Universidad de Antioquia

Reporte 3

Metricas - Parte 1

Author:
Henry Arcila

Supervisors:
Prof. Natalia Gaviria
Prof. Danny Múnera

16 de octubre de 2018

Índice

Resumen

De a cuerdo al World internet usage and poblation statistics, aproximadamente un 54.4 % tienen acceso a internet [6]. Como el recurso por excelencia intercambiado a traves de internet es la información este debe ser protegido; sin embargo, dicha tarea es cada vez mas desafiante debido a la mayor facilidad, numero y sofisticación de los ataques actualmente existentes. Para hacer frente éstos se han creado diferentes sistemas de seguridad como firewalls, antivirus, IDS e IPS entre otros.

Un sistema de seguridad puede ser visto como una caja negra con unas entradas (trafico de red, logs, reportes de hardware, etc.), unas salidas (alarmas, reportes de red, logs) y un proceso cuya finalidad es actuar sobre las entradas, procesarlas y generar las salidas necesarias . Como punto de partida es necesario definir el sistema haciendo las restricciónes necesarias en cuanto a los mecanismos de ataque y defensa. Para el presente caso, el sistema de seguridad a tratar se restringirá a los sistemas de detección de intrusiones (IDS) y el ataque a explorar, será el ataque de denegación de servicios (DoS).

deficion de sistema de seguridad incompleta

1. Objetivos

1. Describir de manera consista el diagrama de bloques de un sistema de seguridad.
2. Hacer un estudio breve de entradas de trafico asociado con ataques de denegacion de servicio.
3. Hacer un inventario a partir de la literatura de algunas metricas del ataque.
4. Cosultar como obtener las metricas.

2. Introducción

En la figura 1 de muestra el diagrama de bloques de un sistema de seguridad simplificado que se divide en los siguientes componentes:

Puede que sea mejor modificar la figura (ver cuaderno)

1. **Preprocesamiento**: Componente que procesa los datos de entrada (datos de red sin procesar) para extraer sus principales caracteristicas con el objetivo de generar una representación equivalente pero mas reducida (datos o vectores caracteristicos, estadisticas) y apropiada para etapas de procesamiento posteriores.
2. **Alarma**: tal y como se muestra en la figura 1, este componente toma los datos caracteristicos y lanza alarmas de red (logs que reporta eventos, reportes de red, etc) con el fin de indicar a los administradores posibles problemas en la red. El papel de las alarmas no se limita meramente al de indicadores, tambien pueden ser empleadas como entradas adicionales a un componente de procesamiento posterior para posterior analisis.

3. **Procesamiento**: este componente lleva a cabo acciones de control (bloquear trafico, limitar ancho de banda, reconfigurar la red, aislar equipos infectados, lanzar indicadores de alarma, etc) con el fin de mitigar problemas en la red sin intervención humana.

posible renombramiento de este componente

Al momento de analizar y probar una propuesta de un sistema de seguridad, una de las limitaciones con las que se cuenta esta relacionada con la disponibilidad de datos de tráfico reales. Para tratar este problema, el presente documento explora diferentes alternativas (como data sets y generadores de tráfico) que, de acuerdo a la literatura pueden ofrecer una manera aceptable de imitar una fuente de tráfico real cuando se carece de esta. Posteriormente, se exploran metricas de analisis de tráfico tratando de hacer enfasis en las mas relevantes para los ataques de denegación de servicio. Finalmente, el documento culminará con una sección dedicada a las discuciones y conclusiones.

