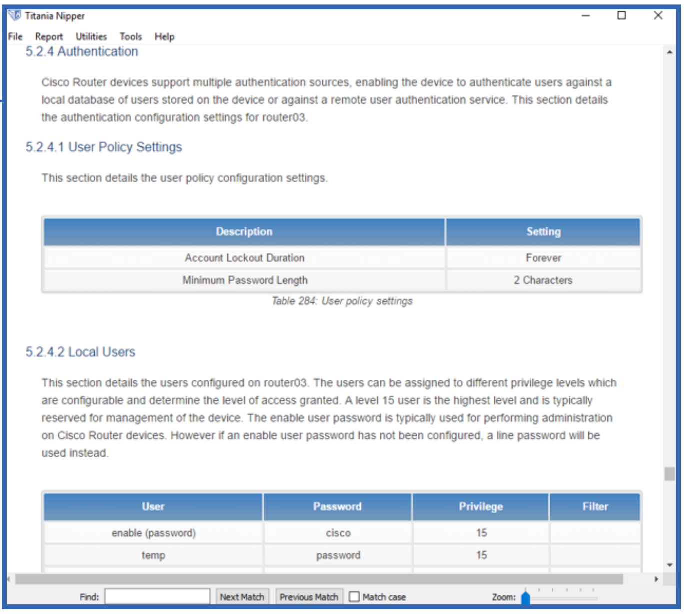


4.2.3.3.3.5 Set 'ip rip authentication mode' to 'md5'
4.2.3.3.4 Require BGP Authentication if Protocol is Used
4.2.3.3.4.1 Set 'neighbor password'
4.3 Devices excluded from CIS Report
4.4 Conclusions

5 Configuration Report
5.1 Introduction
5.2 Cisco Router router03 Configuration Report
5.2.1 Basic Information
5.2.2 Network Services
5.2.3 General Configuration Information
5.2.4 Authentication
5.2.5 Administration
5.2.6 Logon Banner Messages
5.2.7 SNMP Settings
5.2.8 Message Logging
5.2.9 Name Resolution Settings
5.2.10 Network Protocols
5.2.11 Network Interfaces
5.2.12 Routing Configuration
5.2.13 Network Filtering
5.2.14 Intrusion Protection System (IPS) Settings
5.2.15 Time And Date
5.3 Check Point Firewall Management Firewall Policies C:/Program Files/NipperStudio/demo-files/Checkpoint_T110 Configuration Report
5.3.1 Basic Information

By including the **Security Audit** as part of your report, you evidence your effort in identifying and highlighting insecurities in the devices included in your scope, (such as vendor-supplied default passwords, insecure protocol settings and more).

Note: If you have CISCO ASA, IOS12 or IOS15 we also include CIS (Center for Internet Security) Benchmarks to assist with meeting this requirement.



5.2.4 Authentication

Cisco Router devices support multiple authentication sources, enabling the device to authenticate users against a local database of users stored on the device or against a remote user authentication service. This section details the authentication configuration settings for router03.

5.2.4.1 User Policy Settings

This section details the user policy configuration settings.

Description	Setting
Account Lockout Duration	Forever
Minimum Password Length	2 Characters

Table 284: User policy settings

5.2.4.2 Local Users

This section details the users configured on router03. The users can be assigned to different privilege levels which are configurable and determine the level of access granted. A level 15 user is the highest level and is typically reserved for management of the device. The enable user password is typically used for performing administration on Cisco Router devices. However if an enable user password has not been configured, a line password will be used instead.

User	Password	Privilege	Filter
enable (password)	cisco	15	
temp	password	15	

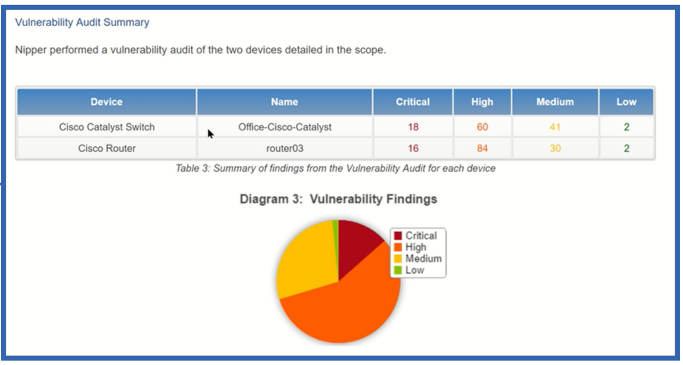
Requirement 6: Develop and maintain secure systems and applications.

