Nombre: Alejandro Asenjo

Objetivo: buscar información de alertas.

Fecha: 22 de julio – 17:28 / Fecha de Verificación 21/07/14 Hora entre 17:30 y del día 22 de julio 17:30.

Herramientas: logs ubicados en el servidor, y base de snort.

- **Open Source Tripwire 2.4** – No presenta errores.

Tripwire es una herramienta de seguridad e integridad de datos. Es útil para monitorizar y alertar de cambios en los ficheros de un sistema de ficheros.

- **Iptables** – No presenta errores.

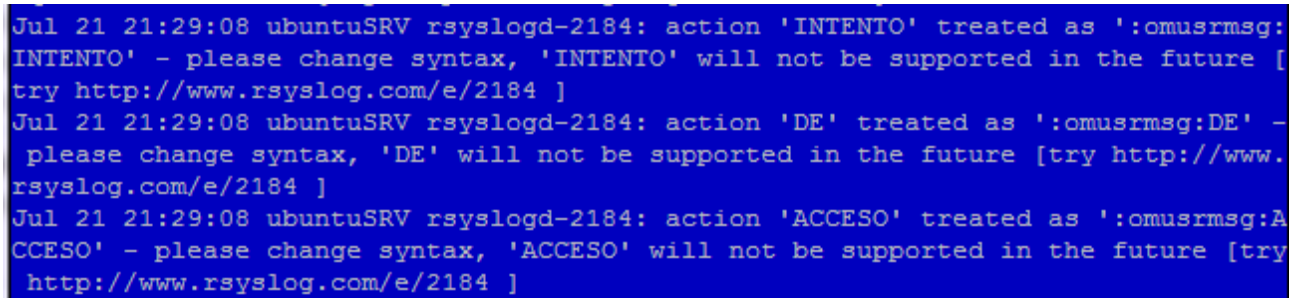
Iptables: es un cortafuegos que permite evitar lo más posibles los ataques de denegación de servicios y vulnerabilidades que otros puedan detectar de nuestro server.

- **Snort con Base** – No presenta ataques relevantes, ni que afecten al sistema.

Snort es un detector de intrusos basado en red (se monitoriza todo un dominio de colisión).

IPTABLE

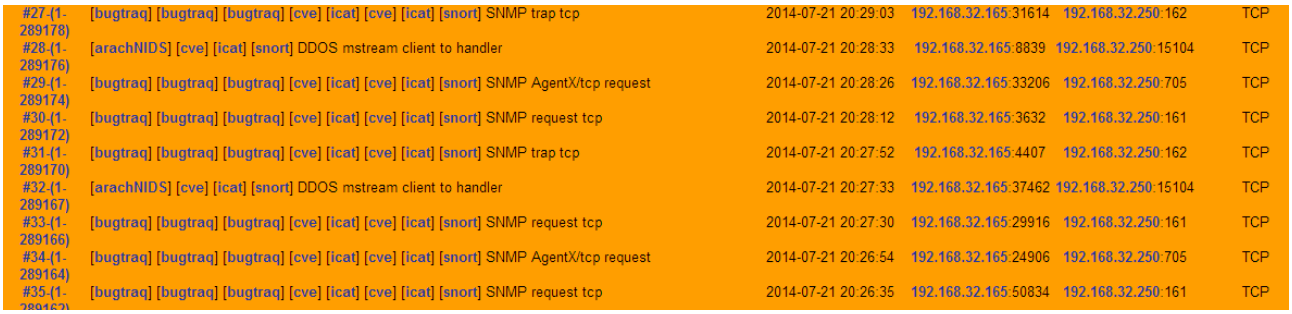
Detecto y bloqueo accesos al servidor.



El error que procesa de syntaxis nos avisa que un futuro habrá que modificarlo. Pero actualmente su funcionamiento es correcto.

SNORT

Se localizan varios intentos de ataques al servidor de distintos ordenadores, como por ejemplo:



Una de las vulenrabilidades es un gran número de implementaciones de SNMP permite a los atacantes remotos provocar una denegación de servicio o ganar privilegios mediante trampa SNMPv1 manejo, como lo demuestra el PROTOS c06-SNMPv1 serie de pruebas.

Esta versión del ataque es del 09/10/2008; el servidor al encontrarse actualizado, este ataque no tendrá importancia relevante.

Uno de los ordenadores tiene un programa que puede provocar una denegación de servicio distribuido master (DdoS), como agente o zombie instalado, tal como (1) Trinoo, (2) Red Tribu Flood (TFN), (3) Tribe Flood Network 2000 (TFN2K), (4) stacheldraht, (5) mstream, o (6) del eje.

Esta vulnerabilidad encontrada afecta a **Cisco**, al no utilizar **Cisco** este problema no nos afecta.