Abstract

Esta investigación intenta demostrar si es posible la introducción de un nuevo dispositivo de red que funcione como un firewall, siendo capaz de analizar los paquetes que circulen a través de él y detectar posibles ataques informáticos en la segunda y tercera capa del modelo OSI, siendo estas la capa de transporte de datos y la capa de red. El principal parámetro que debemos de tener en cuenta será el tiempo que tarda en procesar los paquetes de red, así que para tener valores aproximados se hará una simulación evento a evento.

Palabras clave

Redes, ARP, DNS, Proxy, Ataques de Red

Introducción

Uno de los principales protocolos que utilizan las redes de internet es el protocolo ARP (Address Resolution Protocol). Este permite vincular o asociar direcciones lógicas con direcciones físicas, en otras palabras asociar una dirección IP con su respectiva MAC Address.

Cuando se realiza una petición ARP, se manda dicha petición a todos los dispositivos de la red (broadcast) preguntando quien tiene la MAC en cuestión, el dispositivo que efectivamente la tiene responde; luego el dispositivo que recibe la respuesta guarda en una tabla esta relación para evitar tener que hacer peticiones iguales en el futuro.

Sin embargo este protocolo tiene dos problemas: primero que nada, cuando un dispositivo recibe una respuesta no puede validar que esta sea legitima, y segundo se acepta una respuesta aunque nunca se haya enviado una petición. Esto conlleva a que un dispositivo de la red pueda hacerse pasar otro, en la mayoría de los casos por lo router, a su vez esto conlleva a que el tráfico de la red pase por el dispositivo que realiza este ataque, logrando espiar que acciones se realiza, pudiendo descartarlas o modificarlas.

Para solucionar esta problemática se propone diseñar un dispositivo de red que actué como proxy entre la computadora que se desea proteger y el router, analizando el tráfico que pase por él y detectando el ataque descripto anteriormente, entre otros. Es fundamental que el tráfico no se vea ralentizado demasiado debido al análisis y que el usuario lo siga notando fluido.

Con respecto al dispositivo físico la idea es utilizar una placa Raspbery Pi ya que es sistema embebido que corre sistemas operativos basados en unix y además es de fácil acceso en el mercado

Elementos del trabajo y metodolgia

Se realizó una simulación evento a evento para evaluar si los tiempos de respuesta son factibles y cuánto tiempo están los paquetes de red esperando a ser procesados.

Analisis previo:

Metodologia: Evento a Evento

Variables exógenas:

Datos: IA, TE

Control: CT

Variables endógenas:

Estado: PARP, PT(i)

Resultado: PPS, PEC(i), PTO(i)

Explicación de las variables:

* IA: intervalo de arribo de paquetes en microsegundos
* TE: tiempo de evaluación de paquetes en microsegundos
* CT: cantidad de threads
* PARP: cantidad de paquetes con prioridad que están encolados en la cola virtual
* PT(i): cantidad de paquetes que tiene cada thread
* PPS: promedio de permanencia en el sistema
* PEC(i): promedio de espera en cola de cada thread
* PTO(i): porcentaje de tiempo oscioso de cada thread

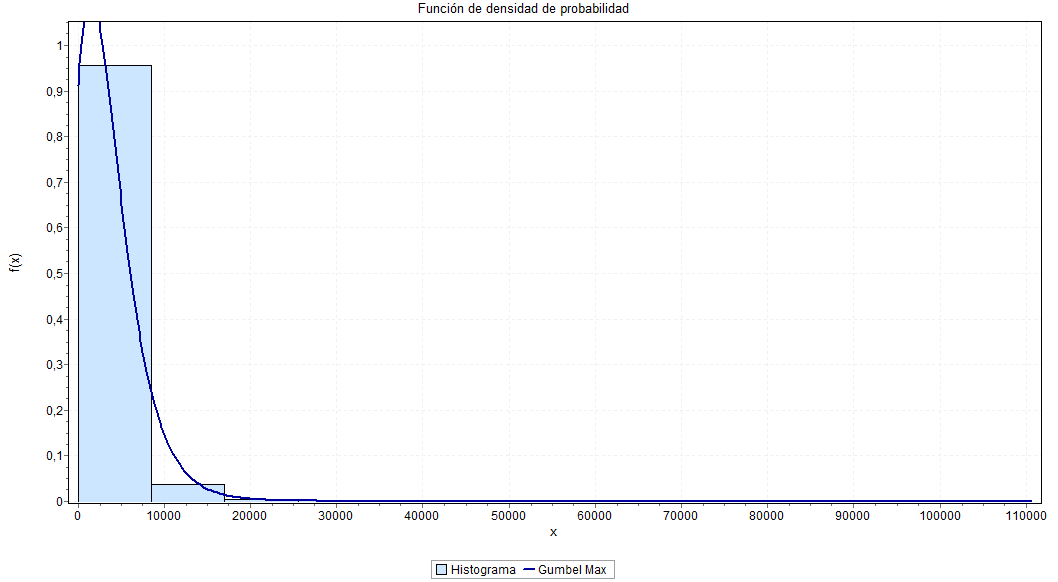
Obtención de las FDP:

Para esta simulación tuvimos que conseguimos dos FDP: IA y TE

Para la obtención de IA lo que hicimos fue correr un programa llamado Wireshark para capturar los paquetes de red que llegaban. El programa nos proporcionó el tiempo de llegada relativo según el primer paquete (siendo para este t=0) entonces exportamos esto a formato csv y mediante un script hicimos los respectivos cálculos para sacar el intervalo de arribo, luego cargamos los valores en el Easy Fit y la distribución que nos sugería fue la de Gumbel Max, cuya función de densidad de probabilidad acumulada es:

Donde y

Grafico obtenido:

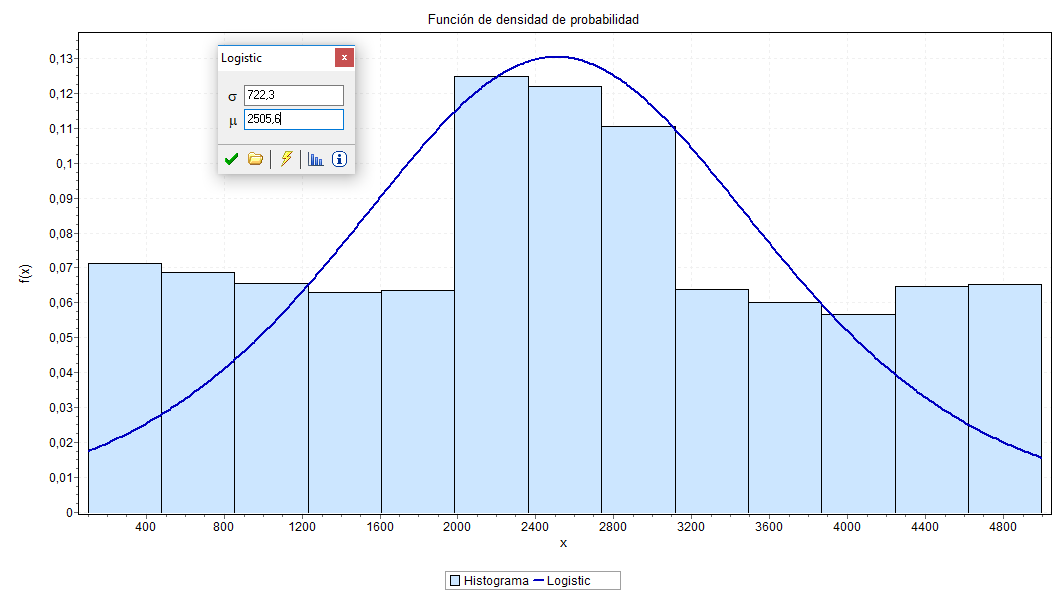


Usamos la metodología de función inversa, quedando:

Para la obtención de la TE corrimos un programa prototipo, similar al que correría en la placa Rasperry Pi. El input de este programa fue la misma captura de paquetes que para la obtención de la IA, por cada paquete analizado se guardó en un archivo la diferencia de tiempo en microsegundos respecto al paquete anterior, luego ese archivo se cargó en el Easy Fit. La distribución que sugirió fue Logistica, cuya función de densidad acumulada es:

Donde y

Grafico obtenido:



Usamos la metodología de función inversa, quedando:

Resultados

Discusion

Conclusion