Nipper assists with: 6.2.b of this requirement.

By running the **Vulnerability Audit** you can identify software vulnerabilities known through the NIST NVD within your report.

All the details known about the vulnerability such as the following will be displayed in the report:

- Issue Severity (ranked and colour coded)
- CVE number and references
- CVSS v2 information
- Summary information
- Affected devices from the scope
- Any vendor security advisories



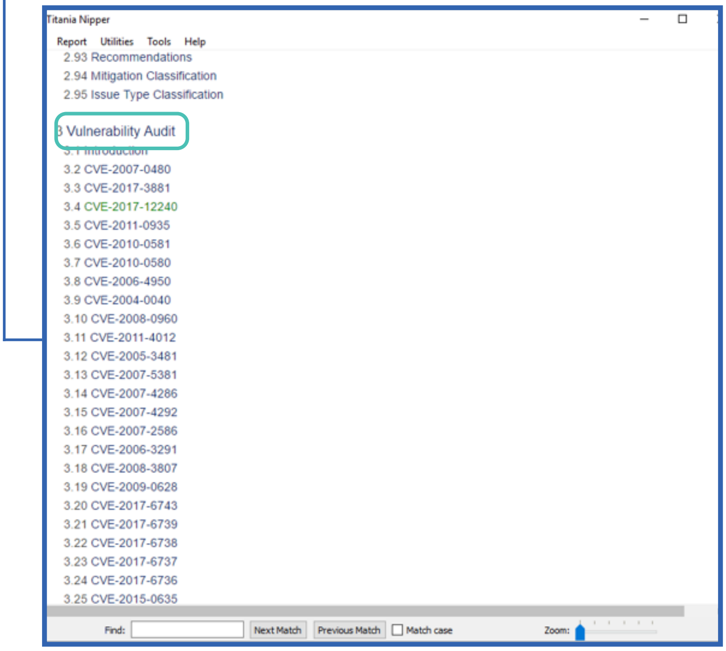
Vulnerability Audit Summary

Nipper performed a vulnerability audit of the two devices detailed in the scope.

Device	Name	Critical	High	Medium	Low
Cisco Catalyst Switch	Office-Cisco-Catalyst	18	60	41	2
Cisco Router	router03	16	84	30	2

Table 3: Summary of findings from the Vulnerability Audit for each device

Diagram 3: Vulnerability Findings



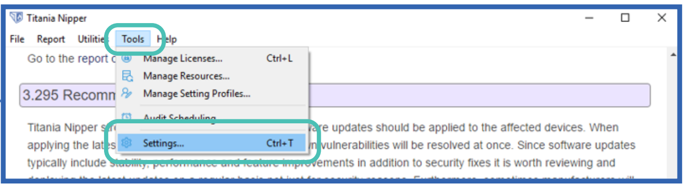
2.93 Recommendations
2.94 Mitigation Classification
2.95 Issue Type Classification

3 Vulnerability Audit
3.1 Introduction
3.2 CVE-2007-0480
3.3 CVE-2017-3881
3.4 CVE-2017-12240
3.5 CVE-2011-0935
3.6 CVE-2010-0581
3.7 CVE-2010-0580
3.8 CVE-2006-4950
3.9 CVE-2004-0040
3.10 CVE-2008-0960
3.11 CVE-2011-4012
3.12 CVE-2005-3481
3.13 CVE-2007-5381
3.14 CVE-2007-4286
3.15 CVE-2007-4292
3.16 CVE-2007-2586
3.17 CVE-2006-3291
3.18 CVE-2008-3807
3.19 CVE-2009-0628
3.20 CVE-2017-6743
3.21 CVE-2017-6739
3.22 CVE-2017-6738
3.23 CVE-2017-6737
3.24 CVE-2017-6736
3.25 CVE-2015-0635

Requirement 8: Identify and authenticate access to system components.

