# پروژه پیاده سازی سیستم تشخیص نفوذ snort

# در سیستم عامل FreeBSD


**تهیه کننده : محمد سلطانی**

**شماره دانشجویی: 92151151614**

**کارشناسی ارشد IT – امنیت اطلاعات**

**استاد راهنما: مهندس احمدی**


**بهمن 92**

# بخش اول:

# سیستم های تشخیص نفوذ(IDS)

- ***سیستم های تشخیص نفوذ و چگونگی کارکرد آن***

تشخیص نفوذ تحلیل بی درنگ داده های شبکه به منظور تشخیص و ثبت و هشدار در زمان بروز حملات .

- IDSها بر سه اصل استوارند:
  - "از کجا مراقبت انجام شود" : مکان ها ی منطقی راکه IDS ها باید موردکنترل قرار دهند مشخص می کند
  - "در برابر چه چیزی مراقبت انجام شود": گویای شرایطی است که باید تحت نظارت قرار گیرد و در صورت لزوم اخطار داده شود.
  - "چه عملی انجام شود": کاری است که IDS در زمان مواجهه با پارامترهای تعریف شده یا خاص انجام می دهد.
- کارکردهای IDS:

1. از IDS استفاده می کنیم تا از ارتباطات اینترنتی آن هایی که از firewall ما رد می شوند ، مراقبت کنیم .
2. بر اساس نوع بسته و ارتباط وفعالیت هایی که این ارتباطات انجام می دهند ، به IDS می گوییم که به دنبال چه حملاتی باشد.
3. مثلا به IDS می گوییم اگر فلان حمله اتفاق افتاد به من ایمیل بزن .
4. هکر شروع به اسکن کردن پورت های ک

- **شناسایی حمله** :از ملزومات اولیه برای سیستم های IDS

## o لزوم اهمیت امنیت در اینترنت

این واقعیتی است که قسمت کوچکی از طراحی شبکه مربوط به بحث امنیت است و هدف اصلی شبکه به اشتراک گذاشتن اطلاعات است .

- در بسیاری از تجارت ها از شبکه های مبتنی بر ip مثل اینترنت استفاده می کنند تا دفاتر ،کارگران وشرکای راه دور خود را وارد محیط شبکه ی مطمئن خود کنند. اینتر نت هر روز بزرگتر و بزرگتر می شود و نقاط بیشتری را بهم متصل می کند .

واضح است که هر چه اینترنت ایمن تر شوند ،شرکت ها بهتر می توانند عملکرد خودشان را به اشتراک بگذارند.

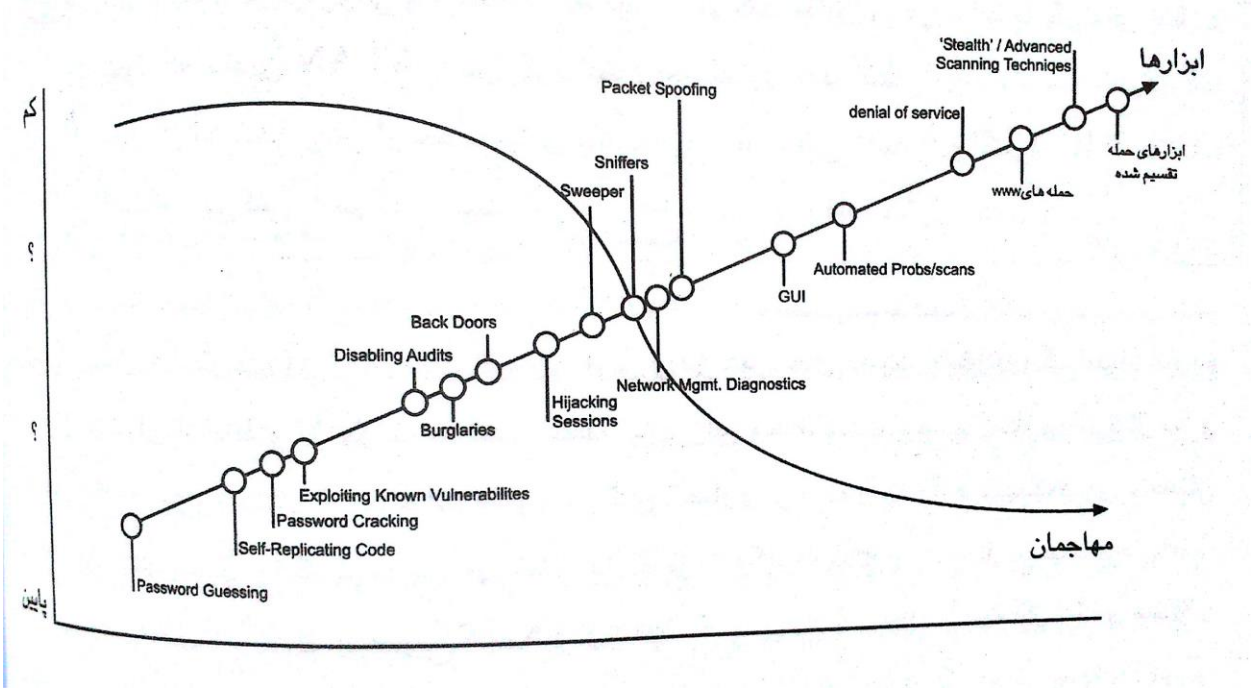
- دسترسی آسان به اینترنت ، آن را به ابزار تجاری قوی تبدیل کرده ولی در عین حال به خطر بزرگی در برابر شرکت ها تبدیل شده است.اینترنت برای اشتراک گذاری داده ها طراحی نه برای امنیت .

✓ این رسانه ی غیرایمن(اینترنت) چگونه می تواند امن شود؟

لایه های امنیتی مختلفی مثل یک بسته مسیریاب اینترنتی و یک فایروال

اما سازمان ها حتما دارای سرور ایمیل و وب سرور هستند و این سرورها از اینترنت قابل دسترسی هستند.

- با رشد اینترنت حملات حرفه ای تر شده اند ولی سطح دانش برای استفاده از این حملا ت کاهش پیدا کرده




- نه مسیریاب نه دیوار آتش نمی توانند بگویند که بسته های اینترنتی در واقعیت شامل یک خطر یا حمله هستند یا خیر . البته شاید سازمان ها ممکن است دارای یک مسئول حرفه ای باشد که سرورهای مهم شرکت را با سیاست های امنیتی از حملات مختلف ایمن کند، اما این سازمان نیاز به شناسایی حملات را مورد توجه قرار نداده.

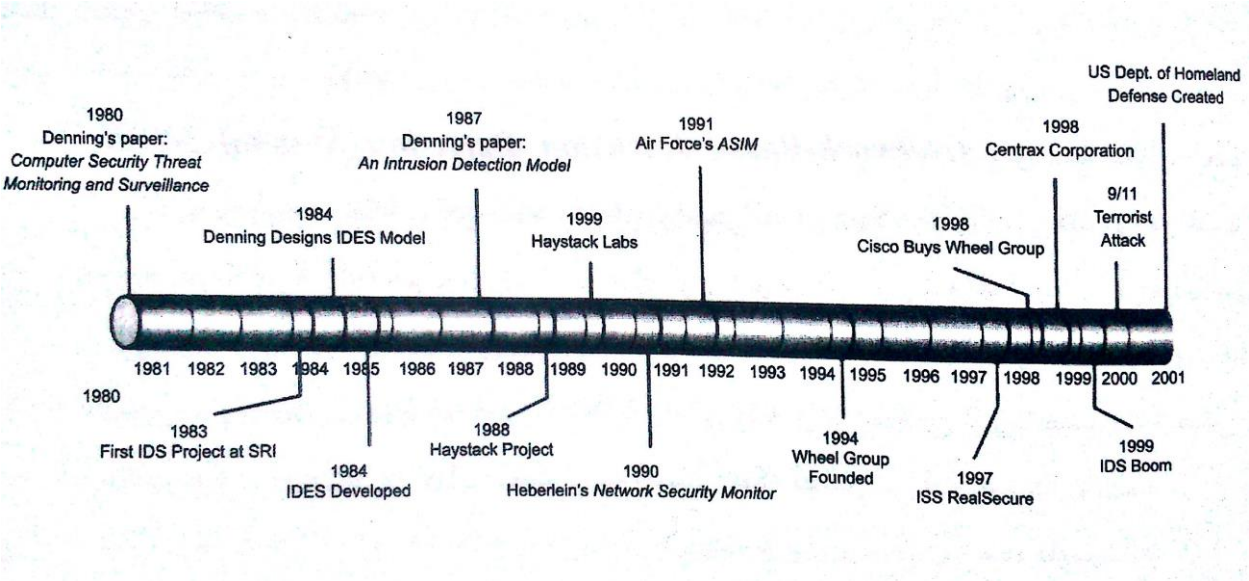
## o نیاز به سیستم های تشخیص نفوذ

- انگیزه یک مهاجم چه جاسوسی باشد ، چه سیاسی ، مالی و یا ایجاد مزاحمت ، به هر حال به شبکه حمله شده . پس نظارت و پایش این حملات نه تنها کاری معقول است ، بلکه یک ضرورت تجاری نیز محسوب می شود.
- یک IDS مثل یک سیستم اخطار برای سیستم عمل می کند، درسته در هر صورت شبکه توسط عوامل امنیتی دیگر محافظت می شود و لی هرگز آن عوامل نمی توانند تشخیص دهند که آیا قصدی برای حمله به شبکه وجود داشته یا نه؟
- هدف شناسایی تهاجم ، کنترل بخش های شبکه و شناسایی رفتار های غیر معمول و حملات و یا متوقف کردن این حملات و حتی ارائه اطلاعاتی برای دستگیری مهاجمان می باشد.

- **تاریخچه توسعه IDS**

تحقیقات در دهه 1980 با تلاش ها و نوشته های Andersonو denning آغاز شد . در دهه 80 از عملکرد های پایه ای IDS استفاده شد که بعدا نام آن را ARPANET گذاشتند.

پس از آن اعضای پروژه Haystack لابراتوار خود را برای اهداف تجاری در مورد شناسایی تهاجم مبتنی بر میزبان (HIDS) به راه انداختند.در زمینه تهاجم مبتنی بر میزبان هم فردی بنام Toddy Heberlien فعالیت هایی در دهه 1990 داشت. در آن زمان لابراتوارهای Haystack و SAIC در حال کار بر روی IDS ها بودند. گروه Wheel در سال 1994 توسط سیستم سنجش خودکار امنیت (ASIM) نیروی هوایی آمریکا و تیمی که این راه حل را ارائه کرد ، تشکیل شد.شرکت سیسکو هم این گروه را در سال 1998 خرید.



- **ویژگی های عمده IDS:**

علاوه بر مواردی که در رابطه با IDS ها در نظرگرفته می شود IDS ها باید قابلیت های زیر رانیز داشته باشد:

- **ارتباط متقابل وقایع**

در صورت وجود چند IDS در شبکه باید IDS ها تمامی وقایعی راکه حس می کنند با هم به اشتراک بگذارند.چون اگر این کار توسط IDS ها انجام نشود ، یک IDS در شبکه بعد تحت کنترل مهاجم در آمدن می تواند تبدیل به وسیله ای برای حمله به IDS ها و دستگاه های دیگر موجود در شبکه درآید.این ارتباط به مدیر شبکه این امکان را می دهد که حمله ها را ردیابی کند.

