

IDS/IPS: Systemy wykrywania i zapobiegania włamaniom do sieci komputerowych

Marian Wrzesień, Łukasz Olejnik, Piotr Ryszawa

Przemysłowy Instytut Automatyki i Pomiarów PIAP

Streszczenie: Zostały zaprezentowane systemy: IDS (ang. *Intrusion Detection System*) i IPS (*Intrusion Prevention System*). Systemy te są wykorzystywane do wykrywania odpowiednio włamań (IDS) i zapobiegania włamaniom (IPS). Technologie te są wdrażane w routerze Cisco 3845 pracującym na styku sieci LAN i WAN w sieci komputerowej PIAP-LAN – jako element oprogramowania routera. Korzystanie z sygnatur firmy Cisco wymaga posiadania aktualnego wsparcia dla stosowanego routera. Omówiono architekturę systemów IDS oraz IPS. Architektura ta oparta jest na rozwiązaniach: hostowe HIDS (tzw. host-based IDS) oraz rozwiązanie sieciowe NIDS (Network IDS). W zakresie topologii, systemy IPS dzielą się na rozwiązania sieciowe, a w tym bazujące na sondzie pasywnej podłączonej do portu monitorującego przełącznika, analizującej wszystkie pakiety w danym segmencie sieci oraz inline – z sondą umieszczoną pomiędzy dwoma segmentami sieci, pozbawioną adresów IP i działającą w trybie przezroczystego mostu przekazującego wszystkie pakiety w sieci. Obie stosowane topologie sieciowe mogą współpracować w środowiskach określonych architekturą HIDS oraz NIDS. Zostały omówiono cechy i parametry systemów IDS i IPS. Przedstawiono również metody i narzędzia przeznaczone do konfiguracji obu systemów ochrony przed włamaniami.

Słowa kluczowe: włamanie, ochrona, IDS, IPS, sieć komputerowa, bezpieczeństwo

1. Wprowadzenie

IDS, IPS (ang. *Intrusion Detection System*, *Intrusion Prevention System*), systemy wykrywania i zapobiegania włamaniom, to urządzenia sieciowe zwiększające bezpieczeństwo sieci komputerowych przez wykrywanie (IDS) lub wykrywanie i blokowanie ataków (IPS) w czasie rzeczywistym. W hierarchii zabezpieczania infrastruktury teleinformatycznej powinny one być lokowane jako kolejne po firewallu – systemy ochrony. IDS służy do monitorowania zagrożeń i incydentów naruszenia bezpieczeństwa oraz do powiadamiania o nich. Z kolei IPS podejmuje dodatkowo działania mające na celu powstrzymanie ataku, minimalizację jego skutków lub aktywną odpowiedź na naruszenie bezpieczeństwa. Tak więc, rozwiązania te umożliwiają zwiększenie poziomu bezpieczeństwa sieci komputerowych poprzez wzmocnienie kontroli komunikacji pomiędzy sieciami o różnym stopniu zaufania. Skuteczny system ochrony bazujący na IDS/IPS powinien uwzględniać specyfikę działalności firmy, szacowane źródła

zagrożeń sieci komputerowej i na tej podstawie przyjąć poziom rozwiązania – wynikający z przeprowadzonej analizy ryzyka. System IPS wykorzystuje wielopoziomowe mechanizmy analizy i zabezpieczeń, takie jak analizy protokołów, wykrywanie anomalii w ruchu sieciowym czy korelacje zdarzeń. Pozwala również na tworzenie własnych reguł opartych na porównaniu wzorców ataków.

System IDS zazwyczaj działa na zasadzie sniffera (program komputerowy, którego zadaniem jest przechwytywanie i analizowanie danych przepływających w sieci) wykrywającego próbę naruszenia bezpieczeństwa i informującego firewall o lokalizacji (adresie IP) przeprowadzającego atak. W konsekwencji firewall blokuje pakiety pochodzące z podanego adresu, które biorą udział w ataku.

