INSTITUTO POLITÉCNICO DE BEJA
Escola Superior de Tecnologia e Gestão
Mestrado em Engenharia de Segurança Informática
Criptografia e Criptanalise Aplicadas

Aplicação de Cifra

Martinho José Novo Caeiro - 23917
Paulo António Tavares Abade - 23919

Beja, outubro de 2025

INSTITUTO POLITÉCNICO DE BEJA
Escola Superior de Tecnologia e Gestão
Mestrado em Engenharia de Segurança Informática
Criptografia e Criptanalise Aplicadas

Aplicação de Cifra

Martinho José Novo Caeiro - 23917
Paulo António Tavares Abade - 23919

Orientador: Rui Miguel Silva

Beja, outubro de 2025

Resumo

Este relatório descreve o desenvolvimento de uma aplicação de segurança informática, implementada em Python, uma linguagem de programação dinâmica. O objetivo é explorar conceitos fundamentais de segurança e demonstrar a aplicação prática desses conceitos. Esta aplicação é desenvolvida no âmbito da unidade curricular de Linguagens de Programação Dinâmicas IPBeja, 2025.

Keywords: python, segurança informática, programação dinâmica

Abstract

This report describes the development of a cybersecurity application implemented in Python, a dynamic programming language. The goal is to explore fundamental security concepts and demonstrate their practical application. This application is developed within the scope of the Dynamic Programming Languages course IPBeja, 2025.

Keywords: python, cybersecurity, dynamic programming language

Índice

Índice de Figuras

1 Introdução

Esta aplicação consistirá na junção de várias ferramentas de segurança informática, tais como Port Scanner, UDP Flooder, SYN Flooder, sistema de Logging, sistema de troca de Mensagens, Port Knocker e Password Manager. A aplicação será desenvolvida em Python (Python Software Foundation, 2025) e tem como base uma interface de linha de comandos (CLI), permitindo ao utilizador interagir com o sistema de forma simples e eficiente. O sistema base a ser utilizado será o Kali Linux (OffSec Services Limited, 2025), devido à sua popularidade na área de segurança informática e à vasta gama de ferramentas disponíveis. Todo o progresso do projeto será documentado no repositório GitHub (Martinho Caeiro, 2025).

2 Introdução Teórica

2.1 Porto

Um porto (Wikipedia, 2025e) é um ponto de extremidade lógico para comunicação em rede, usado para identificar serviços ou aplicações específicas em um dispositivo. Os protocolos que usam principalmente portas são os protocolos da camada de transporte, tais como o Protocolo de controle de transmissão (TCP) e User Datagram Protocol (UDP) do conjunto de protocolos da internet.

2.2 UDP Flood

Um ataque UDP flood (Wikipedia, 2025g) é um tipo de ataque de negação de serviço (DoS) que visa inundar um alvo com pacotes UDP, sobrecarregando a largura de banda e os recursos do sistema.

2.3 SYN Flood

Um ataque SYN flood (Wikipedia, 2025f) é um tipo de ataque de negação de serviço (DoS) que explora o processo de handshake do TCP, enviando uma série de pacotes SYN para um servidor, mas nunca completando o handshake, o que pode levar à exaustão dos recursos do mesmo.

2.4 Logging

Logging (Wikipedia, 2025b) refere-se ao processo de registrar eventos que ocorrem em um sistema de computador. Esses registos, conhecidos como logs, são essenciais para a análise de segurança, pois permitem que os administradores identifiquem atividades suspeitas e respondam a incidentes de segurança.

2.5 Port Knocking

Port Knocking (Wikipedia, 2025d) é uma técnica de segurança que envolve o envio de uma sequência de pacotes para portas específicas em um servidor, a fim de abrir uma porta de acesso (geralmente SSH) que está fechada por padrão. Essa técnica é usada para ocultar serviços de rede e proteger servidores contra ataques automatizados.

2.6 Password

Uma password (ou senha) (Wikipedia, 2025c) é uma sequência de caracteres usada para autenticar a identidade de um utilizador. As passwords são uma das formas mais comuns de autenticação e são usadas para proteger o acesso a sistemas, contas e dados sensíveis.

2.7 2FA

A autenticação de dois fatores (2FA) (Wikipedia, 2025a) é um método de segurança que requer dois tipos diferentes de autenticação para verificar a identidade de um utilizador. Normalmente, isso envolve algo que o utilizador sabe (como uma password) e algo que o utilizador possui (como um dispositivo móvel para receber um código temporário).

3 Configuração do Servidor

A instalação do Kali Linux (OffSec Services Limited, 2025), foi feita numa maquina virtual utilizando o VirtualBox (Oracle Corporation, 2025). Para facilitar a instalação foi utilizado um .iso feito especificamente para o VirtualBox, que já tinha o processo de instalação automatizado, poupando assim tempo na instalação do sistema operativo.

Informações adicionais incluem 4GB de RAM e seis processadores de CPU e a rede está em modo 'bridge'. Foi utilizado o Visual Studio Code (Microsoft Corporation, 2025) como editor de texto para facilitar a edição dos scripts.

