IE4040

Information Assurance and Auditing

Assignment – 2020

Firewall audit using Nipper Studio

B.Sc. (Hons) Degree in Information Technology – Specialization in Computer Systems and Network Engineering

Department of Computer Systems Engineering

Sri Lanka Institute of Information Technology

Name: W.A.K.L. Sanjula

Index: IT17114868

Group: CSN (WE)

TABLE OF CONTENTS

TABLE OF FIGURES ii

1. Introduction 1

 1.1 Importance of firewall audit 1

2. Download and Installation 2

3. Beginning of the auditing process 2

4. Report Overview 5

5. Contents of the audit report 6

6. Conclusion 12

7. References 12

TABLE OF FIGURES

Figure 1:Download versions.. 2
Figure 2:Home Page 2
Figure 3:Access the Firewall 3
Figure 4:Establish the connection 3
Figure 5:Customize report information 4
Figure 6: Second Step 4
Figure 7: Step 3 5
Figure 8: Beginning of the audit report 5
Figure 9: Security audit summary 6
Figure 10:Report Contents 6
Figure 11:Report introduction 7
Figure 12:Security issue overview 7
Figure 13: Issues classification 8
Figure 14:Recommendation for issues 8
Figure 15: Vulnerability findings 9
Figure 16:Vulnerability categorization 9
Figure 17:Recommendations for vulnerabilities 10
Figure 18:Vulnerability severity code definitions 10
Figure 19:Appendix of report 11
Figure 20:Export the audit report 11

1. Introduction

Configurations, access rules and security policies need to be audited regularly to identify weaknesses; however, many organizations don't have the time or resources to do this manually. Titania offers a simple and innovative solution, as its Nipper Studio does all the hard work so you don't have to. Capable of auditing critical infrastructure devices from an impressive range of vendors, it doesn't need to scan the network and so has zero impact on general operations. Nipper Studio analyses device configuration files, allowing it to offer far more detailed reporting than vulnerability scanners. Even better, it includes compliance reporting modules for key data protection regulations, including PCI-DSS, STIG, NIST, SANS plus CIS, and brings them all together to provide essential vulnerability audits and best practice guides.

There are now two methods of interrogating devices. We can upload their configuration files or access them directly from Nipper Studio over Telnet, SSH, HTTP or HTTPS. Either way, the first thing to do is choose a device from the extensive list, which includes Palo Alto, Check Point, Cisco, Dell EMC, Fortinet, HPE, SonicWALL, WatchGuard and more. This software helps us accurately identify risks in our network infrastructure and provides precise remediation, including command line fixes.

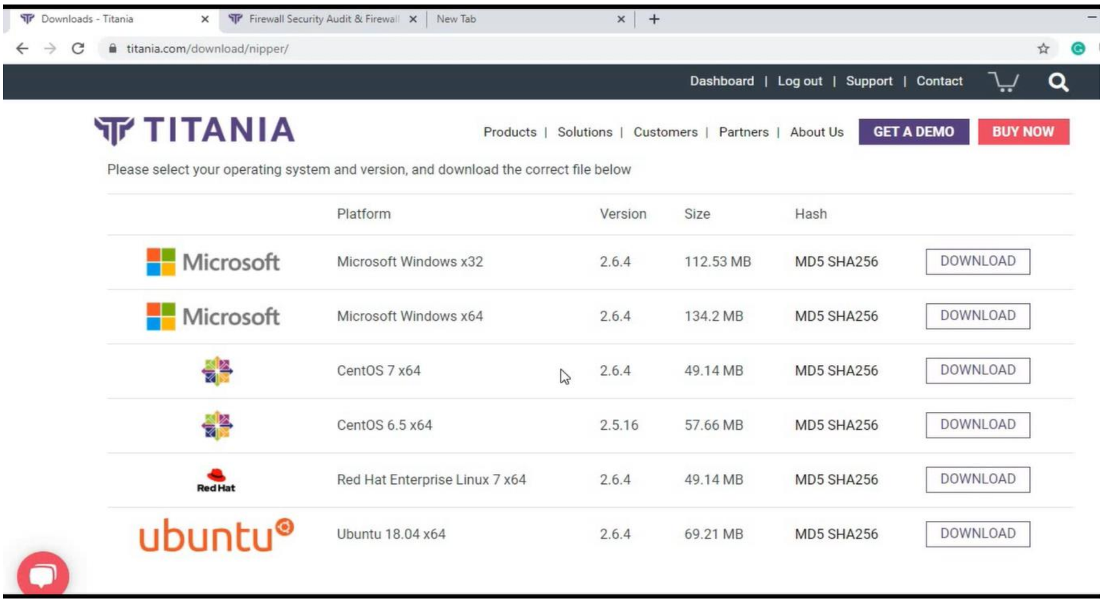
- Nipper discovers vulnerabilities in firewalls, switches and routers, automatically prioritizing risks to our organization
- Automate checks against specified standards, benchmarks or risk management frameworks to save valuable time when auditing compliance
- Identify vulnerabilities and non-compliance with the standards
- Prioritize any risks found against the framework
- Get detailed remediation advice for each non-compliance, so that we can action it and secure our systems and data.

1.1 Importance of firewall audit

Once a firewall is in place, it is critical to security of any business to conduct regular firewall audits on an annual basis at the minimum. Annual audits increase the odd that we will able to catch any weaknesses in the security of our network. In addition to the software associated with firewalls, security controls and policy controls also be reviewed and adapted as necessary to address changes in technology or in our business.

2. Download and Installation

First, Go to the Titania official website using this URL https://www.titania.com/download/nipper/ .Then you can download it for any operating system as shown below.


Downloads - Titania
Firewall Security Audit & Firewall
New Tab
titania.com/download/nipper/
Dashboard | Log out | Support | Contact
TITANIA
Products | Solutions | Customers | Partners | About Us
GET A DEMO
BUY NOW

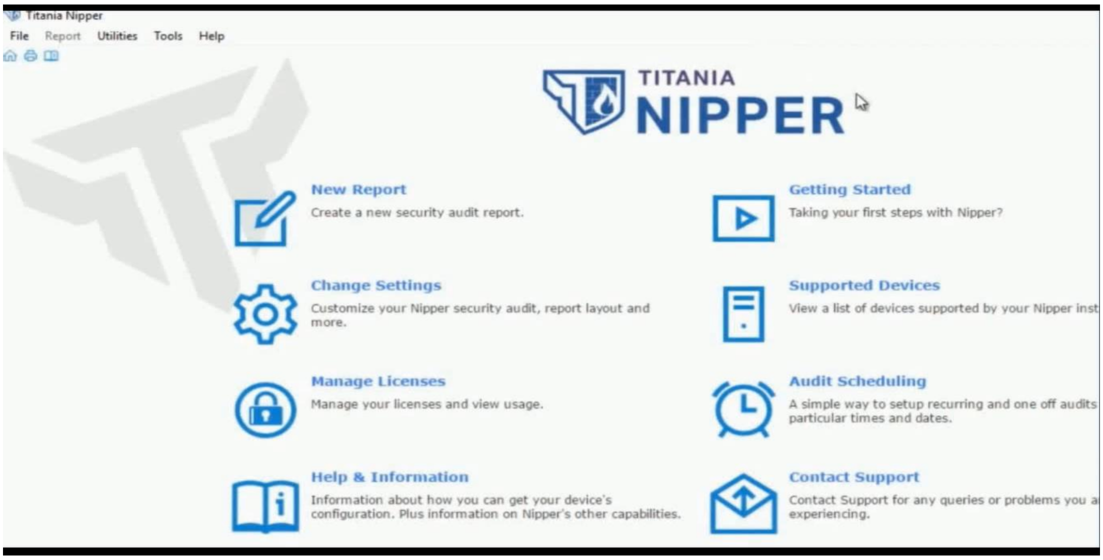
Please select your operating system and version, and download the correct file below

	Platform	Version	Size	Hash	
Microsoft	Microsoft Windows x32	2.6.4	112.53 MB	MD5 SHA256	DOWNLOAD
Microsoft	Microsoft Windows x64	2.6.4	134.2 MB	MD5 SHA256	DOWNLOAD
	CentOS 7 x64	2.6.4	49.14 MB	MD5 SHA256	DOWNLOAD
	CentOS 6.5 x64	2.5.16	57.66 MB	MD5 SHA256	DOWNLOAD
Red Hat	Red Hat Enterprise Linux 7 x64	2.6.4	49.14 MB	MD5 SHA256	DOWNLOAD
ubuntu	Ubuntu 18.04 x64	2.6.4	69.21 MB	MD5 SHA256	DOWNLOAD

Figure 1:Download versions

3. Beginning of the auditing process

When installation is done, Open the Nipper Studio software. Then we can see the home page and to start the audit click on ‘New Report’.



