DGTIC UNAM CERT

Generador de tráfico de red para IPv4 e IPv6

Sergio Anduin Tovar Balderas

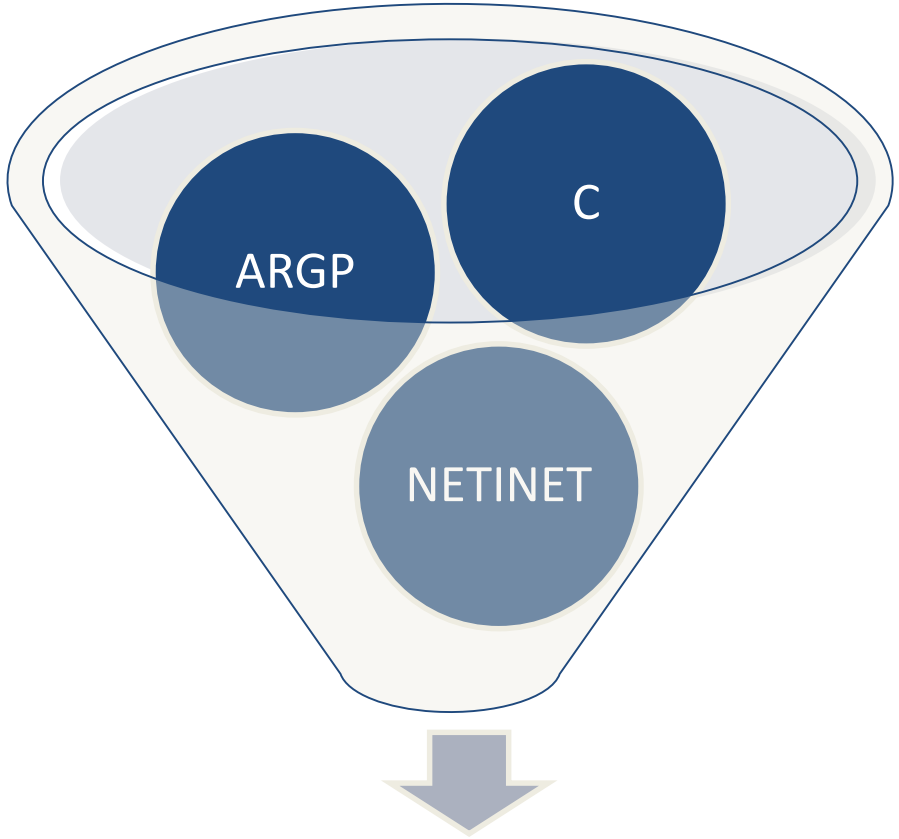
Xocoyotzin Carlos Zamora Parra

Agenda

- Introducción
- Alcance
- Funcionamiento
- Instalación
- Demostración
- Resultados
- Conclusiones

