poirot@34a2bc: $ cat introducao

Seja muito vem vindo ao desafio do processo seletivo LabSEC 24-2. Devido a seus esforços para durante a etapa passada, informações suficientes sobre os criminosos "Rato" e "Cobra" foram coletadas e medidas legais foram tomadas para sua apreensão.

poirot@34a2bc: $ cat proposta

Agora, para fazer parte de nossa equipe, um desafio de verdade o aguarda, cinco tarefas distintas, cada uma avaliando aspectos essenciais para o contexto de assinaturas digitais. Cada tarefa trará um desafio a ser avaliado e julgado de acordo com os seus conhecimentos. Todos as assinaturas e certificados neste desafio **não possuem erro** na sua **estrutura semântica** ou em seus atributos.

poirot@34a2bc: $ cat estrutura-do-documento

Esse documento está organizado de modo que cada tarefa contém suas especificações relacionadas à proposta, ao que entregar e como entregar. Após o término de todas as tarefas, se localiza a descrição de como o entregável e o relatório devem ser feitos.

poirot@34a2bc: $ cat poesia

Security

Tomorrow will have an island. Before night I always find it. Then on to the next island. These places hidden in the day separate and come forward if you beckon. But you have to know they are there before they exist. Some time there will be a tomorrow without any island. So far, I haven't let that happen, but after I'm gone others may become faithless and careless. Before them will tumble the wide unbroken sea, and without any hope they will stare at the horizon. So to you, Friend, I confide my secret: to be a discoverer you hold close whatever you find, and after a while you decide what it is. Then, secure in where you have been, you turn to the open sea and let go.

—William Stafford

poirot@34a2bc: $ cat tarefa-1

Para essa tarefa seu objetivo é avaliar as 5 assinaturas recebidas, de acordo com normativos adequados, como:

- VALIDO: o arquivo não apresenta nenhuma informação errada e seu status é integro;
- INVALIDO: o arquivo atende requisitos de política/perfil vigente

poirot@34a2bc: $ cat entrega

A entrega deverá ser de um arquivo chamado validade.txt gerado através de uma série de N entradas, onde N é o número de arquivos avaliados, com cada entrada contendo o nome do arquivo avaliado seguido de seu status em maiúsculo e sem acentuação gráfica. As entradas devem estar organizadas de modo que estejam em ordem alfabética.

poirot@34a2bc: $ cat tarefa-2

Para esta tarefa, você deverá realizar 3 etapas relacionadas a caminho de certificação:

- Etapa 1: você deverá reconstruir um caminho de certificação entre os arquivos a seguir, realizando um algoritmo em Java utilizando obrigatoriamente a biblioteca Bouncy Castle:
  - → cert_CHOP_SUEY.pem
  - → cert_MANEATER.pem
- Etapa 2: você deverá reconstruir a cadeia TLS do certificado a seguir:
  - → moodle-ufsc-br.pem
- Etapa 3: você deverá gerar um próprio certificado Let's Encrypt com o domínio labsec.local, para isso sugerimos utilizar Apache, Caddy ou DuckDNS.

poirot@34a2bc: $ cat entrega

- Etapa 1: um pacote tar.gz contendo o código criado.
- Etapa 2: os certificados obtidos na reconstrução da cadeia, além um arquivo chamado tls.txt explicitando o caminho da certificação;
- Etapa 3: um arquivo chamado certificado.pem contendo o certificado gerado e um arquivo chamado privatekey.pem contendo a chave privada gerada.

poirot@34a2bc: $ cat tarefa-3

Para essa tarefa seu objetivo é avaliar os carimbos de tempo e validade das 3 assinaturas recebidas como:

- VALIDO: o arquivo não apresenta nenhuma informação errada e seu status é integro;
- INVALIDO: o certificado está expirado.

