T: Bezpieczeństwo systemu operacyjnego. Logi systemowe.

Zadanie1:

Odpowiedz na poniższe pytania:
Co rozumiesz przez bezpieczeństwo systemu operacyjnego?
W jaki sposób chronić system operacyjny?

Lista kontrolna bezpieczeństwa systemu Linux:

- kontrola fizycznego dostępu – umieszczenie komputera w zamykanym na klucz pomieszczeniu, zabezpieczenia na poziomie BIOS i menedżera startu,
- dodawanie kont użytkowników oraz haseł – oddzielne konta, grupy użytkowników oraz silne hasła,
- ustawianie uprawnień do odczytu, zapisu oraz uruchamiania,
- ochrona użytkownika root – nie używać tego konta bez potrzeby,
- używanie zaufanego oprogramowania – pobieranie dystrybucji i programów z serwerów publicznych,
- pobieranie uaktualnień oprogramowania – wykorzystywanie narzędzi dostępnych w każdej z głównych dystrybucji Linuksa do aktualizacji systemu,
- używanie bezpiecznych aplikacji – np. ssh zamiast telnet,
- używanie restrykcyjnie ustawionych zapór sieciowych – systemy biurkowe powinny odrzucać większość połączeń sieciowych,
- włączenie tylko potrzebnych usług,
- ograniczenie dostępu do usług – ograniczenie dostępu tylko dla lub do określonego komputera, domeny lub interfejsu sieciowego,
- sprawdzanie systemu – wykorzystywanie oprogramowania typu nmap, ethereal, nessus,
- monitorowanie systemu – rejestrowanie w dziennikach aktywność systemu (syslogd oraz klogd).

Zadanie2:

Odszukaj informacje na temat definicji logów systemowych.

Dla zwiększenia bezpieczeństwa systemu operacyjnego należy ograniczyć pracę na koncie administratora systemu root. Należy również ograniczyć fizyczny dostęp do serwera dla osób do tego nieuprawnionych (zabezpieczony dostęp do serwerowni).

Często zdarza się, że podczas prac administracyjnych potrzebujemy na bieżąco monitorować działanie systemu a zwłaszcza komunikaty błędów. Obsługa logowania w systemach uniksowych najczęściej zajmuje się osobny deamon - syslogd. Zbiera on z różnych programów informacje(log) a następnie rozdziela, filtruje i magazynuje je w różnych miejscach. Najczęściej logi trafiają do odpowiednich plików w katalogu `/var/log/`. Jeżeli siedzimy przy komputerze, to najłatwiej oglądać logi na osobnej konsoli tekstowej. Konsolę 12 (wywoływaną skrótem klawiaturowym ALT+F12) symbolizuje plik `/dev/tty12`. Wybraliśmy 12, ponieważ jest najrzadziej używaną konsolą, ale oczywiście można wybrać dowolną inną, wolną konsole. Na końcu pliku `/etc/rsyslog.conf` dopisujemy linijkę `"*.* /dev/tty12"` (bez cudzysłowów), co oznacza, że wszystkie logi będą wyświetlane na konsoli tty12. W celu aktualizacji wprowadzonych zmian należy przeładować deamona syslogd poleceniem :

```
/etc/init.d/syslog reload
```

Wyświetlenie zawartości pliku z bieżącymi logami uzyskamy poleceniem:

```
cat /var/log/syslog
```

Wyświetlenie na bieżąco aktualizowanych zmian w pliku z logami uzyskamy poleceniem:

```
tail -f /var/log/syslog
man syslog
man syslog-ng
```

Więcej informacji na stronach:

http://www.techit.pl/Artykuly/View.aspx?273.jak+na+biezaco+ogladac+logi+systemowe+w+systemach+linuxunix
http://kik.pcz.pl/so-add/KSL/lekcje/l_17.html

http://wiemto.info/archiwum/2009/341
http://pl.docs.pld-linux.org/uslugi_syslog-ng.html

Domyślnie instalowanym systemem magazynowania zdarzeń systemowych (logów) jest **syslog-ng** (syslog - new generation), zajął on miejsce klasycznego tandemu **syslogd** i **kalogd.** Jest to program o bogatych opcjach konfiguracji, zapewniający większą pewność działania, a co za tym idzie większe bezpieczeństwo logów.
Syslog-ng jest dostarczany z rozbudowanym plikiem konfiguracji, znajdziemy w nim wiele gotowych do wykorzystania przykładów.

