CHAPTER 10

Configuring Vulnerability Assessment Devices

Revised: November 10, 2007

Vulnerability assessment (VA) devices provide MARS with valuable information about many of the possible targets of attacks and threats. They provide information useful for accurately assessing false positives. This information includes the operating system (OS) running on a host, the patch level of the OS, the type of applications running on the host, as well as detailed logs about the activities occurring on that host.

Note When a vulnerability assessment device is deleted from the MARS web interface, its corresponding vulnerabilities and open ports are not immediately removed from the MARS database. MARS continues to use this event information for false positive analysis until a successful vulnerability assessment import occurs. Upon completion of the new import, the historical event information associated with the deleted device is removed from the database.

This chapter explains how to bootstrap and add the following VA devices to MARS:

Foundstone FoundScan 3.0

To configure MARS to pull data from FoundScan, you must perform three tasks:

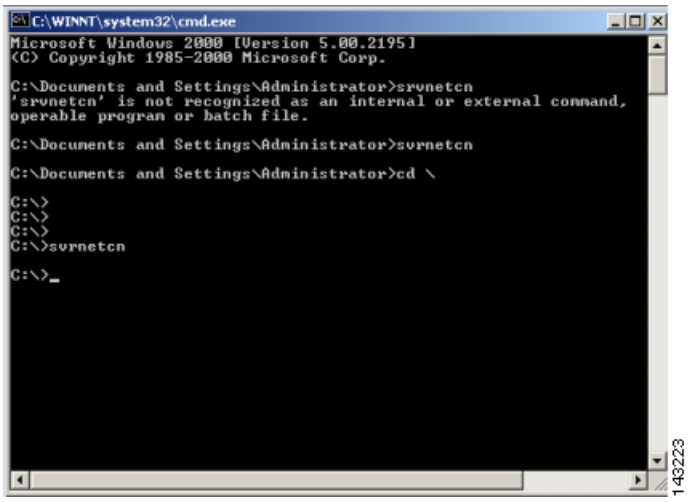
- Configure Foundstone FoundScan to correlate the required data, ensuring that the data is current.
- Add the Foundstone FoundScan server to MARS using the web interface.
- Schedule the interval at which the Foundstone FoundScan server data is pulled by MARS.

This section contains the following topics:

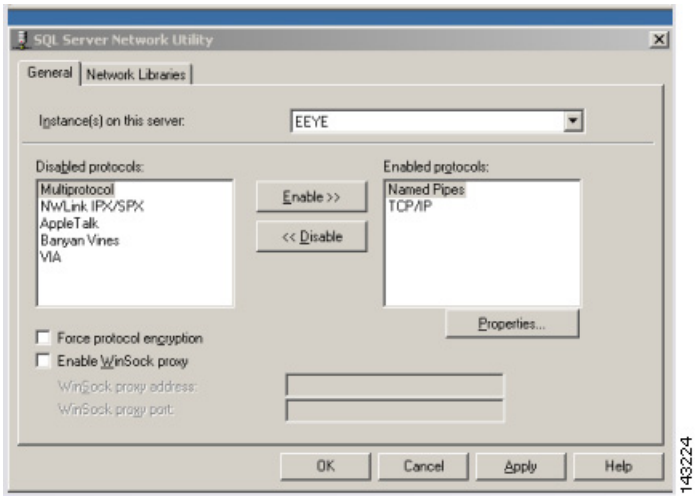
Configure FoundScan to Generate Required Data

To configure FoundScan to provide data to MARS, follow these steps:

Step 1 Run command **svrnetcn** at the DOS prompt on the host where FoundScan is installed.



Step 2 In the SQL Server Network Utility dialog box, enable TCP/IP by moving **TCP/IP** from the Disabled Protocols list to Enabled Protocols list.



Step 3 Verify that the **Force protocol encryption** checkbox is cleared.

Step 4 Click **Apply**.

Add and Configure a FoundScan Device in MARS

To add a FoundScan device in MARS, follow these steps:

Step 1 Select **Admin > Security and Monitor Devices > Add**.

Step 2 Select **Add SW Security apps on a new host** or **Add SW security apps on existing host** from the Device Type list.

