

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології захисту мережної
інфраструктури підприємства (на прикладі ТОВ
“Партнер”))»

Виконав студент II-го курсу групи КБм-22-1
спеціальності 125 «Кібербезпеки»

 М.М. Кухарчук

Керівник завідувач кафедри комп'ютерної інженерії та
кібербезпеки, кандидат технічних наук, доцент

 А.А. Сфіменко

Рецензент доцент кафедри комп'ютерної інженерії та
кібербезпеки, кандидат технічних наук, доцент

 Ю.М. Росінський

Житомир – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ЗАТВЕРДЖУЮ

Завідувач кафедри
комп'ютерної інженерії та
кібербезпеки

 Андрій Єфіменко

13 жовтня 2023 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студент: Кухарчук Максим Михайлович

Тема роботи: **«Методи та технології протидії кібератакам на мережну
інфраструктуру підприємства (на прикладі ТОВ «Партнер»)»**

Затверджена Наказом університету від 13 жовтня 2023 р. № 572/с

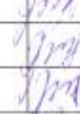
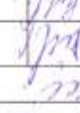
Термін здачі студентом закінченої роботи 11 грудня 2023 р.

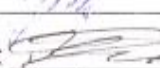
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

1. Об'єкт дослідження – процес захисту мережевої інфраструктура підприємства.

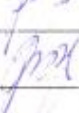
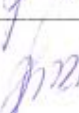
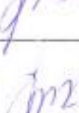
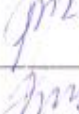
2. Предмет дослідження – методи та технології захисту мережевої інфраструктури підприємства

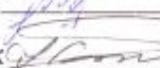
Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	В.В. Воротніков	 2.11.2023	 2.11.2023
2	В.В. Воротніков	 6.11.2023	 6.11.2023
3	В.В. Воротніков	 10.11.2023	 10.11.2023

Студент  М.М. КухарчукКерівник  А.А. Єфіменко

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка задачі	2 листопада 2023	
2	Формулювання технічного завдання	5 листопада 2023	
3	Проектування структури роботи	7 листопада 2023	
4	Написання 1 розділу	8 листопада 2023 – 14 листопада 2023	
5	Написання 2 розділу	15 листопада 2023 – 24 листопада 2023	
6	Написання 3 розділу	25 листопада 2023 – 8 грудня 2023	
7	Перевірка	11 грудня 2023	
8	Захист	26 грудня 2023	

Студент  М.М. КухарчукКерівник  А.А. Єфіменко

РЕФЕРАТ

Випускна робота магістра складається із вступу, трьох розділів, загальних висновків, додатків, списку використаних джерел і має 60 сторінку основного тексту, 20 додатків. Список використаних джерел містить 15 найменування і займає 1 сторінку. Загальний обсяг роботи 60 сторінок.

Метою наукового дослідження, що становить основу мого дипломного проєкту, є аналіз мережевої інфраструктури підприємства ТОВ "Партнер" на основі конкретного випадку. Основним завданням є вивчення сучасних методів та технологій боротьби з кіберзагрозами, які можуть впливати на мережеву інфраструктуру підприємства. Додатковою метою є представлення на практиці найпоширеніших помилок, які виникають при розробці заходів з захисту мережевої інфраструктури підприємства.

ABSTRACT

The master's thesis comprises an introduction, three chapters, general conclusions, appendices, a list of references, and has a main text of 60 pages, with an additional 20 appendices. The list of references includes 15 entries and spans 1 page. The total length of the thesis is 60 pages.

The objective of the research forming the basis of my diploma project is to analyze the network infrastructure of the company "Partner" LLC based on a specific case study. The primary task is to explore contemporary methods and technologies for countering cyber threats that may impact the enterprise's network infrastructure. An additional goal is to demonstrate, through practical examples, the most common errors encountered in the development of measures to protect the enterprise's network infrastructure.

ПЛАН

ВСТУП

РОЗДІЛ 1. АНАЛІЗ МЕТОДІВ ТА ТЕХНОЛОГІЙ ПРОТИДІЇ КІБЕРАТАКАМ НА МЕРЕЖЕВУ ІНФРАСТРУКТУРУ ПІДПРИЄМСТВА

1.1 Методи виявлення та аналізу вразливостей та кіберзагроз

1.2 Методи захисту від кібератак на різних рівнях мережевої інфраструктури

1.3 Аналіз застосування мережевих протоколів та технологій для захисту мережевої інфраструктури

1.4 Аналіз заходів забезпечення безпеки мережевої інфраструктури підприємства

РОЗДІЛ 2. АНАЛІЗ СТАНУ ЗАХИЩЕНОСТІ ТА РОЗРОБКА ПРОЄКТУ ПОКРАЩЕННЯ РІВНЯ ЗАХИСТУ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ ПІДПІДПРИЄМСТВА ТОВ “ПАРТНЕР”

2.1 Аналіз мережевої інфраструктури підприємства ТОВ “Партнер”

2.2 Аналіз загроз та методів протидії кібератакам на мережеву інфраструктуру підприємства ТОВ “Партнер”

2.3 Вибір технологій захисту мережевої інфраструктури

РОЗДІЛ 3. ДОСЛІДЖЕННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ ЗАХОДІВ ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ

3.1 Оцінка ефективності вибраних методів та технологій протидії кібератакам на мережеву інфраструктуру підприємства

3.2 Рекомендації щодо поліпшення захисту мережевої інфраструктури підприємства ТОВ “Партнер”

3.3 Рекомендації щодо подальшого розвитку мережевої інфраструктури підприємства ТОВ “Партнер”

ВИСНОВКИ

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

ВСТУП

Сучасний світ вже давно зазнав впливу інформаційних технологій, які змінили підхід до ведення бізнесу та організації робочих процесів. Зростаюча залежність від цифрових систем та мережевої інфраструктури призвела до виникнення нового виду загроз - кібератак. Ці атаки можуть завдати непоправної шкоди, як фінансовій стійкості підприємств, так і їхній репутації. Протидія кібератакам на мережеву інфраструктуру підприємства стала однією з найважливіших завдань для організацій будь-якої сфери діяльності. Стратегії та методи захисту від кіберзагроз набувають все більшої актуальності, оскільки загрози постійно еволюціонують і стають все більш вдосконаленими та складними для виявлення.

Цей проект має на мені розглянути та дослідити методи та технології протидії кібератакам на мережеву інфраструктуру підприємства. Ціль дослідити і проаналізувати існуючі підходи до захисту від кіберзагроз та розробити комплексну стратегію, яка допоможе забезпечити максимально можливий рівень безпеки для мережевої інфраструктури підприємства. Дослідження зосереджене на різних аспектах кібербезпеки, включаючи виявлення вразливостей, моніторинг активності, реагування на інциденти та відновлення після атаки.

Проект базується на глибокому аналізі наукових джерел, передових практик та відомих кейсів кібератак. Він використовує міждисциплінарний підхід, об'єднуючи знання з областей кібербезпеки, комп'ютерної науки, криптографії та інших відповідних дисциплін.

Результати цього дослідження можуть послужити основою для розробки нових стратегій кібербезпеки та покращення існуючих підходів до захисту мережевої інфраструктури. Вони можуть бути корисними для бізнес-лідерів, кібербезпекових експертів, адміністраторів мереж та всіх зацікавлених сторін, які прагнуть забезпечити стійкість та безпеку своїх цифрових ресурсів.

У наступних розділах цього дипломного проекту будуть розглянуті різні аспекти методів та технологій протидії кібератакам, включаючи виявлення загроз, аналіз вразливостей, застосування захисних механізмів та відновлення після атак. Крім того, будуть розглянуті сучасні тенденції в області кібербезпеки та їх вплив на розробку стратегій захисту мережевої інфраструктури підприємства.

Опис проблеми

У сучасному світі, де мережеві технології перетворилися на необхідну складову діяльності підприємств, кібербезпека стала надзвичайно важливою задачею для бізнесу. Кібератаки стали невід'ємною частиною цього процесу і можуть призвести до серйозних наслідків для підприємства, включаючи втрату даних, порушення роботи мережі, пошкодження репутації, фінансові втрати та навіть банкрутства. Тому розробка ефективної стратегії протидії кібератакам є надзвичайно важливою задачею для кожного підприємства. Це включає в себе розуміння та застосування різних методів та технологій, які забезпечують захист мережевої інфраструктури.

Актуальність теми

Завдання забезпечення безпеки мережевої інфраструктури підприємств в сучасному цифровому світі є однією з найважливіших проблем. Швидкий технологічний розвиток призвів до збільшення обсягів цифрової інформації, яка обмінюється та зберігається в мережевих середовищах. Однак цей розвиток супроводжується зростанням загроз в кібербезпеці. Кіберзлочинці використовують різноманітні техніки та методи для здійснення кібератак, спрямованих на отримання несанкціонованого доступу до конфіденційної інформації, порушення роботи систем, а також викрадення цінних ресурсів.

Серед сучасних загроз можна виділити такі типи кібератак, як DDoS-атаки, фішинг, розповсюдження шкідливих програм, використання вразливостей програмного забезпечення тощо. Ці загрози накладають негативний вплив на бізнес-процеси підприємств, призводять до витоку конфіденційної інформації, втрати репутації та фінансових збитків. Тому виникає важлива потреба у розробці та застосуванні ефективних методів і технологій для протидії цим загрозам.

Однією з основних причин, яка робить цю тему актуальною, є зростання залежності підприємств від інформаційних технологій. Мережева інфраструктура стала невід'ємною частиною функціонування бізнес-середовища, де відбувається обмін даними, здійснюються транзакції та управління ресурсами. Така залежність робить підприємства вразливими перед можливими кібератаками, що можуть викликати значні матеріальні та репутаційні збитки.

Застосування методів та технологій протидії кібератакам стає невідкладною задачею. Важливо визначити потенційні загрози, розробити стратегії виявлення та запобігання атакам, а також реалізувати механізми відновлення після інциденту. Серед інших аспектів, доцільно вивчити методи аутентифікації, шифрування, виявлення аномалій та моніторингу мережевої активності.

Також варто враховувати важливість співпраці між різними суб'єктами: дослідниками, виробниками програмного забезпечення, спеціалістами з кібербезпеки та представниками підприємств. Обмін знаннями та досвідом допоможе швидко реагувати на нові загрози та розробляти відповідні засоби захисту.

У роботі над дипломним проєктом на тему "Методи та Технології протидії кібератакам на мережеву інфраструктуру підприємства" буде проведено комплексне дослідження сучасних методів та технологій кібербезпеки, їхню адаптацію до потреб підприємств та ефективну інтеграцію.

Дослідження теми буде відбуватись не тільки з точки зору теоретичних та інформаційних ресурсів, а також на реальному прикладі мережевої інфраструктури підприємства ТОВ «Партрен». Результати дослідження допоможуть удосконалити практичні підходи до захисту мережевої інфраструктури, забезпечити надійність та стабільність її функціонування, а також сприятимуть загальному зростанню рівня кібербезпеки в бізнес-середовищі.

Інформаційна довідка:

Найбільш поширеними видами кібератак є:

1. Фішинг, спам, та інші методи соціальної інженерії, що сприяють введенню користувачів в оману, щоб отримати доступ до їх даних.

2. Віруси, троянські програми, шпигунський софт та інші віруси-шкідники, які використовуються для розширення доступу до системи та отримання даних.
3. DDoS-атаки, які спрямовані на перевантаження мережі або системи, щоб вони перестали працювати.

Мета та завдання дослідження

Мета цього проєкту полягає у вивченні найпоширеніших на даний момент загроз та дослідженні різних методів та технологій протидії кібератакам на мережеву інфраструктуру підприємства. У роботі буде розглянуто такі теми, як ідентифікація загроз, моніторинг мережі, виявлення та аналіз вразливостей, а також застосування різноманітних технологій захисту, таких як мережеві фаєрволи, інтегровані системи безпеки та захисту кінцевих точок.

