

Instituto Politécnico Nacional

Unidad Profesional Interdisciplinaria   
de   
Ingeniería Y Ciencias Sociales Y Administrativas

ATAQUE DDOS HACIENDO USO DE WIRESHARK Y LOW ORBIT ION CANNON

Materia: Seguridad Informática

Alumnos: ELIZALDE BARRANCO DANIELA

GARCÍA HERNÁNDEZ DIANA BERENICE

GARCÍA PONCE CARLOS ANTONIO

MARCIAL ORTIZ PEDRO SINUHE

MENDOZA GAMINO XIMENA ROTCEH

REYES QUIJANO RAYMUNDO ULISES

RUÍZ MÁRQUEZ ABRAHAM

Ciclo: 2020/1

Profesor: Sandoval Gonzalez Victor L.

Secuencia: 3NM60

ÍNDICE

[**Introducción**](#_heading=h.4xaj4fpsb76) **3**

[**Objetivo**](#_heading=h.m1z79c9gkpcw) **4**

[¿Qué sucedió? … Ocurrió una Denegación de Servicio Distribuido de acceso al Estadio.](#_heading=h.4b4zn8ldcjts) 5

[¿Cómo se hace un DDoS?](#_heading=h.xjff0xeaudm6) 5

[**WireShark**](#_heading=h.24zf1mwr1jxw) **5**

[¿Qué hace?](#_heading=h.2et92p0) 5

[Controles WireShark](#_heading=h.tyjcwt) 6

[Campos de WireShark](#_heading=h.3dy6vkm) 6

[Codificación de color en WireShark](#_heading=h.1t3h5sf) 7

[Comandos o filtros](#_heading=h.4d34og8) 7

[Capturar paquetes](#_heading=h.2s8eyo1) 9

[Filtrar paquetes](#_heading=h.17dp8vu) 11

[Analizar paquetes](#_heading=h.3rdcrjn) 12

[**Hacking**](#_heading=h.26in1rg) **13**

[**Ataque DDoS**](#_heading=h.gzlct3hydu8h) **16**

[Tipos de Ataque](#_heading=h.lnxbz9) 17

[**Low Orbit Ion Cannon**](#_heading=h.35nkun2) **18**

Manual para ataque DDoS con LOIC (Low Orbit Ioc Cannon) **20**

[**Implementación de ataque DDoS**](#_heading=h.1ksv4uv) **21**

**Resumen Hora 11 22**

# Introducción

Hackers. Una palabra que aún no se encuentra en los diccionarios pero que ya suena en todas las personas que alguna vez se interesaron por la informática o leyeron algún diario. Proviene de "hack", el sonido que hacían los técnicos de las empresas telefónicas al golpear los aparatos para que funcionen. Hoy es una palabra temida por empresarios, legisladores y autoridades que desean controlar a quienes se divierten descifrando claves para ingresar a lugares prohibidos y tener acceso a información indebida.

Sólo basta con repasar unas pocas estadísticas. Durante 1997, el 54 por ciento de las empresas norteamericanas sufrieron ataques de Hackers en sus sistemas. Las incursiones de los piratas informáticos, ocasionaron pérdidas totales de 137 millones de dólares en ese mismo año. El Pentágono, la CIA, UNICEF, La ONU y demás organismos mundiales han sido víctimas de intromisiones por parte de estas personas que tienen muchos conocimientos en la materia y también una gran capacidad para resolver los obstáculos que se les presentan\*. Un hacker puede tardar meses en vulnerar un sistema ya que son cada vez más sofisticados. Pero el lema es viejo: hecha la ley, hecha la trampa.

Los medios de comunicación masivos prefieren tildarlos de delincuentes que interceptan códigos de tarjetas de crédito y los utilizan para beneficio propio. También están los que se entrometen en los sistemas de aeropuertos produciendo un caos en los vuelos y en los horarios de los aviones. Pero he aquí la gran diferencia en cuestión. Los crackers (crack=destruir) son aquellas personas que siempre buscan molestar a otros, piratear software protegido por leyes, destruir sistemas muy complejos mediante la transmisión de poderosos virus, etc. Esos son los crackers. Adolescentes inquietos que aprenden rápidamente este complejo oficio. Se diferencian con los Hackers porque no poseen ningún tipo de ideología cuando realizan sus "trabajos". En cambio, el principal objetivo de los Hackers no es convertirse en delincuentes sino "pelear contra un sistema injusto" utilizando como arma al propio sistema. Su guerra es silenciosa pero muy convincente.

# Objetivo

Para comprender el objetivo de la ataque DDos, que se realizará dentro de la red LAN, se puede explicar de la siguiente forma:

Por ejemplo un estadio de fútbol que albergará la final del campeonato mundial, el estadio cuenta con *diversas puertas* para que los aficionados ingresen al estadio, 1 hora antes de inicio del juego la gente *ingresa* de forma ordenada al estadio *a un ritmo lento pero constante*, las personas ubicadas en las puertas encargadas de r*evisar la fiabilidad* de los boletos están muy cansadas pero no se detienen en su labor, de pronto, faltando 5 minutos para el inicio del juego, *una gran cantidad* de personas con *boletos falsos*, arriban al estadio al mismo tiempo, los encargados de revisar los boletos no se dan abasto en atender a tanta gente, las personas que cuentan con su boleto auténtico no pueden entrar al estadio.

Los responsables de restringir el acceso al estadio se ven imposibilitados para diferenciar los boletos auténticos de los falsos y además están exhaustos, la carga de trabajo es excesiva. Se les explica que llevará más tiempo de lo previsto para ingresar, pues se tienen que revisar a detalle cada uno de los boletos, ante este anuncio las personas que no tienen boleto auténtico intentan ingresar al mismo tiempo de forma desorganizada y por la fuerza, por varios minutos los accesos se ven saturados, muy pocas personas logran ingresar, y por el contrario miles de personas se pierden el gran partido aun cuando tenían boleto auténtico.

Se pretende, realizar una ataque DDos por Connection Flood (inundación de conexión): Explota la dificultad del servidor para atender un gran número de peticiones al mismo tiempo, si un atacante realiza 10,000 peticiones al servidor este estará ocupado por un período de tiempo, conforme caduquen las conexiones el atacante vuelve a establecer más conexiones impidiendo así que los clientes utilicen el servicio.

Aunado a esto, se desea realizar una auditación la red para analizar el tráfico, con la herramienta Wireshark, esta aplicación es un analizador de protocolos de red, es de código abierto, tipo sniffer, este es un tipo de software que permite detectar e interceptar tramas de una red, de acuerdo con unos parámetros de búsqueda. Permite capturar, desplegar y filtrar paquetes para este caso, de una red de Windows, sin embargo está disponible también para GNU/Linux, Unix y MAC. Su principal objetivo es el análisis de tráfico, permite obtener soluciones rápidas para una red. A pesar que no es un IDS (Intrusion Detection System), Sistema de Detección de Intrusos o un IPS (Intrusion Prevention System), Sistema de Prevención de Intrusos, aplicaciones que permiten identificar y evitar accesos no autorizados a un computador o a una red, sí es un sniffer como ellos y ofrece ventajas respecto de estos sistemas, como la agilidad para el monitoreo y auditoría extensa en una red, es decir que es eficiente.

Con Wireshark, conectados a una red LAN, auditamos la red, con el fin de visualizar y tomar información confidencial del tráfico de la misma.

## ¿Qué sucedió? … Ocurrió una Denegación de Servicio Distribuido de acceso al Estadio.

Un sitio Web es como una puerta de acceso, sólo puede dar servicio a un número limitado de personas al mismo tiempo, por tanto si recibe más solicitudes de las que puede atender, el servicio se bloquea, nada entra ni sale.

