Recomendaciones para mejorar escenarios de ataques distribuídos de negación de servicio (DDoS)

Autor: CERT.br
Versión: 1.0-ES — 21/04/2016 – Traducción: Ernesto Pérez CSIRT CEDIA

1. Introducción

La negación de servicio, o DoS (*Denial of Service*), es una técnica mediante la cual un atacante utiliza equipos conectados a la red para interrumpir la operación de un servicio, un computador o una red conectada a Internet. Cuando se utiliza de forma coordinada y distribuída, o sea, cuando un conjunto de equipos es utilizado en el ataque, recibe el nombre de **Ataque Distribuido de Negación de Servicio** (DDoS - *Distributed Denial of Service*).

Un ataque de DDoS no tiene el objetivo directo de invadir o recolectar información sino de agotar los recursos y causar fallas en la disponibilidad del objetivo. Los usuarios de estos recursos son directamente afectados y quedan imposibilitados de acceder o realizar las operaciones deseadas ya que el destino del ataque no puede diferenciar los accesos legítimos de los maliciosos y queda sobrecargado al intentar responder todas las peticiones recibidas.

Los ataques de DDoS han sido uno de los grandes problemas enfrentados por las organizaciones y usuarios de Internet. A pesar de no ser posible impedir que estos ocurran, con una planificación adecuada es posible hacerles menos eficaces y dañinos.

Este documento busca reunir buenas prácticas de seguridad que deben ser seguidas por los diversos sectores que forman la Internet para intentar reducir los ataques de DDoS y minimizar los problemas causados por ellos.

Las soluciones presentadas son alternativas a ser consideradas para el tratamiento de los ataques y no representan una lista exhaustiva de posibilidades, ya que nuevas soluciones pueden surgir. No forman parte de este documento un detalle técnico de todas las soluciones aquí mencionadas sino que pretendemos que estas sugerencias puedan servir de referencia al lector.

2. Blancos principales y motivaciones de los ataques de DDoS

Cualquier red, equipamiento o sistema accesible desde Internet puede ser blanco de un ataque de DDoS y, de la misma forma, también puede generar un ataque, en caso de que esté infectado, mal configurado o comprometido. Han sido observados blancos de diversos sectores como proveedores de Internet, sitios de juegos, noticias, bancos, comercio electrónico, gobierno, industria y partidos políticos, entre otros.

El blanco de los ataques puede enfrentar problemas como la imposibilidad de acceder a servicios y recursos legítimos, daños a su imagen, pérdidas financieras, pérdida de credibilidad y dificultad para continuar sus negocios. Los ataques también acostumbran a generar efectos colaterales como el exceso de logs, problemas con respaldos automatizados, aumento de los costos por incremento en el consumo de ancho de banda y, además, mayor consumo de banda y, además, reflejarse hacia otras redes del

mismo proveedor de Internet, de almacenamiento o de la nube.

Así como son variados los blancos, las motivaciones de los atacantes también son de las más variadas y, muchas veces, difíciles de ser determinadas. De forma general estas pueden ser divididas en los siguientes grupos:

- Beneficio económico o financiero: son ataques dirigidos principalmente a empresas y realizados, por ejemplo, para causar perjuicios a la competencia (competencia desleal), intentar exigir dinero y como forma de demostrar "poder de fuego" a posibles clientes y blancos;
- Represalia o venganza: son ataques realizados como respuesta a hechos que los atacantes juzgan han sido injustos o que, de alguna forma, les tienen descontentos;
- Creencias ideológicas o políticas: son ataques realizados por diferencias políticas o religiosas. Acostumbran estar asociados a la práctica del hacktivismo;
- Distractor para otros ataques: son ataques realizados con el objetivo de distraer a los equipos de red y seguridad de las empresas atacadas ya que mientras están ocupados en mitigar este ataque, los atacantes aprovechan para efectuar otras actividades maliciosas como por ejemplo robo de datos o invadir los sistemas del blanco;
- Desafío intelectual: en su mayoría los atacantes de esta categoría son principiantes y realizan los ataques para experimentar y aprender cómo realizar diversos ataques de DDoS;
- Otros: motivaciones individuales y genéricas como la tentativa de la aplazar la entrega de documentos y trabajos.

3. Como se realizan los ataques de DDoS

Debido a la gran cantidad de herramientas disponibles en la Internet, muchas de ellas gratuitas o a precios cada vez más accesibles, es posible que prácticamente cualquier persona pueda realizar un ataque DDoS. De forma general los ataques ocurren de las siguientes formas:

- A través de *botnets* formadas por equipos infectados, mal-configurados o invadidos, como computadoras personales, servidores Web, dispositivos móviles, cámaras, CPEs, ruteadores Wi-Fi, modems de banda ancha, etc. El controlador de una *botnet* envia comandos a estos equipos para que ataquen a un blanco específico;
- A través del escaneo de servicios de Internet, como DNS, NTP, SSDP y CHARGEN, que permiten altas tasas de amplificación de paquetes. El atacante falsifica la dirección IP de la víctima lo que le hace recibir una alta cantidad de paquetes, que le consumen una cantidad considerable de ancho de banda. Diversos equipos como CPEs, acostumbran a tener estos servicios habilitados y pueden ser abusados;
- Por la acción voluntaria de personas que, por intermedio del acceso a sitios específicos o mediante la instalación de herramientas como HOIC, LOIC, RUDY o Slowloris, ofrecen sus computadoras para que participen en estos ataques, los cuales son coordinados desde redes sociales, canales de IRC, entre otros medios;
- Por medio de aplicaciones Web específicas llamadas *booters*, IP *stressers* o *DDoSers*, cuyos servicios muchas veces son ofertados en Internet como herramientas legítimas de prueba de

carga pero que, en verdad, son usadas como una interfaz para ataques que son realizados via *botnets* o máquinas preparadas para este propósito;
- a través de la exploración de vulnerabilidades presentes en servicios y aplicaciones, generalmente causadas por errores de programación y fallas de configuración.

Existen también casos no intencionales de negación de servicio que ocurren por fallas en el dimensionamiento de aplicaciones y problemas de escalabilidad de recursos, entre otros motivos. Estos casos no deben ser confundidos con ataques, pues el propio uso normal de los sistemas puede llevar a la sobrecarga y consecuente lentitud o in-disponibilidad del servicio en cuestión.

4. Tipos de ataques de DDoS

No existe un único tipo de ataque de DDoS e, infelizmente, no hay una solución única para tratar este problema. Por ello, conocer y entender los diferentes tipos de ataques es esencial para que las organizaciones puedan planear adecuadamente las acciones a ser tomadas.

Básicamente existen tres tipos de ataques DDoS: ataques a la capa de aplicación, ataques de agotamiento de recursos de hardware y los ataques volumétricos. Estos pueden ser realizados de forma aislada o en conjunto. Un atacante puede, por ejemplo, realizar un ataque a la capa de aplicación solamente o combinarlo con un ataque volumétrico. Los ataques combinados acostumbran a tener más impacto porque requieren el uso conjunto de diferentes formas de preparación, detección, análisis y mitigación.

