



CONOCIENDO

SNORT

El Cerdito Valiente



OWASP

The Open Web Application Security Project



OWASP

The Open Web Application Security Project

- Acerca de Mi.
- Jaime Iván Mendoza R.
- Analista Ethical Hacking COTAS
- Perl
- Pentester
- jaime981@hotmail.com





OWASP

The Open Web Application Security Project

IDS / IPS ????????????



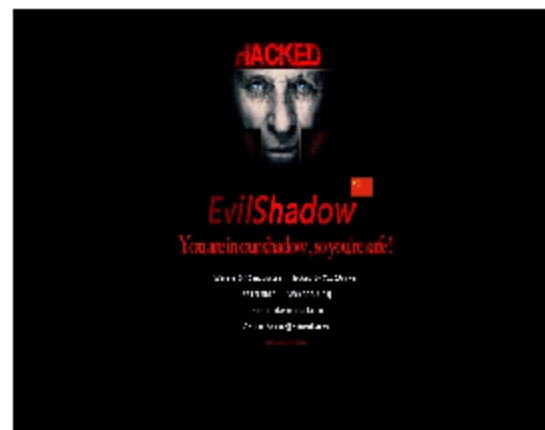
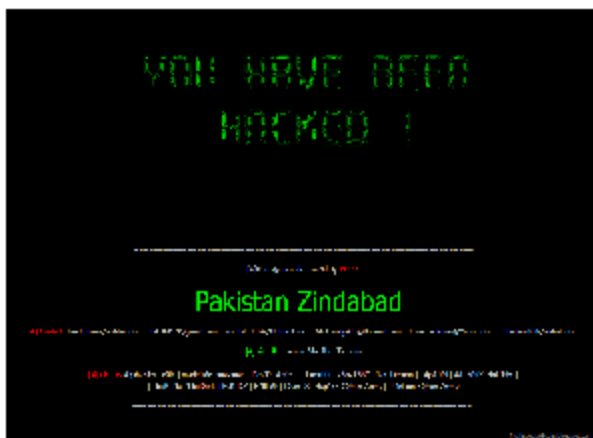
Un **sistema de prevención de intrusos** (o por sus siglas en [inglés IPS](#)) es un [software](#) que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de prevención de intrusos es considerada por algunos como una extensión de los [sistemas de detección de intrusos](#) (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías [cortafuegos](#).



OWASP

The Open Web Application Security Project

DEFACED WEBi!!!!





OWASP

The Open Web Application Security Project

SNORT ?????





OWASP

The Open Web Application Security Project

Un Poco de Historia



En noviembre de 1998, Marty Roesch escribió un programa para Linux llamado APE. Sin embargo, carecía de lo siguiente:

- Trabajar en múltiples Sistemas Operativos.

- Capacidad para trabajar con el formato hexdump.

- Mostrar todos los tipos de paquetes de la misma forma.

- A partir de ello comenzó a desarrollar como una aplicación de libcap, lo que le da gran portabilidad.



OWASP

The Open Web Application Security Project

SNORT EN LA WIKI

Snort es un sniffer de paquetes y un detector de intrusos basado en red. Es un software muy flexible que ofrece capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas





OWASP

The Open Web Application Security Project

Funcionamiento de Snort

Snort permite controlar todos los paquetes que atraviesan la red en la cual se ha instalado. Estos paquetes **son analizados y es posible determinar qué acciones se llevarán a cabo a partir de reglas.**

El comportamiento de *Snort* se establece a partir de **un archivo de configuración**

