Systemy wykrywania intruzów

Piotr Dorosz
Pyton Software
piotr.dorosz@pyton.pl

dr inż. **Przemysław Kazienko**
Zakład Systemów Informacyjnych
Wydział Informatyki i Zarządzania
Politechnika Wrocławska
kazienko@pwr.wroc.pl

Wykrywanie intruzów

- Problemy terminologiczne z ***Intrusion Detection System***
- Nie chodzi o wykrywanie intruzów (osób), lecz ich działań (akcji) - włamań czy naruszeń bezpieczeństwa: *wykrywanie intruzowania, wykrywanie włamań*

Wykrywanie intruzów

Wykrywanie intruzów polega na identyfikacji osobników, którzy korzystają z systemu komputerowego bez odpowiedniego pozwolenia (*authorization*) (wykrywanie krakerów) lub tych, którzy posiadając pewne prawa dostępu, nadużywają je — włamania wewnętrzne (*insider threat, insider's attacks*) [Muk94].

Wykrywanie włamań jest to proces identyfikowania i reagowania na szkodliwą działalność, skierowaną przeciw zasobom informatycznym i sieciowym [Amo99].

Wykrywanie włamań to identyfikacja zbioru akcji, które naruszają integralność, poufność lub dostępność zasobów [Spa00].

Wykrywanie intruzów - pytania

- Co to jest włamanie? Czy jest to nieupoważniony dostęp do zasobów przez kogoś z zewnątrz, czy także z wewnątrz?
- Czy pasywne ataki (np. skanowanie portów, nasłuchiwanie) można kwalifikować jako włamanie?
- Czy nieudana próba włamania to także włamanie?
- Czy systemy wykrywania intruzów tylko wykrywają, czy także reagują na włamania?
- Kim jest intruz?

Czym **nie** są systemy IDS

- Systemami badającymi przepustowość sieci (monitory ruchu sieciowego)
- Narzędziami do wykrywania luk w zabezpieczeniach systemów operacyjnych i usług sieciowych,
- Systemami wykrywającymi wszelkiego rodzaju złośliwe programy (wirusy, konie trojańskie, robaki - *worm*, bakterie, bomby logiczne); mimo, że tego typu systemy posiadają wiele cech systemów IDS — często wykrywają naruszenia bezpieczeństwa.
- Zaporami ogniowymi
- Systemami zabezpieczeń, także systemami kryptograficznymi, np. VPN, SSL, Kerberos, Radius

Rodzaje włamań - definicje

Włamanie – ciąg współzależnych działań intruza, które powodują wystąpienie zagrożeń naruszenia bezpieczeństwa zasobów przez nieautoryzowany dostęp do danej domeny komputerowej lub sieciowej.

Naruszenie – naruszenie polityki bezpieczeństwa systemu może być utożsamiane z udanym włamaniem do systemu.

Atak – nieudana próba wtargnięcia do systemu (nie prowadząca do naruszeń).

Modelowanie włamań – czasowe modelowanie działań składających się na włamanie. Intruz rozpoczyna włamanie działaniem początkowym, po którym następują działania pomocnicze (lub mylące – tzw. uniki) oraz będące dalszymi elementami ciągu. W szczególności w czasie samego włamania w grę wchodzić mogą działania podejmowane przez każdego np. menadżera chronionego zasobu.

Klasyfikacja włamań wg Neumanna i Parkera (1/3)

- NP1 - Zewnętrzne nadużycie
  - Nietechniczne, fizyczne włamania – np. włamanie do laboratorium
- NP2 - Nadużycie sprzętu
  - Problem naruszenia bezpieczeństwa sprzętu – fizyczne symptomy nadużycia sprzętu, zauważalne świadectwa lub doniesienie informatora
- NP3 - Podszywanie się
  - Zwodzenie i zmiany tożsamości – np. liczne jednoczesne występowanie pewnego wzorca (np. wiele logowań na jedno konto), zachowanie nietypowe do zapamiętanego profilu

Klasyfikacja włamań wg Neumanna i Parkera (2/3)

- NP4 - Późniejsze nadużycie
  - Przygotowanie włamań przez modyfikacje, błędy programów oraz wszelkie działania intruzów, w ramach których do systemu wprowadzona zostaje modyfikacja lub błąd. (np. konie trojańskie w programach).
- NP5 - Ominięcie kontroli (rozsz.)
  - Wymknięcie się autoryzowanej ochronie, kontroli np. łamanie hasła.
- NP6 - Aktywne nadużycie zasobu (rozsz.)
  - Nieautoryzowana modyfikacja zasobu – symptom: niewyjaśnione lub dziwne zachowanie, np. zmiana zawartości plików.

Klasyfikacja włamań wg Neumanna i Parkera (3/3)

- NP7 - Pasywne nadużycie sprzętu (rozsz.)
  - Nieautoryzowany odczyt zasobów – symptom: posiadanie różnego rodzaju informacji przez osobę lub grupę
- NP8 - Nadużycie przez zaniechanie
  - Zaniedbanie ochrony zasobu – incydentom należało zapobiec ale nie zostało to zrobione.
- NP9 - Pośrednie wspomaganie
  - Projektowanie narzędzi w celu nadużycia – symptom: dziwne zachowanie systemu używanego do typowych zadań, (np. podczas łamania haseł programem Crack).

Klasyfikacja włamań wg. Lindqvista i Jonssena

- Klasa obejścia umyślnej kontroli (NP 5) podzielona została na podklasy:
  - ataków na hasła
  - fałszowania programów uprzywilejowanych (np. konie trojańskie)
  - wykorzystywania słabego uwierzytelniania
- Klasa aktywnego nadużycia zasobu (NP 6) podzielona została na podklasy:
  - odpowiadającą wykorzystaniom przywilejów zapisu
  - wyczerpania zasobów
- Klasa pasywnego nadużycia zasobu (NP 7) podzielona została na:
  - przeglądanie ręczne i automatyczne z użyciem niepublicznych lub publicznych narzędzi

Podział ataków na potrzeby systemów IDS

- **Pasywne** - mające na celu uzyskanie dostępu i spenetrowanie systemu i nie naruszające zasobów
- **Aktywne -** powodujące zmiany w zasobach

Podział ataków na potrzeby systemów IDS

Ze względu na relację intruza z atakowanym:

- **Wewnętrzne** - dokonane przez pracowników własnej organizacji lub przez osoby blisko z nią związane, np. przez kontrahentów
- **Zewnętrzne** - spowodowane przez osoby z zewnątrz, zwykle są to ataki dokonywane poprzez Internet

Podział ataków na potrzeby systemów IDS

Ze względu na źródło ataku:

