BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI
NR 19, 2003

# Metoda adaptacji zbioru reguł IDS do środowiska sieciowego

**Adam E. PATKOWSKI**

Instytut Teleinformatyki i Automatyki WAT
ul. Kaliskiego 2, 00-908 Warszawa

STRESZCZENIE: Przedstawione zostały metody utrzymania aktualności i skuteczności systemów wykrywania włamań instalowanych w celu przeciwdziałania atakom wewnętrznym w sieciach lokalnych. Określono możliwe metodyki postępowania ze szczególnym uwzględnieniem dążenia do zmniejszenia zaangażowania administratorów w obsługę IDS. Zaprezentowano nową metodę adaptacji zbioru reguł IDS za pomocą benchmarków.

## 1. Wprowadzenie

Jak wykazują statystyki, 80% ataków przeciw systemom komputerowym to ataki wewnętrzne: prowadzone z wnętrza sieci korporacyjnej, zwykle przez pracowników firmy-dysponenta sieci. Tymczasem główny wysiłek twórców reguł systemów wykrywania włamań (*Intruder Detection Systems – IDS*) skierowany jest na ochronę przed atakami zewnętrznymi – prowadzonymi spoza sieci korporacyjnej i wymierzonymi przede wszystkim przeciw serwerom, które są osiągalne z zewnątrz (spoza mechanizmów *Network Address Translation*). Ataki wewnętrzne rządzą się własnymi zasadami, radykalnie różnymi od ataków zewnętrznych. Ponadto sposób prowadzenia ataków wewnętrznych jest silnie zależny od rozwiązań technicznych sieci lokalnych oraz od rozmieszczenia informacji wrażliwych na komputerach w sieci korporacyjnej.

W Instytucie Teleinformatyki i Automatyki WAT prowadzona jest praca naukowo-badawcza pt. „Opracowanie reguł IDS dla obrony przed atakiem wewnętrznym”. Ogólnym celem naukowym jest badanie sposobów ataku

wewnętrznego i ich zależności od rozwiązań technicznych i informacyjnych sieci LAN oraz – jeśli okaże się to możliwe – wskazanie ogólnej metodyki budowania reguł IDS. Celem podstawowym jest jednak opracowanie zbioru aktualnych reguł IDS chroniących sieci lokalne przed atakami wewnętrznymi i rozpoznanie możliwości adaptacji oraz utrzymywania aktualności tego zbioru niewielkim wysiłkiem lokalnych administratorów sieci korporacyjnej. Ponadto przewiduje się opracowania dotyczące metod budowy specyficznych podzbiorów reguł oraz metod utrzymywania aktualności reguł broniących przed atakami wewnętrznymi. W szczególności za użyteczne uznaje się możliwości rutynowego wykorzystywania publikowanych (np. w Internecie) wyników prowadzonych badań: poszukiwania i analiz sygnatur ataków. W przypadku reguł dla IDS *open source* spodziewane jest duże zainteresowanie użytkowników: głównie administratorów sieci lokalnych.

Praca dotyczy przede wszystkim tzw. *network oriented IDS*, tzn. systemów wykrywania włamań osadzonych na komputerze z interfejsem sieciowym pracującym w trybie *promiscuous*, gdzie badaniu przez IDS podlega cały ruch sieciowy w strefie dystrybucji pakietów, zaś obiektami chronionymi są elementy sieci. Należy zauważyć, że dla istoty badań nie ma szczególnego znaczenia, czy tzw. sondą IDS jest pojedynczy komputer jak opisano powyżej, czy też, spełniające tę samą rolę rozproszone po wielu komputerach w sieci oprogramowanie nadzorujące ruch sieciowy docierający do tych komputerów w sieci przełączanej (tzn. takiej, w której do poszczególnych komputerów docierają tylko pakiety do nich adresowane). Rozproszone oprogramowanie nadzorujące ruch sieciowy to tzw. *host oriented IDS* – droższy i wolniejszy w reakcjach. W nowoczesnych sieciach z przełącznikami (*switched networks*) ten rodzaj IDS może okazać się skuteczniejszy. Dla badań dotyczących zbiorów reguł IDS, ich budowy i zachowania w sieciach wewnętrznych nie jest konieczne rozróżnianie między wymienionymi typami IDS.