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 inst

Manage Licenses
Manage your licenses and view usage.

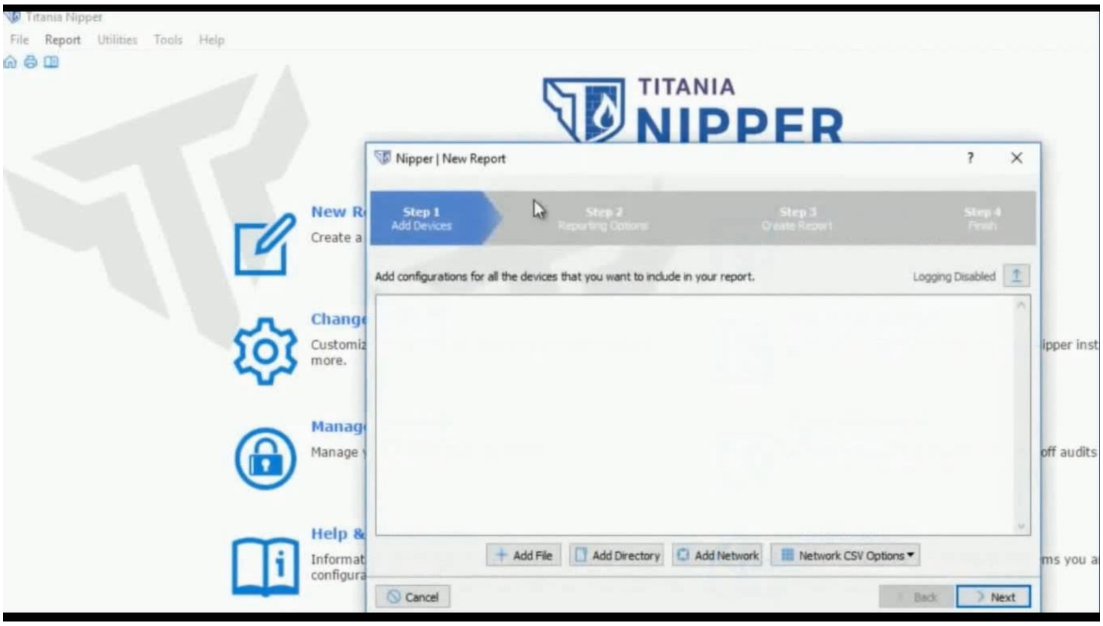
Audit Scheduling
A simple way to setup recurring and one off audits particular times and dates.

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 a experiencing.

Figure 2:Home Page

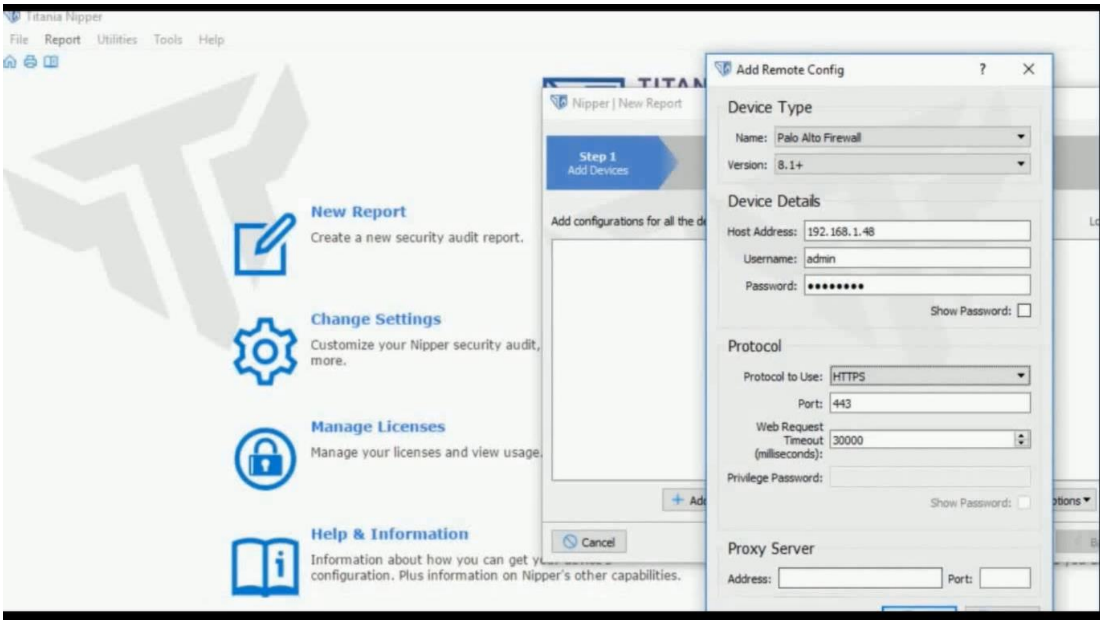
Here we can access our devices in two methods. First one is ‘Add Directory’. But I am going to access my virtual enterprise firewall in Eve-ng using ‘Add network’ method as shown below.



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

Figure 3:Access the Firewall

After Add network, we should fill this information according to the device and click on ‘Add’ button.


Titania Nipper
File Report Utilities Tools Help
Nipper | New Report
Step 1 Add Devices
New Report
Create a new security audit report.
Change Settings
Customize your Nipper security audit, more.
Manage Licenses
Manage your licenses and view usage.
Help & Information
Information about how you can get y... configuration. Plus information on Nipper's other capabilities.
Cancel
Add Remote Config

Add configurations for all the d

Device Type
Name: Palo Alto Firewall
Version: 8.1+

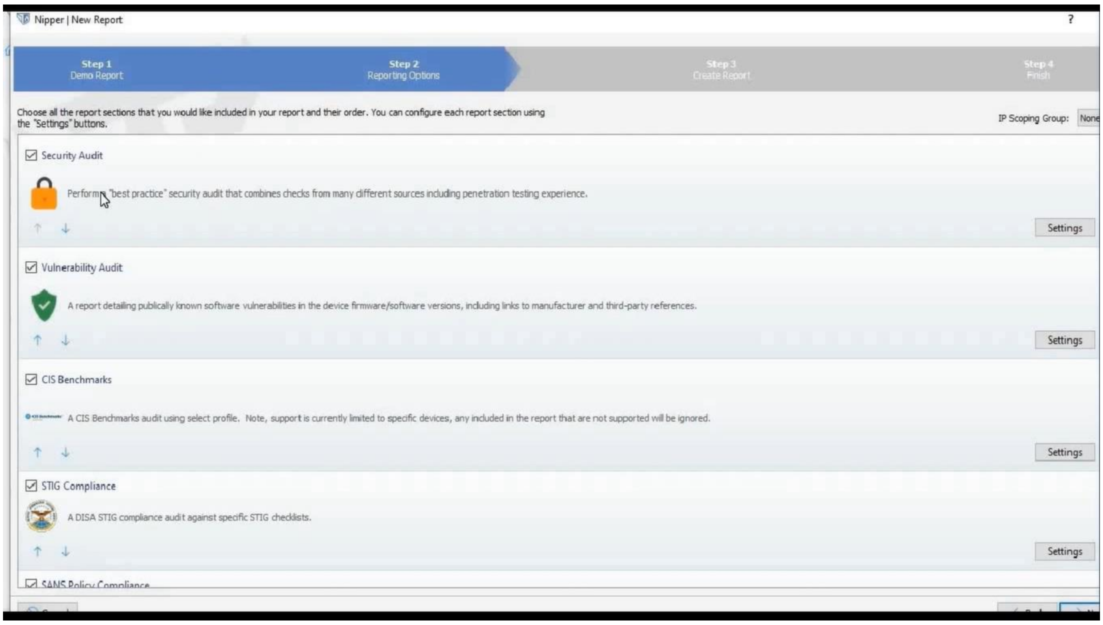
Device Details
Host Address: 192.168.1.48
Username: admin
Password: ••••••••
Show Password: □

Protocol
Protocol to Use: HTTPS
Port: 443
Web Request Timeout (milliseconds): 30000
Privilege Password:
Show Password: □

Proxy Server
Address:
Port:

Figure 4:Establish the connection

Under the first step, we can see what are the information will include our audit report and we can customize those according to our requirement and go to 2nd step click on ‘Next’ button as shown below.



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.

☑ Security Audit

Performs "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.

