Systemy wykrywania intruzów (IDS/IPS)

Jakub Skupień
Daniel Piekarczyk
Kacper Nuckowski
Adam Paździerz
Wydział Matematyki Stosowanej
Poltechnika Śląska

3 lutego 2023

Politechnika Śląska

Spis treści

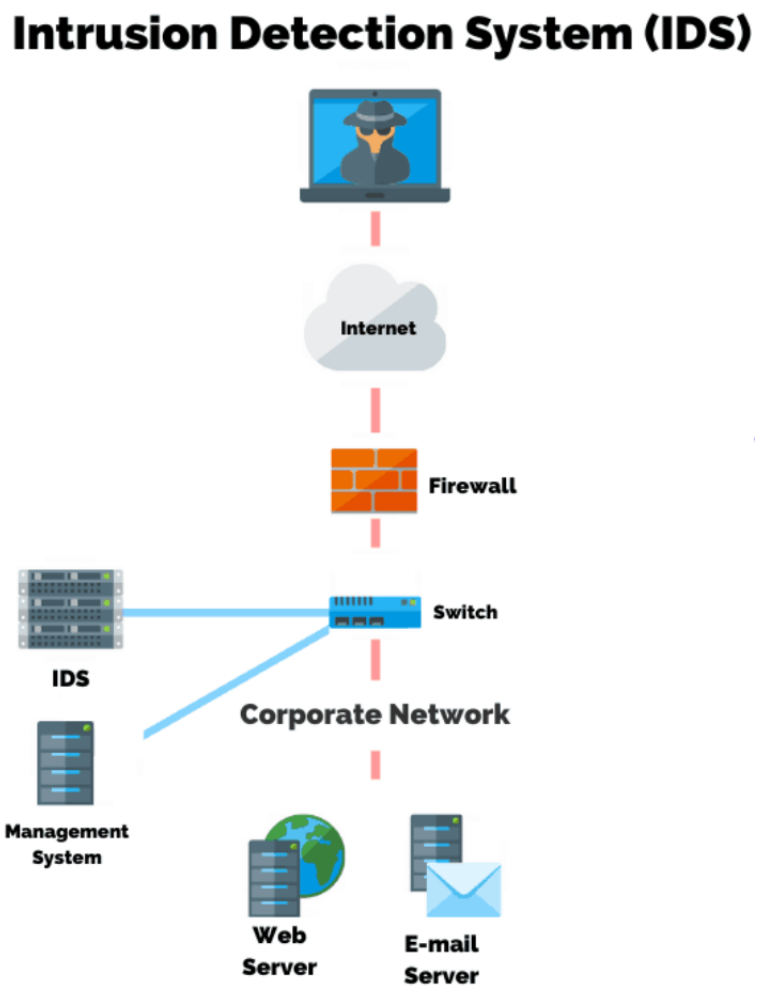
1 Wstęp

1.1 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:

- 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.



Rodzaje alarmów generowanych przez system IDS:

- Fałszywe 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.

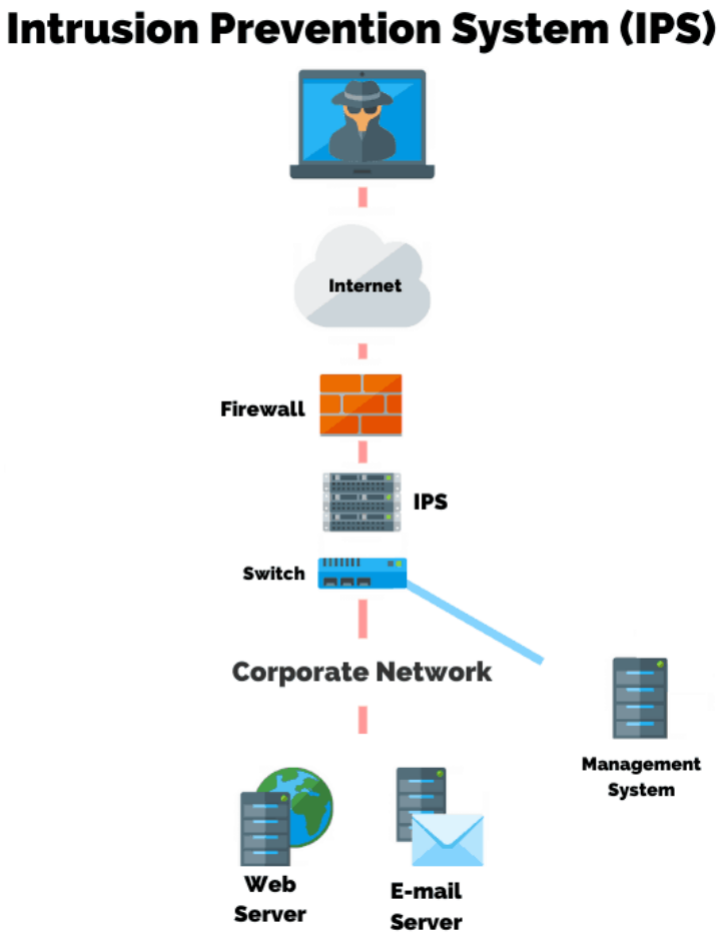
System IDS może występować w dwóch wariantach:

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

1.2 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) - 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,
- Host-Based IPS (HIPS) - HIPS jest programowym agentem instalowanym na systemie operacyjnym podlegającym ochronie. Zapewnia on wykrycie i ochronę przed atakami. Nie wymaga dedykowanego sprzętu.

2 Prezentacja wybranych rozwiązań

2.1 Technologia

Lepszym wyborem dla początkujacego administratora sieci pod względem bezpieczeństwa sieci komputerowych jest technologia IPS, ponieważ oprócz powiadomień o zagrożeniach i incydentach, podejmuje jeszcze działania mające na celu powstrzymanie ataku, minimalizację jego skutków lub aktywną odpowiedz na naruszenie bezpieczeństwa. Wybraliśmy ten produkt, ponieważ po uruchomieniu i skonfigurowaniu nie wymaga większej pracy. Natomiast dla zaawansowanych użytkowników, polecamy IDS (jest on używany w SOC'ach), dlatego ze użytkownik dostaje tylko możliwość monitorowania zagrożeń. Pozwala to na większą swobodę działania. Powiadomienia o atakach nie zawsze oznaczają zagrożenia (Alert mógł się wywołać przez naszego pracownika, który nie miał na celu atakowania naszej sieci) i potrzebują dodatkowego sprawdzenia przez człowieka.

2.2 System

Wybraliśmy system NIDS (Network-Based IDS), sieć komputerowa wyposażona w system NIDS charakteryzuje się zwięszkoną odpornością na ataki z zewnątrz w przeciwieństwie do HIDS (Host-Based IDS). Wykorzystuje do tego monitorowanie ruchu sieciowego. Cechy:

- sprawdzania pakietów, dopasowanie zawartości pakietu do listy reguł typu blacklist,
- analiza sesji - łączenie kilku pakietów w całość i analiza ich zawartości w kontekście sesji,
- analiza heurystyczna ruchu sieciowego - np. określanie kiedy ma miejsce skanowanie portów - przekroczona ilość dozwolonych połączeń z jednego adresu do różnych portów - konkretne wartości progowe są ustalane na podstawie statystyk ruchu,

- próby wykrywania anomalii w ruchu sieciowym - trudne, bo niełatwo określić kiedy ma miejsce nietypowe natężenie ruchu,
- skanowanie logów zawierających zapis ruchu sieciowego i próby ustalenia czy nie miał miejsca atak na serwery,
- współpraca z innymi systemami bezpieczeństwa, np. wymiana informacji z firewallami, aktualizacja listy zabronionych IP, listy reguł itp.,
- informowanie administratora o potencjalnych zagrożeniach.

2.3 Wady i zalety

Zalety:

- Można je dostroić do określonej zawartości w pakietach sieciowych,
- mogą patrzeć na dane w kontekście protokołu,
- mogą kwalifikować i określać ilościowo ataki,
- ułatwiają nadążanie za regulacjami,
- mogą zwiększyć wydajność.

Wady:

- Nie zapobiegną incydentom,
- do administrowania incydentami potrzebny jest doświadczony inżynier,
- nie przetwarzają zaszyfrowanych pakietów,
- ip pakiet może być ciągle sfałszowany,
- są podatne na ataki oparte na protokołach,
- biblioteka sygnatur musi być stale aktualizowana, aby wykrywać najnowsze zagrożenia.

3 Podsumowanie

Podsumowując, narzędzia do wykrywania intruzów stają się coraz bardziej niezbędne do prawidłowego działania systemów bezpieczeństwa. Narzędzia te używają różnych technik i oparte są na różnych architekturach. Dobra implementacja takiego systemu powinna łączyć różne techniki i podejścia, by dać jak najwięcej informacji o stanie systemu. Każdy wariant tej technologii ma swoje wady i zalety. Dlatego, ważną rzeczą jest właściwe umiejscowienie odpowiednich systemów ochrony przed intruzami.

Literatura

[1] IDS/IPS: Systemy wykrywania i zapobiegania włamaniom do sieci komputerowych. Marian Wrzesień, Łukasz Olejnik, Piotr Ryszawa.

[2] https://help.eset.com/efsw/7.3/pl-PL/idh_hips_main.html

[3] https://kapitanhack.pl/2019/06/26/akronimy/co-to-jest-hips/

[4] https://zabezpieczenia.it/nips-hillstone/