КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (19), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.19.96108
УДК 004.056.5:510.22(043.3)

Ільєнко Анна Вадимівна
Кандидат технічних наук, доцент, доцент кафедри комп'ютеризованих систем захисту інформації
Національний авіаційний університет університет, факультет кібербезпеки програмної інженерії,
Київ, Україна
ORCID ID: 0000-0001-8565-1117
ilyenko.a.v@nau.edu.ua

Ільєнко Сергій Сергійович
Кандидат технічних наук, доцент, доцент кафедри автоматизації та енергоменеджменту
Національний авіаційний університет університет, аерокосмічний факультет,
Київ, Україна
ORCID ID: 0000-0002-0437-0995
ilyenko.s.s@nau.edu.ua

Кваша Діана Сергіївна
випускниця кафедри комп'ютеризованих систем захисту інформації
Національний авіаційний університет університет, факультет кібербезпеки та програмної інженерії,
Київ, Україна
ORCID ID: 0000-0003-2299-2736
diana_kvasha@ukr.net

Мазур Яна Сергіївна
Асистент кафедри комп'ютеризованих систем захисту інформації
Національний авіаційний університет, факультет кібербезпеки та програмної інженерії,
Київ, Україна
ORCID ID: 0000-0003-0164-7124
yana.mazur@npp.nau.edu.ua

ПРАКТИЧНІ ПІДХОДИ ЩОДО ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Анотація. Розглядаючи інформаційно-телекомунікаційні мережі бачимо, що передача конфіденційних даних через Інтернет з кожним днем стає все більш частою, а тому, потрібно, щоб наші дані були надійно захищені від різних загроз, вразливостей, які кожного дня стараються отримати доступ до мережі та перехопити дані, знешкодити, отримати доступ до мережевих ресурсів. Саме тому, у наш час захист даних, програмного та апаратного забезпечення від вірусів, різних вразливостей є, як ніколи, необхідним, а не просто проблемою. Виходячи з даних міркувань необхідно як створення нових методів для захисту інформаційно-телекомунікаційних мереж, так і вдосконалення вже існуючих задля кращої безпеки мережі, адже одним із важливих елементів захисту інформації є саме захист мережі. Зважаючи на постійно зростаючу статистику кібератак на інформаційно-телекомунікаційні мережі, після глибокого аналізу та опрацювання зазначеної проблематики, автори статті висвітили сучасний стан забезпечення безпеки інформаційно-телекомунікаційних мереж та рішення щодо безпеки в інформаційно-телекомунікаційних мережах. Автори всебічно охопили та дослідили проблеми забезпечення безпеки в інформаційно-телекомунікаційних мережах, провели аналіз загроз та вразливостей, які завдають шкоди інформаційній мережі та провели дослідження методів протидії сучасним загрозам інформаційно-телекомунікаційних мереж. Також приділено увагу розробленню рішень щодо безпеки в інформаційно-телекомунікаційній мережі. Авторами планується ряд науково технічних рішень щодо розробки та впровадження ефективних методів щодо виявлення вразливостей та засобів щодо забезпечення вимог, принципів та підходів забезпечення безпеки інформаційно-телекомунікаційних мереж.

Ключові слова: мережа, шифрування, Suricata, правила, регістр зсуву, фаєрвол, вразливості.

ВСТУП

Безпека мережі — це процес вжиття фізичних і програмних профілактичних заходів для захисту основної мережевої інфраструктури від неавторизованого доступу, неправильного використання, несправності, модифікації, знищення або неналежного розголошення, таким чином створюючи безпечну платформу для комп'ютерів, користувачів і програм.

Найкращі методи управління вразливістю починаються з мережі. За визначенням, керування вразливістю мережі стосується всіх аспектів вашого середовища, кожного підключеного пристрою, операційної системи, апаратного забезпечення, програмного забезпечення, брандмауерів тощо. Незахищений маршрутизатор Wi-Fi, пристрій IoT із надмірним контролем доступу або неправильна конфігурація брандмауера можуть стати точкою входу для зловмисника у вашу систему. Сканування вразливостей мережі та регулярне встановлення виправлень є важливими, щоб переконатися, що перші лінії захисту зміцнені, зменшуючи ймовірність витоку даних.

Отже, інформаційно-комунікаційні технології (ІКТ) мають великий вплив на соціальний добробут, економічне зростання та національну безпеку в сучасному світі. Як правило, ІКТ включають комп'ютери, пристрої мобільного зв'язку та мережі. ІКТ також охоплює група людей зі зловмисними намірами , також відомих як мережеві зловмисники, кіберзлочинці тощо. Протистояння цій згубній кібердіяльності є одним із міжнародних пріоритетів і важливою областю досліджень.

Саме тому, постає питання реалізації та вдосконалення найбільш ефективних методів виявлення вразливостей в інформаційно-телекомунікаційних мережах.

Постановка проблеми. Застосовуючи сучасні технології, створюються чимало засобів та методів для виявлення вразливостей в інформаційно-телекомунікаційних мережах. Проводяться різні сканування мереж, моніторинг, проводять побудову підключень в мережі з найбільш ефективним результатом для компанії, підприємства чи організації. Зараз є доступно багато мережевих сканерів, які допоможуть просканувати як власну домашню мережу, так і мережу компанії, є різні утиліти, які здатні виявити вразливості в мережі, але постає питання, на скільки дані засоби та методи зможуть попередити про небажані загрози та захисти ваші дані. Саме тому, для ефективності забезпечення безпеки в інформаційно-телекомунікаційних мережах потрібно вдосконалення існуючих методів та створення власних рішень щодо виявлення вразливостей в інформаційно-телекомунікаційних мережах. В статтях [1] і [2] висвітлено основні проблеми, які постають в інформаційно-телекомунікаційних мережах, а в статтях [3-9,18,19] визначено основні дослідження методів протидії загрозам в інформаційно-телекомунікаційних мережах. **Метою статті** є дослідження сучасного стану забезпечення захисту інформації в інформаційно-телекомунікаційних мережах, що дає змогу проаналізувати основні проблеми, та висвітлити основні ідеї авторів щодо їх вирішення та запропонувати практичні підходи щодо виявлення вразливостей в інформаційно-телекомунікаційних мережах.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Характеристика сучасного стану забезпечення безпеки в інформаційно-телекомунікаційних мережах. На сьогоднішній день багато компаній страждають від численних проблем безпеки мережі, навіть не усвідомлюючи цього. Що ще гірше, коли ці проблеми залишаються невирішеними, вони можуть створювати можливості для зловмисників, щоб зламати інфраструктуру безпеки компанії, викрасти дані та загалом сіяти хаос. Існує надто багато потенційних проблем, але буде розглянуто кілька

найпоширеніших проблем безпеки мережі та представлено основні шляхи для їх вирішення.