- **مدیریت حسگر متمرکز**

وجود یک سیستم که بتواند وقایعی که در شبکه توسط سرور ، مسیریاب و یا دیوار آتش ثبت می شود، کنترل کند و همچنین IDS های شبکه را مدیریت کند بسیار حیاتی است.
پس برای داشتن امنیت مناسب وجود یک سیستم مدیریت که بتواند پاسخ حسگر ها را کنترل کند و بین وقایع ارتباط برقرار کند و بتواند در مورد امنیت شبکه گزارش جامعی بدهد ، حیاتی است .

- **سیستم شناسایی حملات شبکه ای (NIDS)**

این سیستمها که به اختصار NIDS نامیده می شوند در بستر شبکه فعالیت میکنند و با پویش ترافیک شبکه و تحلیل آن در تمام لایه های مختلف شبکه، به دنبال کشف نشانه های اقدامات نفوذی و یا حملات هستندانواع حملاتی که به در سطح شبکه میتوانند وجود داشته باشند شامل حملات DOS و حملات پویش پورت هستند .این سیستمها معمولا ترافیک ورودی و یا خروجی از نقطه دسترسی شبکه

را پویش میکنند .معمولا این سیستمها از چندین حسگر نقاط مختلف برای دریافت ترافیک شبکه برخوردارند.
ویژگیهای دریافت شده از این ترافیک به پایگاه مرکزی تحلیل فرستاده می شود تا بر اساس روش های مختلف تشخیص نفوذ، اقدامات نفوذی آشکار شوند.

- **اجزای تشکیل دهنده سیستمهای تشخیص نفوذ مبتنی بر شبکه**

اجزای اصلی این سیستمها عبارتند از حسگر، سرور مدیریت و تحلیل، سرور پایگاه داده، چندین واسط کاربری و سرورهای پایگاه داده .حسگر جزئی است که ترافیک شبکه مربوط به یک یا چند بخش را پویش میکند .واسط شبکهای حسگرها طوری پیکربندی شده که تمام بستههای دریافتی را بدون در نظر گرفتن آدرس مقصد دریافت میکند .تمام حسگرها در یکی از این دو نوع هستند:

1)**نوع مبتنی بر سخت افزار :**این نوع حسگر شامل سخت افزار خاص منظوره طراحی شده به همراه نرم افزار اجرا شوند بر روی آن است .سختافزار برای استفاده جهت کاربرد حسگر بهینهسازی شده است و کارت های واسط شبکهای خاصی بر روی آنها قرار گرفته که تمام ترافیک عبوری را دریافت می کند . این افزارها معمولا شامل سیستم عاملی هستند که به صورت مستقیم توسط مدیر سیستم مورد دسترسی نیست؛ ولی واسط نرمافزاری مناسب امکان ارتباط با کاربر و بخشهای دیگر سیستم تشخیص نفوذ را فراهم میکند.

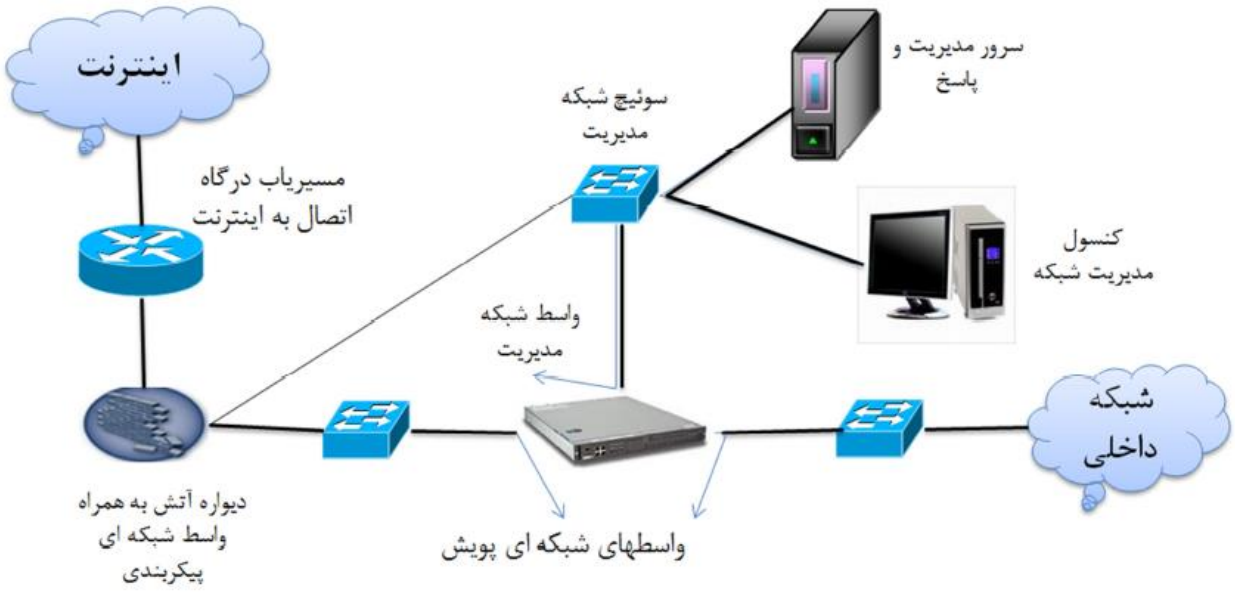
۲)**نوع مبتنی بر نرم افزار:**ا بزار تشخیص نفوذ به عنوان یک نرمافزار عرضه میشود .در این حالت ممکن است نرمافزار به همراه سیستم عامل مربوط به آن ارائه شود یا آنکه نرمافزار قابل نصب بر روی سیستم عامل های همه منظوره باشد .بسیاری از ابزارهای تشخیص نفوذ در این حالت قابل پیکربندی هستند.

- **معماری شبکهای و جایگذاری حسگرها**

برای نصب سیستم؛ ابتدا باید تصمیم گرفته شود که شبکه مدیریت راه اندازی شود یا آنکه ارتباطات سیستم مدیریت و تشخیص نفوذ؛ بر روی بستر شبکه اصلی صورت پذیرد .بعد از این مرحله باید در مورد حالت کاری حسگرها تصمیم گیری شود .حسگرهای IDS می توانند در حالت بی اثر یا برخط پیکربندی شوند.

### o حالت برخط

در این حالت حسگر به نحوی پیکربندی میشود که کل ترافیک شبکه مربوط به آن باید از آن گذر کند. به این منظور حسگر دارای دو واسط شبکهای است. یکی برای ورود ترافیک و یکی برای خروج ترافیک. بیشتر حسگرهای دارای این قابلیت به عنوان یک ابزار میانی با ویژگیهای دیوار آتش و سیستم تشخیص و چلوگیری نفوذ شناخته می شوند.



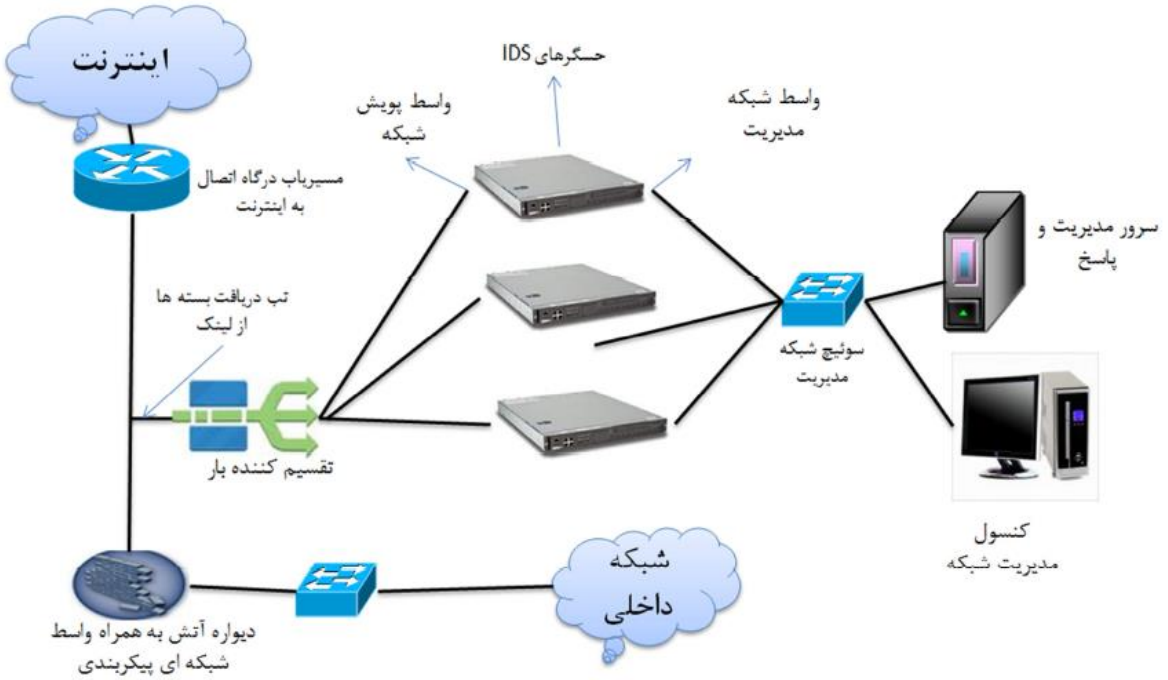

جایگذاری IDS با استفاده از حسگرهای برخط

### o حالت بی اثر

در این حالت حسگرها یک کپی از ترافیک واقعی شبکه رو پویش میکنند و امکان بلوکه کردن مستقیم ترافیم را ندارند .بیشتر سوئیچ های شبکه دارای یک درگاه به نام درگاه پوشان هستند که تمام ترافیک مربوط به این درگاه امکان دسترسی به IDS به همه درگاهها روی آن قرار داده میشود .با اتصال واسط شبکهای ( Networkتمام ترافیک شبکه وجود دارد .همچنین امکان انشعاب مستقیم از لینک ارتباطی وجود دارد در حسگرهای تشخیص نفوذ میتوانند در نقاط کلیدی شبکه و در ورودی قسمتهای مختلف قرارTap). گیرند .از جمله جاهای مهم عبارتند از : بعد از دیوراه آتش، در ابتدای ناحیه غیر نظامی ۱ و همچنین در ورودی شبکه داخلی .ناحیه غیرنظامی زیرشبکه منطقی یا فیزیکی است که شامل سرویسدهندههایی مانند وب، ایمیل و .... به شبکه اینترنت خارجی است .برای دسترسی به این سرویسها امکان ایجاد ارتباط از خارج شبکه نیاز است؛ که این مساله موجب ایجاد آسیب پذیری در مورد حملات میشود .با جدا کردن این ناحیه از

بقیه شبکه داخلی سازمان توسط دیواره آتش مجزا، از شبکه داخلی سازمان در مورد حملات و نفوذهای احتمالی حفاظت میشود .در حالت کلی میتوان گفت سطح امنیتی و سیاست امنیتی این ناحیه نسبت به شبکه داخلی متفاوت و پایینتر است؛ به همین خاطر به آن ناحیه غیرنظامی گفته میشود.

امکان توزیع ترافیک بین حسگرها در نقاطی که ترافیک عبوری سنگین دارند؛ با استفاده از تسهیم کننده ترافیک وجود دارد .این ویژگی در سیستمهای شبکهای توزیع شده به تفصیل مورد بررسی قرار میگیرد. مانند حالت قبل هر کدام از حسگرها خواه با ستفاده از شبکه مدیریت یا با استفاده بستر شبکه اصلی با سرورهای مدیریت ارتباط برقرار میکنند .در این سیستمها انتخاب پاسخ مناسب برای حمله در سرور مدیریت اتفاق میافتد که سیسات مربوطه میتواند از طریق دیواره آتش اعمال شود.



