



How to aggregate your Nipper Audit Reports in Elasticsearch and Explore the Data in Kibana

titania.com

Nipper and Elastic Integration

Reducing your mean time to detect misconfigurations and vulnerabilities in firewalls, switches and routers, Titania Nipper accurately audits network devices, prioritizes risks and provides exact technical fixes to help remediate issues.

Nipper's accurate audit data – such as your detailed compliance posture against standards including DISA STIG, DHS CDM/NIST 800-53 and PCI – can now be injected into the Elastic Stack via JSON, where the combined solution provides greater scope to analyze and remediate large numbers of your machines on a daily basis.

The Kibana dashboard then gives you the power to examine your security posture from different angles, filtering by categories of error and drilling down to precise detail about devices/models impacted and how to mitigate risks.

This user guide shows you step-by-step how to aggregate your Nipper audit reports in Elasticsearch and use your Kibana dashboard to explore the data.

Published May 2022

© Titania Limited 2022, All Rights Reserved

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.

No part of this documentation may be copied or otherwise duplicated on any medium without prior written consent of Titania Limited, publisher of this work.

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: https://www.titania.com/support/nipper-support

TITANIA

Table of Contents

Contents	3
Prerequisites for Aggregating Nipper Audit Reports in Elasticsearch	4
Step 1 Configuring Nipper to Emit JSON in the Correct Format	4
Step 2 Running an Audit	5
Step 3 Creating the Elastic Index	6
Step 4 Use Logstash to Inject Nipper Output into the Elasticsearch Index	7
Step 5 Creating a Kibana Index Pattern	8
Step 6 Exploring the Data	11
Conclusion and Further Help	12

Prerequisites for Aggregating Nipper Audit Reports in Elasticsearch

Before you begin, please ensure you have completed the prerequisite technical set up:

- Download the digital version of this guide from the support section of the Titania website for a link to scripts you will need to download (a zip file called Nipper_Elastic_Ingest),
- » Nipper (v 2.6.3 or above) is licensed and installed on your local Windows 10 machine,
- » WSL is configured and available to run Logstash,
- » Elastic and Kibana are installed and running on your local machine*, there is no security on the Elastic Index, and
- » Docker Desktop is installed on Windows 10 (a powershell script is provided in the Nipper_Elastic_ Ingest zip file to pull and run the containers).

* If Elastic and Kibana are installed remotely, the URLs provided in the digital version of this guide will need to be updated accordingly, and the Logstash conf script adjusted to connect to the instance. An example file 'ls_with_creds.conf' is provided in the Nipper_Elastic_Ingest zip file.

For further information on installing the Elastic stack, please refer to the Elastic website: elastic.co

Step 1

Configuring Nipper to Emit JSON in the Correct Format

Logstash expects JSON in NDJSON. This means that each JSON Object appears on a separate line in the file, and not encapsulated in an array.

In order to configure Nipper to emit the JSON in the correct format you need to:

- » Open Nipper and click 'Settings'
- » Click the 'Logging' icon and open the 'File' tab
- » Ensure that:
 - » 'Enable logging to File' is checked
 - » The file path to the output file is OK
 - » 'Compact JSON' is selected from the dropdown
 - » 'Stream output' is checked, and
 - » 'Select All' Logging Trigger Levels is checked
- » Finally, click 'OK' to confirm the settings.

New to Nipper?

You can download the Nipper Beginner's Guide from the Titania website: titania.com

- » If you need to install Nipper:
 - » Go to the 'Downloading Nipper' section of the Nipper Beginner's Guide
- » If you need to install your license:
 - » Go to the 'Downloading your license' section of the Nipper Beginner's Guide
- » To audit your devices and generate reports:
 - » Open Nipper and select 'New Report' on the Nipper homepage. Step-by-step guides to generating each report can also be found on the website: www.titania.com/support

Nipper - Settings			?	\times
	General Event Log File TCP UDP Email			
	General			
	C Enable logging to File			
Global	Logging File path and name C:/example/nipper.json			
a	Format			
	Format to use as output for file logs Con	mpact JSON		
	JSON Settings			
	Stream output			
	Compact JSON EOL Format Wit	ndows (CR LF)	-	
	CEF Settings			
	EOL Format Wit	ndows (CR LF)	-	
	evels			
	File Logging Trigger Levels			
	✓ Report			1
	> Audit Fail			
	> Audit Pass			
	> Check Fail			
	Check Manual Check Data			
	Check Pass			
	Report Summary			
	✓ System			
	Error			
.				
				_
		V OK	🚫 Ca	ncel

TITANIA

Step 2

Running an Audit

- » Now click the 'Reports' icon to choose the audit you wish to run
- » Follow the onscreen instructions to choose the network device configurations you wish to include in your reports scope
- » Click 'Finish'
- » The file will now appear in the specified directory.