4.1 Ataques a la capa de aplicación

Los ataques a la capa de aplicación acostumbran a ser más difíciles de ser detectados pues pueden ser confundidos con problemas de implementación de la aplicación y n o necesitan de muchos equipos ni de mucho tráfico para realizarse.

Ataques de este tipo buscan explotar características específicas de una aplicación o servicio (capa 7), como forma de:

- saturar los recursos, en caso de que un servicio no haya sido bien dimensionado o configurado;
- exceder el número máximo de peticiones que un servidor Web o sistema de gestión de bases de datos (SGBD) puede manejar;
- realizar consultas complejas a los sistemas que demanden mucho procesamiento.

Ejemplos: HTTP GET, HTTP POST, VoIP (SIP INVITE Flood) y Slow Read DDoS.

4.2 Ataques de agotamiento de recursos de *hardware*

Los ataques de agotamiento de recursos de *hardware* buscan consumir la capacidad de los equipos y agotar sus recursos. Por ejemplo:

- En ruteadores: buscan consumir recursos como CPU y memoria, y la capacidad de enrutamiento de paquetes por segundo (pps);
- En *firewalls* e IPSs: buscan agotar la capacidad de la table de estado de las conexiones,

impidiendo que nuevas conexiones sean establecidas.

Ejemplos: fragmentación y TCP Syn Flood.

4.3 Ataques volumétricos

Los ataques volumétricos buscan agotar el ancho de banda disponible enviando al blanco un enorme volumen de tráfico. Para conseguir generar este volumen los atacantes utilizan medios como *botnets*, equipos con bastante ancho de banda, equipos con poco ancho de banda pero en gran cantidad o, incluso, aprovechan características específicas de servicios UDP que permiten la amplificación del tráfico.

El DRDoS (*Distributed Reflective Denial of Service*) es un ejemplo de ataque volumétrico que:

- usa características de los protocolos de Internet que permiten altas tasas de amplificación de paquetes y;
- utiliza direcciones IP forjadas (spoofeadas) para que los paquetes amplificados sean direccionados hacia el blanco del ataque.

Muchos de los protocolos usados en los ataques de DRDoS hacen parte de la infraestructura pública de Internet. En algunos equipamientos como CPEs, estos son instalados por defecto y usados por atacantes en muchas ocasiones sin que los verdaderos dueños sepan que están proveyendo estos servicios.

A continuación listamos algunos protocolos utilizados y su factor de amplificación (US-CERT Alert TA14-017A):

- DNS (53/UDP): factor de amplificación de 28 até 54 veces;
- NTP (123/UDP): factor de amplificación de 556.9 veces;
- SNMPv2 (161/UDP): factor de amplificación de 6.3 veces;
- NetBIOS (137–139/UDP): factor de amplificación de 3.8 veces;
- SSDP (1900/UDP): factor de amplificación de 30.8 veces;
- CHARGEN (19/UDP): factor de amplificación de 358.8 veces.

Un ejemplo de funcionamiento de este tipo de ataque, abuso de servidores DNS, es mostrado en el documento: Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos. La figura 1 ejemplifica el ataque.

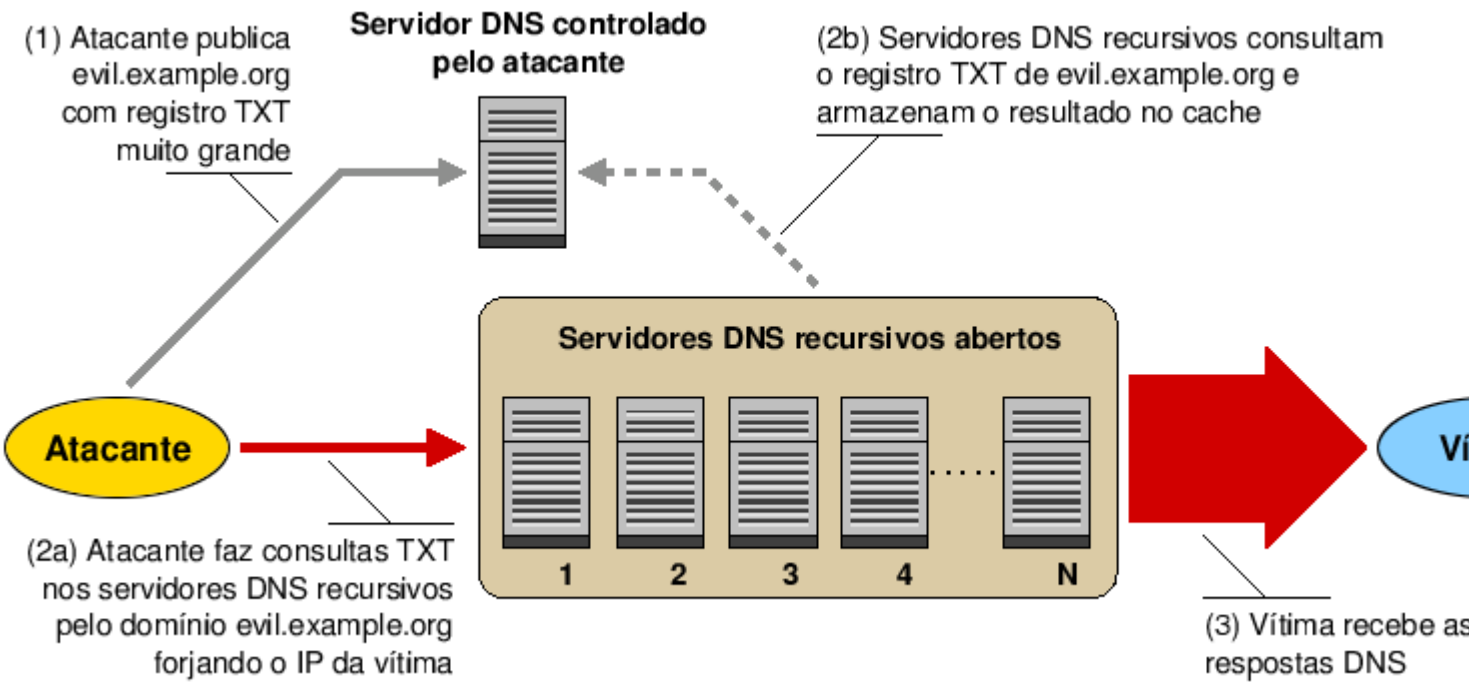

Figura 1: Visión general de un ataque de negación de servicio utilizando servidores DNS recursivos abiertos.

1. El atacante publica un registro muy grande, en general TXT, en un servidor DNS que controla (muchas veces puede ser un servidor comprometido previamente por parte del atacante).
2. El atacante, en posesión de una lista de servidores DNS recursivos abiertos, envía a estos servidores centenares o millares de consultas sobre el registro previamente publicado en el paso anterior, falsificando la dirección IP de origen, colocando la IP de la víctima de forma tal que el atacante hace que las respuestas sean enviadas a la víctima y no al equipo que hizo las consultas. La primera consulta recibida por uno de estos servidores recursivos va a ser realizada al servidor controlado por el atacante (2b), las demás consultas serán enviadas directamente desde la caché del servidor recursivo abierto.
3. La víctima recibe las respuestas de DNS, estas acostumbran a generar una amplificación de entre 28 a 64 veces el tráfico inicial de la consulta, pues para una consulta media de aproximadamente 50 bytes se le pueden retornar unos 2.700 bytes a la víctima.

