STUDIA INFORMATICA 2002
Volume 23 Number 3 (50)

Mirosław SKRZEWSKI
Politechnika Śląska, Instytut Informatyki

SYSTEMY WYKRYWANIA ZAGROŻEŃ (SYSTEMY IDS)

Streszczenie. Systemy wykrywania zagrożeń pojawiły się jako uzupełnienie rozwiązań ochrony sieci lokalnych przed zagrożeniami, mające za zadanie dostarczać aktualnych informacji o stanie bezpieczeństwa sieci. Różne rozwiązania próbują wykorzystywać do tego celu różne zasoby informacji o stanie sieci i różne metody ich analizy. Opracowanie przedstawia dostępne informacje o dokładności, efektywności i ograniczeniach stosowanych metod wykrywania zagrożeń.

INTRUSION DETECTION SYSTEMS (IDS)

Summary. Intrusion Detection Systems appeared on the market as supplementary systems to existing means of LAN protection, with the aim of delivery of up-to-date LAN security related information. In order to achieve this goal different systems attempt to employ different resources of system and network security information and different methods of their analysis. The paper presents available information about the accuracy, efficiency and limitation of methods applied in IDS systems.

1. Wprowadzenie

Systemy wykrywania zagrożeń pojawiły się jako uzupełnienie linii obronnych sieci lokalnych, składających się z ruterów dostępowych oraz systemów ścian ogniowych (firewall-i), tworzących zabezpieczenia sieci oparte na mechanizmach filtracji pakietów, o systemy „szybkiego informowania i reagowania", mające za zadanie dostarczać na bieżąco w miarę aktualne informacje o stanie bezpieczeństwa sieci. Systemy te znajdują się w fazie intensywnego rozwoju, na rynku pojawiają się ciągle nowe rozwiązania wykorzystujące różne zasoby informacji i różne metody ich analizy dla określenia stanu bezpieczeństwa

(zagrożenia) sieci. Celem opracowania jest próba przeanalizowania dostępnych informacji o ograniczeniach, dokładności i efektywności stosowanych metod wykrywania zagrożeń.

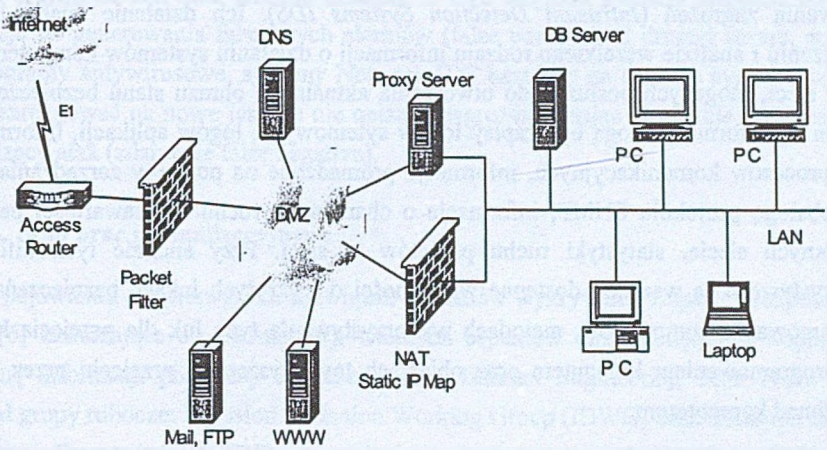
2. Organizacja ochrony sieci przed zagrożeniami

Sieć lokalą stanowi zbiorowisko należących do jednej organizacji maszyn cyfrowych połączonych szybkimi łączami transmisji, mniej lub bardziej odseparowane od otoczenia. Całość komunikacji ze światem zewnętrznym obsługiwana jest przez jeden lub czasem więcej ruterów, obsługujących szybkie łącza szeregowe. Ochrona sieci przed nieuprawnionym dostępem rozpoczyna się na punkcie granicznym, w ruterze z odpowiednio skonfigurowaną listą kontroli dostępu (Access Control List ACL), nakładającą ograniczenia na adresy IP sieci, z których i do których dozwolona jest komunikacja do/z sieci lokalnej. Właściwą linię obrony, umożliwiającą bardzo precyzyjną filtrację ruchu pakietów, z dokładnością do pojedynczych portów i adresów IP zapewniają dedykowane urządzenia (komputery) ściany ogniowej – firewall-e. Ich oprogramowanie umożliwia również wprowadzenie kolejnego mechanizmu ochrony, pozwalającego na ukrycie struktury adresowów IP sieci – mechanizmu translacji adresów. Wykorzystuje on określony w [8] podział adresów IP na prywatne, zastrzeżone dla wykorzystania wewnątrz chronionych sieci bloki adresów 10.0.0.0/8, 172.16.0.0/12 i 192.168.0.0/16, i pozostałe adresy IP, nazwane publicznymi. Adresy prywatne traktowane są przez rutery jako nierutowalne, i zastępowane są przez firewall przydzielonymi adresami publicznymi.