2. Bezpieczeństwo

Kamieniami milowymi w obszarze bezpieczeństwa transmisji danych są: zbudowanie sieci komputerowych, wprowadzenie do sieci struktury internetowej, rozpowszechnienie systemów antywirusowych i antyspamowych, wdrożenie technologii firewall, a wreszcie wyrafinowane metody zabezpieczania transmisji danych pomiędzy sieciami, takie jak IDS oraz IPS.

Bezpieczeństwo infrastruktury teleinformatycznej można wyrazić formułą:

$$\text{Bezpieczeństwo} = \text{widoczność} + \text{kontrola}$$

W celu zapewnienia właściwego poziomu bezpieczeństwa infrastrukturze teleinformatycznej należy ją monitorować i kontrolować jednocześnie. Zapewnia to połączenie technologii IDS z technologią IPS. Technologia IDS zapewnia widoczność, na którą składa się pasywne monitorowanie sieci, przechowywanie zdarzeń oraz raportowanie. Widoczność jest kluczowa w procesie podejmowania decyzji przez Administratora sieci w zakresie bezpieczeństwa. Umożliwia ona tworzenie polityk bezpieczeństwa w oparciu o wymierne, realne dane.

Drugim elementem powyższej formuły jest kontrola. Technologią odpowiedzialną za kontrolę jest IPS, który zapewnia aktywne monitorowanie sieci i pozwala na egzekwowanie ustanowionych przez Administratora sieci polityk bezpieczeństwa w sieci teleinformatycznej.

3. IDS

Systemy wykrywania IDS służą podniesieniu bezpieczeństwa sieci zarówno od wewnątrz jak i od zewnątrz. Atutem systemów IDS jest to, że mogą posłużyć do analizy ruchu sieciowego.

Techniki detekcji stosowane w IDS [1]:

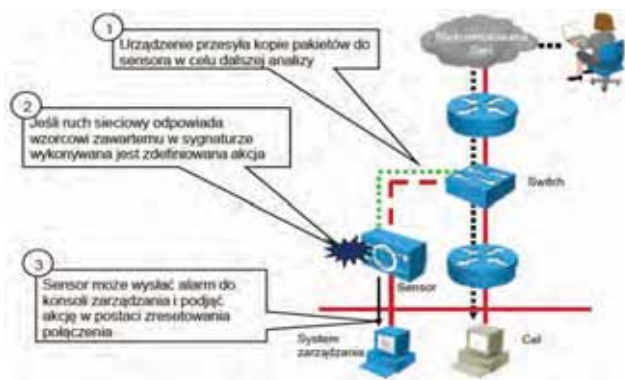
- wykrywanie anomalii (anomaly detection),
- wykrywanie sygnatur (signature detection),
- monitorowanie celu (target monitoring),
- niewidzialne sondowanie (invisible probing),
- detekcja oparta na garnku miodu (honey pot).

Wykrywanie anomalii polega na wykrywaniu niestandardowych wzorców zachowań. Przechowywaniu podlega zbiór standardowych przypadków użycia systemu. Wszystkie zdarzenia odbiegające od tego wzorca są klasyfikowane jako potencjalnie niebezpieczne.

Wykrywanie sygnatur polega na przechowywaniu zbioru wzorców zachowań niepożądanych, w celu wykrycia zbliżonych do nich aktywności intruzów. Te wzorce są sygnaturami.

Monitorowanie celu polega na tym, że system sprawdza czy określone pliki nie zostały zmodyfikowane w sposób nieuprawniony. Porównywanie plików odbywa się za pomocą haszowania (funkcji skrótu) i porównywania haszów. Niewidzialne sondowanie polega na wykrywaniu intruzów, którzy atakują system długookresowo. W celu wykrycia podejrzanych zachowań, technika ta łączy ze sobą wykrywanie anomalii z wykrywaniem sygnatur.

Detekcja oparta na garnku miodu wykorzystuje podstawiony serwer. Umożliwia to odizolowanie ataków od rzeczywistych systemów. Umożliwia analizowanie rodzajów przychodzących ataków i szkodliwych wzorców ruchu. Metoda ta jest przydatna w celu określenia powszechnych ataków na zasoby sieciowe i wprowadzenie na tej podstawie poprawek niezbędnych dla ochrony tych zasobów.