Niezależnie od tego skąd uzyskano reguły, zapewne nie będą one w pełni odpowiadać potrzebom sieci i wystąpi potrzeba ich adaptacji. Jednym z przedmiotów badań jest sposób adaptowania pewnego zbioru reguł do potrzeb konkretnej sieci. Jak się okazuje, problemy adaptacji reguł mogą mieć duże znaczenie praktyczne – od metody adaptacji może zależeć użyteczność i skuteczność IDS, a dokładniej możliwość utrzymywania aktualności IDS. W konsekwencji może ona decydować o szansach powodzenia administratorów sieci lokalnej w ich nieustannej pogoni za rozwojem stanu sztuki w dziedzinie ataków sieciowych.

## 2. System wykrywania włamań (IDS)

Szczególnie użyteczny w niewielkich sieciach lokalnych wydaje się system wykrywania włamań Snort – bezpłatny, z zatem dostępny dla niewielkich firm, których nie stać na drogie, komercyjne rozwiązania. Snort rozpowszechniany jest na licencji GPL. Dostępne są wersje dla systemów Unix i Windows, Snort jest też składnikiem niektórych dystrybucji Linuksa (Trinux, SuSe, Debian) i NetBSD. Snort został wybrany ze względu na jego elastyczność i otwartość oraz dostępność kodów źródłowych, jednak główną przesłanką jego wykorzystania jest czytelny sposób zapisu zbioru reguł. Popularność tego sposobu zapisu stale rośnie i jak się wydaje zbliża się do ustanowienia standardu de facto.

Snort jest snifferem – istotą jego działania jest badanie każdego pakietu docierającego do karty sieciowej komputera-nosiciela, ponadto udostępnia możliwość rejestrowania wybranych elementów ruchu sieciowego. Możliwość rejestracji jest użyteczna w gromadzeniu dowodów przeciwko napastnikom, ale również w trakcie prowadzenia prac badawczych. W konkretnej instalacji o zachowaniu i skuteczności systemu SNORT stanowią dwa elementy: konfiguracja (w klasycznym rozumieniu jako zestaw specyficznych dla instalacji wartości wielkości określonych arbitralnie przez producenta) oraz zbiór rozpoznawanych sygnatur ataków sieciowych, zapisany w postaci zbioru reguł IDS. Na tej podstawie wykrywalne są różne rodzaje ataków na różnych poziomach protokołów, a także próby pozyskiwania informacji (tzw. skanowania). W przeciwieństwie do sond większości firewalli Snort może głęboko analizować treść przesyłanej informacji (nie tylko same nagłówki pakietów), a także dynamicznie reagować na wykrywane zdarzenia, np. resetując sesje (tylko z biblioteką libnet) lub powodując alarmowanie. Wykrywanie ataków (czy ogólniej – zdarzeń) polega na porównywaniu zawartości pakietów lub własności ich strumieni z bazą sygnatur. System detekcji zwykle porównuje po prostu cechy pakietu z zapisami w zbiorze reguł. Jeśli cechy pakietu dopasowują go do którejś z reguł, zostaje podjęta odpowiednia akcja. Do porównywanych cech pakietu należą atrybuty główne – adresy, porty źródłowe i docelowe - oraz opcje pomocnicze: flagi TCP identyfikujące np. żądania związane z WWW, różne typy pakietów ICMP, opcje IP czy wreszcie sama treść pakietu.

Zbiór sygnatur ataków powinien zmieniać się wraz ze zmianami stanu sztuki w dziedzinie ataków. Już z tego powodu zbiory reguł IDS powinny być aktualizowane. Ponadto zwykle tylko pewna część znanych ataków sieciowych jest możliwa w konkretnej sieci – uwzględnianie sygnatur pozostałych ataków w zbiorze reguł sieci jest niecelowe, a zapewne i szkodliwe w przypadku ograniczonej mocy obliczeniowej komputera-nosiciela IDS. I wreszcie – wśród

reguł znajdują się i takie, które powodują niewłaściwe reakcje – w najprostszym przypadku fałszywe alarmy. Przyczyny są różne, ale dające się uogólnić do stwierdzenia, że pewne reguły nie są odpowiednie dla ruchu w konkretnej sieci i powinny zostać skorygowane lub wyeliminowane ze zbioru reguł.

## 3. Zmiany zbioru reguł

Można oczekiwać, że w systemach IDS okresowo występować będzie sytuacja, w której pojawią się nowe reguły, które powinny zostać włączone do aktualnego zbioru reguł. W szczególnym przypadku – na początku – aktualny zbiór reguł może być pusty, a zbiór nowych reguł (aktualizacji) bardzo liczny. W każdym przypadku zajdzie zapewne potrzeba zaadaptowania zbioru reguł do potrzeb sieci. Z pewnością będzie tak w przypadku przyjęcia zbioru reguł z publikacji Internetowych na potrzeby IDS w sieci lokalnej.