If there are lots of devices being audited and/or lots of audit types being conducted, it can take time to write out the file after the audit is complete.

Listing the size of the file a few times until it stops growing in size ensures that the process is complete.

Please note Nipper will append to this file if further audits are performed, so you may wish to move/delete the file before performing a subsequent audit.

PS C	:\example>	ls				
	Directory:	C:\example				
Mode		Lastk	/riteTime	Length	Name	
-a	3	1/01/2020	16:11	7345901	nipper.json	

The contents of nipper.json should look similar to the fragment below, which is shown as an example:

{"audit_type":"Security Audit","date_time":"Fri Jan 31 16:05:41
2020","device":{"collection_ip":"","filename":"3com5500
.txt","hostname":"5500-EI","manufacturer":"3COM","model":"5500 Series
Switch","operating_system":{"name":"SS4","version
":"5500-EI"}},"ease":{"description":"Dictionary-based password
guessing attacks have been widely documented on the Inte
rnet and published media, enabling an attacker with very little
knowledge or experience to perform the attack. There ar
e a numb

* Note there is no '[' opening bracket. Just a '{' opening bracket, and the JSON record is all on one line.

Step 3

Creating the Elastic Index

» Navigate to your Kibana dashboard: http://localhost:5601/app/kibana#/home?_g=()

To Rea	im about how usage data helps us manage and improve	our products and services, see our Privac	y Statement. To stop collection, disable us	age data here.
	ismiss			
5				
	Add Data to Kibana	a into ora-built dashboards and montoria	o sustams	
	and there are the bound of goody can your de		B alacteriate	
			<u> </u>	_
1			<u> </u>	-
	APM	Logging	Metrics	SIEM
	APM automatically collects in-	Ingest logs from popular data	Collect metrics from the	Centralize security events for
	errors from inside your	preconfigured dashboards.	running on your servers.	ready-to-go visualizations.
1	appications.			
	Add APM	Add log data	Add metric data	Add security events

- » Select the 'Dev Tools' icon from the left hand toolbar
- » Now configure the index and apply a mapping. The mapping extends the index length of some fields, and masks out those not needed.

Locate the .txt file script (shown right) in the Nipper_Elastic_Ingest zip file to copy and paste into the Console panel.

» Once the text has been pasted into the console, click anywhere inside the text, then click the 'Run' arrow in the top right hand corner.

This action creates an index called 'nipper' with the correct mappings to accept the data from the tool.

If the index already exists, then you will get an error in the right hand pane after clicking 'Run'.





W TITANIA

» If you wish to start afresh, issue a 'DELETE /nipper' on the Console pane, and then try again.

There is no need to replace the index creation text, just append it in the Console window, click on it, then click 'Run'. Once the index is deleted, you can return to the creation text, click that, and press 'Run' again.

You now have an index with the correct mapping to accept Titania data.

Step 4

Use Logstash to Inject Nipper Output into the **Elasticsearch Index**

The next step is to get the data into the index. An easy way to do this is using Logstash from the Elastic ELK stack. To do this, Logstash needs a config file.

- » Locate the .exe file named 'I.conf' (shown right) in the Nipper_Elastic_Ingest zip file.
- » Now invoke Logstash: cat nipper.json | logstash -f l.conf
- » The nipper.json data is now in Elastic.





Below it is invoked on a WSL (windows subsystem for Linux) Ubuntu instance. Note the output to the console issues some warnings, but completes successfully:

cat nipper.json | logstash -f l.conf --path.data . -l OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release.