5. Como evitar que sus redes y sistemas sean usados para generar ataques de DDoS

Los ataques de DDoS se aprovechan de la gran dependencia e interconexión entre las redes y sistemas en Internet. Deben utilizarse buenas prácticas de seguridad para prevenir que redes y sistemas sean abusados y generen ataques, sin embargo, sin una preparación adecuada, poco puede ser hecho para impedir que un ataque tenga éxito.

De esta forma, la seguridad de cada una de las redes y sistemas depende directamente de la seguridad de los demás. Para resolver el problema de ataques de DDoS es necesaria una acción conjunta de los diversos sectores que forman la Internet. A continuación se describen las acciones que cada uno debe ejecutar para no generar ataques de DDoS.

5.1. Usuarios finales

Algunos usuarios participan en los ataques voluntariamente, ofreciendo sus equipos por medio de la instalación de herramientas o a través del acceso a sitios específicos. Al hacer esto hallan que están contribuyendo a una causa que consideran importante. Esta visión puede ser aprovechada por atacantes para conseguir el apoyo y la participación de un mayor número de personas. Por esto es importante que esos usuarios sean alertados que, tras los ataques de DDoS, no siempre hay motivaciones tan dignas que lo ameriten.

Al contribuir voluntariamente con los ataques de DDoS los usuarios pueden participar en acciones criminales y ser directamente impactados por los efectos colaterales causados. Por ejemplo, el aumento del uso de ancho de banda generado por los ataques puede ser convertido en un aumento de gastos del proveedor de conectividad que, para compensar el prejuicio puede incrementar sus costos hacia los clientes.

La mayoría de los usuarios, entretanto, participan de los ataques de forma involuntaria, al tener sus equipos (computadores, dispositivos móviles, CPEs, etc) infectados por *bots* o invadidos y con herramientas de DDoS instaladas en ellos. Por ello deben ser concienciados sobre la importancia de mantener sus equipos seguros.

Invertir en la concienciación de los usuarios también es una medida esencial en organizaciones que permiten el uso de equipos personales dentro de las redes corporativas. Sin una política de seguridad adecuada, la organización puede verse responsabilizada por ataques que salen de su red generados por los computadores y dispositivos móviles de los usuarios.

La protección de los equipos de los usuarios debe considerar tanto la aplicación de soluciones técnicas como la adopción de una postura preventiva. Las soluciones técnicas ayudan a los usuarios a protegerse de las amenazas ya conocidas y para las cuales ya existen formas de prevención. Mientras que la postura preventiva ayuda en otras amenazas, principalmente las que se relacionan con la ingeniería social.

Las soluciones técnicas giran en torno a:

- proteger los equipos de red, manteniendo actualizado el *firmware* y cambiando la clave de administración;
- proteger los computadores y dispositivos móviles, manteniendo los programas instalados con las versiones más recientes y con todas las actualizaciones aplicadas;
- usar contraseñas bien elaboradas, con una gran cantidad de caracteres y que no contengan datos personales, palabras conocidas ni secuencias del teclado;
- instalar y mantener actualizados mecanismos de seguridad como antivirus, y *firewall* personal.

Una postura preventiva debe incluir cuidados como:

- estar atentos a hacer click en *links*, independientemente de cómo fueron recibidos y de quién los envió. Al acceder a *links* cortos usar plugins que permitan que los links de destino sean visualizados;

- no considerar que mensajes que provengan de conocidos son siempre confiables, pues el campo del remitente puede haber sido falsificado o puede haber sido enviado desde cuentas comprometidas;
- no abrir ni ejecutar archivos sin anter verificarlos con antivirus.

Más consejos para usuarios finales están disponibles en la Cartilha de seguridad para Internet.

5.2 Desarrolladores de aplicaciones Web

Los servidores Web acostumbran a ser máquinas bien conectadas y con gran capacidad de procesamiento y, por eso, son muy apetecidos por los atacantes que, al invadirles, instalan programas maliciosos, como herramientas para realizar ataques de DDoS.

Para garantizar la seguridad de un servidor Web, es necesario, además de seguir las buenas prácticas de administración de equipos descritas en la sección 5.3, adoptar algunos cuidados adicionales como son:

- mantener el servidor actualizado, incluido el servicio web, la base de datos y todas las extensiones, módulos y plugins utilizados;
- jamás ejecutar los servicios utilizando cuentas privilegiadas como “root” o “Administrador”;
- crear usuarios distintos y con privilegios mínimos para los diversos servicios y funciones. Por ejemplo, crear un usuario para el servicio Web, otro para el de Base de Datos y otros para cada aplicación. De esta forma si una de estas cuentas es comprometida, los daños quedarán restringidos solamente a los privilegios asignados a esta cuenta.
- ser cuidadoso con los permisos en los directorios y archivos. Permitir, por defecto, solamente la lectura y autorizar la escritura y la ejecución de acuerdo con las necesidades de los usuarios o grupos;
- deshabilitar los módulos, servicios y recursos innecesarios, incluido:
    - el listado de directorios en el servidor Web;
    - la directiva que muestra informaciones del servidor Web como la versión, caminos del sistema y nombre de las bases de datos, pues estas pueden ser utilizadas en ataques para explotar vulnerabilidades;
    - los métodos TRACE y TRACK, pues ellos permiten depurar informaciones y exponen datos contenidos en *cookies*.

Para mantener un ambiente Web seguro es importante también garantizar la seguridad de las aplicaciones, pues ellas son una de las principales puertas de entrada para el acceso indebido a los servidores Web.

Actualmente las aplicaciones Web son cada vez más complejas y con nuevos recursos integrados. Además de esto, sufren con el descuido de los usuarios y administradores cuando no utilizan buenas contraseñas, con una gran cantidad de sistemas vulnerables, con una presión económica para ser lanzadas rápidamente (conjuntamente con sus problemas) y con una falta de desarrolladores Web capacitados en programación segura.

La seguridad de una aplicación Web necesita ser pensada en todas sus fases, incluyendo la

planificación, el desarrollo, las pruebas, la entrada en producción, la revisión diaria de logs y el mantenimiento. También debe estar presente en todas las partes que componen a una aplicación como el *framework* donde fue desarrollada, el sistema de gestión de contenidos (*Content Management System* – CMS) conque se ejecuta y el sistema de base de datos que esta accede.

Además de esto, es importante destacar que el hecho de que una aplicación esté de conformidad (*compliance*) con normas y certificaciones no le garantiza de que ésta sea segura, pues nuevas vulnerabilidades pueden surgir para las cuales la aplicación no fue probada. Por ello, las precauciones con la seguridad deben ser una tarea cotidiana y un proceso continuo.