## ¿Cómo se hace un DDoS?

Para que el ataque sea realmente efectivo se debe contar con muchas máquinas que envíen peticiones a la página Web. Existen personas que se dedican a infectar equipos y crear grandes redes de equipos “zombie” (botnets) y posteriormente rentarlas.

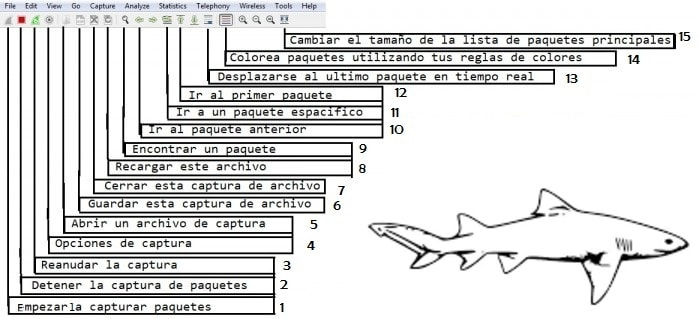
# WireShark

## ¿Qué hace?

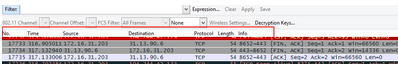
La herramienta intercepta el tráfico y lo convierte en un formato legible para las personas. Esto hace que sea más fácil identificar qué tráfico está cruzando la red, con qué frecuencia y la latencia que hay entre ciertos saltos. Si bien Wireshark admite más de 2.000 protocolos de red, muchos de ellos inusuales o antiguos, los profesionales encuentran una gran utilidad en el análisis de identidades IP. La mayoría de los paquetes son TCP, UPD e ICMP.

Dado el gran volumen de tráfico que atraviesa una red comercial típica, las utilidades de Wireshark ayudan a filtrarlo. Los filtros de captura solo recopilan los tipos de tráfico que le interesan al comercio y los de visualización le ayudan a acercarse al tráfico que quiere inspeccionar. El analizador de protocolo de red proporciona herramientas de búsqueda, que incluyen expresiones regulares y resaltado en color, para que sea más fácil encontrar lo que se está buscando.

## Controles WireShark



## Campos de WireShark

****

**Nro:** este campo indica el número del paquete que se está capturando.

**Time:** indica el tiempo transcurrido en cada paquete capturado.

**Source:** acá se indica la dirección IP origen que está generando la conexión.

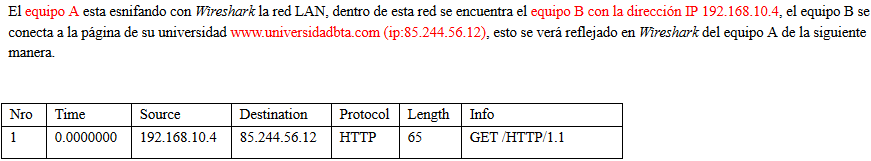
**Destination:** nos indica la dirección IP destino de la conexión.

**Protocol:** este campo nos indica el protocolo que se está utilizando para establecer una conexión.

**Length:** nos indica el tamaño del paquete.

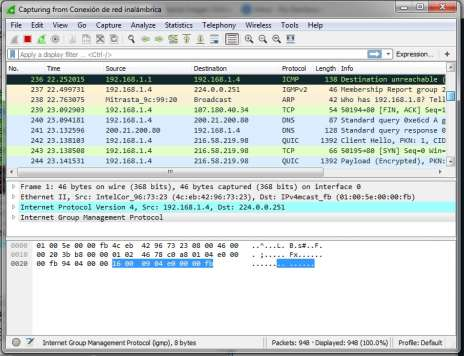
**Info:** este campo nos muestra información en concreto del comportamiento del protocolo utilizado.

**Ejemplo**

****

## Codificación de color en WireShark

Probablemente verá paquetes resaltados en verde, azul y negro. Wireshark utiliza colores para ayudarle a identificar los tipos de tráfico de un vistazo. De forma predeterminada, el verde es el tráfico TCP, el azul es el tráfico DNS, el azul claro es el tráfico UDP y el negro identifica los paquetes TCP con problemas; por ejemplo, podrían haber sido entregados dañados.

****

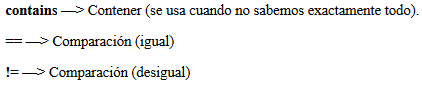
Para ver exactamente lo que significan los códigos de color, haga clic en View> Coloring rules. También puede personalizar y modificar las reglas de coloración de aquí, si lo desea (solo debe hacer doble clic sobre alguno de ellos y escoge el color que quiera).

## Comandos o filtros

Concatenadores:



Operadores:

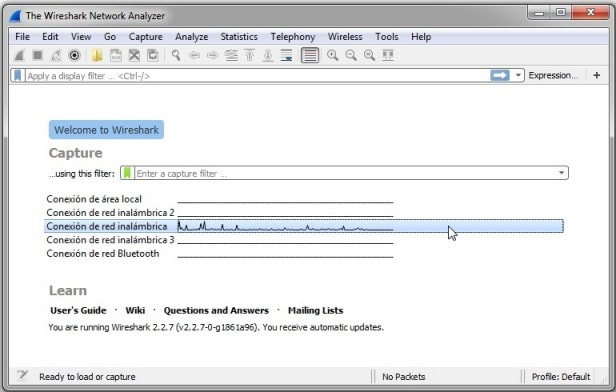


Protocolos:

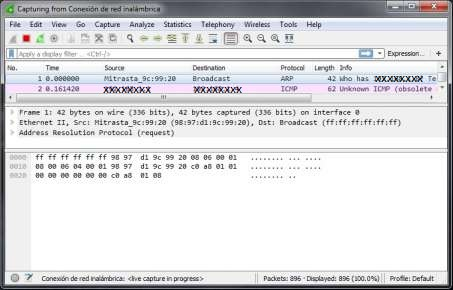
|  |  |
| --- | --- |
| **Sintaxis** | **Significado** |
| ssl | Protocolo SSL (capa segura). |
| telnet | Telnet |
| dns | DNS |
| msnms | Mensajería Instantánea (Messenger) |
| ftp | Protocolo FTP (se podría ver el nombre de usuario y contraseña) |
| dtp-data | Nos permite ver los datos del protocolo FTP |
| ip | Protocolo IP |
| ip.addr==93.184.216.34 | Permite examinar los paquetes de una IP especifica |
| ip.src==192.168.1.1 | Dirección IP origen |
| ip.dst==192.168.1.1 | Dirección IP destino |
| tcp | Protocolo TCP |
| tcp.port==80 | Indicamos los paquetes en el puerto deseado (en este caso 80) |
| tcp.srcport==80 | Indicamos el puerto de origen |
| tcp.dstport==80 | Indicamos el puerto de destino |
| http | Protocolo HTTP |
| http.host==”www.google.com” | Permite ver los paquetes que tengan a Google como host |
| http.date==”Wed, 30 Mar 2011 22:40:55 GMT” | Paquetes respecto a una fecha |
| http.content\_type==”aplication/json” | Muestra el contenido de los paquetes aplicación jason |
| http.content\_type==”image/jpeg” | Muestra el contenido de imágenes jpeg  Nota: otros archivos  \*text/html  \*text/css  \*video/quicktime  \*application/zip |
| http.request.method==”GET” | Permite examinar los metodos  de peticion GET  \*POST |
| http.user\_agent contains “Mozilla” | Permite la obtención de peticiones realizadas desde un navegador determinado.  \*Gecko  \*Microsoft  \*Linux |
| http.server==”ngnix” | Visualiza los paquetes de respuesta del servidor hacia los clientes  \*sffe (Safer Server)  \*gws (Google Web Server)  \*Apache (Aquí mediante la palabra clave contains podemos diferenciar otros valores como PHP, Unix, etc)  \*PWS (Personal Web Server)  \*GFE (GFE/2.0 web server) |
| http.request.uri!=\* | No se visualizan los paquetes NOTIFY \* HTTP |

## Capturar paquetes

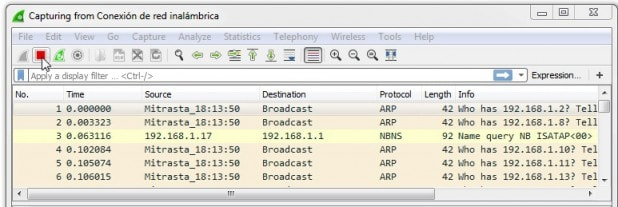
1. Hacer click sobre la interfaz para poder capturar paquetes de la misma.

