

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій

(повне найменування факультету)

Кафедра інформаційної безпеки та наноелектроніки

(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)

магістр

(ступінь вищої освіти)

на тему Аналіз методик співпраці між Blue Team та Red Team в галузі кібербезпеки

(назва теми)

Виконав(ла): студент(ка) 6 курсу, групи БК-812м
Спеціальності 125 Кібербезпека

(код і найменування спеціальності)

Освітня програма (спеціалізація)

Безпека інформаційних і комунікаційних систем

ЧУХНО.І.С.

(ПРІЗВИЩЕ та ініціали)

Керівник НЕЛАСА Г.В.

(ПРІЗВИЩЕ та ініціали)

Рецензент

(ПРІЗВИЩЕ та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
Кафедра інформаційної безпеки та наноелектроніки
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека
(код і найменування)
Освітня програма (спеціалізація) Безпека інформаційних і комунікаційних систем
(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

В.о. завідувача кафедри ІБтаН

Андрій КОРОТУН

«_____» _____ 20__ року

З А В Д А Н Н Я

НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

ЧУХНА Івана Сергійовича

(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Аналіз методик співпраці між Blue Team та Red Team в галузі кібербезпеки..

Analysis of collaboration methods between Blue Team and Red Team in cybersecurity

керівник проєкту роботи к.т.н., доцент НЕЛАСА Ганна Вікторівна,

(науковий ступінь, вчене звання, ПРИЗВИЩЕ, ім'я, по батькові)

затверджені наказом закладу вищої освіти від «28» листопада 2023 року № 475

2. Строк подання студентом проєкту (роботи) «08» грудня 2023 року

3. Вихідні дані до проєкту (роботи) Blue Team, Red Team, Offensive Security, Defensive Security, фреймворк, payload, OWASP

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Провести аналіз методів та підходів до співпраці між Red Team та Blue Team, визначити переваги та недоліки, розробити ряд рекомендацій для підвищення рівню безпеки в кіберпросторі

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів) Ілюстративний матеріал, презентація(12 слайдів)

6. Консультанти розділів проєкту (роботи)

Розділ	ПРИЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-4	НЕЛАСА Г. В., доцент кафедри ІБтаН	10.09.2023	01.12.2023
Нормоконтроль	КОРОЛЬКОВ Р. Ю., доцент кафедри ІБтаН		05.12.2023

7. Дата видачі завдання «10» вересня 2023 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Складання та затвердження завдання на дипломну роботу	10.09.23 – 17.09.23	
2	Підбір інформації та літератури, що відповідає отриманому завданню	18.09.23 – 26.09.23	
3	Огляд нормативно-правової бази	27.09.23 – 10.10.23	
4	Описування основних принципів та засад на яких ґрунтується захист кіберпростору	11.10.23 – 15.10.23	
5	Дослідження напрямків Offensive Security та Defensive Security	16.10.23 – 25.10.23	
6	Аналіз методів співпраці між Red Team та Blue Team	26.10.23 – 11.11.23	
7	Формулювання висновків	12.11.23 – 21.11.23	
8	Оформлення пояснювальної записки	22.11.23 – 27.11.23	
9	Оформлення дипломної роботи	28.11.23 – 05.12.23	

Студент(ка)

(підпис) Іван ЧУХНО
(Ім'я ПРИЗВИЩЕ)

Керівник проєкту (роботи)

(підпис) Ганна НЕЛАСА
(Ім'я ПРИЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до магістерської роботи : 89 с., 14 рис., 3 табл., 49 джерела.

АКТИВНА ОБОРОНА, ЗАХИСНА ОБОРОНА, КІБЕРБЕЗПЕКА, ЧЕРВОНА КОМАНДА, МЕТАСПЛОЙТ, СИНЯ КОМАНДА, СИСТЕМА ЗАПОБІГАННЯ ПРОНИКНЕННЯ, ФІШИНГ

Об'єкт дослідження – взаємодія між Blue Team і Red Team в контексті кібербезпеки. Аналізуються процеси співпраці, обміну інформацією та результативності цих команд, які відповідають за захист інформаційних систем та симуляцію кібератак.

Мета роботи – аналіз переваг та недоліків стратегії співпраці між Blue Team та Red Team в контексті кібербезпеки. Робота спрямована на визначення оптимальних стратегій та ефективних підходів для захисту інформаційних систем в умовах постійно зростаючого ризику кіберзагроз.

Методи дослідження – наукова модель для вивчення теоретичних аспектів співпраці команд, аналіз і синтез для розкриття ключових положень, формалізацію для систематизації вимог до захисту інформації в умовах кібербезпеки, порівняння для об'єктивної оцінки переваг і недоліків методів співпраці команд, та метод системного підходу для комплексного розгляду взаємодії Blue Team та Red Team.

ABSTRACT

Explanatory note to the master's thesis: 89 pages, 14 figures, 3 tables, 49 sources.

BLUE TEAM, CYBERSECURITY, DEFENSIVE SECURITY, INTRUSION PREVENTION SYSTEM, METASPLOIT, OFFENSIVE SECURITY, PHISHING, RED TEAM

The object of the research is the interaction between the Blue Team and Red Team in the context of cybersecurity. The processes of collaboration, information exchange, and the effectiveness of these teams responsible for protecting information systems and simulating cyber attacks are analyzed.

The aim of the study is to analyze the advantages and disadvantages of cooperation between the Blue Team and Red Team in the context of cybersecurity. The research aims to determine optimal strategies and effective approaches for protecting information systems in the face of constantly increasing cyber threat risks.

Research methods include scientific abstraction for studying theoretical aspects of team collaboration, analysis and synthesis for elucidating key points, formalization for systematizing information security requirements in cybersecurity conditions, comparison for objectively assessing the advantages and disadvantages of team collaboration methods, and a systems approach method for a comprehensive examination of the interaction between the Blue Team and Red Team.

ЗМІСТ

Перелік скорочень.....	8
Вступ.....	9
1 Основи кібербезпеки.....	10
1.1 Нормативно-правова база.....	11
1.2 Основні поняття та визначення.....	22
1.3 Огляд головних фреймворків	33
Висновки до 1 розділу.....	38
2 Дослідження напрямку Red Team як складової Offensive Security.....	39
2.1 Визначення Offensive Security та основні принципи напрямку.....	40
2.2 Роль Offensive Security та вплив на кібербезпеку.....	41
2.3 Огляд тактик, методів та процедур, що використовуються в Offensive Security.....	43
2.4 Розбір основних технік та інструментів, що використовуються в Offensive Security.....	45
Висновки до 2 розділу.....	52
3 Дослідження напрямку Blue Team як складової Defensive Security.....	53
3.1 Визначення Defensive Security та основні принципи напрямку.....	54
3.2 Роль Defensive Security та вплив на кібербезпеку	55
3.3 Дослідження методів захисту кіберпростору.....	56
3.4 Розбір основних інструментів, що використовуються в Defensive Security.....	57
Висновки до 3 розділу.....	67
4 Аналіз співпраці між Blue Team та Red Team.....	68
4.1 Розбір організації інфраструктури для співпраці.....	68
4.2 Аналіз стратегії Red Team під час заходу.....	70
4.3 Аналіз стратегії Blue Team під час заходу.....	72

4.4 Координація між командами.....	73
4.5 Дослідження реального випадку співпраці між командами.....	74
4.6 Аналіз переваг та недоліків співпраці заходів червоний-проти-синього.....	78
Висновки до 4 розділу.....	79
Висновки.....	81
Перелік джерел посилань.....	85

ПЕРЕЛІК СКОРОЧЕНЬ

- ЛУЦ – Ланцюг ураження цілі;
- ШПЗ - Шкідливе програмне забезпечення;
- AD - Active Directory (Активна директорія);
- BYOD - Bring Your Own Device (Принеси свій девайс);
- C2 - Command and Control (Фреймворк командування та контролю);
- CIA - Confidentiality, Integrity, Availability (Конфіденційність, цілісність та доступність);
- DoS - Denial-of-Service (Відмова в обслуговуванні);
- DDoS - Distributed Denial-of-Service (Атака на відмову в обслуговуванні);
- HIDS - Host Intrusion Detection System (Система виявлення проникнень на основі хосту);
- IDS - Intrusion Detection System (Система виявлення проникнень);
- IPS - Intrusion Prevention System (Система запобігання проникнень);
- LDS - Lightweight Directory Services (Спрощений сервіс дерикторій);
- NIDS - Network Intrusion Detection System (Система виявлення проникнень на основі мережі);
- NIST - National Institute of Standards and Technology (Національний інститут стандартів та технологій);
- OffSec - Offensive Security (Активна оборона);
- OSINT - Open Source Intelligence (Розвідка на основі відкритих джерел);
- OWASP - Open Web Application Security Project (Відкритий проект безпеки вебзастосунків);
- SOC - Security Operations Center (Операційний центр безпеки);
- TTPs - Tactics, Techniques, and Procedures (Тактики, техніки та процедури);
- ZT - Zero Trust (Нульова довіра).

ВСТУП

В сучасному динамічному цифровому середовищі, де кібербезпека стає необхідністю для забезпечення стабільності та надійності інформаційних систем, актуальність вивчення та розуміння механізмів захисту від кіберзагроз набуває особливого значення. У цьому контексті, співпраця між Blue Team, яка забезпечує захист інформаційних систем, та Red Team, що спеціалізується на симуляції кібератак, визнається як ключовий елемент ефективного кіберзахисту.

Один із головних аспектів безпеки інформаційних систем — це забезпечення конфіденційності та захист від несанкціонованого доступу до даних. Сучасний прогрес у розробці методів електронної ідентифікації та автентифікації, спрямованих на вдосконалення систем захисту інформації, свідчить про необхідність постійного аналізу та оновлення стратегій в цьому напрямі. У світлі цих викликів, мета магістерської роботи полягає у глибокому аналізі переваг та недоліків сучасної стратегії співпраці між Blue Team та Red Team у контексті кібербезпеки.

Розглядання взаємодії цих команд дозволить визначити оптимальні стратегії для максимально ефективного захисту інформаційних систем в умовах постійно зростаючого ризику кіберзагроз. Під час дослідження акцент буде зроблено на взаємодію, обмін інформацією та результативність співпраці між командами, з метою визначення оптимальних підходів до виявлення та запобігання кібератак. Такий аналіз стане важливим внеском у поле кібербезпеки, сприяючи підвищенню загального рівня захищеності інформаційних систем в умовах сучасного цифрового суспільства.

1 ОСНОВИ КІБЕРБЕЗПЕКИ

У сучасному цифровому світі питання інформаційної безпеки є однією з найбільш актуальних та складних проблем. Забезпечення конфіденційності, цілісності та доступності інформації стало викликом у зв'язку з постійним розвитком технологій та розширенням кількості загроз кібербезпеки. У цьому контексті, розгляд аспектів загального стану інформаційної безпеки є необхідним для розуміння величезного спектру викликів та можливостей, які стоять перед сучасними організаціями та суспільством в цілому.

Зростання кількості та складності кіберзагроз, таких як віруси, хакерські атаки, фішинг та інші форми кіберзлочинності, ставлять під сумнів ефективність існуючих заходів інформаційної безпеки. Динамічність сучасного середовища вимагає постійного оновлення та адаптації заходів забезпечення безпеки для виявлення та запобігання новим загрозам.

Електронна ідентифікація та автентифікація вирізняються серед ключових аспектів забезпечення інформаційної безпеки. Здатність ефективно та безпечно ідентифікувати та автентифікувати користувачів стає критичною для запобігання несанкціонованому доступу та збереження конфіденційності інформації.

Огляд поточної законодавчо-нормативної бази в галузі інформаційної безпеки визначає основні рамки, які регулюють заходи забезпечення інформаційної безпеки на різних рівнях, від державних до відомчих та прикладних.

Розгляд сучасних викликів, з якими стикаються системи інформаційної безпеки, дозволяє визначити ключові області для подальшого дослідження та розвитку. Розгляд аспектів глобальних тенденцій та перспектив може визначити напрямки для подальших стратегій та заходів інформаційної безпеки.

1.1 Нормативно-правова база

У сучасному цифровому суспільстві, де інформаційні технології стають не лише необхідністю, але й основним рушієм розвитку, важливість належної законодавчо-нормативної бази для регулювання сфери інформаційної безпеки надто очевидна. З ростом обсягів цифрового обміну та зростанням кількості онлайн-процесів, Україна активно залучається до розробки та постійного вдосконалення цієї бази. Це стає стратегічно важливим кроком для надійного захисту конфіденційної інформації від сучасних кіберзагроз, а також для забезпечення високого рівня кібернетичної стійкості та безпеки всіх сфер життєдіяльності країни.

Україна приділяє велику увагу захисту критичної інформаційної інфраструктури та особистих даних. Деякі ключові закони та нормативи в цій сфері включають: «Про інформацію»; «Про захист персональних даних»; «Про захист інформації в інформаційно-телекомунікаційних системах»; «Про електронні довірчі послуги»; «Про національну безпеку України»; «Про основні засади забезпечення кібербезпеки України».

Законом України «Про інформацію» регулюються вимоги щодо створення, обробки, поширення та захисту інформації. Основні визначення з цього закону [1]:

- Інформація - «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді»;
- Захист інформації - «сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї»;
- Інформація про фізичну особу (персональні дані) - «відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована».

За статтею 20, інформація поділяється на відкриту та інформацію з обмеженим доступом. Також ця стаття визначає «будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом» [1]. Стаття 21 визначає, що «інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація» [1].

Законом України «Про захист персональних даних» регулюються «правові відносини, пов'язані із захистом і обробкою персональних даних» [2]:

- Персональні дані - «відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована»;
- Обробка персональних даних - «будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем».

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» регулюються «відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» [3]:

- Інформаційна (автоматизована) система - «організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів»;
- Інформаційно-комунікаційна система - «сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле»;
- Електронна комунікаційна система - «сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання та/або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб»;

- Комплексна система захисту інформації - «взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації»;
- Обробка інформації в системі - «виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів»;
- Порушення цілісності інформації в системі - «несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст»;
- Несанкціоновані дії щодо інформації в системі - «дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства».

Закон України про «Про електронні довірчі послуги» визначає «правові та організаційні засади надання електронних довірчих послуг, у тому числі транскордонних, права та обов'язки суб'єктів правових відносин у сфері електронних довірчих послуг, порядок здійснення державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг, а також правові та організаційні засади здійснення електронної ідентифікації» [4]:

- Автентифікація - «електронна процедура, яка дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-комунікаційної системи та/або походження та цілісність електронних даних»;
- Пара ключів - «особистий та відповідний йому відкритий ключі, що є взаємопов'язаними параметрами алгоритму асиметричного криптографічного перетворення»;
- Відкритий ключ - «параметр алгоритму асиметричного криптографічного перетворення, який використовується як електронні дані

для перевірки електронного підпису чи печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів»;

– Особистий ключ - «параметр алгоритму асиметричного криптографічного перетворення, який використовується як унікальні електронні дані для створення електронного підпису чи печатки, доступний тільки підписувачу чи створювачу електронної печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів»;

– Електронна довірча послуга - «послуга, яка надається для забезпечення електронної взаємодії двох або більше суб'єктів, які довіряють надавачу електронних довірчих послуг щодо надання такої послуги»;

– Електронна ідентифікація - «процедура використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або представника юридичної особи»;

– Електронний підпис - «електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис»;

– Ідентифікація особи - «процедура використання ідентифікаційних даних особи з документів, створених на матеріальних носіях, та/або електронних даних, в результаті виконання якої забезпечується однозначне встановлення фізичної, юридичної особи або представника юридичної особи»;

– Електронна печатка - «електронні дані, які додаються створювачем електронної печатки до інших електронних даних або логічно з ними пов'язуються і використовуються для визначення походження та перевірки цілісності пов'язаних електронних даних»;

– Електронна послуга - «будь-яка послуга, що надається через інформаційно-комунікаційну систему»;

– Засіб електронного підпису чи печатки - «апаратно-програмний або апаратний пристрій чи програмне забезпечення, які використовуються для створення та/або перевірки електронного підпису чи печатки»;

- Користувачі електронних довірчих послуг - «підписувачі, створювачі електронних печаток, відправники та отримувачі електронних даних, інші фізичні та юридичні особи, які отримують електронні довірчі послуги у надавачів таких послуг відповідно до вимог цього Закону»;
- Надавач електронних довірчих послуг - «юридична особа незалежно від організаційно-правової форми та форми власності, фізична особа - підприємець, яка надає одну або більше електронних довірчих послуг»;
- Самопідписаний сертифікат відкритого ключа - «сертифікат відкритого ключа, який формується центральним засвідчувальним органом або засвідчувальним центром з використанням особистого ключа центрального засвідчувального органу або засвідчувального центру»;
- Сертифікат відкритого ключа - «електронний документ, який засвідчує належність відкритого ключа фізичній або юридичній особі, підтверджує її ідентифікаційні дані та/або надає можливість здійснити автентифікацію веб-сайту»;
- Схема електронної ідентифікації - «система електронної ідентифікації, в якій засоби електронної ідентифікації видаються фізичним, юридичним особам та представникам юридичних осіб».

Розділ III стаття 14 цього закону передбачає засоби електронної ідентифікації, а саме [4]:

- «Електронна ідентифікація здійснюється за допомогою засобів електронної ідентифікації, що підпадають під схему електронної ідентифікації, затверджену Кабінетом Міністрів України»;
- «Міжнародні договори України щодо електронних довірчих послуг повинні передбачати порядок подання повідомлень та визнання схем електронної ідентифікації (із зазначенням рівня довіри для засобів електронної ідентифікації)».

Стаття 15 розділу III визначає схему електронної ідентифікації [4]:

а) «Схема електронної ідентифікації визначається Кабінетом Міністрів України»;

б) «Схема електронної ідентифікації повинна встановлювати високий, середній або низький рівні довіри до засобів електронної ідентифікації»:

- 1) «Низький рівень довіри до засобів електронної ідентифікації повинен характеризувати засоби електронної ідентифікації в контексті схеми електронної ідентифікації, яка забезпечує обмежений ступінь довіри до заявлених або затверджених ідентифікаційних даних і описується з посиланням на технічні специфікації, стандарти і процедури, що до неї відносяться, включаючи технічні засоби контролю, призначенням яких є зниження ризику зловживання або спростування ідентичності»;
- 2) «Середній рівень довіри до засобів електронної ідентифікації повинен характеризувати засоби електронної ідентифікації в контексті схеми електронної ідентифікації, яка забезпечує суттєвий ступінь довіри до заявлених або затверджених ідентифікаційних даних і описується з посиланням на технічні специфікації, стандарти і процедури, що до неї відносяться, включаючи технічні засоби контролю, призначенням яких є істотне зниження ризику зловживання або спростування ідентичності»;
- 3) «Високий рівень довіри до засобів електронної ідентифікації повинен характеризувати засоби електронної ідентифікації в контексті схеми електронної ідентифікації, яка забезпечує найвищий ступінь довіри до заявлених ідентифікаційних даних особи і описується з посиланням на технічні специфікації, стандарти і процедури, що до неї відносяться, включаючи

технічні засоби контролю, призначенням яких є запобігання зловживанню повноваженнями або підміні особи»;

в) «Використання кваліфікованих електронних підписів та печаток забезпечує високий рівень довіри до схем електронної ідентифікації. Використання удосконалених електронних підписів та печаток забезпечує середній рівень довіри до схем електронної ідентифікації».