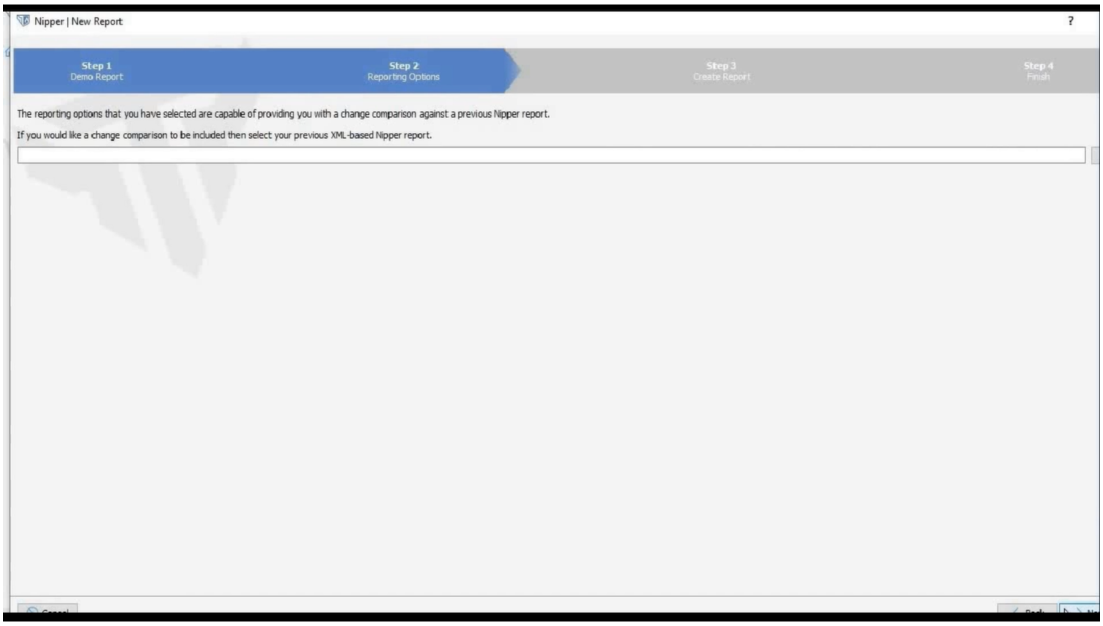
☑ STIG Compliance

A DISA STIG compliance audit against specific STIG checklists.

☑ SANS Policy Compliance

Figure 5:Customize report information

In here Just click on the ‘Next’ button for next step.

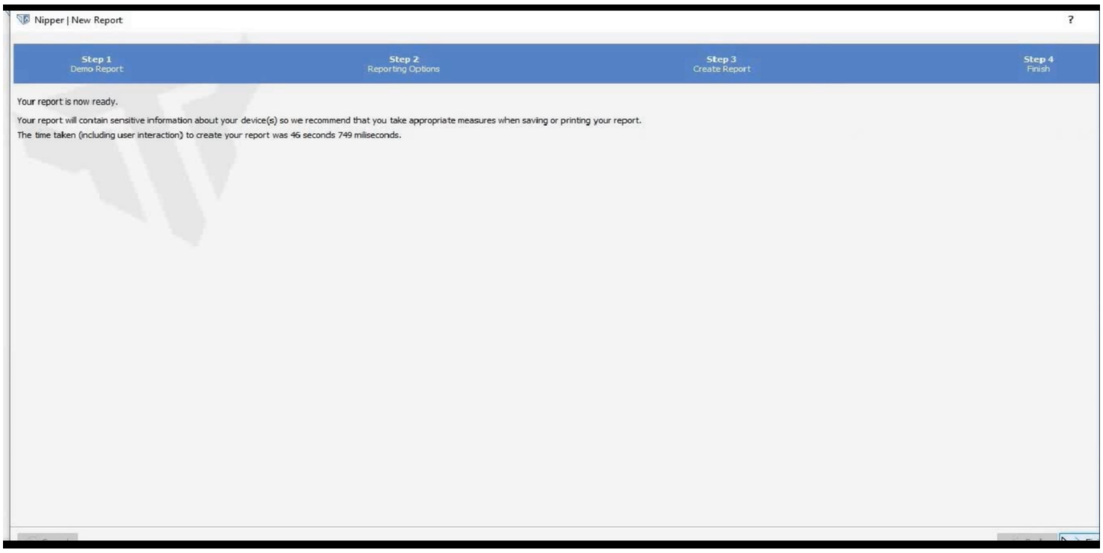


The reporting options that you have selected are capable of providing you with a change comparison against a previous Nipper report.

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

Figure 6: Second Step

Under the 3rd step we can see that our report is ready status and the time it was processed and click on ‘Next’ to get the processed report as shown below.



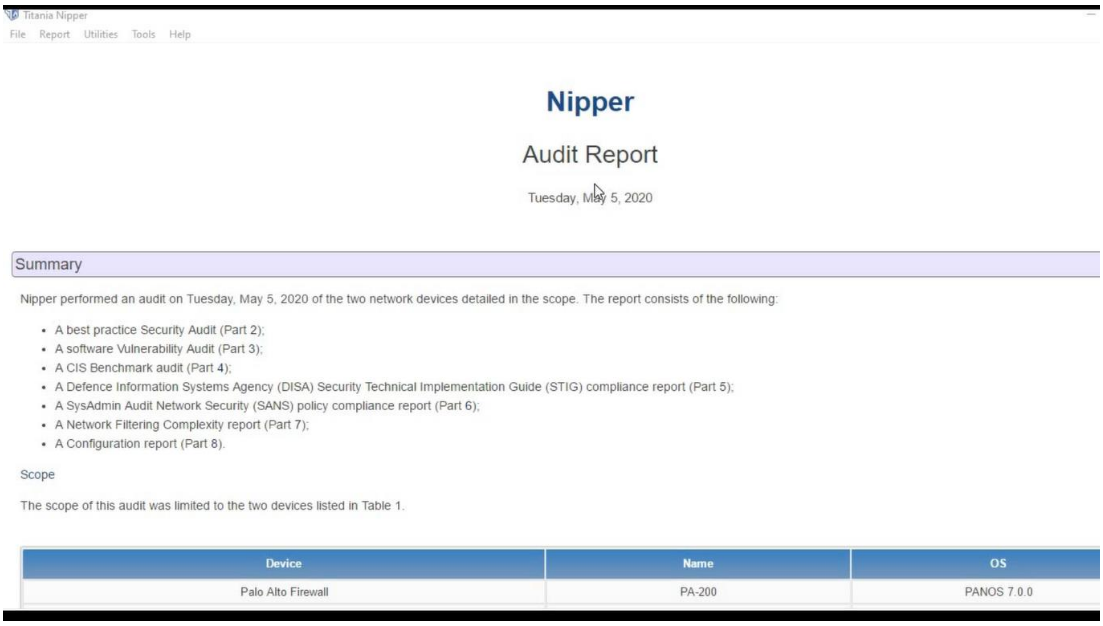
Your report is now ready.

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 46 seconds 749 miliseconds.

Figure 7: Step 3

4. Report Overview

This is the finalized audit report that the nipper studio is processed. It includes information based on seven sections such as a best practice Security Audit, a software Vulnerability Audit, a CIS Benchmark audit, etc. as shown below.



Nipper

Audit Report

Tuesday, May 5, 2020

Summary

Nipper performed an audit on Tuesday, May 5, 2020 of the two 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 Defence Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) compliance report (Part 5);
- A SysAdmin Audit Network Security (SANS) policy compliance report (Part 6);
- A Network Filtering Complexity report (Part 7);
- A Configuration report (Part 8).

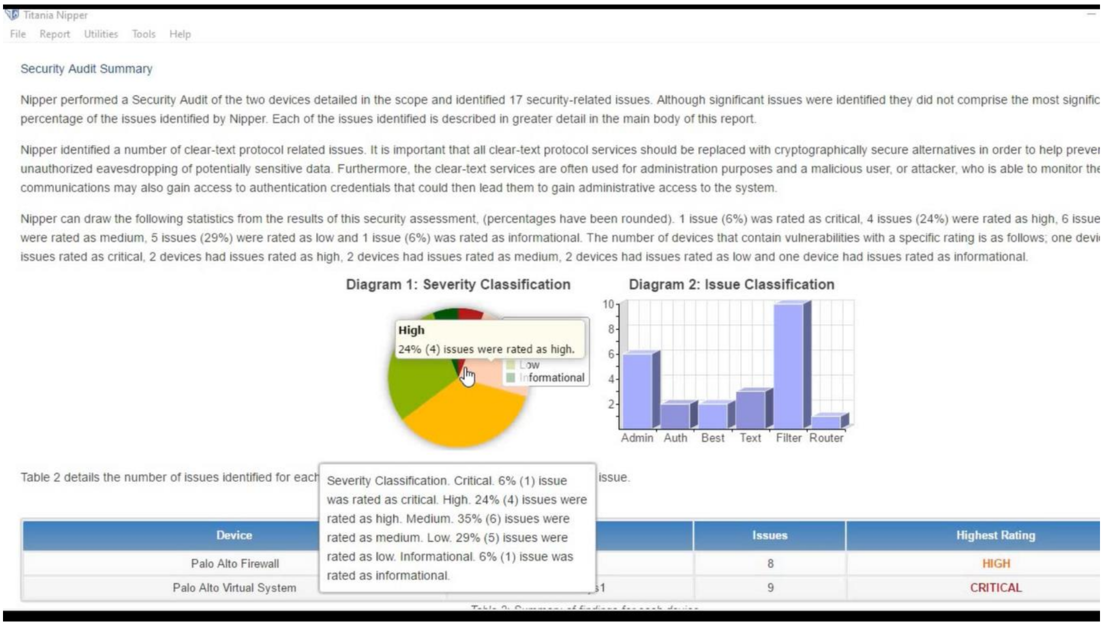
Scope

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

Device	Name	OS
Palo Alto Firewall	PA-200	PANOS 7.0.0

Figure 8: Beginning of the audit report

Under the security audit summary, we can see nipper has identified number of 17 issues in the firewall and nipper has presented that information in pie chart very clearly as shown below.



