

# سیسکو به پارسی



آشنایی با Cisco MARS

نوشته:

شفق زندی

<http://blog.shafagh.com/persian>

<http://forum.shafagh.com>

سایت سیسکو به پارسی

انجمن سیسکو به پارسی

## مقدمه

این ماجرا به اواخر سال ۲۰۰۲ یا ۱۳۸۱ برمیگردد...

بخاطر دارم صبح حدود ساعت ۱۰ که به شرکت رسیدم متوجه گراف MRTG شدم که بیانگر مقدار قابل توجه ای Receive پهنای باند اینترنت بود. بعد از بررسی Port Utilization روی سویچ ها متوجه شدم این ترافیک مربوط به Download هیچ یک از کامپیوتر ها و سرورهای داخل شبکه نیست متوجه Alert های IDS شدم (آن موقع IDS ی از شرکت ISS داشتیم که بعدا توسط IBM خریداری شد) ترافیکی زیاد به مقصد پورت SQL را نشان میداد. در آن روزها بازار کرم های اینترنتی (Worm) مشابه امروز داغ نبود. حمله برای Signature های IDS ناشناس بود (Zero Day) و تنها از غیرمعمول بودن آن خبر میداد (Anomaly Detect) و فرستندگان را در حال Scanning برای طعمه روی این پورت نشان میداد.



به SANS رجوع کردم... دیدم ورمی جدید آمریکا و اروپا را فرا گرفته که از Vulnerability های Microsoft SQL استفاده میکند و توسط این Exploit خود را در اینترنت پخش کرده است. اما در گراف های Traffic Monitor بنظر میرسید این ترافیک هنوز ایران را فرا نگرفته و ما از اولین شبکه هایی بودیم که این ترافیک را روی Sensor های IDS روی PIX525 ، detect کردیم. با موسسه فیزیک نظری که تامین کننده اینترنتمان بود تماس گرفتیم و فرستنده را معرفی کردیم تا روی دستگاه های خود ببندد لذا این ترافیک برای ما در دروازه ورودی شبکه محسوب نشده و پهنای باند ورودی خود را حفظ کنیم.

از جریان بالا چند نتیجه میتوان گرفت، IDS و فایروال کار خود را بخوبی انجام دادند اما وقتی Log های آنها مورد توجه قرار گرفت که روی MRTG تغییر گراف را مشاهده کردیم. پس جای یک Event Correlation و جریانی که Log ها را آنالیز و شسته رفته در اختیار ما قرار دهد در آن روزگار کم بود. اگر ترافیک این حمله در ابعاد کوچکتری بود و آن روز فرصت بررسی نداشتیم یا این کار را از روی تنبل بودن ذات آدمی به فردا موکول میکردیم دو ابزار امن سازی فوق نیز کارآمدی خود را تا حدودی از دست میدهند. حمله فوق موج اول Slammer بود و فردای آن روز ویروس ایران و اخبار را فراگرفت... حال با این مقدمه می توانیم به سوال یکی از دوستان در مورد CS-MARS بپردازیم...



Slammer سومین حمله کرم های اینترنتی در آن سال ها پس از Code Red و NIMDA بود (NIMDA همان ADMIN چپه شده است!) چند وقت قبل از Slammer، کرم Code Red که حمله هکرهای چینی (موج ارتش سرخ) به آمریکا بخاطر اعتراض به سقوط هواپیمای مسافربری چین بود، اینترنت را با استفاده از حفره های امنیتی و Exploit های IIS فرا گرفته بود، که البته بازار خوبی را برای متخصصین شبکه به همراه داشت! چندین سرویس دهنده ایرانی و موسسه دولتی دچار مشکل شدند در حالیکه IIS های ما بخاطر داشتن CSA یا Cisco Secure Agent که Host Intrusion Prevention سیسکو است به مشکلی برنخوردند.

## آشنایی با Cisco Secure MARS

مارس یک راه حل برای دریافت Log از روتر، سویچ، فایروال، IPS، آنتی ویروس ها و همچنین Log و Event های سرورها و نهایتاً آنالیز و به هم ربط دادن آن هاست. به این فرایند که اتفاقات را به هم مرتبط میسازد Event Correlation میگوییم.