*Проблема №1.*Невідомі ресурси в мережі.

Є багато компаній, які не мають повного переліку всіх IT-активів, які вони підключили до своєї мережі. Це величезна проблема. Якщо ви не знаєте про всі активи, що є у вашій мережі, як ви можете бути впевнені, що ваша мережа захищена. Найпростіше вирішити цю проблему — перевірити всі пристрої у вашій мережі та визначити всі платформи, на яких вони працюють. Роблячи це, ви можете дізнатися про всі різні точки доступу, що є у вашій мережі та які з них найбільше потребують оновлень безпеки.

Проблема №2. Зловживання правами облікового запису користувача.

Згідно з даними, наведеними *Harvard Business Review* , за 2016 рік «60% усіх атак було здійснено інсайдерами»[1].Незалежно від того, чи сталося це через чесні помилки (випадкове надсилання інформації на неправильну адресу електронної пошти чи втрату робочого пристрою), навмисні витоки та неправильне використання привілеїв облікового запису чи крадіжку особистих даних у результаті фішингової кампанії чи іншої атаки соціальної інженерії, яка компрометує дані облікового запису користувача, люди у вашій компанії представляють одну з найбільших проблем безпеки, з якою ви коли-небудь стикаєтесь.Оскільки ці загрози надходять від довірених користувачів і систем, їх також найважче виявити та зупинити.

Однак є способи мінімізувати ризик у разі внутрішньої атаки. Наприклад, якщо ваша компанія використовує політику найменших привілеїв (principle of least privilege - POLP), коли йдеться про доступ користувачів, ви можете обмежити шкоду, яку може завдати обліковий запис користувача, який використовується неправильно. У POLP доступ кожного користувача до різних систем і баз даних у вашій мережі обмежується лише тими речами, які потрібні для виконання їхньої роботи.

Проблема №3. Невиправлені вразливості безпеки.

Багато компаній стурбовані експлойтом «нульового дня». Ці експлойти — це ті невідомі проблеми з безпекою в програмах і системах, які ще не використані проти когось. Однак уразливості нульового дня не є проблемою — проблемою є невиправлені відомі вразливості. Як зазначено в одній онлайн-статті CSO [2] , «у 2015 році з'явилося близько 6300 унікальних уразливостей. Symantec каже, що лише 54 з них були класифіковані як нульові дні».

Це пояснюється тим, що коли використовується експлойт «нульового дня», його можна виявити — стати відомою проблемою, над якою постачальник програмного забезпечення може почати працювати. Чим частіше використовується експлойт, тим більша ймовірність його виявлення та виправлення. Також потрібно багато зусиль, щоб самостійно виявити абсолютно невідому вразливість в системі.

Тому зловмисники зазвичай бажають використовувати відомі експлойти. Насправді, як зазначено в статті CSO, «Звіт Verizon про порушення даних за 2016 рік показав, що з усіх виявлених експлойтів більшість походить від уразливостей, датованих 2007 роком. Наступним був 2011 рік» [2]. Іншими словами, вразливості, яким було майже десять років, спричинили більшість порушень у 2016 році. Найпростіший спосіб вирішити цю проблему — дотримуватися чіткого розкладу для оновлення системи безпеки. Крім того, поступова зміна програм і операційних систем у вашій мережі, щоб зробити їх однаковими, може спростити цей процес. Наприклад, якщо кожна система базується на Windows або Mac (а не на суміші Mac, Windows, Linux тощо), то вам потрібно лише відстежувати розклади виправлень системи безпеки Mac OS або Windows OS і сповіщень.

Проблема №4. Відсутність глибокого захисту.

Зрештою, незважаючи на всі ваші зусилля, настане день, коли зловмиснику вдасться зламати безпеку вашої мережі. Однак те, яку шкоду може завдати цей зловмисник, залежить від структури мережі.

Проблема полягає в тому, що деякі підприємства мають відкриту мережеву структуру, де як тільки зловмисник потрапляє в надійну систему, він має необмежений доступ до всіх систем у мережі.

Якщо мережу структуровано з сильною сегментацією, щоб усі її окремі частини були розділеними, тоді можна уповільнити зловмисника настільки, щоб не допустити його до життєво важливих систем, поки ваша команда безпеки працює над виявленням, локалізацією та усуненням зламу.

Проблема №5. Недостатнє управління безпекою IT.

Ще одна поширена проблема для багатьох компаній полягає в тому, що навіть якщо вони мають усі найкращі рішення з кібербезпеки, у них може бути недостатньо людей для належного керування цими рішеннями.

Коли це станеться, критичні сповіщення про кібербезпеку можуть бути пропущені, а успішні атаки можуть бути не усунені вчасно, щоб мінімізувати шкоду.

Дослідження методів протидії сучасним загрозам інформаційно-телекомунікаційних мереж. Методи протидії безпеки безпосередньо пов’язані з такими параметрами, які зберігаються у вигляді мережевих помилок або вразливостей та їхніх наслідків у мережі зв’язку. Проаналізувавши вплив цих параметрів, ми можемо вибрати кілька ключових методів протидії безпеки для мережі.

Вибір і впровадження цих методів протидії в мережевому середовищі залежить від команди адміністратора мережі. Це залежить від їхніх основних знань і обізнаності про мережу, стандартну мережеву архітектуру, параметри трафіку у вигляді поведінки програми (знання мережевих протоколів рівня OSI та TCP/IP і написання правил для безпеки мережі), продуктивність мережевого обладнання, загрози безпеці та наявні слабкі місця в мережі . Приблизні або застарілі знання можуть стати причиною мережевих помилок і вразливостей.

