

CURSO DE SEGURIDAD EN UNA RED LAN O EN UNA PC.

Bueno este pequeño manual va dirigido a la seguridad, específicamente va dirigido a proteger una red LAN o incluso proteger una sola PC contra ataques como por ejemplo: sniffer de red, captura de paquetes, keyloggers etc. Con eso ya de darán una idea de lo que veremos.

Para ello emplearemos el programa snort el es un sencillo IDS (intrusión detection system) o sistema de detección de intrusos ello lo veremos en el video como configurarlo y como protegernos de los atacantes aquí veremos que es un IDS y cómo funciona ya que el objetivo no es solo protegernos si no saber realmente como funcionan los IDS.

Una cosa más el snort corre perfectamente tanto como Linux como Windows con excepción que en Linux hay que introducirlo por línea de comandos y como el so de Windows es más usado lo ejemplificaremos desde Windows.

Ok sin mas preámbulo empezemos con el artículo

En primer lugar definamos que es un ataque o una intrusión: es el acto de entrar a un sitio ya sea PC o sitio web sin permiso es como colarse en una fiesta xd.

En la red una intrusión es el acto de comprometer cualquiera de nuestros dispositivos de red ya sea routers, switches o servidores para obtener privilegios y robar información ya sea bancaria o de uso de la compañía o personal.

Visto de este modo un IDS puede compararse con una alarma, que detecta intrusos y hace sonar la alarma.

Aunque un IDS es algo mas ya que reconoce los intrusos los identifica, detiene los ataques, incluso tiene una data base donde se pueden guardar las ip y así localizar el atacante con un simple localizador de ip con coordenadas como lo es google maps; se puede comparar un IDS con un antivirus ya que los av. analizan los archivos de tu disco duro en busca de código maliciosos básicamente los IDS hacen lo mismo pero analizando los paquetes de datos, trafico de tu red etc. a nivel de ip o de Mac (La *dirección MAC* es la dirección de la tarjeta de red.)

Los IDS utilizan diversas técnicas para lograr detectar las intrusiones por ejemplo: detección de firmas (como los antivirus), huellas de ataques conocidas (spoffin, ataques denegación de servicio, suplantación de Mac etc.) algunos IDS pueden llegar a desconectar el host atacado(así que no se asusten si al usar un IDS se les cae la internet puede ser que están bajo un ataque y esa fue la única solución que encontró el IDS para protegerlos).

TIPOS DE IDS

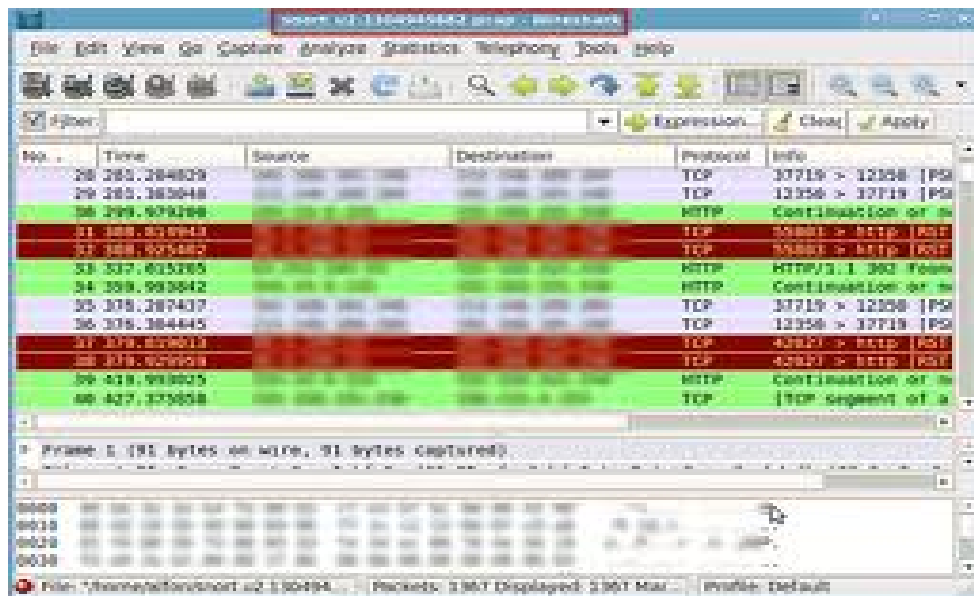
- 1. HIDS (HOSTIDS) :** este IDS del tipo que solo vigila un único host es decir en el caso que solo deseamos proteger una solo PC en estos casos la tarjeta de red no corre en modo

promiscuo(este modo es en síntesis poner a nuestra tarjeta a capturar todos los paquetes que pasen por ella aunque no sean para ella(spoffin)); su mayor ventaja radica en un uso menor del cpu y que hay tarjetas de red que por hardware no es posible ponerlas en modo promiscuo.

