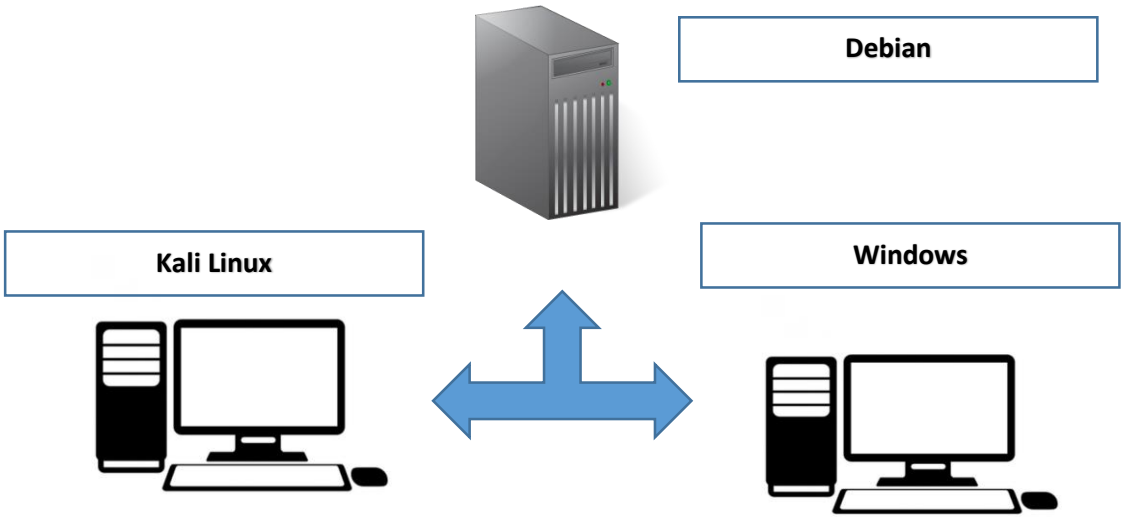
ARP Spoofing

Descrição:

O ARP Spoofing é o comprometimento na segurança ou na integridade da tabela ARP. O objetivo dessa técnica é modificar o endereço na tabela ARP. Para essa técnica vamos utilizar a ferramenta Ettercap. O Ettercap é um conjunto abrangente para o homem nos ataques do meio. Ele apresenta sniffing de conexões ao vivo, filtragem de conteúdo em tempo real e muitos outros truques interessantes. Suporta a dissecação ativa e passiva de muitos protocolos e inclui muitos recursos para análise de rede e host.

Cenário:



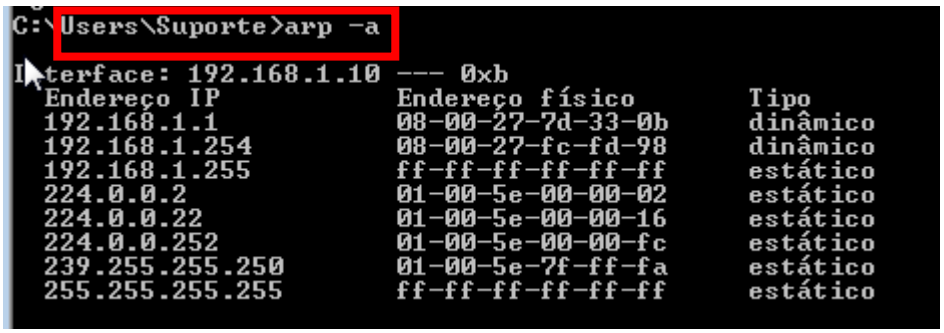
Criar uma Máquina Kali com as mesmas configurações da aula anterior, Placa Interna IP: 192.168.1.254

Criar uma Máquina Windows Professional 32Bits, **Placa Interna IP: 192.168.1.10 – GATEWAY 192.168.1.1!**

Criar uma máquina Debian Server 32 Bits, Placa Interna IP: 192.168.1.1

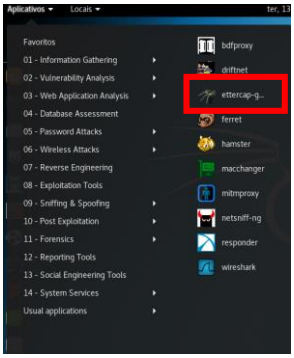
ARP

1. Na máquina Windows analise a tabela arp com o seguinte comando no cmd:

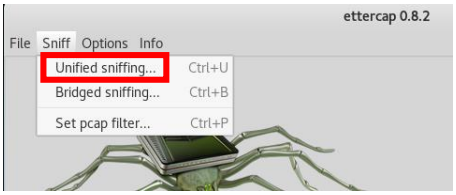


O Comando analisa a tabela arp que está no Windows atualmente, ou seja, mostra exatamente quais são os hosts conhecido pelo Windows, com informações de IP e endereço MAC.

