سیسکو به پارسی

آشنایی با Cisco MARS

نوشته:

شفق زندی

سایت سیسکو به پارسی http://blog.shafagh.com/persian

انجمن سیسکو به پارسی http://forum.shafagh.com

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 بررسیPort Utilization روی سوییچ 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 پورتSQL 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 و 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 قراردهد 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 وNIMDA 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 بهمراه داشت! چندین سرویس دهنده ایرانی و موسسه دولتی دچار مشکل شدند در حالیکه IIS های ما بخاطر داشتن CSA یا Cisco Secure Agentکه Host Intrusion Prevention سیسکو است به مشکلی برنخوردند.

آشنایی با Cisco Secure MARS

مارس یک راه حل برای دریافت Log از روتر، سوییچ، فایروال،IPS ، آنتی ویروس ها و همچنین Log و Event های سرورها و نهایتا 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 بعدا 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 با Oracle روی سخت افزار نصب شده و در مدل های زیر تولید میشود:

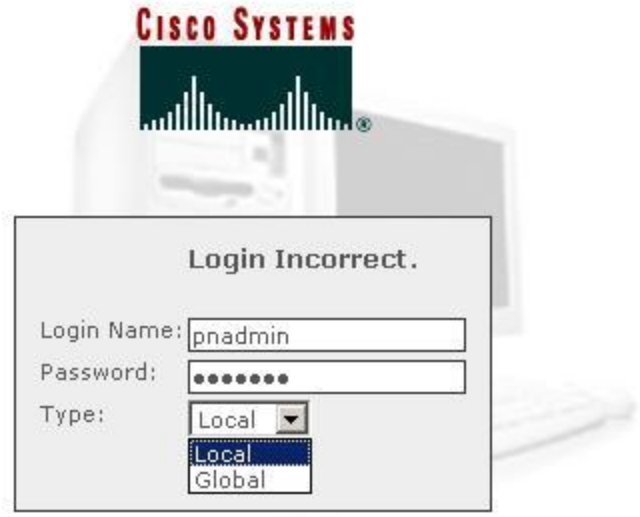
20,25,50,55,100,110,200,210,GC,GC2,GCR,GC2R

Cisco in Persian

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 مثال 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.

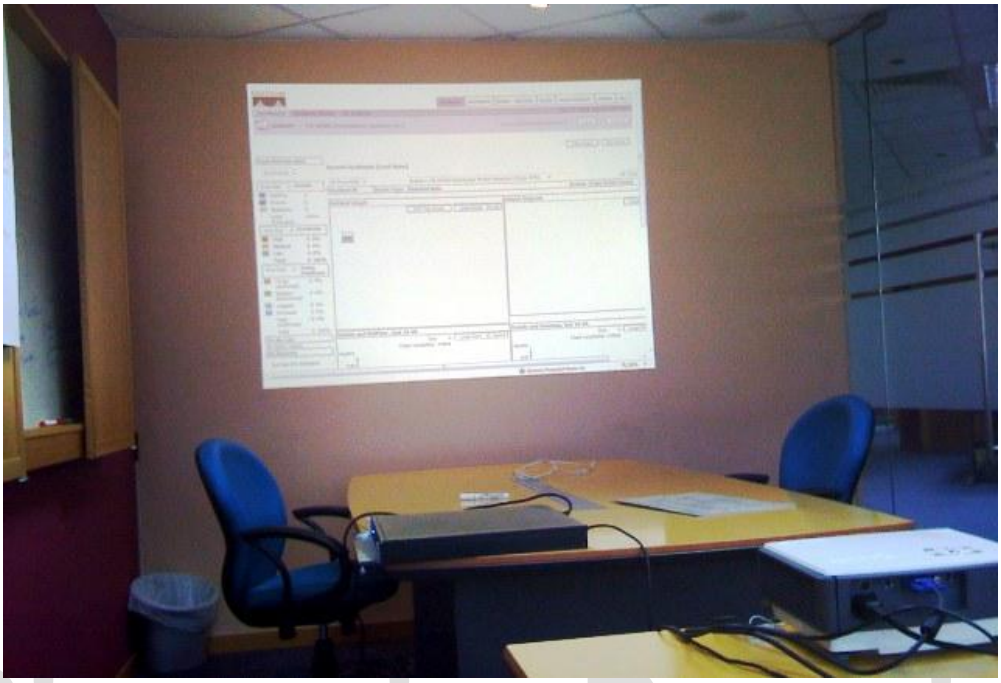
اولین گام بعد از تنظیم IP روی دستگاه وارد شدن به محیط گرافیکی GUI آن است که روی SSL کار میکند .کلمه عبور و نام کاربری قراردادی pnadmin است که از PNMARS یا مارس زمان Protego ارث برده شده...