Nipper assists with: 8.1.4, 8.1.6, 8.1.7, 8.1.8, 8.2.3, 8.2.4 & 8.2.5 of this requirement.

Read through the **Security Audit** report to see any highlighted issues where your user and password policies are in violation.



Titania Nipper
File Report Utilities Tools Help
Manage Licenses... Ctrl+L
Manage Resources...
Manage Setting Profiles...
Audit Scheduling
Settings... Ctrl+T

Go to the report c

3.295 Recomm

Titania Nipper st ... are updates should be applied to the affected devices. When applying the lates ... n vulnerabilities will be resolved at once. Since software updates typically include stability, performance and feature improvements in addition to security fixes it is worth reviewing and

Note: The following parameters for password policies can be

*configured in the **Security Audit** settings:*

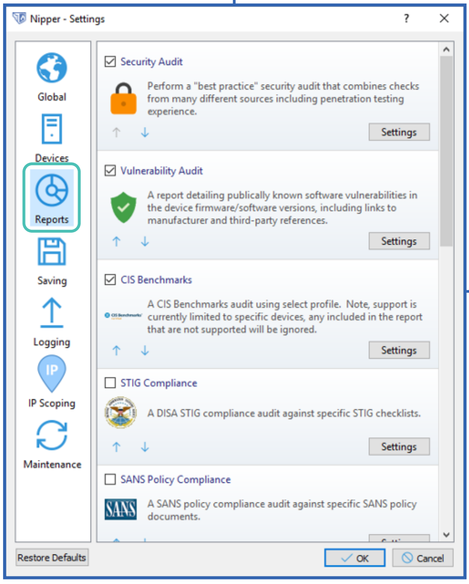
- *Minimum Password Length*
- *Password Complexity, such as character case, including nonalphanumeric*
- *characters, repeating characters, excluding common dictionary-based words and more*
- *Password Age (Minimum and Maximum)*
- *Password History and Expiry*
- *Session Lockout*

To change the settings of the Security Audit to suit the User Policy and Passwords rules required to then audit against:

- Go to **'Tools'** and then **'Settings'**
- Click on **'Reports'**

To then come out of the Security Audit settings:

- Click **'Cancel'**



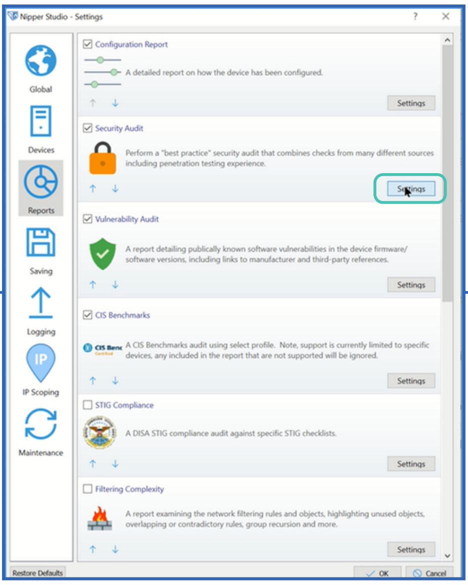
☑ Security Audit
Perform a "best practice" security audit that combines checks from many different sources including penetration testing experience.

☑ Vulnerability Audit
A report detailing publically known software vulnerabilities in the device firmware/software versions, including links to manufacturer and third-party references.

☑ CIS Benchmarks
A CIS Benchmarks audit using select profile. Note, support is currently limited to specific devices, any included in the report that are not supported will be ignored.

☐ STIG Compliance
A DISA STIG compliance audit against specific STIG checklists.

☐ SANS Policy Compliance
A SANS policy compliance audit against specific SANS policy documents.



