# nemasis®

# WHITEPAPER

Version: 1.10

nemasis®: Security Assessment & Vulnerability Management

## Nemasis Introduction

**Nemasis – Vulnerability Management Suite - assists in implementing a comprehensive GRC** (Governance, Risk Management, and Compliance) **strategy** for managing an organization's overall governance, risk, and compliance with regulations.

It is a methodical approach which Executives and risk leaders can use for aligning IT with business objectives, while efficiently managing risk and meeting compliance requirements.

### GRC Definition

**Governance:** Ensures that organizational activities are aligned in a way that supports the organization's business goals.

**Risk:** Risks associated with organizational activities are identified and addressed in a way that supports the organization's business goals.

**Compliance:** Making sure that organizational activities are conducted in a way that adheres to the laws and regulations impacting those systems.

The strategy/solution enables customers/organizations to organize and prioritize thousands of assets and quickly focus on issues that pose the greatest risk to their business.

It is a unified framework for managing security and compliance landscape and reduce overall business risk.

### It uses the following approach

- Define what matters most
- Identify an organization's risk exposure
- Develop a methodology
- Focus on key business processes
- Create a system for continuous review and monitoring purpose
- Catalogue Security Posture Report
- Recommend Remediation Measures
- Put together a Compliance Report

### How It Works

Nemasis conducts scans to assess the risk posture of the systems within an organization. This vulnerability data is used to calculate the risk score associated with each system. Once the report is processed, this vulnerability data is used for risk and compliance management.

### Benefits of Nemasis GRC offering:

**Universal/Central Repository to manage all GRC Processes:** Carry out gap analysis; produce business-related risk profiles and custom-built scoring.

**Eliminate Redundant Costs and Controls:** Nemasis GRC system maps with the latest sources of risk, mitigation and multi-regulatory compliance including SOX, PCI, BASEL II, ISO 27001, COBIT, HIPAA, GLBA, FISMA, and more.

**Reputation Security:** Risk management and compliance are both essential parts and help secure your business reputation.

**Prioritize Investments:** Prioritize investments according to each asset's potential impact and significance to the organization.

**Asset Discovery:** Continuous discovery of organizational Assets.

**Clear Insight into the Risk:** Clear insight into the actual risk of each unique environment by incorporating information on Exploit Exposure, Malware Exposure and weighted risk scores as well as CVSS rankings.

**Duplicative activities:** Having similar processes duplicated across a business is an inefficient way to operate and GRC can free up whole teams to work on other projects. This further saves your organization time and improves ROI.

**Superlative Vulnerability Scanning:** Scans for over tens of thousands of vulnerabilities with more than 200,000 vulnerability checks on Networks, Web Applications, Operating Systems, Databases and Devices.

Have a look at the below Vulnerability statistics:

48,000 plus vulnerabilities gathered using NVTs.

100,000 plus vulnerabilities gathered using CVE.

2,500,000 plus vulnerabilities gathered using CPE.



## Installation:

For installation purposes, MicroWorld will provide Nemasis in the form of customized Debian builds (ISO).

## Supported Platforms

### Supported Devices/Systems /platforms/ applications

- Network devices
- Virtual Systems: VMware ESX, ESXi, etc.
- **Operating systems:** Windows, Mac, Linux, etc.
- **Databases:** Oracle, SQL Server, etc.
- **Web applications:** Web Servers, Web Services, OWASP Top 10 vulnerabilities
- IPv4/IPv6/Hybrid Networks
- Cloud Systems

## BROWSERS (with HTML 5 compatibility)

You can use Nemasis with popular browsers such as below:

- Google Chrome (RECOMMENDED)
- Mozilla Firefox
- Mozilla Firefox ESR
- Safari 7.1
- Safari for iOS
- Microsoft Edge
- Microsoft Internet Explorer 11

# Scheduled Tasks

## Passive Vulnerability Scanner (PVS)

Nemasis Passive Vulnerability Scanner (PVS) plugin is an exclusive network discovery and vulnerability testing software that delivers real-time network profiling and monitoring for constant and continuous assessment of an organization's security demeanour in a non-intrusive manner.