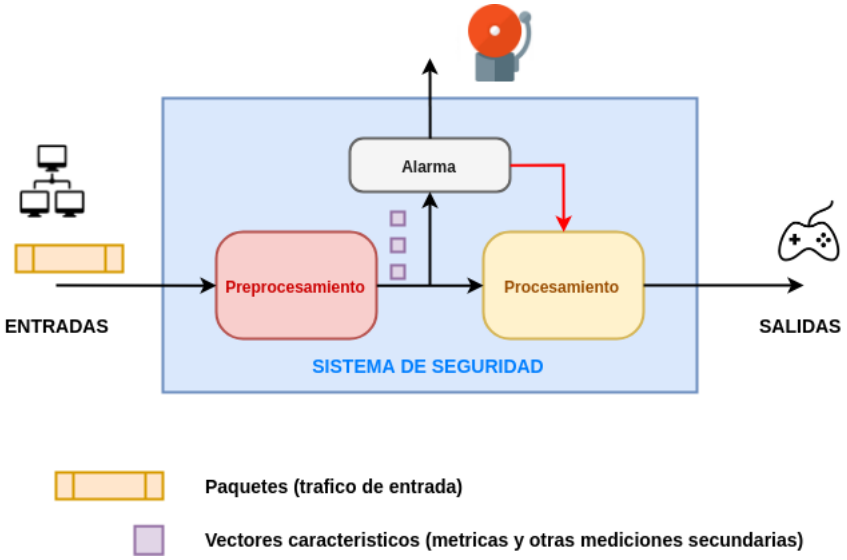

Figura 1: Sistema de seguridad simplificado

3. Entradas

De todos los tipos de entradas existentes (trafico de red, carga de memoria, logs, puertos abiertos, etc), solo unas cuantas son empleadas en un determinado sistema de seguridad. Las entradas utilizadas dependen del tipo de sistema implentado (antivirus, IDS, IPS, firewall, etc). Asi, por ejemplo, antivirus no empleará las mismas entradas que un IDS.

Teniendo en cuenta lo anterior, el primer paso es definir el tipo de sistema a implementar, que, para el caso es el IDS. Un IDS, es un sistema cuya finalidad es evaluar el

tráfico de red en busca de amenazas y lanzar alarmas en caso de detección de un patrón de tráfico anormal.

Una vez definido el sistema de seguridad, el siguiente paso es determinar de todas las entradas existentes cuales utilizar, siendo la entrada para el caso el **trafico de red**. Este se clasifica de la siguiente manera:

- **Trafico real**: En este caso el tráfico es generado por maquinas reales o virtuales conectados a la red.
- **Trafico sintético**: En este caso el tráfico es generado por una aplicación que simula el comportamiento del trafico generado por una maquina real.

Finalmente, como un mismo tipo de entrada puede estar asociada a muchos tipos de ataques, es necesario definir con claridad el ataque en el que se hará énfasis, siendo para el caso, el ataque de Denegación de servicio (DoS) el elegido.

En conclusión y resumiendo lo anterior, la defición de las entradas a emplear en un sistema de seguridad se reduce a los siguientes tres pasos básicos:

1. Definir el sistema de seguridad a emplear.
2. Definir de acuerdo al paso uno, las entradas que el sistema empleará.
3. Definir el ataque que se analizará.

Con estos tres items definidos representados por la triada [**herramienta, tipo de entrada, tipo de ataque**] que para el caso es [**IDS, tráfico de datos, DoS**], se tiene la información suficiente para empezar a definir de manera más específica la fuente que se empleará como entrada en el sistema.

De acuerdo a algunas fuentes de literatura consultadas [11, 16] la generación de tráfico de entrada asociado con ataques de denegación de servicio simples o distribuidos (DoS o DDoS) puede realizarse empleando diferentes tipos de fuentes, las cuales se pueden agrupar en los siguientes tres tipos:

- Datasets
- Herramientas de geneneracion de ataques de denegación de servicio.
- Generadores de tráfico.

En las siguientes secciones se explicará con un poco mas de detalle cada una de estas.

3.1. Fuentes de generación de ataques de degación de servicio

En la figura 2, se muestran las posibles fuentes que pueden ser seleccionadas para la generacion de tráfico de red previamente mencionadas. Tal y como se muestra en dicha fígura, inicialmente se define el tipo de fuente que se va a emplear en el experimento para la generación del tráfico de entrada que se aplicará al sistema de seguridad ya definido.