- Atak dokonywany z **wewnętrznych systemów** (sieci lokalnej),
- Z **Internetu**
- Poprzez **połączenia modemowe** (*remote dial-in*)

Rodzaje ataków i nadużyć wykrywane przez systemy IDS (1/5)

1. Związane z nieautoryzowanym dostępem do zasobów
   - łamanie haseł i praw dostępu
   - konie trojańskie
   - uprowadzenia; zwykle są to uprowadzenia połączeń TCP/IP często wymagające dodatkowych mechanizmów dla zablokowania działania właściwego systemu (np. poprzez powódź); ataki typu MITM (*man in the middle*),

Rodzaje ataków i nadużyć wykrywane przez systemy IDS (2/5)

1. Związane z nieautoryzowanym dostępem do zasobów (c.d.)
   - podszywania (udawanie innego użytkownika a także hosta, np. poprzez fałszowanie zapisów systemu nazw domen - DNS),
   - skanowanie portów i aktywności systemu, w tym także np. skanowanie ICMP (ping), UDP, *TCP Stealth Scanning* i inne,
   - zdalne wykrywanie rodzaju i wersji systemu operacyjnego (*OS Fingerprinting*), np. poprzez badanie reakcji na pakiety o określonych cechach, otwartych portów, standardowych odpowiedzi aplikacji typowych dla danego systemu (*banner checks*), parametrów stosu IP, itd.

Rodzaje ataków i nadużyć wykrywane przez systemy IDS (3/5)

1. Związane z nieautoryzowanym dostępem do zasobów (c.d.)
   - podsłuchiwanie (pasywny atak polegający zwykle na nasłuchiwaniu pakietów sieciowych),
   - kradzieże danych, np. zbiorów
   - nadużycia legalnego dostępu; rodzaj ataku wewnętrznego, np. podejrzany dostęp uprawnionych użytkowników o dziwnych atrybutach (w nietypowych godzinach, z dziwnych adresów),
   - nieupoważnione podłączenia do sieci;
   - wykorzystanie zasobów systemu do prywatnych celów, np. do gromadzenia pornografii
   - wykorzystanie luk systemowych do pozyskania zasobów lub zdobycia uprawnień

Rodzaje ataków i nadużyć wykrywane przez systemy IDS (4/5)

2. Nieuprawnione zmiany zasobów (następujące po uzyskaniu dostępu)
   - modyfikacje uprawnień, np. nadanie sobie praw administratora
   - modyfikacje i kasowanie danych
   - nieuprawnione transmisje i tworzenie danych (zbiorów), np. składowanie numerów kart kredytowych na komputerze rządowym
   - nieupoważniona konfiguracja (modyfikacja) systemów i usług sieciowych (serwerów)

Rodzaje ataków i nadużyć wykrywane przez systemy IDS (5/5)

3. Blokowanie usług (DoS - *Denial of Service*); system nie może obsługiwać zwykłych żądań
   - powodzie
     - ping flood (Smurf)
     - pocztowe (*mail flood*)
     - SYN flood
     - powodzie rozproszone — DDoS (*Distributed Denial of Service*)
   - wyłączenia systemów poprzez wykorzystanie ich luk, ataki na aplikacje
     - przepełnienia buforów, np. *Ping of Death*
     - zdalny shut down
4. Ataki na aplikacje - wykorzystują błędy aplikacji

Objawy włamania

- Powtarzanie się podejrzanego działania
- Omyłkowe polecenia lub odpowiedzi pojawiające się podczas wykonywania sekwencji automatycznych
- Wykorzystanie znanych słabych punktów zabezpieczeń
- Niespójności kierunkowe pakietów i sesji
- Niespodziewane atrybuty jako symptom włamania
- Trudne do wyjaśnienia zdarzenia jako symptom włamania

Objawy włamania

- Powtarzanie się podejrzanego działania
  - Wykorzystanie dużej ilości różnych usług, aplikacji
  - Alarm ogłaszany jest po przekroczeniu progów działań
    - Wartości progowe powtórzeń — rozróżniają działanie legalne od podejrzanych oraz podejrzane od niebezpiecznych. Działania mogą być klasyfikowane na podstawie wartości wielu parametrów wynikających np. z profilu użytkownika lub stanu sesji
    - Czas między powtórzeniami
  - Budowanie wzorców powtórzeń (sygnatur) – często bardzo trudne lub niemożliwe

Objawy włamania

- Omyłkowe polecenia lub odpowiedzi pojawiające się podczas wykonywania sekwencji automatycznych
  - Usługi i protokoły sieciowe – ściśle opisane, aplikacje – działają deterministycznie
  - Niedeterministyczne zachowanie
    - Proces został uszkodzony
    - Działalność intruza

Objawy włamania

- Omyłkowe polecenia lub odpowiedzi pojawiające się podczas wykonywania sekwencji automatycznych
  - Działanie człowieka da się z dużym prawdopodobieństwem stwierdzić w przypadku
    - wykrycia prób usunięcia, a następnie ponownego wpisania błędnie wprowadzonych poleceń lub odpowiedzi
    - wykrycia kilku prób postępowania zgodnie z protokołem, w których znajdują się błędy w pisowni
    - wykrycie uczenia się – popełnianie pomyłek przez ten sam obiekt (usługę, hosta), które są poprawiane i później się nie pojawiają

Objawy włamania

- Wykorzystanie znanych słabych punktów zabezpieczeń
  - Skanery integralności – działające lokalnie lub zdalnie
  - Możliwe jest wykrycie stosowania skanerów integralności
  - Możliwość wykrycia korelacji między skanowaniem a wykorzystaniem luki w zabezpieczeniach

Objawy włamania

- Rodzaje skanerów integralności
  - Systemy służące do oceny bezpieczeństwa systemu (*Vulnerability Assessment Tools*)
    - Baza luk w zabezpieczeniach, baza rad, baza exploitów.
  - Systemy służące do sprawdzania integralności plików
    - Sprawdzające zmianę plików wykonywalnych (np. wykrywanie koni trojańskich)
    - Skanery dzienników systemowych

Objawy włamania

- Niespójności kierunkowe
  - Pakiety przychodzące z Internetu posiadające adresy nadawcy z sieci lokalnej. *IP Spoofing*
  - Pakiety z sieci lokalnej (wyjściowe) kierowane do sieci zewnętrznej z zewnętrznym adresem nadawcy. Próba włamania dokonywana z sieci lokalnej
  - Pakiety z nieoczekiwanymi portami lub adresami przeznaczenia
    - Przykładem jest żądanie usługi telnet na porcie 100, w środowisku gdzie nie należy oczekiwać, że usługa ta obsługiwana jest na tym porcie lub dostępna w ogóle

