Wykrywanie włamań

Materiały pomocnicze do wykładu

Bezpieczeństwo systemów informatycznych

Wykrywanie włamań

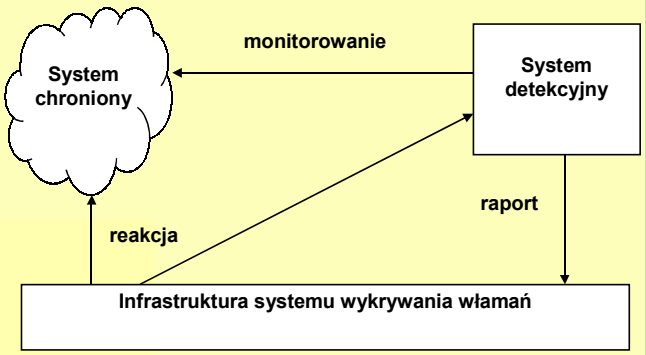
Podstawowe metody ataków

- Skanowanie adresów sieciowych
- Skanowanie portów sieciowych
- Analiza usług sieciowych
- Analiza kont użytkowników
- Sondowanie luk w systemie bezpieczeństwa
- Łamanie haseł dostępu
- Metody zaawansowane

Wymagania dla systemu wykrywania włamań

- Ciągła czujność
- Niewidoczność
- Infrastruktura wspomagająca
- Mylenie przeciwnika

Koncepcja systemu wykrywania włamań



Klasyfikacja IDS według źródeł informacji

- IDS Hostowy (*Host IDS*)
  - *Application-Based IDS*
- IDS Sieciowy (*Network IDS*)
- IDS Węzłowy (*Network Node IDS*)

HIDS

- Oprogramowanie ochronne rezyduje na poszczególnych komputerach
- Analizuje zasoby systemu lokalnego
- Zwykle reaktywne, rzadziej proaktywne (*Intrusion Prevention System*)

Zalety HIDS

- Dzięki swojej obecności bezpośrednio na komputerze i stałemu monitorowaniu lokalnych zasobów mogą wykryć ataki niewidoczne dla sieciowych IDS,
- Niezależność od topologii sieciowej,
- Dzięki integracji z systemem operacyjnym mogą skutecznie działać nawet w oparciu o zaszyfrowane dane,
- Mogą wykrywać różne rodzaje „koni trojańskich" lub pewne rodzaje ataków powodujące naruszenie integralności oprogramowania (kasowanie plików etc.).

Wady HIDS

- Trudne do zarządzania
- Mogą zostać wyłączone przy użyciu pewnych typów ataków DoS
- Wymagające często dużej przestrzeni dyskowej
- Obciążające (zmniejszające wydajność) systemu produkcyjnego

HIDS aplikacyjny

- Monitoruje interakcję użytkownika z aplikacją, co umożliwia dopasowanie niedozwolonych działań do konkretnej osoby.
- Ma dostęp do zaszyfrowanych danych po odszyfrowaniu przez aplikację.
- Może być bardziej podatny na ataki niż zwykły HIDS.
- Dostosowany zwykle monitorowania zdarzeń na poziomie użytkownika, więc może nie wykryć ataku dokonanego przez konia trojańskiego lub innych ataków szkodliwych dla aplikacji.

NIDS

- Dopasowywanie wzorców
- Kontekstowe dopasowywanie wzorców
- Dekodowanie protokołów wyższych warstw
- Analiza heurystyczna
- Analiza anomalii

Zalety NIDS

- Kilka dobrze umiejscowionych sieciowych systemów wykrywania włamań może monitorować rozległą sieć.
- Rozmieszczenie takich systemów nie wpływa na aktualną topologię sieci. Systemy NIDS są przeważnie pasywne w swoich działaniach i nasłuchując w danym segmencie nie zakłócają jednocześnie pracy sieci.
- Są odporne na ataki, mogą nawet zostać skonfigurowane jako niewidzialne dla potencjalnego włamywacza.

Wady NIDS

- Problemy z analizą wszystkich pakietów w rozległej i ruchliwej sieci.
- Kłopoty z lokalizacją
- Brak analizy zaszyfrowanych danych.
- Brak możliwości określenia rzeczywistej skuteczności ataki
- Podatność na ataki wykorzystujące fragmentację pakietów.