It can continuously monitor predefined assets to determine topography, services, and vulnerabilities.

### Challenges faced by Information Security (IS) team:

Surveillance of newly connected assets.
Gaining insights of vulnerabilities between scans

Depending on the scan prevalence, organizations may need near real-time visibility of vulnerabilities on critical assets so they can extenuate them before an adversary exploits them.

Remote Terminal Units, Logic Controllers, and other operational technology devices could be disrupted by active scanning. Security staff needs a way to assess assets in Operational Technology (OT) environments, without the risk of causing an outage.

***Our Passive Vulnerability Scanner overcomes these challenges by implementing below methods.***

**Identify the assets that use the IP protocol:** Assets include IT assets, such as servers, desktops, laptops, network devices, web apps, virtual machines, mobile, tablets, cloud based assets and OT assets, such as PLCs, RTUs, HMIs, Communication Adapters and more.

Apart from asset discovery and profiling capabilities, a passive monitoring solution identifies known vulnerabilities in the assets

## Tasks and Notifications

Generate/ create schedules for Tasks (Scans & Reports) so they run automatically, on a recurring basis (daily, weekly, monthly) or one time only.

Nemasis sends advanced notifications of the next scan to task owner and other users that are included for a SCHEDULED SCAN.

Once the report is generated Nemasis sends notifications to selected users to download reports.

## NOTIFICATIONS/ Alerts

All alerts are displayed on the Alerts Dashboard; however, you can specify subsets of alerts that go via email to specific individuals or to distribution groups.

Be alerted right away about vulnerabilities, misconfiguration issues and other issues that can put you at risk of security breaches.

Notifications section lets you know when the scan notifications should be sent. You get notified days, hours or minutes before the scan starts. You also get notified when the scan is finished and the results are ready to be viewed.

Notifications are received by the task owner. To send notifications to other members, you can select from your existing distribution groups or create a new distribution group with a list of email addresses.

### Schedule Options

There are many schedule options that you can use to control when a task (Scan, Report) runs. The following schedule options are available.

**Once** - Runs task once on a specific date.
**Hourly -** Runs the task every hour.
**Daily -** Runs the task every day.
**Weekly -** Runs the task on certain days of the week.
**Monthly -** Runs the task on a specific day of the month

**Patch verification checks:** Depending on your security policies and routines, you can schedule some scans to run on a monthly basis, such as patch verification checks.

**Compliance checks:** Depending on your security policies and routines, you can schedule some scans to run on an annual basis, such as certain compliance checks.

## Real-time Customizable Dashboards

While most software dashboards are static and can't provide you with the real time data, Nemasis Dashboards are fully customizable by nature and provide highly specialized views of your network.

The **Dashboard module** is configured with multiple dashboards that contain different views/layouts, custom graphs and charts (such as Bar graphs, line graphs, pie charts).

These graphs /charts are fully customizable and allow the user to view the data in a way that provides instant analysis of the important anomalies, with the ability to drill into the underlying data set for further assessment.

Additionally, you can also add more dashboard views, delete the dashboard view based on your preferences, and choose the order in which they appear in the module.

Nemasis dashboards update information and data in real time as it collects data from scans and discovery connections.

Use Nemasis components such as **Scan Display, Asset Display, SecInfo Display** and more to generate multiple dashboards.

Use **Scan Display** component/option to display multiple dashboards grouped by function.
Some of the dashboards displayed under **Scan Display** components are as below.

- Results by Severity Class
- Reports by Severity Class
- Tasks by Status
- Tasks by Severity Class

Use **Asset Display** component/option to display multiple dashboards grouped by function. Some of the dashboards displayed under **Asset Display** components are as below.

- Most Vulnerable Host
- Host by Topology
- Most vulnerable operating Systems

The **SecInfo Display** component/option displays multiple dashboards grouped by function. Some of the dashboards displayed under **SecInfo Display** components are as below.

- NVTs by Severity Class
- CVEs by Creation Time
- CVEs by Severity Class

In addition to this, you can further customize the dashboards & display and view dashboards based on following functions.

