Resposta a Incidentes de Segurança em Ambientes Computacionais

II Workshop de Segurança da Informação
DISI – Dia Internacional de Segurança em Informática

Rafael Soares Ferreira

Grupo de Respostas a Incidentes de Segurança - GRIS/DCC/IM/UFRJ
www.gris.dcc.ufrj.br
rafael@gris.dcc.ufrj.br

Clavis Segurança da Informação
www.clavis.com.br
rafael@clavis.com.br

Agenda

- Conceitos
- Etapas
- Análise em Sistemas Unix
- Análise em Sistemas Windows
- Referências

Conceitos

Segurança da Informação

Garantia de:

- Disponibilidade
- Confidencialidade
- Integridade

Conceitos

CSIRTS

- *“Computer Security Incident Response Team”*
- Respostas, Tratamentos e Prevenção
- Podem ser Técnicos ou de Coordenação
- RFC 2350

Conceitos

Incidentes

- Eventos que ameacem a Segurança da Informação
- Violação da Política de Segurança da Informação

Conceitos

Principais Tipos de Incidentes

Negação de Serviço

- Consumo excessivo de recursos (banda, disco ou CPU)
- Quebra de componentes físicos
- Queda de desempenho ou indisponibilidade completa
- DoS, DDoS e DRDoS

CLAVIS segurança da informação

2008 DISI eu participo!

Principais Tipos de Incidentes

Códigos Maliciosos

- Vírus, Worms, Keyloggers, Rootkits, Trojan Horses etc
- Roubo/Destruição de Informações
- Consumo de recursos computacionais

Principais Tipos de Incidentes

Acesso Não Autorizado

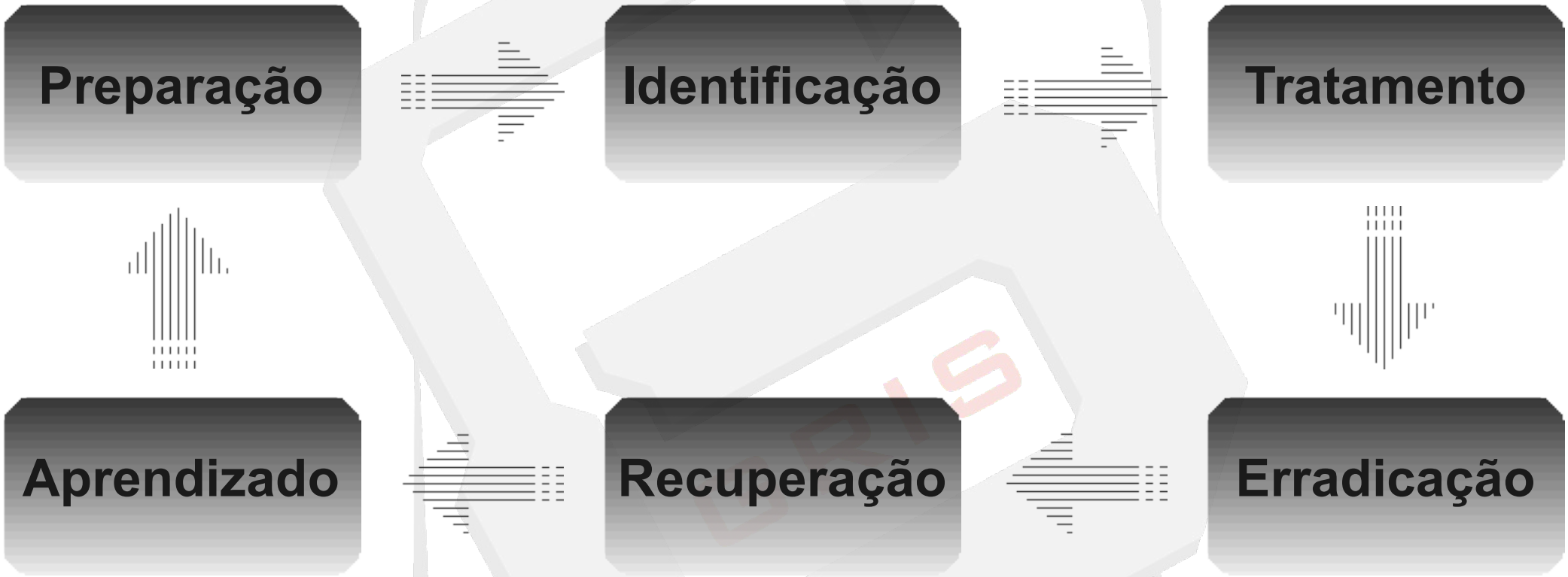
- Acesso físico ou lógico à recursos de TI
- Violação de sistemas de autenticação e monitoramento

Principais Tipos de Incidentes

Uso abusivo

- Violação de políticas de uso aceitável
- Utilização de recursos para atividades não autorizadas

Etapas



CLAVIS
segurança da informação

2008 DISI
eu participo!

Etapas

Preparação

Contatos

- Responsáveis administrativos, CSIRTs, Autoridades
- Telefones, endereços de email, chaves públicas