Ogólne cechy zbioru reguł można określić następująco:

- Skuteczność – proporcjonalna do liczby typów wykrywanych ataków. Im niższa skuteczność, tym większa liczba błędów pierwszego rodzaju (pominięcia ataków). Skuteczność mierzona jest tylko w stosunku do zbioru narażeń (typów ataków, których wystąpienie zostało uznane za możliwe).
- Nadczułość – proporcjonalna do liczby zdarzeń powodujących fałszywe alarmy (błędy drugiego rodzaju). Określana tylko w odniesieniu do zdarzeń, których wystąpienie w trakcie poprawnej pracy systemu uznano za możliwe.
- Informacyjność – proporcjonalna do stopnia informacji o zdarzeniach sieciowych, które to informacje są zachowywane w ramach reakcji zapisanych w regułach IDS. Dla pojedynczej reguły Informacyjność jest maksymalna, gdy zachowane zostaną wszelkie informacje dotyczące zdarzenia dostępne w ruchu sieciowym.
- Obciążalność[1], wynikająca z:
  a. Liczności zbioru reguł.
  b. Angażowania mocy obliczeniowych w realizację sprawdzeń poszczególnych reguł.
  c. Organizacji sprawdzeń.

[1] Obciążalność (dla profilu zachowania się Q) równa się sumie (po wszystkich klasach abstrakcji zdarzeń Z składających się na Q) iloczynów: udziału (części) zdarzeń klasy w całości ruchu przez wnoszone obciążenie jednostkowe wyrażone czasem zajętości procesora. Interpretacją „obciążalności" jest średni czas badania zdarzenia. Jeśli średni czas badania zdarzenia jest zdecydowanie mniejszy niż odwrotność częstotliwości zdarzeń dla profilu, to obciążalność może nie być rozważana w badaniach.

Dla wyznaczenia obciążalności należy dla środowiska wyznaczyć dwa profile ruchu: profil przeciętnego ruchu oraz profil ruchu szczytowego. Dla każdego z nich należy określić częstość wystąpienia każdego typu zdarzeń (pakietów) wyróżnionego ze względu na wprowadzone zaangażowanie mocy obliczeniowych. Dla segmentów Fast Ethernet (100 Mb) zapewnienie, że czas sprawdzania zdarzenia będzie mniejszy niż czas transmisji najkrótszej ramki Ethernetu czyni zapewne dalsze badanie obciążalności niepotrzebnym.

Ocena cech zbioru reguł nie będzie dokładna bez określenia zachowania się ruchu sieciowego w miejscu badania. W rozważanych zastosowaniach IDS w sieciach lokalnych rozważanie obciążalności można pominąć.

Wysoką skuteczność, a zatem zdolność do wykrywania szerokiego spektrum niepożądanych zachowań w sieci, może zostać osiągnięta dzięki pozyskaniu możliwie aktualnego zbioru reguł opracowanego przez godne zaufania gremium – zespół analityków firmy lub innej organizacji specjalizującej się w pracach z zakresu bezpieczeństwa teleinformatycznego. Tak pozyskane, początkowe zbiory reguł powinny zostać zaadaptowane na potrzeby konkretnej sieci drogą określenia wartości zmiennych lokalnych (co jest czynnością stosunkowo prostą i właściwie leżącą w dziedzinie konfiguracji) a następnie przez wyeliminowanie reguł, które nie odpowiadają tej sieci. Eliminacja może dotyczyć tych reguł, które nie mają zastosowania do sieci, ponieważ określają zdarzenia, które nie mogą w niej mieć miejsca (np. dotyczą protokołów, które nie są w sieci wykorzystywane) – ten rodzaj eliminacji, zastosowany dla zmniejszenia obciążalności, nie musi być przeprowadzony, jeśli moce obliczeniowe nosiciela są wystarczające. Istotne znaczenie ma natomiast eliminacja tych reguł, które powodują fałszywe alarmy i to ona stanowi najważniejszy element adaptacji zbioru reguł. Można wskazać trzy sposoby prowadzenia adaptacji: metodę mechaniczną, superekspert i metodę adaptacji różnicowej.