- Results by Severity Class
- Reports by Severity Class
- Reports with High Results
- Tasks by Severity Class
- Task by Schedules
- Task by CVSS
- Task by Most High Results
- Task by High Results per Host
- Reports by CVSS
- Results by CVSS
- Results Description Word Cloud
- Results Vulnerability Word Cloud
- Notes by Active Days
- Notes by Creation Time
- Notes Text Word Cloud
- Vulnerabilities by CVSS
- NVTs by CVSS
- NVTs by Family
- NVTs by QoD
- OVAL Definitions by Class
- OVAL Definitions by CVSS
- CPEs by CVSS
- CPEs by Severity Class

## Alerting Actions

### Constant monitoring and alerts

On every scan & task run, Nemasis finds and collects thousands of threats from the assets. However, a huge number of activities are not serious threats but will cause alarm or set off alerts, which can lead to a collapse for the security team investigating these alerts.

With Nemasis, most prominent events standout from the rest and requires immediate attention and investigation.

The alerting feature has following benefits.

- Constant monitoring and alerts proactively alerts team about the potential threats so problems can be tackled before turning into breaches.
- Alerts can be custom fitted for a wide variety of situations affecting systems, certificates, ports, services and software.
- It also continuously recognizes and proactively locates potential issues, instead of delayed response to incidents.
- MONITORING Assets: Determines which systems you want to monitor. You can recognize systems to monitor via ASSET TAGGING or by IP range.
- Set of Rules: Determines what (i.e. which events) you want to monitor. For example, you can define rulesets to only monitor for new ports on systems. These rule sets can be defined at a granular level so recipients get alerts only for events relevant to them.
- NOTIFICATIONS: Determines which individuals or teams receive alerts.

All alerts are displayed on the Alerts Dashboard, but you can define sub-division of alerts that go via email to specific individuals or groups. You can define different groups for different sets of alerts, and you can design individual alerts over different timeframes.

- Splunk Integration
- Event Logs
- Report Template Types

**Be alerted immediately about vulnerabilities, misconfigurations and other problems that can put you at risk.**

Some of these include:

- Undiscovered systems/OS: Detects when systems appear, disappear, or are running unexpected operating systems. Alerted recipients can immediately drill down to review all gathered data.
- Open Ports: Alerts that let you know about newly open ports which are common vectors for attack and exploit
- SSL CERTIFICATES Expiry: Detects certificates that have already expired, are soon-to-expire, or unknown, all of which are triggers to stop smooth operations of your network services and applications.
- REMEDIATION Incident TICKETS: Detects remediation tickets status such as tickets that are open, resolved or closed.
- SOFTWARE: Detects installation of new or unauthorized software, upgrades or downgrades of existing software, Software version, Software installation date and more.

### Splunk Integration

IT and Security teams need centralized logging and correlation tool.
Nemasis uses its vulnerability detection in alliance with other log data sources such as SPLUNK to provide greater context and acumen into the events happening within its environment

**Splunk Integration uses**

- Easily detect attacks, such as compromised credentials, phishing attacks and others.
- View security incidents by easily correlating assets, users and incidents.
- Conduct extensive investigations about each asset, e.g. ports, services, applications etc.
- Enable monitoring opportunities with deception technology for example (honeypots, honey credentials) to detect attacker behavior.

### Event Logs

Event Log analysis offers log management and real-time event correlation capabilities in a single console that help meet your SIEM needs, tackle security attacks and prevent data breaches.

## Report Template Types

Fast-track your compliance assessments of your network, web applications and infrastructure using industry-recommended best practices such as CIS Benchmarks, OWASP 2010 and PCI.

Use following report templates to achieve these.

- **OWASP 2010:** OWASP 2010 is committed to boost the security of web applications which spots the critical vulnerability from different facets such as Security Mis-Configurations, Cross-Site scripting attacks.
  Choose this report template to detect all types of vulnerabilities in OWASP 2010 and scan commercial and custom built Web applications selected by the user.