Для досягнення цієї мети використовуватимуться різні джерела, включаючи особистий досвід, наукові статті, веб-ресурси, книги та практичні досвіди. У роботі будуть розглянуті різні підходи та методики, які застосовуються для забезпечення кібербезпеки на мережевій інфраструктурі підприємства, та їхні переваги та недоліки. Крім того, у цій роботі будуть розглянуті рекомендації щодо розробки ефективної стратегії протидії кібератакам на мережеву інфраструктуру підприємства, яка може забезпечити базово-прийнятний рівень безпеки для середньостатистичних мережевих інфраструктур.

Оскільки кібербезпека є важливим аспектом діяльності будь-якого підприємства, результат цього проєкту може бути корисними для фахівців з кібербезпеки, адміністраторів мереж, інженерів з безпеки та інших фахівців, які працюють з мережевою інфраструктурою. Результати дослідження також можуть бути корисними для студентів, які вивчають кібербезпеку та інформаційну безпеку.

Завданнями дослідження є:

1. Огляд основних видів кібератак та їхніх наслідків для мережевої інфраструктури підприємства.
2. Опис методів та технологій протидії кібератакам на мережеву інфраструктуру підприємства, включаючи брандмауери, антивірусні програми, системи виявлення вторгнень, антиспам-фільтри, мультифакторну аутентифікацію та резервне копіювання.
3. Вивчення ефективності кожного з цих методів та технологій в протидії кібератакам на мережеву інфраструктуру підприємства.
4. Аналіз проблем та обмежень при використанні цих методів та технологій та запропонування рішень для їх подолання.
5. Розробка рекомендацій щодо вибору та застосування методів та технологій протидії кібератакам на мережеву інфраструктуру підприємства в залежності від його потреб та бюджету.
6. Визначення перспектив розвитку методів та технологій протидії кібератакам на мережеву інфраструктуру підприємства в майбутньому.
7. Розробка рекомендацій щодо підвищення кваліфікації та обізнаності співробітників підприємства у питаннях кібербезпеки.
8. Аналіз потенційних загроз з боку злочинців та хакерів, які можуть атакувати мережеву інфраструктуру підприємства, та розробка стратегії щодо запобігання таких атак.

9. Визначення ролі та відповідальності кожного співробітника підприємства у забезпеченні кібербезпеки та розробка політики кібербезпеки

Об’єктом дослідження є мережева інфраструктура підприємства ТОВ “Партнер”.

Предметом дослідження є методи та технології захисту мережевої інфраструктури підприємства.

Висновки до вступу

Розробка та впровадження комплексної системи протидії кібератакам на мережеву інфраструктуру підприємства є ключовим завданням для забезпечення безпеки та стійкості інформаційних систем. Послідовне виконання плану впровадження та врахування високих стандартів безпеки допоможуть зменшити ризики та наслідки кібератак на підприємство.

РОЗДІЛ 1

АНАЛІЗ МЕТОДІВ ТА ТЕХНОЛОГІЙ ПРОТИДІЇ КІБЕРАТАКАМ НА МЕРЕЖЕВУ ІНФРАСТРУКТУРУ ПІДПРИЄМСТВА

Мережева інфраструктура підприємства є об'єктом постійно зростаючих загроз з боку кіберзлочинців. Аналіз методів та технологій протидії кібератакам є невід'ємною частиною зусиль щодо забезпечення безпеки цієї інфраструктури. Застосування мережевих протоколів та технологій для захисту мережевої інфраструктури є ключовим для підтримки цілісності, конфіденційності та доступності даних та сервісів в організації. Одним з основних аспектів аналізу є вивчення методів виявлення та відстеження кіберзагроз. Від стандартних сигнатурних методів до сучасних систем машинного навчання, існують численні техніки, спрямовані на розпізнавання аномальної активності та недозволеного доступу.

Під час аналізу методів та технологій протидії кібератакам, важливо враховувати специфіку мережевої інфраструктури підприємства та її потреби щодо захисту. Різні сектори та підприємства можуть мати відмінні вимоги щодо кібербезпеки, і, відповідно, можуть вимагати різних підходів та технологій.

В цьому розділі ми розглянемо сучасні підходи до виявлення, запобігання та реагування на кіберзагрози. Ми розглянемо, які технології і методи можуть бути застосовані для ефективного захисту мережі в умовах постійної зміни кіберзагроз та вимог регуляторів.

Класифікація Кібератак:

1. Мережеві атаки:

- DDoS (Distributed Denial of Service) – атаки, спрямовані на виведення з ладу важливих ресурсів.
- Man-in-the-middle (MitM) – атаки, при яких зловмисник перехоплює та може змінювати комунікацію між двома сторонами.
- Phishing – вид шахрайства, спрямований на викрадення конфіденційних даних (наприклад, паролів).

2. Програмні атаки:

- Віруси та трояни – шкідливе програмне забезпечення, що може реплікуватися та виконувати несанкціоновані дії.
- Ransomware – зловмисне ПЗ, що блокує доступ до системи або даних, вимагаючи викуп.

3. Атаки на застосунки:

- SQL injection – вставка шкідливих SQL-запитів через веб-форми.
- Cross-site scripting (XSS) – вставка шкідливих скриптів в веб-сторінки.

4. Фізичні атаки:

- Доступ до обладнання – незаконний фізичний доступ до мережевих пристроїв.
- Завади на лініях зв'язку – перехоплення або знищення даних у фізичних лініях передачі.

Методи та Технології Протидії:

1. Превентивні міри:

- Фаєрволи – захист мережі шляхом контролю вхідного та вихідного трафіку.
- Antivirus/Anti-malware software – захист від шкідливого програмного забезпечення.
- Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS) – системи, що ідентифікують потенційні вторгнення та блокують їх.
- Багаторівнева перевірка автентичності – вимагає від користувача кілька форм автентифікації для доступу до ресурсів.
- Шифрування – захист даних шляхом перетворення інформації в код, який важко дешифрувати без ключа.

- Системи управління ідентичностями та доступом (Identity and Access Management - IAM) – технології, що дозволяють контролювати доступ до різних ресурсів у мережі та управління користувацькими ідентифікаторами.

2. Детективні міри:

- Системи аналізу безпеки – використовують алгоритми машинного навчання для виявлення аномалій у мережі.

- Логування та моніторинг – збір та аналіз логів з мережевих пристроїв для виявлення ознак компрометації.

- SIEM (Security Information and Event Management) – рішення, які забезпечують реальний час моніторингу та аналізу інцидентів безпеки.

3. Реактивні міри:

- Плани реагування на інциденти – документовані процедури для ефективної реакції на кіберінциденти.

- Команди швидкого реагування на комп'ютерні інциденти (Computer Emergency Response Teams - CERTs/CSIRTs) – групи експертів, готових втрутитися при виявленні кібератаки.

- Відновлення після збоїв – використання резервних копій та планів відновлення для відновлення функціонування після атаки.

4. Організаційні міри:

- Політика безпеки інформації – розробка та впровадження комплексних правил та регуляцій щодо кібербезпеки в організації.

- Навчання та свідомість персоналу – регулярне навчання співробітників методам ідентифікації та запобігання кібератакам.

- Аудит безпеки – регулярне оцінювання та перевірка безпеки мережевих систем та процедур.

5. Технічні стандарти та протоколи:

- ISO/IEC 27001 – міжнародний стандарт системи управління інформаційною безпекою.
- NIST Cybersecurity Framework – керівництво, розроблене Національним інститутом стандартів та технологій США, для управління та зниження кібербезпеки ризиків.
- PCI DSS – стандарт безпеки даних для всіх організацій, які приймають, обробляють, зберігають або передають інформацію про кредитні карти.

6. Технологічні інновації:

- Blockchain – технологія розподіленого реєстру може бути використана для підвищення безпеки та непідробності даних.
- Штучний інтелект та машинне навчання – аналізують великі обсяги даних для виявлення зразків, що можуть вказувати на кіберзагрози, а також можуть автоматизувати процеси реагування на інциденти.
- Розширене шифрування – новітні алгоритми шифрування, такі як квантове шифрування, забезпечують вищий рівень безпеки для передачі даних.

7. Стійкість інфраструктури:

- Розділення привілеїв – обмеження доступу до ресурсів для зменшення ризику зловмисних дій з боку внутрішніх користувачів.
- Жорстке сегментування мережі – поділ мережі на сегменти для обмеження поширення атаки всередині мережі.
- Резервне копіювання та відновлення даних – створення та збереження резервних копій даних для забезпечення можливості швидкого відновлення після інцидентів.

8. Комплаєнс і законодавче регулювання:

- GDPR, CCPA та інші норми конфіденційності – дотримання вимог до захисту особистих даних відповідно до різних юрисдикцій.

- Законодавче регулювання галузі – специфічні для галузі вимоги, як-от HIPAA у медичній сфері, або FISMA для урядових організацій.

9. Постійний розвиток та адаптація:

- Адаптивна безпека – розробка та впровадження систем безпеки, які можуть адаптуватися до змін у кіберзагрозах та технологіях.

- Постійне навчання та оновлення політик – регулярне оновлення політик безпеки та процедур, а також навчання співробітників для врахування новітніх загроз і кращих практик.

Аналіз методів та технологій протидії кібератакам повинен також включати регулярний огляд та оцінку ефективності впроваджених заходів безпеки, включаючи технічні рішення, організаційні процеси та політики. Це вимагає комплексного підходу до кібербезпеки, що поєднує технології, процеси та людський фактор для забезпечення гнучкої та стійкої мережевої інфраструктури підприємства.

1.1 Методи виявлення та аналізу вразливостей та кіберзагроз

Методи виявлення та аналізу вразливостей та кіберзагроз – це критичний елемент управління ризиками для будь-якого підприємства. Ці методи можуть бути поділені на кілька основних категорій:

1. Автоматизоване сканування вразливостей:

- Статичний аналіз коду (SAST): цей метод використовується для виявлення вразливостей в програмному коді на ранніх етапах розробки.

- Динамічний аналіз програм (DAST): інструменти DAST тестують програми в режимі реального часу і шукають вразливості під час виконання програми.
- Інтерактивне тестування безпеки програмного забезпечення (IAST): поєднує елементи SAST і DAST для надання більш глибокого аналізу.
- Сканери вразливостей мережі: інструменти, які сканують мережеві пристрої на наявність відомих вразливостей.

2. Пенетраційне тестування:

- Експлойт фреймворки (наприклад, Metasploit): використовуються для тестування систем на наявність вразливостей через емуляцію атак.
- Ручне пенетраційне тестування: проводиться спеціалістами з кібербезпеки, які використовують нестандартні методи для виявлення вразливостей.

3. Моніторинг та логування:

- SIEM системи: збір та аналіз логів з різних систем і пристроїв для виявлення підозрілої поведінки.
- Інструменти моніторингу мережі: використовуються для виявлення аномалій у трафіку, які можуть вказувати на кібератаки.

4. Тестування на проникнення людського фактора:

- Соціальна інженерія: тестування готовності персоналу до атак, які використовують соціальну інженерію.
- Фішингові симуляції: навчальні кампанії, спрямовані на виявлення схильності співробітників до фішингу.

5. Інтелектуальний аналіз кіберзагроз:

- Threat Intelligence платформи: збір та аналіз інформації про актуальні кіберзагрози для попередження можливих атак.
- Кіберрозвідка: дослідження та аналіз інформації з відкритих джерел (OSINT), форумів зловмисників, та інших джерел для ідентифікації потенційних загроз.

6. Застосування штучного інтелекту та машинного навчання:

- Прогнозування та виявлення аномалій: використання алгоритмів машинного навчання для ідентифікації не звичної поведінки, яка може вказувати на кібератаку.
- Автоматизація реагування на інциденти: AI системи можуть автоматично реагувати на певні типи кібератак без втручання людини.

Розвиток методів виявлення та аналізу вразливостей та кіберзагроз є безперервним процесом. Підприємства повинні регулярно оновлювати свої інструменти та методики, щоб відповідати зростаючій складності кіберзагроз і змінам в технологіях. Це також включає тренування та освіту співробітників, розробку і впровадження політик безпеки, а також створення культури безпеки, яка пронизує всі рівні організації.