☑ Configuration Report
A detailed report on how the device has been configured.

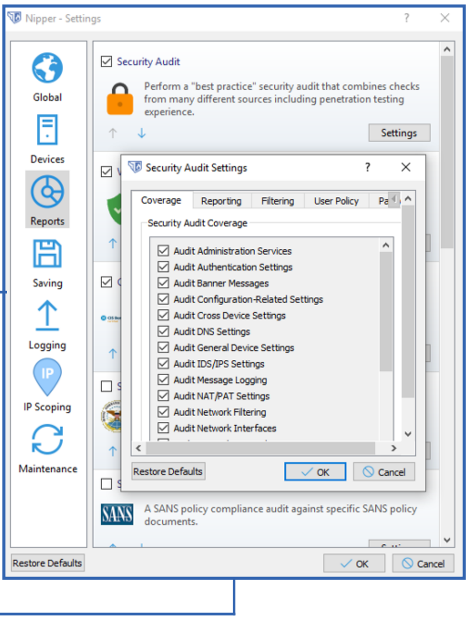
☑ Security Audit
Perform a "best practice" security audit that combines checks from many different sources including penetration testing experience.

☑ Vulnerability Audit
A report detailing publically known software vulnerabilities in the device firmware/software versions, including links to manufacturer and third-party references.

☑ CIS Benchmarks
A CIS Benchmarks audit using select profile. Note, support is currently limited to specific devices, any included in the report that are not supported will be ignored.

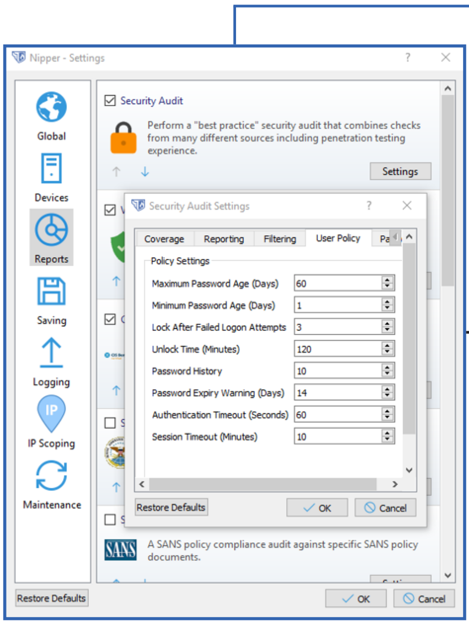
☐ STIG Compliance
A DISA STIG compliance audit against specific STIG checklists.

☐ Filtering Complexity
A report examining the network filtering rules and objects, highlighting unused objects, overlapping or contradictory rules, group recursion and more.



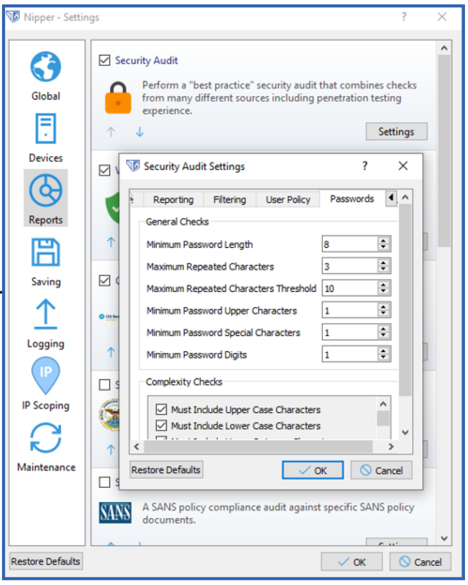
Security Audit Coverage

☑ Audit Administration Services
☑ Audit Authentication Settings
☑ Audit Banner Messages
☑ Audit Configuration-Related Settings
☑ Audit Cross Device Settings
☑ Audit DNS Settings
☑ Audit General Device Settings
☑ Audit IDS/IPS Settings
☑ Audit Message Logging
☑ Audit NAT/PAT Settings
☑ Audit Network Filtering
☑ Audit Network Interfaces



