Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Configuring and Tuning Cisco CS-MARS

ttempting peer-to-peer file sharing, but the firewall log shows those packets were dropped [2]. CS-MARS would mark this as a System Identified False Positive. In another case, a Windows RPC DCOM Overflow might be seen by an IDS system, but the target vulnerability scan shows the host is not running an affected version of Microsoft Windows another false positive (at least for the attack itself). From mountains of IDS, IPS, firewall, router, and system event logs, a properly tuned CS-MARS installation produces a correlated set of incidents that are likely to need real attention. The key to this degree of data reduction is the proper configuration and tuning of the CS-MARS device. The following configuration and tuning steps will be covered in depth, based on tuning work done by the author and his team in a large, worldwide installation....

Copyright SANS Institute
Author Retains Full Rights

AD

Configuring and Tuning Cisco CS-MARS

GCIA Gold Certification

Author: John Jarocki

Adviser: Joey Niem

Accepted: April 22nd 2007

© SANS Institute 2007, Author retains full rights.

1. Introduction 4

2. Getting Started 6

3. Deciding What to Send to MARS 7

4. Configuring Supported Reporting Devices 11

5. Configuring Custom Log Parsers to Support New Devices ... 11

6. Mapping a Custom Log to an Existing Event 12

7. Defining and Discovering Networks 18

8. Vulnerability Information 20

Manual Vulnerability Information Entry 20

Dynamic Vulnerability Scanning 22

9. Tuning Approach 22

Reduce False Positives 23

Alert Only on High Fidelity True Positives 24

Provide Monthly Reports to High Level Executives 24

Watch the Internet Perimeter 24

Audit/Enforce Critical Server Access Compliance 25

Provide Forensic Information 25

10. Some Tuning Tricks 25

Always Click the “Activate” Button 26

White-list the Network Engineer’s Computer 26

© SANS Institute 2007, Author retains full rights.

RPC portmapper looks like nmap… and other stuff 27

Asymmetric routing can lead to ICMP covert channel alerts 27

Peer-to-Peer Software and Denial-of-Service 28

Create New Rules for Recent Exploit IDS Signatures 28

Traffic from localhost considered harmful 30

NFS can cause fragmentation and lost fragments 31

Wireless networks cause fragmentation alerts 32

HTTP CONNECT Tunnel 32

DNS Incremental Zone Transfer 33

11. Summary 33

12. REFERENCES 35

© SANS Institute 2007, Author retains full rights.

1. Introduction

Cisco purchased Protego Networks in December of 2004 [1]. This acquisition added a powerful SIM (Security Information Manager) appliance to Cisco's ever-growing security portfolio: PN-MARS. Re-branded as CS-MARS (Cisco Security Monitoring, Analysis and Response System) and referred to as "MARS," this device receives real-time alerts from IDS sensors, firewalls, Windows domain controllers, and many other devices. SNMP traps and syslog alerts can be forwarded to MARS, and vulnerability scanning information can also be imported. MARS groups events into sessions, and it uses endpoint vulnerability and network topology information to identify false positives automatically when possible. For example, an IDS sensor might report a PC attempting peer-to-peer file sharing, but the firewall log shows those packets were dropped [2]. CS-MARS would mark this as a System Identified False Positive. In another case, a Windows RPC DCOM Overflow might be seen by an IDS system, but the target vulnerability scan shows the host is not running an affected version of Microsoft Windows – another false positive (at least for the attack itself). From mountains of IDS, IPS, firewall, router, and system event logs, a properly tuned CS-MARS installation produces a correlated set of incidents that are likely to need real attention. The key to this degree of data reduction is the proper configuration and tuning of the CS-MARS device. The following configuration and tuning steps will be covered in depth, based on tuning work done by the author and his team in a large, worldwide installation.

- Deciding what information to send to MARS

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

- Configuring Custom Log Parsers
- Defining/discovering networks
- Configuring dynamic vulnerability scanning
- Defining the tuning approach
- Tuning by creating False Positive (Drop) rules
- Tuning by modifying default MARS Rules
- Other tuning tips

© SANS Institute 2007, Author retains full rights.

2. Getting Started

It's Monday morning. As you grab your cup of coffee, settle into your chair, and start to read through your pile of new email, you notice a message from The Big Boss. He has just purchased a Security Information Management (SIM) system called CS-MARS from Cisco. He thinks you are overworked and need help dealing with the pile of firewall, IDS, and system logs to separate the real security incidents from the chaff. MARS is a correlation tool, so it should be able to do most of the work. The boss ends his email with: "And, oh, can you get it configured and start sending me reports by the end of the month? That would be great! Thanks."

Okay. Don't panic.

MARS is a powerful tool… and it's complex. However, if you spend time setting MARS up and plan time for monitoring and ongoing maintenance, it can reduce your overall analysis effort. This assumes, of course that your alternative is analyzing all of those device events yourself. An alternative (sadly chosen too often) is to never look at the events at all – or to only review them after an incident for forensic information. If your goal is to really be kept aware of security-related events in near real time, you probably need a SIM. This paper will focus on only one: CS-MARS. However, you may be able to leverage some of this information for other SIM deployments.

The purpose of the rest of this paper will be to help you focus your energy on the high value features of MARS.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

3. Deciding What to Send to MARS

Cisco refers to firewalls, network, and security systems that can send events to MARS as Reporting Devices. Any device that can be a choke point for attacks (e.g., adding an ACL on a router) is also a Mitigation Device. MARS is pre-configured to support a fairly long list of devices out of the box. In addition, MARS has some pre-installed rules that correlate events from disparate devices to increase the fidelity of incidents. So, adding more devices can improve the value of the information that comes out of MARS. This has to be weighed against the downside (there is always a downside, of course): More devices means more data, which may mean more false positives, overflowing logs, or both.

So, how do you decide what information to forward to MARS? Ask yourself this question: Where would you focus your effort if you had time to manually review a specific set of logs? Would you focus on Oracle because your entire enterprise is based on workflow management using Oracle databases on the backend? Would you focus on your exterior web servers and firewall logs since you are a web hosting service? Would you focus on event logs from domain controllers because you have a centrally managed Active Directory forest? Or perhaps you could care less about Windows and are more interested in syslog information from your Linux workstations and Solaris servers? Forget about *volume* of information, because that is exactly what MARS can help you with. Focus on what information is *important*. What are your auditors going to ask you about? Where have you experienced intrusions before? Where are the crown jewels?

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Now that you have started to formulate an idea of where to focus, think about information that would also be useful for correlation. If you are looking at web servers and firewalls, do you also have border routers and IDS or IPS devices that can track potential attacks across the network? If you are concerned about worms, bot nets and spoofed attacks, do you have devices that can provide ISO Layer 2 information and Network Address Translation (NAT) data? If you are seeing virus and worm propagation across your internal network, consider integrating antivirus and personal firewall logs.

The complete list of devices that are supported by MARS can currently be found at the CS-MARS web site [3], but here are some of the devices that I recommend you have report to MARS.

Routers and Switches – These devices provide the most important information to MARS. They help MARS determine the topology of the network via OSI Layer 2 discovery, they provide normal traffic pattern information via Netflow, they can provide network access control (NAC) information via EAPoUDP (Extensible Authentication Protocol over UDP), and they can act as Mitigation Devices [2, p. 138]. The Mitigation (or Enforcement) Device function allows MARS to suggest choke points in the network where attacks in progress can be stopped by a network or security administrator. An example of such a recommendation is shown in Figure 1 below.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

