Харківський національний університет імені В.Н. Каразіна

Факультет комп'ютерних наук

Безпека інформаційних систем і технологій

«Допущено до захисту»

Зав.кафедрою БІСТ

Сватовський І.І._____

« » червня 2023р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

спеціальність: 125 Кібербезпека

на тему: «Визначення структури і змісту основних завдань сценарної хмари HoneyPot та моделювання її поведінкових реакцій на прикладах типових мережевих атак»

оцінка « »

Голова ЕК

Лемешко О.В. _____

Керівник к.т.н. Малахов С.В._____
(прізвище та ініціали/підпис)

Рецензент Гостев О.Л._____
(прізвище та ініціали/підпис)

Виконавець студент групи КБ-41

Михайленко Д.Д._____
(прізвище та ініціали/підпис)

Харків – 2023

РЕФЕРАТ

Пояснювальна записка містить: 58 сторінок, 9 рисунків, 8 таблиць, 54 використаних джерел, 1 додаток.

Мета роботи: - визначення структури та змісту поведінкових реакцій тестового імітатору Honeypot (HP) на прикладах типових мережевих атак.

Об’єкт дослідження: - технології і засоби активного захисту актуальним загрозам інформаційної безпеки (ІБ).

Предмет дослідження: - поведінкові сценарії зворотних реакцій імітатору HP при парируванні найбільш поширених різновидів мережевих атак.

Основними методами досліджень є аналіз та комп’ютерне моделювання.

В роботі досліджено питання методів порушення параметрів штатного функціонування мережевого обладнання сучасних корпоративних мереж та проаналізовано статистику використання таких методів. Розглянуто концепцію активного захисту та наведено особливості функціонування та впровадження технологій активного захисту на прикладі мережі Honeynet. Визначені можливі напрями використання технологій штучного інтелекту (AI) та машинного навчання (ML) для реалізації поведінкових реакцій системи Honeypot. Імітаційне моделювання зворотних реакцій Honeypot виконано на прикладі реалізації спрощеної (тестової) мережевої структури в умовах відтворення кількох найбільш поширених різновидів мережевих атак. Наведено приклад системи фільтрації трафіку HP. Програмний імітатор HP, реалізовано на мові програмування Python із використанням бібліотек scapy та re. Розглянуті механізми зворотних реакцій HP відповідають визначеному переліку атак.

Результати роботи можуть бути використані в освітніх цілях та, як допоміжний (довідковий) матеріал для розширення рівня професійної обізнаності персоналу підрозділів з ІБ.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, МЕРЕЖЕВІ АТАКИ, АКТИВИНИЙ ЗАХИСТ, HONEYPOT, HONEYNET, ШТУЧНИЙ ІНТЕЛЕКТ.

ABSTRACT

The explanatory note contains: 58 pages, 9 figures, 8 tables, 54 references, 1 appendix.

Purpose of the study: - Determination of the structure and content of behavioral reactions of the Honeypot (HP) test simulator on examples of typical network attacks.

Object of research: - technologies and means of active defense against current information security (IS) threats.

Subject of research: - Behavioral scenarios of HP imitator's response to the most common types of network attacks.

The main research methods are analysis and computer modeling.

The paper investigates the issue of methods of violating the parameters of the normal functioning of network equipment of modern corporate networks and analyzes the statistics of the use of such methods. The concept of active protection is considered and the peculiarities of functioning and implementation of active protection technologies are presented on the example of the Honeynet network. Possible directions of using artificial intelligence (AI) and machine learning (ML) technologies to implement the behavioral reactions of the Honeypot system are identified. Simulation modeling of Honeypot feedback is performed on the example of implementing a simplified (test) network structure in the conditions of reproducing several of the most common types of network attacks. An example of HP traffic filtering system is presented. The HP software simulator is implemented in the Python programming language using the scappy and re libraries. The considered HP response mechanisms correspond to a certain list of attacks.

The results of the work can be used for educational purposes and as auxiliary (reference) material to expand the level of professional awareness of the personnel of IS departments.

Keywords: INFORMATION SECURITY, NETWORK ATTACKS, ACTIVE DEFENSE, HONEYPOT, HONEYNET, ARTIFICIAL INTELLIGENCE.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ СКОРОЧЕНЬ І ТЕРМІНІВ

ПЗ	–	Програмне забезпечення;
ІБ	–	Інформаційна безпека;
СЗІ	–	Системи захисту інформації;
Malware	–	Malicious software;
Botnet	–	robot network;
MITM	–	Man In The Middle;
DNS	–	Domain Name System;
ARP	–	Address Resolution Protocol;
IP	–	Internet Protocol;
SYN	–	Synchronize Sequence Number;
SQL	–	Structured Query Language;
SSL	–	Secure Sockets Layer;
XSS	–	Cross Site Scripting;
БД	–	База Даних;
DOM	–	Document Object Model;
Email	–	Electronic mail ;
HP	–	Honeypot;
ACL	–	Access Control List
DMZ	–	Demilitarized Zone
OSI	–	Open Systems Interconnection
HTTP	–	HyperText Transfer Protocol
ICMP	–	Internet Control Message Protocol
MME	–	Media Mediation Element
ШІ	–	Штучний інтелект
AI	–	Artificial Itelligence

ВСТУП

Виникнення та поширення Інтернету в усі сфері діяльності сучасної людини призвело до збільшення кількості спроб порушення штатного функціонування (тобто те, що передбачено експлуатаційною документацією) використовуваного програмного забезпечення (ПЗ) та/або устаткування, як окремих вузлів, так і цілих мереж. Шкода від успішних атак (зламів) систем росте щорічно [1]. За таких умов спеціалістам у сфері інформаційної безпеки (ІБ) потрібно постійно розробляти нові методи боротьби зі зловмисниками задля мінімізації наслідків мережевих атак.

Запропонована у кінці XX сторіччя ідея активного захисту [2] була розроблена задля надання переваги тим, хто займається проектуванням та супроводом систем захисту інформації (СЗІ). Бурхливі темпи розвитку цього методу явно вказують на потребу усієї профільної спільноти мати додаткові інструменти для більш оперативного та ефективного запобігання та вивчення дій мережевих злочинців (хакерів). Першим вагомим кроком стало винайдення системи Honeypot (HP) [3]. Така система пригорнула увагу фахівців з ІБ та почала впроваджуватися у СЗІ. На основі даної технології було створено низку інших подібних, котрі отримали загальну назву Cyber Deception.

Аналіз відомостей, стосовно найбільш резонансних інцидентів ІБ, свідчить про те, що злочинці розробляють нові способи для зламу інформаційних систем та виявляють інтерес до таких сфер людської діяльності, як державне управління, медицина, банківська сфера тощо.

Одним із перспективних рішень, щодо покращення показників захищеності системи є впровадження методик активного захисту, як складової загальної СЗІ. Тому розгляд питань, щодо можливостей протидії загрозам, які спричиняють матеріальних збитків власникам інформації, є безумовно

актуальним питанням для спеціалістів з ІБ, та потребує детального аналізу концепції активної оборони й проведення відповідних досліджень.

1 ОГЛЯД ІНЦИДЕНТІВ ТА СУЧАСНОГО СТАНУ АТАК НА МЕРЕЖЕВІ РЕСУРСИ РІЗНИХ ГРУП КОРИСТУВАЧІВ

1.1 Перелік та структуризація найпоширеніших атак

Як свідчить аналіз відомих інцидентів безпеки за останні 5 років найчастіше каналом витоку даних є мережа Internet, а зловмисниками найчастіше виступають співробітники компаній, що мають доступ до даних із обмеженим доступом та треті особи. Спостерігається стале зростання обсягу компрометованих даних, перш за все – персональної інформації користувачів[4]. За результатами узагальнення можна стверджувати, що дії, що спричиняють витоки чи пошкодження даних[5] діляться на декілька основних груп (різновидів), що мають свої характерні цільові аудиторії (жертви атак) та характерні методики їх реалізації. Причому до найбільш поширених різновидів атак можна віднести наступні: Фішинг, Malware, DoS, MITM, SQL Injections, XSS, Bruteforce, DNS-spoofing.

Фішингові атаки – тип атаки, при якому жертву обманом змушують завантажити malware чи перейти до підробної веб-сторінки[6]. Найчастіше, ціллю такої атаки є викрадення конфіденційних даних, зараження пристрою програмою для добутку криптовалют (т.з. «miner software») чи приєднання жертви до цільової BotNet для здійснення подальших атак. Найчастіше, використовується email-spoofing, при якому зловмисник видає себе за довірену особу та змушує видати конфіденційну інформацію. Серед найпоширеніших технік також виділяють spear-phishing [7] та whaling [8]. Для запобігання атак даного типу потрібне коректне налаштування корпоративних почтових сервісів (spam filters), розробка політки безпеки, що визначає порядок обміну інформації у межах персоналу.

Атаки типу "людина посередині" (MITM) – атака, при якій зловмисник отримує змогу до перехоплення трафіку жертви. При цьому, зловмисник може

переглядати, модифікувати або блокувати трафік, що йде до жертви[9]. Дана особливість реалізується, коли атакуючому вдається видати себе за вузол-ретранслятор між жертвою або жертвами. Дана атака може бути проведена через використання методів спуфінгу (DNS spoofing, ARP spoofing, IP spoofing, HTTPS spoofing). Отримавши доступ до мережевого трафіку, хакер має можливість вводити в оману інших користувачів, виконуючи раніше вказані методики спуфінгу, крім того стають доступні такі атаки, як: SSL Stripping, Session hijacking, Eavesdropping [10]. Використання криптографічно захищених каналів передачі інформації, перевірка автентифікації вузлів дозволяє організувати захист від подібного роду атак.

DoS атаки – до даного класу атак відносяться дії, метою яких є ізоляція жертви від оточуючого середовища[11]. До даних атаки належать [12]: дії, що блокують трафік після проведення MITM атаки, Smurf-attack, SYN-flood. Однак, якщо при атаці використовуються потужності не одного вузла, а мережі зловмисних пристроїв то такі атаки мають назву Distributed Denial of Service (тобто, DDoS-атаки)[13]. Залучення до атаки інших вузлів у рази підвищує ефективність внаслідок збільшення обчислювальних потужностей та фізичних лімітів об’єму трафіку, що може бути згенеровано.

SQL-ін'єкції – атака, що спрямовані на бази даних. Метою може бути внесення змін або несанкціонований доступ до даних. При здійсненні атаки експлуатується популярна вразливість недостатнього підтвердження автентичності (валідації) вводу користувача [14-15]. У полі вводу, хакер намагається сформувати запит до бази даних (БД) сервера, який потрібно виконати. Для виконання атаки потрібно знати на якій БД працює сервер. Дану задачу атакуючий вирішує на етапі попередньої мережевої розвідки (рекогносцировки) із використанням таких інструментів як nmap [16].

Атаки на міжсайтовий скриптинг (XSS) – Атаки, що спрямовані на виконання зловмисного програмного коду від імені жертви[17]. Як і у випадку SQL-injection, можуть бути здійснені при використанні вразливості недостатньої

валідації вводу користувача. Атаки поділяють на Відбиті (Reflected) XSS, Збережені (Stored) XSS, XSS що базуються на DOM (DOM based XSS) [18].

Атаки грубої сили(Brute-Force) – Атаки грубої сили спрямовані на переборі комбінацій для виявлення конфіденційних даних[19]. Ціллю атаки можуть бути пароль, логін, номер або інші дані кредитної картки. Атаки можуть виконуватись у поєднанні із методами соціальної інженерії [20]., наприклад, якщо хакер вгадує пароль жертви, знаючи день народження, ім'я домашніх улюбленців та іншу інформацію, що може бути частиною пароля.

Список перерахованих атак є невичерпним, оскільки щодня вдосконалюються старі та створюються нові способи та техніки зламу інтернет-ресурсів та ресурсів користувачів.

1.2 Статистика використання атак на мережеві ресурси

У роботі [21] наведено поточну ситуацію (на початок 2023 року), стосовно тенденцій розвитку та використання атак на мережеву інфраструктуру. Згідно зі звітами таких компаній, як CrowdStrike [22], Verizon Data Breach Investigations [23], найбільший інтерес представляють державні установи, медицина, освіта, банківська справа [24-26]. Наслідками реалізації відповідних атак, стають часткове або повне виведення зі строю ключових для держави інтернет-ресурсів, таких як державний реєстр, органи судочинства та виконавчої влади, офіційні портали тощо. Однак найнебезпечнішим (за обсягами та наслідками) є виток даних користувачів. Такі дані збираються у відповідні БД та активно продаються у «тіньовому» інтернет [27]. Згідно зі статистикою [28], найбільшою популярністю користуються номера банківських карток, персональні дані окремих користувачів. Однак, окрім цього, на таких «тіньових магазинах» активно проходить купівля-продаж програмного забезпечення (ПЗ), що використовується при проведенні кібератак[29].

Найбільший попит має ПЗ для отримання функцій віддаленого управління пристроями потенційної жертви атаки (комп'ютер, гаджети, мережеве устаткуванням тощо), в основі яких найчастіше використовуються такі атаки, як MITM, XSS, SQL injection та Brute-force. Для викрадення конфіденційних даних

найчастіше використовуються Malware [30], яке активно використовуються як хакерами-початківцями, так і досвідченими злочинними організаціями.

Так наприклад, Owasp Top Ten [31] надає лист найактуальніших вразливостей, використання яких є базою для здійснення наступних атак: XSS, Brute-Force, DDoS. Тому, у рамках даної роботи буде розглянуто саме ці атаки. Також, буде надано відповідну увагу атаці, що працює на рівні локальних мереж, що є не меншою загрозою – ARP spoofing.