این تکنولوژی توسط شرکت Protego که بعداً توسط سیسکو خریداری شد ارائه گردید. MARS یک راه حل پیشرفته STM یا Security Threat Mitigation است و بصورت سخت افزاری ارائه میشود. سیستم عامل لینوکس Oracle روی سخت افزار نصب شده و در مدل های زیر تولید میشود:

20,25,50,55,100,110,200,210,GC,GC2,GCR,GC2R



تفاوت این مدل های مختلف در قدرت پروسینگ تعداد Log در ثانیه و گنجایش Hard Disk می باشد. نسخه فعلی نرم افزار سیستم عامل CS-MARS نسخه ۶.۰.۳ است. (در زمان نگارش)

برای تنظیم اولیه مارس باید با کابل کنسول با سرعت باند ۱۹۲۰۰ به آن وصل شویم! برخلاف اکثر محصولات سیسکو که ۹۶۰۰ هستند. مارس یکی از ابزارهای Cisco Self-Defending Network است. این عنوان به راه کارها و ادوات سیسکو اشاره میکند که شبکه را توسط خود ابزار شبکه امن نگه میدارند اجزایی مثل IPS, Firewall و غیره. مارس میتواند گراف شبکه را بکشد و براساس اتفاقاتی که دریافت میکند به شما راه کار جلوگیری از حملات را ارائه کند.

اولین گام بعد از تنظیم IP روی دستگاه وارد شدن به محیط گرافیکی GUI آن است که روی SSL کار میکند. کلمه عبور و نام کاربری قراردادی pncadmin است که از PNMARS یا مارس زمان Protego ارث برده شده...



**Login Incorrect.**

Login Name:

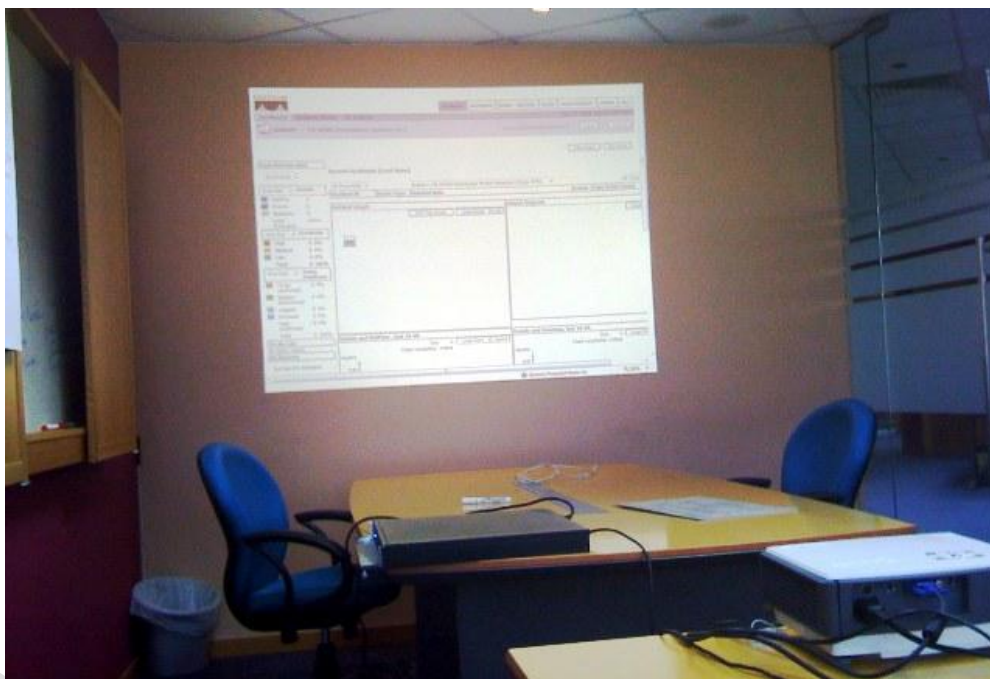
Password:

Type:

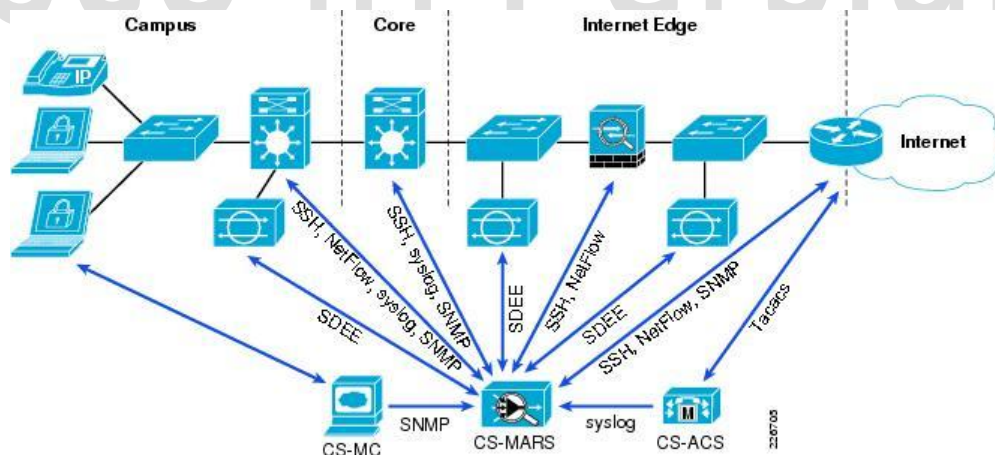
پس از ورود به سیستم حتما باید License آنرا وارد کرد که در این جا من به مشکل جدی برخورددم. یادم نبود، دستگاه را کجا گذاشتم پس از چند دقیقه ای جستجو و باز کردن پنل جلوی دستگاه License آن نمایان میشود:



بعد از وارد کردن کد License صفحه Dashboard ظاهر میشود:



دستگاه های شبکه را تنظیم میکنیم تا توسط Syslog، NetFlow، SNMP، SDEE اتفاقات رخ داده در شبکه را به مارس ارسال کنند.



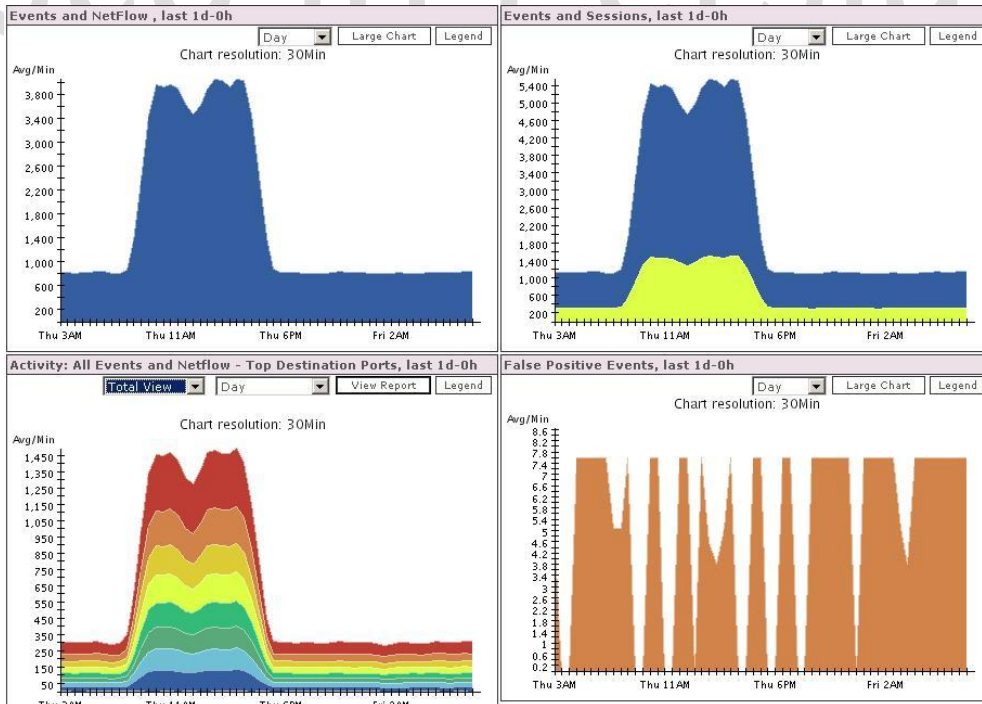
یکی از نکات قابل توجه مارس Data Reduction یا کم کردن دیتایی است که Admin باید با آن روبرو شود فرض کنیم یک حمله طول مسیری را طی میکند تا به مقصد برسد در این بین ۴ دستگاه Event به مارس ارسال میکند و مارس این Event ها متوجه میشود که مربوط به یک Session هستند و تنها به شما وقوع یک Incident را نشان میدهد و در صورت تمایل جزئیات را در اختیار شما قرار میدهد.