Мережева інфраструктура підприємства стає об'єктом постійних кіберзагроз, що можуть призвести до суттєвих наслідків для безперервності бізнесу та захисту конфіденційної інформації. Один із перших етапів в розробці стратегії захисту мережевої інфраструктури - це виявлення потенційних вразливостей і аналіз існуючих кіберзагроз.

Виявлення вразливостей мережевої інфраструктури вимагає використання спеціалізованих інструментів і методів. Один зі способів - це проведення тестів на проникнення (Penetration Testing), які спрямовані на пошук слабких місць у мережевій інфраструктурі шляхом спроби проникнення в

систему, як це може зробити потенційний зловмисник. Важливо виявити та усунути ці вразливості до того, як їх використовують для атаки.

Паралельно з цим, аналіз кіберзагроз є невід'ємною частиною роботи з кібербезпеки. Кіберзагрози можуть бути різними - від вірусів та троянських коней до атаки на рівні перехоплення даних чи збою в роботі мережі. Для їх виявлення та аналізу використовуються системи виявлення і запобігання вторгнення (Intrusion Detection and Prevention Systems, IDS/IPS), які спеціалізуються на виявленні незвичайних та підозрілих активностей в мережі.

Ще одним важливим аспектом виявлення вразливостей та кіберзагроз є аналіз журналів подій (Event Logs) та моніторинг активності в мережі. Цей процес дозволяє вчасно виявляти надзвичайні ситуації та потенційні загрози для мережі.

Крім того, існують інструменти для оцінки стійкості мережевої інфраструктури до атак та вразливостей. Ці інструменти допомагають визначити, наскільки ефективним є захист мережі та чи необхідні подальші заходи для поліпшення безпеки.

Методи виявлення та аналізу вразливостей та кіберзагроз є критичними для розробки ефективних стратегій захисту мережевої інфраструктури підприємства. Після виявлення можливих проблем, розробка та впровадження відповідних заходів безпеки може допомогти підприємствам підвищити рівень захисту та запобігти потенційним кібератакам.

1.2 Методи захисту від кібератак на різних рівнях мережевої інфраструктури

Забезпечення високого рівня кібербезпеки вимагає комплексного підходу, оскільки кібератаки можуть статися на різних рівнях мережевої

інфраструктури підприємства. Для ефективного захисту важливо розглянути методи захисту на кожному з цих рівнів.

На рівні додатків та програмного забезпечення, заходи захисту включають в себе використання кодування, аутентифікації та авторизації для обмеження доступу до даних та функцій. Також важливо надавати патчі та оновлення для програм, що використовуються, щоб запобігти використанню відомих вразливостей.

На рівні мережі, брандмауери, VPN (віртуальні приватні мережі) та сегментація мережі грають важливу роль у захисті від небажаних вторгнень та моніторингу мережевого трафіку. Це дозволяє контролювати доступ та виявляти аномальну активність.

На фізичному рівні, фізичний захист мережевого обладнання та дата-центрів важливий для запобігання фізичним атакам, які можуть призвести до втрати доступу до обладнання.

Крім цього, важливо мати стратегії реагування на кібератаки, включаючи резервне копіювання даних, плани відновлення після аварії та розгортання системи моніторингу безпеки.

Методи захисту на різних рівнях мережевої інфраструктури повинні бути інтегровані в єдину стратегію кібербезпеки підприємства. Це дозволить забезпечити всебічний захист та реагування на кіберзагрози на всіх рівнях мережевої інфраструктури та зменшити ризики для бізнесу.

1.3 Аналіз застосування мережевих протоколів та технологій для захисту мережевої інфраструктури

В контексті забезпечення кібербезпеки мережевої інфраструктури підприємства, вибір та аналіз мережевих протоколів та технологій є надзвичайно важливим завданням. Мережеві протоколи та технології відіграють ключову роль у забезпеченні безпеки передачі даних та захисту мережевої інфраструктури в цілому.

Одним з найважливіших аспектів є шифрування даних під час їх передачі через мережу. Застосування шифрування на рівні мережевих протоколів, таких як SSL/TLS для безпечних з'єднань, дозволяє забезпечити конфіденційність даних та запобігти перехопленню інформації злоумисниками.

Технології віртуальної приватної мережі (VPN) є ефективним засобом для захисту мережевого трафіку при підключенні до віддалених робочих місць або гілок підприємства. Вони забезпечують шифрування та безпеку даних під час їх передачі через публічну мережу, що дозволяє знизити ризики для конфіденційності даних.

Додатково, важливо розглянути застосування мережевих брандмауерів та систем виявлення вторгнень (IDS) на рівні мережі для моніторингу та фільтрації мережевого трафіку. Ці інструменти допомагають виявляти та блокувати небажану активність та потенційні загрози.

Аналіз і вибір мережевих протоколів та технологій для захисту мережевої інфраструктури підприємства вимагає розуміння специфіки бізнес-процесів та загроз, з якими може стикнутися організація. Це дозволить визначити найкращі практики та вирішення, які відповідають потребам безпеки та сприяють надійному функціонуванню мережевої інфраструктури підприємства.

1.4 Аналіз заходів забезпечення безпеки мережевої інфраструктури підприємства.

Забезпечення безпеки мережевої інфраструктури підприємства є завданням великої важливості, оскільки велика частина бізнес-процесів та обміну даними відбувається через мережу. Аналіз заходів забезпечення безпеки допомагає визначити, наскільки дієві і адаптовані до сучасних загроз заходи вживає підприємство.

Одним із ключових аспектів є політика безпеки, яка визначає стандарти та процедури для забезпечення конфіденційності, цілісності та доступності даних. Політика безпеки також включає в себе вимоги до паролів, управління доступом та інші аспекти захисту інформації.

Для ефективності заходів забезпечення безпеки, важливо регулярно навчати персонал щодо найкращих практик кібербезпеки та інструкцій щодо реагування на інциденти.

Важливим аспектом є також моніторинг та аудит безпеки мережі. Це дозволяє вчасно виявляти аномальну активність та потенційні загрози, а також забезпечувати дотримання стандартів безпеки та політики.

Додатково, забезпечення безпеки мережевої інфраструктури включає в себе резервне копіювання даних та плани відновлення після аварії. Це допомагає забезпечити доступність даних та функціонування мережі навіть після потенційних інцидентів.

Аналіз заходів забезпечення безпеки мережевої інфраструктури допомагає підприємству оцінити свій загальний рівень захисту та визначити області для подальших покращень. Впровадження ефективних заходів забезпечення безпеки допомагає запобігти кібератакам та забезпечити надійність мережевої інфраструктури підприємства.

РОЗДІЛ 2

АНАЛІЗ СТАНУ ЗАХИЩЕНОСТІ ТА РОЗРОБКА ПРОЄКТУ ПОКРАЩЕННЯ РІВНЯ ЗАХИСТУ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА ТОВ "ПАРТНЕР"

У цьому розділі проводиться аналіз поточного стану кібербезпеки мережевої інфраструктури на прикладі ТОВ "Партнер". Оцінюються

існуючі заходи безпеки та виявляються можливі слабкі місця. На основі цього аналізу розробляється проєкт, спрямований на покращення рівня захисту мережі та забезпечення надійності функціонування підприємства в умовах постійних кіберзагроз.

2.1 Аналіз мережевої інфраструктури підприємства ТОВ “Партнер”

Мережева інфраструктура є невід'ємною частиною сучасного підприємства, і вона виконує ряд важливих функцій для забезпечення ефективності та безпеки його діяльності. Для нашого дослідження, ми будемо використовувати мережеву інфраструктуру ТОВ “Партнер”, яка складається з різноманітних компонентів, кожен з яких відіграє важливу роль у функціонуванні підприємства. Мережева інфраструктура підприємства складається з таких компонентів:

1. **Сервери баз даних:** Ці сервери відповідають за зберігання та обробку великої кількості корпоративних даних. Вони є надзвичайно важливими для бізнес-процесів, і їх доступність і безпека мають критичне значення.
2. **Файловий сервер:** Файловий сервер використовується для спільного доступу до файлів і ресурсів на мережі. Важливо забезпечити надійне зберігання та обмін даними між користувачами.
3. **Сервер відеоспостереження:** Цей сервер допомагає відслідковувати події та забезпечує безпеку на території підприємства, зокрема, за допомогою системи відеоспостереження.
4. **Персональні комп'ютери користувачів:** Робочі станції користувачів, використовуються для виконання різних завдань і програм, необхідних для робочого процесу.

5. **Маршрутизатор-фаєрвол:** Він є ключовим пристроєм для забезпечення безпеки мережі, контролю трафіку та фільтрації шкідливих даних.
6. **Мережеві комутатори (Switch):** Ці пристрої використовуються для підключення всіх інших пристроїв до мережі та ефективного розподілу трафіку.
7. **Мережевий принтер та IP телефони:** Мережевий принтер та IP телефони дозволяють користувачам спільно використовувати ресурси і забезпечують зручну комунікацію.
8. **IP камери:** IP камери використовуються для відеоспостереження та контролю об'єктів безпеки підприємства.
9. **VPN (віртуальна приватна мережа):** Підприємство надає можливість віддаленим користувачам підключатися до внутрішніх ресурсів через VPN, що забезпечує безпеку та захист конфіденційної інформації при їх передачі.
10. **Оптоволоконні лінії підключення до глобальної мережі INTERNET:** Підприємство має дві оптоволоконні лінії для підключення до Інтернету, що забезпечує надійність та резервність з'єднання з глобальною мережею.

Аналіз цих компонентів мережевої інфраструктури ТОВ “Партнер” є важливим для забезпечення їх ефективності та безпеки. Він допомагає ідентифікувати можливі ризики, визначити слабкі місця та розробити стратегії для покращення інфраструктури, щоб підприємство могло продовжувати безперебійно функціонувати і залишатися конкурентоспроможним. Згідно з аналізом наявних елементів мережевої інфраструктури була складена загальна схема мережі.

Схематична топологія інфраструктури ТОВ “Партнер” відображена в **Додаток 1.**

2.2 Аналіз загроз та методів протидії кібератакам на мережеву інфраструктуру підприємства ТОВ “Партнер”

Мережева інфраструктура підприємства є фундаментальним складовим елементом сучасної ділової діяльності, і вона стає все більш вразливою перед сучасними кіберзагрозами. У даному контексті пропонуємо розглянути таблицю, яка представляє можливі основні критичні точки в мережевій інфраструктурі підприємства, ТОВ “Партнер” а також найактуальніші загрози. Зазначимо, що ця таблиця включає в себе лише обмежений перелік можливих загроз і точок вразливості, і в реальності їх може бути значно більше, що підкреслює необхідність постійного моніторингу та захисту мережі підприємства.

Проаналізувавши раніше складену топологію мережевої інфраструктури підприємства ТОВ “Партнер” було визначено перелік можливих загроз.

Найбільш пріоритетні загрози виведені в таблиці **Додаток 2**.

Як видно з наведеної таблиці, мережева інфраструктура підприємства має багато можливих критичних точок, які можуть бути атаковані злоумисниками, а саме:

1. VPN Server та VPN Client
2. Центральний маршрутизатор-фаєрвол
3. Сервер терміналів
4. Бази даних
5. Файловий сервер
6. Клієнтські робочі станції
7. Клієнтська пошта
8. Система відеоспостереження (камери та відео сервер)

Для кожного елемента в таблиці наведено найактуальніші можливі загрози. Але варто враховувати і той факт, що це не всі можливі загрози їх з часом може бути набагато більше, так як постійно з'являються нові загрози.

Для дослідження теми, та отримання певного результату про стан захищеності мережевої інфраструктури ТОВ “Партнер” я провів повне сканування системи, як зовні, так із середини. Для отримання результатів про стан інфраструктури було використано як фізичний огляд інфраструктури, так і спеціальні інструменти для пінтестингу, а саме: Сканування інфраструктури підприємства проводилось на ОС **Kali Linux**, за допомогою таких інструментів:

1. **Онлайн сканер перевірки відкритих портів.**
2. **Metasploit Framework** - інструмент, що надає інформацію про вразливості системи і допомагає у тестах на проникнення та розробці IDS.
3. **NMAP** - безкоштовне відкрите програмне забезпечення для дослідження та аудиту безпеки мереж та виявлення активних мережевих сервісів.
4. **Nessus** - програма для автоматичного пошуку відомих вразливостей у захисті інформаційних систем.