Mechanizm translacji adresów (NAT) przyjmuje formę translacji dynamicznej lub statycznej. Dynamiczna translacja adresów, nazywana również maskaradą, wykorzystywana jest dla zapewnienia dostepu użytkownikom z sieci chronionej do sieci zewnętrznej (Internetu), i wykorzystuje możliwość inicjowania wielu połączeń przez pojedynczy adres IP z różnych portów źródłowych. Translacja statyczna odpowiada tłumaczeniu pojedynczych adresów prywatnych na adresy publiczne i wykorzystywana jest do „mapowania" wybranych komputerów z sieci chronionej na określone w DNS adresy publiczne.

Często stosuje się rozdzielenie funkcji filtracji pakietów i translacji adresów na osobne komputery ściany ogniowej. Pomiędzy nimi powstaje chroniona mechanizmem filtracji pakietów, pracująca na adresach publicznych podsieć, nazywana strefą zdemilitaryzowaną (DMZ). Na sieci tej instaluje się komputery świadczące usługi lub dostarczające informacji dla użytkowników zewnątrznych – serwery www, ftp, poczty, DNS, dostępowe itp. Omawiane rozwiązania ochrony wykorzystują informacje zawarte w protokołach warstwy trzeciej (sieci) i czwartej (transportowej) architektury sieci. Dla zabezpieczenia wybranych aplikacji, wykorzystywanych w sieci wewnętrznej, stosuje się dedykowane serwery

pośredniczące, konwertujące (NAT) adresy IP i buforujące przesyłaną informację – proxy serwery, określane również jako firewall-e warstwy aplikacyjnej. Rozmieszczenie zabezpieczeń chroniących przykładową sieć lokalną przed zagrożeniami przedstawia rys. 1.



Rys. 1. Rozmieszczenie zabezpieczeń chroniących sieć lokalną
Fig. 1. Placement of security means protecting LAN

3. Charakterystyka systemów wykrywania zagrożeń

3.1. Ograniczenia podstawowych systemów zabezpieczeń

Przedstawione zabezpieczenia sieci mają charakter statyczny – konfiguracja firewall-ów dostrajana jest przez administratorów i nie ulega zmianom bez ważnej potrzeby. Informacje o działaniu systemów zabezpieczających, systemów chronionych gromadzone są w postaci zapisów w logach systemowych, ich przeglądanie i interpretacja wymaga dużego doświadczenia i czasu, i odbywa się okresowo na ogół ze sporym opóźnieniem, dając czas intruzom na zatarcie śladów swojej działalności.

Charakter zabezpieczeń oferowanych przez ściany ogniowe czy też konfigurację ruterów jest bardzo kierunkowy, nastawiony zazwyczaj na obronę przed zagrożeniami z zewnątrz. Nieuprawnione działania użytkowników z wnętrza sieci, stanowiące według [6], [9] większe zagrożenie niż ataki zewnętrzne, nie są w większości wypadków wykrywane przez firewalle. Podobnie działania z zewnątrz, odbywające się w ramach legalnie dozwolonego ruchu w sieci, np. mające formę odpowiednio sformułowanych zapytań kierowanych do serwera www, mogące prowadzić do jego upadku,nie są wykrywane i rejestrowane przez statyczne systemy zabezpieczeń.

3.2. Zadania systemów wykrywania zagrożeń

Rozszerzanie systemów zabezpieczeń sieci o możliwość bieżącej kontroli przebiegu wydarzeń istotnych ze względów bezpieczeństwa doprowadziło do powstania systemów wykrywania zagrożeń (*Intrusion Detection Systems IDS*). Ich działanie oparte jest na gromadzeniu i analizie wszelkiego rodzaju informacji o działaniu systemów komputerowych i pracy sieci, mogących posłużyć do utworzenia aktualnego obrazu stanu bezpieczeństwa. Źródłem tej informacji mogą być zapisy logów sytemowych, logów aplikacji, informacje o stanie procesów komunikacyjnych, informacje gromadzone na potrzeby zarządzania siecią przez obsługę protokołu SNMP, informacje o charakterze ruchu i o zawartości pakietów przesyłanych siecią, statystyki ruchu pakietów w sieci. Przy analizie tych informacji wykorzystywane są wszelkie dostępne wiadomości o wykrytych lukach bezpieczeństwa w oprogramowaniu komputerów, metodach wykorzystywania tych luk dla przejęcia kontroli nad oprogramowaniem komputera oraz objawach towarzyszących przejęciu przez intruza kontroli nad komputerem.