Objawy włamania

- Niespodziewane atrybuty jako symptom włamania
  - Atrybuty kalendarzowe i godzinowe – logowania o dziwnych porach itp.
  - Atrybuty zasobów systemowych – wykorzystanie zasobów systemowych (procesor, pamięć, dysk, procesy systemowe, usługi, połączenia sieciowe)
  - Pakiety z niespodziewanymi ustawieniami potwierdzenia połączenia TCP
  - Atrybuty zestawu usług danego użytkownika

Objawy włamania

- Trudne do wyjaśnienia zdarzenia jako symptom włamania
  - Niewyjaśnione problemy ze sprzętem lub oprogramowaniem, np. dezaktywacja serwerów, w szczególności wyłączenie demonów systemowych, niewyjaśnione próby restartu systemu, zmiany czasu zegara systemowego
  - Niewyjaśnione problemy z zasobami systemowymi: przepełnienie systemu plików, duże obciążenie procesora
  - Dziwne komunikaty od demonów systemowych
  - Niewyjaśnione problemy z wydajnością urządzeń (routerów) lub usług sieciowych
  - Niewyjaśnione zachowanie procesów użytkowników
  - Dziwne atrybuty plików dzienników

35

Zadania systemu wykrywania intruzów

Główne zadanie to:

ochrona systemu komputerowego

poprzez

- **wykrycie ataku** (próby ataku)
- ewentualną **reakcję na atak**

Działania systemu wykrywania intruzów

Infrastruktura systemu wykrywania intruzów

Model systemu wykrywania intruzów

Komponenty systemu wykrywania intruzów

Architektura systemów wykrywania intruzów

- Systemy umieszczone w jednym miejscu
- Systemy rozproszone w chronionej sieci
  - Systemy IDS wymieniające między sobą informacje o włamaniach, naruszeniach
  - Systemy wieloagenckie

Wieloagencka architektura systemów IDS - AAFID

Autonomous Agents For Intrusion Detection

Klasyfikacja systemów wykrywania intruzów (1/4)

- Ze względu na sposób wykrycia ataku dzielimy systemy IDS na wykrywające:
  - **Anomalie** (*anomaly detection*), czasami nazywane *behavior based* — system bazuje na profilu normalnego zachowaniu systemu lub użytkowników
  - **Sygnatury ataków** (*signature detection*), czasami określane terminem *knowledge based* — system w celu wykrycia ataku bazuje na wiedzy o nienormalnych zachowaniach lub sygnaturach ataków.

Klasyfikacja systemów wykrywania intruzów (2/4)

- Podział ze względu na zachowanie w przypadku wykrycia ataku (próby ataku):
  - ***pasywne*** — system ogranicza się do generowania alarmów i tworzenia dzienników aktywności
  - ***aktywne*** — reaguje na atak próbując korygować ewentualne braki w zabezpieczeniach (np. próbując zamykać luki) lub działając proaktywnie (wylogowywując potencjalnych intruzów, blokując podejrzane usługi).

Klasyfikacja systemów wykrywania intruzów (3/4)

- Podział ze względu na częstotliwość wykorzystania systemu:
  - systemy ***działające w czasie rzeczywistym***, najczęściej wykorzystujące strumienie pakietów sieciowych
  - systemy ***uruchamiane okresowo*** (periodycznie bądź nieregularnie), zwykle korzystają z dzienników zdarzeń (audytu),

Klasyfikacja systemów wykrywania intruzów (4/4)

- Podział ze względu na źródło danych wykorzystywanych do tworzenia raportu z audytu
  - Systemy bazujące na danych pochodzących z ***pojedynczego hosta (systemu)*** — *host based*
  - Systemy bazujące na danych pochodzących z ***sieci lokalnej*** (*network based*)

Cechy systemów IDS

- Systemy bazujące na danych pochodzących z pojedynczego hosta (systemu)
  - Systemy monitorujące połączenia do systemu
  - Systemy monitorujące logowania do chronionego przez siebie hosta
  - Systemy monitorujące działania super użytkownika (administrator, root)
  - Systemy monitorujące stan plików systemowych
  - Systemy monitorujące stan rejestru systemowego
  - Systemy bazujące na danych dotyczących procesów monitorowanych przez jądro systemu operacyjnego

Cechy systemów IDS

- Systemy bazujące na danych pochodzących z sieci lokalnej
  - Systemy monitorujące **natężenie ruchu** sieciowego
  - Systemy wykrywania włamań monitorujące **ruch** sieciowy (pakiety) kierowany **do hosta**, na którym są zainstalowane
  - Systemy wykrywania włamań wykorzystujące jako źródło **wszystkie pakiety** sieciowe docierające do interfejsu sieciowego działającego w trybie odbierania (*promiscuous mode*)

Klasyfikacja systemów wykrywania intruzów

Systemy IDS – źródła danych

- **Przetwarzanie audytu** (lub raportu z audytu)
- Systemy działające **w czasie rzeczywistym**

Systemy IDS przetwarzające raport audytu (1/3)

- Przechowywanie raportu audytu
  - W jednym pliku
  - W różnych miejscach sieci
- Ilość zapisywanych zdarzeń w dziennikach
  - Zapisywanie wszystkich zdarzeń powoduje duże zużycie zasobów (systemu lokalnego i sieci)
  - Kompresowanie logów powoduje dodatkowe obciążenia
- Systemy przetwarzające dzienniki mogą być atakowane poprzez zapełnienie wolnej przestrzeni systemu (atak DoS)

Systemy IDS przetwarzające raport audytu (2/3)

- Trudno z góry przewidzieć rozmiary plików raportów z audytu
- Trudno określić jak długo przechowywane powinny być pliki z aktualnego audytu
- Pożądane w tej metodzie jest:
  - umożliwienie parametryzacji zapisywania zdarzeń systemowych i działań użytkowników
  - udostępnienie opcji samoczynnego wyłączenia mechanizmu logowania w przypadku braku miejsca lub ataków DoS
  - jak najmniejsze obciążenie systemu przygotowaniem raportu z audytu
  - przetwarzanie informacji z audytu za pomocą dodatkowych mechanizmów (agregacja, sztuczna inteligencja, wydobywanie danych) ze względu na duże rozmiary plików

Systemy IDS przetwarzające raport audytu (3/3)

- Cele:
  - Tworzenie wzorców dostępu i użytkowania; określenie prawidłowości ruchu sieciowego
  - Odkrycie powtarzających się prób ominięcia zabezpieczeń (zastosowania nietypowych przywilejów, nadużycia, prób ataków)
  - Odstraszenie intruzów poprzez samą świadomość istnienia takiego narzędzia kontroli
  - raport z audytu jest formą ochrony niewinnego użytkownika, np. przed nieuzasadnionym zarzutem wykonania niebezpiecznych akcji