در تصویر زیر صفحه Dashboard مارس را میبینیم برای اینکه همه چیز مثل دنیای نا امن واقعی اینترنت بنظر برسد تعداد زیادی Packet های مختلف حمله و ویروس را در شبکه ایجاد کردم. پس از ۴۸ ساعت کار ۲۶۶۱۳۶۴ اتفاق ثبت گردیده که در این بین ۶۳ درصد صرفه جویی در جمع آوری Data صورت گرفته است.

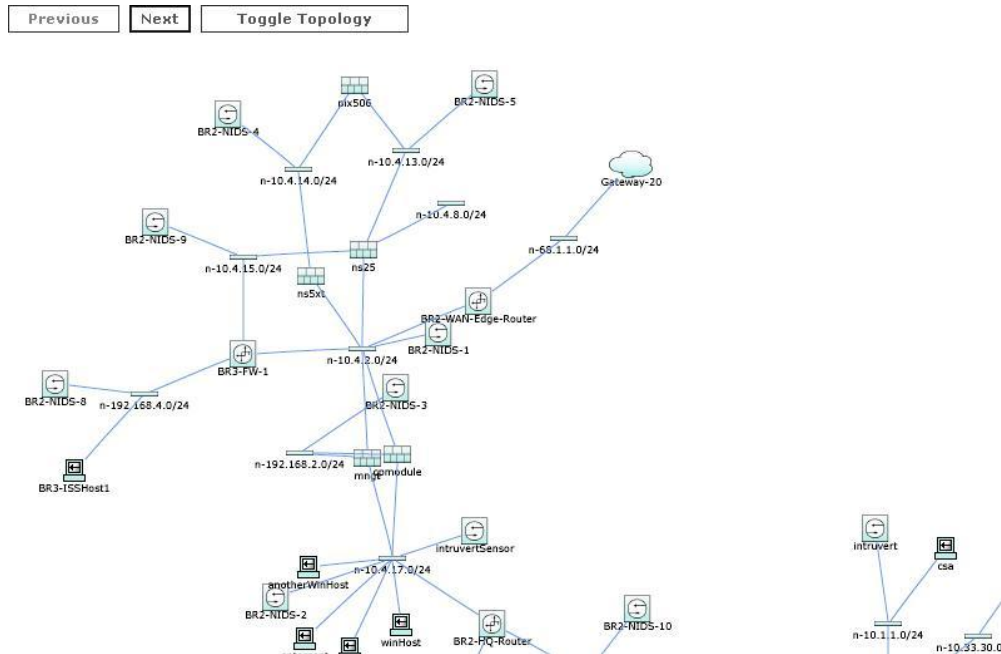
The screenshot shows the Cisco MARS dashboard interface. At the top, there are navigation tabs: SUMMARY, INCIDENTS, QUERY / REPORTS, RULES, MANAGEMENT, ADMIN, and HELP. Below this, the dashboard displays 'Recent Incidents' with a table listing incident IDs, event types, matched rules, action times, and paths. A 'HotSpot Graph' and an 'Attack Diagram' are also visible, showing network activity and attack patterns respectively. On the left side, there are summary statistics for '24 Hour Events' and '24 Hour Incidents'.