Перший етап - перевірка наявних публічних IP адрес підприємства онлайн сканером, для дослідження реакції системи на сканування, та можливих відкритих портів. Результат онлайн сканування наведений в Додатку 3. Як видно з додатку, сканування не виявило відкритих портів, це пов'язано з тим, що в системі встановлений фаєрвол, який налаштований таким чином, щоб реагувати на такі сканери і блокувати IP адреси з яких йдуть спроби сканування. Також варто зазначити, що жодних сповіщень про спробу зовнішнього сканування не відбулось, в LOG фаєрвол записи відсутні.

Другий етап - проведення інструментом Metasploit Framework, сканування веб-серверів для визначення їх версії HTTP-протоколу. Це може бути корисно під час аналізу вразливостей веб-сервера або для отримання інформації про його конфігурацію. Результат сканування наведено в Додаток 4. В результаті сканування на деяких хостах мережі було виявлено застарілі версії HTTP протоколу.

Третій етап - сканування зовні та зсередини IP адрес, інструментом NMAP. Цього разу для отримання більш достовірного результату, IP адреса з якої проводиться сканування, була додана в список дозволених адрес, яку фаєрвол не блокує. Результати сканування наведені в Додатку 5-7.

Як видно з Додатку 5, зовнішнє сканування всіх 65532 портів, вказує на доступність з зовні 3 портів:

1. 53/TCP - Порт DNS
2. 443/TCP - Порт HTTPS
3. 50505/TCP - Не зарезервований порт (Може бути назначений, для будь яких сервісів)

Внутрішнє сканування Додатки 6-8 вказує на доступність великої кількості відкритих портів на різних хостах, які потенційно можуть бути використані для атак на інфраструктуру в цілому, або на окремі елементи мережі.

Четвертий етап - аудиту мережевої безпеки включав в себе використання інструменту NESSUS для систематичного аналізу на вразливості.

Сканування було проведено вибірково в межах корпоративної мережі, використовуючи довірену IP-адресу з метою отримання повної інформації щодо стану мережевої інфраструктури. Результати цього сканування деталізовано в **Додатки 9-21**.

На основі отриманих результатів були виявлені вразливості на всіх рівнях інфраструктури **Додаток 9**. Варто зазначити, що при такому скануванні фаєрвол відобразив в LOG тільки спробу з'єднання з VPN Server, **Додаток 10**. Жодних інших записів, чи попереджень фаєрвол не зафіксував.

На термінальних серверах були виявлені критичні вразливості, такі як використання застарілих операційних систем, які припинили своє обслуговування виробником та мають численні точки вразливості. Зокрема, серед найбільш критичних аспектів були виявлені застарілі SSL протоколи версій 2.0 та 3.0, **Додаток 11**, які представляють серйозну загрозу з точки зору безпеки мережі. Ці вразливості вимагають негайного усунення та вдосконалення заходів безпеки для забезпечення стабільності та надійності мережевої інфраструктури підприємства.

Також під час сканування було виявлено вразливості:

Вразливості ОС, SSL, SMB, HTTP, WEB Server, **Додаток 12-13**.

Численні вразливості в налаштуваннях та ПО обладнанні Cisco, **Додаток 14**.

Вразливості SNMP, **Додаток 15**.

Вразливість в Microsoft SQL, **Додаток 16**.

Чисельні вразливості файлового сервера, **Додаток 17**. Більшість з яких мають високий і середній рівень загрози.

2.3 Вибір технологій захисту мережевої інфраструктури.

Для поліпшення захисту мережевої інфраструктури ТОВ "Партнер" рекомендується прийняти цілеспрямовані заходи, спрямовані на запобігання потенційним кіберзагрозам та забезпечення високого рівня безпеки. Ось деякі рекомендації:

1. **Аудит безпеки мережі:** Періодичне проведення аудиту безпеки, щоб виявляти потенційні вразливості в мережевій інфраструктурі. Це допоможе ідентифікувати потенційні загрози та точки вразливості.
2. **Постійне оновлення ПЗ і апаратного забезпечення:** Забезпечити, щоб всі сервери, роутери, робочі станції і програмне забезпечення були оновлені до останніх версій, і регулярно виконувати патчі та оновлення безпеки.
3. **Захистити точки доступу до VPN:** Підвищення безпеки VPN сервера шляхом використання сильних методів аутентифікації, двофакторної аутентифікації та регулярною зміною паролів. Постійно моніторити журнали VPN на предмет аномальної активності.
4. **Сегментація мережі:** Розділити мережу на сегменти та використовувати фаєрволи для контролю трафіку між ними. Це допоможе уникнути поширення атак внутрішньої мережі.

5. **Захист баз даних:** Використовувати сильні паролі для баз даних, обмежити доступ до них за необхідністю та регулярно робити резервні копії даних. Моніторити журнали баз даних на виявлення аномальної активності.
6. **Навчання персоналу:** Проводити регулярні навчання співробітників розпізнавати фішинг та інші види соціально-інженерних атак. Створити політику безпеки і регулярно проводити навчання з безпеки.
7. **Забезпечення фізичної безпеки:** Захист фізичного доступу до обладнання і серверних приміщень, де знаходяться сервери і мережеве обладнання.
8. **Моніторинг і відповідь на інциденти:** Встановити систему моніторингу безпеки, яка буде слідкувати за активністю в мережі та сповіщати про можливі аномалії. Розробити план відповіді на інциденти та навчити персонал реагувати на них.
9. **Резервне копіювання і відновлення:** Регулярно створювати резервні копії даних і перевіряти їх відновлення. Це допоможе відновити роботу в разі кібератаки або втрати даних.
10. **Використання сучасних методів захисту:** Розглянути можливість використання сучасних методів захисту, таких як застосування шифрування, інтелектуальних систем виявлення загроз і аналізу безпеки мережі.

Важливо пам'ятати, що безпека мережі - це постійний процес, і вона вимагає постійного моніторингу та оновлення заходів захисту для захисту від зростаючого спектру кіберзагроз.

РОЗДІЛ 3

ДОСЛІДЖЕННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ ЗАХОДІВ ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ

У цьому розділі проводиться докладний аналіз та оцінка ефективності заходів, що були впроваджені для підвищення рівня кібербезпеки мережевої інфраструктури. Оцінка включає в себе перевірку впроваджених технологій, процедур та політик безпеки. Результати цього аналізу допоможуть визначити, наскільки ефективно заходи підвищення захищеності відповідають реальним загрозам та як їх можна подальше удосконалити для забезпечення надійного захисту мережі та даних підприємства. Для дослідження ефективності захищеності мережевої інфраструктури підприємства, мною були виділені основні типи загроз: Кібератаки: DOS/DDoS-атаки (розподілені атаки з відмовою обслуговування), атаки на вразливості програмного забезпечення і атаки на мережеву інфраструктуру. Кіберзлочинці можуть намагатися отримати несанкціонований доступ до системи, викрасти конфіденційні дані або завдати шкоди мережі, тому цьому типу атак має приділяється велика увага.

Фішинг: Це один з найпоширеніших на даний момент метод атаки, при якому зловмисники намагаються обманути користувачів для отримання конфіденційних інформацій, таких як паролі та дані банківських карток, розрахований суто на довірливих користувачів.

Віруси та шкідливе програмне забезпечення: Віруси, троянці, черв'яки і інше шкідливе програмне забезпечення можуть інфікувати комп'ютери та сервери в мережі, завдавши шкоди або викрадаючи дані.

Використання вразливостей програмного забезпечення: Зловмисники можуть використовувати вразливості в програмному забезпеченні, які не були виправлені або оновлені, для отримання доступу до системи.

Соціальна інженерія: Цей метод полягає в обмані користувачів, або співробітників підприємства, щоб вони розкрили конфіденційну інформацію або виконали небезпечні дії. Цей метод схожий на фішинг, єдина відмінність в тому що соціальна інженерія має більш широкий спектр впливу і може мати довготривалу дію.

Витік даних: Витік конфіденційної інформації може стати причиною серйозної шкоди для підприємства, особливо якщо ця інформація потрапить до несанкціонованих осіб.

3.1 Оцінка ефективності вибраних методів та технологій протидії кібератакам на мережеву інфраструктуру підприємства

Для перевірки на вразливість вищезазначених елементів мережевої інфраструктури, використані різні інструменти та методи. Нижче наведено загальний перелік інструментів і методів, які були використані для цього:

Центральний маршрутизатор-фаєрвол:

Сканування вразливостей: Використовувались сканери вразливостей:

Nmap, Онлайн сканери відкритих портів, Nessus, для пошуку вразливостей в конфігурації маршрутизатора та фаєрволу.

Аналіз журналів: Перевірялись журнали подій маршрутизатора та фаєрволу на предмет фіксації атак та ненормальної активності.

Сервер терміналів:

Сканування вразливостей: Використовувались ті самі сканери вразливостей для перевірки конфігурації сервера терміналів.

Аналіз журналів доступу: Перевірялись журнали доступу до сервера терміналів на незвичайну активність та невдалих спроби вторгнення, а також реакцію на перебір логінів і паролів доступу облікових записів.

Бази даних:

Тестування SQL-ін'єкцій: Використовуйте інструменти, такі як SQLMap, для тестування на SQL-ін'єкції та ідентифікації можливих вразливостей.

Аналіз даних доступу: Перевірте права доступу до баз даних та правила фільтрації.

Перевірка можливості відновлення Баз після пошкодження.

Файловий сервер:

Сканування вразливостей: Використовуйте сканери для перевірки відкритих портів сервера та можливих вразливостей.

Аналіз прав доступу: Перевірте права доступу до файлів та директорій на сервері.

Клієнтські робочі станції:

Сканування вразливостей: Перевірялась конфігурація ПК користувачів, а також наявність зловмисного та піратського ПЗ.

Клієнтська пошта:

Фішинг атаки: Відправлялись фішингові повідомлення користувачам та перевірялось, як вони реагують на них.

Система відеоспостереження (камери та відео сервер):

Сканування вразливостей мережі камер і сервера: Використовуйте сканери для перевірки вразливостей мережі відеоспостереження.

Злом відеопотоку: Спробуйте зламати або перехопити відеопотік для перевірки безпеки передачі даних.

3.2 Рекомендації щодо поліпшення захисту мережевої інфраструктури підприємства ТОВ “Партнер”

Захист інфраструктури підприємства як правило включає в себе різні технології та методи для забезпечення безпеки різних компонентів мережевої інфраструктури, включаючи VPN сервер і VPN клієнт, центральний маршрутизатор-фаєрвол, сервер терміналів, бази даних, файловий сервер, клієнтські робочі станції, клієнтську пошту та систему

відеоспостереження. Наступним кроком я опишу загальні заходи забезпечення безпеки для кожного з цих компонентів, беручи до уваги дані, які я отримав в попередньому розділі, під час сканування системи на вразливість:

VPN Server та VPN Client:

Використання сильного шифрування: Встановлення VPN-з'єднань з використанням сильного шифрування, такого як AES-256, для захисту даних під час передачі через мережу.

Короткі відомості про шифрування AES-256 (Advanced Encryption Standard 256-bit) вважається дуже надійним і потужним шифруванням. AES був прийнятий у 2001 році як стандарт шифрування федерального уряду США і був розроблений як заміна застарілого стандарту DES (Data Encryption Standard).

Основні характеристики надійності AES-256 включають:

Ключова довжина: AES-256 використовує 256-бітний ключ, що робить його дуже складним для розшифрування шляхом перебору всіх можливих комбінацій ключів. Кількість можливих ключів у цьому режимі шифрування дуже велика, що робить атаки "перебором" не практичними.

Використання аутентифікації: Вимагати аутентифікацію користувачів, таку як ім'я користувача і пароль, або використання двофакторної аутентифікації для додаткового захисту.