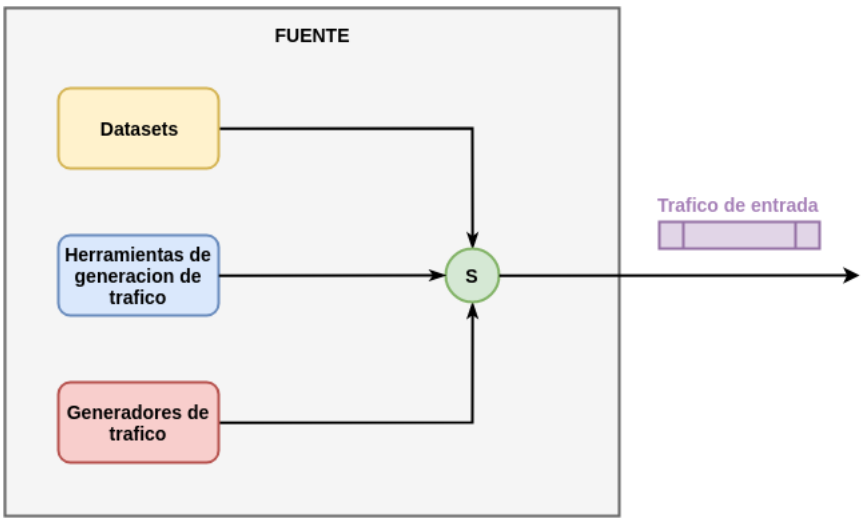

Figura 2: Sistema de seguridad simplificado

Una vez hecho lo anterior, se aplica este tráfico de entrada a dicho sistema con el objetivo de probarlo, evaluarlo y dado el caso (si se emplean tecnicas de machine learning) entrenarlo.

A continuación se aborda con mas detalle cada una de las fuentes mostradas en la figura 2.

3.1.1. Datasets

Un dataset se define como una coleccion de datos (items) distretos y relacionados con diferentes significados según el escenario y que fueron utilizados para alguna clase de experimento o analisis [15].

En la red existe diferentes fuentes de las cuales se pueden obtener datasets de manera libre [9, 7, 1]. En este caso, como la disciplina de interes se centra en datos asociados a tráfico de red, la busqueda y elección de datasets que cumplan con este requisito es aun una tarea desafiante en gran parte, debido a la falta de un sitio centralizado y especializado donde sea facil obtenter este tipo de datos.

Para tratar esta dificultad, Cinthya Grajeda et al [15], presentan un overview de datasets relevantes en analisis digital forense. Asi mismo, recopilan toda esta informacion en un repositorio centralizado [2] para facilitar la busqueda, actualización y uso por parte de la comunidad, de datasets relacionados con escenarios de seguridad. De los datasets allí presentados, los únicos que representan algún interés para nuestro caso, son aquellos relacionados con trafico de red. En la tabla 1 se muestran algunos datasets de interes que pueden ser empleados como fuentes de datos para la reproducción de experimentos relacionados con los ataques de denegación de servicios.

Las pricipales caracteristicas mostradas en la tabla 1 para cada dataset, estan rela-

cionadas con el tipo de datos que los componen (archivos pcap, logs, etc) que son de vital importancia por que determinan los parámetros (variables: IP origen, IP destino, etc) asociados a cada dato, el tamaño del dataset, la fecha de disponibilidad y si es Labeled (L) o Unlabeled (U).

El uso de datasets facilita el diseño de pruebas experimentales pues, permite la aplicación de una misma entrada (dataset como tal) ante diferentes condiciones y configuracióones del sistema de seguridad estudiado. Ademas, los datasets son ampliamente usados en areas de investigacion con machine learning (ML) y sistemas de intrucion (IDS) [21] lo cual hace que valga la pena que estos sean empleados como una fuente de entrada al definir un experimento.

Como se puede enfatizar que este es el ultimo parrafo, se puede deja asi o es necesario hacer este enfasis

Dataset	***Tipo de datos***	***Tamaño***	***Fecha***	***Labeled or Unlabeled***
Digital Corpora	archivos pcap	N/A	2008 - 2009	U
DFRWS 2009 Challenge	archivos pcap	N/A	2009	U
University of New Haven cFREG	archivos pcap	876 KB	2015	U
The CFReDS Project - NIST	trace logs	3.8 MB	2005	?
CAIDA	68 network related datasets	N/A	1998 - 2017	?
University of Oregon Route Views Project	Cisco, Zebra BGP RIBs	N/A	1997 - 2017	?
DARPA	(Raw dataset) TCP/IP Dump files	9.67 GB	1999	L
KDD99	Caracteristicas extraidas y preprocesadas del dataset DARPA usando machine learning	5209460	1999	L
NLS-KSDD	Version reducida del dataset KDD99 (se remueven datos redundantes)	N/A	?	L
CIDDS-001	flujos de red + labels	N/A	?	L