Закони України «Про національну безпеку України» та «Про основні засади забезпечення кібербезпеки України» регулюють кіберзахист об'єктів критичної інфраструктури. Головні терміни [5,6]:

— Стратегія кібербезпеки України - документ довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави»;

— Індикатори кіберзагроз - «показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози»;

— Інцидент кібербезпеки (далі - кіберінцидент) - «подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів»;

— Інформація про інцидент кібербезпеки - «відомості про обставини кіберінциденту, зокрема про те, які об'єкти кіберзахисту і за яких умов зазнали кібератаки, які з них успішно виявлені, нейтралізовані, яким запобігли за

допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз»;

– Кібератака - «спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту»;

– Кібербезпека - «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі»;

– Кіберзагроза - «наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів»;

– Кіберзахист - «сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем»;

– Кіберзлочин (комп'ютерний злочин) - «суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України»;

– Кіберпростір - «середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних».

Стаття 4 визначає об'єкти кібербезпеки [6]:

- Конституційні права і свободи людини і громадянина;
- Суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;
- Держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;
- Національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;
- Об'єкти критичної інфраструктури.

Об'єкти кіберзахисту:

- Комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;
- Об'єкти критичної інформаційної інфраструктури;
- Комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Принципи забезпечення кібербезпеки визначає стаття 7 [6]:

- Верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом;
- Забезпечення національних інтересів України;
- Відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі;
- Державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері;
- Пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід’ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі;
- Пріоритетності запобіжних заходів;
- Невідворотності покарання за вчинення кіберзлочинів;
- Пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;
- Міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях;
- Забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки.

Стаття 12 зазначає «Особи, винні у порушенні законодавства у сферах національної безпеки, електронних комунікацій та захисту інформації, якщо

кіберпростір є місцем та/або способом здійснення кримінального правопорушення, іншого винного діяння, відповідальність за яке передбачена цивільним, адміністративним, кримінальним законодавством, несуть відповідальність згідно із законом» [6].

Необхідно дотримуватися цих правил, щоб захистити людей від несанкціонованого доступу та експлуатації їхніх даних, а також захистити їхню конфіденційність. Щоб переконатися, що наші дослідницькі дії відповідають законодавству та не порушують його положення, нам потрібно знати про ці закони. У зв'язку з тим, що невиконання цих законів може призвести до цивільних чи кримінальних санкцій, люди повинні добре ознайомитися з законами та розуміти можливі наслідки своїх дій. Крім того, важливо, щоб дослідницькі діяльності відповідали цим законам, щоб захистити конфіденційність осіб і запобігти можливому зловживанню їх даними. Кібербезпечні дослідники можуть гарантувати, що дані людей залишаються безпечними та їхні права захищені, дотримуючись цих законів і виявляючи обережність під час проведення дослідницьких заходів.

1.2 Основні поняття та визначення

Оскільки значна частина наших повсякденних дій і операцій переноситься до віртуального середовища, кібербезпека стає не тільки найважливішою, але й надзвичайно складною сферою в сучасному цифровому суспільстві. З цієї переорієнтації виникають нові проблеми з безпекою інформаційних систем і даних. Кібербезпека — це комплекс заходів і методів, спрямованих на забезпечення конфіденційності, цілісності та доступності даних, а також постійного адаптування до змін, які відбуваються в кібератаках і кіберзагрозах.

З кожним днем кількість кіберзагроз і атак постійно зростає, ставлячи під загрозу не лише окремих користувачів, але й великі підприємства та державні організації. У зв'язку з тим, що вони є основними елементами у сфері цифрової безпеки, основні принципи та ідеї кібербезпеки стають важливими компонентами стратегій виявлення, запобігання та відповіді на кіберзагрози. Збереження конфіденційності, цілісності та доступності інформації є життєво важливим завданням, тому необхідно постійно удосконалювати стратегії та застосовувати найновіші технології, щоб забезпечити найвищий рівень безпеки.

На сьогоднішній день визначення основних ідей і принципів безпеки у кіберпросторі стало не лише надійним, але й важливим компонентом стратегій, що реагують на постійні зміни кіберзагроз. Основні ідеї, такі як цілісність, доступність і конфіденційність даних (C.I.A Triad рис. 1.1), не лише визначають основні елементи кібербезпеки, але й стають центром уваги при розробці та вдосконаленні заходів захисту. Крім того, авторизація та аутентифікація, які працюють разом, встановлюють стандарти ідентифікації та доступу, запобігаючи несанкціонованому доступу.

Для ефективного захисту Кібер ланцюг вбивці (КЛВ) визначає етапи кібератак. Крім того, концепції типу Zero Trust (ZT) впроваджують новий рівень підходу до безпеки, вимагаючи постійного моніторингу та переосмислення стратегій у зв'язку зі зростанням загроз. Системи управління доступом, такі як Active Directory (AD), стають необхідними інструментами для ефективного реалізації принципів безпеки. Цей поєднаний набір понять визначає не лише сучасні стратегії кібербезпеки, але і акцентує на важливості постійного розвитку та вдосконалення заходів захисту перед постійно змінюючимися кіберпейзажем.

Для забезпечення конфіденційності організація повинна вживати заходів для того, щоб зберігати дані у секреті або приватності. Для досягнення цього інформаційний доступ повинен бути обмежений, щоб зупинити розповсюдження даних без авторизації, якщо це необхідно або випадково.

Забезпечення того, що особи без необхідного дозволу не можуть отримати доступ до активів, які є важливими для вашої компанії, є ключовою частиною збереження конфіденційності. З іншого боку, добре функціонуюча система також переконується, що правильні люди мають відповідні права доступу. Наприклад, електронні таблиці, банківські рахунки та інші дані, пов'язані з рухом грошей, повинні бути доступні для осіб, які відповідають за фінансові питання організації. Проте доступ може не надаватися великій більшості інших співробітників, і навіть деяким керівникам. Обмеження щодо того, хто може бачити що, повинні бути строгими, щоб гарантувати виконання цих політик. «Конфіденційність може бути порушена кількома способами. Це може включати прямі атаки, спрямовані на отримання доступу до систем, які нападник не має права переглядати. Крім того, це може включати спроби нападника безпосередньо отримати доступ до бази даних або застосунку для крадіжки чи модифікації даних» [7]. Порушення конфіденційності не завжди є навмисними. Слабкі заходи безпеки чи людська помилка також можуть бути причиною. Наприклад, хтось може забути захистити пароль, яким вони використовують доступ до робочого місця чи обмеженої зони. Користувачі можуть вибрати передавати свої дані для входу третім особам або дозволяти комусь бачити їх під час входу в систему. У інших випадках користувач може невірно зашифрувати комунікацію, що дозволить атакуючому перехопити їхні дані. Крім того, злодій може взяти апаратне забезпечення — комп'ютер як ціле або окремих пристрій входу — та використовувати його для отримання доступу до конфіденційних даних.

Збереження цілісності означає забезпечення того, що ваші дані надійні та незмінені. Тільки коли дані є правдивими, точними та надійними, зберігається їхній цілісний стан. Наприклад, інформація про вищих керівників, яку ваш бізнес публікує на своєму веб-сайті, повинна бути точною. Якщо вона є неправдивою, люди, які шукають інформацію на вашому веб-сайті, можуть прийти до висновку, що ваша компанія ненадійна. Особа, яка має особистий інтерес пошкодити репутацію вашої компанії, може спробувати взломати ваш

веб-сайт і змінити біографії виконавчого персоналу, зображення чи посадові титули для завдання шкоди їхній честі чи репутації компанії в цілому. Цілісність часто навмисно порушується. Атакуючий може змінювати конфігурації файлів, щоб дозволити несанкціонований доступ, обходити систему виявлення вторгнень (IDS) або змінювати системні журнали, щоб приховати атаку. Інциденти також можуть порушувати цілісність. Є можливість, що хтось необачно введе неправильний код або зробить щось інше. «Недостатні політики безпеки, засоби захисту та процедури в компанії також можуть призводити до порушень цілісності, не покладаючи вини на конкретного члена організації» [7].

Дані часто не мають сенсу, якщо вони недоступні для осіб у межах компанії та їхніх клієнтів, навіть у випадках, коли забезпечено конфіденційність та цілісність. Це означає, що програми, мережі та системи повинні працювати тоді і як повинні. Крім того, інформацію не повинно бути важко доступати, і ті, хто має до неї доступ, повинні мати можливість використовувати її, коли це потрібно. Доступність може бути ускладнена, наприклад, якщо відсутній план відновлення після катастрофи, який допоміг би користувачам знову отримати доступ до важливих систем у випадку відключення електроенергії. Крім того, користувачі можуть бути не в змозі отримати доступ до своїх робочих станцій та інших пристроїв, які надають додатки чи інформацію, важливу для функціонування бізнесу, через природну катастрофу, таку як повінь чи навіть сильний снігопад. Умисні акти саботажу, такі як використання викупувального програмного забезпечення або атак типу «відмова в обслуговуванні» (DoS), також можуть піддавати ризику доступність.

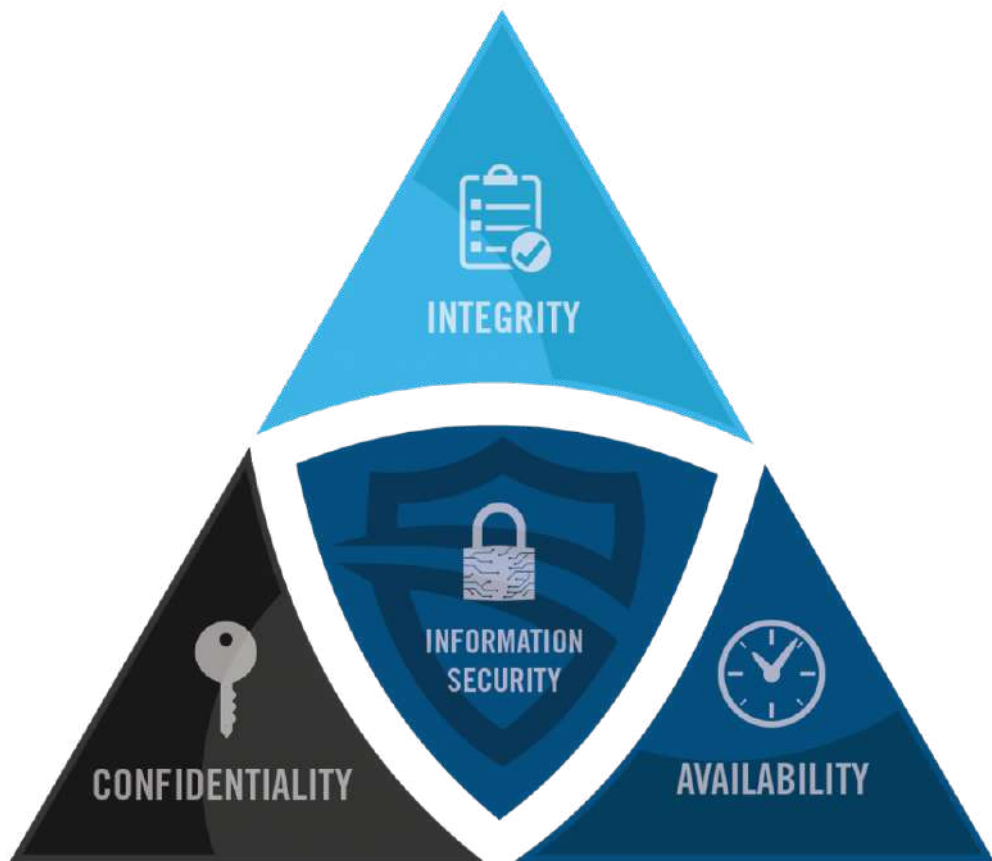


Рисунок 1.1 - C.I.A Triad [49]

Ланцюг ураження цілі (ЛУЦ), «створений компанією Lockheed Martin, є частиною моделі «Інтелектуально-орієнтована оборона», яка використовується для виявлення та припинення кібер-вторгнень» [8]. Модель визначає необхідні кроки, які вживають атакувальники для досягнення своєї мети. Сім кроків ЛУЦ, що зображено на рис. 1.2, покращують розуміння аналітика щодо тактик, методів та процедур противника, надаючи також можливість виявлення самої атаки.

Перший етап у ланцюгу кібератак, відомий як «розвідка, передбачає дослідження можливих цілей перед проведенням будь-якого тестування на проникнення» [8]. Визначення можливих об'єктів, визначення їх вразливостей, встановлення, які сторонні сторони пов'язані з ними та яку інформацію вони можуть отримати і перевірка як відомих, так і потенційно нових точок входу -

це можливі задачі на етапі розвідки. Розвідка може проводитися як в онлайн-режимі, так і офлайн.

Етап озброєння починається після завершення розвідувальних дій і того, як атакуючий зібрав усю необхідну інформацію про можливі цілі, включаючи вразливості. Всі попередні зусилля атакуючого об'єднуються для створення зброї, яку можна використовувати проти конкретної цілі під час етапу озброєння. Процес озброєння може включати розробку абсолютно нового вірусу або модифікацію вже існуючих інструментів для використання в кібератаках. Наприклад, для розробки нового інструменту ЛУЦ злочинці в інтернеті можуть внести невеликі зміни до вже існуючого варіанту вірусу-вимагача.

Третій етап - доставка. «Шкідливе програмне забезпечення(ШПЗ) та інші інструменти ланцюга кібератак використовуються для проникнення в мережу цілі та отримання доступу до користувачів під час етапу доставки» [8]. Доставка може включати відправку фішингових електронних листів зі зловмисними вкладеннями та привабливими темами для отримувачів. Також доставка може відбуватися шляхом вторгнення в мережу компанії та використання вразливостей програмного чи апаратного забезпечення для проникнення всередину.

Після етапів доставки та озброювання настає етап експлуатації. На етапі експлуатації ЛУЦ атаки зловмисники використовують виявлені вразливості з попередніх фаз для подальшого порушення мережі цільового об'єкта та досягнення своїх цілей. Під час цього процесу кіберзлочинці часто переміщуються поперек мережі, щоб дістатися до своїх цілей. У деяких випадках експлуатація може направляти зловмисників до їхніх цілей, якщо адміністратори мережі не застосували методи обману.

Після того як хакери отримали доступ до мережі цільової системи, використовуючи її вразливості, вони розпочинають етап установки в рамках КЛІВ, намагаючись проникнути в мережу цільової системи за допомогою шкідливого програмного забезпечення та інших кіберзасобів для заволодіння

її системами та крадіжки важливих даних. На цьому етапі хакери можуть використовувати інтерфейси командного рядка, троянські коні або задні двері для встановлення шкідливого програмного забезпечення та кіберзасобів.

Кіберзлочинці взаємодіють з ШПВ, яке вони врізали в мережу цільового об'єкта під час етапу керівництва та контролю (C2) ЛУЦ для надання інструкцій ШПЗ чи інструментам, щоб вони могли досягти своїх цілей. Наприклад, «атакуючі можуть використовувати канали зв'язку для надсилання інструкцій машинам, інфікованим ШПЗ Mirai, щоб вони відправляли велику кількість трафіку на веб-сайт або сервери C2, щоб машини виконували конкретні кіберзлочинні завдання» [8].

Остання фаза ЛУЦ - це момент, коли кіберзлочинці виконують свої цілі кібератаки після того, як вони створили ШПЗ, розгорнули її в мережі цільової організації та отримали контроль над цією мережею. Мети кіберзлочинців відрізняються в залежності від типу кібератаки, проте деякі приклади включають використання вимагання викупу як інструменту для кіберексторшингу, розгортання шкідливого програмного забезпечення для викрадання конфіденційних даних від цільової організації та озброєння ботмережі для руйнування послуг за допомогою атак розподіленої відмови в обслуговуванні (DDoS).



Рисунок 1.2 – Ланцюг ураження цілі [44]

Термін «Zero Trust» відноситься до набору еволюційних парадигм кібербезпеки, які орієнтовані на захист користувачів, активів та ресурсів, а не на статичні, мережеві периметри. Промислова та корпоративна інфраструктура та робочі процеси проектуються з використанням принципів

нульової довіри за допомогою архітектури нульової довіри. Концепція нульової довіри передбачає, що не надається імпліцитна довіра активам чи обліковим записам користувачів лише на підставі фізичного розташування активів: локальні мережі проти Інтернету, їх статусу власності: особисті чи корпоративні, чи їхнього мережевого розташування. Перед встановленням сеансу доступу до ресурсу підприємства виконуються окремі процеси аутентифікації та авторизації (як для пристрою, так і для суб'єкта). «Ця концепція є реакцією на тенденції в корпоративних мережах, такі як хмарні активи, які не розташовані в межах корпоративної мережі, віддалені користувачі та пристрої «принеси свій власний» (BYOD)» [11]. Оскільки мережеве розташування вже не розглядається як основний фактор у визначенні безпекової позиції ресурсу, «Zero Trust» надає більше уваги захисту ресурсів: активи, послуги, робочі процеси, мережеві облікові записи тощо, ніж мережевим сегментам.

На основі рекомендацій Національного інституту стандартів та технологій ZT націлене на вирішення наступних основних концепцій [10]:

- «Постійне підтвердження. Перевірка доступ до всіх ресурсів у будь-який час»;
- «Встановлення «радіуса зони пошкодження». Зменшення збитків у разі внутрішнього чи зовнішнього порушення»;
- «Автоматизація збору контексту та відповіді. Для найточніших відповідей враховується поведінкові дані та отримується контекст з усієї ІТ-інфраструктури».

Підхід «довіряй, але перевіряй» до традиційної мережевої безпеки в значній мірі витіснився ZT. Звичайний метод надавав користувачам та кінцевим точкам всередині периметру організації автоматичну довіру, що залишало компанію вразливою перед зловживанням зловмисників всередині та крадіжкою дійсних облікових даних ззовні. Це також надавало несанкціонованим та компрометованим обліковим записам широкий доступ, як тільки вони потрапляли всередину. Цю модель застарілою зробило

прискорення розподіленого робочого середовища та перехід до хмарної міграції ініціатив бізнес-трансформації у 2020 році, спричинене пандемією.