Автоматичне відключення: Встановлення правил автоматичного відключення на VPN сервері для запобігання несанкціонованому доступу.

Оновлення програмного забезпечення: Постійно оновлювати програмне забезпечення VPN сервера та клієнта для усунення відомих вразливостей.

Центральний Маршрутизатор-Фаєрвол:

Фільтрація трафіку: Встановлення правил фільтрації трафіку для блокування несанкціонованих з'єднань та захисту мережі від зовнішніх загроз, а також використання списків доступу. Також виходячи з

попередніх даних, важливо налаштувати запис LOG, які дадуть адміністратору мережі чи фахівцю з кібербезпеки більше даних і дозволять не пропустити важливі інциденти в системі.

Регулярні оновлення: Постійно оновлювати програмне та апаратне забезпечення маршрутизатора-фаєрвола для захисту від нових загроз.

Резервне копіювання конфігурації: Копіювання потенційно може зменшити час розгортання нового обладнання в разі виходу з ладу наявного, або допомогти швидко повернути в стрій наявне обладнання у разі його зламу.

Сервери Терміналів:

Оновлення ОС: Постійне оновлення ОС допоможе уникнути наявності критичних вразливостей, наприклад таких які були виявлені в попередньому розділі на термінальних серверах.

Встановлення прав доступу: Обмеження прав доступу користувачів до сервера терміналів на рівні файлів і даних.

Моніторинг активності: Критично важливий крок, ведення журналів активності користувачів на сервері терміналів для виявлення можливих порушень безпеки.

Бази Даних:

Використання рівнів доступу: Встановлення різних рівнів доступу до баз даних для забезпечення доступу лише для авторизованих користувачів.

Шифрування даних: Шифрування даних у базах даних для запобігання несанкціонованого доступу до них.

Файловий Сервер:

Оновлення ОС: Постійне оновлення ОС допоможе уникнути наявності критичних вразливостей, наприклад таких які були виявлені при скануванні системи в попередньому розділі.

Авторизація та аутентифікація: Вимагати авторизацію та аутентифікацію користувачів перед наданням доступу до файлів та ресурсів на сервері.

Регулярні резервні копії: Робити регулярні резервні копії файлів для відновлення даних у випадку втрати чи пошкодження.

Клієнтські Робочі Станції:

Антивірусне програмне забезпечення: Встановлення та оновлення антивірусного програмного забезпечення на всіх робочих станціях для виявлення та блокування вірусів та шкідливих програм.

Паролі та обмеження доступу: Вимагати складних паролів та встановлення обмежень доступу користувачів до критичних ресурсів. Робота користувачів під обліковими записами без Адміністраторських прав, дозволить уникнути небажаних наслідків у разі відкриття, або скачування зловмисних файлів.

Клієнтська Пошта:

Фільтрація спаму: Використовувати фільтри спаму та антивірусне сканування для захисту від шкідливого вмісту в електронних листах.

Шифрування електронної пошти: Використовувати шифрування для захисту вмісту електронних листів під час передачі.

Система Відеоспостереження:

Забезпечення фізичної безпеки: Розміщення відео серверів в захищеному приміщенні з обмеженим доступом, для запобігання несанкціонованому доступу до обладнання, а також встановлення камер відеоспостереження в тяжко доступних місцях.

Підсумовуючи викладене вище, можна констатувати, що надзвичайно критичним для всіх компонентів інфраструктури підприємства є постійний моніторинг та актуалізація заходів забезпечення безпеки з метою захисту системи від потенційних загроз і кібератак. Важливим аспектом нормального функціонування системи є кваліфікований персонал, наявність складених та затверджених алгоритмів дій у випадку

виникнення аварійних ситуацій, а також постійний моніторинг і актуалізація всіх компонентів інфраструктури підприємства.

Виконання усіх вищезазначених рекомендацій дозволить з великою впевненістю зазначити, що ризик несанкціонованого доступу чи впливу злоумисників на мережеву інфраструктуру підприємства, буде зведений до прийняттого мінімуму. Важливо враховувати, що абсолютно безпечних систем у сучасному світі не існує, і тому наголошується на постійній увазі до питань кібербезпеки та актуальності заходів захисту.

3.3 Рекомендації щодо подальшого розвитку мережевої інфраструктури підприємства ТОВ “Партнер”.

Для подальшого розвитку мережевої інфраструктури ТОВ "Партнер" можна розглянути наступні рекомендації:

Модернізація обладнання та програмного забезпечення:

Постійна перевірка стану і відповідності обладнання сучасним стандартам.

Розглянути можливість оновлення серверів, комутаторів, маршрутизаторів та іншого мережевого обладнання, до рівня який може забезпечити захист від сучасних загроз.

Оновлення програмного забезпечення, включаючи операційні системи, антивірусні програми, фаєрволи та інші безпекові рішення.

Забезпечення високої доступності:

Розглянути можливість впровадження дублювання (резервування) мережевих елементів та даних для забезпечення високої доступності системи.

Використовувати методи балансування навантаження для розподілу трафіку між серверами та забезпечення надійності.

Збільшення безпеки:

Посилювати заходи забезпечення інформації, включаючи впровадження двофакторної аутентифікації, шифрування даних в спокійному та транзитному стані, а також аудит безпеки.

Постійно вдосконалювати політику безпеки, проводити навчання співробітників щодо правил та процедур безпеки.

Запаси та резервне копіювання:

Забезпечити належні запаси запчастин та обладнання для можливості швидкого відновлення у разі відмови.

Регулярно створювати резервні копії даних та перевіряйте процедури відновлення для захисту від можливих втрат даних, а також дублювати резервні копії на декілька окремих носіїв.

Моніторинг та аналіз мережі:

Впровадити систему моніторингу мережі та безпеки для вчасного виявлення проблем та інцидентів.

Аналізувати дані моніторингу, та LOG файлів, для виявлення підозрілої активності та оптимізації ресурсів.

Розширення мережі:

Розглянути можливість розширення мережі для підтримки нових бізнес-процесів та збільшення кількості користувачів.

Планувати мережу так, щоб вона могла легко розширюватися у майбутньому.

Віртуалізація та хмарні рішення:

Розглянути можливість віртуалізації серверів та додатків для ефективного використання ресурсів та зменшення витрат.

Вивчити можливості використання хмарних послуг для забезпечення гнучкості та масштабованості.

Навчання та розвиток персоналу:

Забезпечити навчання та розвиток персоналу, щоб вони мали навички та знання для роботи з новими технологіями та методами безпеки, а також вміли розпізнавати як мінімум базові загрози, такі як фішинг.

Впровадження політик та стандартів:

Розробити та впровадити політики та стандарти щодо безпеки, використання ресурсів та інших аспектів мережевої інфраструктури.

Регулярна перевірка та оцінка:

Проводити регулярні перевірки та оцінки стану мережевої інфраструктури для виявлення слабких місць та можливостей покращення.

Ці рекомендації можуть слугувати основою для подальшого розвитку мережевої інфраструктури ТОВ "Партнер" і допомогти покращити безпеку, доступність та ефективність мережевої інфраструктури підприємства.

ВИСНОВКИ

У цій дипломній роботі, я, як автор даного дослідження, вивчав і аналізував різноманітні методи та технології протидії кібератакам на мережеву інфраструктуру підприємства на конкретному прикладі ТОВ "Партнер". Використовуючи особистий досвід, наукові методи та підходи, я досліджував актуальні проблеми кібербезпеки та виявив найбільш оптимальні шляхи захисту.

Науковий аналіз заходів забезпечення безпеки мережевої інфраструктури підприємства показав, що існує багато перспективних технологій та методів, які можуть ефективно захищати інфраструктуру від загроз, але в більшості випадків, все це не є ефективним, по причині низької пріоритетності та нестачі фінансових ресурсів у підприємства. Великою проблемою для бізнеса є ігнорування заходів з навчання персоналу, що часто призводить до ризиків пов'язаних з втратою репутації чи фінансів. Ретельний аналіз та порівняння методів та технологій захисту мережевої інфраструктури, дозволяють підприємствам обирати найкращі рішення для своєї конкретної ситуації.

Дослідження також показало, що методи виявлення та аналізу кіберзагроз вимагають постійного вдосконалення та використання сучасних аналітичних інструментів для вчасного виявлення аномалій та потенційних загроз, а також постійного підвищення професійної кваліфікації спеціалістів з кібербезпеки, мережевих інженерів, та адміністраторів мереж.

Аналіз конкретного об'єкта дослідження, а саме мережевої інфраструктури ТОВ "Партнер", дозволив мені зрозуміти специфічні виклики та вразливості цього підприємства, що є важливим аспектом для вирішення проблем кібербезпеки на практиці. Як висновок, враховуючи свій особистий досвід, та певні відомості отримані в ході дослідження даної теми, можу з впевненістю сказати, що більшість подібних підприємств мають такі ж проблеми.

За допомогою наукового підходу були обрані та рекомендовані конкретні технології та протоколи захисту, які можуть допомогти підприємству підвищити свій рівень кібербезпеки., щоб в подальшому зменшити ризики пов'язані з втратою інформації та фінансовими втратами.

В цілому, ця наукова робота надає важливий внесок у розуміння і практичне застосування методів та технологій протидії кібератакам на мережеву інфраструктуру підприємства. Вона на практичному прикладі, підкріпленому теоретичними відомостями демонструє, що кібербезпека - це постійний процес, який вимагає наукового підґрунтя та постійного вдосконалення, щоб забезпечити захист у світі, де кіберзагрози постійно еволюціонують та стають складнішими.

Дослідження даної теми та його значення для підприємств надзвичайно важливі у сучасному цифровому віці. Ось кілька аспектів, які підкреслюють важливість цього дослідження:

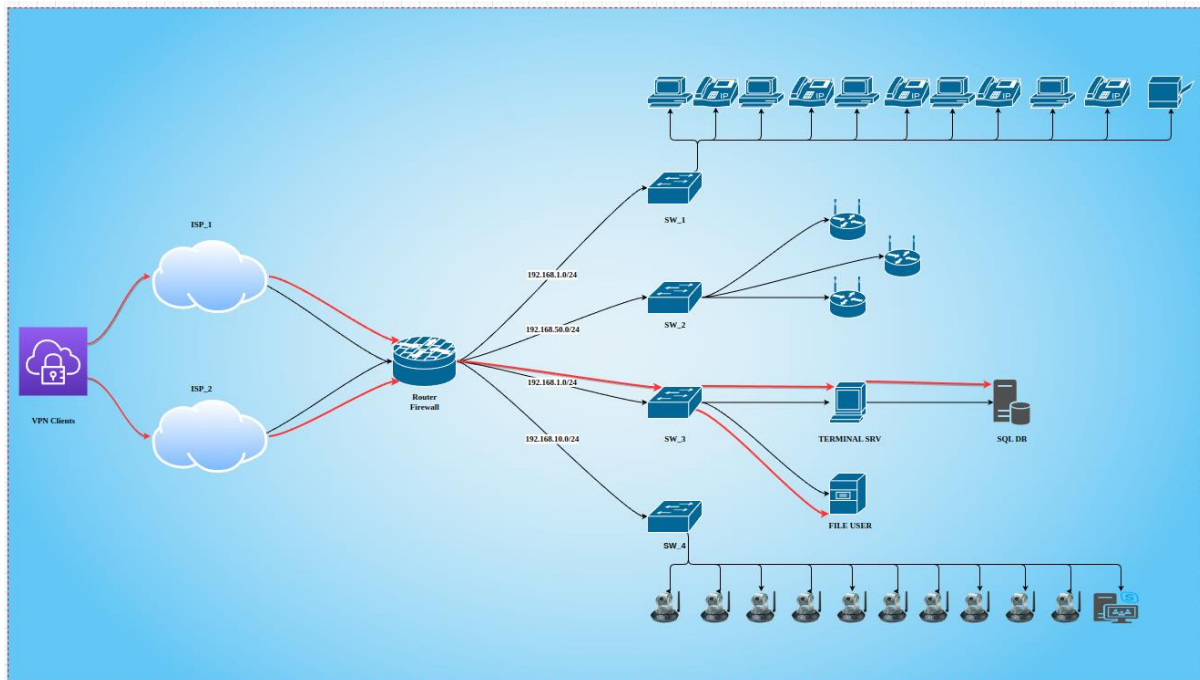
1. Захист конфіденційності даних: Захист даних клієнтів, партнерів та власної конфіденційної інформації є пріоритетною задачею для будь-якого підприємства. Дослідження цієї теми допомагає виявити потенційні слабкі місця у системах та розробити стратегії для їх захисту.
2. Запобігання фінансовим втратам: Кібератаки можуть призвести до серйозних фінансових збитків, включаючи втрату коштів та репутації. Дослідження може допомогти підприємствам визначити оптимальні інвестиції в кібербезпеку, що мінімізуватимуть ризики.
3. Збереження бізнесу: Кібератаки можуть призвести до припинення діяльності підприємства на певний час. Розробка ефективних заходів забезпечення кібербезпеки може допомогти зберегти бізнес та підтримати його стабільність.
4. Довіра клієнтів: Захист даних клієнтів і їхньої особистої інформації є ключовим для збереження довіри клієнтів. Втрата цієї довіри може сильно вплинути на репутацію та прибуток підприємства.