Systemy IDS działające na bieżąco (1/6)

- Główne problemy i zagadnienia systemów wykorzystujących przetwarzanie na bieżąco
  - Przetwarzane przez te systemy akcje są zawsze aktualne, sygnalizują one próbę ataku lub sam atak
  - Metody obróbki danych – wykorzystane algorytmy ograniczają się do szybkich i wydajnych procedur
  - Duże wymagania wobec pamięci operacyjnej (buforów). Nie ma możliwości składowania danych
  - Mała ilość dostępnej dla detektora informacji — tylko zawartości buforów

Systemy IDS działające na bieżąco (2/6)

- Sposoby identyfikacji włamania
  - Wykrywanie wzorców ataków, dokonywane zwykle poprzez proste wyszukiwanie ciągów znaków w pakietach. Przykłady obrazujące różnorodność sygnatur ataków [Fre01]
  - Przetwarzanie pakietów, wymagające wydzielania poszczególnych danych z pakietów; dokonywane dla kolejnych warstw sieciowych

Systemy IDS działające na bieżąco (3/6)

- Wykrywanie wzorców ataków – rodzaje sygnatur:
  - Monitorowanie adresów IP inicjujących połączenie
  - Monitorowanie nieodpowiednich kombinacji flag TCP/IP
  - Wykrywanie wirusów w poczcie elektronicznej poprzez wyszukiwanie odpowiedniego tytułu listu lub nazwy załącznika
  - Wyszukiwanie kodu mającego wykonać się na atakowanym systemie (przepełnienie bufora)
  - Badanie zawartości pakietu i sprawdzenie długości odpowiednich pól (*Ping of Death*)
  - Sprawdzanie ilości wywołań niektórych obciążających system komend (DoS)
  - Sygnatury monitorujące stan sesji użytkownika

Systemy IDS działające na bieżąco (4/6)

- Systemy IDS przetwarzające pakiety (sposoby identyfikacji włamania)
  - Możliwość korelacji pakietu z innymi pochodzącymi z tej samej sesji
  - Konfrontacja z typowymi pakietami danego protokołu
  - Większa czasochłonność niż przy poszukiwaniu sygnatur ataków
  - Duża zależność od systemu (różne implementacje protokołów w różnych wersjach systemów operacyjnych)

Systemy IDS działające na bieżąco (5/6)

- Zalety
  - Wykrycie typowo sieciowych ataków – istnieje wiele ataków, szczególnie typu DoS, które nie mogą być wykryte za pomocą zwykłego audytu systemu, muszą być wykrywane przy pomocy analizy ruchu sieciowego
  - Przetwarzanie na bieżąco umożliwia reagowanie na incydenty w trakcie ich trwania, dzięki czemu można nawet zablokować kontynuowanie ataku
  - System jest obciążony w mniejszym stopniu niż w przypadku wykorzystania raportu z audytu

Systemy IDS działające na bieżąco (6/6)

- Wady
  - Identyfikacja nadawcy odbywa się na podstawie jego adresu sieciowego pochodzącego z pakietu. Ogranicza to możliwości automatycznej reakcji na atak (*IP Spoofing*)
  - Ewentualne kodowanie nie pozwala na analizę zawartości pakietu
  - Moduł analityczny dysponuje ograniczonym zbiorem informacji (tylko zawartość bufora) - jego możliwości wykrywania są ograniczone
  - Systematyczne skanowanie ruchu sieciowego obniża przepustowość sieci tam, gdzie umiejscowiony jest system IDS

Klasyfikacja zachowania użytkownika w systemach IDS

Zachowanie

Klasyfikacja systemów wykrywania intruzów (przypomnienie)

- Ze względu na sposób wykrycia ataku dzielimy systemy IDS na wykrywające:
  - **Anomalie** (*anomaly detection, behavior based*) — system bazuje na profilu normalnego zachowaniu systemu lub użytkowników
  - **Sygnatury ataków** (*signature detection*, *knowledge based*) — system w celu wykrycia ataku bazuje na wiedzy o nienormalnych zachowaniach lub sygnaturach ataków.

Wykrywanie anomalii (1/5)

- Profile normalnego zachowania, pozwalają ustalić **przewidywaną działalność użytkownika i systemu**
- Próba identyfikacji czy nastąpiło włamanie (naruszenie zabezpieczeń systemu) polega na **porównaniu** obecnie **obserwowanych działań** użytkownika **z profilem** i oszacowaniu ewentualnego odchylenia od profilu

Wykrywanie anomalii (2/5)

- Konieczne jest profilowanie początkowe — „nauka” systemu - określenie tego, co jest zwykłym działaniem użytkownika
  - Niebezpieczeństwo pojawienia się nielegalnych działań użytkowników w czasie tworzenia profilu początkowego i potraktowanie ich jako prawidłowe zachowanie
  - Nieodpowiednio stworzony profil nie będzie pozwalał na wykrycie wszystkich nielegalnych działań użytkowników

Wykrywanie anomalii (3/5)

- Powinna istnieć **możliwość zmiany profilu** w czasie i adaptacji do aktualnego zbioru prawidłowych zachowań użytkownika
- Wszystko, co nie mieści się we wcześniej ustalonych ramach zwykłego użytkowania systemu (profilu), jest postrzegane jako działanie podejrzane
  - Wysoka kompletność
  - Dokładność (liczba fałszywych alarmów) – stanowi jednak problem

Wykrywanie anomalii (4/5)

- Zalety
  - Możliwość **wykrycia nieznanego typu ataku**. Anomalie są wykrywane, bez konieczności zrozumienia ich przyczyn i charakterystyki
  - **Mniejsza zależność** IDS od rozwiązań konkretnych **systemów operacyjnych** (w porównaniu do systemów z wykrywaniem sygnatur ataków)
  - Możliwość wykrycia **nadużyć** przywilejów przez **legalnego użytkownika** systemu

Wykrywanie anomalii (5/5)

- Wady
  - Wysoki współczynnik **fałszywych alarmów**. Wszystkie prawidłowe przypadki użycia systemu nie mogą być zaobserwowane podczas fazy budowania profilu
  - Zachowanie użytkowników może zmieniać się w czasie, doprowadzając do **konieczności zmian profilu** normalnego zachowania
  - Chroniony system może stać się obiektem **ataku podczas fazy nauki** (tworzenia profilu). Rezultatem będzie ustalenie profilu uważającego ten typ ataku za zachowanie normalne — nie będzie ogłaszany alarm po wystąpieniu tego rodzaju anomalii

Wykrywanie sygnatur ataków (1/5)

- Systemy posiadające informację o nienormalnym, niebezpiecznym zachowaniu (wzorce ataków)
- Często wykorzystywane w systemach wykrywania włamań na bieżąco
- Sygnatury ataków – opisują wzorce aktywności, mogące stanowić zagrożenie dla bezpieczeństwa
  - Sygnatury ataków – opisują wzorce aktywności, mogące stanowić zagrożenie dla bezpieczeństwa. Przedstawiane są zwykle w postaci **czasowej współzależności ciągów działań**, które mogą być przeplatane czynnościami obojętnymi.
  - Wybrane **ciągi tekstowe** – sygnatury ciągów tekstowych mogących być uznane za **podejrzane** (np. odwołanie do pliku /etc/passwd).