Cuadro 1: Principales caracteristicas de algunos datasets para hacer pruebas con ataques de denegacion de sevicio

3.1.2. Herramientas para lanzar ataques de denegacion de servicio

Existen varios tipos de ataques de denegación de servicio los cuales han sido ampliamente estudiados y clasificados bajo diferentes taxonomias [14, 13]. Con el fin de simplificar la clasificación de estos ataques; para el presente caso, la clasificación se hara en base a tres tipos: los ataques de denegacion de servicio de la capa de aplicación, los ataques de denegación de servicio de la capa de protocolo y los ataques de denegación de servicio basados en volumen [3].

Para llevar a cabo los ataques de denegación de servicio, existe un gran numero de herramientas especializadas [20, 11] las cuales, mediante diferentes técnicas (flooding, smurf, fraggle, ping de la muerte, etc.) y empleando diferentes protocolos (HTTP, UDP, TCP, ICMP, etc) pueden lanzar ataques para hacer un sitio inaccesible. La tabla 2 muestra algunas de estas herramientas:

Herramienta	*Tipo de trafico*	*Método de ataque*	*Tipo de ataque DoS/DDoS*	*Impacto*
GoldenEye	HTTP	GET Flood, POST Flood, Random Flood	Aplicacion	Recurso
LOIC (Low Orbit Ion Cannon)	HTTP, TCP, UDP	GET Flood, TCP Flood, UDP Flood	Aplicacion	Recurso
R.U.DY (R U Dead Yet?)	HTTP	HTTP POST	Aplicacion	Recurso
Slowloris	HTTP	HTTP GET	Aplicacion	Recurso
Dirt Jumper	HTTP	POST Flood, SYN Flood, HTTP Flood	Aplicacion	Recurso
Tor's Hammer	HTTP	slow POST	Aplicacion	Recurso
Nuclear DDoSer	HTTP	Slowloris, Slow POST	Aplicacion	Recurso
Railgun	HTTP	Slowloris o Slow POST	Aplicacion	Recurso
High Orbit Ion Cannon (HOIC)	HTTP	POST Flood, GET Flood	Aplicacion	Recurso
HULK (HTTP Unbearable Load King)	HTTP	TCP SYN flood, HTTP GET flood	Aplicacion	Recurso
TFN (Tribe Flood Network)	ICMP, TCP, UDP	ICMP Flood, SYN Flood, UDP Flood and Smurf attack	Por volumen	Ancho de banda
trin00 (o trino)	UDP, TCP	SYN Flood, UDP flood	Por volumen	Ancho de banda
stacheldraht	ICMP, TCP, UDP	ICMP Flood, SYN Flood, UDP Flood and Smurf attack	Por volumen	Ancho de banda
Hping3	TCP, UDP, ICMP, RAW-IP	?	Por volumen	Ancho de banda
Ddosim	HTTP, TCP, SMTP	Create full TCP connections, when the connection is stablised send HTTP GET request	Aplicación	Recurso
Pyloris	HTTP	?	Aplicación	Recurso
Davoset	HTTP	Abuse of Functionality	Aplicación	Recurso
Trinity	TCP, UDP	Flood attacks	Aplicación	Ancho de banda, Recurso
XOIC	TCP, UDP, HTTP, ICMP	?	Aplicación	Ancho de banda, Recurso
Owasp Http Dos Post	HTTP	HTTP POST attacks, HTTP GET attacks	Aplicación	Recurso
THC-SSL-DoS	SSL	Malformed SSL request	Presentación (Protocol ?)	Recurso
Brobot	TCP, UDP	HTTP POST attacks, HTTP GET attacks	Por volumen	Ancho de banda

Cuadro 2: Principales caracteristicas de algunos datasets para hacer pruebas con ataques de denegacion de sevicio

En la tabla anterior, es importante hacer énfasis en el método de ataque y el tipo de tráfico generado por la herramienta pues estos son criterios de gran importancia para la selección de la herramienta. Finalmente, una de las principales caracteristicas de estas herramientas radica en si facilidad se uso, facilidad de obtención y la gran cantidad de información disponible en la web sobre su modo de empleo lo cual hace que cualquier persona sin la cantidad sufiente de conocimientos tecnicos necesarios sea capaz de llevar a cabo un ataque de esta índole.