Враховуючи наведену вище інформацію, багато дослідницьких організацій призначили деякі найважливіші ключові методи протидії безпеки для мережевої інфраструктури стандартного рівня[8].

Політика безпеки. Надійна політика безпеки виконує ефективну роль у мережі. Якщо політика розробляється після аналізу мережі та поведінки її компонентів, це призводить до значно безпечнішої та безперебійної мережі.

Авторитет ресурсів. Авторизація систем або мережевих ресурсів відіграє важливу роль у протидії безпеці. Після ретельного огляду мережі ми можемо призначити відповідний рівень повноважень для доступу до ресурсів системи. Політика антивірусної програми або список контролю доступу маршрутизатора чи брандмауера можуть визначити повноваження для доступу до мережевих ресурсів належним чином.

Виявляти шкідливі дії. Наявність системи виявлення вторгнень відіграє важливу роль у протидії безпеці. Вивчення та аналіз файлів журналу на наявність шкідливих дій у мережі може врятувати систему. Він забезпечує простий підхід до безпеки від багатьох інших шкідливих цілей.

Пом'якшити можливі напади в мережі. Симптоми зловмисної атаки дають нам уявлення про те, який тип захисту потрібен для системи від цієї атаки. Ми можемо перенастроїти або переконфігурувати параметри нашої системи безпеки, створивши потужний бар’єр проти атаки.

Виправляти основні проблеми. Вирішуючи основні проблеми в системі чи мережі,

ми можемо врятувати систему чи мережу. Ці базові, але ключові проблеми в основному є прихованою точкою, яка існує в будь-якій звичайній мережі чи системі, як-от неправильне оновлення системних програм, застарілі програми та оновлення вірусних патчів (не вчасно), все це може створити недолік безпеки в будь-якій мережі.

Що стосується інструментів протидії безпеки, то до них відносяться 1) *криптографічні методи захисту*, а саме безпечні протоколи IPSec та SSL; 2) *система виявлення вторгнень (IDS)*, яка дозволяє виявляти будь-який несанкціонований доступ або вторгнення в систему чи мережу. Це рішення безпеки, яке має пасивну позицію в системі чи мережі проти цих вторгнень. У розгортанні мережі функцією IDS є моніторинг трафіку або мережевої активності без впливу на трафік [10,11]; 3) *система запобігання вторгненням (IPS), яка* виконує роль захисту від вторгнень, які відбуваються в мережі або локальній системі. Вона працює на основі виведення файлів системного журналу IDS. З цієї причини можна сказати, що система IPS є розширенням системи IDS; 4) *затосування фаєрволу*. Брандмауер – це бар'єр, який виконує ізоляцію між двома різними мережами або системами. Він вирішує, який тип трафіку може проходити через мережу та в якому напрямку. Брандмауери забезпечують додатковий рівень системи захисту, надаючи можливості додавати набагато жорсткіші та складніші правила зв’язку між різними сегментами чи зонами мережі. Брандмауер може містити лише одну систему або складатися з кількох систем. Що стосується його ролі в мережевій безпеці, то він забезпечує захист однієї мережі від іншої мережі, адже архітектура з’єднання брандмауера в мережі полягає в тому, що він створює бар’єр між двома мережами. Для цього він повинен мати принаймні два мережеві інтерфейси, один для мережі, яка призначена для захисту, а інший для мережі, яка піддається впливу [13]. Фаєрвол слугує захистом внутрішньої мережі від зовнішньої; 5) *Suricata* – це спеціалізоване програмне забезпечення для аналізу мережі та виявлення загроз із відкритим кодом, яке використовується більшістю приватних і державних організацій і впроваджується великими постачальниками для захисту своїх активів.

Як бачимо, кожен з розглянутих методів протидії сучасним загрозам має як свої переваги, так і недоліки. Про те, дані методи дозволяють забезпечити надійний захист для мережі, різниця лише в тому, в якій мірі ефективно це вдається зробити кожному з них і яких зусиль потрібно для цього докласти. На основі дослідження, було виділено два найбільш ефективних методи, а саме використання фаєрвола та Suricata. Що стосується фаєрвола, то в його основі лежить застосовування як алгоритмів шифрування, так і написання правил, що є ефективним рішенням для захисту мережі. Коли ж говоримо про Suricata, то тут застосовується також влучне поєднання двох методів, а саме IDS та IPS, що також сприяє підвищенню безпеки мережі та безперебійному її функціонуванні.

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ .

Розглянувши основні проблеми, проаналізувавши загрози та вразливості інформаційно-телекомунікаційних мереж та дослідивши методи протидії цим загрозам було виділено два методи, які несуть у собі більш потужний захист і можливості задля збереження наших даних від втручання зловмисників, забезпечення конфіденційності та безпечного функціонування інформації в мережі великих організацій, державних установ, об’єктів критичної інфраструктури.

Брандмауер є найпоширенішою технологією для захисту внутрішніх активів. Його основна мета — контролювати вхідний і вихідний мережевий трафік шляхом аналізу пакетів даних і прийняття того, чи слід його пропускати, чи ні, на основі попередньо визначеного набору правил.

Мережне шифрування захищає дані, що переміщуються через комунікаційні мережі. Стандарт SSL (рівень захищених сокетів) (технологія, що лежить в основі символу замка в браузері та більш правильно називається безпекою транспортного рівня [TLS]) [14]— це форма захисту мережевих даних за замовчуванням для Інтернет-зв'язку. Багато компаній, які піклуються про безпеку, йдуть далі й захищають не лише свій Інтернет-трафік, але й внутрішні мережі, корпоративні магістральні мережі та віртуальні приватні мережі (VPN) за допомогою шифрування на рівні мережі.

Однак, як і будь-який низькорівневий метод безпеки, шифрування даних на рівні мережі є досить грубим інструментом. Мережа майже повністю не бачить цінності даних, що передаються через неї, і відсутність цього контексту зазвичай налаштована на захист або всього, або нічого. І навіть якщо використовується підхід «захистити все», потенційний зловмисник може отримати цінну інформацію з моделей мережевого трафіку.

