"A dramatic time-saving innovation for device security validation."

MOD Defence Contracts Bulletin
The world’s most secure networks leverage multiple technologies’ strengths. Their goal is to use a multi-layered approach to create a combined solution, which is stronger and more resilient than its individual components.

Each technology is architecturally designed for one specific expertise area. The complementary technologies each have a capability that none of the others adequately provide:

- **Monitoring** – Live Activity Detection
- **Scanning** – Network Discovery
- **Configuration Auditing** – Granular Accuracy
- **SIEM Systems** – Collating the ‘Big Picture’

**Configuration Auditing**: Provides a “Granular View” of security systems. They analyze internal system information already present on your network devices, refining mass configuration and operating system data into precise risks and remediation actions. Granular “line by line” analysis (delivered at scale) and virtual modeling technology builds human understanding into how device settings interact with each other, giving a more accurate picture of security and compliance risks.

---

**DOES MORE & BRINGS GREATER ACCURACY**

**ACCURATE**
Auditing actual settings, software and options creates precise findings

**COVERAGE**
Direct access to a system enables the most complete audit coverage

**NON-DISRUPTIVE**
Audits using standard administrative interfaces limit disruption. Offline auditing produces no network traffic

**FAST**
Auditing is quick in all scenarios

---

**Device Auditing**

<table>
<thead>
<tr>
<th>Device Auditing</th>
<th>Scanners</th>
<th>Nipper</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit without Network Traffic</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>Authentication Configuration</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>Authorization Configuration</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>Account/Logging Configuration</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>Intrusion Detection/Prevention Configuration</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>Password Encryption Settings</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>Timeout Configuration</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>Physical Port Audit</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>Routing Configuration</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>VLAN Configuration</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>Network Address Translation</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>Network Protocols</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>Device Specific Options</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>Time Synchronization</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>Warning Messages (Banners)</td>
<td>✓*</td>
<td>✓</td>
</tr>
<tr>
<td>Network Administration Services</td>
<td>✓*</td>
<td>✓</td>
</tr>
<tr>
<td>Network Service Analysis</td>
<td>✓*</td>
<td>✓</td>
</tr>
<tr>
<td>Password Strength Assessment</td>
<td>✓*</td>
<td>✓</td>
</tr>
<tr>
<td>Software Vulnerability Analysis</td>
<td>✓*</td>
<td>✓</td>
</tr>
<tr>
<td>Network Filtering (ACL) Audit</td>
<td>✓*</td>
<td>✓</td>
</tr>
<tr>
<td>Wireless Networking</td>
<td>✓*</td>
<td>✓</td>
</tr>
<tr>
<td>VPN Configuration</td>
<td>✓*</td>
<td>✓</td>
</tr>
</tbody>
</table>

* Limitations and constraints will prevent a detailed audit

---

Titania.com
CUSTOMIZABLE AUDITS

Security Audit – perform a "best practice" security audit, combining multiple industry & pentesting checks. Use rating systems and mitigation advice to prioritize and plan fixes.

Configuration Audit – detailed configuration reporting, including information such as: filtering, routing protocols, administration services & more. This report offers a quick, clear view of your device settings.

Vulnerability Audit – audit against global public vulnerability repositories such as the US Govt NVD & the NIST CVE databases to find easy-to-exploit security issues and de-risk your business.

INDUSTRY COMPLIANCE

CIS - Nipper audits have been certified as 100% accurate by CIS. They demonstrate compliance with FISMA, HIPPA, NIST, SOX, IRS 1075, FedRAMP, GLBA, ISO 27001, NERC, ETSI and CPNI.

PCI – quickly complete automatable payment card system checks. Generate detailed advice that verifies passes and explains failures so you can validate compliance.

STIG – automate online audits or take them offline in secure environments. Generate detailed, verified reports that include remediation in line with STIG baselines.

SANS – assess compliance with SANS policies and benchmark your security levels according to this globally trusted industry body.