Правила ZT повністю полягають на принцип постійного нагляду за атрибутами юзерів [10]:

- Ім'я користувача та тип облікового запису (програмний, людський);
- Дозволи для облікових записів на кожному пристрої;
- Типовий зв'язок між пристроєм та обліковим записом (патерни поведінки);
- Тип та функція апаратного забезпечення кінцевих точок;
- Географічне розташування;
- Версії прошивки;
- Ризик та протокол аутентифікації;
- Рівні оновлень та версії операційних систем;
- Встановлені програми на кінцевій точці;
- Виявлення проблем безпеки чи інцидентів, таких як ідентифікація підозрілої активності та атак.

В середовищі Windows Server Active Directory (AD) є «службою каталогів. Файли, користувачі, групи, периферійні пристрої та мережеві пристрої - лише кілька комп'ютерних та мережевих ресурсів, які можна знаходити, захищати, керувати та організовувати за допомогою цієї розподіленої ієрархічної структури бази даних» [12].

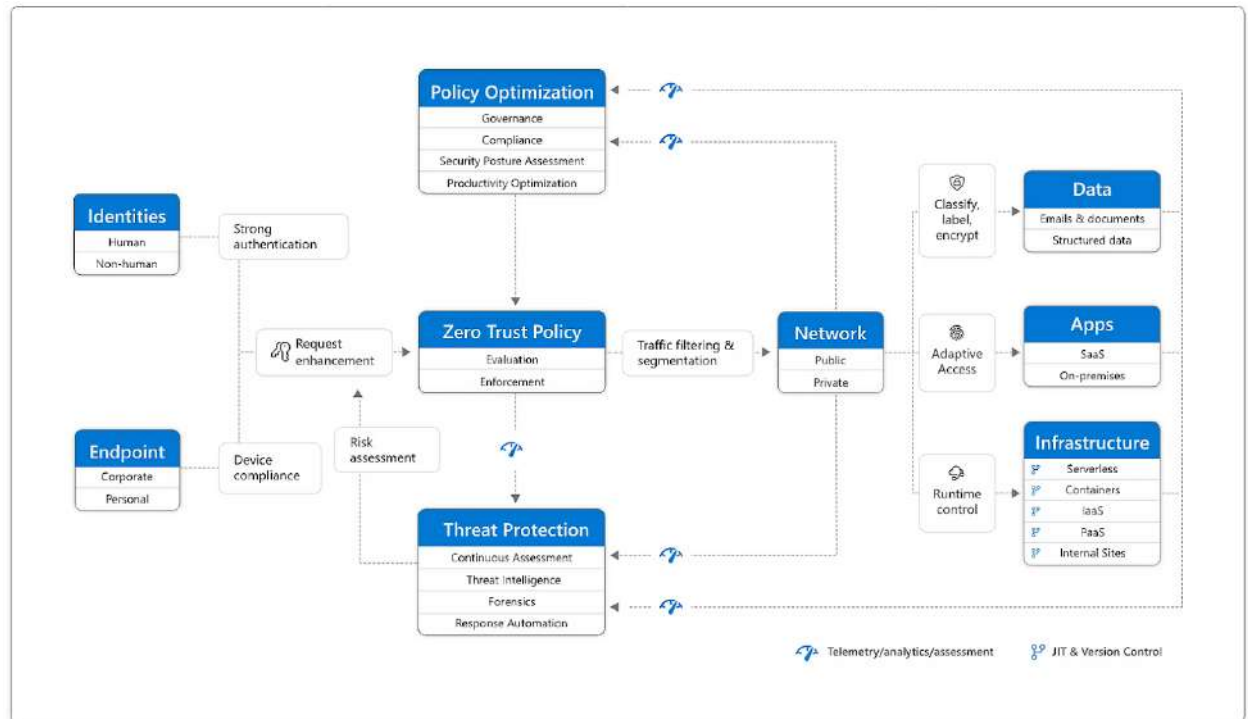


Рисунок 1.3 - Модель Zero Trust від Microsoft [9]

Власна служба каталогів Microsoft - Active Directory, призначена для використання в мережах Windows-домени. Окрім того, вона надає основу для інших подібних служб і виконує завдання авторизації та аутентифікації. Об'єкти мережі зберігаються в каталозі, який є базою даних LDAP. Windows Server - це операційна система, на якій працює AD. До появи Windows 2000 модель авторизації та аутентифікації компанії Microsoft вимагала сегментації мережі на домени та їх з'єднання через складну, іноді нестабільну систему одно- та двосторонніх довір. У Windows 2000 була впроваджена AD як засіб надання каталогових служб для більш обширних та складних середовищ». С того часу Microsoft постійно додає нові сервіси до свого продукту [12].

1. Легка служба каталогів для Active Directory (LDS) - це спрощена версія служби каталогів, яка надає лише базовий функціонал без використання контролерів доменів, лісів або доменів. Ця легка версія служби допомагає зменшити складність та обмежити функціонал на основні опції. Зазвичай

використовується в мережесередовищах із однією або двома невеликими офісами.

2. Служби сертифікатів для Active Directory - сервіси сертифікатів для AD підтримують інфраструктуру відкритого ключа, і надають послуги цифрового сертифікату. Замість того, щоб генерувати ключі локально або зовнішньо, цей сервіс може зберігати, перевіряти, створювати та анулювати публічні ключові облікові записи, які використовуються для шифрування.

3. Служби для Active Directory Federation - надають послугу одноразового входу, веб-орієнтовану службу аутентифікації та авторизації, яка призначена переважно для використання організаціями різного розміру. У зв'язку з цим підрядник може увійти в свою власну мережу та отримати дозвіл на доступ до мережі клієнта.

4. Служби для управління правами в Active Directory - ця служба управління правами обмежує те, що користувач може робити з конкретними файлами чи документами та розбиває авторизацію за межі моделі наданого чи відхиленого доступу. Права та обмеження не пов'язані з користувачем, але зв'язані з документом. Загальні використання цих прав включають зупинку друку, копіювання та створення знімків екрану документів.

Підмножина ресурсів домену може бути об'єднана під управлінням одиниці організації. Хоча вона надає бар'єр безпеки щодо підвищених привілеїв та авторизації, одиниці організації не мають впливу на реплікацію об'єктів у AD.

Для делегування повноважень у межах функціональних груп використовуються одиниці організації. Хоча домени повинні використовуватися для управління реплікацією AD, одиниці організації повинні використовуватися для впровадження та обмеження безпеки та ролей у групах. Структура одиниць організації наведена на рис. 1.4.

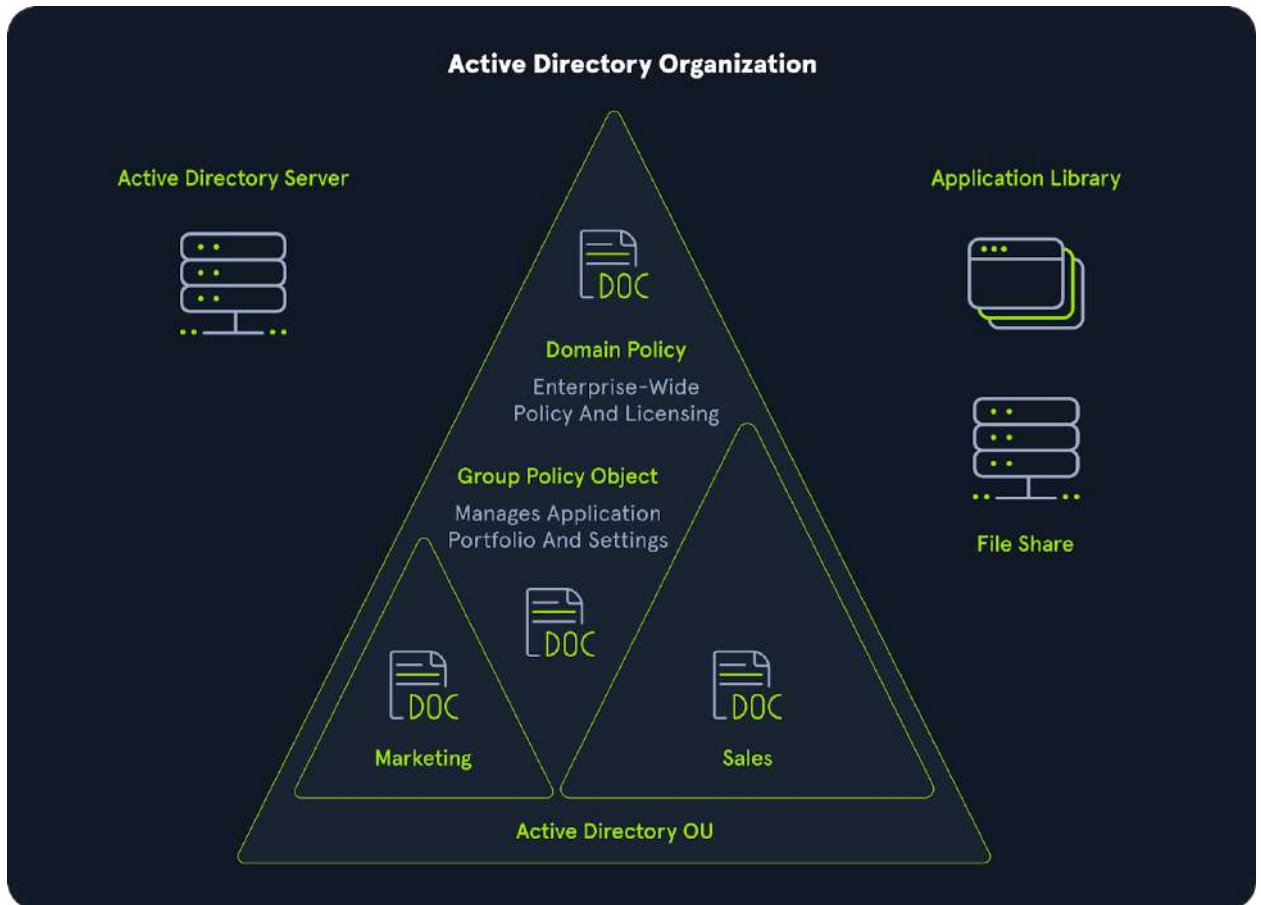


Рисунок 1.4 - Організація Active Directory[45]

1.3 Огляд головних фреймворків

Кібербезпекові фреймворки - це збірки документів, які визначають стандарти, найкращі практики та рекомендації для управління ризиками в галузі кібербезпеки. Метою цих фреймворків є зменшення вразливості організації перед дефектами та вразливостями, які можуть бути використані хакерами та іншими злочинцями в онлайн.

Залежно від потрібної функції існують три різновиди фреймворків:

а) Фреймворк контролю:

- 1) створює базовий план для кібербезпекового відділу компанії;

- 2) надає базовий набір заходів безпеки;
 - 3) оцінює існуючу інфраструктуру та технології на сьогоднішній день;
 - 4) надає пріоритет реалізації контролю за безпекою;
- б) Програмний фреймворк:
- 1) оцінює програму безпеки організації в її поточному стані;
 - 2) створює всеосяжну кібербезпекову програму;
 - 3) оцінює конкурентне оточення та безпеку програми;
 - 4) робить комунікацію між керівниками та виконавчими директорами та командою кібербезпеки простішою та зручнішою;
- в) Фреймворк ризиків:
- 1) визначає процедури, необхідні для управління та оцінки ризиків;
 - 2) розробляє програму безпеки для обробки ризиків;
 - 3) визначає, оцінює та розраховує ризики безпеки, з якими стикається компанія;
 - 4) надає належний пріоритет заходам та заходам безпеки.

Сьогодні одними з найкращих фреймворків вважаються наступні фреймворки.

1. NIST - Компанії в приватному секторі можуть використовувати добровільні стандарти безпеки від NIST для виявлення, визнання та усунення кібератак. У рамках цього фреймворку також містяться рекомендації для допомоги організаціям у запобіганні та відновленні після кібератак.

2. The Center for Internet Security Critical Security Controls (CIS) - підходить для малого бізнесу, який за часом планує розширюватися. Цей фреймворк був створений наприкінці 2000-х років для захисту бізнесу від онлайн-небезпек. Він складається з двадцяти контролів, які регулярно оновлюються експертами з безпеки з різних галузей: уряду, промисловості та академії. Спочатку йде основний розділ фреймворка, за яким слідує

організаційний розділ. З метою відображення стандартів безпеки та надання альтернативних конфігурацій для організацій, які звільнені від обов'язкових протоколів безпеки, але все ще прагнуть підвищити кібербезпеку, CIS використовує відповідники, що базуються на широко визнаних стандартах, таких як HIPAA та NIST.

3. The International Standards Organization (ISO) frameworks ISO/IEC 27001 and 27002(ISO 270K) - вважається, що це є глобально прийнятий стандарт для перевірки кібербезпеки як внутрішньо, так і серед зовнішніх сторін. Робота ISO 270K ґрунтується на наявності системи управління інформаційною безпекою в організації. Керівництво повинно ретельно керувати ризиками інформаційної безпеки своєї організації, зосереджуючись на загрозах і вразливостях, відповідно до стандартів ISO/IEC 27001. ISO 270K має високі вимоги. Фреймворк, який розділений на 14 категорій, пропонує 114 різних контролів. Завдяки обсягу роботи, необхідного для підтримки стандартів, ISO 270K може бути не підходящим для всіх. Однак він вартий уваги, якщо впровадження ISO 270K служить привабливою точкою для привертання нових клієнтів.

Також у галузі кібербезпеки існують вузьконаправлені фрейворки, створенні, щоб допомогти членам як Offensive Security, так і Defensive Security.

Metasploit - за допомогою Metasploit Framework спеціалісти можуть створювати, тестувати та виконувати експлойт-код. Це модульний інструменту для пентесту, побудованого на мові програмування Ruby. За допомогою інструментів у складі фреймворку можна проводити пентест заходи, виявляти вразливості в безпеці, проводити атаки та уникати виявлення. Metasploit Framework, в суті, є набором широко використовуваних інструментів [13,14], які надають комплексне середовище для розробки експлойтів та проведення пентесту. Фреймворк розроблено для використання в Offensive Security.

Таблиця 1.1 - Набір інструментів Metasploit

Exploits	Інструмент для отримання переваг за рахунок вразливостей системи
Payloads	Встановлює шкідливий код
Auxiliary functions	Допоміжні інструменти та команди
Encoders	Конвертує код або інформацію
Listeners	Шкідливе програмне забезпечення, що приховується для отримання доступу
Shellcode	Код який активується після потрапляння до цілі
Post-exploitation code	Допомагає посилити вплив на систему
Nops	Інструкція, яка запобігає від сбою під час використання payload

OWASP TOP 10 - це проект з безпеки веб-застосунків, він представляє собою звіт, який регулярно оновлюється і висвітлює десять найбільших ризиків безпеки, пов'язаних із безпекою веб-додатків. Група міжнародних спеціалістів з безпеки складає цей звіт. OWASP описує Топ-10 як «документ, спрямований на підвищення обізнаності» [15] та рекомендує всім підприємствам інтегрувати цей звіт у свою діяльність для зменшення та/або пом'якшення ризиків безпеки. Приклад 10 найбільших ризиків який востаннє змінювався у 2021 році.



Рисунок 1.6 - Головні вразливості веб-ресурсів у 2021 році [46]

В основному фреймворк використовують представники Defensive Security, проте його можна використати так само і в Offensive Security, для того щоб знайти тактику для виявлення вразливостей на веб-ресурсі

Mitre - Документована компіляція даних щодо зловживання тактик, які групи стійких загроз використовують на різних етапах реальних кібератак. Незважаючи на те, що «фреймворк не є моделлю загроз у традиційному розумінні, MITRE ATT&CK часто використовується організаціями як основа для створення власних індивідуальних моделей загроз» [16]. Це більше база даних, яка перераховує тактики, техніки та процедури (TTPs), якими користуються зловмисники, надає поради щодо ідентифікації та пом'якшення конкретних методик, а також висвітлює риси, відомі поведінки та атрибуції груп зловмисників. Крім того, ATT&CK надає всебічний перелік програмного забезпечення, яке використовується при атаках, включаючи відкритий та комерційно доступний код, який може бути використаний зловмисно або законно, а також шкідливе програмне забезпечення. «Кожен елемент даних, використаний в ATT&CK, збирається з публічно доступних звітів та даних, а також зі спільноти, до якої входять команди забезпечення безпеки та дослідники загроз, які перебувають на передовій і постійно зіштовхуються або аналізують атаки» [17].

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (3)	Abuse Elevation Control Mechanism (3)	Adversary-In-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-In-the-Middle
Gather Victim Host Information (4)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (5)	BITS Jobs	Access Token Manipulation (1)	Access Token Manipulation (1)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (1)
Gather Victim Identity Information (2)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture
Gather Victim Network Information (6)	Compromise Infrastructure (7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection
Gather Victim Org Information (4)	Develop Capabilities (2)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (1)	Compromise Client Software Binary	Direct Volume Access	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Clipboard	Clipboard
Search Closed Sources (2)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Create Account (2)	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Replication Through Removable Media	Data from Cloud Storage
Search Open Technical Databases (7)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (4)	Execution Guardrails (1)	Domain Policy Modification (2)	Modify Authentication Process (8)	Container and Resource Discovery	Software Deployment Tools	Data from Configuration Repository
Search Open Websites/Domains (3)	Trusted Relationship	Software Deployment Tools	Serverless Execution	Event Triggered Execution (14)	Escape to Host	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Debugger Evasion	Taint Shared Content	Data from Information Repository
Search Victim-Owned Websites	Valid Accounts (4)	External Remote Services	Shared Modules	Event Triggered Execution (14)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request Generation	Device Driver Discovery	Use Alternate Authentication Material (2)	Data from Local System
		System Services (3)	Software Deployment Tools	External Remote Services	Hijack Execution Flow (12)	Hide Artifacts (11)	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive
		User Execution (3)	System Services (3)	Hijack Execution Flow (12)	Impair Defenses (11)	Log Enumeration		Group Policy Discovery		Data from Removable

Рисунок 1.7 - Матриця АТТ&СК

Висновки до 1 розділу

Перший розділ нашої магістерської роботи визначив основні правові та концептуальні рамки, які регулюють кібербезпеку в Україні. Аналізуючи нормативно-правову базу, ми виявили, що Україна вдосконалює свої законодавчі інструменти для ефективного регулювання та захисту в кіберпросторі, щоб відповідати сучасним викликам і загрозам.