Шифрування даних під час їх переміщення мережею є лише частиною комплексної стратегії шифрування мережевих даних. Організації також повинні враховувати ризики для інформації в її джерелі — перед її переміщенням — і в кінцевому пункті призначення. Тому, постає питання про вибір метода шифрування у інформаційно-телекомунікаційній мережі.

Розглянувши можливості брандмауерів в попередньому пунктів, ми бачимо, що захист мережі побудований на створенні конфігурації на обладнання та написанні відповідних правил, а саме дозволів та заборон на отримання доступу. Таким чином, даний метод в інформаційно-телекомунікаційній мережі (ІТМ) слугує як ефективний засіб виявленню вразливостей та створенню належної безпеки мережі.

Проаналізувавши дані можливості на фаєрволах та врахувавши особливості побудови захищеної мережі, пропонується застосування потокового шифрування на базі регістра зсуву з лінійним зворотним зв'язком (РЗЛЗЗ).

Даний метод полягає у створенні алгоритму потокового шифрування, де байт за байтом перетворює звичайний текст у код, який неможливо прочитати без належного ключа.

Потокові шифри є лінійними, тому один і той самий ключ шифрує та розшифровує повідомлення. Усі криптографічні методи спрямовані на кодування даних, щоб приховати їх від сторонніх. Але на відміну від своїх аналогів, потокові шифри працюють з кожним бітом даних у повідомленні, а не розбивають повідомлення на групи та шифрують їх блоками.

Реалізація самого методу застосування потокового шифрування на базі регістра зсуву з лінійним зворотним зв'язком (РЗЛЗЗ) до фаєрволу з використанням PyCharm Community Edition 2021.2.2 має наступний алгоритм роботи, а саме:

1.Генерація псевдовипадкової послідовності РЗЛЗЗ.

2.Тестування отриманої псевдовипадкової послідовності за допомогою тестів FIPS-140-1.

3.Перевірка прав отримання доступу до маршрутизатора.

4.Виявлення вразливостей в мережі.

ISSN 2663 - 4023

5.Коректне завершення роботи програми.

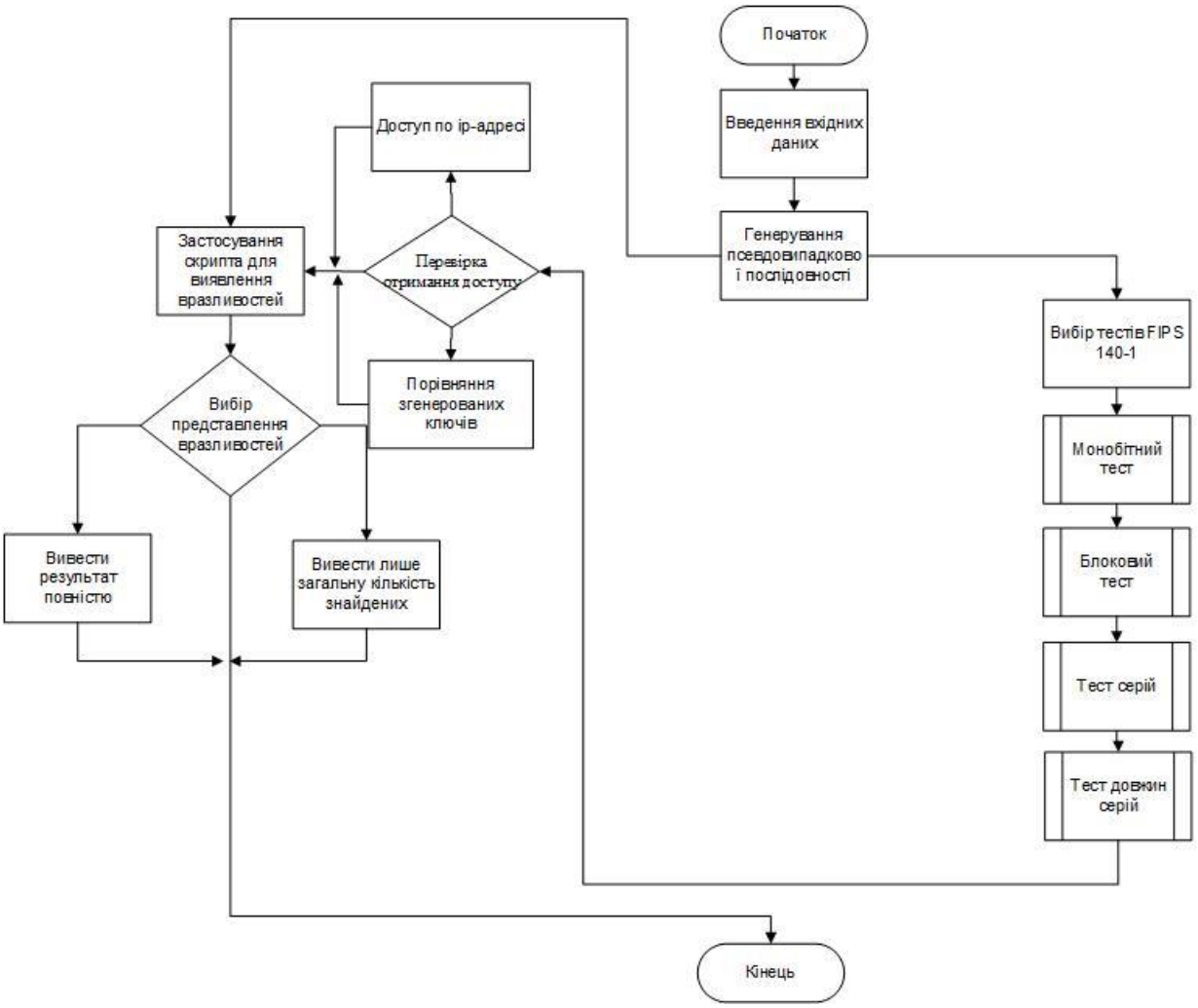

Рис.1. Блок-схема першого виявлення вразливостей в інформаційно-телекомунікаційних мережах