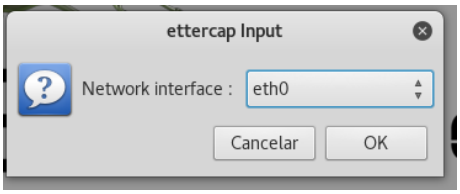
2. Na máquina Kali acesse a aplicação Ettercap:



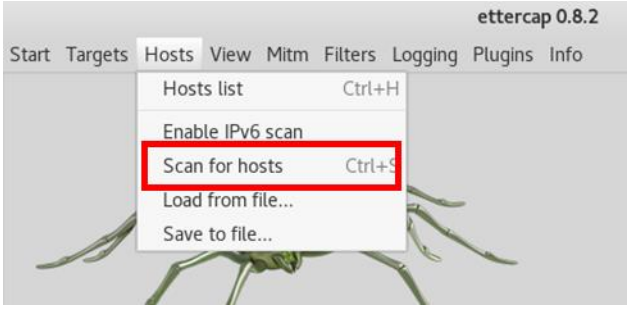
3. Clique em Sniff > Unified sniffing:



4. Selecione a Interface de Rede> eth0 (Essa informação vai depender da sua interface de rede):



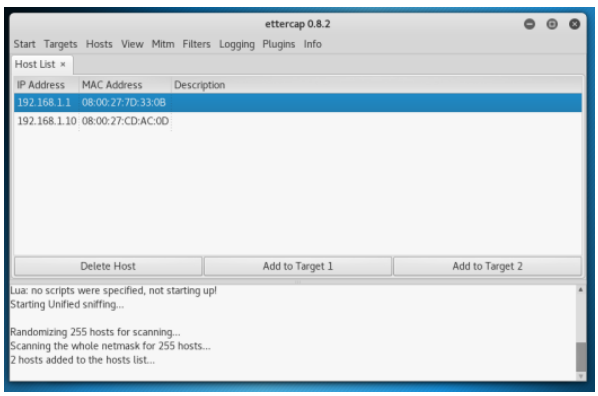
5. Clique em Hosts > Scan for hosts



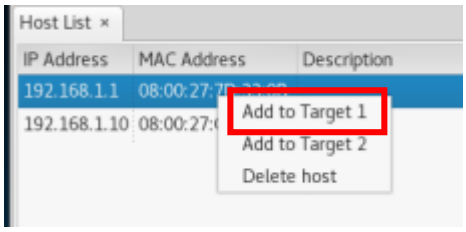
Esse processo demora um pouco pois será feito uma varredura em todos os hosts da rede.

6. Clique em Hosts > Hosts list para visualizá-los

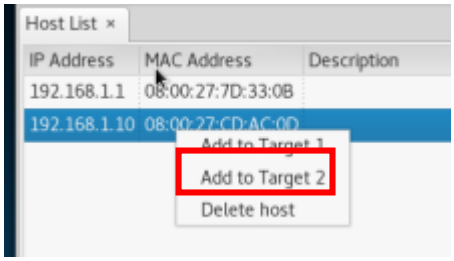
Assim que concluir a verificação ele dará uma lista de host. (SERÁ LISTADO OS DOIS HOSTS O SERVIDOR E A MÁQUINA CLIENTE).



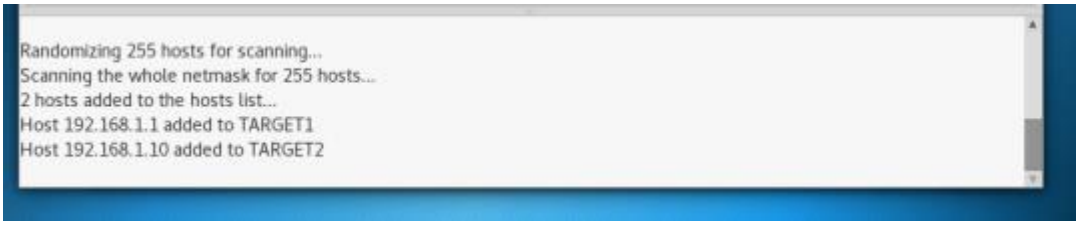
7. Nessa etapa deveremos selecionar o IP do GATEWAY e adicionar com “ADD Target 1”.



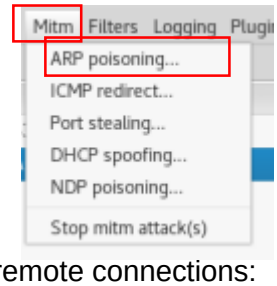
8. Nessa etapa devemos selecionar o IP da vítima (Windows) e adicionar com “ADD Target 2”.



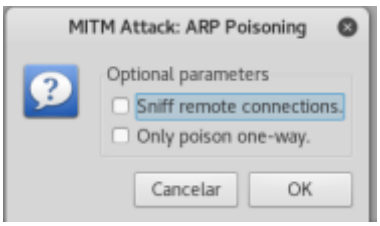
9. O resumo ficará assim:



10. Agora vamos ao ataque de ARP, você deverá selecionar a opção. Clique em Mitm > Arp poisoning:



11. Selecione a opção Sniff remote connections:



12. Será criado 02 grupos de vítimas:

13. Retorne a máquina Windows e verifique a tabela ARP, verifique a tabela arp e veja que todo o direcionamento passa para o MAC do Atacante.