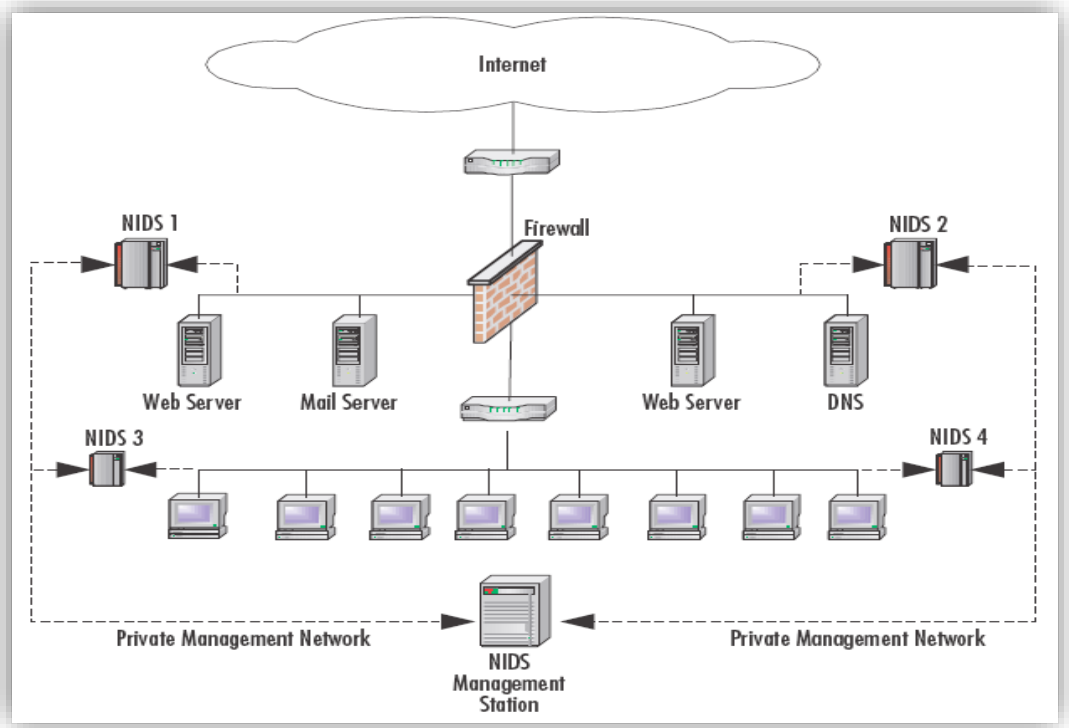

معماری IDS های توزیع شده با استفاده از حسگرهای بی اثر و با امکان توزیع بار

- **سیستم های توزیع شده(DIDS)**

امروزه با روند افزایش پهنای باند شبکه ها و نیاز به پویش بی وقفه این داده ها، سیستم های تشخیص نفوذ تحت شبکه هم باید همگام با آنها توسعه پیدا کنند .امروزه روشهای معماریهای متمرکز مبتنی بر شبکه جوابگوی شبکه های امروزی نیست. این روش ها برای تشخیص حملات چند مرحله ای و نگه داری وضعیت انواع ارتباطات و نیز مرداودات پروتکلی در جریان؛ به خاطر وجود یک نقطه سرویس دهی، سیستم دچار کوبیدگی و افت گذردهی می شود.الگوریتمهای تشخیص نفوذ مبتنی بر یک سری قوانین هستند که به سرعت در حال بزرگ شدن هستند .ایجاد *IDS* های توزیع شده نیاز به تمهیداتی برای معماری شبکه ای، نرم افزار مناسب برای عملکرد توزیع شده و تقسیم ترافیک شبکه بین بخشهای موازی دارد.

این سیستمها از تعدادي NIDS يا HIDS يا تركيبي از اين دو نوع به همراه يك سيستم مديريت مركزي تشكيل شده است .بدين صورت كه هرNIDS ي كه در شبكه موجود است، گزارشهاي خود را براي سيستم مديريت مركزي ارسال مي كند .سيستم مركزي وظيفه بررسي كردن گزارش هاي رسيده و تصميم بر آگاه سازي مسئول *IDS* شبكه را دارا شبكه را دارا *IDS* هاي موجود در شبكه را عهده دار مي باشد .در شكل *3* نحوه پياده سازي يك *DIDS* در شبكه نمايش داده شده است. *NIDS* هاي *1* و *2* وظيفه محافظت از سرويس دهنده هاي عمومي و *NIDS* هاي *3* و *4* وظيفه محافظت از شبكه داخلي را بر عهده دارند.

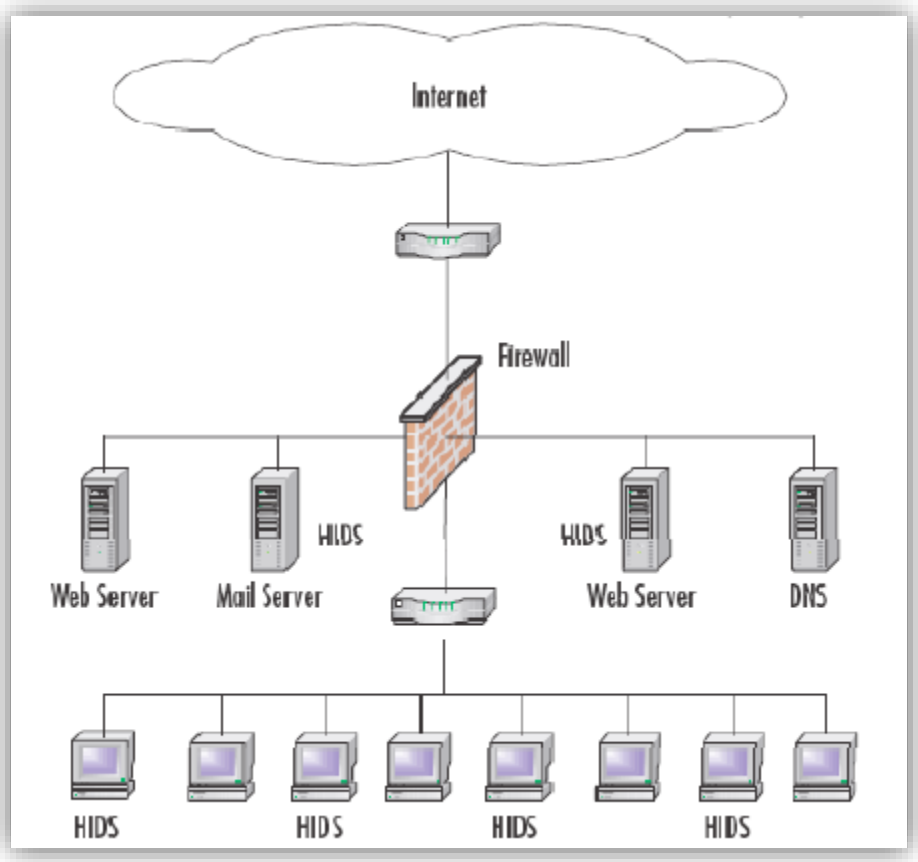
اطلاعات در سيستم مركزي *NIDS* ذخيره مي شود و ممكن است شبكه مابين *NIDS* ها با سيستم مديريت مركزي خصوصي باشد.




- **سیستم شناسایی حملات مبتنی بر میزبان (HIDS)**

این نوع سیستمها از دو جهت با NIDS ها متفاوت می باشند. HIDS تنها از یک میزبان محافظت می کند و تنها بسته های رسیده به کارت شبکه میزبانی که روی آن قرار گرفته است را مورد بررسی قرار می دهد در نتیجه از سرعت بالاتری نسبت به HIDS برخوردار است.

ویژگی بعدی HIDS کمتر بودن تعداد قوانین آن می باشد .برای مثال میزبانی که دارای سرویس domain name service نمی باشد ، هیچ لزومی ندارد قوانین مربوط به شناسایی آسیب پذیری های این نوع سرویس را در خود مورد بررسی قرار دهد .در نتیجه کارایی بالاتر رفته و مصرف CPU کاهش پیدا می کند.




**پیاده سازی چند HIDS در شبکه**

# بخش دوم:

## تشخیص نفوذ

## توسط *snort*

## درسیستم عامل *FreeBSD*

- **نصب vmware در فدورا :**

بدلیل مشکلاتی که در طی نصب vmware به آن برخوردم ، لازم دیدم مراحل نصب آن را توضیح بدم .
Vmware workstation 10 طی این مراحل در فدورا نصب می شود:

نصب پیش نیاز ها :

```
yum install kernel-devel kernel-headers gcc
cp /usr/src/kernels/`uname -r`/include/generated/uapi/linux/version.h /lib/modules/`uname -r`/bui
ld/include/linux/
```

نصب vmware workstation 10 :

```
./VMware-Workstation-Full-10.0.0-1295980.x86_64.bundle
```

احیای مجدد ماژول ها ، در صورتیکه با خطا مواجه شد بهتر است که ورژن جدید را نصب کنید.

```
vmware-modconfig --console --install-all
```

توجه داشته باشید که بعد از هر بار آپدیت کرنل فدورا ، باید دستور زیر را اجرا کنید:

```
cp /usr/src/kernels/`uname -r`/include/generated/uapi/linux/version.h /lib/modules/`uname -r`/bui
ld/include/linux/
vmware-modconfig --console --install-all
```

البته اگر کرنل فدورا دارای پسوند PEA باشد ، اصلا پوشه ای به این نام در دایرکتوری kernels و mouduls ساخته نمی شود، در این حالت :

یا باید در زمان بوت شدن کرنل بدون PEA را انتخاب کرد یا دوباره کرنل را حذف کرد ، در غیر این صورت vmware قادر به لود کردن فایل های header موبوط به کرنل سیستم نیست.

این هم سناریوی مشکل من:

> مشکل خطایی بود که بعد از نصب vmware به نبود فایل header به زبان c مربوط به 3.8.12-200fc-i686-PEA گرفته می شد این در حالیه که من چند روز پیشش بخاطر مشکل نشناختن وایرلس هر چی یکیج شبکه ای بود نصب کردم در بین این ها networkManager l2tp بود که پیش نیازش kernel-madule-extra بود که مدل کرنل رو به PEA..... ارتقا داده بود و وقتی vmware می خواست فایل header کرنل رو پیدا کنه'uname -r' اصلا شاخه ای به نام PEA.... در دایرکتوری kernels وجود نداشته ----------> در نهایت با yum remove kernels و نصب مجدد yum install kernel ، کرنل های قدیمی و PEA... دار ها حذف شدندو کرنل به 3.12.8-200fc.i686 تغییر پیدا کرد.

Vmware با دستور زیر حذف می شود:

```
/usr/lib/vmware-installer/2.1.0/vmware-installer -u vmware-workstation
```

❖ **توجه:**

**در صورتیکه از promiscuous mode کارت شبکه ماشین مجازی استفاده می کنید (زمانی که از اسنورت برای شنود کل ترافیک شبکه استفاده می شود ، این مد مورد نیاز است.) باید مجوز دسترسی پیشفرض به /dev/vmnet*(0-3) را که در اختیار root است به کاربری یا گروه newgroup تغییر دهید یا در کل مجوز ها را با دستور chmod a+rw /dev/vmnet* لغو کنید.**

- **پورت های Freebsd**

*FreeBSD* با مجموعه غنی از ابزارهای سیستمی بعنوان بخشی از سیستم پایه همراه شده. علاوه بر این *FreeBSD* دو تکنولوژی مکمل را برای نصب نرم افزار شخص ثالث فراهم کرده : مجموعه پورت های *FreeBSD* ، برای نصب از منبع ، و پکیج ها ، برای نصب فایل های باینری پیش ساخته . در هر دو روش ممکن است برای نصب نرم افزار از رسانه های محلی یا از شبکه استفاده شود.