Wykrywanie sygnatur ataków (2/5)

- Akcje, które nie są otwarcie postrzegane jako atak są w systemie dozwolone
  - Dokładność tego rodzaju systemów jest wysoka (mało fałszywych alarmów)
  - Zwykle nie osiągają one jednak wysokiej kompletności — są nieodporne na nieznane ataki

Wykrywanie sygnatur ataków (3/5)

- Podejścia stosowane w tego typu systemach IDS
  - **Weryfikacja** pakietów protokołów **niższych warstw** – szukanie błędnych pakietów IP, TCP, UDP czy ICMP
  - **Weryfikacja** protokołów warstwy **aplikacji** - wiele rodzajów ataków wykorzystuje niewłaściwe żądania skierowane do aplikacji sieciowych. Aby efektywnie wykrywać tego rodzaju ataki, system IDS musi mieć zaimplementowanych wiele protokołów warstwy aplikacji

Wykrywanie sygnatur ataków (4/5)

- Zalety
  - Systemy oparte na sygnaturach nienormalnego zachowania mają bardzo **niski współczynnik fałszywych alarmów**
  - Zwykle **nie powodują** one znaczącego **obciążenia** chronionego systemu

Wykrywanie sygnatur ataków (5/5)

- Wady
  - Trudności w zdobywaniu informacji o nowych typach ataków i co za tym idzie utrzymaniu systemu aktualnej bazy sygnatur
  - Nie potrafią wykrywać nieznanych im ataków, zwłaszcza nowych
  - Utrzymanie systemu IDS wymaga dokładnego analizowania potencjalnych luk w zabezpieczeniach systemu, co jest zajęciem czasochłonnym
  - Wiedza o atakach jest specyficzna dla systemu operacyjnego, jego wersji, platformy oraz używanych aplikacji
  - Uznaje się, iż **wykrywanie ataków wewnętrznych** w tego typu systemach jest **utrudnione**. Zwykle według systemu podczas nadużycia uprawnień legalnego użytkownika, nie dochodzi do próby włamania (ze względu na brak informacji o uprawnieniach użytkownika oraz strukturę sygnatur ataków).

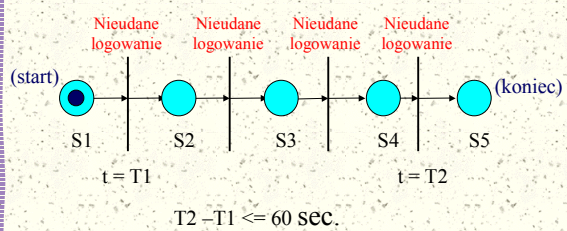
Wykrywanie ataków na podstawie zgodności parametrów ze wzorcem

- **Administratorzy monitorują** wiele rozmaitych cech systemu i sieci. Uzyskane w ten sposób informacje mają stałą, określoną specyfikę
- Wykorzystanie codzienne **doświadczenie administratorów** jako podstawę do wykrycia anomalii
- Pozwala wykryć nieznane metody ataków
- Brak możliwości analizy przez człowieka dużej ilości informacji – część ataków nie będzie wykryta

Techniki przetwarzania w systemach IDS (1/3)

- Mechanizmy przetwarzania w systemach bazujących na wykrywaniu sygnatur ataków
  - **Systemy ekspertowe**. Zdarzenia tłumaczone na fakty. Wzorce – reguły.
  - **Analiza sygnatur** (*signature analysis*). Sygnatury do postaci audytu. Efektywna i często stosowana. Osobne wzorce dla odmian OS
  - **Sieci Petriego** (kolorowane). Problem powiązania wzorców z audytem.
  - **Analiza przejść-stanów** (*state-transition analysis*). Wzorzec: zbiór podcelów i przejść intruza. Diagramy stanów przejść i ich analiza.

Techniki przetwarzania w systemach IDS – sieci Petriego (2/3)



T2 –T1 <= 60 sec.

Techniki przetwarzania w systemach IDS (3/3)

- Techniki przetwarzania w systemach bazujących na wykrywaniu anomalii
  - **Metoda oparta na statystykach**
  - **Systemy ekspertowe**
  - **Sieci neuronowe**. Częściowo zbieżne ze statystykami
  - **Identyfikacja intencji** użytkownika. Zadania i funkcje użytkowników
  - **Odporność komputerów** (*computer immunology*). Typowe zachowanie OS
  - **Uczenie maszynowe**. Wektor listy wywoływanych komend
  - **Wydobywanie danych** (*data mining*)

Klasyfikacja systemów wykrywania intruzów (przypomnienie)

- Podział ze względu na zachowanie w przypadku wykrycia ataku (próby ataku)
  - ***pasywne*** — system ogranicza się do generowania alarmów i tworzenia dzienników aktywności
  - ***aktywne*** — reaguje na atak próbując korygować ewentualne braki w zabezpieczeniach (np. próbując zamykać luki) lub działając proaktywnie (wylogowując potencjalnych intruzów, blokując podejrzane usługi).

Pasywne systemy wykrywania intruzów

- Rodzaje akcji podejmowanych przez systemy IDS z pasywnym systemem reakcji
  - Logowanie podejrzanych połączeń, pakietów
    - zapis odpowiednich informacji w logach
    - dodanie odpowiednich wpisów do alertów systemowych (zapis odpowiednich zdarzeń w dziennikach),
    - zapis treści pakietów pochodzących od podejrzanego użytkownika
    - uruchomienie mechanizmów badania korelacji z danymi pochodzącymi z innych sesji podejrzanego użytkownika lub danymi pochodzącymi z innych źródeł
  - Informowanie użytkownika
    - email do użytkownika (administratora),
    - dźwięki
    - wysłanie informacji SMS (pager).