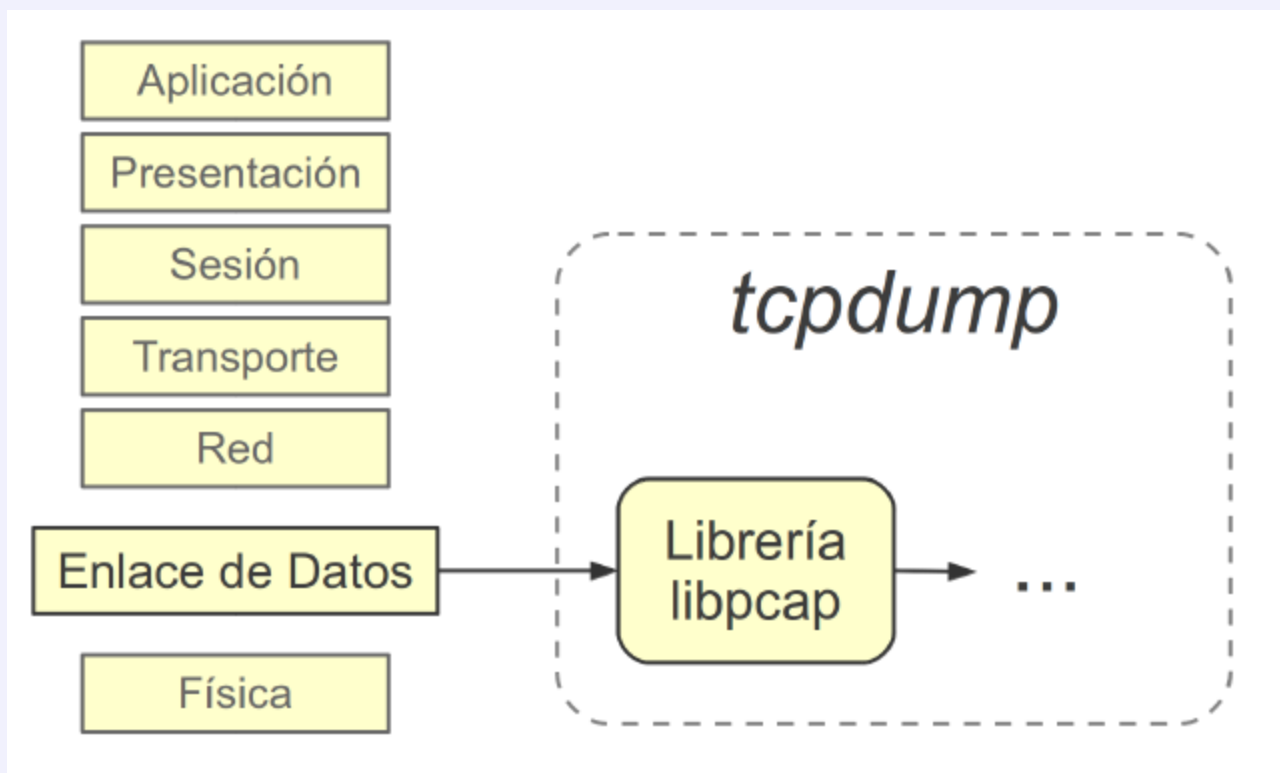




OWASP

The Open Web Application Security Project

EL CORAZON DE SNORT: LIBPCAP

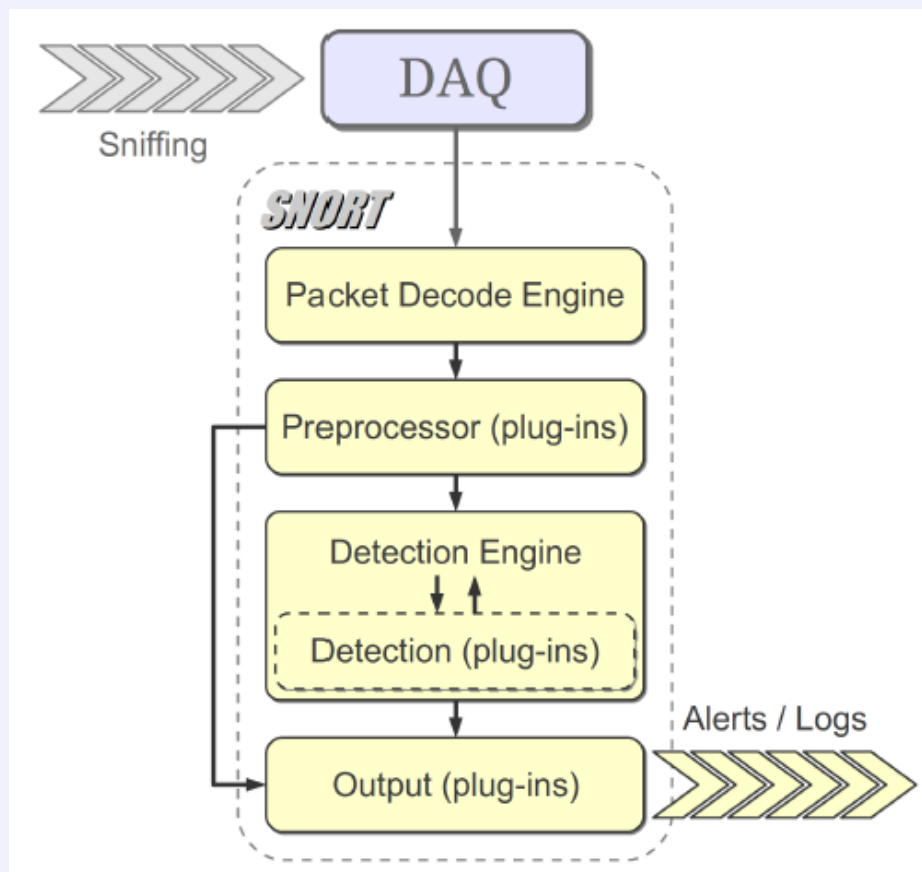




OWASP

The Open Web Application Security Project

COMO FUNCIONA SNORT???