WARNING: An illegal reflective access operation has occurred WARNING: Illegal reflective access by com.headius.backport9.modules.Modules (file:/usr/share/logstash/logstash-core/lib/jars/jruby-complete-9.2.8.0.jar) to field java.io.FileDescriptor.fd

WARNING: Please consider reporting this to the maintainers of com.headius.backport9.modules.Modules

WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations

WARNING: All illegal access operations will be denied in a future release

Thread.exclusive is deprecated, use Thread::Mutex

WARNING: Could not find logstash.yml which is typically located in \$LS_HOME/config or /etc/logstash. You can specify the path using -path.settings. Continuing using the defaults

Could not find log4j2 configuration at path /usr/share/logstash/config/log4j2.properties. Using default config which logs errors to the console

- [INFO] 2020-01-31 18:01:44.570 [main] writabledirectory Creating directory {:setting=>"path.queue", :path=>"./queue"}
- [INFO] 2020-01-31 18:01:44.593 [main] writabledirectory Creating directory {:setting=>"path.dead_letter_queue"; :path=>"./dead_letter_queue"}

- [WARN] 2020-01-31 18:01:45.367 [LogStash::Runner] multilocal Ignoring the 'pipelines.yml' file because modules or command line options are specified [INFO] 2020-01-31 18:01:45.386 [LogStash::Runner] runner Starting Logstash ("logstash.version"=>"7.5.2") [INFO] 2020-01-31 18:01:45.428 [LogStash::Runner] agent No persistent UUID file found. Generating new UUID {uuid=>"5b1127a5-1139-4949-aec4-c18a3e88fbfa", :path=>"./uuid"} [INFO] 2020-01-31 18:01:47.634 [Converge PipelineAction::Create<main>] Reflections Reflections took 66 ms to scan 1 urls, producing 20 keys and 40 values
- [INFO] 2020-01-31 18:01:49.890 [[main]-pipeline-manager] elasticsearch Elasticsearch pool URLs updated {:changes=>{:removed=>[], :added=>[http://localhost:9200/]}}

[WARN] 2020-01-31 18:01:50.199 [[main]-pipeline-manager] elasticsearch - Restored connection to ES instance {:url=>"http://localhost:9200/"}

[INFO] 2020-01-31 18:01:50.475 [[main]-pipeline-manager] elasticsearch - ES Output version determined {:es_version=>7]

[WARN] 2020-01-31 18:01:50.482 [[main]-pipeline-manager] elasticsearch - Detected a 6.x and above cluster: the 'type' event field won't be used to determine the document _type {:es_version=>7} [INFO] 2020-01-31 18:01:50.563 [[main]-pipeline-manager] elasticsearch - New Elasticsearch output {:class=>"LogStash::Outputs::Elasticsearch", :hosts=>["//localhost:9200"]}

[INFO] 2020-01-31 18:01:50.647 [Ruby-0-Thread-5: :1] elasticsearch - Using default mapping template

[WARN] 2020-01-31 18:01:50.714 [[main]-pipeline-manager] LazyDelegatingGauge - A gauge metric of an unknown type (org.jruby.specialized.RubyArrayOneObject) has been create for key: cluster_uuids. This may result in invalid serialization. It is recommended to log an issue to the responsible developer/development team

[INFO] 2020-01-31 18:01:50.726 [[main]-pipeline-manager] javapipeline - Starting pipeline [d=>*main", "pipeline.workers"=>8, "pipeline.batch.size"=>125, "pipeline.batch.delay"=>50, "pipeline. max_inflight"=>1000, "pipeline.sources"=>["/c/example/l.conf"], :thread=>*#<Thread:0x6dd7bd2c run>"}