Introducción

Introducción

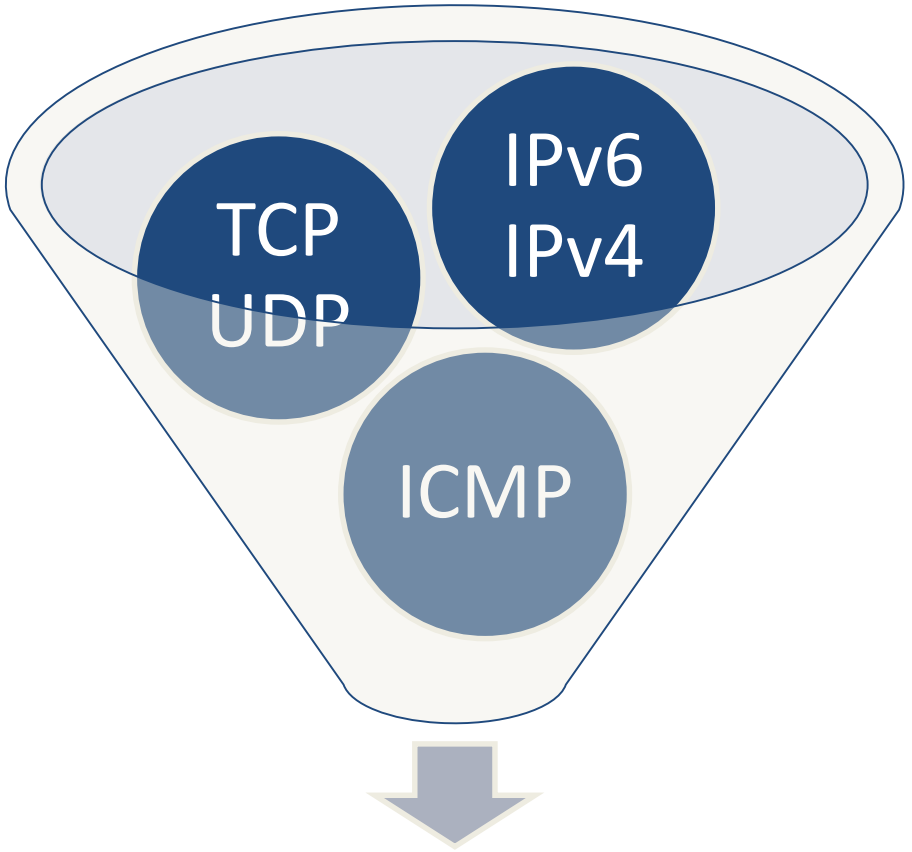


traffgen

Traffgen

- Elaborada para generar tráfico en IPv4 e IPv6
- Escrita en Lenguaje C
  - Mejor desempeño
  - Portabilidad del código
- Disponible para arquitecturas de 32 y 64 *bits*.
- Se requiere de un equipo con gcc

Traffgen



Traffgen

- Es posible realizar:
  - Pruebas de carga
  - Generar tráfico ICMP, TCP y UDP en IPv4 e IPv6