OWASP

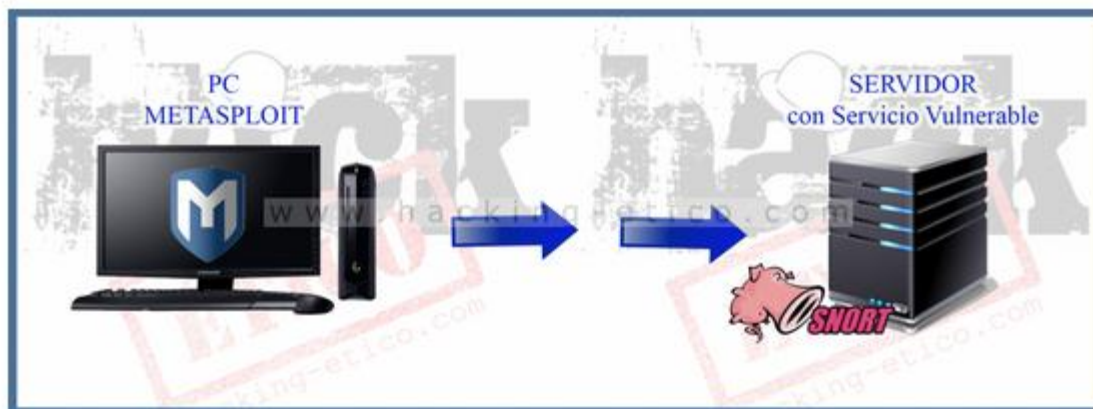
The Open Web Application Security Project

ALGUNOS USOS DE SNORTiii

Parando Metasploit con Snort

[febrero 20, 2015](#) / [Eduardo Sánchez](#) / [2 comments](#)

Hoy vamos a ver como podemos detectar cualquier tipo de ataque a una aplicación vulnerable de nuestro servidor, simplemente analizando aquellos posibles exploit que puedan ser lanzados contra este y añadiendo una regla en nuestro IDS para detectarlos y pararlos, en nuestro caso utilizaremos Snort. El escenario sería el siguiente:



<http://hacking-etico.com/2015/02/20/parandometasploitconsnort/>



OWASP

The Open Web Application Security Project

MEJORANDO SNORTiiii

Una característica muy importante e implementada desde hace pocas versiones es FlexResp. Permite, dada una conexión que emita tráfico malicioso, darla de baja, hacerle un DROP mediante el envío de un paquete con el flag RST activa, con lo cual cumpliría funciones de firewall, cortando las conexiones que cumplan ciertas reglas predefinidas. No sólo corta la conexiones ya que puede realizar otras muchas acciones



OWASP

The Open Web Application Security Project

SNORT + CISCO



<http://www.muycomputerpro.com/2014/03/06/cisco-snort>



OWASP

The Open Web Application Security Project

SNORT DESDE LA NUBE

CLOUD | NOTICIAS | 13 JUL 2010

Sourcefire ofrecerá la prevención de intrusiones de Snort desde la nube

Tags: Servicios Internet

El creador de Snort, software de detección de intrusiones de código abierto, proporcionará IPS basado en cloud utilizando la plataforma Amazon Web Services (AWS).

[Tweet](#)

[in](#) Compartir

0

[G+](#) Compartir

0

IDG.es

Con este salto, tanto [Snort](#) como las reglas del equipo de investigación de vulnerabilidades (VRT) de Sourcefire estarán disponibles a través de **Amazon Elastic Compute Cloud (Amazon EC2)** en forma de **AMI (Amazon Machine Image)**, de forma que los usuarios podrán monitorizar la actividad de su red de forma proactiva en busca de comportamientos maliciosos y proporcionar una respuesta automatizada.

