Universidade Federal do Rio de Janeiro
Instituto de Matemática
Departamento de Ciência da Computação
Grupo de Resposta a Incidentes de Segurança

Rio de Janeiro, RJ – Brasil

Relatório de Atividades

GRIS-2005-RA-1

ESTE DOCUMENTO APRESENTA UM RESUMO DO TRABALHO DO GRIS NOS PRIMEIROS 23 MESES DE EXISTÊNCIA DO PROJETO. NESTE CONTEXTO, SÃO APRESENTADAS AS ESTATÍSTICAS DE INCIDENTES DE SEGURANÇA TRATADOS PELO GRIS, AS VULNERABILIDADES MAIS CRÍTICAS, PROJETOS, ARTIGOS, PUBLICAÇÕES, CURSOS E INFORMAÇÕES SOBRE A ÁREA DE SEGURANÇA DE MODO GERAL, NO REFERIDO PERÍODO REFERENCIADO.

GRIS – Grupo de Resposta a Incidentes de Segurança
CCMN Bloco I 1° andar
Sala: I1021
Av. Brigadeiro Trompowski, s/nº
Cidade Universitária - Rio de Janeiro/RJ
CEP: 21949-900
Telefone: +55 (21) 2598-3309

Sumário

1. Primeiro processo seletivo

O GRIS iniciou o ano de 2005 com seu primeiro processo seletivo, aberto a todos os estudantes de graduação da UFRJ. Superando todas as espectativas, contamos com a inscrição de não menos que 37 alunos dos mais variados centros, entre eles Ciência da Computação, Engenharia Elétrica, Engenharia Eletrônica, e até mesmo Geografia. O processo seletivo durou todo o mês de março e contou com três fases: dinâmica de grupo, exame de seleção e entrevista. Na dinâmica de grupo os alunos foram testados no que tange o trabalho em equipe, comunicação e liderança, características imprescindíveis para profissionais de Segurança da Informação. O processo da dinâmica foi combinado ao exame de seleção do GRIS, uma prova escrita baseada no padrão OSSTMM que testou a criatividade e a capacidade de resolução de problemas, para eliminar o maior número de candidatos. Finalmente, a entrevista individual nos permitiu identificar aqueles que melhor se encaixavam no perfil do GRIS para ocupar as 10 vagas disponíveis. É importante ressaltar que um exame de seleção com a qualidade e abrangência oferecidas só foi possível graças à parceria do GRIS com a *Insight*, empresa júnior do curso de Psicologia da UFRJ que nos deu total apoio na execução da dinâmica e da entrevista.

1º Encontro com os novos membros do GRIS 1

- Número de alunos candidatos: 37
- Candidatos selecionados: 10
- Cursos de origem:
  - Ciência da Computação
  - Engenharia Elétrica
  - Engenharia Eletrônica
  - Geografia

2. Palestras ministradas internamente

Com a entrada dos novos membros, o GRIS retomou suas palestras internas de nivelamento, procurando oferecer aos iniciantes a infraestrutura necessária para que pudessem entrar em atividade o quanto antes, sem que isso prejudicasse a eficiência e a qualidade dos serviços já prestados. Todas as palestras foram ministradas por membros do GRIS que adquiriram conhecimentos e experiências necessárias para tal tarefa. Os temas foram:

- "CSIRTs - Grupos de Resposta a Incidentes de Segurança"
- "Linux Básico"
- "Introdução ao Protocolo TCP/IP"
- "Estrutura Básica de Sistemas Windows"
- "Estrutura Básica de sistemas POSIX"
- "Gestão de CSIRTs"
- "Análise de Processos de Triagem"

Cada palestra teve em média 2 horas de duração, e procurou introduzir conceitos, elementos e procedimentos essenciais para a atividade do GRIS da maneira menos cansativa possível. Paralelamente às palestras, os iniciantes eram estimulados a solidificar o aprendizado ao aplicar os conhecimentos obtidos na resolução de problemas simples e estudos aprofundados sobre determinadas características de um macro-tema.