[INFO] 2020-01-31 18:01:50.768 [Ruby-0-Thread-5::1] elasticsearch - Attempting to install template {:manage_template=>{"index_patterns"=>"logstash-*", "version"=>60001, "settings"=>{"index. refresh_interval"=>"5s", "number_of_shards"=>1}, "mappings"=>{"dynamic_templates"=>{{"message_field"=>{"path_match"=>"message", "match_mapping_type"=>"string", "mapping"=>{"type"=>"text", "norms"=>false}}}, {"string_fields"=>{"match_mapping_type"=>"string", "mapping"=>{"type"=>"text", "norms"=>false, "fields"=>{"type"=>"keyword"=>{"type"=>"keyword"=>{"type"=>"keyword"=>{"type"=>"keyword"=>{"type"=>"keyword"=>{"type"=>"keyword", "geore_above"=>256}}}}, "properties"=>{"@timestamp"=>{"type"=>"date"}, "@version"=>{"type"=>"keyword"}, "geore=>"text", "norms"=>false, "fields"=>{"type"=>"text", "norms"=>false, "fields"=>{"type"=>"keyword"=>{"type"=>"keyword", "geore_above"=>256}}}, "properties"=>{"@timestamp"=>{"type"=>"date"}, "@version"=>{"type"=>"keyword"}, "geore=>"text", "norms"=>false, "fields"=>{"type"=>"keyword"=>"type"=>"keyword", "geore_above"=>256}}}, "float", "longitude"=>{"type"=>"alf_float"})}"}

[INFO] 2020-01-31 18:01:50.965 [[main]-pipeline-manager] javapipeline - Pipeline started {"pipeline.id"=>"main"}

- The stdin plugin is now waiting for input:
- [INFO] 2020-01-31 18:01:51.130 [Agent thread] agent Pipelines running {:count=>1, :running_pipelines=>[:main], :non_running_pipelines=>[]}
- [INFO] 2020-01-31 18:01:51.792 [Api Webserver] agent Successfully started Logstash API endpoint {:port=>9600}
- [INFO] 2020-01-31 18:01:57.911 [LogStash::Runner] runner Logstash shut down.

Step 5

Creating a Kibana Index Pattern

- » Firstly, click on the 'Settings' icon in the Kibana dashboard
- » And click on the 'Index Patterns' link



» Click on the blue 'Create Index Pattern' button



» Now type the name of the index you created into the index pattern box

You don't have to type the complete name - you can use wild cards (this helps if you want Kibana to look over multiple Elastic indexes) - but in this case, typing nipper* works.

It will tell you Kibana has matched with the Elastic index called nipper*.

- » Click the 'Next Step' button
- » Select date_time from the drop down box, and click the 'Create Index' pattern.

The date_time is the field you mapped to contain the date of the events in the Nipper JSON output.

You will now see that the index has been created.

Elasticsearch							
Index Management	nipper*						* 2
Index Lifecycle Policies	Time Filter field name: da	ite_time					
Transforms	This page lists over	field in the pippert index	and the field's	associated our	o tuno oo rooordu	nd by Electionen	roh. To obango a fi
Remote Clusters	type, use the Elastic	search Mapping API %	und the neid a	0330010100 001	e type as record	to by Elasticate	ren. To enunge u n
Snapshot and Restore							
License Management	Fields (267)	Scripted fields (0)	Source filte	ers (0)			
8.0 Upgrade Assistant	0.00						
Vibana	QFilter						All field types
Index Patterns	Name		Туре	Format	Searchable	Aggregatable	Excluded
Saved Objects	@timestamp		date		•	•	
Reporting	@version		string		•		
Advanced Settings	@version.keyword		string		•		
	_id		string		•	•	
	_index		string		•	•	
	_score		number				
	_source		_source				
	_type		string		•		
	audit_type		string		•		
	audit_type.keyword		string		•	•	
	Rows per page: 10 🗸					< 1 2	3 4 5 27



» Next, click on the 'Discover' icon on the left toolbar.

If the data you are analysing wasn't created in the last 15 minutes, it is likely you will need to change the time window with the calendar item to see the data.

» Now you should see the data loaded into Elastic. In this case there are 3221 records.