NNIDS

Zalety

- Wydajniejsze niż NIDS gdyż nie zajmują się wszystkimi pakietami krążącymi w sieci.
- Niezależne od topologii sieciowej.
- Możliwość analizy danych szyfrowanych.

Wady

- Konieczność instalowania na wielu komputerach.
- Brak możliwości ochrony grupy komputerów.
- Podatność na ataki.
- Obciążanie komputera produkcyjnego.

Klasyfikacja według metod analizy

- Wykrywanie nadużyć (*Misuse Detection*)

  Analizowana jest wszelka aktywność, w celu odnalezienia zdarzenia lub ciągu zdarzeń pasujących do znanego schematu ataku. Schematy takie są nazywane sygnaturami, stąd inna nazwa *signature-based detection*.

- Detekcja anomalii (*Anomaly Detection*)

  Wykrywanie niezwyczajnych zachowań (anomalii) na komputerze lub w sieci. Ataki znacząco różnią się od „zwykłej" (dozwolonej) aktywności i dzięki temu mogą być wykrywane.

Wykrywanie nadużyć – zalety i wady

- Generuje niewielką ilość fałszywych alarmów.
- Umożliwia szybkie i trafne wykrycie zastosowanej metody lub narzędzia ataku.
- Pozwala na łatwe wyśledzenia problemów związanych z bezpieczeństwem nawet mniej zaawansowanym administratorom.
- Umożliwia wykrycie tylko znanych wcześniej typów ataków.
- Niemożność detekcji nieco zmodyfikowanej wersji ataku.

Detekcja anomalii – zalety i wady

- Możliwość wykrycia symptomów ataku bez specyficznej wiedzy o nim samym.
- Generowanie danych wykorzystywanych później do definiowania sygnatur dla detektorów nadużyć.
- Duża liczba fałszywych alarmów.
- Konieczność stosowania rozległych „zbiorów treningowych".

Metody wykrywania włamań - szczegóły

- Przetwarzanie raportów audytu
- Przetwarzanie na bieżąco
- Profile normalnego zachowania
- Sygnatury nienormalnego zachowania
- Zgodność parametrów z wzorcem

Dobry system wykrywania włamań powinien stosować kilka różnych technik.

Przetwarzanie raportów audytu

- Przegląd wzorców w dostępie i użytkowaniu.
- Odkrycie powtarzających się prób ominięcia zabezpieczeń.
- Odkrycie zastosowania nietypowych przywilejów.
- Odstraszanie.
- Dodatkowa forma ochrony użytkownika.

Klasyfikacja według typów odpowiedzi

- Odpowiedzi aktywne
  - Zbieranie dodatkowych informacji
  - Zmiana środowiska
  - Podjęcie akcji przeciwko intruzowi
- Odpowiedzi pasywne
  - Alarmy i powiadomienia
  - Pułapki SNMP

Wykrywalność ataków przez systemy IDS

NETWORK IDS SIGNATURE RESULTS

Attack	CVE	No. of packets	Cisco Secure IDS 2.5	Enterasys Dragon 4.2	Intrusion.com SecureNet Pro 3.2	ISS BlackICE Sentry 2.5	ISS RealSecure 5.5	NFR Security NFR Network Intrusion Detection	Snort 1.7	Symantec NetProwler 3.5
AMD	CVE-1999-0704	11	Y	Y	N	Y	Y	N	Y	N
RDS	CVE-1999-1011	22	Y	Y	N	Y	Y	Y	Y	Y
WU-FTP	CVE-1999-0368	44	N	Y	N	N	Y	Y	Y	N
SNMP write	CAN-1999-0517	2	N	Y	N	N	Y	Y	N	N
Guest SMB login	CAN-1999-0519	19	N	Y	N	Y	Y	N	Y	N
IMAPD	CVE-1999-0005	8	Y	Y	Y	N	Y	Y	Y	N
PHF	CVE-1999-0067	10	Y	Y	Y	Y	Y	Y	Y	Y
Unicode	CVE-2000-0884	10	Y	Y	N	Y	Y	Y	Y	N
IIS 5 ISAPI	CAN-2001-0241	11	Y	Y	N	N	N	Y	Y	N
Total (out of 9)			6	9	2	5	8	7	8	2
Detect attacks fragmented (Frag-19)			Y	Y	Y	Y	Y	Y	Y	N

Y = YES N = NO

Typologia włamań

- NP1 - zewnętrzne nadużycie.
- NP2 - nadużycie sprzętu.
- NP3 - maskarada.
- NP4 - późniejsze nadużycie.
- NP5 - obejście kontroli.
- NP6 - aktywne nadużycie zasobu.
- NP7 - pasywne nadużycie zasobu.
- NP8 - nadużycie przez zaniechanie.
- NP9 - pośrednie wspomaganie.