• Total de Palestras ministradas internamente : 7

3. SegInfo – I Congresso de Segurança da Informação da UFRJ

Durante todo o primeiro semestre de 2005 o GRIS dedicou boa parte de seu tempo na organização e estruturação do I SegInfo, um congresso de segurança da informação completo, envolvendo pesquisadores, profissionais e estudantes da área e abrangendo aspectos técnicos, jurídicos e de gestão. O SegInfo contou com o apoio incondicional do Núcleo de Computação Eletrônica da UFRJ, patrocínio do Banco do Brasil e da Fundação Universitária José Bonifácio e contou com participações nacionais e internacionais, dentre os quais (em ordem de apresentação):

- Deputado Federal Luiz Piauhylino Monteiro, autor do Projeto de Lei sobre Crimes de Informática
- Paulo Quintiliano, Chefe da Perícia de Informática da Polícia Federal
- Denny Roger, Diretor da Batori Software & Security
- Alberto Bastos, Sócio-fundador da Módulo Security Solutions
- Bernadette Castilho, Gerente de Inteligência e Segurança da Informação da Petrobrás
- Nelson Murilo Rufino, Gerente de Segurança da Pangéia Informática
- Antônio Marcelo - Responsável pelo projeto Honeypot-BR
- Gustavo Alberto, Coordenador do Curso de Pós-Graduação M.S.I. em Segurança da Informação - do NCE-UFRJ e Consultor de Segurança
- Sandro Melo, CSO da 4Linux
- Renato Opice Blum, da Opice Blum Advogados Associados
- Lance Spitzner, Fundador do "Honeynet Project"
- João Bonnassis, Consultor Técnico da EMC Brasil
- Mehran Misaghi, Coordenador do curso de pós-graduação em Segurança da Informação do IST
- Leonardo Ricciardi, pesquisador-chefe do CETAD
- Alexandre Freire, consultor de segurança sênior da Schlumberger para a América Latina
- Ronaldo Vasconcellos, Analista de Segurança do Centro de Atendimento a Incidentes de Segurança da RNP
- Wanderley Abreu Júnior, Chefe da Coordenadoria de Investigações Eletrônicas do Ministério Público do Estado do Rio de Janeiro
- Demétrio Carrión e equipe do projeto AirStrike (RAVEL/COPPE-UFRJ)
- Ivo Peixinho, Analista de Segurança Sênior do Centro de Atendimento a Incidentes de Segurança da RNP
- Breno G. de Oliveira, Diretor do GRIS-UFRJ
- Luiz F. Martins de Castro, Presidente do Instituto Brasileiro de Política e Direito da Informática
- Francisco Portugal, Conselheiro do Instituto Brasileiro de Política e Direito da Informática
- Demócrito Reinaldo Filho, Juiz de Direito e Diretor do Instituto Brasileiro de Política e Direito da Informática

O SegInfo é um congresso diferenciado de todos os eventos acadêmicos e empresariais já organizados. No SegInfo, representantes dos segmentos político, acadêmico e empresarial têm espaço para expor suas experiências com a segurança da informação e discutir suas implicações para a sociedade em todos os seus aspectos.

O Congresso é voltado para estudantes e profissionais das áreas de ciências exatas e jurídicas, executivos e gerentes de empresas com foco em tecnologia, além de acadêmicos da ciência da computação e interessados em questões relacionadas a segurança. Através de exposições e palestras de nomes chave do cenário da segurança no Brasil, coloca os participantes em contato com o que existe de mais atual no assunto.

ESTATÍSTICAS DO I SEGINFO

As palestras da manhã tiveram, em média, um público de 60 pessoas por dia, ou seja, aproximadamente 90% da capacidade máxima do auditório. As inscrições esgotaram-se uma semana antes do evento.

As palestras da tarde tiveram, em média, um público de 340 pessoas por dia, nos 4 dias de evento.

Houve ainda aqueles que assistiram as palestras on-line simultaneamente, atingindo um pico de 50 pessoas conectadas ao site do evento.

Foram ao todo 24 palestrantes do Brasil e do Mundo discutindo aspectos técnicos, jurídicos e de gestão da Segurança da Informação.

Em torno de 90 pessoas estiveram envolvidas em todas as etapas do evento, que teve seu processo organizacional iniciado em fevereiro. Há estimativas de um total de 4300 horas trabalhadas exclusivamente no evento, além de muito trabalho paralelo.

O total de palestras somou quase 30 horas.

