**Selecciono Denegación de servicios**

Puede ser explicado como un ataque a un grupo de computadoras o red con el objetivo de negar o inhabilitar un servicio o recurso para los computadores que consuman los mimos. Estos ataques suelen consistir en la saturación por medio de múltiples peticiones a un servidor para causar que el mismo no pueda dar respuesta a las solicitudes.

Sin embargo todos los tipos de ataques de denegación de servicio suelen utilizan el protocolo TCP/IP para lograr su cometido. Por otro lado estos se pueden clasificar por su objetivo final en 5 “tipos”: Obstrucción de medios de comunicación, Alteración de información de estado, Consumo de recursos computacionales, Interrupción de componentes físicos de la red y Alteración de información de configuración.

En este documento se centrara en la obstrucciones de métodos de comunicación entre el servidor y el cliente y de forma sutil tocara La alteración de información de configuración.

La obstrucción de métodos de comunicación consistirá en dificultar la comunicación del usuario por medio de internet al servidor, ente caso como el servidor estará representado por otra máquina en la misma red, el objetivo es vera evidenciado por la negación de la navegación en la red en la computadora cliente y la alteración de información de configuración consistirá en modificar las tabla ARP de la maquina cliente para que en su ruta de conexión al servicio de internet pases por el equipo atacante y este puede realizar la “obstrucción”.

En conclusión esta combinación de tipos de ataques permite inhabilitar un servicio fundamental como es la navegación por internet, lo cual de manera adyacente perjudica varios aspectos al computador servidor. Por o genera este combinación de ataques es transparente en la vista del cliente, ya que no hay ningún indicio de los cambios que se le realizo a la maquina desde otra máquina en la misma red. Por otro lado dependiendo de la complejidad del ataque este puede fácil de solucionar o muy complejo desde la computadora victima (usuario), lo que causaría que si el ataque es simple, la victima lo podría solucionar desde su maquina corrigiendo parámetros afectados por el ataque.

**Escenario frente a la temática seleccionada.**

El escenario consistirá en la negación de servicio de navegación por internet una o más páginas en la maquina victima Windows 8.1 la cual se encuentra en la misma red que maquina atacante kali Linux (virtualizada), la cual por medio de las herramientas como por ejemplo: ARP Spofing y Deloryan.py (con configuración extras de tablas de enrutamiento en la maquia atacante) se lograra el objetivo de Obstrucción de métodos de comunicación y la alteración de información de configuración en determinados casos que lo requieran. Tener en cuenta que ambas maquinas tienen acceso a internet por lo cual este servicio es usado frecuentemente por la víctima para comunicarse con servicios en la red que necesita.

**Funcionalidades de herramientas para resolver lo antes descritos.**

Las 5 herramientas seleccionadas son las siguientes:

1. Arp spofing / deloryan
2. Testing.pl
3. MVC/ ping
4. Loic(Low Orbit Ion Cannon)
5. Sloworris

La herramienta numero 1 consiste en la modificación de la fecha de la computadora victima por medio de hombre en el medio con el objetivo de invadir el redireccionamiento de paquetes del servicio de reloj por internet, Al hacer esto se lograra modificar la fecha tantos años en el futuros de la maquina victima que al navegar por internet los protocolos comenzaran a fallar y a restringir el ingreso a diferentes paginas debido a que no se es posible establecer protocolos necesarios para las misma páginas, a raíz de la fecha modificada.

La herramientas numero 2 consiste en la saturación por un puerto a un servidor el cual presta un servicio especifico por dicho puerto atacado, lo que se traduce en múltiples peticiones en un lapso de tiempo corto que causa la inhabilitación del servicio por ese puertos a las peticiones de clientes legítimos, debido a que esta respondiendo a las cientos de peticiones que le manda el tipo de ataque.

La herramienta numero 3 consiste en el envío de paquetes mediante el código ping por medio del cmd, Sin embargo en ese caso los paquetes se les puede modificar el peso en bit al igual que la cantidad de mensajes enviados en una cantidad de tiempo y tal vez lo mas importante el intervalo entre el envió del mensaje siguiente . Todo lo anterior se logra ejecutando el cmd como administrador y teniendo conocimiento de la ip de la víctima. Con la finalidad de saturar la ip y así lograr que deje de funcionar en condiciones óptimas.

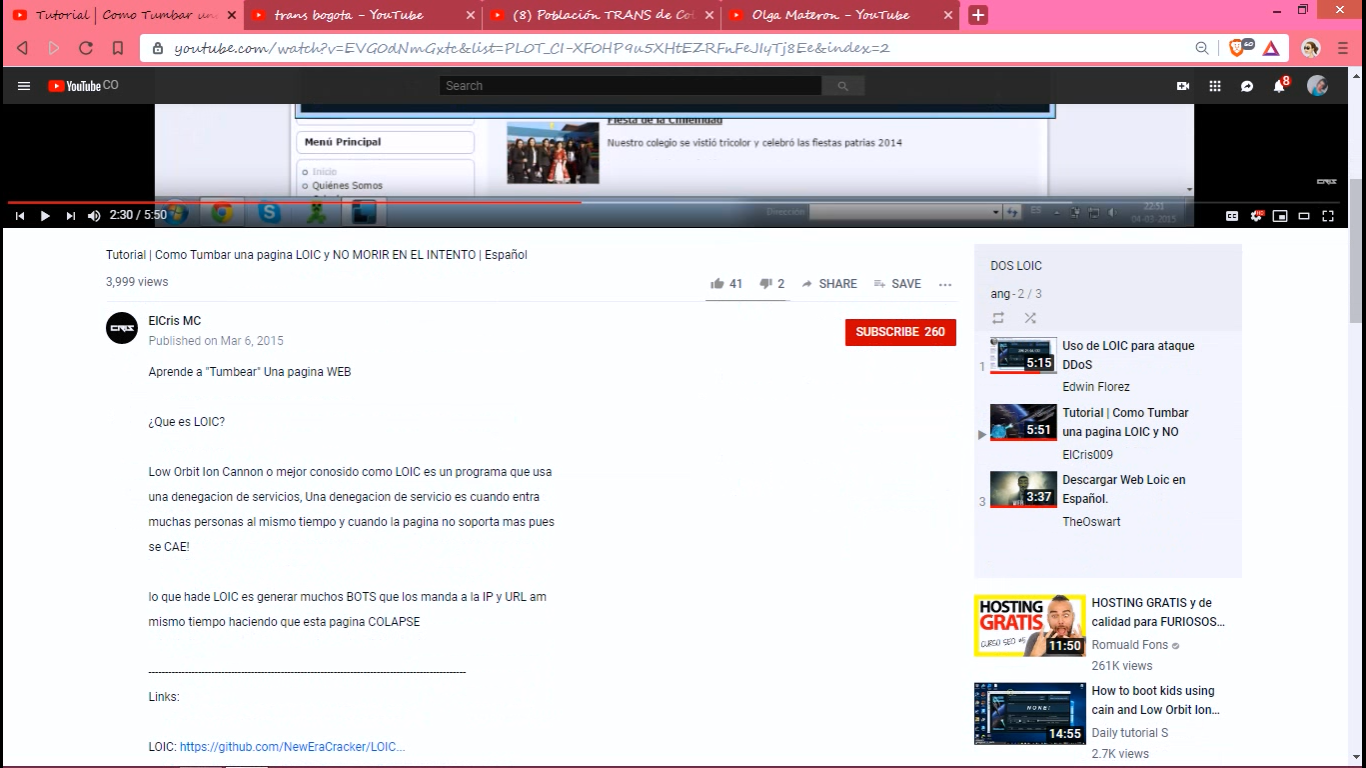
La herramienta numero 4 consiste en varias opciones de saturación a un ip y puerto en específico, las saturaciones pueden ser TCP, UDP y HTTP. Al igual que en casos anteriores, se envía una gran cantidad de solicitudes para que el servicio ligado a ese servidor y más específica, entente a ese puerto deje de funcionar de manera correcta y comience a sufrir caídas en el mismo.

