Для того, щоб уникнути або частково зменшити ймовірність успішної реалізації атаки типу «сканування файлової системи», можна розробляти захищені системи «з нуля», але, на жаль, прикладів таких систем небагато через складність і значну вартість проведення таких робіт. Лише TrustedXenix, TrustedMach, Harris CX/SX, XTS 300 STOP, а в Україні - ATMNIS вдалося створити системи, які в подальшому були сертифіковані на відповідність найвищим класам вимог.[2]

Як показала практика, модернізація існуючих систем є одним з найефективніших підходів для досягнення побудови захищених ОС. Перевагами цього методу є:

- менший обсяг робіт з розробки та реалізації системи;
- можливість збереження сумісності з існуючими рішеннями;
- модернізовані системи наслідують імідж систем-прототипів, а це підвищує довіру до них за рахунок відомості фірм-розробників і дозволяє використати наявний досвід експлуатації;
- економічна ефективність.

Типовими прикладами такого підходу є ОС TrustedSolaris та BBos.

При розробці захищеної ОС шляхом модернізації, слід розглядати користувача, не як довірену особу, яка є елементом схеми адміністрування і має можливість призначати/змінювати правила розмежування доступу, але й сприймати його як потенційного зловмисника, який може свідомо чи несвідомо здійснити несанкціонований доступ до інформації.[3] Для досягнення даної мети можна:

- додавати функції шифрування;
- розподіляти обов'язки адміністратора системи між різними обліковими записами;
- впроваджувати додаткові засоби ідентифікації.

В якості висновку можна зазначити що більшість сучасних універсальних ОС не виконують у повному обсязі вимоги що висуваються до захисту автоматизованих систем для оброблення конфіденційної інформації. Тому, вони не можуть бути використанні без додаткових засобів захисту та застосовуватися для захисту навіть не конфіденційної інформації. Утім, основні проблеми захисту викликані не тим, що розробниками не виконані окремі вимоги до механізмів захисту в ОС, а недосконалістю в реалізованих ОС концепцій захисту, розроблення яких потребує подальшого наукового дослідження.

Список використаних джерел

1. Блавацька Н.М. Аналіз відповідності засобів захисту сучасних операційних систем вимогам до оброблення конфіденційної інформації // Information Security of the Person, Society and State, № 2 (12), 2013
2. Захист інформації в операційних системах, базах даних і мережах [Електронний ресурс]. Режим доступу: http://its.kpi.ua/subjects/38/Documents/Конспект_Захист_інформації_2014.pdf
3. Корнієнко Б.Д., Щербак Л.О. Реалізація захисту інформації в ком'ютерних системах та мережах на основі операційної системи FreeBSD // Національний авіаційний університет «Захист інформації» [Електронний ресурс]. Режим доступу: http://jrnl.nau.edu.ua/index.php/ZI

УДК 004.056.2

СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ ЯК ІНСТРУМЕНТ ЗАХИСТУ ВІД КІБЕРАТАК

Лисиця Т.А., Яковлєв О.О., студ. гр. КБ-171
Петренко Т.А., ст. викладач кафедри кібербезпеки та математичного моделювання
Чернігівський національний технологічний університет

Сьогодні системи виявлення комп'ютерних атак (IDS - Intrusion Detection Systems) - один з найважливіших елементів систем інформаційної безпеки мереж будь-якого сучасного підприємства, враховуючи, як зростає в останні роки число проблем, пов'язаних з комп'ютерною безпекою. Хоча технологія IDS не забезпечує повний захист інформації, проте вона відіграє досить помітну роль в цій галузі. На відміну від брандмауера, який контролює тільки параметри сесії (IP, номер порту і стан зв'язків), IDS «заглядає» всередину пакета (до сьомого рівня OSI), аналізуючи дані, що передаються. Саме тому використання систем виявлення комп'ютерних атак є актуальним.

Система виявлення атак (вторгнень) — програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними, в основному через Інтернет. [1]

Вперше термін «виявлення атак» був введений Джеймсом Андерсеном в його роботі «Моніторинг і контроль загроз інформаційній безпеці», опублікованій в 1980 р. У цій роботі була висловлена гіпотеза про можливість виявлення загроз безпеки за допомогою збору та аналізу інформації, що міститься в журналах аудиту операційних систем.[2] На сьогоднішній день дослідженнями в даній сфері займаються такі українські вчені: Головко В.А, Д. Ю. Гамаюнов, І.В. Рубан, В.О. Мартовицький, С.О. Партика.

Будь-яка IDS включає в себе (Рис.1):

– сенсорну підсистему, яка постійно відстежує події, пов'язані з безпекою системи;

– підсистему аналізу, яка відбирає з усіх подій, обраних сенсором, підозрілі. IDS з активною підсистемою аналізу в разі виявлення підозрілої діяльності можуть вжити заходів у відповідь, пасивні IDS лише повідомлять адміністратору про підозрілий дії.