یک پورت *FreeBSD* ، یک مجموعه فایل های طراحی شده برای خودکار کردن فرایند کامپایل یک برنامه از سورس کد است. فایل هایی که دربردارنده پورتی شامل تمام اطلاعات ضروری برای خودکارسازی دانلود ، استخراج ،پچ کردن ، کامپایل و نصب برنامه است .

- **جستجو در مجموعه پورت**

مکانیسم جستجوی توکار مجموعه پورت ها ، راهی دیگر برای جستجوی نرم افزار است. برای استفاده از این قابلیت به */usr/ports* ، بروید و سپس *make serch name = 'program name'* را اجرا کنید ،

*program name* نام برنامه ایست که بدنبال آن هستید.

- # cd -/usr/ports
- # make search name=lsof

Port: lsof-4.88.d,8

Path: -/usr/ports/sysutils/lsof

Info: Lists information about open files (similar to fstat(1))

Maint: ler@lerctr.org

برای دریافت اطلاعات کمتر ، از خاصیت quicksearch استفاده کنید:

- # cd -/usr/ports
- # make quicksearch name=lsof

Port: lsof-4.88.d,8

Path: -/usr/ports/sysutils/lsof

- **نصب مجموعه پورتها در freebsd:**

در صورتیکه تا بحال مجموعه پورت ها را نصب نکردید ، با دستورات زیر می توانید ، مجموعه پورت های freebsd را ابتدا از سرور ها و mirror های freebsd واکشی وسپس مستقر کنید.

Portsnap یک ابزار سریع و کاربرپسندبرای بازیابی مجموعه پورتهاو یک پیشنهاد مناسب برای اغلب کاربران است.

- `portsnap fetch`

زمانیکه *portsnap* را برای اولین بار اجرا می کنید ، *snapshot* رو در */usr/ports/* استخراج کنید.

- `portsnap extract`

بعداز اولین استفاده از دستور *portsnap* مطابق دو مرحله قبل، */usr/ports/* در صورت نیاز با دستور زیر می تواند بروز شود:

- `portsnap fetch update`

## • نصب پورت ها در freebsd

این قسمت دستورات پایه ای استفاده از مجموعه پورتها را برای نصب و حذف نرم افزار را فراهم کرده.

❖ اخطار

قبل از کامپایل هر پورتی ، همانطور که در قسمت قبل توضیح داده شد از آپدیت بودن پورت ها مطمئن شوید.چون نصب هر نرم افزار شخص ثالثی می تواند آسیب پذیری های امنیتی بدنبال داشته باشد، پیشنهاد می شود در ابتدا نگاهی به **http://vuxml.freebsd.org/** برای دانستن مسائل امنیتی مربوط به پورت ها داشته باشید. متناوبا ، اگر ports-mgmt/portaudit نصب شده ، portaudit –F را قبل از نصب پورت جدید اجرا کنید. این دستور طوری می تواند پیکربندی شود که بصورت خودکار بازرسی امنیتی و بروز رسانی پایگاه داده آسیب پذیری رو در خلال بررسی امنیتی سیستم انجام دهد.

❖ برای استفاده از مجموعه پورتها باید به اینترنت متصل بود وهمچنین کاربر باید مدیر سیستم باشد.

❖ بعضی از محصولات DVD شخص ثالث از قبیل FreeBSD Toolkit از freebsdmall.com شامل distfile هایی هستند که می تواند پورت ها رو بدون اتصال به اینترنت نصب کند.DVD را در /cdrom مانت کنید. اگر شما از نقطه مانت متفاوت استفاده می کنید، CD_MOUNTPTS را بعنوان متغییر بگیرید. اگر distfileها در دیسک موجود باشند بصورت خودکار نصب می شوند. گرچه تعداد کمی از پورت ها اجازه استخراج را از DVD نمی دهند.این مسئله بخاطر اینکه برای بعضی از دانلود ها و توزیع ها نیاز به ثبت نام کامل هست، منطقی بنظر می رسد.هنوز هم برای نصب پورتی که در DVD موجود نیست ، نیاز به اتصال به اینترنت است.

❖ برای کامپایل و نصب پورت ، به مسیر پورتی که می خواهید نصب کنید بروید،سپس *make install* راتایپ کنید ، پیام ها فرایند را نشان خواهند داد:

- # cd -/usr/ports/sysutils/lsof
- # make install

```
>> lsof_4.88D.freebsd.tar.gz doesn't seem to exist in -/usr/ports/
distfiles/.
>> Attempting to fetch from ftp://lsof.itap.purdue.edu/pub/tools/
unix/lsof/.
===>  Extracting for lsof-4.88
[extraction output snipped]
>> Checksum OK for lsof_4.88D.freebsd.tar.gz.
===>  Patching for lsof-4.88.d,8
===>  Applying FreeBSD patches for lsof-4.88.d,8
===>  Configuring for lsof-4.88.d,8
[configure output snipped]
===>  Building for lsof-4.88.d,8
[compilation output snipped]
===>  Installing for lsof-4.88.d,8
[installation output snipped]
===>   Generating temporary packing list
===>   Compressing manual pages for lsof-4.88.d,8
===>   Registering installation for lsof-4.88.d,8
===>  SECURITY NOTE:
    This port has installed the following binaries which execute ↺
with
    increased privileges.
/usr/local/sbin/lsof
```

بخاطر اینکه lsof یک برنامه با حق امتیاز بالاست ، یک اخطار امنیتی بدلیل نصب آن نمایش داده شده. وقتیکه نصب کامل شد ، اعلان دوباره برمی گردد.

❖ بعضی پوسته ها نهانگاهی(cach) از دستوراتی را که در دایرکتوریهای موجود در متغییر محیطی PATH هســت ، در خود نگه می دارند.اینکار برای سرعت بخشیدن به عملکرد مراجعه به فایل های اجرایی این دســتورات است.کاربران پوسته tcsh باید برای اینکه نیازی به وارد کردن مسیر کامل دستورات جدید نباشد ، rehash را اجرا کنند. hash –r همان کار را در پوسته sh انجام می دهد. برای اطلاعات بیشتر به اسنادپوسته مراجعه کنید.

❖ در طی نصــب ، یک دایرکتوری فرعی بمنظور ذخیره فایل های موقت مورد نیاز برای کامپایل ایجاد می شود. حذف این دایرکتوری فضای دیسک را آزاد می کندو احتمال مشکلات بعد از ارتقا پورت به نسخه جدیدتر را به حداقل می رساند:

- # make clean
- ===> Cleaning for lsof-88.d,8

- توجه:برای حذف این گام اضافی از دستور make install clean در زمان کامپایل پورت استفاده کنید.

- **نصب سفارشی پورت ها:**

❖ بعضی پورت ها گزینه هایی برای build کردن شامل : فعال یا غیر فعال کردن اجزا ، مهیا کردن گزینه های امنیتی را فراهم میکنند.

اگر پورت به پورتهایی وابسته باشد که آن پورتها دارای گزینه هایی برای پیکربندی باشند ، ممکنه به دفعات عملیات برای تعامل با کاربر متوقف شود چون رفتار پیشفرض اینست که بوسیله ی یک منو گزینه های انتخابی به کاربر اعلان شود. برای جلوگیری از این ، *make config-recursive* را در داخل اسکلت پورت اجرا کنید تا این پیکربندی در یک مرحله انجام شود.سپس *make install[clean]* را برای کامپایل و نصب پورت اجرا کنید.

❖ نکته

زمانیکه از config-recursive استفاده می کنید ، لیست پورت هایی که باید پیکربندی شوند بوسیله -all depends-list target جمع آوری می شود.پیشنهاد می شود تا زمانیکه تمام گزینه های پورتهای وابسته تعیین نشده اند ، make config-recursive را اجرا نکنید. این زمانیست که بعد از مدت کوتاهی صفحه گزینه های پورت ها ظاهر می شود تا مشخص شود تمام گزینه های وابسته پیکربندی شده اند.

❖ بعداز اینکه پورت *build* می شود ،چندین راه برای اضافه کردن، حذف کردن و یا تغییر دادن گزینه های *build* پورت وجود دارد. یک روش اینست که به دایرکتوری شامل پورت برویم و تایپ کنیم *make config* . گزینه دیگر استفاده از *make showconfig* است. گزینه دیگر اجرای *make rmconfig* است که تمام گزینه های انتخاب شده را حذف می کندو به شما اجازه می دهد تا دوباره شروع کنید.

❖ سیستم پورت از دستور fetch برای دانلود سورس فایل ها استفاده می کند، که از متغییر های محیطی زیادی هم حمایت می کند.اگر سیستم FreeBSD پشت یک دیوار آتش یا FTP/HTTP پراکسی باشد از متغییر های FTP_PROXY , FTP_PASSIVE_MODE ،و FTP_PASSWORD استفاده می شود.

❖ برای کاربرانی که همیشه نمی توانند به اینترنت متصل باشند ،می توانید make fetch را در مسیر /usr/ports اجرا کنید، که در واقع باعث می شود تمام diftfile ها واکشی می شوند . می توانید این دستور را در مسیر /usr/ports/net یا هر اسکلت پورت دیگری اجرا کنید. توجه داشته باشید که اگر پورت وابسته هایی در طبقه بندی دیگر یا اسکلت پورت دیگری داشته باشد ، آن وابسته ها واکشی نمی شوند.به جای آن دستور ، دستور make fetch-recursive را استفاده کنید تا تمام وابسته ها در صورت انتخاب هر اسکلت پورتی واکشی خواهد شد.

❖ در موارد نادر ، مثل زمانیکه یک سازمان دارای یک مخزن محلی است ، متغییر MASTER_SITES محل دانلودی که در فایل makefile مشخص شده را لغو می کند:

```
# cd /usr/ports/directory
# make MASTER_SITE_OVERRIDE= \
ftp://ftp.organization.org/pub/FreeBSD/ports/distfiles/ fetch
```

❖ متغییرهای WRKDIRPREFIX و PREFIX دایرکتوری پیشفرض را لغو می کند،برای مثال:

```
# make WRKDIRPREFIX=/usr/home/example/ports install
```

❖ پورت را در /usr/home/example/ports/ کامپایل می کند و آن را در /usr/local نصب می کند

```
# make PREFIX=/usr/home/example/local install
```

❖ پورت را در /usr/ports کامپایل می کند و آن را در /usr/home/example/local نصب می کند.و :

```
# make WRKDIRPREFIX=../ports PREFIX=../local install
```

هر دو را مخلوط می کند.

این مورد هم بااستفاده از متغییرهای محیطی قابل پیاده سازی است.

- **حذف پورت ها در Freebsd**:

❖ پورت های نصب شده با دستور pkg_delete حذف می شوند.همچنین ، اگر سیستم FreeBSD برای استفاده از pkg پیکربندی شود، پورت می تواند با دستور pkg delete حذف شود.مثال هایی از این دستورات در قسمت های قبل زده شده.دستور Make deinstall در دایرکتوری پورت هم همین کار را انجام می دهد.

```
# cd -/usr/ports/sysutils/lsof
make deinstall
===>  Deinstalling for sysutils/lsof
===>  Deinstalling
Deinstallation has been requested for the following 1 packages:
lsof-4.88.d,8
The deinstallation will free 229 kB
[1/1] Deleting lsof-4.88.d,8... done
```

❖ توصیه می شود پیام هایی که در حین حذف پورت نمایان می شود را بخوانید.در صورتیکه پورت دارای برنامه های وابسته باشد ، این برنامه ها نمایش داده می شود ولی در هر صورت فرایند حذف انجام می شود. در چنین مواردی بهتر است برای محافظت از وابستگی های شکسته شده ، برنامه را دوباره نصب کرد.

