SOFTWARE LIVRE PARA VERIFICAÇÃO DE ADEQUAÇÃO DE SERVIDORES GNU/LINUX À NORMA DE SEGURANÇA NBR ISO/IEC 27002

Acadêmico: Fernando Lucio Cugik

Orientador: Prof. Fabio Rafael Segundo

www.furb.br

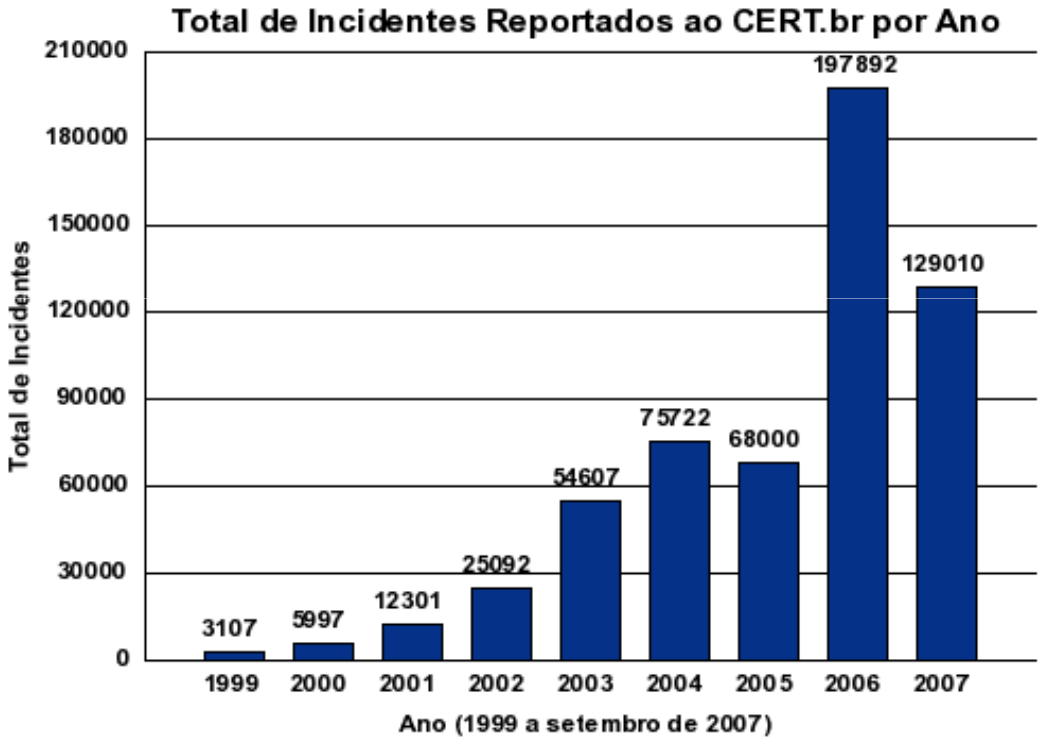
Roteiro

- Introdução
- Fundamentação teórica
- Desenvolvimento do Software Livre
- Resultados e Discussão
- Conclusão
- Extensões

Introdução

Contexto

Preocupações quanto à segurança da informação



Normas de Segurança

Segurança em servidores GNU/Linux

Objetivos do trabalho

Objetivo Principal

Desenvolver uma aplicação com interface web para auditoria de segurança em servidores GNU/Linux, verificando a sua adequação com a norma de segurança NBR ISO/IEC 27002 através da implementação e verificação dos controles da norma no servidor GNU/Linux.

Objetivos do trabalho

Objetivos Específicos

- **Trazer mais informações sobre a aplicação das normas da família ISO/IEC 27002**

- **Levantar informações atualizadas e de fontes especializadas sobre as melhores práticas de segurança em servidores GNU/Linux**

- **Desenvolver uma ferramenta baseando sua implementação nos controles da norma NBR ISO/IEC 27002 e seguindo as recomendações das melhores práticas de segurança em servidores GNU/Linux**

Objetivos do trabalho

Objetivos Específicos

- **Identificar e implementar os controles utilizados na ferramenta**
- **Emitir relatório com o resultado da verificação de adequação**
- **Comprovar o funcionamento em diferentes servidores**
- **Publicação da ferramenta como Software Livre**

Fundamentação teórica

Conceitos e tecnologias estudas para o desenvolvimento da ferramenta.

