**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ**
**КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ**

# Пояснювальна записка

до бакалаврської роботи
на тему:

**«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ КІНЦЕВИХ ТОЧОК ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА НА БАЗІ РІШЕННЯ NESSUS»**

Виконав студент 4 курсу, групи БСД-42
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Говоруха М. М.
(прізвище та ініціали)
Керівник Марчено В. В.
(прізвище та ініціали)
Рецензент _____
(прізвище та ініціали)
Нормоконтролер _____
(прізвище та ініціали)

КИЇВ – 2023

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ**

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітня програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
"____"_____2023 року

**З А В Д А Н Н Я**
**НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ**

Говорусі Марку Миколайовичу
(прізвище, ім'я, по батькові)

1. Тема бакалаврської роботи: «Дослідження шляхів та розробка рекомендацій щодо управління вразливостями кінцевих точок інформаційної системи підприємства на базі рішення Nessus»
керівник бакалаврської роботи Марченко В. В., ст. викладач
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «24» лютого 2023 року №26.

2. Строк подання студентом бакалаврської роботи 29.05.2023 р.

3. Вихідні дані до бакалаврської роботи
корпоративна інформаційна система;
програмний комплекс менеджменту вразливостей;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз методів забезпечення безпеки кінцевих точок та їх загроз
2. Дослідження шляхів та методів управління вразливостями кінцевих точок
3. Розробка рекомендацій щодо управління вразливостями кінцевих точок ic підприємства на базі рішення nessus

5. Перелік графічного матеріалу
1. Тема бакалаврської роботи.
2. Об’єкт, предмет, мета та наукові завдання дослідження.
3. Результати аналізу методів забезпечення безпеки кінцевих точок та їх загроз
6. Рекомендацій щодо управління вразливостями кінцевих точок іс підприємства на базі рішення nessus.
7. Висновки за результатами роботи.

6. Дата видачі завдання 24.02.2023 р.

## КАЛЕНДАРНИЙ ПЛАН

| № зп | Назва етапів бакалаврської роботи | Строк виконання етапів бакалаврської роботи | Примітка |
|---|---|---|---|
| 1. | Визначення актуальності проблеми менеджменту вразливостей в інформаційних системах | 24.02.2023 р. | |
| 2. | Аналіз наукової та технічної літератури з питань теми бакалаврської роботи. | 28.02.2023 р. | |
| 3. | Аналіз методів та засобів менеджменту вразливостей інформаційних систем підприємства | 26.03.2023 р. | |
| 4. | Розроблення рекомендацій щодо впровадження та використання ПЗ Nessus для менеджменту вразливостей | 13.04.2023 р. | |
| 5. | Оформлення результатів дослідження. | 10.05.2023 р. | |
| 6. | Підготовка доповіді до захисту. | 29.05.2023 р. | |

Студент _____ Говоруха М. М.
(підпис) прізвище та ініціали

Керівник бакалаврської роботи _____ Марченко В. В
(підпис) прізвище та ініціали

# ВІДГУК РЕЦЕНЗЕНТА

на бакалаврську роботу

студента Говорухи Марка Миколайовича
на тему: « Дослідження шляхів та розробка рекомендацій щодо управління вразливостями кінцевих точок інформаційної системи підприємства на базі рішення nessus»

**Актуальність:** З урахуванням бурхливого росту кількості кіберінцидентів та пов'язаних з ними загроз, забезпечення безпеки інформаційних систем набуває все більшої актуальності для підприємств. Ключовим елементом кібербезпеки є управління вразливостями. Вразливості в інформаційних системах можуть створювати шляхи для несанкціонованого доступу та атак, що може призвести до втрати конфіденційності, цілісності та доступності даних. Розуміння вразливостей та ефективне управління ними стає критично важливим фактором у запобіганні кіберінцидентам та пом'якшенні їхніх наслідків. Тому тема бакалаврської роботи є актуальною та своєчасною.

**Позитивні сторони:**

1. Проведено дослідження вразливостей кінцевих точок інформаційної системи на базі рішення Nessus. Результати аналізу дозволили виявити потенційні вразливості та оцінити ризики, що допоможе підприємству знизити загрози кібербезпеки.
2. Досліджено функціональні можливості рішення Nessus та проаналізовано його обмеження. Це дозволить підприємству краще розуміти, як ефективно використовувати цей інструмент для виявлення та управління вразливостями.
3. В роботі розроблені рекомендації щодо управління вразливостями кінцевих точок інформаційної системи підприємства на базі рішення Nessus. Ці рекомендації можуть бути цінним додатком для підприємства, допомагаючи йому забезпечити кращу кібербезпеку та знизити ризики кіберінцидентів.
4. Робота викладена грамотно, послідовно та чітко. Висновки сформульовано ясно і змістовно, а графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить здатність користуватись актуальними джерелами інформації.

**Недоліки:**

1. У бакалаврській роботі було б доцільно провести аналіз можливих умов функціонування рішення Nessus в різних інформаційних системах підприємства. Це дозволило б з'ясувати, як цей інструмент може бути ефективно використаний для виявлення та управління вразливостями в різних середовищах.
2. Бажано було б провести експеримент з застосуванням рішення Nessus на вихідних даних, які відображають конкретні вразливості та кінцеві точки інформаційної системи підприємства. Це дозволило б з'ясувати, наскільки ефективно рішення Nessus виявляє та оцінює вразливості і які рекомендації можуть бути надані для їх управління.

**Висновок:** Враховуючи недоліки, бакалаврська робота заслуговує оцінку **добре**, а студент **Говоруха М. М.** – присвоєння кваліфікації: бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

| | |
|---|---|
| Якість роботи | |
| Виконано на замовлення підприємства | |
| Виконано за тематикою НДР | |
| Виконано з макетом | |
| Виконано з застосуванням ЕОМ та МПТ | √ |
| Має практичну цінність | √ |
| Проект-частина комплексної теми | |

Підпис рецензента (_____)
Підпис засвідчую
Підпис особи, що засвідчує (_____)

# РЕФЕРАТ

Текстова частина бакалаврської роботи: 61 сторінок, 35 рисунків, 3 таблиці, 16 джерел.

*Об'єкт дослідження* - nessus як інструмент управління вразливостями в інформаційних системах.

*Предмет дослідження* - методи та засоби щодо управління вразливостями кінцевих точок інформаційної системи підприємства.

*Мета роботи* - отримання характеристики ефективності програмного забезпечення Nessus для менеджменту вразливостей інформаційних систем. Створення рекомендацій на основі дослідженного матеріалу.

*Методи дослідження* - опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів, проведення експерименту.

Встановлено оптимальні налаштування програмного забезпечення Nessus для проведення менеджменту вразливостей інформаційних систем. Проаналізовано результати сканування на вразливість інформаційних систем. Розкрито важливість використання політики менеджменту вразливостей для інформаційї системи. Розкрито кращі практики та фреймворки для менеджменту вразливостей.

Галузь використання – кібербезпека корпоративних інформаційних систем.

КІБЕРБЕЗПЕКА, МЕНЕДЖМЕНТ ВРАЗЛИВОСТЕЙ, КОРПОРАТИВНА ІНФОРМАЦІЇНА СИСТЕМА, ВІДСЛІДКОВУВАННЯ ТА ВИПРАВЛЕННЯ ВРАЗЛИВОСТЕЙ, АВТОМАТИЗОВАНЕ СКАНУВАННЯ ВРАЗЛИВОСТЕЙ

# ЗМІСТ

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІС – інформаційна система

ПЗ – програмне забезпечення

CVE – Common Vulnerability Exposures

HIPPA – Health Insurance Portability and Accountability Act

PCI DSS – Payment Card Industry Data Security Standard

ISO – International Organization for Standardization

# ВСТУП

Захист корпоративних інформаційних систем має вирішальне значення в цифрову епоху. Управління вразливостями є невід'ємною частиною досягнення цієї мети. Інтерфейс між користувачами і технологіями, кінцеві пристрої є ключовим джерелом доступності інформації, але це також робить їх вразливими до кібератак. В останні роки вразливості кінцевих пристроїв стають все більш поширеними через те, що вони є основним засобом комунікації та обміну інформацією.

Спектр зовнішніх загроз, з якими стикаються ці пристрої, величезний: від вірусів або зловмисного програмного забезпечення, які викрадають конфіденційні дані, до прихованих тактик, таких як фішинг, спам і встановлення шахрайських програм. Управління вразливістю є критично важливим аспектом кібербезпеки, який з року в рік набуває все більшого значення. Потужним інструментом для керування вразливими місцями є мережеве сканування, яке сканує точки вразливості для виявлення дефектів і вразливостей в інфраструктурі та системах. Це служить основою для розробки надійних стратегій управління ризиками та захисту від потенційних атак. Сканування також підвищує ефективність присутніх протоколів безпеки та дає можливість удосконалити та покращити заходи захисту.

*Об'єкт дослідження* - nessus як інструмент управління вразливостями в інформаційних системах.

*Предмет дослідження* - методи та засоби щодо управління вразливостями кінцевих точок інформаційної системи підприємства.

*Мета роботи* - отримання характеристики ефективності ПЗ Nessus для менеджменту вразливостей інформаційних систем. Створення рекомендацій на основі дослідженого матеріалу.

Завдання бакалаврської роботи:

Встановити оптимальні налаштування ПЗ Nessus для проведення менеджменту вразливостей інформаційних систем. Проаналізувати результати

сканування на вразливість інформаційних систем. Розкрити важливість використання політики менеджменту вразливостей для інформаційних системи. Розкрити кращі практики та фреймворки для менеджменту вразливостей.

*Методи дослідження* - опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів, проведення експерименту.

*Практичне значення одержаних результатів*: рекомендації щодо менеджменту вразливостей корпоративних інформаційних систем

# 1 АНАЛІЗ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КІНЦЕВИХ ТОЧОК ТА ЇХ ЗАГРОЗ

## 1.1. Аналіз стану та важливості забезпечення безпеки кінцевих точок інформаційної системи на сьогоднішній день

Забезпечення безпеки кінцевих точок інформаційної системи є важливим аспектом у сучасному світі, де інформаційні технології відіграють ключову роль. Кінцеві точки, такі як комп’ютери, смартфони, роутери та інші пристрої, забезпечують доступ до інформації та ресурсів.

Вразливість кінцевих точок може бути використана злочинцями для виконання різноманітної зловмисної діяльності, такої як крадіжки даних, шпигунство та інше. Відтак, захист кінцевих точок є необхідною для забезпечення безпеки інформаційної системи та захисту від зловмисної діяльності. Застаріле або невиправлене програмне забезпечення вразливе до великої кількості експлойтів, що включає вірусні загрози, SQL-ін’єкції, атаки на відмову в обслуговуванні та інші. Сучасний бізнес без належного захисту кінцевих точок буде наражати себе на більший ризик ускладнень функціонування бізнес-процесів, втрати даних, зниження репутації та пов’язані з цим фінансові втрати.

Глобальна загроза кіберзлочинності постійно зростає і стає важким питанням для бізнесу та населення. В останні роки збитки від кіберзлочинів зростають, а загальна вартість витоку даних постійно збільшується. Це свідчить про те, що організації повинні приділяти більше зусиль для захисту своїх кінцевих точок та інформаційних систем в цілому.

Очікується, що глобальні витрати на кіберзлочинність зростатимуть на 15 відсотків на рік протягом наступних трьох років і досягнуть 10,5 трильйонів доларів США на рік до 2025 року [6].

За 2021 рік середня загальна вартість витоку даних зросла майже на 10% у порівнянні з минулим роком, найбільше однорічне збільшення витрат за останні сім років [5].

Очікується, що глобальний ринок безпеки кінцевих точок зростатиме із річним темпом зростання у 7,6%, щоб досягти 18,4 мільярда доларів США до 2024 року з 12,8 мільярда доларів США у 2019 році. Основними факторами зростання ринку є зростання кількість кінцевих точок і BYOD серед підприємств.(Endpoint Security Market by Solution [7].

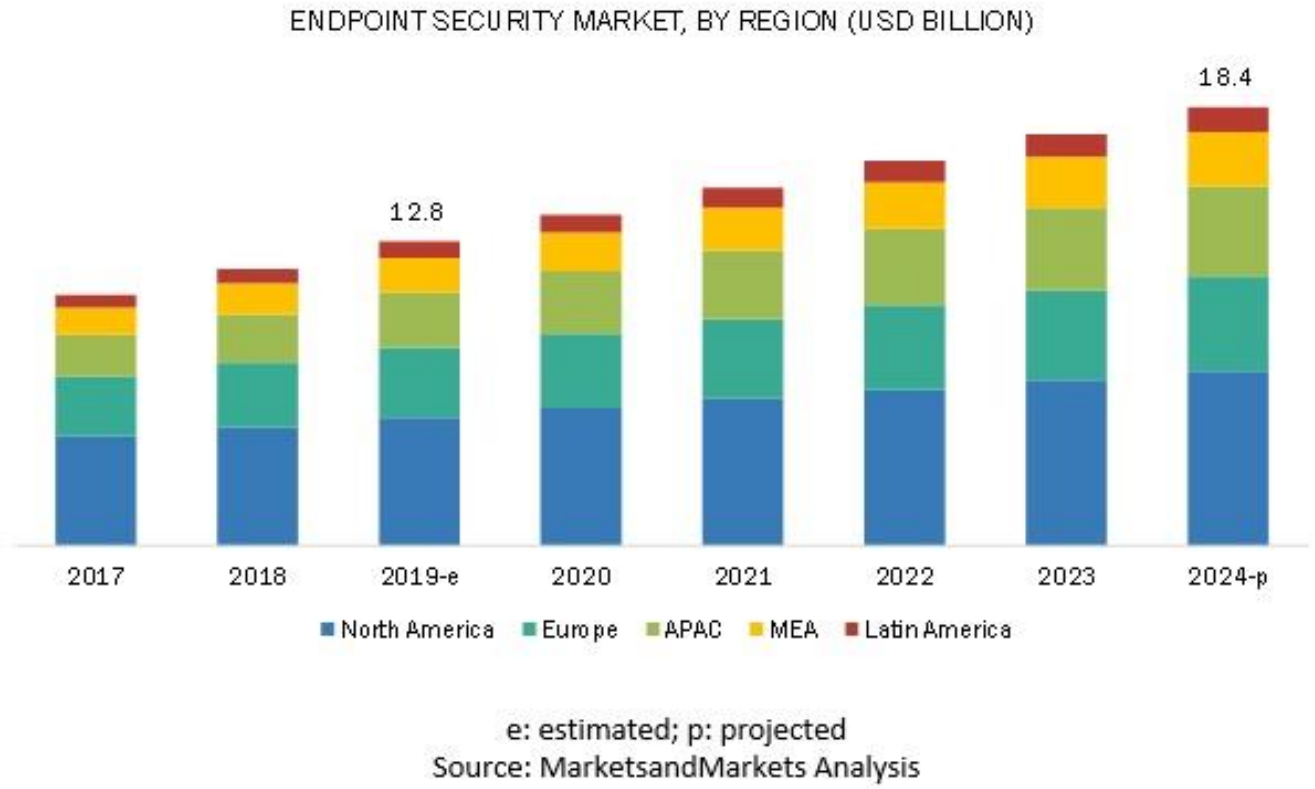



Рис.1.1. Темпи зростання ринку безпеки кінцевих точок

Зростання ролі інформаційних технологій у бізнес-операціях є одним із головних трендів кібербезпеки. Сучасні компанії все частіше використовують інформаційні технології для оптимізації своєї діяльності, підвищення продуктивності та покращення взаємодії з клієнтами. Однак збільшення використання цифрових технологій також призводить до збільшення кількості кіберзагроз, з якими стикаються підприємства.

