ATEC

9190 – Programação Orientada à Cibersegurança

26 de Junho de 2025

1 Aplicação de Segurança Informática

Os formandos têm o objetivo de realizarem uma aplicação de segurança informática construída com uma linguagem de programação dinâmica: Python.

A escrita de código adicional na linguagem de programação C/C++ com o eventual uso de bibliotecas adicionais é possível.

Os alunos devem realizar uma ferramenta de segurança informática que:

- permita detetar que portos de rede se encontram disponíveis numa ou mais máquinas remotas;
- permita determinar que conexões se encontrem ativas numa determinada máquina;
- processar ficheiros de log dum sistema Linux tentando obter informação sobre as tentativas indevidas de acesso de pelos menos 2 serviços (ex: http, SSH), nomeadamente:
  - listas de origem por país;
  - datas e horas de tentativas;
- outras caraterísticas de segurança informática podem ser incorporadas no trabalho sendo valorizadas casuisticamente.

A ferramenta pode ser projetada para uso em modo de linha de comando ou modo gráfico dando-se preferência ao modo de linha de comando.

A aplicação deve permitir a exportação das listas para um ficheiro de texto e CSV, permitindo ao utilizador escolher entre as duas.

A aplicação deve de guardar as informações referentes a logs numa base de dados SQLite.

Alguns elementos de interesse para esta aplicação que podem ser considerados como pontos de investigação autónomos:

- uso das bibliotecas de rede de Python ou outras linguagens de programação dinâmicas;
- uso da biblioteca libpcap;
- a geração de PDFs com reportlab;
- gráficos com estatísticas, nomeadamente usando a biblioteca matplotlib; (mais complexo)
- mapas geográficos usando as bases de dados GeoIP (caso implementem funcionalidade pesquisar IPs nas bases de dados GeoIP);
- cifragem dos dados, e armazenamento dessa informação numa base de dados em SQLite;
- Integração com uma ou mais plataformas de Cyber Intelligence para extração de informação sobre endereços de IP ou domínios. (ex.: AlienVault OTX, VirusTotal)

A aplicação projetada pode usar bibliotecas e ferramentas externas à aplicação.

2 Avaliação de aplicação vulnerável - BufferOverflow

Será facultado uma aplicação de servidor a instalar numa máquina Windows que possui vulnerabilidade de Buffer Overflow. O formando deverá de usar os conhecimentos que adquiriu em aula para analisar a aplicação facultada, e apresentar todo o código que desenvolveu até ao momento.

O formando deverá demonstrar o controlo do Extended Instruction Pointer (comprovado pelo Immunity Debugger), e indicar qual o offset em que a aplicação, i.e., quantos caracteres são necessários para o sistema falhar.

3 Modo de Funcionamento

O tema do trabalho é idêntico para todos os alunos. A avaliação poderá ser individual ou em grupos de 2 formandos.

3.1 Sistema Operativo

O sistema operativo escolhido para a realização do trabalho pode ser em Linux ou Windows

Sugere-se que o trabalho seja desenvolvido numa máquina virtual ligeira e com um editor de texto de tal como VisualStudio Code ou similar.

3.2 Data e Modo de Entrega

A data limite para a entrega do trabalho é até à meia-noite de dia 13 de Julho até às 2025.

Os alunos devem entregar o trabalho num ficheiro .zip com a seguinte estrutura.

Nome ficheiro zip: **nomeAluno_nº_python.zip**

Ficheiro **nomeAluno_nº_python.zip** deverá conter:

Todo o código referente ao programa desenvolvido;

Anotações sobre bibliotecas que seja necessário importar para o código funcionar corretamente.

Componentes da Avaliação

O trabalho é composto pelas seguintes parcelas que serão avaliadas:

E - aplicação e scripts executáveis;

C - código da aplicação;

U - documentação para o utilizador (caso haja);

É importante salientar duas questões fundamentais:

- a originalidade e inventividade das soluções;
- a honestidade na realização e na atribuição dos créditos intelectuais.

3.2.1 Aplicação Executável

A funcionalidade geral da aplicação, a obediência, e eventual ultrapassagem dos requisitos será levada em conta. Fatores de robustez e segurança na utilização da aplicação também serão importantes.

3.2.2 Código da Aplicação

No código da aplicação, entre outros aspetos, serão tomados em conta:

- a clareza do código;
- a estrutura do código;
- os conhecimentos de programação específicos para cada linguagem;
- a utilização correta do sistema de controlo de versões;
- a originalidade das soluções propostas;

- a referência adequada das fontes de inspiração do código.

E - aplicação executável;

C - código da aplicação;

R - relatório do trabalho;

U - documentação para o utilizador;

Bom trabalho!