1. Metoda mechaniczna.

Najmniej absorbująca dla administratorów – zarówno co do sposobu adaptowania reguł, jak i w trakcie użytkowania zaadaptowanego zbioru. Pozwala na wykorzystanie doświadczeń środowiska – wielu ekspertów i administratorów pracujących nad zbudowaniem uniwersalnego zbioru reguł IDS, w szczególności niekomercyjnego Snorta. Istotą postępowania jest czysto mechaniczny (bez rozważania przyczyn i skutków) zabieg eliminacji, z pewnego początkowego zbioru reguł, wszystkich reguł powodujących fałszywe alarmy w trakcie okresu adaptacji (w sieci docelowej lub reprezentatywnej zakłada się, że w okresie adaptacji nie występują zdarzenia, na które IDS powinien reagować i eliminuje się wszelkie reguły, które powodują sygnalizację); na koniec okresu

adaptacji otrzymuje się docelowy zbiór reguł. Długość okresu adaptacji może być arbitralnie ustalona lub może trwać do wygaśnięcia sygnalizacji (pojawiania się alarmów IDS). Oczywiście po zakończeniu okresu adaptacji następuje okres użytkowy, w trakcie którego każda sygnalizacja jest podstawą do wszczęcia postępowania – tzw. obsługi incydentu. Główną wadą tej metody jest to, że wymaga akceptowalnego prawdopodobieństwa, że istotnie w trakcie okresu adaptacji nie zajdą w sieci zdarzenia niepożądane, gdyż w czasie okresu adaptacji IDS nie chroni sieci, a co gorsza zajście ataku powoduje „znieczulenie" systemu na ten atak.

Dla opisywanej metody aktualizacja zbioru reguł to powtarzanie całej procedury adaptacji od początku dla nowego, początkowego zbioru reguł. Niestety im częściej to się czyni, tym więcej występuje okresów adaptacji, w trakcie których system nie jest chroniony. Nagrodą za częstą aktualizację, jest znaczna aktualność i skuteczność zbioru reguł IDS między okresami adaptacji – zestawy reguł bardziej nadążają za wysiłkami hakerów i odwrotnie. Zaangażowanie intelektualne administratorów lokalnej sieci polega tylko na właściwym zdefiniowaniu (nadaniu wartości początkowych) zmiennym języka definicji reguł, a w trakcie eksploatacji na decyzjach o podjęciu aktualizacji.

2. Metoda supereksperta.

Metoda ta wymaga największego zaangażowania od obsługi – zbiór reguł jest budowany, po czym aktualizowany na bieżąco przez ekspertów na podstawie znajomości sygnatur ataków sieciowych. Alarmy są analizowane na bieżąco przez ekspertów i za każdym razem podejmowana jest decyzja, czy regułę powodującą alarm należy usunąć ze zbioru reguł, czy też wszcząć postępowanie w sprawie incydentu.

3. Metoda adaptacji różnicowej.

Początkowe postępowanie realizowane jest jak w metodzie czysto adaptacyjnej: zdefiniowanie wartości zmiennych i okres adaptacji z eliminacją reguł aż do wygaśnięcia alarmów. Następnie po każdej publikacji nowego zestawu reguł, lub po opublikowaniu pojedynczej sygnatury ataku, następuje określenie różnicy zbiorów: nowego i zaakceptowanego, oraz dodanie nowego zbioru do zbioru reguł zaakceptowanych. Różnicowy zbiór reguł przez pewien ustalony czas jest zachowywany dla celów analizy alarmów: po alarmie, jeśli reguła powodująca alarm nie należy do zbioru różnicowego, wszczynane jest postępowanie w związku z incydentem, zaś gdy reguła ta należy do zbioru różnicowego – przeprowadzana jest analiza i podejmowana decyzja: incydent, czy eliminacja. Ten sposób postępowania rokuje największe nadzieje.

Metoda różnicowa to nie wymagający specjalnych kwalifikacji sposób nadążania za stanem sztuki w dziedzinie włamań, ale niestety przez okres

adaptacji system jest nieodporny właśnie na najnowsze ataki; co gorsza, jeśli ktoś przeprowadzi atak z syndromem wyzwalającym rozpoznawanym przez reguły należące do zbioru różnicowego, to spowoduje zablokowanie rozpoznawania takiego ataku już „na zawsze".

Sposobem na uniknięcie takich zagrożeń, jest przeniesienie badania do sieci testowych lub skrócenie do minimum pojedynczego okresu adaptacji. Skuteczne sprawdzenie tą drogą reguł należących do zbioru różnicowego jest możliwe, ponieważ jakość sprawdzania zależy nie od czasu, ale od liczby zachodzących w trakcie badania różnorodnych zdarzeń sieciowych. Dobrym rozwiązaniem wydaje się dokonanie zapisu całego ruchu w punkcie instalacji sondy IDS (nagranie „benchmarku" sieciowego) w warunkach „normalnej eksploatacji sieci wzorcowej" i potem poddanie zbioru reguł badaniom symulując ruch za pomocą odtwarzania tego benchmarku.