****

1. Tan pronto como hagas clic en el nombre de la interfaz, verás que los paquetes empiezan a aparecer en tiempo real. Wireshark captura cada paquete enviado hacia o desde tu sistema. Si estás haciendo capturas en una interfaz inalámbrica y tienes el modo promiscuo activado en sus opciones de captura (el cual está habilitado por defecto), también verá los paquetes de los otros paquetes de la red.

****

1. Haz clic en el botón detener captura (Boton Rojo cuadrado #2) cerca de la esquina superior izquierda de la ventana cuando desees detener la captura de tráfico.

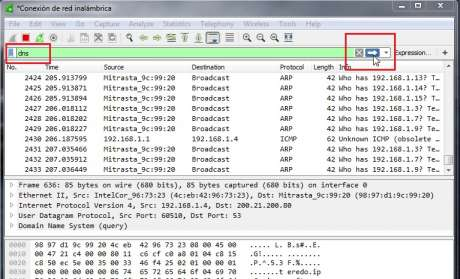


1. Luego de que haya presionado el botón Detener captura usted puede guardar esa captura para examinarla posteriormente, presionando Ctrl + Shift + S, o simplemente vaya hacia File>Save as, y coloca un nombre de su preferencia, como por ejemplo Primera Captura. Luego presiona Guardar.
2. Si no hay nada interesante en tu propia red para inspeccionar, Wireshark te tiene la solución. La página web de Wireshark contiene una página de archivos de captura de ejemplo que puede cargar e inspeccionar.
3. Abrir un archivo de captura es fácil; Simplemente, después de que tengas guardado cualquier paquete, cierre wireshark y vuélvalo a abrir, aparecerá de inmediato el paquete que capturó anteriormente, haz doble clic en el archivo y este se abrirá en la pantalla principal de Wireshark automáticamente, sino también puedes desde el menú de Wireshark File -> Open. También puedes guardar tus propias capturas en Wireshark y abrirlas más tarde.

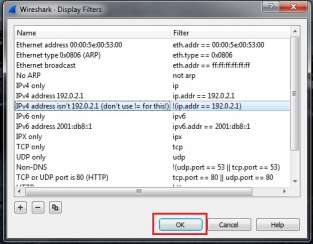
## Filtrar paquetes

Si está intentando inspeccionar algo específico, como el tráfico que envía un programa al llamar a casa, ayude a cerrar todas las demás aplicaciones que utilizan la red para reducir el tráfico. Sin embargo, es probable que tenga una gran cantidad de paquetes para filtrar. Ahí es donde entran los filtros de Wireshark.

La forma más básica de aplicar un filtro es escribiéndola en el cuadro de filtro en la parte superior de la ventana y haciendo clic en Aplicar (o presionando Enter). Por ejemplo, escriba dns y verá sólo paquetes DNS. Cuando comience a escribir, Wireshark te ayudará a completar tu filtro automáticamente, luego también puedes darle clic en la flecha azul de la imagen de abajo para enfocarte en lo que buscas.

****

También puede hacer clic en el menú Analizar y seleccionar Mostrar filtros para crear un nuevo filtro.

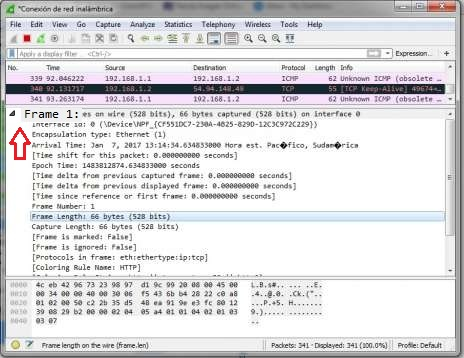


Otra cosa interesante que puedes hacer es hacer clic con el botón derecho del ratón en un paquete y seleccionar Follow  -> TCP Stream (seguir la secuencia TCP).Verá la conversación completa entre el cliente y el servidor.

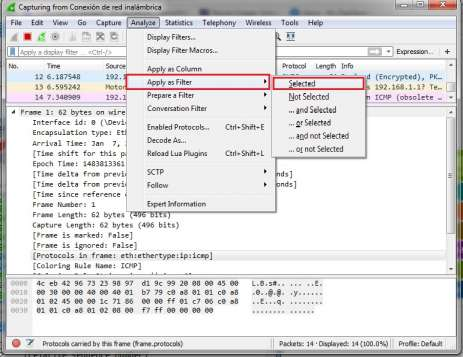


## Analizar paquetes

1. Haz clic en un paquete para seleccionarlo y puedes bajar para ver sus detalles.



1. También puedes crear filtros desde aquí: haz clic derecho en uno de los detalles y usa el submenú Aplicar como filtro para crear un filtro basado en él.



# Hacking

El hacking informático recurre a la manipulación de la conducta normal de un equipo y de los sistemas que tiene conectados. Esto se hace generalmente mediante scripts o programas que manipulan los datos que pasan a través de una conexión de red con el fin de acceder a la información del sistema. Las técnicas de hacking incluyen el uso de virus, gusanos, Troyanos, ransomware, secuestros del navegador, rootkits y ataques de denegación de servicio.

A continuación describiremos brevemente algunos ataques o vulnerabilidades que se pueden presentar en el sistema.

Malware

El término Malware se refiere de forma genérica a cualquier software malicioso que tiene por objetivo infiltrarse en un sistema para dañarlo. Aunque se parece a lo que comúnmente se le conoce como virus, el virus es un tipo de malware. Igualmente existen otros como los gusanos, troyanos, etc.

**Virus**

El virus es un código que infecta los archivos del sistema mediante un código maligno, pero para que esto ocurra necesita que nosotros, como usuarios, lo ejecutemos. Una vez que se ejecuta, se esparce por todo nuestro sistema a donde nuestro equipo o cuenta de usuario tenga acceso, desde dispositivos de hardware hasta unidades virtuales o ubicaciones remotas en una red.

**Gusanos**

Un gusano es un programa que, una vez infectado el equipo, realiza copias de sí mismo y las difunde por las red. A diferencia del virus, no necesita nuestra intervención, ni de un medio de respaldo, ya que pueden transmitirse utilizando las redes o el correo electrónico. Son difíciles de detectar, pues al tener como objetivo el difundir e infectar a otros equipos, no afectan al funcionamiento normal del sistema.

**Troyanos**

Son similares a virus, pero no completamente iguales. Mientras que el virus es destructivo por sí mismo, el troyano lo que busca es abrir una puerta trasera para favorecer la entrada de otros programas maliciosos.

Su nombre es alusivo al “Caballo de Troya” ya que su misión es precisamente, pasar desapercibido e ingresar a los sistemas sin que sea detectado como una amenaza potencial. No se propagan a sí mismos y suelen estar integrados en archivos ejecutables aparentemente inofensivos.

**Spyware**

Un spyware es un programa espía, cuyo objetivo principal es obtener información. Su trabajo suele ser también silencioso, sin dar muestras de su funcionamiento, para que puedan recolectar información sobre nuestro equipo con total tranquilidad, e incluso instalar otros programas sin que nos demos cuenta de ello.