Rys. 1. Architektura IDS

Fig. 1. IDS architecture

Rodzaje alarmów generowanych przez system IDS:

- Falszywe alarmy:
 - False positive: normalny, zwyczajny ruch sieciowy powoduje uruchomienie akcji związanej z sygnaturą,
 - False negative: niedozwolony ruch sieciowy nie uruchamia akcji powiązanej z sygnaturą, prowadzony atak nie zostaje wykryty,
- Prawdziwe alarmy:
 - True positive: niedozwolony ruch sieciowy uruchamia akcję powiązaną z sygnaturą, prowadzony atak zostaje wykryty,

- True negative: normalny, zwyczajny ruch sieciowy nie powoduje uruchomienia akcji związanej z sygnaturą, normalny ruch nie powoduje alarmu.

System IDS może występować w dwóch wariantach:

- oparty na hoście Host-Based IDS (HIDS),
- oparty na sieci Network-Based IDS (NIDS).

3.1. Host-Based IDS (HIDS)

Systemy HIDS zbierają i analizują dane na komputerach (hostach), na których jest zaimplementowany ten system. Zebrane dane można poddawać analizie lokalnie lub na komputerze dedykowanym do tego celu.

Zastosowaniem HIDS może być implementacja, której zadaniem jest zbieranie logów systemowych i aplikacyjnych z innych komputerów. W przypadku dużych sieci rozwiązanie to jest nieefektywne i niewygodne. Jednym z sugerowanych systemów zbierającym logi jest IBM Tivoli [1].

3.2. Network-Based IDS (NIDS)

Działanie NIDS polega na weryfikacji pakietów przesyłanych w sieci komputerowej. Pakiety są poddawane analizie, a następnie klasyfikowane w aspekcie prawidłowości. Sieć komputerowa wyposażona w NIDS charakteryzuje się zwiększoną odpornością na ataki z zewnątrz. Systemy takie bardzo dobrze radzą sobie z nieautoryzowanym dostępem. Ograniczeniem stosowania systemów NIDS są sieci, w których transmisja odbywa się w sposób szyfrowany lub transmisja jest bardzo szybka (powyżej 80 Mbps). Wtedy analiza przesyłanych treści staje się niepełna. Przykładem takiego rozwiązania IDS jest urządzenie Cisco IDS-4215. Rozwiązaniem eliminującym to ograniczenie jest zastosowanie systemu hybrydowego złożonego z HIDS i NIDS. Przykładem takiego rozwiązania jest rozproszona sieć agentów (oprogramowanie klienckie), w której agenci wymieniają się informacjami między sobą.

4. IPS

Cechą systemu IPS jest to, że poza tym, że wykrywa ataki na systemy teleinformatyczne (tak, jak w przypadku systemu IDS), uniemożliwia ich przeprowadzenie. Od strony technicznej IPS w dużym uproszczeniu jest połączeniem IDS z systemem Firewall.

W zakresie topologii, systemy IPS dzielą się na rozwiązania sieciowe, a w tym bazujące na sondzie pasywnej podłączonej do portu monitorującego przełącznika analizującej wszystkie pakiety w danym segmencie sieci oraz inline – z sondą umieszczoną pomiędzy dwoma segmentami sieci, pozbawioną adresów IP i działającą w trybie przezroczystego mostu przekazującego wszystkie pakiety w sieci.

Sensory IPS porównują ruch sieciowy z sygnaturami. Sygnatury mają trzy charakterystyczne cechy: typ sygnatury, trigger, podejmowana akcja.

- Systemy IPS mogą występować w dwóch wariantach:
 - Network-Based IPS (NIPS),
 - Host-Based IPS (HIPS).