Incident ID	Event Type	Matched Rule	Action Time	Path	Cases
1:2439680472	Built/teardown/permitted IP connection	System Rule: Client Exploit - Mass Mailing Worm	Apr 24, 2009 7:30:34 AM PDT - Apr 24, 2009 7:40:27 AM PDT		
1:2439680471	Built/teardown/permitted IP connection	System Rule: Client Exploit - Mass Mailing Worm	Apr 24, 2009 7:20:29 AM PDT - Apr 24, 2009 7:30:31 AM PDT		
1:2439680469	IIS Dot Dot EXECUTE, IIS Dot Dot Crash, WWW WinNT cmd.exe Exec, WWW IIS Unicode Directory traversal, IIS CGI Double Decode	Nimda Rule	Apr 24, 2009 7:21:53 AM PDT		
1:2439680470	IIS Dot Dot Crash, WWW WinNT cmd.exe Exec, WWW IIS Unicode Directory traversal, IIS CGI Double Decode	System Rule: Server Attack: Web - Attempt	Apr 24, 2009 7:21:53 AM PDT		
1:2439680468	Built/teardown/permitted IP connection	System Rule: Client Exploit - Mass Mailing Worm	Apr 24, 2009 7:10:30 AM PDT - Apr 24, 2009 7:20:09 AM PDT		

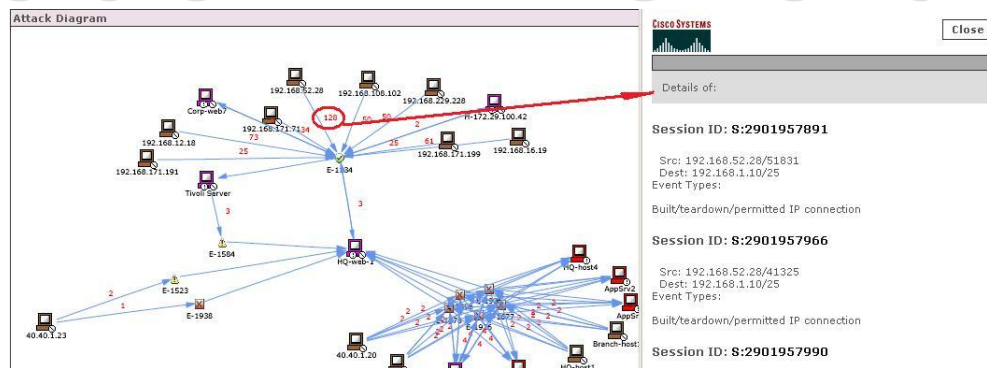
در تصویر زیر نمودار حملات در سی دقیقه اخیر نشان داده شده است.




یکی از قابلیت های مارس ترسیم توپولوژی شبکه بصورت اتوماتیک است.




در نمودار زیر بردار حملات از هکر به مقصد نشان داده شده. همانطور که مبینید در یکی از حملات ۱۲۸ اتفاق ثبت شده که با کلیک روی آن از جزئیات آن مطلع میشویم. حمله فوق به پورت ۲۵ یا سرویس SMTP است.



به بخش Incident میرویم تا این حمله را بررسی کنیم. در تصویر زیر Incident از پیش تعریف شده ای را می بینیم که وقتی دستگاهی در بازه زمانی مشخص ۲۰ بار به یک سرور SMTP کند در لیست حمله کنندگان قرار میگیرد.


SUMMARY INCIDENTS QUERY / REPORTS RULES MANAGEMENT ADMIN HELP

Incidents False Positives Cases Apr 24, 2009 7:22:11 AM PDT



INCIDENTS | CS-MARS Standalone: pnmars v4.1
 Login: user, demo (demo) ::
Logout Activate

Select Case: 
View Cases New Case


Incident ID:  Show  
 Session ID:  Show


Offset	Open (	Source IP	Destination IP	Service Name	Event	Device	Reported User	Keyword	Severity	Count	Close
1		SAME, ANY	ANY, ANY	smtp (src port: ANY, dst port: 25, proto: UDP), smtp (src port: ANY, dst port: 25, proto: TCP), smtps (src port: ANY, dst port: 465.	ANY	ANY	None	ANY	ANY	20	