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

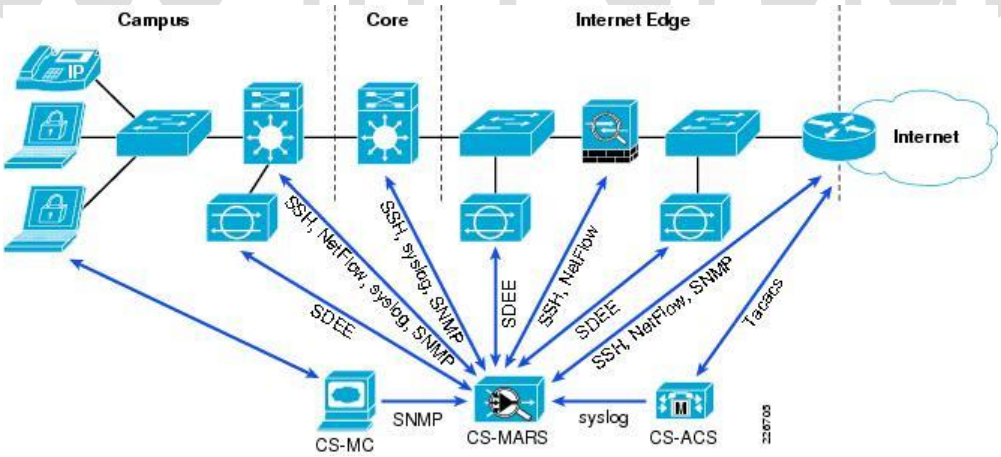
Cisco in Persian

بعد از وارد کردن کد License صفحه Dashboard ظاهر میشود:



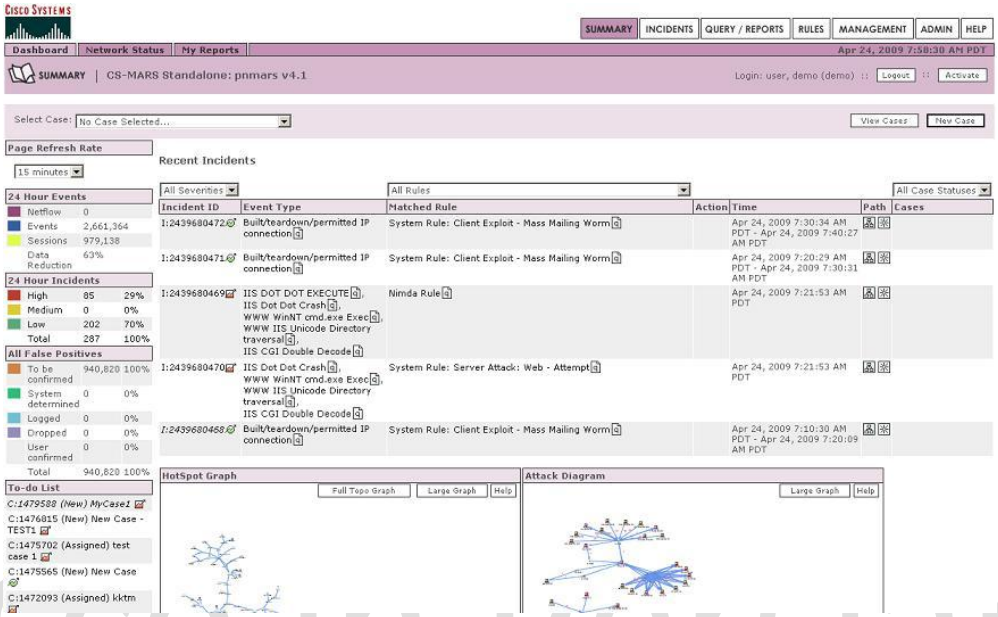
Cisco in Persian

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

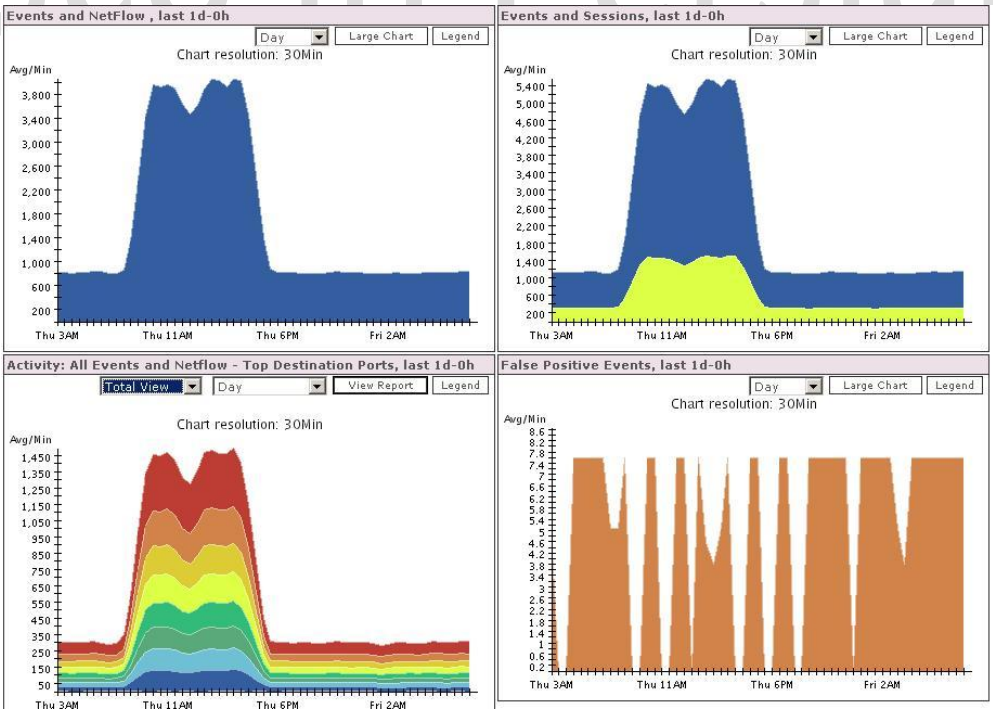


یکی از نکات قابل توجه مارس Data Reduction یا کم کردن دیتایی است که Admin باید با آن روبرو شود فرض کنیم یک حمله طول مسیری را طی میکند تا به مقصد برسد در این بین ۴ دستگاه Event به مارس ارسال میکند و مارس این Event ها متوجه میشود که مربوط به یک Session هستند و تنها به شما وقوع یک Incident را نشان میدهد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

