Segurança e Auditoria de Sistemas

- Auditoria
  - Coleta de dados,
  - Análise de dados,
  - Auditoria preventiva

Auditoria

- Auditaria:
  - Coleta
    - recolher dados sobre o funcionamento de um sistema ou aplicação e
  - Análise
    - descobrir vulnerabilidades ou
    - violações de segurança, ou
    - examinar violações já constatadas, buscando suas causas e possíveis consequências [Sandhu and Samarati, 1996].

Coleta de dados

- Os dados de interesse devem ser coletados
  - a partir de suas fontes e
  - registrados de forma adequada para
    - análise e
    - arquivamento.
- Dependendo da natureza do evento a coleta pode ser feita
  - Aplicação
    - Ações realizadas por um servidor HTTP.
  - Sub-sistema
    - Ações no espaço de usuário do sistema operacional. Ex. Autenticação de usuários e falhas.
  - Núcleo
    - eventos envolvendo hardware
    - Eventos internos do núcleo (sockets, semáforos, memória, reinicialização...)

Coleta de dados

- Aspecto importante – forma de representação.
  - Arquivo de registro (logfiles)
    - Sequencia cronológica de descrições textuais de eventos
    - Normalmente, uma linha por evento.
      - No UNIX – autenticação de usuários -/var/log/segurity

```
...
Sep  8 23:02:09 espec sudo: e89602174 : user NOT in sudoers ; TTY=pts/1 ; USER=root ; COMMAND=/bin/su
Sep  8 23:19:57 espec userhelper[20480]: running '/sbin/halt' with user_u:system_r:hotplug_t context
Sep  8 23:34:14 espec sshd[6302]: pam_unix(sshd:auth): failure; rhost=210.210.102.173  user=root
Sep  8 23:57:16 espec sshd[6302]: Failed password for root from 210.103.210.173 port 14938 ssh2
Sep  8 00:08:16 espec sshd[6303]: Received disconnect from 210.103.210.173: 11: Bye Bye
Sep  8 00:35:24 espec gdm[9447]: pam_unix(gdm:session): session opened for user rodr by (uid=0)
Sep  8 00:42:19 espec gdm[857]: pam_unix(gdm:session): session closed for user rafael3
```

Coleta de dados

- A infra-estrutura tradicional de registro de eventos dos sistemas UNIX é
  - daemon chamado syslogd (System Log Daemon).
    - usa um socket local e um socket UDP
    - recebe mensagens descrevendo eventos,
      - geradas pelos demais sub-sistemas e aplicações através de uma biblioteca específica.
    - registra a data de cada evento recebido e
    - decide seu destino:
      - armazenar em um arquivo,
      - enviar a um terminal,
      - avisar o administrador,
      - ativar um programa externo ou
      - enviar o evento a um daemon em outro computador..
  - Os eventos são:
    - descritos por mensagens de texto e
    - rotulados por suas fontes em
      - serviços
        - (AUTH, KERN, MAIL, etc.) e
      - níveis
        - (INFO, WARNING, ALERT, etc.).

Análise de dados

- **O objetivo** da análise é identificar possíveis violações da segurança
  - em andamento (online) ou
  - já ocorridas (offline).

- Uma vez registrada a ocorrência de um evento de interesse para a segurança do sistema, deve-se proceder à sua análise.
  - sobre os registros dos eventos à medida em que são gerados (online)
    - é importante que seja rápida e leve.
    - visa detectar problemas de segurança com rapidez, para evitar que comprometam o sistema.
      - Anti-vírus.
  - sobre registros previamente armazenados (offline).
    - pode ser mais profunda e detalhada
    - possivelmente de vários sistemas
    - não tem compromisso com uma resposta imediata
    - permitindo o uso de técnicas de mineração de dados
      - para buscar correlações entre os registros, que possam levar à descoberta de problemas de segurança mais sutis.
    - usada em sistemas de detecção de intrusão,
      - para analisar a história do comportamento de cada usuário
      - frequentemente usada em sistemas de informação bancários

Análise de dados

- As ferramentas de análise de registros de segurança podem adotar duas abordagens:
  - Análise por assinaturas ou
    - tem acesso a uma base de dados contendo **informações sobre os problemas** de segurança conhecidos.
      - Ex.: antivírus
    - Um problema com essa forma de análise é sua incapacidade de detectar novas ameaças cuja assinatura não esteja na base.
  - Análise por anomalias.
    - base de dados descrevendo o que se espera como **comportamento ou conteúdo normal** do sistema.
    - O maior problema com esta técnica é caracterizar corretamente o que se espera como comportamento **normal**
    - pode ocasionar muitos erros.
      - Falso positivo e falso negativo.

Auditoria preventiva

- Além da coleta e análise de dados sobre o funcionamento do sistema, a auditoria pode agir de forma **preventiva**.
  - Buscando problemas potenciais que possam comprometer a segurança do sistema.
  - Há um grande número de ferramentas de auditoria, que abordam aspectos diversos da segurança do sistema, entre elas [Pfleeger and Pfleeger, 2006]:
    - *Vulnerability scanner*
    - *Portscanner*
    - *Rootkit scanner*
    - *Verificador de integridade*

Ferramentas de auditoria

- *Vulnerability scanner*:
  - verifica os softwares instalados no sistema e
  - confronta suas versões com uma base de dados de vulnerabilidades conhecidas,
  - identificar possíveis fragilidades,
  - investigar as principais configurações do sistema,
  - ferramentas deste tipo : *Metasploit*, *Nessus Security Scanner* e SAINT (*System Administrator's Integrated Network Tool*).

Ferramentas de auditoria

- *Portscanner*:
  - Analisa as portas de rede abertas em um computador remoto, buscando identificar
    - os serviços de rede oferecidos pela máquina,
    - as versões do softwares que atendem esses serviços e
    - a identificação do próprio sistema operacional subjacente.
    - O *NMap* é provavelmente o *scanner* de portas mais conhecido atualmente.

Ferramentas de auditoria

- *Password cracker*:
  - tentar descobrir as senhas dos usuários, para avaliar sua robustez.
  - A técnica normalmente usada por estas ferramentas é o ataque do dicionário
    - Ex. o *John the Ripper* para UNIX e *Cain and Abel* para Windows.
- *Rootkit scanner*:
  - visa detectar a presença de *rootkits* em um sistema,
  - normalmente usando uma técnica *offline* baseada em assinaturas
  - normalmente as ferramentas de detecção devem ser aplicadas a partir de uma mídia externa confiável (CD ou DVD).

Ferramentas de auditoria

- Verificador de integridade:
  - a segurança do sistema operacional depende da integridade do núcleo e dos utilitários necessários à administração do sistema.
  - analisam periodicamente os principais arquivos do sistema operacional,
    - comparando seu conteúdo com informações previamente coletadas.
    - Para agilizar a verificação de integridade são utilizadas somas de verificação (checksums) ou resumos criptográficos como o MD5 e SHA1.
    - Essa verificação de integridade pode se estender a outros objetos do sistema, como
      - a tabela de chamadas de sistema,
      - as portas de rede abertas,
      - os processos de sistema em execução,
      - o cadastro de softwares instalados, etc.
      - Ex. Tripwire [Tripwire, 2003].