- **PCI:** PCI is used to protect and secure the cardholder details.
  Use this report template to generate a compliance report for payment card industry (PCI) assets. The report gives you all the security precautions to protect your assets.

- **CIS:** The Center of Internet Security (CIS) is a non-for-profit organization that cultivate their own Configuration Policy Benchmarks, or CIS benchmarks, that allow organizations to improve their security and compliance programs and posture. Use this template to generate report for CIS compliance.

## Data filtering options

Filter your report/dashboard content to create a unique view of your assets and vulnerabilities.

Filter your asset data by state (active/inactive), asset tags, as well as by various facets such as Service Names, Open Ports, and Service Protocols.

When dealing with networks of huge number of assets, it is necessary to concentrate on a specific subset. Filtered asset search filters helps you to search and look up for assets based on site, operating system, IP address, services, vulnerabilities, and asset name.

You can then save these results as a dynamic asset group for capturing, scanning, and reporting purposes.

The search filters allows you to find assets of most importance to you. This helps you to focus your remediation efforts and to handle the sheer quantity of assets running on a broad network.



### Configuration of asset search filters

Use search filter to choose and use the attributes of the assets that you are most interested in.

You can Add multiple filters for precise searches.

For example, you could build filters for a given IP address range, or a particular site, and then combine these filters to return a list of all the assets that simultaneously meet the specified criteria.

Use fewer filters to increase number of search results.

**The following asset search filters are available:**

- Filter by host type
- Filter by IP address
- Filter by asset name
- Filter by containers
- Filter by CVE ID
- Filter by IP address type
- Filter by last scan date
- Filter by mobile device last sync time
- Filter by open port numbers
- Filter by operating system name
- Filter by vulnerability CVSS score
- Filter by vulnerability exposures
- Filter by vulnerability risk scores
- Filter by vulnerability title
- Filter by software name
- Filter by presence of validated vulnerabilities
- Filter by CVSS risk vectors
- Filter by vulnerabilities assessed
- Filter by vulnerability category
- Filter by other IP address type
- Filter by operating system name
- Filter by PCI compliance status
- Filter by service name

### IPv4/IPv6 addresses

Nemasis allows security professionals to focus on the Highest Priority Issues.

Almost 95% of IPv4 address volume has been allocated already and with devices requiring one or multiple IPs, the transition to the next generation IPv6 is not far away.

With Nemasis you can

- Carry out an IPv6 discovery over an IPv4 network, and enable organizations to disable IPv6 devices in IPv4 networks as it can present a potential security risk in future.
- Build a vital asset group and find assets with known IPv4 addresses that once had undiscovered IPv6 addresses, creating significant efficiencies by automating traditional manual processes.
- Execute a report to show IPv6 enabled devices and scan for vulnerabilities.

## Configuration Audit Policy Management

Perform regular audits of configuration settings on your assets and verify that your assets meet a specific set of configuration standards.

Like vulnerability scans, policy scans are useful to standardize your security posture. They help to verify that your department is following the secure and correct configuration practices.

Our Policy Manager setting provides compliance checks for several configuration standards such as below.

- USGCB 2.0 policies
- USGCB 1.0 policies
- FDCC policies
- CIS benchmarks

## Detailed Events and Vulnerability Analysis Tools

### SCAP compliance

Nemasis abides with the Security Content Automation Protocol (SCAP) yardstick. SCAP is a collection of standards for expressing security data in standardized ways. The compliance is made mandatory by the US government and maintained by the National Institute of Standards and Technology (NIST).

It relies on multiple open standards and policies, including OVAL, CVE, CVSS and CPE policies for identification of vulnerability

The Common Platform Enumeration (CPE) based on the generic syntax for Uniform Resource Identifiers (URI), is a method for diagnosing operating systems and software applications.

The Common Vulnerabilities and Exposures (CVE) standard defines how the product should detect and identify vulnerabilities, which makes it easy for security products to exchange vulnerability data.

The Common Vulnerability Scoring System (CVSS) is an open framework for calculating vulnerability risk scores.

