LABORATORIUM BEZPIECZEŃSTWO TECHNOLOGII INFORMATYCZNYCH

Data wykonania ćwiczenia:	24.10.2023
Rok studiów:	3
Semestr:	5
Grupa studencka:	2
Grupa laboratoryjna:	2B

Ćwiczenie nr.	4

Temat: Analiza Logów Systemowych w Poszukiwaniu Podejrzanych Aktywności

Osoby wykonujące ćwiczenia:

1. Igor Gawłowicz

Katedra Informatyki i Automatyki

Cel zadania:

Celem tego laboratorium jest zapoznanie studentów z narzędziami do analizy logów systemowych w systemie Kali Linux, takimi jak Logwatch i Syslog-ng. Studenci zdobędą praktyczne doświadczenie w konfiguracji i korzystaniu z tych narzędzi w celu monitorowania i analizy logów systemowych.

Część 1: Konfiguracja Logwatch na Kali Linux

Pierwszym krokiem będzie zainstalowanie potrzebnych aplikacji:

`sudo apt-get install logwatch`

`sudo apt-get install syslog-ng`

Możemy teraz zaobserwować że po uruchomieniu otrzymamy blok zawierający wszystkie aktualne logi, nie potrzebujemy absolutnie wszystkich informacji więc uruchomimy program logwatch z parametrami `--detail low` oraz `--range today`

```
┌──(igor㉿igor)-[~]
└─$ sudo logwatch --detail Low --range today

 ################### Logwatch 7.7 (07/22/22) ####################
        Processing Initiated: Sun Nov  5 17:05:25 2023
        Date Range Processed: today
                              ( 2023-Nov-05 )
                              Period is day.
        Detail Level of Output: 0
        Type of Output/Format: stdout / text
        Logfiles for Host: igor
 ################################################################

 --------------------- dpkg status changes Begin -----------------------

 Installed:
    bsd-mailx:amd64 8.1.2-0.20220412cvs-1
    exim4-base:amd64 4.97~RC3-1
    exim4-config:all 4.97~RC3-1
    exim4-daemon-light:amd64 4.97~RC3-1
    libdbi1:amd64 0.9.0-6
    libesmtp6:amd64 1.1.0-3.1
    libivykis0:amd64 0.42.4-1
    liblockfile1:amd64 1.17-1+b1
    librdkafka1:amd64 2.3.0-1
    libriemann-client0:amd64 1.10.4-3
    libsys-cpu-perl:amd64 0.61-3+b1
    libsys-meminfo-perl:amd64 0.99-2+b1
    libunistring5:amd64 1.1-2
    logwatch:all 7.7-1
    python3-cachetools:all 5.3.0-2
    python3-google-auth:all 1.5.1-3
    python3-kubernetes:all 22.6.0-2
```

```
    python3-oauthlib:all 3.2.2-1
    python3-requests-oauthlib:all 1.3.0+ds-1
    syslog-ng-core:amd64 4.3.1-2
    syslog-ng-mod-add-contextual-data:amd64 4.3.1-2
    syslog-ng-mod-amqp:amd64 4.3.1-2
    syslog-ng-mod-examples:amd64 4.3.1-2
    syslog-ng-mod-geoip2:amd64 4.3.1-2
    syslog-ng-mod-graphite:amd64 4.3.1-2
    syslog-ng-mod-http:amd64 4.3.1-2
    syslog-ng-mod-mongodb:amd64 4.3.1-2
    syslog-ng-mod-python:amd64 4.3.1-2
    syslog-ng-mod-rdkafka:amd64 4.3.1-2
    syslog-ng-mod-redis:amd64 4.3.1-2
    syslog-ng-mod-riemann:amd64 4.3.1-2
    syslog-ng-mod-slog:amd64 4.3.1-2
    syslog-ng-mod-smtp:amd64 4.3.1-2
    syslog-ng-mod-snmp:amd64 4.3.1-2
    syslog-ng-mod-sql:amd64 4.3.1-2
    syslog-ng-mod-stardate:amd64 4.3.1-2
    syslog-ng-mod-stomp:amd64 4.3.1-2
    syslog-ng-mod-xml-parser:amd64 4.3.1-2
    syslog-ng-scl:all 4.3.1-2
    syslog-ng:all 4.3.1-2

Upgraded:
    gnutls-bin:amd64 3.7.9-2 => 3.8.1-4+b1
    libbson-1.0-0:amd64 1.24.2-1 => 1.24.4-1
    libgnutls-dane0:amd64 3.7.9-2 => 3.8.1-4+b1
    libgnutls30:amd64 3.7.9-2 => 3.8.1-4+b1
    libmongoc-1.0-0:amd64 1.24.2-1 => 1.24.4-1
    libpython3.11-dev:amd64 3.11.4-1 => 3.11.6-3
    libpython3.11-minimal:amd64 3.11.4-1 => 3.11.6-3
    libpython3.11-stdlib:amd64 3.11.4-1 => 3.11.6-3
    libpython3.11:amd64 3.11.4-1 => 3.11.6-3
    libsnmp-base:all 5.9.3+dfsg-2 => 5.9.4+dfsg-1
    libsnmp40:amd64 5.9.3+dfsg-2 => 5.9.4+dfsg-1
    python3.11-dev:amd64 3.11.4-1 => 3.11.6-3
    python3.11-minimal:amd64 3.11.4-1 => 3.11.6-3
    python3.11:amd64 3.11.4-1 => 3.11.6-3
    snmp:amd64 5.9.3+dfsg-2 => 5.9.4+dfsg-1
    snmpd:amd64 5.9.3+dfsg-2 => 5.9.4+dfsg-1

---------------------- dpkg status changes End -------------------------


---------------------- Disk Space Begin ------------------------

Filesystem      Size  Used Avail Use% Mounted on
/dev/sda1        25G   14G  9.9G  58% /


---------------------- Disk Space End -------------------------
```

```
--------------------- lm_sensors output Begin ------------------------

BAT0-acpi-0
Adapter: ACPI interface
in0:          10.00 V


---------------------- lm_sensors output End ------------------------


####################### Logwatch End #########################
```