وقتی روی این اتفاق کلیک میکنیم وقوع آن را بصورت یک Session به ما نشان میدهد. این حمله یک بار اتفاق افتاده اما در سه جا شناسایی شده ابتدا موقع عبور از فایروال سپس توسط سویچ ۶۵۰۰ و پس از آن روی روتر شبکه دیده شده است. دقت کنید که پس از عبور از فایروال IP دستگاه مقصد که سرور ماست تغییر میکند زیرا NAT شده اما MARS این اتفاق را بصورت هوشمندانه متوجه شده و آنرا حمله ای جداگانه نشان نمیدهد.


SUMMARY INCIDENTS QUERY / REPORTS RULES MANAGEMENT ADMIN HELP

Incidents False Positives Cases Apr 24, 2009 7:22:11 AM PDT


[pnmars] Raw Events - Windows Internet Explorer


Apr 24, 2009 7:25:35 AM PDT

Standalone: pnmars v4.1 Login: user, demo (demo) :: Close

Event / Session / Incident ID	Reporting Device	Time	Raw Message
E:2902015040, S:2902015040, I:2439680468	HQ-FW-1	Apr 24, 2009 7:10:30 AM PDT	10.33.10.2 <142>%PIX-6-302013: Built outbound TCP connection 2000 for inside:192.168.1.10/25 (100.1.4.10/25) to outside:192.168.171.199/5255 (192.168.171.199/5255)
E:2902015039, S:2902015040	HQ-SW-1-msfc	Apr 24, 2009 7:10:30 AM PDT	172.30.1.2 Mon Jun 9 14:46:31 2003 <46>485232: Jun 9 14:46:29 PDT: %SEC-6-IPACCESSLOGP: list outside permitted tcp 192.168.171.199 (5255) -> 100.1.4.10(25), 1540 packet
E:2902015041, S:2902015040	HQ-WAN-Edge-Router	Apr 24, 2009 7:10:30 AM PDT	100.1.20.2 Mon Jun 9 14:46:31 2003 <46>485232: Jun 9 14:46:29 PDT: %SEC-6-IPACCESSLOGP: list CSM-acl-FastEthernet0/0 permitted tcp 192.168.171.199(5255) -> 100.1.4.10(25), 1540 packet

باکلیک روی Incident Vector بردار حملات به webserver را بصورت جداگانه به همراه توضیحات پکت های دریافت شده در سمت چپ تصویر را برای ما نمایان میکند.



Incident ID	Event Type	Matched Rule	Action	Time	Path
2439680471	Built/teardown/permitted IP connection	System Rule: Client Exploit - Mass Mailing Worm		Apr 24, 2009 7:20:20	

[pnmars] Incident Graph for I:2439680471 - Windows Internet Explorer

Session ID: S:2902023413  
 Src: 192.168.229.228/23016  
 Dest: 192.168.1.10/25  
 Event Types: Built/teardown/permitted IP connection

Session ID: S:2902023497  
 Src: 192.168.229.228/5771  
 Dest: 192.168.1.10/25  
 Event Types: Built/teardown/permitted IP connection

Session ID: S:2902023696

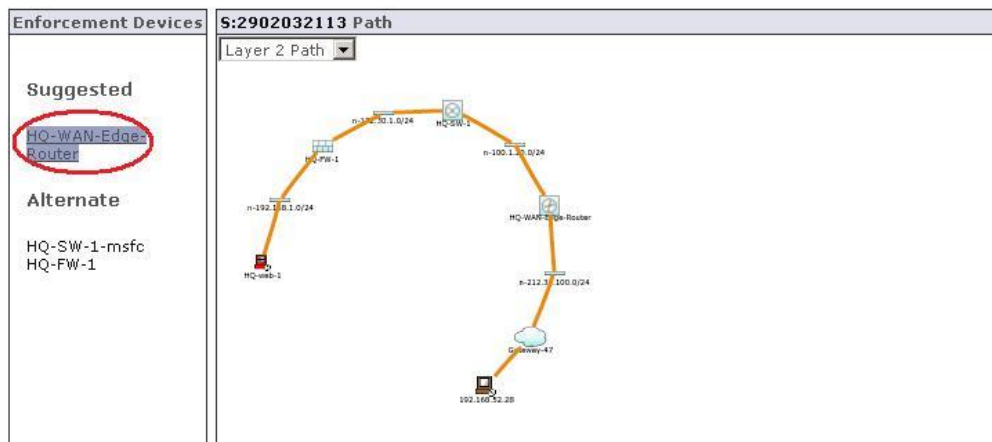
اگر روی Path Information کلیک کنیم نمودار عبور بسته ها در طول شبکه از Hacker به Target را نشان میدهد:

Incident ID	Event Type	Matched Rule	Action	Time	Path
2439680471	Built/teardown/permitted IP connection	System Rule: Client Exploit - Mass Mailing Worm		Apr 24, 2009 7:20:20	

[pnmars] Incident Graph for I:2439680471 - Windows Internet Explorer

Previous Next Toggle Topology

یکی از قابلیت های جالب MARS این است که به شما پیشنهاد میدهد چگونه و با چه Access-list ی روی کدام دستگاه جلوی حمله را بگیرید یا اینکه خودش دست به کار شده و در لایه دو MAC آدرس حمله کننده را روی پورت سویچ فیلتر میکند...



در تصویر زیر راه حل مارس بستن پورت SMTP سرور برای دستگاه هکر است.

**Enforcement Device: HQ-WAN-Edge-Router**, Suggested

Default gateway: 212.31.100.1

**L3 Enforcement Device Information**

Device	Type	Manager	Children	Log To	Collects From	Info
HQ-WAN-Edge-Router	Cisco IOS 12.2	PN-MARS on pnmars		PN-MARS on pnmars		

**Interface Information**

Direction	Interface Name	MAC Address	MAC Update Time
Inbound	FastEthernet0/0	N/A	N/A
Outbound	FastEthernet1/0	N/A	N/A

**Recommended L3 Policies/Commands**

ip access-list extended CSM-acl-FastEthernet0/0  
deny tcp host 192.168.52.28 host 100.1.4.10 eq 25

Or

ip access-list extended CSM-acl-FastEthernet0/0  
deny tcp host 192.168.52.28 any

مارس به محصولات سیسکو محدود نشده و از هر دستگاهی حتی سرورهای مایکروسافت و برنامه های آنتی ویروس میتواند Log دریافت کرده و بصورت همزمان رخداد ها را نمایش دهد. بدین صورت با کمک این تکنولوژی مدیریت امنیت شبکه بسیار ساده تر و در عین حال پویا تر از قبل میشود. به همین دلیل است که امروزه وقتی مشتریان برای مشاوره و طراحی امنیت شبکه به سراغ ما می آیند ما راه حلی برای Perimeter Security یا امنیت در دروازه ورودی شبکه ارائه