The OVAL acronym stands for Open Vulnerability and Assessment Language and is a main component of the SCAP standard. It is used to describe security vulnerabilities or desired configuration of systems.

## Distributed Scanner Support

If your organization has multiple offices located in different locations, it is best to setup scanners in the regions to best utilize network bandwidth. It also calls for a superior distributed and load-balanced scanning.

Nemasis provides Master-Slave support for this purpose and these scanners can be distributed throughout an Enterprise.

The Nemasis scanner features high speed discovery, configuration auditing, asset profiling, and vulnerability analysis of your security framework.

Hence we have Master scanner and multiple slave/remote scanners (scan engines). A user can individually configure a scan for the slave/remote scanners (scan engine) via the web interface of the master scanner depending on requirements and permissions.

### Advantages of using distributed scanning

Scanning Very Large / distributed Networks
Decreased Scan Time
Internal and External Perimeter Scanning
Less Stress on the Network Infrastructure

### Plan your Scan Engine Deployment

Your assessment of your security objectives/design and your environment, including your asset inventory, will help you plan how and where to deploy Scan Engines.

The setting up and deployment includes a security console and one or more Scan Engines to detect assets on your network, collect information about them, and test these assets for vulnerabilities.

### Distribute Scan Engines strategically

Distributed Scan Engines allow you to audit your network from the inside. They are mostly ideal for servers and workstations. Deploy these distributed Scan Engines anywhere on your network to obtain multiple views. This affability is valuable when it comes to scanning a network with multiple subnets, firewalls, and other forms of segmentation.

### Deploying Scan Engine Pools

A scan engine pool is a collective group of Scan Engines over which a scan job is distributed. Pools are assigned to sites in the same way an individual Scan Engine is assigned to a site. For gilt-edge performance, we recommend that pooled Scan Engines are located within the same network or geographic location.

## Data Analysis Output

XML Export, contains a consolidated scan data with minimal structure. The content can be easily parsed and can be easily integrated with 3rd party software like SIEM, CRM Analyzers, etc. It arranges and organizes data in a human-readable XML and is ideal for exporting it to other document formats.

You can also automatically send a report, as an email attachment, once a scan completes. Report formats available include PDF, TXT, RTF and HTML.

# Console Login Authentication

## LDAP/TNS Authentication

Use LDAP and TNS integration for authorized and monitored access.
You can either add TNS OR LDAP Authenticated User.
You can create one or more organizational users (security managers or custom roles) as per your requirements. If the LDAP service becomes unavailable, you can still log in with TNS-authenticated administrator/security manager.
Following are the functions performed using **LDAP** and **TNS** Authentication.

| Option | Remarks |
|---|---|
| Role | The role is assigned to the user. Administrator users can create Administrator or Security Manager user accounts and other accounts at their own privilege level or lower. |
| Group | The group where you want to assign the user account.<br>A user's group determines their access to Nemasis resources. |
| Asset | Assigns a user to an asset list for which the user is accountable. Allocating a user to an asset list makes it easier to detect who in a group or organization should be assigned tickets, notifications, and other tasks to resolve particular issues. |

**Note :**

**LDAP (Lightweight Directory Access Protocol):**

LDAP is an open and cross platform protocol used for directory service authentication. LDAP provides the intercommunication language that applications can use to communicate with other directory services servers.

Directory services store the users, passwords, and computer accounts.

Active Directory is a directory services implementation that provides all sorts of functionality like authentication, group and user management, policy administration and more.

Active Directory is one example of a directory service that supports LDAP. There are other directory services that support LDAP.

LDAP is a protocol that many different directory services and access management solutions can understand.

- LDAP is a directory services protocol.
- Active Directory is a directory server that uses the LDAP protocol.

**TNS (Transparent Network Substrate):**

The TNS (Transparent Network Substrate) connection type is an appropriate option for Oracle Database events/instances.

Oracle uses TNS services to handle communication within Oracle components. TNS uses the underlying protocol, which could be TCP/IP, SPX/IPX, DECNET, AppleTALK, etc.

The Oracle Transparent Network Substrate (TNS) facilitates simple inter-database communication.