K	D Discover				0	
Θ	New Save Open Share	Inspe	ect			
0	🖹 🗸 Search			KQL 🛗 🗸 Last 1 year Show dates	C Refre	esh
6	🗐 – + Add filter					
	nipper*	0		3,221 hits		
80	Q. Search field names			Jan 31, 2019 @ 18:32:22.892 - Jan 31, 2020 @ 18:32:22.892 - Auto 🗸		
	Filter by type 0		3000			(III)
8	Selected fields	3	2500 E 2000			
(†)	⊕ _source	ŝ	5 1500 1000			
2	Available fields		500			
5	Cimestamp		2019-02-01 2019-03-01 2019-	24-01 2019-05-01 2019-06-01 2019-07-01 2019-08-01 2019-09-01 2019-10-01 2019-11-01 2019-12-01 2020-01-	01	
Ŧ	t @version		Time -	cate_time per week		
0 0 0	t _id t _index # _score t _type t audk_type	>	> Jan 31, 2020 € 16:11:02.000	<pre>message.level Critical comment Dimension 30, 2020 0 10 01:55.050 1116: Aules Follow Monthly Fullering Complexity detributes a 1, 2020 0 15:1112.200 160 manual folse National Towards Provide Comments and Provide State State State State State Market State State State State State</pre>	ng Deny A : IP68W	411
۲	e aucits e comment	>	> Jan 31, 2020 0 16:11:02.000	<pre>ressage_level: Critical comment: @timestamp: Jam 31, 2020 0 16:01:55.688 title: Mules Follwi audit.type: Filtering Complexity date time: Jam 31, 2020 0 16:11:02.000 1d: manual: false host: MURLMPT097 device.collection.jb; device.filement: Matchard_JTM_S_Series.woll device compression multime news/ Multi device content monthment 12.3 during multi-false</pre>	ng Deny A	All
	count			device.model: XTM 5 Series device.hostname: XTM_5.Series message_type: Compliance Test Fail	multition	
	t device.collection_ip	>) Jan 31, 2020 0 16:11:02.000	message_level: Critical comment: 0timestamp: Jan 31, 2020 0 18:01:55.085 title: Rules Follwi audit_type: Filtering Complexity date_time: Jan 31, 2020 0 16:11:02.000 id: manual: false	ng Deny A	A11
	t device.hostname			hest: TRUKLAPTOP79 device.collection_ip: device.filename: device.operating_system.name: CP device.operating_system.version: 4.1 device.manufacturer: Check Point device.model: CheckPoint	VPN-1 Ec	dge
	device manufacturer			3G device.hostname: TDemo_Check_VPN message_type: Compliance Test Fail product: nipper messag	e:	

- » Load in the dashboard
- » And select the 'Settings' menu again

K	Discover							0 2
0	New Save Open Share	Insp	pect					
0	🗑 🗸 Search			KQL	*	Last 1 year S	ihow dates	O C Refrest w dates c Refrest c Refrest
	🗇 - + Add filter							
80	R Search field names	0		Jan 31, 2019 @ 18:32:22.8	12 - Jan	3,221 hits 31, 2020 @ 18:32:22.892 — Auto ~		
	Image: Selected Fields 0		3000 2500 2000 1000 500					
9 P	@ @timestamp @version id		0 2019-02-01 2019-03-01 2019 Time -	-04-01 2019-05-01 2019-06-01	2019-07-0	1 2019-08-01 2019-09-01 2019-10-01 2019-11-01 20 date_time per week	19-12-01 2020-	-01-01
6 6	<pre>t _index # _score t _type t audit.type</pre>		> Jan 31, 2020 ⊕ 16:11:02.000	message_level: Critical audit_type: Filtering Co host: TWUKLAPTOP79 devis device.operating_system. device.hostname: TDemo_C	comment plexity e.coller rersion: reck_IP6	Bimestamp: Jan 31, 2020 0 18:01:55.085 txl date.time: Jan 31, 2020 0 16:11:02.000 id: tion.jp: device.filename: device.operating. 4.1 device.mundraturer: (beck Point device. Bw message_type: Compliance Test Fail product:	e: Rules Fol manual: false system.name: odel: CheckPo nipper mess	lwing Deny All CP wint IP60W age:
0	e audits e comment // count		> Jan 31, 2020 ⊕ 16:11:02.000	message_level: Critical audit_type: Filtering Co host: TWUKLAPTOP79 devir device.operating_system. device.model: XTM 5 Seri	comment plexity e.colled ame: XT	<pre>#timestamp: Jan 31, 2020 @ 18:01:55.688 txtl date_time: Jan 31, 2020 @ 16:11:02.000 id: tion_lp: device_filemame: MatchOand_XINLS_See M Gevice_operating_system_version: 11.7.3 device choatame: XMLS_Seriem message_type: Compliant</pre>	e: Rules Fol manual: false ries.xml ce.manufactur mce Test Fail	lwing Deny All
	t device.collection_ip t device.filename		> Jan 31, 2020 @ 16:11:02.000	message_level: Critical audit_type: Filtering Co host: TWUKLAPTOP79 devia	comment plexity e.colled	@timestamp: Jan 31, 2020 0 18:01:55.688 titl date_time: Jan 31, 2020 0 16:11:02.000 id: m titon_ip: device.filename: device.operating_s	ie: Rules Fol manual: false system.name:	lwing Deny All CP