**AdWare**

La función principal del adware es la de mostrar publicidad. Aunque su intención no es la de dañar equipos, es considerado por algunos una clase de spyware, ya que puede llegar a recopilar y transmitir datos para estudiar el comportamiento de los usuarios y orientar mejor el tipo de publicidad.

**Ransomware**

Este es uno de los más sofisticados y modernos malwares ya que lo que hace es secuestrar datos y pedir un rescate por ellos. Normalmente, se solicita una transferencia en bitcoins,la moneda digital, para evitar el rastreo y localización. Este tipo de ciberataque va en aumento y es uno de los más temidos en la Actualidad.

**Phishing**

El phishing no es un software, se trata mas bien de diversas técnicas de suplantación de identidad para obtener datos de privados de las victimas, como por ejemplo las contraseñas o datos de seguridad bancarios.

Los medios más utilizados son el correo electrónico, mensajería o llamadas telefónicas, se hacen pasar por alguna entidad u organización conocida, solicitando datos confidenciales, para posteriormente utilizar esos datos en beneficio propio.

**Denegación de servicio distribuido (DDoS)**

De todos los tipos de ataques informáticos este es uno de los más conocidos y temidos, ya que es muy económico su ejecución y muy difícil de rastrear al atacante.

La eficacia de los ataques DDoS se debe a que no tienen que superar las medidas de seguridad que protegen un servidor, pues no intentan penetrar en su interior, sólo bloquearlo.

Los ataques de DDoS consisten en realizar tantas peticiones a un servidor, como para lograr que este colapse o se bloquee. Existen diversas técnicas, entre ellas la más común es el uso de botnets, equipos infectados con troyanos y gusanos en los cuales los usuarios no saben que están formando parte del ataque.

El ataque que realizamos fue el de DDoS por lo tanto explicaremos un poco más del tema.

# Ataque DDoS

Un ataque DDoS tiene como objetivo in habilitar un servidor, un servicio o una infraestructura. Existen diversas formas de ataque DDoS: por saturación del ancho de banda del servidor para dejarlo inaccesible, o por agotamiento de los recursos del sistema de la máquina, impidiendo así que esta responda al tráfico legítimo.

Durante un ataque DDoS, se envían simultáneamente múltiples solicitudes desde distintos puntos de la red. La intensidad de este «fuego cruzado» compromete la estabilidad, y, en ocasiones, la disponibilidad del servicio.

DDos (que viene de Distributed Denial of Service) es un ataque (que se puede realizar de diversas formas) a un sistema de computadoras que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos del sistema de la víctima (incluso aunque tengas un VPS, por ejemplo).

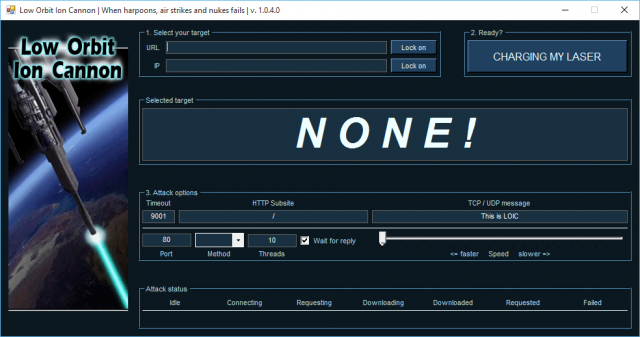
## Tipos de Ataque

|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre del ataque** | **Nivel OSI** | **Tipo de ataque** | **Explicación del ataque** |
| ICMP echo request flood | L3 | Recursos | También denominado Ping Flood. Envío masivo de paquetes (ping), que implican una respuesta por parte de la víctima con el mismo contenido que el paquete de origen. |
| IP Packet Fragment Attack | L3 | Recursos | Envío de paquetes IP que remiten voluntariamente a otros paquetes que nunca se envían, saturando así la memoria de la víctima. |
| SMURF | L3 | Ancho de banda | Ataque por saturación ICMP que usurpa la dirección de origen para redirigir las múltiples respuestas hacia la víctima. |
| IGMP Flood | L3 | Recursos | Envío masivo de paquetes IGMP (protocolo de gestión de grupos de internet) |
| Ping of Death | L3 | Explotación | Envío de paquetes ICMP que explotan fallos del sistema operativo |
| TCP SYN Flood | L4 | Recursos | Envío masivo de solicitudes de conexión TCP |
| TCP Spoofed SYN Flood | L4 | Recursos | Envío masivo de solicitudes de conexión TCP usurpando la dirección de origen |
| TCP SYN ACK Reflection Flood | L4 | Ancho de banda | Envío masivo de solicitudes de conexión TCP a un gran número de máquinas, usurpando la dirección de origen por la dirección de la víctima. En ancho de banda de la víctima queda saturada por las respuestas a dichas peticiones. |
| TCP ACK Flood | L4 | Recursos | Envío masivo de acuses de recibo de segmentos TCP |
| TCP Fragmented Attack | L4 | Recursos | Envío de segmentos TCP que remiten voluntariamente a otros que nunca se envían, saturando la memoria de la víctima |
| UDP Flood | L4 | Ancho de banda | Envío masivo de paquetes UDP (sin necesidad de establecer conexión previa) |
| UDP Fragment Flood | L4 | Recursos | Envío de datagramas que remiten voluntariamente a otros datagramas que nunca se envían, saturando así la memoria de la víctima |
| Distributed DNS Amplification Attack | L7 | Ancho de banda | Envío masivo de peticiones DNS usurpando al dirección de origen de la víctima hacia un gran número de servidores DNS legítimos. Como la respuesta tiene un mayor volumen que la pregunta, el ataque se amplifica |
| DNS Flood | L7 | Recursos | Ataque de un servidor DNS mediante el envío masivo de peticiones |
| HTTP(S) GET/POST Flood | L7 | Recursos | Ataque de un servidor web mediante el envío masivo de peticiones |
| DDoS DNS | L7 | Recursos | Ataque de un servidor DNS mediante el envío masivo de peticiones desde un gran número de máquina s controladas por el atacante |

# Low Orbit Ion Cannon

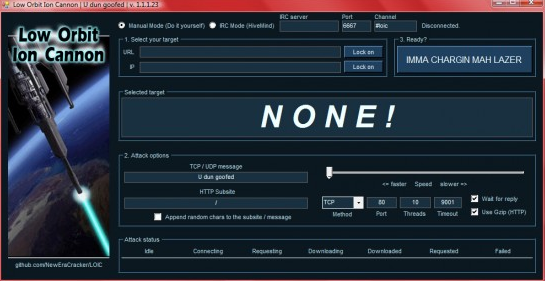
Es posible realizar un ataque con ayuda de la herramienta Low Orbit Ion Cannon. que es es una aplicación diseñada para realizar un ataque de denegación de servicio desarrollada por «praetox» usando el lenguaje de programación C# (Existe también un fork en C++ y Qt llamado LOIQ). La aplicación realiza un ataque de denegación de servicio del objetivo enviando una gran cantidad de paquetes TCP, paquetes UDP o peticiones HTTP con objeto de determinar cuál es la cantidad de peticiones por segundo que puede resolver la red objetivo antes de dejar de funcionar.

Se recomienda esconder la IP antes de realizar un ataque, para evitar ser rastreados. El primer paso es introducir la IP o la URL del servidor donde se realizará el ataque y seleccionarla como objetivo. Podemos seleccionar el puerto, tiempo, protocolo (TCP, UDP, HTTP) y si queremos esperar respuesta del servidor. El siguiente paso es escribir el mensaje TCP/UDP que queremos enviar con los paquetes y la velocidad a la que serán enviados. Una vez seleccionados los parámetros, simplemente seleccionamos enviar carga. Se comenzarán a enviar miles de peticiones a la IP seleccionada, con ayuda de Wireshark podemos visualizar las peticiones, su origen y el protocolo que usan.