Typowe symptomy włamań

- Powtarzanie się podejrzanego działania.
- Omyłkowe polecenia lub odpowiedzi pojawiające się podczas wykonywania sekwencji automatycznych.
- Wykorzystanie znanych słabych punktów.
- Niespójności kierunkowe w pakietach przychodzących lub wychodzących.
- Niespodziewane atrybuty pewnego żądania usługi lub pakietu.
- Niewyjaśnione problemy z pewnym żądaniem usługi, z systemem lub środowiskiem.

Typowe symptomy włamań

- Zewnętrzna wiedza o włamaniu.
- Pojawianie się podejrzanych objawów w ruchu pakietów w sieci.
- Logowanie się użytkowników o dziwnych porach,
- Nieudane próby zalogowania się,
- Niewyjaśnione ponowne uruchamianie systemu lub zmiany zegara systemowego,
- Nieautoryzowane użycie polecenia ***su***,

Typowe symptomy włamań

- Logowanie się użytkowników z nietypowych miejsc w sieci,
- Ruch sieciowy związany ze skanowaniem ICMP, portów lub połączenia z nielegalnymi portami,
- Niektóre operacje tworzenia lub modyfikacji plików systemowych, modyfikacji kont i praw dostępu.

Pułapki internetowe

Internetowa pułapka jest zbiorem elementów funkcjonalnych, które posługują się legalnym i uprawnionym oszustwem w celu odwrócenia uwagi potencjalnego intruza od rzeczywistych, wartościowych zasobów poprzez użycie zasobów fikcyjnych i skierowanie intruza do systemu gromadzenia informacji wiążących się z włamaniami oraz reagowania.

Pułapki internetowe

Zagadnienia techniczne:
- Wykrywanie działań, które są włamaniami
- Wykrywanie działań wyzwalających
- Odwołanie kwalifikacji zdarzeń jako włamania
- Pozostawanie w ukryciu

Przygotowanie pułapki
- Korespondencja od administratora
- Sfabrykowana pocztę
- Sfabrykowane punkty skanowania
- Fikcyjny plik haseł
- Komunikaty systemowe

Internetowe pułapki WWW

Pułapki WWW

http://*adres_pułapki*/http://*adres_pierwotny*

Problemy:
- Wiersz stanu przeglądarki
- Wiersz adresu
- Adresy URL wpisywane przez użytkownika
- Podgląd źródła dokumentu

Cel stosowania pułapek internetowych

- Poznanie sposobu działania intruza oraz uzyskanie informacji o technikach z jakich korzysta. Zdobytą wiedzę można użyć do lepszego zabezpieczenia sieci produkcyjnej.
- Zdobycie niepodważalnych dowodów włamania, które można wykorzystać do zlokalizowania włamywacza oraz w postępowaniu prawnym.

Umiejscowienie pułapek internetowych

- Tarcza (*shield*) - emulowanie niewykorzystywanych serwisów sieciowych na serwerach produkcyjnych.
- Pole minowe (*minefield*) - umieszczenie komputerów pułapek bezpośrednio między serwerami produkcyjnymi jako kolejnych maszyn.
- ZOO - całe wirtualne podsieci, które kuszą napastnika słabymi zabezpieczeniami.

Przesłanki decyzji o zastosowaniu pułapki

- Czy firma ma dostatecznie zasoby by pozwolić na dodatkowe maszyny pełniące role wabików?
- Czy jest ktoś, kto będzie czuwał nad logami i alarmami generowanymi przez system?
- Czy firma zamierza tropić i ścigać prawnie włamywaczy?
- Czy są dostępne odpowiednie środki by odpowiadać na atak?

