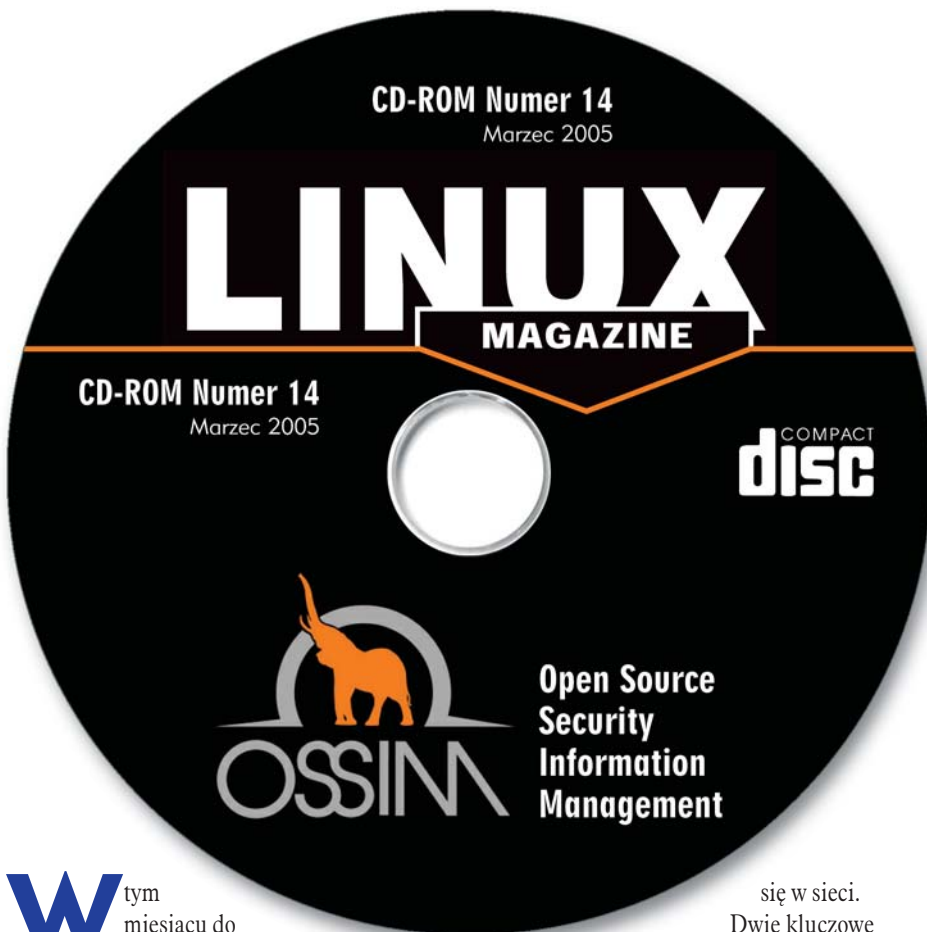


Linux Magazine CD



W tym miesiącu do Linux Magazine dołączamy kompletny system monitorowania sieci i hostów oraz wspomaganie wykrywania włamań, OSSIM (Open Source Security Information Management). Celem tego projektu jest dostarczenie środowiska, które dawałoby spójny obraz tego, co dzieje się w danej sieci, a także ułatwiałoby wykrywanie anomalii, pobierając i analizując informacje przesyłane z czujek.

Istnieje wiele otwartych narzędzi do monitorowania sieci i raportowania, często o bardzo dużych możliwościach, jednak zintegrowanie ich w taki sposób, by można było w każdej chwili uzyskać spójny i kompletny obraz tego, co dzieje się w danej sieci, nie jest zadaniem łatwym. Twórcy OSSIM postanowili wypełnić tę lukę i stworzyć projekt, który – poprzez integrację narzędzi takich jak ntop, snort, p0f i inne – pozwoli łatwo zorientować się, co w danej chwili dzieje

się w sieci. Dwie kluczowe funkcje OSSIM to: korelacja, czyli zebranie w jednym miejscu wszystkich zdarzeń dotyczących sieci, w jednym formacie i w wygodnej formie, oraz ocena zagrożenia, czyli analiza zdarzeń pod kątem potencjalnej niepożądanego aktywności. Cały system obsługiwany jest z jednego miejsca przez interfejs WWW.