2 МОЖЛИВОСТІ ТЕХНОЛОГІЙ АКТИВНОГО ЗАХИСТУ МЕРЕЖЕВИХ РЕСУРСІВ ТА АНАЛІЗУ ДІЙ АТАКУЮЧОЇ СТОРОНИ

2.1 Основні ідеї моделі активного захисту

Темпи зростання числа кіберзагроз, постійний винахід та удосконалення технік зламу ПЗ ставлять сторону захисту у вкрай невигідне становище. Необхідність збору відомостей про нові тенденції світу кіберзагроз змушує фахівців у галузі ІБ постійно шукати нові можливі атаки та методи, якими зловмисник може скористатися для заподіяння шкоди. Крім того, система реагування на інциденти безпеки побудована таким чином, що розслідування та притягнення до відповідальності відбувається вже після завдання збитків. Це надає хакерам суттєвий запас часу на підготовку атаки, що забезпечує певну перевагу атакуючій стороні. Також, вдосконалення методів захисту інформації має ретроспективний характер, оскільки інформація про наявні загрози стає доступною лише після реалізації цих загроз безпеки [32-33], що обумовлює появу нових технологій захисту, наприклад XDR [34-35].

У противагу цьому, з'явилася ідея переходу від класичної (пасивної) моделі захисту до активної моделі. Активний захист - це нова модель захисту, яка передбачає використання технологій, що намагаються спровокувати зловмисників до виявлення та введення їх в пастку, замість того, щоб тільки захищати систему від вторгнень. Ця модель базується на активній взаємодії зловмисника (або ресурсів зловмисника, наприклад бот-системи та/або бот-мережі) та системи захисту потенційної жертви, де система захисту «намагається» змінити спосіб дій зловмисника або перехопити його дії. Це досягається шляхом використання таких технологій Honeypots і Honeynets [36], що створюють штучні пастки для зловмисників та намагаються перехопити їх дії. Ця модель передбачає навмисну обфускацію ПЗ та/або заздалегідь підготовленої інформації, що захищається, шляхом введення додаткових

компонентів, які представляють інтерес для кіберзлочинців. Під обфускацією мається на увазі ускладнення системи захисту задля створення для атакуючої сторони додаткових труднощів при аналізі цих компонентів (тобто при атаці ресурсу). Недоліком методу активного захисту, в певної мірі (що залежить від кваліфікації атакуючого), може стати необхідність введення додаткових компонентів, які представляють інтерес для кіберзлочинців, що може бути менш ефективно із точки зору безпеки ніж пасивні методи захисту (антивірусне ПЗ, система виявлення та запобігання вторгненням - IDS/IPS, Firewalls тощо). Тому слід розглядати таку модель як корисне доповнення до традиційних методів захисту, задля посилення загального рівня захисту від інформаційних загроз, і першим з таких компонентів став саме Honeypot.

2.2 Огляд технології Honeypot

Honeypot – це програма або система, що імітує реальний ресурс котрий призначений для того, щоб максимально привернути увагу зловмисників. Зазвичай Honeypot (HP) створюється таким чином, щоб бути «привабливим» для атак, але при цьому не містити справжньої інформації або функцій, які можуть бути використані зловмисниками в подальшому. Ця особливість досягається внаслідок відкритості ресурсу для сканування та повної зовнішньої автентичності наявних відомостей і впроваджуваних процедур їх оригіналам, проте не представляє практичного інтересу для добропорядних користувачів.

HP складається з трьох основних компонентів, а саме:

- сервер, якій налаштований таким чином, щоб виглядати як справжній ресурс і водночас мати заздалегідь визначені «прогалини» (локальні процедурні пастки) в своєї безпеці;
- компонент прослуховування трафіку, що має виявляти аномальну поведінку користувачів та перенаправляти трафік зловмисників до окремого серверу-пастки;
- систему збереження подій, що відбуваються у Honeypot.

При проведенні атаки, HP збирає дані про використовуване обладнання, інструменти та дії, що спрямовані на завдання шкоди. Таким чином стає

доступним активний аналіз дій зловмисника на етапі їх проведення, а не після здійснення атаки, що дозволяє стороні захисту завчасно та/або своєчасно реагувати на загрози, що виникають. Ідея HP була вперше запропонована в роботі "The Cuckoo's Egg" Кліффа Столла, який в 1986 році створив систему, яка імітувала комп'ютер в його лабораторії ІБ. В результаті, він зібрав велику кількість інформації про хакерську групу, яка використовувала його систему для здійснення атак на різні комп'ютерні мережі. З того часу ідея HP стала популярною серед фахівців з ІБ і використовується для захисту різних систем і ресурсів в Інтернеті.

У залежності від типу загроз, Honeypots поділяють на [37]:

- Email trap or Spam trap;
- Decoy Database;
- Malware Honeypot;
- Spider Honeypot.

Можливі зворотні реакції HP називають сценарним полем. Сценарне поле відрізняється залежно від характеру взаємодії з хакером, місця розгортання, обсягом параметрів конфігурації тощо [38]. Наприклад, можуть використовуватися такі захисні поведінкові реакції, як: - маршрутизація трафіку, збільшення часу очікування, зміна інтерфейсних параметрів, імітація вразливості, імітаційне шифрування доступного контенту та ін. При цьому, маршрутизація трафіку передбачає обмеження доступу до певних ресурсів або встановлення фільтрів для трафіку. Збільшення часу очікування передбачає умисне уповільнення роботи системи, щоб дати хакеру видимість успішної атаки. Зміна параметрів містить у собі переналаштування тих компонентів, які можуть бути використані для ідентифікації системи або параметрів інтерфейсу користувача (мова, час, геолокація тощо). Імітація вразливості передбачає створення вразливостей, які здаються реальними, але насправді не мають жодного практичного значення.

Місце розгортання HP, також, може вплинути на сценарне поле. Наприклад, Honeypot, розташований у віртуальному просторі, може бути

використаний для спостереження за взаємодією хакера з системою та не передбачати зворотних реакцій. Водночас, HP розташований на окремому пристрої (вузлі), може використовуватися для більш активної взаємодії з хакером задля уточнення деталей його дій (параметрів та методики атаки).

Межі цієї технології обмежуються конфігурацією HP, що розгортається.

Система HP здатна аналізувати і ефективно реагувати на загрози безпеки, тільки якщо цій ресурс виглядає досить правдоподібно, щоб привернути увагу хакера, а також підтримує досить широке сценарне поле для адекватного реагування на можливі дії нападників. Однак слід мати на увазі, що такий ресурс навіть при коректному налаштуванні може бути розкрито та використано (скомпрометовано) проти основної системи яка захищається, тобто модель активного захисту, яку використовує Honeypot, не є повноцінним та завершеним рішенням для захисту комп'ютерних мереж і окремих вузлів.

2.3 Сутність технології Cyber Deception

Ідея використання мережевих «пасток» продовжила свій розвиток та трансформувалася у технологію Cyber Deception, яка використовує додаткові дані, як відповідні пастки для хакера. Найосновнішими є [39]:

- Honeypot;
- Honeytoken – дані, що привертають увагу хакерів, проте використання яких є маркером присутності у системи злочинця;
- Honeyport – порт, підключення до якого слугує маркером початку атаки (*або мережевої розвідці*) на систему;
- Honeynet – об’єднання декількох технологій пасток в одну загальну мережу, що створює комплексну систему-пастку.

Таким чином створюється обфусковане середовище, де сторона захисту може теж атакувати хакера, вводячи в оману та змушуючи видавати свої дані та марно витрачати час. На сьогодні така система описується як «гра» між сторонами атаки та захисту, а процеси такої гри можна розкрити з точки зору теорії ймовірностей, а саме теорії ігор. Такий підхід дає можливість більш ефективно розуміти та аналізувати мережеві процеси, що відбуваються при

захисті ресурсів основної - цільової системи. Це дозволяє змогу усвідомити, як кожна сторона процесу (атаки і захисту) може посилити свої можливості та зменшити потенціальні ризики в ході такої гри. Крім того, за допомогою теорії ігор можна дослідити різні стратегії атаки та захисту, що дозволяє удосконалити існуючі та розробляти більш ефективні методики, методи, засоби та заходи безпеки. [40-41].

Існують ряд компаній [42-44], що активно займаються розробкою та впровадженням відповідних систем, які збирають власну базу знань, що постійно оновлюється та надають актуальну інформацію профільним спеціалістам, наприклад:

- Mitre Shield;
- Attivo ThreatDefend Deception and Response Platform;
- Illusive Shadow;
- CounterCraft Cyber Deception Platform,
- Fidelis Deception platform

2.4 Узагальнення можливостей AI при реалізації Static та Dynamic HP для покращення параметрів захисту

З попередньої публікації автора даної роботи[45] відомо, що при використанні HP, адміністратору з безпеки необхідно провести налаштування середовища HP для максимальної схожості з реальним (тим, що імітується) джерелом, оскільки в іншому випадку зловмисник швидко зрозуміє, що має справу лише з аватаром бажаного ресурсу. Тому, для підтримки актуального стану зворотних реакцій HP, після його розгортання необхідно забезпечувати постійний моніторинг поточної мережевої активності, що забезпечить вчасне детектування проявів діяльності хакера, та гарантує превентивне реагування на його деструктивні дії, навіть на перших фазах атаки. Фахівці, які контролюють функціонування HP, змушені постійно стежити за змістом відповідних log-файлів, що в умовах розгалуженої корпоративної інфраструктури, призводить до значних витрат сил адміністратора подібної системи, та збільшенню витрат на її утримання з боку власника ресурсу, що захищається. Ці ускладнення можуть

бути значно спрощені при використанні можливостей штучного інтелекту та «Machine Learning» (ML) [46]. HP, що здатні адаптуватись під особливості їх мережевого оточення, без втручання людини, називають «Dynamic Honeypots».

В роботі [47] її автори наводять порівняльну характеристику «Static» та «Dynamic HP» що представлено у Таблиці 2.1. З наведених відомостей слід, що «Dynamic HP» не вимагає втручання людини та не потребує специфічних знань і навичок зі сторони персоналу, тобто в цьому випадку, фахівець з ІБ «перекладає» частину своєї роботи на штучний інтелект (AI). Такий HP складається із трьох модулів, що реалізують:

- збір даних;
- конфігурування системи/засобу HP;
- первинне розгортання HP.

Таблиця 2.1 – Порівняльна характеристика Static та Dynamic HP

Функція	Static	Dynamic
Поведінка	Фіксована	Змінюється автоматично у залежності від поточного стану
Адаптивність	Система не підлаштовується під дії зловмисника	Адаптується у залежності від дій зловмисника та стану оточуючого середовища
Людські зусилля	Потребує переналаштування	Не потребує переналаштування
Компетентність персоналу	Потребує навичок та досвіду	Не потребує навичок та досвіду

У роботі [48] автори розглядають, як штучний інтелект може допомагати адміністратору з ІБ, та виділяють 2 різні підходи:

1) Expert system. Система шукає подібний випадок ІБ у наявній БД, щоб реагування було актуальним саме для конкретної ситуації. Таким чином, чим більше сигнатур атак є в базі – тим більш адекватна зворотна реакція подібної системи/засобу.

2) Case based reasoning. Система прийматиме рішення на основі отриманого досвіду попередніх загроз. Відомості, що зберігаються в БД, містяться у вигляді кейсів в парадигмі «Питання - рішення». Даним підходи часто користуються служби підтримки.

Однак, попри досить великі теоретичні напрацювання, на практиці, «Dynamic HP» тільки починають з'являтися на ринку відповідних рішень ІБ. Наявні пропозиції або полегшують вирішення конкретних завдань (наприклад, DMARC – аналізатор поштових повідомлень, що перешкоджає спуфінгу та фішингу), або знаходяться на етапі розробки (Sphinx project). Загальною рисою є те, що усі компоненти «Dynamic HP» є власністю компанії. Користувачеві, в цьому разі, може бути доступна лише гнучка конфігурація окремих елементів, а потрібний функціонал та перелік елементів системи може змінити лише група розробників цього рішення. Таким чином, якщо існуюче рішення не задовольняє кінцевого користувача по одному з пунктів, то він змушений шукати інший продукт, оскільки налаштування HP в цьому випадку неможливе. Крім того, через авторське право, незалежний аудит даної HP, також неможливий. Адміністратору ІБ залишається лише довіритись розробнику, в тому, що всі елементи HP є надійними та не мають вразливостей.

Таким чином, можна констатувати, що на практиці більш зручним та надійнішим є рішення, яке може конфігуруватися безпосередньо обслуговуючим персоналом, тобто її кінцевим користувачем HP. На цей час існують Open Source HP [49], автори яких охоче діляться вихідним кодом своїх рішень. Загальний принцип роботи системи, яка повністю доступна для користувальницької конфігурації, представлено на Рис. 2.1 В даному прикладі, управління HP здійснює безпосередньо штучний інтелект (AI-Artificial Intelligence), при цьому адміністратору ІБ (Administrator) доступний повний log-файл взаємодії. У випадку, якщо AI не здатний протидіяти (тобто інцидент є унікальним для його поведінкових алгоритмів) атаці хакера (на рис.2.1 позначено як, Hacker), то адміністратор може особисто здійснювати контроль над HP. Крім того, лише адміністратор модифікує основний ресурс, що захищається (Defended Node),

оскільки основне завдання AI в цій схемі, це спростити роботу адміністратора, а не замінити його. При даній організації взаємодії, AI управляє HP за допомогою «AI-HoneyPot interaction module», суть якого полягає в наступному:

1) Передача відомостей про поточний стан системи HP (засобу);

2) Збір даних про реакції AI на загрози (телеметрія спрацювань);

3) Контроль санкціонування доступу до управління HP (якщо адміністратору потрібно втрутитися в процес конфігурації HP, то йому буде надана ця можливість. Інакше управління здійснює AI).