Można zatem określić kolejną metodę:

4. Metoda adaptacji za pomocą benchmarków ruchu sieciowego.

Postępowanie to może być prowadzone według wzorca opisanego w dowolnej z wcześniej opisanych metod. Istotną różnicą jest prowadzenie adaptacji zbioru reguł w dwukomputerowej sieci testowej, gdzie do komputera-nosiciela IDS podłączony jest (np. przez tzw. *crosslink*) drugi komputer, pracujący jako generator ramek symulowanego ruchu sieciowego, odtwarzający tzw. benchmark, czyli reprezentatywny fragment ruchu nagrany, najlepiej dobrany i przygotowany wcześniej przez eksperta. Poza tym, że metoda ta zajmuje (wyłączając z użytkowania na okres adaptacji zbioru reguł) dwa komputery, ma ona tę zaletę, że po przygotowaniu benchmarków do jej realizacji, ma zalety odpowiedniej wcześniej opisanych metod, bez ich wad, w szczególności bez okresów adaptacji, w trakcie których sieć jest pozbawiona ochrony. Do chwili zakończenia badania nowego zbioru reguł nie wprowadza się modyfikacji „produkcyjnego" IDS. Najwłaściwsza, bo najprostsza w realizacji, wydaje się metoda mechaniczna z wykorzystaniem benchmarków.

## 4. Narzędzia adaptacji

Dla administratora małej sieci niestety nawet realizacja pozornie prostej metody mechanicznej z wykorzystaniem benchmarków wydaje się zbyt skomplikowana. Głównym problemem będzie, jak się wydaje, brak oprogramowania do nagrywania i odtwarzania ruchu sieciowego. Nagrywanie ruchu można przeprowadzić za pomocą dowolnego sniffera rejestrującego (także

za pomocą Snorta), ale obecnie dostępne narzędzia zdolne do odtwarzania tak zarejestrowanego ruchu nie są doskonałe.

Oprócz odtwarzania ruchu sieciowego zarejestrowanego w standardowym formacie (np. przez Snorta) pożądana jest możliwość łatwej edycji zarejestrowanego ruchu; przynajmniej z dwóch powodów:

Dla umożliwienia ekspertom możliwości zmniejszenia zapisu o fragmenty (np. całe sesje) powtarzające się. Pozwoli to zmniejszyć objętość zapisu i czas testowania.

Dla usunięcia z poszczególnych sesji danych nieistotnych dla celu testowania, a niosących informacje uznawane za wrażliwe przez dysponenta sieci.

Dodatkowym wymaganiem, którego spełnienie może w przyszłości mieć istotne znaczenie, jest zachowanie zależności czasowych (harmonogramu) zarejestrowanego ruchu. Oznacza to potrzebę rejestrowania czasów nadejścia poszczególnych pakietów, a następnie zachowania odpowiednich zależności czasowych przy odtwarzaniu ruchu. Obecnie reguły IDS nie uwzględniają zależności czasowych w badanym ruchu poza rozpoznawaniem skanowania[2] i tzw. ataków zalewania (np. *syn-flooding*). Pominięcie zależności czasowych w odtwarzanym ruchu sieciowym obecnie może mieć tylko korzystne skutki, dzięki skróceniu czasu badania, gdyż podczas badania zarejestrowane pakiety będą nadchodzić tylko szybciej niż w rzeczywistości. Obecnie zaś nie są znane syndromy, dla których przyspieszenie zdarzeń w ruchu sieciowym powodowałoby ich nierozpoznanie.

Opracowanie oprogramowania pozwalającego na wygodną edycję zarejestrowanego ruchu sieciowego i zdolnego do jego odtwarzania wydaje się konieczne dla udostępnienia benchmarkowych metod adaptacji zbiorów reguł IDS do szerokiego wykorzystania. Oprogramowanie to może stać się również użytecznym narzędziem w bardziej wyrafinowanych przedsięwzięciach – badawczych lub takich, w których celem jest przygotowanie zbiorów reguł dla całych klas sieci.

Póki co można używać z powodzeniem np. programu IRIS firmy eEye[3] – ten komercyjny sniffer pozwala na wysyłanie zarejestrowanego ruchu ze stałym interwałem, a także udostępnia pewne możliwości edycyjne – usuwanie pakietów.

[2] Snort zawiera mechanizmy zwane preprocesorami (nie w pełni odpowiadające opisywanemu tu modelowi reguł), które pozwalają na uwzględnienie ciągów zdarzeń i zależności czasowych w ruchu sieciowym. Spodziewany jest rozwój tych mechanizmów.
[3] Iris™ the Network Traffic Analyzer firmy eEye Digital Security.