4.1. Host-Based IPS

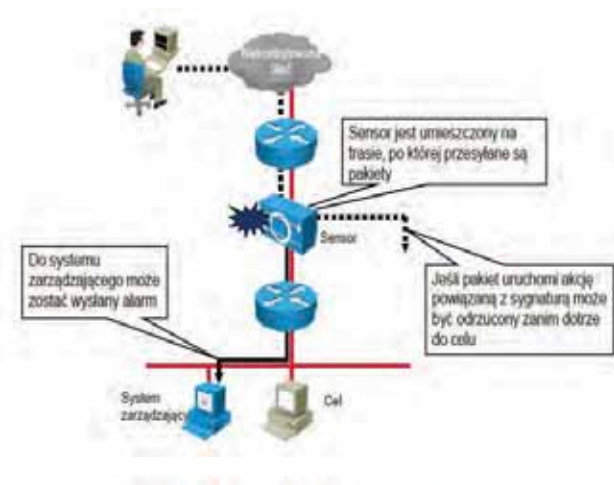
HIPS jest programowym agentem instalowanym na systemie operacyjnym podlegającym ochronie. Zapewnia on wykrycie i ochronę przed atakami. Nie wymaga dedykowanego sprzętu.

Cechy HIPS:

- dedykowany systemowi, na którym jest zainstalowany,
- rejestruje informacje o przeprowadzonych przez intruza atakach,
- szyfrowanie transmisji danych nie ogranicza działania systemu.

Ograniczenia HIPS:

- brak możliwości korelowania zdarzeń w przypadku obserwacji odosobnionych agentów,
- każdy agent wymaga licencji,
- brak oprogramowania (agent) dla niektórych platform programowych wprowadzonego przez dostawcę systemu.



Rys. 2. Topologia IPS
Fig. 2. IPS topology

4.2. Network-Based IPS

W przypadku technologii NIPS sensory są podłączone do segmentów sieci, przy czym pojedynczy sensor może monitorować kilka komputerów. Rozbudowa sieci nie wpływa na skuteczność ochrony dodanych urządzeń, które wprowadzono bez dodatkowych sensorów. Sensory te są urządzeniami sieciowymi dostosowanymi do zapobiegania włamaniom określonego typu. Cechy sieciowych IPS:

- efektywne kosztowo (pojedynczy sensor może chronić dużą sieć),
- zapewniają analizę ruchu podczas ataków w niższych warstwach modelu ISO/OSI,

- są niezależnym systemem operacyjnym,
- mają wiele możliwości wykrywania,
- są niewidoczne w sieci (brak przypisanego IP).

Ograniczenia sieciowych IPS (wydajność):

- mogą być przeciążone ruchem sieciowym,
- mogą wystąpić różnice między ruchem sieciowym postrzeganym przez IPS i odbieranym przez cel,
- nie działają w sieci szyfrowanej.

4.3. Typy sygnatur

Typy sygnatur to:

- Atomic,
- Composite.

Sygnatury typu Atomic mają proste formy. Zawierają opis pojedynczego pakietu, aktywności oraz zdarzenia. Nie wymagają przechowywania informacji o stanie („horyzont zdarzeń”) w systemie IPS. Sygnatury te są łatwe do zidentyfikowania.

Sygnatury typu Composite często nazywane są sygnaturami stanowymi. Określają sekwencję działań na wielu hostach. Sygnatura tego typu musi zawierać informacje o jej stanie.

5. Konfiguracja IPS w routerze CISCO

Konfigurację IPS rozpoczyna się od utworzenia katalogu sygnatur (w PIAP: ips) - poprzedzonego pobraniem dedykowanych sygnatur z witryny CISCO (w formie paczki), w celu umieszczenia ich w utworzonym katalogu.

```

R1# mkdir ips
Create directory filename [ips]?
Created dir flash:ips
R1#
R1# dir flash:
Directory of flash:/
 5 -rw- 51054964 Jan 10 2009 15:46:14 -08:00
c3800nm-advipservicesk9-mz.124-10.71.bin
 6 drwx- 0 Jan 15 2009 11:36:13 -08:00 ips
64016384 bytes total (12693504 bytes free)
R1#
    
```

Rys. 3. Proces tworzenie katalogu ips w routerze
Fig. 3. Process of creating the ips directory on the router

