Segurança Computacional

Auditoria

Prof. Carlos Maziero

DInf UFPR, Curitiba PR

Julho de 2019

Conteúdo I

Introdução

Auditoria

Auditar

Coletar dados sobre o funcionamento de um sistema e **analisá-los** para descobrir **violações de segurança**, ou para examinar violações já constatadas, buscando suas possíveis **causas e consequências**.

Atividades-chave da auditoria:

- Coleta de dados
- Análise de dados

Coleta de dados

Coleta de dados

Um sistema computacional processa uma grande quantidade de eventos.

- abertura/fechamento de arquivos
- lançamento de processos
- recepção/envio de pacotes de rede

Alguns eventos são relevantes para a segurança do sistema:

- Autenticação de um usuário
- Tentativa malsucedida de autenticação
- Mudança de credenciais
- Lançamento/encerramento de um serviço

Os dados desses eventos devem ser coletados e registrados de forma adequada para a análise e arquivamento.

Pontos de coleta de dados

Aplicação: eventos internos, com semântica específica à aplicação.

- Ocorrem dentro da aplicação
- Normalmente registrados pela própria aplicação
- Muitas vezes usam formatos próprios para os registros.

Exemplos:

- Ações realizadas por um servidor HTTP (páginas fornecidas, páginas não encontradas, erros de autenticação, pedidos não suportados, etc.)

Pontos de coleta de dados

Sub-sistema: eventos não específicos a uma aplicação.

- ocorrem no espaço de usuário do sistema operacional.
- Registro a cargo dos processos ou bibliotecas envolvidos.

Exemplos:

- Autenticação de usuários (ou erros de autenticação)
- lançamento ou encerramento de serviços do sistema
- atualizações de software ou de bibliotecas
- criação ou remoção de usuários, etc

Pontos de coleta de dados

Núcleo: eventos relacionados ao núcleo do sistema operacional.

- Inacessíveis aos processos dos usuários
- Registro a cargo do núcleo

Exemplos:

- Eventos envolvendo o hardware (detecção de erros ou mudança de configurações)
- eventos internos do núcleo (criação de *sockets* de rede, semáforos)
- Boot/reboot/shutdown do sistema

Pontos de coleta de dados

Rede: eventos relacionados ao tráfego de rede.

- Envolvem hosts locais e remotos
- Rede local ou toda a rede corporativa
- Coletados através de sondas em locais estratégicos

Exemplos:

- Estabelecimento de conexões TCP
- Pacotes de gerenciamento ICMP e IGMP
- Varredura de hosts e portas

Representação de dados

Registro de um evento:

- Data/hora
- Origem
- Descrição
- Detalhes

Formas de armazenamento:

- Arquivo de texto (*log files*)
- Base de dados

Arquivo de log UNIX

```
1  Sep  8 23:02:09 espec sudo: e89602174 : user NOT in sudoers ; TTY=pts/1 ; USER=root ; COMMAND=/bin/su
2  Sep  8 23:19:57 espec userhelper[20480]: running '/sbin/halt' with user_u:system_r:hotplug_t context
3  Sep  8 23:34:14 espec sshd[6302]: pam_unix(sshd:auth): failure; rhost=210.210.102.173  user=root
4  Sep  8 23:57:16 espec sshd[6302]: Failed password for root from 210.103.210.173 port 14938 ssh2
5  Sep  8 00:08:16 espec sshd[6303]: Received disconnect from 210.103.210.173: 11: Bye Bye
6  Sep  8 00:35:24 espec gdm[9447]: pam_unix(gdm:session): session opened for user rodr by (uid=0)
7  Sep  8 00:42:19 espec gdm[857]: pam_unix(gdm:session): session closed for user rafael3
8  Sep  8 00:49:06 espec userhelper[11031]: running '/sbin/halt' with user_u:system_r:hotplug_t context
9  Sep  8 00:53:40 espec gdm[12199]: pam_unix(gdm:session): session opened for user rafael3 by (uid=0)
10 Sep  8 00:53:55 espec gdm[12199]: pam_unix(gdm:session): session closed for user rafael3
11 Sep  8 01:08:43 espec gdm[9447]: pam_unix(gdm:session): session closed for user rodr
12 Sep  8 01:12:41 espec sshd[14125]: Accepted password for rodr from 189.30.227.212 port 1061 ssh2
13 Sep  8 01:12:41 espec sshd[14125]: pam_unix(sshd:session): session opened for user rodr by (uid=0)
14 Sep  8 01:12:41 espec sshd[14127]: subsystem request for sftp
15 Sep  8 01:38:26 espec sshd[14125]: pam_unix(sshd:session): session closed for user rodr
16 Sep  8 02:18:29 espec sshd[17048]: Accepted password for e89062004 from 20.0.0.56 port 54233 ssh2
17 Sep  8 02:18:29 espec sshd[17048]: pam_unix(sshd:session): session opened for user e89062004 by (uid=0
18 Sep  8 02:18:29 espec sshd[17048]: pam_unix(sshd:session): session closed for user e89062004
19 Sep  8 09:06:33 espec sshd[25002]: Postponed publickey for mzr from 159.71.224.62 port 52372 ssh2
20 Sep  8 06:06:34 espec sshd[25001]: Accepted publickey for mzr from 159.71.224.62 port 52372 ssh2
21 Sep  8 06:06:34 espec sshd[25001]: pam_unix(sshd:session): session opened for user mzr by (uid=0)
22 Sep  8 06:06:57 espec su: pam_unix(su-l:session): session opened for user root by mzr(uid=500)
```

Serviço de logs UNIX

Infraestrutura de logs baseada no serviço *Syslog*:

- *daemon* `syslogd` (*System Log Daemon*)
- recebe mensagem em *socket* local e socket UDP
- biblioteca *syslog* permite enviar eventos ao serviço
- eventos são descritos por mensagens de texto

Ações possíveis para cada evento:

- armazenar em um arquivo
- enviar a um terminal
- avisar o administrador
- ativar um script ou programa externo
- enviar o evento a um *daemon* em outro computador

