Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

O Ettercap pode detectar quando as informações relevantes como senhas são transmitidas através dele. No entanto, muitas vezes não é suficiente para interceptar um conjunto de credenciais ao realizar um teste de penetração, podemos estar à procura de outras informações como números de cartão de crédito, números de segurança social, nomes, fotos ou documentos.

Capturar o tráfego com o Wireshark

Portanto, é útil ter uma ferramenta que possa pegar todo o tráfego na rede para que possamos salvá-lo e analisá-lo mais tarde; Esta ferramenta é um sniffer e o melhor para os nossos propósitos é Wireshark e está incluído no Kali Linux.

Capturar o tráfego com o Wireshark

Nesta aula, vamos usar o Wireshark para capturar todos os pacotes enviados entre o cliente e o servidor para obter informações relevantes.

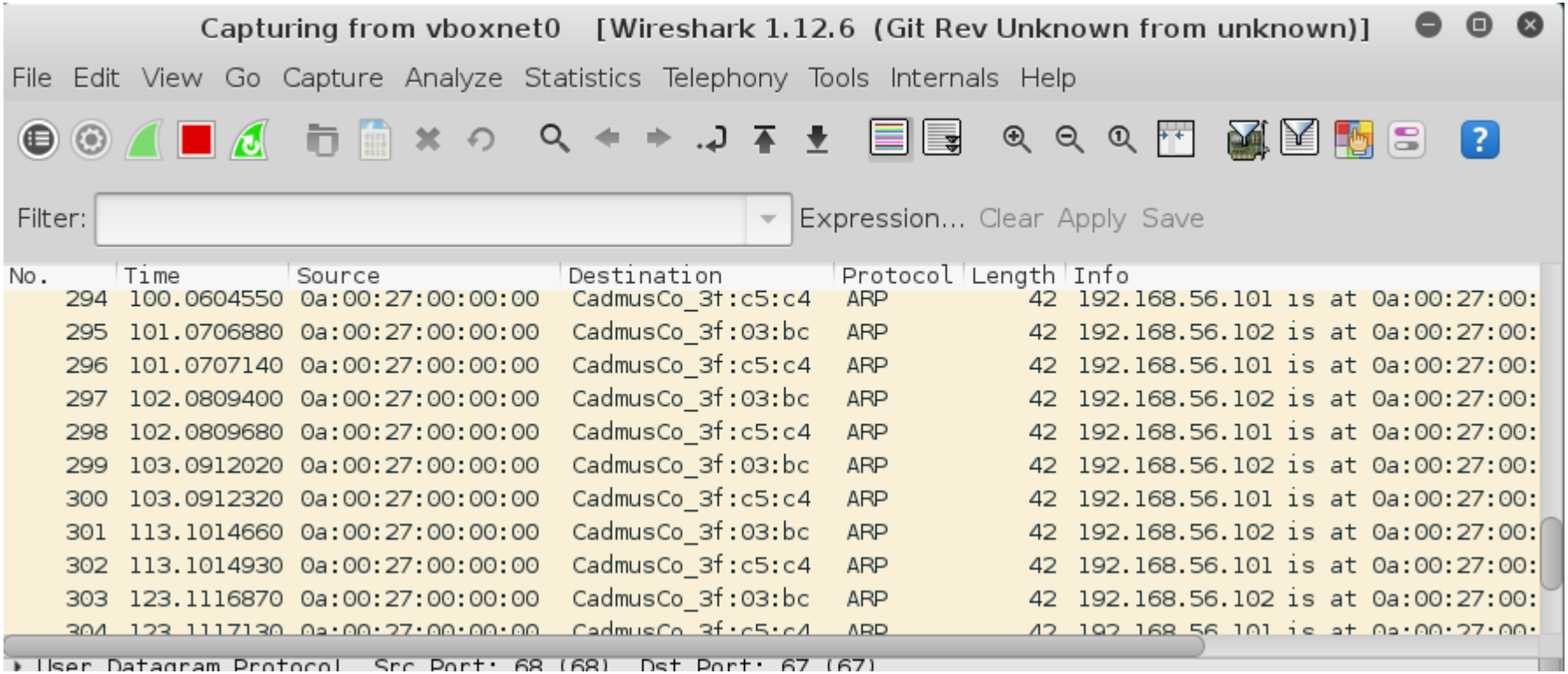
Capturar o tráfego com o Wireshark

Abra o wireshark pelo comando do terminal:

```
# wireshark
```

Capturar o tráfego com o Wireshark

Quando Wireshark carrega, selecione a interface de rede da qual você deseja capturar pacotes. E depois clique em **Start**



Capturar o tráfego com o Wireshark

Agora, vá para a máquina virtual e navegue para

http://192.168.1.X/dvwa e inicie sessão no **DVWA** e escreva o

login e senha.