Z pobranej i rozpakowanej paczki należy odczytać klucz kryptograficzny.

```

realm-cisco.pub signature.txt - Notepad
File Edit Format View Help
crypto key pubkey-chain rsa
named-key realm-cisco pub signature
key-string
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02020101
00C19E93 A8AF124A D6C07A24 5097A975 208BE3A2 06FB113F 6F12C85E 4E441F16
17E630D5 C02AC252 912BE27E 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EF8624 7E0764BF 3E53053E
5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
50437722 FFBEB85B 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
2F56D826 8918EF3C 80CA4F4D 87BFC3B BFF668E9 689782A5 CF31CB6E B4B094D3
F3020301 0001
quit
exit
exit
    
```

Rys. 4. Zawartość klucza kryptograficznego
Fig. 4. Content of a cryptographic key

Następnie klucz ten należy skopiować i wkleić w trybie globalnej konfiguracji do routera.

```
R1# conf t
R1(config)#
```

Rys. 5. Przejście do trybu globalnej konfiguracji

Fig. 5. Go to the global configuration mode

W kolejnych krokach (rys. 6 – rys. 10) należy uruchomić funkcjonalność IPS w routerze.

```
R1(config)# ip ips name iosips
R1(config)# ip ips name ips list ?
<1-199> Numbered access list
WORD Named access list
R1(config)#
R1(config)# ip ips config location flash:ips
R1(config)#

R1(config)# ip http server
R1(config)# ip ips notify sdee
R1(config)# ip ips notify log
R1(config)#

R1(config)# ip ips signature-category
R1(config-ips-category)# category all
R1(config-ips-category-action)# retired true
R1(config-ips-category-action)# exit
R1(config-ips-category)#
R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# retired false
R1(config-ips-category-action)# exit
R1(config-ips-category)# exit
Do you want to accept these changes? [confirm] y
R1(config)#

R1(config)# interface GigabitEthernet 0/1
R1(config-if)# ip ips iosips in
R1(config-if)# exit
R1(config)#exit

R1(config)# interface GigabitEthernet 0/1
R1(config-if)# ip ips iosips in
R1(config-if)# ip ips iosips out
R1(config-if)# exit
R1(config)# exit
```

Rys. 6. Proces uruchamiania IPS w routerze

Fig. 6. Process of IPS running on the router

W następnym kroku należy wgrać do routera pobrane sygnatury. W tym celu można wykorzystać serwer FTP, na którym wcześniej zostały umieszczone sygnatury.

```
R1# copy ftp://r1as:raser@10.1.1.1/208-8776-CLI.pkg idrnsf
Loading 208-8776-CLI.pkg (.....)
[OK - 740871/4094 bytes]
*Jan 15 16:44:47 PST: NIPS-0-ENGINE_BUILD_STARTED: 16:44:47 PST Jan 15 2005
*Jan 15 16:44:47 PST: NIPS-0-ENGINE_BUILDING: multi-string - 5 signatures - 1 of 13 engines
*Jan 15 16:44:47 PST: NIPS-0-ENGINE_READY: multi-string - build time 4 ms - packets for this
engine will be scanned
*Jan 15 16:44:47 PST: NIPS-0-ENGINE_BUILDING: service-http - 612 signatures - 2 of 13 engines
*Jan 15 16:44:48 PST: NIPS-0-ENGINE_READY: service-http - build time 4024 ms - packets for this
engine will be scanned

~Output~

*Jan 15 16:45:10 PST: NIPS-0-ENGINE_BUILDING: service-sm-advanced - 18 signatures - 11 of 13
engines
*Jan 15 16:45:10 PST: NIPS-0-ENGINE_READY: service-sm-advanced - build time 18 ms - packets
for this engine will be scanned
*Jan 15 16:45:10 PST: NIPS-0-ENGINE_BUILDING: service-icmp - 15 signatures - 14 of 13 engines
*Jan 15 16:45:10 PST: NIPS-0-ENGINE_READY: service-icmp - build time 11 ms - packets for this
engine will be scanned
*Jan 15 16:45:10 PST: NIPS-0-ALL_ENGINES_BUILDS_COMPLETE: elapsed time 1647 ms
```

Rys. 7. Kopiowanie sygnatur do routera

Fig. 7. Copy signatures to router

W celu konfigurowania sygnatur (uruchamiania) i przeglądania zdarzeń, alarmów można wykorzystać bezpłatne oprogramowanie CISCO SDM lub Cisco Configuration Professional.