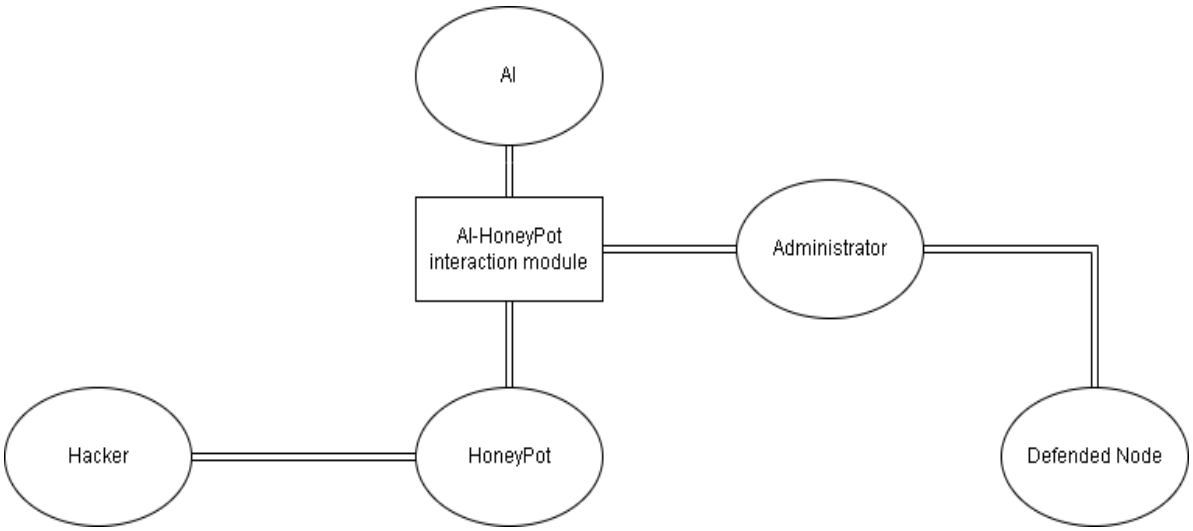


Рисунок 2.1 - Схема роботи HP із гнучкою конфігурацією

Основними складнощами наведеного принципу організації HP є:

1) AI. Існування широкого переліку загроз ІБ, обумовлює широке поле зворотного реагування (тобто поведінкових реакцій HP). Адміністратору необхідний вибір моделі AI, яка найкраще підходить для вирішення конкретного переліку завдань;

2) Модуль взаємодії між AI та HP («AI-HoneyPot interaction module»). Потенційна різноманітність модулів HP та реалізацій AI веде до відмінностей на рівні взаємодії цих модулів.

Можливим шляхом вирішенням цих складнощів є активна підтримка з боку профільної спільноти. Довіривши розробку окремих компонентів Open Source HP, третім особам, адміністратору ІБ залишається своєчасно

контролювати нетипові інциденти, та вірно налаштувати HP. Після цього управління системою HP здійснюється в напівавтоматичному режимі.

3 ПРИНЦИПИ ПОБУДОВИ, ЗАВДАННЯ ТА НАЛАШТУВАННЯ ТЕСТОВОГО ІМІТАТОРУ HONEYNET

3.1 Основні вимоги до мережі Honeynet

Перед безпосереднім проектуванням Honeynet, необхідно визначити основні завдання даної системи. Перш за все, така система спрямована на відволікання уваги хакера, змушуючи його витрачати ресурси та час на атаку завчасно створених хибних ресурсів, що є основним завданням для цієї мережі. Такого результату можна досягнути, використовуючи можливості відповідного сценарного поля Honeynet. Таким чином, система повинна бути наділена відповідними механізмами взаємодії із хакером задля створення хибного уявлення про успішність його дій. При цьому, час подолання цих механізмів залежить від: - компетентності зловмисника, періоду відновлення або реконфігурації HP після проведення атаки, рівню взаємодії із атакуючим та інших факторів.

Слід мати на увазі, що у разі збігу обставин чи заздалегідь спланованої хакером послідовності дій, система може не надати достатньо часу задля затримки атакуючого. Результатом такого інциденту буде викриття Honeynet, її злам та, можливо, використання системи задля атаки на об’єкт захисту. Тому, система повинна бути наділена механізмами сповіщення про нетипові інциденти та функціями протидії вторгненням, які мають використовуватись задля припинення потенційно небезпечних дій із боку хакера. Реалізація таких механізмів на рівні окремих компонентів є небезпечною та ненадійною, оскільки такі компоненти теж є ціллю для атакуючого. В цьому разі, якщо зловмисник здійснить успішну атаку, то гарантувати коректну роботу таких компонентів неможливо. Крім того, масштабування такої мережі потребує узгодження механізмів протидії задля усунення протиріч і поведінкових колізій. Саме тому, механізми протидії повинні бути «розміщені» у компоненті, що керує доступом

до інших ресурсів мережі HP, управління яким здійснюється безпосередньо адміністратором безпеки.

Додаткове завдання – збір інформації щодо дій хакера у системі. Тому, компоненти системи мають вести детальні log-файли, що повністю відображують дії хакера у межах цього компоненту із метою подальшого аналізу цих дій.

Зрештою, система HP повинна однозначно розрізняти трафік «порядних» користувачів від трафіку та дій зловмисника, крім того дії атакуючого не повинні впливати на функціонування об’єкта захисту, тому необхідна фільтрація та маршрутизація трафіку, що циркулює. Дана вимога повинна бути реалізована в межах створення окремого компонента, що виконує функцію маршрутизації трафіку. Впровадження всіх цих функцій у honeypots можливе, але це буде призводити до виникнення помилок при створенні правил (поведінкових сценаріїв) роботи HP, які можуть суперечити одне одному, що безпосередньо впливає на надійність такої системи в цілому.

3.2 Особливості розміщення Honeynet

Розташування Honeynet впливає на доступність системи хакеру. Відкрита система майже одразу приверне увагу хакера як доступна ціль, у той час, як закрита система може залишитись непоміченою чи такою, злам якої немає сенсу з точки зору атакуючого. Однак, система що немає ніяких механізмів захисту, буде занадто підозрілою для компетентного зловмисника. Тому, така система буде розміщена у сегменті мережі, компоненти якої є загальнодоступними для користувачів та захищені лише листами контролю доступу (ACL). Таке розташування є компромісом між захищеністю та доступністю та є найпоширенішим варіантом серед провідних компаній, що займаються розгортанням систем HP. Налаштування відповідних правил доступу до компонентів мережі відбувається на вхідному маршрутизаторі, що виступає аналогом міжмережевого екрану. На виході із сегмента такої мережі встановлено міжмережевий екран (ММЕ), що відокремлює сегмент розташування Honeynet та внутрішню мережу, що є об’єктом захисту. Тобто, розташування компонентів

системи Honeynet відбувається у демілітаризованій зоні (DMZ). Структурна схема організації мережі Honeynet наведена на Рис. 3.1, основними компонентами котрої є:

1) Firewall 1 – вхідний маршрутизатор с функцією MME. Приймає трафік із «зовнішньої» мережі згідно із встановленими правилами ACL. Відповідно до цих правил, відбувається маршрутизація пакетів до внутрішнього комутатору або MME (на схемі Firewall №2), або до одного з можливих HP в межах цієї Honeynet;

2) Honeynet system – система-пастка, що може складатися з декількох HP;

3) Firewall 2 – вихідний (відносно Honeynet) комутатор або MME, що виступає шлюзом, через який відбувається безпосередній доступ до об’єкта (ресурсів) захисту.

Детальний опис налаштувань буферних (кінцевих) елементів Honeynet та перелік її компонентів наведено далі.

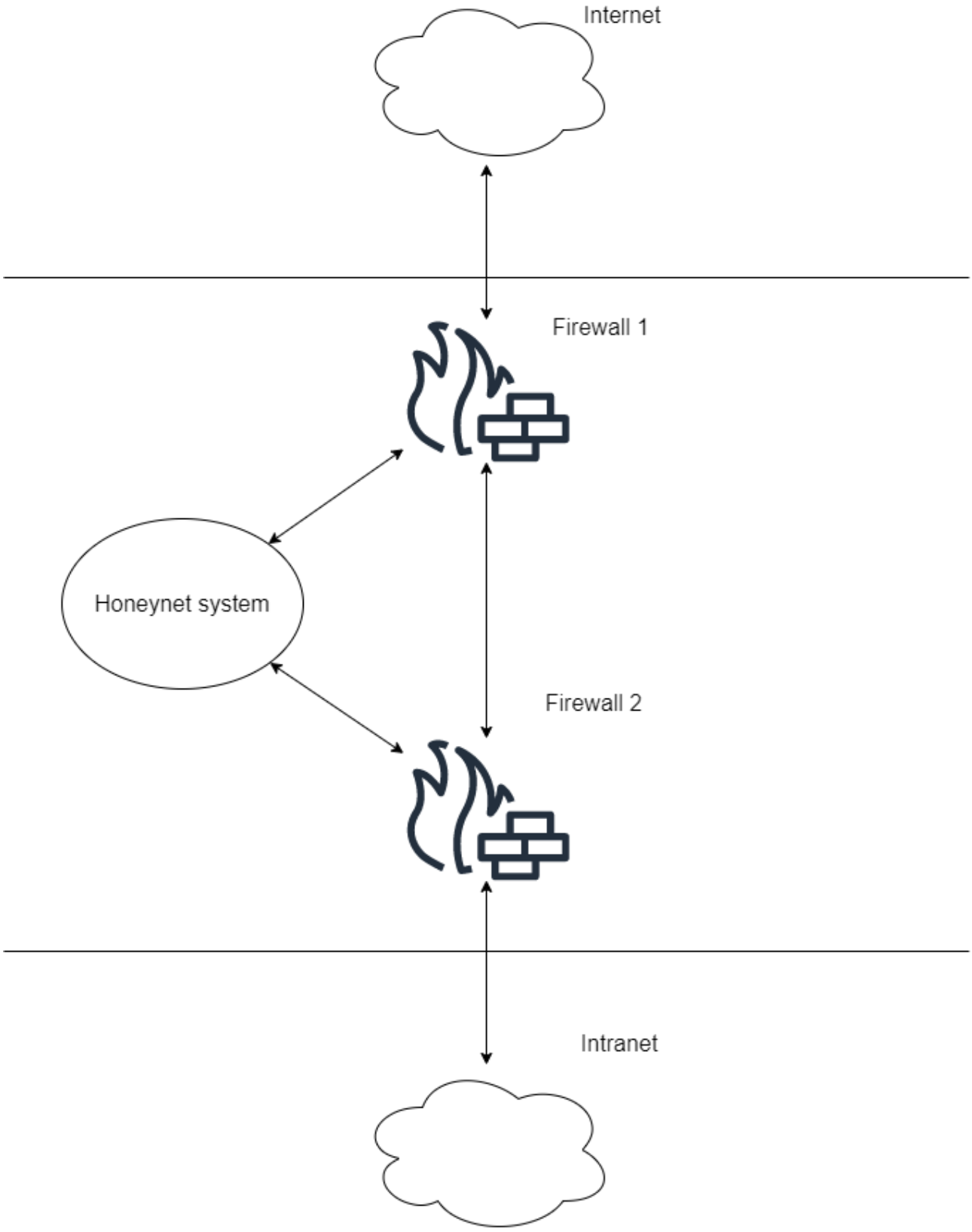


Рисунок 3.1 – Структурна схема і основні елементи Honeynet

3.3 Призначення складових компонентів

Спираючись на зміст основних завдань та вимог до системи Honeynet, має бути сформовано перелік компонентів, які дозволяють виконувати усі поставлені завдання. Виходячи з підрозділу 3.1, Honeynet має наступний перелік складових компонентів (підсистем):

1) HP, що є безпосередньою пасткою для хакера. Повинна надавати (синтезувати) хакеру середовище для здійснення їм атаки та реалізовувати функції створення, збереження та обміну log-файлами;

2) Підсистема виявлення аномалій мережевого трафіку. Під аномаліями слід розуміти будь-яке відхилення мережевого трафіку від штатного режиму функціонування елементів мережі, що захищається. Поведінка, що непередбачена системою, повинна бути проаналізована системою аналізу на предмет спроби реалізації атаки. Оскільки, перелік атак є вичерпним та у рамках даної роботи є статичним, то виявлення атак реалізовано, як порівняння властивостей трафіку з поточною БД, що містить система аналізу. Така БД зберігає властивості, що притаманні спробам зламу системи;

3) Підсистема маршрутизації трафіку, основним завданням якої є перенаправлення підозрілого або аномального трафіку на ресурси HP Дана система має керуватись рішеннями, що прийняті у рамках системи виявлення аномалій мережевого трафіку.

4) Підсистема взаємодії із хакером. Під взаємодією мається на увазі поведінка HP у відповідь на дії хакера, тобто створення сценарного поля Honeypot. Однією з поведінкових реакцій повинно бути розірвання сеансу зв’язку із хакером. Така підсистема має отримувати актуальні дані, щодо стану всіх елементів Honeynet.

Кількість підсистем (або складових) Honeypot впливає на якість імітації усієї мережі. Існування (тобто використання) лише однієї системи-приманки (HP) можливо та є достатнім, однак практично не має сенсу, оскільки така система не відповідає реальній інфраструктурі Intranet. Задля створення кращої імітації реальної мережі потрібні сервери обробки, зберігання, та передавання

інформації в цій мережі. Тому, систему Honeynet слід розширити до: - сервер зберігання інформації (Data server); - сервер корпоративної пошти (Corporate mail server) та FTP сервер що дублює процес роботи Data server. Одночасне існування Data server та FTP серверу потрібно задля переправлення трафіку зловмисника з одного серверу на інший, що буде детально пояснено при описі сценарного поля використовуваного Honeypot (тобто, простішого Honeynet, що складається з одиничного HP).

З переліку компонентів системи Honeynet можливо зробити такі висновки:

1) Система виявлення аномалій мережевого трафіку, система маршрутизації та система взаємодії з хакером є основними управляючими вузлами Honeynet, що тісно взаємодіють між собою;

2) Усі основні вузли Honeynet повинні мати канал зв'язку з адміністратором безпеки задля створення можливості постійного моніторингу та корегування подій;

3) Основні вузли Honeynet здатні коректно функціонувати лише у випадку, коли мають доступ до крос читання всіх log-файлів Honeynet. Задля реалізації такої взаємодії повинна існувати «Система аналізу поточного стану Honeynet».

Вочевидь, що одночасне існування 4-х окремих систем управління є надлишковим та неефективним з точки зору розгортання Honeynet та її подальшої підтримки. Оскільки ці системи залежать одна від іншої, повинні взаємодіяти з адміністратором безпеки та мають доступ до компонентів Honeynet system, то найкращим рішенням є інтеграція цих систем у єдиний модуль управління[50], склад та структура якого наведено на Рисунку 3.2.