5. Відповідність законодавству: Законодавство про захист даних надає велике значення вимогам до кібербезпеки. Дослідження цієї теми допомагає підприємствам бути відповідними законам та нормативам, запобігаючи можливим штрафам та санкціям.

Усі ці аспекти підкреслюють необхідність інвестування у кібербезпеку та проведення досліджень у цій галузі. Підприємства, які вдосконалюють свої заходи забезпечення кібербезпеки, не лише захищають свою інформацію та фінанси, але і підтверджують свою відповідальність перед клієнтами та партнерами, зберігаючи своє місце на ринку та зміцнюючи свою позицію в глобальному бізнес-середовищі.

ДОДАТКИ

Додаток 1



Додаток 2

VPN	Злам безпеки: Неуспішна реалізація протоколів шифрування може призвести до проникнення зловмисників у VPN-з'єднання. Втрояння в мережу: Атаки типу "Man-in-the-Middle" або "DDoS" можуть призвести до обмеження доступу до VPN або його компрометації.
Router	Перехоплення трафіку: Атаки "Man-in-the-Middle" можуть використовувати роутер для перехоплення і зловмисного аналізу трафіку. Вразливості маршрутизатора: Наявність вразливостей у програмному забезпеченні роутера може дозволити зловмисникам здійснити віддалене вторгнення.
Terminal Server	Брутфорс атаки: Зловмисники можуть спробувати зламати пароль, використовуючи автоматизовані методи. Вразливості ПЗ: Наявність вразливостей у операційній системі або програмному забезпеченні термінального сервера може призвести до несанкціонованого доступу.
SQL DB	SQL Injection: Зловмисники можуть ввести шкідливі SQL-запити через вразливість в програмах, які взаємодіють з базою даних. Необхідність оновлень: Не оновлений ПЗ бази даних може залишити вразливості, які можуть бути зловмисно використані.
File Server	Несанкціонований доступ: Відсутність належних контролів доступу може дозволити зловмисникам отримати доступ до конфіденційної інформації. Ransomware: Шифрування файлів на сервері, з метою викупу за їх розшифрування.
PC Client	Віруси та шкідливе ПЗ: Клієнтські комп'ютери можуть бути заражені вірусами, троянами та іншим шкідливим ПЗ. Соціальний інжиніринг: Зловмисники можуть спробувати обдурити користувачів та отримати від них конфіденційну інформацію.
CCTV	Несанкціонований доступ до відео: Вразливості у системі відеоспостереження можуть призвести до незаконного перегляду або запису відео. Злам паролів: Недостатньо складні паролі можуть бути зламані зловмисниками.
Client mail	Фішинг: Зловмисники можуть відправляти фішингові листи, щоб отримати конфіденційну інформацію від клієнтів. Злам аккаунтів: Вразливості у системі пошти можуть призвести до компрометації електронних адрес і листів.

Сканер портів

Він показує, які порти відкриті на вашому комп'ютері або сервері, і за що вони відповідають. Перевірка відбувається через сканер nmap і відображає, наскільки відкритий ваш пристрій для зовнішнього світу.

Введіть IP-адресу або домен

193.107.73.185

Вставити мою IP-адресу

Введіть IP-адресу або домен

Популярні порти

Почати сканування

Результати перевірки

Nmap done: 1 IP address (1 host up) scanned in 201.29 seconds

Якщо результат «Host seems down», значить мережевий екран або роутер IP-адреси, що перевіряється, блокує пінг.

```
msf6 auxiliary(scanner/http/http_version) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf6 auxiliary(scanner/http/http_version) > use auxiliary/scanner/http/http_version
msf6 auxiliary(scanner/http/http_version) > run
```

[+]	192.168.1.2:80	mini_httpd/1.19	19dec2003
[+]	192.168.1.3:80	nginx	
[+]	192.168.1.4:80	Microsoft-HTTPAPI/2.0	
[+]	192.168.1.5:80	lighttpd	
[+]	192.168.1.6:80	mini_httpd/1.19	19dec2003
[+]	192.168.1.7:80	mini_httpd/1.30	260ct2018
[+]	192.168.1.10:80	mini_httpd/1.19	19dec2003
[+]	192.168.1.14:80	mini_httpd/1.30	260ct2018
[+]	192.168.1.20:80		
[+]	192.168.1.24:80	mini_httpd/1.30	260ct2018
[+]	192.168.1.25:80	Apache/2.4.6 (CentOS) (403-Forbidden)	
[*]	Scanned 26 of 256 hosts (10% complete)		
[+]	192.168.1.28:80	mini_httpd/1.19	19dec2003
[+]	192.168.1.48:80	Apache (302-https://192.168.1.48:8081/)	
[*]	Scanned 52 of 256 hosts (20% complete)		
[*]	Scanned 77 of 256 hosts (30% complete)		
[+]	192.168.1.97:80	Apache/2.2.15 (CentOS) (Powered by PHP/5.3.3)	
[+]	192.168.1.102:80	mini_httpd/1.19	19dec2003
[*]	Scanned 103 of 256 hosts (40% complete)		
[+]	192.168.1.108:80	mini_httpd/1.19	19dec2003
[+]	192.168.1.112:80	mini_httpd/1.19	19dec2003
[+]	192.168.1.114:80	mini_httpd/1.19	19dec2003
[+]	192.168.1.115:80	mini_httpd/1.19	19dec2003
[+]	192.168.1.119:80	mini_httpd/1.19	19dec2003
[+]	192.168.1.122:80	mini_httpd/1.19	19dec2003
[+]	192.168.1.126:80	Multimedia Phone	
[*]	Scanned 128 of 256 hosts (50% complete)		
[*]	Scanned 154 of 256 hosts (60% complete)		
[*]	Scanned 180 of 256 hosts (70% complete)		
[*]	Scanned 205 of 256 hosts (80% complete)		
[*]	Scanned 231 of 256 hosts (90% complete)		
[*]	Scanned 256 of 256 hosts (100% complete)		
[*]	Auxiliary module execution completed		

```
msf6 auxiliary(scanner/http/http_version) >
```

Додаток 5

```
(cybercat@CyberCat)-[~]
$ nmap -p- 193.107.73.185
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-14 13:00 EET
Nmap scan report for host73185.net-city.net (193.107.73.185)
Host is up (0.0021s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE
53/tcp    open  domain
443/tcp   open  https
50505/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 11.10 seconds

(cybercat@CyberCat)-[~]
$
```

Додаток 6

```
(cybercat@CyberCat)-[~]
$ nmap -p- 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-14 12:49 EET
Nmap scan report for 192.168.1.1
Host is up (0.0034s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE
53/tcp    open  domain
443/tcp   open  https
50505/tcp open  unknown

Nmap scan report for 192.168.1.2
Host is up (0.0015s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap scan report for 192.168.1.3
Host is up (0.00032s latency).
Not shown: 65525 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
515/tcp   open  printer
631/tcp   open  ipp
3910/tcp  open  prnrequest
3911/tcp  open  prnstatus
5355/tcp  open  llmnr
8080/tcp  open  http-proxy
9100/tcp  open  jetdirect
53048/tcp open  unknown

Nmap scan report for 192.168.1.4
Host is up (0.00059s latency).
Not shown: 65513 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2382/tcp  open  ms-olap3
3050/tcp  open  gds_db
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdaapi
5985/tcp  open  wsman
9080/tcp  open  glrpc
9996/tcp  open  palace-5
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49162/tcp open  unknown
49163/tcp open  unknown
49165/tcp open  unknown
63166/tcp open  unknown

Stats: 0:02:30 elapsed; 233 hosts completed (27 up), 23 undergoing Connect Scan
Connect Scan Timing: About 23.78% done; ETC: 12:56 (0:04:16 remaining)
```

Додаток 7

Stats: 0:06:25 elapsed; 233 hosts completed (27 up), 23 undergoing Connect Scan
Connect Scan Timing: About 89.20% done; ETC: 12:56 (0:00:38 remaining)

Nmap scan report for 192.168.1.5

Host is up (0.00041s latency).

Not shown: 65529 closed tcp ports (conn-refused)

PORT STATE SERVICE

80/tcp open http

199/tcp open smux

443/tcp open https

623/tcp open oob-ws-http

9666/tcp open zoomcp

9999/tcp open abyss

Nmap scan report for 192.168.1.6

Host is up (0.00097s latency).

Not shown: 65534 closed tcp ports (conn-refused)

PORT STATE SERVICE

80/tcp open http

Nmap scan report for 192.168.1.7

Host is up (0.00039s latency).

Not shown: 65534 closed tcp ports (conn-refused)

PORT STATE SERVICE

80/tcp open http

Nmap scan report for 192.168.1.9

Host is up (0.0012s latency).

Not shown: 65534 closed tcp ports (conn-refused)

PORT STATE SERVICE

22/tcp open ssh

Nmap scan report for 192.168.1.10

Host is up (0.00073s latency).

Not shown: 65534 closed tcp ports (conn-refused)

PORT STATE SERVICE

80/tcp open http

Nmap scan report for 192.168.1.14

Host is up (0.00029s latency).

Not shown: 65533 closed tcp ports (conn-refused)

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

Nmap scan report for 192.168.1.17

Host is up (0.0020s latency).

Not shown: 65531 closed tcp ports (conn-refused)

PORT STATE SERVICE

22/tcp open ssh

23/tcp open telnet

443/tcp open https

4786/tcp open smart-install

Nmap scan report for 192.168.1.18

Host is up (0.0064s latency).

Not shown: 65533 closed tcp ports (conn-refused)

PORT STATE SERVICE

22/tcp open ssh

53/tcp open domain

Nmap scan report for 192.168.1.20

Host is up (0.00018s latency).

Not shown: 65530 closed tcp ports (conn-refused)

Додаток 8

Nmap scan report for 192.168.1.97

Host is up (0.00019s latency).

Not shown: 65529 filtered tcp ports (no-response)

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

3306/tcp open mysql

5038/tcp open unknown

8080/tcp closed http-proxy

10062/tcp open unknown

Nmap scan report for 192.168.1.102

Host is up (0.00074s latency).

Not shown: 65534 closed tcp ports (conn-refused)

PORT STATE SERVICE

80/tcp open http

Nmap scan report for 192.168.1.108

Host is up (0.00070s latency).

Not shown: 65534 closed tcp ports (conn-refused)

PORT STATE SERVICE

80/tcp open http

Nmap scan report for 192.168.1.112

Host is up (0.00073s latency).

Not shown: 65534 closed tcp ports (conn-refused)

PORT STATE SERVICE

80/tcp open http

Nmap scan report for 192.168.1.114

Host is up (0.00084s latency).

Not shown: 65534 closed tcp ports (conn-refused)

PORT STATE SERVICE

80/tcp open http

Nmap scan report for 192.168.1.115

Host is up (0.00070s latency).

Not shown: 65534 closed tcp ports (conn-refused)

PORT STATE SERVICE

80/tcp open http

Nmap scan report for 192.168.1.119

Host is up (0.0019s latency).