**Manual para ataque DDoS con LOIC (Low Orbit Ioc Cannon)**

1. Antes de comenzar a usar el programa LOIC, se requiere deshabilitar el antivirus en el equipo donde se va a realizar el ataque.
2. Al comenzar el programa, nos aparecerá la siguiente ventana:



1. Hay dos formas de realizar el ataque:
   1. Automática:

Los datos importantes para ejecutar los ataques DDoS son:

IRC Server: url del servidor

Port: puerto, en general suele ser 6667.

Channel: por defecto está en LOIC, pero a veces cambia.

Los organizadores de los ataques DDoS los suministran. De esta forma, es todo automatizado. Ellos controlan los ataques desde su PC y los dirigen a dónde quieren.

Una vez insertados los datos, marcamos IRC Mode (HiveMind).

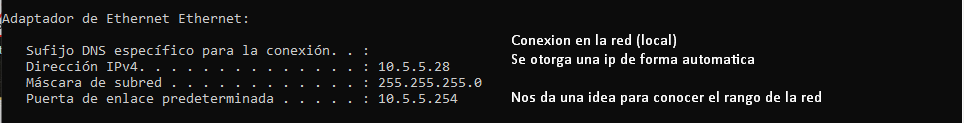
El programa solo se conectará y empezará los ataques DDoS. Abajo, en Requested, puedes ver los paquetes.

* 1. Manual:

Primero debes introducir la URL el sitio que queremos atacar (en URL, dentro de Selected Target). Una vez introducida la URL pulsamos Lock on, y en Selected Target saldrá una IP (unos números separados por puntos). Después pulsamos IMMA CHARGIN MAH LAZER.

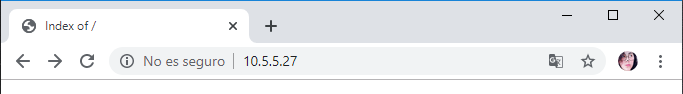
El programa solo se conectará y empezará a lanzar los ataques DDoS. Abajo, en Requested, puedes ver los paquetes.

# Implementación de ataque DDoS

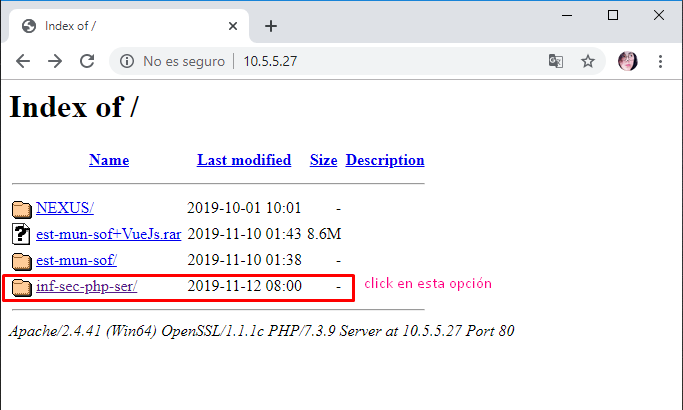
1. Nos conectamos a la red de área local donde se realizará el monitoreo de la red y el ataque de denegación de servicios. Se nos otorga una dirección IP generada de manera dinámica cuando nos conectamos a la red. La dirección puede ser visualizada con ayuda del comando ipconfig, dentro de las direcciones desplegadas podemos encontrar la puerta de enlace predeterminada (Gateway), que nos permitirá tener un indicio del rango de direcciones que se encuentran en la LAN.
2. Si no podemos obtener una dirección de manera automática o necesitamos obtener una nueva, podemos hacer uso del comando ipconfig /renew, el cual libera la dirección IPv4 para el adaptador especificado.



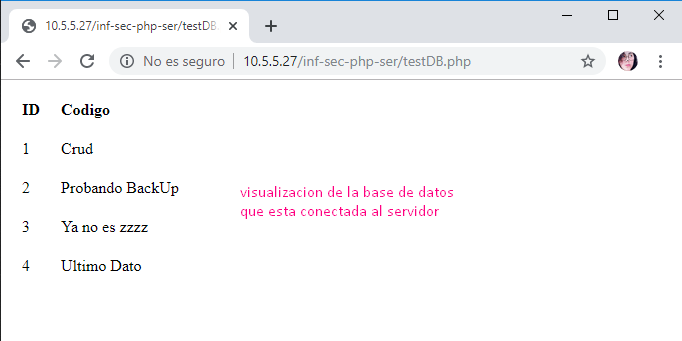
1. Abrimos un navegador web y escribimos la dirección del servidor: 10.5.5.27 Al realizar esta acción el servidor recibirá nuestra petición y nos redirigirá a la interfaz gráfica de Apache. Nuestra petición puede ser visualizada desde el servidor. En este ataque se conoce la dirección IP del servidor por lo que fue menos complejo hacer peticiones, en caso de desconocer la dirección IP del servidor al cual vamos a realizar el ataque, debemos analizar el tráfico de paquetes mediante un filtro en WireShark, debemos deducir la dirección IP del servidor mediante el análisis de tráfico, pues a la dirección a la que le estén llegando más paquetes será muy seguramente el servidor.



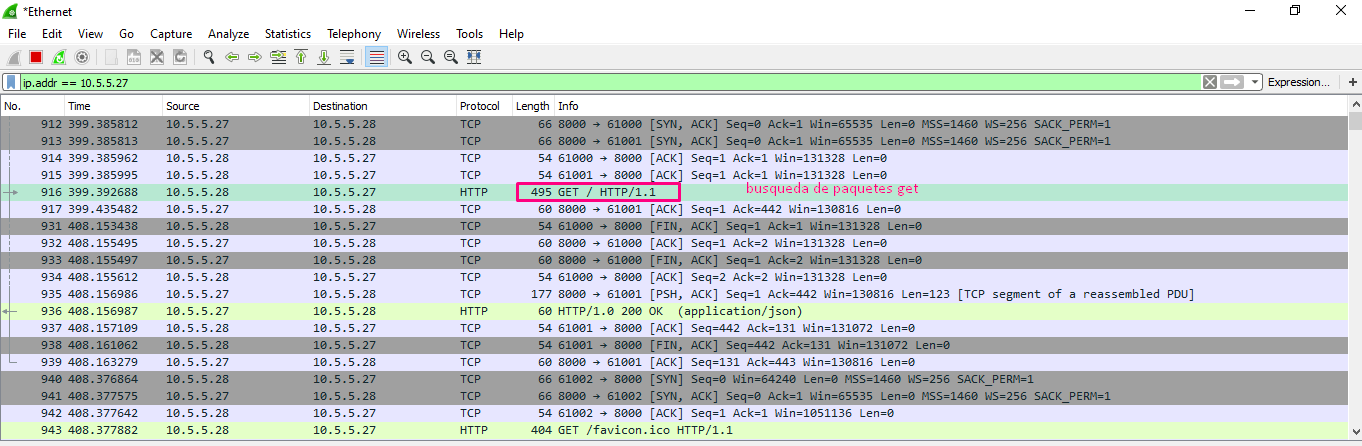
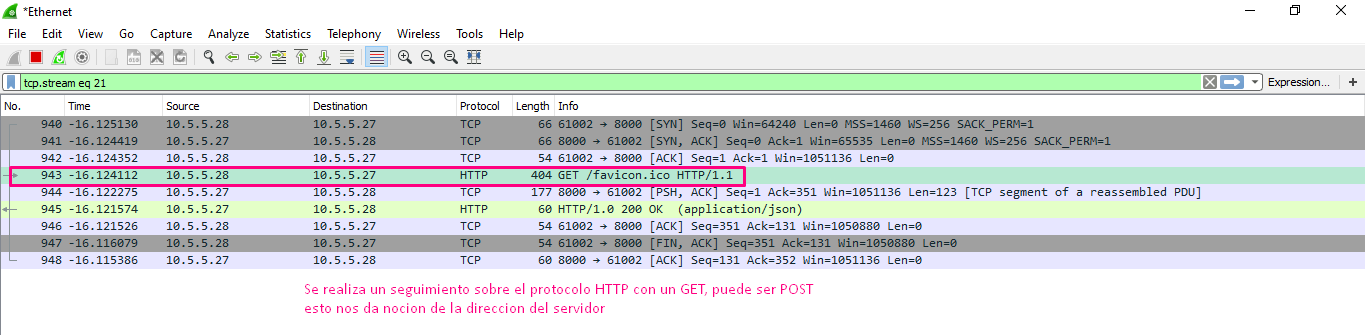
1. Una vez dentro de la interfaz de Apache del servidor debemos ingresar a la carpeta inf-sec-php-ser/