Oprócz dążenia do eliminacji reguł z pewnych nadmiarowych zbiorów reguł, zbiory reguł mogą być badane na skuteczność wykrywania syndromów ataków. W takim przypadku byłoby można zebrać zapis ruchu sieciowego zawierający syndromy ataków i wykorzystać je w badaniach w podobnych konfiguracjach sprzętowo-programowych. O ile jednak benchmark „normalnego" ruchu wykorzystywany był do wykrycia i eliminacji reguł powodujących fałszywe alarmy, o tyle zapis ruchu z syndromami ataków zostałby użyty *á rebous*: dla zlokalizowania brakujących reguł w zbiorze reguł. W ostatnich zdaniach użyto trybu warunkowego – nie wydaje się bowiem rozsądne tworzenie zapisu ruchu drogą symulacji ataków przez eksperta, po czym badanie zbioru reguł, gdy nierównie prostszy wydaje się po prostu przegląd przez tegoż eksperta zbioru reguł. Poza tym, trzeba mieć do dyspozycji eksperta o odpowiedniej wiedzy.

Dla badania zbioru reguł na skuteczność wykrywania ataków rozsądne wydaje się wykorzystanie (podobnie jak w przypadku adaptowanych zbiorów reguł) wiedzy ekspertów zawartej w tzw. skanerach bezpieczeństwa. Skanery bezpieczeństwa[4] mogą z powodzeniem zastąpić zapisy ruchu sieciowego zawierającego syndromy ataków - można ich użyć jako generatorów ruchu nasyconego syndromami. Jako uzupełnienia można użyć tzw. exploitów[5].

Dla porządku należy jednak zwrócić uwagę, że badanie zbioru reguł na skuteczność wydaje się potrzebne tylko w przypadku braku zaufania do kompletności zbioru reguł. W przypadku rekomendowanego wcześniej podejścia zmierzającego do wykorzystywania publikowanych zbiorów reguł taka sytuacja w ogólnym przypadku nie wystąpi. Wydaje się jednak, że po eliminacji niektórych reguł (powodujących fałszywe alarmy) mogą zajść podejrzenia, że zbiór reguł utracił zdolność reagowania na syndromy ataków, do wykrywania których przeznaczone były wyeliminowane reguły. W takim przypadku sprawdzenie zbioru reguł za pomocą odpowiednich exploitów lub odpowiednio wysterowanych skanerów bezpieczeństwa wydaje się bardzo użyteczną metodą rozstrzygnięcia wątpliwości.

## 5. Dwie drogi

Dla ilustracji dalej przedstawione zostały dwa różne podejścia do adaptacji publikowanych syndromów ataków na potrzeby sieci lokalnych w celu

[4] Skanerem bezpieczeństwa nazywa się program (rzadziej urządzenie) zdolne do przeglądania (badania) zadanego zbioru komputerów na obecność podatności.

[5] Eksploit to rutynowy algorytm (często w postaci skryptu lub programu) wykorzystania słabości systemu komputerowego ze szkodą dla bezpieczeństwa tego systemu. Eksploit są dostępne w Internecie.

zwalczania ataków lokalnych: podejście minimalne, przeznaczone dla administratorów niewielkich sieci, nie mających kwalifikacji lub czasu na obsługę IDS i na rozwiązywanie problemów związanych z niepewną sygnalizacją incydentów, oraz podejście maksymalistyczne – wymagające angażowania własnych ekspertów w badania nad sygnaturami ataków, nadal jednak zmierzające do uzyskania konfiguracji IDS minimalizującej liczbę fałszywych alarmów.

Dla osiągnięcia dobrych efektów z możliwie małym wysiłkiem lokalnych administratorów i bez angażowania ekspertów można zalecić następujący tryb postępowania:

1. Wybór miejsca włączenia sondy IDS.
2. Nagranie całego ruchu w miejscu włączenia sondy IDS w trakcie typowej pracy sieci.
3. Edycja nagranego zapisu ruchu dla otrzymania benchmarku do testów (ten krok nie jest niezbędny, pozwoli jednak znakomicie skrócić czas badania).

Po każdej publikacji nowego zbioru reguł:

4. Wykonanie kopii instalacji sondy IDS i wprowadzenie do niej nowego zbioru reguł.
5. Połączenie bezpośrednie nowego IDS z komputerem testowym, generującym ruch z opracowanego benchmarku.
6. Usunięcie ze zbioru reguł wszystkich reguł, które spowodowały alarmy w trakcie odtwarzania ruchu.
7. Wyłączenie starego IDS i włączenie w to miejsce nowego IDS.