CLAVIS segurança da informação

2008 DISI eu participo!

Etapas

Preparação

Sistema para registros de incidentes

- Telefone celular ou fixo em regime 24x7
- Endereço de email destinado a equipe de RI
- Formulário on-line

Etapas

Preparação

Software para Criptografia

- Comunicação segura
- Armazenamento seguro
- Integridade, Confidencialidade e não-repúdio

CLAVIS segurança da informação

2008 DISI eu participo!

Etapas

Preparação

War room

- Conversas envolvendo informações sigilosas
- Configurações e medidas de defesa
- Análise de Incidentes
- Permanente ou sob demanda

CLAVIS segurança da informação

2008 DISI eu participo!

Etapas

Preparação

Dispositivo seguro de armazenamento

- Coleta de evidências
- Proteção de materiais sensíveis
- Backups

CLAVIS segurança da informação

2008 DISI eu participo!

Etapas

Preparação

"*Sniffers*" e Analisadores de Protocolos

- Monitoramento da rede
- Captura do tráfego de rede
- Análise da atividade de rede recente

Etapas

Preparação

Documentação

- Principais vulnerabilidades
- Topologia da rede
- Serviços e versões

CLAVIS segurança da informação

2008 DISI eu participo!

Etapas

Preparação

Binários confiáveis

- Sistemas comprometidos não são confiáveis
- Ferramentas de análise e diagnóstico
- Executados a partir de mídias removíveis

Etapas

Preparação

“*Known Goods*” ou “*Known Bads hashes*”

- Verifica a integridade dos arquivos
- Identifica presença de malwares conhecidos
- Base de HIDS

CLAVIS
segurança da informação

2008 DISI
eu participo!

Etapas

Identificação

- Comportamento anômalo detectado por IDSs
- Alertas de Anti-vírus, anti-spyware, anti-spam etc
- Verificações de integridade
- Logs de Sistemas Operacionais, serviços e aplicações
- Novas vulnerabilidades ou exploits (0-day)
- Alerta de usuários

CLAVIS segurança da informação

2008 DISI eu participo!

Etapas

Tratamento

- Danos ou perda de informações
- Preservação das evidências
- Disponibilidade do Serviço
- Tempo e recursos necessários para o tratamento
- Efetividade do tratamento

CLAVIS
segurança da informação

2008 DISI
eu participo!

Etapas

Erradicação

- Remoção de artefatos maliciosos
- Remoção de usuários e serviços não utilizados
- Localização e remoção de arquivos ocultos

Etapas

Recuperação

- Restauração de backups
- Validação através de Varreduras de Vulnerabilidades
- Aplicação de patches e atualizações

Etapas

Aprendizado

- Política de atualização
- Auditoria de sistemas
- Auditoria de redes
- Proteção contra artefatos maliciosos
- Concientização e Treinamento

CLAVIS segurança da informação

2008 DISI eu participo!

Análise em sistemas Unix

- Diretórios e arquivos com logs de eventos

  /var/log/

- Listagem de eventos recentes

  wtmp, who,last, lastlog

- Configurações de rede

  arp –an, route -n

Análise em sistemas Unix

- Conexões de rede

  netstat –tupan, lsof –i

- Listagem de usuários do sistema

  more /etc/passwd

- Tarefas agendadas

  more /etc/crontab, ls /etc/cron.*

Análise em sistemas Unix

- Configurações de resolução de nomes

  more /etc/resolv.conf, more /etc/hosts

- Serviços iniciados junto com o boot

  ls /etc/rc*.d

- Listagem dos processos em execução

  ps aux

Análise em sistemas Unix

- Arquivos modificados recentemente

  ls –lart /, find / -mtime 2

- Histórico de comandos executados

  bash_history

Análise em sistemas Windows

- Visualizador de Registro de eventos

  eventvwr

- Configurações de rede

  arp –a, netstat -nr

- Conexões de rede

  netstat –nao, netstat -vb, net session, net use

Análise em sistemas Windows

- Listagem de grupos e usuários

  net users, net localgroup [grupo]

- Programas iniciados junto com o boot

  autorun

- Listagem de processos

  taskmgr

Análise em sistemas Windows

- Listagem dos serviços

  net start

- Configurações de resolução de nomes

  more %SystemRoot%\System32\Drivers\etc\hosts, ipconfig /displaydns, ipconfig /all

- Verificação de integridade dos arquivos do sistema

  sigverif

Análise em sistemas Windows

- Arquivos modificados recentemente

  dir /a/o-d/p %SystemRoot%\System32

- Windows Explorer modifica diversos arquivos, utilize preferencialmente o cmd

Referências

- **Handbook for Computer Security Incident Response Teams (CSIRTs)** - Carnegie Mellon University and Software Engineering Institute

- **Computer Security Incident Handling Guide** - National Institute of Standards and Technology (NIST)

CLAVIS segurança da informação

2008 DISI eu participo!

Dúvidas?

Muito Obrigado!