http://goo.gl/ZB1W50

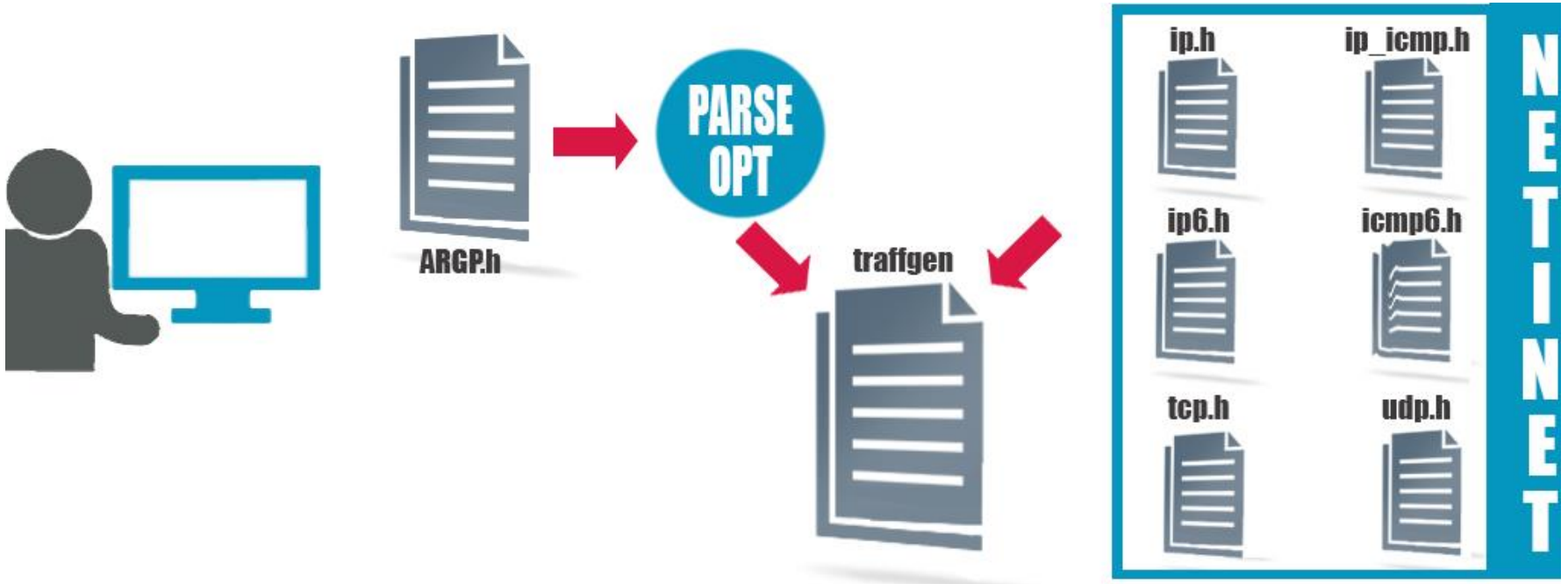
Alcance

Alcance

- Generación de paquetes en los protocolos:
  - Protocolo de Control de Transmisión (TCP)
  - Protocolo de Datagrama de Usuario (UDP)
  - Protocolo de Control de Mensajes de Internet (ICMP)
  - Protocolo de Internet versión 4 y 6 (IPv4 e IPv6)
- Cuenta con diferentes niveles de tiempo para el envío de tráfico

Funcionamiento

Diseño




```
IP 132.247.234.3.46256 > 132.247.234.7.5432: UDP, length 24
        0x0000:  4500 0034 a45d 0000 ff11 3961 84f7 ea03  E..4.]....9a....
        0x0010:  84f7 ea07 b4b0 1538 0020 35f7 4265 6361  .......8..5.Beca
        0x0020:  7269 6f73 4f63 7461 7661 4765 6e65 7261  riosOctavaGenera
        0x0030:  6369 6f6e                                cion
IP 132.247.234.3.46256 > 132.247.234.7.5432: UDP, length 24
        0x0000:  4500 0034 a45d 0000 ff11 3961 84f7 ea03  E..4.]....9a....
        0x0010:  84f7 ea07 b4b0 1538 0020 35f7 4265 6361  .......8..5.Beca
        0x0020:  7269 6f73 4f63 7461 7661 4765 6e65 7261  riosOctavaGenera
        0x0030:  6369 6f6e                                cion
```

Captura tcpdump

Funcionamiento

- Desde línea de comandos especificando:
  - Direcciones IP origen y/o destino (IPv4 e IPv6)
  - Puertos origen y/o destino
  - Banderas TCP
  - Tipos y códigos ICMP
  - Carga útil (*payload*)
  - Niveles de tiempo (normal, rápido y flujo)