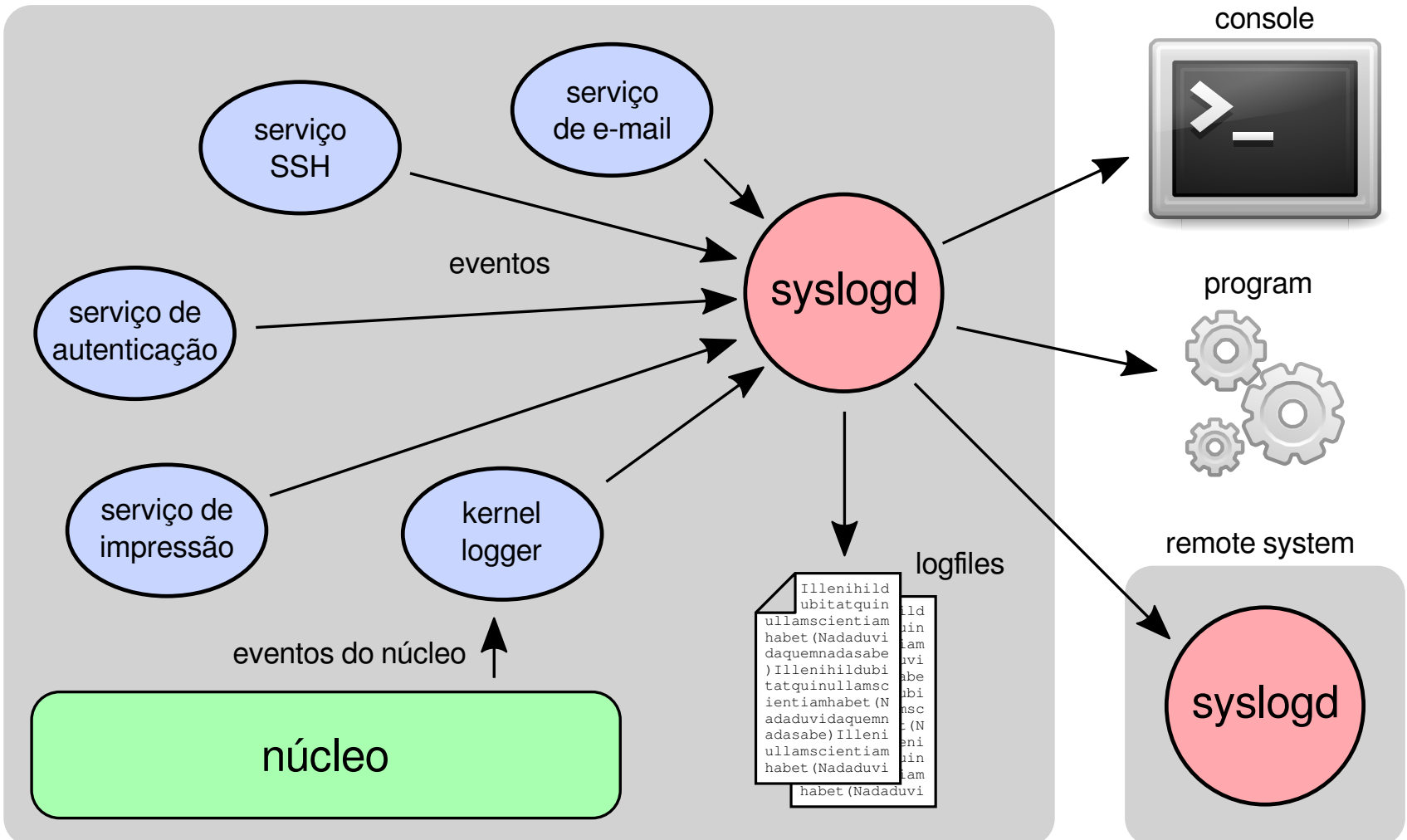
Rótulos dos eventos: Serviços

AUTH	security/authorization messages
AUTHPRIV	security/authorization messages (private)
CRON	clock daemon (cron and at)
DAEMON	system daemons without separate facility value
FTP	ftp daemon
KERN	kernel messages
LOCAL0 ... LOCAL7	reserved for local use
LPR	line printer subsystem
MAIL	mail subsystem
SYSLOG	messages generated internally by syslogd
USER	generic user-level messages

Rótulos dos eventos: Prioridades

EMERG	system is unusable
ALERT	action must be taken immediately
CRIT	critical conditions
ERR	error conditions
WARNING	warning conditions
NOTICE	normal, but significant, condition
INFO	informational message
DEBUG	debug-level message

Serviço de logs UNIX



Serviço de logs Windows

Arquitetura semelhante ao UNIX, mas mais sofisticada:

- Evento gerados por LSASS, SRM, aplicações e núcleo
- Serviço *Windows Event Log* centraliza os eventos
- LSASS: eventos relativos à autenticação dos usuários
- SRM: registra os acessos a cada objeto conforme a SACL
- Eventos são descritos em formato XML

Aplicações externas podem se registrar no *Windows Event Log Service* para receber eventos de interesse (*publish/subscribe*)

Análise de dados

Análise de dados

Quanto ao instante da análise:

- Online
- Offline

Quanto ao método de análise:

- Por assinatura
- Por anomalia

Análise de dados

Análise *online*:

- feita sobre os registros dos eventos assim que gerados
- visa detectar problemas de segurança com **rapidez**
- funciona simultaneamente ao funcionamento do sistema
- deve ser rápida e leve, para não prejudicar o desempenho