<http://cso.computerworld.es/cloud/sourcefire-ofrecera-la-prevencion-de-intrusiones-de-snort-desde-la-nube>



OWASP

The Open Web Application Security Project

DETECTING SIP ATTACKS WITH SNORT



La protección de la red contra amenazas de VoIP es sólo la mitad de la historia . El resto consiste en la detección de que su sistema está bajo ataque . Sistemas de detección de intrusiones , como Snort se puede configurar para ayudar con esta tarea . Actualmente el uno puede encontrar algunas normas relacionadas con el SIP en las últimas reglas de la comunidad Snort . Estas reglas son capaces de detectar ataques (generados con herramientas como swar y svcrack) que crean un gran número de INVITE o registrarse solicitudes SIP , así como " 401 no autorizado " respuestas SIP .

<http://blog.sipvicious.org/2008/02/detecting-sip-attacks-with-snort.html>



OWASP

The Open Web Application Security Project

ELASTIX Y SNORT

Extendiendo la
Seguridad de Elastix
con Snort





OWASP

The Open Web Application Security Project

SNORT + KALI + RASPBERRY PI IDS COMPACTO

Tuesday, September 23, 2014

Installing Kali Linux and Snort on a Raspberry Pi



Last week I wrote about [building a passive network tap](#) with about \$10 in off-the-shelf parts. Building a tap is a nice little project, but what do you do with it? A simple first step is to install Wireshark on a laptop and capture some packets. I wanted something a little more elegant though. Earlier this year I posted an [April Fools gag](#) on various uses for a Raspberry Pi ... this time I am putting it to legitimate use.

The Raspberry Pi is a minimalist computer: a processor; a bit of memory; ports for network, video, and sound; an SD card slot for data and operating system storage; a few USB ports to attach additional components; and a micro-USB port to supply power. Altogether a bare-bones Pi costs about \$35. You can buy a Pi with a protective case, an SD card, and a power supply for around \$50 to \$60. I picked up bundle with the Raspberry Pi model B, clear case, and wireless adapter for \$49.95, plus a 16 GB SD card for another \$10. In truth, I could have gotten by with a smaller SD card, but the software tools I had in mind to use take up some space, and network captures can quickly fill up a drive.

<http://www.diva-portal.se/smash/get/diva2:819555/FULLTEXT01.pdf>

<http://www.securityforrealpeople.com/2014/09/installing-kali-linux-and-snort-on.html>

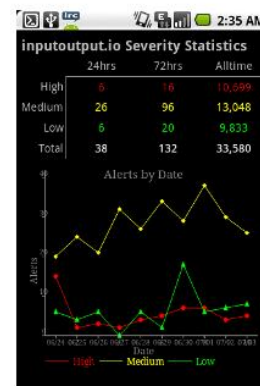
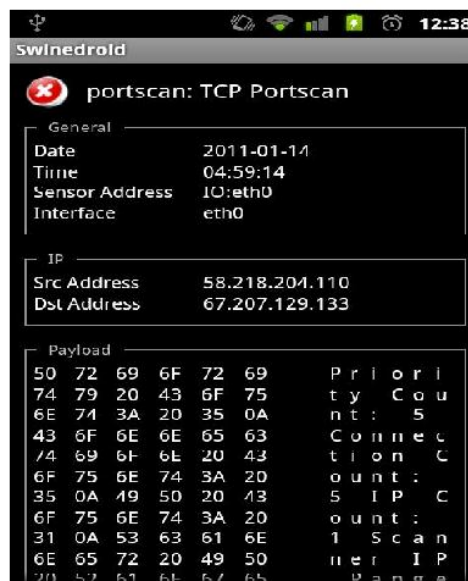


OWASP

The Open Web Application Security Project



SWINEDROID



<https://github.com/Hainish/Swinedroid>



OWASP

The Open Web Application Security Project

MODOS DE OPERAR SNORT..

Snort es una herramienta que funciona en cuatro modos:

- Sniffer Mode.
- Packet Logger Mode.
- Network Intrusion Detection System (NIDS).
- Inline Mode.