Instalación

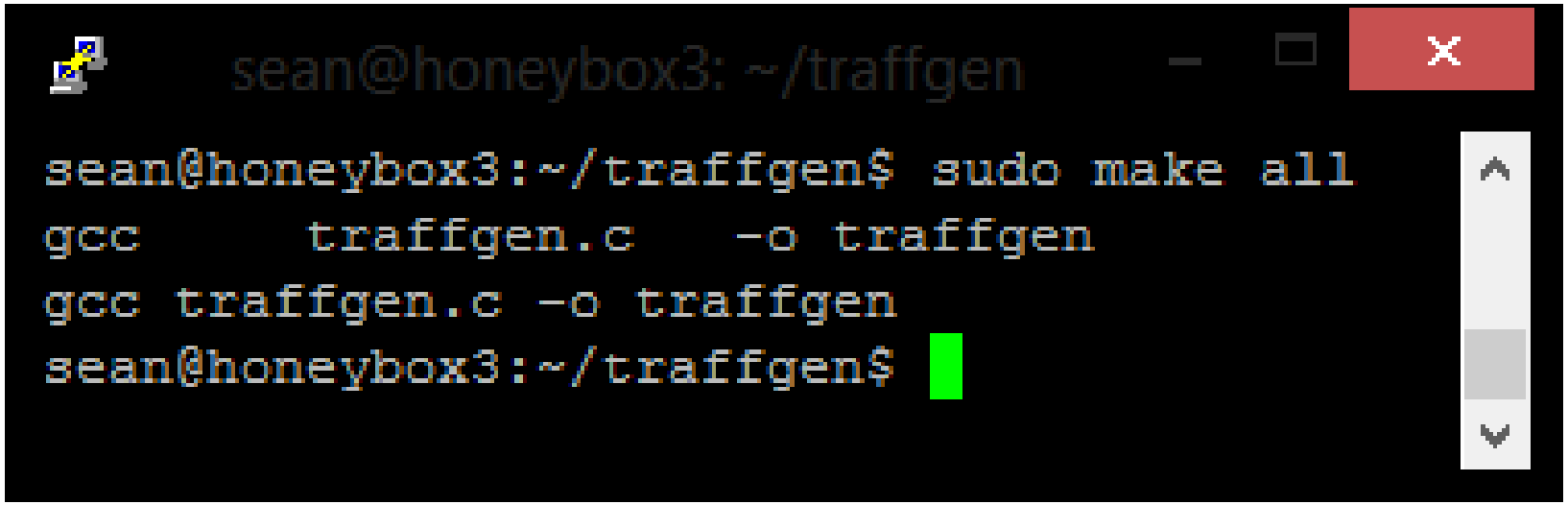
http://goo.gl/ICSDXI

Instalación

- Fácil descarga e instalación.
- La herramienta tiene un programa que permite compilar, instalar y desinstalar la herramienta en sistemas operativos de 32 y 64 *bits*.
- Incluye la documentación de la herramienta en formato *man*.