La herramienta numero 5 consiste en el envío de paquetes aun mismo puerto dentro de un ip, con el objetivo de saturar de peticiones el puerto y denegar el servicio que este otorgando.

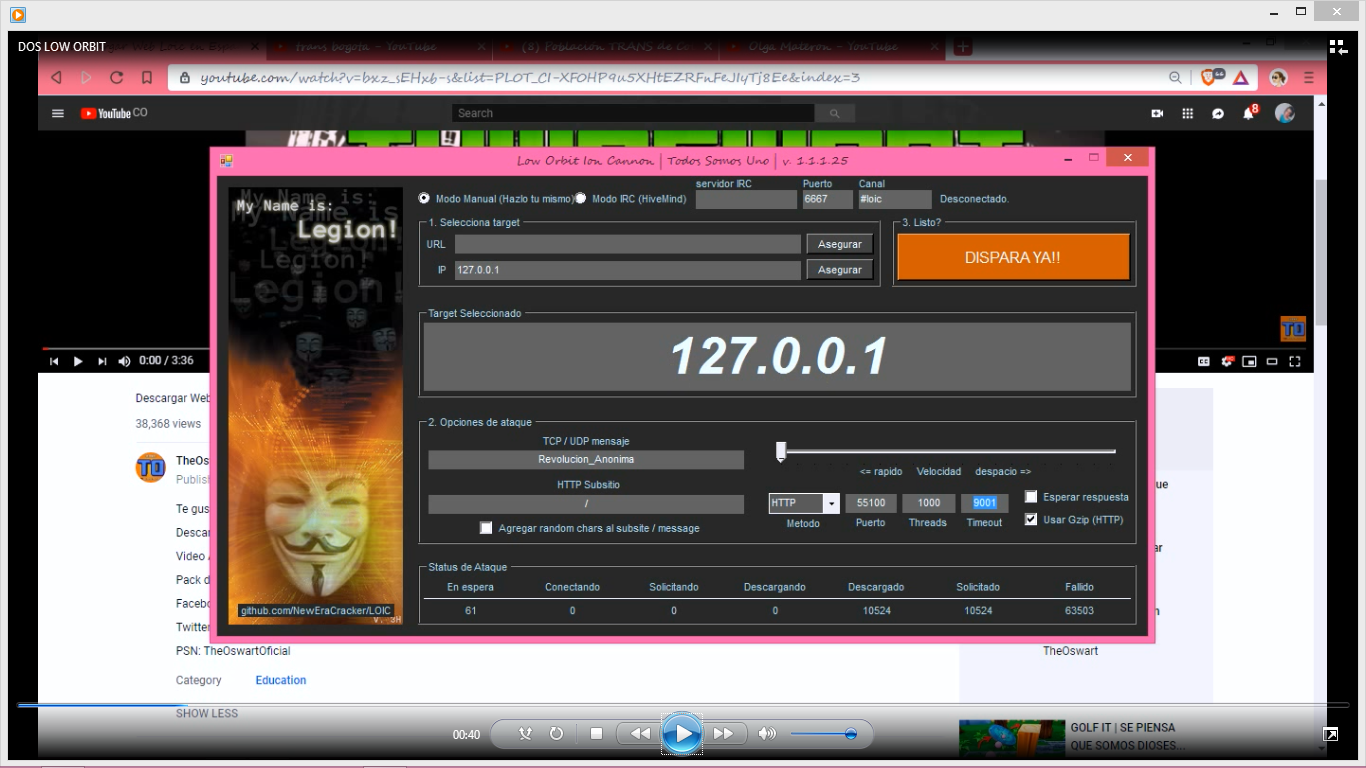
**Demostración ´practica de dos herramientas.**

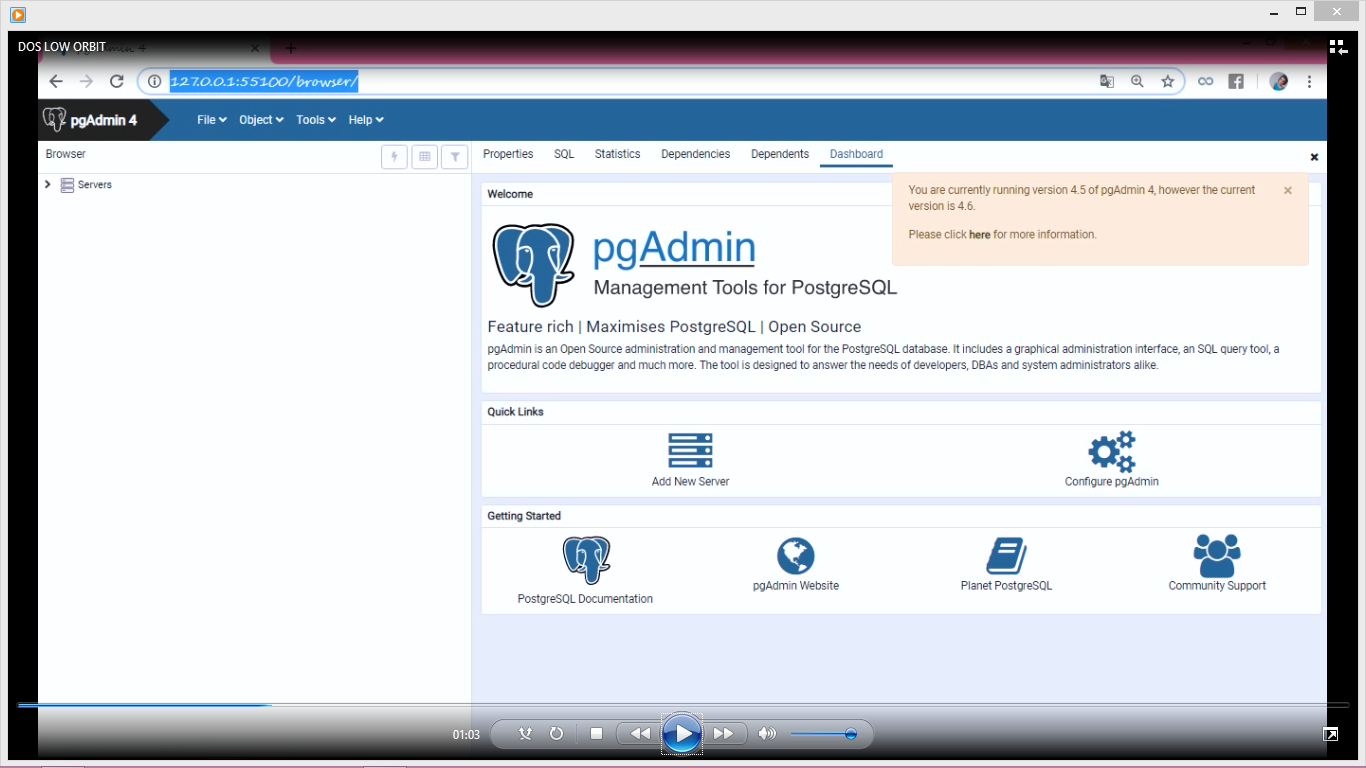
**Low Orbit Ion Cannon**

La siguiente imagen corresponde al video seguido para realizar este DOS, donde se negó el servicio de la pagina local host, la cual en este caso está siendo usada para la gestión de una base de datos postgresql que esta alojada en un servidor centos en la misma LAN