В даному випадку, це буде перекривати один із недоліків фаєвола, а саме вдасться таким чином приховати локальну мережу з мережі Інтернет. Всі дані, які передаються з локальної мережі, та в локальну мережу будуть приховані та, якщо, під час їх передачі будуть спостерігатися певні вразливості, то вони будуть швидко виявленні та опрацьовані. Як бачимо, на рис.2 представлена схема застосування потокового шифрування в інформаційно-телекомунікаційній мережі. Вся інформація, яка надходить від локальної мережі і проходить перевірку правил у фаєрволі буде зашифрована у вигляді двійкового коду. Також, за допомогою тестів FIPS 140-1 буде проходити перевірка доступу до проміжного обладнання та перевірка на вразливості при спробі виходу в Internet і, відповідно, така ж перевірка буде проходити при отриманні даних безпосередньо в локальну мережу. Тобто, всі дані, які по каналам зв'язку виходять з локальної мережі та надходять в локальну мережу з інших ресурсів, інтернету, проходять перевірку на вразливості, автентифікацію та при цьому є зашифрованими.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (19), 2023
ISSN 2663 - 4023

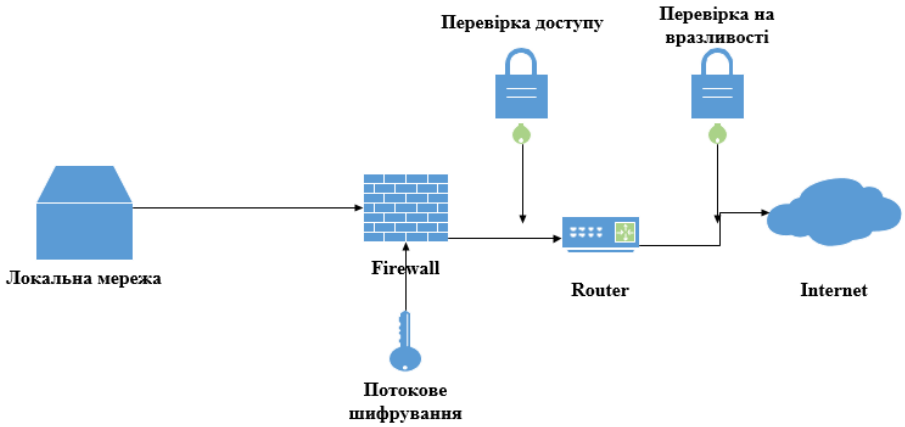

Рис.2. Застосування потокового шифрування в ІТМ

Що стосується другого методу виявлення вразливостей в інформаційно-телекомунікаційній мережі, то було обрано використання системи виявлення і попередження мережевих вторгнень, а саме Suricata (рис.3).

```
  GNU nano 5.4                                /home/diana/suricataparser/kvasha.rules
alert udp $HOME_NET any → any 53 (msg: "TThreatHunter Rule -  Observed DNS Query to public CryptoMining pool Domain (xmrpool.eu)"; conten>
alert dns $HOME_NET any → any any (msg: "TThreatHunter Rule -  Observed DNS Query to public CryptoMining pool Domain (ppxxmr.com)"; dns_q>
alert udp $HOME_NET any → any 53 (msg: "TThreatHunter Rule -  Observed DNS Query to public CryptoMining pool Domain (ppxxmr.com)"; conten>
alert dns $HOME_NET any → any any (msg: "TThreatHunter Rule -  Observed DNS Query to public CryptoMining pool Domain (alimabi.cn)"; dns_q>
alert udp $HOME_NET any → any 53 (msg: "TThreatHunter Rule -  Observed DNS Query to public CryptoMining pool Domain (alimabi.cn)"; conten>
alert dns $HOME_NET any → any any (msg: "TThreatHunter Rule -  Observed DNS Query to public CryptoMining pool Domain (aeon-pool.com)"; dn>
alert udp $HOME_NET any → any 53 (msg: "TThreatHunter Rule -  Observed DNS Query to public CryptoMining pool Domain (aeon-pool.com)"; con>
alert udp $HOME_NET any → $EXTERNAL_NET 53 (msg: "TThreatHunter Rule -  Suspicious dns request"; flow:established,to_server; content:"|01>
alert icmp any any → any any (msg: "TThreatHunter Rule -  ICMP Tunnel Detection Of Type Eight"; icode:0; itype:8; content:!"|101112131415>
alert icmp any any → any any (msg: "TThreatHunter Rule -  ICMP Tunnel Detection Of Type Zero"; icode:0; itype:0; content:!"|1011121314151>
alert tcp any any → any any (msg: "TThreatHunter Rule - "Hacker backdoor or shell  Microsoft Corporation"; flow:to_server,established; co>
alert tcp any any → any any (msg: "TThreatHunter Rule - "Hacker backdoor or shell Microsoft Windows"; flow:established; content:"|4D 69 6>
alert http any any → any any (msg: "TThreatHunter Rule -  **Windows Powershell Request UserAgent**"; flow:established; content:"PowerSh>
alert http any any → any any (msg: "TThreatHunter Rule -  **Linux wget/curl download .sh script**"; flow:established,to_server; content>
alert http $EXTERNAL_NET any → $HOME_NET any (msg: "TThreatHunter Rule - "Suspicious netstat command traffic"; flow: established,to_clien>
alert tcp $HOME_NET any → any any (msg: "TThreatHunter Rule - "http GET data"; flow: established;  content:"|47 45 54|"; depth: 10; conte>
alert tcp any any → any any (msg: "TThreatHunter Rule -  System Information Collection By Trojan"; flow:to_server; content:"GET"; http_me>
alert tcp $HOME_NET any → $EXTERNAL_NET any (msg: "TThreatHunter Rule -  Cryptocurrency Miner Check By Submit"; flow:to_server,establishe>
alert tcp $EXTERNAL_NET any → $HOME_NET any (msg: "TThreatHunter Rule -  Pools Response Cryptocurrency Miner"; flow:to_client,established>
alert http any any → any any (msg: "TThreatHunter Rule -  msfconsole powershell response"; flow:established; content:!"<html>"; content:!>
alert tcp $HOME_NET any → any 3306 (msg: "TThreatHunter Rule - "mysql general_log write file"; flow: established;  content:"|03|"; depth:>
alert http $EXTERNAL_NET any → $HOME_NET any (msg: "TThreatHunter Rule - "Weevely PHP Backdoor Response"; flow: established,to_client; co>
alert http $EXTERNAL_NET any → $HOME_NET any (msg: "TThreatHunter Rule - "Weevely PHP Backdoor Response"; flow: established,to_client; co>
alert http $HOME_NET any → $EXTERNAL_NET any  (msg: "TThreatHunter Rule - "Powershell Empire HTTP Request "; flow: established, to_server>
alert http $EXTERNAL_NET any → $HOME_NET any (msg: "TThreatHunter Rule - "Powershell Empire HTTP Response "; flow: established,to_client;>
alert http any any → any any (msg: "TThreatHunter Rule -  webshell_caidao_php"; flow:established; content:"POST";http_method; content:".p>
alert http $EXTERNAL_NET any → $HOME_NET any (msg: "TThreatHunter Rule - "China hacker tools caidao response - column directory"; flow: e>

^G Help      ^O Записать  ^W Поиск     ^K Cut       ^T Execute   ^C Location  M-U Отмена    M-A Set Mark
^X Выход     ^R ЧитФайл   ^\ Замена     ^U Paste     ^J Выровнять ^_ К строке  M-E Повтор    M-6 Copy
```