- **Segurança da Informação**
- **Norma NBR ISO/IEC 27002**
- **Software Livre**

Segurança da Informação

- **A importância da informação**
- **O que é segurança da informação?**
- **Como alcançar?**

Norma NBR ISO/IEC 27002

- **O que é?**
- **História**
- **Objetivo**
- **Como ela é organizada?**

Norma NBR ISO/IEC 27002

- **Seções(categorias):**

a) política de segurança da informação (1);

b) organizando a segurança da informação (2);

c) gestão de ativos (2);

d) segurança em recursos humanos (3);

e) segurança física e do ambiente (2);

f) gestão das operações e comunicações (10);

g) controle de acesso (7);

h) aquisição, desenvolvimento e manutenção de sistemas de informação (6);

i) gestão de incidentes de segurança da informação (2);

j) gestão da continuidade do negócio (1);

k) conformidade (3).

Software Livre

- O que é o Software Livre e as 4 liberdades

- Licenças
  - GPL
  - BSD

Desenvolvimento do Sistema

- **Levantamento dos requisitos**
- **Especificação do software livre**
  - Através dos diagramas UML de casos de uso, classes e seqüência
- **Implementação do Software Livre**
  - Contendo as técnicas, ferramentas e operacionalidade

Requisitos do Trabalho

➢ Requisitos Funcionais

Considerações quanto à auditoria de sistemas de informação (seção 15.3 da norma)
Gerar um relatório com o nível de aderência do servidor auditado
Permitir o acesso ao sistema somente por usuários autorizados e autenticados
Possibilitar a seleção dos controles para verificação
Implementar os controles da norma para servidores GNU/Linux

Requisitos do Trabalho

➢ Requisitos Não Funcionais

Processamento correto nas aplicações (seção 12.2)
Compatibilidade com distribuições GNU/Linux Debian, Fedora, Red Hat e Ubuntu
Linguagem de programação PHP e comandos BASH

Especificação do Software Livre

- **Diagramas UML (Enterprise Architect)**
  - Diagrama de casos de uso
  - Diagrama de classes
  - Diagrama de seqüência