Ten tryb postępowania wymaga posiadania narzędzia: oprogramowania generatora (a dla realizacji punktu 3 także i edytora) zapisanego ruchu sieciowego.

Dla większej sieci, a w szczególności dla grupy podobnych sieci opłacalne może być wprowadzenie badań przygotowujące reguły IDS, w którym bierze udział własna grupa ekspertów wykorzystując jednak również przede wszystkim publikowane reguły. Poniżej przedstawiono schemat postępowania w przygotowaniu zbioru reguł bez uwzględniania możliwości wykorzystania benchmarków – oczywiście wszelkie badania „w sieci docelowej" (lub reprezentatywnej) mogą zostać zastąpione dużo tańszym i bezpieczniejszym badaniem za pomocą benchmarku.

1. Jeśli zachodzi potrzeba włączenia do wyników prac zewnętrznych, powinny być one akceptowane w postaci zbiorów reguł. W takim przypadku:
    a. Należy określić zbiór różnicowy zbioru reguł zewnętrznych i zbioru reguł zaakceptowanych (zbiór wszystkich reguł należących do zbioru reguł zewnętrznych i nie należących do zbioru reguł zaakceptowanych).

   b. Poddać analizie (przez ekspertów w dziedzinie budowy lokalnej sieci, niekoniecznie ataków sieciowych) zbiór różnicowy i w jej wyniku odrzucić wszystkie te reguły, które z pewnością nie mają zastosowania dla sieci docelowej.

   W szczególności na początku eksploatacji systemu zbiór reguł zaakceptowanych może być zbiorem pustym, zaś jako pierwszy zostanie włączony do badań zbiór reguł pozyskany z ogólnie akceptowanego źródła. W rezultacie analizie zostanie poddany zbiór zewnętrzny (jako różnica tego zbioru i zbioru pustego).
2. Jeśli w wyniku analiz własnych opracowano nowe reguły, należy dołączyć je do zbioru reguł zaakceptowanych.
3. Zbiór reguł zaakceptowanych należy poddać badaniu w sieci testowej, dla sprawdzenia zbioru reguł na skuteczność wykrywania ataków.
   a. Badanie za pomocą uznanych wzorców ataków – skanerami bezpieczeństwa.
   b. Badanie technikami heurystycznymi.
4. Zbiór reguł zaakceptowanych należy poddać badaniu w sieci docelowej, dla sprawdzenia możliwości fałszywych alarmów w warunkach naturalnej aktywności licznych użytkowników. Wynikiem badania powinien być zapis aktywności IDS i dodatkowych narzędzi rejestrujących (jeśli zostały włączone).
5. Jeśli zarejestrowano sygnalizację IDS podczas badania fałszywych alarmów w sieci docelowej, należy poddać analizie nadesłane materiały, dla rozstrzygnięcia, które z sygnałów świadczą o:
   a. Rzeczywistym incydencie – w takim przypadku należy zaniechać zmian w zbiorze zaakceptowanych reguł i sporządzić raport o incydencie dla administratora sieci docelowej. Jeśli dla tego rozstrzygnięcia wcześniej wprowadzono specjalne ustawienia mechanizmów rejestracji – należy je teraz wyeliminować.
   b. Fałszywym alarmie – w takim przypadku należy wyeliminować regułę powodującą fałszywe alarmy. Dla każdej z wyeliminowanych reguł należy sporządzić:
      i. opis wykrywanego zdarzenia,
      ii. listę ataków (zdarzeń), dla których owo zdarzenie jest symptomatyczne,
      iii. ocenę skutków pominięcia reguły,
      iv. analizę i budowę reguł zastępczych.

      Jeśli dla tego rozstrzygnięcia wcześniej wprowadzono specjalne ustawienia mechanizmów rejestracji – należy je teraz wyeliminować.
   c. Niejasnej przyczynie sygnalizacji przez regułę – dla takich przypadków należy ustalić nowe ustawienia mechanizmów

rejestracji, nie zmieniając zawartości zbioru reguł zaakceptowanych.

6. Jeśli wyniki badań z punktów 3 i 4 nie spełniają postawionych wstępnie wymagań, należy powtórzyć cykl badań od punktu 1. W przeciwnym przypadku można zbiór reguł zaakceptowanych uznać za ostateczny a samo badanie można uznać za zakończone. Reguły, dla których powstał problem kwalifikacji pomimo zmian ustawień mechanizmów rejestracji zdarzeń, należy jednak, w przypadku sieci docelowej bez sprawnej obsługi informatycznej, wyeliminować.