Następnie chcemy skonfigurować oba programy tak aby, logi z syslog-ng spływały nam także do logwatcha. Możemy to zrobić w taki sposób żeby wszystkie informacje przychodziły nam drogą mailową przez lokalny server połączony z siecią, jednak w moim przypadku wypiszę wszystko do konsoli ponieważ gdy pracowałem nad tą częścią zadania nie miałem połączenia z internetem.

Aby skonfigurować aplikacje w taki sposób logwatcha zostawimy bez zmian na parametrze

```
output: stdout
```

a do syslog-ng dodawmy linijke zawierającą następujące polecenie

```
destination logwatch { program("/usr/sbin/logwatch --output mail"); };
```

Po zmodyfikowaniu i zapisaniu konfiguracji musimy wczytać nową konfiguracje poprzez reset za pomocą:

```
sudo systemctl restart syslog-ng
```

Co ciekawe napotkałem w tym kroku problem z restartem więc miałem okazje wykorzystać funkcjonalność sysloga aby dowiedzieć się co jest nie tak, wywołałem więc program i od razu dowiedziałem się, że przez przypadek w jakiś sposób wkleiła mi się jedna linia więcej niż bym chciał.

```
┌──(igor㉿igor)-[~]
└─$ sudo syslog-ng
[2023-11-05T17:34:04.215326] smart-multi-line: error opening smart-multi-line.fsm
file; filename='/usr/share/syslog-ng/smart-multi-line.fsm', error='No such file or
directory (2)'
[2023-11-05T17:34:04.216046] smart-multi-line: your smart-multi-line.fsm seems to
be empty or non-existent, automatic multi-line log extraction will probably not
work; filename='/usr/share/syslog-ng/smart-multi-line.fsm'
[2023-11-05T17:34:04.298739] WARNING: Configuration file format is too old,
syslog-ng is running in compatibility mode. Please update it to use the syslog-ng
4.3 format at your time of convenience. To upgrade the configuration, please
review the warnings about incompatible changes printed by syslog-ng, and once
completed change the @version header at the top of the configuration file; config-
version='3.38'
[2023-11-05T17:34:04.951692] WARNING: Your configuration file uses an obsoleted
keyword, please update your configuration; keyword='stats_freq', change='Use the
stats() block. E.g. stats(freq(1));', location='/etc/syslog-ng/syslog-
ng.conf:10:4'
```

```
Error parsing config, syntax error, unexpected LL_IDENTIFIER, expecting end of
file in /etc/syslog-ng/syslog-ng.conf:161:1-161:5:
156
157     ###
158     # Include all config files in /etc/syslog-ng/conf.d/
159     ###
160     @include "/etc/syslog-ng/conf.d/*.conf"
161---> sudo systemctl restart syslog-ng
161---> ^^^^
162     destination logwatch { program("/usr/sbin/logwatch --output stdout"); };
```

Dzięki temu w bardzo szybki sposób rozwiązałem problem i przeszedłem do następnego kroku.