Especificação do Software Livre

- **Diagrama de casos de uso**

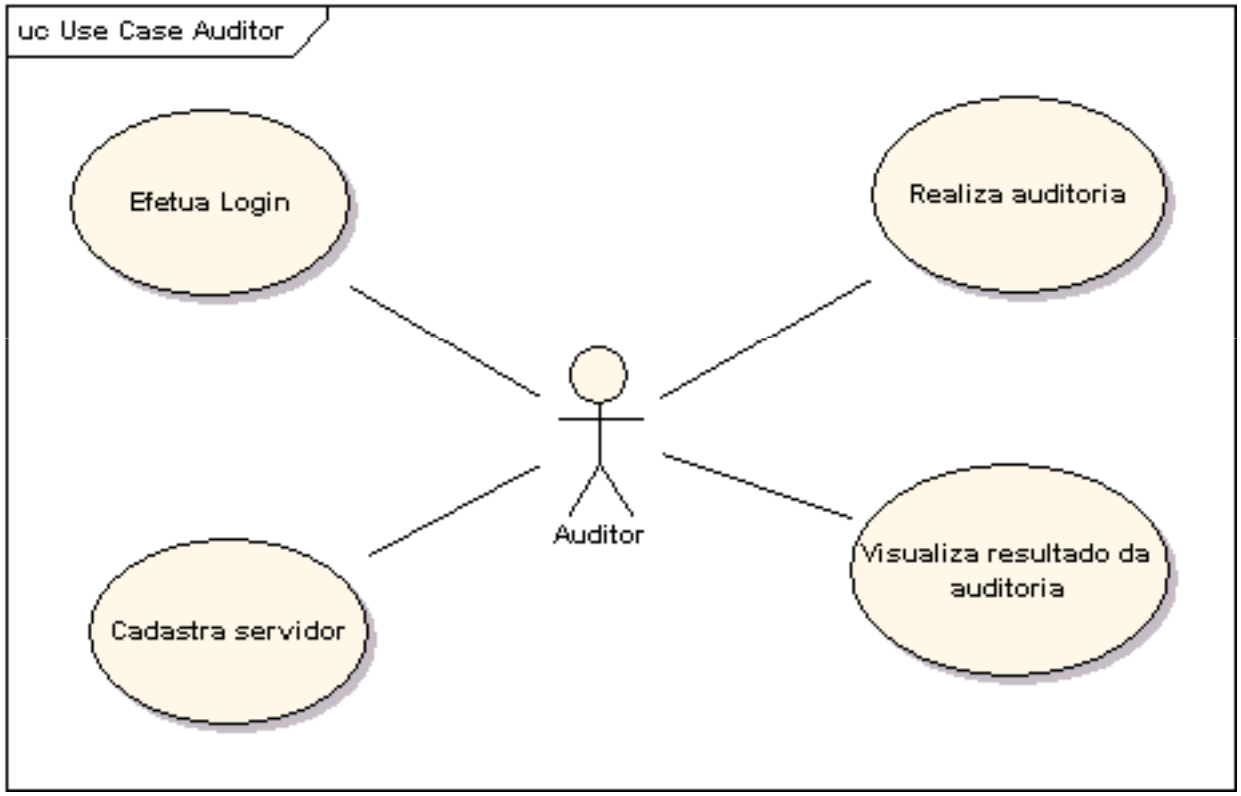


Diagrama de classes