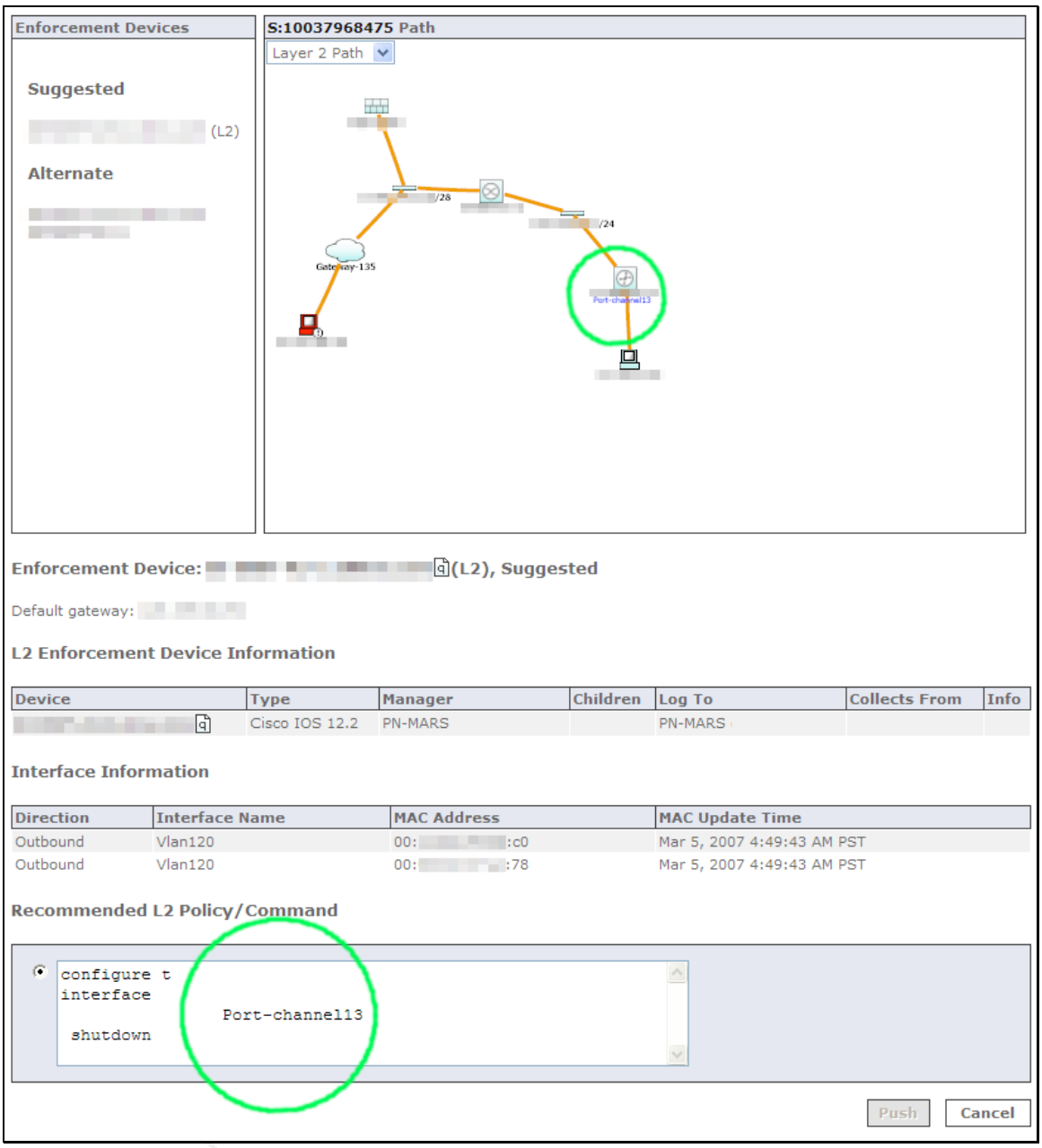


Figure 1

Firewalls (Checkpoint, Netscreen, Cisco) – Logs from these devices help MARS determine if an attack was blocked at the network perimeter or not. This is a very important part of the bigger picture, and you should make sure your Internet firewalls are sending logs to MARS if you want an accurate view. Firewalls are also Mitigation

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Devices, and MARS may recommend specific firewall rule changes to block attack traffic.

VPN (Cisco) – If a remote user connects to your network via VPN from their infected home PC, you will normally receive IDS alerts that have a source address that has been dynamically assigned by your VPN server. MARS, with VPN log information, can link the VPN connection to the alert and show the external IP address and even username [2, p.134]

NIDS/NIPS (Snort, Cisco, Symantec, ISS, Enterasys, etc.) – Logs from Network Intrusion Detection devices typically supply most of the actual events that MARS correlates into incidents. When the signatures from network IDS devices contain information about affected operating systems and patch levels, MARS can mark these as false positives automatically if (and only if) it can determine the vulnerability information for the destination hosts. These devices also provide raw packet context data that can be attached to the incident to help in further in analysis [2, p.135]. Since Cisco often sells MARS in conjunction with their own IDS/IPS devices, much of this paper will focus on that integration.

HIDS/HIPS (Cisco CSA, McAfee, ISS) – Because host-based intrusion detection is closest to the location of the potential compromise, the information from HIDS software is often the most important piece of the puzzle. For example, the NIDS may detect an attempted buffer overflow launched over the network, but the HIPS on the target host can inform MARS if the attack was actually blocked [2, p.135].

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

AAA and 802.11x Authentication – These logs enable MARS to attach user information to sessions and incidents.

Other logs – This information can be helpful, but you might want to wait until your initial roll out is complete.

Anti-virus (Symantec, McAfee, etc.)

Web servers

Oracle database servers

Solaris/Linux host logs (via syslog)

Windows logs – Active Directory servers, in particular, are good log sources.

4. Configuring Supported Reporting Devices

Cisco has provided excellent step-by-step instructions for configuring reporting devices for MARS, so we will not detail the steps here. For detailed information on configuring various devices, see [4] and [2].

5. Configuring Custom Log Parsers to Support New Devices

If you do not find your device the supported list, all hope is not lost. Cisco doesn't provide very much documentation on the topic, but you *can* customize MARS to accept events from new devices and to analyze those events.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

The way to teach MARS to support a previously unsupported device is by using the "Custom Log Parser" feature. This can be used to achieve several different goals:

- To parse and support new events from supported devices (such as IDS sensors) that have frequent signature updates,
- To support devices that can forward log information via syslog,
- To define custom events relevant to your organization.

The MARS User Guide [4] explains how to configure custom log parsers, but since the operation is somewhat complicated, I will provide an example in the next section.

6. Mapping a Custom Log to an Existing Event

In our environment, we use a sudo work-a-like called "root." In order to track privilege escalation in our environment we forwarded system syslog data to MARS and created custom log parsers to parse the syslog messages. In order to duplicate what we did, you have to first configure your host to send syslog data to you MARS server. Next, in MARS, click the **Admin** button, **Custom Setup** tab, and **User Defined Log Parser Templates**. Then you will see a view similar to the one in Figure 2.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

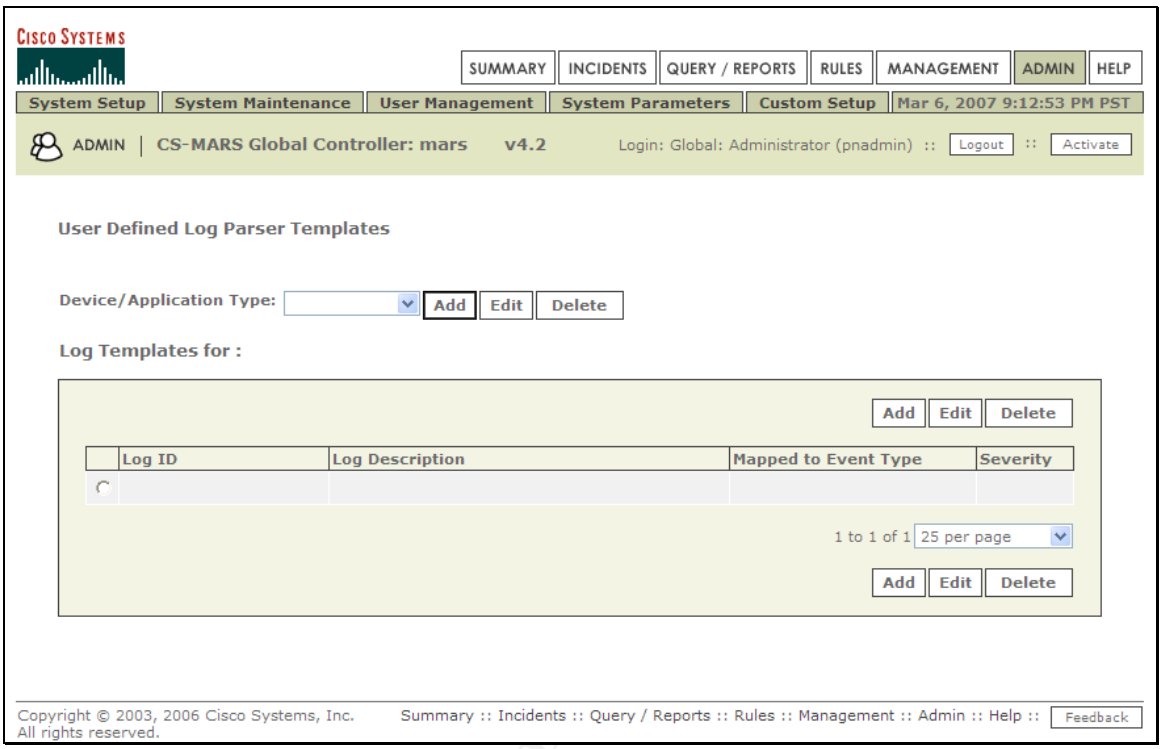


Figure 2

First, since this is a custom device, you need to define the device/application in MARS. In Figure 3 you can see an example for the application "root version 1.0" with a vendor of "Internet One."