SECURITY & CONVENIENCE

- Agentless - no additional software to install or maintain
- Scriptable for 24/7 continual analysis
- Enhances enterprise scanning and removes accuracy concerns
- Integrates easily with existing systems

CONNECTIVITY OPTIONS

- Audit online, offline, onsite, in the cloud, virtually or integrated into enterprise systems
- Standalone for remote workers and audit teams, or
- Fully integratable into SIEM solutions for SOCs and NOCs

What if your network is secret or air-gapped? According to Gartner, Nipper is:

"the only offline configuration review tool."

Gartner Inc.

Which means, one solution can handle both!

Titania.com/register/trial
TITANIA NIPPER STUDIO

Total compliance with data protection regulations is now essential, otherwise businesses could find themselves faced with hefty fines. There is a wide range of security auditing solutions available, but some can be prohibitively expensive, many rely only on network scanning and few extend their focus beyond firewalls.

Nipper Studio takes a refreshingly new approach to security auditing, as it supports an impressive range of firewalls, switches and routers from all the major players. Naturally, Cisco is at the top of the list, but it can also audit devices from Brocade, Check Point, Fortinet, HP, Juniper, WatchGuard and many more.

Installation takes minutes and auditing is a simple, two-step process. First, you need to download the configuration file from the devices to be interrogated. We tested with HP ProCurve and Cisco Catalyst switches, and found the process well documented. You point Nipper Studio to the configuration file location and it identifies the device from its contents. Usefully, you can specify a directory where multiple files are stored and it can create a single report on them all.

Four options for the level of auditing and reporting are available. The security audit covers more than 20 key areas, including administrative access, authentication, IDS/IPS, SNMP, port configurations and software vulnerabilities. Each can be enabled or disabled as required and you can apply a range of filters to fine-tune the information you want presented.

Two rating systems are supported, with the software defaulting to Nipper’s own system. A valuable feature is support for v2 of the CVSS (Common Vulnerability Scanning System) open framework.

Prior to report generation, you can select CVSS and also configure other associated environmental metrics. These include settings for CDP (collateral damage potential), target distribution, plus confidentiality requirements, so you can define and prioritise which areas are important.

User policies tell Nipper Studio what password tests you want carried out. These include checks on the maximum and minimum password ages, authentication timeouts, length, repeated characters and so on. Nipper Studio can include a full report on device configurations and also provide it in raw format as well.

Reports are generated quickly, and we score Nipper Studio highly for their classy design and content. The reports are well structured and very clear, so they will appeal to a much wider audience than just technical staff. The reports can be branded with your own company name and logo, and start with a summary of the audit scope, with devices and graphs showing a breakdown of issues identified.

The level of information in the reports is quite remarkable. Not only do they clearly highlight security issues with firewalls, but also provide an impact assessment, potential security breaches and recommendations for remedial actions.

Other areas of concern - such as weak passwords, unsecured administrative access and open services for all devices - are clearly highlighted, and each graded with ratings for overall impact and ease of remediation. Where the CLI can be used to fix a problem, the report includes a list of all relevant commands and their format, so there’s no need to rummage through the device’s user manual.

Nipper Studio provides change management features, as during report configuration you can point it to a second file taken from an earlier time. The report compares them and highlights any differences, so you can see easily if unauthorised changes have been made to critical devices.

Nipper Studio can start auditing straight from the box and its sophisticated reporting takes all the guesswork out of regulatory compliance. It represents very good value, and is far more efficient and informative than products that rely only on network scanning.

