

Solaris auditing

Jan Vydrář
2.9.2010

Agenda

- úvod do problematiky bezpečnost/auditování – dotazník
- vyhodnocení dotazníku
- možnosti auditingu v Solarisu
- výhody a nevýhody
- vzdálené auditování
- ukázka zprovoznění základního auditování

Úvod do bezpečnosti a auditování

- Solaris Basic Security Module (BSM)
 - Trusted Solaris
- Co se stalo?
- Kdo to udělal?
- Jak monitorujete činnost uživatelů?
- Auditing není záplata na nezabezpečený systém
 - Zabránění vniknutí
 - Omezení aplikací
 - Uzavření síťových portů

Auditované události

- Start, restart, zastavení systému
- Login a logout uživatelů
- Spouštění procesů a jejich ukončování, včetně vláken
- Operace se soubory
- Identifikace a autorizace uživatelů
- Změna práv uživatelem nebo procesem
- Instalace sw

Jak to funguje

- Pokud je zapnuté auditování
 - dojde k vytvoření události
 - zformátování do auditního záznamu
 - zápis v binární podobě do souboru případně v textové do syslogu

 - uzavření logu, aby bylo možné uskutečnit jeho přesun/rotování
 - případná analýza

Výhody a nevýhody

- + Jednoduchá aktivace
- + Jednoduchá konfigurace
- +/- Sbírám pouze informace které chci = nesbírám nic navíc = informace mi mohou chybět
- +/- Auditing vybraných uživatelů/skupin
- + Možnost auditovat zóny
- - Možnost podvržení logu v případě logování lokálně
- - Zabraný prostor, výkon CPU a zátěž na hdd
- - správa logů, rotace

Možnosti ukládání auditních logů

Uložení	Lokálně	NFS	syslog
Protokol	File system	File system	UDP
Umístění	HDD	Vzdálený server	Vzdálený Syslog server
Data	Binární	Binární	text
Délka záznamu	Bez omezení	Bez omezení	1024 Bytes
analýza	Dávkově	Dávkově	online

Zapnutí auditování, konfigurace

- Zapnutí auditování:

```
# /etc/security/bsmconv
```

```
# reboot
```

Do /etc/system automaticky přidá set c2audit:audit_load = 1

- Konfigurace: **/etc/security/audit_startup**

```
/usr/sbin/auditconfig -setpolicy +cnt
```

```
/usr/sbin/auditconfig -setpolicy +argv
```

```
/usr/sbin/auditconfig -setpolicy +zonename
```

```
/usr/sbin/auditconfig -setpolicy +perzone
```

```
/usr/sbin/auditconfig -conf
```

```
/usr/sbin/auditconfig -aconf
```

