Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Configurando um ataque de spoofing com Ettercap

O spoofing de Protocolo de Resolução de Endereços (ARP) é talvez o ataque MITM mais comum. Baseia-se no fato de que o protocolo de resolução de endereços - aquele que converte endereços IP em endereços MAC - não verifica a autenticidade das respostas recebidas por um sistema.

Isto significa que, quando o computador pede a todos os dispositivos na rede, "qual é o endereço MAC da máquina com IP xxx.xxx.xxx.xxx", ele acreditará na resposta que recebe de qualquer dispositivo, seja ele o **servidor desejado ou não**, o spoofing ARP ou o ARP poisoning funciona através do envio de lotes de respostas ARP para ambas as extremidades da cadeia de comunicações, dizendo a cada um que o endereço MAC do invasor corresponde ao endereço IP de sua contraparte.

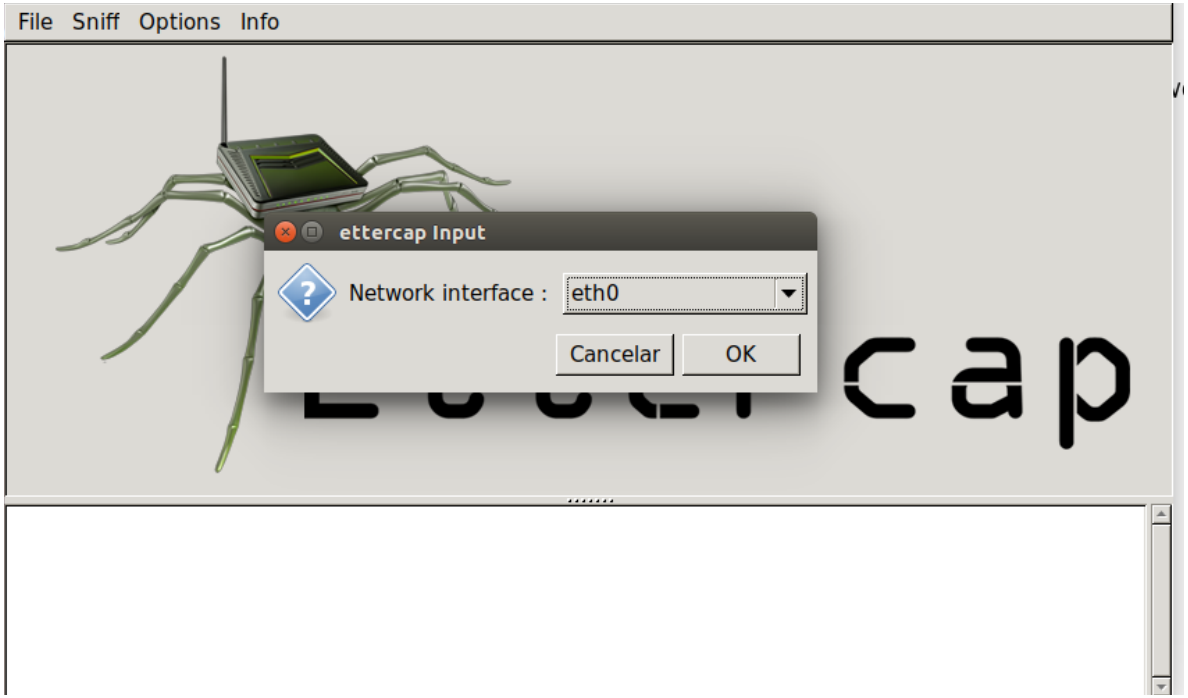
Configurando um ataque de spoofing com Ettercap

Nessa aula, vamos usar 2 máquinas virtuais para o nosso ataque. Com ambas as máquinas virtuais em execução, o nosso host Kali Linux será a máquina atacante. Abra um terminal e execute o seguinte comando.

```
# ettercap -G
```

Configurando um ataque de spoofing com Ettercap

No menu principal do Ettercap, selecione **Sniff | Unified Sniffing.** No pop-up selecione a interface de rede que você deseja usar.