© SANS Institute 2007, Author

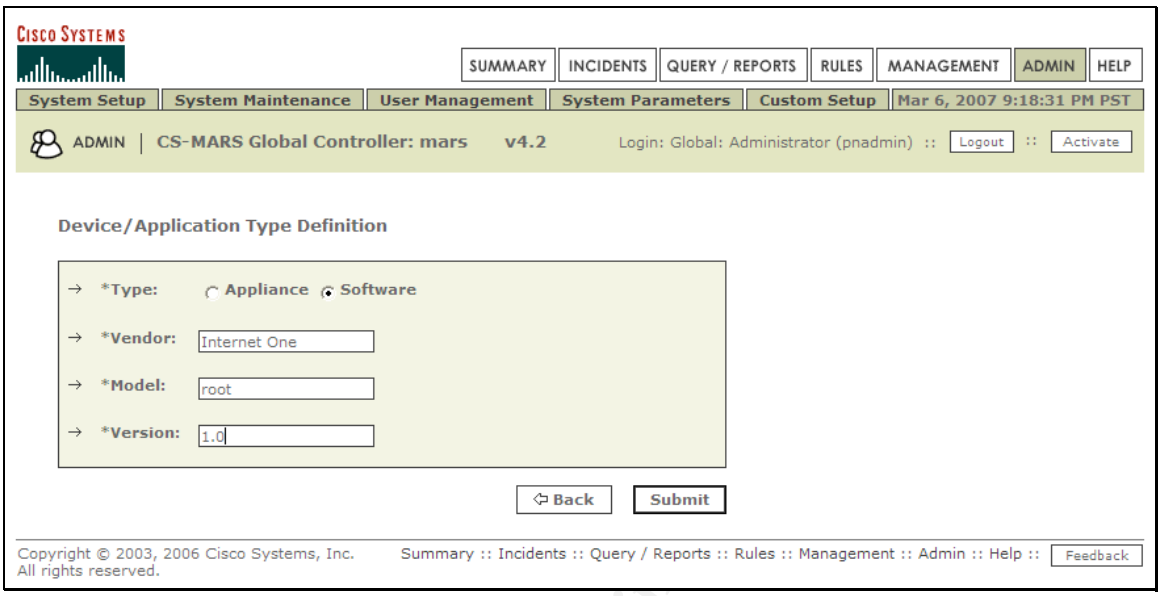


Figure 3

After submitting this change, you can select the Device/Application type as "Internet One root 1.0" and click the **Add** button under "Log Templates for:" to add a new log parser. Each log parser parses a string of log information into a single event. You may have one or several (probably thousands if you are defining a custom log parser for a new IDS device). The first step, shown below, is to define a Log ID and Description. You can also map this to an existing Event type or create a new one. I highly recommend using the existing Event types, because this allows MARS to use the inspection rules it already has to add some logic around your new parsed logs. For example, MARS can create a "Multiple root login failures" incident if this event is seen repeatedly.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

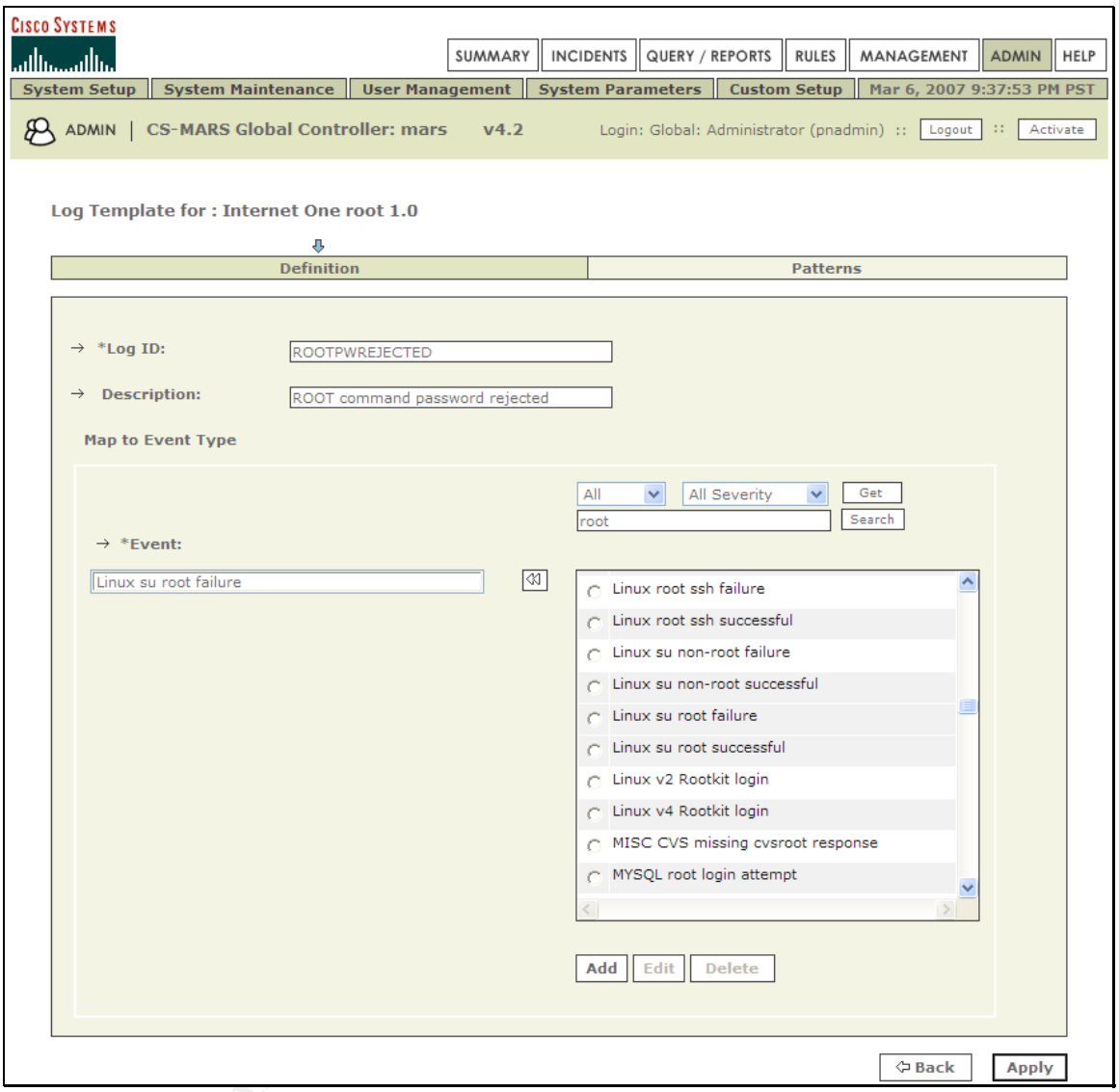


Figure 4

After entering the log parser definition information, click on the **Patterns** tab. This view lets you create the regular expression patterns that make up your log parser. The log parser starts at the left of the log message and parses each of your Key/Value patterns in order until it reaches the end of your log line, the end of the patterns, or the parser fails because it does not match one of the patterns.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