Такий модуль дозволяє здійснювати централізоване управління системою Honeynet і виконує наступні завдання:

1) Встановлює ACL для вхідного маршрутизатора (див. рис. 3.2), за допомогою чого здійснюється реакція систем Honeypot у відповідь на дії хакера та, у разі необхідності, переривання сесії зловмисника. Такі реакції спрацюють незалежно від режиму функціонування компонентів Honeypots, та впроваджують

єдину поведінкову стратегію реакції системи на спробу реалізації атак, що підвищує шанси на «довіру» із боку хакера;

2) Прослуховує трафік з вхідного маршрутизатора, перевіряючи наявність поведінкових аномалій та спрямовує трафік до мережі Intranet або до Honeypots на основі результатів цього аналізу;

3) Відслідковує поточний стан всіх складових Honeynet (включаючи використовувані HP) та звітує (логує) адміністратору безпеки.

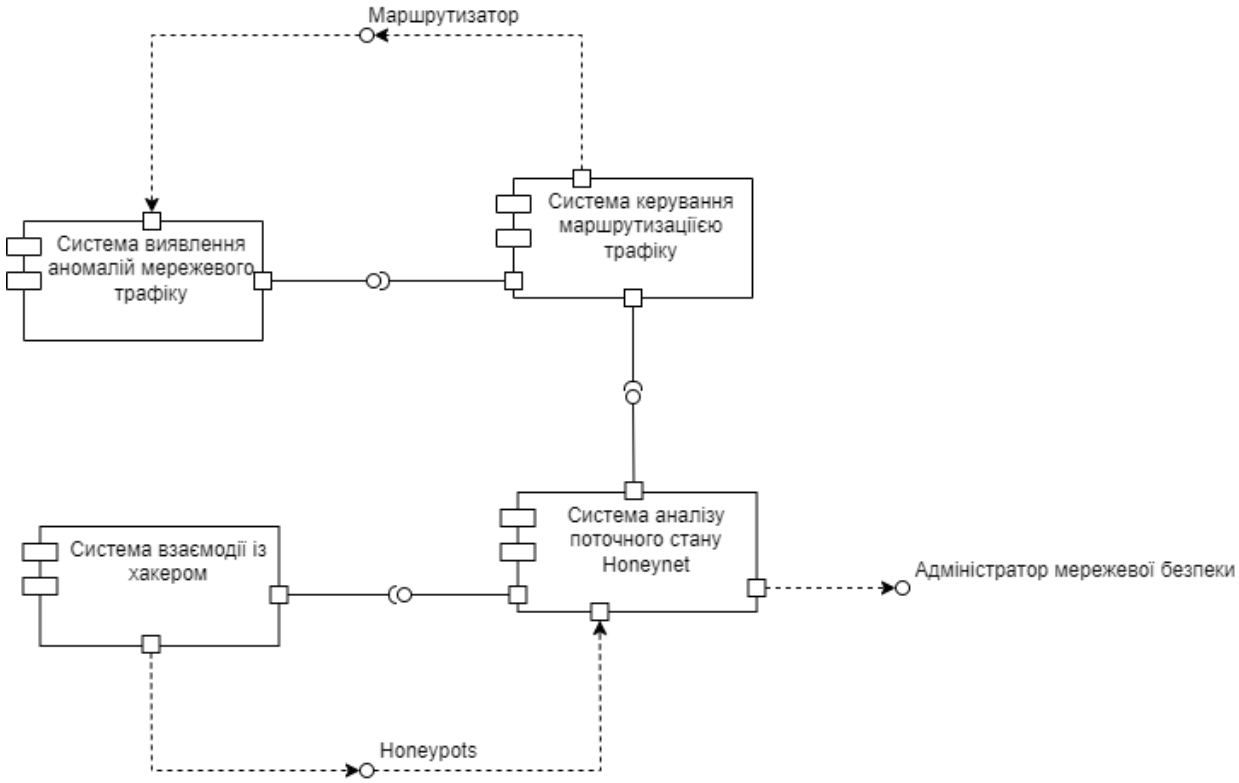


Рисунок 3.2 – Структура зв’язків компонентів інтегрованого модуля керування Honeynet system

3.4 Синтез мережі

Визначений склад компонентів мережі Honeynet дозволяє реалізувати поставлені завдання, однак є недостатнім для побудови мережі. Перш за все, для маршрутизації трафіку зловмисника між елементами Honeynet потрібні додаткові пристрої управління трафіком. Такі функції може здійснювати комутатор, оскільки весь контроль трафіку відбувається у рамках DMZ цієї локальної мережі. Також, така система дозволяє встановити набір правил на канальному рівні моделі OSI, що слугує додатковим інструментом контролю всередині мережі. Такий комутатор, за своєю функціональною суттю, є найпростішим MME, а саме керованим комутатором. Ще один важливий компонент – 2-й вихідний (для Honeynet) комутатор або MME.

Передбачається, що ціллю хакера будуть інформаційні ресурси Honeypots, але потрібно враховувати і спроби атакуючого блокувати саме маршрутизатор у рамках проведення DoS атаки на, як він вважає, справжній мережевий ресурс - жертву. Якщо основний маршрутизатор буде виведено з ладу, функціонування усієї системи буде порушено. Тому, потрібен ще один резервний вузол, з функцією маршрутизації, що буде підтримувати безперервну роботу системи у разі тимчасової відмови вхідного компонента Honeypots. Резервування маршрутизатора (див. Табл.3.1) відбувається за допомогою наступних протоколів [51]:

- HSRP (Hot Standby Router Protocol) – пропрієтарний протокол Cisco, що виконує резервування шляхом використання на двох або більше маршрутизаторах однієї віртуальної IP та MAC адреси. Маршрутизатори об'єднуються в HSRP групу, в ній і задаються параметри (віртуальна IP-адреса, ім'я групи, таймінги для перемикання з резервного на активний та інше). Таких груп може бути кілька (у першій версії HSRP протоколу може бути 255 груп, у другій - 4096). Віртуальна IP-адреса має бути з тієї самої мережі (в даному випадку сегменті DMZ), в якій розташований маршрутизатор (-ри) і не може збігатися з уже використаними IP-адресами. Таким чином, у HSRP групі один маршрутизатор є активним (active), який здійснює передачу пакетів і тільки один

резервним (standby). Решта маршрутизаторів можуть бути тільки слухачами. Маршрутизаторам можна задавати пріоритет, при цьому активним маршрутизатором є той, що має найвищий пріоритет, якщо пріоритет однаковий, то активним стає маршрутизатор із більшою IP адресою.

- VRRP (Virtual Router Redundancy Protocol) – відкритий протокол, що розробляється IEEE. Створений на основі протоколу HSRP. Принцип роботи протоколу схожий на HSRP. Група маршрутизаторів об'єднується в один віртуальний роутер і їм призначається одна загальна IP-адреса. Як і в протоколі HSRP можна використовувати кілька HSRP-груп. Один маршрутизатор може, так само, одночасно перебувати в декількох віртуальних роутерах (групах). Тільки один із фізичних роутерів стає головним (VRRP Master router), який виконує маршрутизацію, всі інші є резервними (VRRP Backup router). На відміну від HSRP протоколу в VRRP може бути кілька резервних маршрутизаторів, а не один. Також плюсом VRRP є те, що як віртуальну IP-адресу можна використовувати вже призначену IP-адресу на інтерфейсі маршрутизатора, що не можна робити в HSRP. Використання даного протоколу доцільне у разі об’єднання обладнання від різних вендорів.
- GLBP (Gateway Load Balancing Protocol) – пропрієтарний протокол від компанії Cisco, призначений для резервування маршрутизаторів Cisco, а також балансування їхнього навантаження. Балансування навантаження здійснюється завдяки використанню однієї спільної IP-адреси та кількох MAC-адрес. На відміну від HSRP і VRRP, в даному випадку у маршрутизації беруть участь усі роутери віртуальної групи. Підтримується чотири режими роботи GLBP. Режим, у якому не використовується балансування (None). Балансування навантаження пропорційно «вазі» маршрутизатора (Weighted Load Balancing). Певний хост завжди використовує один і той самий маршрутизатор у групі (Host Dependant Load Balancing). Віртуальну MAC-адресу кожного маршрутизатора підставлятимуть у відповідь на ARP-запит для віртуального IP по черзі (Round Robin Load Balancing).

Таблиця 3.1 – Порівняльна характеристика протоколів

Критерій порівняння	VRRP	HSRP	GLBP
Розробник	IEEE	Cisco	Cisco
Тип протоколу	Відкритий(RFC 5798)	Пропрієтарний (RFC 2281)	Пропрієтарний
IPv6	–	+	+
Віртуальна IP адреса	Може бути однаковою із фізічною IP адресою	Не може бути однаковою із фізічною IP адресою	Не може бути однаковою із фізічною IP адресою
Ролі маршрутизаторів	Головний (Master) маршрутизатор та маршрутизатор відновлення (backup)	Активний (Active) та очікуючий (Standby)	Активний віртуальний шлюз (Active Virtual Gateway), активний віртуальний послідовник (Active Virtual Follever)
Віртуальна MAC адреса	VRRP група записується у останньому октеті MAC адреси	HSRP група записується у останньому октеті MAC адреси	Четвертий та п'ятий октети визначають номер групи GLBP. Шостий октет визначає номер AVF.

Таким чином, маючи повний перелік компонентів стає можливим синтез мережі Honeynet, структура якої зображена на Рис. 3.3.

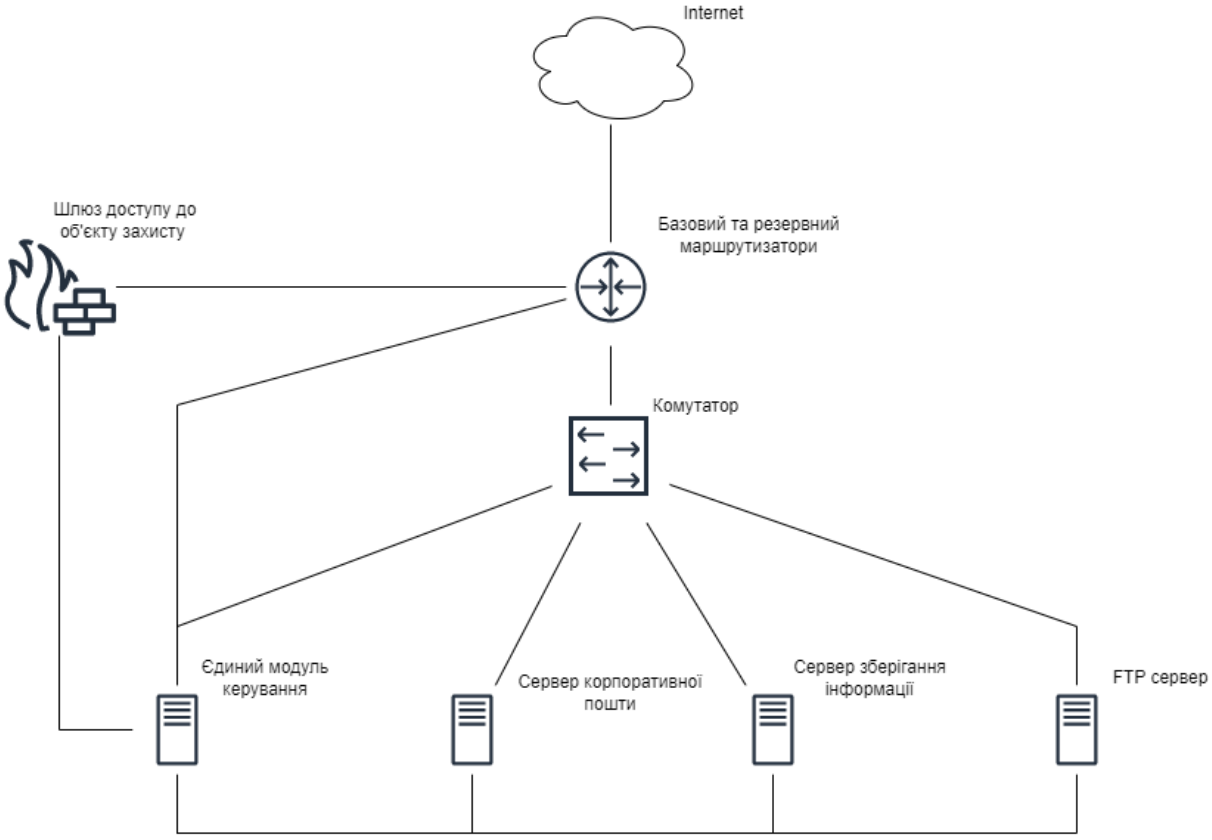


Рисунок 3.3 – Структурна схема мережі Honeynet

3.5 Опис сценарного поля

Сценарне поле HP (або Honeynet) описує набір дій, що є реакцією системи на дії атакуючої сторони. Його доскональність та варіативність можливостей безпосередньо впливають на якість імітації системи HP. Задля створення сценарного полю системи Honeynet потрібно визначити та постійно корегувати (доповнювати) відповідний лист загроз та реакцій системи на кожну із них.

Для DoS – обмеження пропускної спроможності, тобто виділити атакуючому канал фіксованої ширини (наприклад, 0.1 від загальної пропускної спроможності), тобто штучно затримувати час опрацювання кожного пакета порушника. Також захист від DoS атак здійснюється через додання правил ACL на заборону фрагментованих пакетів (протидія Teardrop), ICMP пакети великого розміру (протидія Ping of Death).

XSS – обмеження хакеру в доступі до деяких методів та заголовків HTTP, перемикаючи атакуючого на зовнішні фейкові ресурси, після всіх його спроб - блокувати трафік. В цьому випадку найгірший варіант - якщо зловмисник

скомпрометує фейковий ресурс. У такому разі треба змінити ACL маршрутизатора на відхилення всіх пакетів від «зламаного» вузла.

Path traversal – уповільнення трафіку атакуючого, що збільшить час, необхідний на перебір варіантів. У разі, коли відомо, який саме ресурс вишукує хакер можна обмежити доступ через створення відповідного правила ACL.

ARP spoofing – налаштування статичної маршрутизації, уповільнення трафіку атакуючого.