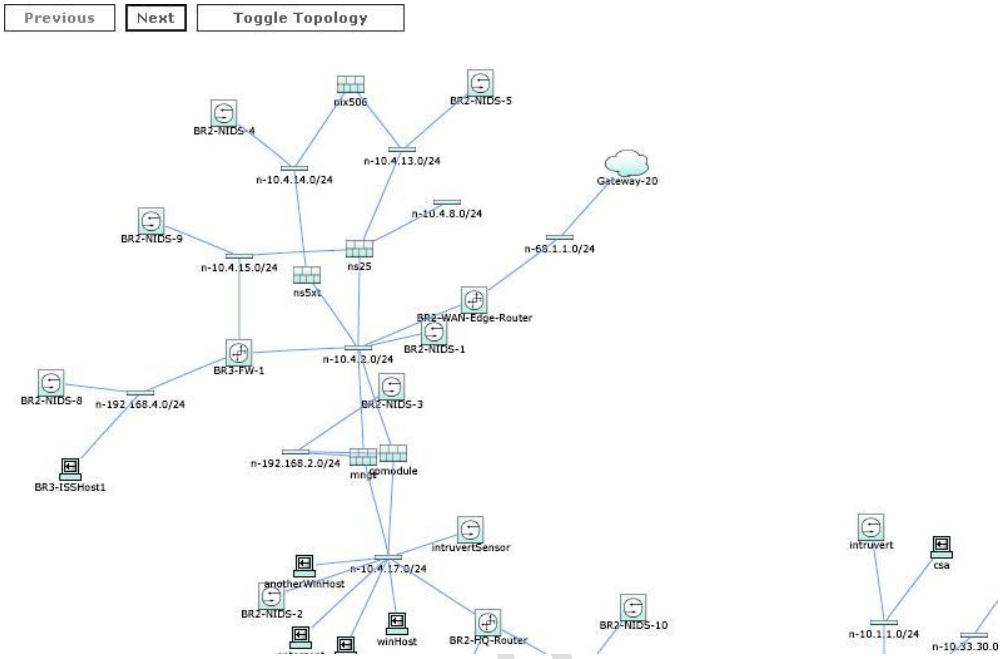


در تصویر زیر نمودار حملات در سی دقیقه اخیر نشان داده شده است.

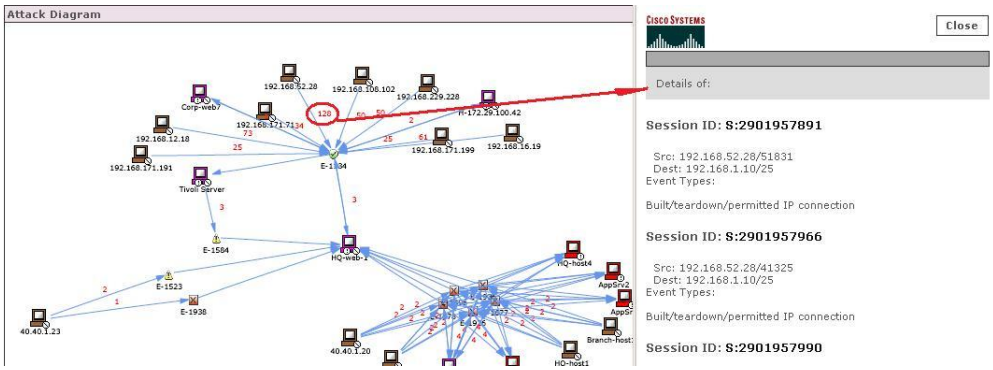


Cisco in Persian

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

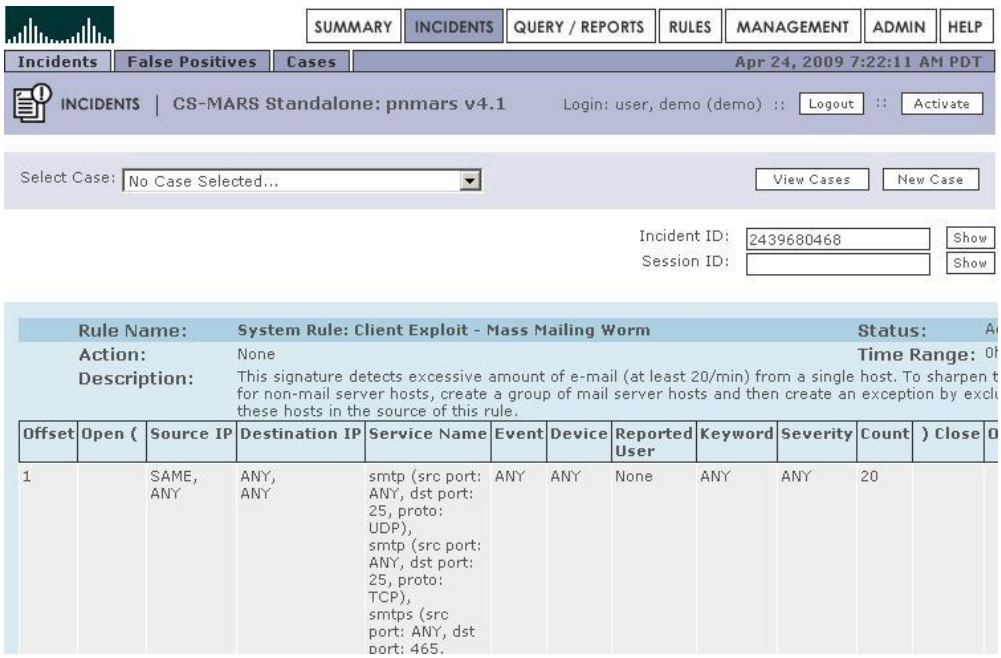


در نمودار زیر بردار حملات از هکر به مقصد نشان داده شده. همانطور که میبینید در یکی از حملات ۱۲۸ اتفاق ثبت شده که با کلیک روی آن از جزییات آن مطلع میشویم. حمله فوق به پورت ۲۵ یا سرویس SMTP است.