Збільшення виробництва рішень для захисту кінцевих точок є ще однією важливою тенденцією в кібербезпеці. Підприємства все більше усвідомлюють необхідність захисту своїх кінцевих пристроїв та інвестують у придбання та впровадження рішень для забезпечення безпеки. Зростаюча кількість кінцевих

точок і популярність Bring Your Own Device (BYOD) на підприємствах також сприяють розвитку ринку безпеки кінцевих точок. Кінцеві точки є основними цілями для кіберзлочинців і після успішної можуть використовуватися для отримання доступу до конфіденційної інформації. Тому, компанії слідкують за забезпечення безпеки кінцевих точок, у тому числі за допомогою використання антивірусного програмного забезпечення, віддаленого моніторингу, антифішингу та сканування вразливостей.

Зростання глобальної вартості кіберзлочинності є третьою основною тенденцією в кібербезпеці. Однією з ключових причин зростання кількості загроз стала поява нових технологій і трендів, таких як Інтернет речей, хмарні сервіси та мобільні додатки. Ці технології збільшують площу атаки, відкриваючи нові шляхи для проникнення зловмисників у системи через кінцеві точки. Кіберзлочинність стає все більш серйозною загрозою для компаній і громадян, що призводить до зростання витрат на інформаційну безпеку.

Кібербезпека не обмежується лише технічними заходами. Вона також включає елементи управління ризиками та формування культури безпеки в організації. Успішна концепція кібербезпеки вимагає наявності політик, процедур і засобів контролю, які охоплюють усі сфери інформаційної безпеки. Компанії повинні розробляти і впроваджувати політику кібербезпеки, яка включає оцінку ризиків, управління доступом, навчання співробітників, контроль доступу до даних і моніторинг заходів безпеки.

Ці три тенденції вказують на те, що кібербезпека стає все більш важливою для бізнесу та громадян. Розуміння кіберзагроз та захисту від них стає ключовим питанням для бізнесу, організацій та держави.

### 1.1.1. Класифікація кінцевих точок

Кінцеві точки можна розділити на різні групи на основі їхніх особливостей і функцій. Деякі з поширених категорій включають настільні та портативні комп’ютери, мобільні пристрої, такі як смартфони та планшети, сервери, які

утворюють основу мережі та зберігають важливі дані та програми, пристрої Інтернету речей, такі як пристрої розумного дому та камери безпеки, і системи торгових точок, які використовуються для обробки транзакцій у роздрібних магазинах. Кожен тип кінцевої точки може мати унікальні вимоги до безпеки, тому важливо мати ретельний план безпеки кінцевої точки, який враховує ці особливі потреби [16].

Категоризація кінцевих точок зазвичай базується на функціональних або структурних особливостях організації. Наприклад, категорії можуть включати сервери, робочі станції, мобільні пристрої, мережеві пристрої, системи контролю доступу тощо. Кожна така категорія може мати свої власні унікальні характеристики та вразливості, які впливають на ступінь критичності та можливий ефект на організацію. Одним з підходів до класифікації кінцевих точок є поділ їх за рівнями доступу до ресурсів інформаційних систем. Наприклад, розрізняють адміністративні пристрої, які мають повний доступ до всіх інформаційних ресурсів системи і застосовуються адміністраторами. Далі йдуть користувацькі пристрої, які співробітники організації використовують для виконання своїх задач. Це можуть бути як робочі станції, так і ноутбуки, планшети тощо. Найнижчий рівень доступу - гістьові пристрої, які застосовуються для тимчасових користувачів або для спільного використання

Таблиця 1.1.

Класифікація кінцевих точок за категорією

| Категорія | Приклади кінцевих точок |
|---|---|
| Робоче місце | Ноутбук, настільний комп’ютер, робоча станція |
| Мобільний пристрій | Смартфон, планшет, ноутбук |
| Інтерактивний пристрій | Тачскрін, сенсорний термінал, інтерактивна дошка |
| Інтернет речей | Камера відеоспостереження, смартпристрої |

Таблиця 1.2

Классифікація кінцевих точок за критичністю

| Критичність кінцевої точки | Приклади кінцевих точок за критичністю | Опис |
|---|---|---|
| Критичні кінцеві точки | Сервери, мережеві комутатори, точки продажу(POS) | Пристрої, які є незамінними для функціонування бізнесу і їх відсутність призведе до зупинки процесів. |
| Важливі кінцеві точки | Принтери, сканери, телефонні пристрої | Пристрої, які не є критичними для функціонування, але їх відсутність може суттєво ускладнити процеси |
| Неважливі кінцеві точки | Персональні планшети та смартфони працівників | Пристрої, відсутність яких не вплине на процеси |

Класифікація критичності кінцевих точок визначає міру значущості кожної кінцевої точки для підприємства. Ця класифікація зазвичай включає такі чинники, як доступ до конфіденційної інформації, важливість виконуваних функцій, вплив на процеси та ділову репутацію, ймовірність проникнення, а також інші ризикові показники. На основі цієї класифікації можна визначити різні рівні захисту для кожної категорії кінцевих точок.

Щоб досягти необхідного рівня безпеки для кожного рівня доступу, категоризація кінцевих точок є життєво важливою. Ця класифікація визначає, до яких даних можна отримати доступ на пристрої. Наприклад, конфіденційні документи можна зберігати на рівні адміністратора; тим часом рівень гостьового доступу обмежений для доступу до таких даних.

Витік даних і порушення можна пом’якшити, дотримуючись політик і стандартів, встановлених класифікацією кінцевих точок. Дотримання цих правил розширить можливості користувачів системи, ефективно зменшуючи ризики.

Класифікація кінцевих точок має вирішальне значення для захисту інформаційних систем, мінімізації ризиків і гарантування безпеки даних користувачів. Цей процес відіграє важливу роль в ідентифікації.

### 1.1.2. Класифікація загроз кінцевих точок

*Неправильна конфігурація* є однією з найпоширеніших вразливостей системи, яка в основному спричинена людським фактором, ці вразливості можуть дозволити неавторизований доступ до системи. Неправильна конфігурація може статися, як навмисно, так і ненавмисно та може бути використана зловмисниками для отримання доступу до ваших ресурсів.

*Паролі за замовчуванням* – це стандартні паролі, котрі були налаштовані під час виробництва системи чи продукт. Ці паролі призначені для першочергового доступу користувачем під час початкового процесу. Однак, якщо користувачі нехтують оновленням своїх паролів і продовжують використовувати стандартні

паролі за, вони ризикують залишити свої пристрої та системи вразливими для атак грубої сили та словникових атак, тому, що ці стандартні паролі відомі всім.

*Недоліки додатків* – це помилки під час написання програмного забезпечення, які зазвичай спричинені неуважністю або некваліфікованістю. Ці помилки програмування можуть створювати значні ризики безпеки, включаючи несанкціонований доступ до баз даних чи переповнення буферу. Щоб створювати високозахищені програми, які включають адекватну перевірку та авторизацію для користувача, розробники повинні знати поширені недоліками безпеки програмного забезпечення та як цього уникати.

*Недоліки в архітектурі системи* — це вразливості, які можуть бути присутніми на всіх пристроях і операційних системах. Ці недоліки можуть охоплювати такі проблеми, як слабке шифрування або недостатня валідація даних, які зловмисники можуть використовувати, щоб обійти механізми безпеки або виявлення та отримати несанкціонований доступ до систем. Недоліки дизайну подібні до недоліків додатків, розробники повинні їх ідентифікувати та усунути, щоб створити більш безпечну систему.

*Відкриті порти* – це може означати, що на цих портах наразі працюють служби. Відкриті порти та служби на цих портах можуть створювати ризики безпеки, несанкціонований доступ або атаки на відмову в обслуговуванні. Зловмисники можуть використовувати ці відкриті порти та можливі вразливості сервісів для подальшої атаки на інші підключені пристрої. Щоб зменшити ці ризики, адміністратори мережі повинні регулярно перевіряти наявність незахищених або непотрібних портів і служб і закривати незадіяні порти або приховувати їх за брандмауером з для зменшення потенційної вразливості в мережі.

*Переповнення буфера* — це тип уразливості програмного забезпечення, яка часто виникає через помилки під час програмування, забезпечуючи точку входу для зловмисників, через неповноцінну стерилізацію. Під час атаки переповнення буфера зловмисник намагається отримати контроль над системою шляхом запису

даних, розмір яких перевищує розмір виділеного буфера для змінної . Оскільки буфер не може керувати даними поза межами своєї місткості, зайві дані перетікають у сусідні місця пам’яті та перезаписують їхні значення даних, наприклад на зловмисний програмний код. Як внаслідок, переповнення може призвести до нестабільності системи, збою або нестабільної поведінки програми й навіть до повної компрометації.

*Недоліки в операційній системі* — це можливі вразливості, які зловмисник може використовувати для зараження троянами, хробаками і вірусами. Ці атаки використовують вразливі місця в операційній системі та використовують шкідливий код, сценарії для отримання контролю над системою. Щоб запобігти таким атакам, системним адміністраторам важливо своєчасно встановлювати оновлення операційної системи, розгортати мінімум програмного забезпечення для зменшення радіуса атаки [11].

Загрози кінцевих точок можна класифікувати за критичністю у разі їх виникнення. Зазвичай, критичність оцінюється за наслідками, які можуть виникнути у випадку реалізації загрози [12].

Таблиця 1.3

Класифікація загроз кінцевих точок за критичністю

| Рівень критичності | Опис загрози |
|---|---|
| Високий | Загроза, що може призвести до великих фінансових втрат, втрати конфіденційної інформації, порушення правил та законів, втрати бізнес-даних, пошкодження репутації компанії, витоку персональних даних тощо. |
| Середній | Загроза, що може призвести до незначних фінансових втрат, порушення приватності, невеликого витоку даних, порушення правил і законів, зменшення продуктивності тощо. |
| Низький | Загроза, що може призвести до незначних фінансових втрат, зниження продуктивності, затримки в роботі тощо. |

## 1.2. Порівняння рішень для менеджменту вразливостей кінцевих точок

Щоб захистити ваші кінцеві точки, потрібен багатогранний підхід, який включає як керування оновленнями, так і тестування вразливостей. Керування оновленнями передбачає регулярне оновлення операційних систем, програм та інших компонентів, що використовуються на кінцевих точках. Таким чином можна виправити відомі вразливості та покращити безпеку системи.

Тестування вразливостей передбачає пошук потенційних уразливостей у програмному забезпеченні, що використовується на кінцевих точках, шляхом виконання цільових тестів і сканування портів і протоколів зв'язку. Цей підхід може бути використаний зовнішніми експертами з безпеки, внутрішньою командою з аудиту безпеки або за допомогою спеціальних програмних засобів. Після виявлення вразливостей можна вжити заходів для їх усунення та підвищення безпеки системи. Завдяки такому підходу ви можете переконатися, що ваші кінцеві точки захищені від потенційних загроз безпеці.

На ринку є безліч сканерів вразливостей, від сканерів з інтерфейсом командної строки, до прогресивних сканерів, які розробляє велика команда, але більшість з них не такі вишукані, як Nessus. Більшість сканерів не мають таку велику базу даних уразливостей або не пропонують такий самий рівень налаштування, як Nessus. Крім того, багато сканерів не надають докладних звітів про вразливості які було знайдено під час сканування, що ускладнює ідентифікацію та визначення пріоритетів ризиків.

Крім того, деякі альтернативні сканери можуть не мати великої спільноти підтримки чи вичерпної документації, що може бути важливо для користувачів, які тільки починають користуватись сканером або потребують додаткової допомоги. Nessus — це популярний сканер вразливостей, який пропонує багато переваг для організацій, які хочуть керувати ризиками безпеки. Він вирізняється серед інших сканерів великою базою даних уразливостей, яка регулярно оновлюється, щоб охопити широкий спектр систем і програм. Крім того, Nessus надає параметри

сканування як з обліковими даними, так і без них, що дозволяє більш повно виявляти вразливості.

Nessus також має зручний інтуїтивно зрозумілий інтерфейс, який надає докладні звіти про вразливості та їх критичність. Його також можна налаштувати відповідно до конкретних потреб, що робить його універсальним інструментом для різних організацій і випадків використання та позитивно виділяє серед інших рішень по менеджменту вразливостей.

Ще однією перевагою Nessus є потужна спільнота підтримки та повна документація, яка допомагає користувачам швидко розпочати роботу та розв'язати будь-які проблеми, які можуть виникнути. Для тих, кому потрібна додаткова допомога, Tenable, компанія, що стоїть за Nessus, пропонує професійні послуги підтримки.

Nessus є одним з найбільш універсальних сканерів вразливостей, оскільки працює з широким спектром різних протоколів, включаючи HTTP, HTTPS, FTP, SMTP, SSH, Telnet, SNMP, SMB, RDP і багато інших. У порівнянні з альтернативними сканерами, такими як OpenVAS, Qualys і Rapid7, Nessus має більш широкий спектр сумісних протоколів, що дозволяє йому виявляти вразливості на різних типах пристроїв і мереж.

Загалом, Nessus — це потужний сканер уразливостей, який підходить для організацій будь-якого розміру та галузей. Велика база даних уразливостей, параметри сканування, які можна налаштувати, зручний інтерфейс і потужна спільнота підтримки роблять його чудовим вибором для тих, хто хоче ефективно керувати ризиками безпеки [9].

### 1.3. Можливості рішення для менеджменту вразливостей Nessus

Nessus Community — це безплатна версія програмного забезпечення від Tenable, яка дозволяє вам ідентифікувати загрози безпеці вашої мережі, хостів та мобільних пристроїв за допомогою сканування можливих вразливостей і оцінки безпеки за різними шкалами оцінки. Можливості Nessus community включають

сканування мережі, виявлення активних хостів, перевірку відповідності мережевих пристроїв і програмного забезпечення стандартам безпеки, звітування про вразливості, багатоплатформну підтримку, перевірку системи конфігурації, аналіз вразливостей вебдодатків і сканування вразливостей мережевих пристроїв. Nessus community також підтримує різні типи сканування [10].