Використання навіть цього обмеженого переліку зворотних дій дає можливість сформувати просте сценарне поле, що дозволяє ефективно протидіяти атакам та створити відповідні багатоходові ланцюжки дій HP, щодо протидії різним комбінаціям наведених в 1-му розділі атак:

- Сповільнення трафіку – обмеження пропускної здатності є поширеною опцією серед маршрутизаторів. Задля створення відповідного правила потрібно визначити IP/MAC-адресу та задати для атакуючого бажане значення пропускної здатності каналу зв’язку .
- Перенаправлення трафіку – хакер, що звертається до конкретного ресурсу отримує IP-адресу пристрою та подальший обмін пакетами відбувається через цю адресу. Механізм перенаправлення трафіку може бути реалізований як обмін IP-адресами пристроїв у мережі. Така реакція Honeynet забезпечує найкращі результати, якщо заміна йде між двома, схожими за призначенням вузлами. Наприклад, заміна сервера зберігання даних, що працює на SFTP, на хибний сервер зберігання даних, якій працює на FTP.
- Блокування трафіку від конкретного вузла – реалізація даної поведінки можлива через внесення змін до правил ACL комутатора або маршрутизатора, а саме додаванням відповідного правила на блокування трафіку від адреси хакера (бажано включати після 2-х попередніх реакцій, що дає змогу виграти час і отримати більший обсяг інформації про атакуючого).

3.6 Створення правил ACL

Для початку роботи, системі необхідно задати стандартний список правил ACL, що використовується у випадках, коли система Honeynet не виявила

вторгнень (режим штатного функціонування). Згідно з рекомендаціями компанії Cisco [52] побудова ACL здійснюється за наступними принципами:

- ACL має структуру з декількома твердженнями від найбільш конкретного до найменш конкретного;
- до мережевого інтерфейсу Cisco можна застосувати max 2 ACL: один ACL може бути застосований до вхідного інтерфейсу, інший – для вихідного.

Вхідні маршрутизатори (див. рис.3.3) за замовченням приймають будь-який трафік, тому його ACL в режимі штатного функціонування має не заважати проходженню пакетів. Відповідний приклад ACL наведено у Табл. 3.2, де є правіло для вхідного інтерфейсу маршрутизатору.

Комутатор, що керує трафіком між вузлами мережі Honeynet (рис.3.3) повинний заважати проходженню пакетів, адреси джерела та призначення котрих є вузлами мережі Honeynet, за винятком зв'язків з «Модулем керування» (правило №1 в Табл.3.3). Тому, потрібно відповідне правило, яке обмежує маршрутизацію пакетів з однієї приватної мережі (правило №2 в Табл.3.2). Крім того, потрібно окреме правило (приклад №3, Табл. 3.2), що поєднує комутатор із вхідним маршрутизатором (або FW №1 та FW№2 на рис.3.1).

Таблиця 3.2 – Приклад таблиці ACL для вхідного інтерфейсу

Номер правила	Запис у маршрутизаторі	Опис
1	access-list 1 permit any any	Дозволити будь-який трафік від будь-якого джерела до будь-якого пункту призначення

Таблиця 3.3 –ACL для міжелементної взаємодії HP

Номер правила	Запис у комутаторі	Опис
1	access-list 1 permit ip host 192.168.3.111 host 192.168.3.113	Дозволити будь-який трафік між «Модулем керування» та «Сервером зберігання інформації» (приклад)
2	access-list 1 deny 192.168.0.0 0.0.0.255	Заборонити будь-який трафік між вузлами однієї приватної мережі крім «Модулю керування HP», наприклад з «сервером зберігання інформації».
3	access-list 1 permit any any	Дозволити будь-який трафік від будь-якого джерела до будь-якого пункту призначення

3.7 Розробка механізмів протидії вторгненням

Наступним кроком є налаштування функціонування Honeynet у разі виявлення вторгнення. Усе сценарне поле системи реалізується через переналаштування мережевого обладнання (маршрутизатор, комутатор та FW, на рис.3.1) та роботи Honeypots, котрий змінює логіку роботи елементів на рис.3.3, а саме зміна ACL та переналаштування IP конфігурації вузлів мережі Honeynet. При цьому, перш за все потрібно визначити механізм реалізації сценарного поля, що залежить від конкретних дій атакуючої сторони (типу атаки та послідовності його дій).

Обмеження пропускної здатності для конкретної IP-адреси здійснюється через використання функції Quality of Service (QoS) що реалізована виробником мережевого обладнання. Така функція дозволяє визначити клас трафіку, до якого слід застосувати обмеження та визначити ширину смуги пропускання використовуваного для зв’язку з атакуючим, каналу зв’язку.

Перенаправлення трафіку здійснюється через обмін IP-адресами між вузлами мережі. Для цього потрібно «зайти» у налаштування мережі у вузлі

(ifconfig, netsh) та змінити адресу сервера. Зміна маски підмережі не потрібна, оскільки обидва вузли знаходяться у рамках однієї мережі. При реалізації такого методу потрібно враховувати, що сервери повинні мати однакові налаштування та однаковий доступ до ресурсів мережі.

Ще один варіант перенаправлення трафіку – використання системи балансування навантаження (GLBP та інші). Незалежно від методу реалізації, результатом буде автоматичне перенаправлення сесії зловмисника.

Блокування трафіку здійснюється через додавання потрібних правил до ACL вхідного маршрутизатора та/або правила фільтрації трафіку першого FW (наприклад, в залежності від різниці поточного часу на вузлах HP та устаткуванням атакуючого). При цьому, потрібно враховувати, що дане правило потрібно розміщувати на початку ACL маршрутизатора. Загальний синтаксис такої команди:

access-list 1 deny host <IP-адреса>,

де IP-адреса, це IP-адреса зловмисника.

Зазначення специфічної адреси у правилах має сенс, лише у випадку, коли хакер не використовує proxy-сервери для зміни IP-адреси. У випадках, коли IP-адреса змінюється, слід застосовувати ключове слово “any”, що дозволить заблокувати трафік незалежно від джерела. Після реалізації кожного сценарного полю HP, потрібно визначити порядок дій у разі здійснення атак.

3.7.1 DoS

Реакція системи (Табл.3.4) на атаку «Відмова в обслуговуванні» виглядає наступним чином: - ініціалізація правил ACL, що блокуватимуть трафік, котрий пов'язаний з атаками DoS, наприклад, пакети з фрагментацією, ICMP-пакети великого розміру. В цьому разі, ще однією корисною реакцією HP буде завдання обмеження пропускної здатності для конкретної (атакуючої) IP-адреси.

Таблиця 3.4 – Приклади ACL для випадку DoS атаки

Номер правила	Запис у комутаторі	Опис
1	access-list 1 deny tcp host <IP-адреса хакера> any fragments	Заборонити трафік, що складається із фрагментованих TCP пакетів.
2	access-list 1 deny icmp host <IP-адреса хакера> any packet-too-big	Заборонити ICMP трафік, занадто великого розміру.
3	access-list 1 permit any any	Дозволити будь-який трафік від будь-якого джерела до будь-якого пункту призначення.

3.7.2 XSS

Обмеження дій хакера при здійсненні атаки Cross Site Scripting здійснюється через фільтрацію HTTP запитів, перенаправлення та блокування трафіку зловмисника.

Таблиця 3.5 – Приклади ACL для випадку протидії XSS

Номер правила	**Запис у комутаторі**	**Опис**
1	access-list 1 deny tcp host <IP-адреса хакера> any eq www method <Назва методу>	Заборонити доступ до певних методів протоколу HTTP. Такими методами можуть бути POST, PUT, GET, PATCH та інші.
2	access-list 1 deny tcp host <IP-адреса хакера> any eq www host <IP-адреса хосту>	Заборонити доступ до певних адрес

Продовження Таблиці 3.5

Номер правила	Запис у комутаторі	Опис
3	access-list 1 deny tcp host <IP-адреса хакера> any eq www header User-Agent "malicious-agent"	Заборонити доступ до певних заголовків HTTP
4	access-list 1 permit any any	Дозволити будь-який трафік від будь-якого джерела до будь-якого пункту призначення.

3.7.3 Path Traversal

Атака «Обхід директорій» є підтипом Brute-force (див. Розділ 1), та час її виконання залежить від швидкості перебору варіантів кодових комбінацій атакуючим. В цьому випадку адекватною реакцією HP є обмеження швидкості обробки трафіку від зловмисника, що викличе значне збільшення часу. Якщо, відомо, який ресурс вишукує зловмисник, можна задати правило ACL, що забороняє доступ до певного ресурсу (елементу в межах самої Honeynet). Синтаксис такого правила:

access-list 1 deny tcp host <IP-адреса хакера> any eq www path /../ ,

де /../ – шлях, до якого потрібно заблокувати доступ.

3.7.4 ARP spoofing

За допомогою ACL є можливість заборонити або переправити до потрібного вузлу той трафік, що містить ARP запити/відповіді. Вказівка у правилі IP адреси відправника, дозволяє обмежити проходження ARP від конкретної IP адреси (див. Табл. 3.6).

Таблиця 3.6 – Приклади ACL для випадку здійснення ARP spoofing

Номер правила	Запис у комутаторі	Опис
1	access-list 1 deny arp host <IP-адреса хакера> any	Заборонити проходження трафіку, що містить ARP.
2	access-list 1 permit any any	Дозволити будь-який трафік від будь-якого джерела до будь-якого пункту призначення.

3.8 Відпрацювання механізму виявлення аномалій мережевого трафіку

Виявлення спроб несанкціонованої зміни штатних параметрів функціонування будь-яких елементів об’єкту захисту, є механізмом, що дозволяє виявляти незвичайні - аномальні або підозрілі шаблони у мережевому трафіку для виявлення потенційних загроз та атак на інформаційну систему. Виявлення таких аномалій відбувається шляхом використання статистичних методів, машинного навчання, AI та інших технік для виявлення аномальних шаблонів та відхилень у мережевому трафіку. Програмний імітатор HP, що розглядається у даній роботі, спрямовано на протидію заданому переліку найпоширеніших атак (розділ 1). Відповідно, процес аналізу мережевого трафіку реалізовано, як перевірка пакетів на наявність характерних для цих атак, спроб. Структура пакетів, що аналізуються та обробляються мережею описана у документах RFC [53], розробкою яких займається некомерційна організація World Wide Web Consortium (W3C). У даній роботі, використано знання про структуру IP-пакету, що описано в RFC 791 [53]. Структура IP-пакету наведено у табл.3.7.

Таблиця 3.7 Структура IP-заголовку

<table>
<tr><td>Версія
(4 біти)</td><td>Довжина
заголовку
(4 біти)</td><td>Тип сервісів
(8 біт)</td><td colspan="2">Загальна довжина
(16 біт)</td></tr>
<tr><td colspan="3">Ідентифікатор (16 біт)</td><td>Флаги
(3 біти)</td><td>Зміщення фрагменту
(13 біт)</td></tr>
<tr><td colspan="2">Час життя (8 біт)</td><td>Протокол (8 біт)</td><td colspan="2">Контрольна сума заголовку (16 біт)</td></tr>
<tr><td colspan="5">MAC-адреса відправника (32 біти)</td></tr>
<tr><td colspan="5">MAC-адреса отримувача (32 біти)</td></tr>
<tr><td colspan="4">Опції</td><td>Зсув</td></tr>
</table>

3.8.1 DoS

Механізм виявлення подібних атак, повинен враховувати можливість наявності фрагментовних пакетів, зсув яких налаштовано некоректно (Teardrop) та ICMP пакетів занадто великого розміру (Ping of Death). Функція teardrop_check (ip_header_array) встановлює чи є у пакеті ознаки Teardrop атаки. У якості аргументу, функція приймає масив заголовків IP сесії – ip_header_array. Виявлення полягає у визначенні відстані між останнім пакетом, та тими, що були до нього.

Таким чином, якщо зсув було порушено, функція повертає значення True, що є «флагом» початку Teardrop атаки (рис.3.4).

```
def teardrop_check(ip_header_array):
    Teardrop = False

    for i in range(len(ip_header_array) - 1):
        current_packet = ip_header_array[i]
        next_packet = ip_header_array[i + 1]

        packet_shift = next_packet - current_packet

        if packet_shift != 1:
            Teardrop = True
            break

    return correct_shifts
```

Ln: 7, Col: 9

Рисунок 3.4 – Алгоритм виявлення Teardrop

Передбачається, що для виявлення Teardrop потрібно зберігати сесію до її завершення, оскільки в іншому випадку перевірка коректності зсуву пакетів неможлива.

Задля виявлення Ping of death потрібен метод(is_ping_of_death), який приймає наступні аргументи:

- packet – перехоплений пакет з мережі
- max_icmp_length – максимальна довжина icmp повідомлення у даній системі.