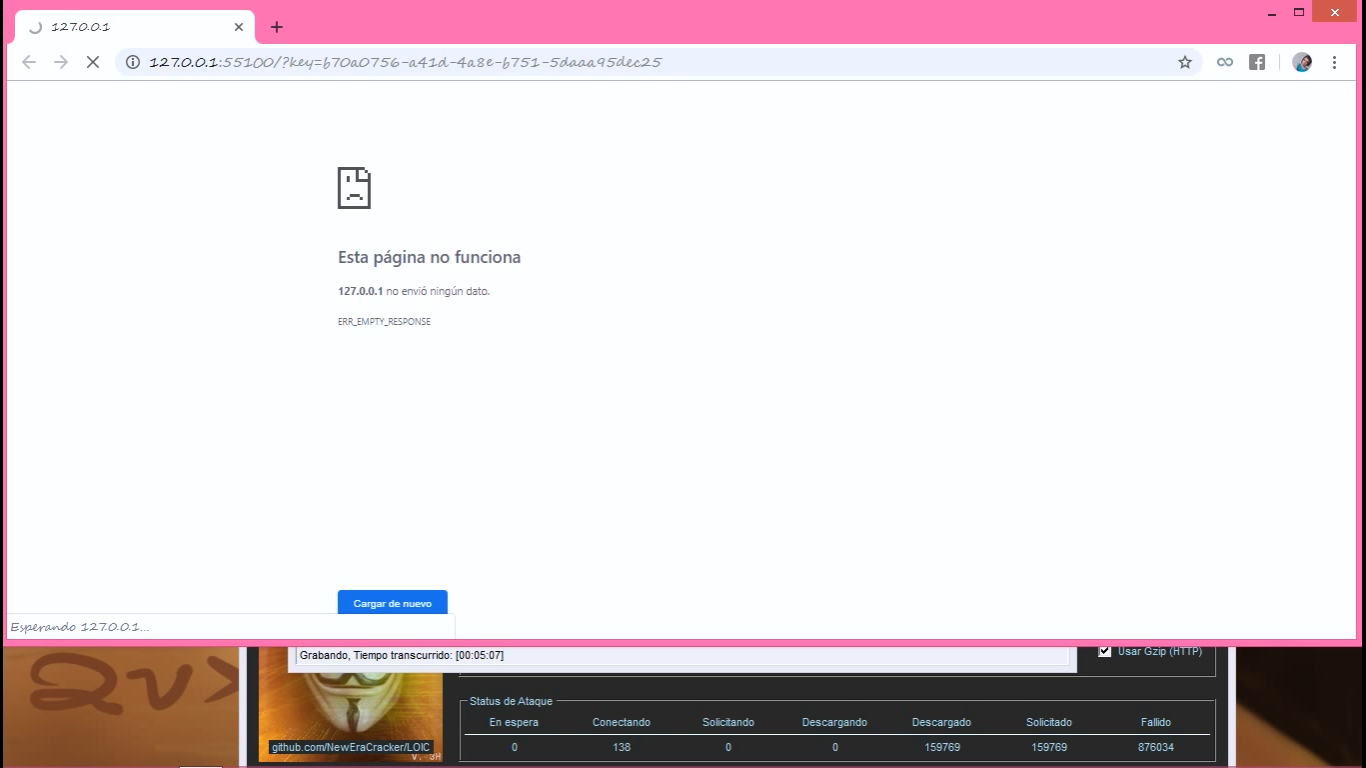
Esta es la herramienta utilizada y donde solo toca especificar la ip y port a atacar en la parte de abajo , este tiene varias opciones de ataque sin embargo utilizaremos el modo HTTP y desmarcaremos la opcion de esperar respuesta , con esto configurado podemos iniciar el ataque con el boton “Disparar ya”



En la siguiente imagen comprobamos el servicio que se encuantra alojado en el localhost con su respectivo puerto, en su estado optimo cuando aun no ha sido atacado.

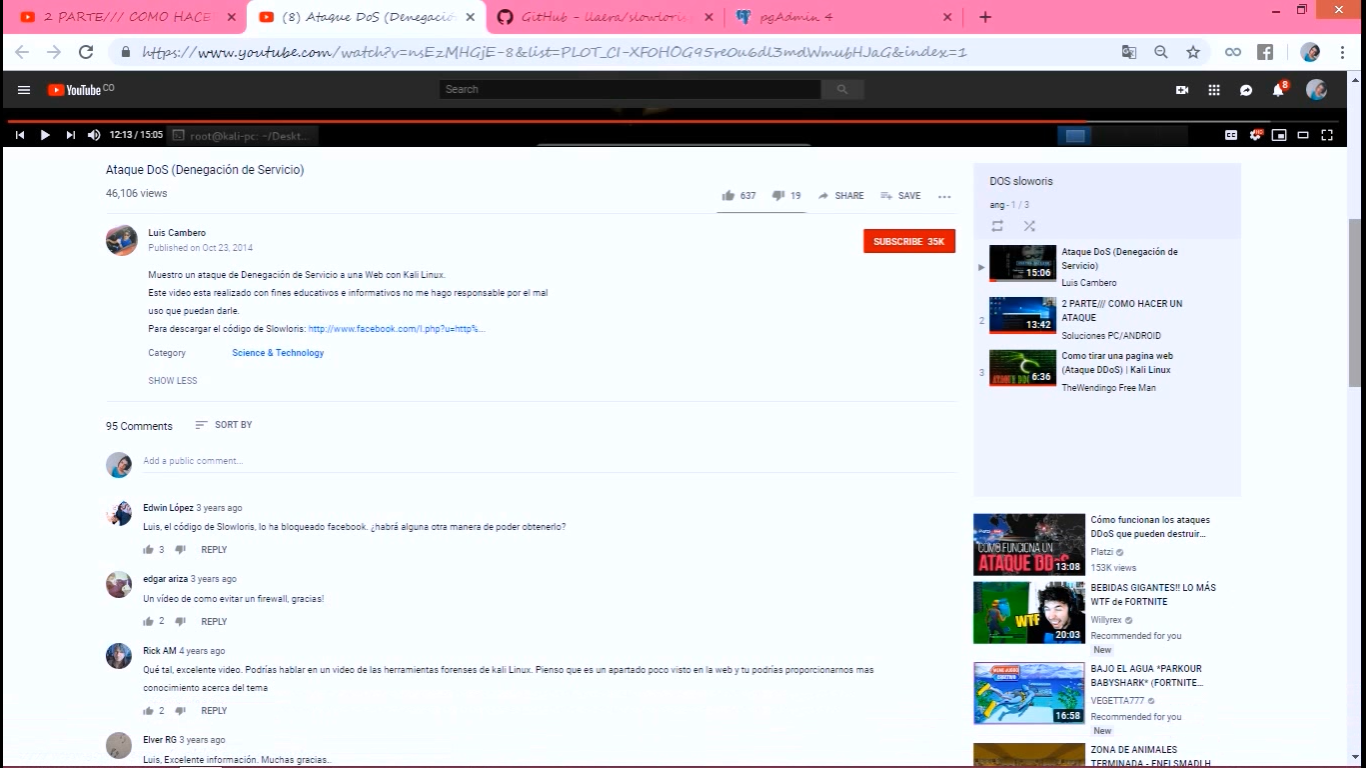
En la siguiente imagen podemos ver el servidor centos 7x , donde se encuentra alojado el servicio de postgresql

En la siguiente imagen al intentar reingresar al localhost, podemos ver que ya ha sido inabilitado por el ataque.