3.3. Podział i własności systemów wykrywania zagrożeń

W zależności od głównego źródła analizowanych informacji systemy [6] wykrywania zagrożeń dzielą się na związane z systemem (Host IDS) i związane z siecią (Network IDS).

Działanie Host IDS oparte jest głównie na analizie zapisów z logów systemowych, logów aplikacji, metryk ochrony systemu plików i informacji o aktualnym stanie procesów w systemie, co pozwala wykrywać efekty działania intruzów zarówno z zewnątrz, jak i z wnętrza sieci. Ponieważ zapisy w logach pojawiają sie dopiero po zajściu zdarzenia, systemy Host IDS informuja o już dokonanych zmianach, i to z pewnym opóźnieniem. Z drugiej strony, informacje te, jeśli występują, są na ogół pewne.

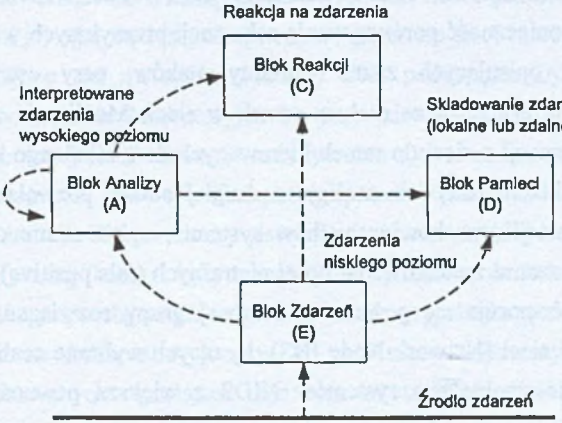
Network IDS bazują [1], [5] na informacjach pochodzących z sieci (statystyki ruchu, z SNMP, z własnego „nasłuchu" pakietów). W celu wykrycia oznak świadczących o zbliżającym się zagrożeniu posługują sie one bazą informacji o charakterystycznych sekwencjach pakietów z określoną zawartością, zarejestrowanych w poznanych metodach ataków – „sygnaturami" ataków. Dla zapewnienia skuteczności Network IDS sygnatury te powinny być często uaktualniane, aby obejmować jak największą bazę aktualnych zagrożeń.

Rozpoznanie znanej sygnatury rozwijającego się ataku pozwala na wygenerowanie informacji ostrzegającej administratora o występującym zagrożeniu jeszcze przed wystąpieniem jego skutków, oraz daje możliwość wprowadzenia mechanizmów automatycznego reagowania, np. w postaci uruchomienia skryptów blokujących czasowo dostęp do chronionej sieci z adresu IP wystepującego w podejrzanych ramkach [4].

Taka reakcja systemu IDS może jednak dać w efekcie niepotrzebne zablokowanie dostępu do usług chronionej sieci, ponieważ wykrycie w monitorowanym ruchu w sieci znanej sekwencji ramek, przypominajacej poczatek określonego rodzaju ataku nie świadczy jeszcze o tym, że taki atak właśnie nastąpił. Z tego wzgledu systemy Network IDS mają tendencje do generowania fałszywych alarmów (false positive). Z drugiej strony, podobnie jak programy antywirusowe, systemy Network IDS bazujące na analizie sygnatur nie są w stanie zareagować na nowe jeszcze nie opisane zagrożenia, dając w efekcie brak reakcji na zachodzący atak (zdarzenie false negative).

3.4. Stan prac normalizacyjnych

Po pojawieniu się pierwszych rozwiązań systemów wykrywania zagrożeń rozpoczęły się prace [6] zmierzające do normalizacji istotnych aspektów umożliwiających współpracę i wymianę informacji pomiędzy systemami IDS. Internet Engineering Task Force (IETF) powołał grupy robocze: Intrusion Detection Working Group (IDWG) oraz Common Intrusion Detection Framework (CIDF) z zadaniem opracowania standardów obejmujących zagadnienia IDS. Powstały pierwsze wersje (Internet Draft) dokumentów: *"Intrusion Detection Exchange Format Requirements and Data Model"*, *"Intrusion Alert Protocol"*, *"Intrusion Detection Exchange Protocol"* oraz *"Intrusion Detection Message Exchange Format XML"*, brak na razie finalnych dokumentów RFC.