До найбільш використовуваних можливостей рішення для менеджменту вразливостей Nessus належать:

сканування вразливостей: Nessus Community дозволяє сканувати мережу на наявність вразливостей та потенційні загрози безпеці;

розпізнавання активних хостів: Програмне забезпечення може виявити всі активні хости в мережі та сканувати їх для виявлення вразливостей;

аудит відповідності: Nessus Community дозволяє перевіряти відповідність мережевих пристроїв і хостів стандартам безпеки, таким як HIPAA, PCI DSS, ISO 27001 та інші;

створення звітів: програмне забезпечення може збирати інформацію про виявлені вразливості та створювати звіти, які можуть бути використані для аналізу та виправлення вразливостей;

підтримка декількох платформ: Nessus Community підтримує сканування різних операційних систем, включаючи Windows, Linux та macOS;

перевірка конфігурації системи: програмне забезпечення може перевіряти конфігурацію системи на відповідність стандартам безпеки та рекомендаціям;

аналіз вразливостей вебдодатків: Nessus Community може сканувати вебдодатки на вразливості та потенційні загрози безпеці;

пошук вразливостей у мережевих пристроях: програмне забезпечення може сканувати мережеві пристрої, такі як маршрутизатори та комутатори, на вразливості та потенційні загрози безпеці;

різні типи сканування: Nessus Community підтримує різні види сканування вразливостей;

Nessus можна використовувати як компонент корпоративної програми безпеки. Якщо його правильно налаштувати та використовувати, Nessus може допомогти менеджерам із безпеки знайти та виправити проблеми їхній інфраструктурі.

Однією з головних переваг Nessus є те, що він дозволяє автоматизувати виявлення вразливостей у різних системах, при цьому для роботи з програмою не потрібно багато досвіду. Це скорочує час, необхідний для розв'язання проблеми, і забезпечує більш точні результати з меншими зусиллями. Також Nessus проводить детальний аналіз виявлених уразливостей і дає рекомендації щодо їх усунення. Це полегшує, швидше та ефективніше вирішення проблеми у вашій інфраструктурі. Ці можливості рішення Nessus дозволяють використовувати його як частину управління вразливістю.

### 1.3.1. Кращі практики та фреймворки для менеджменту вразливостей кінцевих точок

В управлінні вразливостями процес оцінки та встановлення пріоритетів уразливостей безпеки в програмному забезпеченні, системах і мережах є одним з найважливіших етапів. Кращими практиками для менеджменту вразливостей кінцевих точок буде:

*Використання підходу, що ґрунтується на оцінці ризику*: визначаючи пріоритетність вразливостей на основі рівня ризику та враховуючи потенційний вплив і ймовірність використання можна сильно покращити час та ефективність реагування. Цей підхід допомагає організаціям зосередитися на найбільш критичних уразливостях і краще розподіляти ресурси.

*Регулярне сканування*: виконуючи регулярне сканування для виявлення нових вразливостей, які могли бути введені через зміни у системі або оновлення програмного забезпечення, ми отримуємо кращий огляд нашої інфраструктури.

*Управління виправленнями*: шляхом впровадження процесу швидкого застосування виправлень для усунення виявлених вразливостей інфраструктура залишається вразливою протягом коротшого періоду часу.

*Аналіз загроз:* Аналізуючи можливі загрози, ми сприяємо виявленню нових загроз і ранньому усуненню потенційних вразливостей.

*Автоматизація.* Використовуючи автоматизацію для оптимізації процесів керування вразливостями, наприклад автоматизованого сканування та усунення вразливостей, час реагування на вразливості та виявлення проблем можна значно зменшити.

Деякі популярні фреймворки для керування вразливостями включають:

*Концепція кібербезпеки Національного інституту стандартів і технологій*: забезпечує основу для організаційного управління та пом’якшення ризиків кібербезпеки компанії. NIST пропонує структурований підхід до управління вразливістю, що дозволяє використовувати цей підхід протягом усього життєвого циклу кібербезпеки.

*Відкритий проєкт безпеки вебдодатків Топ 10:* Визначає 10 найпоширеніших вразливостей у безпеці веб-додатків і містить вказівки щодо їх усунення. Цей фреймворк допоможе класифікувати знайдені вразливості та швидко усувати виявлені проблеми.

*Система оцінки вразливості*: надає стандартизований метод для оцінки та передачі інформації про серйозність уразливості. Ця система використовується в Nessus.

*ISO/IEC 27001 Система управління інформаційною безпекою:* забезпечує систематизований підхід до управління конфіденційною інформацією компанії для забезпечення її безпеки. Дотримуючись цього стандарту можна покращити загальну безпеку компанії [2].

**Висновки до першого розділу**

Результати дослідження у першому розділі дипломної роботи свідчать про надзвичайну важливість забезпечення безпеки кінцевих точок інформаційних систем. Проведений аналіз сучасного стану засвідчив, що безпека кінцевих точок є гострою проблемою, яка потребує негайної уваги та втручання. Класифікація кінцевих точок дозволяє виявити критичні елементи та визначити їх класи, що є основою для ефективної розробки стратегій безпеки. Дослідження загроз кінцевих точок розкриває різноманітність потенційних небезпек і дозволяє розставити пріоритети у сфері інформаційної безпеки. Порівняння рішень для управління вразливостями, включаючи Nessus, демонструє вагому перевагу та ефективність останнього. Аналіз проведених досліджень вказує на те, що Nessus забезпечує широкий спектр функціональності і можливостей для виявлення та управління вразливостями кінцевих точок. Нарешті, розгляд найкращих практик та фреймворків для управління вразливостями кінцевих точок надає поради та настанови щодо оптимального підходу до забезпечення безпеки. Загалом, цей розділ дає глибоке розуміння сутності та важливості управління вразливостями кінцевих точок інформаційних систем.

# 2 ДОСЛІДЖЕННЯ ШЛЯХІВ ТА МЕТОДІВ УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ КІНЦЕВИХ ТОЧОК

## 2.1. Переваги та недоліки рішень щодо управління вразливостями. Аргументація вибору рішення Nessus

Першим кроком в управлінні вразливостями є визначення кінцевих точок і подальше виявлення проблемних областей в безпеці інформаційної системи вашої компанії. Цей етап називають Інвентаризація. Цього можна досягти шляхом сканування портів, використовуючи такі засоби, як Nessus. Сканування допоможе вам візуалізувати поточний стан ваших ресурсів, що знадобиться для подальшої корекції віднайдених проблем.

Виправлення та оновлення є одним із найефективніших, водночас найлегших способів зменшити ризик уразливості. Під час цього кроку застосовуються оновлення і виправлення до програмного забезпечення чи операційної системи. Розробники програм можуть виправляти вразливості та випускати виправлення та оновлення. Тому необхідно стежити за оновленнями й за тим, що вони виправляють.

Іншим ефективним методом є встановлення антивірусного програмного забезпечення, яке забезпечить захист від відомих загроз та деяких атак.

Важливо переконатися, що дані, які передаються, зашифровані, тому впровадження шифрування навіть на хости з вразливостями може захистити їх.

Виявлення вразливості може допомогти забезпечити вищий рівень безпеки кінцевої точки та мережі. Однак важливо пам'ятати, що сканування проводитися з урахуванням можливих наслідків для цієї системи. Крім того, після виявлення вразливостей необхідно вжити заходів для забезпечення безпеки системи. Перш за все, виявлення вразливостей дозволяє застосовувати проактивний підхід до безпеки, який дозволяє виявляти та виправляти вразливості до того, як вони будуть використані для атаки. Це дозволяє знизити ризик порушення безпеки та забезпечити вищий рівень безпеки системи в цілому.

Крім того, виявлення вразливостей дозволяє оцінити рівень безпеки системи та виявити присутні проблеми, які можуть бути пропущені іншими методами контролю безпеки.

Також виявлення вразливостей є одним з етапів розробки стратегії забезпечення безпеки систем і може використовуватися для ідентифікації потреб у подальших методах захисту.

Таким чином, виявлення вразливості є важливим практичним етапом безпеки кінцевих точок, і його слід виконувати перед використанням будь-яких інших методів контролю безпеки[1].

Nessus — потужний і добре відомий інструмент для виявлення вразливостей у мережевих пристроях і програмному забезпеченні. Він має широкі можливості та докладні звіти, які дозволяють швидко та ефективно виявляти вразливості та забезпечувати високий рівень безпеки системи.

Кожен тип управління вразливостями має свої переваги та недоліки, оскільки базується на різних стратегіях роботи з вразливостями та ризиками безпеки. Реактивний підхід означає реагування на виявлені вразливості шляхом вжиття відповідних заходів з їх усунення. Такий підхід допоможе організації ефективно розв’язувати проблеми в короткостроковій перспективі, але може призвести до затримок у реагуванні та невиправданих витрат ресурсів.

З іншого боку, проактивний підхід може запобігти виникненню вразливостей і знизити ризики шляхом виявлення та усунення проблем до того, як вони стануть реальною загрозою. Такий підхід дозволяє організації мінімізувати ризик постраждати від вразливості та заощадити ресурси в довгостроковій перспективі, але він також може призвести до вищих витрат на виправлення та відновлення.

Крім того, стратегія адаптивного управління - це поєднання реактивного та проактивного підходів, що забезпечує баланс між ефективністю та зниженням ризиків. Однак такий підхід може бути менш ефективним у конкретних ситуаціях, коли необхідно зосередитися на конкретному засобі захисту.

Нижче наведені приклади управління вразливостями та їх переваги та недоліки:

Виправлення та оновлення

*Переваги*:

Оновлення помилок забезпечують виправлення відомих уразливостей та інших причин, які знижують безпеку системи;

Оновлення може покращити функціональність і продуктивність системи;

Оновлення - це дешевий і простий спосіб управління вразливостями;

*Недоліки*:

Оновлення може порушити сумісність програмного забезпечення та пристроїв, що призведе до недоступності або несправності системи;

Оновлення може спричинити перезавантаження системи, що спричинить падіння продуктивності та затримки;

Антивірусне програмне забезпечення

*Переваги*:

Антивірусне програмне забезпечення захищає систему від шкідливих програм і вірусів;

Антивірусне програмне забезпечення може виявляти та блокувати нові загрози;

*Недоліки*:

Антивірусне програмне забезпечення може знизити продуктивність системи, працюючи у фоновому режимі;

Антивірусне програмне забезпечення може не виявляти нові загрози, які не включено до його вірусної бази даних;

Шифрування

*Переваги*:

Шифрування забезпечує конфіденційність і захист інформації від несанкціонованого доступу;

Шифрування може захистити пристрої в разі втрати або крадіжки, не даючи зловмисникам отримати збережену на них інформацію;

Шифрування є ефективним методом захисту від різних типів кібератак, таких як перехоплення даних або атаки типу "людина посередині";

*Недоліки*:

Шифрування може знизити продуктивність системи через додаткову обробку даних;

Для налаштування та керування шифруванням можуть знадобитися додаткові зусилля та ресурси;

Виявлення вразливостей

*Переваги*:

Сканування показує вразливі частини системи й дозволяє уникнути кібератак через отриману інформацію;

Сканування може допомогти виявити проблеми з безпекою на ранній стадії, дозволяючи вчасно вжити заходів для їх усунення;

*Недоліки*:

Сканування може займати значні обчислювальні ресурси та бути трудомістким процесом;

Сканування може бути неефективним, якщо воно використовується неправильно або не в поєднанні з іншими методами захисту;

Nessus - це надійне програмне забезпечення для виявлення вразливостей і ризиків в мережі з простим інтерфейсом і можливістю отримання об'єктивної інформації про стан безпеки організації, який може бути використанний для аналізу

та оцінки ризиків. Nessus краще за деякі інші продукти для сканування вразливостей у низці аспектів, таких як швидкість сканування, глибина сканування, підтримка операційних систем і протоколів, наявність великої бази даних вразливостей, а також можливість автоматизації сканування та аналізу отриманих результатів.

## 2.2. Ознайомлення з інтерфейсом та можливостями рішення Nessus

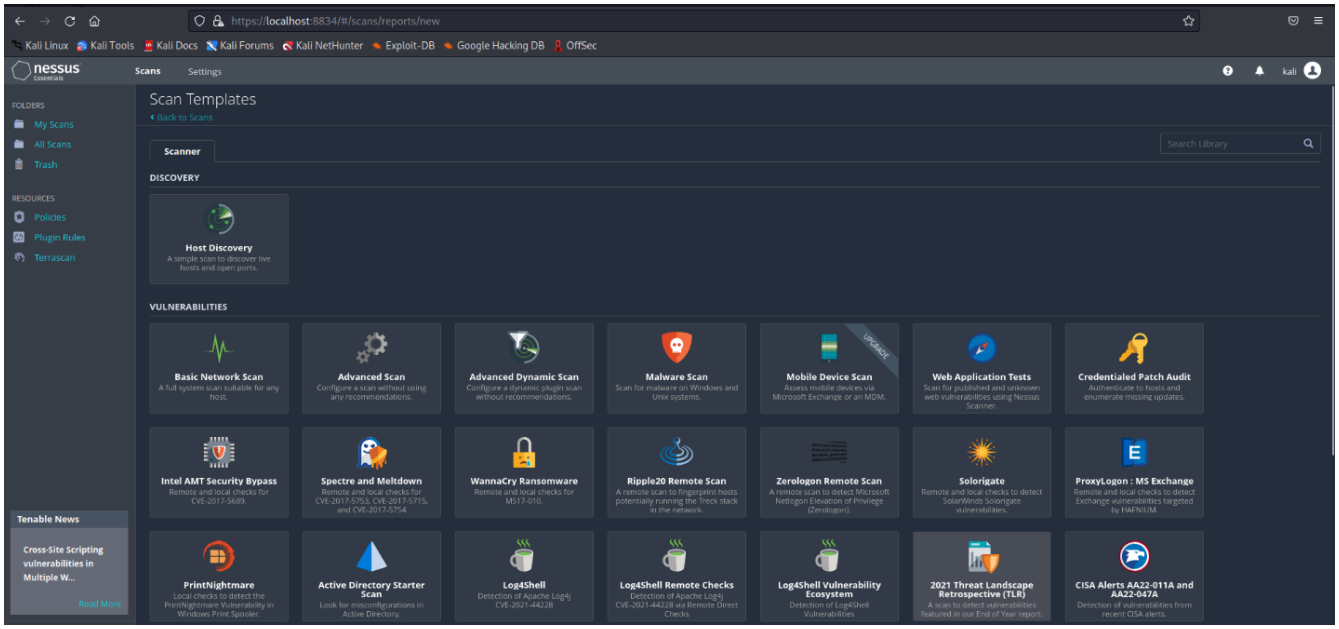



Рис. 2.1. Інтерфейс Nessus essentials

Основний дашборд Nessus essentials складається з усіх можливих типів сканування:

1. *Базове сканування мережі* — це найпростіший спосіб сканування мережі, який дозволяє знайти основні вразливості в системах і пристроях, розташованих у мережі.

