Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

DNS spoofing

A falsificação de DNS é um ataque no qual a pessoa que executa o ataque MITM para alterar a resolução do nome na resposta do servidor DNS para a vítima, enviando-os para uma página maliciosa em vez de para a que eles solicitaram enquanto ainda usava o nome legítimo.

DNS spoofing

Nesta aula, vamos usar o Ettercap para realizar um ataque de spoofing DNS e fazer a vítima visitar o nosso site quando eles realmente queriam visitar um site diferente.

DNS spoofing

Vamos usar a nossa máquina virtual de cliente Windows, mas desta vez com o adaptador de rede em ponte para consultar a resolução DNS. Seu endereço IP será 192.168.1.84

DNS spoofing

A máquina atacante será a nossa máquina Kali Linux com o endereço IP 192.168.1.144. Ele também precisará ter um servidor Apache em execução e ter uma página demo index.html, o nosso vai conter o seguinte:

```
<h1>Spoofed SITE</h1>
```

DNS spoofing

Supondo que já tenhamos o nosso servidor Apache em execução e o site falso configurado corretamente, vamos editar o arquivo /etc/ettercap/etter.dns para que ele contenha somente a seguinte linha.

* A 192.168.1.144

DNS spoofing

Vamos definir apenas uma regra: Todos os registros A (registros de endereços) resolverão para 192.168.1.144, que é o nosso endereço do Kali.

DNS spoofing

Desta vez, vamos executar o Ettercap a partir da linha de comando. Abra um terminal e emita o seguinte comando.

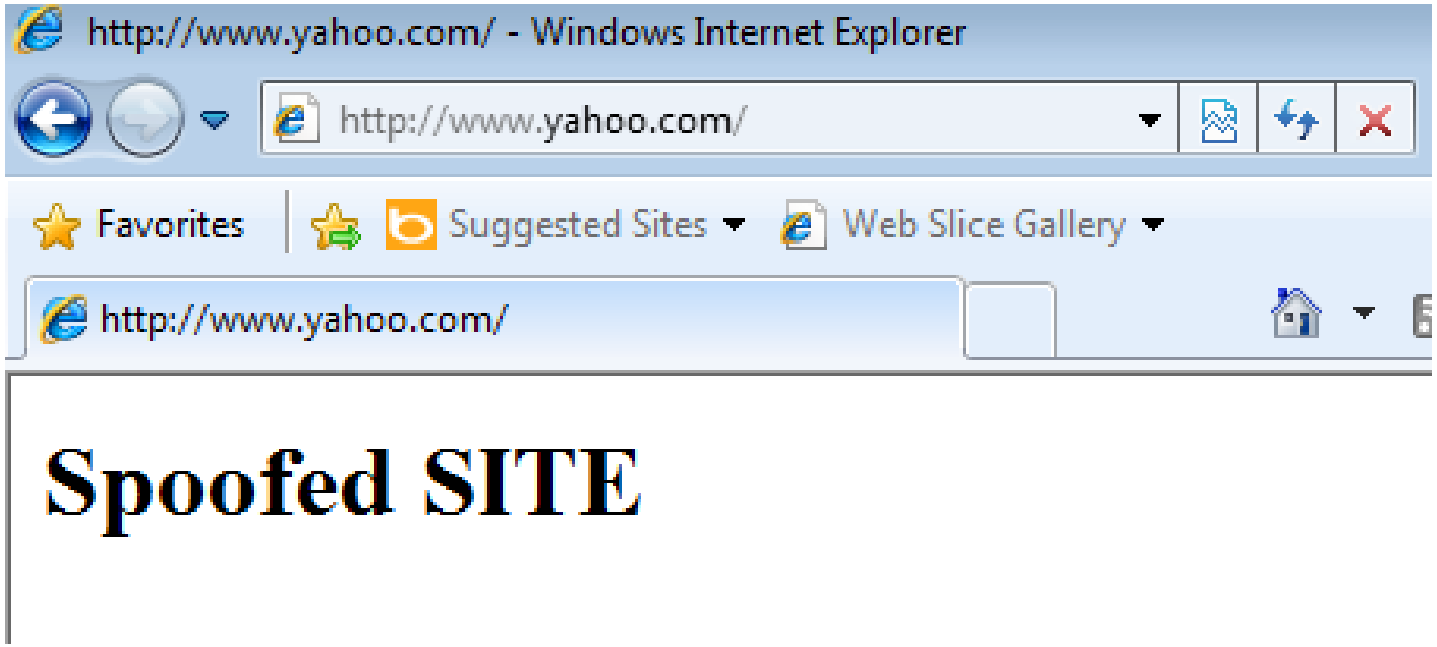
```
# ettercap -i eth0 -T -P dns_spoof -M arp /192.168.1.84///
```

DNS spoofing

Ele irá executar o Ettercap no modo de texto executando o spoofing ARP com o plugin de spoofing DNS habilitado, tendo apenas 192.168.1.84 como um destino alvo de nosso ataque.

DNS spoofing

Tendo iniciado o ataque, vamos para a máquina widows e tentamos navegar até um site usando seu nome de domínio, por exemplo, www.yahoo.com, como mostrado.



DNS spoofing

Observe como o endereço e as barras de título mostram o nome do site original mesmo que o conteúdo seja de um local diferente.