Studia i Materiały Informatyki Stosowanej, Tom 4, Nr 7, 2012
str. 16-21

IDS/IPS: SYSTEMY WYKRYWANIA I ZAPOBIEGANIA WŁAMANIOM DO SIECI KOMPUTEROWYCH

Marian Wrzesień, Łukasz Olejnik, Piotr Ryszawa

Przemysłowy Instytut Automatyki i Pomiarów PIAP w Warszawie
Al. Jerozolimskie 202,02-486 Warszawa

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 klucze: *włamania, ochrona, IDS, IPS, sieć komputerowa, bezpieczeństwo*

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. This architecture is based on solutions: hosted HIDS (known as host-based IDS) and network solution NIDS (Network IDS). In 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*

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 o porównanie 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:
Bezpieczeństwo = widoczność + 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 (anomalny detection)
- wykrywanie sygnatur (signature detection)
- monitorowanie celu (target monitoring)
- niewidzialne sondowanie (invisible probing)
- detekcja oparta o garnek 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 o garnek 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.
Rodzaje alarmów generowanych przez system IDS:

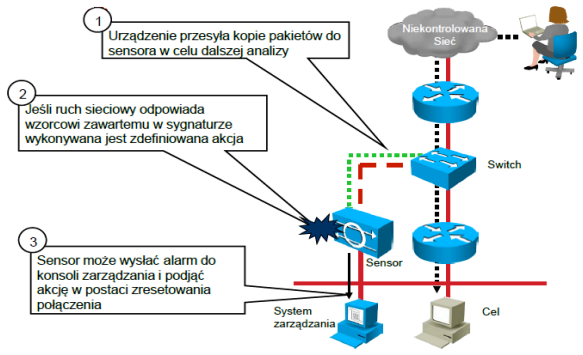
- Fałszywe alarmy

- False positive: normalny, zwyczajny ruch siecio-wy powoduje uruchomienie akcji związanej z sygnaturą.
- False negative: niedozwolony ruch sieciowy nie uruchamia akcji powiązanej z sygnaturą, prowa-dzony 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)



Rysuek. 1 Architektura IDS

3.1. Host-Based IDS (HIDS)

Systemy HIDS zbierają i analizują dane na komputerze (hoście), na którym 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].
W niniejszym artykule przedstawiono algorytm klasteryzacji metodą k-średnich, a także jego implementację w języku C++. Nie zamieszczono kodu źródłowego niektórych funkcji, ale są one stosunkowo proste do odtworzenia, dlatego nie istnieje po prostu taka potrzeba. Dla zainteresowanych autor udostępni pełny kod źródłowy drogą mailową.

Klasteryzacja metodą k-średnich to stosunkowo prosty algorytm służący do klasyfikacji danych. Jak widać jest on również łatwy do implementacji.

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 przeprowadzanie.
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, triger, podejmowana akcja
Systemy IPS mogą występować w dwóch wariantach:

- Network-Based IPS (NIPS)
- Host-Based IPS (HIPS)

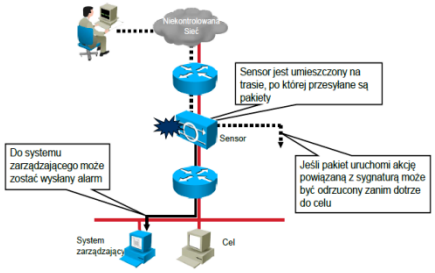
4.1. Host-Based IPS

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 przy-padku obserwacji odosobnionych agentów,
- każdy agent wymaga licencji,
- brak oprogramowania (agent) dla niektórych platform programowych wprowadzony przez dostawcę systemu.



Rysuek. 2 Topologia IPS

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 siecio-wym postrzeganym przez IPS i odbieranym przez cel,
- nie działają w sieci szyfrowanej.

4.3. Typy sygnatur

Typy sygnatur to:

- Atomic
- Composite

Sygnatury typu Atomic posiadają 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 informację o jej stanie.

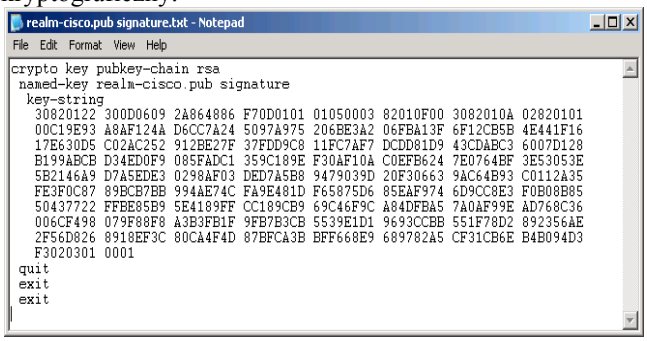
5. KONFIGURACJA IPS W ROUTERZE CISCO

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-   51054864 Jan 10 2009 15:46:14 -08:00
                     c2800nm-advipservicesk9-mz.124-20.T1.bin
   6 drw-          0 Jan 15 2009 11:36:36 -08:00 ips
64016384 bytes total (12693504 bytes free)
R1#
```

Rysuek. 3 Proces tworzenie katalogu ips w routerze

Z pobranej i rozpakowanej paczki należy odczytać klucz kryptograficzny.



Rysuek. 4 Zawartość klucza kryptograficznego

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

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

Rysuek. 5 Przejście do trybu globalnej konfiguracji

W kolejnym 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
```

Rysuek. 6 Proces uruchamiania IPS w routerze

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://cisco:cisco@10.1.1.1/IOS-S376-CLI.pkg idconf
Loading IOS-S310-CLI.pkg !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 7608873/4096 bytes]
*Jan 15 16:44:47 PST: %IPS-6-ENGINE_BUILDS_STARTED: 16:44:47 PST Jan 15 2008
*Jan 15 16:44:47 PST: %IPS-6-ENGINE_BUILDING: multi-string - 8 signatures - 1 of 13 engines
*Jan 15 16:44:47 PST: %IPS-6-ENGINE_READY: multi-string - build time 4 ms - packets for this
                      engine will be scanned
*Jan 15 16:44:47 PST: %IPS-6-ENGINE_BUILDING: service-http - 622 signatures - 2 of 13 engines
*Jan 15 16:44:53 PST: %IPS-6-ENGINE_READY: service-http - build time 6024 ms - packets for this
                       engine will be scanned

<Output omitted>

*Jan 15 16:45:18 PST: %IPS-6-ENGINE_BUILDING: service-smb-advanced - 35 signatures - 12 of 13
engines
*Jan 15 16:45:18 PST: %IPS-6-ENGINE_READY: service-smb-advanced - build time 16 ms - packets
                       for this engine will be scanned
*Jan 15 16:45:18 PST: %IPS-6-ENGINE_BUILDING: service-msrpc - 25 signatures - 13 of 13 engines
*Jan 15 16:45:18 PST: %IPS-6-ENGINE_READY: service-msrpc - build time 32 ms - packets for this
                      engine will be scanned
*Jan 15 16:45:18 PST: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 31628 ms
```

Rysuek. 7 Kopiowanie sygnatur do routera

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

Literatura

1. Maciej Szmit, Marek Gusta, Mariusz Tomaszewski 101 zabezpieczeń przed atakami w sieci komputero-wej, 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 V, Helion 2012.