Security Audit Summary

Nipper performed a Security Audit of the two devices detailed in the scope and identified 17 security-related issues. Although significant issues were identified they did not comprise the most signific percentage of the issues identified by Nipper. Each of the issues identified is described in greater detail in the main body of this report.

Nipper identified a number of clear-text protocol related issues. It is important that all clear-text protocol services should be replaced with cryptographically secure alternatives in order to help preve unauthorized eavesdropping of potentially sensitive data. Furthermore, the clear-text services are often used for administration purposes and a malicious user, or attacker, who is able to monitor the communications may also gain access to authentication credentials that could then lead them to gain administrative access to the system.

Nipper can draw the following statistics from the results of this security assessment, (percentages have been rounded). 1 issue (6%) was rated as critical, 4 issues (24%) were rated as high, 6 issue were rated as medium, 5 issues (29%) were rated as low and 1 issue (6%) was rated as informational. The number of devices that contain vulnerabilities with a specific rating is as follows; one devi issues rated as critical, 2 devices had issues rated as high, 2 devices had issues rated as medium, 2 devices had issues rated as low and one device had issues rated as informational.

Diagram 1: Severity Classification
High
24% (4) issues were rated as high.
Low
Informational
Diagram 2: Issue Classification
10
8
6
4
2
Admin
Auth
Best
Text
Filter
Router

Table 2 details the number of issues identified for each issue.

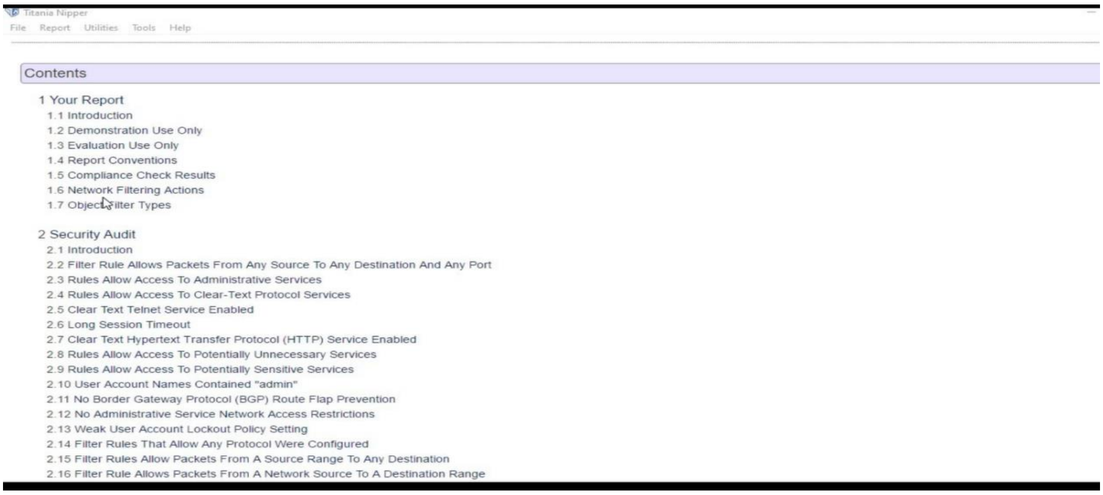
Severity Classification. Critical. 6% (1) issue was rated as critical. High. 24% (4) issues were rated as high. Medium. 35% (6) issues were rated as medium. Low. 29% (5) issues were rated as low. Informational. 6% (1) issue was rated as informational.

Device		Issues	Highest Rating
Palo Alto Firewall		8	HIGH
Palo Alto Virtual System	1	9	CRITICAL

Figure 9: Security audit summary

5. Contents of the audit report

Here we can see our report contents under different topics as Your report, Security audit, Vulnerability report, CIS Benchmark, DISA STIG Compliance, SANS Policy Compliance, Filtering Complexity Report, Configuration Report and Appendix as shown figure 10



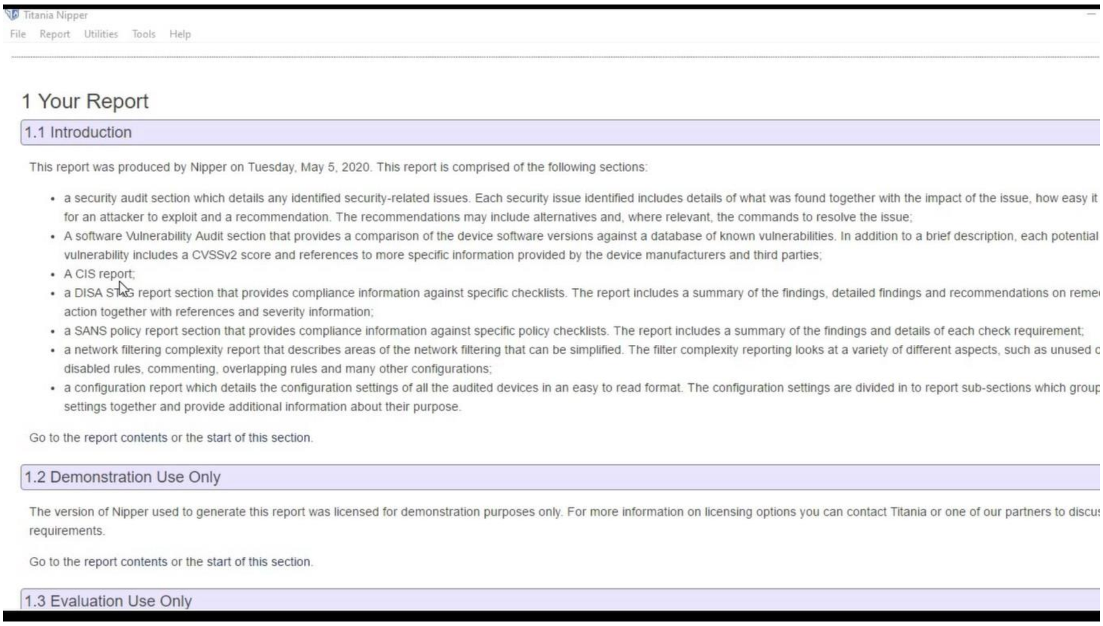
Contents

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

2 Security Audit
2.1 Introduction
2.2 Filter Rule Allows Packets From Any Source To Any Destination And Any Port
2.3 Rules Allow Access To Administrative Services
2.4 Rules Allow Access To Clear-Text Protocol Services
2.5 Clear Text Telnet Service Enabled
2.6 Long Session Timeout
2.7 Clear Text Hypertext Transfer Protocol (HTTP) Service Enabled
2.8 Rules Allow Access To Potentially Unnecessary Services
2.9 Rules Allow Access To Potentially Sensitive Services
2.10 User Account Names Contained "admin"
2.11 No Border Gateway Protocol (BGP) Route Flap Prevention
2.12 No Administrative Service Network Access Restrictions
2.13 Weak User Account Lockout Policy Setting
2.14 Filter Rules That Allow Any Protocol Were Configured
2.15 Filter Rules Allow Packets From A Source Range To Any Destination
2.16 Filter Rule Allows Packets From A Network Source To A Destination Range

Figure 10:Report Contents

Under introduction we can see that this report includes a security audit section, a software vulnerability audit section, a CIS report, a DISA STIG report section, a network filtering complexity report and a configuration report.



1 Your Report

1.1 Introduction

This report was produced by Nipper on Tuesday, May 5, 2020. This report is comprised of the following sections:

- a security audit section which details any identified security-related issues. Each security issue identified includes details of what was found together with the impact of the issue, how easy it for an attacker to exploit and a recommendation. The recommendations may include alternatives and, where relevant, the commands to resolve the issue;
- A software Vulnerability Audit section that provides a comparison of the device software versions against a database of known vulnerabilities. In addition to a brief description, each potential vulnerability includes a CVSSv2 score and references to more specific information provided by the device manufacturers and third parties;
- A CIS report;
- a DISA STIG report section that provides compliance information against specific checklists. The report includes a summary of the findings, detailed findings and recommendations on reme action together with references and severity information;
- a SANS policy report section that provides compliance information against specific policy checklists. The report includes a summary of the findings and details of each check requirement;
- a network filtering complexity report that describes areas of the network filtering that can be simplified. The filter complexity reporting looks at a variety of different aspects, such as unused c disabled rules, commenting, overlapping rules and many other configurations;
- a configuration report which details the configuration settings of all the audited devices in an easy to read format. The configuration settings are divided in to report sub-sections which group settings together and provide additional information about their purpose.

