Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Configurando um ataque SSL MITM

Se tentarmos um sniff em uma sessão com HTTPS usando o que vimos até agora, não seremos capazes de obter muito dele, pois toda a comunicação é criptografada.

Configurando um ataque SSL MITM

Para interceptar, ler e alterar conexões SSL e TLS, precisamos fazer uma série de etapas preparatórias para configurar nosso proxy SSL. O SSLsplit funciona usando dois certificados, um para dizer ao servidor que ele é o cliente para que ele possa receber e descriptografar as respostas do servidor e um para dizer ao cliente que ele é o servidor.

Configurando um ataque SSL MITM

Para este segundo certificado, se vamos substituir um site que possua seu próprio nome de domínio e seus certificados tenham sido assinados por uma Autoridade de Certificação (CA), precisamos ter uma CA para emitir um certificado raiz para nós e, como nós agindo como atacantes, precisamos fazer por nosssa própria conta.

Configurando um ataque SSL MITM

Nesta aula, vamos configurar nossa própria autoridade de certificação e algumas regras de encaminhamento de IP para realizar os ataques de **SSL Man In The Middle**.

Configurando um ataque SSL MITM

Em primeiro lugar, vamos criar uma chave privada da CA no computador Kali:

```
# openssl genrsa -out certaauth.key 4096
```

Agora vamos criar um certificado assinado com essa chave:

```
# openssl req -new -x509 -days 365 -key certaauth.key -out ca.crt
```

Preencha todas as informações solicitadas (ou simplesmente pressione Enter para cada campo).

Configurando um ataque SSL MITM

Em seguida, precisamos habilitar o encaminhamento IP para ativar a funcionalidade de roteamento do sistema (encaminhar pacotes IP não destinados à máquina local para o gateway padrão).

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Configurando um ataque SSL MITM

Agora vamos configurar algumas regras para impedir o encaminhamento de tudo. Em primeiro lugar, vamos verificar se há alguma coisa na tabela NAT do nosso iptables.

```
# iptables -t nat -L
```

Se houver alguma coisa lá, você pode querer fazer *backup*

porque nós vamos limpar tudo, como mostrado.

```
# iptables -t nat -L > iptables.nat.bkp.txt
```

Agora vamos limpar a tabela:

```
# iptables -t nat -F
```

Em seguida, vamos criar as regras de roteamento:

```
# iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-ports 8080
```

```
# iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT --to-ports 8443
```

Configurando um ataque SSL MITM

Agora estamos prontos para detectar conexões criptografadas!

Agora vamos para a próxima aula!