Рис.3. Вивід створених правил на виявлення вразливостей

Suricata – це безкоштовний механізм виявлення мережевих загроз із відкритим кодом, який забезпечує виявлення вторгнень, запобігання вторгненням і моніторинг безпеки мережі. Проект Suricata керується спільнотою та зосереджується на безпеці, зручності та ефективності, а також належить і підтримується Open Information Security Foundation (OISF). Suricata відрізняє себе від інших подібних механізмів виявлення мережевих загроз, таких як Snort 1, забезпечуючи багатопотоковість, що забезпечує кращу продуктивність [16]. Крім того, мова правил Suricata полегшує зіставлення умов у протоколі прикладного рівня без глибшого розуміння структури пакетів і протоколів.

Підписи або правила є важливим аспектом Suricata, оскільки це те, що IDS використовує для виявлення підозрілих дій у мережі. Адміністратор може використовувати існуючі набори правил, такі як надані OISF, але також можна

ISSN 2663 - 4023

створювати власні підписи або змінювати існуючі [17].

Отже, після проведених досліджень, можна сказати, що створення правил та застосування їх використовуючи Suricata сприяє швидкому та ефективному способу отримання інформації про те, що відбувається в інформаційно-телекомунікаційній мережі з детальною інформацією, на скільки це можливо, про зловмисника.

На основі даних тестувань було проведено моніторинг результатів швидкодії та кількості виявлених вразливостей в інформаційно-телекомунікаційній мережі, а саме було досліджено швидкодію та кількість знайдених за відповідний час вразливотей до застосування розроблених методів та після їх впровадження.

Як бачимо з рис.3 та рис.4 , при впровадженні розроблених методів маємо кращі показники як швидкодії, так і кількості виявлених вразливостей.

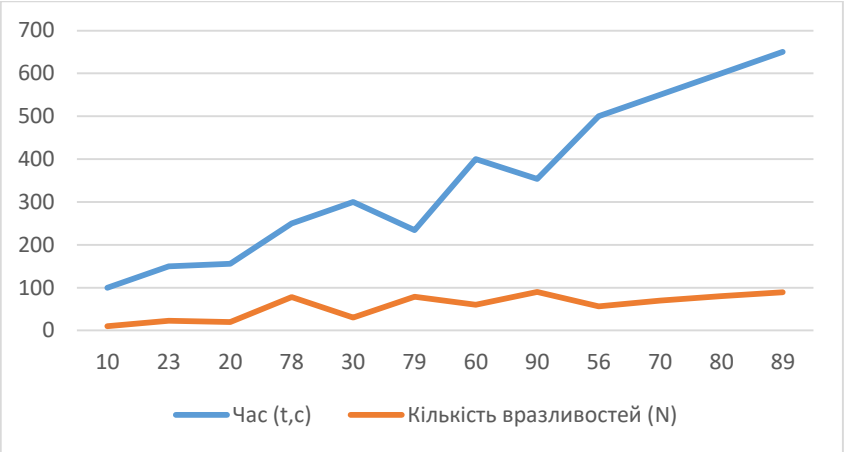

Рис.4.Залежність швидкодії від кількості виявлених загроз в ІТМ до впровадження методів виявлення вразливостей

За графіками можемо спостерігати, що до впровадження методів (рис.3) час пошуку вразливостей суттєво зростав, при цьому загальна кількість знайдених вразливостей за відповідний час навіть зменшувалась, а мала б зростати, так як час на їх пошук збільшувався, тому на графіку можемо бачити «падіння», що говорить про те, що потрібно покращувати дані методи виявлення вразливостей, щоб графік був стабільний і витрачалось менше часу на пошук вразливостей.

Відповідно, коли було впроваджено власні розроблені методи, моніторинг показав, що ситуація дещо покращилась (рис.4). Звичайно є певні «падіння», але не такі значні як були до впровадження методів. При цьому, за допомогою правильно розробленому алгоритму дій, який закладено в основу кожного із запропонованих методів вдалось навіть дещо зменшити час пошуку вразливостей, але при цьому збільшити кількість знайдених вразливостей, що є дуже ефективно, коли говоримо про великі організації. Виходячи з результатів наведених на графіках (рис.4, рис.5) було сформовано загальний графік залежності швидкодії та кількості виявлених загроз в інформаційно-телекомунікаційних мережах до впровадження методів та після їх впровадження (рис.6), де було представлено загальну кількість потраченого часу на виявлення вразливостей та загальну кількість виявлених вразливостей за цей час.