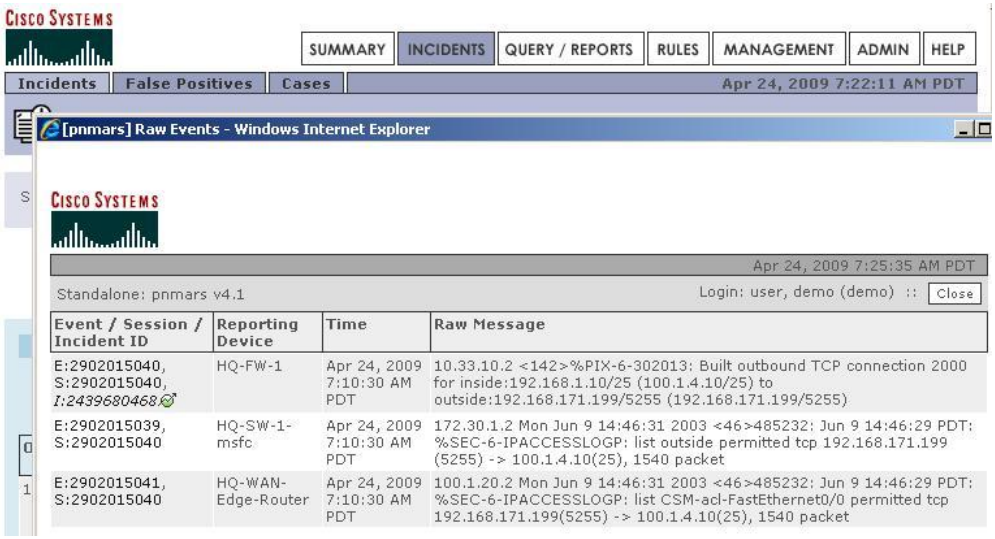
به بخش Incident میرویم تا این حمله را بررسی کنیم. در تصویر زیر Incident از پیش تعریف شده ای را می بینیم که وقتی دستگاهی در بازه زمانی مشخص ۲۰ بار به یک سرور SMTP کند در لیست حمله کنندگان قرار میگیرد.

Cisco in Persian

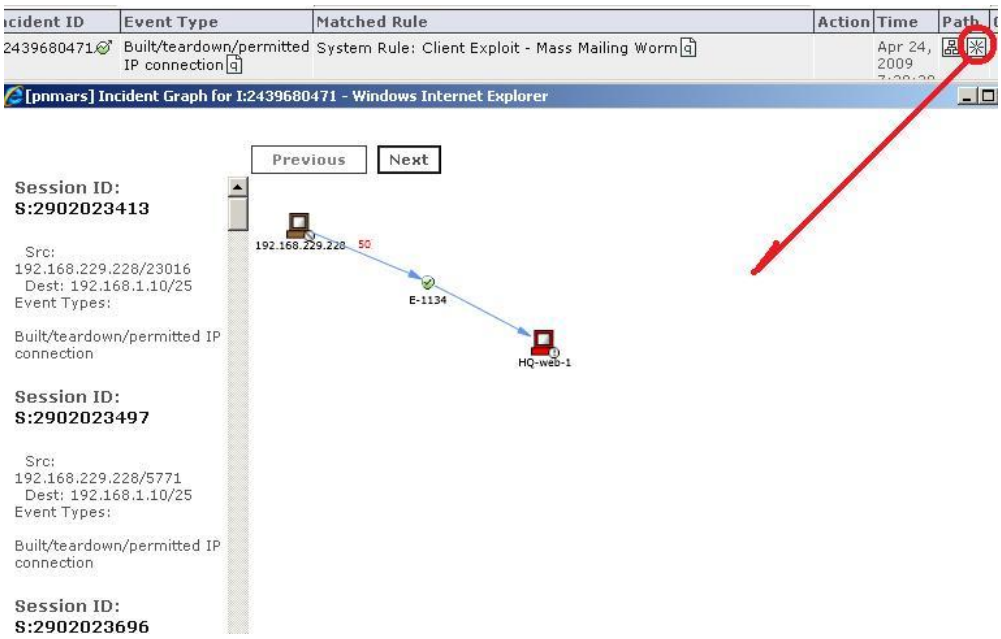


وقتی روی این اتفاق کلیک میکنیم وقوع آن را بصورت یک Session به ما نشان میدهد. این حمله یک بار اتفاق افتاده اما در سه جا شناسایی شده ابتدا موقع عبور از فایروال سپس توسط سوییچ ۶۵۰۰ و پس از آن روی روتر شبکه دیده شده است. دقت کنید که پس از عبور از فایروال IP دستگاه مقصد که سرور ماست تغییر میکند زیرا NAT شده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