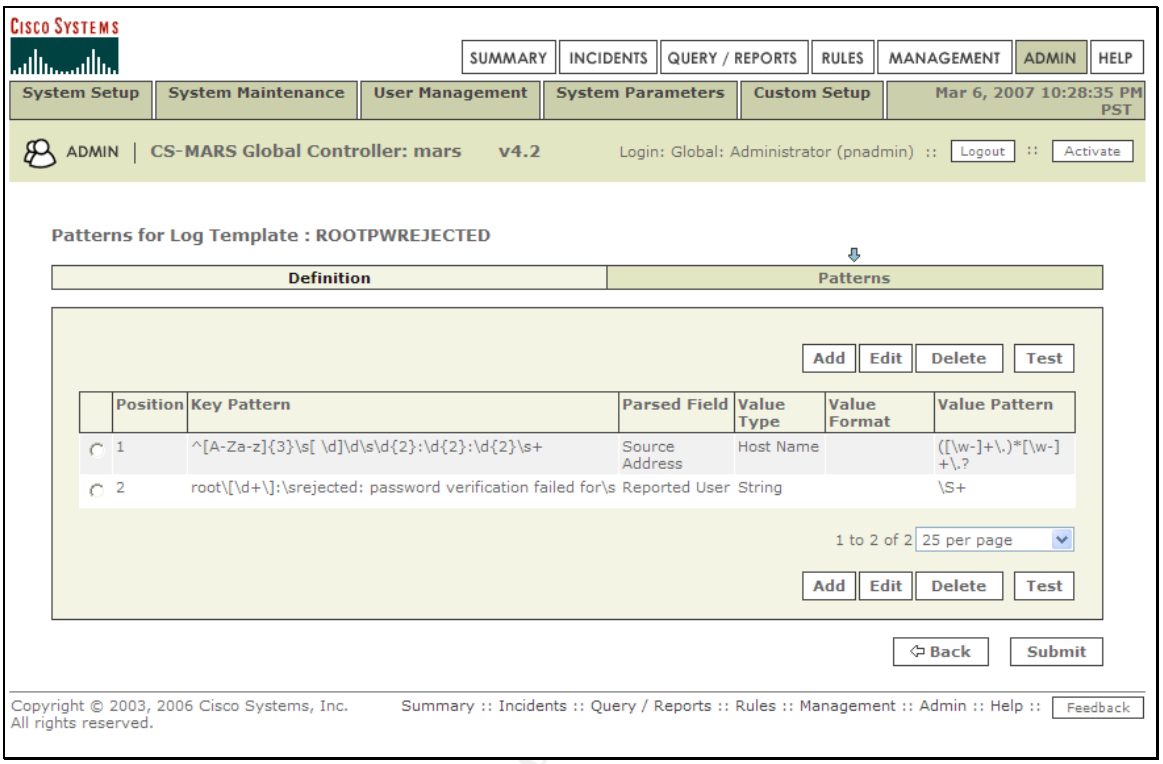


Figure 5

After defining the parser patterns, you can test them out by clicking the **Test** button. This lets you paste a copy of a log entry and see the Parsed Values that MARS matches.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

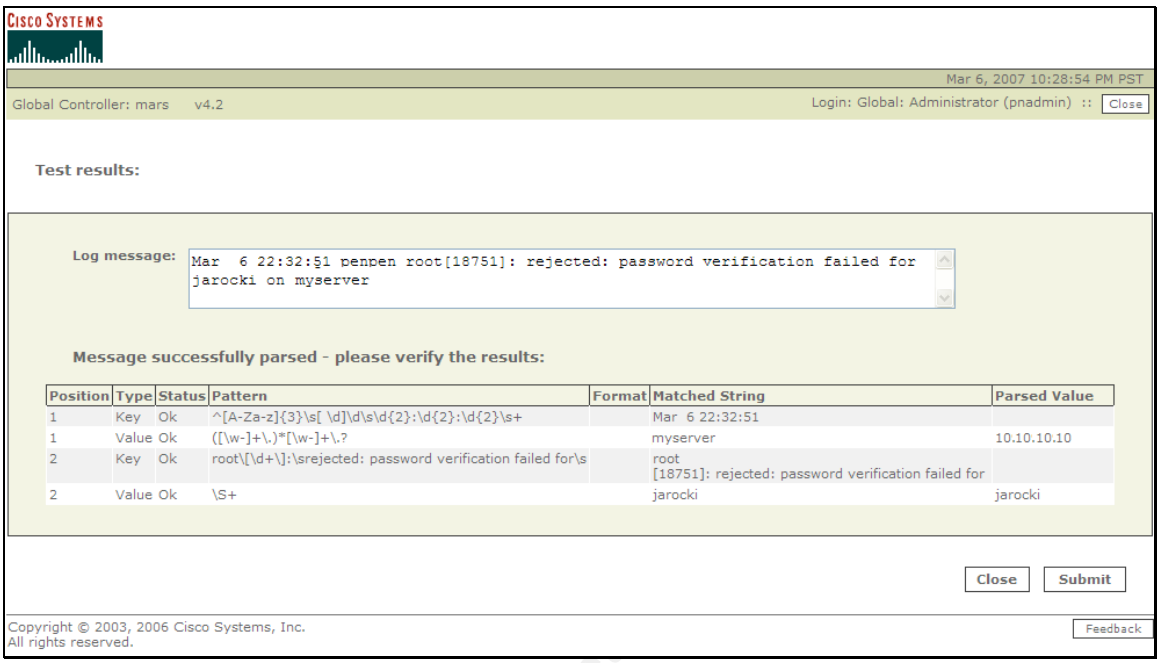


Figure 6

Finally, if all is good, you can click **Submit** to create your new log parser. Make sure to click **Activate**, and you should see a new Log Template as shown below:

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

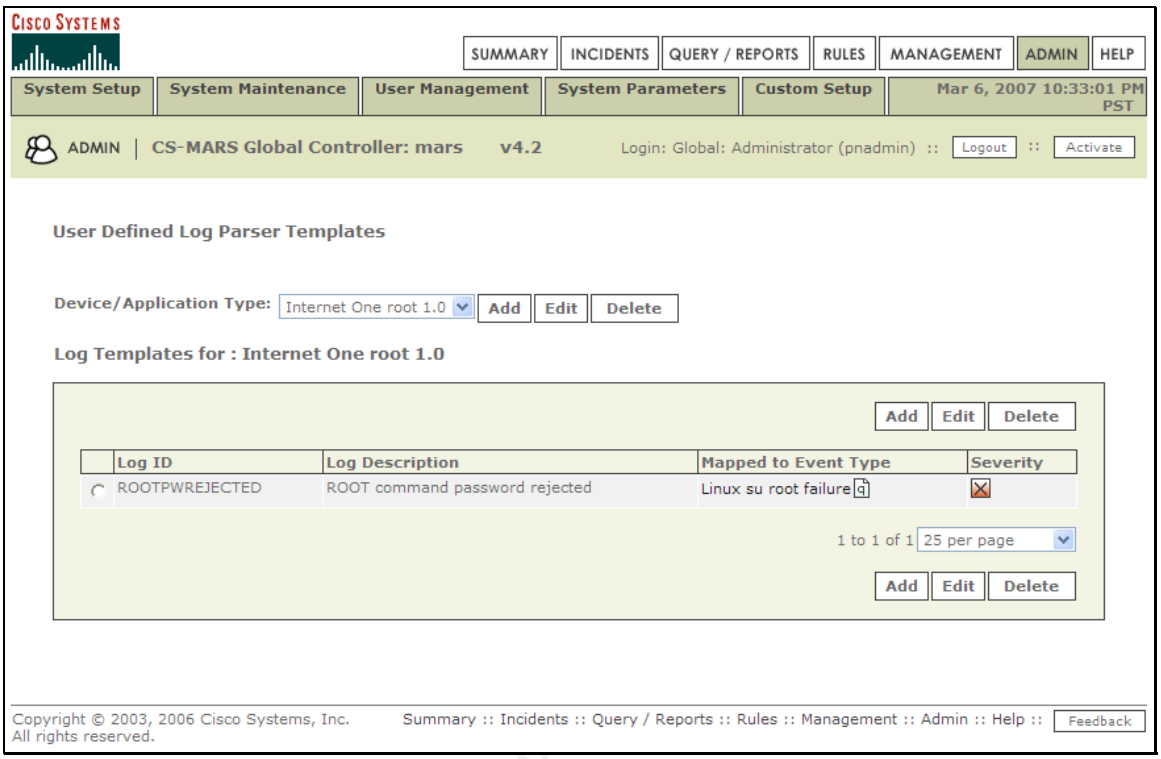


Figure 7

Chris Durkin has also collected several excellent log parser demos and made them available on his Cisco MARS web log [5].

7. Defining and Discovering Networks

MARS attempts to determine the paths that sessions and incidents take through your network based on events received from various devices and based on the source and destination IP (OSI Layer 3) and MAC (OSI Layer 2) addresses. Additionally, MARS can follow NAT (Network Address Translation) that takes place at firewalls, VPN concentrators, and similar devices. In order to gather this information, MARS must be configured to discover your network.

To configure discovery, navigate to **Admin** -> **System Setup** on

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

the MARS web administration interface.