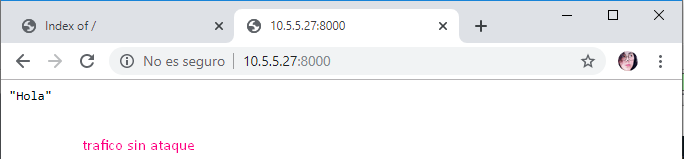
1. Debemos seleccionar el archivo testDB.php 
2. Podremos visualizar una base de datos del servidor



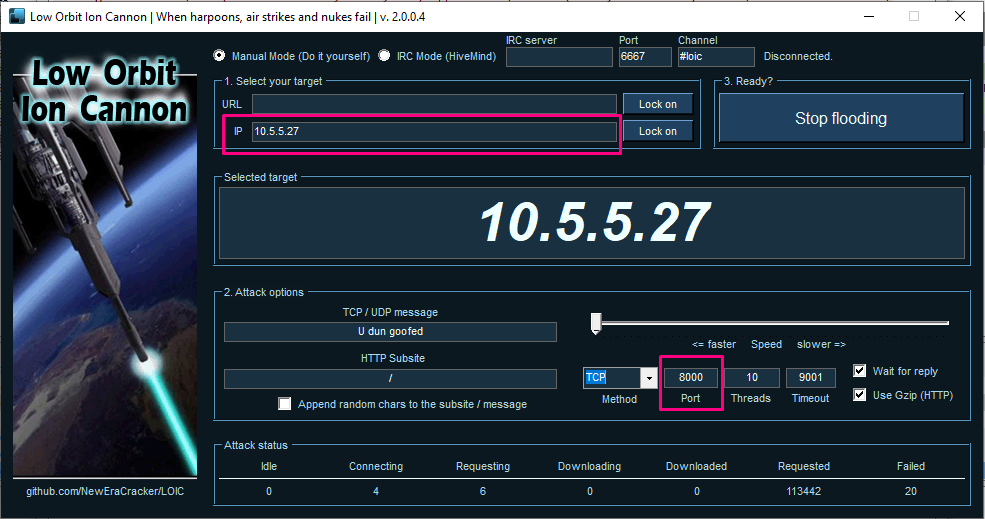
1. Aplicamos un filtro a Wireshark para visualizar la actividad del servidor en la red con el filtro: ip.addr==10.5.5.27, se debe dar un seguimiento a los paquetes GET para el protocolo HTTP para tener una noción de la dirección del servidor. Podemos observar que esta traza dio respuesta a nuestra solicitud desde el servidor.



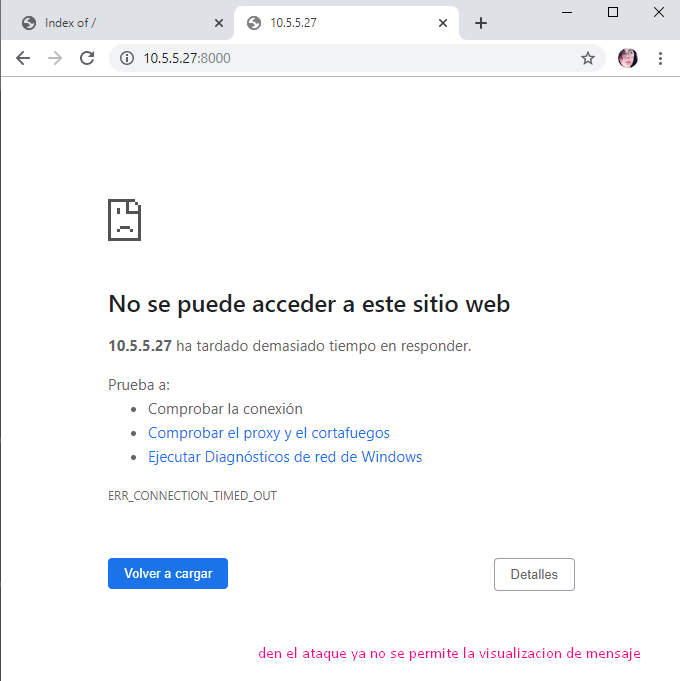
1. Verificamos que el servidor esté activo y funcional. Escribimos la dirección 10.5.5.27 en el puerto 8000 (10.5.5.27:8000). Nos llevará a un mensaje, esto nos indica que el servidor está procesando y respondiendo solicitudes con normalidad.