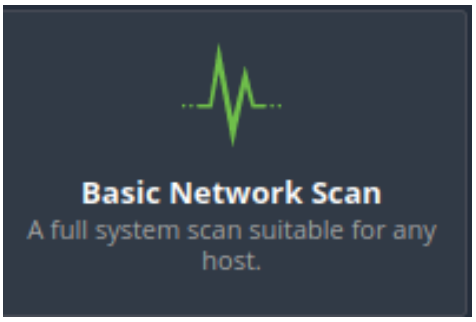



Рис. 2.2. Базове сканування мережі

2. *Розширене сканування* — це більш потужний метод мережевого сканування, який дозволяє знаходити складніші вразливості в системах і пристроях, розташованих у мережі. Розширене сканування дає користувачам можливість налаштовувати конкретніші параметри сканування, наприклад вибирати певні порти, налаштовувати додаткові параметри сканування та виключати певні пристрої зі сканування.

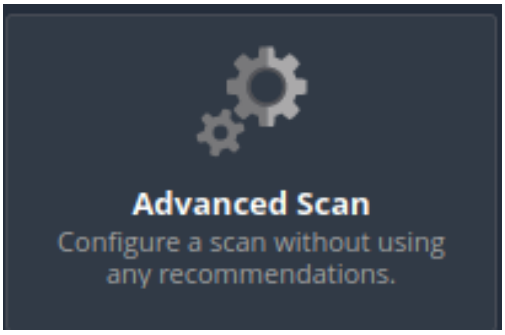



Рис. 2.3. Розширене сканування

3. *Розширене динамічне сканування* — Це вид динамічного сканування, який дозволяє створювати скан або політику з динамічними фільтрами плагінів замість того, щоб вручну вибирати групи плагінів або окремі плагіни.

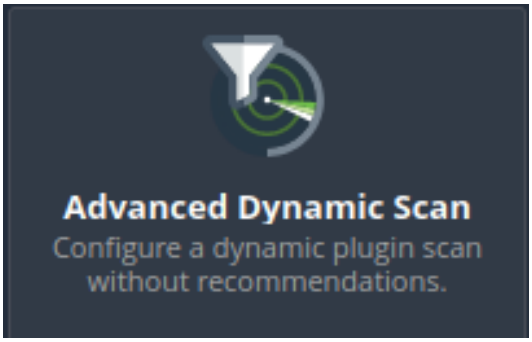



Рис. 2.4. Розширене динамічне сканування

4. *Сканування шкідливих програм* — це сканер, який виявляє наявність шкідливих програм у системі. Сканування зловмисного програмного забезпечення допомагає користувачам знаходити зловмисне програмне забезпечення, яке може спричиняти проблему безпеки комп'ютера.


Рис. 2.5. Сканування шкідливих програм

5. *Тести вебдодатків* — це сканер, який виявляє вразливості у вебдодатках, які працюють на серверах. Цей сканер виявляє різні вразливості, включаючи XSS, SQL, підвищення привілеїв, вразливість ін'єкції даних та інші.

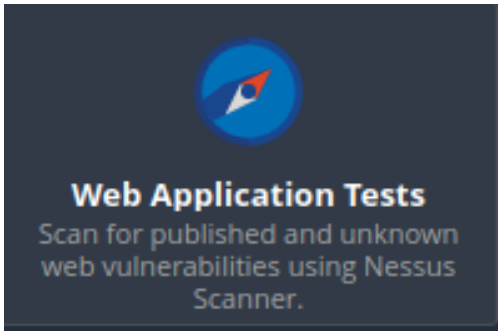



Рис. 2.6. Тести вебдодатків

6. *Аудит патчів з обліковими даними* — це сканер, який дозволяє виявляти проблеми з оновленнями програмного забезпечення та виправленнями в системах. Цей сканер використовує облікові дані користувача, щоб отримати доступ до системи та перевірити наявність оновлень і виправлень для встановлених програм і компонентів.

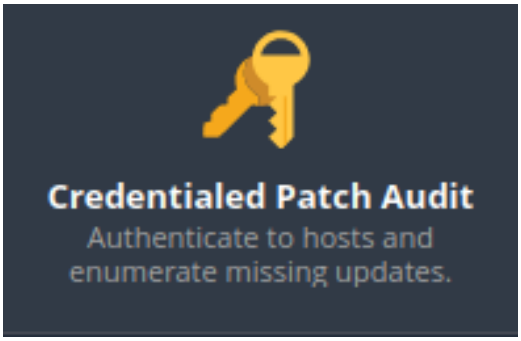



Рис. 2.7. Аудит патчів з обліковими даними

7. *Intel Active Management Technology (AMT) Security Bypass* — це сканування на вразливість, яка дозволяє зловмиснику зберегти доступ до системи, на якій працює технологія Intel AMT. Цю вразливість можна використовувати для здійснення різноманітних атак, включаючи перехоплення даних, керування системою та отримання конфіденційної інформації.

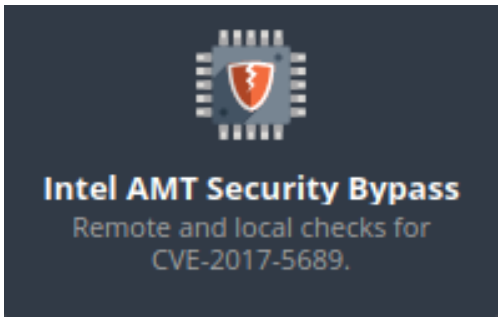



Рис. 2.8.. Intel Active Management Technology security bypass

8. *Spectre і Meltdown* — це дві уразливості, про які стало відомо у 2018 році. Вони впливають на більшість процесорів, що використовуються в комп’ютерах і мобільних пристроях. Ці вразливості використовуються зловмисниками для отримати доступу до конфіденційної інформації, такої як паролі, ключі шифрування та інші дані, що зберігаються в пам’яті пристрою.


Рис. 2.9. Spectre and Meltdown

9. *WannaCry Ransomware* – є однією з найбільших відомих атак 2017 року. Ця атака використовувала вразливість в операційній системі Windows, яка дозволяла зловмисникам віддалено шифрувати файли на комп’ютерах, підключених до Інтернету. Програма-вимагач WannaCry вимагала від користувачів значні суми грошей за розшифровку їхніх даних.

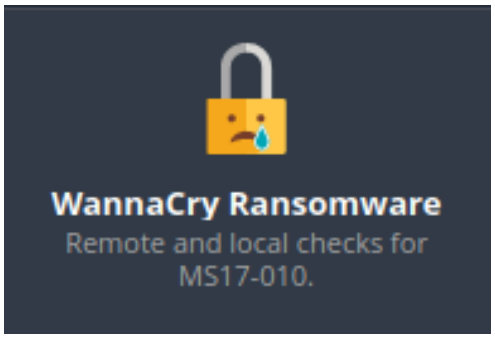



Рис. 2.10. WannaCry Ransomware

10. *Ripple20* — це вразливість, виявлена в серпні 2020 року в бібліотеках Treck, які використовуються для створення пакетів TCP/IP на різних пристроях. Ця вразливість дозволяє зловмисникам використовувати вразливість у програмному забезпеченні для виконання віддаленого коду на підключених пристроях.

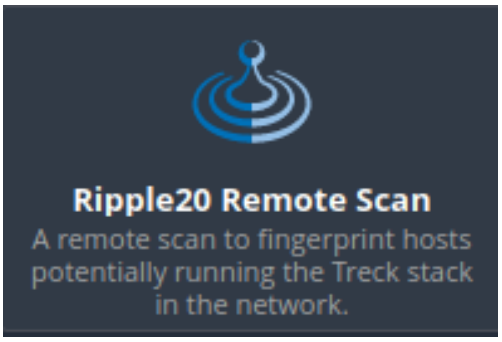



Рис. 2.11. Ripple20

11. *Zerologon* — це вразливість, виявлена в серпні 2020 року, яка дозволяє зловмиснику отримати необмежений доступ до системи, на якій працює контролер домену Active Directory. Цю вразливість можна використовувати для отримання адміністративних привілеїв, зміни паролів та виконання інших зловмисних дій.

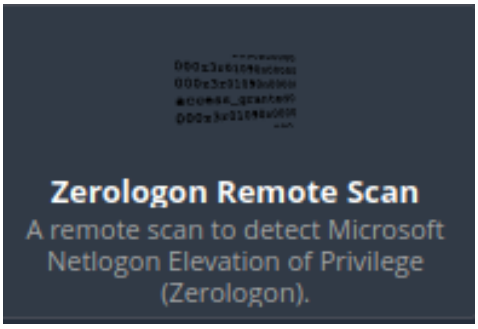



Рис. 2.12. Zerologon

12. *SolarWinds Sunburst*, також відома як Solorigate, є однією з найзначніших і найскладніших кібератак в історії. Ця атака була виявлена в грудні 2020 року в результаті зламу мережевих продуктів SolarWinds. Зловмисники використовували спеціально створений шкідливий код для отримання доступу до мереж та інформації підприємств і установ.


Рис. 2.13. SolarWinds Sunburst

13. *ProxyLogon* — це назва вразливості в Microsoft Exchange Server, яку було виявлено в березні 2021 року. Ця вразливість дозволяє зловмисникам здійснювати віддалені кодові виклики та отримувати неавторизований доступ до серверів Exchange. В результаті атаки зловмисник може отримати доступ до поштових скриньок, відправляти та отримувати листи та іншу конфіденційну інформацію.

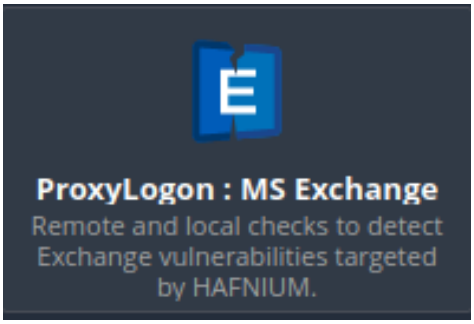



Рис. 2.14. ProxyLogon

14. *PrintNightmare* – це назва вразливості, яка з’явилася в середині 2021 року і пов’язана з драйверами принтерів в операційних системах Microsoft Windows. Ця вразливість дозволяє зловмисникам виконувати віддалені кодові виклики та отримувати неавторизований доступ до системи.

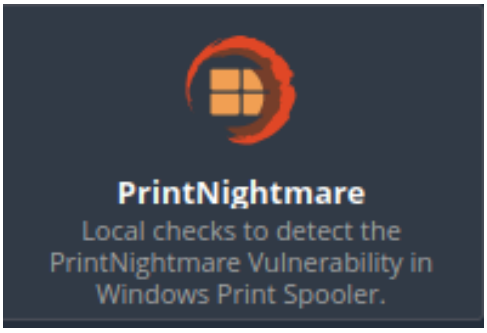



Рис. 2.15. PrintNightmare

15. *Початкове сканування Active Directory* — це функція, яка дозволяє сканувати та перевіряти Active Directory, збираючи інформацію про наявність уразливостей і проблеми безпеки.

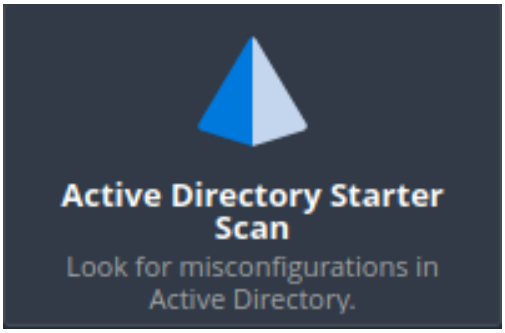



Рис. 2.16. Початкове сканування Active Directory

16. *Log4Shell* — це вразливість у програмному забезпеченні Apache Log4j, яка дозволяє зловмисникам виконувати код на сервері, який використовує цю бібліотеку. Ця вразливість стала досить відомою завдяки широкому використанню Apache Log4j у багатьох вебдодатках та інших програмах.

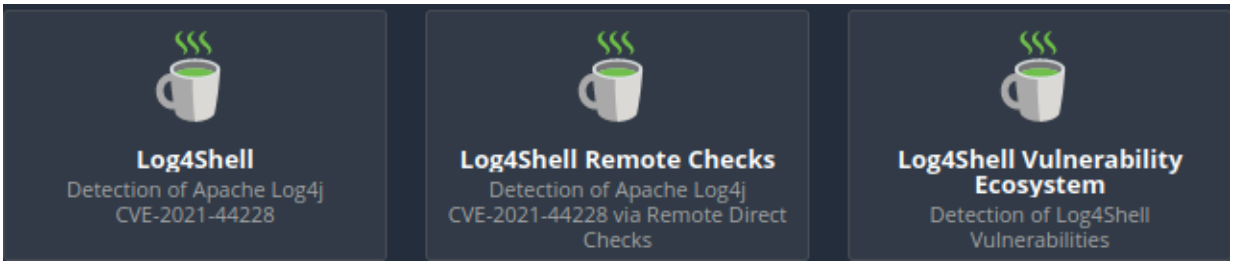



Рис. 2.17. Log4Shell

17. *Ретроспектива ландшафту загроз 2022* – це аналіз загроз кібербезпеці та тенденцій, які спостерігалися протягом року. Він має на меті надати розуміння методів і способів, які використовували зловмисники, організацій і галузей, які були цілями, а також уразливості, які були використані.


Рис. 2.18. Ретроспектива ландшафту загроз 2022

18. *AA22-011A* — це попередження високого рівня серйозності, яке вказує на вразливість у Microsoft Exchange Server. Зокрема, це сповіщення спрацьовує, коли Nessus виявляє недолік у панелі керування Exchange, який може дозволити зловмиснику виконати довільний код на сервері Exchange. Ця вразливість відстежується як CVE-2021-28480.


Рис. 2.19. AA22-011A

19. *ContiLeaks* — це кіберзлочинна група, яка нещодавно привернула увагу через витік конфіденційних даних і фінансової інформації з цільових організацій. Вони відомі використанням програм-вимагачів і крадіжкою даних, для того, щоб вимагати гроші у своїх жертв. Вони розкрили 30 невідомих вразливостей, які цей скан може зафіксувати.