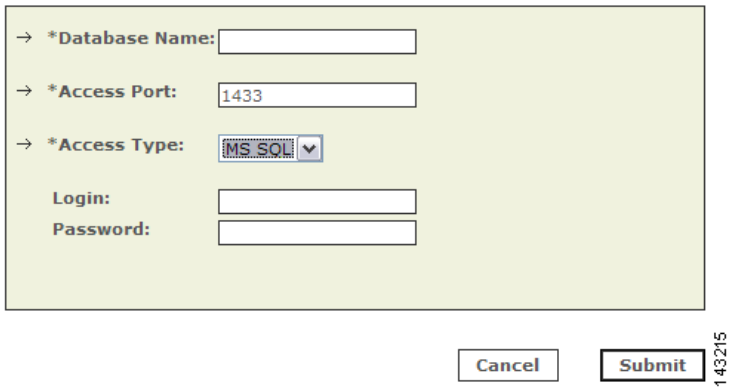
Step 3 Enter the device name and IP addresses if adding a new host.

Step 4 Click **Apply**.

Step 5 Click the **Reporting Application** tab

Step 6 From the Select Application list, select **Foundstone FoundScan 3.0**

Step 7 Click **Add**.



Step 8 Enter the following information:

- **Database Name—**The name for this database.
- **Access Port—**The default access port is 1433.
- **Access Type**—Verify the value is MS SQL.
- **Login—**The login information for the database.
- **Password—**The password for the database.

Step 9 Click **Submit**.

Step 10 Click **Apply**.

Once you activate this device (click Activate in the web interface), you must define the schedule at which MARS should pull data from it. For more information, see Scheduling Topology Updates, page 2-40.

eEye REM 1.0

To configure MARS to pull this REM data, you must perform three tasks:

- Configure eEye REM to correlate the required data, ensuring that the data is current.
- Add the eEye REM server to MARS using the web interface.
- Schedule the interval at which the eEye REM server data is pulled by MARS.

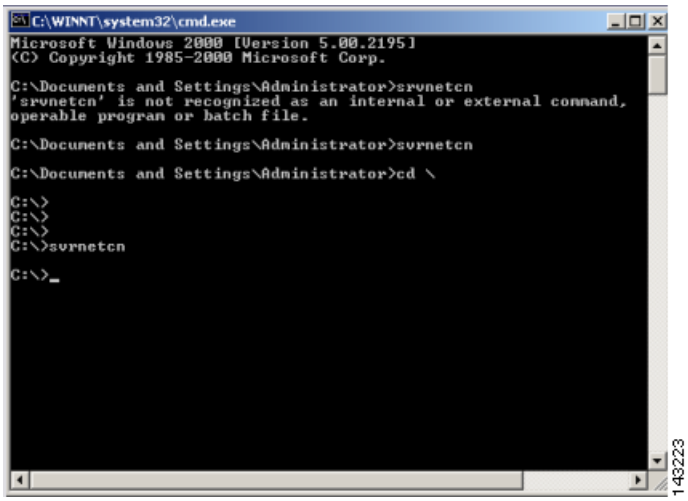
This section contains the following topics:

- Add and Configure the eEye REM Device in MARS, page 10-5

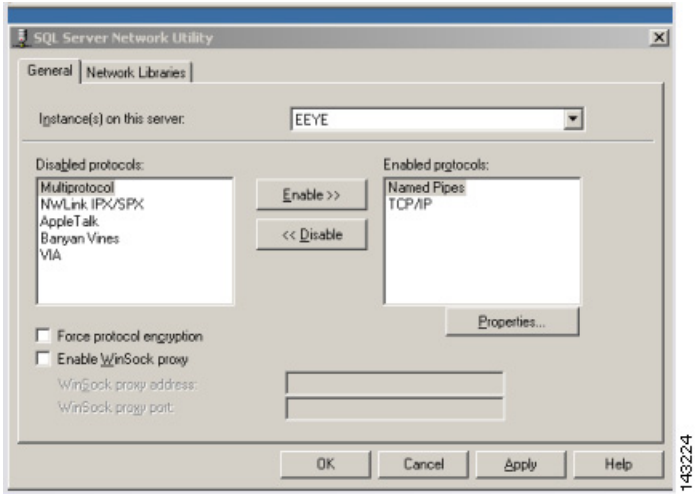
Configure eEye REM to Generate Required Data

To configure eEye REM to provide the correct data to MARS, follow these steps:

Step 1 Run command **svrnetcn** at the DOS prompt on the host where eEye REM 1.0 is installed.