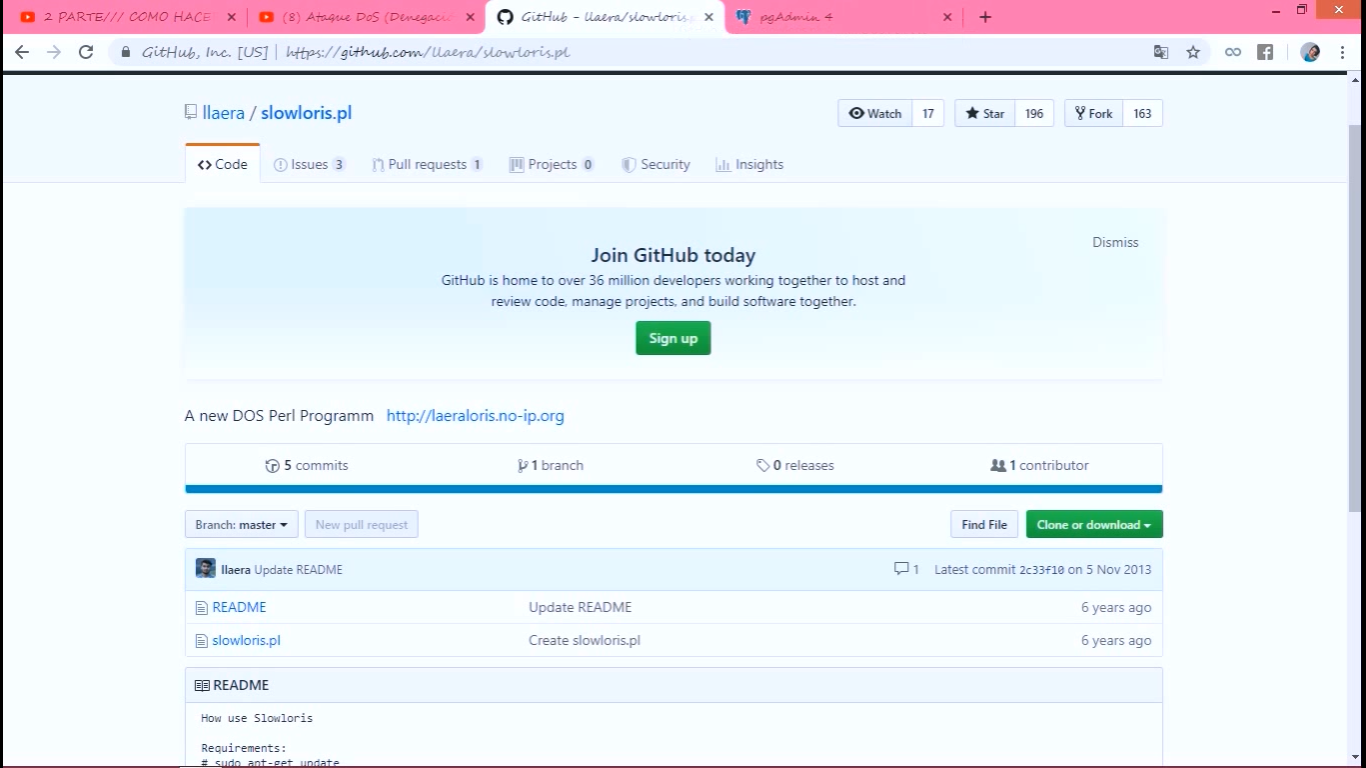


**Sloworris**

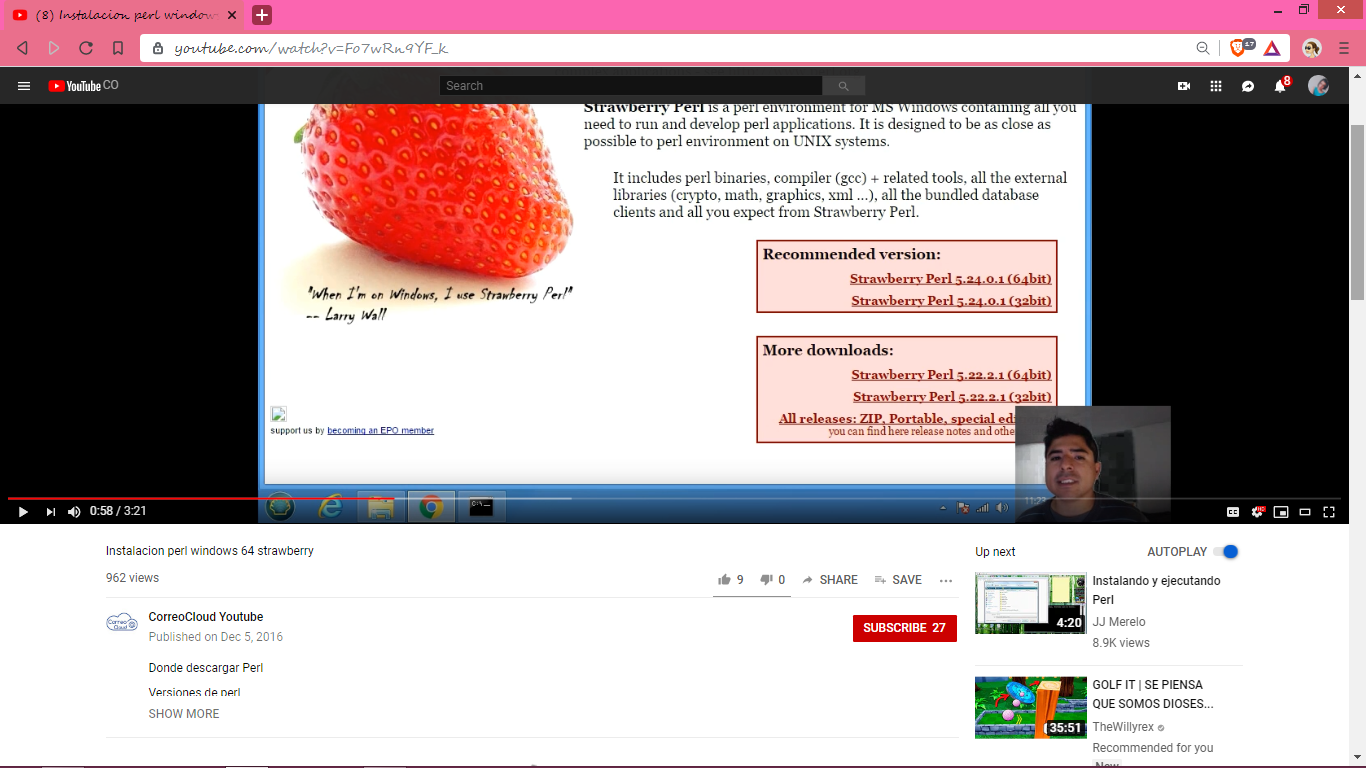
La siguiente imagen corresponde al video seguido para realizar este DOS, donde se negó el servicio de la página local host, la cual en este caso está siendo usada para la gestión de una base de datos postgresql que esta alojada en un servidor centos en la misma LAN