Exemplo: antivírus instalado no SO

Análise de dados

Análise *offline*:

- Realizada com dados previamente coletados
- Pode congregar/cruzar dados de vários sistemas
- Não tem compromisso com uma resposta imediata
- Pode ser mais profunda e detalhada (mineração de dados)
- Usada para análise forense de segurança

Exemplo: sistemas de identificação de fraudes bancárias

Análise de dados

Análise por assinaturas: “Sabemos o que é problema”

- Base de dados contém informações sobre problemas conhecidos
- Um evento que se encaixa na base é uma violação de segurança
- Problema: dificuldade em detectar ataques desconhecidos

Exemplo: antivírus (base de assinaturas)

Análise de dados

Análise por anomalias: “Sabemos o que é normal”

- Base de dados descreve o comportamento normal do sistema
- Eventos fora dos padrões são vistos como violações
- Também é chamada de análise baseada em heurísticas
- Usada em alguns antivírus e sistemas de detecção de intrusão
- Como caracterizar corretamente o comportamento “normal”?

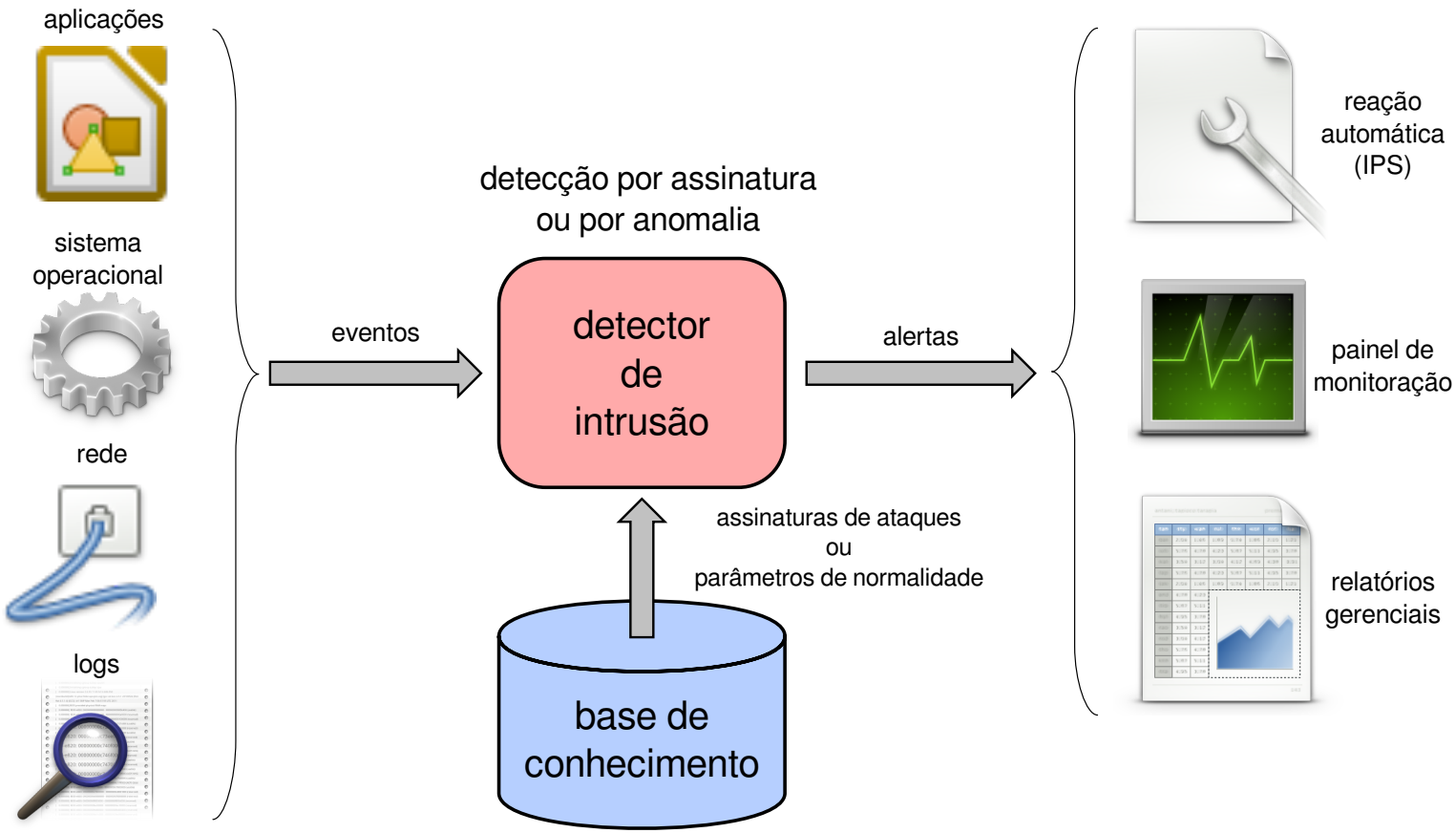
Exemplo: sistemas de identificação de fraudes bancárias