Foi realizada uma pesquisa de opinião preenchida pelos participantes, com os seguintes resultados:
Quesito / Média (até 5)

- Conteúdo : 4,4
- Organização: 4,2
- Estrutura : 4,3
- Inscrição : 4,1
- Kits : 4,2
- Preço : 4,7
- Divulgação : 3,6

Foram ao todo 61 avaliações preenchidas.

A média de idade das pessoas que participaram do evento foi de:

- até 22 anos: 52,4%
- de 22 a 32 : 27,9%
- de 33 a 43 : 14,8%
- acima de 44: 4,9%

E o tipo de público foi:

- Universidades: 63,9%
- Órgãos Públicos: 19,7%
- Empresas: 16,4%

4. Projeto Truta

Banner do projeto Truta 1

O Projeto Truta faz parte da política proativa do GRIS e foi idealizado em virtude do alto índice de ataques do tipo “Phishing Scams”, golpes aplicados via correio eletrônico e páginas maliciosas na Web que visam obter acesso a computadores e senhas – geralmente de bancos – de usuários desavisados.

O projeto tem dois objetivos bem definidos:

- Criação de um banco de dados de golpes desse tipo, com a maior abrangência possível;
- Educação de usuários caseiros sobre como detectar, evitar e responder a ataques dessa natureza.

Dessa maneira, os usuários saberão proteger-se desse tipo de ataque e, caso ainda tenham dúvidas em relação à veracidade do *email*, poderão procurar pelo mesmo (ou por similares) na base de dados do Truta ou mesmo encaminhar o possível golpe aos nossos responsáveis, que farão a análise e responderão no menor tempo possível.

Até a data deste documento, haviam 3 (três) casos reportados no site (http://gris.dcc.ufrj.br/truta/casos.php) referentes a casos de ataques dessa natureza, sendo eles:

- Falso e-mail do Banco do Brasil
- Falso e-mail da Microsoft
- Falso e-mail da MSN

5. Projeto Tamoio

O Tamoio é sem dúvida um dos mais ambiciosos projetos do GRIS. Trata-se de uma remasterização do OpenBSD, aclamado como um dos sistemas operacionais mais seguros e confiáveis do mundo, funcionando na forma de um *live-CD* (sistemas que são executados diretamente a partir de um CD, sem modificar nada no sistema do computador hospedeiro). Seu objetivo é oferecer aos administradores de rede e profissionais da área de Segurança da Informação um sistema completo, seguro, confiável e portátil.

Dentre as principais características do Tamoio, destacam-se sua abordagem "segura por padrão" em relação aos utilitários instalados e uma suíte completa de ferramentas de segurança e administração de sistemas testadas pelo GRIS e prontas para uso.

Todas essas qualidades tornam o Tamoio ideal para computação forense, testes de invasão, auditorias locais e remotas, recuperação de desastres e, naturalmente, utilização como um sistema local para uso e aprendizado.

O resultado desse ambicioso projeto está disponível para *download* no site do GRIS em (http://www.gris.dcc.ufrj.br/tamoio.php) sua versão mais atualizada e em constante atualização.

6. Projeto Labrador

O Labrador é uma ferramenta multiplataforma desenvolvida para identificar quaisquer modificações indesejadas feitas em seu sistema. Pode ser utilizado como verificador de integridade e como sistema de detecção de intrusão local (HIDS).

O que começou como um simples verificador de integridade evoluiu para um sistema completo de detecção, prevenção e resposta a invasões, violações de política e mudanças indesejadas de um modo geral em sistemas computacionais.

Hoje o Labrador conta com as mesmas características de ferramentas similares já consagradas no mercado, além de verificações exclusivas idealizadas a partir do reconhecimento das necessidades reais de administradores de redes, que não podem perder tempo com verificações manuais mas também não podem se dar ao luxo de negligenciar a segurança de seus sistemas.

Outra característica marcante do Labrador é seu enfoque na facilidade de uso. O principal motivo disso foi a percepção de que a problemática de modficações indesejadas não se prende apenas a profissionais da Informática, mas também afeta usuários caseiros com poucas noções de segurança e nenhum tempo a perder com ferramentas complicadas e procedimentos obscuros.

O Labrador está disponível para *download* no site do GRIS em (http://gris.dcc.ufrj.br/ferramentas.php).