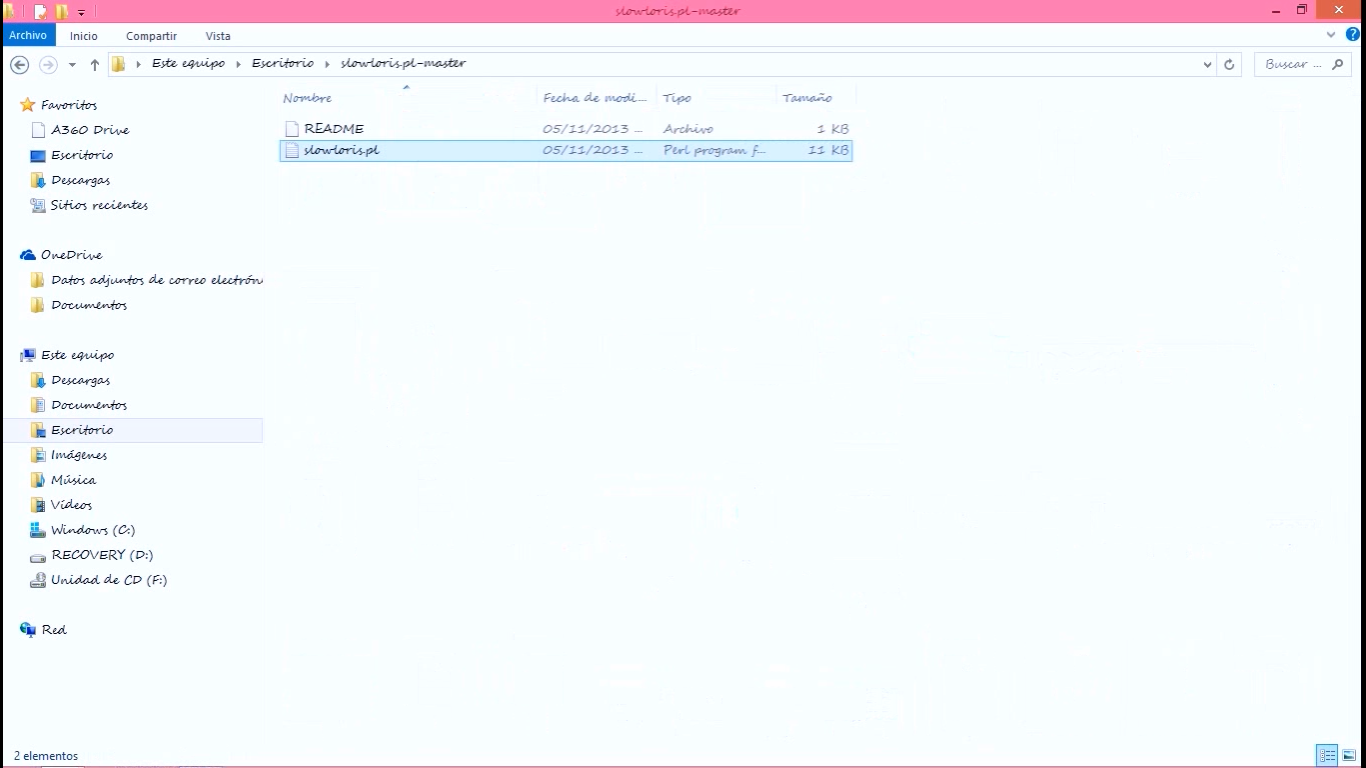
La siguiente imagen corresponde al repositorio de donde se descargo la herramienta a usar.

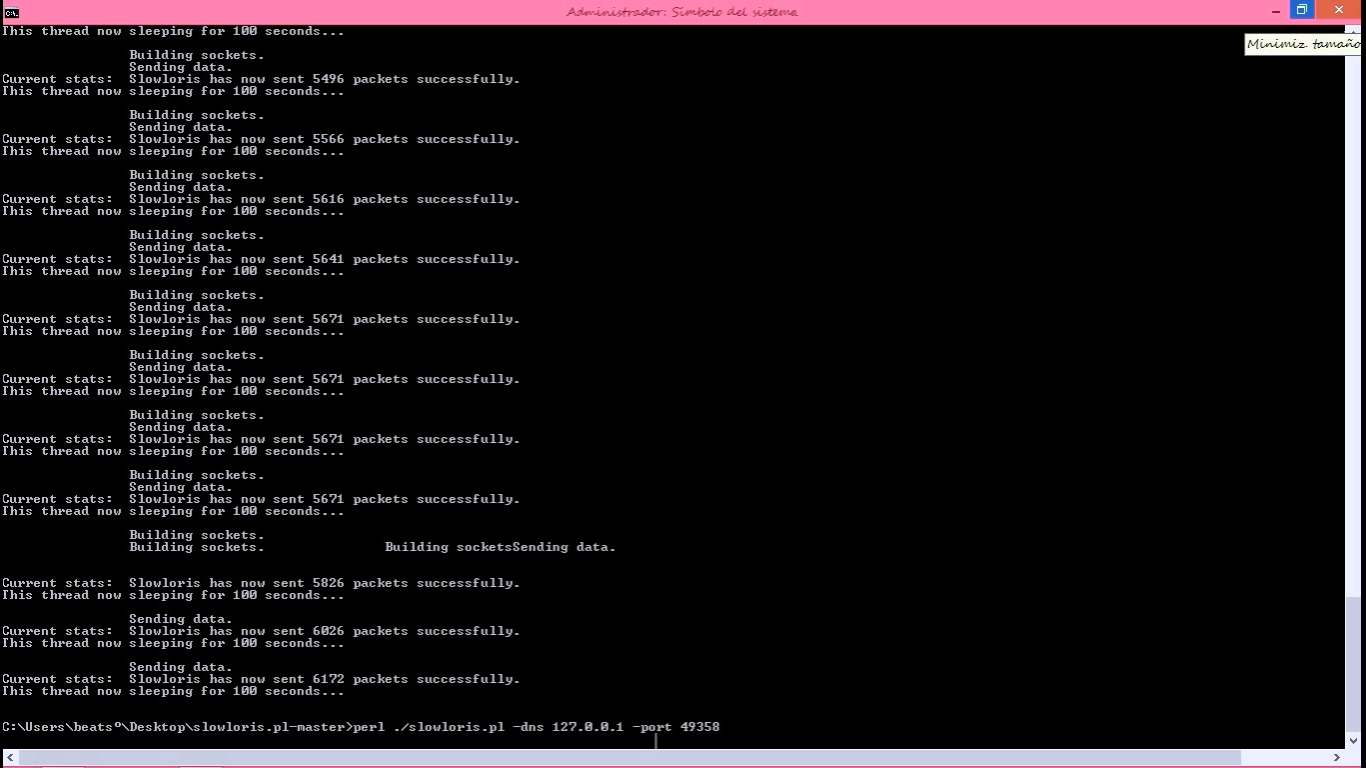


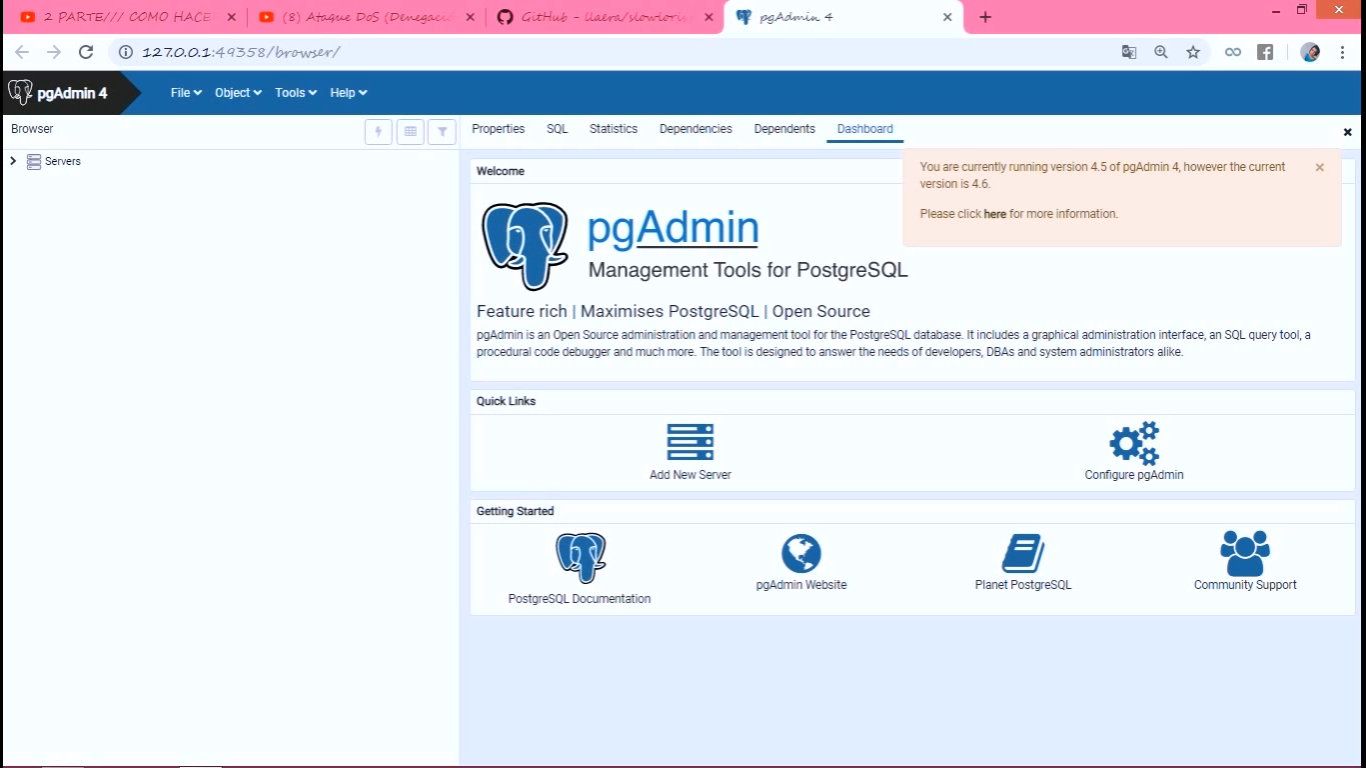
En la siguiente imagen se evidencia el video que se siguió para la instalación de una herramienta extra, la cual es perl. Para poder ejecutar la aplicación que nos permitirá realizar el ataque.

