Grupo de Resposta a Incidentes de Segurança

Segurança da Informação

Área de pesquisa muito ampla dentro de uma temática muito específica:

- Informática em todos os setores da sociedade

- Segurança em todos os setores da informática

GRIS

Objetivos:

- Objetivo primário: CSIRT GRIS

- GRIS Acadêmico

- GRIS na Sociedade

- GRIS UFRJ

O que é um CSIRT:

- *Computer Security Incident Response Team*

- Detecção, resolução e prevenção de incidentes de segurança

- Atuação técnica sob demanda

- Enfoque acadêmico

- CAIS - RNP

CSIRT GRIS

O que faz o CSIRT GRIS:

- Auxiliar no reparo a danos causados por incidentes de segurança

- Analisar sistemas comprometidos buscando causas, danos e responsáveis (análise forense)

- Avaliar condições de segurança da rede

- Monitorar laboratórios

- Trabalho conjunto com o NCE

GRIS ACADÊMICO

O que faz o GRIS Acadêmico:

- Treinamento, capacitação e qualificação

- Pesquisa, busca por novas tecnologias

- Atualização, interoperação e intercâmbios de informação

GRIS NA SOCIEDADE

Onde está a segurança da informação na Sociedade:

- Últimos 5 anos, problemas provindos da informática tornaram-se frequentes

- Falta de profissionais capacitados a lidar com esses problemas

- Preocupação em massa com a segurança

- Segurança nas empresas (BS7799 e ABNT27001)

GRIS NA SOCIEDADE

Como ajudar:

- Divulgação de alertas

- Educação

- Divulgação de práticas de segurança

- Informativos

GRIS e a UFRJ:

- Tornar a UFRJ centro de excelência em Segurança da Informação

- Colocar o GRIS no cenário nacional

- Interoperar com outros CSIRTS e Grupos de Segurança

- Gerar e deter tecnologia e treinamento de ponta

GRIS UFRJ

Como:

- Participar dos maiores eventos nacionais

- Trazer a atenção para a UFRJ

- Unir e interagir outros grupos de segurança acadêmicos

- Gerar tecnologia

GRIS – Muito mais que um CSIRT

Maiores dificuldades:

- Financeira

- Falta de estrutura física

- Perda de mão de obra qualificada

GRIS – Muito mais que um CSIRT

Resultados:

ALGUNS LABORATÓRIOS 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 - CCS)
- Núcleo de Estudos do Quaternário e Tecnógeno (NEQUAT - IGeo)
- Laboratório de Gestão do Território (LAGET – IGeo)
- Laboratório de Geoprocessamento (LAGEOP – IGeo)
- DRE Decania CCMN

- Total de 70 atendimentos

GRIS – Muito mais que um CSIRT

Resultados:

TRABALHOS ACADÊMICOS:

- Uma tese de mestrado e três projetos de final de curso
- Quinze publicações realizadas
- Uma apresentação em congresso internacional
- Quatro apresentações em congressos nacionais
- 5º CSIRT Acadêmico reconhecido pela RNP, sendo o 1º do estado do Rio de Janeiro
- I SegInfo – Congresso de Segurança da Informação
- II SegInfo – Workshop de Segurança da Informação
- EnCSIRTs

GRIS – Muito mais que um CSIRT

Resultados:

TECNOLOGIA:

- Labrador
- FerrO
- Truta
- Tamoio BSD
- Devoid
- Nostradamus
- PWLess
- Publicação de pesquisas: Dicas, Artigos, Tutoriais, Palestras, Cursos, etc...