Under **Discovery Information**, click **Community String and Networks**. Add the correct SNMP read community string (you do *not* need to provide a write community string). Add the IP range or IP addresses this string is valid for. This sets the SNMP read community string to be used when discovering on these networks. Click **Submit** and **Activate**.

Under **Valid Network Addresses**, setup the seed SNMP device (**SNMP Target**). This should be the closest network router to the MARS controller. Setup the Network range that is valid to discover from this seed device.

If all network devices allow the controller SNMP read access, then only ONE seed router (SNMP Target) and IP Range combination needs to be listed. Click **Submit** and **Activate**. If you want to do an initial discovery, click **Discover Now**. If you have multiple MARS Local Controllers reporting to a Global Controller, you have an important decision to make: either you can have each Local Controller list ONLY the networks that contain the devices reporting to that controller, or you can configure each Local Controller to discover all network devices. If you do the latter, you will be able to see the recommended mitigation point in your network from any incident at any controller. However, doing so will also cause additional load on your network and might make the network diagrams in MARS more confusing to look at. Cisco does not provide an opinion on which option is better. When I posed this question to an engineer from the Cisco Technical Assistance Center he gave the response, "The question is more of a design

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

question and there could be several different solutions depending on what's best for your network set up.

Topology/Monitored Device Update Scheduler: After the initial discovery, further discoveries will not be performed unless you add a discovery group. There may be a Default Discovery Group, but it is probably a good idea to add one or more groups that explicitly cover the networks listed in the Valid Network Addresses screen. The updates should be scheduled to run frequently enough to keep the topology accurate, but not so frequently as to create too much network overhead. I recommend a weekly update schedule, but the best schedule will depend on your network layout.

8. Vulnerability Information

MARS can use vulnerability information of nodes to determine whether a potential incident is mark as a false positive or not. MARS supports asynchronous import of vulnerability information from the following products [3]:

- eEye REM 1.0
- Qualys QualysGuard 3.x
- Foundstone Foundscan 3.0

However, if you have none of these products, you can still input vulnerability information into MARS through manual entry or by using the dynamic vulnerability scanning feature of MARS.

Manual Vulnerability Information Entry

Source and Destination hosts in MARS have information stored

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

with them on what operating system and services they run.

To manually enter this information in MARS, click the **Management** button, click the **IP Management** tab, and select View Host (rather than all) to see hosts that MARS has seen in events so far. To modify one of these hosts, click the check box to the left of the host in the table, and click **Edit**. You can also create a new host definition by simply clicking the **Add** button.

On the **General** tab in the view that appears (shown below), you can enter the device name, operating system, NetBIOS name (if applicable) and network interface information.

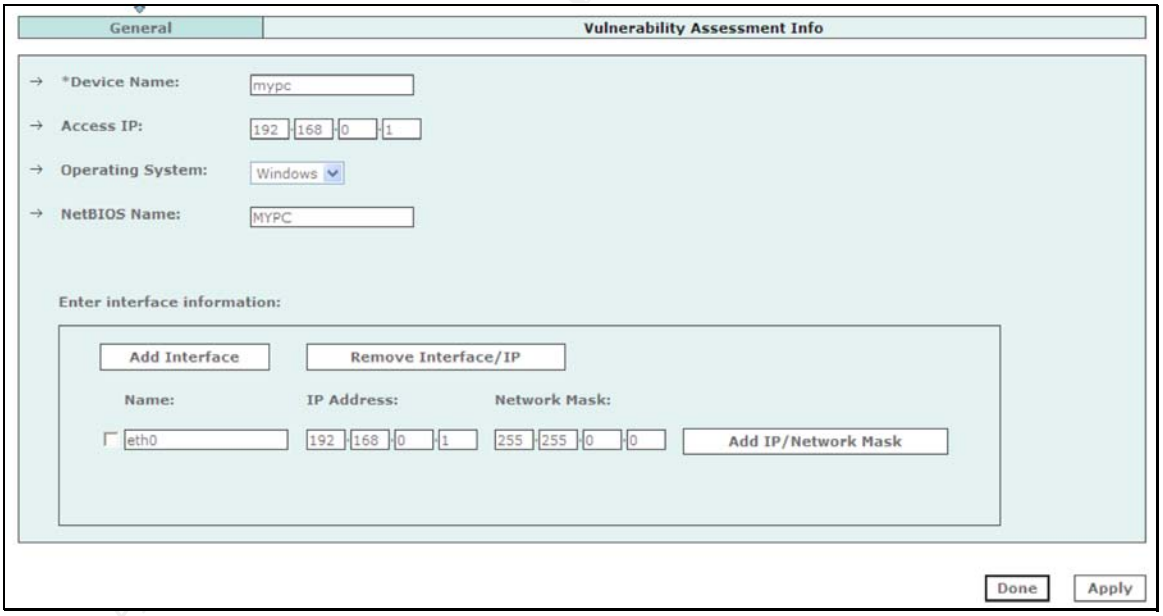


Figure 8

On the **Vulnerability Assessment Info** tab, the operating system and version can be selected as well as any services that you expect to be running on that host.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

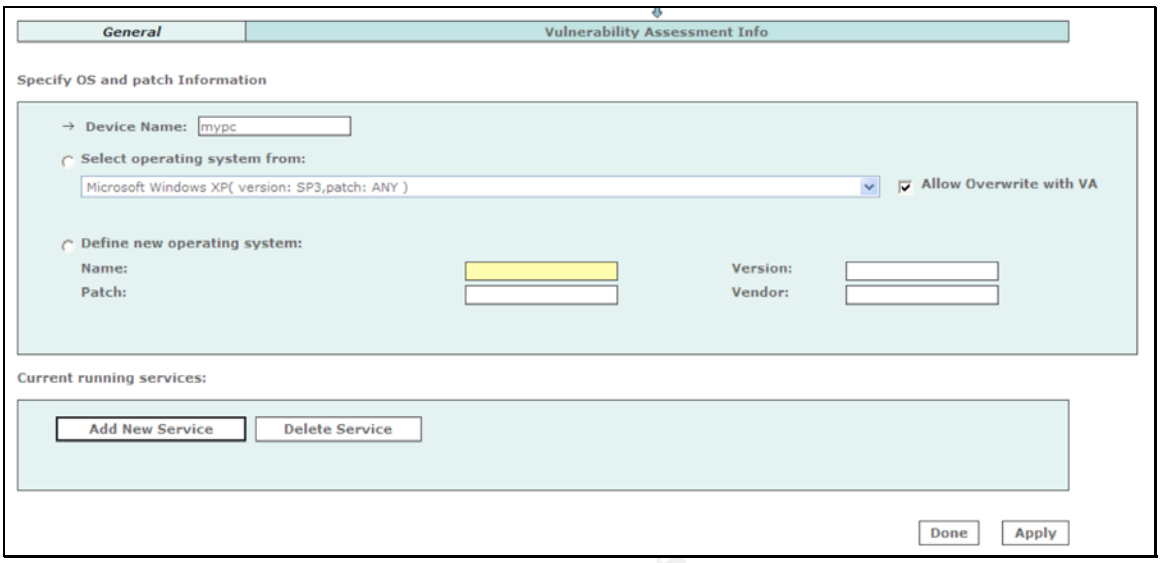


Figure 9

Dynamic Vulnerability Scanning

MARS also has a sparsely documented dynamic vulnerability scanning feature that uses a built in version of Nessus to perform targeted scanning of destination hosts in events to determine if they are vulnerable to the attempted attack. This version of Nessus and its plug-ins are rather old, and not currently kept up to date or supported by Tenable Security, the author of Nessus [6]. For more information on this capability, see [2, p.124].

9. Tuning Approach

Tuning MARS requires setting goals for your environment. If you have the time to complete a risk assessment, you should be able to determine potential targets, their relative value, and the risks that they face. Once you have some of this information, you can define the goals for your MARS installation. With the goals in hand, you can determine

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

the tuning approach that will work best to achieve them. Here are some example goals along with the tuning approaches they lead to.

Reduce False Positives

Reducing false positives is often cited as one of the top goals in any intrusion detection installation [7]. If intrusion prevention is implemented (meaning that attacks are actually *blocked* rather than simply alerted on), you certainly want false positives as to be as low as possible (hopefully zero, because even one false positive is going to be a disruption to your organization) [8, p. 75]. In general, reducing false positives (alerts that do not represent a real incident for your organization) typically means increasing the incidence of false negatives – *real incidents that your intrusion detection system didn't alert you to.* Because your intrusion detection systems have a false alarm base rate that you have little control over, tuning the number of false positives is affected by a statistical theorem known as the Base Rate Fallacy [9].