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

1.2 Demonstration Use Only

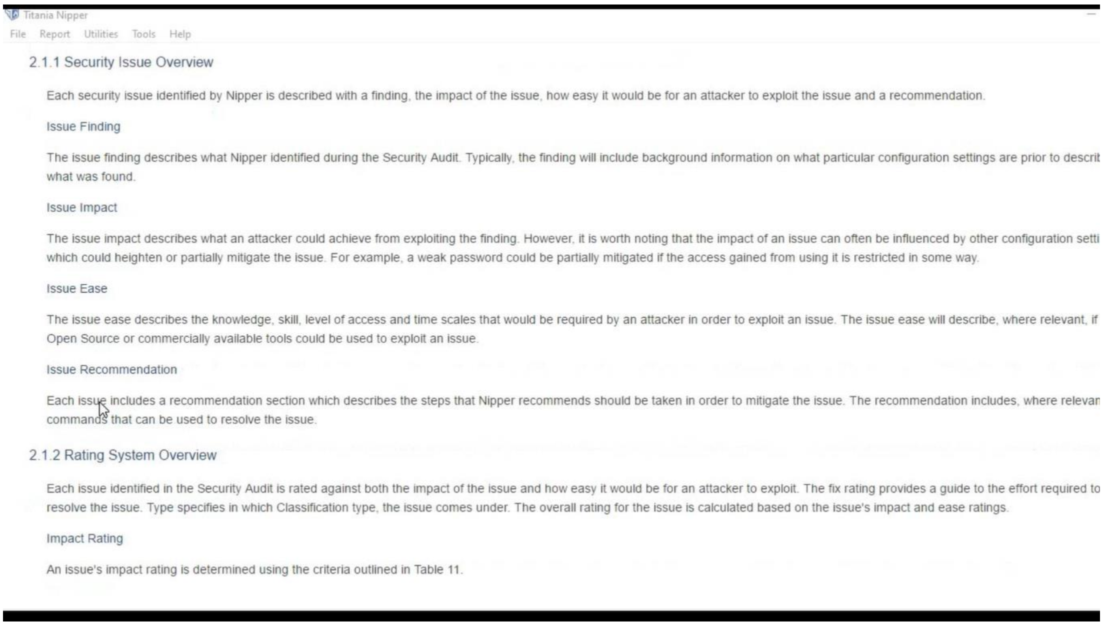
The version of Nipper used to generate this report was licensed for demonstration purposes only. For more information on licensing options you can contact Titania or one of our partners to discus requirements.

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

1.3 Evaluation Use Only

Figure 11:Report introduction

The security issue overview provides all the information about an issue with Issue Finding, Issue Impact, Issue Ease and Issue Recommendation as shown below.



2.1.1 Security Issue Overview

Each security issue identified by Nipper is described with a finding, the impact of the issue, how easy it would be for an attacker to exploit the issue and a recommendation.

Issue Finding

The issue finding describes what Nipper identified during the Security Audit. Typically, the finding will include background information on what particular configuration settings are prior to describ what was found.

Issue Impact

The issue impact describes what an attacker could achieve from exploiting the finding. However, it is worth noting that the impact of an issue can often be influenced by other configuration setti which could heighten or partially mitigate the issue. For example, a weak password could be partially mitigated if the access gained from using it is restricted in some way.

Issue Ease

The issue ease describes the knowledge, skill, level of access and time scales that would be required by an attacker in order to exploit an issue. The issue ease will describe, where relevant, if Open Source or commercially available tools could be used to exploit an issue.

Issue Recommendation

Each issue includes a recommendation section which describes the steps that Nipper recommends should be taken in order to mitigate the issue. The recommendation includes, where relevan commands that can be used to resolve the issue.

2.1.2 Rating System Overview

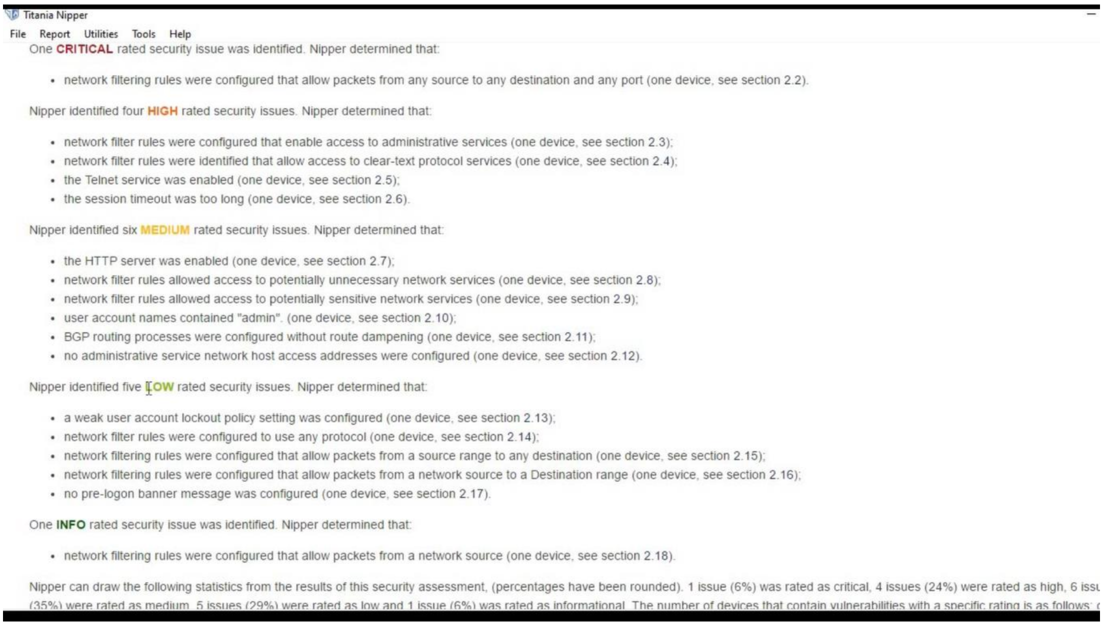
Each issue identified in the Security Audit is rated against both the impact of the issue and how easy it would be for an attacker to exploit. The fix rating provides a guide to the effort required to resolve the issue. Type specifies in which Classification type, the issue comes under. The overall rating for the issue is calculated based on the issue's impact and ease ratings.

Impact Rating

An issue's impact rating is determined using the criteria outlined in Table 11.

Figure 12:Security issue overview

Nipper has identified one critical rated issue, 4 high rated issues, 6 medium rated issued, five low rated issues and one info rated issue as shown below.



One **CRITICAL** rated security issue was identified. Nipper determined that:

- network filtering rules were configured that allow packets from any source to any destination and any port (one device, see section 2.2).

Nipper identified four **HIGH** rated security issues. Nipper determined that:

- network filter rules were configured that enable access to administrative services (one device, see section 2.3);
- network filter rules were identified that allow access to clear-text protocol services (one device, see section 2.4);
- the Telnet service was enabled (one device, see section 2.5);
- the session timeout was too long (one device, see section 2.6).

Nipper identified six **MEDIUM** rated security issues. Nipper determined that:

- the HTTP server was enabled (one device, see section 2.7);
- network filter rules allowed access to potentially unnecessary network services (one device, see section 2.8);
- network filter rules allowed access to potentially sensitive network services (one device, see section 2.9);
- user account names contained "admin". (one device, see section 2.10);
- BGP routing processes were configured without route dampening (one device, see section 2.11);
- no administrative service network host access addresses were configured (one device, see section 2.12).

Nipper identified five **LOW** rated security issues. Nipper determined that:

- a weak user account lockout policy setting was configured (one device, see section 2.13);
- network filter rules were configured to use any protocol (one device, see section 2.14);
- network filtering rules were configured that allow packets from a source range to any destination (one device, see section 2.15);
- network filtering rules were configured that allow packets from a network source to a Destination range (one device, see section 2.16);
- no pre-logon banner message was configured (one device, see section 2.17).