Algunos consejos para mejorar la seguridad de aplicaciones Web son:

- inforporar prácticas de desarrollo seguro de Software desde las primeras fases del proyecto;
- seguir buenas prácticas de programación segura. En el OWASP Top Ten Project se encuentran recomendaciones de cómo evitar los riesgos de seguridad más críticos, como *Cross-Site Scripting* (XSS), referencia insegura y directa a objetos y, principalmente, a una incorrecta configuración de seguridad;
- implementar los recursos de seguridad, como por ejemplo la validación de datos en entrada, soempre en el servidor Web pues, cuando se implementan protecciones del lado del cliente, estas pueden ser burladas tanto por los usuarios al deshabilitar, por ejemplo, el JavaScript, como por los atacantes al utilizar herramientas específicas para interactuar con el servidor sin pasar poe la interfaz del cliente;
- asegurar que las aplicaciones generen logs que faciliten el monitoreo, la detección de errores y la identificación de intentos de ataque y de acceso indebido;
- usar sistemas de control de versión de código, pues en caso de una falla será más fácil encontrar cuándo fue incorporada y cuáles versiones necesitan ser modificadas;
- mantener seguros los computadores usados para el desarrollo de la aplicación, pues si fuesen comprometidos o infectados ellos pueden comprometer también el ambiente de producción;
- considerar que las aplicaciones serán ejecutadas en un ambiente hostil y, por ello, deben ser probadas no solamente para los casos de uso, sino además para los de abuso;
- usar herramientas de prueba, como son el OWASP Zed Attack Proxy Project que analiza el comportamiento de la aplicación y muestra posibles vulnerabilidades;
- mantener el CMS protegido:
    - mantener el CMS y los *plugins* actualizados, siempre con las versiones más nuevas;
    - restringir el acceso a la interfaz de administración solamente a los administradores de las aplicaciones;
    - no usar cuentas por defecto de administración, como por ejemplo el usuario "admin";
    - usar contraseñas fuertes y, de ser posible, habilitar la autenticación en dos etapas;
    - seguir las guías de seguridad de los proveedores del CMS;
    - utilizar *plugins* que permitan mejorar la seguridad del CMS, como por ejemplo el Wordfence. Consejos de cómo utilizarlo pueden ser obtenidos en Wordfence – un plugin de seguridad para Wordpress.

- considerar el uso de un *firewall* de aplicación Web (*Web Application Firewall* – WAF) pues este ofrece recursos extras de protección que ayudan a identificar y bloquear los ataques más comunes;
    - a pesar de que un WAF puede ayudar a proteger las aplicaciones, este debe ser utilizado como una capa más y no como la solución única de seguridad, pues cualquier falla que presente puede colocar en riesgo a toda la aplicación.
- estar atento a sitios web y blogs de seguridad para estar al tanto de las nuevas tendencias de ataques o vulnerabilidades.

Más sugerencias pueden ser en Dicas para mantener un ambiente Web seguro.

5.3 Administradores de redes

Los administradores de redes pueden ayudar a mejorar el escenario de los ataques de DDoS implementando buenas prácticas que impidan que la infraestructura de la cual son responsables sea abusada para generar ataques. Algunas de las buenas prácticas son:

- mantener los equipos actualizados, no solamente el Sistema Operativo, sino también todos los servicios que en él son ejecutados;
- apagar servicios innecesarios (*hardening*), pues cuanto menos servicios estén siendo ejecutados, menores serán las oportunidades de vulnerabilidad que puedan ser explotadas;
- configurar adecuadamente los servicios, principalmente los que pueden ser abusados para la amplificación del tráfico (más detalles en la sección sección 5.4);
- ser cuidados al usar y elaborar contraseñas y, si se puede, utilizar autenticación en dos etapas;
- crear usuarios distintos para los distintos servicios y funciones del sistema;
- revisar los *logs*, en la búsqueda de errores y de intentos de explotar vulnerabilidades;
- verificar el tráfico de entrada en la red en búsqueda de intentos de accesos no autorizados;
- verificar el tráfico de salida de la red, en búsqueda de indicios de fuga de datos, escaneos y de accesos indebidos originados desde la red;
- habilitar filtros *antispoofing*, implementando mecanismos de *egress filtering* que impidan la salida de la red de paquetes cuya dirección de origen pertenezca a una red reservada y que no formen parte de bloques de direcciones de la red interna. Detalles sobre este tipo de filtrado pueden ser encontrados en el Portal de boas práticas para a Internet no Brasil;
- hacer campañas de concienciación de usuarios, alertando sobre los riesgos y formas de prevención;
- crear una política de seguridad definiendo las reglas de uso de equipos personales dentro de la organización;
- tener personal entrenado para tratar incidentes de seguridad, pues en caso de que la red sea utilizada para generar ataques de DDoS son altas las probabilidades del administrador de que reciba notificaciones por la red o sistema atacado;
- estar atento a sitios web y blogs de seguridad para estar al tanto de las nuevas tendencias de ataques o vulnerabilidades.

5.4 Provedores de internet

Así como los administradores de las redes, los proveedores de Internet (ISP – *Internet Service Provider*) pueden ayudar a reducir los ataques de DDoS implementando buenas prácticas que impidan que las infraestructuras de ellos y de sus clientes sean abusadas para generar ataques. Para ello es necesario el combate a los ataques de tipo DRDoS.

Los principales motivos de ataques de DRDoS son tan poderosos son el tráfico falso, el abuso de los servicios que permiten la amplificación de tráfico y una gran cantidad de equipos de red, tales como CPE instalados sin consideraciones de seguridad. Algunas buenas prácticas que pueden ayudar a revertir este escenario son:

- habilitar filtro *antispoofing*, implementando mecanismos de *egress filtering* que impidan la salida de paquetes con dirección de origen perteneciente a una red reservada y que no sean parte de uno de los bloques de direcciones de las redes internas. Detalles sobre este tipo de filtrado pueden ser encontrados en Portal de boas práticas para a Internet no Brasil;
- proteger los CPEs de los clientes:
    - deshabilitar servicios innecesarios;
    - mantener los equipos actualizados, incluído el *firmware*;
    - no usar contraseñas por defecto, pues ellas, pues estas son muchas veces obvias y fácilmente encontradas en listados de Internet;
    - usar contraseñas bien elaboradas, con gran cantidad de caracteres y que no contengan datos personales, palabras conocidas y secuencias de teclado.
- configurar adecuadamente los servicios, principalmente los que pueden ser abusados para amplificación de tráfico:
    - servicio DNS (53/UDP):
        - contactar a los administradores de los servidores vulnerables para que corrijan los problemas;
        - permitir acceso a los servidores recursivos solamente para la red interna;
        - deshabilitar la recursividad en los servidores autoritativos;
        - usar el recurso *Response Rate Limit* (RRL) para limitar a cantidad de consultas. Más detalles pueden ser encontrados en el documento Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos.
    - servicio NTP (123/UDP):
        - considerar una implementación más simple, como OpenNTP;
        - actualizar a la versión más reciente;
        - deshabilitar la función "monitor" en el archivo de configuración;
        - configurar para que el servicio se ejecute solamente como cliente;
        - responder solamente a peticiones de la red interna.
    - servicio SNMP (161/UDP):
        - si es posible posible actualizar para a versión más reciente;
        - no utilizar la comunidad "Public".
    - servicio SSDP (1900/UDP):

- deshabilitar el acceso a los equipos via WAN y UPnP, si no fuera necesario.

