Nemasis

Vulnerability Management Suite

MicroWorld Technologies's Nemasis is a Vulnerability Management Suite which assists in implementing a comprehensive GRC (Governance, Risk Management, and Compliance) strategy for managing an organization's overall governance, risk, and compliance with regulations. Nemasis integration with the GRC strategy helps in managing security and compliance to reduce the overall business risk. Nemasis GRC offers various advantages like eliminating redundant cost, performing vulnerability scan in depth, optimizing the investment, securing the business reputation, asset discovery, and more.

Nemasis is used to scan the network vulnerabilities such as open ports, running applications on each system, and active services. Nemasis generates many types of reports based on NIST, OVA, World bodies, and more. Nemasis is supported by almost every platform, systems, applications, databases, devices, and browsers.

Nemasis Key Features

Passive Vulnerability Scanner *

Nemasis 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 demeanor in a non-intrusive manner. It continuously monitors the assets, such as servers, desktops, laptops, network devices, web apps, virtual machines, mobile, tablets, cloud-based assets, and more, that use IP protocol to determine topography, services, and vulnerabilities. It also tracks the network changes within your organization's infrastructure. Nemasis provides OS fingerprinting, Service fingerprinting, database password management, and more configuration (Limited Configuration) for Windows platform is currently available. Nemasis inbuilt Passive Vulnerability Scanner has a capability that will allow you to provide the discovery and the network topology. For more technical details https://www.nemasisva.com/resource-library/Nemasis-Passive-Scanner.pdf

Compliance and Configuration Assessment

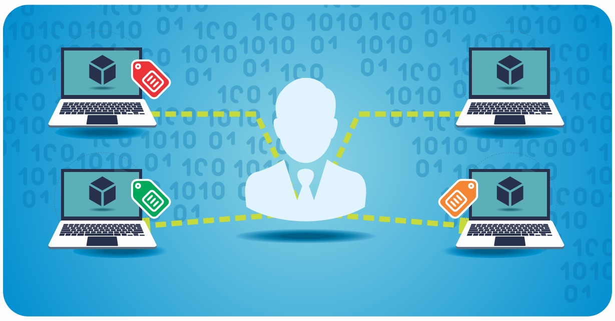
Nemasis allows fast-track the compliance assessments of network, web application, and infrastructure according to industries standard and best practices such as Center of Internet Security (CIS), Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), OWASP 2010, and many more. Each compliance report template has its own uniqueness in assessment, for example, PCI is specifically used for protecting and securing the cardholder details. Use this report template to generate a compliance report for PCI assets and the report gives you all the security precautions to protect your assets. It also performs and generates a unified report of configuration and compliance assessment. Nemasis not only has a compliance report template but also allows customizing the reports according to specific business needs which makes it stand out.

Dashboard Data Sources

Nemasis combine the information from the Scan plugins, CVE (Common Vulnerability and Exposures), and the CERT and displays real-time data easily in the web interface in dashboards. It displays the data on the dashboard based on the data gathered from the Scan plugins. Nemasis has a long list of vulnerabilities which is linked to relevant groups like Mitre and other CVE Numbering Authorities and uses them for further visibility.

Asset Tagging *

Nemasis Asset tagging feature provides a scalable and flexible way to organize the assets in the network to identify and track data or events of that particular



asset. It also ensures that the scans and reports are always synchronized with the changing business need.

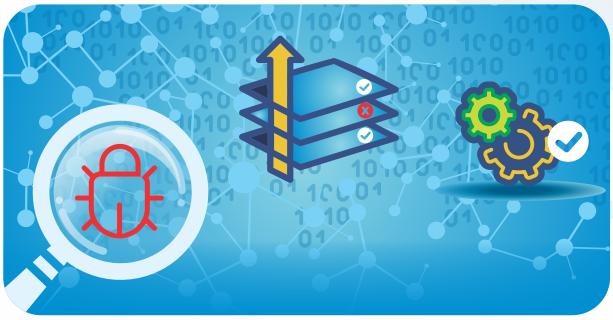
Internal and External Scanning

The only reason, Nemasis suggest using both internal and external vulnerability scan is to understand the scope of vulnerabilities inside and outside your organization, as threats can emanate from anywhere. The internal scan assesses your network security from inside your firewall, which can be both with/without credentials. The external scan is performed remotely from outside, which is normally non-credential/unauthenticated scans.