Aktywne systemy wykrywania intruzów (1/4)

- Typy działań
  - Reakcje związane ze zmianą parametrów połączenia
    - rekonfiguracja zapory – uniemożliwienie intruzowi ataku z danego adresu lub na dany port
    - zamknięcie sesji z danym użytkownikiem poprzez podrobienie odpowiedniego pakietu (TCP FIN, RESET)
    - wylogowanie podejrzanego użytkownika
  - Zmiana polityki bezpieczeństwa związanej z danym kontem użytkownika
    - blokada (czasowa lub stała) konta podejrzanego użytkownika
    - modyfikacja (ograniczenie) uprawnień użytkownika
    - blokada dostępu do zasobów dla danego użytkownika: czasowa, stała, czasowa z możliwością „uniewinnienia" (przynęty i pułapki)

Aktywne systemy wykrywania intruzów (2/4)

- Typy działań (c.d.)
  - Załatanie luk w zabezpieczeniach
    - próba sprowadzenia i instalacji odpowiednich łat (*patch*)
    - próba instalacji nowej wersji oprogramowania do obsługi danej usługi sieciowej lub reinstalacja wersji starej
    - próba rekonfiguracji usług sieciowych, np. zmiana parametrów (zwiększenie wielkości buforów), uruchomienie lub zmiana opcji szyfrowania, itp.
  - Uruchomienie dodatkowych mechanizmów systemu wykrywania intruzów
    - SNMP Trap — wysłanie pakietów SNMP rekonfigurujących router
    - próba tropienia napastnika: ping, Nslookup, traceroute, skanowanie portów, rusers, rcpInfo, whois, showmount, zdalna identyfikacja systemu operacyjnego (*OS fingerprinting*), finger

Aktywne systemy wykrywania intruzów (3/4)

- Typy działań (c.d.)
  - Uruchomienie dodatkowych mechanizmów systemu IDS
    - uruchomienie mechanizmu pułapki (przeniesienie do systemu pułapki, zakwalifikowanie działań użytkownika jako podejrzanych i zastosowanie w stosunku do niego środków bezpieczeństwa)
    - wykorzystanie pułapki tropiącej, w której system pułapki śledzi działania podejrzanego użytkownika aż do momentu porzucenia przez niego jego przybranej (fałszywej) tożsamości
    - w przypadku systemu wykorzystującego technologię wieloagencką – wysłanie agentów w inne miejsce
    - zastosowanie mechanizmów kontrpenetracji (*reverse cracking*)

Aktywne systemy wykrywania intruzów (4/4)

- Typy działań (c.d.)
  - Inne działania
    - ignorowanie ruchu sieciowego kierowanego (przez danego użytkownika lub przez wszystkich użytkowników) do danej usługi sieciowej
    - wyłączenie usługi
    - wylogowanie wszystkich (grupy) użytkowników
    - restart systemu
    - wyłączenie systemu

Ataki wymierzone przeciwko systemom IDS

- Zaślepienie sensora IDS *(blind the sensor)*
- Zaślepienie bufora przechowującego zdarzenia
- Ataki typu DOS, DDoS
- Fragmentacja
- Unikanie wartości domyślnych
- Powolne skanowanie
- Skoordynowany powolny atak
- Uniknięcie wykrycia poprzez zmianę wzoru *(pattern change evasion)*

Problemy związane z efektywnością systemów IDS (1/3)

- Problem z **przetwarzaniem** przez IDS **ruchu sieciowego** w przypadku szybszych łącz oraz dużej ilości pakietów
- Problem związany z **odpornością** systemu wykrywania włamań na ataki DoS i DDoS
- Problemy związane z niewykryciem rzeczywiście przeprowadzanej próby ataku na chroniony system (*false negative*) – **niewykryte ataki**
- Raportowanie przez IDS ataku gdy nie miał on miejsca (*false positive*) – **fałszywe alarmy**

Problemy związane z efektywnością systemów IDS (2/3)

- Problem **fragmentacji pakietów** w systemach IDS
- Problem z wykorzystaniem **złożonych algorytmów** przetwarzania pakietu **w czasie rzeczywistym**
- Problem **korelacji pakietów** użytkownika z
  - Innymi pakietami użytkownika z tej samej sesji
  - Pakietami użytkownika pochodzącymi z innych sesji
  - Pakietami innych użytkowników
  - Problem synchronizacji czasu między systemami komputerowymi
- Wykorzystanie systemów IDS nie działających w czasie rzeczywistym – **opóźnienia reakcji**

Problemy związane z efektywnością systemów IDS (3/3)

- Wyszukiwanie dużej liczby wzorców ataków jest nieefektywne
  - Sygnatury są mocno powiązane z systemami operacyjnymi, wersją oprogramowania itp.
  - Instalacja wielu sensorów systemów IDS (każdy monitoruje część sygnatur) – nieekonomiczne i słabo skalowalne
- Wykorzystanie algorytmów kryptograficznych – zagrożenie dla systemów IDS

Problemy związane z architekturą systemów IDS

- Systemy wykrywania włamań działające w oparciu o **pojedynczy system** nie są w stanie wykryć wszystkich ataków (w szczególności **ataków sieciowych**)
- Przejście na architekturę **sieci przełączanych** utrudnia wykorzystanie systemów IDS wykorzystujących szperacze (*sniffer*) jako źródło informacji o pakietach sieciowych kierowanych do chronionej sieci

2 x 45

Przynęty

Przynęta – system lub zasób sieciowy nie udostępniający żadnych strategicznych dla działania organizacji usług sieciowych. Podstawową funkcją tego zasobu jest bycie atakowanym.

Powodem instalacji przynęt w sieci organizacji jest możliwość oceny zagrożeń związanych z bezpieczeństwem, na jakie narażone są systemy działające w danej sieci oraz działanie prewencyjne systemu przynęty (w ograniczonym zakresie) [Spi01].

Działanie przynęt

- Przynęty mają prowokować intruza do ataku. Przykłady:
  - Instalowanie systemu, który nie ma żadnego zadania poza logowaniem wszystkich prób dostępu
  - Instalowanie specjalnego zaprojektowanego w tym celu, oprogramowania (emulującego działanie aplikacji udostępniających usługi sieciowe)
  - Instalowanie słabo zabezpieczonego systemu operacyjnego w sieci organizacji
- Z każdego istniejącego systemu operacyjnego można stworzyć przynętę

Cechy przynęt

- System przynęty powinien wyglądać jak najmniej podejrzanie
- Należy liczyć się z możliwością przejęcia przynęty przez intruza i wykorzystania go do ataku na inne systemy w sieci organizacji
- System przynęty powinien być tworzony w sposób przypominający system przechowujący interesujące, wewnętrzne informacje organizacji
  - listy płac,
  - wyniki finansowe

Zalety przynęt (1/3)