Policy Settings

Maximum Password Age (Days)	60
Minimum Password Age (Days)	1
Lock After Failed Logon Attempts	3
Unlock Time (Minutes)	120
Password History	10
Password Expiry Warning (Days)	14
Authentication Timeout (Seconds)	60
Session Timeout (Minutes)	10



General Checks

Minimum Password Length	8
Maximum Repeated Characters	3
Maximum Repeated Characters Threshold	10
Minimum Password Upper Characters	1
Minimum Password Special Characters	1
Minimum Password Digits	1

Complexity Checks

☑ Must Include Upper Case Characters
☑ Must Include Lower Case Characters

Requirement 10: Track and monitor all access to network resources and cardholder data.

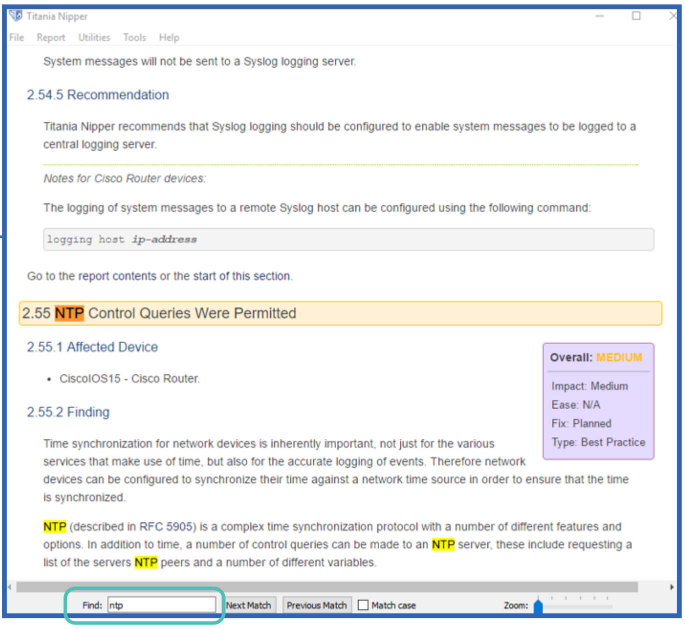
Nipper assists with: 10.4.1 & 10.4.2 of this requirement.

Recording logs is a common way to monitor network resource access, which involves ensuring the correct time is logged for events to enable better issue investigation.

- To monitor network resources, use the **Configuration Report** to give information about the Network Time Protocol (NTP)
- The **Security Audit** then highlights the issues with that configuration, such as:
  - Identifying if time synchronization is enabled
  - Identifying if the time synchronization is secure

Note: As necessary, use the 'Find' function at the bottom of the screen

to find where 'NTP' features within the report. By using the Find function, NTP will be highlighted for easy identification.



System messages will not be sent to a Syslog logging server.

2.54.5 Recommendation

Titania Nipper recommends that Syslog logging should be configured to enable system messages to be logged to a central logging server.

Notes for Cisco Router devices:

The logging of system messages to a remote Syslog host can be configured using the following command:

```
logging host ip-address
```

Go to the report contents or the start of this section.

2.55 NTP Control Queries Were Permitted

2.55.1 Affected Device

- CiscoIOS15 - Cisco Router.

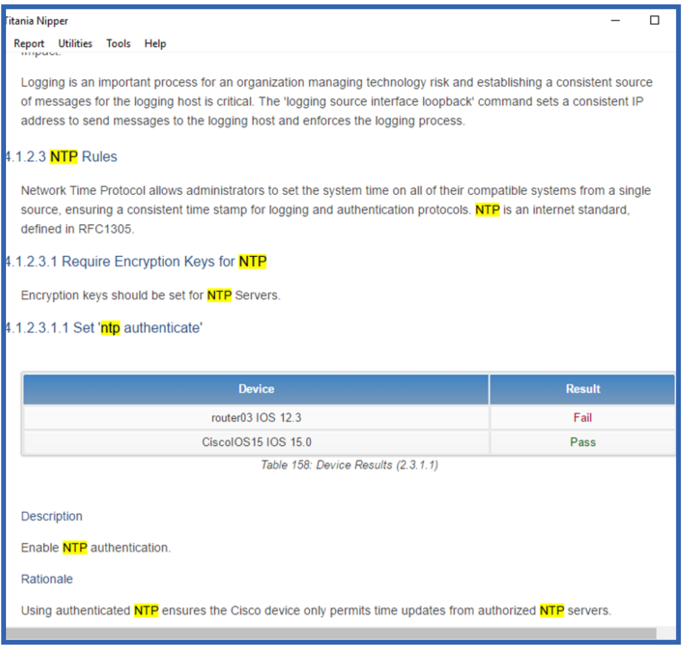
Overall: MEDIUM
Impact: Medium
Ease: N/A
Fix: Planned
Type: Best Practice

