Rozdział 1

Raportowanie

1.1 Logowanie do pliku

Logowanie pakietów przy użyciu opcji *-j LOG*, w domyślnej konfiguracji zapisuje pakiety do pliku */var/log/messages*. W tym pliku zapisywane są wszystkie zdarzenia logowane na komputerze. Mnogość logowanych zdarzeń może utrudniać filtrowanie interesujących nas informacji z systemu IPS. Dlatego też, należy przekierować zapisywanie zapisów do osobnego pliku. W systemie Ubuntu 10.4, domyślnym systemem logowania jest *rsyslog*, dlatego przedstawiona zostanie konfiguracja dla tego systemu.

Cechą wspólną wszystkich zapisów tworzonych przez opisywany system IPS, jest występowanie frazy "IPS:". Wszystkie wpisy zawierające powyższą frazę traktujemy jako wpis systemu i przekierowujemy do osobnego pliku. Aby to osiągnąć, umieszczamy plik konfiguracyjny:

Listing 1.1: /etc/rsyslog.d/ips.conf

```
1 :msg, contains, "IPS: " -/var/log/ips.log
2 & ~
```

1.2 Logowanie do bazy danych

Ponieważ operowanie na plikach tekstowych jest zarówno niewygodne jak i mniej optymalne niż operowanie na rekordach bazy danych, zdarzenia będą zapisywane do bazy danych.

Zapisywania będziemy dokonywać, uruchamiając co minutę skrypt na pisany w języku Python. Skrypt ten będzie filtrować plik */var/log/ips.log*, zawierający zdarzenia z systemu IPS, tak, aby uzyskać tylko zdarzenia zarejestrowane w poprzedniej minucie. Następnie przeprowadzi analizę wpisów zdarzeń i dokona wpisu do bazy danych.

Każdy rekord w bazie danych, reprezentujący zdarzenie, będzie zawierał podstawowe parametry zdarzenia, tj:

- czas w którym nastąpiło wykrycie zdarzenia
- typ ataku
- adres źródłowy ataku
- adres docelowy ataku
- port źródłowy
- port docelowy

- użyty protokół
- dokładny wpis wygenerowany przez iptables