Rys. 2. Model systemu wykrywania zagrożeń wg IETF
Fig. 2. IETF Intrusion Detection System model

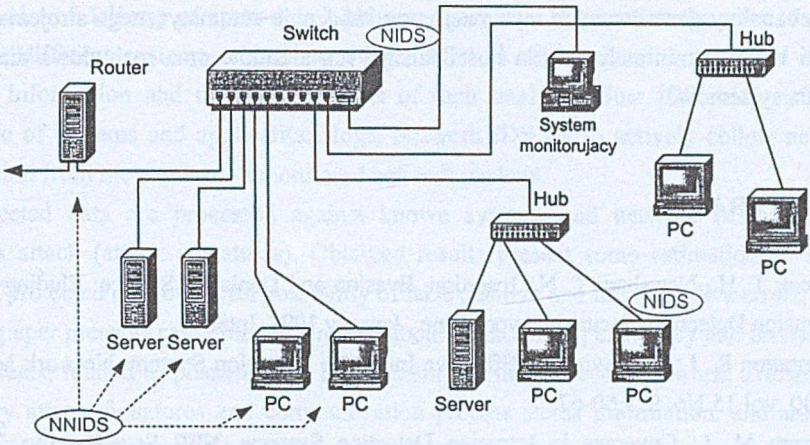
Rysunek 2 przedstawia przyjęty przez IETF model (framework) budowy systemu IDS w postaci zespołu współpracujących, niezależnych bloków funkcjonalnych oraz wystepujące między nimi przepływy informacji, będący podstawą prowadzonych prac.

3.5. Wymagania instalacyjne systemów IDS

O skuteczności działania systemu IDS decyduje, oprócz odpowiednio dobranych, aktualnych reguł analizy informacji, dobór właściwego miejsca instalacji systemu i jego sond na obszarze chronionej sieci. W przypadku rozwiązań związanych z systemem (Host IDS) istotny jest ułatwiony dostęp do wszystkich form informacji (logów) generowanych przez chronione systemy, z drugiej strony, ze względów bezpieczeństwa, odseparowanie systemu IDS od monitorowanych systemów i możliwie dokładne zamaskowanie jego obecności w sieci. W przypadku rozwiązań związanych z siecią (Network IDS) istotne jest takie ich rozmieszczenie, aby systemy IDS miały dostęp do wszystkich ramek transmitowanych z/do chronionej sieci. Ponieważ rozwój technologii sieci zdąża w kierunku rozwiązań opartych na przełącznikach kanałów (switch-e), w nowoczesnej sieci lokalnej trudno jest znaleźć dobre miejsce dla instalacji systemu NIDS, z którego widoczna jest całość ruchu w sieci.

Dostępnymi rozwiązaniami jest zainstalowanie całego systemu na firewall-u (przez który przechodzi całość ruchu sieciowego), rozdzielenie systemu IDS na kilka części (sond), monitorujących ruch ramek z wykorzystaniem wyjść monitorujących poszczególnych przełączników, lub rozproszenie całego systemu IDS na poszczególne komputery sieci i monitorowanie lokalnego ruchu ramek z/do danego komputera w połączeniu z gromadzeniem i przetwarzaniem całościowego obrazu stanu bezpieczeństwa w systemie zarządzającym. Przykładowe miejsca rozmieszczenia elementów systemu IDS przedstawia rys. 3.

Systemy Network IDS w swoim działaniu mają wiele wspólnego z systemami antywirusowymi - konieczność porównywania sekwencji przesyłanych w sieci ramek z bazą wzorców sygnatur, opisujących znane warianty ataków, przy ostrych wymaganiach czasowych nadążenia z analizą za ruchem ramek w sieci. Możliwość zmniejszenia ilości analizowanych informacji z sieci do ramek kierowanych do/z lokalnego komputera pozwala na prowadzenie dokładniejszej ich analizy, z drugiej strony pozwala na skorzystanie z dodatkowych informacji przechowywanych w systemie, np. o stanie otwartych połączeń sieciowych, co daje szanse zredukowania ilości nietrafnych (fals positive) decyzji. Być może z tych powodów obserwuje się powstawanie nowej grupy rozwiązań, określanych jako związane z węzłami sieci (Network Node IDS), łączących wybrane cechy obu poprzednich wersji – reagowania na bieżąco systemów NIDS z większą pewnością diagnozowania systemów HIDS.