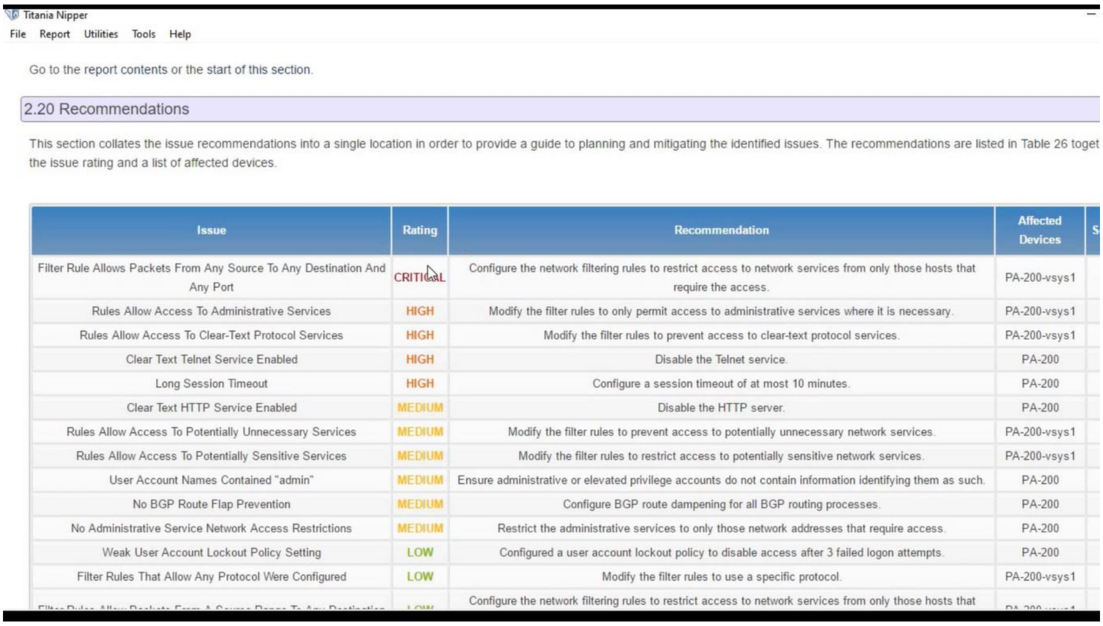
One **INFO** rated security issue was identified. Nipper determined that:

- network filtering rules were configured that allow packets from a network source (one device, see section 2.18).

Nipper can draw the following statistics from the results of this security assessment, (percentages have been rounded). 1 issue (6%) was rated as critical, 4 issues (24%) were rated as high, 6 issu
(35%) were rated as medium, 5 issues (29%) were rated as low and 1 issue (6%) was rated as informational. The number of devices that contain vulnerabilities with a specific rating is as follows: c

Figure 13: Issues classification

These are the recommendations that nipper has identified for above mentioned issues and suggest the recommendation for each issue according to their situation as Critical, High, Medium or Low as shown in figure 14.



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

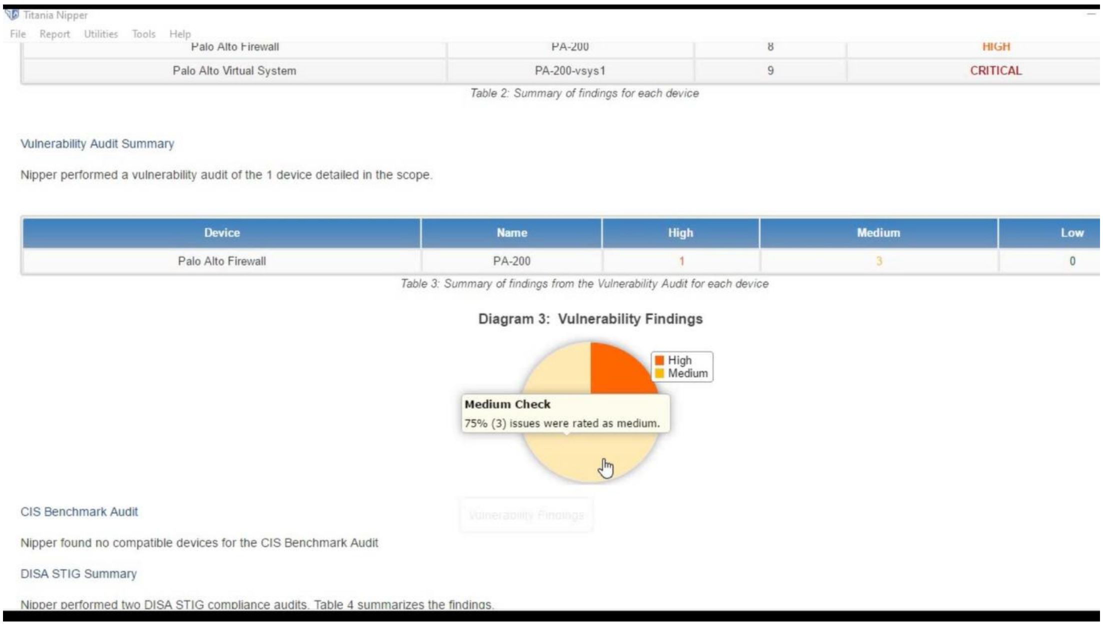
2.20 Recommendations

This section collates the issue recommendations into a single location in order to provide a guide to planning and mitigating the identified issues. The recommendations are listed in Table 26 toget
the issue rating and a list of affected devices.

Issue	Rating	Recommendation	Affected Devices	S
Filter Rule Allows Packets From Any Source To Any Destination And Any Port	CRITICAL	Configure the network filtering rules to restrict access to network services from only those hosts that require the access.	PA-200-vsys1	
Rules Allow Access To Administrative Services	HIGH	Modify the filter rules to only permit access to administrative services where it is necessary.	PA-200-vsys1	
Rules Allow Access To Clear-Text Protocol Services	HIGH	Modify the filter rules to prevent access to clear-text protocol services.	PA-200-vsys1	
Clear Text Telnet Service Enabled	HIGH	Disable the Telnet service.	PA-200	
Long Session Timeout	HIGH	Configure a session timeout of at most 10 minutes.	PA-200	
Clear Text HTTP Service Enabled	MEDIUM	Disable the HTTP server.	PA-200	
Rules Allow Access To Potentially Unnecessary Services	MEDIUM	Modify the filter rules to prevent access to potentially unnecessary network services.	PA-200-vsys1	
Rules Allow Access To Potentially Sensitive Services	MEDIUM	Modify the filter rules to restrict access to potentially sensitive network services.	PA-200-vsys1	
User Account Names Contained "admin"	MEDIUM	Ensure administrative or elevated privilege accounts do not contain information identifying them as such.	PA-200	
No BGP Route Flap Prevention	MEDIUM	Configure BGP route dampening for all BGP routing processes.	PA-200	
No Administrative Service Network Access Restrictions	MEDIUM	Restrict the administrative services to only those network addresses that require access.	PA-200	
Weak User Account Lockout Policy Setting	LOW	Configured a user account lockout policy to disable access after 3 failed logon attempts.	PA-200	
Filter Rules That Allow Any Protocol Were Configured	LOW	Modify the filter rules to use a specific protocol.	PA-200-vsys1	
Filter Rules Allow Packets From A Source Range To Any Destination	LOW	Configure the network filtering rules to restrict access to network services from only those hosts that	PA-200-vsys1	

Figure 14:Recommendation for issues

In here, we can see the vulnerabilities which are identified by Nipper software and there are four vulnerabilities has occurred in the firewall system as shown below.



Palo Alto Firewall	PA-200	8	HIGH
Palo Alto Virtual System	PA-200-vsys1	9	CRITICAL

Table 2: Summary of findings for each device

Vulnerability Audit Summary

Nipper performed a vulnerability audit of the 1 device detailed in the scope.