» Select the 'Saved Objects' link



» Click the 'Import Objects' button

» Select the 'Dashboard' icon

» Now from the requester, import the nipper_kibana_dashboard.ndjson provided in the Nipper_Elastic_Ingest zip file.

This file contains the definitions of example visualisations, as well as a dashboard containing those visualisations.

	Management / Saved o	bjects	0
Э	Elasticsearch		
0	Index Management Index Lifecycle Policies	Saved Objects	🛆 Export 2 objects 🛛 🕁 Import 🙄 Refresh
1	Rollup Jobs Transforms	From here you can delete saved objects, such as saved searches. You can also edit via their associated application, which is probably what you should use instead of t	it the raw data of saved objects. Typically objects are only modified this screen.
3	Remote Clusters	O Search	Time v Tr Delete
1	License Management	et opnom	Decce Expert.
	8.0 Upgrade Assistant	Type Title	Actions
	• 101	III Advanced Settings [7.5.1]	810
	Kibana	☐ ♣ nipper*	
	Saved Objects	Rows per page: 20 🗸	
	Reporting		
	Advanced Settings		
2			
3			

Kanagement / Saved objects 0 1 Elasticsearch Index Management Index Lifecycle Policies Rollup Jobs Saved Objects ۲ From here you can delete saved o modified via their associated app the raw data of saved obje tead of this screen. ects. Typically objects are only £ Transforms Remote Clusters Snapshot and Res 8 Q Search... туре 🗸 白 Type Title Actions 8 Advanced Settings [7.5.1] 0 📕 Kibana Advanced Settings [7.4.2] 8 ndex Patt B Nipper Saved Objects 6 A nipper* ę A nipper** đ 🗆 🚓 keith* ۵ A. apm-* ... Ŷ III /goto/224c Ş ... ۲ Audit Session Lis In Test Status 位 Chooser ...

» And finally, click on the Nipper dashboard link.

K 🖸 D.	ashboards	
٩		
۲	Dashboards	① Create dashboard
10	Q Search	
80		
Ê	Title Description	Actions
&	Nipper	Ø
69	Rows per page: 20 \sim	
8		
æ		
Ð		
ି		
a		
Ŷ		
\$		
۲		

TITANIA

Step 6 Exploring the Data

- » You will now be presented with a dashboard like this allowing you to click and filter on the results in the usual Kibana manner
- » Scroll down the dashboard to see heat maps and detailed audit findings and vulnerabilities

Here you can explore your security posture from different angles, filtering by categories of error and drilling down to precise detail about devices/models impacted and how to mitigate risks...





	apirro o 1		Nexus	• 4 - 5				
		Eu Catalyst Quidway	SA Idemon Switch Firewall Switch Router	• 5 - 6 • 6 - 7				
(CheckPoi Ch	nt 2200 Appliance CheckPoint eckPoint VPN-1 E	e (Gaia) - IP60W - dge 3G -	6 - 10				
			NSA-FUTR-83					
:=				Finding		L		
Sec	urity Au	ıdit				ලා		
Fi	inding	Title ≑	Impac Rating	Impact ⇒	Count	-		
N FI O	SA- LTR- 20	Filter Rules Allo Packets From A Source To Any Destination An Any Port	ow Critica Any d	If network filtering rules are not configured to restrict access to network services from only those hosts that require the access then unauthorized access may be gained to those services covered in this issues finding. For a network edge device, this could lead to a remote attacker gaining access to network service. For an internal device this could lead a malicious user gaining unauthorized access to a service.	8	ļ		
N Fl O	SA- LTR- 20	Filter Rules Allo Packets To Any Destination An Any Port	w Mediu / d	If network filtering rules are not configured to restrict access to network services from only those hosts that require the access then unauthorized access may be gained to those services covered in this issues finding. For a network edge device, this could lead to a remote attacker gaining access to network service. For an internal device this could lead a malicious user gaining unauthorized access to a service.	5			
N F O	SA- LTR- 20	Filter Rules Allo Packets To Network Destinations	er Rules Allow Informational If network filtering rules are not configured to restrict access to network services from only those hosts that require the access then unauthorized ckets To access may be gained to those services covered in this issues finding. For a network edge device, this could lead to a remote attacker gaining twork access to network service. For an internal device this could lead a malicious user gaining unauthorized access to a service. stinations					
NSA- Filter Rules Allow Medium If network filtering rules are not configured to restrict access to network services from only those hosts that require the access then unauthorized access may be gained to those services covered in this issues finding. For a network edge device, this could lead to a remote attacker gaining								
STI	G Detail					Ś		
Fi	inding	Title ≑	Category	heck \Leftrightarrow Description \Rightarrow Fix \Leftrightarrow	Count	*		
V	-3143	Devices exist with standard	CATI	eview the network devices configuration to determine if the vendor default Network devices not protected with strong Remove any assword is active. If any vendor default passwords are used on the device, this is a password schemes provide the opportunity for one to crace the password the resolution access word the resolution access.	17			

