|  |  |  |  |
| --- | --- | --- | --- |
| **MODALIDADE:** | Curso de Especialização Tecnológica (CET) | **Ficha 9: Metasploit – Metasploitable** | |
| **CURSO:** | Técnico especialista em cibersegurança | | |
| **UFCD:** | Wargamming | **CÓDIGO UFCD:** | 9197 |
| **FORMADOR/A:** | Ricardo Lobo | **DATA:** | 28/04/2023 |
|  |  |  |  |
| **OBJETIVOS** | | | |
| * Conhecer o Metasploitable 2. * Primeiro contacto com o Metasploit | | | |

# Metasploitable 2

O Metasploitable 2 é uma máquina virtual criada para ser usada como um ambiente de teste para avaliação de segurança e aprendizagem de técnicas de testes de penetração. Este sistema foi projetado para conter múltiplas vulnerabilidades conhecidas e exploráveis, permitindo que os *pentesters* pratiquem técnicas de exploração de vulnerabilidades num ambiente controlado e seguro.

## Passo 1

Efetue o *download* do ficheiro “**Metasploitable.vmdk**” que se encontra disponível para *download* na localização abaixo:

[https://wetransfer.com/downloads/dc624cdac826392712063428446fd8cd20230427232423/43181cb46725d86d003802ad98b7815d20230427232443/21ba89](https://wetransfer.com/downloads/dc624cdac826392712063428446fd8cd20230427232423/43181cb46725d86d003802ad98b7815d20230427232443/21ba89?trk=TRN_TDL_01&utm_campaign=TRN_TDL_01&utm_medium=email&utm_source=sendgrid)

## Passo 2

Crie uma máquina virtual no seu computador utilizando o ficheiro “**Metasploitable.vmdk**” fornecido pelo formador.

Vídeo: <https://www.youtube.com/watch?v=I6WfFLQwoPg&t=30s>

Requisitos da máquina virtual:

* Memória RAM: 512MB
* Processadores: 1
* Adaptador de rede: Rede LAB (apenas com comunicação com a VM do Kali Linux).

## Passo 3

Execute as VMs do Metasploitable e do Kali e faça testes de conetividade entre as máquinas, para confirmar o correto funcionamento.

**Dados de acesso à VM do Metasploitable 2:**

* Username: **msfadmin**
* Password: **msfadmin**

Uma imagem com texto

Descrição gerada automaticamente

## Passo 4

No Kali Linux, abra o terminal e atualize a base de dados do seu Metasploit, executando o comando abaixo.

|  |
| --- |
| **Comando** |
| msfupdate |

## Passo 5

Execute o Metasploit no Kali Linux, executando o comando abaixo.

|  |
| --- |
| **Comando** |
| Msfconsole |

Uma imagem com texto

Descrição gerada automaticamente

## Passo 6

Recorrendo ao Metasploit, faça uma pesquisa das vulnerabilidades presentes na VM do Metasploitable 2.

|  |
| --- |
| **Comando** |
| db\_nmap -v --script vuln [IP VM Metasploitable 2] |
| Exemplo: |

|  |
| --- |
| **Registe com capturas de ecrã, os passos que efetuou e os resultados obtidos** |
|  |

## Passo 7

Com base nos diapositivos disponibilizados pelo formador, efetue a exploração da vulnerabilidade no serviço de FTP (**vsftpd**).

|  |
| --- |
| **Registe com capturas de ecrã, os passos que efetuou e os resultados obtidos** |
|  |

Depois de realizada a ficha de trabalho, submeta este ficheiro na tarefa criada para o efeito.

**Bom trabalho**