poirot@34a2bc: $ cat entrega

A entrega deverá ser de um arquivo chamado timestamp.txt gerado através de uma série de N entradas, onde N é o número de arquivos avaliados, com cada entrada contendo o nome do arquivo avaliado seguido de seu status, o status do certificado e o status do carimbo de tampo, todas entradas em maiúsculo e sem acentuação gráfica. As entradas devem estar organizadas de modo que estejam em ordem alfabética.

poirot@34a2bc: $ cat tarefa-4

Para essa etapa, deve-se analisar as 5 assinaturas recebidas, de acordo com o conceito de revogação, elas devem ser avaliadas como:

- VALIDO: o arquivo não apresenta nenhuma informação errada e seu status é integro;
- REVOGADO: o arquivo contém certificados em sua assinatura que estão revogados.

poirot@34a2bc: $ cat entrega

A entrega deverá ser de um arquivo chamado revogacao.txt gerado através de uma série de N entradas, onde N é o número de arquivos avaliados, com cada entrada contendo o nome do arquivo avaliado seguido de seu status em maiúsculo e sem acentuação gráfica. As entradas devem estar organizadas de modo que estejam em ordem alfabética.

poirot@34a2bc: $ cat tarefa-5

Para esta tarefa, você deverá realizar duas etapas relacionadas a listas de confiança:

- Etapa 1: você deverá analisar o arquivo LU.xml e explicitar os serviços de confiança prestados por LuxTrust S.A;
- Etapa 2: você deverá explicar de o motivo da invalidade da assinatura cms anexada, considerando tl.xml como a lista de confiança vigente.

poirot@34a2bc: $ cat entrega

- Etapa 1: A entrega deverá ser de um arquivo chamado listas.txt gerado através de uma série de N entradas, onde N é o número de serviços de confiança realizados, com cada entrada contendo o nome do serviço realizado e seu identificador.;
- Etapa 2: o status da assinatura, como VALIDO ou INVALIDO em um arquivo nomeado assinatura-lista.txt.

poirot@34a2bc: $ cat entrega

Para a entrega, deverão ser considerados os templates anexados em cada diretório challenge/solution/tarefa-?/

Para cada tarefa, deverá ser preenchido o template de acordo com as instruções fornecidas em cada etapa. É necessário enviar apenas o arquivo final, portanto renomeie o nome de <entregavel>.template.txt para <entregavel>.txt.

No caso da etapa 1 da tarefa 2, o esqueleto do código disponível em challenge/solution/tarefa-2/ deve ser preenchido de acordo com as intruções do arquivo Main.java.

A entrega final deverá conter também um relatório, descrevendo o processo de resolução, endereçado como /challenge/solution/relatorio.pdf

poirot@34a2bc: $ cat relatorio

Para o relatório, deve-se descrever detalhadamente os procedimentos realizados em cada tarefa, mencionando ferramentas, documentos, arquivos, normativos e o raciocínio lógico utilizados para cada processo. Arquivos individuais de cada tarefa serão desconsiderados caso não haja uma argumentação sobre sua elaboração no relatório final. Qualquer relatório ou artefato que aparentar ser gerado por IA poderá ser desconsiderado.

PLÁGIO NÃO SERÁ TOLERADO

1.Link Úteis

1.1.Documentação

- https://datatracker.ietf.org/doc/html/rfc3161
- https://datatracker.ietf.org/doc/html/rfc5280
- https://en.wikipedia.org/wiki/ASN.1
- https://datatracker.ietf.org/doc/html/rfc5652
- https://www.jensign.com/sigview/index.html
- https://www.w3.org/TR/xmldsig-core2/

1.2.Normativos

- DOC-ICP-15.03 v8.0
- Creation and Validation of AdES Digital Signatures
- Part 1: Building blocks and XAdES baseline signatures
- Part 1: Building blocks and CAdES baseline signatures
- Trusted Lists

1.3.Ferramentas

- https://lapo.it/asn1js/
- https://manpages.ubuntu.com/manpages/kinetic/man1/dumpasn1.1.html
- https://openssl-library.org/