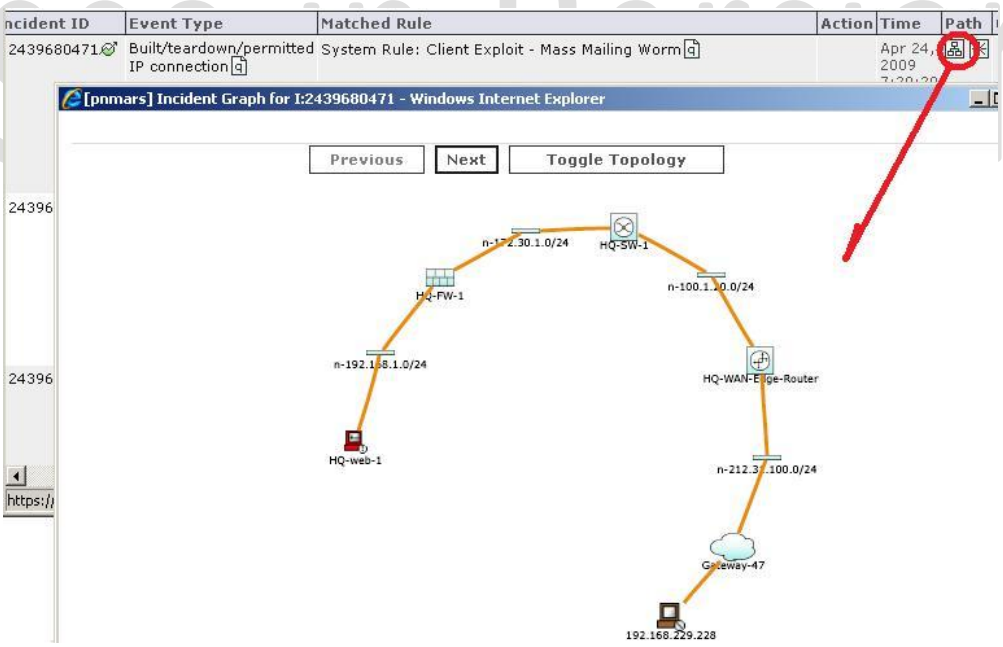
Cisco in Persian



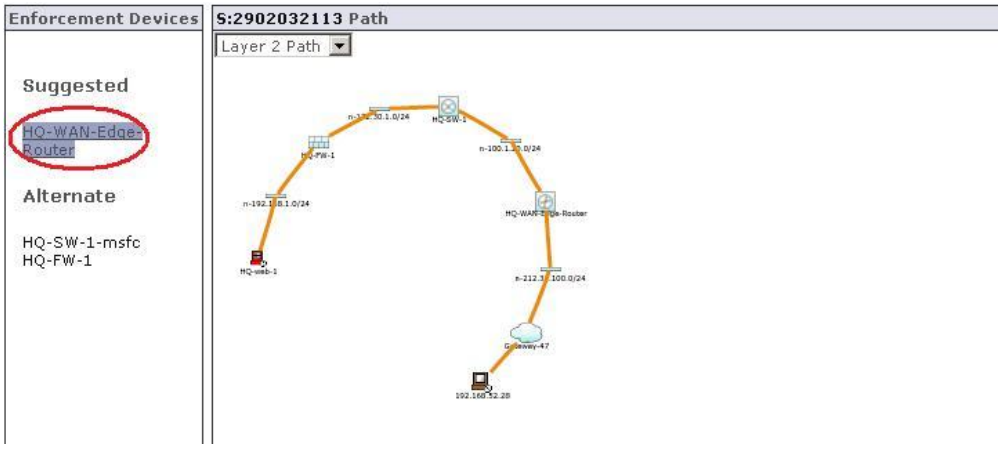
باکلیک روی Incident Vector بردار حملات به webserver را بصورت جداگانه بهمراه توضیحات پکت های دریافت شده در سمت چپ تصویر را برای ما نمایان میکند.