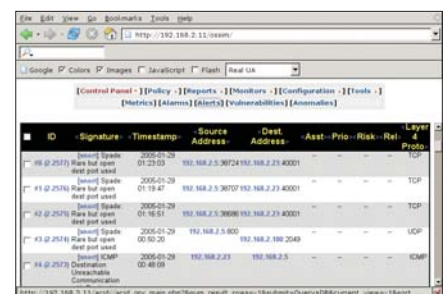
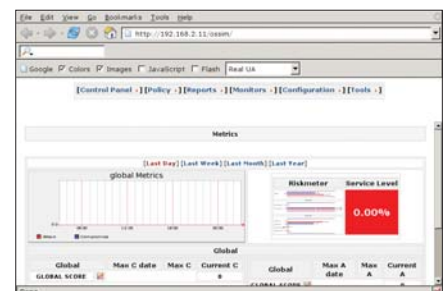
Instalacja

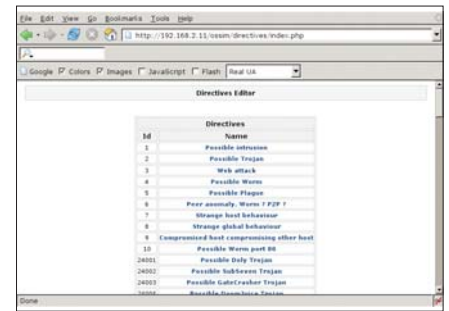
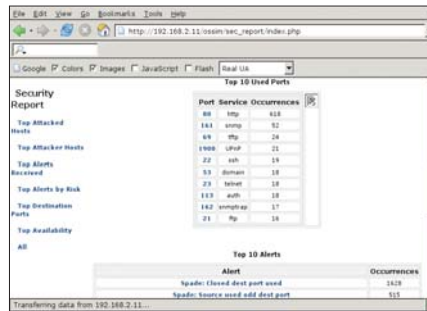
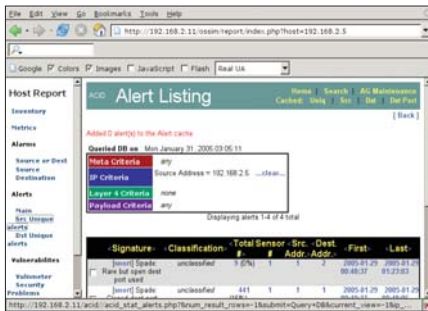
OSSIM instalujemy podobnie jak większość pozostałych dystrybucji: umieszczamy płytę CD w napędzie, następnie restartujemy komputer, pamiętając, że w BIOS-ie powinna być włączona opcja „Uruchamianie systemu z dysku CD/DVD”. UWAGA: instalacja usunie z dysku wszystkie istniejące systemy i dane, powinniśmy więc przeprowadzać ją wyłącznie na dedykowanym komputerze! Po pojawieniu się ekranu powitalnego naciskamy klawisz Enter i czekamy na zakończenie instalacji.

Wersja OSSIM dołączona do bieżącego numeru Linux Magazine oparta jest na dystrybucji Fedora Core 2, tak więc po ponownym uruchomieniu komputera powinno pojawić się okno menedżera startu, GRUB. Po naciśnięciu Enter system zostanie uruchomiony i przygotowany do pracy. Musimy jedynie pamiętać o zmianie domyślnych haseł, np. hasło roota jest puste.

Konfiguracja

Po pomyślnym uruchomieniu serwera pora na jego konfigurację. Na komputerze klienckim uruchamiamy przeglądarkę i łączymy się z serwerem OSSIM, wpisując jego numer IP w pasku adresowym przeglądarki. W oknie dialogowym wpisujemy nazwę użytkownika „ossim” i hasło „ossim_password”. Naszym oczom powinien się ukazać ekran główny interfejsu, otwarty na zakładce pozwalającej monitorować całość wybranych sieci.





Aby rozpocząć pracę z OSSIM, należy przede wszystkim dodać nową czujkę. Czujka może być umieszczona na serwerze, choć często będziemy chcieli rozmieszczać czujki w wielu miejscach sieci, by uzyskać najbardziej kompletny obraz sytuacji. Aby dodać czujkę, klikamy na zakładce „Policy”, a następnie „Sensors”, po czym wybieramy pozycję „Insert New Sensor” („dodaj nową czujkę”). W dalszej kolejności należy wypełnić pola formularza: „Hostname” to nazwa czujki, IP to jej adres IP, „Priority” to priorytet, który ma wpływ na ocenę zagrożenia w sieci, „Port” to port komunikacji z serwerem (40001), zaś „Description” to opcjonalny opis. Po dodaniu czujki powinniśmy ujrzeć odpowiedni wpis na liście czujek dostępnych w systemie.

Kolejnym krokiem jest dodanie grup sygnatur, dzięki którym można wyodrębnić zestaw interesujących nas alarmów, jak również logicznie je podzielić. W tym celu wybieramy pozycję „Policy->Signatures->Insert new signature group”. Następnie zaznaczamy odpowiednie pozycje, dodajemy opcjonalny opis i zatwierdzamy wpisane wartości, klikając „OK”.