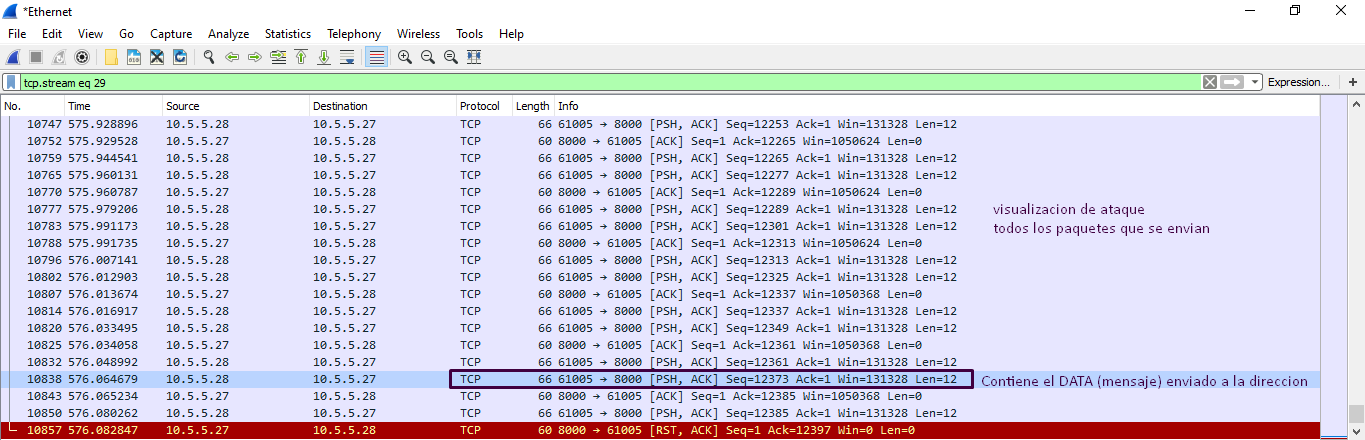


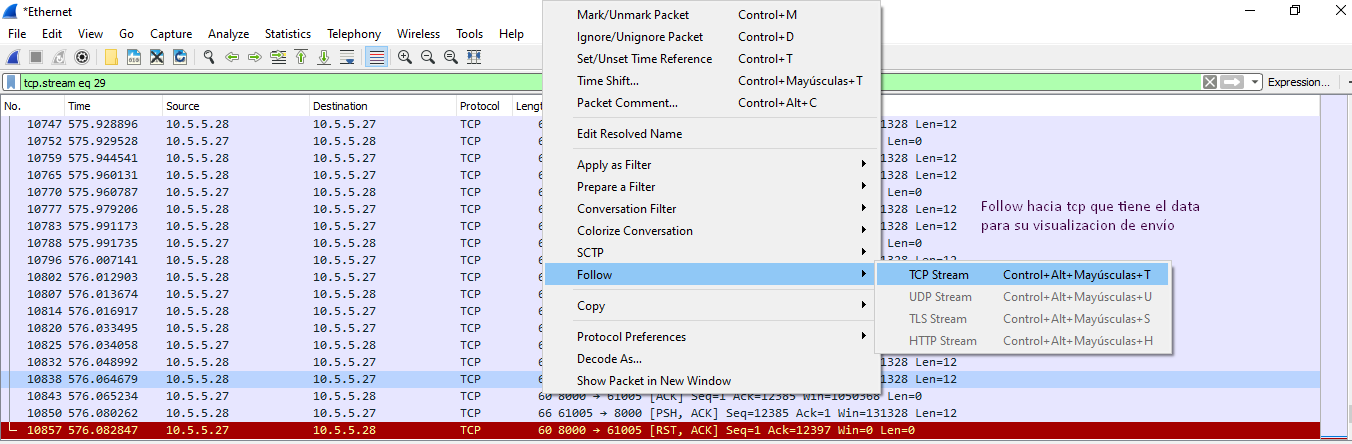
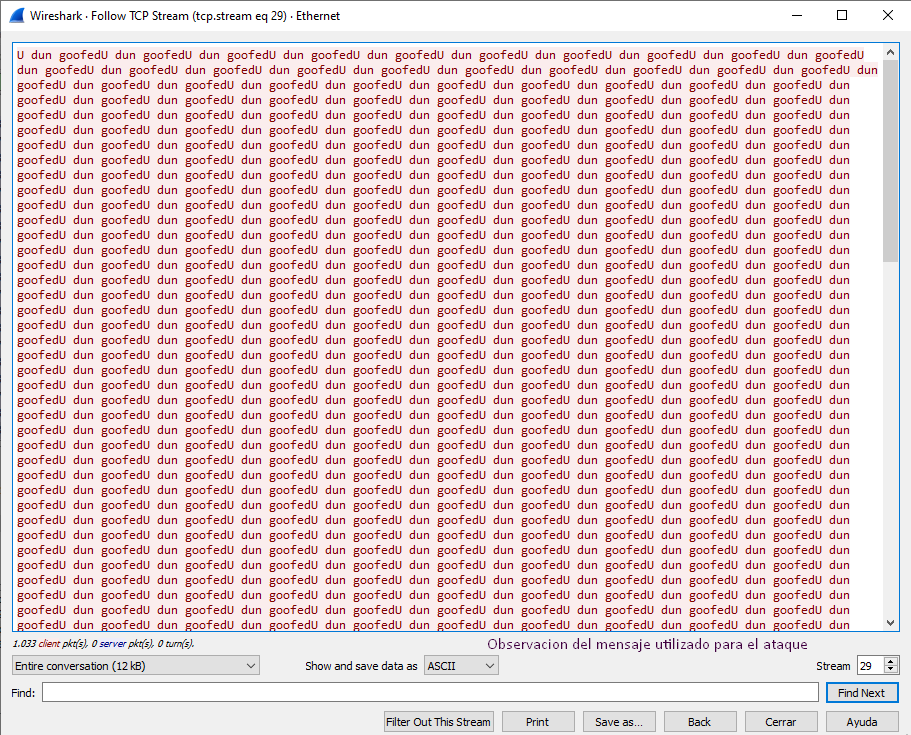
1. Abrimos nuestra herramienta Low Orbit Ion Cannon, debemos escribir la dirección a donde dirigimos el ataque y la confirmamos con lock on: 10.5.5.27 en este caso fue un ataque mediante la IP con el protocolo TCP pero tambien podria ser mediante el protocolo http con la dirección URL. Escribimos también el puerto por donde escucha el servidor: 8000. El ataque que se realizó fue por TCP, se enviaron cerca de 120,000 solicitudes.



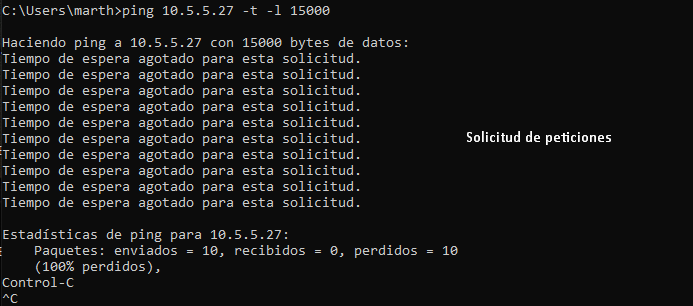
1. Después de un corto período de tiempo el servidor termina por caerse debido a la cantidad de solicitudes simultáneas que llegan. Esto se confirma al actualizar la página. El servidor ya no nos envía respuesta.



1. Con ayuda de Wireshark podemos buscar las trazas que contienen nuestro ataque.
2. Seleccionando la traza y con ayuda de Follow, TCP Stream podemos visualizar toda la información contenida en nuestro ataque.



1. Este método sólo satura la red, es decir en el servidor se puede visualizar que la taza del tráfico de red aumentó en un momento durante el ataque, se genera un pico de peticiones, pero no ocurre nada al procesador del servidor. Para saturar el procesamiento del servidor podemos hacer uso del comando ping 10.5.5.27 -t -l 15000. Con este comando haremos ping a la dirección del servidor hasta que se escriba Ctrl + c, el tamaño de los paquetes será de 15000 bytes. Podemos observar en el servidor que los recursos de procesamiento están saturados, se visualiza en el servidor un pico alto en el procesamiento durante las peticiones de ping.



**Resumen Hora 11**

**Confidencialidad, integridad y disponibilidad.**

La confidencialidad, la integridad y la disponibilidad son la "tríada de la CIA", el concepto fundamental de la seguridad de la información. La tríada, que se muestra en la Figura 1.1, forma el trípode.

La seguridad de la información de las heces se basa en. El orden del acrónimo puede cambiar (algunos prefiera "AIC", tal vez para evitar la asociación con cierta agencia de inteligencia), pero

Los conceptos son esenciales. Este libro usará el acrónimo "CIA".

**Confidencialidad**

La confidencialidad busca evitar la divulgación no autorizada de información: mantiene secreto de datos En otras palabras, la confidencialidad busca evitar el acceso de lectura no autorizado a los datos. Un ejemplo de ataque de confidencialidad sería el robo de información de identificación personal (PII), como la información de la tarjeta de crédito.



**Identidad y autenticación**

La identidad es un reclamo: si tu nombre es "Persona X", te identificas diciendo "Soy Persona X ”. La identidad por sí sola es débil porque no hay pruebas. También puedes identificar usted mismo diciendo "Soy la persona Y". Probar un reclamo de identidad se llama autenticación: usted autentica el reclamo de identidad, generalmente al proporcionar una información o un objeto que solo usted posee, como una contraseña o su pasaporte.

**Autorización**

La autorización describe las acciones que puede realizar en un sistema una vez que se haya identificado y autenticado. Las acciones pueden incluir leer, escribir o ejecutar archivos o programas

**Responsabilidad**

La rendición de cuentas responsabiliza a los usuarios por sus acciones. Esto generalmente se logra mediante el registro y el análisis de los datos de auditoría. Hacer cumplir la responsabilidad ayuda a mantener “Gente honesta”. Para algunos usuarios, saber que los datos están registrados no es suficiente para proporcionar responsabilidad: deben saber que los datos se registran y auditan y que las sanciones pueden resultar de la violación de la política.

**Comunicación simple, semidúplex y dúplex completo**

La comunicación simple es unidireccional, como la radio de un automóvil sintonizada en una estación de música. La comunicación Halfduplex envía o recibe una sola vez (no simultáneamente), como un walkie-talkie Las comunicaciones full-duplex envían y reciben simultáneamente, como dos personas conversando cara a cara.