# Dashboard Data Sources

**Vulnerabilities(CVE,NVT,CERT)**

Nemasis combines the information from the NVTs (Network Vulnerability Tests), CVEs (Common Vulnerability and Exposures) and the CERT and displays data comfortably in the web interface in dashboards.

**Note**

**NVTs**

These are the Network Vulnerability Tests. These tests test the target systems for potential vulnerabilities.

NVTs are test schedules that check for the proximity of vulnerabilities on target systems. You can configure which Network Vulnerability Tests (NVTs) can be tested against your hosts.

Nemasis displays dashboard data based on data gathered from NVTs.

**CVE**

Common Vulnerability and Exposures are vulnerabilities published by security professionals/researchers.

Nemasis has a diverse list of vulnerabilities to address through its vulnerability management solution. Each and every vulnerability has links to relevant groups like Mitre and other CVE Numbering Authorities. Nemasis uses these vulnerabilities for additional visibility.

**CERT**

Computer Emergency Response Team

The main task of CERT is the operation of warning and information service publishing information regarding new vulnerabilities and security risks as well as threats for IT systems.

## NIST/NVD

The CVEs, CPEs and OVAL definitions are published and made attainable by NIST as part of the National Vulnerability Database (NVD).

The National Institute of Standards and Technology (NIST) in the USA provides the National Vulnerability Database (NVD).

NVD is the U.S. government repository of standards-derived vulnerability management reference data. NVD provides information regarding security vulnerabilities, configuration settings, vulnerability impact metrics, technical assessment methods and more.

The NVD reference data supports security automation demeanor based on the Security Content Automation Protocol (SCAP).

The Security Content Automation Protocol is a combination of different interoperable standards. The SCAP protocol includes the following components:

- **Languages**
  - XCCDF: The Extensible Configuration Checklist Description Format
  - OVAL: Open Vulnerability and Assessment Language
  - OCIL: Open Checklist Interactive Language
  - Asset Identification
  - ARF: Asset Reporting Format

- **Enumeration**
  - CCE: Common Configuration Enumeration
  - CPE: Common Platform Enumeration
  - CVE: Common Vulnerabilities and Exposure
- **Scoring systems:**
  - CVSS: Common Vulnerability Scoring System
  - CCSS: Common Configuration Scoring System
- **Integrity**
  - TMSAD: Trust Model for Security Automation Data



## Data Management

**XML Report formats/XML DATA EXPORTS**

Reports generated in XML formats make it possible to integrate reports with third-party systems.

XML Export contains consolidated scan data with minimal structure. The contents can be parsed so that other systems can use its information.

XML arranges and organizes data in a human-readable format and is ideal for exporting to other document formats.

Customize reports to sort by vulnerability or asset, create Executive Summaries, or compare scan reports and use native XML data exports.

Configure your report and download it in desired text format next time you login to the console.

Additionally, you can configure the report date/time/period and assets or target group for which vulnerability data is displayed.

## Credential Management for Authenticated Scans

An authenticated scan provides more vulnerability data/details on the scanned system. An authenticated scan scans target from both sides - outside via the network and inside via a valid user login.

Before running scans, you must first define credentials for the devices and applications in the network that should be managed.

**Nemasis provides following types of authenticated scans**

**SNMP**

The SNMP authentication for a vulnerability scan on network devices is based on a password called a "community string".

Each "community string" can be configured inside the SNMP daemon that runs on the device to have access to distinct “Views" of the information available on the MIB.

**SMB**

It iterates through the list targets (IPv4/hostnames) and requests both SMB version support and NetBIOS information from the targets.

Registry, software versions and patch level are accessible with this authentication.

**SSH**

This credential scan is carried out for Unix/Linux systems.

Nemasis performs credential scans on assets that authenticate users with SSH public keys. This process is known as asymmetric key encryption, involves the creation of two related keys, random numbers.

- A public key that any entity can use to encrypt authentication data.
- A private key that trusted entities can use to decrypt the data encrypted by its paired public key.