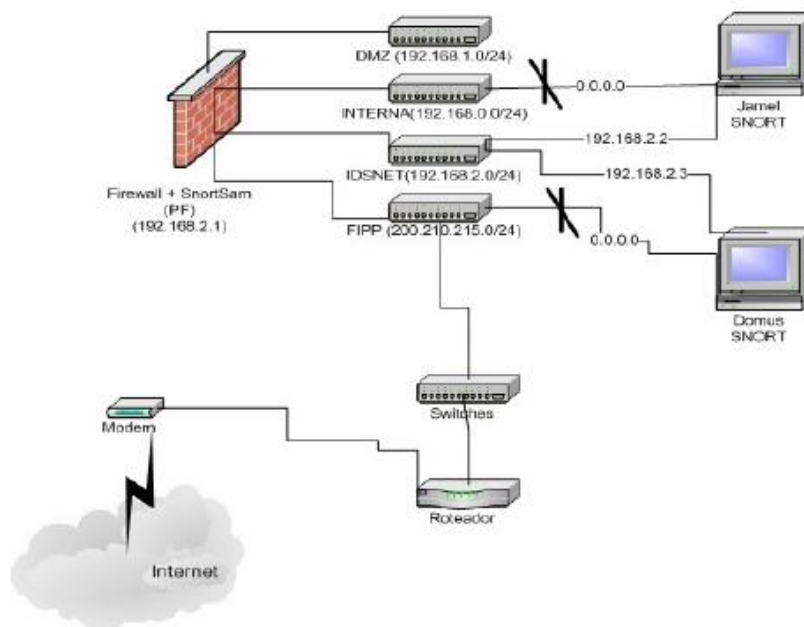
OWASP

The Open Web Application Security Project

SNORT + SNORTSAM iiiii

Esquema de rede com Snort

- Snort + SnortSam:





OWASP

The Open Web Application Security Project

DESCRIPCION MODOS DE OPERACIÓN SNORT

Modo sniffer

El modo sniffer permite escuchar todo el tráfico de la red y mostrarlo en pantalla. Una vez que finaliza el modo sniffer nos muestra una estadística del tráfico. Para iniciar el modo sniffer y visualizar en pantalla todo el tráfico TCP/IP debemos ejecutar el comando:

Modo Packet Logger

Si ejecutamos snort en modo sniffer veremos gran cantidad de información pasar por nuestra pantalla, con lo cual sería interesante guardar estos datos en disco para su posterior estudio. El modo Packet Logger escucha todo el tráfico de la red y los registra en un determinado directorio. Para ejecutar snort en este modo debemos utilizar el parámetro `-l /var/log/snort`. Donde `/var/log/snort` es el directorio donde se registra el tráfico.

Modo Sistema de Detección de Intrusos de Red

Este será el modo de funcionamiento en el que nos centraremos en este artículo. Es la opción más completa y configurable. Permite analizar el tráfico de la red en busca de intrusiones a partir de los patrones de búsqueda (rules) definidos por el usuario. Snort nos informará de intentos de acceso no permitido a nuestro host, así como de escaneos de puertos, ataques DOS, ejecución de exploits, etc. Para que Snort funcione en modo IDS, debemos pasar el parámetro `-c directorio` hacia `snort.conf`. Como hemos visto antes, en el fichero de configuración `snort.conf`, especificamos la configuración deseada. Una vez realizada la configuración, el siguiente paso es hacer que snort se ejecute cada vez que arrancamos. Para ello, podemos realizarlo de distintas formas. Una de ellas es incluir el siguiente comando en el archivo de arranque: `/etc/rc.d/rc.local`:

Modo Inline

Permite configurar el NIDS para que interactúe con el cortafuegos de forma que si snort detecta un ataque puede enviar a iptables la petición para que corte el tráfico. Para utilizar el modo snort-inline debemos configurar nuestro sistema en modo bridge y utilizar un módulo de salida para que se comunique con iptables (por ejemplo, snortsam www.snortsam.net).

http://www.adminso.es/index.php/SNORT-Modos_de_ejecuci%C3%B3n



OWASP

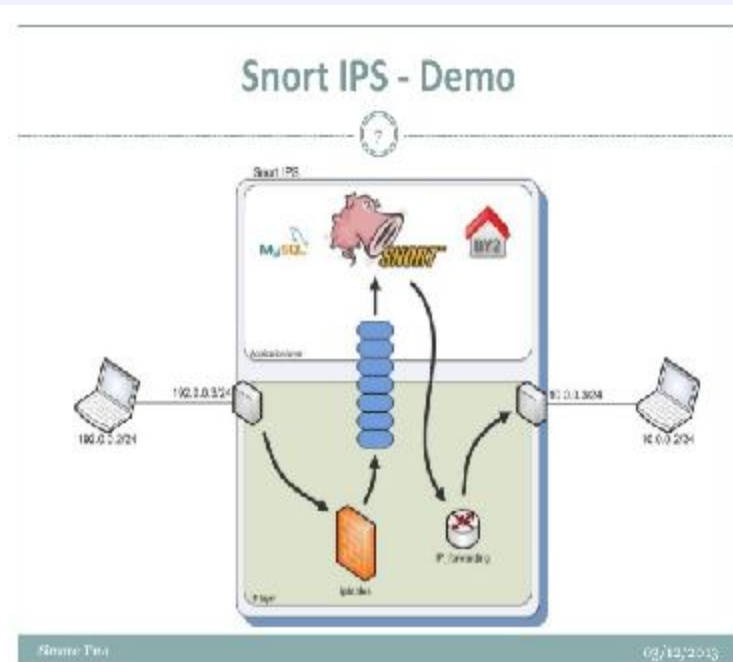
The Open Web Application Security Project