3.1.3. Generadores de trafico

Los generadores de trafico son herramientas usadas para inyectar en la red trafico (aleatorio o personalizado) de manera controlada. Dentro de los principales usos de estos se encuentran: la simulación de tráfico (legitimo o de ataque) de red, evaluación de desempeño, evaluación de mecanismos de defensa (firewals, IDS e IPS) y automatización de testing de redes mediante scripting. Los generadores pueden ser tanto de hardware como de software siendo este último, el caso en el cual se hará énfasis. La siguiente tabla muestra algunos de los generadores de tráfico disponibles en la red [11] haciendo enfasis en el tipo de tráfico generado y la capa OSI con mayor relación:

Generador	***Tipo de trafico***	***Capa***
Bit-twist	TCP, UDP, IP, ARP, ICMP.	Enlace, red, transporte
D-ITG	IP, TCP, UDP, ICMP, DCCP, SCTP.	Enlace, red, transporte
Karat	IP, PPoE, TCP, UDP, ICMP, VRRP, IGMP, ARP, DHCP, OAM, VLAN, MPLS, Spanning tree.	Enlace, red, transporte, aplicación
Ostinato	Ethernet, SNAP, VLAN, ARP, IP, IP Tunnelling TCP, UDP, ICMP, IGMP, MLD, HTTP, SIP, RTSP, NNTP, etc.	Enlace, red, transporte, aplicación
Scapy	TCP, IP, Ethernet, ICMP, ARP, DHCP, ICMP, SNMP, UDP, etc.	Enlace, red, transporte, aplicación
packeth	Ethernet, ARP, IP, UDP, TCP, ICMP, IGMP, RTP, etc.	Enlace, red, transporte, aplicación
curl-loader	HTTP, HTTP, FTP, HTTPS.	Aplicación
iperf	TCP, UDP.	Transporte
Netperf	TCP, SCTP, DLPI, UDP, IP	Transporte
HTTPperf	HTTP, SSL	Aplicación
UDP Generator	UDP	Transporte
ipgen	IP.	Red
pacgen	TCP, UDP, Ethernet, IP	Transporte, enlace, red
mgen	TCP, UDP	Transporte

Cuadro 3: Generadores de tráfico

4. Analisis de trafico

Segun Marcus Ranum un sistema de analisis forense de red (NFA - Network forenstics Analysis) es aquel concebido para la captura, almacenamiento y analisis de eventos de red para descubir la fuente de los ataques de seguridad u otros incidentes [10]. Un sistema NFA es soportado mediante un conjunto de herramientas las cuales permiten el procesamiento de unos datos para obtener unas métricas que ofrezcan la evidencia necesaria para conocer el ataque realizado. En esta sección se hará una revisión breve de herramientas y métricas importantes.

4.1. Herramientas para el análisis de trafico

Estas herramientas permiten la captura, almacenamiento y visualización del trafico de red para facilitar el analisis posterior. En la web se encuentran disponibles herramientas tanto libres como propietarias [4, 17]. La tabla 4 muestra alguna de dichas herramientas haciendo enfasis en las tareas basicas sobre el trafico que pueden ser realizadas por estas:

Herramienta	*Caracteristicas básicas*
Wireshark	Analisis de protocolo (completar)
tcpdump	Analiza protocolos por linea de comandos, permite obtener tráfico desde una interfaz de red o desde un archivo previamente creado, permite mostrar los paquetes capturados en pantalla o almacenarlos en un archivo, soporta filtros.
tcprelay	Permite usar tráfico previamente capturado en formato pcap para testear una amplia variedad de dispositivos de red, permite la clasificación de trafico como de cliente o servidor, puede editar archivos de trafico pcap (modificando cabeceras de las capas L2, L3 y L4), incluye varias herramientas (tcpprep, tcprewrite, tcpreplay, tcpliveplay, tcpliveplay, tcpreplay-edit, tcpbridge, tcpcapinfo)
tshark	Versión orientada a terminal de Wireshark por lo que soporta las mismas opciones que dicha herramienta.
Networkminer	Permite analisis de trafico de red tanto de manera activa (capturando trafico directamente de la red) como pasiva (leyendolo de algun archivo de trafico), permite deteccion de sistemas operativos, sesiones, hostnames, puertos abiertos, etc. sin necesidad de poner trafico en la red, desplique de información relacionada de manera amigable.
Ngrep	Analizador de tráfico con capacidad de aplicar expresiones regulares al payload de los paquetes analizados, trabaja con varios tipos de protocolos como IPv4/6, TCP, UDP, ICMPv4/6, etc, permite analisis de trafico de red de manera activa y pasiva.
Snort	Pese a ser un IDS tiene la capacidad de funcionar como snifer permitiendo realizar análisis de trafico, soporta diferentes archivos de red (pcap por ejemplo), permite lectura de tráfico de manera pasiva y activa, permite obtener estadisticas del tráfico.
Driftnet	snifer enfocado en la obtencion de imagenes dentro del trafico de red, permite ademas la extracción de audio MPEG de la red para escucharlo.
Xplico	Permite el analisis de trafico de red de manera online y ofline, amigable, multiprotocolo (HTTP, SIP, IMAP, POP, SMTP, TCP, UDP, IP,...), facilita la obtención y visualización de estadisticas e información relevante relacionada con el tráfico analizado como imagenes, URLs, etc.
Fenris	
Flow-Tools	
tcptrack	
tcpwrite	Edición de archivos de trafico **pcap** que permite reescribir headers TCP/IP y de capa 2, asi mismo permite generar trafico mediante el reuso de paquetes **pcap** ya disponibles.
tcpreplay	Permite el reuso de paquetes de trafico previamente capturados a velocidades arbitrarias en la red
nmap	Herramienta para escaneo de puertos y exploración de redes
tcptrack	Usada para sniffing y despliegue de información (IPs fuente y destino, estado de la conexion, idle time, Puertos fuente y destino y uso del ancho de banda en la conexion entre otros) de las conexiones de red vistas en la interfaz de red.

4.2. Metricas

El término métricas describe un amplio rango de herramientas y técnicas empleadas para evaluar datos. Los datos evaluados se emplean como medidas que se comparan con uno o más puntos de referencia para producir un resultado que facilite la toma de decisiones. No todas las métricas son buenas, por ende, elegir buenas métricas es indispensable para el análisis de un fenómeno o sistema; desde el punto de vista más básico una buena métrica es aquella que responde sin ambigüedad alguna a la pregunta del porqué se está usando [5].

Existe un gran número de métricas que permiten medir el desempeño de una una red (por ejemplo capacidad y utilización del canal, retardo y jitter, pérdidas de paquetes y errores entre otros) y sus nodos (disponibilidad, memoria, utilización de la CPU, memoria disponible, etc) [8]. También, existe una relación entre el tipo de ataque y el comportamiento de la red, pues, una red cuando está bajo ataque se comporta de manera diferente que cuando no lo está. Por lo tanto, es necesaria la selección adecuada de las características a monitorear para la detección de diferentes tipos de ataques. A continuación, se muestra una tabla tomada de [12] donde se muestra la relación entre

algunas de las diferentes características monitoreadas de la red y los ataques con los cuales estas se relacionan:

Características	***Tipos de ataques***
Packet rate	Flooding DDoS, flash crowds
Percentage of ICMP packet	icmp flooding, scan attack, worm
Percentage of TCP packet	tcp flooding, tcp worm
Percentage of UDP packet	udp flooding, udp worm
Percentage of large packet	Self-carried worm
Percentage of short packet	Scan attack
Percentage of SYN/ACK/RST	DDoS
Distribution of IP address	DDoS, scan
Distribution of port	Scan, worm
Interval of arriving packet	DDoS
Duration of each flow/session	SYN flooding
Packets/bytes per flow	Flooding DDoS, flash crowds
Percentage of single flow	DDoS
Growth of new flow	Scan attack
Special protocol of application layer	Worm, botnet