Далі, ми детально розглянули основні принципи та поняття у сфері кібербезпеки. Концепції, такі як CIA Triad, надають фундаментальні вказівки для забезпечення конфіденційності, цілісності та доступності інформації. Особлива увага була приділена таким інноваційним підходам, як Zero Trust та

використання Active Directory, що відображає сучасні тенденції у побудові надійних систем безпеки.

У другій частині розділу, ми вивчили важливі фреймворки, які визначають стандарти та методології в галузі кібербезпеки. NIST CIS, ISO 27001, Metasploit, OWASP та Mitre ATT&CK представляють собою необхідні інструменти для розробки ефективних стратегій захисту та виявлення кіберзагроз.

У цьому розділі ми з'ясували не тільки певні аспекти правового регулювання, але й важливі концепції та інструменти, які будуть розглянуті та розвинуті в подальших частинах нашого дослідження. Вивчення цих основ дало нам цінний фундамент для подальших аналізів та рекомендацій з покращення системи кібербезпеки.

2 ДОСЛІДЖЕННЯ НАПРЯМКУ RED TEAM ЯК СКЛАДОВОЇ OFFENSIVE SECURITY

Offensive Security є ключовим підходом у сфері кібербезпеки, що набуває все більшого значення в умовах постійно зростаючого рівня кіберзагроз. Цей підхід визначається як систематична практика, що полягає в використанні контрольованих атак для імітації реальних загроз з метою виявлення вразливостей та підвищення рівня стійкості інформаційних систем. Offensive Security виступає важливим елементом стратегії кіберзахисту, допомагаючи підвищити готовність до атак та зменшити ризики виникнення серйозних кіберінцидентів.

У межах Offensive Security використовується інноваційний підхід, спрямований на виявлення слабких місць інформаційних систем та ефективне управління цими ризиками. Цей процес включає в себе використання різноманітних технік, таких як етичне використання експлойтів, аналіз вразливостей та пентестинг, забезпечуючи повніший інсайт у реальний стан кіберзахисту організації.

Центральною метою Offensive Security є не лише імітація атак, але й постійне вдосконалення стратегій та заходів кіберзахисту. Цей підхід дозволяє пристосовувати заходи безпеки до зростаючих загроз та надає можливість керувати ризиками в умовах невизначеності. Offensive Security виступає критичним компонентом у багаторівневій системі кіберзахисту, де важливо не лише реагувати на загрози, але і активно передбачати їх та адекватно реагувати на їх еволюцію.

2.1 Визначення Offensive Security та основні принципи напрямку

Offensive Security (OffSec) представляє собою стратегічний підхід до кібербезпеки, що акцентується на систематичному використанні контрольованих атак для імітації реальних кіберзагроз. У контексті цього підходу, безпека стає не лише реактивною, але й активною сферою захисту інформаційних систем.

Одним із ключових принципів OffSec є постійний аналіз та перевірка безпеки систем. Це передбачає систематичне проведення пентестів, аналіз вразливостей та сценаріїв атак для активного виявлення слабких місць. Імітація атак дозволяє не лише виявляти потенційні загрози, але й адекватно готувати відповіді на їх можливе використання.

Другий принцип OffSec полягає в управлінні ризиками через реалістичне моделювання атак. Це включає в себе використання експлойтів, аналіз вразливостей, а також ефективний соціальний інженеринг. Організації, що дотримуються OffSec, не тільки реагують на виявлені загрози, але й активно працюють над зменшенням ймовірності їх виникнення.

Основна мета OffSec полягає в тому, щоб виявити та усунути потенційні вразливості до того, як вони можуть бути використані несанкціонованими суб'єктами для здійснення атак. Цей підхід визнає, що традиційні методи реагування на кіберзагрози не завжди дозволяють ефективно протистояти сучасним атакам, що стають більш вдосконаленими та складними. Замість цього, OffSec пропонує проактивний підхід, орієнтований на аналіз імітованих атак для покращення загального рівня безпеки.

Ще однією ключовою рисою Offensive Security є упорядкування інцидентів у контрольованому середовищі. Це передбачає створення сценаріїв, що імітують реальні ситуації, а також використання технік реальних атак для аналізу реакції інформаційно-безпечності системи. Такий підхід

дозволяє не лише імітувати ризиковані сценарії, але й ефективно оцінювати здатність системи реагувати на нові та еволюційні загрози.

Важливо підкреслити, що Offensive Security вимагає від організацій постійної готовності до викликів кіберпростору та активного залучення до аналізу власної інфраструктури на предмет слабкі місця. Це допомагає організаціям впроваджувати ефективні стратегії захисту, підвищуючи при цьому стійкість до потенційних кібератак та забезпечуючи безпеку інформаційних активів.

2.2 Роль Offensive Security та вплив на кібербезпеку

У контексті невинного розвитку кіберзагроз, роль OffSec у стратегії кіберзахисту стає необхідною та визначальною. Згідно із звітом «2022 Randori State of Offensive Security», який вивчає стан обороноздатності інформаційних систем, «67% організацій за останні два роки спостерігали зростання своєї атакованої поверхні» [20]. Слова експертів також підтверджують, що «відбувається постійне зростання витрат на кіберзлочинність. Очікується, що щорічні витрати на збитки від глобальної кіберзлочинності зростатимуть на 15% протягом наступних трьох років і досягнуть рівня \$10,5 трільйонів USD щорічно до 2025 року, що порівняно із \$3 трільйонами USD у 2015 році» [21]. Це свідчить про тенденцію до постійного розширення потенційних точок атак, що ставить під загрозу кібербезпеку підприємств. Додатково, «30% зазначених організацій визнали важкість ефективного управління обсягом нових вразливостей» [19], що демонструє необхідність активного використання OffSec для забезпечення надійного кіберзахисту та адаптації до швидко змінюючих кіберландшафту.

Цей підхід акцентує необхідність надання пріоритету не лише реактивним методам виявлення та відповіді на існуючі загрози, але й

систематичному виявленню потенційних ризиків за допомогою контрольованих атак та аналізу вразливостей. OffSec виникає як стратегічний інструмент, спрямований на активне підвищення стійкості інформаційних систем та ефективну підготовку до ризиків кібербезпеки.

У стратегічному вимірі, OffSec допомагає організаціям визначати критичні області, які можуть бути використані несанкціонованими суб'єктами для вторгнень або експлуатації. Це передбачає не лише аналіз внутрішніх вразливостей, але й врахування зовнішніх загроз, що дозволяє створити повний образ загрозового ландшафту. Сприяючи формуванню цього образу, OffSec дозволяє приймати інформовані рішення щодо розробки та вдосконалення заходів з кіберзахисту.

Крім того, OffSec є критичним інструментом для попередження кібератак, забезпечуючи організаціям можливість передбачити та адекватно реагувати на вразливості, які можуть бути використані в якості витоку для злоумисників. Його роль полягає не лише у виявленні, але й у систематичному оновленні і вдосконаленні заходів захисту, забезпечуючи узгоджений підхід до кібербезпеки.

2.3 Огляд тактик, методів та процедур, що використовуються в Offensive Security

Зловмисники використовують ті ж самі тактики, методи та процедури (TTPs), як і експерти Offensive Security. Фахівці OffSec можуть тестувати поточні програми забезпечення захисту, використовуючи ці TTP для виявлення потенційних вразливостей, які можуть експлуатувати реальні хакери. Стандарні TTPs складаються з [22].

1. Договірний етап - включає в себе внесення змін до контракту та надання клієнтові відповідної інформації. Кожен необхідний тест, разом з

усіма його компонентами, має точне визначення та документується у контракті. Під час особистої зустрічі чи конференц-виклику робляться різноманітні підготовки, включаючи:

- Мети угод про нерозголошення;
- Область проведення тестів;
- Оцінка часу;
- Правила участі.

2. Збір інформації - на різноманітні методи, які OffSec використовує для отримання даних про необхідні компоненти. З метою виявлення можливих дір в безпеці, які можна використовувати як точку входу, ведеться пошук інформації про цільову компанію, а також апаратне та програмне забезпечення, яке використовується;

3. Оцінка вразливостей - після переходу до етапу оцінки вразливостей аналізується результати етапу збору інформації, виявляючи відомі вразливості в системах, додатках та різних версіях кожного з них для виявлення можливих шляхів атаки. Оцінка вразливостей - це оцінка потенційних вразливостей, яка проводиться як вручну, так і з використанням автоматизованих засобів. Це використовується для визначення рівня загрози та вразливості мережевої інфраструктури компанії перед кібератаками;

4. Експлуатація - під час фази експлуатації тестується атаки на потенційні вектори та застосовуються отримані результати до цільових систем з метою отримання першого доступу до цих систем;

5. Пост-експлуатація - на даному етапі пентесту вже є доступ до скомпрометованої системи, і треба переконатися, що цей доступ залишиться непорушним навіть у випадку внесення змін. На цьому етапі ведеться пошук критичної інформацію, що становить для клієнта об'єкт захисту, таку як облікові дані, і спроби підняти привілеї для отримання максимальних прав доступу. Іноді пост-експлуатація виконується, щоб продемонструвати клієнту значущість доступу до системи. Час від часу пост-експлуатація здійснюється як складова частина процесу бічного переміщення;

6. Бічний рух - термін «бічний рух» використовується для опису переміщення в межах внутрішньої мережі цільової компанії з метою отримання доступу до додаткових вузлів з таким самим або вищим рівнем привілеїв. До досягнення мети це часто є ітераційним процесом, сплетеним з діями після експлуатації. Наприклад, вдається взяти під контроль веб-сервер, підвищити рівень доступу та виявити пароль в реєстрі. Проводяться додаткові перерахунки і встановлюємо, що цей пароль надає доступ локального адміністратора до сервера баз даних. Звідси можна подальше розширити свій доступ в мережу, отримуючи додаткові облікові дані та крадучи конфіденційну інформацію з бази даних. Зазвичай на цьому етапі використовуються різноманітні стратегії в залежності від даних, які можна отримати з компрометованого хоста чи сервера;

7. Підтвердження заходу - на цьому етапі ми фіксуємося всі кроки, які було виконано для досягнення компрометації мережі або отримання певного рівня доступу. Метою цього етапу є створення образу того, як вдалося ланцюгувати різноманітні вразливості для досягнення поставленої мети, щоб клієнт міг чітко усвідомити, як кожна вразливість впливає та допомогти визначити пріоритети для їхніх зусиль з усунення;

8. Післяпроектний етап - під час фази післяпроектного етапу створюється глибока документація, яка допомагає адміністраторам та керівництву клієнтської компанії зрозуміти серйозність виявлених вразливостей. На цьому етапі також видаляються всі сліди дій з усіх хостів та серверів. Генеруються звітні матеріали для клієнта, проводимо зустріч для розгляду звіту та, за необхідності, робиться виконавча презентація перед керівництвом цільової компанії. Зрештою, відповідно до контрактних обов'язків та корпоративної політики, архівуються дані тестування. Зазвичай ці дані зберігаються протягом певного часового періоду або до проведення оцінки післяліквідаційних заходів для підтвердження виправлень клієнта.

2.4 Розбір основних технік та інструментів, що використовуються Red Team

У сучасному динамічному кіберпросторі, де високотехнологічні інфраструктури переплітаються зі складними викликами кібербезпеки, важливим аспектом є впровадження стратегій, які не лише реагують на існуючі загрози, але й прогнозують та попереджають майбутні ризики. Red Team виступає ключовим гравцем у цьому контексті, використовуючи ряд вдосконалених технік та атак для імітації реальних кіберзагроз.

OSINT: Open Source Intelligence є стратегічним компонентом для «аналізу та збору відомостей з різних відкритих джерел, таких як соціальні мережі, публічні бази даних, новинні портали та інші публічно доступні ресурси» [24]. Цей підхід дозволяє отримувати контекстуалізовану інформацію про об'єкти дослідження, включаючи фізичні та цифрові аспекти, що стає важливим інструментом в контексті кібербезпеки, ділового аналізу та наукового дослідження. У зазначеному контексті, вивчення та розуміння методів, засобів та етичних вимог OSINT стає необхідним елементом для забезпечення надійності та ефективності цього процесу в сучасному цифровому середовищі. Єтичні хакери та зловмисники використовують різні веб-ресурси та фреймворки для збору публічної інформації:

- а) Веб-ресурси
 - 1) Shodan;
 - 2) Webmii;
 - 3) DarkSearch.io
 - 4) Ahmia;
- б) Фреймворки:
 - 1) Reacon-ng;
 - 2) Metagoofil;
 - 3) theHarvester.

Соціальний інжиніринг: «усі тактики, спрямовані на переконання цільової аудиторії розголошувати певну інформацію або виконувати конкретні дії з сумнівними мотивами» [23]. У кіберпросторі ця техніка використовується шляхом інформаційно-технологічних засобів для підтримки психологічних методик маніпуляції для досягнення цілі поза сферою ІТ, такої як отримання банківських облікових даних шляхом фішингової атаки з метою подальшого викрадення грошей цільової особи, або використовуючи психологічну маніпуляцію для отримання додаткового доступу до ІТ-системи, де фактична мета афериста знаходиться, наприклад, представляючись важливим клієнтом під час телефонного дзвінка з метою заманити цільову особу на відвідування шкідливого веб-сайту для інфікування робочої станції цільової особи [23].

Фішинг: це обманлива техніка, «при якій злочинець виступає в ролі надійної організації або особи у електронному листі чи іншій переписці» [25]. Атаки за допомогою фішингу часто використовуються зловмисниками для поширення шкідливих посилань або вкладень, що дозволяє їм отримати номери рахунків, логін даних та іншу особисту інформацію від потенційних жертв. В залежності від цілей та методів фішинг поділяється на [26].

1. Email phishing - цей тип атак, що є найпоширенішим видом фішингу, вводить отримувачів електронних листів в оману, використовуючи тактики, як підроблені гіперпосилання. Зловмисники часто виглядають як колеги по роботі чи провайдери основних облікових записів, таких як Microsoft або Google.

2. Malware phishing - цей вид атаки, який також є досить поширеним, передбачає внесення вірусів до прикріплення електронного листа, яке здається надійним (наприклад, банківський виписка чи резюме). Відкриття шкідливого прикріплення може в рідкісних випадках призвести до непрацездатності всіх ІТ-систем.

3. Spear phishing - у той час як спеціальний фішинг використовує інформацію, отриману в результаті дослідження соціального та професійного

життя цільової особи, більшість атак фішингу націлені на широку аудиторію. Завдяки їхній екстремальній настроєності, ці атаки особливо ефективні у проходженні основних заходів кібербезпеки.

4. Whaling - термін «whaling» вживається для позначення випадків, коли недобросовісні особи націлені на «великих риб» – таких, як знаменитості чи керівники бізнесу. Ці шахраї часто детально вивчають своїх цілей з метою визначення оптимального часу для крадіжки чутливих даних, таких як дані для входу. Атаки «whaling» можуть принести величезний виграш особам, які можуть втратити значні активи.

Розвідка: техніки, які вороги використовують для активного чи пасивного збору даних, які можуть бути використані для підтримки вибіркового нападу. Ці деталі можуть стосуватися організації-жертви, персоналу чи інфраструктури. Ворог може використовувати цю інформацію для підтримки інших етапів життєвого циклу ворога. Наприклад, «ворог може використовувати інформацію для обговорення та визначення пріоритетів об'єктів після компрометації, планування та виконання початкового доступу або організації та керування додатковими операціями розвідки» [27]. У розвідка виділяють дві категорії в залежності від характеру взаємодії з об'єктом [28]:

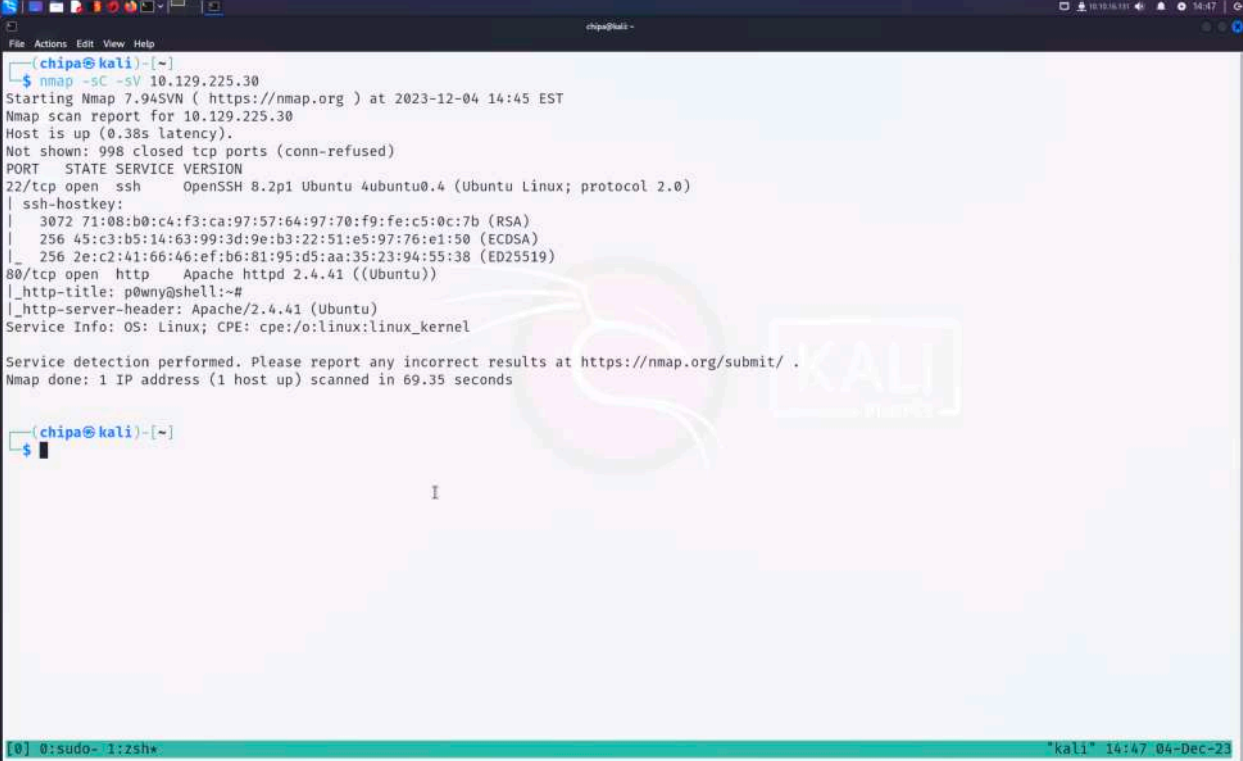
- активна розвідка передбачає активне взаємодію з мережею, хостами, персоналом тощо. (Сканування портів, сканування веб-додатків, сканування вразливостей);

- пасивна розвідка використовує дані, що доступні загалом громадськості. (Пошукові системи, whois, OSINT, DNS).

