Artigo

Metasploit – parte II

Aprenda como uilizar workspaces e procurar por máquinas vulneráveis com o framework Metasploit.

Por Alexandre Borges

Em minha coluna anterior abordei a forma de instalação do Metasploit em um ambiente Ubuntu e, naquele momento, evitamos utilizar a distribuição BackTrack para que tivéssemos a oportunidade de observar os passos envolvidos na configuração inicial do framework. A partir de agora não fará grande diferença se o leitor estiver usando o BackTrack ou uma instalação do Metasploit feita manualmente no Ubuntu.

O Metasploit é um framework que nos permite realizar ataques dos mais variados e por isso é importante conhecer alguns termos:

Exploit: método usado pelo hacker para atacar um serviço ou aplicativo da máquina alvo com o intuito de aproveitar-se de uma vulnerabilidade.
Payload: código ou comando a ser executado contra nosso alvo através (ou após) de uma vulnerabilidade explorada.
Shellcode: código normalmente escrito em linguagem Assembly que pode ser executado na máquina alvo e fornecer ao hacker um Shell interativo.
Módulos auxiliares: softwares que podem ser usados com finalidades complementares, por exemplo, realizar um escaneamento.

Para iniciar o Metasploit, execute o comando `msfconsole`. Uma vez dentro do console Metasploit, teremos acesso à todas as alternativas possíveis para realizar os passos de um ataque e sem qualquer restrição. É interessante notar que, assim que o comando `msfconsole` é executado, é apresentado um pequeno relatório com a versão do Metasploit, o número de exploits, payloads e módulos auxiliares que estão inclusos nesta versão. É por isto que, habitualmente, costumo atualizar as definições do framework com os exploits mais recentes. Para realizar esta tarefa, basta executar o comando `msf > msfupdate`.

O Metasploit utiliza um banco de dados PostgreSQL por padrão (e atualmente é o único suportado). As opções presentes do framework são diversas e, por exemplo, podemos executar comandos que nos ajudem a fazer o levantamento das informações sobre as máquinas nas quais estamos interessados:

```
msf > whois linuxmagazine.com.br

msf > nmap -sS 192.168.1.1
```

Isso funciona bem mas pode ser muito trabalhoso e incômodo gravar os resultados da saída de comandos com o `nmap`. Por este motivo, é possível que os resultados dos comandos sejam armazenados no próprio banco de dados do Metasploit e, mais especificamente, em uma área de trabalho (*workspace*) da ferramenta.

Para que possamos listar quais workspaces temos, digite o comando `msf > workspace``. Por padrão, sempre teremos o workspace "`default`" setado como ambiente principal.

Antes de prosseguirmos, surgiro que o leitor faça o download do ambiente Metasploitable 2 [1], com a finalidade de acompanhar o tutorial sobre o assunto. Trata-se de uma máquina virtual (VMware, é claro) com uma série de vulnerabilidades que podem ser testadas e exploradas pelo framework do Metasploit. Para facilitar a vida do leitor, o usuário e senha padrão do Metasploitable 2 é `msfadmin`. Caso haja tempo livre, surgiro fortemente ler os documentos na página da ferramenta [2].

Com o ambiente Metasploitable 2 no ar, é possível usar uma variante do `nmap` para armazenar os resultados do escaneamento:

```
msf > db_nmap - sS 192.168.1.107        //( esta seria nossa máquina Metasploitable 2)
```

Depois de o escaneamento ser concluído, os resultados armazenados podem ser verificados de muitas formas. Por exemplo, para listar

quais hosts foram escaneados até aqui, execute o comando `msf > hosts`. O resultado será algo como:

```
Hosts

=====

address        mac                name  os_name  os_flavor  os_sp  purpose  info  comments

———        —                  —-  ——-  ———  —-  ——-  —-  ———-

192.168.1.107  00:0C:29:D9:66:B9        Unknown                   device
```

A máquina listada neste resultado possivelmente tem diversos serviços no ar. Para realizar uma listagem deles, execute o comando `msf > services`. Note que todos os resultados estão guardados no Metasploit e, quando necessário (e nas colunas futuras) poderemos usá-los da forma que nos for mais conveniente.

Caso não seja mais o nosso objetivo guardar tais resultados, apague o workspace com o comando `msf > workspace -d default` e em seguida verifique o estado dos hosts com `msf > hosts`.

O resultado do último comando deverá vir vazio pois a apagamos o workspace no qual trabalhávamos. Como este workspace era o único que tínhamos, automaticamente o Metasploit cria um novo workspace para nós. Caso o leitor desejasse trabalhar com mais do que um workspace, poderá criar diversas outros através do comando `msf > workspace -a teste`.

Para alternar entre os workspaces, faça:

```
msf > workspace teste

msf > workspace

msf> workspace default
```

Na próxima coluna voltarei com mais sobre o Metasploit. Até mais.

Mais informações

[1] Metasploitable 2: http://sourceforge.net/projects/metasploitable/files/Metasploitable2/
[2] Documentos do Metasploitable 2: https://community.rapid7.com/docs/DOC-1875

Alexandre Borges é Oracle ACE, escreve para o OTN (*Oracle Tecnology Network*), trabalhou como instrutor contratado na Sun Microsystems de 2001 à 2010. Atualmente é instrutor da Symantec, ministra cursos para parceiros Oracle, é instrutor da EC-Council e de diversos cursos especializados sobre segurança da informação. Seu blog é http://alexandreborges.org.

Notícias