Można przyjąć, że przygotowywanie IDS do pracy w konkretnej sieci, a następnie utrzymanie jego skuteczności powinno obejmować trzy procesy:

- Analityczny: budowanie i/lub adaptacja zbioru reguł odpowiadającego profilom ruchu w sieciach wewnętrznych; wymyślanie nowych syndromów ataków (i w konsekwencji reguł wykrywających te syndromy) i sprawdzanie skuteczności; cel: minimalizacja błędów pierwszego rodzaju (poszukiwanie własnych reguł).
- Doświadczalny – obserwacyjny: badanie w rzeczywistym środowisku, dla wykrywania i minimalizacji fałszywych alarmów (badanie nadczułości).
- Eksperymentalny – poszukiwanie reguł zastępczych dla tych, które powodują fałszywe alarmy: wszechstronne badanie eksperymentalne zdarzeń, dla których stwierdzono błędy drugiego rodzaju w trakcie badań doświadczalnych, reguł powodujących sygnalizację fałszywych alarmów oraz zdarzeń, do których wykrywania owe reguły były przeznaczone; formułowanie alternatywnych reguł; ponadto badanie skuteczności w warunkach wymuszanych ataków.

Ogólnie należy zmierzać do tego, aby w jak najszerszym stopniu wykorzystywać pracę innych – obcych ekspertów. Jak łatwo zauważyć najbardziej uproszczone sposoby utrzymywania IDS sprowadzają się do wykorzystania wyników etapu analitycznego obcych zespołów ekspertów, po czym realizacji tylko etapu doświadczalnego bez zawracania sobie głowy etapem eksperymentalnym.

## 6. Podsumowanie

Systemy wykrywania włamań do tej pory praktycznie nie były dostępne w większości małych i średnich sieci biurowych Windows, należących do oszczędnie gospodarujących firm. Duże, oferowane komercyjnie systemy są za drogie i nie mieszczą się w rozsądnie skalkulowanych nakładach na bezpieczeństwo, zaś darmowe systemy *open source* wymagają zbyt wiele

od administratorów sieci: w zakresie kwalifikacji lub czasu angażowanego na obsługę. Intencją niniejszego tekstu była prezentacja rozwiązania tego problemu – wskazanie sposobu obsługi darmowego systemu IDS, zapewniającego, co prawda po opracowaniu dodatkowych narzędzi, rutynową obsługę i pewność sygnalizacji. Pozwoli to na skuteczność IDS nawet w przypadku, gdy obsługą sieci zajmuje się pracownik bez gruntownego wykształcenia informatycznego.

Dla utrzymania stałej skuteczności IDS w sieciach wewnętrznych najskuteczniejsze wydaje się wykorzystanie dorobku grup ekspertów pracujących nad rozpoznawaniem nowych sygnatur ataków. Najtańsze jest wykorzystanie takich sygnatur, już wstępnie przygotowanych w postaci zbiorów reguł dla IDS, publikowanych bezpłatnie dla systemów *open source*. Istotny jest jednak problem każdorazowego przystosowania publikowanych materiałów do potrzeb konkretnej sieci, głównie dla uniknięcia fałszywych alarmów. Chodzi przede wszystkim o wysoką pewność sygnalizacji – administrator powinien mieć zaufanie do systemu tak, aby nie tracić czasu na rozstrzyganie, czy po sygnale IDS należy wszcząć procedurę obsługi incydentu, czy nie.

Adaptacja publicznie dostępnych zbiorów reguł stanowi pewien problem dla IDS zainstalowanych w sieciach lokalnych dla obrony przed atakami wewnętrznymi. Przyczyną jest publikowanie zbiorów reguł przeznaczonych głównie do wykrywania ataków z sieci zewnętrznej (zwykle Internetu), co w konsekwencji powoduje znaczne liczby fałszywych alarmów w przypadku wykorzystania tych reguł w sieci lokalnej dla obrony przed atakami wewnętrznymi. Największe nadzieje dla utrzymywania aktualności IDS rokuje adaptowanie zbiorów reguł drogą ich badania z wykorzystaniem benchmarków ruchu sieciowego z docelowej sieci.

## Literatura:

[1] http://aris.securityfocus.com/
[2] http://echelon.pl/pubs/snort.html
[3] http://www.silicondefense.com/software/snortsnarf/
[4] http://www.snort.org/
[5] http://www.snort.org/docs/writing_rules/
[6] http://www.whitehats.com/ids/
[7] http://www.winsnort.com/

*Recenzent: prof. dr hab. inż. Włodzimierz Kwiatkowski*

*Praca wpłynęła do redakcji 19.11.2003*