Step 2 In the SQL Server Network Utility dialog box, enable TCP/IP by moving **TCP/IP** from the Disabled Protocols list to Enabled Protocols list.



Step 3 Click **Apply**.

Add and Configure the eEye REM Device in MARS

To add the eEye REM device in MARS, follow these steps:

Step 1 Select **Admin > Security and Monitor Devices > Add**.

Step 2 Select **Add SW Security apps on a new host** or **Add SW security apps on existing host** from the Device Type list.

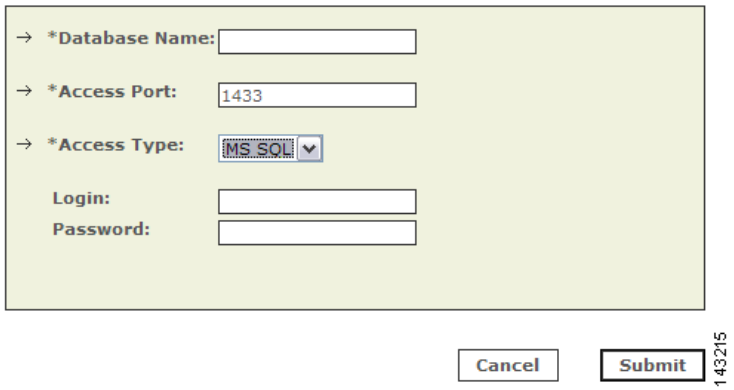
Step 3 Enter the device name and IP addresses if adding a new host.

Step 4 Click **Apply**.

Step 5 Click the **Reporting Applications** tab.

Step 6 From the Select Application list, select **eEye REM 1.0**.

Step 7 Click **Add**.



Step 8 Enter the following information:

- **Database Name—**The name for this database.
- **Access Port—**The default access port is 1433.
- **Login—**The login information for the database.
- **Password—**The password information for the database.

Step 9 Click **Submit**.

Step 10 Click **Apply**.

Once you activate this device (click Activate in the web interface), you must define the schedule at which MARS should pull data from it. For more information, see Scheduling Topology Updates, page 2-40.

Qualys QualysGuard Devices

In MARS, a QualysGuard device represents a specific report query to the QualysGuard API Server, which is the central API server hosted by Qualys. The only one that you configure to work with MARS is the QualysGuard API Server. You want to ensure that the QualysGuard API Server can provide reports about the devices on the network segments that you are monitoring with the MARS Appliance, as each MARS Appliance is responsible for identifying false positives for the network segments it monitors.

If you have a subscription to the QualysGuard service, MARS can pull VA data from the QualysGuard database using the QualysGuard XML API. To configure MARS to pull this data, you must perform three tasks:

- Configure QualysGuard to collect the required data, ensuring that the data is current.
- Add the QualysGuard device that represents a report query to MARS using the web interface.
- Schedule the interval at which the QualysGuard device data is pulled by MARS.

Note If a proxy server resides between the QualysGuard server and the MARS Appliance, the settings defined on the Admin > System Parameters > Proxy Settings page are used. For more information, see Specify the Proxy Settings for the Global Controller or Local Controller, page 6-20 of the "Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System, Release 4.2.x."

This section contains the following topics:

Configure QualysGuard to Scan the Network

MARS uses the QualysGuard XML API and password-based authentication over SSL (TCP port 443) to retrieve scan reports from the QualysGuard API Server. As such, you do not need to configure the QualysGuard server to accept connections from MARS. The only required configuration is that you have an active account and Qualys subscription that is configured correctly to scan your network.