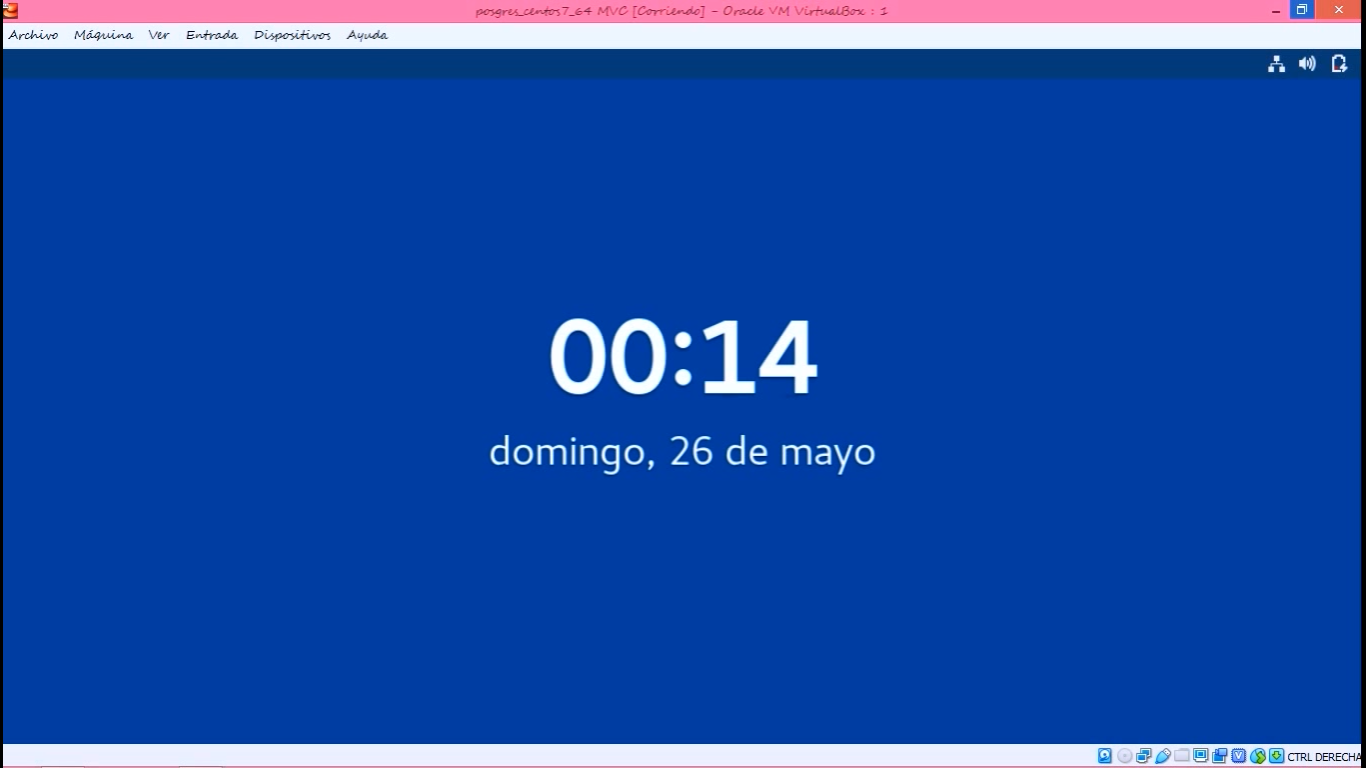


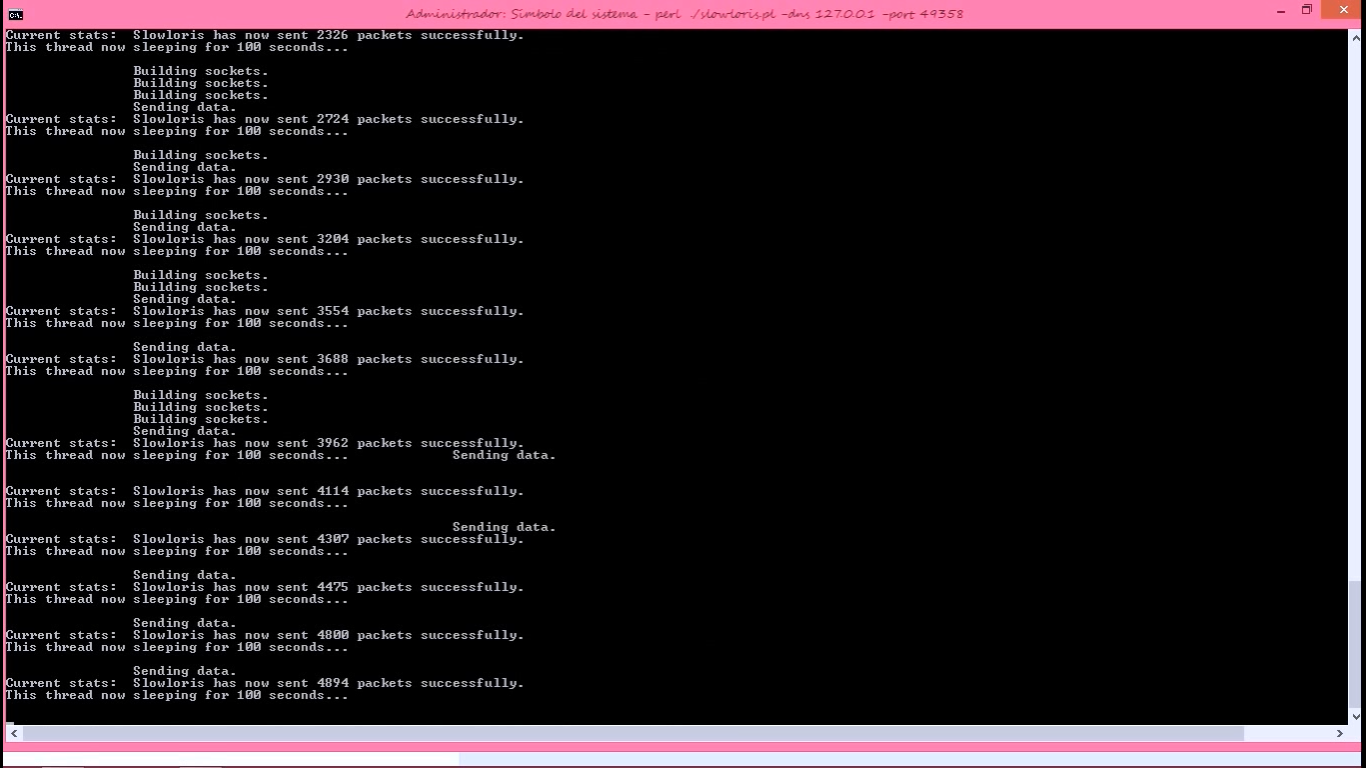
En la siguiente imagen se evidencia la ubicación de la herramienta que nos permitirá hacer el ataque.