Credential Management for Authenticated Scans

An authenticated Scan scans the target network from both, external via the network and from the internal via a valid user login. Nemasis provides an SNMP authentication scan which mostly scans network devices, SMB authentication scans which checks the patch level and locally installed software for Windows, SSH authentication scans which checks for patch-levels on UNIX- and Linux-based systems, and ESXi authentication scans which tests the VMware ESXi servers locally.

Remediation



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. Using Remediation Projects you can build dynamic projects that track vulnerabilities related to Microsoft patches as they are identified in your environment. Nemasis allows you to report the vulnerability based on various options such as CVSS, Scan plugins, Port/Protocol/Services, and Patches like OS patches, application patches, and more. For example, Using patch option Nemasis can leverage credentials for the patch management systems to perform patch auditing on systems for which credentials may not be available to the Nemasis scanner. Scan plugins are tested against the host and Nemasis display the data reports gathered from Scan plugins.

Scalability and Flexible Deployment

The systems and network infrastructure of each organization are distinct. Nemasis provides you scalable and flexible deployment option based on the requirement (volume of scanned IP's). To increase the speed and accuracy of your assessments, the ability to optimize your VMS according to the specific needs of your organization is very important. As your organization develops, your VM solution should be able to grow quickly and easily just by adding scan engines to your current deployment at minimal or no additional cost. Nemasis helps to scale your VM simply by adding Scan engines to your current deployment, and additionally, it helps you to configure the concurrent Scan Plugins and Number of hosts with respect to a single scan.

Distributed Scanner Support *

Nemasis provides Master-Slave support for the purpose of superior distributed and load-balanced scanning and these scanners can be distributed throughout an entire Enterprise. The Nemasis scanner features high-speed discovery, configuration auditing, asset profiling, and vulnerability analysis of your security framework. Distributed scanning helps to scan the large/distributed network in very less time by putting less stress on the network infrastructure.

Discovery

Before you start scanning the network, you should know what assets you have so that you can manage the risk easily. Nemasis helps you to provide a range of IPs to scan them using Host Discovery Scan option and also asset can be tagged to owner/groups.

Data Filtering Options

Asset data can be filtered by state (active/inactive), asset tags, service names, open ports, and service protocols. When dealing with a large number of network assets, it is necessary to filter out the assets on specific conditions or subsets. This helps you to focus your remediation efforts and to handle the assets running on a complex or distributed network. 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 meet the specified criteria. Nemasis provide a large number of search filters based on host, service and software names, CVE ID, IP address, PCI compliance status, and others.

Network Scan

Nemasis supports various types of network scanner such as TCP, WMI, UDP, SSH, SNMP, HTTP, SMB, and LDAP. Each of the scanners performs different sets of scanning. For example, TCP scanner scans all the ports that are vulnerable for attacks using Stealth scan (SYN) method while HTTP scanner checks for HTTP servers, web server options, and server configuration.

Audit Trail

Nemasis audit trail provides information to analyze the entire trail of events to its origin. It includes user activities, access to data, login attempts, or administrator activities. Admins can view and export the report to gain deeper insights of any malicious events that may have occurred.

Reporting

The reports are automatically sent as an email attachment once the scan is completed. Reports are available in different format such as HTML, PDF, TXT, RTF, and XML. These reports are interactive by nature when viewed on the Nemasis console. Reports generated in XML formats make it possible to integrate reports with third-party software like SIEM, CRM Analyzers, and more. Reports generated in CSV format can be exported as XLS, where further filtering such as Severity, Software, protocol, and many more can be done. Remediation report validation can be done by re-scanning the whole network or system. Nemasis helps you to customize your reports according to the specific need of the organization, for example, based on tagged asset groups, severity, and many more.