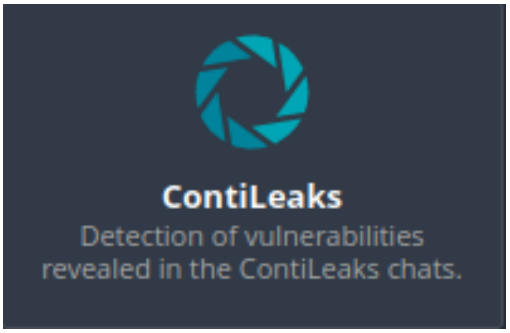



Рис. 2.20. ContiLeaks

20. *Екосистема програм-вимагачів* — це взаємопов'язана мережа осіб, груп і технологій, які беруть участь у розробці, розповсюдженні та розгортанні програм-вимагачів. Система включає розробників програм-вимагачів, розповсюджувачів і операторів, а також інструменти та служби, які використовуються для створення та запуску атак програм-вимагачів.


Рис. 2.21. Екосистема програм-вимагачів

## 2.3. Демонстрація використання Nessus для проведення сканування на вразливості кінцевої точки

Для прикладу вразливої кінцевої точки я обрав віртуальну машину Metasploitable2 від компанії rapid7 [8].

Metasploitable2 віртуальна машина, створена для демонстрації вразливостей та експлойтів у мережевому середовищі. Вона спеціально створена з низьким рівнем безпеки, вміщує велику кількість уразливостей і сервісів, які можна експлуатувати.

Metasploitable2 моделює реальну систему з вразливостями, яка симулює справжню мережу. Це полегшує розуміння та відтворення реальних сценаріїв атак та захисту. Metasploitable2 можна використовувати для навчання та проведення

практичних досліджень у сфері кібербезпеки. Він дозволяє студентам і фахівцям зрозуміти основи атак і захисту, а також дослідити реальні сценарії вразливостей.

Віртуальна машина містить багато різноманітних типів вразливостей, включаючи слабкі паролі, вразливості веб-додатків, вразливості мережевих протоколів тощо. Це дозволяє продемонструвати різноманітні варіанти сценаріїв атак і різні способи експлуатації.

Завантаживши віртуальний диск цієї вразливої операційної системи та встановивши його до програмного гіпервізора VirtualBox, я перевіряю, чи є у машини адреса, та у якому мережевому режимі вона працює.

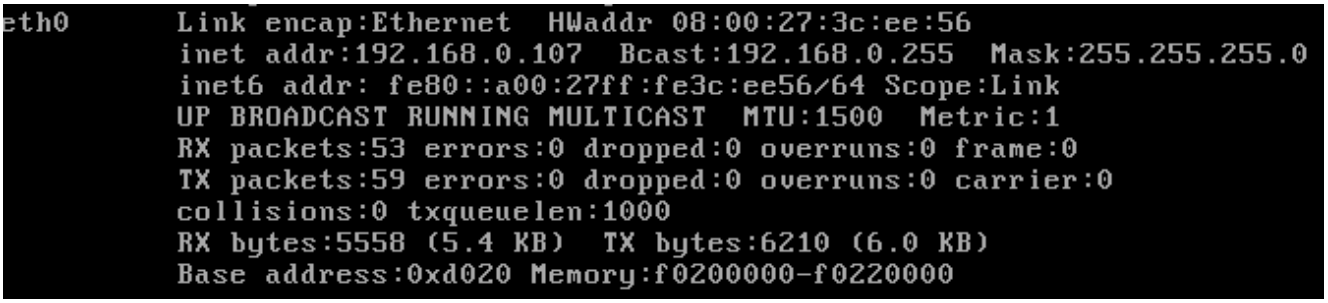



Рис. 2.2. Мережевий інтерфейс віртуальної машини Metasploitable2

Під час сканування кінцевої точки процес зазвичай починається зі сканування мережі на доступні хости, якщо інформація про кінцеву точку невідома. Для цього можна використовувати різні інструменти, такі як сканери портів або програми для виявлення пристроїв у мережі. Для цього типу сканування у Nessus присутня своя функція.

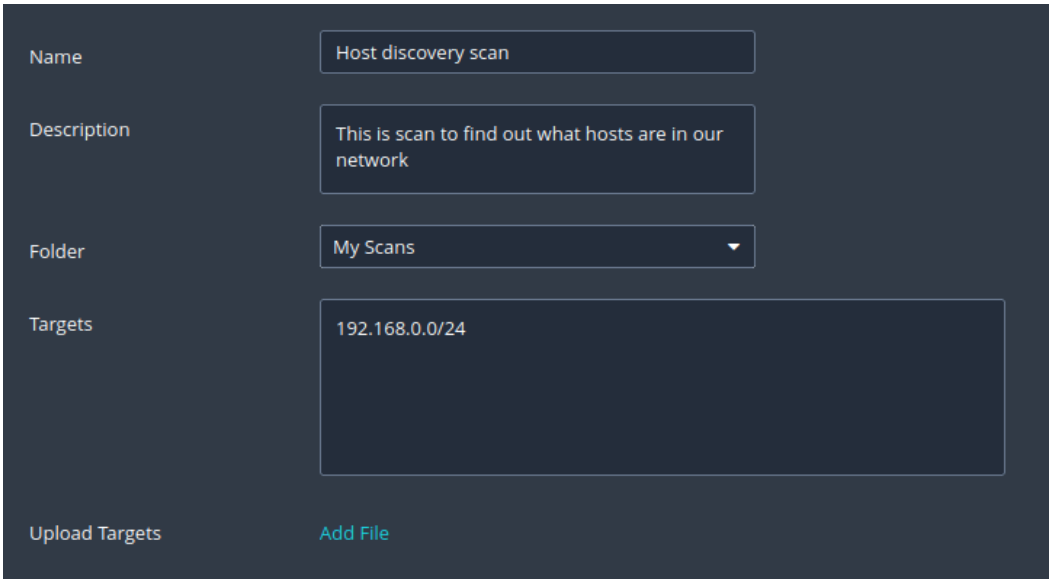



Рис. 2.3. Налаштування для Host Discovery scan

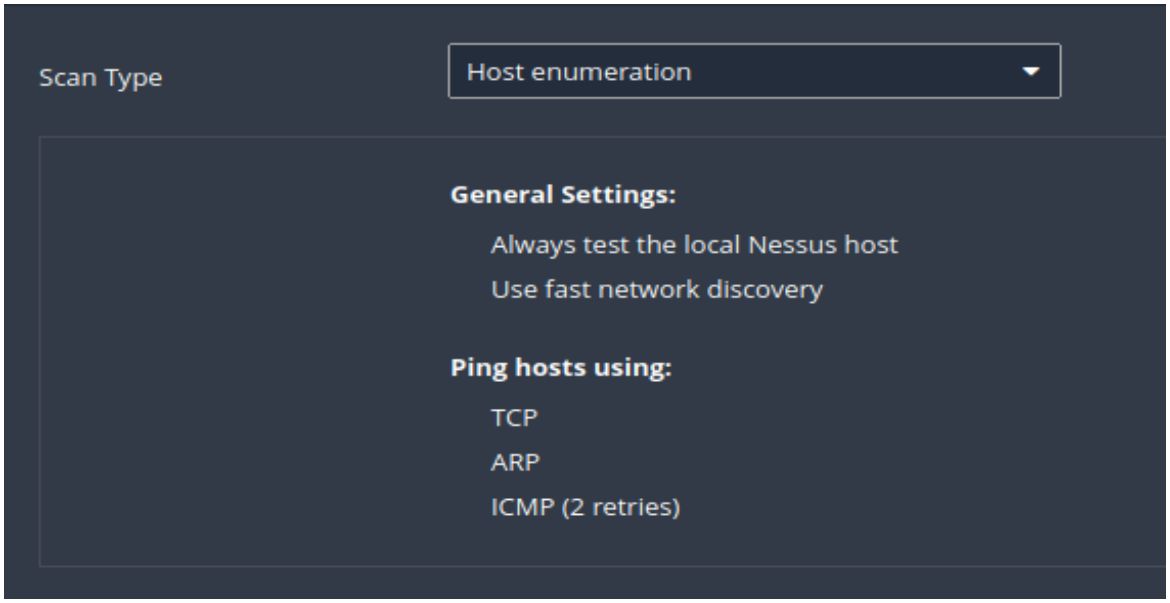



Рис. 2.4. Налаштування типу сканування для Host Discovery scan

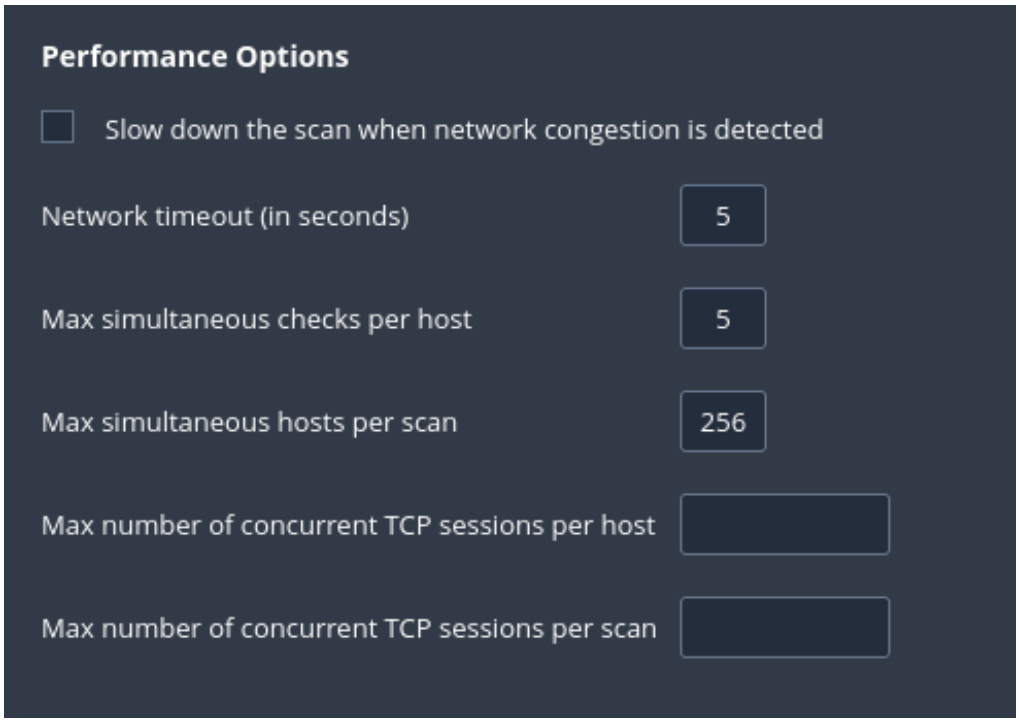



Рис. 2.5. Налаштування продуктивності для Host Discovery scan

Вказавши цілі для сканування, що є мережею, у яку входить Metasploitable2, обравши тип скану без енумерації всіх портів, та вказавши налаштування продуктивності я почав сканування мережі.


Рис. 2.6. Результат роботи Host Discovery scan

В результаті такого сканування я отримав список усіх знайдених хостів та можливі відкриті відомі порти. Цей тип сканування може бути пропущений, якщо ви знаєте адреси хостів, які збираєтесь перевіряти. Зазвичай у компаніях використовують статичне присвоєння адреси для важливих серверів та хостів, що дозволяє не проводити сканування на віднайдення хостів у мережі та уникнути збільшення використання можливостей ресурсів мережі.

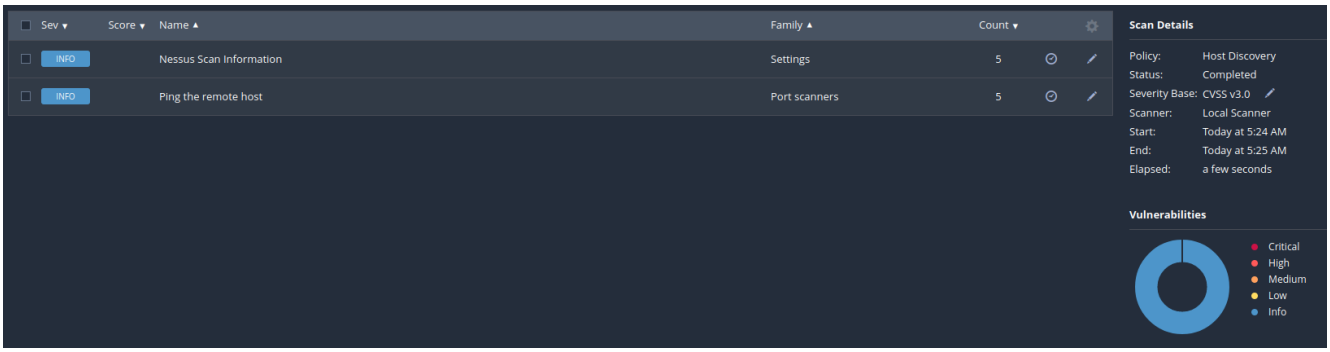



Рис. 2.7. Вразливості Host Discovery scan

У звіті сканування хостів бачимо дві вразливості інформаційного характеру. Це означає, що хост відповідає на ping запроси.

Дізнавшись на практиці, яка адреса відповідає хосту Metasploitable, можемо запускати глибше сканування для знаходження вразливостей.