Rys. 3. Możliwe miejsca instalacji systemów Network IDS
Fig. 3. Possible ways of Network IDS installation

3.6. Efektywność i skalowalność systemów IDS

Systemy wykrywania zagrożeń, szczególnie te związane z siecią, oparte są na analizie dużego strumienia informacj zawartych w przesyłanych siecią pakietach. Wyniki tej analizy zapisywane są w kolejnych logach, których przeglądanie i ocena zawartych w nich informacji wymaga czasu i doświadczenia w korzystaniu z systemu. Ilości generowanych informacji i problemy z szybkim jej ogarnięciem rosną wraz z rozmiarem sieci i ilością monitorowanych systemów. Pojawiające się na rynku systemy IDS poddawane były różnym testom, symulujacym w warunkach laboratoryjnych, przy niewielkim ruchu ramek określone zagrożenia dla chronionej sieci i na ogół radziły sobie z tymi zadaniami. W połowie 2001 roku redakcja czasopisma Network Computing przedstawiła wyniki wielomiesiecznych testów różnych systemów IDS na rzeczywistej sieci uniwersyteckiej liczącej ponad 10 000 komputerów [7]. Systemy badane były na specjalnej podsieci, do której kopiowany był z głównego wejściowego przełącznika cały ruch ramek przychodzących i wychodzących z sieci. Przeprowadzone badania wykazały, że wiekszość testowanych systemów IDS, niezależnie od stosowanych rozwiązań nie była w stanie poradzić sobie z tak dużym natężeniem ruchu, nie sygnalizowała, w których momentach gubiła (nie nadążała z analizą) ramki oraz generowała w krótkim czasie wielkie ilości komunikatów, których nikt nie był w stanie śledzić. Nawet uznane za najlepsze z testowanych rozwiazania nie posiadały dobrych narzędzi wspomagających analizę dużych ilości generowanych danych. Wydaje się, że te mankamenty wyznaczają potencjalny kierunek rozwoju (dojrzewania) systemów IDS – poprawa efektywności przetwarzania zdarzeń wejściowych, wprowadzenie efektywnych

narzędzi analizy generowanych informacji, wprowadzenie automatycznego strojenia procesu detekcji w celu zminimalizowania ilości fałszywych alarmów oraz rozbudowa diagnostyki działania systemów.

LITERATURA

1. Ptacek T. H., Newsham T. N.: Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection. Secure Networks, Inc., January 1998, Internet.
2. Hontanon R. J.: Deploying an Effective Intrusion Detection System. Network Magazine, 2000, vol.15 No. 9, s.60-67.
3. Ranum M. J.: Coverage in Intrusion Detection Systems. NFR Security, Inc. Technical Publications, June 2001, Internet.
4. Ranum M. J.: Experiences Benchmarking Intrusion Detection Systems. NFR Security, Inc. Technical Publications, Dec. 2001, Internet.
5. Miller L.: A Network Under Attack: Leverage Your Existing Instrumentation to Recognize and Respond to Hacker Attack. NetScout Systems, Inc., 2001, Internet.
6. Arcuri G., Noakes-Fry K.: Intrusion Detection Systems (IDS): Perspective. TechRepublic, Inc., 2001, www.techrepublic.com.
7. Mueller P., Shipley G.: To catch a Thief. Network Computing, 2001, Vol. 12 No. 7, s.37-67.
8. Rekhter Y., Moskowitz B., Karrenberg D., de Groot G.J., Lear D.: Address Allocation for Private Internets, RFC1918.
9. Warren S.: Design the best security topology for your firewall. TechRepublic, Inc., 2002, www.techrepublic.com.

Recenzent: Dr inż. Ryszard Winiarczyk

Wpłynęło do Redakcji 6 maja 2002 r.

Abstract

Intrusion Detection Systems appeared on the market as a supplement to existing means of local area network protection, such as router access control lists and many kinds of firewalls,

with the aim of delivery of up-to-date LAN security related information. In order to achieve this goal different systems attempt to utilize different resources of system and network security information and different methods of their analysis. Host IDS relay mainly on multitude of systems and applications logs, Network IDS try to actively collect necessary information from the contents of monitored network packets.

Collected data are processed against known systems and network behavior during intruders attack (attack signatures). Obtained results present some estimation of security status of protected network, with possibility of false positive and false negative errors.

The paper presents available information about the accuracy, efficiency and limitations of IDS systems, related to placement of IDS systems on the protected network, availability of necessary attack signatures and communication process status information, and amount of generated low-level event information.