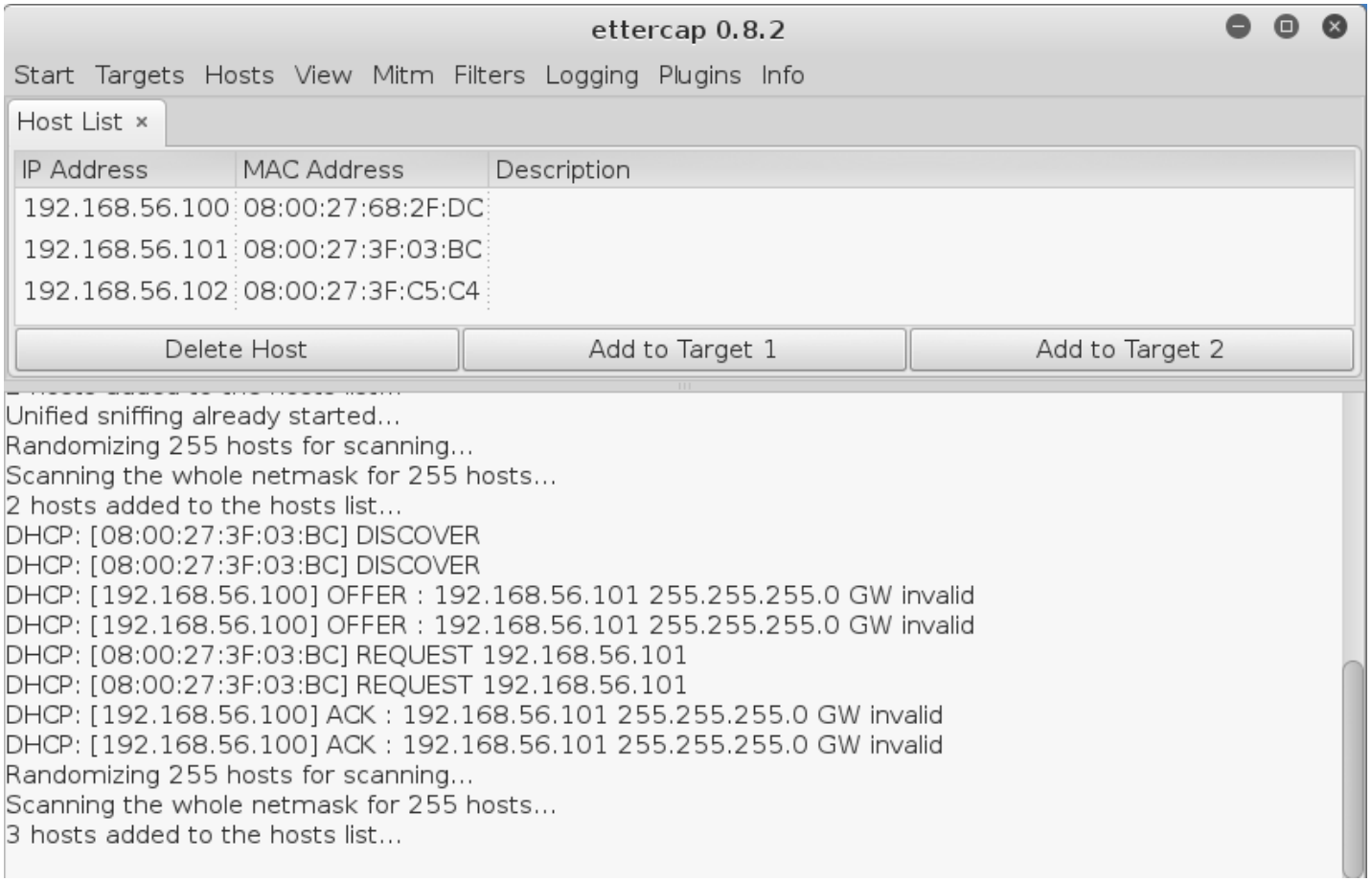


Configurando um ataque de spoofing com Ettercap

Agora que estamos vasculhando a rede, o próximo passo é identificar quais hosts estão se comunicando. Para fazer isso, vá para **Hosts** no menu principal e, em seguida, **Scan for hosts**.

Configurando um ataque de spoofing com Ettercap

A partir dos hosts que encontramos, vamos selecionar nossos alvos. Para fazer isso no menu **Hosts**, selecione **Hosts list**:



Na lista, selecione 192.168.1.x e clique em **Add to Target 1**

Em seguida, selecione 192.168.1.x e clique em **Add to Target 2**

Agora vamos verificar os alvos: no menu **Targets**, selecione

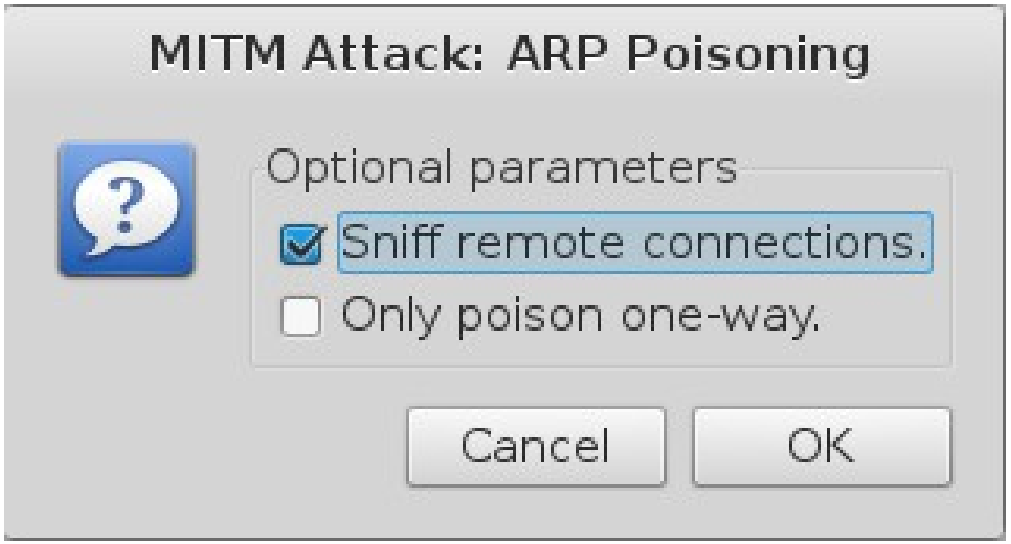
Current targets:

Configurando um ataque de spoofing com Ettercap

Agora estamos prontos para iniciar o ataque de spoofing e posicionar-nos entre o servidor e o cliente. No menu **Mitm**, selecione **ARP poisoning**

Configurando um ataque de spoofing com Ettercap

Na janela *pop-up*, marque a caixa **Sniff** conexões remotas e clique em **OK**



Configurando um ataque de spoofing com Ettercap

E é isso, agora podemos ver todo o tráfego entre o cliente e o servidor.