Якщо перехоплений пакет має 3 рівень моделі OSI, та тип повідомлення – ICMP із довжиною, що перевищує максимально допустиму довжину, це атака Ping of death (рис.3.5). Функції getlayer(), proto() належать до бібліотеки scapy [54]:

```python
def is_ping_of_death(packet, max_icmp_length):
    ip_packet = packet.getlayer(IP)
    if ip_packet and ip_packet.proto == ICMP and len(ip_packet) > max_icmp_length:
        return True
    return False
```

Рисунок 3.5 – Процедура виявлення Ping of death

3.8.2 XSS

Задля виявлення пакетів, що містять XSS, потрібно проаналізувати HTTP-повідомлення на наявність специфічного синтаксису, що слугує задля завантаження javascript-коду. Метод is_XSS(packet_data) приймає пакет, що перехоплено у мережі та проводить наступні дії:

1) Перетворює повідомлення у рядок тексту;
2) Перевіряє наявність методів HTTP;
3) Шукає параметри методів і перевіряє зміст параметрів. Якщо у цих параметрах є частини синтаксису HTML, що слугують для виділення фрагменту javascript коду, такі як «<script>» або «javascript», система розпізнає спробу початку XSS атаки (рис.3.6).

```python
import re

def is_XSS(packet_data):
    # Преобразование пакета в строку
    packet_str = packet_data.decode('utf-8')

    # Поиск HTTP-запросов в пакете
    http_requests = re.findall(r'(GET|POST|PUT|DELETE|HEAD) (.*?) HTTP/1.[01]', packet_str)

    for method, path in http_requests:
        # Извлечение параметров из пути запроса
        params = re.findall(r'[\?&]([^=]+)=([^&]+)', path)
        for param, value in params:
            # Проверка значения параметра на наличие потенциально опасных символов или шаблонов
            if re.search(r'<script|javascript:|on\w+=', value):
                # Потенциальная XSS-атака
                return True

    return False
```

Рисунок 3.6 – Процедура фільтрації пакетів, що містять XSS

3.8.3 Path Traversal

Аналіз пакетів, що містять Path Traversal, подібний до аналізу на предмет наявності XSS. Як і у попередньому випадку, сенс полягає в перетворенні пакету у рядок, пошук методів HTTP та пошук специфічних значінь параметрів, шо вказують на атаку. Однак, у випадку Path traversal (рис.3.7) такими значеннями є шляхи, що рекурсивно звертаються до каталогів більш високого рівня ОС, тобто мають «../» або звертаються до критичних для системи файлів та директорій (passwd, System32). Методи findall (), search () належать до бібліотеки re, що оброблює регулярні вирази (Regular Expressions)

```
1  import re
2
3  def is_path_traversal(packet_data):
4      # Преобразование пакета в строку
5      packet_str = packet_data.decode('utf-8')
6
7      # Поиск HTTP-запросов в пакете
8      http_requests = re.findall(r'(GET|POST|PUT|DELETE|HEAD) (.*?) HTTP/1.[01]', packet_str)
9
10     for method, path in http_requests:
11         # Проверка пути запроса на наличие потенциально опасных шаблонов
12         if re.search(r'\.\./|\.\.\\|/\.\./|/etc/passwd|C:\\\\Windows\\\\System32', path):
13             # Потенциальная атака Path Traversal
14             return True
15
16     return False
```

Рисунок 3.7 – Процедура фільтрації пакетів, що містять *Path traversal*

3.8.4 ARP Spoofing

Фільтрація пакетів, що містять ARP spoofing, передбачає аналіз Ethernet кадрів на наявність некоректних ARP-запитів та ARP-відповідей.

Метод is_ARP_spoofing(eth_frame_data) приймає у якості аргументу кадр канального рівня моделі OSI – eth_frame_data. З заголовку кадру(eth_header) отримуються наступні дані:

1) MAC-адреси відправника та отримувача;
2) Тип повідомлення.

У разі, якщо тип повідомлення це ARP (у коді представлено, як 0x0806, що відповідає значенню протоколу ARP у полі EtherType кадру 2 рівня) із вмісту

кадру стає відомим тип повідомлення (запит чи відповідь) та MAC-адреси відправника та отримувача. Таким чином, якщо MAC-адреси із кадру та вмісту повідомлення не збігаються, то це повідомлення йде від зловмисника, що здійснює ARP-spoofing (рис.3.8):

```python
import struct
import socket

def is_ARP_spoofing(eth_frame_data):
    # Чтение заголовка Ethernet-кадра
    eth_header = eth_frame_data[:14]
    eth_header_unpack = struct.unpack('!6s6sH', eth_header)
    destination_mac = eth_header_unpack[0]
    source_mac = eth_header_unpack[1]
    eth_type = eth_header_unpack[2]

    # Проверка типа Ethernet-кадра на ARP
    if eth_type == 0x0806:
        # Чтение заголовка ARP
        arp_header = eth_frame_data[14:42]
        arp_header_unpack = struct.unpack('2s2s1s1s2s6s4s6s4s', arp_header)
        arp_opcode = arp_header_unpack[4]
        arp_sender_mac = arp_header_unpack[5]
        arp_sender_ip = socket.inet_ntoa(arp_header_unpack[6])

        # Проверка корректности ARP-запроса или ответа
        if arp_opcode == b'\x00\x01' and arp_sender_mac != source_mac:
            # Потенциальная атака ARP Spoofing
            return True
        if arp_opcode == b'\x00\x02' and arp_sender_mac != source_mac:
            # Потенциальная атака ARP Spoofing
            return True

    return False

```

Рисунок 3.8 – Процедура фільтрації пакетів, що містять ARP-spoofing

ВИСНОВКИ

Швидкі темпи розвитку зловмисного ПЗ, а також методів і стратегій здійснення атак інформаційних ресурсів приватних користувачів і корпоративного сегменту сучасної IT сфери, змушують фахівців з ІБ постійно вдосконалювати наявні методики та засоби захисту. Тому, до традиційних (пасивних, або реактивних) засобів захисту, необхідно додавати засоби активної - превентивної оборони, що помітно ускладнюють умови проведення атак або помітно звужують можливості для їхнього «успішного» проведення.

Використання концепції активного захисту надає можливість аналізувати дії хакерів задля синтезу нових методів та стратегій відбиття сучасних атак. Застосування в складі контуру безпеки відразу декількох рішень активного захисту (HP, Honeynet, IDS\IPS, FW рівня Next Generation тощо), демонструє значно кращі результати, але водночас вимагає більше ресурсів на їх розгортання та підтримку, але з урахуванням можливих наслідків та частотою здійснення та складністю сучасних атак, це відходить на другий план .

Системи HP та Honeynet є одними із важливих компонентом сучасних систем захисту, та в різному вигляді інтегровані до найкращих рішень й технологій (наприклад входять до складу сучасних XDR платформ).

Ефективність використання HP можливо покращити за рахунок активного впровадження в дійсні логічні ланцюги алгоритмів управління мережевих пасток, елементів AI та ML. Це дозволяє скоротити витрати часу із боку спеціалістів з ІБ при виникненні інцидентів безпеки, а також покращити рентабельність обслуговування подібної системи. Існуючі зразки HP, в своєї більшості, є пропрієтарними і не підлягають незалежному аудиту. Використання таких систем повністю «базується» на довірі до їх розробника. Альтернативою пропрієтарним HP, є розробка Open Source систем із можливістю гнучкої конфігурації, як окремих елементів HP (або Honeynet), так і системи взагалі.

Розглянутий приклад реалізації програмного імітатору Honeynet дозволяє реалізувати потрібні захисні реакції для визначеного кола атак. Структура цієї системи організована в DMZ сегменті тестової локальної мережевої структури та забезпечує наступні захисні функції: - переналаштування ACL вхідного маршрутизатора та комутатора; - обмеження пропускної здатності каналу зв'язку; - переривання сесії зловмисника. Розглянутий приклад організації HP, демонструє можливість впровадження гнучких адаптивних рішень активного мережевого захисту, що враховують, особливості топології та специфіки використання мережевих ресурсів, що захищаються.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 50+ статистических данных, тенденций и фактов о кибербезопасности, которые имеют значение на 2023 год. URL: https://www.websiterating.com/ru/research/cybersecurity-statistics-facts/ (дата звернення 06.05.2023)

2 What Is Active Defense and What Does It Mean in Cybersecurity. URL: https://www.fortinet.com/resources/cyberglossary/active-defense (дата звернення 06.05.2023)

3 Stoll C. CUCKOO'S EGG. New York, 2012, 326 p.

4 A Study on Global Data Leaks in H1 2018. URL: https://infowatch.com/report2018_half (дата звернення 06.05.2023)

5 Найпопулярніші види кібератак у 2021 InfoWatch | 10Guards. URL: https://10guards.com/ua/articles/the-most-common-types-of-cyber-attacks-in-2021/ (дата звернення 06.05.2023)

6 Business E-mail Compromise: The 3.1 Billion Dollar Scam. URL: https://www.ic3.gov/Media/Y2016/PSA160614 (дата звернення 06.05.2023)

7 Halevi T., Memon N., Nov O., Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks. New York, 2015. 10 с.
DOI: http://dx.doi.org/10.2139/ssrn.2544742

8 Pienta D., Thatcher J. B., Johnston A. Protecting a whale in a sea of phish // Journal of Information Technology 2020, Vol. 35(3) 214–231 URL: https://journals.sagepub.com/doi/pdf/10.1177/0268396220918594

9 FBI. FBI Warns of Rise in Schemes Targeting Businesses and Online Fraud of Financial Officers and Individuals. URL: https://www.fbi.gov/contact-us/field-offices/cleveland/news/press-releases/fbi-warns-of-rise-in-schemes-targeting-businesses-and-online-fraud-of-financial-officers-and-individuals (дата звернення 18.04.2023)

10 What Is a Man-in-the-Middle Attack? Definition, Detection, and Prevention Best Practices for 2022. URL: https://www.spiceworks.com/it-security/data-security/articles/man-in-the-middle-attack/ (дата звернення 18.04.2023)

11 FBI. TDOS: Telecommunication Denial of Service. URL: https://www.fbi.gov/audio-repository/news-podcasts-inside-tdos-telecommunication-denial-of-service.mp3/view (дата звернення 18.04.2023)

12 CISA. Understanding Denial-of-Service Attacks. URL: https://www.cisa.gov/news-events/news/understanding-denial-service-attacks (дата звернення 18.04.2023)

13 United States Department of Justice. Georgia Man Admits Engaging In Distributed Denial Of Service Attacks Against Company. URL: https://www.justice.gov/usao-nj/pr/georgia-man-admits-engaging-distributed-denial-service-attacks-against-company (дата звернення 18.04.2023)

14 OWASP foundation. SQL Injection Prevention Cheat Sheet. URL: https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html (дата звернення 23.05.2023)

15 Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets. URL: https://www.ic3.gov/media/news/2020/201022-1.pdf (дата звернення 23.05.2023)

16 Nmap Documentation - Free Security Scanner For Network Exploration & Security Audits. URL: https://nmap.org/docs.html (дата звернення 13.02.2023)

17 CISA. Iranian State-Sponsored Advanced Persistent Threat Actors Threaten Election-Related Systems. URL: https://www.ic3.gov/media/news/2020/201022-2.pdf (дата звернення 13.02.2023)

18 Cross Site Scripting (XSS) OWASP Foundation. URL: https://owasp.org/www-community/attacks/xss/ (дата звернення 13.02.2023)

19 Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments. URL:

https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF (дата звернення 13.02.2023)

20 Лєсная Ю., Мисливцев К., Малахов С. Узагальнення можливостей протидії прийомам соціального інжинірингу, як інструменту реалізації інсайдерських загроз. Матеріали конференцій Молодіжної наукової ліги. (2022). Вилучено із https://ojs.ukrlogos.in.ua/index.php/liga/article/view/17891

21 Михайленко, Д., Чорна, Т., Мелкозьорова, О. Сучасні тенденції кібератак на мережеві ресурси. Технології, інструменти та стратегії реалізації наукових досліджень: матеріали V Міжнародної наукової конференції. (с. 162-165). 24 лютого, 2023, Київ, Україна: МЦНД. - Вінниця: Європейська наукова платформа.

22 CrowdStrike Team. GLOBAL THREAT REPORT. URL: https://www.crowdstrike.com/global-threat-report/ (дата звернення 15.12.2022)

23 Data Breach Investigations Report. URL: https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf (дата звернення 15.12.2022)

24 Бегаль І. У 2022 році кількість кібератак на Україну зросла майже втричі. 90% хакерських груп з РФ контролюють силовики. Forbes Ukraine. URL: https://forbes.ua/news/v-2022-rotsi-kilkist-kiberatak-na-ukrainu-zrosla-mayzhe-vtrichi-90-khakerskikh-grup-z-rf-kontrolyuyut-siloviki-04052023-13454 (дата звернення 15.12.2022)

25 Укрінформ. Держспецзв'язку попереджає про кібератаку фейковими «оновленнями операційної системи». URL: https://www.ukrinform.ua/rubric-technology/3702479-derzspeczvazku-poperedzae-pro-kiberataku-fejkovimi-onovlennami-operacijnoi-sistemi.html (дата звернення 15.12.2022)

26 BRAD DRESS. Ukraine's millennial minister leads digital fight against Russia The Hill. URL: https://thehill.com/policy/defense/3961775-ukraines-millennial-minister-leads-digital-fight-against-russia/ (дата звернення 15.12.2022)

27 Lance Whitney. What it costs to hire a hacker on the Dark Web | TechRepublic. URL: https://www.techrepublic.com/article/what-it-costs-to-hire-a-hacker-on-the-dark-web/ (дата звернення 20.03.2023)

28 Cedric Pernet. 2022 Dark Web prices for cybercriminals services | TechRepublic. URL: https://www.techrepublic.com/article/dark-web-prices/ (дата звернення 20.03.2023)

29 Богданова Є., Михайленко Д. ОГЛЯД ПРОБЛЕМАТИКИ ВИКОРИСТАННЯ ЕКСПЛОЙТІВ. Теоретичне та практичне застосування результатів сучасної науки: матеріали III Міжнародної студентської наукової конференції, м. Біла Церква, 7 жовтня, 2022 рік / ГО «Молодіжна наукова ліга». – Вінниця: ГО «Європейська наукова платформа», 2022. – 332 с. DOI 10.36074/liga-inter-07.10.2022

30 Cisco. What Is Malware? - Definition and Examples. URL: https://www.cisco.com/site/us/en/products/security/what-is-malware.html (дата звернення 20.03.2023)

31 OWASP Foundations. OWASP Top Ten. URL: https://owasp.org/www-project-top-ten/ (дата звернення 20.03.2023)

32 Богданова, Є., Чорна, Т., Малахов, С. (2022). Огляд поточного стану загроз, що обумовлені впливом експлойтів. Комп'ютерні науки та кібербезпека, (2), 35-40. https://periodicals.karazin.ua/cscs/article/ view/21039/19745

33 Лахтін, І., Михайленко, Д., & Нарєжній, О. (2022). Порівняння комерційних сканерів вразливостей веб-додатків та сканерів з відкритим кодом. Комп'ютерні науки та кібербезпека, (2), 41-49. https://periodicals.karazin.ua/cscs/article/view/21040/19746

34 Погоріла К.В., Богданова Є.С.,Колованова Є.П. Огляд можливостей та узагальнення специфіки реалізації XDR-технології, як засобу комплексної протидії актуальним загрозам інформаційної безпеки. Технології, інструменти та стратегії реалізації наукових досліджень: матеріали IV Міжнародної наукової конференції, м. Суми, 7 жовтня, 2022 р. / Міжнародний центр наукових досліджень. – Вінниця: Європейська наукова платформа, 2022. - 142 с. DOI10.36074/mcnd-07.10.2022

35 10 Best XDR Solutions: Extended Detection And Response Services In 2022. URL: https://www.softwaretestinghelp.com/xdr-security-solutions/ (дата звернення: 30.09.2022).