- **ارتقا پورتها در *freebsd*:**

❖ با گذشت زمان ، نسخه های جدیدتر نرم افزار در مجموعه پورت ها در دسترس است.این قسمت نرم افزار هایی که قابل ارتقا هستند را مشخص می کندو چگونگی ارتقا این نرم افزار ها رو توضیح می دهد.

❖ برای اینکه مطمئن شوید پورتها بروز هستند، درخت پورت را در آخرین نسخه نگه دارید.

این دستور هم برای دیدن نسخه های قدیمی پورت استفاده می شود:

```
# pkg_version --l -"<"
```

❖ **مهم**

قبل از اقدام به ارتقا ، آخرین تاریخ ارتقا یا نصب سیستم را در ابتدای فایل /usr/ports/UPDATING بخوانید . این فایل گام های اضافی و مسائل مختلفی که کاربران ممکنه در زمان ارتقا یک پورت با آن مواجه شوند را توضیح می دهد. از جمله این مسائل می توان به : تغییر فرمت فایل، تغییر مکان فایل های پیکربندی ، یا هر ناسازگاری با نسخه های قبلی اشاره کرد. توجه داشته باشید که از هر پورتی که نیاز به ارتقا دارد را مطابقت دهید و زمانی که در حال ارتقا هستید مطابق این دستورالعمل ها عمل کنید.

❖ از دستورات portmaster یا portupgrade می توان برای ارتقا استفاده کرد.

- **نصب snort:**

❖ تذکر:

پلاگین mysql در نسخه های قبلی اسنورت بعنوان یک output plugin هنگام نصب اسنورت با دستور make install clean در دایرکتوری اسکلت پورت اسنورت نصب می شد .

❖ توضیحاتی که در داکیومنت های سایت snort.org داده شده اشاره ای به پلاگین mysql و نصب barnyard2 نکرده و شیوه نصب اسنورت هم قدیمی است و ارائه دایرکتوری های پیشفرض غلط هم گواه این مطلب است.

❖ تذکر:

در زمان آپدیت به ورژن جدید اسنورت پیشنهاد می شود از فایل های ***local.rules***, ***snort.conf***, ***threshold.conf***, ***list.rules***, و ***black_list.rules*** نسخه پشتیبان تهیه شود.

❖ تذکر:

قبل از نصب مطمئن شوید اسکریپت ldconfig شروع بکار کرده باشد.

- Cd /etc/rc.d
- ./ldconfig stop
- ./ldconfig start

باید پیغام زیر نمایش داده شود:

*ELF ldconfig path: /lib /usr/lib /usr/lib/compat /usr/local/lib*
*32-bit compatibility ldconfig path: /usr/lib32*

نیازمندی های اسنورت:

***gcc*** *version 4.2.x (including libraries),* ***zlib*** *(1.2.3 or higher),* ***libpcap*** *(1.0.0 including* ***libpcap-devel****),* ***pcre*** *(8.2x),* ***bison*** *(2.4.3.x),* ***m4*** *(1.4.16),* ***libiconv*** *(1.13),* ***gettext*** *(0.18.1),* ***libdnet*** *(1.11 including* ***libdnet-devel****) and* ***tcpdump*** *(4.0.0 or higher).*

با اجرای دستور *make install clean* تمام نیازمندی های بالا نصب می شوند.

در ضمن ابزار DAQ هم بدلیل اینکه پیشنیاز اسنورت با دستور بالا نصب می شود.

با دستور زیر می توانید گزینه هایی رو حذف یا اضافه کرد.

- *./configure*
  - ❖ در صورتیکه در این مرحله نصب متوقف شد، فایل config.log را که در دایرکتوری /usr/local/etc/snort است بررسی کنید.
- Make install clean

با اجرای این دستور اسنورت در دایرکتوری پیشفرض /usr/local/etc/snort نصب می شود، اسکریپت شروع بکار آن هم در /usr/local/etc/rc.d نصب می شود.

- **نصب rule ها:**

برای دانلود rule ها به سایت snort.org مراجعه کنید. بعد از ثبتنام می توانید rule ها رو تنها با اختلاف یک ماه نسبت به کاربرانیکه اشتراک پرداخت می کنند، دریافت کنید.

- *tar zvxf <path to>snortrules-snapshot-<nnnn>.tar.gz*
- *touch /etc/snort/rules/white_list.rules /etc/snort/rules/black_list.rules*

rule ها را در دایرکتوری rules/.. کپی کنید.همینطور so_rulesو preproc_rules را در دایرکتوری های خودشان کپی کنید ، اطلاعات موجود در etc را هم در دایرکتوری /.. کپی کنید.

- **ایجاد فایل ها لازم دیگر**

- *cd /usr/local/lib*
- *mkdir snort_dynamicrules*

- *cd /var/log*
- *mkdir snort*
- *chmod 755 snort*

اجرای دستور زیر باعث می شود مطمئن شویم که فایل مورد نظرمان کامپایل می شود.

- *cd /usr/sbin*
- *ln -s /usr/local/bin/snort snort*
- *chmod 755 snort*

- **ایجاد کاربر و گروه اسنورت:**

- Pw groupadd snort

با اجرای دستور فوق خط زیر به فایلetc/passwd/ اضافه می شود.

*snort:*:40000:40000:Snort IDS:/var/log/snort:/usr/sbin/nologin*

- useradd

با اجرای دستور فوق خط زیر به فایل/etc/group اضافه می شود.

*snort:*:40000:snort*

فرمت این فایل در زیر توضیح داده شده:

*Columns 1-5 (the username, in this case 'snort')*
*Column 7 (the 'x' indicates that the password is encrypted)*
*Columns 9-13 (the user id (UID) 40000)*
*Columns 15-19 (the group id (GID) 40000, in this case the group is 'snort')*
*Columns 21-29 (the full name of the user, in this case 'SNORT_IDS')*
*Columns 28-44 (the default directory for this user, in this case '/var/log/snort')*
*Columns 46-58 (the shell script or login option for this user)*

- **دادن مالکیت به فایل هایی که در زمان اجرا استفاده می شوند:**

- *cd /etc/snort*
- *chown -R snort:snort **

- *cd /var/log*
- *chown -R snort:snort snort*

- *cd /usr/local/lib*
- *chown -R snort:snort snort**
- *chown -R snort:snort snort_dynamic**
- *chown -R snort:snort pkgconfig*
- *chmod -R 700 snort**
- *chmod -R 700 pkgconfig*

- *cd /usr/local/bin*
- *chown -R snort:snort daq-modules-config*
- *chown -R snort:snort u2**
- *chmod -R 700 daq-modules-config*
- *chmod 700 u2**

- *cd /etc*
- *chown -R snort:snort snort*
- *chmod -R 700 snort*

- **پیکربندی snort:**

فایل پیکربندی اسنورت بصورت پیشفرض در دایرکتوری /usr/local/etc/snort به شکل snort.conf.sample ذخیره می شودکه بعدا با فایل آپدیت جدید جایگزین میشود.

خطوط زیر را در فایل snort.conf باید تغییر داد:

- *var RULE_PATH /etc/snort/rules*
- *ipvar HOME_NET 192.168.1.0/24*
- *ipvar EXTERNAL_NET !$HOME_NET*
- *var SO_RULE_PATH /etc/snort/so_rules*
- *var PREPROC_RULE_PATH /etc/snort/preproc_rules*
- *var WHITE_LIST_PATH /etc/snort/rules*
- *var BLACK_LIST_PATH /etc/snort/rules*

این خط را هم باید برای اتصال به barnyard2 از حالت کامنت در آورد.

- **# output unified2: filename merged.log, limit 128, mpls_event_types, vlan_event_types**

- **اسکریپت شروع بکار:**

با اسکریپت /usr/local/etc/rc.dاین اسکریپت را می توانید از سایت دانلود کنید.و در دایرکتوری پیشفرض جایگزین کنید.

```
----- CUT HERE -----
#!/bin/sh
#
# Snort Startup Script modified for FreeBSD 8.x or 9.x
#
# Original Script from Spanish Honeywell Project (2004)
# Script modified to add status parameter to 'usage'
#
# Script variables (modify to match your system layout)
LAN_INTERFACE=em0
RETURN_VAL=0
BINARY=/usr/local/bin/snort
```

```
PATH=/bin:/usr/local/bin
PID=/var/run/snort_${LAN_INTERFACE}_ids.pid
LOGDIR="/var/log/snort"
DATE=`/bin/date +%Y%m%d`
CONFIG_FILE=/etc/snort/snort.conf
PROG=snort
USER=snort
GROUP=snort
if [ ! -x "$BINARY" ]; then
echo "ERROR: $BINARY not found."
exit 1
fi
if [ ! -r "$CONFIG_FILE" ]; then
echo "ERROR: $CONFIG_FILE not found."
exit 1
fi
start()
{
# Check if log directory is present. Otherwise, create it.
if [ ! -d $LOGDIR/$DATE ]; then
mkdir $LOGDIR/$DATE
/usr/sbin/chown -R $USER:$GROUP $LOGDIR/$DATE
fi
/bin/echo "Starting $PROG: "
# Snort parameters
# -D Run Snort in background (daemon) mode
# -i <if> Listen on interface <if>
# -u <uname> Run snort uid as <uname> user (or uid)
# -g <gname> Run snort uid as <gname> group (or gid)
# -c Load configuration file
# -N Turn off logging (alerts still work) (removed to enable logging) :)
# -l Log to directory
# -t Chroots process to directory after initialization
# -R <id> Include 'id' in snort_intf<id>.pid file name
$BINARY -D -i $LAN_INTERFACE -u $USER -g $GROUP -c $CONFIG_FILE -l
$LOGDIR/$DATE -t $LOGDIR/$DATE -R _ids
/bin/echo "$PROG startup complete."
return $RETURN_VAL
}
stop()
{
if [ -s $PID ]; then
/bin/echo "Stopping $PROG with PID `cat $PID`: "
kill -TERM `cat $PID` 2>/dev/null
RETURN_VAL=$?
/bin/echo "$PROG shutdown complete."
```

```
rm -f $PID
else
/bin/echo "ERROR: PID in $PID file not found."
RETURN_VAL=1
fi
return $RETURN_VAL
}
status() {
if [ -s $PID ]; then
echo "$PROG is running as pid `cat $PID`:"
else
echo "$PROG is not running."
fi
}
restart()
{
stop
start
RETURN_VAL=$?
return $RETURN_VAL
}
case "$1" in
start)
start
;;
stop)
stop
;;
status)
status
;;
restart|reload)
restart
;;
*)
/bin/echo "Usage: $0 {start|stop|status|restart|reload}"
RETURN_VAL=1
esac
exit $RETURN_VAL
----- CUT HERE -----
```

❖ **توجه**

آدرس فایل پیکربندی را باید در این اسکریپت بروز کرد و در صورت نیاز تغییراتی را انجام داد.