Konfigurace, třídy (class) událostí, auditování uživatele

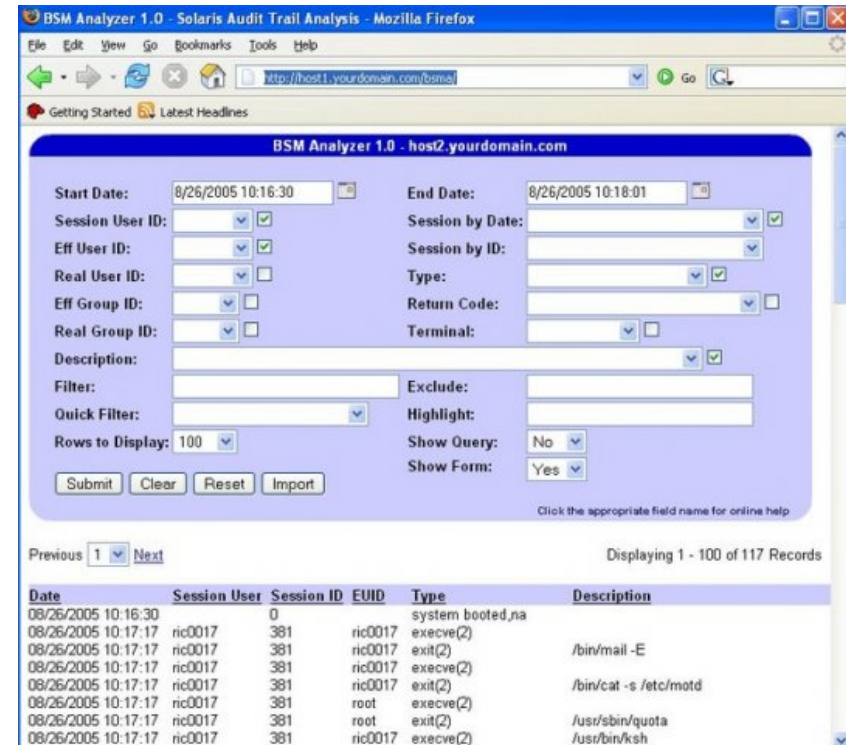
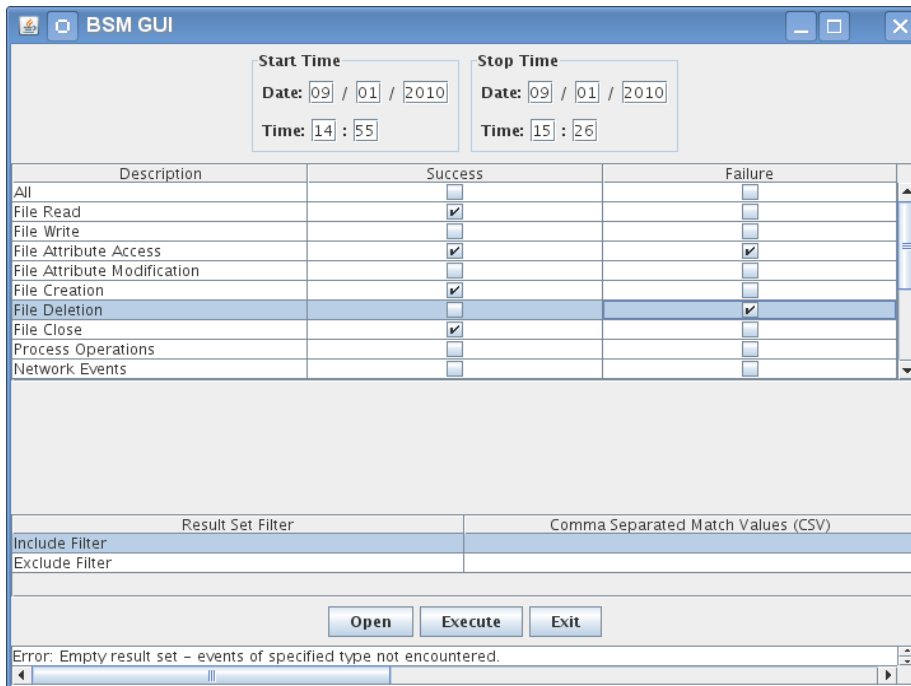
- /etc/security/audit_control
 - dir:/var/audit
 - flags:lo,ex
 - minfree:20
 - naflags:lo
 - plugin:name=audit_syslog.so; p_flags=lo,-am
 - /etc/security/audit_user
 - honza:all,^+fr:no
- ex: execution
 - fr: file read
 - fw: file write
 - nt: network
 - lo: login or logout
 - fc: file create
 - fd: file delete
 - all: All events
 - ...

Správa a analýza logů

- Rotace logů
 - # audit -n
- Třídění
 - # auditreduce -c lo /var/audit/nejakyauditlog > novy-pouze-lo-log
- Formátování
 - # praudit -x /var/audit/*.not_terminated.demo-212 > /tmp/soubor.xml
 - šablona v /usr/share/lib/xml/style/

Analyza logů

- Aplikace
 - BsmGUI – Java App
 - the BSM Analyzer - php



Jan Vydrář
Avnet Technology Solutions
V Olšínách 75
Praha 10
T +420 602 371 805

www.avnet.com/ts/cz