Інструменти, які використовуються для активної розвідки:

- Nmap;
- gobuster;
- enum4linux-ng;
- waf00f;

- Nikto;
- fuzz.



```

(chipa@kali)~$ nmap -sC -sV 10.129.225.30
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-04 14:45 EST
Nmap scan report for 10.129.225.30
Host is up (0.38s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 3072 71:08:b0:c4:f3:ca:97:57:64:97:70:f9:fe:c5:0c:7b (RSA)
|_ 256 45:c3:b5:14:63:99:3d:9e:b3:22:51:e5:97:76:e1:50 (ECDSA)
|_ 256 2e:c2:41:66:46:ef:b6:81:95:d5:aa:35:23:94:55:38 (ED25519)
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_ _http-title: p0wny@shell:~#
|_ _http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 69.35 seconds

(chipa@kali)~$

```

Рисунок 2.1 - Приклад викроистання Nmap

C2(Command and Control) фреймворки: зловмисники та ґтичні хакери використовують набір інструментів та технік, що називається інфраструктурою керування та контролю, або C&C, для забезпечення зв'язку з компрометованими пристроями після початкової експлуатації. Навіть якщо конкретні механізми, використовувані в кожній атаці, значно відрізняються, C2, як правило, складається з одного чи декількох потайних каналів зв'язку між платформою під контролем атакуючого та пристроями в організації-жертві. «Ці канали комунікації використовуються для відправки команд на інфіковані пристрої, завантаження додаткових шкідливих навантажень та передачі ворованої інформації назад до атакуючого» [29]. На ринку представлена велика кількість як open-source, так і комерційних C2

фреймворків, найпопулярніші з них: Cobalt Strike, Sliver, PowerShell Empire. Розглянемо з чого складається C2 фреймворк, на основі Cobalt Strike [30]:

а) Team Server - Складова C2-сервера, яка приймає загальні веб-запитання, виклики BEACON та підключення клієнтів;

б) Client(рис. 2.1) - інтерфейс для підключення до командного серверу;

в) Beacon - стандартна вірус-закладка, яка використовується Cobalt Strike для встановлення з'єднання з сервером команд. Активні сесії зворотних викликів до цілі також називаються «beacons»:

- 1) Stager - шляхом відправлення спочатку невеликого навантаження shellcode BEACON, яке виконує лише кілька простих перевірок, оператори можуть «ініціювати» своє вредоносне програмне забезпечення. Потім воно запитує конфігурованого командно-контрольного сервера для отримання повнофункціональної задньої двері;
- 2) Full backdoor - можуть буди доставлені до системи за допомогою ініціатору, або за допомогою прямого застосування ReflectiveLoader DLL. Допомогає встановити контроль та зв'язок із системою;

г) Listener - компонент фреймворку який використовується beacon для встановлення зворотнього зв'язку із командним сервером, підтримує зв'язок за допомогою наступних протоколів:

- 1) HTTP/HTTPS;
- 2) DNS;
- 3) SMB;
- 4) Raw TCP.

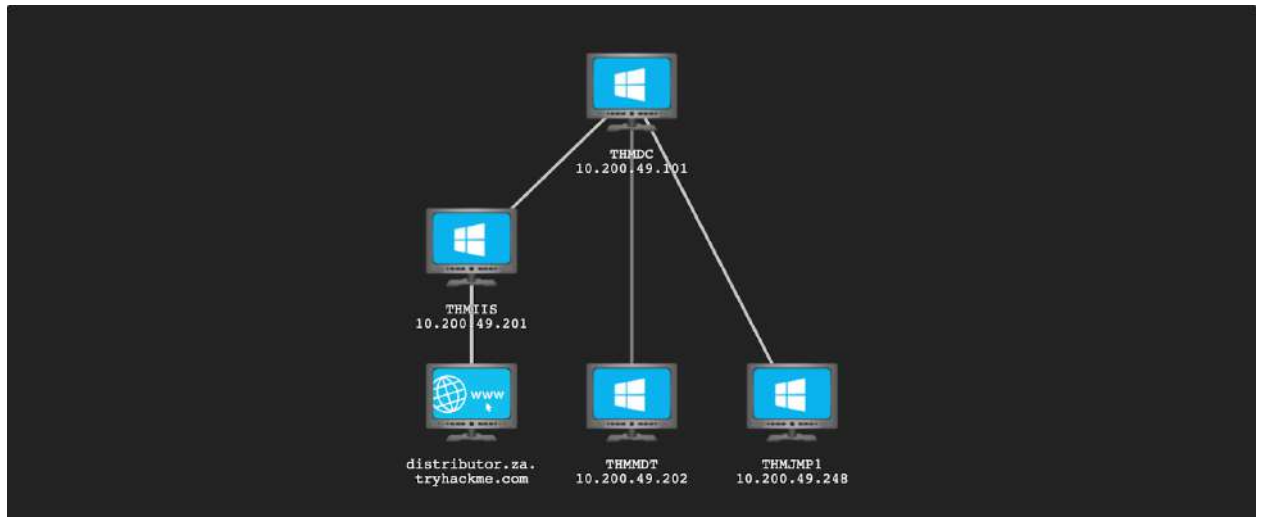


Рисунок 2.2 - Інтерфейс клієнту Cobalt Strike

Маніпуляції із трафіком: У сучасному контексті кібербезпеки, маніпуляції трафіком є однією з ключових аспектів стратегій Red Team, яка зосереджена на імітації реальних кіберзагроз. Перехоплення трафіку та атака типу «Man-in-the-Middle» представляють собою високоризиковані техніки, використовувані хакерами та командами «red team» для отримання несанкціонованого доступу до мережі та конфіденційної інформації.

Перехоплення трафіку включає аналіз та втручання у передачу даних між двома або більше сторонами, використовуючи різноманітні техніки, такі як аналіз пакетів, перенаправлення мережевого трафіку або впровадження шпигунського програмного забезпечення. Для цього використовуються такі інструменти як WireShark та tcpdump.

Атаки «Man-in-the-Middle» передбачають втручання в комунікацію між двома точками, використовуючи методи, які дозволяють атакуючій стороні перехоплювати, змінювати або блокувати передачу даних. Це може включати в себе використання хибних точок доступу, аналіз шифрованого трафіку та використання проксі-серверів. Найчастіше досягається за допомогою наступних інструментів: mintm6, responder(рис 2.3), ntlmrelayx.py.



Рисунок 2.3 - Перехоплення трафіку внутрішньої мережі за допомогою Responder

Висновки до 2 розділу

В другому розділі роботи було ретельно розглянуто основні визначення та поняття в області Offensive Security (OffSec). Детально проаналізовано роль OffSec у кібербезпеці, виявивши її визначальне значення у сфері захисту інформаційних активів. Зазначено, що OffSec виступає не лише як реакційний елемент, але і як стратегічна ініціатива, спрямована на ефективне виявлення та запобігання кіберзагрозам.

Також, у розділі висвітлено тактики, які використовує Red Team, зокрема, підкреслено важливість пентестінгу, експлуатації вразливостей та інших методів для забезпечення комплексного тестування інформаційних

систем. Особливу увагу було приділено найпоширенішим атакам та вразливостям, таким як OSINT, соціальний інжиніринг, фішинг, розвідка, фреймворки командного та контролю (C2), а також маніпуляції із трафіком.

Висновуючи цей розділ, важливо підкреслити, що ретельне вивчення та розуміння цих аспектів OffSec є ключовим етапом у формуванні ефективних стратегій кібербезпеки. Здобуті знання дозволяють не лише ідентифікувати потенційні ризики, але й розробляти ефективні заходи протидії, щоб забезпечити високий рівень захисту в інформаційному середовищі. У подальших розділах роботи розглядатимуться конкретні заходи та рекомендації для усунення та попередження кіберзагроз, що базуються на розглянутих принципах OffSec.

3 ДОСЛІДЖЕННЯ НАПРЯМКУ BLUE TEAM ЯК СКЛАДОВОЇ DEFENSIVE SECURITY

Defensive Security, в контексті кібербезпеки, представляє собою комплекс стратегічних та технічних заходів, спрямованих на захист інформаційних ресурсів, інфраструктури та мережевих систем від потенційних кіберзагроз. Основною метою Defensive Security є створення надійного оборонного каркасу, який не лише перешкоджає можливим атакам, але й забезпечує швидке виявлення, аналіз та ефективне реагування на інциденти безпеки. Цей напрямок визнає важливість збереження конфіденційності, цілісності та доступності даних у відкритому та динамічному кіберпросторі.

Однією з ключових складових Defensive Security є використання технічних засобів, таких як брандмауери, системи виявлення вторгнень, антивірусне програмне забезпечення та інші рішення, які спрямовані на захист мережевих інфраструктур та ендпоінтів. Шифрування даних та сегментація мережі також відіграють значущу роль у створенні непроникної оборонної лінії. Подібно до офанзивних стратегій кібербезпеки, Defensive Security вимагає постійного вдосконалення та адаптації, оскільки кіберзагрози постійно еволюціонують.

Однак Defensive Security охоплює не лише технічні аспекти. Відчутливість до людського фактору, освіта користувачів, та вдосконалення процесів управління безпекою є також невід'ємними елементами цього підходу. Збалансована комбінація технічних та не-технічних заходів визначає успіх в ефективному захисті від різноманітних кіберзагроз, що дозволяє забезпечити стійку безпеку в умовах постійно змінюючогося кіберсередовища.

3.1 Визначення Defensive Security та основні принципи напрямку

Defensive Security представляє собою комплексний підхід до кібербезпеки, спрямований на забезпечення захисту інформаційних систем від потенційних загроз та атак. Його первинною метою є попередження несанкціонованого доступу, виявлення та ліквідація вразливостей у системах та забезпечення безпеки конфіденційної інформації. У цьому контексті, визначення Defensive Security включає у себе усі аспекти, спрямовані на зменшення ризиків та підвищення рівня стійкості інформаційних ресурсів.

Принципи Defensive Security базуються на концепції передбачуваного та проактивного підходу до кіберзахисту. Передбачуваність передбачає розробку та впровадження стратегій захисту, які передбачають можливі загрози та розробляють відповіді на них. Це включає в себе створення міцних політик безпеки, визначення ролей та обов'язків внутрішнього персоналу та виявлення критичних активів для подальшої захисту.

Проактивний підхід передбачає активне виявлення та виправлення потенційних вразливостей до того, як вони можуть бути використані несанкціонованими суб'єктами. Це охоплює регулярні аудити безпеки, вивчення нових загроз та використання передових технологій для виявлення аномалій та потенційних атак. Defensive Security також включає в себе навчання персоналу з питань кібербезпеки та розробку ефективних заходів реагування на інциденти для швидкого відновлення роботи систем.

3.2 Роль Defensive Security та вплив на кібербезпеку

Роль Defensive Security у стратегії кіберзахисту визначається як невід'ємна та ключова компонента, спрямована на попередження, виявлення

та виправлення потенційних загроз для інформаційних систем. Основна мета цього підходу – «забезпечити високий рівень безпеки інформаційних активів та даних, уникнути несанкціонованого доступу та запобігти можливим інцидентам кібербезпеки» [31]. Defensive Security виявляє свою важливість у контексті постійно зростаючого обсягу кіберзагроз та їхньої ускладненості.

У стратегічному плані, Defensive Security включає розробку та впровадження ефективних політик безпеки, які охоплюють широкий спектр заходів, починаючи від аутентифікації та авторизації, завершуючи моніторингом та виявленням інцидентів. Приділяється особлива увага постійному оновленню та удосконаленню заходів безпеки відповідно до нових загроз та технологічних вдосконалень. Зокрема, відіграючи важливу роль у підтримці стійкості та інтегритету інформаційних систем, Defensive Security допомагає відвертати можливі атаки, а також реагувати на них, забезпечуючи важливий компонент внутрішньої кібербезпекової інфраструктури.

Однією з ключових рис Defensive Security є його активний підхід до моніторингу та реагування на інциденти. Це включає в себе систематичне вивчення потенційних загроз, виявлення аномалій та вчасну реакцію на виявлені атаки. Організації, що дотримуються Defensive Security, надають пріоритет удосконаленню інфраструктури для забезпечення надійності та стійкості проти кіберзагроз.

Компанії часто скасовують послуги від постачальників третіх сторін, але забувають видаляти пов'язані записи DNS. Це тому, що для запису DNS не передбачається додаткових витрат. RedHuntLabs провели дослідження «у 2020 році, і вони виявили, що понад 400 000 піддоменів із 220 мільйонів були вразливі до захоплення піддоменів. 62% з них належали сектору електронної комерції» [32].

3.3 Дослідження методів захисту кіберпростору

Тактики оборонної кібербезпеки забезпечують цілісність даних і надають постійний захист від різноманітних загроз, гарантуючи, що інформація залишається послідовною та надійною протягом всього її життєвого циклу. Вони також зменшують правові та регуляторні ризики, полегшуючи виконання вимог галузевих нормативних актів.

Можливі суспільно-економічні порушення зменшуються завдяки оборонним стратегіям, які передбачають запобігання або зменшення наслідків порушень безпеки. Оборонні стратегії взаємодіють з атакуючими заходами в галузі кібербезпеки для забезпечення комплексного та надійного підходу до захисту цифрових активів та репутації організації. Перелік основних тактик [33].

1. Ідентифікація активів: Визначте, які активи є важливими та потребують першочергового захисту. Це включає з'ясування місць розташування та руху чутливих даних як всередині компанії, так і за її межами;

2. Моделювання загроз: Розпізнавання можливих небезпек для організації та впровадження відповідних заходів захисту;

3. Створення стратегії пошарового захисту: Також відомий як захист у глибину, цей підхід передбачає впровадження кількох рівнів контролю безпеки та заходів захисту даних;

4. Створення плану реагування на інцидент та забезпечення його виконання: Розробіть план реагування на інциденти та переконайтеся, що існують процедури для зменшення шкоди, відновлення компрометованих даних та відновлення цілісності системи у випадку порушення безпеки;

5. Освіта та підвищення свідомості: Переконайтеся, що кожен співробітник осведомлений про можливі ризики безпеки, здатний їх виявляти та відзначати. Регулярна підготовка гарантує, що людський фактор виступає як потужний елемент оборони.

3.4 Розбір основних інструментів, що використовують Blue Team

Blue Team використовує різноманітні техніки та інструменти для забезпечення безпеки інформаційно-технічних систем та виявлення можливих кіберзагроз. Для досягнення цієї мети використовується велика кількість технік та інструментів.

Firewall: У приватній комп'ютерній мережі «файерволи діють як контрольні кордони або шлюзи для регулювання потоку авторизованого та неавторизованого онлайн-трафіку» [34]. Принцип роботи цього програмного забезпечення або спеціалізованого апаратно-програмного обладнання полягає у дозволі чи блокуванні певних пакетів даних. Зазвичай його метою є запобігання зловживанням та припинення участі кого-небудь у незаконних онлайн-активностях, незалежно від того, чи вони знаходяться всередині, чи поза приватною мережею. Файерволи забезпечують безпеку комп'ютерної мережі, використовуючи стратегії управління веб-трафіком та зазвичай призначені для уповільнення поширення онлайн-загроз.

За місцем встановлення файерволи поділяють на [34].

1. **Мережевий:** використовуються для забезпечення захисту між внутрішніми приватними мережами та зовнішніми мережами. Вони контролюють потік даних у мережах, розділяючи внутрішні мережі, такі як корпоративні інтранети, національні інтранети та домашні Wi-Fi-мережі, від зовнішніх громадських мереж, таких як Інтернет. Мережеві файерволи можуть бути впроваджені у вигляді віртуальних, програмних або присвячених апаратних пристроїв;

2. **Програмний:** використовується на окремих пристроях користувачів та інших закритих кінцевих точках приватної мережі для розподілу пристроїв у мережі включає. Цим хостам або пристроям надають персоналізоване управління трафіком від та до конкретних комп'ютерних програм. Файерволи хостів можуть виконувати функції додатків з безпеки

кінцевих точок або служб операційних систем на локальних пристроях. Брандмауери хостів дозволяють контролювати не лише звідки поступає вміст, але й який вміст потрапляє до комп'ютеру за допомогою його фільтрації на основі протоколів мережевих протоколів, таких як HTTP/HTTPS.

Фільтрація трафіку досягається за допомогою заздалегідь встановлених або динамічно вивчених правил. «Файервол контролює потік веб-трафіку через приватну мережу та особисті комп'ютери, використовуючи ці правила» [34]. Усі файерволи, незалежно від типу, мають можливість фільтрації з використанням будь-якої комбінації параметрів.

Таблиця 3.1 - Параметри фільтрації файерволу

Джерело	Джерело трафіку
Призначення	Кінцева точка трафіку
Вміст	Інформація що передається
Протоколи пакетів	Протоколи, які використовуються для встановлення з'єднання між джерелом та призначенням. TCP/IP є найбільш поширеними мережевими протоколами серед хостів для «розмови» один з одним як у межі внутрішніх мереж, так і в Інтернеті
Протоколи застосунків	HTTP, SSH, FTP, Telnet та інш

Класифікація файерволів за техніками фільтрації [34].

1. Файервол із статичним фільтруванням пакетів: Аналізують кожен окремий пакет даних, що надсилається по мережі відповідно до його походження та призначення, вони забезпечують елементарне фільтрування.

Цікаво, що з'єднання, які вже були прийняті, не фіксуються. Це означає, що кожного разу, коли надсилається пакет даних, кожне з'єднання повинно бути повторно схвалене;

2. Шлюзовий мережевий файервол: дозволяють безперервне відкрите з'єднання між двома мережами, аналізуючи з'єднання для функціональних пакетів. Коли це відбувається, файервол більше не веде моніторинг за з'єднанням. Постійне, ненаглядне з'єднання становить ризик, оскільки його можна перехопити законними засобами;

3. Firewall зі становим інспектуванням: відрізняються від статичної фільтрації тим, що вони можуть запам'ятовувати попередні з'єднання та відстежувати поточні. Дозволяють чи забороняють трафік відповідно до технічних характеристик, таких як конкретні протоколи пакетів, IP-адреси чи порти, як це роблять брандмауери із статичною фільтрацією. Проте ці брандмауери також використовують таблицю стану для унікального відстеження та фільтрації з'єднань на основі їхнього поточного стану. На основі подій попередніх з'єднань, які реєструються із таблицею стану, цей тип файерволів модифікує свої правила фільтрації;

4. Проксі файервол: на відміну від інших видів файерволів, він виступає як додаткова пара хостів - один служить «проксі» або представником для кожної мережі - між внутрішніми хост-комп'ютерами та зовнішніми мережами. Використовує не лише IP-адреси, порти та фундаментальні протоколи пакетів (UDP, ICMP), основою для фільтрації є дані рівня застосування. Можливість читати та розуміти протоколи, такі як FTP, HTTP, DNS та інші, відкриває можливість більш глибокого дослідження та хрест-фільтрації для широкого спектру атрибутів даних.