By default, MARS assumes that you want to retrieve the most recent scan report saved on the QualysGuard server. Depending on the number of IP addresses analyzed, the QualysGuard scan takes from a few seconds to several minutes. You need to estimate this time so that you can schedule automated scans of your network with a frequency that ensures a recent saved scan report is available. Using the QualysGuard administrative interface, you can determine how long a scan takes and set the schedule accordingly.

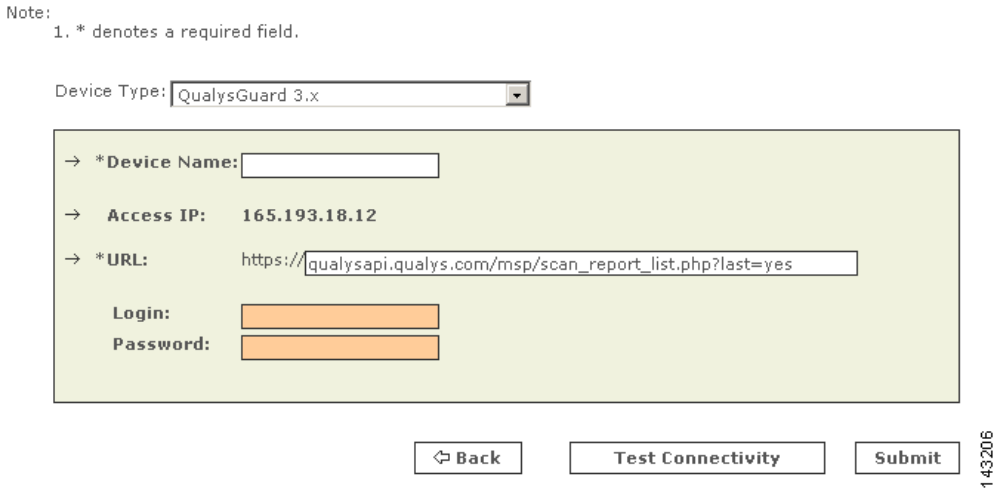
Add and Configure a QualysGuard Device in MARS

Adding an internal QualysGuard device as a reporting device entails identifying the QualysGuard API Server, which is the central API server hosted by Qualys, from which the reports are pulled and providing credentials that MARS can use to log in to the device to pull the reports. You can specify whether you want to pull saved scan reports that are run on a schedule or whether you want to initiate and retrieve an on-demand scan report. Each reporting device identifies a unique query to the QualysGuard API Server.

To add a QualysGuard device, follow these steps:

Step 1 Select **Admin > Security and Monitor Devices > Add**.

Step 2 Select **QualysGuard ANY** from the Device Type list.



Step 3 Enter the name of the Qualys device in the Device Name field.

This name is used to identify the Qualys device uniquely within MARS. It is used in reports and query results to identify this device.

The IP address field is read only. The value is also fixed at 165.193.18.12, which is significant because you can only define one schedule for pulling all report queries defined as Qualys devices on the Local Controller. However, you can define unique schedules across different Local Controllers. For more information, see Scheduling Topology Updates, page 2-40.

Step 4 Enter the URL that identifies the device and report type in the URL field.

The URL provides the following information:

- **Server**. Identifies the server from which the report should be pulled. This value can be specified as a hostname or IP address that identifies the primary Qualys server.
- **Report type**. Real-time vs. Last Saved. The default value.
  - *Real-time Report*. qualysapi.qualys.com/msp/scan.php?ip=[*addresses*]

    The *addresses* attribute specifies the target IP addresses for the scan request.

    IP addresses may be entered as multiple IP addresses, IP ranges, or a combination of the two. Multiple IP addresses must be comma separated, as shown below:

    ```
    123.123.123.1,123.123.123.4,123.123.123.5
    ```

    An IP address range specifies a start and end IP address separated by a dash (-), as shown below:

    ```
    123.123.123.1-123.123.123.8
    ```

    A combination of IP addresses and IP ranges may be specified. Multiple entries must be comma separated, as shown below:

    ```
    123.123.123.1-123.123.123.5,194.90.90.3,194.90.90.9
    ```

    Note You must use a Scanner Appliance to scan private IP addresses on your internal network.

