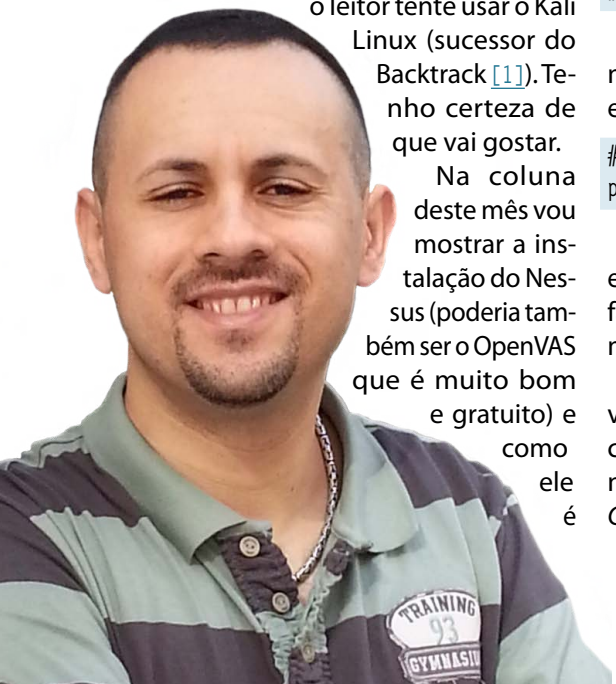
Coluna do Alexandre

Metasploit – parte 5

Nesta edição, aprenda como utilizar o scanner Nessus para procurar por vulnerabilidade em potenciais alvos.

por Alexandre Borges

Eu não tenho qualquer dúvida de que o Metasploit é a melhor ferramenta, a mais completa e mais útil para realizar (ou auxiliar, em alguns casos) na invasão de computadores. Todavia, existem outras ferramentas que podem complementar os recursos do Metasploit: estamos falando dos scanners de vulnerabilidade como Nessus, OpenVAS, Nexpose, Core Impact, Retina e por aí vai. Estes scanners são fundamentais para apontar todas as vulnerabilidades da máquina ou rede que queremos atacar e, uma vez com todos os dados em mãos, utilizar o Metasploit torna-se trivial. Caso o leitor esteja usando a distribuição Ubuntu, poderá prosseguir exatamente como demonstrado mais adiante, sendo que, para outras distribuições os passos podem ser ligeiramente diferentes. Por exemplo, sugiro que o leitor tente usar o Kali Linux (sucessor do Backtrack [1]). Tenho certeza de que vai gostar.



Na coluna deste mês vou mostrar a instalação do Nessus (poderia também ser o OpenVAS que é muito bom e gratuito) e como ele é integrado dentro do Metasploit. Vamos aos passos:

- a) Certifique-se de que sua instalação do Ubuntu está atualizada, através dos comandos `apt-get update` e `apt-get upgrade`, realize o download do Nessus [2] e registre-o [3] no site da Tenable.
- b) Instale o Nessus e execute o registro local da ferramenta com o código recebido ao cadastrar-se no site da Tenable:

```
#  dpkg -i Nessus-5.2.1-debian6_ ➥
amd64.deb
#  /opt/nessus/bin/nessus-fetch ➥
--register WEBEVAL-XXXX-XXXX- ➥
XXXX-XXXX-XXXX
```

- c) Adicione o usuário que será utilizado para realizar o escaneamento e inicialize o Nessus:

```
# /opt/nessus/var/nessus/logs# ➥
/opt/nessus/sbin/nessus-adduser
#  /etc/init.d/nessusd start
```

Depois da primeira inicialização, mantenha os plugins atualizados executando o comando:

```
# /opt/nessus/sbin/nessus-update- ➥
plugins
```