- **تست صحت پیکربندی و اجرای اسنورت:**

➢ *cd /usr/local/bin*

- *./snort -T -i em0 -u snort -g snort -c /etc/snort/snort.conf*

- **اجرای اسنورت:**

- *cd /usr/local/bin*
- *./snort -i em0 -D -u snort -g snort -c /etc/snort/snort.conf*

- **اطمینان از اجرای اسنورت:**

- *ps aux | grep -i "snort"*

باید چنین خروجی نمایش داده شود:

*snort 1313 0.0 16.1 427808 166868 ?? Ss 6:39PM 0:02.51 /usr/local/bin/snort -D -i em0 -u snort -g snort -c /etc/snort/snort.conf -l /var/log/snort/20120611 -t /var/log/snort/20120611 -R _ids*

- **خطاهای ممکن که با آن ها موجه شدم:**

❖ خطاهای نمایش داده شده یا در terminal هستند یا در فایل /var/log/messages

? ! خطا می دهد cannot decode datelink

☑ علتش نذاشتن سوئیچ *-I em0* بود.

```
snort[69421]: Acquiring network traffic from "usbus0".
snort[69421]: Initializing daemon mode
snort[69424]: Daemon initialized, signaled parent pid: 69421
snort[69424]: Reload thread starting...
snort[69424]: Reload thread started, thread 0x35687e00 (69424)
snort[69424]: FATAL ERROR: Cannot decode data link type 186
snort[69421]: Child exited unexpectedly
mohammad: /usr/local/etc/rc.d/snort: WARNING: failed to start snort
```

Screen clipping taken: 2014/02/06 10:45 PM

? در مد deamon یا همون سرویس background ،

☑ با اینکه گروه و یوزرsnort را ساختم ، و مالکیت تمام فایل ها و فولدر های مورد نیاز را به یوزر snort اختصاص دادم.

خطای زیر را می دهد.

```
root@msoltani:/usr/local/bin # snort -i em0 -D -u snort -g snort -c /usr/local/etc/snort/snort.conf
Spawning daemon child...
My daemon child 2064 lives...
Parent waiting for child...
Child terminated unexpectedly (-979029292)
Daemon parent exiting (0)
root@msoltani:/usr/local/bin #
```

```
snort[2063]: pcap DAQ configured to passive.
snort[2063]: Acquiring network traffic from "em0".
snort[2063]: Initializing daemon mode
snort[2064]: Daemon initialized, signaled parent pid: 2063
snort[2064]: Reload thread starting...
snort[2064]: Reload thread started, thread 0x3ba38300 (2064)
snort[2064]: Decoding Ethernet
snort[2064]: Checking PID path...
snort[2064]: PID path stat checked out ok, PID path set to /var/run/
snort[2064]: FATAL ERROR: Failed to Lock PID File "/var/run//snort_em0.pid" for PID "2064"
```

☑ هر دو فایل را از دایرکتوری */var/run* پاک کردم درست شد.

?

```
snort[13100]: Writing PID "13100" to file "/var/run//snort_em0.pid"
snort[13100]: Set gid to 40000
snort[13100]: Set uid to 40000
snort[13100]:
snort[13100]:         --== Initialization Complete ==--
snort[13100]: Commencing packet processing (pid=13100)
```

Screen clipping taken: 2/16/2014 5:55 AM

```
root@msoltani:/var/log/snort # snort -c /usr/local/etc/snort/snort.conf -i em0 -D -u snort -g snort
Spawning daemon child...
My daemon child 13105 lives...
Parent waiting for child...
Child terminated unexpectedly (-981611696)
Daemon parent exiting (0)
root@msoltani:/var/log/snort #
```

Screen clipping taken: 2/16/2014 5:56 AM

به این خاطر بود که اسنورت در حال اجرا بود

در زمان اجرای این دستور باید توجه داشت که استارت آپ اسکریپت *snort* موجود در */etc/rc.d* و */usr/local/etc/rc.d* باید با اینتر فیس *em0* و *config file path=/usr/local/etc/snort/snort.conf* پیکربندی شود.()

#Service snort start/stop/restart

- **barnyard2**:

یک ابزار خروجی برای snort است.این ابزار به snort کمک میکند که خروجی باینری خود را به پایگاه داده ارسال کند تا راحت تر بتوان خروجی ها را بوسیله ابزارهای دیگر بررسی کرد.

Barnyardخروجی های snort را که با فرمت u2(Unified format) هستند را گرفته و دادهای پردازش شده را به پایگاه داده مقصد در اینجا mysqlاست بفرستد.در واقع همین فرمت یکسان و یک شکل شده رمز موفقیت barnyard2 است.

مهمترین مزیت آن اینست که کندی اتصال مستقیم به پایگاه داده هایی مثل mysqlو postresql را ندارد، در واقع با پردازشگر جدید logو alert ، از سربار ناشی از ذخیره سازی کند داده ها در پایگاه های داده یا شبکه جلوگیری می شود.

.مزیت دیگر استفاده از Barnyard این است که قابلیت آنرا دارد که در صورت کار نکردن پایگاه داده داده ها را ذخیره کند

- **نصب barnyard2**:

برای نصب barnyard2 فقط کافیست دستور make install clean را در اسکلت پورت /usr/ports/security/barnyard2 اجرا کرد.

- # make install clean

لازم به ذکر است که پلاگین mysql درون make files اسکلت پورت barnyard2 موجود است وبا اجرای دستور بالا تمام پلاگین های موجود نصب خواهند شد.

اسکریپت شروع بکار هم در دایرکتوری /usr/local/etc/rc.d است که می توان تنظیماتی را در آن در نظر گرفت.

Barnyard2 در سه حالت راه اندازی می شود که ما از حالت پیوسته continual استفاده می کنیم.

فایل راهنمای waldoبه منظور بررسی کارکرد Barnyard استفاده میشود و زمان از کار افتادن Barnyard میتوان از طریق این فایل Barnyardادامه کار خود را انجام دهد.

- **touch /var/log/snort/barnyard2.waldo**
- **chown -R snort:snort /var/log/snort**

- **پیکر بندی barnyard2**:

فایل پیکربندی barnyard2 در دایرکتوری /usr/local/etc است.

- **config logdir: /var/log/barnyard2**
- **config hostname: localhost**
- **config interface: snort0**
- **config daemon**
- **config set_gid:snort**
- **config set_uid:snort**
- **config waldo_file: /var/log/snort/barnyard2.waldo**
- **input unified2**
- **output database: log, mysql,**
  **user=snort,password=password,dbname=barnyard2 ,**
  **host=localhost**

بعد از نصب mysql نحوه راه اندازی این ابزار هم توضیح داده می شود.

- **Mysql**
  - **نصب Mysql**

Mysql با دستورات زیر نصب می شود:

```
cd /usr/ports/databases/mysql55-server
make install clean
```

استارت آپ اسکریپت هم در دایرکتوری /usr/local/etc/rc.d ذخیره می شود.پایگاه داده هم در دایرکتوری /var/db/mysql ذخیره می شود.

  - **شروع بکار mysql**

Rc.conf باید شامل خط زیر باشد تا به mysql اجازه شروع داده شود.

```
'mysql_enable="YES"
```

برای هر بار اجرا در صورت وارد نکردن خط بالا باید دستور زیر اجرا شود:

```
/usr/local/etc/rc.d/mysql-server start
```

  - **پسوورد ریشه:**

برای هر بار شروع mysql باید اکانت های ریشه های ریشه واکانت های بدون نام کاربری (anonymous) پسوورد را وارد کنند.

برای گذاشتن پسوورد به کاربران بدون نام کاربری باید از دستورات زیر استفاده کرد:

```
# mysql -u root
# SET PASSWORD FOR ''@'localhost' = PASSWORD('newpwd');
# SET PASSWORD FOR ''@'host_name' = PASSWORD('newpwd');
```

و برای گذاشتن پسوورد به کاربر ریشه باید از دستورات زیر استفاده کرد:

```
# mysql -u root
# SET PASSWORD FOR 'root'@'localhost' =
PASSWORD('newpwd');
# SET PASSWORD FOR 'root'@'host_name' =
PASSWORD('newpwd');
```

برای وارد کردن پایگاه داده های پیشفرض از این دستور استفاده می شود:

- /usr/local/bin/mysql_secure_installation

```
Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MySQL
root user without the proper authorisation.

You already have a root password set, so you can safely answer 'n'.

Change the root password? [Y/n] n
 ... skipping.

By default, a MySQL installation has an anonymous user, allowing anyone
to log into MySQL without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] n
 ... skipping.

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] n
 ... skipping.

By default, MySQL comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] ■
```

Screen clipping taken: 2/16/2014 11:07 PM

بیشتر سوالاتی که پرسیده می شود در مورد اجاره های دسترسی کاربران و دسترسی از راه دور به پایگاه داده است ، و پاسخ ها با توجه به سیستم میزبان ونیاز امنیتی متفاوت است.
همانطور که در شکل زیر دیده می شود ، تعدادی جدول به پایگاه داده اضافه شده.

```
Remove test database and access to it? [Y/n] n
 ... skipping.

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
 ... Success!

Cleaning up...



All done!  If you've completed all of the above steps, your MySQL
installation should now be secure.

Thanks for using MySQL!


root@msoltani:~ #
```

```
mysql> select table_type,table_name,table_schema from information_schema.tables where table_rows>=1;
+------------+-----------------------------------------------+--------------------+
| table_type | table_name                                    | table_schema       |
+------------+-----------------------------------------------+--------------------+
| BASE TABLE | db                                            | mysql              |
| BASE TABLE | general_log                                   | mysql              |
| BASE TABLE | help_category                                 | mysql              |
| BASE TABLE | help_keyword                                  | mysql              |
| BASE TABLE | help_relation                                 | mysql              |
| BASE TABLE | help_topic                                    | mysql              |
| BASE TABLE | proxies_priv                                  | mysql              |
| BASE TABLE | slow_log                                      | mysql              |
| BASE TABLE | user                                          | mysql              |
| BASE TABLE | cond_instances                                | performance_schema |
| BASE TABLE | events_waits_current                          | performance_schema |
| BASE TABLE | events_waits_history                          | performance_schema |
| BASE TABLE | events_waits_history_long                     | performance_schema |
| BASE TABLE | events_waits_summary_by_instance              | performance_schema |
| BASE TABLE | events_waits_summary_by_thread_by_event_name  | performance_schema |
| BASE TABLE | events_waits_summary_global_by_event_name     | performance_schema |
| BASE TABLE | file_instances                                | performance_schema |
| BASE TABLE | file_summary_by_event_name                    | performance_schema |
| BASE TABLE | file_summary_by_instance                      | performance_schema |
| BASE TABLE | mutex_instances                               | performance_schema |
| BASE TABLE | performance_timers                            | performance_schema |
| BASE TABLE | rwlock_instances                              | performance_schema |
| BASE TABLE | setup_consumers                               | performance_schema |
| BASE TABLE | setup_instruments                             | performance_schema |
| BASE TABLE | setup_timers                                  | performance_schema |
| BASE TABLE | threads                                       | performance_schema |
| BASE TABLE | base_roles                                    | snort              |
+------------+-----------------------------------------------+--------------------+
27 rows in set (0.02 sec)
```

Screen clipping taken: 2/16/2014 11:07 PM

برای ایجاد پسورد جدید دستور زیر را اجرا کنید:

- # mysqladmin password newpassword

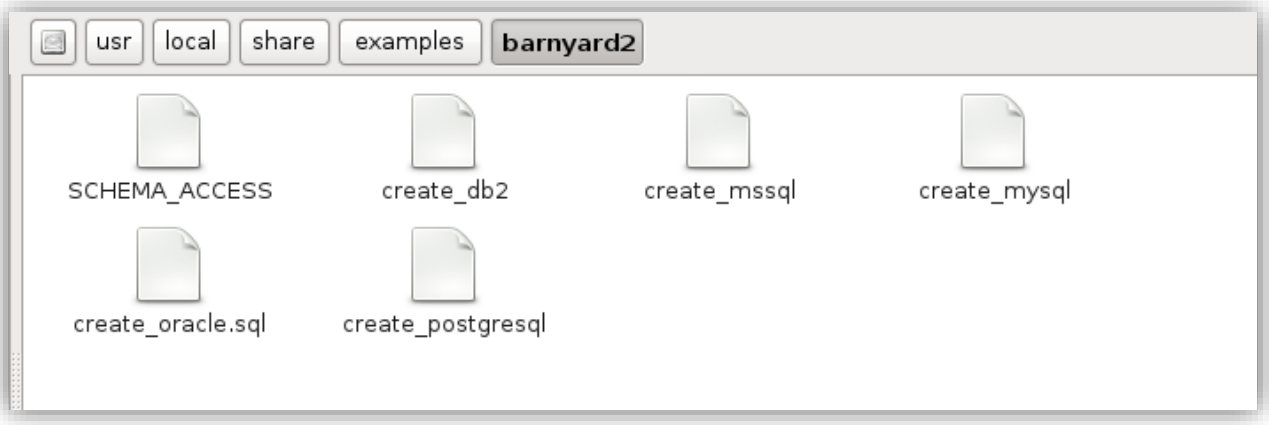
- **ایجاد پایگاه داده barnyard2 در mysql :**

با دستور زیر پایگاه داده barnyard2 در mysql ساخته می شود.