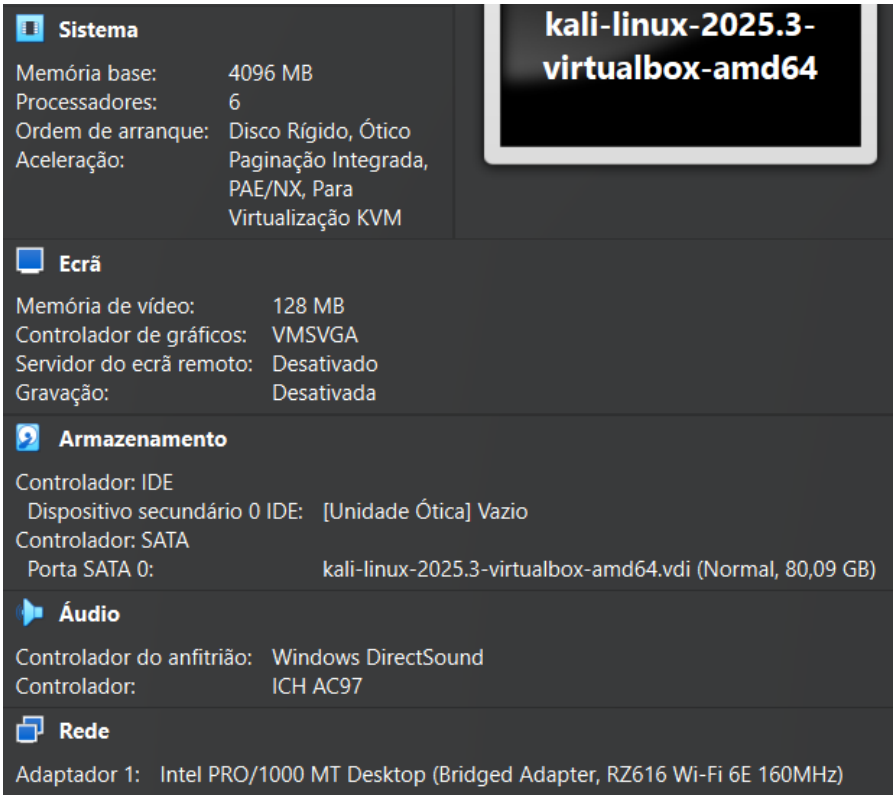

Figura 1: Exemplo de Maquina Utilizada

4 Desenvolvimento dos Scripts

Todos os seguintes scripts foram desenvolvidos em Python e todos verificam se a maquina possui os pacotes necessários para o funcionamento da ferramenta, irá perguntar se quer instalar para poder continuar a utilizar. Caso o utilizador deseje prosseguir, o script irá instalar os pacotes necessários e depois irá ativá-los. Cada script pode ser executado individualmente ou através do menu principal.

4.1 Menu

O menu é o metodo principal para a interação com a ferramenta. Para aceder a uma funcionalidade, o utilizador deve selecionar a opção correspondente no menu. Para executar o menu apenas é necessário escrever 'python menu.py'.

O menu apresenta-se da seguinte forma:

```
========== MENU PRINCIPAL - LPD-TOOL ==========
1 - Port Scanner
2 - UDP Flooder
3 - SYN Flooder
4 - Logger
5 - Messenger
6 - Port Knocker
7 - Password Manager
0 - Sair
================================================
Escolha uma opção:
```

4.2 Port Scanner

4.3 UDP Flooder

4.4 SYN Flooder

4.5 Logger

4.6 Messenger

4.7 Port Knocker

4.8 Password Manager

5 Conclusão

O desenvolvimento deste laboratório permitiu explorar conceitos fundamentais de segurança informática e linguagens de programação dinâmicas. Apesar de alguns desafios encontrados, foi possível implementar as ferramentas solicitadas e configurar um menu centralizado para facilitar a utilização dos mesmos. Durante este processo, foram revistos conceitos previamente estudados, como o Port Knocking, e foi dada a oportunidade de aprender novos, como UDP Flooding e SYN Flooding.

Bibliografia

IPBeja. (2025). *Disciplina: Linguagens de Programação Dinâmicas | IPBeja* [Página LPD]. Obtido outubro 29, 2025, de https://cms.ipbeja.pt/course/view.php?id=1164

Martinho Caeiro. (2025). *LPD-Tool - Repositório de Código* [Repositório da Aplicação LPD-Tool]. Obtido outubro 29, 2025, de https://github.com/MartinhoCaeiro/LPD-Tool

Microsoft Corporation. (2025). *Visual Studio Code* [Editor de Texto Visual Studio Code]. Obtido outubro 29, 2025, de https://code.visualstudio.com/

OffSec Services Limited. (2025). *Get Kali | Kali Linux* [Instalador Kali Linux]. Obtido outubro 29, 2025, de https://www.kali.org/get-kali/#kali-platforms

Oracle Corporation. (2025). *VirtualBox* [Software de Virtualização VirtualBox]. Obtido outubro 29, 2025, de https://www.virtualbox.org/

Python Software Foundation. (2025). *Welcome to Python.org* [Linguagem de Programação Python]. Obtido outubro 29, 2025, de https://www.python.org/

Wikipedia. (2025a). *Autenticação de Dois Fatores*. Obtido outubro 29, 2025, de https://en.wikipedia.org/wiki/Multi-factor_authentication

Wikipedia. (2025b). *Logging (Computação)*. Obtido outubro 29, 2025, de https://en.wikipedia.org/wiki/Logging_(computing)

Wikipedia. (2025c). *Password*. Obtido outubro 29, 2025, de https://en.wikipedia.org/wiki/Password

Wikipedia. (2025d). *Port Knocking*. Obtido outubro 29, 2025, de https://en.wikipedia.org/wiki/Port_knocking

Wikipedia. (2025e). *Porto (Redes de Computadores)*. Obtido outubro 29, 2025, de https://en.wikipedia.org/wiki/Port_(computer_networking)

Wikipedia. (2025f). *SYN flood*. Obtido outubro 29, 2025, de https://en.wikipedia.org/wiki/SYN_flood

Wikipedia. (2025g). *UDP flood*. Obtido outubro 29, 2025, de https://en.wikipedia.org/wiki/UDP_flood