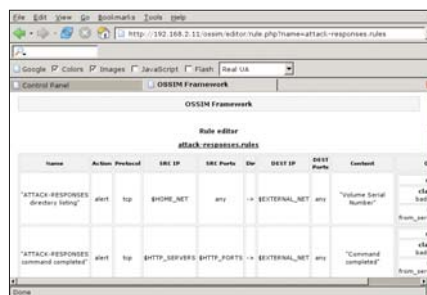
Bardzo ważne jest zdefiniowanie sieci, które będą monitorowane. Sieć dodajemy podobnie jak czujki i sygnatury, wybierając pozycję „Policy->Networks->Insert new network”. W polu Ips należy wpisać adres sieci, np. 192.168.0.0/24. „Threshold C” i „Threshold A” to wartości progowe alarmów – litera „A” odnosi się do potencjalnego ataku, zaś „C” – udanego włamania. Pole „Sensors” wskazuje, które czujki nadzorują tę sieć. Pewnym udogodnieniem jest opcja „Enable nessus scan”, która dodaje możliwość skanowania sieci za pomocą pop-

ularnego narzędzia do wykrywania luk w bezpieczeństwie, Nessus. W podobny sposób jak sieci i sygnatury można zdefiniować grupy portów, ograniczając zestaw portów znajdujących się w polu zainteresowania OSSIM.

Jedną z najbardziej użytecznych możliwości systemu jest funkcja nadawania priorytetów zdarzeniom, dzięki czemu administrator nie jest nękany fałszywymi alarmami. Priorytety można definiować i modyfikować na ekranie, który pojawi się po wybraniu pozycji „Policy->Priority & Reliability”. Po kliknięciu na pole „Id” można modyfikować zarówno priorytet, jak i wiarygodność wywołanego alarmu.

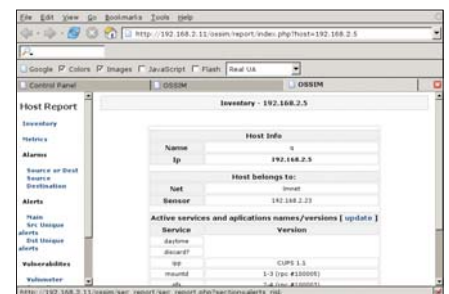
Kiedy wykonano wszystkie powyższe kroki, można przejść do utworzenia nadzorowanego komputera lub ich grupy ('Host'). Można to uczynić na dwa sposoby: ręcznie, podając adres IP, albo automatycznie, dzięki skanowaniu sieci w poszukiwaniu podłączonych komputerów. Aby ręcznie dodać nowy komputer, wybieramy pozycję 'Policy->Hosts->Insert new host'. Po dodaniu danego komputera na liście hostów powinien pojawić się nowy wpis.

Najistotniejszym elementem konfiguracji jest zdefiniowanie zasad monitorowania

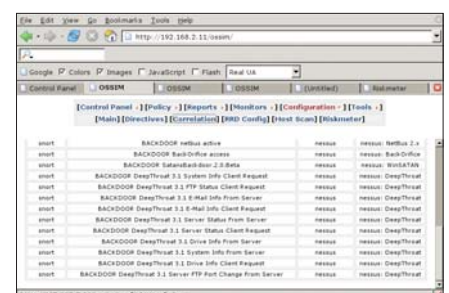


i alarmowania (Policy). W tym celu wybieramy pozycję 'Policy->Policy->Insert new policy'. Dla danego zestawu zasad możemy wybrać adres źródłowy (source) i docelowy (destination), zdefiniowane uprzednio czujki, porty i grupy sygnatur, jak również priorytety i zakres czasowy. Po zdefiniowaniu zasad monitorowania i alarmowania system jest gotowy do pracy.

Więcej informacji na temat wykrywania anomalii, raportowania, zaawansowanej konfiguracji i zakresu monitorowanych usług można znaleźć w dokumentacji, która obejmuje podręcznik użytkownika, ogólne zasady pracy z systemem oraz dokumenty HOWTO.



Warto przy okazji wspomnieć, że użytkownicy dystrybucji takich jak Debian czy Fedora również mogą zainstalować OSSIM, jest to jednak procedura bardzo czasochłonna i wymagająca wielu zabiegów. Najłatwiejszym sposobem na rozpoczęcie pracy z tym niezwykle przydatnym zestawem narzędzi jest zainstalowanie OSSIM z płyty dołączonej do bieżącego numeru Linux Magazine. Owocnego eksperymentowania!



UWAGA!

Płyta CD dołączona do numeru nie zawiera dystrybucji typu LiveCD! Procedura instalacyjna wymazuje zawartość twardego dysku, zastępując istniejące dane obrazem z płyty, należy więc pamiętać o tym, by uruchamiać

ją jedynie na komputerach, które mają służyć wyłącznie jako serwery monitorowania i wykrywania anomalii. Instalacja na dysku, na którym znajdują się jakieś dane, spowoduje ich usunięcie.