- #mysqladmin -u root -p create barnyard2

حالا باید مکانی که جداول های پیشفرضی که barnyard2 برای mysql در نظر گرفته پیدا کنیم وبا دستور زیر آن هارا به پایگاه داده barnyard2 اصافه کنیم.

- #mysql -u root -p -D barnyard2 < /usr/local/share/example/create_mysql




Screen clipping taken: 2/16/2014 11:18 PM

```
mysql> select table_type,table_name,table_schema from information_schema.tables where table_rows>=1;
+------------+-------------------------------------------+--------------------+
| table_type | table_name                                | table_schema       |
+------------+-------------------------------------------+--------------------+
| BASE TABLE | detail                                    | barnyard2          |
| BASE TABLE | encoding                                  | barnyard2          |
| BASE TABLE | schema                                    | barnyard2          |
| BASE TABLE | db                                        | mysql              |
| BASE TABLE | general_log                               | mysql              |
| BASE TABLE | help_category                             | mysql              |
| BASE TABLE | help_keyword                              | mysql              |
| BASE TABLE | help_relation                             | mysql              |
| BASE TABLE | help_topic                                | mysql              |
| BASE TABLE | proxies_priv                              | mysql              |
| BASE TABLE | slow_log                                  | mysql              |
| BASE TABLE | user                                      | mysql              |
| BASE TABLE | cond_instances                            | performance_schema |
| BASE TABLE | events_waits_current                      | performance_schema |
| BASE TABLE | events_waits_history                      | performance_schema |
| BASE TABLE | events_waits_history_long                 | performance_schema |
```

Screen clipping taken: 2/16/2014 11:28 PM

**حالا باید مجوز های دسترسی لازم را به جداول بدهیم:**

- **#mysql -u root -p #Mysql>GRANT ALL PRIVILEGES ON barnyard2.* TO snort@localhost WITH GRANT OPTION**
- **#Mysql>SET PASSWORD FOR snort@localhost=PASSWORD('*password*');**

- **راه اندازی barnyard2:**

- **#barnyard2 -c /usr/local/etc/barnyard2.conf -d /var/log/snort/ -w /var/log/snort/barnyard2.waldo -f merged.log -u snort -g snort -D**

- **خطاهای احتمالی که برخورد کردم:**

?

```
Set gid to 40000
Set uid to 40000
FATAL ERROR: spo_unified2.c(317) Could not open /var/log/snort/merged.log: Permission denied
```

Screen clipping taken: 2/16/2014 5:18 AM

**Chown snort:snort merged.log**

? دوباره خطایی مبنی بر اینکه barnyard2 قادر استخراج timestamp extension از merged.log می داد.

merged.log را بنا بر توصیه فردی در انجمن winsnort پاک کردم.
(البته این فایل در اسکریپت زمان اجرای اسنورت ساخته می شود و در پوشه های جداگانه قرار می گیرد ، من merged.log موجود در /var/log/snort/ را پاک کردم)

- **مدیریت سرور mysql با phpmyAdmin :**

Phpmyadmin یک ابزار جالب برای مدیریت پایگاه داده mysql است.این ابزار یک رابط وب است که اجازه اجرای پرسجوهای SQL ، اضافه کردن کاربر و تنظیم محدوده دسترسی آن ها و پشتیبان گیری از پایگاه داده را می دهد.

- **قبل از نصب آن باید سرور apache22و php5 و php extensions را نصب و تنظیماتی را انجام داد.**

- **نصب apache22:**

برای نصب این سرور به پورت مربوطه بروید و آن را نصب کنید:

```
cd /usr/ports/www/apache22
make install clean
```

بعد از نصب apache22 خط زیر را به فایل /etc/rc.conf اضافه کنید.این خط باعث می شود که apache22 بصورت خودکار در زمان بوت اجرا شود.

❖ apache24_enable="YES"

حالا apache22 را با دستور زیر اجرا کنید.

➢ /usr/local/etc/rc.d/apache24 start

- **نکته ای راجع به hostname (rc.conf و hosts)**

- باید hostname به فرمت قابل قبول برای سرور باشه. مثل : msoltani.com
پس hostname را در این فایل Etc/rc.conf تغییر داد.

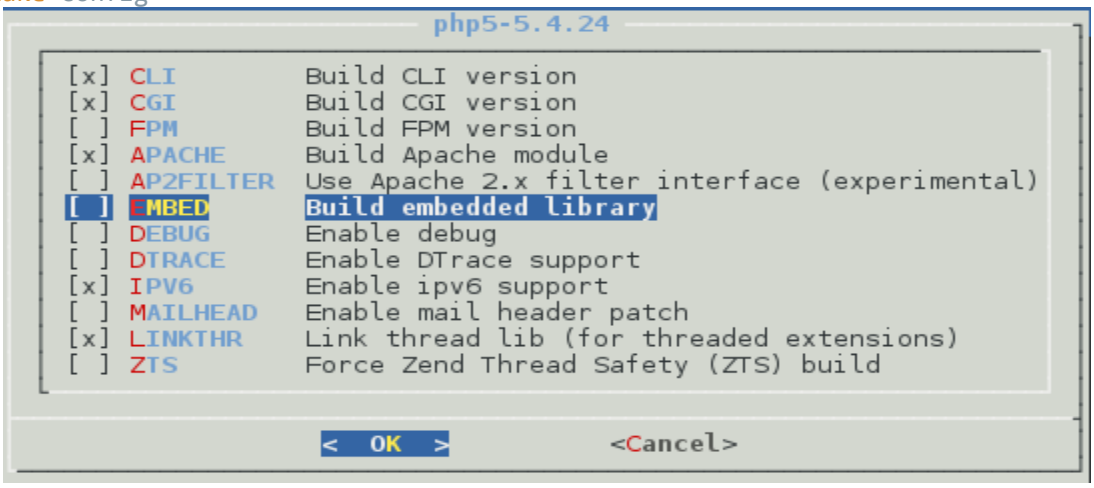
- و *ip* هم همون *ip local* کارت شبکه که با دستور *ifconfig* بدست میاد.
پس خط زیر را باید در *Etc/host* اضافه کرد.

➢ *Msoltani.com 192.168.137.129*

- **نصب php**

حالا باید php را نصب کنیم ، چون ابزار هایی مثل phpMyAdmin و Base بر پایه ی php نوشته شده اند. در ضمن باید در زمان نصب پیکربندی انجام شود.

- cd /usr/ports/lang/php5
- make config




منویی بالا می آید و گزینه هایی برای پیکربندی در اختیار می گذارد. باید حتما گزینه ی build Apache module فعال شود . و حتما embed را غیرفعال کرد.

در نهایت با دستور make install clean نصب می شود.

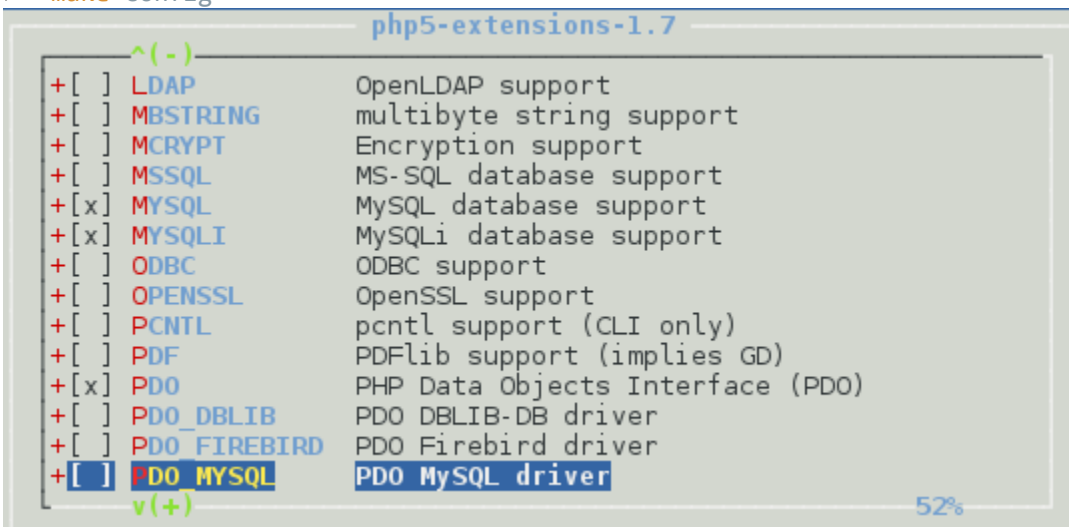
ساخت فایل پیکربندی تنها بااجرای کد زیر:

```
cp /usr/local/etc/php.ini-development /usr/local/etc/php.ini
```

- **نصب php5-extensions**:

باید extension مورد استفاده php را نصب کرد ، در ضمن برای ارتباط با mysql server نیاز به پیکربندی متفاوت از پیکربندی پیشفرض هستیم.

```
cd /usr/ports/lang/php5-extensions/
make config
```




باید MySQL database supportوMySQLi database support را انتخاب کرد.

در آخر هم نصب :

- Make install clean

- **نصب phpmyadmin** :

phpmyAdmin از طریق پورت با دستورات زیر اجرا می شود:

```
cd /usr/ports/databases/phpmyadmin/
make config
```

مطمئن شوید این دو MYSQL M(DB_connect): PHP MySQL support via mysql client و MYSQLI M(DB_connect) PHP Improved MySQL client support فعال باشند.

```
make install clean
```

- پیکربندی **phpmyAdmin** :

phpmyAdmin در دایرکتوری /usr/local/www/ phpmyAdmin بصورت پیشفرض نصب می شود.با ساخت میزبان مجازی می توان از یک دامنه بوسیله phpmyAdmin.yourdomain.com به آن دسترسی داشت.در آن صورت باید این دایرکتوری را رمز گذاری کرد تا در خارج از سیستم دسترسی کامل به آن وجود نداشته باشد.این کار با اضافه کردن این خطوط به فایل /etc/httpd.conf انجام می شود:

```
<VirtualHost *:80>
DocumentRoot /usr/local/www/phpMyAdmin
ServerName phpmyadmin.yourdomain.com
CustomLog /usr/local/www/logs/phpmyadmin-access_log combined
ErrorLog /usr/local/www/logs/phpmyadmin-error_log
</VirtualHost>

<Directory "/usr/local/www/phpMyAdmin">
Options Indexes FollowSymLinks
AllowOverride AuthConfig
Order deny,allow
Allow from all
</Directory>
```

البته در صورت داشتن یک وب سرور مثل apache22 می توان دایرکتوری پیشفرض آن را به /usr/local/www/ phpmyAdmin تغییر داد واز طریق server address به آن دسترسی داشت.