7. Projeto FerrO

O Projeto FerrO – contração para *Ferramentas Online* – baseia-se na construção de um núcleo de ferramentas de segurança disponibilizadas diretamente no site do GRIS para uso direto ou download. É o desenvolvimento de um Framework com objetivo de auxiliar nas buscas por soluções de segurança para o usuário final.

Sabemos que atualmente, a maior causa do tráfego malicioso que existe na Internet é a desinformação do usuário final, que deixa incontáveis brechas em seus sistemas, prontas para serem exploradas por usuários e programas maliciosos. O Projeto FerrO, tem a intenção de auxiliar pessoas tecnicamente não capacitadas a fazer uma avaliação de segurança e informar sobre falhas em seu sistema.

Baseado no conceito de *home-scan*, muito utilizado nas empresas de antivírus, o Projeto FerrO terá como primeira ferramenta o VPO - Sésamo. O VPO - Sésamo (Varredura de Portas Online - Sésamo) poderá ser utilizado por qualquer usuário da grande rede, e servirá para retornar informações de status de interfaces nas máquinas que o acessarem.

Outras ferramentas já estão em desenvolvimento nesta suíte de aplicações para a Web, sempre com o intuito de ajudar a comunidade a sanar a maior deficiência criada pela rapidez do desenvolvimento tecnológico humano: a desinformação de parte da população.

As ferramentas estão desponíveis para *download* no endereço http://gris.dcc.ufrj.br/ferro/index.pl

8. Palestras ministradas para o DCC (sobre o GRIS)

Durante seu processo de formalização ante ao Departamento de Ciência da Computação, o GRIS realizou três eventos especiais com os professores. O primeiro foi a apresentação da proposta inicial de atuação do GRIS, sua formação inicial e importancia não apenas como um grupo de resposta, mas como suporte acadêmico a todos os alunos de graduação que desejassem se especializar na área de Segurança da Informação. O segundo foi a apresentação do Projeto GRIS em reunião de departamento para aprovação. Finalmente, o terceiro foi uma apresentação das atividades do GRIS aos alunos de mestrado do NCE/IM, como forma de divulgação do trabalho do GRIS e do I Congresso de Segurança da Informação da UFRJ, o I SegInfo.

Todas as apresentações contaram com público atento e receptivo, que ficaram bastante satisfeitos com as propostas e atividades do GRIS.

- Total de palestras ministradas para o DCC: 3

9. Resumo sobre as ferramentas

Todas as ferramentas disponibilizadas no GRIS foram desenvolvidas por seus próprios membros e são liberadas para a comunidade sob a licença GPL. São elas:

Labrador: Ferramenta multiplataforma desenvolvida para identificar quaisquer modificações indesejadas feitas em seu sistema. Pode ser utilizado como verificador de integridade e como sistema local de detecção de intrusão.

Devoid: Script de terminal que varre o sistema em busca de usuários e grupos definidos mas que não possuam nenhum arquivo ou diretório (contas e grupos que provavelmente podem ser removidas do sistema sem causar complicações, ajudando o mesmo a permanecer mais seguro).

Nostradamus: Ferramenta que gera listas de possíveis senhas a partir de palavras chaves arbitrárias e parâmetros especiais, podendo ser utilizada em ataques de dicionário, identificando que tipo de senhas *NÃO* devem ser utilizadas.

Pwless: Ferramenta multiplataforma escrita em Perl capaz de identificar configurações suspeitas em arquivos

de senha *NIX, como contas sem senha, contas do sistema permitindo login, e contas com privilégios de *root* (além da própria 'root').

Estas são as **quatro** ferramentas mais recentes do GRIS e que estão disponíveis para *download* no site do Grupo em http://www.gris.dcc.ufrj.br/ferramentas.php

10. Resumo sobre as dicas

Como parte de sua política proativa, o GRIS mantém em seu sítio na Web uma seção dedicada exclusivamente à divulgação de pequenas dicas relacionadas à Segurança da Informação. Tratam-se de informações pontuais sobre os mais variados assuntos, muito requisitadas por administradores de redes e usuários caseiros mas que acabam ocultas em enormes manuais de configuração ou em meio a anotações rabiscadas em arquivos esquecidos.