2.55.2 Finding

Time synchronization for network devices is inherently important, not just for the various services that make use of time, but also for the accurate logging of events. Therefore network devices can be configured to synchronize their time against a network time source in order to ensure that the time is synchronized.

NTP (described in RFC 5905) is a complex time synchronization protocol with a number of different features and options. In addition to time, a number of control queries can be made to an NTP server, these include requesting a list of the servers NTP peers and a number of different variables.

Find: ntp



Logging is an important process for an organization managing technology risk and establishing a consistent source of messages for the logging host is critical. The 'logging source interface loopback' command sets a consistent IP address to send messages to the logging host and enforces the logging process.

4.1.2.3 NTP Rules

Network Time Protocol allows administrators to set the system time on all of their compatible systems from a single source, ensuring a consistent time stamp for logging and authentication protocols. NTP is an internet standard, defined in RFC1305.

4.1.2.3.1 Require Encryption Keys for NTP

Encryption keys should be set for NTP Servers.

4.1.2.3.1.1 Set 'ntp authenticate'

Device	Result
router03 IOS 12.3	Fail
CiscoIOS15 IOS 15.0	Pass

Table 158: Device Results (2.3.1.1)

Description

Enable NTP authentication.

Rationale

Using authenticated NTP ensures the Cisco device only permits time updates from authorized NTP servers.

Requirement 11: Regularly test security systems and processes.

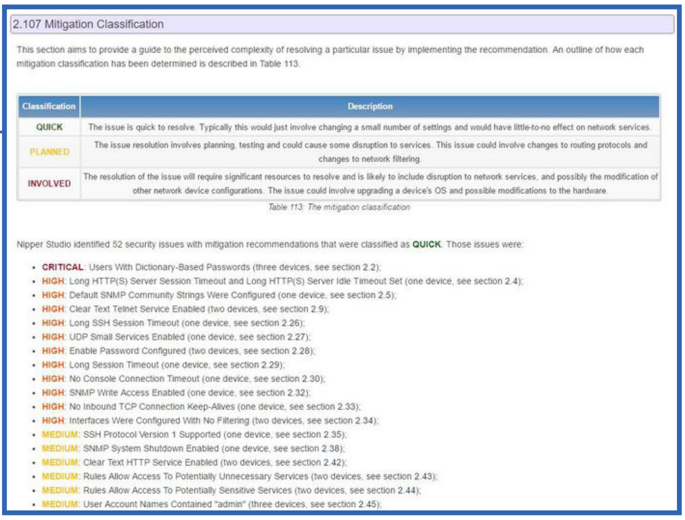
Nipper assists with: 11.2.1 & 11.2.3 of this requirement.

Use the **Security Audit** section to evidence your testing of network devices. From the **Security Audit** report you can highlight the identified security issues and provide the following information:

- » Issue severity (ranked and colour coded)
- » Description of the finding
- » Description of the impact if the finding isn't addressed
- » Description of the ease of exploiting the finding
- » *Recommended remediation steps

By saving a copy of the report each time it is run you can demonstrate the regularity for this requirement.

