

Artigo



Metasploit - parte I

Uma visão geral sobre a versão Community, de código aberto, do framework de detecção de vulnerabilidade de segurança Metasploit no Ubuntu.

Por Alexandre Borges

Outra dia um aluno comentou comigo que estava estudando alguns livros de segurança e que, invariavelmente, em todos eles sempre havia um capítulo no qual o autor se dedicava a ensinar como efetuar uma invasão, mas o que era mostrado sempre era feito de modo superficial, pois partiam de premissas muito generosas (quase todas elas com acesso local à máquina) e nunca demonstravam técnicas de fato interessantes. Disse então que isto o desestimulava a aprender sobre segurança, já que havia a impressão de sempre estar faltando algo. Expliquei a ele que não há uma fórmula pronta para se aprender uma área tão complexa e que ele deveria insistir e continuar lendo. Sem dúvida, os pré-requisitos de aprendizado que um profissional de segurança necessita saber são: C, Assembly, diversas técnicas de coleta de dados, escaneamento, craqueamento de senhas, debugging, reversing etc, o que talvez torne pouco mais difícil e moroso aprender. É assim mesmo. Na ocasião, mencionei se, por acaso, ele já teria tentado explorar o *Metasploit*; porém, como muitos, ele me disse que já tinha lido algo a respeito e desistido, pois não entendia o mecanismo de forma clara. Neste momento percebi que deveria escrever a respeito do Metasploit. Não é minha intenção varrer o assunto de ponta a ponta, mas ao menos mostrar como as tarefas mais simples podem ser executadas para, quem sabe, incentivar interessados a investigar mais a fundo sobre este framework tão fascinante.

O projeto Metasploit foi desenvolvido primeiramente em Perl (depois totalmente reescrito em Ruby, sendo que a parte mais fundamental é a biblioteca *Ruby Extension - Rex*) por HD Moore por volta de 2003 (Spoonm e Matt Miller entraram pouco depois, e hoje em dia existem cerca de 21 colaboradores). Em 2009, a *Rapid7* adquiriu o projeto Metasploit e, com isso, trouxe uma visão mais comercial ao framework, sendo que atualmente existem a versão "*Metasploit Community*" (sem custos), "*Metasploit Express*" (proprietária, que oferece uma maneira robusta de realizar a exploração remota de forma simples e automatizada, além de possibilitar uma auditoria de senhas quebradas e fornecer múltiplos modelos de relatórios de penetração) e a versão *Metasploit Pro* (também proprietária, incluindo todos os itens da versão Express e outros diversos recursos, como escaneamento de aplicativos web, módulos de engenharia social, pivoteamento de VPNs, técnicas de ataques a IDS/IPS e total integração com o *Nexpose*).

Aliás, já que mencionamos as versões do framework, tomaremos uma linha diferente: nos exemplos que mostrarei nesta coluna e nas próximas, o foco da nossa abordagem será o Metasploit Community, porém ao invés de explicá-lo em cima do *BackTrack 5* (que é uma ferramenta de hacking e análise forense extraordinária), vamos instalar o Metasploit no Ubuntu aproveitando a instalação que provavelmente o leitor já possui (a minha versão é a 11.10 – caso o leitor não esteja seguro de qual versão está usando, poderá executar o comando `lsb_release -a` para descobrir) e, ao mesmo tempo, saindo um pouco do lugar comum ao usar o Backtrack. O download do Metasploit Community pode ser feito em <http://www.metasploit.com/download/>. De modo adicional, o leitor pode também instalar o Metasploit no Windows (com o antivírus e antispys desabilitado), mas não falaremos a respeito disto nesta coluna.

Uma vez feito o download, para instalar o Metasploit é necessário entrarmos com:

```
# chmod u+x metasploit-latest-linux-x64-installer.run  
# ./metasploit-latest-linux-x64-installer.run
```

Com isso, a instalação do Metasploit ocorre sem qualquer problema e, por padrão, o local que ele será instalado é em `/opt/metasploit`. Para ter certeza que tudo ocorreu bem, digite `# msfconsole -v`. Se obtiver a versão (a minha é a 4.6.0-dev), significa que a instalação ocorreu sem problemas. Como o projeto Metasploit está constantemente incluindo técnicas novas de ataque e exploração, recomendo fortemente que o leitor sempre mantenha a instalação o mais atualizada possível executando o comando `# msfupdate`.

Existem outras maneiras de instalar e atualizar o Metasploit. Por exemplo, o leitor pode escolher fazer tudo através do subversion. Mesmo que seja elegante, ainda tenho a preferência pela maneira que mostrei acima. Seguem os passos com subversion:

```
# apt-get install subversion  
# mkdir /opt/metasploit ; cd /opt/metasploit  
# svn co https://www.metasploit.com/svn/framework3/trunk/
```

```
# cd trunk ; ls ; svn update
```

O framework do Metasploit traz embutido o banco de dados Postgre para que seja factível usar e guardar os resultados obtidos; mas não se engane, esta base será muito importante para nós nas próximas colunas. Normalmente, quando se entra no console de operação do Metasploit, já estamos conectados à base, porém mesmo assim pode ser útil, em algumas ocasiões, sabermos qual a senha de conexão. Para descobrir, entre com:

```
# more /opt/metasploit/apps/pro/ui/config/database.yml
```

Procure pelo campo “password” da configuração de produção (production). Desta forma, facilmente conseguiremos a senha necessária.

Por enquanto é isso. No mês que vem volto com mais novidades sobre o Metasploit. Até lá.

Alexandre Borges é Oracle ACE, escreve para o OTN (*Oracle Technology 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

MP denuncia Cartorio Virtual por venda de dados sigilosos, inclusive do WhatsApp

Publicado em: 18/09/2015 às 9:34 | leituras | [Ver 0 comentários](#)

O Ministério Público denunciou à Justiça, o dono do site 'cartório virtual', que segundo o MP, faz venda de dados considerados sigilosos, entre eles, cópias de contas telefônicas, lista de bens e, até mesmo, conversas mantidas no WhatsApp, aplicativo de mensagem do Facebook, revela reportagem do jornal O Estado de São Paulo, desta sexta-feira, 18/09.

Lançado novo Portal do Software Público Brasileiro

Publicado em: 15/09/2015 às 17:27 | leituras | [Ver 0 comentários](#)

Construção da nova versão do portal começou em 2013 e recebeu mais de duzentas contribuições.

Desemprego seletivo

Publicado em: 13/09/2015 às 9:10 | leituras | [Ver 0 comentários](#)

Até julho o desemprego cresceu de 4,95 para 7,5%.A situação atual é decorrente de problemas macroeconômicos e sem dúvida que o ajuste fiscal empreendido pelo Governo federal contribui significativamente.

Red Hat reúne líderes de tecnologia do Nordeste para ampliar negócios na região

Publicado em: 11/09/2015 às 14:34 | leituras | [Ver 0 comentários](#)

Eventos realizados na semana passada em Fortaleza, Salvador e Recife reuniram cerca de 200 profissionais de TI e mostraram como as empresas locais de vários tamanhos podem transformar os desafios atuais da economia em oportunidades por meio de tecnologias que podem refletir em uma redução em até 50 % de seus custos em TI.

Estudantes de SP começam a aprender Internet das Coisas com kit Android da Samsung

Publicado em: 09/09/2015 às 13:52 | leituras | [Ver 0 comentários](#)

O programa tem previsão de início prático em 2016, embora algumas escolas já estejam implantando o curso em fase de testes na zona sul paulistana.