Todas as dicas disponibilizadas pelo GRIS são antes validadas pela equipe e formatadas de modo a conter o máximo de informação relevante e o mínimo de dados desnecessários ao processo, além de uma descrição concisa sobre o objetivo da dica e quaisquer contra-indicações. Dentre as que já foram publicadas, podemos citar:

- Série *"Escondendo versões de programas"*, cujo objetivo é ensinar rapidamente os procedimentos necessários para esconder as versões de uma série de programas servidores, de modo a dificultar a ação de atacantes. Os programas já contemplados por essa série incluem: Apache, BIND, OpenSSH, Sendmail e Proftpd.
- *"Monitorando tráfego da rede em Tempo Real"*, ensina a exibir em tempo real os pacotes que circulam pelo computador, facilitando a detecção de tráfego anômalo como bots, varreduras de portas, etc.
- *"Criando um CD de Instalação do OpenBSD com Inicialização"* mostra como criar facilmente um CD de instalação do sistema operacional OpenBSD que inicia direto do CD.
- *"Definindo zonas de Segurança do Internet Explorer"* demonstra como personalizar as configurações de segurança para as zonas de internet do Internet Explorer.
- *"Restringindo Registro de Crawlers com o 'robots.txt'"* mostra como criar seu próprio arquivo "robots.txt" para que sites de busca indexem apenas as páginas que você quiser em seu site.

• Total de dicas disponibilizadas no site do GRIS: 5

11. Resumo sobre os artigos e tutoriais

A partir de estudo e pesquisa direcionados, os membros do GRIS são estimulados a culminarem seu aprendizado repassando à comunidade os conhecimentos obtidos. Isso é feito através da construção sistemática de artigos e tutoriais, disponibilizados pública e gratuitamente em nosso sítio na Web.

Os artigos podem ser **técnicos** ou voltados para o **usuário leigo**, especialmente quando abordam boas práticas ou procuram elucidar conceitos obscuros da área de Segurança da Informação. Dentre os artigos já publicados, temos:

- "Fundamentos da Criptologia Parte I": Iniciando a série "Fundamentos da Criptologia", este artigo visa introduzir o leitor no mundo da criptografia e criptoanálise, apresentando fatos históricos e curiosidades sobre o tema.

- "Fundamentos da Criptologia Parte II": Continuando a série "Fundamentos da Criptologia", este artigo aborda a

criptografia de chave simétrica, apresentando cifras de substituição como a ROT-X, Vigenère, entre outras mono e polialfabéticas, com exemplos em linguagem C.

- "Fundamentos da Criptologia Parte III": Continuando a série "Fundamentos da Criptologia", este artigo complementa o artigo anterior no tema de criptografia de chave simétrica, apresentando cifras computacionais como XOR, DES e suas variações, com exemplos em linguagem C.

- "Google como Ferramenta de Ataque (e Defesa) a Sistemas": Artigo demonstrando como o Google (e outros buscadores da Internet) podem ser explorados para efetuar, desde o levantamento de informações e roubo de senhas a invasões completas, e como proteger-se desses problemas. Mostra, entre outras coisas, recursos poderosos mas pouco conhecidos do buscador Google, capazes de filtrar suas buscas para alvos específicos.

- "Como Escolher uma Senha": Artigo que expõe a problemática das senhas para usuários caseiros e sugere uma série de métodos simples de criação de senhas minimamente seguras, indicando vantagens, desvantagens e peculiaridades de cada um deles.

- "Honeypots": Possui como principal objetivo o entendimento dos conceitos inerentes a honeypots, sua origem e desenvolvimento, bem como suas características e aplicações práticas.

Os tutoriais procuram sempre descrever passo-a-passo instalação e uso de uma determinada ferramenta de segurança, ou explicitar uma metodologia ou procedimento que possa ser reproduzido facilmente através de passos bem definidos. Dentre os tutoriais já publicados, temos:

- "Usando o GNU Privacy Guard (GnuPG)": Ensina passo-a-passo como instalar, configurar e utilizar o GnuPG para criptografar e assinar arquivos e mensagens de correio eletrônico em diversas plataformas, com exemplos em Windows e GNU/Linux.
- "Procurando por 'Rootkits' em sistemas GNU/Linux": Ensina a instalar e usar o chkrootkit e o rkhunter, alem de como fazer algumas buscas manualmente por arquivos com SUID root, etc.
- "Recompilando o kernel linux": Ensina detalhadamente as etapas necessárias para (re)compilar um kernel Linux, tão importante para a manutenção de um sistema seguro e, no entanto, tantas vezes negligenciado por administradores pela mística da dificuldade dos procedimentos.
- "Restrição de Acesso a Servidores Apache Baseada em Autenticação por Senha": Ensina a restringir o acesso a áreas específicas de seu sítio web rodando o servidor Apache por IP, usuários ou grupos, através do arquivo *".htaccess"* e derivados.

