Segurança em Redes - Linux

Realizado em 17/04/1998

- Arnaldo Mandel - IME - am@ime.usp.br
- Adriano Nagelschmidt Rodrigues - IME - anr@ime.usp.br

Conceituação

1. Protegendo o quê?
2. Protegendo do quê/quem?
3. Qual a real possibilidade de acontecer um ataque.
4. Implementar medidas de proteção, com análise de custo/benefício.
5. Ter esquema de revisão e aprimoramento.

Identificando Recursos

- Hardware
- Software
- Dados
- Gente
- Documentação
- Material de consumo

Hardware

- CPU's, placas
- teclados

- terminais, estações, micros
- impressoras
- drives de disco, fita, CD
- linhas de comunicação

Software

- Programas fonte
- Programas objeto
- Utilitários
- Programas de diagnóstico
- Sistemas operacionais
- Programas de comunicação

Dados

- Em execução
- On-line
- Off-line
- Backups
- Logs
- Bancos de dados
- Dados em fluxo de comunicação

Ataques

- Acesso não autorizado a recursos e/ou informação
- Divulgação não intencional/autorizada de informação
- Negação de serviço

Tradeoffs de segurança

- serviços oferecidos X segurança provida
- facilidade de uso X segurança
- custo da segurança X custo de possíveis ataques

Diretrizes gerais

- Atendimento a serviços realmente usados
- Separação de serviços
- Tudo permitido / tudo proibido

BIBLIOGRAFIA

WWW:

- COAST
- CERT
- Rootshell
- Jornal da RNP

Textos:

- Practical UNIX & Internet Security, 2nd Edition
- Site security handbook (online)

USENET: -- Vários grupos

Listas:

seguranca@pangeia.com.br via majordomo@pangeia.com.br

bugtraq@netspace.org via listserv@netspace.org (arquivos)

Segurança interna de um sistema

- Autenticação
- Proteção de arquivos
- Fraquezas clássicas
- Sistemas de detecção

Autenticação

Usuário identificado por (username, password)

Passwords estão criptografados em /etc/passwd, /etc/shadow, mapas de NIS, NIS+

Autenticação: criptografar o password dado e comparar com o registrado

Procedimento de login

Login:

exec login -p username

Password

Se autentica

su - user

Proteção de arquivos

- User, group, other
- Permissão de execução: suid, sgid
- Permissões especiais para diretórios

Fraquezas clássicas

Password:

Quem descobre um password passa a ser o usuário.

Métodos:

- Olho
- Engenharia social
- Ataques de força bruta - crack

Suid:

Programas suid devem ser escritos com máximo cuidado. Exemplos de ataques:

- Race conditions: durante o tempo que leva para amarrar um objeto físico a um objeto lógico, altera-se o objeto físico
- Esmagamento da pilha (stack smashing, buffer overrun, overwriting a buffer): programas mal escritos não verificam se os dados estão sendo lidos dentro de memória alocada para isso. Dados especialmente construídos podem instalar código na pilha de execução, e dar um login de root.
- Seguir links simbólicos: um core dump às vezes segue um link simbólico. Permite que se sobreescrevam arquivos do sistema.

\tmp:

Diretórios que permitem escrita pública podem servir para certas brincadeiras. Principalmente quando usados por programas que escrevem arquivos de nome previsível.

Exploits (programas de exploração):

www.rootshell.com contém vários programas que exploram essas fraquezas para obter senha de root. Outros pacotes chamados rootkits instalam versões de programas dos sistema que permitem ação não detectável.

Sistemas de detecção

- Crack
- COPS
- tripwire

Segurança de rede

- Conectividade
- Serviços
- Protetores
- Firewalls

Conectividade

PERIGOS:

- Ataques físicos
- Negação de serviço

Serviços

- Nomes (NIS e DNS): Ambos serviços permitem variadas formas de impostura, e passagem de informações falsas. Remédio: BIND bem configurado.
- Login remoto: telnet e rlogin mandam senha aberta pela rede. rlogin permite login remoto sem autenticação, na base da confiança . Remédio: ssh.
- Mail: Correio eletrônico deve ser confiável, confidencial e eficiente. O popular sendmail não é nenhum dos três, e tem o clube do ``bug do mês''. Remédio: qmail.
- WWW: Servidores de WWW podem ser induzidos a capturar arquivos e executar programas indevidos. O popular Apache pode ser configurado para evitar esses problemas.

Protetores

- TcpWrapper: Permite controlar acesso a cada serviço de rede, permitindo ou negando por domínio, IP, usuário.
- Tcpserver : Permite controlar o uso de recursos por um daemon.

Firewalls

Idéia

Prevenção e Detecção de Intrusões

- Prevenção:
  - Utilizar versões seguras de software - patches de segurança
  - Configurar levando em conta a sgurança
  - Usar ferramentas como tcpwrappers e firewalls
  - Educar os usuários
- Detecção:
  - tripwire
  - verificação de logs - swatch
  - monitoramento periódico de uso de recursos

Tratamento de Intrusões

Dilema: minimizar prejuízo X contra-atacar

- Minimizar prejuízo
  - Fechar acessos - contas, logins, conexões
  - Matar processos
  - Reinstalar o sistema
  - Recuperar dados
- Contra-ataque
  - Ler The Cuckoo's Egg, por Cliff Stoll .

- Determinar origem do ataque
- Contactar sistemas de origem
- Avisar listas/entidades apropriadas

Esperar que a legislação se adapte a essa realidade