Apresentação, Metodologia e Recomendações do NBSO—NIC Br Security Office

Cristine Hoepers
<cristine@nic.br>
Klaus Steding-Jessen
<jessen@nic.br>

SSI'99
Simpósio Segurança em Informática
São José dos Campos–SP
14–16 de setembro de 1999

Apresentação, Metodologia e Recomendações do NBSO

- Apresentações: CG, GTS, NBSO
- Forma de operação
- Casos Acompanhados
- Recomendações

Comitê Gestor—CG

Criado por portaria interministerial MCT/MC 147, de 31 de maio de 1995.

- Recomendar padrões e ética de uso para a Internet no Brasil

- Atribuição de IPs e registro de domínio

CG—Estrutura

- Membros
- Grupos de Trabalho
  - GTS
  - GTER
  - GTRH

GTS

- Assessora o CG. Subgrupos:
  - SGTS-Backbones
  - SGTS-Provedores
- Desenvolve ferramentas, documentos e padrões organizacionais relacionados com a segurança da Internet/Br

NBSO—NIC Br Security Office

- Criado em junho de 1997

- Atua coordenando as ações e provendo informações para os sites envolvidos nos incidentes reportados

NBSO—NIC Br Security Office

- Recebe notificações de incidentes de segurança

- Encaminha essas notificações para os responsáveis das redes envolvidas

- Correlaciona dados

- Se necessário, ajuda no site (dependendo da gravidade)

Como Proceder num Incidente

- quem contactar
  - responsáveis pelo domínio / backbone
  - NBSO <nbso@nic.br>
- não retirar de imediato a máquina da rede ou reinstalar
- preservar evidências
  - Não remover nenhum arquivo
  - fazer backup completo

Como Proceder num Incidente (cont)

- monitorar as atividades na máquina
  - monitorar todos os acessos pela rede
  - arquivos inseridos ou modificados pelo invasor
  - backdoors / processos
  - contas criadas / utilizadas
- reinstalação segura
  - corrigir as vulnerabilidades detectadas durante a monitoração

Aspectos Legais

Legislação:

- Não há lei específica
  - Projeto de Lei 84, de 1999
- Crimes previstos nas leis vigentes
  - Escuta telemática (sniffing)
  - Dano

Aspectos Legais (cont)

Evidências Válidas:

- Sniffers instalados
- Alterações no sistema (arquivos, processos, etc)
- Logs
- Monitoração do tráfego do invasor

Vulnerabilidades mais Exploradas

- rpc.cmsd
- rpc.statd
- mountd
- IIS

Evidências mais comuns após uma Invasão

- rootkit (ps, netstat, ifconfig, ls, login, last, etc)
- sniffer
- backdoor / shell suid
- trojan de sshd / inetd / popd / fingerd
- bots de IRC

Deficiências Graves nos Casos Acompanhados

- Uso de protocolos como pop, ftp, telnet
  - Resistência à troca
- Ausência de sistema de log (syslogd)
- Análise de logs inexistente / ineficiente
- Falta de NTP

Deficiências Graves nos Casos Acompanhados (cont)

- Utilização de backups comprometidos
- Serviços desnecessários ou desconhecidos pelo administrador
- Tripwire com base de dados na própria máquina
- Falta de reclamações de ataques
- Filtragem de pacotes inexistente / ineficiente

Casos Acompanhados
Exemplo #1

Instituição A

- Invasores com acesso privilegiado em várias máquinas
- o telnetd foi substituído por um trojan, dando acesso privilegiado sem senha
- acessavam essas máquinas de dezenas de sites (Brasil e exterior)
- eram utilizadas como base para ataques a redes brasileiras, .gov, .com e .edu (EUA) além de outros países

Casos Acompanhados
Exemplo #1 (cont)

- contas próprias foram criadas no sistema
- registraram domínios informando as contas criadas como email de contato
- usavam as máquinas como repositório de dados e ferramentas
- registraram nomes no DNS

Casos Acompanhados
Exemplo #1 (cont)

Deficiências na Instituição A

- não possuiam syslogd
- utilizavam somente telnet, ftp, pop, etc.
- não verificavam as origens das conexões dos seus usuários
- não verificavam os programas em execução
- senha de root muito fraca
- mantinham serviços desnecessários

Casos Acompanhados
Exemplo #2

Instituição B

- obtiveram acesso privilegiado em diversas máquinas
- instalação de sniffer, capturando todos os pacotes de conexões telnet, ftp e smtp
- instalação de vários backdoors (que eram iniciados via rc)
- modificação do inetd e outros programas
- ftp dos mails da máquina para sites no exterior

Casos Acompanhados
Exemplo #2

Deficiências da Instituição B

- utilizavam somente telnet, ftp, pop, etc.
- utilizavam backups comprometidos
- não verificavam programas em execução
- mantinham serviços desnecessários

Recomendações

- uso de ssh, S/KEY
- aplicação de patches / atualização do sistema
- manter apenas serviços imprescindíveis
- filtragem de pacotes

Recomendações (cont)

- pgp
- log host centralizado
- sincronização de relógio via NTP
- md5 / tripwire
- denunciar scans e tentativas de invasão

Colaboradores do NBSO

- SACC/PF — Setor de Apuração de Crimes por Computador

- CAIS/RNP — Centro de Atendimento a Incidentes de Segurança

- Movimento Brasileiro Anti-Spam

URLs de Interesse

- http://www.nic.br/nbso.html
- http://www.nic.br/book
- http://www.cg.org.br
- http://www.antispam.org.br
- http://www.cais.rnp.br