УДК 004.056.5

ПРИЧИНИ, НАСЛІДКИ ТА СПОСОБИ ЗАПОБІГАННЯ КІБЕРАТАКАМ ТИПУ «СКАНУВАННЯ ФАЙЛОВОЇ СИСТЕМИ»

Куник В. І., студ. гр. КБ - 181
Петренко Т.А., ст. викладач кафедри кібербезпеки та математичного моделювання
Чернігівський національний технологічний університет

Протягом останніх десятиліть відбувається стрімкий розвиток інформаційних технологій та їх проникнення у всі сфери людської діяльності. В зв'язку з цим постійно зростає кількість злочинів в галузі інформаційної безпеки. Одним із напрямів в яких діють кіберзлочинці є кібератаки атаки з використанням уразливостей сучасних операційних систем. Аналізуючи результати дослідження аналітичної компанії RootShell (табл. 1 та рис. 1) можна зазначити, що найбільш поширеним типом кібератак на операційні системи залишається сканування файлової системи.

Таблиця 1 - Кількість успішних кібератак на критично-важливі інформаційні системи з використанням уразливостей операційних систем в країнах ЄС

Тип	Кількість за 2018 рік	%
Сканування файлової системи	324501	31,6
Викрадення ключової інформації	275635	24,1
Підбирання паролів	139924	19,8
Збирання сміття	108748в	10,6
Перевищення повноважень	93816	8,4
Програмні закладки	74762	5,5

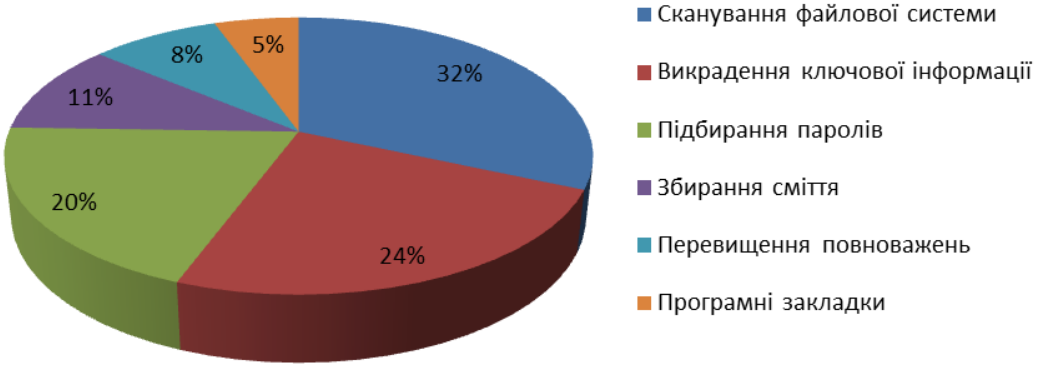

Рис.1. Співвідношення кількості успішних кібератак на критично-важливі інформаційні системи з використанням уразливостей операційних систем в країнах ЄС, 2018р.

В Україні питаннями захисту інформації на рівні операційних систем займається багато науковців. Серед них можна відзначити Н.М. Блавацьку, В.Г.Проскурина, С.В.Крутова, І.В.Мацкевича та інших. Багато з них прийшло до висновку що більшість сучасних операційних систем має дефекти у забезпеченні безпеки даних у системі, що зумовлено виконанням завдання забезпечення максимальної доступності системи для користувача. [1] Саме тому дослідження спрямовані на підвищення ефективності захисту інформації на рівні операційних систем є актуальними.

Як вже зазначалося, сканування файлової системи це одна з найбільш розповсюджених кібератак на рівні операційної системи, яка водночас є найнебезпечнішою для конфіденційності даних. Насамперед це атака на політику безпеки. Атака полягає в тому, що порушник, який має можливість переглядати (сканувати) всю файлову систему, намагається отримати доступ до файлів, прочитати та скопіювати їх. Крім читання та копіювання порушник може здійснити заміну або видалення файлів. Для такої атаки, зазвичай, використовується спеціальне програмне забезпечення. І що найцікавіше, будь-який легальний користувач системи може зробити це.[3]

Причинами виникнення такої загрози є насамперед погана захищеність ОС, пов'язана з недоліками засобів захисту:

- відсутність забезпечення замкнутості програмного середовища;
- некоректна реалізація механізму управління доступом;
- відсутність антивірусного програмного забезпечення;
- відкриті, незахищені порти;
- відсутність firewall.

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;