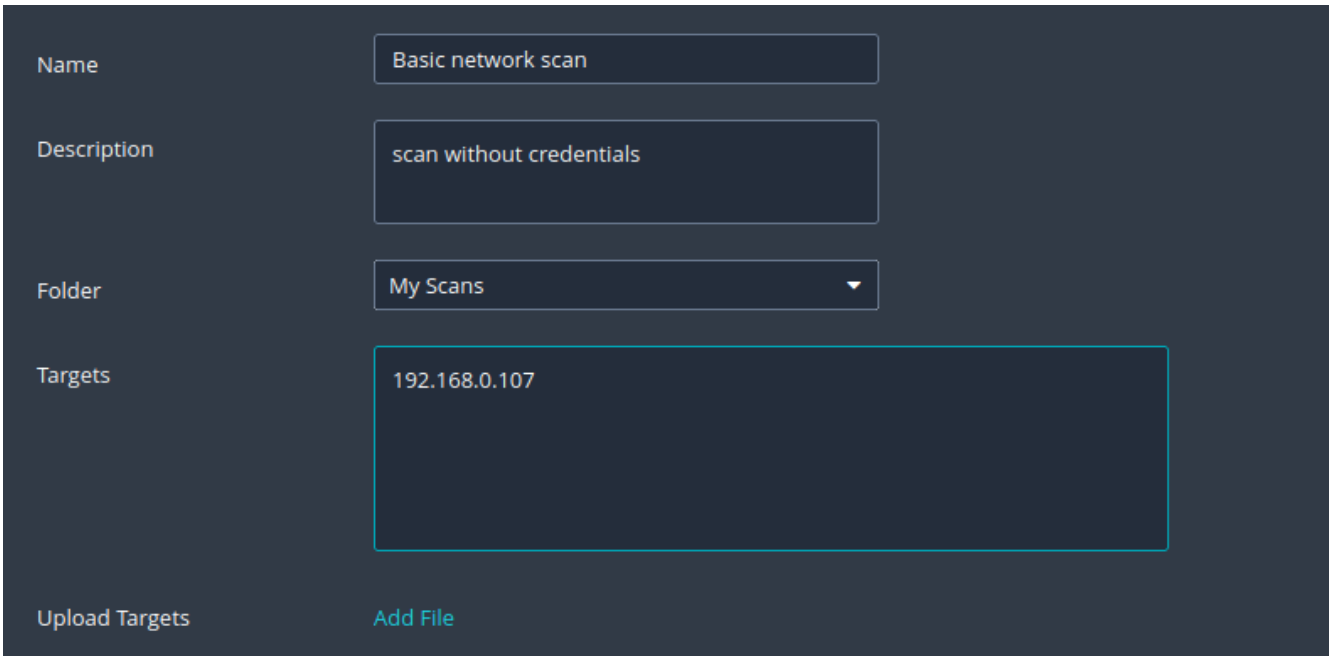
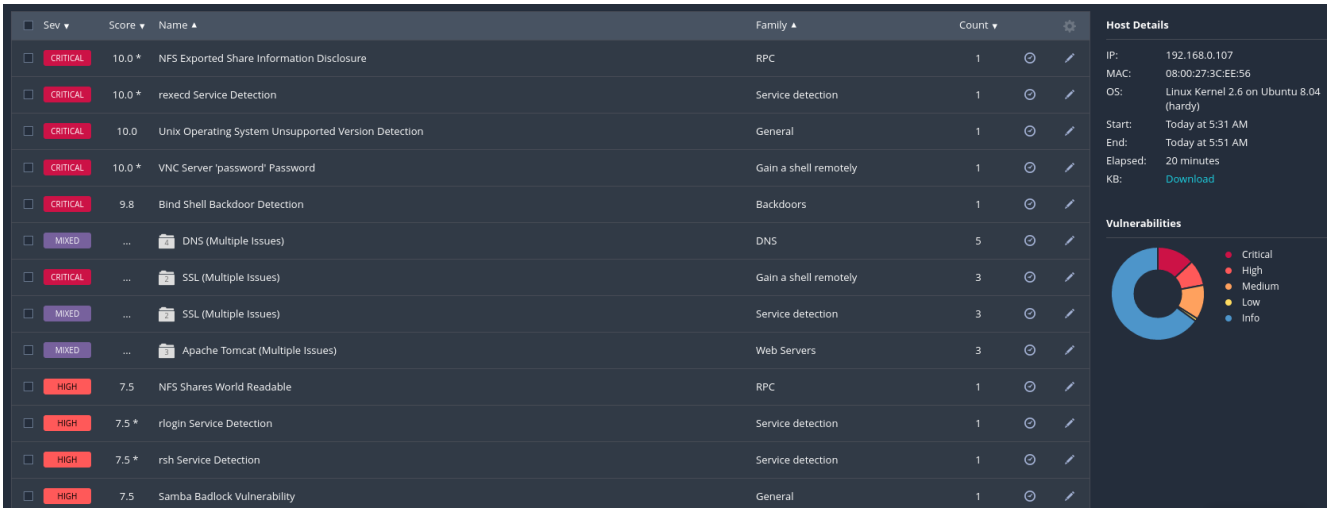



Рис. 2.8. Налаштування для Basic Network scan

Стандартний скан через мережу дозволяє використовувати різні плагіни для виявлення вразливостей. Якщо не вказувати, які плагіни використовувати під час сканування, то буде використаний стандартний набір плагінів, що у нашому випадку буде непогано, бо ми не знаємо які сервіси працюють на цьому хості.

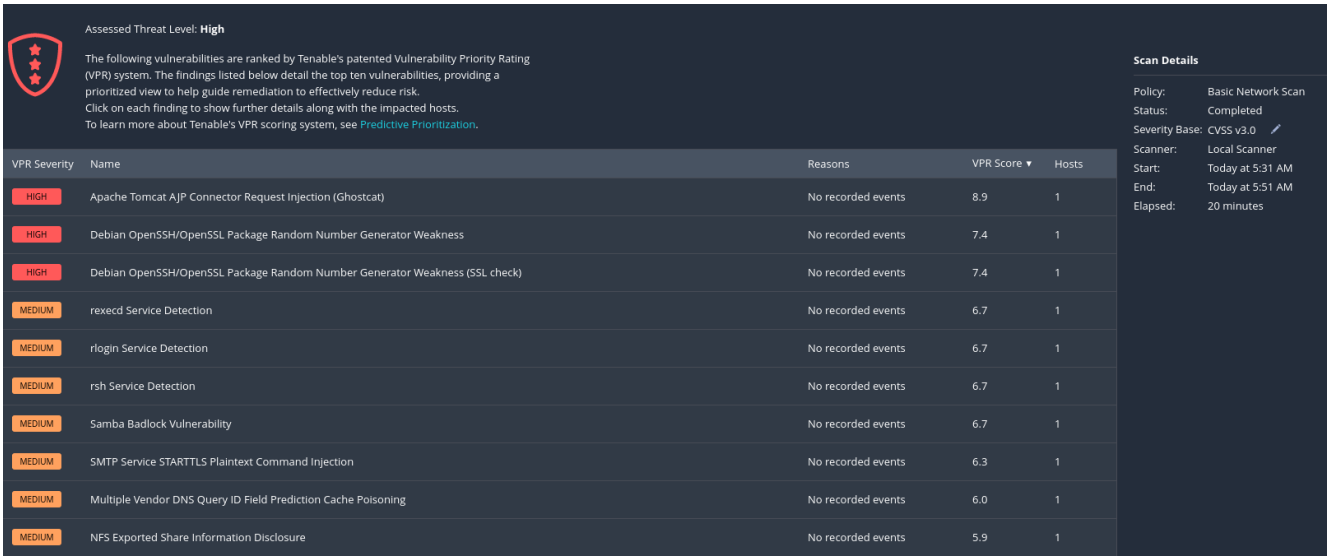


| Sev | Score | Name | Family | Count |
|---|---|---|---|---|
| CRITICAL | 10.0 * | NFS Exported Share Information Disclosure | RPC | 1 |
| CRITICAL | 10.0 * | rexecd Service Detection | Service detection | 1 |
| CRITICAL | 10.0 | Unix Operating System Unsupported Version Detection | General | 1 |
| CRITICAL | 10.0 * | VNC Server 'password' Password | Gain a shell remotely | 1 |
| CRITICAL | 9.8 | Bind Shell Backdoor Detection | Backdoors | 1 |
| MIXED | ... | DNS (Multiple Issues) | DNS | 5 |
| CRITICAL | ... | SSL (Multiple Issues) | Gain a shell remotely | 3 |
| MIXED | ... | SSL (Multiple Issues) | Service detection | 3 |
| MIXED | ... | Apache Tomcat (Multiple Issues) | Web Servers | 3 |
| HIGH | 7.5 | NFS Shares World Readable | RPC | 1 |
| HIGH | 7.5 * | rlogin Service Detection | Service detection | 1 |
| HIGH | 7.5 * | rsh Service Detection | Service detection | 1 |
| HIGH | 7.5 | Samba Badlock Vulnerability | General | 1 |



Рис. 2.9. Результат Basic Network scan для хоста Metasploitable2

Виконавши сканування ми бачимо діаграму типів вразливостей  за кількістю та критичністю.



Assessed Threat Level: **High**

The following vulnerabilities are ranked by Tenable's patented Vulnerability Priority Rating (VPR) system. The findings listed below detail the top ten vulnerabilities, providing a prioritized view to help guide remediation to effectively reduce risk.
Click on each finding to show further details along with the impacted hosts.
To learn more about Tenable's VPR scoring system, see Predictive Prioritization.

| VPR Severity | Name | Reasons | VPR Score | Hosts |
|---|---|---|---|---|
| HIGH | Apache Tomcat AJP Connector Request Injection (Ghostcat) | No recorded events | 8.9 | 1 |
| HIGH | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness | No recorded events | 7.4 | 1 |
| HIGH | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) | No recorded events | 7.4 | 1 |
| MEDIUM | rexecd Service Detection | No recorded events | 6.7 | 1 |
| MEDIUM | rlogin Service Detection | No recorded events | 6.7 | 1 |
| MEDIUM | rsh Service Detection | No recorded events | 6.7 | 1 |
| MEDIUM | Samba Badlock Vulnerability | No recorded events | 6.7 | 1 |
| MEDIUM | SMTP Service STARTTLS Plaintext Command Injection | No recorded events | 6.3 | 1 |
| MEDIUM | Multiple Vendor DNS Query ID Field Prediction Cache Poisoning | No recorded events | 6.0 | 1 |
| MEDIUM | NFS Exported Share Information Disclosure | No recorded events | 5.9 | 1 |



Рис. 2.10. Сортування знайдених вразливостей за CVSS v3.0

Також ми можемо подивитись на вразливості у порядку спадання критичності за базою CVSS v3.0.

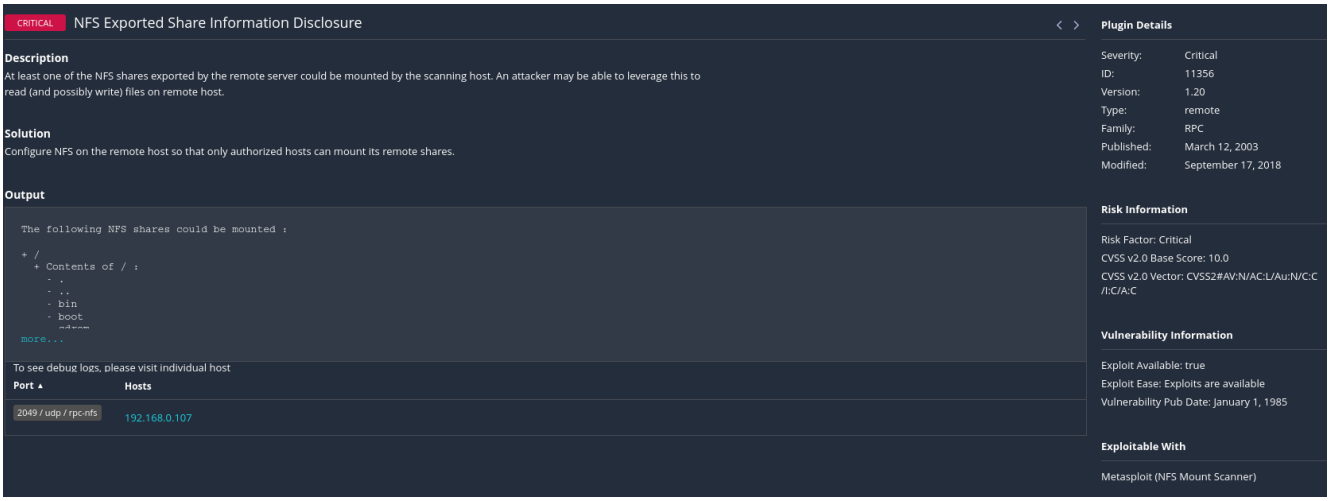



Рис. 2.11. Приклад звіту вразливості знайденої на Metasploitable2

Кожна з вразливостей у звіті є інтерактивною, і дає інформацію про вразливість та шляхи її застосування. Також ці сторінки мають інформацію про версію сервісу на якій ця вразливість з’являється, тип вразливості, дата публікації у відкритий доступ, та її критичність.

**Висновки до другого роділу**

Розглянуто переваги та недоліки рішень для управління вразливостями та наведено аргументи на користь рішення Nessus. Аналіз різних рішень показав, що Nessus характеризується високою точністю виявлення, швидкістю сканування та надійністю результатів. Обґрунтування вибору Nessus базується на його суттєвих перевагах, які роблять його оптимальним рішенням для управління вразливостями кінцевих точок Інтерфейс Nessus зручний і простий у використанні, зі зрозумілою навігацією. Nessus надає широкий спектр можливостей налаштування, що дозволяє адаптувати його до потреб конкретної організації. Nessus можна застосовувати для ефективного сканування та виявлення вразливостей кінцевих точок. Це дозволяє організаціям здобувати важливу інформацію про захищеність своїх систем.

# 3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ КІНЦЕВИХ ТОЧОК ІС ПІДПРИЄМСТВА НА БАЗІ РІШЕННЯ NESSUS

## 3.1. Налаштування рішення Nessus для управління вразливостями кінцевих точок

Щоб ефективно використовувати Nessus, ось кілька рекомендованих варіантів налаштування.

Сканування Nessus можна налаштувати так, щоб включати або виключати певні IP-адреси, порти або протоколи. Переконайтесь, що ви налаштували параметри діапазону, які відображають структуру мережі вашої організації і активи, які ви хочете перевірити. Це допоможе зберегти обчислювальні ресурси підприємства і зменшити вплив на критичні хости, які не включені в пул сканування.

Налаштуйте звіти, які генерує Nessus, щоб надати детальну інформацію про виявлені вразливості. Персоналізуйте звіти так, щоб у них відображалася інформація, важлива для зацікавлених сторін вашої організації.

Налаштуйте Сповіщення, щоб надсилати повідомлення на електронну пошту про вразливості високого рівня небезпеки або інші критичні події.

Постачальник також рекомендує кілька способів оптимізувати процедуру сканування.

Використовуйте фільтр вразливостей. Якщо вразливість неможливо виправити зараз, або це буде дорожче, ніж атака на цей ресурс, ви можете скористатися фільтром вразливостей. Це налаштування дозволяє підвищити ефективність сканування за рахунок видалення зі звіту уразливостей, які не становлять високої загрози по CVE, і видалення зі звіту уразливостей, які ви вкажете.

Налаштуйте процес сканування за допомогою використання пароля. Цей спосіб налаштування дозволяє виконувати сканування як внутрішній аудитор. Це налаштування допоможе вам

відповідати нормам і стандартам, які вимагають оцінки вразливостей із зазначенням облікових даних відповідно до стандартних вимог [13].

Важливо мати комплексне рішення для управління вразливостями, яке може забезпечити видимість всіх активів і вразливостей по всій поверхні атаки компанії, включаючи хмарні технології, операційні технології та контейнерні середовища. Традиційних сканерів для управління вразливостями може бути недостатньо для сучасного підприємства з динамічним мережевим середовищем.