Httpd.conf :

```
<Directory "/usr/local/www/phpMyAdmin">
#<Directory "/usr/local/www/base">
DocumentRoot "/usr/local/www/phpMyAdmin"
#DocumentRoot "/usr/local/www/base"
```

قبل از اینکه مرورگرتان را باز کنید باید فایل پیکربندی phpmyAdmin را ویرایش کرد و جزئیات sql server را در آن وارد کرد:

- `cp /usr/local/etc/php.ini-development /usr/local/etc/php.ini`

فایل پیکر بندی در usr/local/www/ phpmyAdmin/config.inc.php قرار دارد.در صورتیکه پسورد ریشه را تغییر داده اید، این خطوط را وارد کنید:

```
$cfg['Servers'][$i]['user']     = 'root';
$cfg['Servers'][$i]['password'] = 'your_pass';
```

- **پیکربندی apache22(httpd.conf):**

با اضافه نمودن این دو خط فایل های شاخص به سرور معرفی می شوند.

- `DirectoryIndex index.html`
- `DirectoryIndex index.html index.htm index.php`

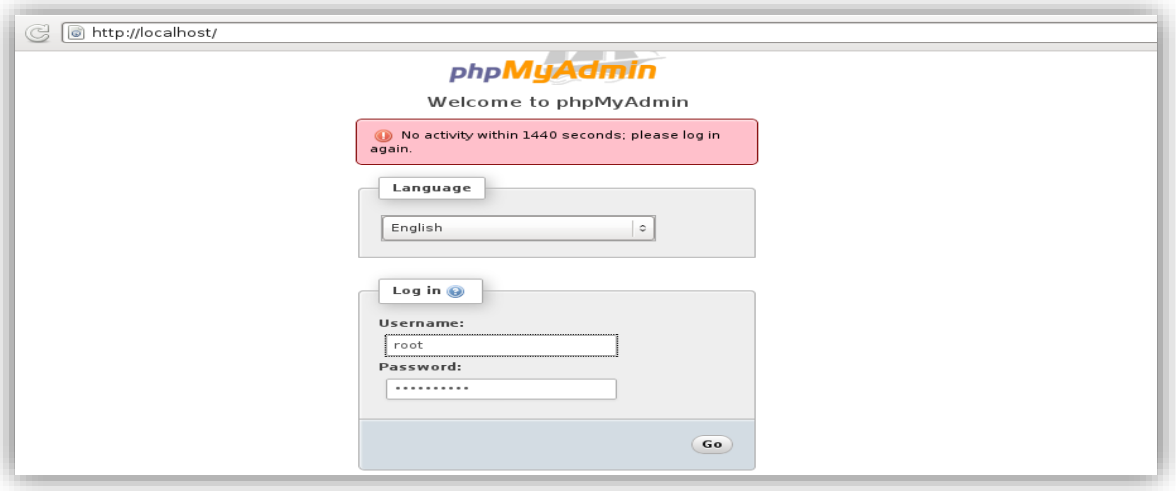
این چند خط هم اجازه اجرای فایل های php، htm ، html در کنار هم می دهد:

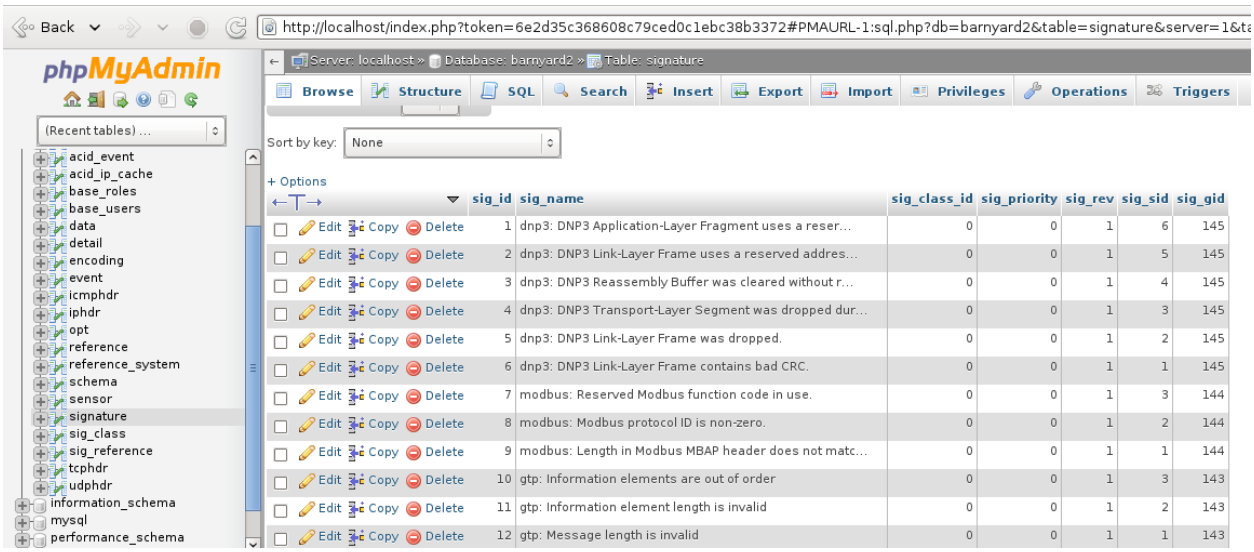
- AddType application/x-httpd-php .php
  AddType application/x-httpd-php-source .phps

- AddType application/x-httpd-php .php .htm .html

- **اجرای و تست phpmyadmin:**

تنها کافیست localhost را در مرورگر خود تایپ کنید تا آپاچی به دایرکتوری ریشه خود مراجعه کندو فایل index.php موجود در آن را اجرا کند.






حالا براحتی می توان جداول barnyard2 را مشاهده و پرس و جو های مختلف را بروی آن انجام داد.

- **نصب hping-devel**:

این نرم افزار قادر است انواع بسته های tcp، utp و ... را در مد های مختلف بر روی پورت های متفاوت در دوره های زمانی مشخص به ماشین های مقصد بفرستد.

برای نصب این نرم افزار کافیست دستور make install cleanرا در اسکلت پورت /usr/ports/net/hping-devel اجرا کرد.

- نمونه هایی از فراخوانی این نرم افزار :

**# hping example.com -S –V**

**پکت های SYN TCP را به پورت 0 میزبان example.com می فرستد.**

**# hping example.com -S -A -F -V -p 443**

**پکت های TCP را به پورت 443 میزبان example.com با تنظیم فلگ های SYN + ACK + FIN**

- **تست اسنورت:**

فایلی با نام test.rules در پوشه ../rules/ می سازیم ، و rule زیر را در آن وارد می کنیم.آدرس این فایل رو باید به فایل پیکربندی اسنورت اضافه کرد.

```
alert tcp any any -> any any (content:"https://www.google.co.th/";
msg:"someone one google website ..."; sid:1231213;)
```

اگر اسنورت در مد ids درست پیکربندی شده باشد ، با فراخوانی آدرس زیر در مرورگر باید پیغام زیر این کار را بعنوان هشدار در اعلان خود نمایش دهد.


```
Commencing packet processing (pid=20758)
02/18-18:00:45.824480  [**] [1:1231213:0] someone one google website ... [
**] [Priority: 0] {TCP} 173.194.70.94:80 -> 192.168.153.128:24953
```

- **تشخیص حمله :**

حمله synflood توسط نرم افزار hping-devel

- # Hping -S -p 80 --flood -rand-source <dist-adress>-V -I em0

سوئیچ S– فلگ SYN را فعال می کند و سوئیچ p– شماره پورت را مشخص می کند. سوئیچ ran-source– هم همانطور آدرس مبدا را بصورت رندوم تغییر می دهد. سوئیچ I– هم رابط شبکه ای که بسته از آن ارسال می شود را مشخص می کند.

```
root@msoltani:/usr/ports/net/hping-devel # hping 192.168.1.3 -S -p 80 --flood --rand-so
urce -V -I em0
using em0, addr: 192.168.1.2, MTU: 1500
HPING 192.168.1.3 (em0 192.168.1.3): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.1.3 hping statistic ---
835640 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

خط زیر را در  هما ن فایل  test.rules که در بالا ساختیم ، وارد کنید.

- alert tcp any any -> $HOME_NET 80 (flags: S; msg:" Alert Dos Attack!! :("; flow: stateless ;

  threshold: type both, track by_dst, count 70, seconds 10; sid:100000; rev:1;

با اجرای دستور زیر اخطار ها در اعلان نمایش داده می شوند.

Snort –c /usr/local/snort/snort.conf –A console –I em0

همانطور که در شکل زیر می بینید حمله بدرستی تشخیص داده شده:

```
Commencing packet processing (pid=21945)
02/19-15:19:58.340005  [**] [1:100000:1] Dos Att
02/19-15:20:08.005159  [**] [1:100000:1] Dos Att
02/19-15:20:18.005417  [**] [1:100000:1] Dos Att
02/19-15:20:40.056088  [**] [1:100000:1] Dos Attack !!! [**] [Priority: 0] {TCP} 1.159.248.36:37555 -> 192.168.1.3:80
02/19-15:20:52.221306  [**] [1:100000:1] Dos Attack !!! [**] [Priority: 0] {TCP} 85.103.176.209:38396 -> 192.168.1.3:80
02/19-15:21:07.326877  [**] [1:100000:1] Dos Attack !!! [**] [Priority: 0] {TCP} 38.159.162.35:17305 -> 192.168.1.3:80
02/19-15:21:17.017803  [**] [1:100000:1] Dos Attack !!! [**] [Priority: 0] {TCP} 144.167.201.85:54495 -> 192.168.1.3:80
02/19-15:21:27.005229  [**] [1:100000:1] Dos Attack !!! [**] [Priority: 0] {TCP} 79.143.77.214:22804 -> 192.168.1.3:80
02/19-15:21:37.005934  [**] [1:100000:1] Dos Attack !!! [**] [Priority: 0] {TCP} 134.38.17.229:61244 -> 192.168.1.3:80
02/19-15:21:47.005032  [**] [1:100000:1] Dos Attack !!! [**] [Priority: 0] {TCP} 122.172.178.41:6608 -> 192.168.1.3:80
02/19-15:21:57.005855  [**] [1:100000:1] Dos Attack !!! [**] [Priority: 0] {TCP} 126.110.103.182:48939 -> 192.168.1.3:80
02/19-15:22:07.029735  [**] [1:100000:1] Dos Attack !!! [**] [Priority: 0] {TCP} 179.192.122.32:4870 -> 192.168.1.3:80
02/19-15:22:17.005844  [**] [1:100000:1] Dos Attack !!! [**] [Priority: 0] {TCP} 147.178.227.255:29522 -> 192.168.1.3:80
02/19-15:22:27.005215  [**] [1:100000:1] Dos Attack !!! [**] [Priority: 0] {TCP} 182.67.148.77:16496 -> 192.168.1.3:80
02/19-15:22:37.005350  [**] [1:100000:1] Dos Attack !!! [**] [Priority: 0] {TCP} 8.109.95.64:59203 -> 192.168.1.3:80
02/19-15:22:47.005030  [**] [1:100000:1] Dos Attack !!! [**] [Priority: 0] {TCP} 208.237.240.1:43267 -> 192.168.1.3:80
02/19-15:22:57.006472  [**] [1:100000:1] Dos Attack !!! [**] [Priority: 0] {TCP} 104.96.169.153:22282 -> 192.168.1.3:80
--- 192.168.1.3 hping statistic ---
835640 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@msoltani:/usr/ports/net/hping-devel #
```