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.

****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.

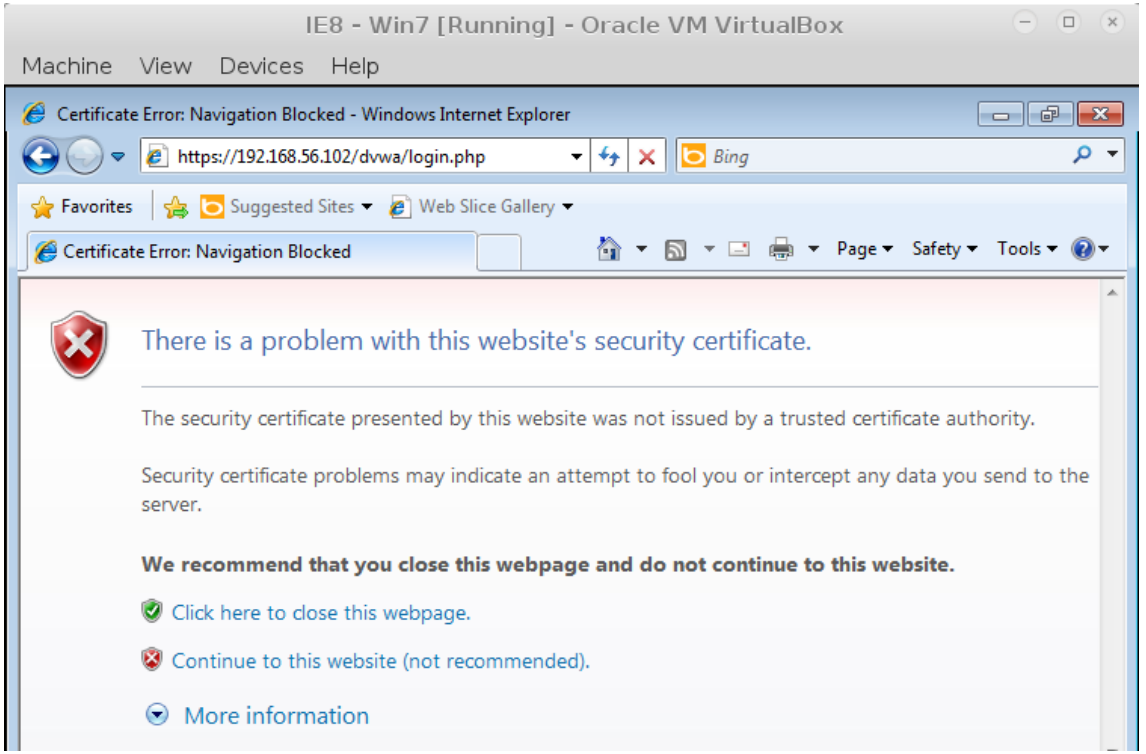
```
# sslsplit -D -l connections.log -j /tmp/sslsplit -S logdir -k

certaauth.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: http**s**://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

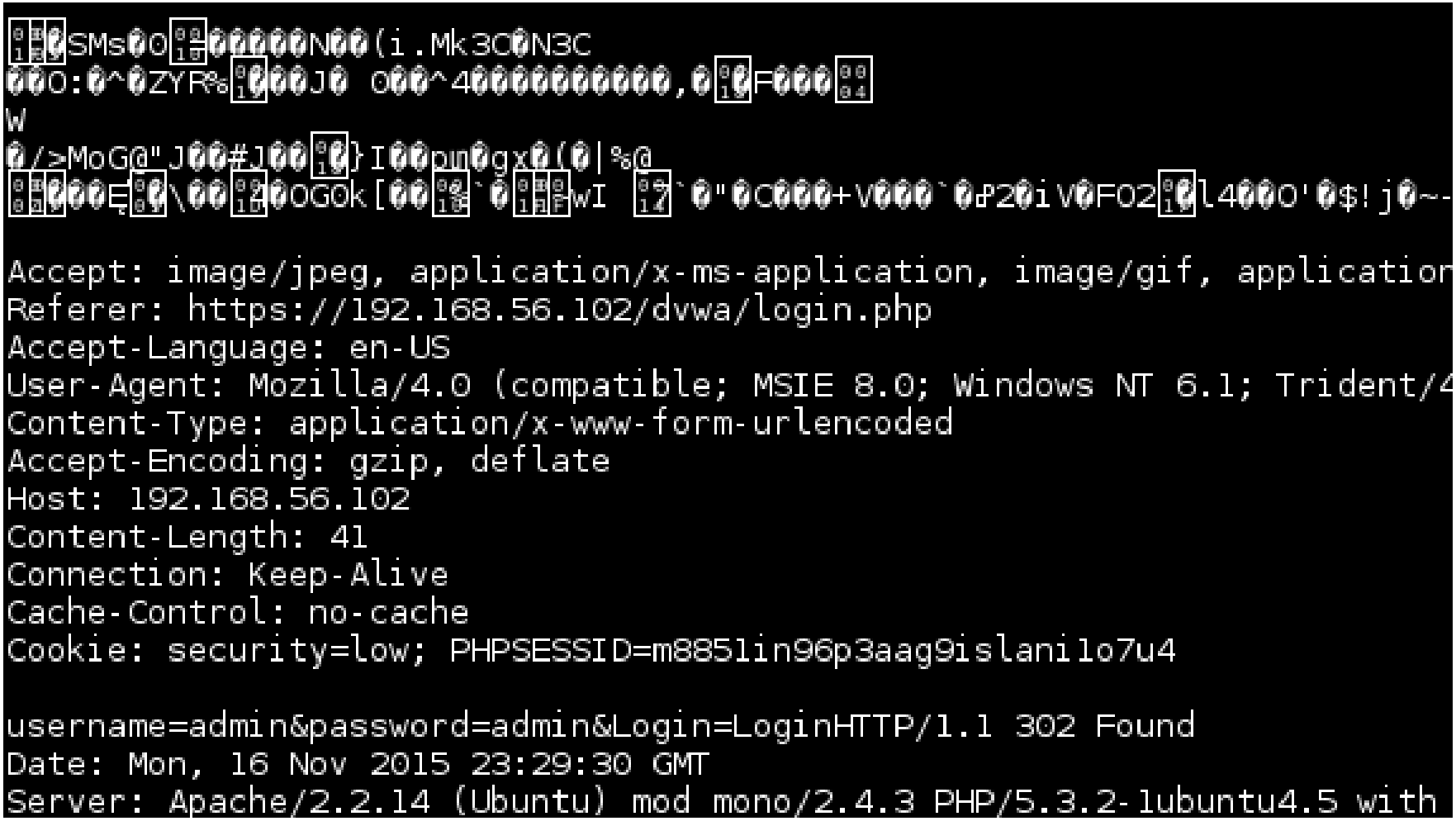
Agora inicie sessão no DVWA utilizando o admin na senha e login

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



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.