Specter Intrusion Detection System

Emulowane systemy operacyjne:

- Windows NT
- Windows 98
- SunOS / Solaris
- NeXTStep
- Tru64 (Digital Unix)
- Linux
- Windows2000
- MacOS
- Digital Unix
- Irix
- Unisys Unix

- Konfigurowalny stopień zabezpieczeń emulowanych systemów (pięć poziomów)
- Emulacja plików z hasłami
- Konfigurowalny stopień trudności haseł (siedem poziomów)

Specter Intrusion Detection System

Emulowane serwisy:

- SMTP
- FTP
- Telnet
- Finger
- NetBios
- HTTP

Pułapki:

- POP3
- IMAP4
- DNS
- SUN-RPC
- BO2K
- SUB-7
- Generic

Verizon NetFacade

Emulowane serwisy:

- Cisco IOS
- Redhat Linux
- SunOS 4.1.4 dla Sun Sparc
- IRIX
- Solaris
- Microsoft Windows NT 4.0

Atrapy serwisów:

- FTP
- Telnet
- SMTP
- HTTP (Apache, Microsoft IIS, Netscape Ent.)
- SSH
- Echo
- IMAP
- Rlogin
- Portmap/tcpbind
- Finger
- Rusers
- Daytime
- Mountd

Reagowanie na incydenty

Reagowanie na incydenty składa się z decyzji i działań podejmowanych przez menedżerów zasobów w czasie rzeczywistym. Działania te mają na celu minimalizację wpływu incydentu *na zasoby* i zmniejszenie ryzyka ponownego naruszenia bezpieczeństwa. Podstawą podejmowanych decyzji i działań są dostępne świadectwa incydentu.

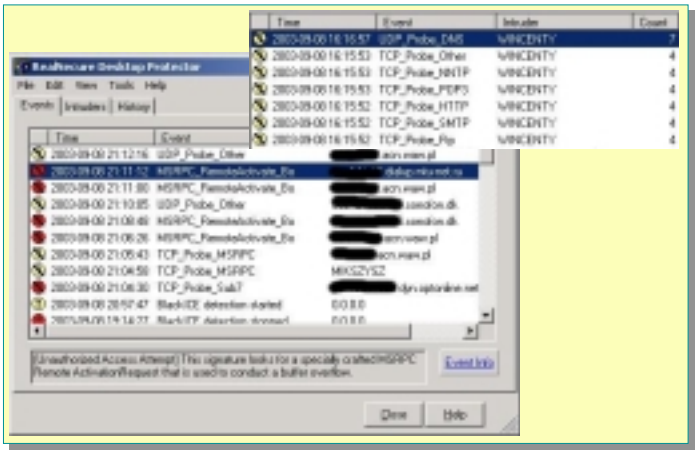
Czynniki decydujące o reakcji

- Jakie zasoby zostały uszkodzone? Czy mają one kluczowe znaczenie? Czy nastąpiło pogorszenie wydajności zasobu?
- Czy incydent wystąpił po raz pierwszy?
- Czy został wywołany przez źródło szkodliwe czy nieszkodliwe?
- Czy źródło informacji o incydencie jest wiarygodne?

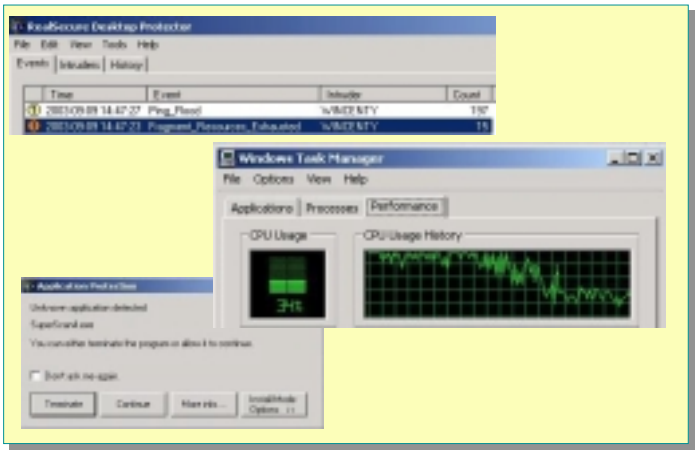
Czynniki decydujące o reakcji

- Jaki będzie skutek modyfikacji funkcji chronionego systemu? Czy ma to być wyłączenie wszystkich operacji? Czy ma to być odcięcie usług wewnętrznych czy zewnętrznych? Czy ma to być odcięcie usług dla zadanej lokalizacji (adresu)?
- Jakie będą skutki zaniechania działań? Ze względu na niepewność lub niemożność podjęcia decyzji często nie reaguje się na incydenty.
- Czy proponowana reakcja jest legalna i mieści się w ramach polityki bezpieczeństwa?

RealSecure Desktop Protector



RealSecure Desktop Protector



eTrust Intrusion Detection

eTrust Intrusion Detection