Компанія Tenable - один з лідерів у сфері управління вразливостями, який пропонує комплексний підхід до управління вразливостями, включаючи виявлення та ідентифікацію активів, сканування та оцінку вразливостей, визначення пріоритетів та їх усунення, а також звітність про відповідність вимогам нормативно-правових актів. Nessus розроблений для забезпечення повної видимості поверхні атак підприємства, що дозволяє більш проактивно та ефективно управляти вразливостями. Також важливо регулярно проводити сканування корпоративних мереж для виявлення потенційних вразливостей і ризиків безпеки. Зловмисники постійно досліджують мережі на предмет вразливостей, які можна використати, тому компаніям важливо залишатися пильними та проактивними в управлінні вразливостями.

Вразливості в контексті бізнес ризиків - важливо мати рішення для управління ризиками, яке допоможе підприємствам зосередити свої зусилля на вразливостях, що становлять найбільшу ступінь ризику для їхнього бізнесу. Недостатньо просто виявити вразливості, підприємства повинні зрозуміти повний контекст кожної вразливості, щоб ефективно розставити пріоритети у своїх зусиллях по усуненню вразливостей.

Рішення для управління вразливостями від Tenable пропонує комплексний підхід, який включає оцінку критичності заражених активів, а також поточну та

ймовірну майбутню активність зловмисників. Ця інформація дозволяє підприємствам зосередити свої зусилля на вразливостях, які становлять найбільший ризик для їхнього бізнесу, і вжити рішучих заходів для зменшення цього ризику з найменшими зусиллями.

Розставляючи пріоритети в управлінні вразливостями, компанії можуть досягти більш результативного підходу до безпеки, знижуючи при цьому загальний бізнес-ризик. Такий підхід також дозволяє підприємствам більш доцільно розподіляти свої ресурси, гарантуючи, що найбільш критичні вразливості будуть усунуті в першу чергу.

Динамічно аналізуйте зміни на вашій поверхні атаки для безперервного та динамічного управління вразливостями. Ландшафт загроз постійно змінюється, і вразливості можуть з'явитися в будь-який момент, тому важливо мати систему управління вразливостями, яка може адаптуватися до цих змін в режимі реального часу.

Рішення для управління вразливостями від Tenable використовує автоматизацію машинного навчання для безперервного аналізу понад 20 трильйонів точок даних про загрози, вразливості та активи. Такий підхід дозволяє прогнозувати, які вразливості є найбільш важливими, надаючи компаніям практичну інформацію, що дозволяє їм зосередити свої зусилля на мінімізації найбільш значущих ризиків.

Постійно аналізуючи зміни у вразливостях, загрозах та критичності активів по всій поверхні атаки підприємства, Tenable може допомогти організаціям випереджати потенційні загрози та зменшити ризик порушення безпеки. Цей підхід також допомагає організаціям оптимізувати свої зусилля з управління вразливостями, гарантуючи, що вони усувають найбільш критичні вразливості в першу чергу.

Проактивне управління ризиками та прийняття стратегічних рішень підкреслює обмеження традиційних статичних рішень для управління вразливостями, які покладаються на дані в режимі реального часу і можуть

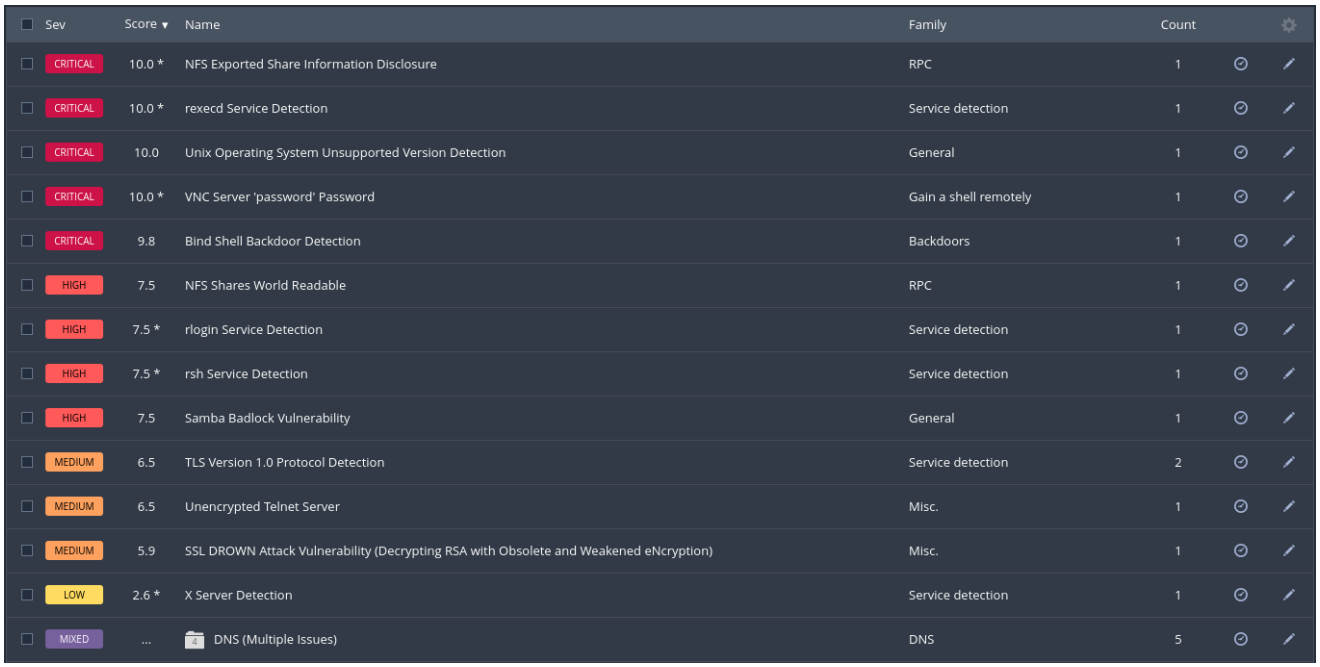
реагувати на нові експлойти або атаки нульового дня лише в міру їх виникнення. Такий реактивний підхід може зробити організації вразливими до нових і нових загроз і ускладнити ефективне визначення пріоритетів для ефективного управління вразливостями.

Nessus усуває ці обмеження, використовуючи моделі машинного навчання для автоматичного зіставлення даних про вразливості з ключовими контекстними елементами. Такий підхід забезпечує чітке розуміння того, що впливає на мережу організації в будь-який момент часу, що дозволяє приймати проактивні стратегічні рішення, які максимізують ефективність і результативність.

Постійно аналізуючи загрози, вразливості та дані про активи, Tenable може допомогти організаціям випередити потенційні загрози та зменшити ризик порушення безпеки. Цей проактивний підхід дозволяє підприємствам ефективно розставляти пріоритети в управлінні вразливостями, гарантуючи, що вони в першу чергу усувають найбільш критичні вразливості [15].

### 3.2. Результат сканування та виявлення вразливостей. Резюме проведеного дослідження

Результатом сканування є список виявлених вразливостей, який можна сортувати за критичністю, часом знаходження, оцінкою.



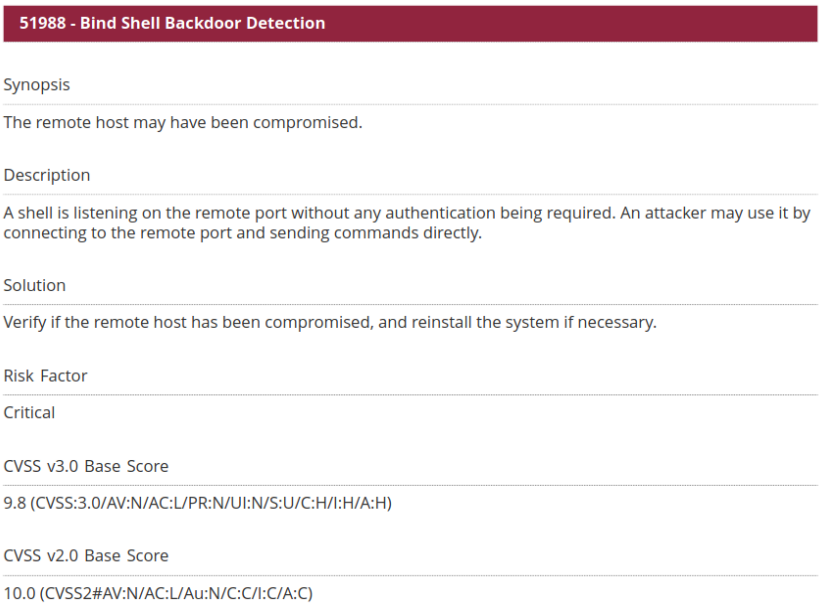
| Sev | Score ▾ | Name | Family | Count |
|---|---|---|---|---|
| CRITICAL | 10.0 * | NFS Exported Share Information Disclosure | RPC | 1 |
| CRITICAL | 10.0 * | rexecd Service Detection | Service detection | 1 |
| CRITICAL | 10.0 | Unix Operating System Unsupported Version Detection | General | 1 |
| CRITICAL | 10.0 * | VNC Server 'password' Password | Gain a shell remotely | 1 |
| CRITICAL | 9.8 | Bind Shell Backdoor Detection | Backdoors | 1 |
| HIGH | 7.5 | NFS Shares World Readable | RPC | 1 |
| HIGH | 7.5 * | rlogin Service Detection | Service detection | 1 |
| HIGH | 7.5 * | rsh Service Detection | Service detection | 1 |
| HIGH | 7.5 | Samba Badlock Vulnerability | General | 1 |
| MEDIUM | 6.5 | TLS Version 1.0 Protocol Detection | Service detection | 2 |
| MEDIUM | 6.5 | Unencrypted Telnet Server | Misc. | 1 |
| MEDIUM | 5.9 | SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) | Misc. | 1 |
| LOW | 2.6 * | X Server Detection | Service detection | 1 |
| MIXED | ... | DNS (Multiple Issues) | DNS | 5 |

Рис. 3.1. Перелік вразливостей знайдених на Metasploitable2 за критичністю

Серед вразливостей, знайдених в Metasploitable 2, є вразливості в програмному забезпеченні, такі як Apache, Samba, ProFTPD тощо, вразливості в операційних системах, такі як відсутність паролів адміністратора та слабка аутентифікація, а також вразливості в мережевих протоколах, таких як FTP, SSH та інші. Наприклад, у веб-сервері Apache була знайдена уразливість, яка дозволяє виконання коду на сервері, що може призвести до компрометації сервера та несанкціонованого доступу.

Деякі вразливості вважаються критичними через їхні потенційно серйозні негативні наслідки та ймовірність зловживання. Наприклад, вразливість, яка дозволяє зловмиснику отримати несанкціонований доступ до системи або виконувати код на віддаленому сервері, може бути використана для викрадення конфіденційної інформації, порушення роботи системи або встановлення додаткового шкідливого програмного забезпечення.

Згенерувавши PDF-документ з інформацією про сканування кінцевої точки, ми бачимо таку картину:



**51988 - Bind Shell Backdoor Detection**

Synopsis

The remote host may have been compromised.

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Risk Factor

Critical

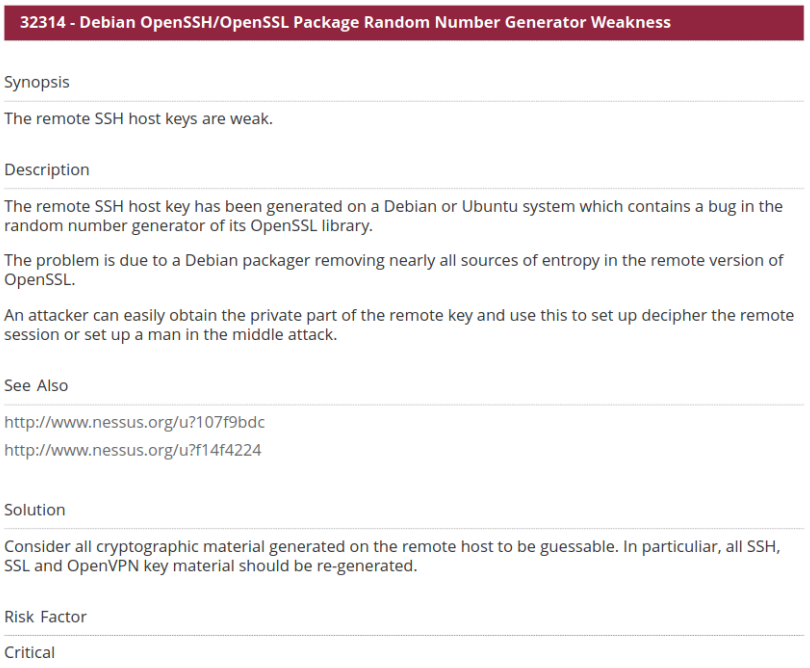
CVSS v3.0 Base Score

9.8 (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 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Рис. 3.2. Опис вразливості Bind Shell Backdoor Detection знайденої на Metasploitable2



**32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness**

Synopsis

The remote SSH host keys are weak.

Description

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

See Also

http://www.nessus.org/u?107f9bdc

http://www.nessus.org/u?f14f4224

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor

Critical

Рис. 3.3. Опис вразливості Debian OpenSHH/OpenSSL Package RNG weakness

Кожна з вразливостей отримує опис, важливі посилання для подальшого ознайомлення та спосіб виправлення. Також, цей документ надає оцінку вразливості за CVSS v2.0 – v 3.0, CVE, XREF.

Враховуючи кількість вразливостей та їх критичність, можна резюмувати, що на цьому хосту не оновлювалось програмне забезпечення понад 10 років, була проведена погана конфігурація системи, сервісів та привілеїв. Враховуючи, що цей сервер «спадковий», критичні вразливості будуть присутні через неможливість обновити або виправити програмне забезпечення. Неможливість настає після припинення підтримки від компанії постача, застаріння заліза серверу та залежності від іншого спадкового програмного коду.

Установа може не мати можливості прибрати або виправити застаріле програмне забезпечення, через те, що бізнес-процеси покладаються саме на це програмне забезпечення, бібліотеку або прошивку. В таких випадках кращим способом зменшення ризику буде додатковий шар оборони вразливих серверів [3].

Але треба розуміти, що залишати невиправлене програмне забезпечення, навіть якщо воно буде додатково захищено шифруванням, обмеженням доступу користувачів, обмеженим доступом до мережі, ризик компрометації залишається набагато більшим, ніж у нового програмне забезпечення, де вразливості ще не виявлені. В таких випадках рекомендується паралельно розроблювати більш сучасне програмне забезпечення та інтегрувати його до роботи, до повної заміни застарілого програмного забезпечення.

### 3.3. Розробка рекомендацій щодо управління вразливостями кінцевих точок ІС підприємства

*Регулярно скануйте кінцеві точки*: заплануйте регулярне сканування всіх кінцевих точок у вашій організації за допомогою Nessus для виявлення вразливостей. Це допоможе вам бути в курсі останніх патчів безпеки та виправлень.

