Tratamento de Incidentes de Segurança na Internet Br pelo NBSO

NIC Br Security Office

<nbso@nic.br>

http://www.nic.br/nbso.html

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

Security Forum '99
Rio de Janeiro–RJ
19–20 de outubro 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)

- analisar as atividades suspeitas na máquina
  - analisar todas as conexões não autorizadas
  - arquivos inseridos ou modificados pelo invasor
  - backdoors / processos
  - contas criadas / utilizadas
- reinstalação segura
  - corrigir as vulnerabilidades detectadas durante a análise

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
- Análise do tráfego do invasor

Vulnerabilidades mais Exploradas

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

Vulnerabilidades mais Exploradas (cont)

ftp://ftp.technotronic.com/unix/

```
[DIR] Parent Directory
[DIR] aix-exploits . . . . . .  [Sep 18 08:58]
[DIR] bsd-exploits . . . . . .  [Apr 22 15:00]
[DIR] cgi-bin-exploits . . . . .  [Aug 18 18:03]
[DIR] digital-exploits . . . . .  [Apr 22 13:04]
[DIR] ftpd-exploits. . . . . .  [Sep 15 18:12]
[DIR] hp-ux-exploits . . . . . .  [Oct 14  1998]
[DIR] irix-exploits. . . . . .  [Jul  7 00:07]
[DIR] linux-exploits . . . . . .  [Oct  7 12:44]
[DIR] log-tools. . . . . .  [Jun 25 15:14]
[DIR] mail-exploits. . . . . .  [Jun 25 14:43]
[DIR] nameserver-exploits. . . .  [Aug  1 17:03]
[DIR] network-scanners . . . . .  [Oct  3 11:11]
[DIR] network-sniffers . . . . .  [Sep 22 13:45]
[DIR] packet-assembly. . . . . .  [Jul 20 18:14]
[DIR] passwd-crackers. . . . . .  [Dec  3  1998]
[DIR] sco-exploits . . . . . .  [Oct 13 08:20]
[DIR] security-tools . . . . . .  [Jul 26 08:20]
[DIR] solaris-exploits . . . . .  [Sep 28 22:50]
[DIR] sun-exploits . . . . . .  [May 24 23:24]
[DIR] tcp-exploits . . . . . .  [Apr 23 11:40]
[DIR] trojans. . . . . .  [Aug 19 10:16]
[DIR] udp-exploits . . . . . .  [Mar 27  1998]
```

Vulnerabilidades mais Exploradas (cont)

ftp://ftp.technotronic.com/microsoft/

```
[DIR]   Parent Directory
[FILE]  iis-injector.c . . . . .  [Jun 16 11:51]
[FILE]  iishack.asm. . . . . .  [Jun 15 22:27]
[FILE]  iishack.exe. . . . . .  [Jun 15 22:26]
[FILE]  lc15exe.zip. . . . . .  [Nov  5  1997]
[FILE]  lc252install.zip . . . .  [Jun 15 12:27]
[FILE]  lsasecrets.c . . . . . .  [May  5  1998]
[FILE]  msproxy2_0_exploit.tx. .  [Oct 11  1998]
[FILE]  nat10_tar.gz . . . . . .  [Jul  6  1998]
[FILE]  nat10bin.zip . . . . . .  [Nov  5  1997]
[FILE]  nc11nt.zip . . . . . .  [Feb  7  1998]
[FILE]  ncnt090.zip. . . . . .  [Nov  5  1997]
[FILE]  ncx.exe. . . . . .  [Jun 16 15:53]
[FILE]  ncx99.exe. . . . . .  [Jun 16 09:28]
[FILE]  net-fizzV0.1.zip . . . .  [Jun 13 13:00]
[FILE]  netbus.zip . . . . . .  [Aug 25  1998]
[FILE]  netmonex.tgz . . . . . .  [Jan 31  1998]
[FILE]  nn29a.exe. . . . . .  [Oct 19  1998]
[FILE]  nn29b.exe. . . . . .  [Apr 23 11:30]
[FILE]  noaccess.txt . . . . . .  [Apr  7  1998]
[FILE]  nph-iefinal.exe. . . . .  [May  3  1998]
[FILE]  nstat.c. . . . . .  [Oct  1  1998]
[FILE]  ntfaq2.zip . . . . . .  [May  5  1998]
```

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
- tcpwrappers como única forma de proteção
- 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
- 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 (cont)

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
- análise constante do tráfego da rede

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

- Mails e URLs de Interesse
  - <nbso@nic.br>
  - http://www.nic.br/nbso.html
  - http://www.cg.org.br
  - http://www.antispam.org.br
  - http://www.cais.rnp.br
  - http://www.nic.br/book
  - http://www.securityfocus.com