Device	Name	High	Medium	Low
Palo Alto Firewall	PA-200	1	3	0

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

Diagram 3: Vulnerability Findings

CIS Benchmark Audit

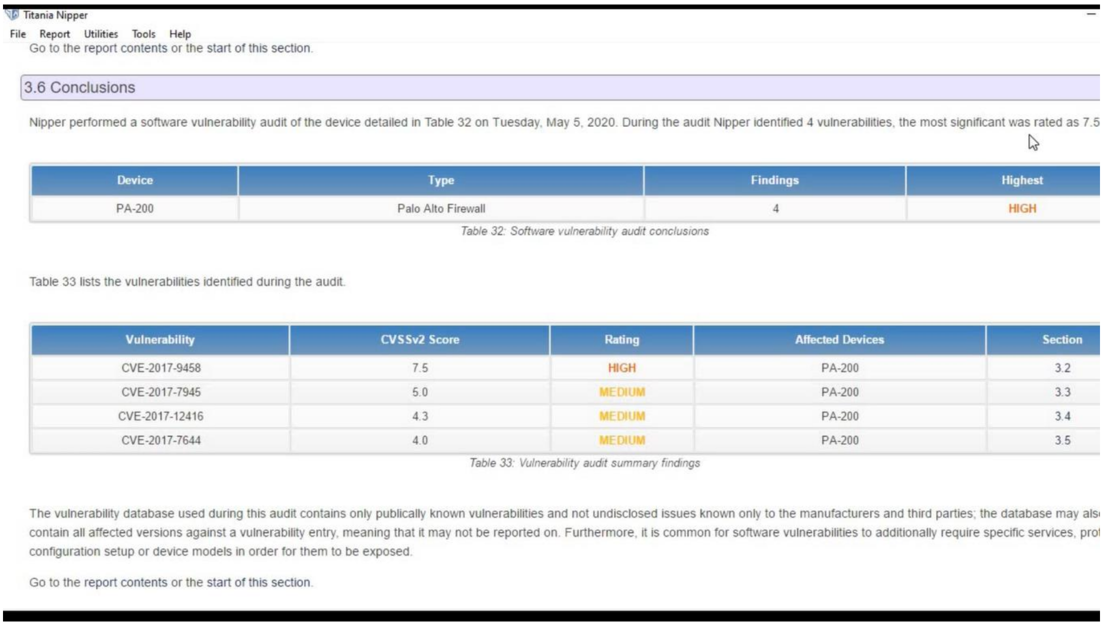
Nipper found no compatible devices for the CIS Benchmark Audit

DISA STIG Summary

Nipper performed two DISA STIG compliance audits. Table 4 summarizes the findings.

Figure 15: Vulnerability findings

Under conclusion section of the vulnerability findings, each occurred vulnerability has categorized to rating level such as High, Medium and Low and the CVSSv2 score for each vulnerability has assigned by the Nipper studio as shown figure 16.



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

3.6 Conclusions

Nipper performed a software vulnerability audit of the device detailed in Table 32 on Tuesday, May 5, 2020. During the audit Nipper identified 4 vulnerabilities, the most significant was rated as 7.5

Device	Type	Findings	Highest
PA-200	Palo Alto Firewall	4	HIGH

Table 32: Software vulnerability audit conclusions

Table 33 lists the vulnerabilities identified during the audit.

Vulnerability	CVSSv2 Score	Rating	Affected Devices	Section
CVE-2017-9458	7.5	HIGH	PA-200	3.2
CVE-2017-7945	5.0	MEDIUM	PA-200	3.3
CVE-2017-12416	4.3	MEDIUM	PA-200	3.4
CVE-2017-7644	4.0	MEDIUM	PA-200	3.5

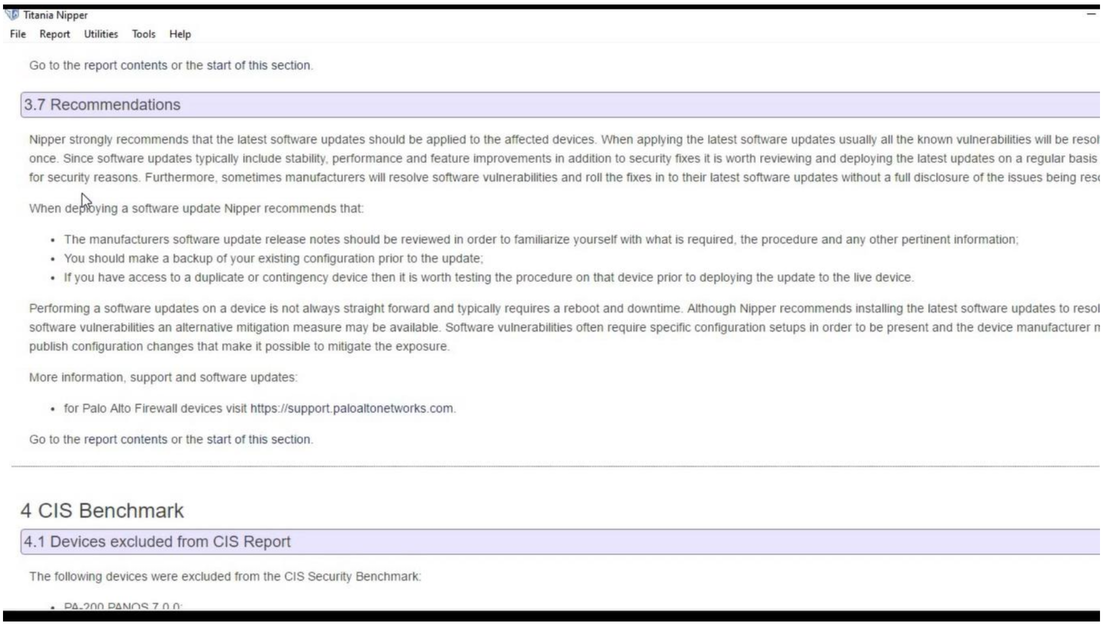
Table 33: Vulnerability audit summary findings

The vulnerability database used during this audit contains only publically known vulnerabilities and not undisclosed issues known only to the manufacturers and third parties; the database may als contain all affected versions against a vulnerability entry, meaning that it may not be reported on. Furthermore, it is common for software vulnerabilities to additionally require specific services, prot configuration setup or device models in order for them to be exposed.

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

Figure 16:Vulnerability categorization

For vulnerability issues, Nipper strongly recommends that the latest software updates should be applied to the affected device and when applying the latest software updates usually all the known vulnerabilities will be resolve.



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

3.7 Recommendations

Nipper strongly recommends that the latest software updates should be applied to the affected devices. When applying the latest software updates usually all the known vulnerabilities will be resol once. Since software updates typically include stability, performance and feature improvements in addition to security fixes it is worth reviewing and deploying the latest updates on a regular basis for security reasons. Furthermore, sometimes manufacturers will resolve software vulnerabilities and roll the fixes in to their latest software updates without a full disclosure of the issues being res

When deploying a software update Nipper recommends that:

- The manufacturers software update release notes should be reviewed in order to familiarize yourself with what is required, the procedure and any other pertinent information;
- You should make a backup of your existing configuration prior to the update;
- If you have access to a duplicate or contingency device then it is worth testing the procedure on that device prior to deploying the update to the live device.

Performing a software updates on a device is not always straight forward and typically requires a reboot and downtime. Although Nipper recommends installing the latest software updates to resol software vulnerabilities an alternative mitigation measure may be available. Software vulnerabilities often require specific configuration setups in order to be present and the device manufacturer n publish configuration changes that make it possible to mitigate the exposure.

More information, support and software updates:

- for Palo Alto Firewall devices visit https://support.paloaltonetworks.com.

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

4 CIS Benchmark

4.1 Devices excluded from CIS Report

The following devices were excluded from the CIS Security Benchmark:

- PA-200 PANOS 7.0.0;

Figure 17:Recommendations for vulnerabilities

We can see here vulnerability severity code definition table and Nipper has mentioned that any vulnerability, the exploitation of which will directly and immediately result in loss of confidentiality, availability or integrity.