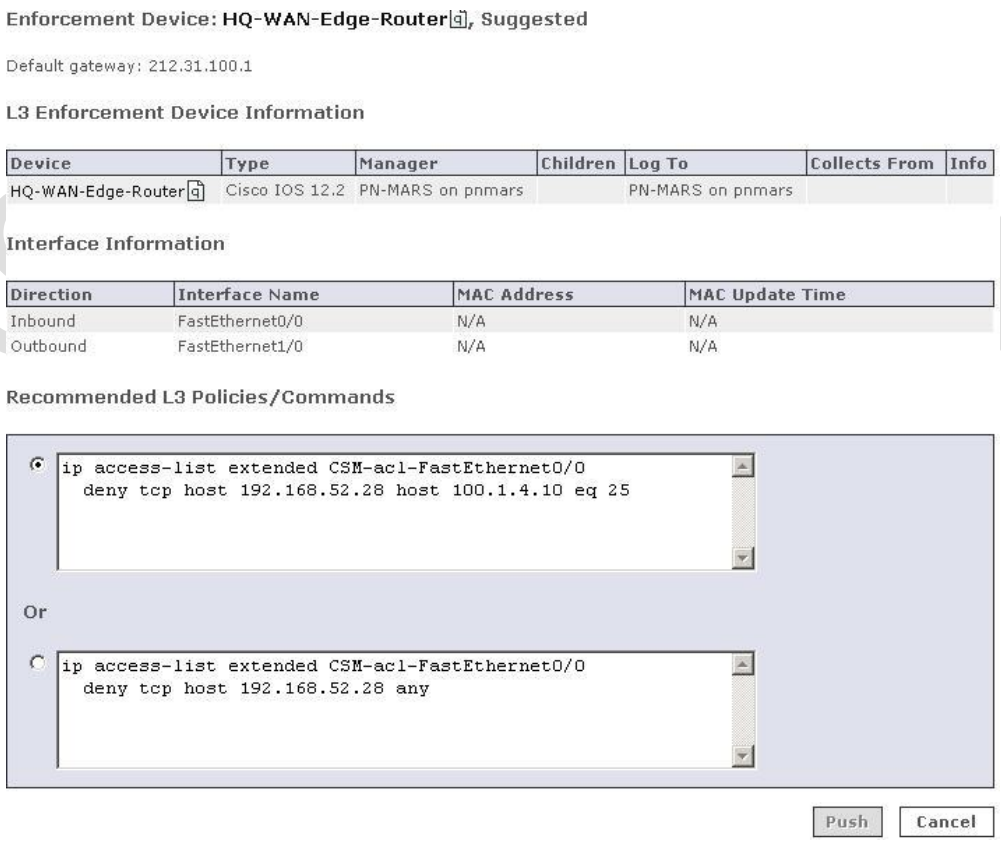
اگر روی Path Information کلیک کنیم نمودار عبور بسته ها درطول شبکه از Hacker به Target را نشان میدهد:



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 سوییچ فیلتر میکند...