Кожен тип функціонує на відмінному рівні в межах моделі міжсистемного взаємодії відкритих систем (OSI), яка є стандартизованою моделлю комунікацій.

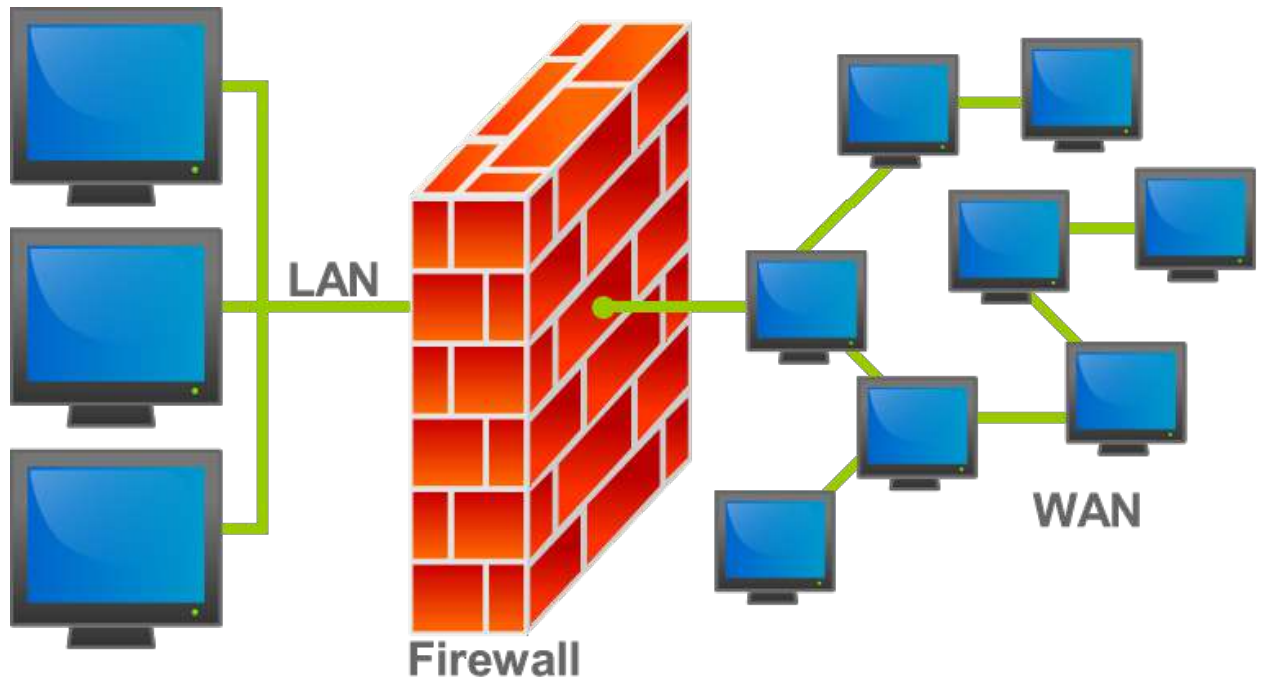
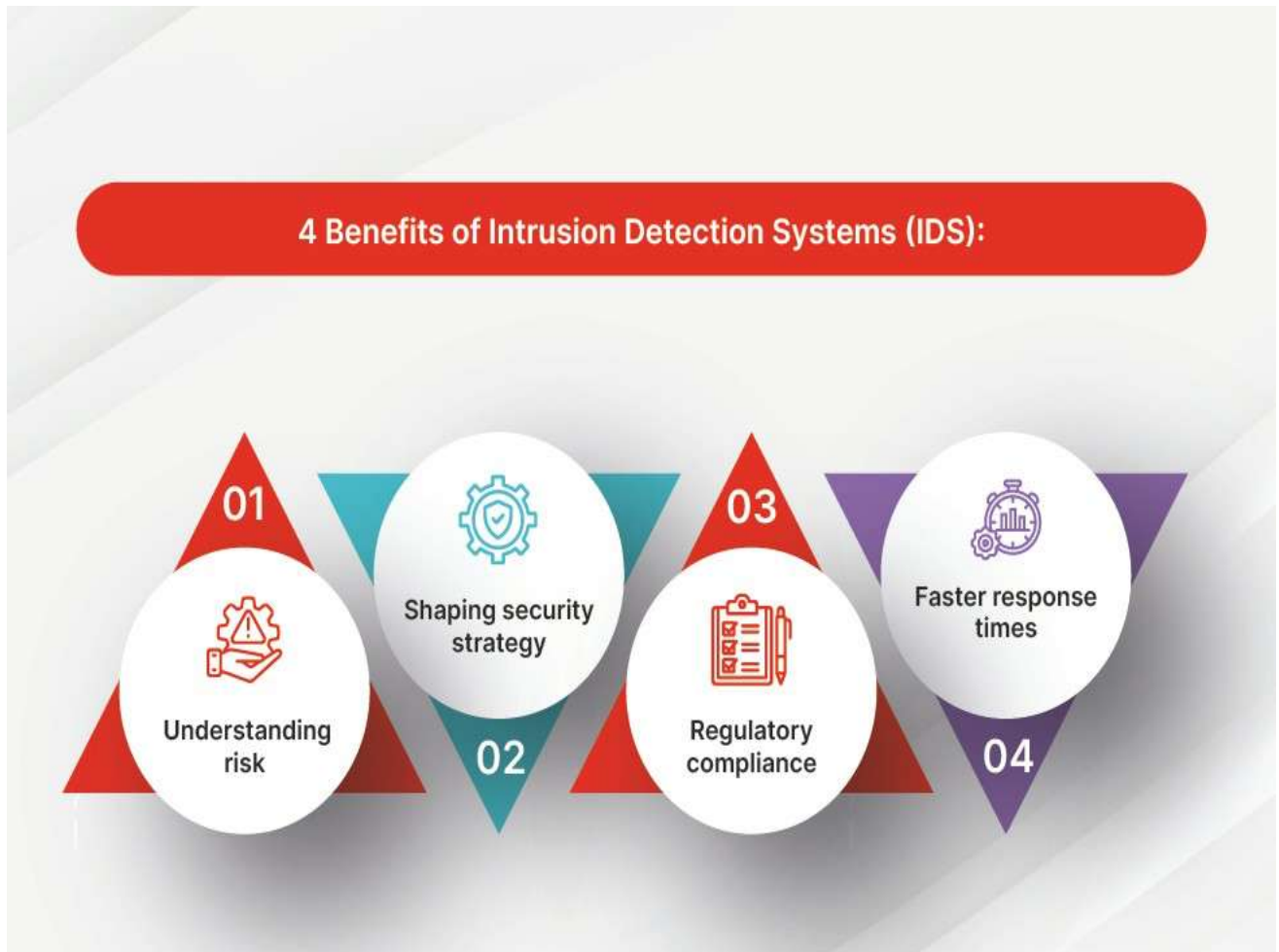


Рисунок 3.1 - Схематичне зображення роботи файрволу [47]

Intrusion Detection System (IDS): спостерігає за мережевим трафіком та виявляє відомі загрози, а також незвичайну чи зловмисну діяльність. Коли IDS виявляє будь-які загрози або ризики безпеки, він сповіщає IT-команду та команду безпеки. Коли вони помічають аномалію, більшість рішень IDS лише ведуть моніторинг та повідомляють про підозрілу діяльність та трафік. Деякі ж можуть піти ще далі й блокувати зловмисний чи підозрілий трафік, якщо вони помічають незвичайну активність. Зазвичай IDS є програмними продуктами, які працюють на апаратному забезпеченні організації або як засіб мережевої безпеки. Крім того, існують системи виявлення вторгнень, що базуються на хмарних технологіях, які призначені для захисту даних, активів та систем підприємств у їх хмарних середовищах та розгортаннях.



1 - розуміння ризиків; 2 - формування стратегії захисту;
3 - відповідність нормативним вимогам; 4 - швидке реагування.

Рисунок 3.2 - Переваги використання IDS [35]

Моніторинг мережевого трафіку та виявлення аномальної активності - це два напрямки, IDS виявляють свою ефективність. Вони розташовані стратегічно по всій мережі або на пристроях самостійно, щоб моніторити мережевий трафік та виявляти будь-які ознаки надходження атаки. Коли система виявлення вторгнень виявляє активність, яка відхиляється від зазначеного нормального, вона шукає сигнатури відомих типів атак. Після цього адміністратори отримують сповіщення про ці аномалії та, можливо, зловмисні дії, щоб рівні додатків та протоколи могли розглянути їх. Це

дозволяє організаціям визначати можливі показники того, що зловмисник запускає чи виконує атаку. Реалізацію цього IDS досягає за допомогою кількох функцій, таких як [35]:

- здійснення постійного моніторингу функціональності важливих файерволів, файлів, маршрутизаторів та серверів з метою виявлення, блокування та пом'якшення кібератак;
- надання допомоги адміністраторам систем у керуванні та розумінні відповідних слідів перевірки та журналів операційних систем, які часто є важкими для зберігання та відстеження;
- надання співробітникам, які не є експертами у сфері безпеки, доступу до інтуїтивного інтерфейсу, щоб вони могли допомагати у керуванні системами організації;
- надання великої бази даних атакованих підписів для порівняння та виявлення загроз;
- створення оперативної та ефективної системи звітності у випадку підозрілої або зловмисної активності, що дозволяє ескалацію загрози на вищий рівень управління;
- вироблення сигналів, які, у випадку порушення, сповіщають відповідні сторони, такі як команди забезпечення безпеки та системні адміністратори.

Рішення IDS доступні у різних формах з різноманітними функціональними можливостями. Зазвичай використовуються IDS таких типів [35].

1. Network intrusion detection system (NIDS): використовується моніторингу вхідного та вихідного трафіку.

2. Host intrusion detection system (HIDS): цю систему встановлюють на окремих пристроях, які пов'язані як зі внутрішньою мережею організації, так і з Інтернетом. Окрім того, що вона може ідентифікувати додатковий зловмисний трафік, який NIDS-рішення не може виявити, це рішення може визначити пакети, які виникають зсередини компанії. Також вона може

ідентифікувати зловмисні загрози, що виникають з хоста, наприклад, хоста, який інфікований шкідливим програмним забезпеченням, що намагається розповсюдити інфекцію по системі компанії.

3. Signature-based intrusion detection system (SIDS): рішення SIDS відстежує кожен пакет, який проходить через мережу компанії, та порівнює його із сигнатурами атак, збереженими в базі даних відомих загроз.

4. Anomaly-based intrusion detection system (AIDS): стежить за мережевим трафіком та порівнює його з передвстановленим стандартом, який вважається «нормальним». Вона виявляє незвичайну поведінку та активність в усіх областях мережі, включаючи порти, пристрої, пропускну здатність та протоколи. У рішенні AIDS використовуються техніки машинного навчання для створення базового рівня нормальної поведінки та відповідної політики безпеки. Це гарантує, що компанії можуть виявляти нові, розвиваючісЯ ризики, які не виявляються рішеннями SIDS.

5. Perimeter intrusion detection system (PIDS): для виявлення спроб вторгнення в критичну інфраструктуру організації використовується рішення PIDS, яке встановлюється на мережі.

6. Virtual machine-based intrusion detection system (VMIDS): шляхом стеження за віртуальними машинами система VMIDS може виявляти вторгнення. Організації можуть використовувати її для моніторингу трафіку, який протікає через всі системи та пристрої, до яких підключені їхні пристрої;

7. Stack-based intrusion detection system (SBIDS): TCP/IP, яке використовується як комунікаційний протокол в приватних мережах, інтегрується з SBIDS в систему TCP/IP організації. За допомогою цього методу з мережі вилучаються шкідливі пакети до того, як вони можуть бути оброблені операційними системами чи додатками, що дозволяє системі виявлення вторгнень моніторити пакети під час їхнього проходження через компанію.

Intrusion Prevention System(IPS): тип технології безпеки, який використовується для активного виявлення та запобігання зловмисній активності, небажаному доступу та іншим загрозам в межах комп'ютерної

мережі або системи. Це є необхідною складовою будь-якого плану мережевої безпеки, яка поєднується з іншими заходами безпеки для надання всебічного виявлення загроз та оборони. Оскільки обидві системи відслідковують зловмисну активність в мережевому трафіку та/або системних діях, системи запобігання вторгненням, також відомі IDPS, розглядаються як розширення IDS. Основною відмінністю між ними є те, що, хоча IDS виявляє зловмисну активність, він не вживає заходів, IPS активно запобігає або блокує виявлені вторгнення.

IPS використовується головним чином для моніторингу мережевого трафіку, порівняння його з попередньо встановленими правилами безпеки чи сигнатурами та вживання негайних заходів для зупинки або заподіяння будь-якій потенційно шкідливій або підозрілій активності. Спостерігаючи за потоками пакетів, технології IPS можуть забезпечувати дотримання безпечних протоколів та запобігати використанню небезпечних. До мережевих атак, які вони виявляють та зупиняють, належать атаки «brute force», атаки DDoS та зловживання вразливостями. Важливі характеристики та переваги IPS [36]:

- підвищення безпеки: IPS пропонує кращу безпеку додатків, співпрацюючи з іншими кібербезпековими рішеннями для виявлення загроз, які їм не вдається виявити;
- понфігурування: Для надання унікальних засобів управління безпекою, IPS може бути налаштований із зовнішніми політиками безпеки;
- ефективність: IPS зменшує ручну працю, необхідну для команд безпеки, та покращує ефективність інших засобів безпеки, фільтруючи зловмисну активність до того, як вона потрапляє до інших засобів або контролюється ними.

Intrusion Prevention Systems

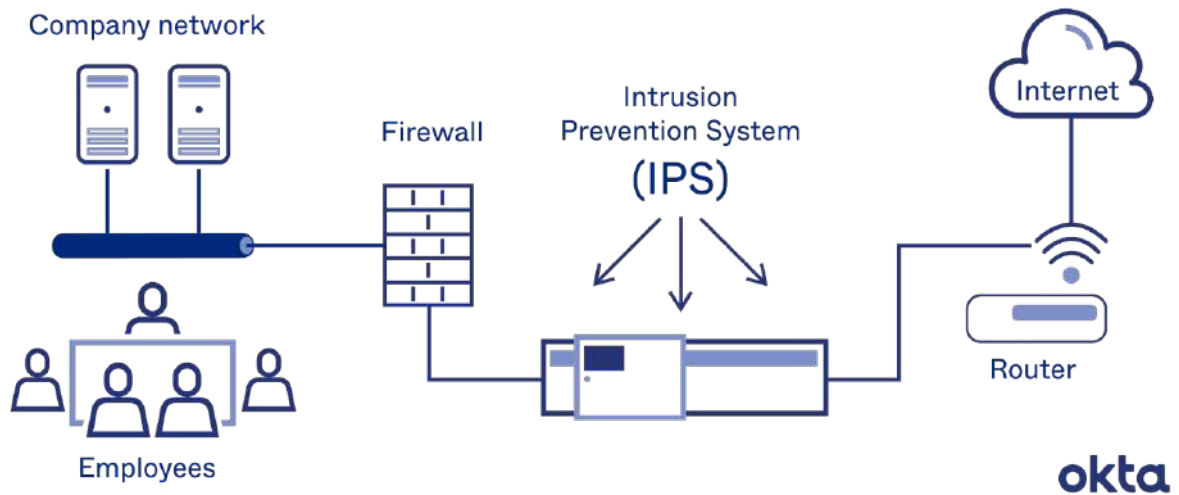


Рисунок 3.3 - Інтеграція IPS у мережу організації [48]

Метою систем запобігання вторгнення є ідентифікація та припинення різних видів загроз безпеці мережі. Ось кілька часто зустрічаються атак, які система запобігання вторгнення (IPS) допомагає ліквідувати.

1. Атаки методом «Brute Force»: У цих атаках хакер спробує безліч комбінацій імен користувачів та паролів з метою несанкціонованого доступу до системи.
2. DDoS-атаки (атаки розподіленого відмови у обслуговуванні): Ці атаки характеризуються множинними джерелами трафіку, які затоплюють цільову систему, роблячи атаку важкою для протидії.
3. Зловживання вразливостями: Системи запобігання вторгнення мають здатність ідентифікувати та припиняти атаки, які використовують вразливості програмного забезпечення для заволодіння системою.
4. Worms: Саморозмножуючі віруси можуть завдати шкоди та розгортатися в мережі. Їх поширення можна виявити та зупинити за допомогою IPS.

5. Віруси: Зловмисні програми, які можуть інфікувати та завдати шкоди системам, відомі як віруси, і IPS може допомогти ідентифікувати та припиняти їх поширення.

6. Небезпечні протоколи: IPS може запобігти використанню небезпечних протоколів, таких як ті, що використовують слабкі шифри чи застарілі версії SSL.

7. Видалення зловмисного вмісту: Після атаки IPS може допомогти замінити або видалити будь-який залишковий зловмисний вміст, що може залишитися в мережі. Це включає очищення заголовків, перепакування пакетів та видалення інфікованих вкладень з файлових або електронних поштових серверів.

8. Zero-day: Ці зловмисні програми атакують вразливості, які або не виявлені, або для яких ще не було надано виправлення. Навіть якщо IPS не завжди можуть ідентифікувати та припинити кожен «Zero-day» експлойт, вони все ж можуть забезпечити додатковий рівень безпеки, ліквідуючи трафік, який проявляє підозрілу активність або відповідає встановленим шаблонам атак.

Різні системи IPS працюють за різними принципами. Фактично існує чотири основні категорії IPS [36].

1. Network-based Intrusion Prevention System (NIPS): Цей вид IPS, вивчаючи поведінку протоколів, стежить за будь-якою незвичайною активністю в мережі. Вона розташована в ключових місцях для спостереження за всією мережевою активністю та виявлення потенційних загроз безпеці.

2. Wireless Intrusion Prevention System (WIPS): WIPS спостерігає за бездротовими мережами, усуваючи небажані пристрої.

3. Host-based Intrusion Prevention System (HIPS): HIPS розміщується на певних хостах або кінцевих точках та виявляє потенційно небезпечну активність.

4. Application-based Intrusion Prevention System (AIPS): AIPS призначена для моніторингу та захисту певних сервісів або додатків, таких як бази даних чи веб-сервери.

Ці типи IPS можуть бути впроваджені окремо або в поєднанні, щоб надати комплексний захист мережі. Часто вони інтегруються з іншими інструментами безпеки, такими як файерволи нового покоління або рішення управління загрозами, для підвищення видимості мережі та автоматизації реагування на загрози.