Reducing False Positives in MARS means focusing on the following process:

- Make sure all reporting devices for the intended target coverage area are configured to report to MARS.
- Configure those reporting devices to send only relevant security events and not (for example) summary traffic reports that MARS can create itself [4].
- Allow MARS to perform frequent later 2/3 discovery to provide accurate path information and NAT translation.
- Enter as much endpoint vulnerability information as possible, so

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

MARS can identify false positives.

- Identify Inspection Rules that indicate normal conditions in your network and tune them by adding exceptions based on source or destination IP address. For example, a "Mass Mailing Worm" from your mail server might just be a normal volume of email.
- When you find a false alarm, tune it by clicking on the "False Positive" link to the right of the event listed in MARS.

Alert Only on High Fidelity True Positives

Although this seems like a modified version of the previous goal, it really is almost the opposite. Because of this, the best place to start if you want to only receive alerts you *know* will indicate real attacks is by turning off all IDS signatures except the ones you know will be true positives. Next you will want to disable all Inspection Rules in MARS except the ones that again indicate only true positives.

Provide Monthly Reports to High Level Executives

MARS has many canned reports, and you can add many more. Make sure that you create your reports on a consistently repeated interval (monthly, for example) and that you highlight the trends for your management. This might require annotating the reports to point out where, for example, upgrades were performed or there were large Internet worm outbreaks.

Watch the Internet Perimeter

To have MARS watch your network perimeter, make sure any IDS devices inside and outside the firewalls forward logs to MARS.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Additionally, routers, switches, and application servers in your DMZ network should send information to MARS.

Audit/Enforce Critical Server Access Compliance

There are many reports that can be produced periodically (and even emailed) directly from MARS. In order to get good compliance data, I suggest you concentrate on making sure that Oracle, firewalls, Windows, Linux, and Solaris servers all report to MARS. Additionally any authentication (AAA) servers and network access (NAC) servers should also be configured into MARS.

Provide Forensic Information

MARS can be very valuable in forensics investigations, but the most important place to focus if this is your primary goal is on making sure that MARS is archiving data and that you test access to those archives frequently.

10. Some Tuning Tricks

While tuning MARS (and the devices that report to it), I have come across some anomalies that are worth noting. My intent is to pass them along to you, so you don't have to repeat all the same steps (and missteps). A typical session of drilling down into one of these anomalies typically includes opening a dozen windows showing MARS reports, syslog data, nmap results, network diagrams, and spending anywhere from an hour to several weeks researching on the web and by interview with system and network engineering staff. This work makes you a better analyst, but it is difficult to find the time to drill down into

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

every event.

Always Click the "Activate" Button

This is not really a tuning tip as much as a tip on working with MARS in general, but it is such an important tip that I feel compelled to repeat it: Anytime you make a change in MARS, click the Activate button (as shown in Figure 10). This will save you many headaches.

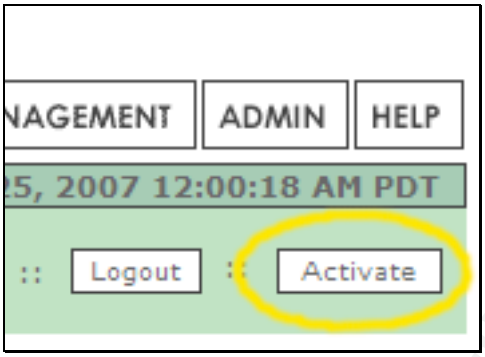


Figure 10

White-list the Network Engineer's Computer

The first place to start when tuning IDS devices is by white-listing the network and security team members' systems. Ask them to use a static IP Address. If they tend to use a roaming laptop, you can suggest they create a central network scanning system they can connect to remotely or at least ask them to assign themselves a reserved DHCP address. Make it part of your change management process to inform the MARS team when changes to network scanners take place. Remember to include systems running HP OpenView, CiscoWorks, AirMagnet, and patch or vulnerability management

© SANS Institute 2007, Author retains full rights.

software.

RPC portmapper looks like nmap… and other stuff

If you are using MARS and IDS sensors inside your internal network, and if you have Unix-based systems on your internal network, you probably will see a large number of "port scans" to the portmapper (usually UDP port 111). This is really "normal" traffic if you allow ONC/RPC traffic on your network. Unless you are on a mission to wipe out RPC traffic, you will want to tune these events. You may also see "port scanning" from NIS servers where the source port is ypservd (e.g., port 1023 on some Solaris boxes).

Asymmetric routing can lead to ICMP covert channel alerts

Several bot nets and hacker tools use Loki [10] as a communications and control protocol. Loki transmits messages via ICMP reply messages. When MARS alerted our team that Loki traffic was found on our network, my immediate reaction was to start looking for a bot net. However, by pulling out the network diagrams and using traceroute, I was able to see that the route from Host A to Host B was not the same as the route from Host B to Host A. This asymmetric routing was confusing the IDS sensors that were placed so they only saw one path at a time. When seemingly unsolicited ICMP Reply messages started arriving from B to A, the IDS sensor started sending covert Loki channel alerts to MARS. Asymmetric routing can also trigger other false alarms, such as Tribe Flood Network (TFN) Client or Server signatures [11]. This highlights the importance of knowing your network – or at least knowing the people who do. If you cannot remove

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

the asymmetric route, you will need to analyze the traffic payload to see if it contains bot net commands.

Peer-to-Peer Software and Denial-of-Service

Peer-to-peer software, such as BitTorrent, can trigger Denial-of-Service (DoS) incidents to fire. Since such alerts might be either false positives or real incidents [12] you must analyze them in the context of your own environment. If peer-to-peer software is forbidden on your network by policy, then every alert of this type is a real incident and requires investigation. If you have no policy prohibiting peer-to-peer software, a DoS alert may still be an important event. With MARS you use this situational awareness to guide you to deciding whether these events:

a. Require an alert by pager and immediate attention because they are exhausting shared network resources,

b. Are sent to a security analyst to determine if the peer-to-peer software policy has been violated, or

c. Serve as data for a report to be generated monthly by MARS to provide data to help policy makers create a peer-to-peer policy.

Create New Rules for Recent Exploit IDS Signatures

You have MARS tuned, and things are running well. You can see worm outbreaks when someone connects an infected home PC to the corporate network, you ask the help desk to let new employees know that the peer-to-peer file sharing software MARS detected violates your acceptable use policy, and you can see that all those recon scans from

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

international (probably spoofed) addresses that are bouncing off your firewalls. Then, your IDS vendor releases a signature update. So you upgrade the IDS devices worldwide and tell your boss that you're protected because those devices are forwarding all events to MARS, right? *Wrong!* In fact, MARS only knows how to parse the events it has been configured to parse. Currently MARS 4.2 supports 2693 Snort 2.0 events – Snort signatures 9644 and later are not parsed. MARS currently knows 2000 Cisco IPS 5.x signatures. The last Cisco IPS signature supported as of the time of this writing is NR-5831/0. Even if you keep MARS upgraded to the latest release, there will still be new signatures that are not available in MARS. If you want MARS to alert you to these bleeding-edge attacks, you will have to do so by creating custom log parsers as described above or by creating new inspection rules to watch for them based on keywords as shown in Figure 11:

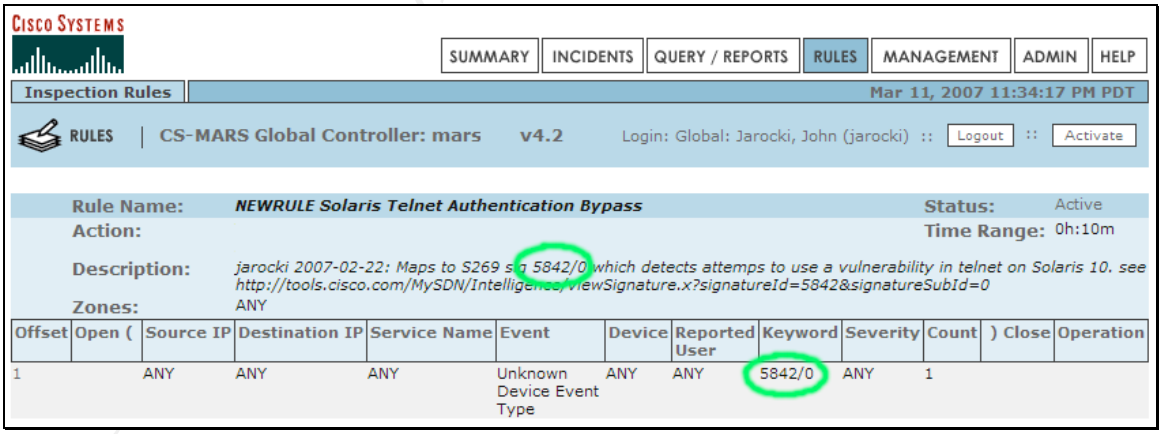


Figure 11

Notice that the Event is listed as "Unknown Device Event Type." This is the default event type for any unparsed event received by MARS. For this reason, you can monitor new events by running a

