Grupo de Resposta a Incidentes de Segurança

O que é um incidente de segurança?

*"Qualquer evento **adverso**, confirmado ou sob suspeita, que pode ameaçar a segurança dos sistemas de computação ou das redes de computadores."*

O que é um incidente de segurança?

*"Qualquer evento **adverso**, confirmado ou sob suspeita, que pode ameaçar a segurança dos sistemas de computação ou das redes de computadores."*

- ou -

"O ato de violar uma política de segurança, explícita ou implícita."

O que é um incidente de segurança?

Exemplos:

- Tentativas (com ou sem sucesso) de ganhar acesso não autorizado a sistemas ou a seus dados

O que é um incidente de segurança?

Exemplos:

- Tentativas (com ou sem sucesso) de ganhar acesso não autorizado a sistemas ou a seus dados

- Interrupção indesejada ou negação de serviço

O que é um incidente de segurança?

Exemplos:

- Tentativas (com ou sem sucesso) de ganhar acesso não autorizado a sistemas ou a seus dados
- Interrupção indesejada ou negação de serviço
- Uso não autorizado de um sistema para processamento ou armazenamento de dados

O que é um incidente de segurança?

Exemplos:

- Tentativas (com ou sem sucesso) de ganhar acesso não autorizado a sistemas ou a seus dados
- Interrupção indesejada ou negação de serviço
- Uso não autorizado de um sistema para processamento ou armazenamento de dados
- Modificações nas características de hardware, firmware ou software de um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema

O GRIS

CSIRT formalizado para receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança dentro da UFRJ

- Centralização e organização no tratamento a incidentes
- Velocidade na resposta

O GRIS

Alguns laboratórios já contemplados:

- Laboratório de Informática da Graduação (LIG - IM)
- Laboratório de Matemática Aplicada (LABMA - IM)
- Laboratório do Curso de Informática (LCI - IM)
- Núcleo de Tecnologia Educacional para a Saúde (NUTES - CSS)
- Núcleo de Estudos do Quaternário e Tecnógeno (NEQUAT - IGeo)
- Laboratório de Gestão do Território (LAGET - IGeo)

GRIS – Muito mais que um CSIRT

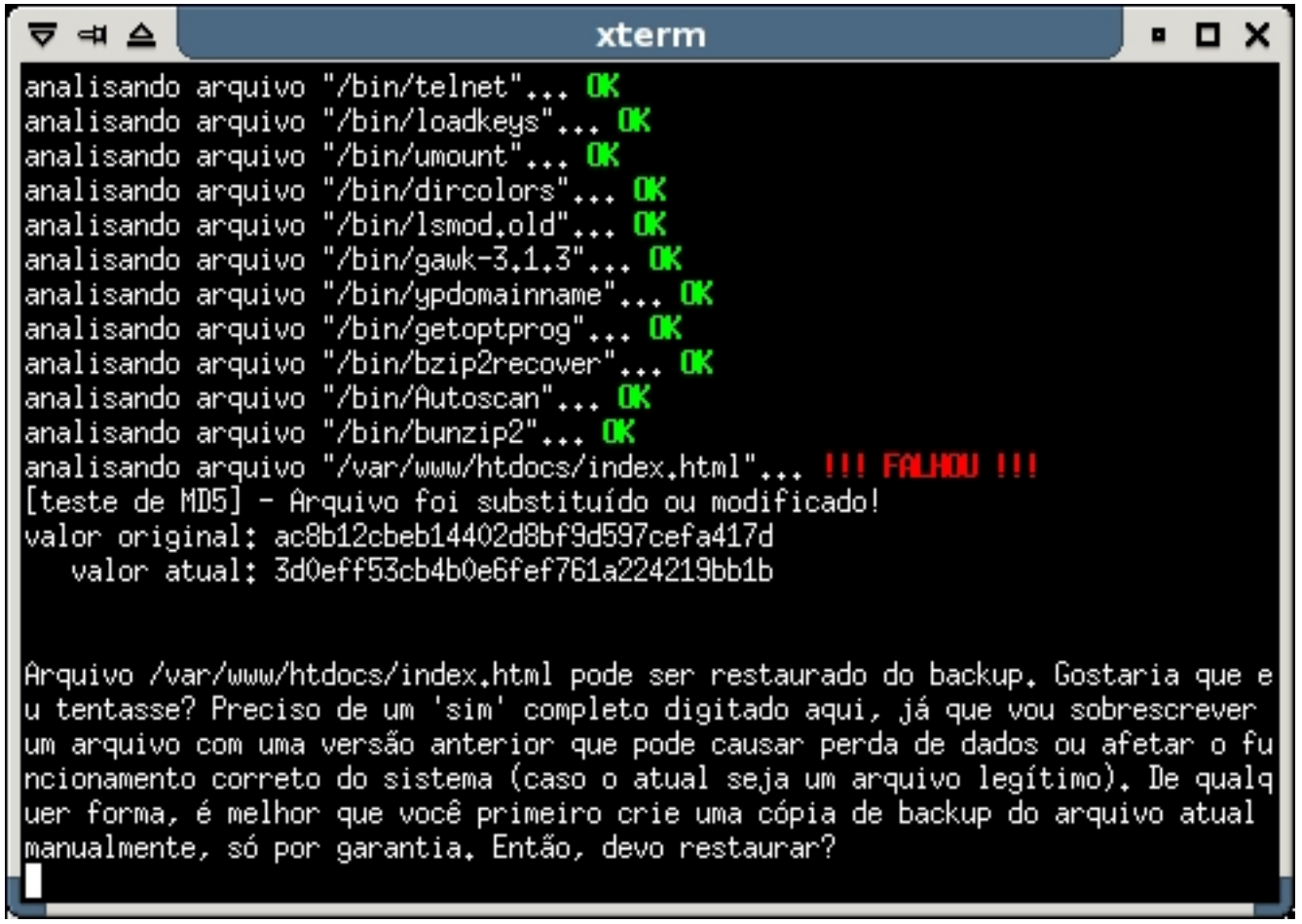
- Grupos de estudo e seminários internos

- Fomento à pesquisa e produção de

  - Artigos (populares e técnico/científicos)
  - Tutoriais
  - Ferramentas

GRIS – Projetos em Andamento

Labrador-IDS



GRIS – Projetos em Andamento

FerrO

- Varredura de portas
- Detecção de vírus
- Detecção de links quebrados
- Proxy anônimo

GRIS – Projetos em Andamento

Tamoio BSD

- Live-CD seguro baseado em OpenBSD
- Ferramentas de RI e auditoria
- Análise em redes isoladas ou com configurações específicas
- Execução de serviços provisórios (sshd, httpd) em máquinas comprometidas

GRIS – Projetos em Andamento

Truta

- Análise de Golpes (Phishing Scams)
- Busca por Golpes documentados
- Educação

Dúvidas?