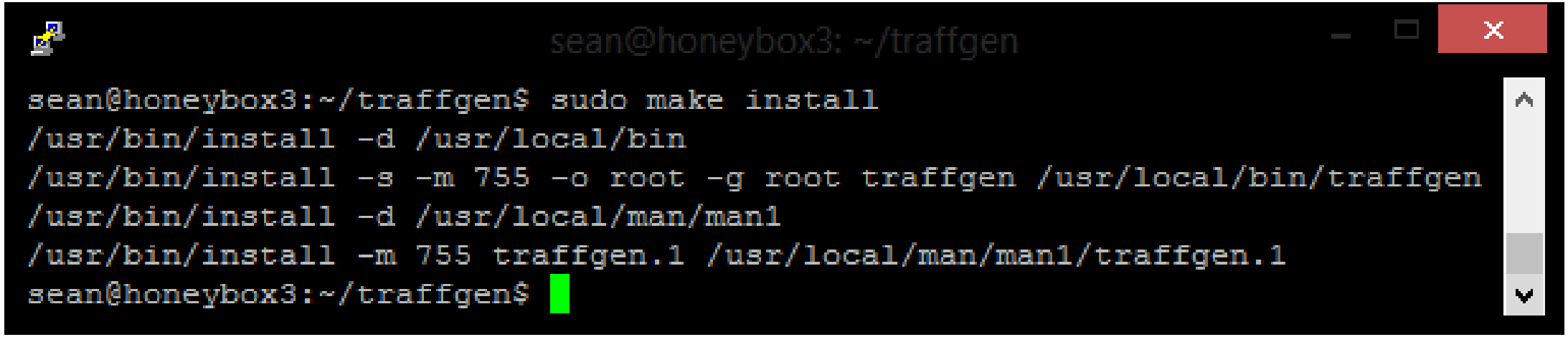
Compilar

- Compilar
  - *make all*



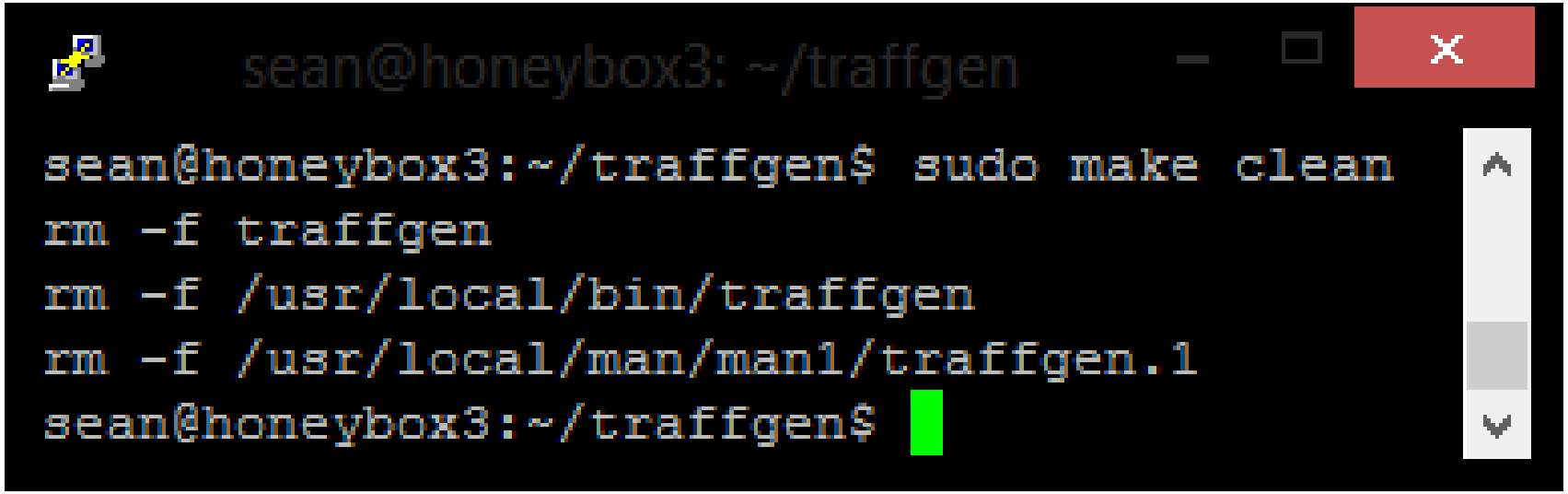
Instalar

- Instalar
  - *make install*



Desinstalar

- Desinstalar
  - *make clean*



Demostración

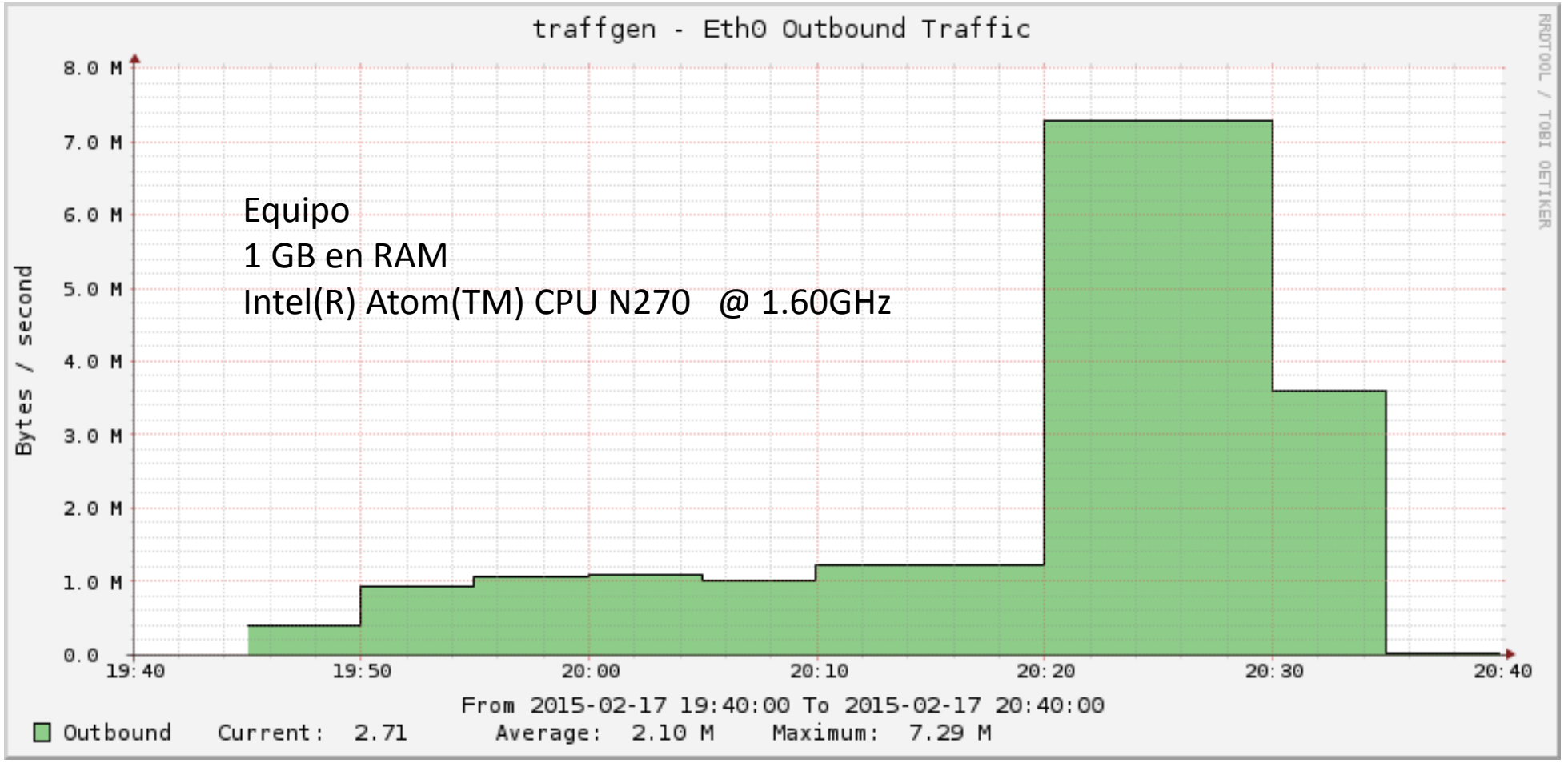
Demostración

http://goo.gl/gvdK00

Resultados

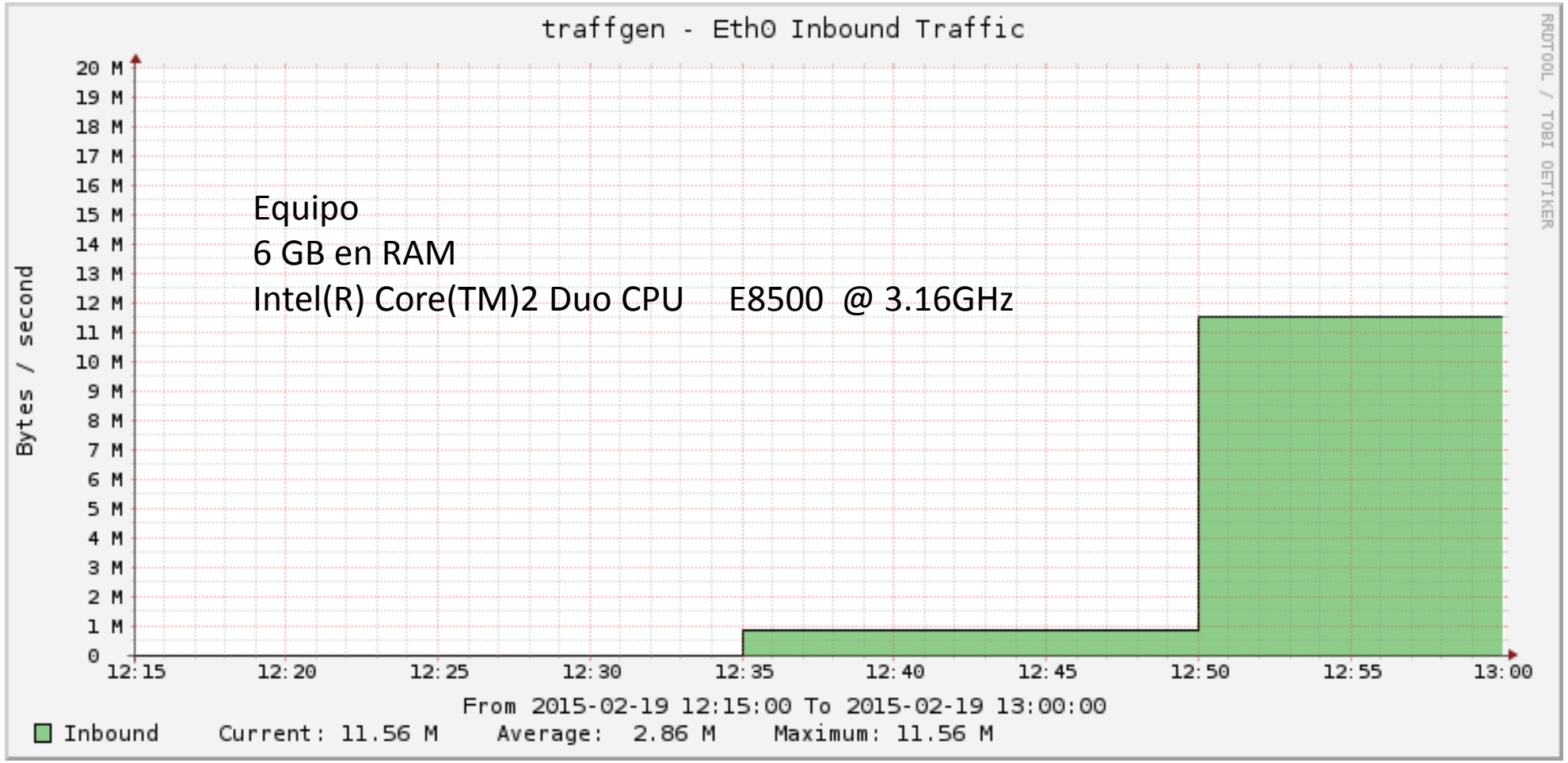
http://goo.gl/S83vLi

Resultados



Equipo
1 GB en RAM