**ESXi**

Nemasis uses this access to test VMware ESXi servers locally. By default, ESXi users are reserved to read-only roles.

## User Access Control

Cogent use of scan information depends on how your organization analyzes and distributes it, who gets to see it, and for what reason. Managing access to information in the application involves creating target asset groups and assigning roles and permissions to users.

Nemasis allows for the definition and the management of different users with different roles and permissions. The first user, an administrator, is created by default. This user allows the login and management of additional users.

Nemasis user management supports a role based permission concept when accessing the web interface. Multiple roles are already set up by default. Additional roles can be created. The role defines which options of the web interface can be viewed and modified by the user. Read and write access can be assigned to roles separately.

In addition to the roles, Nemasis user management supports groups. This serves mainly for logical grouping. Groups and roles can be used to assign permissions to several users at once. Distributed Admin teams for large networks can use these benefits.

## Network Scan

Nemasis performs following Network Scans.

**TCP Scans/SCANNER**

TCP ports are the endpoints of logical connections through which networked computers carry on conversations. Well Known Ports are those most commonly found to be open on the Internet.

Each vulnerability check may add a set of ports to be scanned. Various back doors, trojan horses, viruses, and other worms create ports after they have installed themselves on computers. Rogue programs and hackers use these ports to access the compromised computers. These ports are not predefined, and they may change over time. Output reports will show which ports were scanned during vulnerability testing, including maliciously created ports.

Various types of port scan methods are available as custom options. Most built-in scan templates incorporate the Stealth scan (SYN) method, in which the port scanner process and sends TCP packets with the SYN (synchronize) flag. This is the most reliable method. It's also fast. A SYN port scan is approximately 20 times faster than a scan with the full-connect method, which is one of the other options for the TCP port scan method.

**WMI Scanner**

This scan is intended for Windows-based systems and requires authentication credentials. A WMI based scan determines only open ports, thus ignoring any port ranges specified.

**UDP Scanner**

This option engages Nemasis built-in UDP scanner to identify open UDP ports on the targets. This scan works by sending a UDP packet to every targeted port.

**SSH Scanner**

This scan is intended for Linux/Unix-based systems and requires authentication credentials.

On Unix/Linux systems and supported network devices, Nemasis uses Secure Shell (SSH) protocol based programs for host-based checks. This mechanism encrypts the data in transit to protect it from being viewed by sniffer programs.

On Linux systems and supported devices, Nemasis uses Secure Shell (SSH) protocol based programs (e.g., OpenSSH, Solaris SSH, etc.) for host-based checks.

**SNMP scanner**

Nemasis uses the Simple Network Management Protocol (SNMP) to make version and information queries to routers and switches.

**HTTP scanner**

It checks for HTTP servers, web server options and server configuration.

**SMB scanner**

Server Message Block (SMB) is a file-sharing protocol that allows computers to share information across the network. Providing this information to Nemasis will allow it to find local information from a remote Windows host. For example, using credentials enables Nemasis to determine if important security patches have been applied.

**LDAP scanner**

LDAP-supportive Microsoft technology that automates centralized, secure management of an entire network's users, services, and resources.

The Lightweight Directory Access Protocol (LDAP) is an industry standard protocol for accessing and maintaining directory services across an organization. Once connected to an LDAP server, Nemasis administrators can add users straight from their directory and these users can authenticate using their directory credentials.

## Report options

Note: Patching vulnerabilities: This is the process of getting patches -- usually from the vendors of the affected software or hardware -- and applying them to all the affected areas in a timely way. This is sometimes an automated process, done with the patch management tools.

**CVSS SCORE**

The charts on the Vulnerabilities page display your vulnerabilities by CVSS score and exploitable skill levels. The CVSS Score chart displays how many of your vulnerabilities fall into each of the CVSS score ranges. This score is based on access, complexity, authentication, and impact on data. The score ranges from 1 to 10, with 10 being the worst, so you should prioritize the vulnerabilities with the higher numbers.

**Patch**

Combine patch management capabilities of your patch management system with the scan data from Nemasis, and apply patches to vulnerable assets without delay.