6. Como manejar ataques DDoS

Toda organización, tarde o temprano, puede ser objeto de un ataque DDoS y, por esto, debe planificar con antelación las acciones, tanto técnicas como no técnicas, a ser tomadas cuando el ataque ocurra. La planificación incluye las fases de preparación, detección, análisis, mitigación y posterior al ataque que serán descritas detalladamente a continuación.

6.1 Preparación

La preparación es la fase principal de la planificación pues representa la base para las etapas subsequentes (detección y análisis, mitigación y posterior al ataque). Además de esto, como es la única a ocurrir anticipadamente, cuando el ataque todavía no ha sucedido, puede ser realizada de forma más detallada y cuidadosa.

Para una preparación adecuada es importante:

Conocer la organización: cuanto mayor sea la base de conocimiento sobre la misión de la organización y sobre sus recursos, más fácil será definir lo que debe ser protegido y priorizar las acciones a ser tomadas.

- hacer un análisis de riesgo, identificando lo que es crítico para la organización, incluyendo los dados, servicios y clientes;
- informarse sobre lo que ocurre, tanto en la propia organización como en otros medios (*situation awareness*):
    - monitorear fuentes públicas de información, como buscadores, repositorios de datos, redes sociales, canales de IRC y *blogs*, buscando referencias al nombre y a los productos de la organización, pues algunos ataques acostumbran a ser previamente anunciados;
    - informarse sobre acciones de la organización que pueden atraer demasiada atención, como el lanzamiento de nuevos productos, el patrocinio de eventos o el apoyo a causas polémicas;
    - informarse sobre los ataques ya ocurridos contra la organización, intentar prevenir la posibilidad de que ocurran nuevamente, buscar establecer la frecuencia conque ocurren e identificar cuáles son los blancos preferidos.
- verificar con las áreas jurídica y administrativa cuál es la política a ser seguida en caso de posibles intentos de extorsión.

Conocer el patrón de uso: el monitoreo de recursos permite identificar previamente el comportamiento normal y, de esta forma, detectar rápidamente los cambios de comportamiento.

- identificar la media y los picos de tráfico de la red, tanto en bps (bits por segundo) como en pps (paquetes por segundo);
- identificar a tasa de uso de recursos y cuáles son los servicios más usados por los usuarios;
- identificar cuáles son los servicios más codiciados por los atacantes;
- identificar a cantidad media de errores HTTP de tipo 4xx y 5xx (por ejemplo, "404 – no

encontrado" y "503 – servicio no disponible").

Diminuir las posibilidades de ataque: cuanto menos expuestos estén los servicios, sistemas y equipos, menores serán las oportunidades de que sean atacados.

- hacer un inventario de la red, procurando detectar cuáles sistemas están más expuestos, la importancia de ellos dentro de la organización y cuáles son los posibles cuellos de botella y puntos de falla. No olvidar mantenerlos actualizados;
- deshabilitar los servicios innecesarios:
    - cuanto menos servicios estén siendo ejecutados, menores serán las oportunidades de que vulnerabilidades existentes en ellos sean explotadas;
    - el mantenimiento de las máquinas también será más fácil pues los administradores podrán concentrar sus esfuerzos en los servicios realmente necesarios para la organización.
- verificar la localización de *firewalls*, WAFs e IPSs en la topología de la red;
    - aunque estos equipos pueden apoyar en la mitigación de ataques DDoS simples, en algunos casos estos pueden empeorar el problema ya que, dependiendo de la posición y de como están implementados, pueden representar cuellos de botella y puntos de falla en común. Al intentar analizar los paquetes y las peticiones estos pueden sobrecargarse y causar lentitud en la red. También pueden quedar in-operativos y dejar inaccesibles todas las redes y sistemas que de ellos dependen;
    - conocer los limites y la capacidad de cada equipo o sistema y, siempre que sea posible, posicionarlos en la topologia de forma que los de mayor capacidad protejan a los de menor capacidad.
- verificar la asignación de direcciones IP:
    - equipos de infraestructura, como ruteadores, *firewalls* y servidores DNS, no deben estar en la misma subred de servicios y de clientes;
    - servicios con varias direcciones IP deben tener, si fuera posible, cada IP asignado en una subred diferente;
    - servidores DNS autoritativos deben estar en subredes diferentes.

Proteger los recursos que pueden ser atacados: servicios que son accesibles por Internet pueden ser atacados y por eso, deben ser protegidos.

- mantener los servidores y equipos actualizados para que las vulnerabilidades sean corregidas, antes de que los atacantes intenten explotarlas;
- habilitar o configurar módulos específicos de servidores Web que puedan bloquear algunos tipos de ataques de DDoS, como ModEvasive y ModSecurity en Apache;
- reducir los valores de TTL (*time-to-live*) de los registros de DNS de los sistemas que puedan ser atacados, pues esto facilita la redirección del tráfico y permite que los cambios sean fácilmente detectados;
- configurar *rate limiting* en los equipos de red, tanto en el plano de control (*control-plane*) cuanto en el plano de datos (*data-plane*), si está disponible. Esta funcionalidad permite que la

organización descarte el tráfico basado, por ejemplo, en una tasa excesiva de tráfico de un determinado protocolo;
- activar la opción de *SYN cookies* en los equipos que soporten esta funcionalidad, para que sean dedicados recursos solamente para conexiones TCP de clientes legítimos. Más informaciones en la RFC 4987;
- sincronizar los servidores via NTP (*Network Time Protocol*), pues esto facilita la correlación de *logs* y la notificación de un ataque. Más informaciones en NTP.br.

Prepárese para absorber y filtrar el ataque: analizar la resiliencia de la red y de los sistemas, o sea, la capacidad de ellos de resistencia, adaptación y recuperación frente a ataques DDoS.

- usar servicios de protección contra ataques DDoS, como comunidades BGP (*Border Gateway Protocol*) para *Black Hole* y *Sink Hole*;
    - servicios de *Black Hole*, también llamados de *null-routing*, llevan todo el tráfico destinado a una determinada máquina o servicio, reduciendo los efectos del ataque en otros servicios dejando sin embargo al blanco no disponible;
    - servicios de *Sink Hole*, también llamados de *clean-pipe* y *traffic-scrubbing*, redireccionan el tráfico del ataque hacia servidores fuera de la organización, que analizan y filtran el tráfico y retornan a la organización solamente el que es considerado legítimo. Deben ser usados con cautela cuando se maneja tráfico con datos sensibles, pues pueden afectar la confidencialidad de la información y la privacidad de los usuarios;
    - considerar la forma de implantación dependiendo de la manera en cómo una red se conecta a Internet;
        - redes que poseen sistema autónomo (*Autonomous System* – AS) propio tienen autonomía para controlar los anuncios de ruta y activar los servicios de *Black Hole* y *Sink Hole*;
        - redes que no poseen deben verificar si su contrato con el proveedor de internet incluye servicios de protección contra ataques DDoS y cuáles son sus costos.
- verificar la posibilidad de participación en el servicio colaborativo UTRS (*Unwanted Traffic Removal Service*), que facilita la mitigación de ataques DDoS para las víctimas que tengan el mismo. En este servicio, la víctima anuncia vía BGP su IP bajo ataque y los demás participantes pueden entonces descartar tráfico, pero cerca del origen, para este destino;
- verificar si el contrato con el proveedor de Internet incluye las cláusulas abajo listadas y cuáles son los costos:
    - cobro de uso de ancho de banda en la modalidad percentil 95, que permite que los picos de uso no sean considerados;
    - flexibilización de uso de ancho de banda en caso de mayor consumo (modalidad de contrato *on-demand*);
        - en este caso es importante planificar para que la interfaz física tenga capacidad mayor que el ancho de banda efectivamente contratado.
- dimensionar los recursos considerando holguras (super dimensionamiento – *overprovision*),