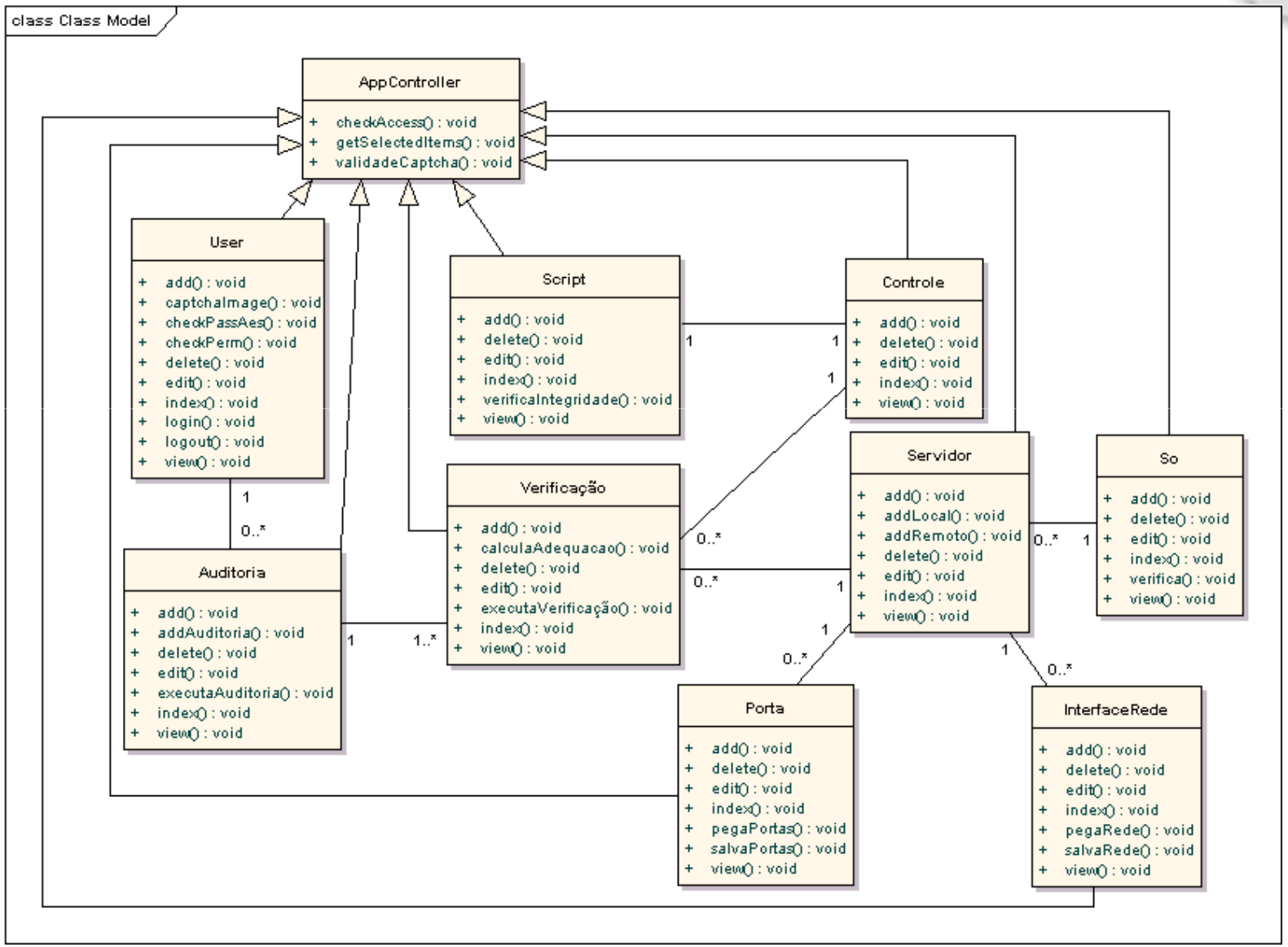
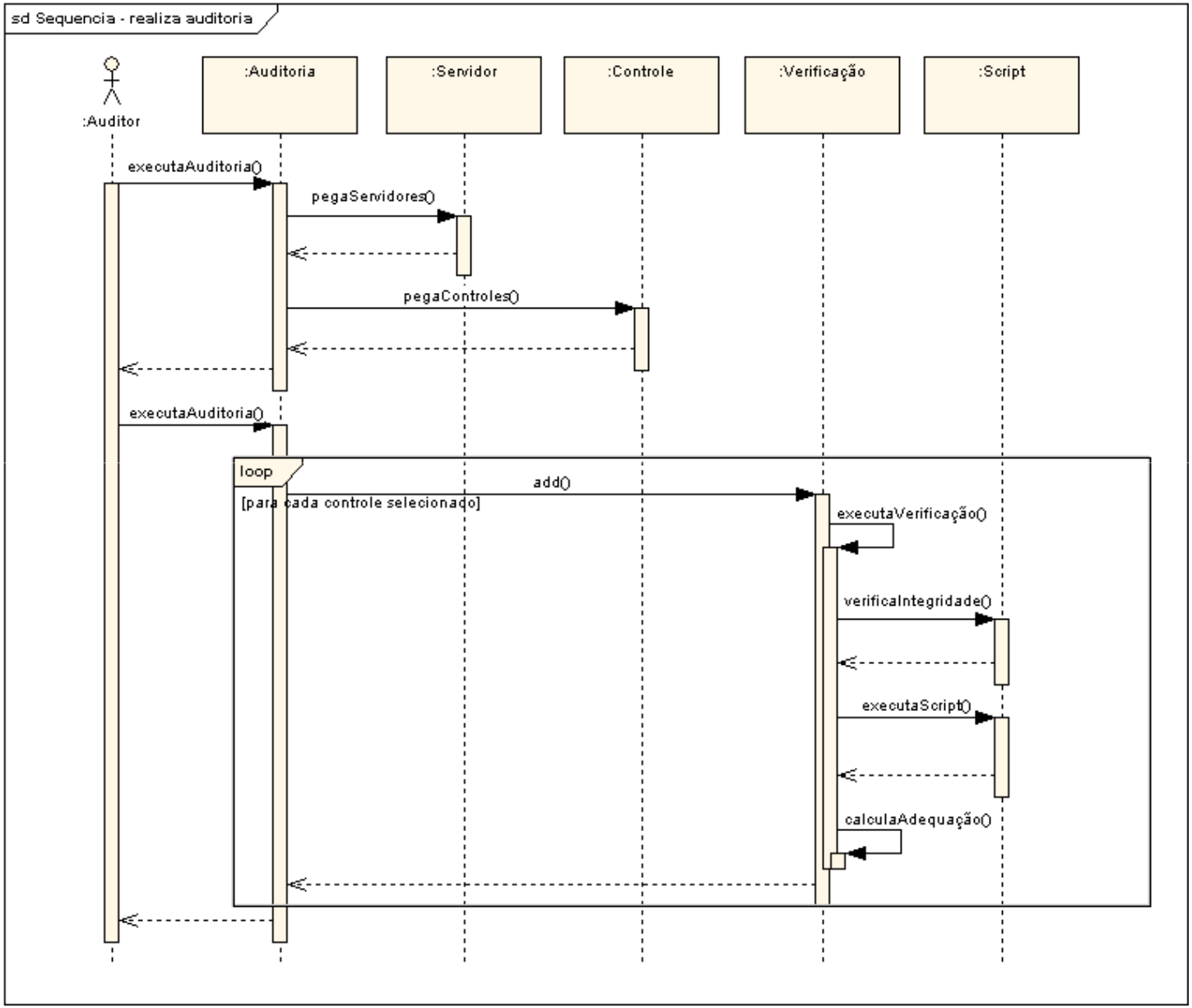