  - *Last Saved Report*. qualysapi.qualys.com/msp/scan_report_list.php?last=yes

Step 5 Enter the username of the account that MARS will use to access the Qualys device in the Login field.

Step 6 Enter the password that corresponds to the account identified in Step 5 in the Password field.

Step 7 (Optional) To verify that the settings are correct and that the MARS Appliance can communicate with this Qualys device, click **Test Connectivity**.

If you receive error messages during this test, refer to Troubleshooting QualysGuard Integration, page 10-9.

Step 8 To add this device to the MARS database, click **Submit**.

Once you activate this device (click Activate in the web interface), you must define the schedule at which MARS should pull data from it. For more information, see Schedule the Interval at Which Data is Pulled, page 10-8.

Schedule the Interval at Which Data is Pulled

Once you activate one or more Qualys devices (where each device represents a report query run on the QualysGuard API Server), you must define the schedule at which MARS pulls data from them. The schedule, or update rule, that you define is the same for all Qualys devices. This update rule is based on the fixed IP address of 165.193.18.12, which is the Qualys Access IP. When you define an update rule using this address, all Qualys devices are updated based on that schedule. Even if you have more than one Qualys device on your network, you cannot stagger when MARS queries those Qualys devices. However, you can define unique schedules across different Local Controllers.

For more information on the broader use of update rules, see Scheduling Topology Updates, page 2-40.

To define the rule by which all Qualys devices will be discovered, follow these steps:

Step 1 Click **Admin > Topology/Monitored Device Update Scheduler**.

The Topology/Monitored Device Update Scheduler page displays.

Step 2 Click **Add**.

Step 3 Enter *Qualys Devices* or another meaningful value in the Name field.

This name identifies the rule in the list of rules that appears on the Topology/Monitored Device Update Scheduler page.

Step 4 Select the **Network IP** radio button, and enter 165.193.18.12. and 255.255.255.255 in the Network IP and Mask fields respectively.

Step 5 Click **Add** to move the device into the selected field.

Step 6 In the Schedule table, select **Daily**, and select a time value from **Time of Day** list.

We recommend that you pull this data daily, during off-peak hours, however, you can define any interval required by your organization.

Step 7 Click **Submit**.

The update rule appears in the list on the Topology/Monitored Device Update Scheduler page.

Step 8 Click **Activate**.

Tip To perform this discovery on demand, select the check box next to the rule you just defined and click **Run Now**.

Troubleshooting QualysGuard Integration

Table 10-1 identifies possible errors and likely causes and solutions.

Table 10-1 Error Table for QualysGuard and MARS Integration

Error/Symptom	Workaround/Solution
Test connectivity failed. Click the View Errors button for more information. Server unavailable.	This error means that MARS was unable to connect to the Qualys device. Four possible issues can account for this message: • You have entered an invalid hostname or IP address in the URL field. Verify the value was entered correctly. • The traffic may be blocked by either a proxy server or firewalls and gateways on your network. Enable SSL traffic (TCP port 443) to traverse between the MARS Appliance and the Qualys device. Enter the correct settings for your proxy server on the Admin > System Parameters > Proxy Setting page.
Fail to parse scan report.	This error means that MARS was unable to parse the scan report that it pulled from the Qualys device. Two possible issues can account for this message: • Data corruption on the QualysGuard device. • Format changes to the report due to an issue on the QualysGuard device or due to a software upgrade on the QualysGuard device. Verify that the QualysGuard device is running a supported version and that the device data is not corrupted.
Invalid user credentials.	This error means that MARS was unable to authenticate to the Qualys device. Two possible issues can account for this message: • The provided login credentials are incorrect. Verify these values were entered correctly, and verify that the provided account has sufficient privileges. • Your account has expired. Renew your subscription services with Qualys.
Test connectivity failed for qualys. Unknown host: qualysapi.qualys.com Please make sure that, • Proxy settings are configured correctly, If there is no direct connection exists from CS-MARS to Qualys server • The hostname specified in the URL string is correct • Login name and Password is valid.	Make sure that the DNS server is configured correctly for the MARS Appliance. For more information on these DNS settings, see Specifying the DNS Settings, page 5-16.