incluyendo *links* con capacidad mayor que los picos de tráfico y productos/servicios que permitan escalabilidad bajo demanda (elasticidad);
- asegurarse que los servidores y equipos de red están configurados de acuerdo con las necesidades y preparados para tratar eventuales picos de utilización, por ejemplo, emitiendo alertas cuando los limites normales de uso fueren sobrepasados;
- verificar la capacidad de carga de las aplicaciones, considerando los picos de uso;
    - identificar cuellos de botella en el procesamiento, como consultas muy lentas a la base de datos, y analizar las soluciones aplicables para mejorar el desempeño;
    - definir una política de balanceo de carga en base a los resultados de la identificación antes realizada, como mejorar la capacidad y/o la cantidad de servidores, tener un *hardware* dedicado, usar un balanceador externo de carga, usar servicios que permitan escalabilidad automática bajo demanda y soluciones como *proxy* reverso, Anycast, GSLB (*Global Server Load-Balance*) y CDNs (*Content Delivery Network*);
        - CDNs ofrecen funcionalidades que permiten absorber altos volúmenes de tráfico, distribuir el contenido en diferentes servidores/*datacenters*, ofrecer los contenidos cercanos al solicitante y filtrar los ataques más comunes contra servidores y aplicaciones Web, por medio de WAFs;
        - estas funcionalidades pueden introducir latencia en las comunicaciones y afectar el tiempo de respuesta en las conexiones y, por ello, pueden no ser recomendadas para sistemas cuyo tiempo de respuesta sea crítico para su funcionamiento.

Prepararse para lidiar con un ataque de DDoS: tener personal preparado para actuar frente al problema y políticas claras de comunicación.

- tener un grupo de respuesta a incidentes preparado y entrenado para tratar ataques DDoS;
    - establecer canales de comunicación efectivos para que usuarios, clientes, administradores de red y grupos de seguridad puedan reportar problemas de acceso a los servicios de la organización;
    - establecer contacto con otros grupos de seguridad;
    - definir los procedimientos a ser seguidos en caso de un ataque y mantenerles actualizados;
        - asignar algunas personas del grupo para tratar del ataque de DDoS y dejar otras disponibles para las tareas cotidianas, ya que algunos ataques son realizados con el objetivo de distraer a los equipos de seguridad cuando otros ataques son realizados;
        - definir modelos de notificaciones de incidentes para agilizar el contacto con las redes involucradas.
- tener personal de red preparado y entrenado para lidiar con el ataque e implantar medidas de mitigación;
    - definir dentro y fuera de la organización quiénes son los responsables por los sistemas y servicios, de forma que puedan ser fácilmente contactados;
    - definir junto al proveedor de Internet el canal de comunicación a ser usado y, si fuera

posible, probarlo con antelación;
        - formas de contacto que dependan de la red o de servidores específicos pueden estar inaccesibles durante el ataque, por esto es importante determinar otros medios, como listar los números de teléfono y direcciones de *e-mail* alternativas.
- preparar formas alternativas de comunicar a los usuarios/clientes de la organización sobre la falta de disponibilidad de los servicios, como tener un *blog* o página Web en localizaciones alternativas y que puedan ser direccionadas, por ejemplo, vía cambios en los DNS;
- capacitar al personal de la central de atención al cliente (*call center*), en caso de que la organización tenga este servicio, para lidiar con los reclamos de clientes/usuarios y definir los procedimientos a ser seguidos por ellos;
- estar preparado para hacer informes de gestión, estimando los perjuicios causados por el ataque y los costos involucrados en la mitigación del problema;
- estar preparado para lidiar con entrevistas o hacer declaraciones públicas, pues muchos ataques atraen la atención de los medios.

6.2 Detección y análisis

La detección de ataques DDoS depende directamente de cuán preparada la organización está, o sea, de cuanto esta ha invertido en tiempo y recursos en la fase de preparación, pues puede ser bastante difícil notar cambios y modificaciones en lo que no está siendo monitoreado.

La detección y el análisis consisten en los siguientes pasos:

Descartar otras posibilidades de problemas: es necesario tener cautela antes de considerar que cualquier cambio en el comportamiento es un ataque de DDoS, pues:

- algunos límites configurados en los equipos pueden ser no adecuados para el uso en su ambiente;
- puede tratarse de un problema no intencional, causado, por ejemplo, por:
    - alguna actualización reciente en servicios lo que haya introducido fallas;
    - alguna campaña de *marketing* o lanzamiento que pueda estar atrayendo tráfico por encima del normal;
    - algún problema de conectividad, como falla en el equipamiento de red o rotura de la fibra;
    - alguna falla local de conexión que afecte solamente algunos usuarios;
        - existen algunos servicios *online* que pueden auxiliar a probar si la falla en la disponibilidad es local o general, como Down for Everyone or Just Me?, Is It Down Right Now? e Just Down For Me?.

Intentar identificar el tipo de ataque: luego de concluirse que realmente se trata de un ataque DDoS es necesario intentar entender sus características e identificar de que tipo es, o sea, si es volumétrico, de aplicación, de agotamiento de recursos de *hardware* o mixto.

- buscar cambios en el patrón, comparando los resultados actuales con los anteriores, por medio, por ejemplo, de herramientas de análisis y monitoreo de flujo de red (*netflows*) que ofrecen

informaciones resumidas sobre protocolos, puertos y direcciones IP de origen/destino más accedidos;
- intentar descubrir cuáles son los recursos que están siendo o fueron afectados, como uso de ancho de banda por encima de lo normal, número excesivo de peticiones a un determinado servicio o carga excesiva en algún equipo de red;
- intentar identificar si el ataque es dirigido a una o más máquinas, uno o más servicios o, una o más aplicaciones.

Obter más detalles sobre el ataque: al reducir las posibilidades es el momento de levantar la mayor cantidad posible de datos sobre el ataque.

- intentar determinar el horario de inicio y de fin, la duración y si el ataque todavía está ocurriendo;
- detectar cuáles son los servicios que están siendo usados, tanto en el origen como en el destino;
- analizar los *logs* más específicos, por ejemplo, de la aplicación o del equipo que está siendo atacado;
- analizar otras informaciones que puedan ser útiles para el análisis.

Intentar determinar el impacto: procurar determinar el impacto del ataque dentro de la organización.