– сховище, яке нагромаджує первинні події і результати аналізу;

– панель управління, яка дає можливість користувачу відстежувати роботу системи.

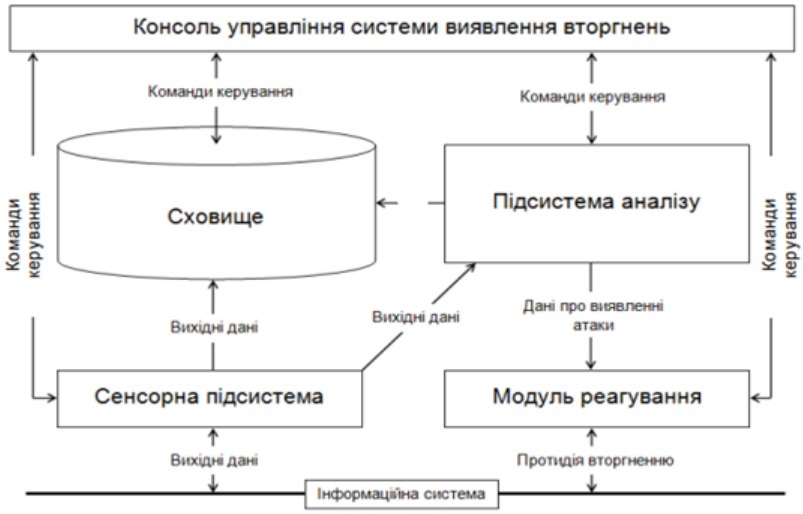

*Рис.1. Основні компоненти IDS[*3]

На українському ринку IDS – системи представлені:

– Cisco Systems - серія продуктів Cisco IDS містить рішення для різних рівнів. У неї входять три системи, серед яких 4210 оптимізована для середовища 10 / 100Base-T (45 Мбіт / с), 4235 - для середовища 10/100 / 1000Base -TX, (200 Мбіт / с) і 4250 - для 10/100 / 1000Base-TX (500 Мбіт / с).

– Internet Security Systems - компанія ISS свого часу зробила різкий стрибок в даній області і займає провідні позиції в частині реалізації систем виявлення атак. Аналізуючи мережевий трафік і зіставляючи його з базою сигнатур атак, сенсор виявляє різні порушення політики безпеки.

- Enterasys Networks – випускає IDS Dragon (типу network-based). Внутрішня архітектура шостої версії системи має підвищену масштабованість. Система включає компоненти централізованого моніторингу безпеки мережі в реальному масштабі часу Dragon Security Information Manager.

- Computer Associates - високоефективний і досить простий програмний продукт надає можливості моніторингу, виявлення атак, контролю за WWW-трафіком, ведення журналів. Бібліотека шаблонів атак регулярно оновлюється, і з її допомогою автоматично визначаються атаки.

- NFR Security - система NFR NID забезпечує моніторинг мережевого трафіку в реальному часі, виявляючи підозрілу активність, атаки, заборонене поводження в мережі і різні статистичні відхилення. Сенсори можуть працювати зі швидкостями 1 Гбіт / с і 100 Мбіт / с без втрат пакетів.

Snort – програма аналізує протокол передачі, виявляє різні атаки, наприклад, переповнення буфера, сканування, CGI-атаки, спроби визначення ОС і т. п.. Система проста в налаштуванні і обслуговуванні, однак в ній досить багато доводиться налаштовувати "вручну".

Підвиди IDS за методами виявлення атак:

– Метод аналізу сигнатур: В цьому випадку пакети даних перевіряються на наявність сигнатур атак. Сигнатура атаки - це відповідність події одному із зразків, що описують відому атаку. Цей метод досить ефективний, бо при його використанні повідомлення про помилкові атаки досить рідкісні.

– Метод аномалій: за його допомоги виявляються неправомірні дії в мережі і на хостах. На підставі історії нормальної роботи хоста і мережі створюються спеціальні профілі з даними про це. Потім в гру вступають спеціальні детектори, які аналізують події. За допомогою різних алгоритмів вони виробляють аналіз цих подій, порівнюючи їх з «нормою» в профілях.

– Метод політик: Ще одним методом виявлення атак є метод політик. Суть його - у створенні правил мережевої безпеки, в яких, наприклад, може вказуватися принцип взаємодії мереж між собою і використовуються при цьому протоколи. Складність полягає в непростому процесі створення бази політик.[4]

Система виявлення вторгнень має два основні завдання: аналіз джерел інформації і адекватна реакція, заснована на результатах аналізу. Для виконання цих завдань система IDS здійснює такі дії:

– моніторить і аналізує активність користувачів;

– займається аудитом конфігурації системи і її слабких місць;

– перевіряє цілісність найважливіших системних файлів, а також файлів даних;

– проводить статистичний аналіз станів системи, що базується на порівнянні з тими станами, які мали місце під час уже відомих атак;

– здійснює аудит операційної системи.