Conclusion and Further Help

If you have followed this guide, you will see how quick and easy it is to aggregate your Nipper audit reports in Elasticsearch.

Now you can explore your data in Kibana, prioritize your risks and use Nipper's exact technical fixes to help remediate any vulnerabilities or issues on your network.

If you would like any help or advice about the steps or scripts included in this guide, simply contact our dedicated Support team on:

Tel: (+44)1905 888 785 Email: support@titania.com

Our solution advisors will be more than happy to help walk you through this or any other auditing processes with our Nipper software.

			Missi	ion Critical Net	twork				
				CATI					
Result	Scope	#	Title				Severity	Responsil	bilit
FAIL	2	V-3196	An insecure version of St	NMP is being us	sed.		CAT I	IAO	
FAIL	٥	V-3062	Passwords are viewable	V-30	85 F/				
Result	Scope	#	Title	HTTP server is The network element must he administrative access disable	not disabled ave HTTP service for rd.	Severity Rule ID	GAT III SV-41467r2_rule		ilit
FAIL	9	V-3085	HTTP server is not disat			STIDIO	NET0740		
FAIL	6	V-3966	More than one local acc	Findings	Туре		Sever	ity	
FAIL	6	V-3969	Network element must of	router03 router29	Cisco Router Cisco Router		Missic	on Critical on Critical	
FAIL	2	V-14671	NTP messages are not a	Quidway Office-Juniper-SRX 1000-61	Huawei Quidway Swito Juniper SRX Firewall 3COM 15500 Series SW	h Iton yr	Missie Missie Missie	on Critical on Critical	
FAIL	0	V-31285	BGP must authenticate	XTM_5_Series	WatchGuard XTM 5 Se	ries XTM5'5	Missie	on Critical	
				watch555 router318	WatchGuard XTM Cisco Router		Missie	on Critical	
Result	Scope	#	Title	Remediation	ble using HTTP (port 80) for ad	ministrative access			ilit
FAIL	0	V-3020	DNS servers must be det	fined for client i	resolver.		CAT III	IAO	

Example analytics shows the prioritization of remediation that can be achieved when audit data is combined with value chain data on the mission criticality of the device/ network.

About Nipper

Nipper accurately audits the security of firewalls, switches and routers to detect exploitable misconfigurations that pose risk to the network, prioritized by criticality. Applying Nipper's compliance lens to the findings also provides the evidence needed to assure compliance with RMFs including DISA RMF, NIST 800-53/171, STIG, CMMC and PCI. All findings are output as an easy-to-read report, or a JSON for integration with SIEM, GRC and other data visualization systems.

Nipper's risk remediation advice and exact technical fixes for misconfigurations also support and accelerate the process of becoming secure and compliant.

About Titania

Protecting over 25 million people globally, Titania software is trusted to secure the world's most critical networks against preventable attacks. Nipper intelligently automates configuration auditing to analyze misconfigurations and validate your network security against the latest risk management frameworks, assurance and compliance standards.

Stay secure and complaint with Nipper. Find out more.

titania.com/products/nipper/

titania.com