** If CISCO devices are being audited, the report will give command lines to fix the vulnerability, which can be copied and pasted.*



2.107 Mitigation Classification

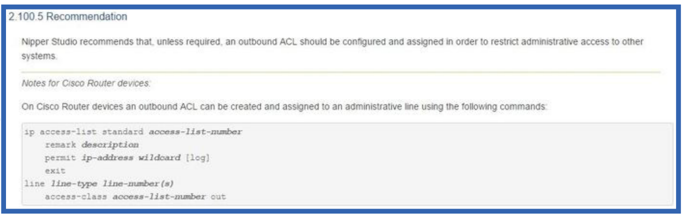
This section aims to provide a guide to the perceived complexity of resolving a particular issue by implementing the recommendation. An outline of how each mitigation classification has been determined is described in Table 113.

Classification	Description
QUICK	The issue is quick to resolve. Typically this would just involve changing a small number of settings and would have little-to-no effect on network services.
PLANNED	The issue resolution involves planning, testing and could cause some disruption to services. This issue could involve changes to routing protocols and changes to network filtering.
INVOLVED	The resolution of the issue will require significant resources to resolve and is likely to include disruption to network services, and possibly the modification of other network device configurations. The issue could involve upgrading a device's OS and possible modifications to the hardware.

Table 113: The mitigation classification

Nipper Studio identified 52 security issues with mitigation recommendations that were classified as **QUICK**. Those issues were:

- **CRITICAL**: Users With Dictionary-Based Passwords (three devices, see section 2.2);
- **HIGH**: Long HTTP(S) Server Session Timeout and Long HTTP(S) Server Idle Timeout Set (one device, see section 2.4);
- **HIGH**: Default SNMP Community Strings Were Configured (one device, see section 2.5);
- **HIGH**: Clear Text Telnet Service Enabled (two devices, see section 2.9);
- **HIGH**: Long SSH Session Timeout (one device, see section 2.26);
- **HIGH**: UDP Small Services Enabled (one device, see section 2.27);
- **HIGH**: Enable Password Configured (two devices, see section 2.28);
- **HIGH**: Long Session Timeout (one device, see section 2.29);
- **HIGH**: No Console Connection Timeout (one device, see section 2.30);
- **HIGH**: SNMP Write Access Enabled (one device, see section 2.32);
- **HIGH**: No Inbound TCP Connection Keep-Alives (one device, see section 2.33);
- **HIGH**: Interfaces Were Configured With No Filtering (two devices, see section 2.34);
- **MEDIUM**: SSH Protocol Version 1 Supported (one device, see section 2.35);
- **MEDIUM**: SNMP System Shutdown Enabled (one device, see section 2.38);
- **MEDIUM**: Clear Text HTTP Service Enabled (two devices, see section 2.42);
- **MEDIUM**: Rules Allow Access To Potentially Unnecessary Services (two devices, see section 2.43);
- **MEDIUM**: Rules Allow Access To Potentially Sensitive Services (two devices, see section 2.44);
- **MEDIUM**: User Account Names Contained "admin" (three devices, see section 2.45);



2.100.5 Recommendation

Nipper Studio recommends that, unless required, an outbound ACL should be configured and assigned in order to restrict administrative access to other systems.

Notes for Cisco Router devices:

On Cisco Router devices an outbound ACL can be created and assigned to an administrative line using the following commands:

```
ip access-list standard access-list-number
    remark description
    permit ip-address wildcard [log]
    exit
line line-type line-number(s)
    access-class access-list-number out
```

Conclusion and further help

You should now find that you have quickly and easily audited several sub sections of the PCI DSS requirements.

With IP Scoping in place you will find your audit condensed to only include relevant information, providing an easier to navigate and interpret report.

For any further help or advice, contact the Support team on:
Tel: (+44)1905 888 785
Email: support@titania.com

Our team are more than happy to help walk you through this or any other auditing processes with our Nipper software.

See how Nipper can benefit you with PCI auditing:

titania.com/register/trial/nipper

> **“From running the first check to delivering a full PCI report to our clients takes just 15 minutes. This saves us hours with every use so we can deliver more value at every engagement.”**
>
> **QSA at Leading IT Consultany**