36 Рузудженк С., Погоріла К., Кохановська Т., Малахов С. Особливості захисту корпоративних ресурсів за допомогою технології Honeypot // Комп'ютерні науки та кібербезпека. 2020. № 4. С. 22-29. URL: https://periodicals.karazin.ua/cscs/article/view/15751

37 CrowdStrike team. HONEYPOTS IN CYBERSECURITY EXPLAINED. URL: http://surl.li/hpjhd (дата звернення 20.03.2023)

38 Кохановська Т., Нарежний О., Дьяченко О. Дослідження можливостей технології Honeypot // Комп'ютерні науки та кібербезпека. 2020. № 1 (1). С. 33-42. URL: https://periodicals.karazin.ua/cscs/article/view/16170

39 A Guide To Cybersecurity Deception Techniques. URL: https://www.blumira.com/cybersecurity-deception-techniques/ (дата звернення 20.03.2023)

40 Pawlick J., Zhu Q. Deception by Design: Evidence-Based Signaling Games for Network Defense. URL: https://arxiv.org/pdf/1503.05458v1.pdf

41 Ferguson-Walter K. J., Major M. M., Johnson C. K., Muhleman D. H. Examining the Efficacy of Decoy-based and Psychological Cyber Deception. URL: https://www.usenix.org/system/files/sec21-ferguson-walter.pdf

42 Shields Up: A Good Cyber Defense Is an Active Defense. URL: https://www.mitre.org/news-insights/impact-story/shields-good-cyber-defense-active-defense (дата звернення 01.06.2023)

43 Attivo Networks ThreatDefend Platform. URL: https://citrixready.citrix.com/attivo-networks/threatdefend-platform.html (дата звернення 01.06.2023)

44 Beyond Threat Detection and Response | One Step Ahead of Attackers. URL: https://www.countercraftsec.com (дата звернення 01.06.2023)

45 Михайленко Д., Чорна Т. ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ AI ПРИ РЕАЛІЗАЦІЇ STATIC ТА DYNAMIC HONEYPOT ДЛЯ ПОКРАЩЕННЯ ПАРАМЕТРІВ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ. Технології, інструменти та стратегії реалізації наукових досліджень: матеріали IV Міжнародної наукової конференції, м. Суми, 7 жовтня, 2022 р. / Міжнародний центр наукових досліджень. – Вінниця: Європейська наукова платформа, 2022. – 142 с. DOI10.36074/mcnd-07.10.2022

46 Искусственный интеллект в кибербезопасности. URL:: https://dou.ua/lenta/articles/ai-in-cybersecurity/ (дата звернення 01.06.2023)

47 Zakaria W., Kiah L.M. A review on artificial intelligence techniques for developing intelligent honeypot. URL: http://dx.doi.org/10.2306/scienceasia1513-1874.2013.39S.001.

48 Zakaria W., Kiah L.M. A review of dynamic and intelligent honeypots. Science Asia. 39s. 1-5. 10.2306 / scienceasia 1513 - 1874.2013.39S.001. URL: http://surl.li/hpjhq

49 GitHub - paralax/awesome-honeypots: an awesome list of honeypot resources : веб-сайт. URL:: https://github.com/paralax/awesome-honeypots (дата звернення 30.09.2022)

50 Михайленко Д., Нємцев М. Особливості технології мережевих пасток як інструменту активного захисту та аналізу дій атакуючої сторони. Proceedings of the XXI International Scientific and Practical Conference. Melbourne, Australia – 2023 – Pp. 483-487 – URL: https://isg-konf.com/scientists-and-methods-of-using-modern-technologies/
Available at: DOI: 10.46299/ISG.2023.1.21

51 HSRP vs VRRP vs GLBP Protocols – GeeksforGeeks. URL: https://www.geeksforgeeks.org/hsrp-vs-vrrp-vs-glbp-protocols/ (дата звернення 01.06.2023)

52 Access Control Lists (ACL) Explained / Cisco Community. URL: https://community.cisco.com/t5/networking-knowledge-base/access-control-lists-acl-explained/ta-p/4182349 (дата звернення 01.06.2023)

53 Information Sciences Institute. RFC 791: Internet Protocol / World Wide Web Consortium // University of Southern California, Admiralty Way, del Rey, California 90291 : веб-сайт. URL: https://www.rfc-editor.org/rfc/rfc791 (дата звернення 01.06.2023)

54 Scappy. URL: https://scapy.net/ (дата звернення 01.06.2023)

ДОДАТОК А

МАТЕРІАЛИ
IV МІЖНАРОДНОЇ
НАУКОВОЇ КОНФЕРЕНЦІЇ

МЦНД
Міжнародний Центр Наукових Досліджень

ТЕХНОЛОГІЇ, ІНСТРУМЕНТИ
ТА СТРАТЕГІЇ РЕАЛІЗАЦІЇ
НАУКОВИХ ДОСЛІДЖЕНЬ

7 ЖОВТНЯ 2022 РІК
м. Суми, Україна

Вінниця, Україна
«Європейська наукова платформа»
2022

Технології, інструменти та стратегії реалізації наукових досліджень

СЕКЦІЯ VIII.
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ

ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ AI ПРИ РЕАЛІЗАЦІЇ STATIC TA DYNAMIC HONEYPOT ДЛЯ ПОКРАЩЕННЯ ПАРАМЕТРІВ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Михайленко Дмитро Денисович
студент факультету комп'ютерних наук (бакалаврат)
Харківський національний університет імені В.Н. Каразіна, Україна

Чорна Тетяна Едуардівна
студентка факультету комп'ютерних наук (бакалаврат)
Харківський національний університет імені В.Н. Каразіна, Україна

Науковий керівник: Малахов Сергій Віталійович
канд. техн. наук, доцент кафедри безпеки інформаційних систем і технологій, старший науковий співробітник
Харківський національний університет імені В.Н. Каразіна, Україна

Тенденції та темпи розвитку сучасного світу сприяють до масштабного переходу багатьох життєвих, промислових та бізнес процесів в онлайн формат. Як наслідок - спостерігається постійне розширення можливостей хакерів та підвищення їх «інтересу» до ресурсів, що мають будь-яку цінність. Із кожним днем хакери удосконалюють існуючі атаки та знаходять нові. Спеціалістам в області захисту інформації доводиться практично в режимі нон-стоп вивчати новий «матеріал», щоб мати уявлення про актуальні загрози та останні методики атак, що, нажаль, не усуває ймовірність виявлення існуючих вразливостей через багато років [1-2].

Ці обставини перетворюють процес забезпечення потрібного рівня інформаційної безпеки (ІБ) у евристику, де «захиснику» необхідно захиститись від невідомості. В певної мірі одним із шляхів вирішенням даної проблеми є використання можливостей технології *HoneyPot* (*далі HP*) [3-5]. Вперше описана в роботі «*The Cuckoo's Egg*», ця технологія пропонувала створити пастку для хакера. Відвертаючи увагу атакуючого зловмисника на відповідним чином підготовлений, підставний ресурс-пастку, з'являється можливість вивчити можливості, інструменти та модель поведінки цього зловмисника. На основі отриманих даних основний ресурс може бути модифікований таким чином, щоб максимально ефективно перешкоджати подібним інцидентам в подальшому. Крім того, поки атакуюча сторона витрачає свій час на пастку, фахівці справжнього ресурсу можуть провести модифікацію його захисту та/або змінити алгоритми поведінки самої пастки, що ще більше ускладнює роботу зловмисника, стосовно досягнення бажаної їм цілі.

При використанні *HP*, фахівцю необхідно провести налаштування середовища для максимальної схожості з реальним джерелом, оскільки в іншому випадку зловмисник швидко зрозуміє, що має справу лише з аватаром бажаного ресурсу. Тому,

Рисунок А.1 — Наукове видання [45], сторінка 54

СЕРТИФІКАТ
УЧАСНИКА

МЦНД

Михайленко Дмитро Денисович

взяв(-ла) участь у IV Міжнародній науковій конференції
ТЕХНОЛОГІЇ, ІНСТРУМЕНТИ ТА СТРАТЕГІЇ РЕАЛІЗАЦІЇ НАУКОВИХ ДОСЛІДЖЕНЬ
7 ЖОВТНЯ 2022 РОКУ ♦ СУМИ, УКРАЇНА

ВІЦЕ-ПРЕЗИДЕНТ МЦНД
ГОЛОВА ОРГКОМІТЕТУ
РАБЕЙ НАСТАСІЯ

МЦНД
МІЖНАРОДНИЙ ЦЕНТР НАУКОВИХ ДОСЛІДЖЕНЬ

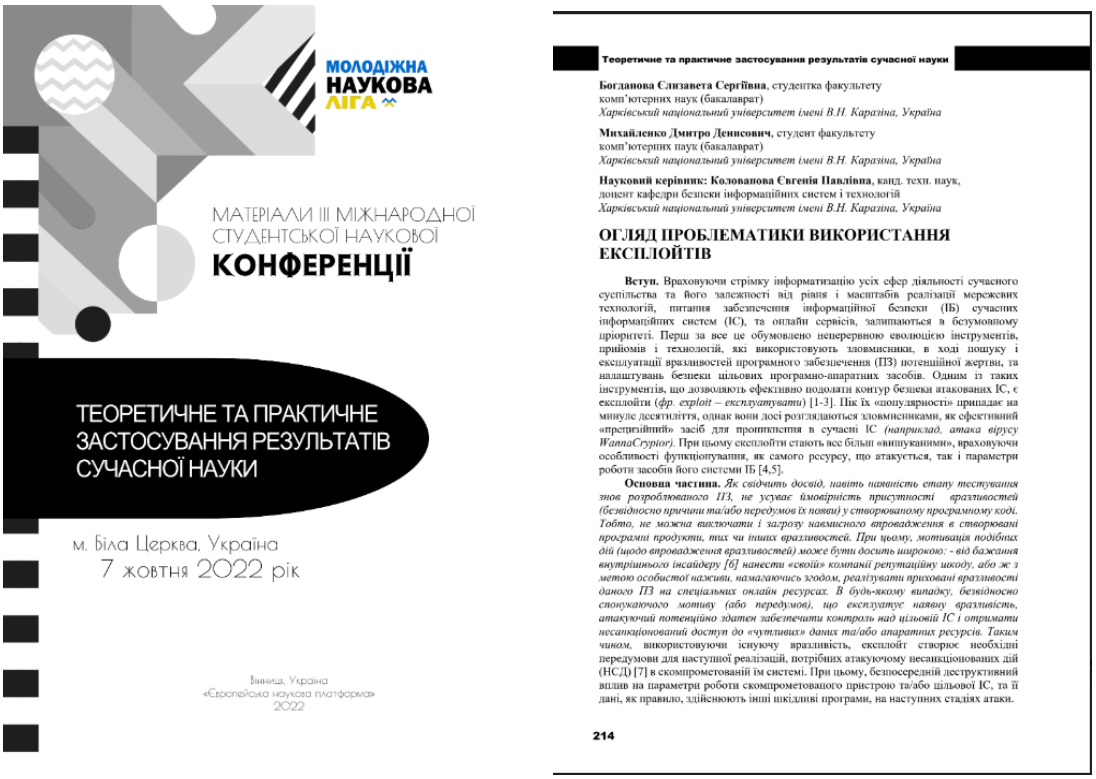
Матеріали учасника конференції опубліковані та знаходяться у відкритому доступі за посиланням:
https://doi.org/10.36074/mcnd-0710.2022

Організаційний комітет конференції рекомендує на підставі цього сертифікату зарахувати не менше 0,1 кредиту ЄКТС за результатами самоосвіти, як форми професійного навчання, науково-педагогічним та педагогічним працівникам, державним службовцям та іншим фахівцям, що проходять стажування.

Посвідчення ЯкріНТЕІ
№ 343 від 29.08.2022

МІЖНАРОДНИЙ ЦЕНТР НАУКОВИХ ДОСЛІДЖЕНЬ

Рисунок А.2 – Сертифікат участі для роботи [45]



МОЛОДІЖНА НАУКОВА ЛІГА

МАТЕРІАЛИ III МІЖНАРОДНОЇ СТУДЕНТСЬКОЇ НАУКОВОЇ
КОНФЕРЕНЦІЇ

ТЕОРЕТИЧНЕ ТА ПРАКТИЧНЕ ЗАСТОСУВАННЯ РЕЗУЛЬТАТІВ СУЧАСНОЇ НАУКИ

м. Біла Церква, Україна
7 жовтня 2022 рік

Вінниця, Україна
«Європейська наукова платформа»
2022

Теоретичне та практичне застосування результатів сучасної науки

Богданова Єлизавета Сергіївна, студентка факультету комп'ютерних наук (бакалаврат)
Харківський національний університет імені В.Н. Каразіна, Україна

Михайленко Дмитро Денисович, студент факультету комп'ютерних наук (бакалаврат)
Харківський національний університет імені В.Н. Каразіна, Україна