Tym razem po uruchomieniu logwatcha możemy zauważyć stanowczo więcej informacji

```
┌──(igor㉿igor)-[~]
└─$ sudo logwatch --detail Low --range today
^[[B^[[A
 ################### Logwatch 7.7 (07/22/22) ####################
        Processing Initiated: Sun Nov  5 17:58:46 2023
        Date Range Processed: today
                              ( 2023-Nov-05 )
                              Period is day.
        Detail Level of Output: 0
        Type of Output/Format: stdout / text
        Logfiles for Host: igor
 ################################################################

 --------------------- dpkg status changes Begin -----------------------

 Installed:
    bsd-mailx:amd64 8.1.2-0.20220412cvs-1
    exim4-base:amd64 4.97~RC3-1
    exim4-config:all 4.97~RC3-1
    exim4-daemon-light:amd64 4.97~RC3-1
    libdbi1:amd64 0.9.0-6
    libesmtp6:amd64 1.1.0-3.1
    libivykis0:amd64 0.42.4-1
    liblockfile1:amd64 1.17-1+b1
    librdkafka1:amd64 2.3.0-1
    libriemann-client0:amd64 1.10.4-3
    libsys-cpu-perl:amd64 0.61-3+b1
    libsys-meminfo-perl:amd64 0.99-2+b1
    libunistring5:amd64 1.1-2
    logwatch:all 7.7-1
    python3-cachetools:all 5.3.0-2
    python3-google-auth:all 1.5.1-3
    python3-kubernetes:all 22.6.0-2
    python3-oauthlib:all 3.2.2-1
    python3-requests-oauthlib:all 1.3.0+ds-1
    syslog-ng-core:amd64 4.3.1-2
    syslog-ng-mod-add-contextual-data:amd64 4.3.1-2
```

```
    syslog-ng-mod-amqp:amd64 4.3.1-2
    syslog-ng-mod-examples:amd64 4.3.1-2
    syslog-ng-mod-geoip2:amd64 4.3.1-2
    syslog-ng-mod-graphite:amd64 4.3.1-2
    syslog-ng-mod-http:amd64 4.3.1-2
    syslog-ng-mod-mongodb:amd64 4.3.1-2
    syslog-ng-mod-python:amd64 4.3.1-2
    syslog-ng-mod-rdkafka:amd64 4.3.1-2
    syslog-ng-mod-redis:amd64 4.3.1-2
    syslog-ng-mod-riemann:amd64 4.3.1-2
    syslog-ng-mod-slog:amd64 4.3.1-2
    syslog-ng-mod-smtp:amd64 4.3.1-2
    syslog-ng-mod-snmp:amd64 4.3.1-2
    syslog-ng-mod-sql:amd64 4.3.1-2
    syslog-ng-mod-stardate:amd64 4.3.1-2
    syslog-ng-mod-stomp:amd64 4.3.1-2
    syslog-ng-mod-xml-parser:amd64 4.3.1-2
    syslog-ng-scl:all 4.3.1-2
    syslog-ng:all 4.3.1-2

 Upgraded:
    gnutls-bin:amd64 3.7.9-2 => 3.8.1-4+b1
    libbson-1.0-0:amd64 1.24.2-1 => 1.24.4-1
    libgnutls-dane0:amd64 3.7.9-2 => 3.8.1-4+b1
    libgnutls30:amd64 3.7.9-2 => 3.8.1-4+b1
    libmongoc-1.0-0:amd64 1.24.2-1 => 1.24.4-1
    libpython3.11-dev:amd64 3.11.4-1 => 3.11.6-3
    libpython3.11-minimal:amd64 3.11.4-1 => 3.11.6-3
    libpython3.11-stdlib:amd64 3.11.4-1 => 3.11.6-3
    libpython3.11:amd64 3.11.4-1 => 3.11.6-3
    libsnmp-base:all 5.9.3+dfsg-2 => 5.9.4+dfsg-1
    libsnmp40:amd64 5.9.3+dfsg-2 => 5.9.4+dfsg-1
    python3.11-dev:amd64 3.11.4-1 => 3.11.6-3
    python3.11-minimal:amd64 3.11.4-1 => 3.11.6-3
    python3.11:amd64 3.11.4-1 => 3.11.6-3
    snmp:amd64 5.9.3+dfsg-2 => 5.9.4+dfsg-1
    snmpd:amd64 5.9.3+dfsg-2 => 5.9.4+dfsg-1

 ---------------------- dpkg status changes End -------------------------
 ---------------------- Kernel Begin ------------------------


 WARNING:  Kernel Errors Present
    21:52:00.517386 main     VBoxClient VMSVGA: Error: unable to conne ...:  1
Time(s)
    [drm:vmw_host_printf [vmwgfx]] *ERROR* Failed to send  ...:  1 Time(s)

 ---------------------- Kernel End ------------------------


 --------------------- pam_unix Begin ------------------------

 lightdm:
    Unknown Entries:
```

```
      session opened for user igor(uid=1000) by (uid=0): 1 Time(s)

  lightdm-greeter:
     Unknown Entries:
        session closed for user lightdm: 2 Time(s)
        session opened for user lightdm(uid=125) by (uid=0): 2 Time(s)

  sudo:
     Sessions Opened:
        igor -> root(uid=0): 50 Time(s)


  ---------------------- pam_unix End ------------------------


  --------------------- Connections (secure-log) Begin ------------------------

  New Users:
     Debian-exim (132)

  New Groups:
     Debian-exim (143)


  **Unmatched Entries**
     lightdm: pam_systemd(lightdm-greeter:session): Failed to release session:
Transport endpoint is not connected: 1 Time(s)
  ---------------------- Connections (secure-log) End -------------------------


  --------------------- Sudo (secure-log) Begin ------------------------


  igor => root
  ------------
  /usr/bin/apt-get               -   4 Time(s).
  /usr/bin/nano                  -  19 Time(s).
  /usr/bin/systemctl             -  18 Time(s).
  /usr/sbin/logwatch             -   5 Time(s).
  /usr/sbin/syslog-ng            -   4 Time(s).

  ---------------------- Sudo (secure-log) End -------------------------


  --------------------- Syslog-ng Begin ------------------------


  Syslog-ng started:                                 3 Time(s)
  Syslog-ng stopped:                                 2 Time(s)

  ---------------------- Syslog-ng End -------------------------


  --------------------- Disk Space Begin ------------------------
```

```
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda1        25G   14G  9.9G  58% /


---------------------- Disk Space End -------------------------


--------------------- lm_sensors output Begin ------------------------

BAT0-acpi-0
Adapter: ACPI interface
in0:          10.00 V


---------------------- lm_sensors output End -------------------------


####################### Logwatch End #########################
```