Capturar o tráfego com o Wireshark

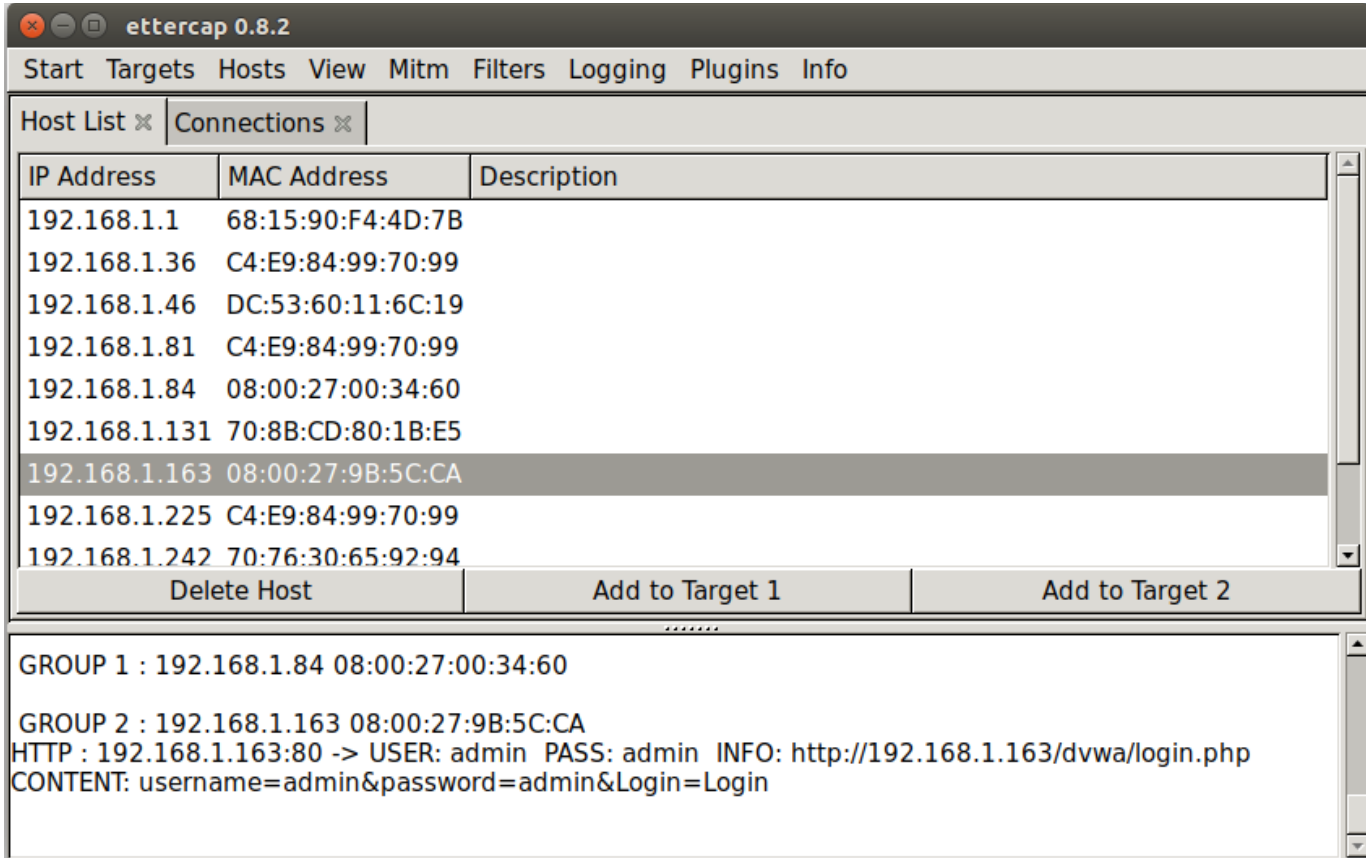
No Wireshark, procure um pacote HTTP de IP de sua máquina virtual para o DVWA com POST /dvwa/login.php no seu campo info.

Capturar o tráfego com o Wireshark

Se olharmos através de todos os pacotes capturados, vamos encontrar o que correspondente à autenticação e visualizar o que foi enviado em texto claro para que possamos obter o nome de usuário e senha.

Capturar o tráfego com o Wireshark

Se nos usarmos o Ettercap para ver as credenciais, também podemos visualizar.



Estudar os dados do Wireshark é um pouco cansativo, por isso é muito importante aprender a usar os filtros de exibição para capturar os pacotes. Você pode acesar os seguintes sites para saber mais:

https://www.wireshark.org/docs/wsug_html_chunked/ChWorkDisplayFilterSection.html

https://wiki.wireshark.org/DisplayFilters

https://wiki.wireshark.org/CaptureFilters