- sistemas críticos que afectan la imagen y los negocios de la empresa deben ser tratados con alta prioridad;
- mientras que los sistemas no críticos no necesariamente requieren de prioridad máxima y pueden ser tratados de forma menos prioritaria.

Estar atento a otros ataques: una vez que el ataque esté controlado es importante redoblar la atención ante potenciales ataques, tanto de DDoS como de otros tipos.

- algunos ataques ocurren en "olas", como forma de probar la capacidad de la organización en lidiar con el problema, o sea, pueden ocurrir nuevamente y en forma más potente;
- algunos ataques son realizados con el objetivo de distraer los equipos de red y seguridad, pues mientras están lidando con el DDoS, otros ataques también están siendo realizados contra la organización y pueden no recibir la atención debida.

6.3 Mitigación

Luego de analizar y concluir que realmente se trata de un ataque DDoS es necesario mantener la calma y seguir los procedimentos definidos en la etapa de preparación.

La etapa de preparación es esencial para realizar la mitigación del ataque más rápida y efectiva. Entretanto, si la organización está sometida a un ataque DDoS por primera vez y/o no se planificó con antelación, no significa que no pueda hacer nada para mitigar el problema, solamente que tal vez sea más demorado y trabajoso.

Es importante comprender que no es fácil contener un ataque de DDoS en desarrollo, sin embargo contamos con acciones y técnicas que pueden auxiliar a reducir los daños causados. De preferencia, la

mitigación debe ser aplicada al más próximo posible del origen del ataque para que el exceso de tráfico impacte lo menos posible las demás redes.

Las técnicas listadas en esta sección son un resumen de algunos de los puntos citados con detalles en la sección 6.1.

Documentar las acciones tomadas: antes de comenzar a actuar es importante recordar registrar las acciones que están siendo tomadas.

- el registro de las acciones ayudará a describir los problemas y será esencial en la etapa posterior al ataque (seción 6.4).

Distribuir el blanco del ataque: usar recursos para distribuir el tráfico del ataque entre diferentes servidores, de preferencia, entre los que están localizados próximo a los atacantes.

- distribuir el blanco entre diferentes servidores, por medio de técnicas como GSLB, Anycast y CDN.

Usar servicios de mitigación: por medio de comunidades BGP es posible redirigir y filtrar el tráfico.

- activar servicios de *Sink Hole* (*clean-pipe* o *traffic-scrubbing*) para intentar filtrar el tráfico malicioso;
- activar servicios de *Black Hole* (*null-routing*) para descartar el tráfico destinado al blanco del ataque;
- activar el servicio colaborativo UTRS, informando el IP atacado para que los demás participantes puedan descartar el tráfico a él destinado.

Intentar reducir el volumen de tráfico: efectuar un filtrado de tráfico, respetando los limites de la infraestrutura ya que, en dependencia del ataque, el procesamiento (*overhead*) necesario para analizar y filtrar el tráfico puede sobrecargar los equipos y dejar la red fuera de servicio.

- filtrar el tráfico por IP o puerto de origen o destino;
- usar *rate-limiting* y ACLs en equipos de red;
- usar control de ancho de banda (bps) y de tasa de paquetes (pps);
- activar el uso de *SYN cookies* en los equipos que soporten esta funcionalidad;
- verificar la posibilidad de obtener un aumento temporal de ancho de banda.

Intentar mitigar los ataques a la capa de aplicación: aplicar medidas de mitigación para proteger la aplicación que está siendo atacada.

- si es posible servir temporalmente páginas estáticas en vez de dinámicas y de imágenes con una menor resolución;
- si la aplicación blanco se ejecuta en un servidor que también tiene otros servicios, intentar moverla para un servidor exclusivo y, de esta forma, minimizar el impacto sobre los demás servicios;
- mover la aplicación para una máquina con más capacidad de procesamiento o usar servicios de virtualización que permitan agregar recursos bajo demanda.

Notificar las redes que están generando el ataque: informar las redes que están generando el ataque para que tomen medidas para interrumpir esta actividad maliciosa.

- modelos de notificaciones están disponibles en el documento Recomendações para Notificações de Incidentes de seguridad.

6.4. Posterior al ataque

Luego del ataque es el momento de:

- documentar el incidente, destacando tanto las acciones que ayudaron como las que no surtieron el efecto deseado;
- observar lo que podría haber sido hecho previamente que hubiera ayudado en las etapas de preparación, detección, análisis y mitigación del ataque;
- actualizar los contratos de prestadores de servicio, como proveedor de Internet y de servicios en la nube y de CDN;
- revisar las cláusulas de los contratos, en caso de que estos no estuvieran de acuerdo con las necesidades;
- adecuar las etapas de preparación, detección, análisis y mitigación que presentaran problemas;
- verificar otros incidentes que puedan haber sucedido durante el ataque;
- analizar cuidadosamente los archivos con los *logs* guardados durante el ataque para intentar recolectar información adicional que pueda ser útil;
- notificar a las instituciones que que contribuyeron a generar tráfico durante el ataque. A pesar de que es poco viable de haber evidencia de uso de IPs forjados, puede ser útil en caso de servicios mal configurados que están siendo abusados, por ejemplo, DNS abiertos (*open resolver*).

7. Glosario

ACL
: *Access Control List* – Lista de Control de Acceso.

AS
: *Autonomous System* – Sistema autónomo; es un grupo de redes IP, bajo un único administrador y que comparten una misma política de enrutamiento. RFC 1930 – https://tools.ietf.org/html/rfc1930.

BGP
: *Border Gateway Protocol*. Protocolo de enrutamiento usado para intercambiar informaciones sobre caminos entre diferentes redes.

bps
: *bits per second* – bits por segundo.

CDN
: *Content Delivery Network* – red de distribución de contenido.

CHARGEN
: *Character Generator Protocol* – Protocolo de generación de caracteres. Utiliza los puertos 19/UDP y 19/TCP.

CMS

Content Management System – Sistema de gestión de contenidos.

CPE

Customer Premises Equipment. Nombre genérico que se refiere a los equipos de red instalados en el punto de acceso del usuario/abonado de un servicio de telecomunicaciones. ejemplos: *modem* ADSL, ruteador Wi-Fi (Fuente: Wikipedia).

DNS

Domain Name System – Sistema de nombres de dominios. Servicio responsable de la traducción, entre otros tipos, de nombres de máquinas/dominios a direcciones IP correspondiente y viceversa. Utiliza los puertos 53/UDP y 53/TCP.

DDoS

Distributed Denial of Service – Negación distribuida de servicio. Actividad maliciosa, coordinada y distribuida mediante la cual un conjunto de computadores y/o dispositivos móviles son utilizados para interrumpir la operación un servicio, un computador o una red conectada a Internet.

DoS

Denial of Service – Negación de servicio. Actividad maliciosa mediante la cual un atacante utiliza un computador o dispositivo móvil para interrumpir la operación de un servicio, un computador o una red conectada a Internet.

DRDoS

Distributed Reflective Denial of Service – Negación distribuida de servicio con uso de amplificación. Tipo de ataque volumétrico que explora características en protocolos de Internet, que permiten altas tasas de amplificación de paquetes, y utiliza direcciones IP forjadas (spoofeadas), para que los paquetes amplificados sean direccionados para el blanco del ataque.