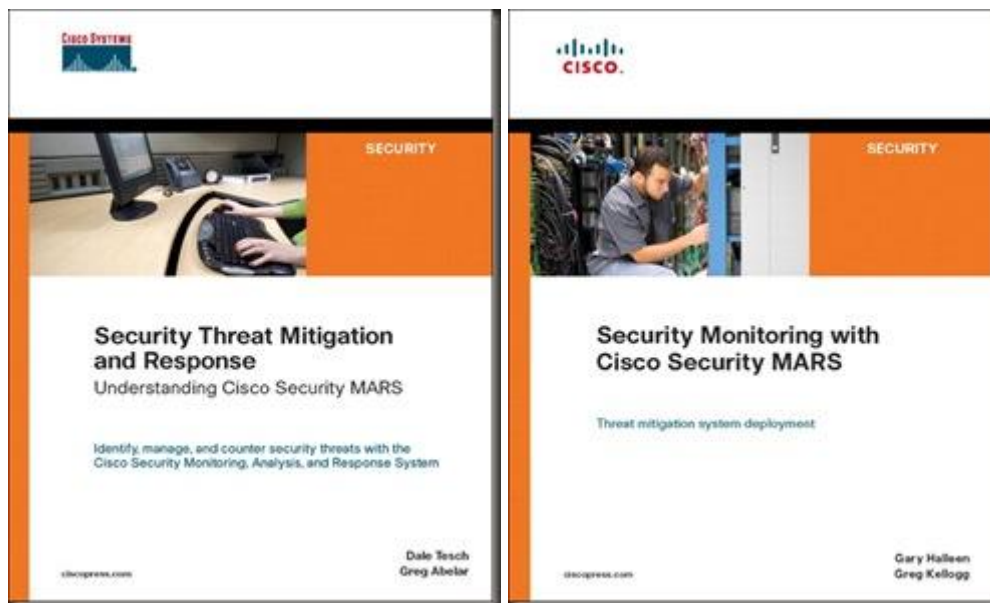


نمیکنیم چراکه این مدل قدیمی قابلیت جلوگیری حملات از داخل شبکه را ندارد امنیت باید در نقطه نقطه شبکه پیاده شود با خریدن یک BOX بدست نمی آید.



# Cisco in Persian

برای MARS انتشارات سیسکو دو کتاب منتشر کرده که مطالعه هر دو آنها ضروری است:



کتاب Security Monitoring with Cisco Security MARS نوشته گری هالن و گرگ کیلاگ برای محافظت از شبکه، نظارت و دفع حملات بکمک مارس، استفاده از مارس همراه با NAC و سازگاری و دستیابی به استانداردهای PCI و Regularity ها نوشته شده:

<http://www.ciscopress.com/bookstore/product.asp?isbn=1587052709>

کتاب Security Threat Mitigation and Response: Understanding Cisco Security Mars برای آشنایی و نحوه برخورد با انبوه Log ها و مدیریت سیستم های امنیتی منتشر شده است:

<http://www.ciscopress.com/bookstore/product.asp?isbn=1587052601>

برای دریافت Configuration Guide های سیسکو مارس نیز میتوانید به سایت سیسکو رجوع کنید:

<http://www.cisco.com/go/mars>

[http://www.cisco.com/en/US/products/ps6241/tsd\\_products\\_support\\_configure.html](http://www.cisco.com/en/US/products/ps6241/tsd_products_support_configure.html)

موسسه SANS در مورد تنظیم مارس:

[http://www.sans.org/reading\\_room/whitepapers/logging/configuring\\_and\\_tuning\\_cisco\\_csmars\\_2044](http://www.sans.org/reading_room/whitepapers/logging/configuring_and_tuning_cisco_csmars_2044)

## Update!

از ۳ June سال ۲۰۱۱ فروش مارس متوقف خواهد شد و پس از چندی پشتیبانی و ارائه Update برای آن نیز پایان خواهد یافت. مارس بزرگترین پیاده سازی SIEM در چند سال اخیر است که سیسکو هم اکنون جایگزینی برای آن ندارد.

The screenshot displays the Cisco MARS Incident Details interface. At the top, there are navigation tabs: SUMMARY, INCIDENTS, QUERY / REPORTS, RULES, MANAGEMENT, ADMIN, and HELP. The current view is 'INCIDENTS' for 'CS-MARS Standalone: pnmars v4.2'. The incident ID is 2908116, and the session ID is also 2908116. The rule name is 'System Rule: State Change: Network Device' with a status of 'Active'. The description states: 'This correlation rule detects significant network status state change events such as system failing, failover occurring, interface cards coming up down, etc.' Below this, there is a table with columns: Offset, Open, Source IP, Destination IP, Service Name, Event, Device, Reported User, Keyword, Severity, Count, and Close Op. Two rows are visible in this table. At the bottom, there is a table for the incident details with columns: Offset, Session / Incident ID, Event Type, Source IP/Port, Destination IP/Port, Protocol, Time, Reporting Device, Reported User, Path / Mitigate, and False Positive. One row is shown for an event on April 24, 2007, at 8:30:20 PM PDT, reported by user c3750, with a 'False Positive' status.

دوستانی که برای CCSP آماده میشوند بهتر است روی امتحان [642-545 MARS](http://642-545.MARS) حساب باز نکنند که بزودی از بین خواهد رفت.