Wynik ten możemy podsumować takimi sekcjami:

- Wersja Logwatch i Informacje o Dacie/Czasie:
    - Podaje informacje o używanej wersji Logwatch oraz dacie i czasie rozpoczęcia analizy logów.
- Logi Hosta:
    - Wskazuje nazwę hosta, dla którego przeprowadzono analizę logów.
- Zmiany w Statusie dpkg:
    - Ta sekcja zawiera listę zainstalowanych i zaktualizowanych pakietów. Dostarcza szczegółowe informacje na temat nazw pakietów, architektury oraz zmian w wersji.
- Jądro (Kernel):
    - Ta sekcja wyświetla informacje związane z jądrem systemu oraz możliwe ostrzeżenia lub błędy. Pokazuje wpisy związane z jądrem wraz z datą i godziną.
- pam_unix:
    - Tutaj można zobaczyć informacje dotyczące sesji użytkowników oraz szczegóły logowania i wylogowania się z systemu.
- Połączenia (secure-log):
    - Dostarcza informacje na temat nowo utworzonych użytkowników i grup. Ponadto lista niesparowanych wpisów dotyczących połączeń.
- Sudo (secure-log):

    - Ta sekcja raportuje użycie polecenia sudo. Pokazuje, którzy użytkownicy wykonali polecenia sudo i wyświetla polecenia, które wykonali. Jest to dziennik związany z bezpieczeństwem.

- Syslog-ng:
    - Ta część raportu dotyczy aktywności związanej z usługą syslog-ng, w tym informacje o jej uruchamianiu i zatrzymywaniu.

- Przestrzeń Dyskowa:
    - Pokazuje informacje na temat przestrzeni dyskowej na zamontowanych systemach plików.

- Wynik lm_sensors:
    - Ta część może zawierać odczyty czujników systemowych, takie jak poziomy napięcia.

Wnioski

Logi systemowe w systemach Unixowych, w tym aplikacje Logwatch i Syslog-ng, odgrywają kluczową rolę w monitorowaniu i zarządzaniu tymi systemami. Logwatch pozwala na czytelną analizę logów, umożliwiając identyfikację aktywności systemu, zaktualizowanego oprogramowania oraz działań użytkowników. Jest to nieocenione narzędzie do szybkiej reakcji na potencjalne problemy. Z kolei Syslog-ng umożliwia zaawansowaną konfigurację logów, co pozwala na dostosowanie systemu logowania do konkretnych potrzeb i zwiększa niezawodność procesu logowania. Wprowadzenie tych narzędzi znacząco poprawia zarządzanie i bezpieczeństwo systemów Unixowych oraz umożliwia efektywną reakcję na ewentualne incydenty.