Alerting Actions

Nemasis identifies thousands of threats from the endpoints of the network by constant monitoring. However, huge numbers of activities are not serious threats but will cause alarm or set off alerts, which help security teams to proactively be alerted about potential threats so problems can be tackled before turning into breaches. Alerts can be customized according to the need of the user depending upon the risks such as open ports, SSL certificates, and unwanted services and software. You can define different groups for different sets of alerts, and you can design individual alerts over different timeframes.

Logging and Monitoring

Nemasis detects vulnerability in alliance with other log data sources such as SPLUNK, Office CRMs, which allow organizations to analyze, search, monitor, and visualize big data coming from websites, networks, sensors, applications, servers, and mobile assets. Splunk integration helps Nemasis to easily detect attacks, view security incidents, conduct extensive investigations, enables monitoring opportunities with deception technology. You can even get the detailed log of vulnerability, compliances, configurations, and many more through Nemasis dashboard, single log, and separate log. These logs can be exported in various formats like PDF, XML, text, and more. Also, these logs can be back up automatically in case of future use.

Prioritization

Nemasis dashboard and reports offer a granular representation of vulnerabilities with respect to the CVSS and also provides the total risk scenario for any scan. It also provides statistical data based on days/month/year in a real-time dashboard. False positive function is also provided as a temporal metric for Vulnerabilities which are accepted risk scenarios by the organization and can be defined in the range of Low/Medium/High/Log/False Positive. Nemasis also provides host tagging, which is available based on Owner/Groups wherein, the criticality levels can be defined that will publish the priorities based on the

final score in a report. Nemasis also provide our own internal threat intelligence gathering, which can be prioritized based on their criticality level.

Audit Policy Management

Performing regular audits of configuration settings on your assets may be necessary for your organization. You may need to verify that your assets meet a specific set of configuration standards such as USGCB 2.0 policies, USGCB 1.0 policies, FDCC policies, CIS benchmarks.

Management and Administration: (Password Policy Management will be releasing soon)

Nemasis Dashboards are interactive by nature and provide specialized views of your network in a customizable and drag-and-drop interface along with the real-time data. You can add, delete, and move the dashboard according to your preferences, and choose the order in which they should appear in the module. Nemasis use components such as Scan Display, Asset Display, SecInfo Display and many more to generate multiple dashboards.

Agent-based Scanning: (Agent-based solution will be releasing soon) *

Nemasis, for now, provides the agentless solution. In the near future, Nemasis agent-based solution will be well suited for performing power management tasks. Agents need to be easy to install and lightweight so as not to take up much network bandwidth. This is ideal for distributed networks with remote locations that have limited bandwidth, based on pull technology. It will enable in-depth scanning of a system without providing system credentials, and it performs patch management and asset management tasks on disconnected machines.

Container Assessment: (This feature will be releasing soon) *

Nemasis VMS will identify and prevent vulnerabilities throughout the entire application lifecycle while prioritizing risk. It will help the developers to integrate VM into their CI process, while security teams want to continuously monitor, identify, and prevent risks to all the containers, images, and hosts in their infrastructure.

Integration: (Hybrid, that is, agent-based will be releasing soon) *

The virtual and cloud asset's risk to safeguard the environment is identified and assessed dynamically by our Nemasis on-premise solution. While Nemasis hybrid solution has the capabilities to perform the host scanning with the help of access levels granted by the cloud services provider. Nemasis integrate with Syslog, Splunk, and other orchestration tools which allow organizations to analyze, search, monitor, and visualize big data coming from websites, networks, sensors, applications, servers, and mobile assets. Nemasis will also integrate with the enterprise ticketing system and RESTful APIs, which can be custom configured according to the organization's specific need.

Updates, Support, and License

Nemasis provides the application update both automatically and manually. There are regular updates on the new vulnerability that are being added to your database. The License provided by Nemasis is based on the number IPs within the organization and it covers only hotfixes, minor or major updates but also the new version of the solution. We offer 24x7 free online technical support to our customers through e-mail and live chat. We also provide free telephonic support to our customers during our business hours. The Nemasis technical support team is available round the clock to assist you with your queries. If you have any queries, suggestions, and comments regarding Nemasis, please write to us at support@nemasisva.com.

Note: * Features are not available in the Nemasis Pro