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

periodic “Unknown Events” report:

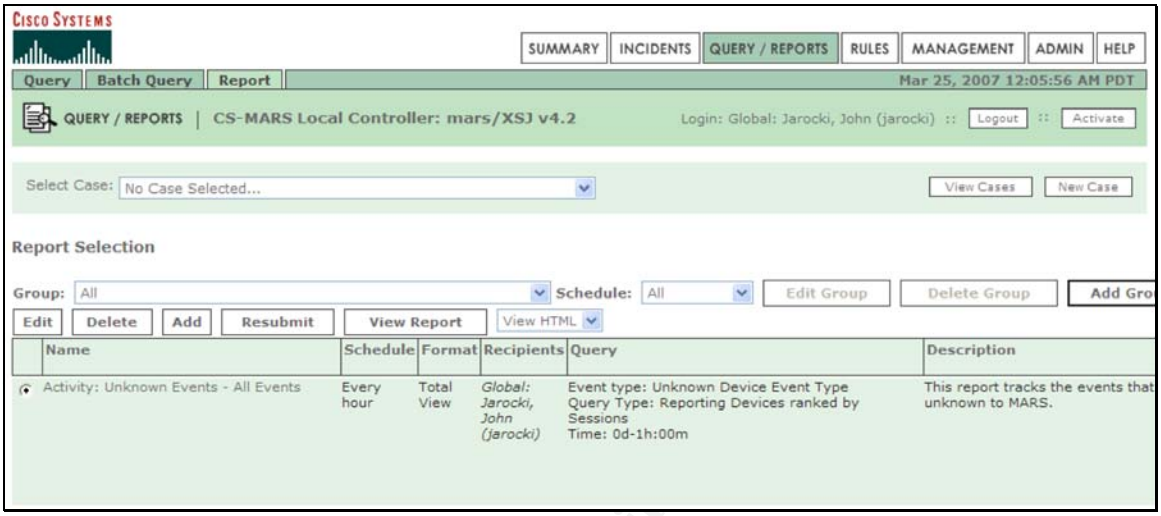


Figure 12

Traffic from localhost considered harmful

Before I spent time analyzing our IDS events in depth, I would have said packets with a source address of 127.0.0.1 would be extremely unlikely, and only if something malicious was occurring. However, we have seen many “Spoofed Localhost Address” alerts caused by a combination of a network stack oddities, a version of BIND that tickles the kernel issues, and 127.0.0.1 listed in the resolv.conf. This is not really a new issue. Paul Vixie and others on the BIND USENET newsgroup explained in 1995 how certain BSD-based kernels could produce this condition. An extract of that conversation is now found on the TCP/IP Domains FAQ [13]:

```
Question 5.15.  resolv.conf

Date: Fri Feb 10 15:46:17 EST 1995
```

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

```
The question was asked one time, "Why should I use 'real' IP
addresses in /etc/resolv.conf and not 0.0.0.0 or 127.0.0.1" ?

It's historical.  Some kernels can't unbind a UDP socket's source
address, and some resolver versions (notably not including BIND
4.9.2 or 4.9.3's) try to do this.  The result can be wide area
network traffic with 127.0.0.1 as the source address.  Rather
than giving out a long and detailed map of version/vendor
combinations of kernels/BINDs that have/don't this problem, I
just tell folks not to use 127.0.0.1 at all.
```

You can get rid of these false alarms on your network altogether and eliminate the possibility of truly spoofed packets at the same time by configuring your routers to not route packets from 127.0.0.1 [14] recommend creating ACLs like the following example (for Cisco devices) as part of standard router configuration:

```
router(config)#access-list 11 deny 10.0.0.0 0.255.255.255
router(config)#access-list 11 deny 127.0.0.0 0.255.255.255
router(config)#access-list 11 deny 172.16.0.0 0.15.255.255
router(config)#access-list 11 deny 192.168.0.0 0.0.255.255
router(config)#access-list 11 deny 224.0.0.0 15.255.255.255
router(config)#access-list 11 deny host 0.0.0.0
router(config-if)# ip access-group 11 in
```

NFS can cause fragmentation and lost fragments

If you have IDS sensors near Network File Service (NFS) file servers, they may send an overwhelming number of fragmentation events to MARS because NFS over UDP is guaranteed to fragment its 8 KB datagrams into multiple packets when a default MTU of 1500 bytes is used [15] [16]. You can tune your IDS devices to not send alerts to

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

MARS on some of these fragmentation signatures, or you can tune MARS by creating drop rules that ignore certain conditions (such as UDP port 2049 and 4096 in the case of NFS).

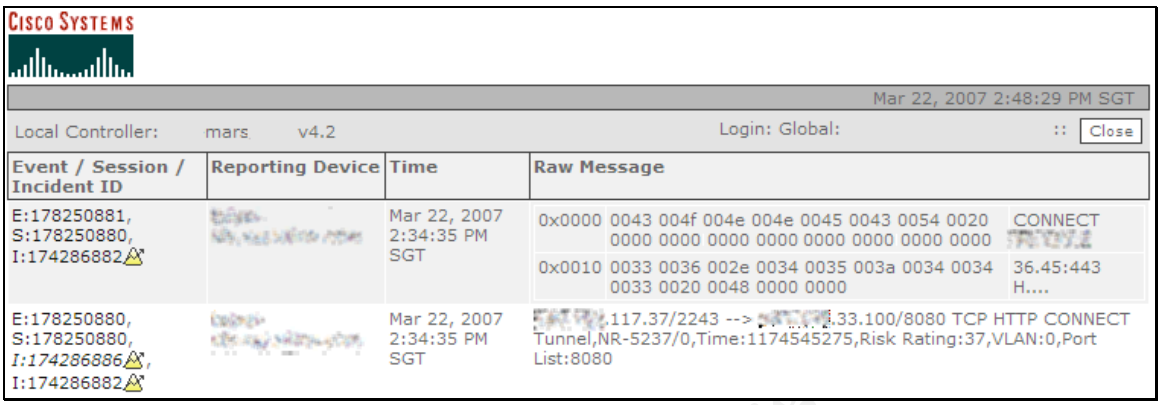
Wireless networks cause fragmentation alerts

Because the 802.11 standard allows wireless network interface cards (NICs) to fragment packets to compensate for radio frequency (RF) interference, IDS sensors watching wireless segments can observer a large number of fragmentation alerts. These will need to be tuned, but fragmentation can also be used in wireless attacks, so some caution is required here as well.

HTTP CONNECT Tunnel

If you use web proxy servers to relay HTTP traffic to and from the Internet, MARS will often flag this as "HTTP Connect Tunnel" traffic. The simplest way to eliminate this false positive is by modifying the MARS rule to exclude the proxy hosts as destinations for this rule. If you are monitoring IDS sensors or firewalls between the Internet and your proxy servers, you also want to exclude them as valid sources for this rule. Figure 13 shows the raw message for such a tunnel. In this case, the destination (with IP address ending in 33.100) was a valid proxy server.

© SANS Institute 2007, Author retains full rights.