Not shown: 65534 closed tcp ports (conn-refused)

PORT STATE SERVICE

80/tcp open http

Nmap scan report for 192.168.1.122

Host is up (0.00079s latency).

Not shown: 65534 closed tcp ports (conn-refused)

PORT STATE SERVICE

80/tcp open http

Nmap scan report for 192.168.1.126

Host is up (0.00036s latency).

Not shown: 65533 closed tcp ports (conn-refused)

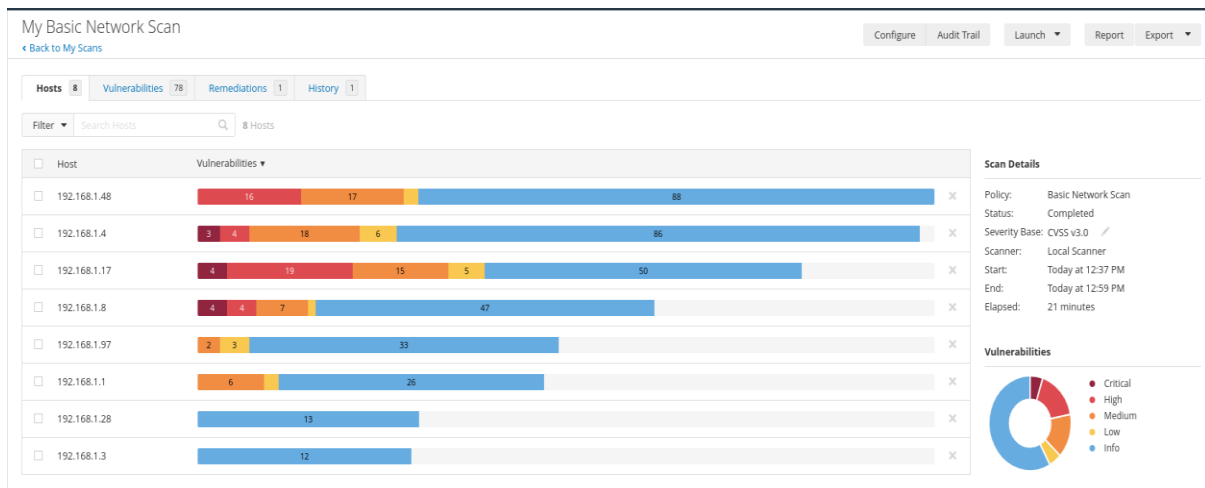
PORT STATE SERVICE

23/tcp open telnet

80/tcp open http

Nmap done: 256 IP addresses (27 hosts up) scanned in 479.95 seconds

Додаток 9



Додаток 10

290	Nov/16/2023 12:39:45	memory	ipsec, error	phase1 negotiation failed due to time up 192.168.1.1[500]<=>192.168.1.47[500] 7669454675387976:de...
291	Nov/16/2023 12:40:34	memory	ipsec, info	respond new phase 1 (Identity Protection): 192.168.1.1[500]<=>192.168.1.47[38693]
292	Nov/16/2023 12:40:34	memory	ipsec, error	192.168.1.47 failed to get valid proposal.
293	Nov/16/2023 12:40:34	memory	ipsec, error	192.168.1.47 failed to pre-process ph1 packet (side: 1, status 1).
294	Nov/16/2023 12:40:34	memory	ipsec, error	192.168.1.47 phase1 negotiation failed.
295	Nov/16/2023 12:40:36	memory	ipsec, info	respond new phase 1 (Identity Protection): 192.168.1.1[500]<=>192.168.1.47[38693]
296	Nov/16/2023 12:40:36	memory	ipsec, error	192.168.1.47 failed to get valid proposal.
297	Nov/16/2023 12:40:36	memory	ipsec, error	192.168.1.47 failed to pre-process ph1 packet (side: 1, status 1).
298	Nov/16/2023 12:40:36	memory	ipsec, error	192.168.1.47 phase1 negotiation failed.
299	Nov/16/2023 12:40:38	memory	ipsec, info	respond new phase 1 (Identity Protection): 192.168.1.1[500]<=>192.168.1.47[38693]
300	Nov/16/2023 12:40:38	memory	ipsec, error	192.168.1.47 failed to get valid proposal.
301	Nov/16/2023 12:40:38	memory	ipsec, error	192.168.1.47 failed to pre-process ph1 packet (side: 1, status 1).
302	Nov/16/2023 12:40:38	memory	ipsec, error	192.168.1.47 phase1 negotiation failed.

Додаток 11

My Basic Network Scan / Plugin #20007

Configure Audit Trail Launch Report Export

Hosts 8 Vulnerabilities 78 Remediations 1 History 1

CRITICAL SSL Version 2 and 3 Protocol Detection

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.

See Also

<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>
<http://www.nessus.org/u?b06c7e95>
<http://www.nessus.org/u?7247c4540>
<https://www.openssl.org/~bodo/ssl-poodle.pdf>
<http://www.nessus.org/u?5d15ba70>
<https://www.imperialviolet.org/2014/10/14/poodle.html>
<https://tools.ietf.org/html/rfc7507>
<https://tools.ietf.org/html/rfc7568>

Plugin Details

Severity: Critical
ID: 20007
Version: 1.34
Type: remote
Family: Service detection
Published: October 12, 2005
Modified: April 4, 2022

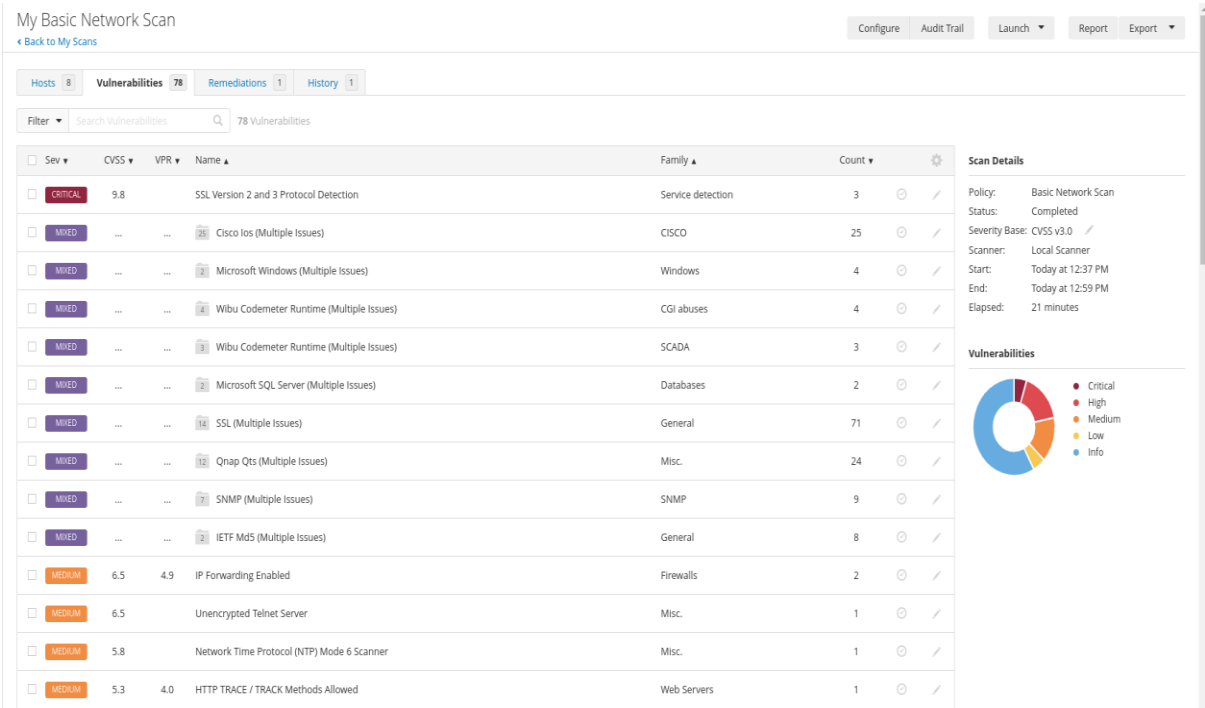
Risk Information

Risk Factor: Critical
CVSS v3.0 Base Score 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

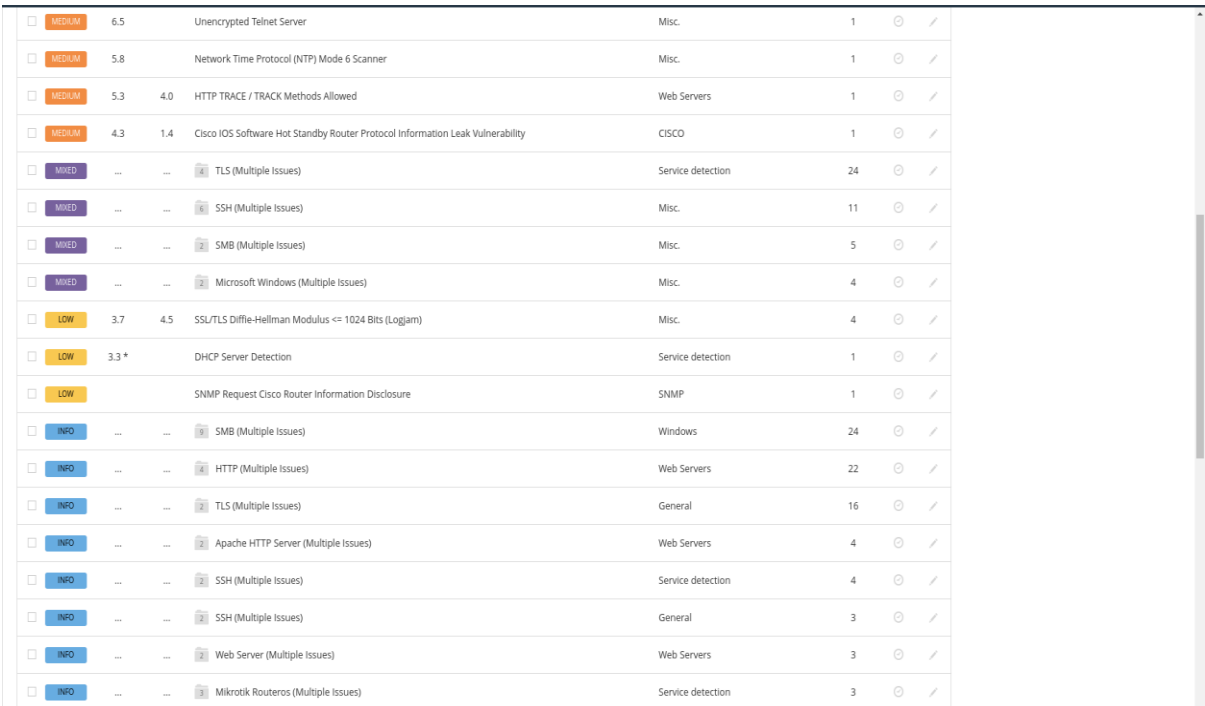
Vulnerability Information

In the news: true

Додаток 12



Додаток 13



Додаток 14

My Basic Network Scan / Cisco Ios (Multiple Issues)

[Back to Vulnerabilities](#)