- Total de tutoriais e artigos produzidos: **10**

12. I SegInfo CSIRT

Vertente do SegInfo que trata da discussão acerca dos "Computer Security Incident Response Team", ou Grupos de Resposta a Incidentes Computacionais de Segurança, o I SegInfo CSIRT's pretende firmar-se como o principal evento no Brasil para o intercâmbio de idéias relacionadas aos CSIRT's. Para isso, a primeira versão do SegInfo CSIRT's já contará com a presença de membros dos principais CSIRT's acadêmicos e empresariais do Brasil. O contato com estes grupos será feito através do GRIS, que é o CSIRT do DCC-IM da UFRJ, e dos próprios organizadores do SegInfo, que já possuem um canal de comunicação estabelecido com eles. Este evento lançará definitivamente a UFRJ como referência nacional e internacional na área de Segurança da Informação, nas áreas acadêmica, de pesquisa e profissional. Entre os principais grupos que deverão participar do evento estão os seguintes:

- CAIS/RNP -- Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Pesquisa
- CERT.br -- Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
- CERT-RS -- Computer Emergency Response Team - Rio Grande do Sul
- CSIRT ABN AMRO Real
- CSIRT Santander Banespa
- CSIRT Embratel
- CSIRT Unicamp -- Computer Security Incident Response Team - Universidade Estadual de Campinas

- CTIR Gov -- Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal
- Equipe de Seguranca de Redes e Resposta a Incidentes - Universidade de São Paulo - USP
- GRC/Unesp - Grupo de Redes de Computadores / Universidade Estadual Paulista "Julio de Mesquita Filho"
- Grupo de Segurança da RedeRio - CEO/RedeRio
- GSR/INPE -- Grupo de Segurança de Redes - Instituto Nacional de Pesquisas Espaciais
- NARIS - Núcleo de Atendimento e Resposta a Incidentes de Segurança da UFRN
- CSIRT Star One
- CSIRT Telefonica

Formato do I SegInfo CSIRT's

O I SegInfo CSIRT's acontecerá ao longo de dois dias, 2 e 3 de fevereiro de 2006, e terá início às 9:00 prolongando-se até as 18:00, com pausa de 12:30 às 14:00 para almoço. O local do evento será um auditório (a ser definido) que deverá ter capacidade para acomodar entre 100 e 120 pessoas. Nas manhãs acontecerão três exposições curtas, com duração total de uma hora (incluído o tempo para perguntas). Após o almoço, acontecerão três palestras mais longas (uma hora e vinte minutos) no primeiro dia, enquanto no segundo dia acontecerão duas palestras curtas seguidas de um debate. O I SegInfo CSIRT's está programado para acontecer na primeira quinta e sexta-feira (dias 2 e 3) de fevereiro de 2006.

Atividades

As atividades do I SegInfo CSIRT's serão as palestras, grupos de discussão e mesa-redonda:

- Palestras: ocuparão a maioria da grade horária do evento. Serão palestras de profissionais escolhidos cuidadosamente com o objetivo de expor as práticas mais modernas e as questões mais desafiadoras envolvendo CSIRT's.
- Grupos de Discussão: envolverá a discussão de temas de interesse a líderes de CSIRT's.
- Mesa Redonda: Irá fechar o evento e terá a participação de personalidades-chave da S.I. no Brasil.

Público Alvo

O público esperado para o I SegInfo CSIRT's é um público mais especializado que na versão "geral" do SegInfo. Deverão estar presentes CSO's de grandes empresas, líderes de CSIRT's e profissionais de segurança de alto nível em geral, somados ainda exclusivamente aos interessados da UFRJ, sejam alunos, professores, profissionais ou curiosos. A quantidade de participantes deverá girar em torno de 100 pessoas, entre profissionais, e pessoas ligadas à UFRJ (estudantes e acadêmicos).