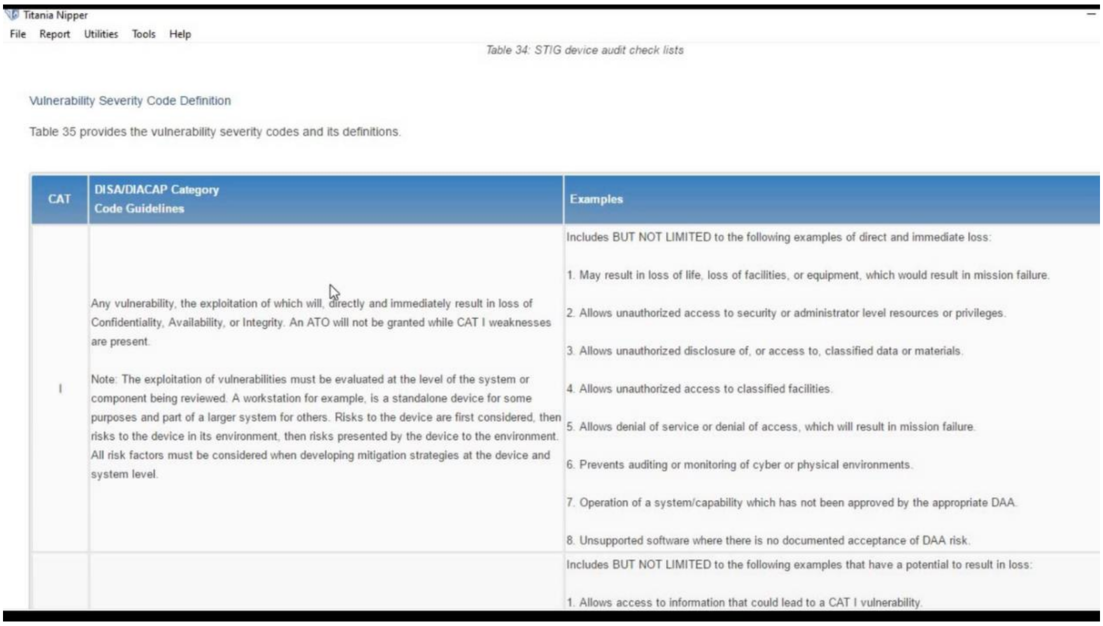


Table 34: STIG device audit check lists

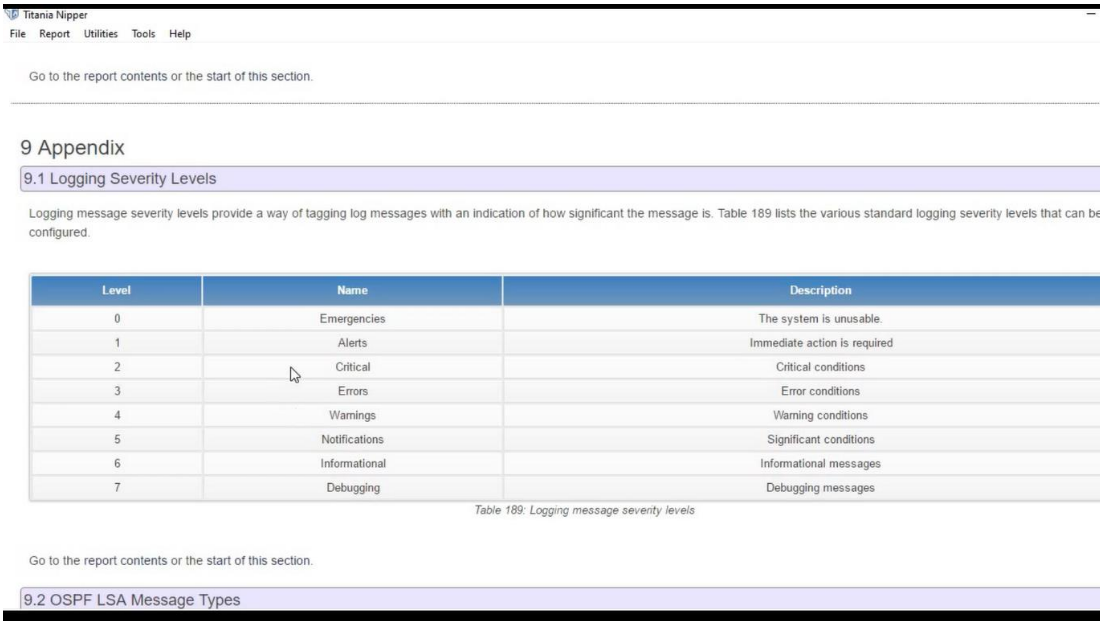
Vulnerability Severity Code Definition

Table 35 provides the vulnerability severity codes and its definitions.

CAT	DISA/DIACAP Category Code Guidelines	Examples
I	Any vulnerability, the exploitation of which will, directly and immediately result in loss of Confidentiality, Availability, or Integrity. An ATO will not be granted while CAT I weaknesses are present. Note: The exploitation of vulnerabilities must be evaluated at the level of the system or component being reviewed. A workstation for example, is a standalone device for some purposes and part of a larger system for others. Risks to the device are first considered, then risks to the device in its environment, then risks presented by the device to the environment. All risk factors must be considered when developing mitigation strategies at the device and system level.	Includes BUT NOT LIMITED to the following examples of direct and immediate loss: 1. May result in loss of life, loss of facilities, or equipment, which would result in mission failure. 2. Allows unauthorized access to security or administrator level resources or privileges. 3. Allows unauthorized disclosure of, or access to, classified data or materials. 4. Allows unauthorized access to classified facilities. 5. Allows denial of service or denial of access, which will result in mission failure. 6. Prevents auditing or monitoring of cyber or physical environments. 7. Operation of a system/capability which has not been approved by the appropriate DAA. 8. Unsupported software where there is no documented acceptance of DAA risk.
		Includes BUT NOT LIMITED to the following examples that have a potential to result in loss: 1. Allows access to information that could lead to a CAT I vulnerability.

Figure 18:Vulnerability severity code definitions

At the end of the audit report we can see appendixes that nipper audit tool has used to generate this firewall audit report. We can see there are eight levels such as 0 to 7 and their name and description as shown here.



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

9 Appendix

9.1 Logging Severity Levels

Logging message severity levels provide a way of tagging log messages with an indication of how significant the message is. Table 189 lists the various standard logging severity levels that can be configured.

Level	Name	Description
0	Emergencies	The system is unusable.
1	Alerts	Immediate action is required
2	Critical	Critical conditions
3	Errors	Error conditions
4	Warnings	Warning conditions
5	Notifications	Significant conditions
6	Informational	Informational messages
7	Debugging	Debugging messages

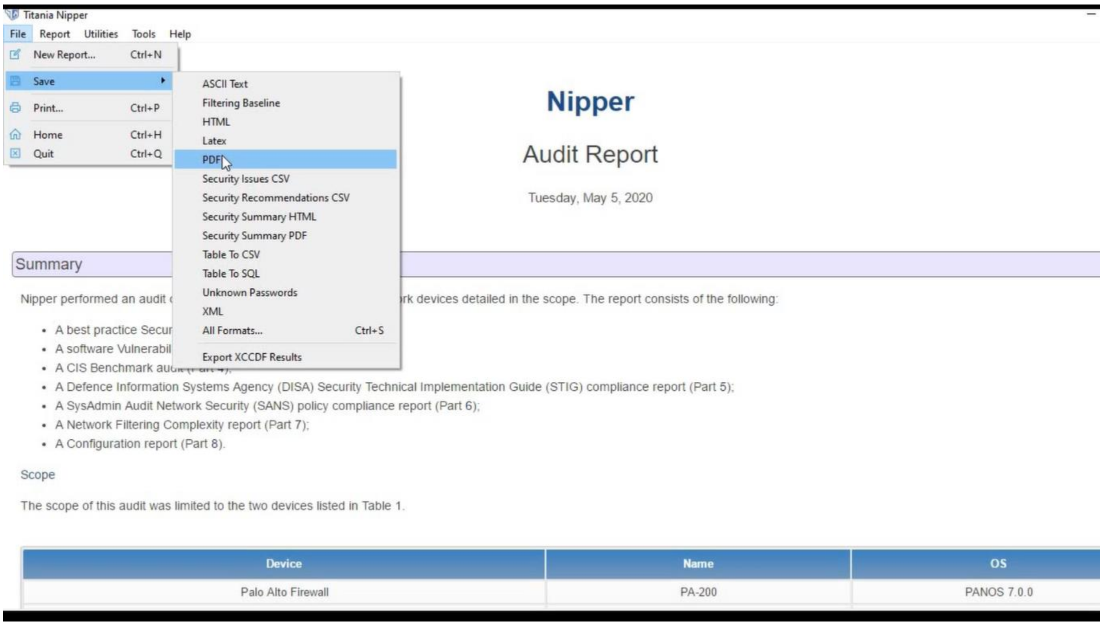
Table 189: Logging message severity levels

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

9.2 OSPF LSA Message Types

Figure 19:Appendix of report

Finally, we can save our firewall audit report as several file formats, Hence I choose PDF to save the report as shown figure 20.



Nipper

Audit Report

Tuesday, May 5, 2020

Summary

Nipper performed an audit rk devices detailed in the scope. The report consists of the following:

- A best practice Secur
- A software Vulnerabil
- A CIS Benchmark aud
- A Defence Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) compliance report (Part 5);
- A SysAdmin Audit Network Security (SANS) policy compliance report (Part 6);
- A Network Filtering Complexity report (Part 7);
- A Configuration report (Part 8).

Scope

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

Device	Name	OS
Palo Alto Firewall	PA-200	PANOS 7.0.0

Figure 20:Export the audit report

6. Conclusion

There are different types of firewall auditing tools. They have different auditing mechanisms and different processing methods. Using nipper studio audit tool, we can identify what are the vulnerabilities are occurred and which kind of issues that we have. This will provide better solution for an organization to maintain a good performance.

7. References

[1] "Firewall Security Audit & Firewall Vulnerability Testing - Titania", *Titania.com*, 2020. [Online]. Available: https://www.titania.com/products/nipper/. [Accessed: 07- May- 2020].

[2] T. Studio, "Titania Nipper Studio Product Review | SC Media", *SC Media*, 2020. [Online]. Available: https://www.scmagazine.com/review/titania-nipper-studio/. [Accessed: 07- May- 2020].

[3] K. Michael, "Why Businesses Should Be Conducting Annual Firewall Assessments and Reviewing Rules - Rochester, Buffalo, Syracuse | Dox", *Dox*, 2020. [Online]. Available: https://www.doxnet.com/2018/01/businesses-conducting-annual-firewall-assessments-reviewing-rules/. [Accessed: 07- May- 2020].