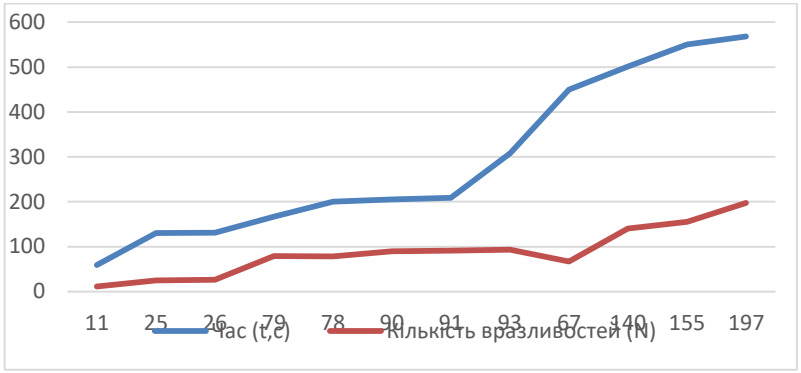

Рис.5. Залежність швидкодії від кількості виявлених загроз в ІТМ після впровадження методів виявлення вразливостей

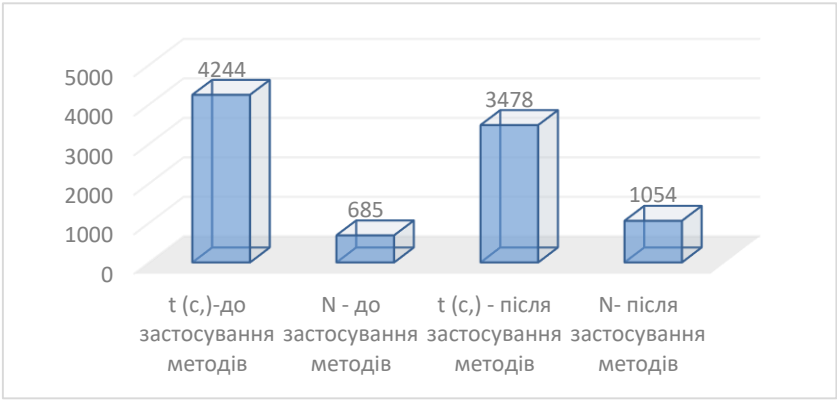

Рис.6. Діаграма швидкодії та кількості виявлених загроз до та після впровадження методів виявлення вразливостей

Як бачимо, на діаграмі наочно видно, що швидкодія до використання методів становить 4244 секунди (1 год. 18 хв.) і при цьому було знайдено 685 вразливостей в мережі. Після впровадження розроблених методів було витрачено 3478 секунд (58 хвилин) та знайдено 1054 загрози. Відповідно, швидкодія після впровадження методів знизилась на 766 секунд (13 хвилин), а кількість знайдених вразливостей при цьому збільшилась на 369, що ще раз говорить про те, що дані методи є доцільними для їх впровадження в інфомаційно-телекомунікаційну мережу.

ВИСНОВКИ

Підсумовуючи викладене в даній статті, можна сказати, що на сьогоднішній день безпека мережі відіграє все більшу роль. Майже кожного дня велика компанія чи звичайний користувач стикаються з проблемами у власній мережі. Зрозуміло, що ресурси для захисту у підприємства, мережа якого має масштаби утричі більші, чим наша домашня мережа є дороговартісними і потужними. Сюди відносяться як і маршрутизатори з відповідною конфігурацією для безпеки, і фаєрволи з особистими правилами, і різні сканери, які все швидко фіксують, коли ж в домашнього користувача є загальні сканери, які доступні, а деякі навіть і цим не користуються та можуть тривалий час і не знати, що їх мережа відкрита для будь-яких впливів, і дані, що в ній циркулюють стали вже не конфіденційними.

Відповідно, на основі даних міркувань, було розглянуто можливі методи виявлення

вразливостей в інформаційно-телекомунікаційній мережі, зроблено їх порівняльний аналіз та обрано два найбільш ефективних методи, які здатні виявити вразливості та забезпечити надійний захист мережі як для великої компанії так і для звичайного домашнього користувача.

В статті запропоновано програмний застосунок виявлення вразливостей з використанням PyCharm Community Edition 2021.2.2, за рахунок впровадження потокового шифрування до фаєрвола та конфігурування правил Suricata. Удосконалено процес виявлення вразливостей в інформаційно-телекомунікаційних мережах, за рахунок впровадження методу потокового шифрування на базі регістра зсуву з лінійним зворотним зв'язком та вдосконалення методу застосування правил Suricata, що дозволяє показати адекватність їх роботи та доцільність використання в інформаційно-телекомунікаційних мережах і зменшити час на виявлення загроз до 1,22 разів та збільшити кількість виявлених загроз до 1,53 разу. Дані методи було протестовано, показано результати захисту даних в мережі та виявлення вразливостей. Це все допоможе швидко аналізувати дії, які відбуваються в мережі, а не чекати поки сканери все просканують і нададуть результати, адже чим довше ми не можемо справитись з проблемою, тим більше ресурсів вона встигає захопити і тим більше втрат ви понесете.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 The Biggest Cybersecurity Threats Are Inside Your Company. https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company.
2 Zero-days aren’t the problem -- patches are. https://www.csoonline.com/article/3075830/zero-days-arent-the-problem-patches-are.html.
3 Glossary of Internet Security Terms http://www.auditmypc.com/glossary-of-internet-security-terms.asp.
4 Introduction to Computers/System Software-Wikiversity. http://en.wikiversity.org/wiki/Introduction_to_Computers/System_software.
5 Lai, Y.-P., Hsia, P.-L. (2007). Using the vulnerability information of computer systems to improve the network security. *Computer Communications*, *30*(9), 2032–2047. https://doi.org/10.1016/j.comcom.2007.03.007
6 Guideline for the analysis of LAN Security. http://www.itl.nist.gov/fipspubs/fip191.htm.
7 Computer System Laboratory Bulletin. http://csrc.nist.gov/publications/nistbul/csl94-03.txt.
8 Idaho National Laboratory.Control System Cyber Security; Defence in Depeth Strategies//external report # INL/EXT-06-11478.
9 Stallings, W. (2003). *Network security essentials: Applications and standards* (2-ге вид.). Pearson Education.
10 Beale, J., Baker, A. R., Esler, J., Kohlenberg, T., Northcutt, S. Snort: IDS and IPS toolkit.
11 Firewall. http://www.vicomsoft.com/knowledge/reference/firewalls1.html.
12 What is Network Encryption? https://cpl.thalesgroup.com/faq/encryption/what-network-encryption.
13 Stream Cipher. https://www.okta.com/identity-101/stream-cipher/.
14 What is suricata? https://blogs.opentext.com/category/technologies/security/.
15 Suricata rules. https :// suricata.readthedocs.io/en/suricata - 6.0.2/rules/intro.html, n.d.
16 Ilyenko , A., Ilyenko , S., Vertypolokh , O. (2020). МЕТОД ЗАХИСТУ ТРАФІКУ ВІД ВТРУЧАННЯ DPI СИСТЕМ НА БАЗІ ВИКОРИСТАННЯ DOH ТА DOT ПРОТОКОЛІВ. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2*(10), 75-87. https://doi.org/10.28925/2663-4023.2020.10.7587
17 Ilyenko , A., Ilyenko , S., Kravchuk, I., Herasymenko , M. (2022). ПЕРСПЕКТИВНІ НАПРЯМКИ АНАЛІЗУ ТРАФІКУ ТА ВИЯВЛЕННЯ ВТОРГНЕНЬ НА ОСНОВІ НЕЙРОМЕРЕЖ. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1*(17), 46-56. https://doi.org/10.28925/2663-4023.2022.17.4656