6. Podsumowanie

Sieciowe systemy wykrywania i zapobiegania włamaniom NIDS/NIIPS mają przewagę nad innymi systemami wykrywania i zapobiegania włamaniom, ponieważ nie obciążają nadzorowanych hostów. Podczas implementacji należy zwrócić szczególną uwagę na sposób konfiguracji wdrażanego systemu NIDS/NIPS, gdyż źle skonfigurowany będzie generował setki tysięcy fałszywych alarmów, co istotnie utrudni analizę zdarzeń. O przydatności NIDS/NIPS świadczy niska liczba alarmów fałszywych.

Najnowsze systemy NIDS umożliwiają także rozpoznawanie nadzorowanego systemu operacyjnego na podstawie charakterystycznych cech stosu TCP/IP danego systemu. Funkcjonalność ta umożliwia wprowadzanie hierarchii ważności poszczególnym alarmom w zależności od typu tego systemu.

Wdrożenie systemu NIDS/NIPS powinno być poprzedzone szczegółową analizą nadzorowanej sieci teleinformatycznej zarówno jej struktury jak i charakteru danych w niej przesyłanych. To powinno posłużyć właściwemu ulokowaniu elementu systemu NIPS, decydującemu o stabilności działania sieci.

Wdrożony system NIDS/NIPS wymaga ciągłego dostosowywania go do zmieniających się zagrożeń jak i charakteru ruchu sieciowego. W procesie tym bardzo ważnym aspektem jest dokumentowanie wprowadzanych sygnatur i poleceń w celu zachowania przejrzystości, czytelności i odtwarzalności – na wypadek ewentualnej przebudowy systemu.

Dobrze skonfigurowany NIDS to najlepsze źródło informacji na temat bezpieczeństwa sieci teleinformatycznej.

Bibliografia

1. Maciej Szmit, Marek Gusta, Mariusz Tomaszewski, *101 zabezpieczeń przed atakami w sieci komputerowej*, Helion 2005.
2. Jake Babbin, Graham Clark, Angela Orebaugh, Becky Pinkard, Michael Rash, *IPS Zapobieganie i aktywne przeciwdziałanie intruzom*, PWN-Mikom 2005.
3. Karol Krysiak, *Sieci komputerowe. Kompendium. Wydanie II*, Helion 2005.
4. Andrew S. Tanenbaum, David J. Wetherall, *Sieci komputerowe*, Wydanie 5, Helion 2012. ■

IDS/IPS Systems to detect and prevent intrusions into computer networks

Abstract: There were presented systems: IDS (called Intrusion Detection System) and IPS (Intrusion Prevention System). These systems are used for intrusion detection (IDS) and intrusion prevention (IPS), respectively. These technologies are implemented in the Cisco 3845 router working at the interface between the LAN and WAN network PIAP-LAN – as part of a software router. Using Cisco signatures requires a current support for the used router. Discusses the architecture of IDS and IPS systems. terms of topology, IPS systems can be divided into network solutions, including probe-based passive monitoring port connected to the switch, analyzing all packets in a network segment and inline – with the probe placed between two network segments, with no IP address and operating in transparent bridge mode transmitting all packets on the network. Both network topologies can be used to work in specific environments HIDS and NIDS architecture. Have discussed the characteristics and parameters of IDS and IPS systems. It also presents methods and tools for configuring both intrusion prevention systems.

Keywords: hacking, security, IDS, IPS, network, security

dr inż. Marian Wrzesień

Główny Informatyk Instytutu, Administrator Sieci Informatycznej PIAP-LAN, Adiunkt.

e-mail: mwrzesien@piap.pl



mgr inż. Łukasz Olejnik

Inżynier sprzętowy Sieci Informatycznej PIAP-LAN.

e-mail: lolejniki@piap.pl



inż. Piotr Ryszawa

Programista Sieci Informatycznej PIAP-LAN.

e-mail: pryszawa@piap.pl