Cabe aclarar que la relación expuesta en esta tabla no está restringida solo a los ataques de denegación de servicio; sin embargo, las características mostradas de una u otra manera inciden en mayor o menor medida en estos. Para esto se pueden emplear técnicas estadísticas [5] como: la media, la mediana, la agregación (sumatoria, máximo y mínimo, desviación estándar, varianza) y series de tiempo entre otras sobre los datos, con el fin de obtener todas aquellas relaciones ocultas que mediante el análisis de los datos en bruto no se pueden encontrar.

Finalmente, mas alla de las metricas elegidas y del ataque al que se asocian; todo se reduce en principio a tareas de procesamiento sobre datos en bruto (trafico de red haciendo enfasis en uno o varios campos de los paquetes de datos) siendo el metodo y transfomación sobre estos lo que varia tal y como se muestra en algunos articulos como [19, 18]

5. Experimento

Seccion dedicada a describir pasos importantes sobre el experimento (ojo con los enlaces comentados):

http://www.iv2-technologies.com/HowToTestAnIPS.pdf

En el fondo esto seria lo ideal a montar (enlace comentado)

6. Conclusiones

El código ejemplo se encuentra disponible en: `https://github.com/tigarto`

Referencias

[1] Awesome public datasets. (Date last accessed 15-September-2018).

[2] Datasets for cyber forensics. (Date last accessed 15-September-2018).

[3] Dos website in kali linux using goldeneye. (Date last accessed 2-October-2018).

[4] Forensics wiki. (Date last accessed 16-October-2018).

[5] How can you build and leverage snort ids metrics to reduce risk? (Date last accessed 11-October-2018).

[6] Internet world stats. (Date last accessed 21-August-2018).

[7] Kaggle. (Date last accessed 15-September-2018).

[8] Network startup resource center. (Date last accessed 11-October-2018).

[9] Uci machine learning repository. (Date last accessed 15-September-2018).

[10] Website marcus ranum. (Date last accessed 16-October-2018).

[11] Sunny Behal and Krishan Saluja. Characterization and comparison of ddos attack tools and traffic generators -a review. 19:383–393, 04 2017.

[12] Xiao-Fan Chen and Shun-Zheng Yu. Cipa: A collaborative intrusion prevention architecture for programmable network and sdn. *Computers & Security*, 58:1 – 19, 2016.

[13] M. De Donno, A. Giaretta, N. Dragoni, and A. Spognardi. A taxonomy of distributed denial of service attacks. In *2017 International Conference on Information Society (i-Society)*, pages 100–107, July 2017.

[14] Christos Douligeris and Aikaterini Mitrokotsa. Ddos attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks*, 44(5):643 – 666, 2004.

[15] Cinthya Grajeda, Frank Breitinger, and Ibrahim Baggili. Availability of datasets for digital forensics – and what is missing. *Digital Investigation*, 22:S94 – S105, 2017.

[16] N. Hoque, Monowar H. Bhuyan, R.C. Baishya, D.K. Bhattacharyya, and J.K. Kalita. Network attacks: Taxonomy, tools and systems. *Journal of Network and Computer Applications*, 40:307 – 324, 2014.

[17] R. Hunt and S. Zeadally. Network forensics: An analysis of techniques, tools, and trends. *Computer*, 45(12):36–43, Dec 2012.

[18] P. Kamboj, M. C. Trivedi, V. K. Yadav, and V. K. Singh. Detection techniques of ddos attacks: A survey. In *2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON)*, pages 675–679, Oct 2017.

[19] Parneet Kaur, Manish Kumar, and Abhinav Bhandari. A review of detection approaches for distributed denial of service attacks. *Systems Science & Control Engineering*, 5(1):301–320, 2017.

[20] Gulshan Kumar. Denial of service attacks – an updated perspective. *Systems Science & Control Engineering*, 4(1):285–294, 2016.

[21] Atilla Özgür and Hamit Erdem. A review of kdd99 dataset usage in intrusion detection and machine learning between 2010 and 2015. *PeerJ Preprints*, 4:e1954v1, April 2016.