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

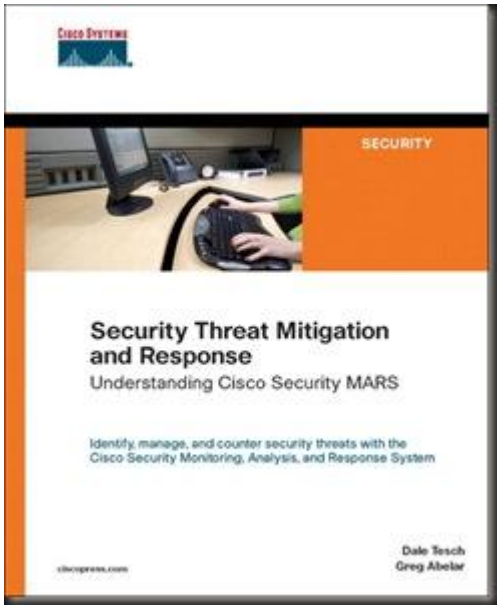


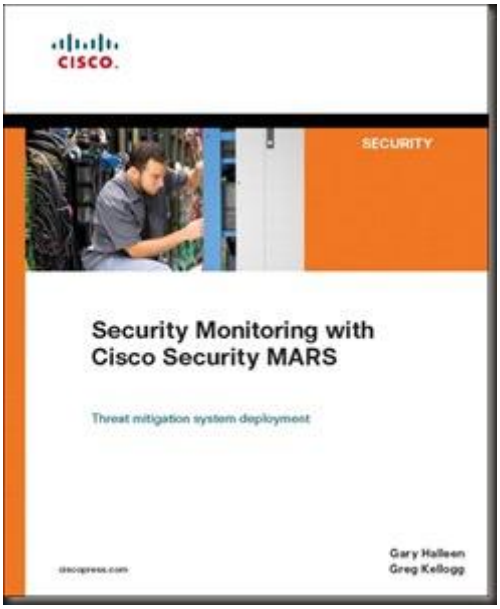
مارس به محصولات سیسکو محدود نشده و از هر دستگاهی حتی سرورهای مایکروسافت و برنامه های آنتی ویروس میتواند Log دریافت کرده و بصورت همزمان رخداد ها را نمایش دهد. بدین صورت با کمک این تکنولوژی مدیریت امنیت شبکه بسیار ساده تر و در عین حال پویا تر از قبل میشود. به همین دلیل است که امروزه وقتی مشتریان برای مشاوره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

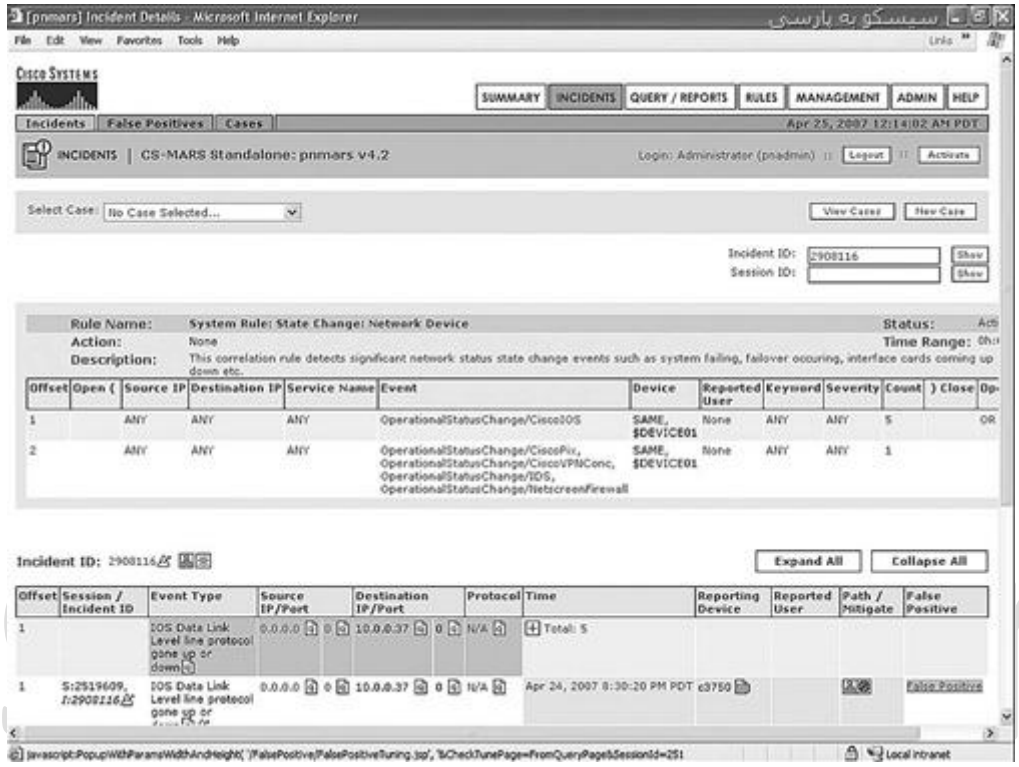
Cisco in Persian

موسسه SANS در مورد تنظیم مارس:

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.



دوستانی که برای CCSP آماده میشوند بهتر است روی امتحان 642-545 MARS حساب باز نکنند که بزودی از بین خواهد رفت.