- Systemy przynęt nie reagują na włamanie. Umożliwiają wykrycie całości działań intruza
- Przynęty ułatwiają łatwą identyfikację włamania
  - Ich dzienniki systemowe gromadzą najczęściej bardzo małą ilość informacji
  - Próba łączenia się z systemem przynęty oznacza podejrzaną działalność
  - Próba nawiązania połączenia z innym systemem przez system przynęty oznacza najczęściej przejęcie systemu przynęty przez intruza

Zalety przynęt (2/3)

- Przynęty są lub udają, że są łatwym celem dla intruza
  - Wysyłanie informacji o wersji i nazwie oprogramowania podczas nawiązywania połączenia przez intruza (*banner checks*)
- Przynęta może jedynie emulować działanie usługi sieciowej (usługa ta nie musi działać na systemie przynęty)
- Przynęty gromadzą bardzo małe ilości najczęściej cennych danych

Zalety przynęt (3/3)

- Ze względu na małe ilości danych kierowanych do przynęty, może ona logować wszystkie akcje podejmowane przez intruza
- Systemy przynęt mogą być odłączone od sieci organizacji bez utraty dostępu do strategicznych dla niej usług sieciowych. Systemy przynęt mogą być długo analizowane po wystąpieniu ataku

Wady przynęt (1/2)

- Przynęta może być wykorzystana do ataku na inne systemy znajdujące się w sieci organizacji
- Przynęta nie jest systemem aktywnie zachęcającym intruza do przeprowadzenia próby włamania
  - Nie atakowana przynęta jest bezużyteczna
- Systemy przynęt zwiększają złożoność sieci organizacji
  - Dodatkowe wydatki związane z administrowaniem siecią

Wady przynęt (2/2)

- Wartość przynęt jako systemów odstraszających intruzów jest mocno dyskusyjna
- Instalowanie systemu przynęty (jako systemu mającego na celu zwodzenie intruza) często jest niecelowe
  - Automatyczne narzędzia do przeprowadzania ataków
  - Robaki internetowe

Cel instalowania systemu przynęty

- Przygotowanie specyficznej dla danej organizacji polityki reakcji na incydenty
- Uzyskanie szczegółowej wiedzy na temat bezpieczeństwa systemów komputerowych
- Stworzenie (przy wykorzystaniu przynęty) swego rodzaju systemu wczesnego ostrzegania

Rodzaje przynęt (1/2)

- Aplikacja nasłuchująca na danym porcie
- Systemy emulujące działanie usługi sieciowej – umożliwiają intruzowi interakcję
  - Implementują część protokołu wykorzystywanego do interakcji z intruzem
  - Protokół jest implementowany w całości
- Przynęty emulujące działanie wielu różnych protokołów
  - Systemy emulujące zbiór protokołów
  - Systemy emulujące działanie całego systemu operacyjnego

Rodzaje przynęt (2/2)

- Oprogramowanie pozwalające na stworzenie (jednego lub większej liczby) wirtualnych systemów przy wykorzystaniu jednej fizycznej maszyny
  - Często istnieje możliwość „wycofania” całej sesji intruza z systemem
- Rzeczywiste (najczęściej słabo zabezpieczone) systemy

Pułapki

Pułapka – zbiór elementów funkcjonalnych i proceduralnych, które posługują się legalnym i uprawnionym oszustwem w celu odwrócenia uwagi potencjalnego intruza od rzeczywistych, wartościowych zasobów przez użycie zasobów fikcyjnych i skierowanie jej na gromadzenie informacji, wiążących się z włamaniami i na reagowanie [Amo99].

Model działania pułapki (1/2)

- Intruz wchodzi w interakcję ze zbiorem zasobów, podczas gdy jego aktywność jest monitorowana
- Po uzyskaniu dowodów na złe zamiary intruza jest on kierowany do fikcyjnego systemu
- Skierowanie do fikcyjnego zasobu może być wywołane
  - Wydaniem komendy, która jest groźna (np. próba skasowania ważnych plików w systemie
  - Przekroczeniem wartości jakiegoś wskaźnika (trzecie nieudane logowanie)
  - Wyzwalacz w niektórych przypadkach może być niedeterministyczny

Model działania pułapki (2/2)

- Możliwe jest powtórne przeniesienie intruza do rzeczywistych zasobów. Może to nastąpić gdy
  - Uzyskano wystarczające świadectwo niewinności intruza
  - Możliwe jest przeniesienie aktywności i działań intruza ze środowiska fikcyjnego do rzeczywistego (intruz nie wprowadził zmian niemożliwych do wprowadzenia w rzeczywistym systemie)
- Przywrócenie intruzowi dostępu do rzeczywistego środowiska może być bardzo trudne a niejednokrotnie niewykonalne

Model interakcji z systemem pułapki

Trudności związane z implementacją pułapek

- Bezbłędne wykrycie działań będących włamaniami
  - Przeniesienie intruza do fikcyjnego systemu powinno odbyć się tylko po uzyskaniu pewności co do tego, że jest on intruzem
- Wykrywanie działań wyzwalających
  - Konieczne jest określenie granicy między działaniem w systemie rzeczywistym, a działaniem w systemie pułapki
  - Poznanie tego mechanizmu może ułatwić intruzowi pozostanie w rzeczywistym systemie
  - Przeniesienie wiąże się z dużym zużyciem zasobów
- Pułapka musi pozostać w ukryciu aby spełniać swoje funkcje

Typy pułapek

- Środowisko rzeczywiste z elementami pułapki
  - rzeczywiste środowisko systemu UNIX i fałszywy plik haseł dostępny dla intruza
- Małe środowisko z duża pułapką
  - Środowisko nie zawiera kluczowych ani szczególnie ciekawych zasobów. System jest dużą i zachęcającą pułapką
- Podobne (w sensie rozmiarów) środowisko i pułapka
  - Pułapka jest odzwierciedleniem rzeczywistego systemu
- Duże środowisko z małą pułapką
  - Duże i potencjalnie interesujące środowisko i mała pułapka. Rozsądne, gdy tworzenie dużej i skomplikowanej pułapki jest ekonomicznie i technologicznie niemożliwe

Względy prawne związane z wykorzystaniem pułapek i przynęt

- Konieczna jest zgoda na monitorowanie działań użytkowników
- Zapewnienie legalności działań podejmowanych przez pułapkę w wyniku reakcji na działanie użytkownika jest również konieczne
- Konieczne jest zapewnienie, że użycie systemu pułapki nie stanowi naruszenia polityki bezpieczeństwa i innych regulaminów organizacji
- Ochrona niewinnych użytkowników – pułapka nie może niszczyć, naruszać ochrony i blokować zasobów należących do niewinnych użytkowników

Wykorzystanie cech systemu operacyjnego do budowy pułapki (1/3)