13. II SegInfo

O II SegInfo ocorrerá entre os dia 22 a 25 de agosto de 2006. A segunda versão deste já reconhecido evento de segurança contatará com a presenças dos mais respeitados nomes nacionais e internacionais da Segurança da Informação. O projeto “II SegInfo” já está em fase final de documentação. Apartir do dia 20 de outubro de 2005, iremos remeter o pedido de patrocinio para deversas instituições. Algums instituições já entraram em contato com os membros da equipe do GRIS que lideram a área de projetos, com o interesse de participar ou até patrocinar o evento. Entre elas podemos citar:

- Petrobrás
- Departamento de Policia Federal do Brasil (Área de Crimes de Informática)
- ABIN (Agência Brasileira de Inteligência Nacional)
- Furnas Centrais Elétricas
- Fundação Real Grandeza

Logo, consideramos que a possibilidade de II SegInfo repetir ou até expandir o sucesso de sua primeira versão é extenso.

14. II Processo Seletivo

Já está aberto o II Processo Seletivo do GRIS. Assim como no primeiro processo, os candidatos passarão pelas etapas de prova escrita, dinâmica de grupo e entrevista. Todas as etapas serão executadas pelos membros mais experientes do GRIS e supervisionado pelo Coordenador do projeto.

Até o momento da edição deste documento, já haviam 35 alunos inscritos no processo, que está divulgado em pontos estratégicos dos centros CCMN e CT através de cartazes. Para efetivar a inscrição, o candidato deve ir ao site do GRIS (www.gris.dcc.ufrj.br), acessar o link disponível na página principal e preencher o formulário de inscrição.

Após as etapas citadas, os aprovados passarão por um período de treinamento que consiste em palestras dos mais variados assuntos. Essas palestras serão ministradas pelos membros e colaboradores mais experientes do GRIS e ocorrerão nas dependências do Grupo ou em salas cedidas pelo DCC.

15. Notícias publicadas

No sítio do GRIS há, constantemente atualizada, uma lista das três notícias mais recentes sobre os assuntos referentes à segurança da informação e a temas do Grupo. No caso de o visitante desejar ter acesso às notícias anteriores, há uma opção para listar todas as notícias já publicadas.

16. Participação do GRIS no FISL 6.0

O GRIS foi destaque no FISL 6.0. O Grupo de Resposta a Incidentes de Segurança apresentou o projeto Labrador ao mundo no sexto **Fórum Internacional de Software Livre**, realizado entre os dias 1 e 4 de junho em Porto Alegre. O evento contou com a participação de personalidades do mundo da informática, como Eric Raymond (diretor da OSI e autor do livro *The Cathedral and the Bazaar*) e Jon 'Maddog' Hall (diretor da Linux International), sendo assistida presencialmente por 4400 pessoas e via Internet por mais de 12 mil pessoas. O Fórum assumiu destaque na mídia nacional e internacional, como na rede televisiva BBC de Londres. O aluno-diretor do GRIS, Breno Guimarães de Oliveira, criador da ferramenta Labrador, fez sua palestra de uma hora em auditório cheio no dia 4 de junho, onde apresentou a ferramenta e discutiu seu futuro com a comunidade.

Figura 1 - Breno G. de Oliveira no FISL 6.0

16. Participação do GRIS na II Semana de Software Livre

Durante o período entre 18/10/2004 e 20/10/2004, os membros do GRIS fizeram uma série de minicursos relacionados a segurança de computadores, por ocasião da II Semana de Software Livre realizada na UNIRIO. A participação visou aprimorar o conhecimento dos mesmos para melhor atender às atividades do Projeto GRIS.