**LAN, WAN, MAN y PAN**

Una LAN es una red de área local. Una LAN es una red comparativamente pequeña, típicamente confinado a un edificio o un área dentro de uno. Un hombre es una red de área metropolitana,

que generalmente se limita a una ciudad, un código postal, un campus o un parque de oficinas. Una WAN es una red de área amplia, que generalmente cubre ciudades, estados o países.

En el otro extremo del espectro, la más pequeña de estas redes son PAN: Redes de área personal, con un rango de 100m mucho menos. Las tecnologías inalámbricas de baja potencia como Bluetooth se utilizan para crear PAN.

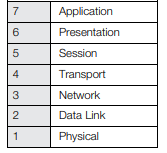
**Internet, Intranet y Extranet**

Internet es una colección global de redes pares que funcionan con TCP / IP, que proporciona servicio de mejor esfuerzo. Una Intranet es una red privada que ejecuta TCP / IP, como como una red de la empresa Una extranet es una conexión entre intranets privadas, como como conexiones con el socio comercial Intranets.

**El modelo OSI**

El modelo de referencia OSI (Interconexión de sistema abierto) es una red en capas modelo. El modelo es abstracto: no ejecutamos directamente el modelo OSI en nuestros sistemas (la mayoría ahora usa el modelo TCP / IP); se utiliza como punto de referencia, por lo que "Capa 1" (física) se entiende universalmente, ya sea que esté ejecutando Ethernet o ATM, por ejemplo. La "Capa X" en este libro se refiere al modelo OSI.

El modelo OSI tiene siete capas, como se muestra en la Tabla siguiente. Las capas pueden estar listadas en orden de arriba hacia abajo o de abajo hacia arriba. Usando este último, física, enlace de datos, red, transporte, sesión, presentación y aplicación.



**ANÁLISIS DE RIESGO**

Todos los profesionales de seguridad de la información evalúan el riesgo: lo hacemos con tanta frecuencia que se convierte en segunda naturaleza. El análisis preciso de riesgos es una habilidad crítica para la seguridad de la información profesional. Debemos juzgarnos a un nivel más alto al juzgar el riesgo. Nuestro las decisiones de riesgo dictarán qué salvaguardas implementaremos para proteger nuestros activos y la cantidad de dinero y recursos que gastamos al hacerlo. Las malas decisiones resultarán en dinero desperdiciado o, peor aún, en datos comprometidos.

**Bienes**

Los activos son recursos valiosos que está tratando de proteger. Los activos pueden ser datos, sistemas, personas, edificios, propiedades, etc. El valor o la importancia crítica del activo determinarán qué medidas de seguridad implementará.

**CONCEPTOS DE PROGRAMACIÓN**

Comencemos por comprender algunos conceptos básicos de programación. A medida que las computadoras se han vuelto más poderosas y ubicuas, el proceso y los métodos utilizados para crear software de computadora han crecido y cambiado.

**Código de máquina, código fuente y ensambladores**

El código de máquina (también llamado lenguaje de máquina) es un software que se ejecuta directamente por la CPU. El código de máquina depende de la CPU; Es una serie de 1s y 0s que traducen a las instrucciones que entiende la CPU. El código fuente es computadora instrucciones del lenguaje de programación que están escritas en texto que deben traducirse en código máquina antes de la ejecución por parte de la CPU.

El lenguaje ensamblador es un lenguaje de programación de computadora de bajo nivel. Montaje las instrucciones de idioma son mnemotécnicos cortos, como "AGREGAR", "SUB", (restar), y "JMP" (salto), que coinciden con las instrucciones del lenguaje de máquina. Un ensamblador convierte el lenguaje ensamblador en lenguaje máquina. Un desensamblador intenta convertir lenguaje de máquina en ensamblador.

**CONCEPTOS CRIPTOGRÁFICOS DE ESQUINA**

Los conceptos criptográficos fundamentales están incorporados en todos los cifrados fuertes y deben ser entendido antes de aprender sobre implementaciones específicas.

**Términos clave**

La criptología es la ciencia de las comunicaciones seguras. La criptografía crea mensajes cuyo significado está oculto; El criptoanálisis es la ciencia de romper mensajes cifrados (recuperar su significado). Muchos usan el término criptografía en lugar de criptología: es importante recordar que la criptología abarca tanto la criptografía y criptoanálisis.

Un cifrado es un algoritmo criptográfico. Un texto sin formato es un mensaje sin cifrar. El cifrado convierte el texto sin formato en texto cifrado. El descifrado devuelve un texto cifrado en un texto sin formato.

**Confidencialidad, integridad, autenticación y no repudio**

La criptografía puede proporcionar confidencialidad (los secretos permanecen secretos) e integridad (datos no se modifica de manera no autorizada): es importante tener en cuenta que no Proporcionar directamente la disponibilidad. La criptografía también puede proporcionar autenticación (prueba un reclamo de identidad).

Además, la criptografía puede proporcionar no repudio, lo cual es una garantía que un usuario específico realizó una transacción específica y que la transacción sí Sin cambio.

**CONCEPTOS DE DISEÑO SEGURO DEL SISTEMA**

El diseño seguro del sistema trasciende implementaciones específicas de hardware y software y representa las mejores prácticas universales.

**Capas**

Las capas separan la funcionalidad de hardware y software en niveles modulares. La complejidad de un problema, como leer un sector desde una unidad de disco, está contenida en una capa (la capa de hardware en este caso). Una capa (como la capa de aplicación) no es directamente afectado por un cambio a otro.

**SEGURIDAD ADMINISTRATIVA**

Un aspecto fundamental de la seguridad de las operaciones es garantizar que existan controles para inhibir a las personas comprometiendo inadvertidamente o intencionalmente la confidencialidad, integridad o disponibilidad de datos o los sistemas y medios que contienen esos datos. La seguridad administrativa proporciona los medios para controlar el acceso operativo de las personas a los datos.

**Etiquetas**

Los objetos tienen etiquetas y los sujetos tienen espacios libres. Las etiquetas de objeto utilizadas por muchos los gobiernos mundiales son confidenciales, secretos y de alto secreto. Según ejecutivo

Orden 12356 — Información de seguridad nacional,

* "alto secreto" se aplicará a la información, cuya divulgación no autorizada razonablemente podría esperarse que cause un daño excepcionalmente grave al país seguridad.
* "secreto" se aplicará a la información, cuya divulgación no autorizada razonablemente podría esperarse que cause graves daños a la seguridad nacional.
* "confidencial" se aplicará a la información, la divulgación no autorizada de que razonablemente podría causar daños a la seguridad nacional.

Las empresas del sector privado utilizan etiquetas como "Solo para uso interno" y "Empresa Propiedad."

**PANORAMA Y PROCESO DE BCP Y DRP**

Los términos y conceptos asociados con la continuidad del negocio y la recuperación ante desastres La planificación a menudo se malinterpreta. Comprensión clara de lo que se entiende por ambos Planificación de la continuidad del negocio y la recuperación ante desastres, así como lo que implican, es crítico para el CISSP candidato.

**Planificación de la Continuidad del Negocio**

Aunque muchas organizaciones simplemente usarán las frases Planificación de continuidad del negocio (BCP) o Planificación de recuperación ante desastres de manera intercambiable, son dos disciplinas distintas. El objetivo general de un BCP es garantizar que la empresa continuar operando antes, durante y después de un evento de desastre.

El enfoque de un BCP está en el negocio en su conjunto y en asegurar que aquellos críticos servicios que proporcionan el negocio o funciones críticas que el negocio regularmente las actuaciones aún se pueden llevar a cabo tanto después de una interrupción como después de que la interrupción haya sido resistida.