DONDE ESTA UBICADO SNORTiii

La colocación de Snort en nuestra red puede realizarse según el tráfico quieren vigilar: paquetes que entran, paquetes salientes, dentro del firewall, fuera del firewall... y en realidad prácticamente donde queramos.



ESCENARIOS CON SNORTiii

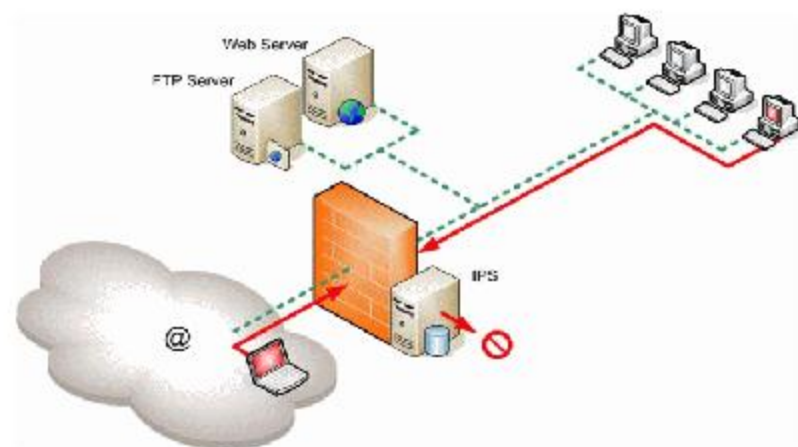
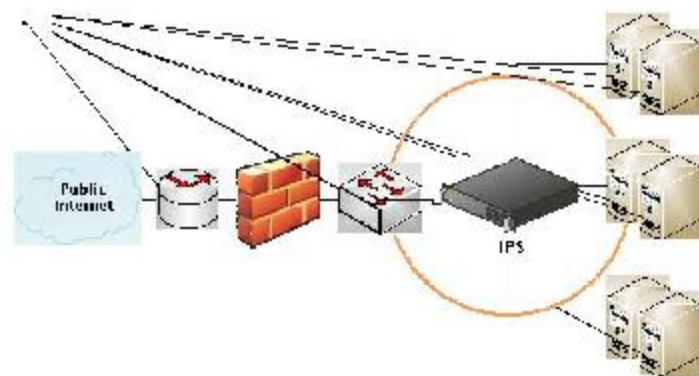




OWASP

The Open Web Application Security Project

ESCENARIOS CON SNORTiii

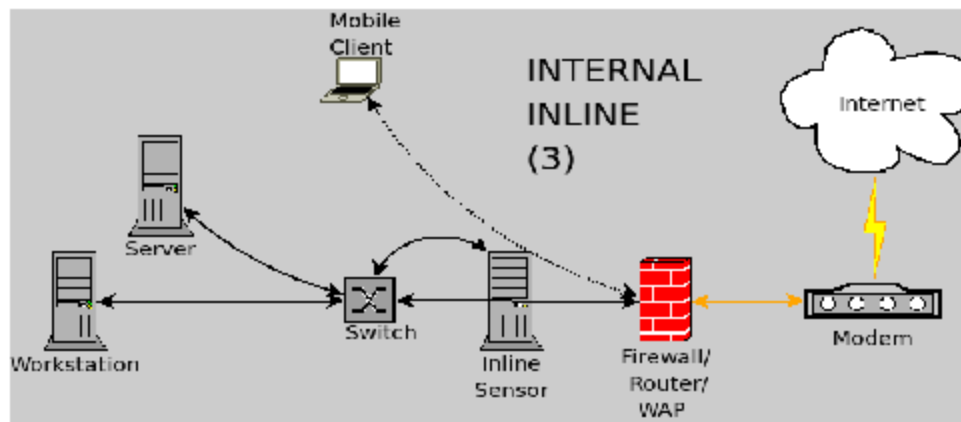
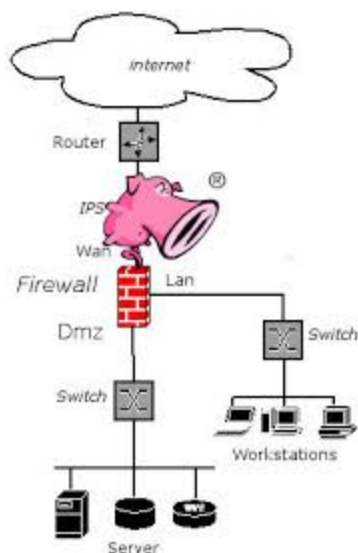