Use Nemasis to Verify High Severity Vulnerabilities and patch or fix them without delay.

• Scan Policy management and schedules

**Microsoft patch**

Using Remediation Projects you can build dynamic projects that track vulnerabilities related to Microsoft patches as they are identified in your environment.

**NVT**

You can configure which Network Vulnerability Tests (NVTs) can be tested against your hosts. Nemasis displays report data based on data gathered from NVTs.

**Port/ Protocol/Service**

You can SPECIFY AND generate reports based on Service Names, Open Ports & Service Protocols.

## Scan Policy management and schedules

### Create, setup and define scan/policies templates.

Define following settings /configurations such as name of the scan, assets to be scanned, target groups, whether the scan is scheduled, and which users has access to the scan. Assets in the target group are used as scan targets.

Targets Groups: Specify one or more target group to be scanned.

By default, scans are not scheduled. You can configure scan templates and enable settings to schedule scans on daily, weekly monthly or on yearly basis.

- **Daily:** Schedule scans to trigger on a daily basis, at a specific time
- **Weekly:** Schedule scans to trigger on a persistent basis, by time and day of week,
- **Monthly:** Schedule scans to trigger every month, by time and day or week of month.
- **Yearly:** Schedule the scan to trigger every year, by time and day

**Email Notification**

**Email Recipient(s):** Specify zero or multiple email addresses that should to be alerted when a scan completes and the results are available.

Use settings and assign various permissions to groups and individual users. When you assign a permission to a group, that permission applies to all users within the group.

You can set following permissions/settings

No Access

Users and groups set to No Access mode cannot interact with the scan in any possible way. Hence when a scan or policy is created, no other users or groups have access to it.

Visibility

Users and groups set to visibility mode can view the results of the scan.

Authority mode

Users and groups set to authority mode can launch, pause, and stop a scan, as well as view its results.

Configure

Users and groups set to configure mode can modify the configuration of the scan in addition to all other permissions.

Nemasis allows you to configure the scans or policies and use authentication credentials during scanning. Using configured credentials allows Nemasis to perform a wide variety of checks that result in more accurate scan results.

## Report Output Formats

Choosing correct format is important in report creation/generation.

Formats not only influence how reports appear and are utilized, but they also can have some effect on what information appears in reports.

These formats make report data easy to distribute, open, and read immediately:

- Text can be opened, viewed, and edited in any text editing program.
- PDF can be opened and viewed in Adobe Reader.
- HTML can be opened and viewed in a Web browser.
- RTF can be opened, viewed, and edited in Microsoft Word.

XML Report formats/XML DATA EXPORTS

Reports generated in XML formats make it possible to integrate reports with third-party systems.

XML Export, contains a consolidated scan data with minimal structure. The contents can be parsed so that other systems can use its information.

XML arranges and organizes data which is human-readable XML and is ideal for exporting to other document formats.

**Copyright and other Intellectual Property Rights:**



**Disclaimer:**
MWTI is as diligent as possible in compiling and updating the information present in its fact files. However, MWTI does not guarantee the completeness of the information provided herein. Equally, MWTI does not guarantee that this information is up to date. For questions concerning Nemasis and other products, their specifications and their utilization, please refer a qualified expert of MWTI.

**Reservation concerning changes:**
All information, representations, links or other messages may be changed by MWTI at any time without prior notice.

**Exclusion of liability:**
The information on this data sheet is provided "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose or non-infringement of intellectual property rights.

**Specifications concerning products and applications:**
The specifications provided in this document do not constitute recommendations or guidance for decisions concerning the purchase of technical products. The information on provided by MWTI only serves for information purposes. It may be subject to change at any time without prior notice to the user

Therefore, technical specifications concerning products of MWTI and information about applications related to those products offered may differ. Binding specifications and information are only those in the instruction manual of the product purchased by the client.

In these matters – particularly but not exclusively concerning the question whether a product of MWTI fulfils the needs of the customer, the required features, technical specifications and applications – you should obtain advice from a qualified expert of MWTI or one of our official distributors. All specifications are subject to change without notice.