Diagrama de seqüência – Realiza auditoria



Implementação

- **Técnicas utilizadas**
  - Orientação a objetos
  - Modelagem de banco de dados
  - MVC – através do CakePHP

Implementação

- **Ferramentas utilizadas**
  - **Eclipse**
    - PHPEclipse
    - Subclipse
  - **DBDesigner**
  - **PHPMyadmin**
  - **CakePHP**
  - **Servidor web Apache**
  - **Linguagem de programação PHP**
  - **Comandos do BASH**
  - **Banco de dados MySQL e a linguagem SQL**

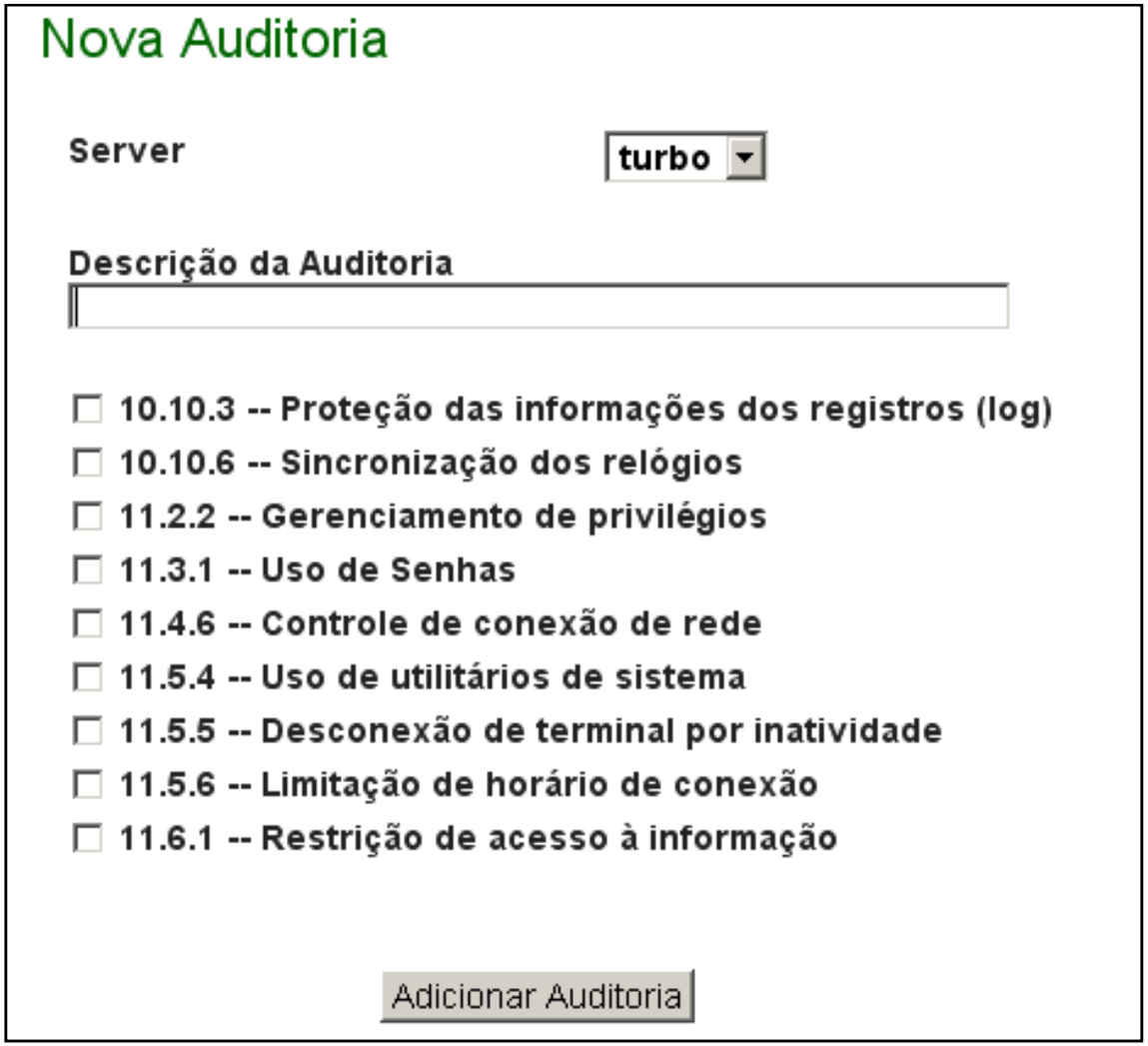
Operacionalidade

- **Utilização da ferramenta**

Tela Principal do software

Operacionalidade

➢ Utilização da ferramenta



Resultados e discussão

- Módulo de reconhecimento automático do servidor
- Suporte pelas distribuições GNU/Linux e comparativo de execução nas distribuições suportadas
- Cálculo da adequação
- Projeto e implementação pensando na segurança
- Falso positivo e falso negativo nos *scripts* e as formas de aperfeiçoamento destes
- Fácil operabilidade para o usuário auditor
- O que é necessário para publicar um software livre

Conclusão

- Importância do estudo da norma e documentos de segurança para o GNU/Linux para o desenvolvimento dos *scripts*

- Framework CakePHP trouxe produtividade

- *Scripts* podem não reconhecer todas as possibilidades

- Importância de projetar e desenvolver com os requisitos de segurança bem definidos

- Os objetivos propostos para este trabalho foram atingidos agregando conhecimento nos temas:
  - Segurança da Informação
  - Norma NBR ISO/IEC 27002
  - Segurança em servidores GNU/Linux

- Utilidade como ferramenta de segurança e na adequação à norma

Extensões

- Revisão ou melhoramento da implementação de segurança da ferramenta
- Integração com outras ferramentas de segurança
- Assinatura digital
- Relação desta ferramenta com as outras normas da família 27000.

Obrigado!

“Mantenha-se simples, bom, puro, sério, livre de afetação, amigo da justiça, temente aos deuses, gentil, apaixonado, vigoroso em todas as suas atitudes. Lute para viver como a filosofia gostaria que vivesse. Reverencie os deuses e ajude os homens. A vida é curta.”

Marco Aurélio

Imperador Romano e filósofo (121 – 180)