Висновки до 3 розділу

Третій розділ надає глибокий та системний огляд основних аспектів Defensive Security, включаючи визначення, роль у кібербезпеці, тактики та використанні техніки та інструменти. Акцент на цих ключових аспектах є важливим етапом для розуміння та реалізації ефективних стратегій кіберзахисту в організаційних та технічних середовищах.

Аналіз ролі Defensive Security в контексті кібербезпеки вказує на його стратегічну значущість. Відзначаючи його важливість у забезпеченні конфіденційності, цілісності та доступності інформації, розділ підкреслює його центральну роль у створенні всебічної системи безпеки.

Розгляд тактик визначає ключові стратегії, які забезпечують ефективний захист. Вивчені тактичні підходи, такі як ідентифікація активів, моделювання загроз, та реагування на інциденти, формують базу для розробки та впровадження ефективних заходів безпеки.

Розділ також розглядає різноманітні техніки та інструменти, які використовуються Blue Team. Від застосування файерволів та систем виявлення вторгнень до запобігання інцидентів за допомогою систем запобігання вторгнень, надається зрілий огляд засобів захисту.

В цілому, розділ виокремлює ключові аспекти Defensive Security, допомагаючи впроваджувати необхідні стратегії та засоби для забезпечення високого рівня безпеки в сучасному кіберсередовищі.

4 АНАЛІЗ СПІВПРАЦІ МІЖ BLUE TEAM ТА RED TEAM

Зростаюча кількість підприємств прагне підвищити кваліфікацію працівників, зменшити відсоток необхідних спеціалістів у галузі кібербезпеки та покращити ефективність реагування на інциденти за допомогою кібервправ та заходів «capture the flag». Через реалістичну симуляцію, досвід red on blue надає участь фірмам безпечне середовище «пісочниці», де можна протестувати на міцність свої бізнес-процеси та оцінити готовність реагувати на реальні кіберкатастрофи.

Діяльність команд Red/Blue не є новаторським концептом. Подібно до багатьох інших термінів, що використовуються в галузі інформаційної безпеки, «основна ідея була вперше встановлена під час Першої світової війни» [37]. Основна концепція полягала в тому, щоб використовувати симуляції для відображення ефективності атаки. Військові та галузь кібербезпеки обидві використовують симуляції, які базуються на реальних методах, які противник міг би використовувати, і ці симуляції відомі своєю ефективністю.

4.1 Розбір організації інфраструктури для співпраці

Через реалістичну симуляцію, досвід «червоний проти синього» надає участь компаніям безпечне середовище для випробування стрес-тестів своїх бізнес-процесів та оцінки готовності реагувати на реальні кібер-катастрофи.

Середовище, призначене для підвищення кваліфікації та проведення симуляційних вправ з кібербезпеки, називається кібердіапазоном, де зазвичай відбувається інцидент відповіді «червоний проти синього». «В кібердіапазоні

розміщуються виробничі або подібні до виробничих системи, які можуть використовуватися як в режимі червоний, так і в режимі синій» [37].

Кібердіапазон встановлює систему, яка імітує бізнес-мережу, що стежить за командою центру забезпечення інформаційної безпеки (SOC), щоб активувати сценарій «синій». Зазвичай у цей синій сценарій включаються засоби моніторингу мережі та засоби відповіді на інциденти компанії.

З іншого боку, ряд реальних атак імітує кіберзлочинців, які намагаються скомпрометувати комп'ютерну мережу та системи компанії. Для проведення сценарію «червоний» використовуються найновіші автоматизовані засоби атак та методи ручного тестування на проникнення.

Кібердіапазони пропонують організаціям різноманітні гнучкі та настроювані враження, що дозволяють компаніям фокусуватися на атаках, захисті або балансу між ними. Крім того, кібердіапазон може надавати додатковий персонал для управління однією стороною або іншою, якщо компанія бажає сфокусувати свої ресурси виключно на один аспект.

«Для успішного проведення справи важливо, щоб обидві сторони були ознайомлені з метою та правилами взаємодії перед початком справи» [38]. Бізнес визначає мету та регламент справи. Мета може бути більш конкретною, наприклад, оцінка певної області мережі чи точки фізичного доступу. З іншого боку, вона може мати більш широкі цілі, такі як визначення рівня безпеки компанії.

Дії команд обмежені правилами взаємодії. Це є ключовою інформацією. Команда Red Team часто використовує методи, схожі на ті, що використовують справжні хакери, щоб якнайто точніше імітувати реальні загрози. Організація може відрізнити їх від зловмисних атак, встановивши стандарти.

Збір інформації є початковим етапом процедури для обох сторін. Це включає оцінку вразливостей та стратегічне планування для Red Team. Це також означає виявлення та посилення будь-яких існуючих вразливостей для Blue Team.

Наступним етапом є реалізація. Тактика Red Team протистоять посиленню мережі Blue Team. Red Team може заздалегідь знати плани Blue Team або взагалі не знати нічого, згідно встановленим вказівкам.

Коли плани атаки та захисту вже були втілені, команди переходять до дебрифінгу. Оскільки обидві команди можуть відкрито обмінюватися знаннями та досвідом на цьому етапі вправи, це може бути найважливішим.

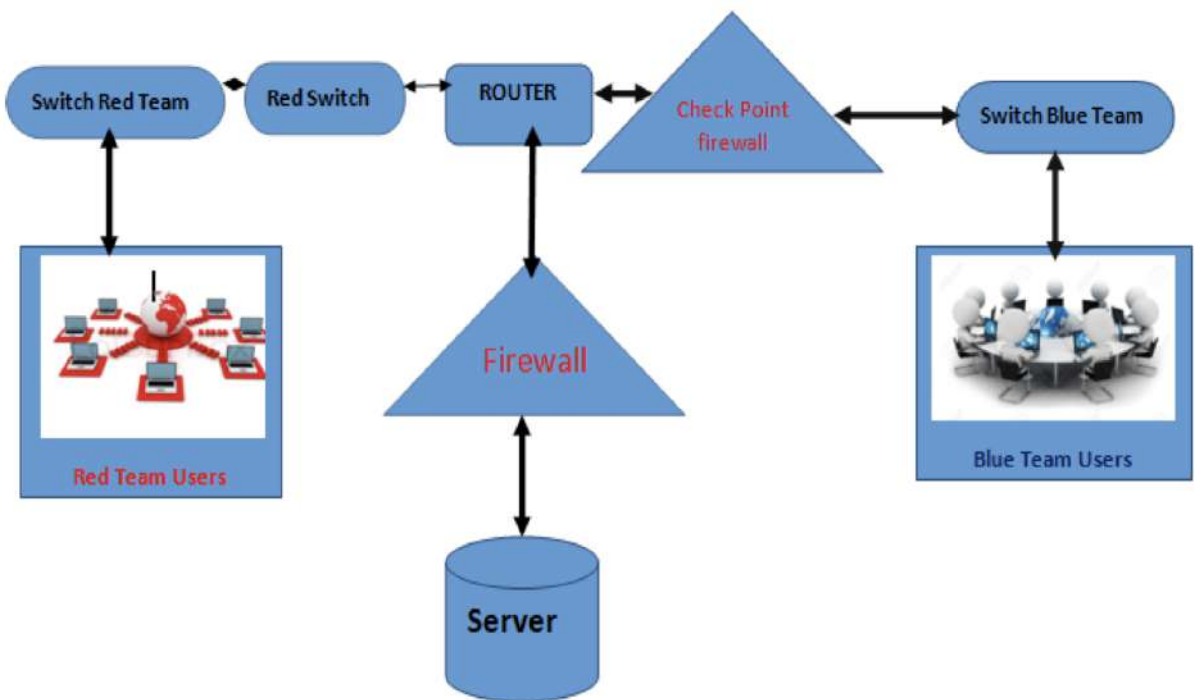


Рисунок 4.1 - Інфраструктура для червоний-проти-синього випробування [37]

4.2 Аналіз стратегії Red Team під час заходу

Зазвичай головною метою Red Team є проникнення в систему безпеки цільової організації та виявлення ризиків з метою посилення її захисту. Якщо команда досягає успіху у своїх зусиллях, це свідчить про те, що загальна цінність та ефективність групи зменшуються. Важливо розуміти, що «основна

відповідальність такого типу команди полягає в ускладненні завдань випробувань на проникнення, навіть якщо тести на проникнення занадто часто отримують велике задоволення від вторгнень в підприємства за допомогою простих методів» [39].

Red Team починають з вивчення якнайбільше можливої інформації про технічний стек цілі. Вони розпочинають з визначення операційних систем, які використовуються, таких як: Windows, macOS або Linux. Оскільки кожна з них має свої недоліки. Також вони визначають марку та модель обладнання для мережі: комп'ютери, сервери, комутатори, маршрутизатори та точки доступу. За допомогою цієї інформації вони складають карту мережі, щоб визначити, які хости надають певні послуги, і де протікає трафік. Також вони вивчають будь-які заходи фізичної безпеки, такі як двері, замки, камери та охоронці, якщо вони планують здійснювати фізичний напад особисто, а не запускати віддалений напад, наприклад, крадіжку жорсткого диска.

Таблиця 4.1 - Техніки Red Team під час заходу

Penetration Testing	Кібератаки, які симулюються та налаштовуються для досягнення конкретних тестових завдань
Social Engineering	Практика психологічного обману кого-небудь для отримання конфіденційної інформації
Phishing	Практика звертання до жертви та контактування з нею за допомогою текстових повідомлень, телефону чи електронної пошти, представляючи себе як офіційна компанія
Перехоплення зв'язку	Перегляд вмісту електронних листів, телефонних розмов та інших електронних комунікацій шляхом їх перехоплення

Кінець таблиці 4.1

Клонування біометрії	Процес створення магнітно-смугових карток за допомогою викрадених даних з платіжних карток з чіпами EMV
----------------------	---

4.3 Аналіз стратегії Blue Team під час заходу

Завданням Blue Team є виявлення ворогів та зупинення їхньої спроби проникнення в інфраструктуру компанії. Ця робота є величезною: «межі IT-інфраструктури організації часто визначаються нечітко та динамічно, програми вимагають великих зусиль для підтримання актуальності, а користувачі завжди ненавмисно можуть надати зловмисникам доступ до системи» [39]. Ще однією річчю, на яку варто звернути увагу, є постійна загроза, яку бізнес стикається від експлойтів «нульового дня», які можуть використовуватися для надання зловмисникам доступу до інфраструктури. Несанкціоноване використання IT, іноді відоме як «тіньове IT», сприяє неконтрольованій інфраструктурі, що може надати зловмисникам доступ до системи. Завдання, що стоїть перед Blue Team, подібне до завдання воротаря у футбольному матчі, за винятком того, що злочинці використовують різноманітні м'ячі для забиття голів, а ворота завжди рухаються.

Експерти із реагування на інциденти, які надають консультації IT-командам щодо управління кібератаками, зазвичай складають Blue Team. Blue Team проводить оцінку ризиків, збирає інформацію та визначає системи, які потребують захисту перед атакою. «Процес виявлення та оцінки потенційних загроз відомий як оцінка ризиків» [40]. Після цього вони вживають заходів забезпечення безпеки для захисту найважливіших активів організації.

Для досягнення цілей захисту, Blue Team використовує різноманітні методи, включаючи [40]:

- Перевірку DNS для запобігання розсилці фішингових атак;
- Використання цифрового аналізу для встановлення базового рівня мережевої активності та полегшення виявлення аномальної поведінки;
- Встановлення антивірусного програмного забезпечення на віддалених комп'ютерах та мобільних телефонах;
- Використання програмного забезпечення як засобу детекції та запобігання для систем виявлення та запобігання вторгнень, або IDS та IPS;
- Переконавання в правильності налаштування та впровадження засобів периметрової безпеки, зокрема брандмауерів та антивірусних програм.

4.4 Координація між командами

Під час виклику Red Team / Blue Team, наглядач може не завжди бути присутнім чи доступним. «Його обов'язок підтримувати та захищати інтереси виклику у відповідний момент, а також надавати пояснення, професійні поради та допомогу при прийнятті рішень» [41].

Коли Red Team вдається взломати систему, робота як команди Blue Team, так і Red Team, продовжується. На цьому етапі ще багато роботи, і всі ці команди повинні тісно співпрацювати.

Метод Red Team проти Blue Team корисний, оскільки він сприяє комунікації та взаємодії, перетворюючи перешкоду в можливість покращити здатність організації виявляти та нейтралізувати загрози. Метою такого співробітництва повинен бути постійний розвиток; команда Blue Team повинна розглядати операції Red Team як можливість вивчення стратегій, методів та тактик майбутнього атакувальника.

Хоча невдача Blue Team у виявленні вторгнення може бути наслідком помилок його працівників, вона також може виникнути внаслідок недостатніх заходів безпеки проти надзвичайно вишуканих чи навіть невідомих методів. Ці вразливості можуть бути розкриті в результаті атаки Red Team, ще до того, як справжні злочинці матимуть можливість їх використовувати. У кожній команді будуть власні цілі, і, отже, їхні методи також будуть різнитися.

В кінцевому звіті обов'язково повинна міститися детальна інформація про механізм порушення, часову лінію атаки, вразливості, які були використані для отримання доступу та, за потреби, підняття привілеїв, а також бізнес-вплив на компанію чи організацію [37].

4.5 Дослідження реального випадку співпраці між командами

Вправа червоний-проти-синього, фінансована програмою DARPA FTN, відбувалася з жовтня 2002 року по травень 2003 року [42]. Метою вправи було оцінити спільну систему оборони від розподіленого DDoS, що складалася з автономного захисту D-WARD та розподіленої системи COSSACK. Red Team складалася з дослідників національних лабораторій Сандії, Blue Team - з розробників перевірених систем з USC/ISI та UCLA, а наглядачем виступає BBN Technologies, який відповідав за всю координацію, виконання експериментів, збір результатів та аналіз.

Хоча COSSACK та D-WARD виявляють атаки DDoS у комбінованому режимі, реагує на загрозу лише D-WARD. У вправі кожна крайова мережа працює із системою D-WARD та «сторожовим песиком» COSSACK. За допомогою методів мультикастингу COSSACK локальний сторож біля жертви повідомляє віддаленим сторожам про атаки, коли він стає в них усвідомлений.

Дев'ять крайових мереж були з'єднані симульованою основною мережею, створеною мультипортовим маршрутизатором Cisco, у

експериментальній топології. На рисунку 4.2 відображена топологія. У цій вправі аутентичний трафік генерувався за допомогою системи виробництва трафіку Skaion. Під час тестування використовувалися напівавтономні програмні агенти, іноді відомі як боти, для генерації трафіку. Під час тестування група машин для генерації трафіку обладнана ботами, які можуть спілкуватися як із людськими хостами, так і між собою. Боти використовують власне програмне забезпечення, такі як веб-додатки, SSH і Telnet, для генерації трафіку. Їхньою метою є широке стохастичне відтворення бажаного змішаного трафіку, яке вони намагаються реплікувати.

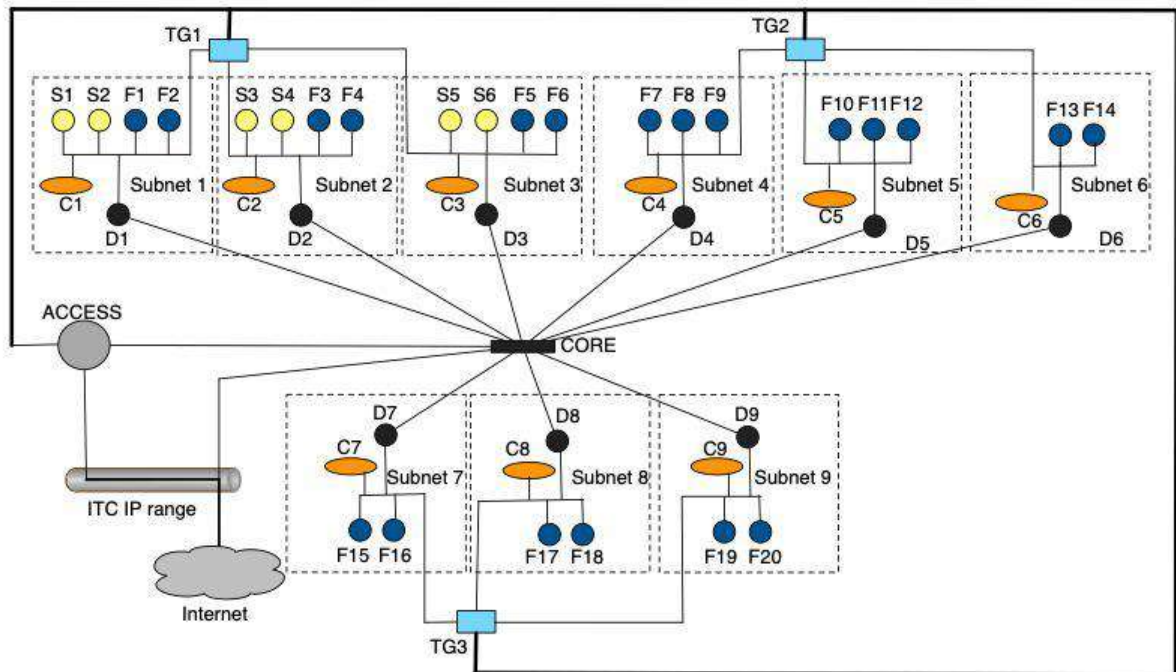


Рисунок 4.2 - Топологія COSSAK/D-WARD мережі[42]

Задачею Red Team було створювати напади, які на одній чи декількох крайових мережах суттєво погіршували або перешкоджали доступність мережесих ресурсів. Зниження - це результат зниження пропускної здатності трафіку до та від крайової мережі порівняно із пропускною здатністю, яка була

зафіксована до атаки. Відмова вказує на те, що, незважаючи на заходи COSSACK/D-WARD, послуги крайової мережі більше не доступні. Red Team не оцінювала сценарії часткового впровадження чи сценарії, які тестували масштабованість захистів, оскільки їхня увага була спрямована на атаки, які навантажують або обминають захисти. Зокрема COSSACK та D-WARD обидві впроваджують реакцію в непрямій близькості до джерел атаки для сценаріїв часткового впровадження.

Деякі атакувальники можуть проживати в мережах без D-WARD або COSSACK, в такому випадку їхній трафік може досягати жертви без перешкод і, якщо він достатньо великий, спричиняти атаку відмови в обслуговуванні. Було прикладено багато зусиль, щоб забезпечити те, що код атаки не може випадково вилетіти з експериментального середовища або бути вкрадений фактичними атакувальниками, які компрометують експериментальні хости для використання коду у майбутніх реальних атаках. За допомогою SSH через VPN весь виконавчий код атаки був завантажений в експериментальну мережу.