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (19), 2023
ISSN 2663 - 4023

Ilyenko Anna
Candidate of Technical Sciences, assistant professor , assistant professor of Information Security Systems Department National Aviation University of Kyiv, Faculty of Cyber Security and Software Engineering, Ukraine
ORCID ID: 0000-0001-8565-1117
ilyenko.a.v@nau.edu.ua

Ilyenko Sergii
Candidate of Technical Sciences, assistant professor , assistant professor of Automation and Energy Management Department National Aviation University of Kyiv, Aerospace Faculty, Ukraine
ORCID ID: 0000-0002-0437-0995
ilyenko.s.s@nau.edu.ua

Kvasha Diana
Master of CyberSecurity, Information Security Systems Department
National Aviation University of Kyiv, Faculty of Cyber Security and Software Engineering, Ukraine
ORCID ID: 0000-0003-2299-2736
diana_kvasha@ukr.net

Mazur Yana
Assistant of Information Security Systems Department National Aviation University of Kyiv, Faculty of Cyber Security and Software Engineering, Ukraine
ORCID ID: 0000-0003-0164-7124
yana.mazur@npp.nau.edu.ua

PRACTICAL APPROACHES TO DETECTING VULNERABILITIES IN INFORMATION AND TELECOMMUNICATION NETWORKS

Abstract. Looking at information and telecommunication networks, we see that the transmission of confidential data via the Internet is becoming more frequent every day, and therefore, it is necessary that our data be reliably protected from various threats, vulnerabilities that every day try to gain access to the network and intercept data, neutralize, gain access to network resources. That is why, in our time, protecting data, software and hardware from viruses and various vulnerabilities is more necessary than ever, and not just a problem. Based on these considerations, it is necessary both to create new methods for protecting information and telecommunication networks, and to improve existing ones for better network security, because one of the important elements of information protection is network protection itself. Taking into account the constantly growing statistics of cyber attacks on information and telecommunication networks, after in-depth analysis and processing of the mentioned issues, the authors of the article highlighted the current state of ensuring the security of information and telecommunication networks and solutions regarding security in information and telecommunication networks. The authors comprehensively covered and investigated the problems of ensuring security in information and telecommunication networks, conducted an analysis of threats and vulnerabilities that harm the information network, and conducted research on methods of countering modern threats to information and telecommunication networks. Attention is also paid to the development of security solutions in the information and telecommunications network. The authors plan a number of scientific and technical solutions for the development and implementation of effective methods for detecting vulnerabilities and means for ensuring the requirements, principles and approaches for ensuring the security of information and telecommunication networks.

Keywords: network, encryption, Suricata, rules, shift register, firewall, vulnerabilities.

REFERENCES

1 The Biggest Cybersecurity Threats Are Inside Your Company. https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company.
2 Zero-days aren't the problem -- patches are. https://www.csoonline.com/article/3075830/zero-days-arent-the-problem-patches-are.html.
3 Glossary of Internet Security Terms http://www.auditmypc.com/glossary-of-internet-security-terms.asp.
4 Introduction to Computers/System Software-Wikiversity. http://en.wikiversity.org/wiki/Introduction_to_Computers/System_software.
5 Lai, Y.-P., Hsia, P.-L. (2007). Using the vulnerability information of computer systems to improve the network security. Computer Communications, 30(9), 2032–2047. https://doi.org/10.1016/j.comcom.2007.03.007
6 Guideline for the analysis of LAN Security. http://www.itl.nist.gov/fipspubs/fip191.htm.
7 Computer System Laboratory Bulletin. http://csrc.nist.gov/publications/nistbul/csl94-03.txt.
8 Idaho National Laboratory.Control System Cyber Security; Defence in Depeth Strategies//external report # INL/EXT-06-11478.
9 Stallings, W. (2003). Network security essentials: Applications and standards. Pearson Education.
10 Beale, J., Baker, A. R., Esler, J., Kohlenberg, T., Northcutt, S. Snort: IDS and IPS toolkit.
11 Firewall. http://www.vicomsoft.com/knowledge/reference/firewalls1.html.
12 What is Network Encryption? https://cpl.thalesgroup.com/faq/encryption/what-network-encryption.
13 Stream Cipher. https://www.okta.com/identity-101/stream-cipher/.
14 What is suricata? https://blogs.opentext.com/category/technologies/security/.
15 Suricata rules. https :// suricata.readthedocs.io/en/suricata - 6.0.2/rules/intro.html, n.d.
16 Ilyenko , A., Ilyenko , S., Vertypolokh , O. (2020) *Method for protection traffic from intervention of dpi systems. Cybersecurity: Education, Science, Technique, 2*(10), 75-87. https://doi.org/10.28925/2663-4023.2020.10.7587
17 Ilyenko , A., Ilyenko , S., Kravchuk, I., Herasymenko , M. (2022). Prospective directions of traffic analysis and intrusion detectionbased on neural networks. *Cybersecurity: Education, Science, Technique, 1(*17), 46-56. https://doi.org/10.28925/2663-4023.2022.17.4656