Konfiguracja demona polega na zdefiniowaniu pewnych obiektów, a następnie połączenie ich ze sobą w reguły. Mamy trzy rodzaje obiektów:
- **źródła** – wskazują miejsca pochodzenia komunikatów,
- **filtry** – pozwalają selekcjonować dane,
- **cele** – wskazują sposób i miejsce magazynowania logów (zwyczajowo jako pliki tekstowe w katalogu /var/log).

Całą konfigurację umieszczamy w jednym pliku `/etc/rsyslog.conf (/etc/syslog-ng/syslog-ng.conf)`.
Przykładowe wpisy:

```
source  src  { internal(); };
source  udp  { udp(); };
source  tcp  { tcp(ip(192.168.1.5) port(1999) max-connections(20)); };
filter f_emergency { level(emerg); };
filter f_daemon    { facility(daemon); };
filter f_foo       { host("foo"); };
filter f_su_sudo   { program("^su|sudo$"); };
filter f_syslog  { not facility(authpriv, cron, lpr, mail, news); };
filter f_ppp     { facility(daemon) and program(pppd) or program(chat); };
destination  kernel       { file("/var/log/kernel"); };
destination  console_all  { file("/dev/tty12"); };
destination  root         { usertty("root"); };
destination  loghost      { udp("10.0.0.1"); };
log { source(src);  destination(console_all); };
log { source(src);  filter(f_emergency);  destination(loghost); };
```

Aby zmiany weszły w życie oraz utworzone zostały nowe pliki dzienników, należy ponownie uruchomić demona. Wykorzystujemy do tego polecenie:

```
service syslog reload
/etc/init.d/syslog restart
```

Pliki dzienników umieszczone w katalogu `/var/log`:
- boot.log – zawiera komunikaty wskazujące uruchomione i zamknięte usługi systemowe,
- cron – zawiera komunikaty demona crond, który okresowo uruchamia wykonywanie zadań,
- dmesg – zapis komunikatów wyświetlanych przez jądro w trakcie uruchamiania systemu,
- xferlog – zawiera informacje o plikach transferowanych za pomocą usługi ftp,
- http/access_log – zawiera żądania względem serwera Apache,
- http/error_log – błędy w dostępie do serwera Apache,
- maillog – zawiera adresy użytkowników wymieniających pocztę e-mail,
- rpmpkgs – zawiera listę pakietów rpm zainstalowanych w systemie,
- secure – zawiera daty i próby logowania w systemie,
- messages – plik ogólnego przeznaczenia, zawiera komunikaty wielu komunikatów,
- Xorg.0.log – komunikaty wygenerowane przez serwer X,
- samba/log.smbd – komunikaty demona serwera smbd,
- squid/access.log – zawiera komunikaty związane z serwerem proxy,
- vsftpd.log – zawiera komunikaty związane z serwerem vsftpd,
- sendmail – komunikaty błędów serwera sendmail.

Logi systemowe można przekierować do innego serwera. W tym celu w pliku konfiguracyjnym /etc/syslog.conf wpisujemy:

```
*.* @serwer_name
```

Na zdalnym serwerze należy uruchomić serwer syslog z opcją -r. Warto również pamiętać o tym, że serwer będzie nasłuchiwał na porcie 514, który odpowiednio powinien być zabezpieczony w konfiguracji firewalla przed niepowołanym dostępem (przepełnienie partycji zbędnymi informacjami).

Odzyskiwanie konta administratora (zapomniane hasło):

```
init=/bin/bash        (Recovery)
mount -rw -o remount /
passwd
mount -n -o remount,rw /
```