- System operacyjny powinien umożliwiać manipulowanie przynależnością użytkowników do poszczególnych grup
- Monitorowanie akcji użytkownika wbudowane w jądro systemu – zmniejszy możliwość przekłamań
- Wielopoziomowa budowa systemu plików
- Dobrym posunięciem byłoby dołączenie zewnętrznych pułapek tropiących. Pułapki mogą stanowić skuteczne narzędzie do śledzenia tożsamości włamywacza, który mógłby zostać zwabiony do ujawnienia tożsamości

Wykorzystanie cech systemu operacyjnego do budowy pułapki (2/3)

- Poprawna konstrukcja przynęt – przynęta polega na udostępnianiu zasobów. Wiąże się to z:
  - Zachowaniem wymogów prawnych związanych z tworzeniem przynęt i pułapek
  - Dostosowaniem materiałów w przynęcie do oczekiwań intruzów
  - Przynęta nie może nie może zbyt manifestacyjnie okazywać łatwości i dostępności
  - Interesujące dla włamywaczy mogą być
    - narzędzia intruzów (sugestywne katalogi i nazwy plików)
    - Informacje finansowe
    - Poczta innych użytkowników

Wykorzystanie cech systemu operacyjnego do budowy pułapki (3/3)

- Zwiększenie realizmu systemu pułapki
  - Korespondencja z administratorem – w systemie powinna znaleźć się poczta od administratora. Komunikaty mogą powiadamiać o niedostępności niektórych zasobów
  - Sfabrykowana poczta
  - Zapewnienie możliwości wykorzystania błędów w zabezpieczeniach systemu
  - Komunikaty systemowe – pułapka mogłaby sama tworzyć realistyczne komunikaty systemowe i wprowadzać je do raportu audytu

Trendy dominujące w systemach wykrywania intruzów (1/2)

- Wykorzystanie **szperaczy** jako źródła danych
  - Działających na pojedynczym systemie
  - Umożliwiających analizę ruchu sieciowego z całej sieci lokalnej
- Prowadzone są badania nad podwyższeniem **efektywności przetwarzania** informacji przez IDS, przy łączach o przepustowości równej 100 Mb/s (*Fast Ethernet*) i większej (*Gigabit Ethernet*)
- Trwają prace nad określeniem **jednolitego formatu** plików będącymi wynikiem **audytu**. Podobne prace prowadzone są nad określeniem zawartości samego raportu audytu.

Trendy dominujące w systemach wykrywania intruzów (2/2)

- Badane są sposoby analizy danych pochodzących z audytu:
  - Analiza na podstawie **sygnatur ataków** jest obecnie rozwijana głównie przez **komercyjne** przedsiębiorstwa, mimo iż udowodnione zostało, iż nie nadaje się ona do wykrycia każdego typu ataku
  - Podejście bazujące na **wykrywaniu anomalii** jest rozwijane głównie przez organizacje **naukowe**, jednak powstaje coraz więcej komercyjnych systemów wykrywania włamań korzystających z takiego podejścia
  - Prowadzone są prace nad wykrywaniem **ataków wewnętrznych**

Obszary badań związanych z systemami IDS

Kierunki rozwoju systemów IDS (1/4)

- Integracja IDS z zaporą ogniową
  - Ustawienie IDS **przed zaporą** – wykrywanie wszystkich ataków
  - Ustawienie IDS **za zaporą** – wykrywanie intruzów, którym udało się przejść przez zaporę
  - Ustawienie IDS **przed i za zaporą** – umożliwia zebranie większej ilości kompletnych informacji dotyczących ataku
  - Ustawienie IDS **równolegle do zapory** - pozwala na wykorzystanie systemu wykrywania włamań jako dodatkowego mechanizmu wnioskowania dla zapory ogniowej
  - Ustawienie IDS **wewnątrz** korporacyjnej **sieci** firmy – pozwala na wykrywanie nadużyć legalnego użytkownika działającego w korporacyjnym Intranecie organizacji

Kierunki rozwoju systemów IDS (2/4)

- Integracja systemów wykrywania włamań (lub niektórych ich funkcji) w rozwiązania sprzętowe
  - bramy sprzętowe
  - przełączniki
  - VPN (*Virtual Private Networks*)
- Wykorzystanie architektury wieloagenckiej
- Wykorzystanie mechanizmów kontrpenetracji
- Stworzenie jednolitego standardu zapisu danych z raportu audytu, standaryzacja formatu zapisu systemowych mechanizmów protokołowania

Kierunki rozwoju systemów IDS (3/4)

- Wykorzystanie systemów IDS do wykrywania podejrzanych informacji zawartych np. w listach elektronicznych – *Carnivore*
- Stworzenie architektury systemów wykrywania włamań odpornej na ataki typu odmowa usługi (DoS i DDoS)
- Systemy wykrywania włamań będą instalowane między sieciami lokalnymi, przechwytując cały ruch między nimi, same zaś pozostając praktycznie niewidzialnymi dla ruchu sieciowego - *Hogwash*

Kierunki rozwoju systemów IDS (4/4)

- Systemy włamań będą rozwijały możliwości korelacji filtrowanego przez nie ruchu z danymi wcześniej analizowanymi
- Architektury pozwalające na wymianę informacji w sieciach rozległych, pozwalające na integrację informacji dostępnych z każdego rodzaju sprzętu sieciowego, systemu IDS.

Ocena systemu wykrywania intruzów

- Dokładność
  - Dokładność kwalifikacji działań użytkownika jako groźne. Ważna liczba fałszywych alarmów.
- Kompletność
  - Ważna liczba przeoczeń rzeczywistych ataków
- Wydajność
  - Możliwość działania w czasie rzeczywistym
- Odporność na ataki
- Czas reakcji
  - Czas propagacji informacji o niebezpieczeństwie i szybkość reakcji systemu IDS

Wymogi dla idealnego systemu wykrywania włamań (1/2)

- Powinien móc działać bez przerw z minimalnym nadzorem ze strony człowieka
- Musi być odporny na błędy, być w stanie podjąć działanie po zawieszeniu się systemu (wrócić do stanu sprzed incydentu)
- Musi być odporny na działalność wywrotową (*subversion resistant)*
- Musi być wysoce konfigurowalny

Wymogi dla idealnego systemu wykrywania włamań (2/2)

- Musi być zdolny do zaadoptowania się do zmian w zachowaniu użytkowników systemu jak i samego systemu
- Musi być wysoce skalowalny, aby monitorować wiele komputerów dostarczając aktualnego raportu dotyczącego ich stanu
- Nie może być podatny na uszkodzenia (wyłączenie) swoich własnych modułów
- Musi pozwalać na dynamiczną zmianę konfiguracji bez konieczności restartu systemu

Czas na prezentację...

- System snort – darmowe środowisko IDS.
- System autorski