- d) Acesse o Nessus através do endereço `http://localhost:8834` (por favor, tenha paciência porque o primeiro acesso demora um pouco...).
- e) Uma vez realizado o login, vá para a aba *Polices* (Políticas) e crie uma nova política clicando no botão *New Policy*. Na seção *General Settings*, matenha a opção *Setting Type* em *Basic*, dê um nome para a sua política (a minha chamei de Linux Magazine) e, em seguida, vá para a seção *Plugins*. Lá, sugiro ao leitor desabilitar todos os plugins que não se encaixam em seu ambiente. Por exemplo, em meu ambiente existem máquinas com sistemas Linux (Ubuntu 12.04, CentOS 6, Metasploitable 2), Solaris 11 e Windows (XP e 7) e, por isto, desabilito todos plugins não relacionados (CISCO, Gentoo, AIX, FreeBSD, Fedora, Mac OS, HPUX etc.) e também os plugins que executam ataques de negação de serviços (DoS – *Deny of Services*). Não esqueça de clicar no botão *Update*.
- f) Vá para aba *Scan Queue*, clique em *New Scan*, dê um nome para seu escananeamento (o meu chamei de LM Metasploit), escolha a política criada (*Linux Magazine*, no meu caso) e cadastre o endereço IP das máquinas que serão avaliadas. Concluída esta etapa, pressione o botão *Start Scan*.
- g) Após finalizado o escaneamento, o leitor pode ir até a aba *Results* e clicar duas vezes no nome do escananeamento (*LM Metasploit*). Neste momento, todas as vulnerabilidades de todas as máquinas serão mostradas (no meu caso foram 139!).

Agora seria possível, através da interface web, usar as vulnerabilidades relatadas pelo Nessus e realizar diversos ataques aos

nossos alvos usando estas informações. Entretanto, podemos verificar estes mesmos resultados também dentro do Metasploit. Para isto, vamos executar o framework, carregar o módulo Nessus, conectar-se a ele (o Nessus está instalado na mesma máquina do Metaploit), listar os relatórios provenientes do escananeamento e importar o relatório que foi criado pela ferramenta:

```
# msfconsole
msf > load nessus
msf> nessus_connect    nessus_ ➥
user:nessus ➥
password@127.0.0.1:8834 ok
msf > nessus_report_list ➥
ID    Name         Status    Date
--       --        --      --
b2666002-e4b8-2381-d4ec- ➥
8e8ca54c0e5b4d2575fe1da13967  LM ➥
Metasploit  completed  03:29 ➥
Aug 10 2013 ➥
[*] You can: [*]         Get a ➥
list of hosts from the report: ➥
nessus_report_hosts <report id>
msf > nessus_report_get b2666002- ➥
e4b8-2381-d4ec- ➥
8e8ca54c0e5b4d2575fe1da13967 ➥
[*] importing b2666002-e4b8-2381- ➥
d4ec-8e8ca54c0e5b4d2575fe1da13967
```

Mais informações

[1] Kali Linux: http://www.kali.org/downloads

[2] Download do Nessus: http://www.tenable.com/products/nessus/select-your-operating-system

[3] Registro do Nessus: http://www.tenable.com/products/nessus/evaluate

Deste ponto em diante, podemos produzir um sumário dos hosts, serviços e vulnerabilidades que o Nessus encontrou e que estão agora registrados no banco de dados do Metasploit:

```
msf > hosts -c address,svcs,vulns
```

Alternativamente, o leitor pode executar os seguintes comandos para listar de maneira detalhada todos os IPs, serviços e vulnerabilidades que estão registrados no banco de dados do Metasploit:

```
msf> hosts
msf> services
msf> vulns
```

Finalmente, estamos preparados para usar o Metasploit com eficiência. Vejo vocês no mês que vem. ■

Alexandre Borges (linkedin: br.linkedin.com/in/aleborges) é instrutor e especialista sênior em sistemas operacionais Unix, Linux, Banco de Dados, Virtualização, Cluster, Storage, Servidores, Backup, Desempenho e Segurança, além de possuir profundo envolvimento com assuntos relacionados ao kernel Linux.