Red Team провели ряд різноманітних атак [42] на мережу, таких як:

Таблиця 4.2 - Техніки Red Team під час заходу

Spoofing Floods	Атакуючі комп'ютери, які використовують техніку підроблення для створення повеней, імітують джерелові адреси з /24 підмережі, в якій вони розташовані.
Rolling Floods	Ці атаки використовують часові аспекти механізму COSSACK/D-WARD. Рухомі повені координують багато агентів повені, використовуючи ці часові аспекти.

Кінець таблиці 4.2

HTTP Flood Attacks	Метою цих атак є вичерпання ресурсів цілі, висилаючи безперервний потік фальшивих запитів HTTP.
HTTP-Rolling Attacks	Ця атака поєднує атаку HTTP Flood та Rolling Flood
Connection Attacks	Оскільки таблиця стану, яку використовує операційна система для запису даних про з'єднання, має обмежений розмір, є строгий ліміт на кількість активних TCP-з'єднань одночасно для кожної операційної системи. Атаки на з'єднання намагаються займати місце в цій таблиці, встановлюючи частково відкриті TCP-з'єднання.
Connection-Rolling Attacks	Гібрид Rolling Flood та Connection Attack.
Proxy ACK Attacks	Концепція полягала в тому, щоб підробити TCP ACK для кожного TCP SYN-пакету, що надходить, з метою затоплення цілі.

Як результат, переваги інтеграції систем COSSACK та D-WARD виявились не настільки суттєвими, як очікувалося, оскільки D-WARD ідентифікував усі атаки, окрім ACK Proxy, COSSACK пропустив багато атак, і сумісна керувалася діями D-WARD.

4.6 Аналіз переваг та недоліків співпраці заходів Red Team vs Blue Team

Цінність інтегрованих операцій Red vs Blue очевидна: кожна команда приносить свої унікальні таланти на стіл, що призводить до більш надійної підтримки клієнтів. Blue Team забезпечує більш комплексний погляд на мережу, оскільки вона може виконувати енумерацію мережі великого масштабу. Red Team вносить «агресивне мислення та хитрі тактики у пошук шкідливих програм та збір інформації» [43].

Заходи червоний-проти-синього підтверджують, що системи оборони забезпечують ефективний захист від атак, для яких вони були призначені відвертати, але не здатні виявляти складні атаки. Саме такі заходи дають можливість Blue Team отримати досвід та інформацію про вразливості свого захисту, перед реальними хакерами, які шукають нестандартні шляхи прогникнення до мережі. Зрештою, такі заходи мали б більш вагомий результат, якби учасники могли взаємодіяти більш тісно і якщо всі команди брали участь у всіх фазах заходу. Якщо б Red Team отримували би інформацію про мережу таку, як слабкі місця, які слід більш ретельно перевіряти і на яких треба фокусуватися, не витрачаючи час на «кролячі діри». Та якщо Blue Team мало дозвіл переналаштовувати свою програму після кожної успішної атаки, якість оборони швидко покращилася. Цей вдосконалений захист потім міг бути перевірений для того, щоб переконатися, що виявлені вразливості були ефективно вирішені, а також для виявлення додаткових проблем.

Саме тому, для підвищення успіху в протидії складним загрозам та поліпшення загального стану безпеки наших підприємств, категорії Blue та Red повинні бути об'єднані. У майбутньому командам слід припинити діяти як противники, а замість цього почати партнерство та спільну роботу. Потенціал величезний, а вхідні бар'єри дійсно низькі. Інформаційна безпека пройшла

довгий шлях, але критично важливо продовжувати інновації та дослідження нових способів захисту.

Для покращення стратегії взаємодії пропоную наступну модель: команда Blue Team використовує платформу співпраці, щоб надати Red Team доступ до сеансу обміну екраном на одній з можливо уразливих систем. Red Team може виявити помилковий позитивний результат за десять хвилин, тоді як на його розслідування витратили б години. Крім того, Blue Team зможе виявити збої в платформі оплати компанії, хоча їх не можна однозначно призначити Red Team чи чому-небудь іншому. Спільно команди вдасться виявити вразливість щодо доступності платформи, обмінюючись логами та проводячи обговорення.

Висновок до 4 розділу

У цьому розділі було ретельно досліджено різні аспекти та елементи співпраці між командами Red та Blue у контексті кібербезпеки. Методологія та підходи до співпраці були проаналізовані для забезпечення ефективності обох команд у досягненні спільних цілей.

Стратегії, що використовуються Red Team під час заходу, і Blue Team під час заходу, були ретельно розглянуті. Це включало в себе агресивні тактики Red Team та стратегії виявлення та відповіді на загрози від Blue Team. Виявлено, що обидві команди вносять унікальні елементи, що сприяють покращенню загального кіберзахисту.

Крім того, детально проаналізовано координацію між командами. Виявлено, що ефективна комунікація та взаємодія є ключовими факторами для успіху спільних заходів. Реальний приклад заходу надав можливість детальніше розглянути, як взаємодія між Red та Blue Team може бути реалізована в практиці.

Аналіз співпраці між командами підкреслив важливість взаємодії обох сторін для ефективного виявлення, протидії та виправлення потенційних кіберзагроз. З урахуванням усіх аспектів, зазначених у цьому розділі, можна зробити висновок, що співпраця між Red та Blue Team виявляється ключовим елементом для досягнення оптимального кіберзахисту в організації.

ВИСНОВКИ

В магістерській роботі проведено ґрунтовний аналіз взаємодії Red Team та Blue Team, які вносять вагомий вклад у сучасні методи та стратегії захисту кіберпростору.

В ході виконання роботи було виконано наступні завдання.

1. Захист кіберпростору є надзвичайно важливим завданням, і для його успішного вирішення необхідно чітко відділяти дії в межах нормативно-правових актів. Дотримання законодавства, стандартів та оволодіння новітніми технологіями є визначальними факторами для забезпечення ефективного захисту від сучасних кіберзагроз та вдосконалення загального кібербезпекового стану.

2. У ході дослідження основних аспектів кібербезпеки в даній роботі, були ретельно проаналізовані та вивчені ключові фреймворки та стандарти. Це включало в себе детальний розгляд нормативних вимог, які регулюють кіберпростір, а також вивчення визнаних методик та стандартів забезпечення безпеки. Отримані знання про ці фреймворки та стандарти надають надійну основу для розробки та реалізації стратегій захисту, сприяючи ефективній та комплексній безпеці кіберпростору.

3. Дослідження Offensive Security в цій магістерській роботі привернуло увагу до важливості активного підходу у сфері кіберзахисту. Offensive Security визначається як стратегія, спрямована на виявлення вразливостей та недоліків у системах з метою попередження можливих атак. Роль Offensive Security у захисті кіберпростору полягає в імітації атак для виявлення слабких місць у системі та їхнього подальшого вдосконалення. Основні методики включають проведення пенетраційних тестів, етичного хакінгу та імітації реальних кібератак. Техніки Offensive Security охоплюють широкий спектр методів, від аналізу вразливостей програмного забезпечення до соціальної інженерії, щоб надати повний обзор системи та виявити можливі

шляхи атаки. Результати цього дослідження сприяють розумінню принципів та тактик Offensive Security для покращення загального рівня кібербезпеки в організаціях.

4. Дослідження розділу Defensive Security дозволило глибше розкрити роль цього напрямку у захисті кіберпростору. Defensive Security визначається як системний підхід до захисту інформаційних ресурсів, орієнтований на здатність вчасно виявляти, запобігати та виправляти кіберзагрози. Основною метою є створення резистентних та відповідальних механізмів у відповідь на різноманітні атаки. У рамках дослідження були розглянуті основні методики, такі як виявлення вразливостей, контроль доступу, моніторинг мережі та аналіз журналів подій. Техніки, що використовуються в Defensive Security, охоплюють відновлення даних, виявлення та ізоляцію загроз, а також розробку стратегій реагування на інциденти. Результати дослідження свідчать про важливість вдосконалення та постійного удосконалення заходів Defensive Security для ефективного протистояння сучасним та еволюційним кіберзагрозам.

5. В ході дослідження проведено ретельний огляд заходів, організованих Red та Blue team, з акцентом на їхні ролі, стратегії та методи координації під час заходу. Команда Red Team виступає в ролі агресора, використовуючи тактики, що імітують атаки кіберзлочинців, з метою виявлення вразливостей у системах та інфраструктурі. Їхня стратегія базується на агресивних атаках, які максимально наближені до реальних загроз. З іншого боку, Blue Team призначений для виявлення та відвертання атак, використовуючи проактивні заходи безпеки. Їхня стратегія орієнтована на виявлення та блокування небезпечних дій, забезпечуючи стійкість інфраструктури. Координація між командами важлива для ефективної реакції на загрози, і вона включає обмін інформацією, аналіз результатів атак та швидке прийняття відповідей. Співпраця між Red та Blue team виявилася вирішальною для розкриття потенційних вразливостей та розробки комплексної стратегії кіберзахисту.

6. Розглянуто конкретний випадок співпраці між Red та Blue team, який спрямовувався на перевірку захисту мережі від DDoS атак. Застосування технологій COSSAK та D-WARD дозволило вивчити реальні аспекти цього виклику в кіберпросторі. Red Team впроваджував атаки, щоб симулювати потенційні DDoS-атаки. Цей експеримент дозволив не лише побачити реальні сценарії DDoS-атак, а й визначити ефективність співпраці між командами. Зокрема, симульовані атаки дозволили Blue Team виявити слабкі місця у своїй системі захисту мережі. Кожен етап експерименту підкреслив важливість взаємодії між командами для подолання викликів у сфері кібербезпеки. Зазначені технології не лише допомагають ефективно захищати мережу від DDoS, але й підкреслюють, наскільки ключовою є синергія між Red та Blue team для досягнення максимального рівня кіберзахисту в сучасному цифровому середовищі.

7. Під час проведення комплексного аналізу взаємодії між командами Red та Blue, особливу увагу приділено виявленню ключових проблем, які впливають на ефективність їхніх заходів. Однією з основних проблем, виявленою під час дослідження, є недостатній рівень комунікації між командами та обміну зворотнього зв'язку під час проведення заходу. Цей недолік істотно розтягує часовий рамки та грошові витрати, оскільки невідосконала комунікація може призвести до неефективності стратегій та технік, використовуваних обома командами. Відсутність чіткого механізму обміну інформацією та зворотнього зв'язку впливає на швидкість реагування на загрози та виявлення вразливостей, що може серйозно підірвати успішність спільних заходів.

8. Розроблені рекомендації, викладені у цій магістерській роботі, ґрунтуються на глибокому аналізі, в якому були виявлені важливі проблеми та можливості для вдосконалення стратегії кіберзахисту. Перш за все, рекомендації наголошують на необхідності об'єднання команд Red та Blue замість їхнього протистояння. Визначено, що спільна робота і взаємодія стають ключовими факторами для ефективного реагування на кіберзагрози.

Зокрема, рекомендації вказують на потребу у постійному обміні інформацією між командами, що дозволить швидше виявляти та реагувати на потенційні загрози. Крім того, рекомендації спрямовані на спільне розроблення стратегій захисту та атаки, щоб забезпечити гармонійність дій обох команд. Це підкреслює необхідність створення інтегрованої підходу до кіберзахисту, де Red та Blue Team працюють в синергії для досягнення вищого рівня безпеки та впорядкування реакцій на виклики кіберпростору.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII : станом на 27 лип. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
2. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 27 жовт. 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
3. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР : станом на 1 лип. 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр#Text>
4. Про електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII : станом на 1 січ. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>
5. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII : станом на 31 берез. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>
6. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 17 серп. 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
7. What is the CIA Triad and Why is it important? | Fortinet. Fortinet. URL: <https://www.fortinet.com/resources/cyberglossary/cia-triad>
8. The Cyber Kill Chain: The Seven Steps of a Cyberattack. Cybersecurity Exchange. URL: <https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/>
9. Embrace proactive security with Zero Trust. Microsoft Security. URL: <https://www.microsoft.com/en-us/security/business/zero-trust>

10. What is Zero Trust Security? Principles of the Zero Trust Model. crowdstrike.com.

URL: <https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/>

11. Zero Trust Architecture. NIST. URL: <https://www.nist.gov/publications/zero-trust-architecture>

12. Active Directory - Definition and Details. Paessler - The Monitoring Experts. URL: <https://www.paessler.com/it-explained/active-directory>

13. Metasploit Framework | Metasploit Documentation. Docs @ Rapid7. URL: <https://docs.rapid7.com/metasploit/msf-overview/>

14. Buckbee M. What is Metasploit? The Beginner's Guide. Varonis: We Protect Data. URL: <https://www.varonis.com/blog/what-is-metasploit>

15. OWASP Top Ten | OWASP Foundation. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: <https://owasp.org/www-project-top-ten/>

16. MITRE ATT&CK: What It Is, How it Works, Who Uses It and Why | F5 Labs. F5 Labs. URL: <https://www.f5.com/labs/learning-center/mitre-attack-what-it-is-how-it-works-who-uses-it-and-why>

17. MITRE ATT&CK®. MITRE ATT&CK®. URL: <https://attack.mitre.org/>

18. Offensive Cybersecurity: The Definitive Guide - Flare. Flare | Cyber Threat Intel | Digital Risk Protection. URL: <https://flare.io/learn/resources/blog/offensive-cybersecurity/>

19. What is offensive security? | IBM. IBM in Deutschland, Österreich und der Schweiz | IBM. URL: <https://www.ibm.com/topics/offensive-security>

20. IBM Randori Recon. IBM in Deutschland, Österreich und der Schweiz | IBM. URL: <https://www.ibm.com/products/randori-recon>

21. Cybercrime To Cost The World 8 Trillion Annually In 2023. Cybercrime Magazine. URL: <https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/>

22. HTB Academy : Cybersecurity Training. Best Online Cybersecurity Courses & Certifications | HTB Academy. URL: <https://academy.hackthebox.com/module/90/section/936>
23. What is "Social Engineering"? ENISA. URL: <https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering>
24. What is Open Source Intelligence (OSINT)? SentinelOne. URL: <https://www.sentinelone.com/cybersecurity-101/open-source-intelligence-osint/>
25. Gillis A. S. What is Phishing and How Does it Work? | Definition from TechTarget. Security. URL: <https://www.techtarget.com/searchsecurity/definition/phishing>
26. What is Phishing. Microsoft Security. URL: <https://www.microsoft.com/en-us/security/business/security-101/what-is-phishing>
27. Reconnaissance, Tactic TA0043 - Enterprise | MITRE ATT&CK®. MITRE ATT&CK®. URL: <https://attack.mitre.org/tactics/TA0043/>
28. Linode. Red Team Reconnaissance Techniques. Linode Guides & Tutorials. URL: <https://www.linode.com/docs/guides/red-team-reconnaissance-techniques/>
29. Grimmick R. What is C2? Command and Control Infrastructure Explained. Varonis: We Protect Data. URL: <https://www.varonis.com/blog/what-is-c2>
30. Cobalt Strike | Defining Cobalt Strike Components & BEACON. Mandiant. URL: <https://www.mandiant.com/resources/blog/defining-cobalt-strike-components>
31. What Are the Vital Roles of the Blue Team in Cybersecurity? - Cyber Insight. Cyber Insight. URL: <https://cyberinsight.co/what-are-the-roles-of-the-blue-team/>

32. Internet-Wide Analysis of Subdomain Takeovers – Wave 1 -. RedHunt Labs: Comprehensive Attack Surface Management Solution. URL: <https://redhuntlabs.com/blog/project-resonance-wave-1/>
33. Fox J. Thinking Like an Attacker: Offensive Versus Defensive Cybersecurity. Pentest as a Service | Cobalt. URL: <https://www.cobalt.io/blog/offensive-versus-defensive-cybersecurity-tactics>
34. What is a firewall? Definition and explanation. www.kaspersky.com. URL: <https://www.kaspersky.com/resource-center/definitions/firewall>
35. What is Intrusion Detection Systems (IDS)? How does it Work? | Fortinet. Fortinet. URL: <https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system>
36. What Is an Intrusion Prevention System? IPS Definition | Proofpoint US. Proofpoint. URL: <https://www.proofpoint.com/us/threat-reference/intrusion-prevention-system-ips>
37. Mugisha D. CYBER SECURITY: Improving Cyber Defense Through Coherent Joint Red Team and Blue Team. The Journal of Defense Modeling and Simulation Applications Methodology Technology. № 01.04.2019.
38. Red Team vs Blue Team Exercise: Its Role in Finding Your Cybersecurity Flaws. Codemotion Magazine. URL: <https://www.codemotion.com/magazine/cybersecurity/red-team-vs-blue-team-exercise-its-role-in-finding-your-cybersecurity-flaws/>
39. Dale C. Red, Blue and Purple Teams: Combining Your Security Capabilities for the Best Outcome. A SANS Whitepaper. 2019.
40. Cybersecurity 101: What's the Difference Between Red Team vs. Blue Team?. Career Hub | Duke University. URL: <https://careerhub.students.duke.edu/blog/2023/11/11/cybersecurity-101-whats-the-difference-between-red-team-vs-blue-team/>
41. Take 2. think do. RED TEAM / BLUE TEAM CHALLENGE. Clinical Excellence Commission. 2015.

42. Testing a Collaborative DDoS Defense In a Red Team/Blue Team Exercise / J. Mirkovic et al. IEEE Transactions on Computers. 2008. Vol. 57, no. 8. P. 1098–1112.

43. Haney J., Paul C. Toward Integrated Tactical Operations for Red/Blue Cyber Defense Teams. Baltimore, August 2018.

44. HTB Academy : Cybersecurity Training. Best Online Cybersecurity Courses & Certifications | HTB Academy.
URL: <https://academy.hackthebox.com/module/148/section/1363>

45. HTB Academy : Cybersecurity Training. Best Online Cybersecurity Courses & Certifications | HTB Academy.
URL: <https://academy.hackthebox.com/module/74/section/699>

46. Your Partner in Open Source | Debricked.
URL: <https://debricked.com/blog/wp-content/uploads/2021/09/owasp-top10-list-2021-debricked-100-1024x341.jpg>

47. Wikimedia Commons.
URL: <https://upload.wikimedia.org/wikipedia/commons/thumb/5/5b/Firewall.png/640px-Firewall.png>

48. Employee and Customer Identity Solutions | Okta.
URL: <https://www.okta.com/sites/default/files/media/image/2021-05/IntrusionPreventionSystem.png>

49. Log In < Old Dominion University WordPress – WordPress.
URL: <https://sites.wp.odu.edu/darcyjudd/wp-content/uploads/sites/20195/2022/04/CIA-Triad.png>