– Загальні способи обходу IDS

– Нестандартна фрагментація пакетів на рівнях IP, TCP або, наприклад, DCERPC, з якої IDS часом не здатна впоратися.

– Пакети з прикордонними або некоректними значеннями TTL або MTU також можуть оброблятися IDS некоректно.

– Неоднозначність сприйняття накладаються TCP-фрагментів (номерів TCP SYN) може трактуватися IDS інакше, ніж на сервері або клієнта, якому цей TCP-трафік призначався.

– Підставний пакет TCP FIN, наприклад з невірною контрольною сумою (т. Н. TCP un-sync), може бути сприйнятий як кінець сесії замість ігнорування.[5]

Вирішити ці проблеми можливо за рахунок повної бази сигнатур, що порівнюють пакети даних з сигнатурами відомих атак, а також обладнання, яке може аналізувати потік вхідних даних.

Проте, головна задача IDS полягає у виявленні та реєстрації атак, а також сповіщення при спрацьовуванні певного правила і покладатися лише на неї не можна.

Підводячи підсумок, можна зазначити що системи виявлення вторгнень це ефективний інструмент захисту користувача від різного роду несанкціонованих атак, проте не варто забувати, що якщо ми говоримо про повноцінну безпеки, IDS - всього лише елемент даної системи. Повноцінна безпека це: політика безпеки інтрамережі; система захисту хостів; мережевий аудит; захист на базі маршрутизаторів; міжмережевий екран; система виявлення вторгнень;політика реагування на виявлені атаки. І тільки правильно поєднуючи всі перераховані вище типи захисту, користувач може бути спокійний за безпеку зберігання і передачі важливих даних.

Список використаних джерел

1. IDS [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/IDS.
2. Что такое IDS? [Електронний ресурс] – Режим доступу до ресурсу: https://elhow.ru/kompjutery/kompjuternye-terminologii/chto-takoe-ids.
3. Системы обнаружения атак [Електронний ресурс] – Режим доступу до ресурсу: https://www.bytemag.ru/articles/detail.php?ID=6608.
4. Рубан І. В. Класифікація методів виявлення аномалій в інформаційних системах [Електронний ресурс] / І. В. Рубан, В. О. Мартовицький, С. О. Партика. – 2016. – Режим доступу до ресурсу: www.hups.mil.gov.ua/periodic-app/.../soivt_2016_3_24.pdf.
5. IDS - что это такое? Система обнаружения вторжений (IDS) как работает? [Електронний ресурс] – Режим доступу до ресурсу: http://fb.ru/article/186268/ids---chto-eto-takoe-sistema-obnarujeniya-vtorjeniy-ids-kak-rabotaet.

УДК 004.056.55

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ АНАЛІЗУ КЛАВІАТУРНОГО ПОЧЕРКУ

Мальцева М.В., студ.гр. КБ-161

Петренко Т.А., ст. викладач кафедри кібербезпеки та математичного моделювання

Чернігівський національний технологічний університет

У сучасному світі загальної інформатизації особливого значення набувають завдання захисту інформації. Основні проблеми захисту інформації при роботі з нею, можна умовно розділити на три типи: перехоплення інформації (порушення конфіденційності інформації), модифікація інформації (спотворення вихідного повідомлення або заміна іншою інформацією), підміна авторства (крадіжка інформації та порушення авторського права). Основною задачею безпеки інформаційних комп'ютерних систем є обмеження кола осіб, що мають доступ до конкретної інформації, і захисту її від несанкціонованого доступу.

Існує багато методів захисту інформаційних систем, такі як: фізичні, програмні та апаратні. Ці методи захисту інформації передбачають використання певного набору засобів.

Одними з найбільш перспективних і активно розвиваючих фізичних методів є метод біометричної аутентифікації. Біометричні системи аутентифікації - системи, що використовують для посвідчення особи людей їх біометричні дані. Біометрична аутентифікація - процес докази і перевірки автентичності заявленого користувачем імені, через пред'явлення користувачем свого біометричного способу і шляхом перетворення цього образу відповідно до заздалегідь певним протоколом аутентифікації. Біометричні системи розпізнають людей на основі їх анатомічних особливостей (відбитків пальців, способу особи, малюнка ліній долоні, райдужної оболонки, голоси) або поведінкових рис (підписи, ходи) [1]. Оскільки ці риси фізично пов'язані з користувачем, біометричний розпізнавання надійно в ролі механізму, що стежить, щоб тільки ті, у кого є необхідні повноваження, могли потрапити в будівлю, отримати доступ до комп'ютерної системи або перетнути кордон держави. Біометричні системи також мають унікальні перевагами - вони не дозволяють відректися від досконалої транзакції і дають можливість визначити, коли індивідуум користується декількома посвідченнями