Os minicursos realizados foram:

18/10 - Tutorial Construção de Firewalls para Segurança de Perímetro de Redes com Software Livre
Palestrante: Sandro Melo
Membros participantes: Frederico Henrique Bohm Argolo
Duração: 4 horas

19/10 - Instalação e configuração de um sistema OpenLDAP
Palestrante: Marcone Luis Theisen
Membros participantes: Bruno Salgado Guimarães
Duração: 9 horas

20/10 - Monitoramento com Software Livre
Palestrante: Rodrigo Albina
Membros participantes: Breno Guimarães de Oliveira, Bruno Salgado Guimarães
Duração: 4 horas

17. Participação do GRIS na III Semana de Software Livre

Com a parceria da empresa Clavis Segurança da Informação, o GRIS participou da III Semana de Software Livre, realizada na UNIRIO, oferecendo uma palestra e um minicurso de 8 horas, ambos voltados para Segurança da Informação. Foram eles:

15/10 - Segurança da Informação com Software Livre
Palestrantes: Breno Guimarães de Oliveira e Fábio Martins dos Santos
Membros participantes: Victor B. da S. Santos
Duração: 8 horas.

16/10 - Labrador, uma Ferramenta Multiplataforma de Verificação de Integridade
Palestrante: Breno Guimarães de Oliveira
Duração: 50 minutos

18. Atendimento aos laboratórios da UFRJ

Uma das atividades do GRIS é a visita aos laboratórios que tenham sofrido algum incidente de segurança da informação e fazer um trabalho de reparo dos incidentes e prevenção de futuros incidentes.

Como resultado, temos os seguintes laboratórios da UFRJ atendidos, com valores aproximados de visitas que foram necessárias para a solução dos problemas.

- LCI: 13 visitas
- LABMA: 3 visitas
- LIG: 5 visitas
- NUTES: 2 visitas
- LAGEOP: 10 visitas (Laboratório sendo atendido)
- PPGG: 12 visitas (Laboratório sendo atendido)
- EDUGEO: 9 visitas (Laboratório sendo atendido)
- DRE: 4 visitas

- NEQUAT: 2 visitas

• Total de visitas realizadas em laboratórios da UFRJ: **60** visitas

19. Teses e projetos finais gerados através de pesquisas no GRIS

Com o conhecimento adquirido no GRIS os membros inspiram-se para fazer seus trabalhos finais de curso e escolher seus temas de mestrados com base nas atividades e assuntos do Grupo. Dessa forma, já temos alguns resultados nesse sentido como por exemplo os listados abaixo:

Projeto Final de Curso

Autor: Breno Guimarães de Oliveira
Título: Automatização em Computação Forense
Descrição: O projeto avalia macro etapas necessárias em um procedimento de computação forense de redes e sistemas arbitrários e propõe um modelo para o mesmo, verificado através da criação de ferramenta de execução automática das etapas previstas, da coleta à correlação dos dados em forma de evidências. O projeto foi concebido graças a experiência do autor nas atividades do GRIS, cuja estrutura foi utilizada também para grande parte dos testes da ferramenta.

Autor: Bruno Salgado Guimarães
Título: Criando CSIRTs em Universidades: Metodologias, Problemas, Soluções e Guia Prático de Implantação
Descrição: Este projeto final visa, a partir do estudo de caso dos problemas e soluções encontradas durante o processo de implantação do GRIS-DCC-IM-UFRJ, estabelecer metodologias e recomendações para todas as etapas necessárias para a criação e evolução de um CSIRT Universitário. Esse projeto é unico e inovador no Brasil, visto que não existem documentos específicos para a implantação de CSIRTs no país - e o GRIS foi o meio pelo qual esse macro-projeto tornou-se possível.

Autor: Frederico Henrique Bohm Argolo
Título: Análise Forense em Sistemas GNU/Linux
Descrição: O projeto faz um levantamento sobre as necessidades legais de um procedimento de computação forense em ambientes GNU/Linux, bem como técnicas e ferramentas necessárias para realizar tal procedimento nos dias de hoje. Para tal, o autor contou com toda a infraestrutura do GRIS e pode dessa forma realizar diversos testes, validações e refutações de ferramentas.

Projeto de Mestrado

Autor:Raphael Machado
Título: Caos e Criptografia
Descrição: O trabalho faz uma análise das aplicações da área de sistemas dinâmicos caóticos à comunicação segura de informações. Estas aplicações abrangem a segurança de informações discretas (sinais digitais) e contínuas (sinais contínuos). Por fim, propõe-se a extensão de conceitos da criptografia tradicional (como segurança, difusão e mistura) para o domínio das transformações contínuas.

• Total de teses e projetos finais gerados através de pesquisas no GRIS: **4**