Product: Nipper Studio
Supplier: Titania Ltd
Telephone: +44 (0)1905 888785
Website: www.titania.com

www.computingsecurity.co.uk
Titania Nipper Studio provides change management tools that automate and simplify the process of assessing network health and security. Nipper Studio is capable of scanning multiple files and creating a comprehensive inventory of the tools that are available. This allows it to break down issues identified into a clear prioritised list. With Nipper Studio, you can define and prioritise which areas are most critical to your organisation and focus your efforts accordingly. Nipper Studio supports an impressive range of firewalls, including administrative access, and can scan multiple files stored and it can create a breakdown of issues identified. Prior to report generation, you can select the scope, with devices and graphs showing a potential impact, target distribution, plus recommendations for remedial actions. Nipper Studio is particularly appealing to a much wider audience than just security professionals, due to its ease of use and its ability to support a range of devices and operating systems. It is highly recommended for its comprehensive reporting capabilities, which take all the guesswork out of security auditing.
Examining systems using automated configuration & build analysis tools is a huge advantage for a SOC or NOC. Using these tools to examine your system set-ups, in detail and at speed – means you can find and close exploitable vulnerabilities that monitoring or scanning based solutions would miss.

An attacker normally probes and scans a network using a variety of tools to gain knowledge of available entry points and routes to data.

Many powerful tools are available which detect common attacker behaviour, providing valuable early warnings of potential attacks.

(For more information, see Titania’s whitepaper: ‘The Future of Autonomous Mitigation’.)

Configuration and build analysis tools have no need to scan systems, so do not generate mass network traffic and therefore avoid the risk of killing network services.

You can quickly gain detailed knowledge of your systems’ defences, the monitoring capabilities you have deployed, and more importantly, any vulnerabilities you have.

PRACTICAL EXAMPLE

When Pentesters automate a build review, Nipper is their tool of choice for providing granular accuracy. Now, Enterprise teams dissatisfied with false positives and plagued by alert fatigue from their current systems have also added Nipper to provide a true baseline of accurate information.

Nipper helps secure the networks of clients including: The Department of Defence, FBI, global banks, financial institutions, US Treasury and payment providers (such as Visa and Mastercard).

In this example, ‘New Report’ has been selected and a router configuration added to the device audit list.

The following example shows how easy it is to perform a detailed security review of a network router.

In this example, Nipper is used to perform a review of a Cisco router (one of the most popular network routing devices).

We are using Nipper to query a backup of a saved configuration. One distinct advantage of auditing this way is that it does not disturb potentially business critical devices.
There are many report and compliance audits available within Nipper, including configuration build reviews and industry standards such as the CIS benchmarks.

Vulnerabilities are categorised by severity and area affected e.g. Administration, Authentication, Best Practice, Clear Text (Encryption) and Filtering issues.

A Mitigation Classification Table is also provided. Mitigation includes:

- The easiest issues to fix quickly (low hanging fruit)
- What to do to fix those issues
- Command line fixes (device specific)

The reporting options can be used to export all report information and data tables. These can be fed into SIEM consoles (or other systems) as data feeds. In addition to the GUI, a full command line version is available with APIs.

"Nipper enables Cisco to test devices in a fraction of the time it would normally take to perform a manual audit."

Cisco Systems Inc.

Titania.com/register/trial
**Support Options**

<table>
<thead>
<tr>
<th></th>
<th>Bronze</th>
<th>Silver</th>
<th>Gold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product updates and maintenance</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Email-based support</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Web-based support</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Phone support</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>24/7 support logging</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Guaranteed response 24 working hours</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guaranteed response 8 working hours</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Remote assistance</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Free</td>
<td>15%</td>
<td>20%</td>
</tr>
</tbody>
</table>

**System Requirements**

- **Microsoft Windows Vista or above** (Server 2008 or above)
  - 400MB disk space
  - 2GB memory

- **GNU/Linux** (RHEL, Ubuntu, Fedora, CentOS, openSuSE)
  - 300MB disk space
  - 2GB memory

- **macOS Sierra or above**
  - 500MB disk space
  - 2GB memory

**OPTIONAL EXTRAS**

- **TITANIA PAWS**
  - Advanced configuration reviews for workstations, servers & databases
  - Online and offline auditing support for Windows, Linux and Mac OS
  - Advanced SQL database analysis
  - Policy editor enables complete customization of analysis
  - Integrate into existing enterprise systems
  - Combines procedural and configuration compliance checks

**Trial Nipper**

Want to ditch alert fatigue and get more accurate results?

DOWNLOAD

www.titania.com/register/trial