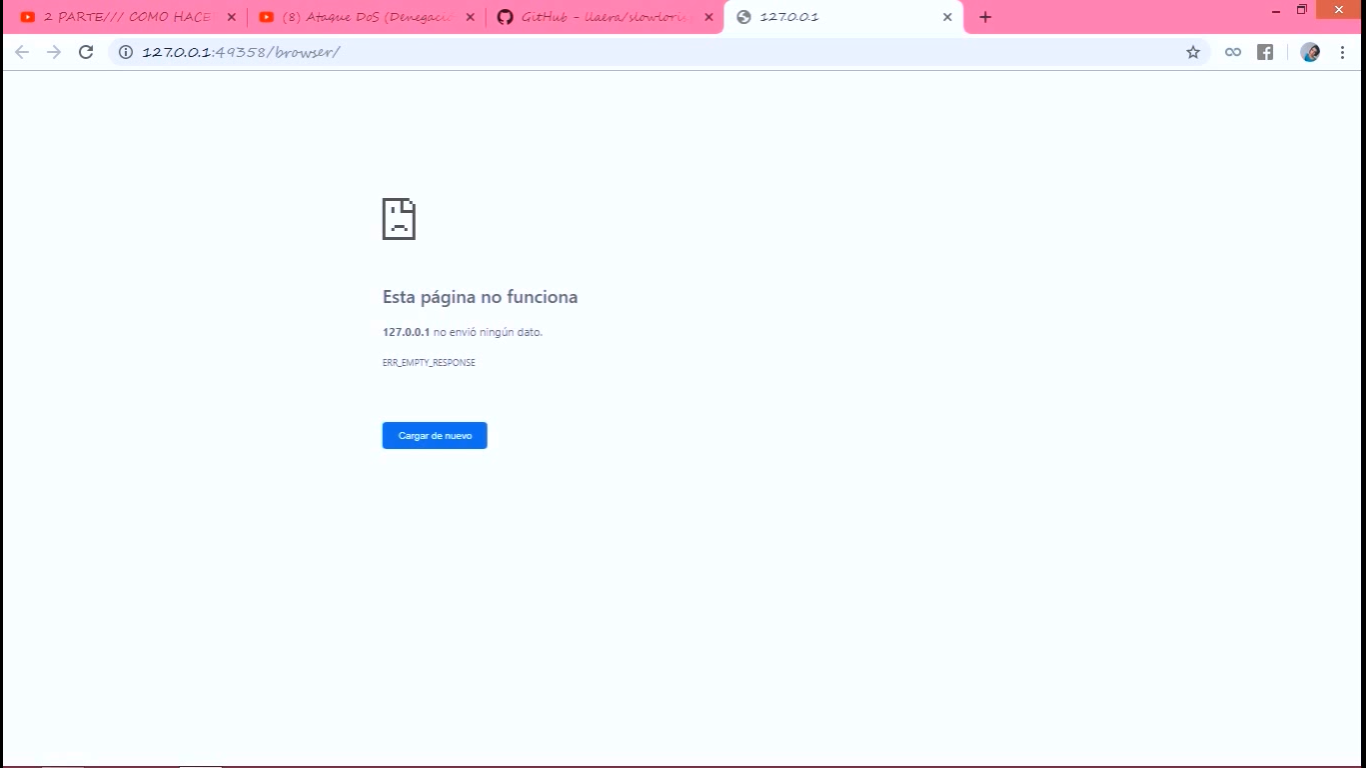
En la siguiente imagen se evidencia que nos encontramos en la misma ruta que la aplicación descargada y que se ejecuta con el comando que se ve en consola donde se indica la ip y el puerto. En este caso es local host y el puerto por donde se comunica pg Admin, gestor grafico remoto de postgresql,

La siguiente imagen muestra el servicio ubicado en local host con su respectivo puerto. En su estado optimo antes del ataque.

En la siguiente imagen se evidencia el servidor Centos que aloja el servicio de postgresql.

En la siguiente imagen se evidencia lo que debe mostrar el cmd cuando se ejecuta el ataque y ya esta en marcha la denegación.

En la siguiente imagen se puede evidenciar el servicio denegado de local host.