Detecção e Prevenção de Intrusão

Detecção e Prevenção de Intrusão

- **Intrusão**: violação das propriedades de segurança do sistema
- **Detecção de Intrusão**: identificação de intrusões ou tentativas
- **Intrusion Detection System (IDS)**: componente de software e/ou hardware que monitora os eventos de um sistema para identificar intrusões
- **Intrusion Prevention System (IPS)**: detecta e reage às tentativas de intrusão, buscando bloqueá-las ou mitigar seus efeitos

Sistemas de detecção de intrusão



Tipos de IDS

Conforme a origem dos dados:

- **NIDS** (Network IDS): analisa tráfego de rede
- **HIDS**: (Host IDS): analisa eventos em um computador
- **AIDS**: (Application IDS): analisa eventos de aplicação

Conforme a técnica de análise:

- **Por assinatura**: busca padrões de ataques
- **Por anomalia**: busca desvios de comportamento

Erros de classificação

Um IDS é um **classificador** de eventos

Erros de classificação podem ocorrer!

Evento	**não é um ataque**	**é um ataque**
não gerou alerta	verdadeiro negativo	falso negativo
gerou alerta	falso positivo	verdadeiro positivo

Qual o pior tipo de erro?

Auditoria preventiva

Auditoria preventiva

Técnicas para **prevenir** incidentes de segurança

Abordagens

- Varredura de vulnerabilidades
- Quebra de senhas
- Varredura de portas
- Verificação de integridade
- Testes de intrusão (*pentests*)

Auditoria preventiva

Vulnerability scanner:

- verifica se os programas instalados possuem vulnerabilidades conhecidas
- Pode atuar local ou remotamente
- Investiga as principais configurações do sistema
- Exemplos: *Metasploit*, *Nessus*, SAINT

Auditoria preventiva

Port scanner:

- analisa as portas de rede abertas em um host remoto
- identifica os serviços de rede oferecidos pela máquina
- analisa versões de serviços e do próprio SO
- Exemplo: *NMap*, B&W

Auditoria preventiva

Password cracker:

- Avalia robustez das senhas dos usuários
- Baseia-se em ataque do dicionário e outras técnicas
- Exemplos: *John the Ripper*, *Cain & Abel*, *HashCat*

Rootkit scanner:

- Usa técnica *offline* baseada em assinaturas
- ferramentas devem ser aplicadas a partir de outro sistema

Auditoria preventiva

Verificador de integridade:

- Analisa a integridade de arquivos do sistema operacional
- Usa somas de verificação (*checksums*) ou resumos criptográficos
- Pode verificar registros, tabela de *syscalls*, etc
- Exemplos: Tripwire, OSSEC, AIDE, Samhain