GRIS – Muito mais que um CSIRT

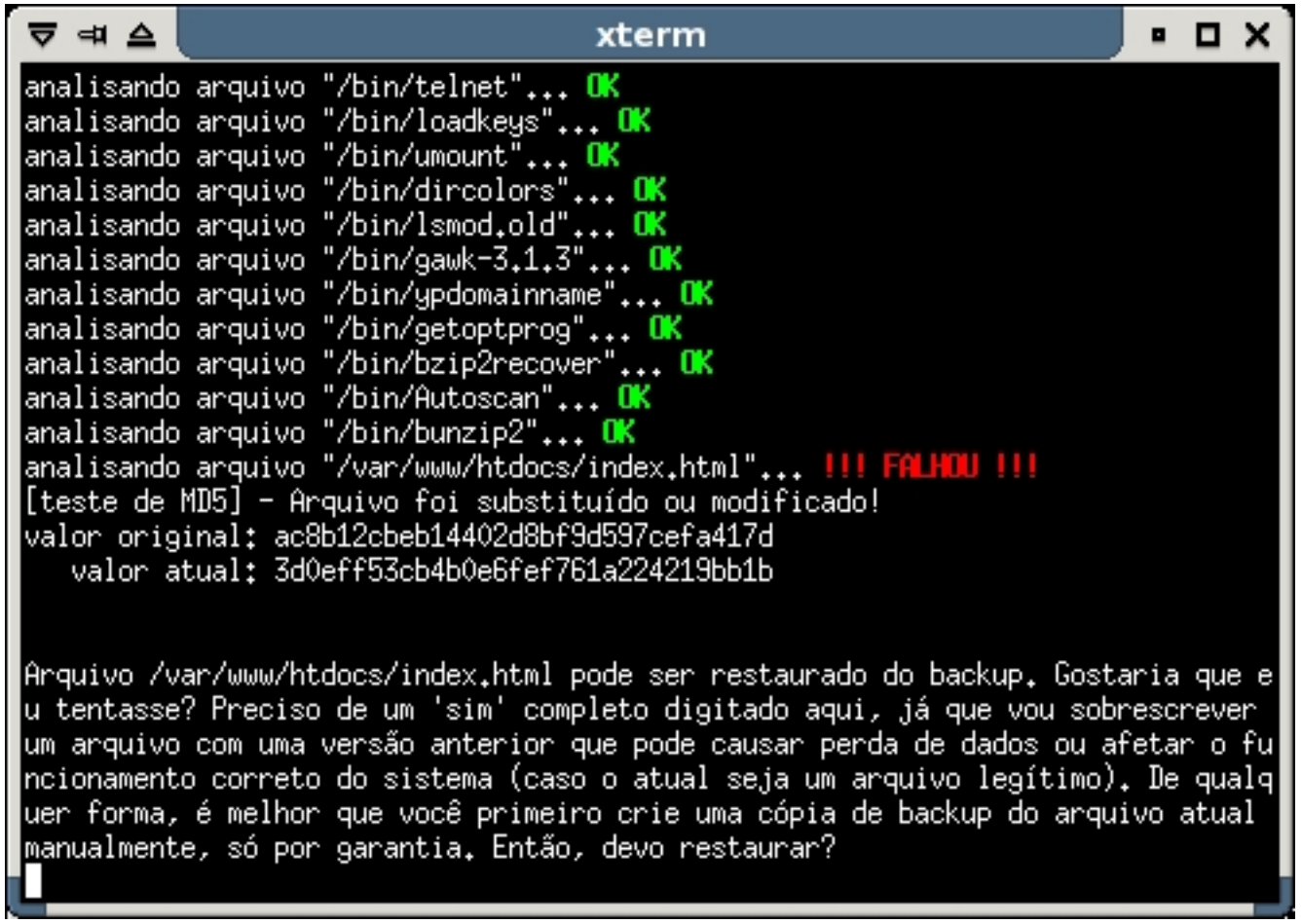
Resultados:

SOCIEDADE:

- Newsletter
- Fonte de pesquisas e informação
- Notificação nacional e internacional
- Análises de artefatos e casos
- Educação e treinamento

GRIS – Projetos em Andamento

Labrador-IDS



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 em máquinas comprometidas

GRIS – Projetos em Andamento

Truta

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

GRIS – Eventos

- SegInfo: Maior congresso de SI do Rio de Janeiro
- EnCSIRTs: Primeiro encontro de CSIRTs Acadêmicos Nacionais
- Richard's Day: Fundador da Free Software Foundation na UFRJ
- IV Fórum de Software Livre: GRIS colocando a segurança em pauta