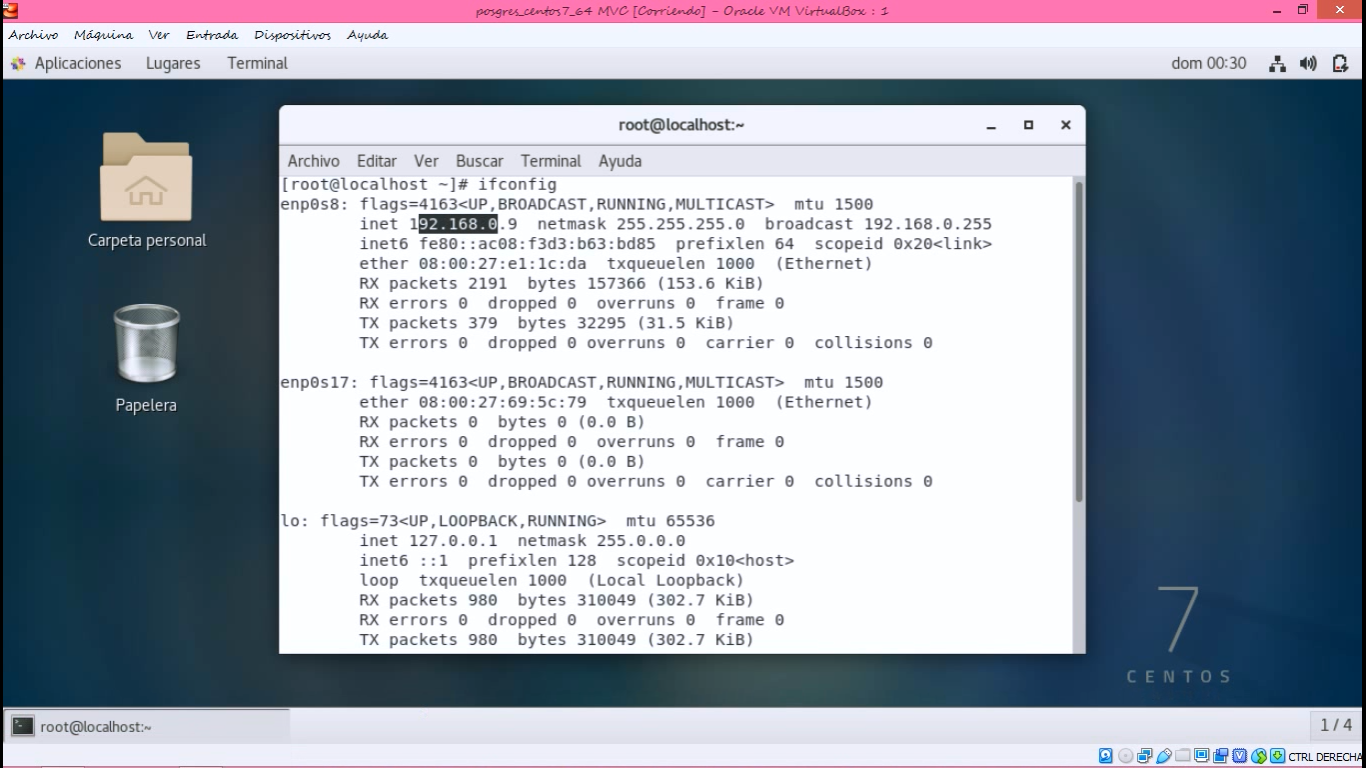


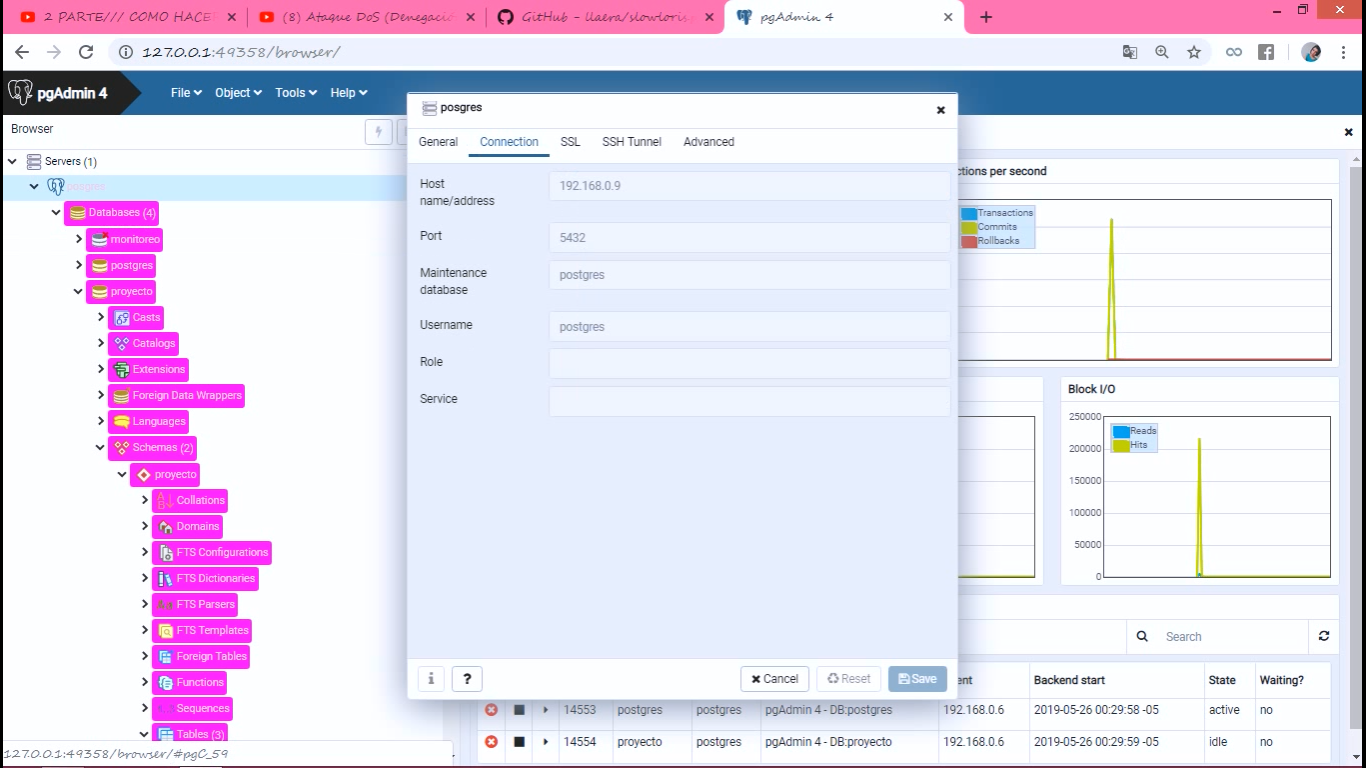
**Mismo escenario pero en escenario cliente servidor**

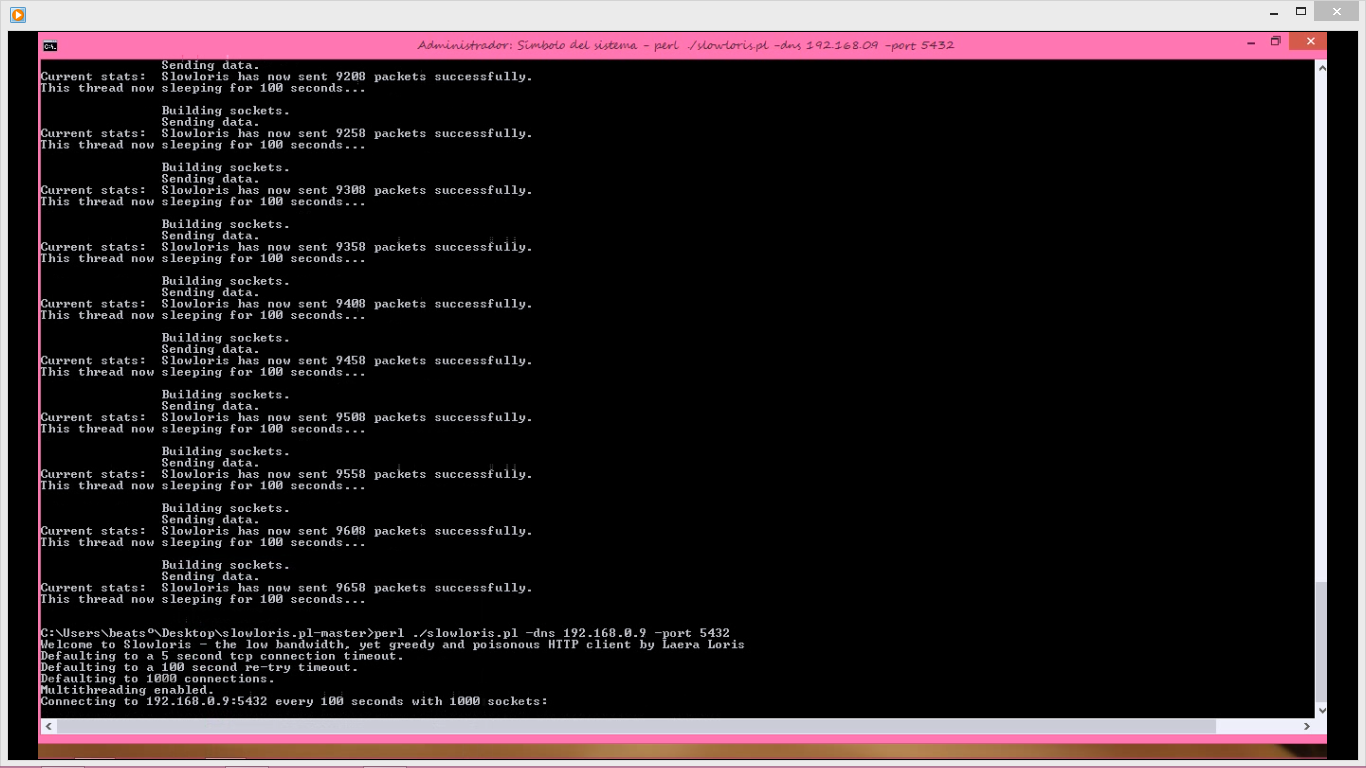
**Sloworris**

Debido a que es la misma herramienta utilizada en los ataques anteriores solo se explicara las diferencias que se tienen que ejecutar en este caso.

En la siguiente imagen se muestra la ip de nuestro servidor que brinda el servicio de postgresql a al cliente.



En la siguiente imagen se muestra como el cliente esta conectado a el servidor y su puerto respectivo.

Utilizando el puerto y la direccion ip del servidor la cual se encuentra en la misma red que el cliete se procede a hacer el ataque como se evidencia en la ventana del cmd. Al ejecutarse se denegara el servicio.

Por ultimo, despues de ejecutado el ataque lo que veremos es inactividad del servicio postgresql en la ventana de estadisticas lo que nos indicas que no esta pasando nada en el, cuando en realidad es que el puerto esta saturado y es por ello que el mismo no nos reporta la informacion que le estamos solicitando desde el cliente.