GSLB

Global Server Load-Balance. Balanceador de carga de servidor global.

HOIC

High Orbit Ion Cannon. Herramienta que puede ser usada para la generación de ataques DDoS.

IPS

Intrusion Prevention System – Sistema de prevención de intrusos.

IRC

Internet Relay Chat.

ISP

Internet Service Provider – proveedor de servicios de Internet.

LOIC

Low Orbit Ion Cannon. Herramienta que puede ser usada para la generación de ataques DDoS.

NetBIOS

Network Basic Input/Output System – Sistema básico de red de entrada y salida. Utiliza los puertos 137/UDP, 138/UDP y 139/UDP.

NTP

Network Time Protocol – Protocolo de tiempo en la red. Tipo de protocolo que permite la sincronización de los reloj de los dispositivos de una red, como servidores, estaciones de trabajo, ruteadores y otros equipos, a partir de referencias de tiempo confiables (Fuente:http://ntp.br/). Utiliza el puerto 123/UDP.

OWASP

Open Web Application Security Project – https://www.owasp.org/.

pps

packets per second – paquetes por segundo.

RUDY

R.U.D.Y., R-U-Dead-Yet?. Herramienta que puede ser usada para generar ataques DDoS.

RRL
Response Rate Limit.
SGBD
Sistema de gestión de base de datos o *Database Management System* (DBMS).
Slowloris
Herramienta que puede ser usada para generar ataques DDoS.
SNMP
Simple Network Management Protocol – Protocolo simples de gestión de red. Utiliza los puertos 161/UDP y 161/TCP.
SSDP
Simple Service Discovery Protocol. Protocolo simple de descubrimiento de servicios. Utiliza el puerto 1900/UDP.
TTL
Time to Live.
UPnP
Universal Plug and Play.
WAF
Web Application Firewall.
WAN
Wide Area Network.
XSS
Cross-Site Scripting.

8. Referencias

Listamos referencias que apoyaron a la redacción del documento y recomendado como lectura complementaria

Informes, artículos y guías sobre ataques de DDoS

- *DDoS Basics*
  https://www.team-cymru.com/ReadingRoom/Whitepapers/2010/ddos-basics.pdf
- *DDoS Overview and Incident Response Guide*
  http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_14_09_DDoS_final.pdf
- *DDoS: Proactive and Reactive measures*
  https://www.cert.be/files/DDoS-proactive-reactive.pdf
- *Network DDoS Incident Response Cheat Sheet*
  https://zeltser.com/ddos-incident-cheat-sheet

Artículos sobre ataques de DRDoS

- *Amplification Hell: Revisiting Network Protocols for DDoS Abuse*
  http://www.internetsociety.org/doc/amplification-hell-revisiting-network-protocols-ddos-abuse
- Ataques de amplificación UDP
  https://www.security.unicamp.br/artigos/24-amplificacao-udp.html

- *Exit from Hell? Reducing the Impact of Amplification DDoS Attacks*
  https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/kuhrer
- *Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attack*
  https://www.usenix.org/conference/woot14/workshop-program/presentation/kuhrer
- Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos
  http://www.cert.br/docs/whitepapers/dns-recursivo-aberto
- *US-CERT Alert (TA13-088A) – DNS Amplification Attacks*
  http://www.us-cert.gov/ncas/alerts/TA13-088A
- *US-CERT Alert (TA14-017A) – UDP-Based Amplification Attacks*
  https://www.us-cert.gov/ncas/alerts/TA14-017A

Presentaciones en eventos sobre ataques DDoS

- Ataques DDoS – Panorama, mitigación e Evolución
  ftp://ftp.registro.br/pub/gter/gter39/08-AtaquesDdosPanoramaMitigacaoEvolucao.pdf
- *Community tools to fight against DDoS*
  http://sanog.org/resources/sanog27/SANOG27-Conference_Community_tools_to_fight_against_DDoS.pdf
- Como se proteger contra los ataques de DDoS
  http://www.cert.br/docs/palestras/certbr-abranet-curitiba2015.pdf
- Estratégias de Defesa Contra Ataques de Negación de servicio
  ftp://ftp.registro.br/pub/gts/gts26/03-estrategia-ddos.pdf

Buenas prácticas – *AntiSpoofing*

- BCP 38, RFC 2827: *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*
  https://tools.ietf.org/html/rfc2827
- BCP 84, RFC 3704: *Ingress Filtering for Multihomed Networks*
  https://tools.ietf.org/html/rfc3704
- Portal de Boas Práticas para a Internet no Brasil
  http://bcp.nic.br/

Consejos de seguridad para ambientes Web

- 10 Dicas para mantener su Joomla seguro
  https://www.security.unicamp.br/22-dicas-seguranca-joomla.html
- *OWASP Top Ten Project*
  https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=OWASP_Top_10_for_2013

- *Defending Against Application Level DoS Attack*
  https://www.owasp.org/images/0/04/Roberto_Suggi_Liverani_OWASPNZDAY2010-Defending_against_application_DoS.pdf
- Dicas para mantener su ambiente Web seguro
  https://www.security.unicamp.br/31-dicas-para-manter-seu-ambiente-web-seguro.html
- *OWASP Zed Attack Proxy Project*
  https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
- Wordfence – un plugin de seguridad para Wordpress
  https://www.security.unicamp.br/67-wordfence-um-plugin-de-seguranca-para-wordpress.html

Recomendaciones y modelos para notificación de incidentes

- Recomendações para Notificações de Incidentes de seguridad
  http://www.cert.br/docs/whitepapers/notificacoes/
- Modelos de notificações – DDoS por *botnet* sem *spoofing*
  http://www.cert.br/docs/whitepapers/notificacoes/#8.9
- Modelos de notificações – Ataque de negación de servicio distribuído con uso de amplificación (DRDoS)
  http://www.cert.br/docs/whitepapers/notificacoes/#8.10

Otras referencias

- Cartilha de seguridad para Internet
  http://cartilha.cert.br/
- *Open Resolver Project*
  http://openresolverproject.org/
- Práticas de seguridad para Administradores de redes Internet
  http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html
- *TCP SYN Flooding Attacks and Common Mitigations*
  https://tools.ietf.org/html/rfc4987/
- *The Measurement Factory – DNS Survey: Open Resolvers*
  http://dns.measurement-factory.com/surveys/openresolvers.html
- *UTRS – Unwanted Traffic Removal Service*
  http://www.team-cymru.org/UTRS/

9. Agradecimientos

Nos gustaría agradecer a Miriam von Zuben por el desarrollo de la versión inicial de este documento y a Cristine Hoepers, Gustavo Rodrigues Ramos, Iguatemi Eduardo de la Fonseca, Klaus Steding-Jessen, Lucimara Desiderá, Marcelo H. P. C. Chaves y Wilson Rogério Lopes por la revisión y por sugerencias

para la elaboración de este documento.

10. Histórico de Revisiones

- **versión 1.0-ES** traducción al Español, 21/04/2016 - Ernesto Pérez CSIRT CEDIA
- **versión 1.0** versión Inicial, 19/04/2016