OWASP

The Open Web Application Security Project

ESCENARIOS CON SNORTiii

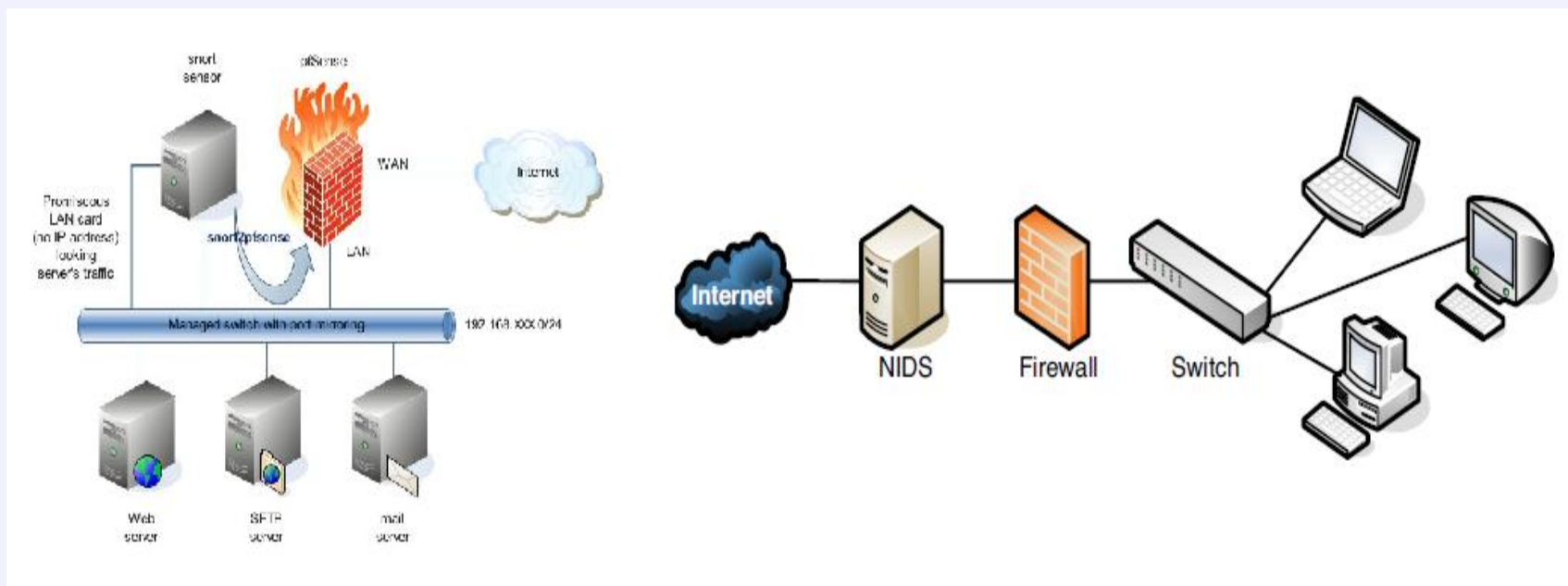




OWASP

The Open Web Application Security Project

ESCENARIOS CON SNORTiii

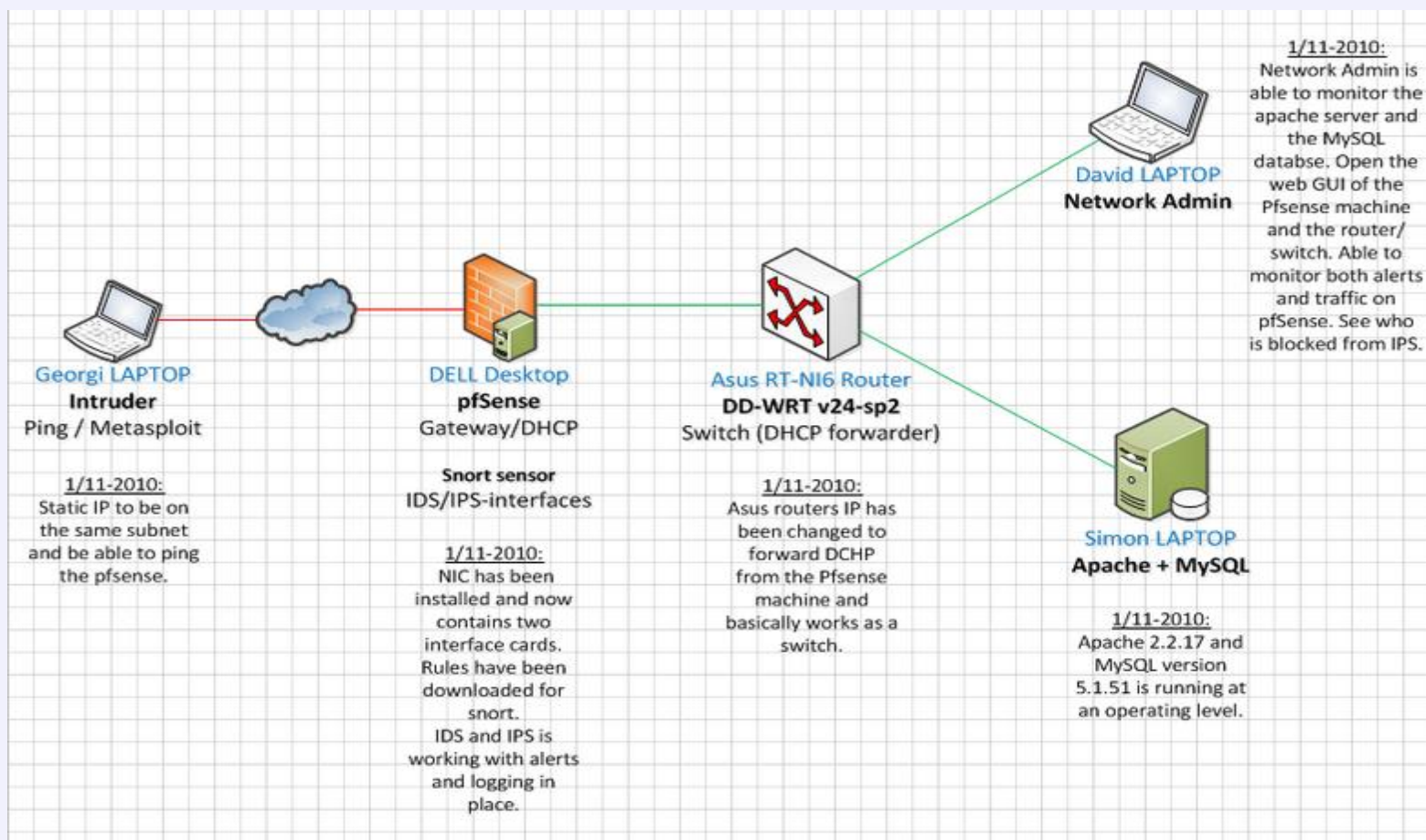




OWASP

The Open Web Application Security Project

ESCENARIOS CON SNORTiii





OWASP

The Open Web Application Security Project

EL PODER DE SNORTiiii

El poder y expansión de Snort se debe en gran parte a la influencia y al alcance de la comunidad de usuarios de Snort, ya que entre ellos existe un gran número de programadores que testean y publican resultados y opiniones acerca de las funcionalidades de Snort y del conjunto de reglas.

Como aventuró Eric Raymond en su obra, y posteriormente se comprobó en el desarrollo de GNU/Linux, cuando en una comunidad Open Source se detectan fallos, se responde ante ellos de forma más rápida y eficiente que en un entorno de desarrollo propietario.



OWASP

The Open Web Application Security Project

EL PODER DE SNORTiiii

Gracias al hecho de ser una aplicación Open Source, Snort cuenta con la ventaja de ser un sistema configurable y adaptable a necesidades concretas, por lo que puede ser una buena solución si se busca un sistema personalizado. Este es uno de los motivos por los que grandes organismos, como gobiernos y organizaciones militares, han decidido implementar sus propios sistemas de detección de intrusos utilizando Snort en lugar de aplicaciones propietarias que en muchos casos no alcanzan el mismo rendimiento ni las prestaciones de Snort



OWASP

The Open Web Application Security Project



QUESTIONS?



OWASP

The Open Web Application Security Project



Demo



OWASP

The Open Web Application Security Project



*Muchas
Gracias!*