Configure

Audit Trail

Launch

Report

Export

Hosts8

Vulnerabilities78

Remediations1

History1

Search Vulnerabilities

25 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count		
CRITICAL	9.8	8.9	Cisco IOS Software Smart Install Remote Code Execution Vulnerability	CISCO	1		
CRITICAL	9.8	7.4	Cisco IOS Cluster Management Protocol Telnet Option Handling RCE (cisco-sa-20170317-cmp)	CISCO	1		
CRITICAL	9.8	7.4	Cisco IOS Software DHCP Remote Code Execution Vulnerability	CISCO	1		
HIGH	8.8	7.4	Cisco IOS Software Link Layer Discovery Protocol Buffer Overflow Vulnerabilities (cisco-sa-20180328-lldp)	CISCO	1		
HIGH	8.6	6.0	Cisco IOS DHCP Multiple Vulnerabilities	CISCO	1		
HIGH	8.6	4.4	Cisco IOS EnergyWise DoS (cisco-sa-20170419-energywise)	CISCO	1		
HIGH	8.1	5.9	Cisco IOS Software DNS Forwarder Denial of Service Vulnerability (cisco-sa-20160928-dns)	CISCO	1		
HIGH	7.8 *	3.7	Cisco IOS Software Multiple Network Address Translation (NAT) Denial of Service Vulnerabilities (cisco-sa-...	CISCO	1		
HIGH	7.8 *	3.6	Cisco IOS Software RSPV DoS (cisco-sa-20140924-rsvp)	CISCO	1		
HIGH	7.5	6.1	Cisco IOS iKev1 Packet Handling Remote Information Disclosure (cisco-sa-20160916-ikev1) (BENIGNCERTA...	CISCO	1		
HIGH	7.5	5.1	Cisco IOS Software Smart Install DoS (cisco-sa-20180328-smi)	CISCO	1		
HIGH	7.5	4.4	Cisco IOS Smart Install Packet Image List Parameter Handling DoS (cisco-sa-20160323-smi)	CISCO	1		
HIGH	7.5	3.6	Cisco IOS AAA Login DoS (cisco-sa-20160928-aaados)	CISCO	1		
HIGH	7.5	3.6	Cisco IOS L2TP Parsing DoS (cisco-sa-20170322-l2tp)	CISCO	1		
HIGH	7.5	3.6	Cisco IOS Smart Install Memory Leak (cisco-sa-20160928-smi)	CISCO	1		

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:37 PM
End: Today at 12:59 PM
Elapsed: 21 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

Додаток 15

My Basic Network Scan / SNMP (Multiple Issues)

[Back to Vulnerabilities](#)

Configure

Audit Trail

Launch

Report

Export

Hosts8

Vulnerabilities78

Remediations1

History1

Search Vulnerabilities

7 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count		
HIGH	7.5 *	3.4	SNMP Agent Default Community Name (public)	SNMP	1		
MEDIUM	5.0 *	3.6	SNMP 'GETBULK' Reflection DDoS	SNMP	1		
INFO			SNMP Protocol Version Detection	SNMP	2		
INFO			SNMP Server Detection	SNMP	2		
INFO			SNMP Query System Information Disclosure	SNMP	1		
INFO			SNMP Request Network Interfaces Enumeration	SNMP	1		
INFO			SNMP Supported Protocols Detection	SNMP	1		

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:37 PM
End: Today at 12:59 PM
Elapsed: 21 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

Додаток 16

My Basic Network Scan / Microsoft SQL Server (Multiple Issues)

[Back to Vulnerabilities](#)

Configure

Audit Trail

Launch

Report

Export

Hosts8

Vulnerabilities78

Remediations1

History1

Search Vulnerabilities

2 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count		
CRITICAL	10.0		Microsoft SQL Server Unsupported Version Detection (remote check)	Databases	1		
INFO			Microsoft SQL Server UDP Query Remote Version Disclosure	Databases	1		

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:37 PM
End: Today at 12:59 PM
Elapsed: 21 minutes

Vulnerabilities

Critical

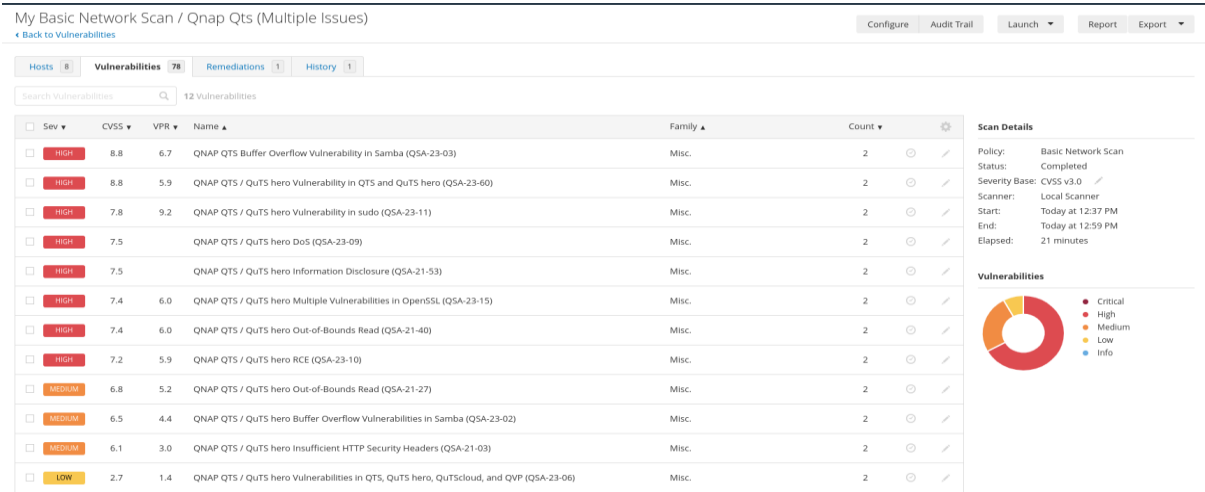
High

Medium

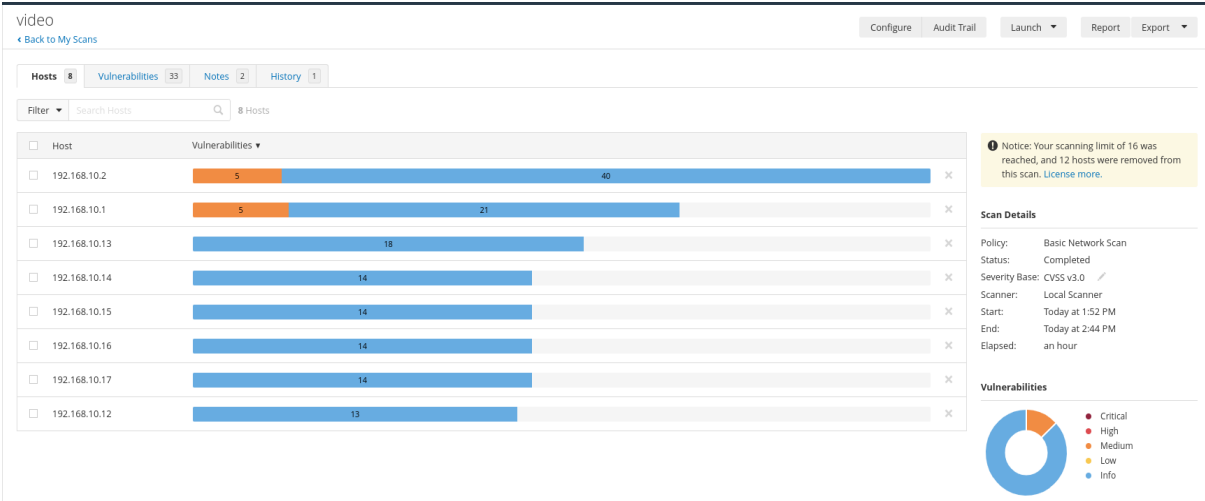
Low

Info

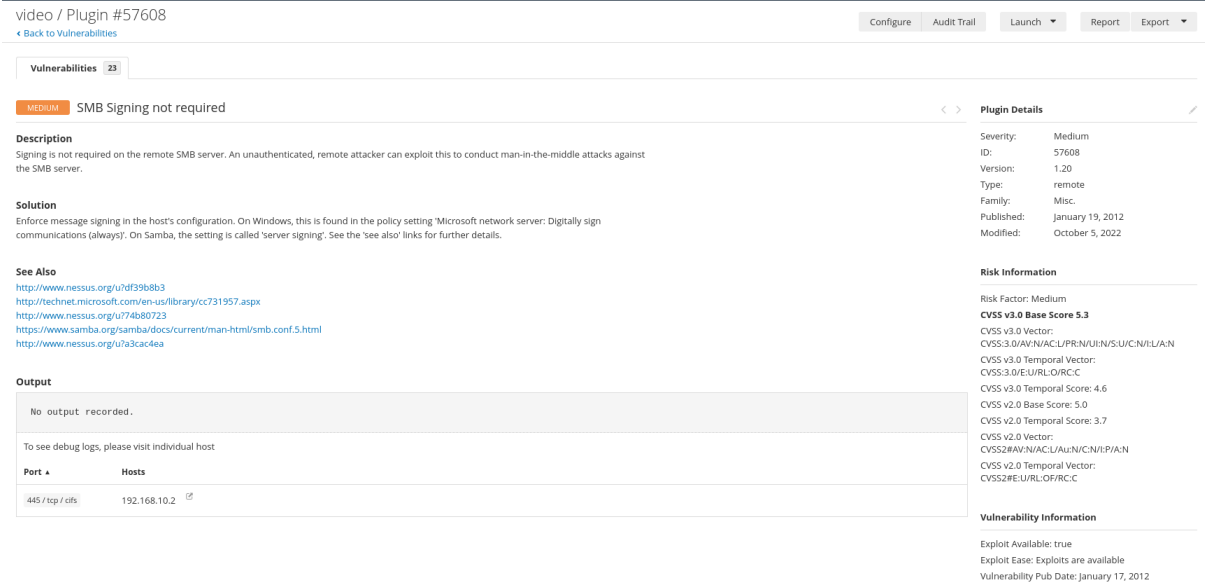
Додаток 17



Додаток 18



Додаток 19



video / 192.168.10.2 / SSL (Multiple Issues)

Configure

Audit Trail

Launch

Report

Export

Vulnerabilities23

Search Vulnerabilities

9 Vulnerabilities

☐	Sev	CVSS	VPR	Name	Family	Count	
☐	MEDIUM	6.5		SSL Certificate Cannot Be Trusted	General	1	
☐	MEDIUM	6.5		SSL Self-Signed Certificate	General	1	
☐	MEDIUM	5.3		SSL Certificate Expiry	General	1	
☐	MEDIUM	5.3		SSL Certificate with Wrong Hostname	General	1	
☐	INFO			SSL Certificate 'commonName' Mismatch	General	1	
☐	INFO			SSL Certificate Information	General	1	
☐	INFO			SSL Cipher Block Chaining Cipher Suites Supported	General	1	
☐	INFO			SSL Cipher Suites Supported	General	1	
☐	INFO			SSL Perfect Forward Secrecy Cipher Suites Supported	General	1	

Notice: Your scanning limit of 16 was reached, and 12 hosts were removed from this scan. [License more.](#)

Scan Details

Policy:Basic Network Scan

Status:Completed

Severity Base:CVSS v3.0

Scanner:Local Scanner

Start:Today at 1:52 PM

End:Today at 2:44 PM

Elapsed:an hour

Vulnerabilities

Critical

High

Medium

Low

Info

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. "Кібербезпека. Інформаційна безпека від А до Я" (автор: Олександр Шарай) - видана в 2017 році.
2. "Кібербезпека в Україні: сучасний стан та перспективи розвитку" (автори: Андрій Костенко, Андрій Палагнюк) - видана в 2018 році.
3. "Кібербезпека в державному управлінні: теорія та практика" (автор: Володимир Олійник) - видана в 2018 році.
4. "Кібербезпека підприємств: протидія кіберзагрозам" (автор Лукаш Л., видавництво "Альфа-книга", 2018).
5. "Кібербезпека для керівників: практичний підхід" (автор Іщенко І., видавництво "К.І.С.", 2020).
6. "Кібербезпека підприємства: захист від кіберзагроз" (автор Горелова І., видавництво "Видавничий дім "Інфра-М", 2021).
7. "Кібербезпека підприємств: методологія та практика" (автор Голуб Д., видавництво "Кніга-Центр", 2019).
8. "Кібербезпека: методи захисту від кіберзагроз" (автор Коваленко В., видавництво "Комп'ютерпрес", 2020).
9. "Кібербезпека в бізнесі: підходи та рекомендації" (автори Лозинський О., Кузьмін В., видавництво "Книгарня "Є", 2019).
10. "Кібербезпека підприємств: організаційний підхід" (автор Старовойтов І., видавництво "Універсум-Про", 2020).