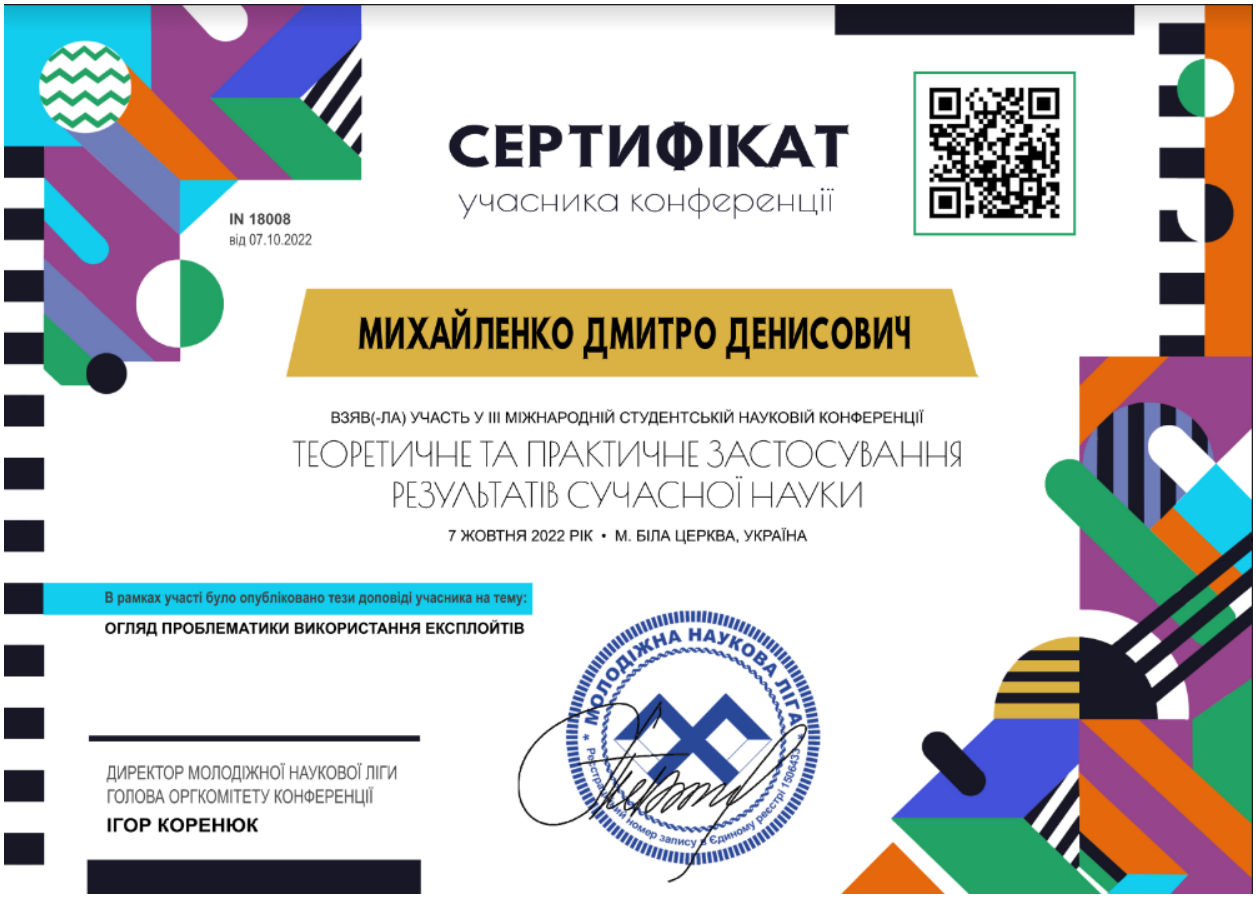
Науковий керівник: Колованова Євгенія Павлівна, канд. техн. наук, доцент кафедри безпеки інформаційних систем і технологій
Харківський національний університет імені В.Н. Каразіна, Україна

ОГЛЯД ПРОБЛЕМАТИКИ ВИКОРИСТАННЯ ЕКСПЛОЙТІВ

Вступ. Враховуючи стрімку інформатизацію усіх сфер діяльності сучасного суспільства та його залежності від рівня і масштабів реалізації мережевих технологій, питання забезпечення інформаційної безпеки (ІБ) сучасних інформаційних систем (ІС), та онлайн сервісів, залишаються в безумовному пріоритеті. Перш за все це обумовлено неперервною еволюцією інструментів, прийомів і технологій, які використовують зловмисники, в ході пошуку і експлуатації вразливостей програмного забезпечення (ПЗ) потенційної жертви, та налаштувань безпеки цільових програмно-апаратних засобів. Одним із таких інструментів, що дозволяють ефективно подолати контур безпеки атакованих ІС, є експлойти (*фр. exploit – експлуатувати*) [1-3]. Пік їх «популярності» припадає на минулі десятиліття, однак вони досі розглядаються зловмисниками, як ефективний «прецизійний» засіб для проникнення в сучасні ІС *(наприклад, атака вірусу WannaCryptor)*. При цьому експлойти стають все більш «вишуканими», враховуючи особливості функціонування, як самого ресурсу, що атакується, так і параметри роботи засобів його системи ІБ [4,5].

Основна частина. *Як свідчить досвід, навіть наявність етапу тестування знов розроблюваного ПЗ, не усуває ймовірність присутності вразливостей (безвідносно причини та/або передумов їх появи) у створюваному програмному коді. Тобто, не можна виключати і загрозу навмисного впровадження в створювані програмні продукти, тих чи інших вразливостей. При цьому, мотивація подібних дій (щодо впровадження вразливостей) може бути досить широкою: - від бажання внутрішнього інсайдеру [6] нанести «своїй» компанії репутаційну шкоду, або ж з метою особистої наживи, намагаючись згодом, реалізувати приховані вразливості даного ПЗ на спеціальних онлайн ресурсах. В будь-якому випадку, безвідносно спонукаючого мотиву (або передумов), що експлуатує наявну вразливість, атакуючий потенційно зможе забезпечити контроль над цільовій ІС і отримати несанкціонований доступ до «чутливих» даних та/або апаратних ресурсів. Таким чином, використовуючи існуючу вразливість, експлойт створює необхідні передумови для наступної реалізації, потрібних атакуючому несанкціонованих дій (НСД) [7] в скомпрометованій їм системі. При цьому, безпосередній деструктивний вплив на параметри роботи скомпрометованого пристрою та/або цільової ІС, та її дані, як правило, здійснюють інші шкідливі програми, на наступних стадіях атаки.*

Рисунок А.3 — Наукове видання [29], сторінка 214



СЕРТИФІКАТ
учасника конференції

IN 18008
від 07.10.2022

МИХАЙЛЕНКО ДМИТРО ДЕНИСОВИЧ

ВЗЯВ(-ЛА) УЧАСТЬ У III МІЖНАРОДНІЙ СТУДЕНТСЬКІЙ НАУКОВІЙ КОНФЕРЕНЦІЇ
ТЕОРЕТИЧНЕ ТА ПРАКТИЧНЕ ЗАСТОСУВАННЯ РЕЗУЛЬТАТІВ СУЧАСНОЇ НАУКИ
7 ЖОВТНЯ 2022 РІК • М. БІЛА ЦЕРКВА, УКРАЇНА

В рамках участі було опубліковано тези доповіді учасника на тему:
ОГЛЯД ПРОБЛЕМАТИКИ ВИКОРИСТАННЯ ЕКСПЛОЙТІВ

МОЛОДІЖНА НАУКОВА ЛІГА
Реєстраційний номер запису в Єдиному реєстрі 1586453

ДИРЕКТОР МОЛОДІЖНОЇ НАУКОВОЇ ЛІГИ
ГОЛОВА ОРГКОМІТЕТУ КОНФЕРЕНЦІЇ
ІГОР КОРЕНЮК

Рисунок А.4 – Сертифікат участі для роботи [29]

МАТЕРІАЛИ
V МІЖНАРОДНОЇ
НАУКОВОЇ КОНФЕРЕНЦІЇ

Міжнародний Центр Наукових Досліджень

ТЕХНОЛОГІЇ, ІНСТРУМЕНТИ ТА СТРАТЕГІЇ РЕАЛІЗАЦІЇ НАУКОВИХ ДОСЛІДЖЕНЬ

24 ЛЮТОГО 2023 РІК
м. Київ, Україна

Вінниця, Україна
«Європейська наукова платформа»
2023

Технології, інструменти та стратегії реалізації наукових досліджень

СЕКЦІЯ XVII.
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СИСТЕМИ

СУЧАСНІ ТЕНДЕНЦІЇ КІБЕРАТАК НА МЕРЕЖЕВІ РЕСУРСИ

Михайленко Дмитро Денисович
студент факультету комп'ютерних наук (бакалаврат)
Харківський національний університет імені В.Н. Каразіна, Україна

Чорна Тетяна Едуардівна
студентка факультету комп'ютерних наук (бакалаврат)
Харківський національний університет імені В.Н. Каразіна, Україна

Науковий керівник: Мелкозьорова Ольга Михайлівна
ORCID ID: 0000-0002-1134-2925
канд. техн. наук, доцент кафедри безпеки інформаційних систем і технологій
Харківський національний університет імені В.Н. Каразіна, Україна

Забезпечення потрібного рівня кібербезпеки при експлуатації інформаційно-телекомунікаційних систем є критично важливим напрямом діяльності в сучасному, технологічно залежному світі. Загроза кібератак стала постійною проблемою, як для окремих Інтернет користувачів, так і для корпоративних інформаційних ресурсів підприємств і державних структур. Сучасні кіберзловмисники постійно вдосконалюють тактику і методики нападу для крадіжки конфіденційної інформації, компрометації цільових систем і максимальної нанесення шкоди виробничим та бізнес процесам жертви.

Оскільки залежність сучасного інформаційного суспільства від технологій продовжує лише зростати, то вкрай важливо своєчасно робити відповідні кроки, стосовно розуміння сутності і способів реалізації відомих кібератак [1-3], щоб прогнозувати можливі дії в напряму нейтралізації потенційних загроз безпеки, на послідуючої інтеграції їх розвитку. Така робота охоплює ретельний аналіз загальних властивостей різних типів атак та постійне вдосконалення існуючих технологій і методик їх використання для своєчасного реагування на інциденти інформаційної безпеки (ІБ) різної природи, масштабів і наслідків [4-5].

В межах даного матеріалу проведено стислий розгляд найбільш часто використовуваних різновидів кібератак на мережеві корпоративні ресурси (далі Web-ресурси), та огляд відповідних заходів для їх протидії.

За даними *FireEye Labs* [6] найчастіше, хакерські атаки зачіпають такі галузі як: - фінансові установи, телекомунікації, виробництво і страхування. А відповідний звіт від *Positive Techonologies* [7], декілька доповнює даний перелік, додатково поширюючи його на такі галузі, як: - державні установи, освіта та медицина, відзначаючи, при цьому, що біля 67% відомих атак, мали яскраво виражений цілеспрямований характер. Атаки можуть бути націлені на широке коло потенційних жертв, від окремих користувачів до інформаційних систем підприємств та/або урядів.

Рисунок А.5 — Наукове видання [21], сторінка 162

СЕРТИФІКАТ УЧАСНИКА

Михайленко Дмитро Денисович

взяв(-ла) участь у V Міжнародній науковій конференції

ТЕХНОЛОГІЇ, ІНСТРУМЕНТИ ТА СТРАТЕГІЇ РЕАЛІЗАЦІЇ НАУКОВИХ ДОСЛІДЖЕНЬ

24 ЛЮТОГО 2023 РОКУ ♦ КИЇВ, УКРАЇНА

ВІЦЕ-ПРЕЗИДЕНТ МЦНД
ГОЛОВА ОРГКОМІТЕТУ
РАБЕЙ НАСТАСІЯ

МЦНД
МІЖНАРОДНИЙ ЦЕНТР НАУКОВИХ ДОСЛІДЖЕНЬ

Матеріали учасника конференції опубліковані та знаходяться у відкритому доступі за посиланням:
https://doi.org/10.36074/mcnd-24.02.2023

Організаційний комітет конференції рекомендує на підставі цього сертифікату зарахувати не менше 0,1 кредиту ЄКТС за результатами самоосвіти, як форми професійного навчання, науково-педагогічним та педагогічним працівникам, державним службовцям та іншим фахівцям, що проходять стажування.

Посвідчення №ДНТЕІ
№ 09 від 06.01.2023

МІЖНАРОДНИЙ ЦЕНТР НАУКОВИХ ДОСЛІДЖЕНЬ

Рисунок А.6 – Сертифікат участі для роботи [21]

ОСОБЛИВОСТІ ТЕХНОЛОГІЇ МЕРЕЖЕВИХ ПАСТОК ЯК ІНСТРУМЕНТУ АКТИВНОГО ЗАХИСТУ ТА АНАЛІЗУ ДІЙ АТАКУЮЧОЇ СТОРОНИ

Михайленко Дмитро Денисович
студент факультету комп'ютерних наук (бакалаврат)
Харківський національний університет імені В. Н. Каразіна, Україна

Немцев Максим Олександрович
студент факультету комп'ютерних наук (бакалаврат)
Харківський національний університет імені В. Н. Каразіна, Україна

Науковий керівник:
Малахов Сергій Віталійович
канд. техн. наук, ст. науковий співробітник, доцент кафедри
Харківський національний університет імені В.Н. Каразіна, Україна

Вступ. Темпи зростання числа кіберзагроз та постійне удосконалення використовуваних технік атаки програмно-апаратних ресурсів користувачів, ставлять сторону захисту у вкрай невигідне, відносно атакуючої сторони, становище. Фахівці у галузі інформаційної безпеки (ІБ) змушені постійно аналізувати відомості про нові інциденти безпеки та методи атак, якими зловмисники скористалися при реалізації чергової атаки. В цьому сенсі слід враховувати, що система реагування на інциденти безпеки побудована таким чином, що розслідування та притягнення до відповідальності відбувається вже після завдання збитків. Саме це надає хакерам суттєвий запас часу на підготовку атак, що забезпечує певну перевагу атакуючій стороні. Крім того, вдосконалення існуючих методів протидії новим способам здійснення атак, має ретроспективний характер, оскільки інформація про поточні загрози стає доступною лише після їх реалізації, що обумовлює певну пролонгованість циклу зворотних реакцій і модифікації наявних технологій захисту [1-4]. Саме тому у профільних фахівців з ІБ з'явилася ідея переходу від класичної (*пасивної або реактивної*) моделі захисту до активної моделі.

Основна частина. Активний захист - це нова модель захисту, яка передбачає використання технологій, що намагаються заздалегідь спровокувати зловмисників до їх виявлення та/або введення їх в пастку, замість того, щоб тільки захищати систему від вторгнень. Ця модель базується на активній взаємодії зловмисника *(або ресурсів зловмисника, наприклад бот-системи та/або бот-мережі)* та системи захисту потенційної жертви, де система захисту «намагається» змінити спосіб дій зловмисника або перехопити його дії. Це досягається шляхом використання в тому числі таких технологій, як *Honeypots* та *Honeynets* [5-6], що синтезують та використовують штучні пастки для потенційних зловмисників і таким чином намагаються перехопити їх дії.

Рисунок А.7 — Наукове видання [50], сторінка 483

Рисунок А.8 – Сертифікат участі для роботи [50]