Intel(R) Atom(TM) CPU N270 @ 1.60GHz

Resultados



Equipo
6 GB en RAM
Intel(R) Core(TM)2 Duo CPU E8500 @ 3.16GHz

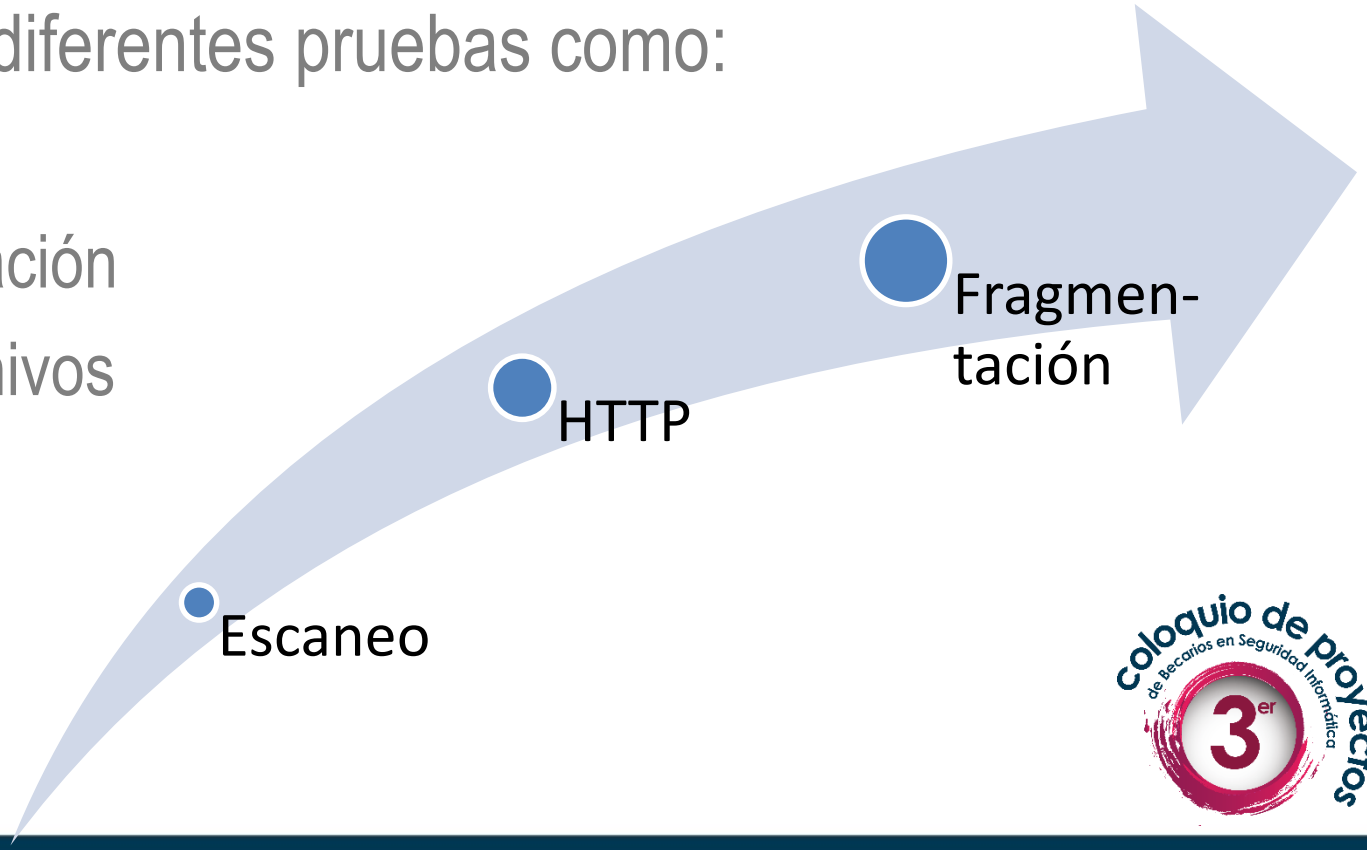
Resultados

- Es posible también realizar
  - *Escaneo a dispositivos de red*
  - *Peticiones legitimas*

  Pruebas de:
  - Evasión de IDS
  - Evasión de IPS
  - Evasión de *firewall*
- Perdida de paquetes en dispositivos de red
- Existen colisiones
- Interfaces de red
- Medio

Desarrollo futuro

- Agregar opciones para realizar diferentes pruebas como:
  - Escaneos
  - Protocolos de la capa de aplicación
  - Soporte de *payload* desde archivos
  - Lectura de respuestas
  - Tamaño de paquetes
  - Fragmentación



Conclusiones

Conclusiones

- Se logró el desarrollo una herramienta flexible que permite la creación de paquetes de forma especifica.
- Es posible realizar pruebas (carga, evasión y verificación) a equipos de seguridad
- La herramienta esta limitada a los recursos del equipo en donde se ejecute para generar tráfico
- Es posible generar grandes cantidades de tráfico en poco tiempo

Preguntas

http://goo.gl/XCqwG3

Sergio Anduin Tovar Balderas
Xocoyotzin Carlos Zamora Parra

Coordinación de Seguridad de la Información / UNAM-CERT

56628169

anduin.tovar@cert.unam.mx

xocoyotzin.zamora@cert.unam.mx