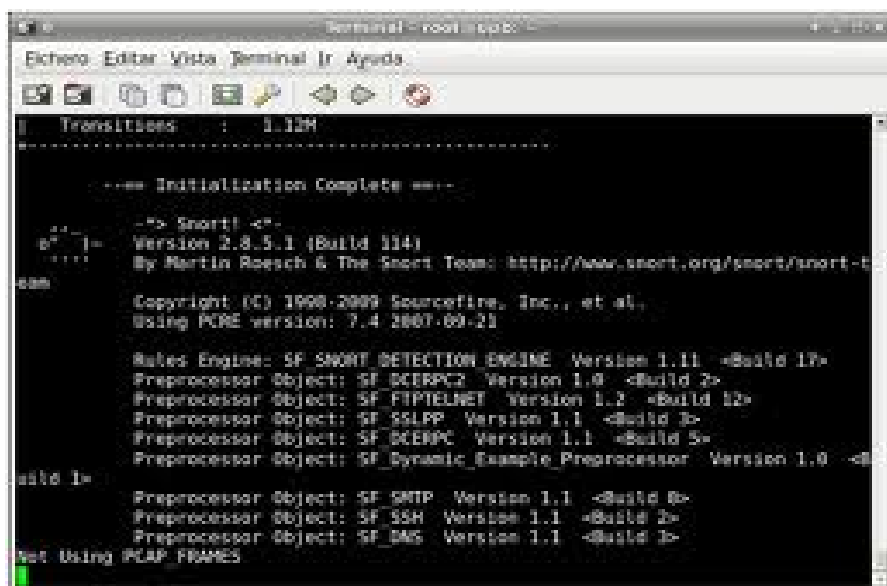
2. NIDS (NETWORKIDS) O IDS BASADOS EN RED: Este tipo de sistemas detectan ataques a todo segmento de red en el que corre el IDS, el inconveniente con este método es que la tarjeta de red debe correr en modo promiscuo, la utilización de este sistema debe ser analizada antes de ser empleada o puedes llegar a comprometer toda tu red.

3. DIDS (DISTRIBUTEDIDS) O IDS DISTRIBUIDOS: Esto es un sistema basado en arquitectura cliente/servidor es decir el IDS esta distribuido por toda la red como sensores, localizan ataques y los centralizan en una data base.

Ejemplo de cómo se vería la data base centralizada



La captura es con snort en Windows.



```
Transitioses : 1.12M
-----
--== Initialization Complete ==--
--> Snort! <P>
Version 2.8.5.1 (Build 114)
By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-
Copyright (C) 1998-2009 Sourcefire, Inc., et al.
Using PCRE version: 7.4 2007-09-21

Rules Engine: SF_SNRORT_DETECTION_ENGINE Version 1.11 <Build 17>
Preprocessor Object: SF_ICERPCD Version 1.0 <Build 2>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 12>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 3>
Preprocessor Object: SF_DCEMPC Version 1.1 <Build 5>
Preprocessor Object: SF_Dynamic_Example_Preprocessor Version 1.0 <B
uild 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 8>
Preprocessor Object: SF_SSH Version 1.1 <Build 2>
Preprocessor Object: SF_BAG Version 1.1 <Build 3>
Not Using PCAP_FRAMES
```

Captura de snort con Linux.

Con un IDS puede monitorizar servidores de base de datos (SQL, MYSQL, ORACLE) servidores DNS, servidores de mail y también CMS (panel de webs) así podemos evitar un desfase de webs.

Bueno espero les allá gustado este breve tuto de IDS en el video se le mostrara como instalar un IDS concretamente snort y como establecer reglas para nuestra seguridad aquí el link de descarga del snort <http://www.snort.org/dl/binaries/win32/> o lo buscan en san google jajá xd si no se fían de el link :P para usarlo deben tener pre instalado ya sea Oracle o mysql o SQL ósea una data base, a veces dependiendo de lo que harán necesitaran php o python entre otras cosas que el snort les pedirá también tener instalado el wincap <http://www.wincap.polito.it> usen la versión 2.3 que funciona perfectamente con snort.

Pd: revisar si no tienen wincap ya que mayormente varios programas en Windows usan wincap por lo tanto viene pre instalado.

Me despido

BY **ZERO.CRAKER**