Mar 22, 2007 2:48:29 PM SGT

Local Controller: mars v4.2 Login: Global: :: Close

Event / Session / Incident ID	Reporting Device	Time	Raw Message
E:178250881, S:178250880, I:174286882	[redacted]	Mar 22, 2007 2:34:35 PM SGT	0x0000 0043 004f 004e 004e 0045 0043 0054 0020 0000 0000 0000 0000 0000 0000 0000 0000 CONNECT [redacted] 0x0010 0033 0036 002e 0034 0035 003a 0034 0034 0033 0020 0048 0000 0000 36.45:443 H....
E:178250880, S:178250880, *I:174286886*, I:174286882	[redacted]	Mar 22, 2007 2:34:35 PM SGT	[redacted].117.37/2243 --> [redacted].33.100/8080 TCP HTTP CONNECT Tunnel,NR-5237/0,Time:1174545275,Risk Rating:37,VLAN:0,Port List:8080

Figure 13

DNS Incremental Zone Transfer

DNS zone transfers are often a sign of network reconnaissance that precedes attacks [17, p. 89]. If you observe zone transfers from your name servers to hosts on the Internet, you have cause for alarm. However, if MARS alerts you to zone transfers inside your organization (particularly across wide area networks); you are most likely observing normal activity between your primary and secondary servers. You may want to "white list" this activity via MARS Drop Rules or by modifying the built-in MARS inspection rules to exclude internal-to-internal transfers. A more effective strategy is to remove this rule from internal IDS sensors and only leave it active on the perimeter. Finally, consider turning on BIND access control lists or transaction signatures (TSIG) [18].

11. Summary

MARS can be a powerful tool in your organization for providing a

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

consolidated view of your security infrastructure. However, it is still only a tool, and it will only be as effective as the effort applied to it. Hopefully this paper has armed you with some new knowledge to make MARS as effective in your environment as possible.

© SANS Institute 2007, Author retains full rights.

12. REFERENCES

[1] Cisco Systems. (2004, December 20). Cisco Systems to Acquire Protego Networks, Inc., Retrieved December 10, 2006, from News @ Cisco Web site: http://newsroom.cisco.com/dlls/2004/corp_122004.html

[2] Tesch, D., & Abelar, G. (2007). *Security Threat Mitigation and Response: Understanding Cisco Security MARS*. Indianapolis, IN: Cisco Press.

[3] Supported and Interoperable Devices and Software for Cisco Security MARS Local Controller 4.2.x. Retrieved March 21, 2007, from Cisco Security Monitoring, Analysis and Response System Web site: http://www.cisco.com/en/US/products/ps6241/products_device_support_table09186a0080467232.html

[4] User Guide for Cisco Security MARS Local Controller, Release 4.2.x. Retrieved March 21, 2007, from User Guide for Cisco Security MARS Local Controller, Release 4.2.x Web site: http://www.cisco.com/en/US/products/ps6241/products_user_guide_book09186a00806c08d0.html

[5] Durkin, Chris (2007, March 16). [Weblog] Part 3 of the Custom Parser Demo is now Available. *Cisco MARS Blog*. Retrieved March 16, 2007, from http://ciscomars.blogspot.com/2007/03/part-3-of-custom-parser-demo-is-now.html

[6] Gula, R. (2005, Dec 28). RE: Tuning false positives (Nessus in CS-MARS). Retrieved April 14, 2007 from Security Focus web site: http://seclists.org/focus-ids/2005/Dec/0071.html

[7] Kessler, G. (2001, August). New directions in intrusion detection. *Information Security Magazine*, Retrieved March 24, 2007, from http://infosecuritymag.techtarget.com/articles/august01/cover.shtml

[8] Rash, M., Orebaugh, A., Clark, G., Pinkard, B., & Babbin J., (2005). *Intrusion*

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Prevention and Active Response: Deploying Network and Host IPS. Rockland: MA.

[9] Axelsson, Stefan (2000).The base-rate fallacy and the difficulty of intrusion detection. *ACM Transactions on Information and System Security (TISSEC)*. *3*, 186-205.

[10] Daemon9. (1996, August). Project Loki. Retrieved March 24, 2007, from Phrack Magazine, Volume Seven, Issue Forty-Nine: http://www.phrack.org/archives/49/P49-06

[11] Cisco Systems Countermeasures Research Team, (2003). TFN Client Request. Retrieved March 23, 2007, from Network Security Database Web site: http://secops.hottubinc.com/CiscoEvents/html/expsig_6501.html

[12] Wagner, A., & Plattner, B. (2002). Peer-to-Peer Systems as Attack Platform for Distributed Denial-of-Service. *ACM SACT Workshop 2002*, Retrieved March 24, 2007, from http://www.tik.ee.ethz.ch/~ddosvax/publications/papers/icisp06.pdf.

[13] Vixie, P. (1995, February 10). Question 5.15. resolv.conf. Retrieved March 24, 2007, from comp.protocols.tcp-ip.domains FAQ Web site: http://www.faqs.org/faqs/internet/tcp-ip/domains-faq/part2/

[14] Northcutt, S., Zeltser, L., Winters, S., Kent, K., & Ritchey, R. W. (2005). *Inside Network Perimeter Security, 2nd Edition*. Indianapolis, IN.: Sams.

[15] Smith, Christopher (2006, May 2). Optimizing NFS Performance. Retrieved March 24, 2007, from NFS How To Web site: http://nfs.sourceforge.net/nfs-howto/ar01s05.html

[16] Stevens, R. W., & Wright, G. R. (1995). *TCP/IP Illustrated Volume 2*. Indianapolis, IN: Addison-Wesley Professional.

[17] Whitaker, A., & Newman, D. (2006). *Penetration Testing and Network Defense: Performing Host Reconnaissance*. Indianapolis: IN.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

[18] Lau, Steven (2003, March 17). Why is securing DNS zone transfer necessary? Retrieved March 25, 2007, from SANS Reading Room Web site: http://www.sans.org/reading_room/whitepapers/dns/868.php

© SANS Institute 2007, Author retains full rights.

Last Updated: April 21st, 2014

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Abu Dhabi 2014	**Abu Dhabi, AE**	**Apr 26, 2014 - May 04, 2014**	**Live Event**
US Cyber Crime Conference	**Leesburg, VAUS**	**Apr 27, 2014 - Apr 28, 2014**	**Live Event**
SANS Austin 2014	**Austin, TXUS**	**Apr 28, 2014 - May 03, 2014**	**Live Event**
Security Leadership Summit	**Boston, MAUS**	**Apr 29, 2014 - May 07, 2014**	**Live Event**
SANS Security West 2014	**San Diego, CAUS**	**May 08, 2014 - May 17, 2014**	**Live Event**
SANS Secure Europe 2014	**Amsterdam, NL**	**May 10, 2014 - May 24, 2014**	**Live Event**
SANS ICS410 London 2014	**London, GB**	**May 12, 2014 - May 16, 2014**	**Live Event**
SANS Melbourne 2014	**Melbourne, AU**	**May 12, 2014 - May 17, 2014**	**Live Event**
SANS Malaysia @MCMC 2014	**Cyberjaya, MY**	**May 12, 2014 - May 24, 2014**	**Live Event**
SANS Bahrain May 2014	**Manama, BH**	**May 17, 2014 - May 22, 2014**	**Live Event**
AUD307: Foundations of Auditing Security and Controls of IT Systems	**Oklahoma City, OKUS**	**May 21, 2014 - May 23, 2014**	**Live Event**
SANS Secure Thailand	**Bangkok, TH**	**May 26, 2014 - May 31, 2014**	**Live Event**
Digital Forensics & Incident Response Summit	**Austin, TXUS**	**Jun 03, 2014 - Jun 10, 2014**	**Live Event**
SANS Rocky Mountain 2014	**Denver, COUS**	**Jun 09, 2014 - Jun 14, 2014**	**Live Event**
SANS Pen Test Berlin 2014	**Berlin, DE**	**Jun 15, 2014 - Jun 21, 2014**	**Live Event**
SEC511 Continuous Monitoring and Security Operations	**Washington, DCUS**	**Jun 16, 2014 - Jun 21, 2014**	**Live Event**
SANS Milan 2014	**Milan, IT**	**Jun 16, 2014 - Jun 21, 2014**	**Live Event**
SANSFIRE 2014	**Baltimore, MDUS**	**Jun 21, 2014 - Jun 30, 2014**	**Live Event**
SANS Canberra 2014	**Canberra, AU**	**Jun 30, 2014 - Jul 12, 2014**	**Live Event**
SANS Capital City 2014	**Washington, DCUS**	**Jul 07, 2014 - Jul 12, 2014**	**Live Event**
FOR518 Mac Forensic Analysis	**San Jose, CAUS**	**Jul 07, 2014 - Jul 12, 2014**	**Live Event**
SANS San Francisco 2014	**San Francisco, CAUS**	**Jul 14, 2014 - Jul 19, 2014**	**Live Event**
SANS London Summer 2014	**London, GB**	**Jul 14, 2014 - Jul 21, 2014**	**Live Event**
FOR518 Mac Forensic Analysis	**OnlineVAUS**	**Apr 22, 2014 - Apr 27, 2014**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**