*Пріоритезація вразливостей*: використовуйте Nessus для визначення пріоритетності вразливостей на основі їх критичності та потенційного впливу на

організацію. Це допоможе вам спершу зосередитися на найбільш критичних вразливостях і знизити ризик порушення безпеки.

*Усунення вразливостей*: після виявлення вразливостей використовуйте Nessus, щоб усунути їх, застосувавши патчі або інші виправлення. Переконайтеся, що ви перевірили ці виправлення, перш ніж розгортати їх у робочому середовищі.

*Моніторинг кінцевих точок*: постійно відстежуйте свої кінцеві точки за допомогою Nessus, щоб виявити будь-які нові вразливості чи загрози. Це допоможе вам бути проактивним і виявляти потенційні порушення безпеки до їх виникнення.

*Використовуйте плагіни Nessus*: Nessus пропонує різноманітні плагіни, які допоможуть вам визначити вразливі місця у ваших кінцевих точках спеціально під ваші потреби. Переконайтеся, що ви використовуєте ці плагіни, щоб отримати максимальну віддачу від Nessus, і переконайтеся, що ви виявили будь-які потенційні вразливості.

*Переглядайте звіти*: Регулярно переглядайте звіти, створені Nessus, щоб визначити тенденції та закономірності в управлінні вразливостями. Це допоможе вам визначити області, де можна покращити захист кінцевих точок.

*Навчіть свою команду*: переконайтеся, що ваша команда навчена ефективно використовувати Nessus для керування вразливими місцями. Це допоможе вам отримати максимальну віддачу від інструменту та забезпечити ефективний захист кінцевих точок.

Крім того можна ще додати рекомендації для сучасного підходу до проведення менеджменту з вразливостей з використанням Nessus

Одним із найефективніших способів зменшити поверхню атаки є впровадження надійного рішення для керування вразливістю. Таке рішення може допомогти виявити та визначити пріоритети вразливостей у мережі, системах і програмах вашої організації. Регулярно скануючи вразливості та застосовуючи виправлення та оновлення, організації можуть значно зменшити вплив кіберзагроз.

Для кращого управління вразливостями треба використовувати такі рекомендації:

Виявлення активів:

Швидкий скан це чудовий спосіб почати програму керування вразливістю. Перший важливий крок — запустити сканування, щоб виявити всі пристрої у вашій мережі. Отримавши вичерпний список пристроїв, ви зможете визначити пріоритети, які з них сканувати на вразливості в першу чергу, виходячи з їх критичності для вашого бізнесу та рівня впливу, який вони мають для зовнішнього світу.

Також важливо пам’ятати, що управління вразливістю має бути постійним процесом, а не одноразовою подією. Постійно виявляються нові вразливості, і в мережу регулярно додаються нові пристрої. Ось чому важливо планувати регулярне сканування та підтримувати ваше рішення для керування вразливостями в актуальному стані.

Частота сканування:

Важливо виконувати регулярне сканування вразливостей, щоб виявити будь-які прогалини в безпеці, які можуть існувати у вашому IT-середовищі. Частота цих сканувань залежатиме від розміру та складності мережі вашої організації, а також від типів систем і програм, які використовуються.

Багато організацій проводять сканування вразливостей щомісяця або щокварталу, але Центр безпеки Інтернету (CIS) рекомендує збільшити частоту принаймні до кожних двох тижнів або навіть щотижня. Це пояснюється тим, що постійно з’являються нові вразливості та нові загрози, а це означає, що чим більше часу проходить між скануваннями, тим уразливішими можуть стати ваші системи [4].

Пріоритезація активів:

Категоризація та пріоритезація активів на основі їх функцій є критично важливим кроком в управлінні вразливостями. Це дозволяє організаціям визначити

пріоритети своїх зусиль і зосередитися на захисті своїх найважливіших систем і даних.

Класифікуючи активи, важливо враховувати такі фактори, як функції системи, тип даних, які вона зберігає або обробляє, і їх важливість для бізнес-операцій. Наприклад, вебсервер, який зберігає конфіденційні дані клієнтів, імовірно, вважатиметься критичним активом, тоді як принтер або некритична робоча станція можуть мати не такий високий пріоритет.

Після того, як активи класифіковані, їх можна розставити за пріоритетністю залежно від рівня ризику, який вони становлять для організації, якщо вони скомпрометовані. Наприклад, критичні активи можуть вимагати більш частого сканування вразливостей, жорсткішого контролю доступу та більш ретельного тестування перед впровадженням будь-яких оновлень або виправлень. Це дозволяє організаціям ефективніше розподіляти ресурси та спершу усунути найбільш критичні вразливості, допомагаючи зменшити ризик успішної атаки.

Категоризуючи активи та встановлюючи пріоритети, організації можуть розробити більш цілеспрямований підхід до управління вразливістю, покращуючи загальну безпеку та зменшуючи ризик витоку даних або кібератак.

Запуск сканування:

Регулярне сканування систем на наявність вразливостей є важливою частиною підтримки надійної безпеки. Як ви згадали, більшість сканерів уразливостей дозволяють налаштувати профілі сканування, які збалансовують швидкість і глибину сканування вразливостей. Важливо вибрати профіль сканування, який відповідає потребам і цілям вашої організації.

Окрім регулярних перевірок, бажано проводити глибоку перевірку всіх пріоритетних активів. У цих скануваннях використовуються системні облікові дані та тести на вразливості, які взаємодіють з операційними системами та програмами, щоб надати більш детальні звіти про вразливості. Це допомагає виявити будь-які приховані або складні вразливості, які неможливо виявити стандартним скануванням, забезпечуючи повне уявлення про стан безпеки вашої організації.

Перегляд і виправлення:

При усуненні вразливостей важливо використовувати комплексний підхід. Це може включати застосування патчів або оновлень програмного забезпечення, зміну конфігурації систем або параметрів мережі або впровадження додаткових заходів безпеки для зменшення ризику, пов’язаного з уразливістю. Також важливо тестувати будь-які зміни чи оновлення перед впровадженням їх у робоче середовище, щоб уникнути небажаних наслідків [14].

**Висновки до третього розділу**

Налаштування Nessus вимагає вибору правильних параметрів сканування, включаючи визначення цільових кінцевих точок, типів сканування і налаштувань безпеки. Правильне налаштування робить Nessus надійним інструментом для пошуку вразливостей кінцевих точок. За допомогою Nessus ми змогли виконати ефективне сканування кінцевих точок і виявити безліч вразливостей. Цей огляд підкреслює важливість використання інструменту для виявлення вразливостей кінцевих точок як частини процесу управління вразливостями. Звідси випливає необхідність розробки рекомендацій щодо управління вразливостями кінцевих точок в корпоративних інформаційних системах. Врахування результатів сканування Nessus дозволяє розробити конкретні рекомендації щодо підвищення рівня безпеки кінцевих точок корпоративних інформаційних систем.

# ВИСНОВКИ

Досліджено використання Nessus як інструменту управління вразливостями інформаційної системи організації. Дослідження показали, що Nessus є потужним і ефективним інструментом для виявлення вразливостей в інформаційній системі, який можна використовувати для зниження ризиків безпеки.

Nessus забезпечує комплексне сканування IT-інфраструктури організації, виявлення вразливостей, якими можуть скористатися зловмисники. Він також надає рекомендації щодо виправлення, які можуть допомогти організаціям пом’якшити ці вразливості, перш ніж їх виправлять. Використання Nessus як інструменту керування вразливими місцями може допомогти організаціям підтримувати проактивний підхід до безпеки шляхом виявлення та виправлення вразливостей, перш ніж їх можна буде використати зловмиснику.

Підсумовуючи, Nessus є цінним інструментом, який можна використовувати для виявлення та керування вразливими місцями в інформаційній системі організації. Його ефективність полягає в його здатності сканувати та визначати вразливості, а також надавати рекомендації щодо виправлення. Організаціям, які віддають перевагу безпеці, слід розглянути впровадження Nessus як частину своєї стратегії управління вразливістю.

Попри те, що Nessus є цінним інструментом для виявлення та керування вразливими місцями в інформаційній системі організації, його не слід розглядати як повне рішення безпеки саме по собі. Натомість його варто використовувати в комбінації з іншими заходами безпеки, зокрема міжмережевими екранами, системи запобігання вторгнень і регулярними перевірками безпеки.

Використання Nessus може бути дуже ефективним, якщо дотримуватися таких рекомендацій, як визначення частоти сканування, що відповідає потребам установи, визначення пріоритету активів, що підлягають скануванню, та запуск сканувань у відповідному режимі, наприклад, вночі, коли система не

використовується. Належне використання цих рекомендацій може допомогти організаціям мінімізувати ризик порушення безпеки та забезпечити захист своїх інформаційних систем.

# ПЕРЕЛІК ПОСИЛАНЬ


1. Що таке керування вразливостями?. *Microsoft*. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-vulnerability-management (дата звернення: 21.05.2023).

2. 7 Cybersecurity Frameworks To Reduce Cyber Risk. *Cyber Risk Management Solutions | Bitsight*. URL: https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk (date of access: 21.05.2023).

3. 7 Ways to Protect Legacy Systems from Cyberthreats - Prescient Solutions. *Prescient Solutions*. URL: https://www.prescientsolutions.com/blog/7-ways-to-protect-legacy-systems-from-cyberthreats/ (date of access: 21.05.2023).

4. CIS Control 7: Continuous Vulnerability Management. *Netwrix Blog | Insights for Cybersecurity and IT Pros*. URL: https://blog.netwrix.com/2022/05/04/continuous-vulnerability-management/ (date of access: 21.05.2023).

5. Cost of a Data Breach report 2021. *IBM - Deutschland | IBM*. URL: https://www.ibm.com/downloads/cas/OJDVQGRY (date of access: 21.05.2023).

6. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. *Cybercrime Magazine*. URL: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (date of access: 21.05.2023).

7. Endpoint security Market Growth Drivers & Opportunities | MarketsandMarkets. *MarketsandMarkets*. URL: https://www.marketsandmarkets.com/Market-Reports/endpoint-security-market-29081235.html (date of access: 21.05.2023).

8. Metasploitable 2 | Metasploit Documentation. *Docs @ Rapid7*. URL: https://docs.rapid7.com/metasploit/metasploitable-2/ (date of access: 21.05.2023).

9. Nessus Competitive Comparison. *Tenable®*. URL: https://www.tenable.com/nessus/competitive-comparison (date of access: 21.05.2023).

10. Nessus has been deployed by more than one million users across the globe for vulnerability, configuration and compliance assessments. *Tenable*®. URL: https://www.tenable.com/sites/drupal.dmz.tenablesecurity.com/files/datasheets/NessusPro-(DS)-EN-v4.pdf (date of access: 21.05.2023).

11. Patil P. Different types of Vulnerability Classification. *Medium*. URL: https://systemweakness.com/different-types-of-vulnerability-classification-3b1cf6b0a413 (date of access: 21.05.2023).

12. sensei. Classification of Assets by Criticality. *Enhancing Your Business Performance*. URL: https://leanmanufacturing.online/classification-of-assets-by-criticality/ (date of access: 21.05.2023).

13. Tenable. 6 ways to optimize your Nessus scans. *Tenable*® URL: https://static.tenable.com/marketing/whitepapers/Whitepaper-6_Ways_to_Optimize_Your_Nessus_Scans.pdf (date of access: 21.05.2023).

14. Top 5 Vulnerability Management Best Practices. *IT Security and Compliance Software | New Net Technologies | NNT*. URL: https://www.newnettechnologies.com/top-5-vulnerability-management-best-practices.html (date of access: 21.05.2023).

15. Vulnerability Management: Five Steps to Cybersecurity Success. *Tenable*®. URL: https://www.tenable.com/solutions/vulnerability-management (date of access: 21.05.2023).

16. What is Endpoint Security? Why it's Crucial to Business | Avast. *Avast*. URL: https://www.avast.com/business/resources/what-is-endpoint-security (date of access: 21.05.2023).

# ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
## (ПРЕЗЕНТАЦІЯ)

Актуальність - Ключовим елементом кібербезпеки є управління вразливостями. Вразливості в інформаційних системах можуть створювати шляхи для несанкціонованого доступу та атак, що може призвести до втрати конфіденційності, цілісності та доступності даних.

Об'єкт дослідження - nessus як інструмент управління вразливостями в інформаційних системах.

Предмет дослідження - методи та засоби щодо управління вразливостями кінцевих точок інформаційної системи підприємства.

Мета дослідження - отримання характеристики ефективності ПЗ Nessus для менеджменту вразливостей інформаційних систем. Створення рекомендацій на основі дослідженого матеріалу.

Завдання дослідження

Встановити оптимальні налаштування ПЗ Nessus для проведення менеджменту вразливостей інформаційних систем. Проаналізувати результати 10 сканування на вразливість інформаційних систем.

Розкрити важливість використання політики менеджменту вразливостей для інформаційних системи.

Розкрити кращі практики та фреймворки для менеджменту вразливостей.

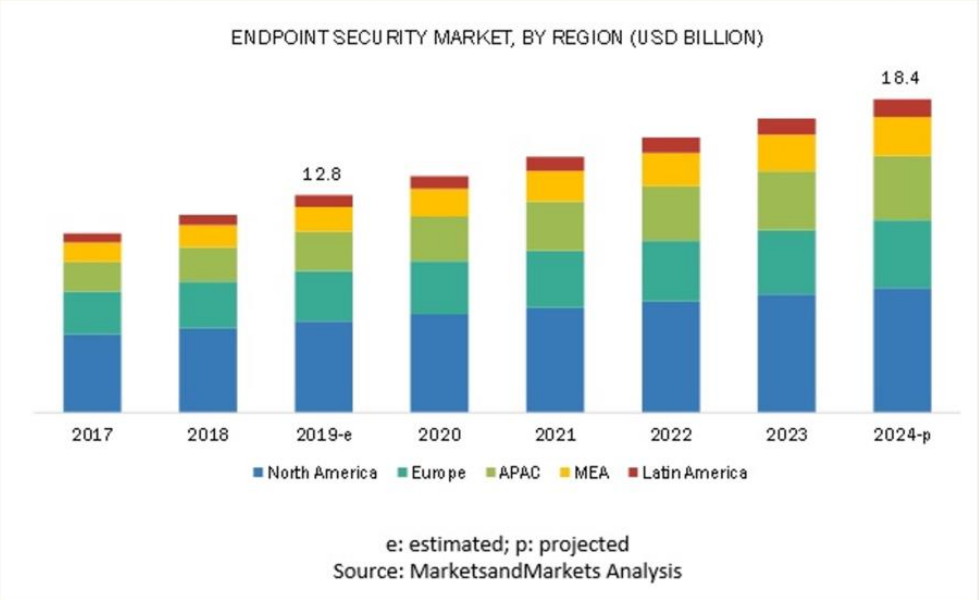
2

# Що таке управління вразливістю та чому це важливо

- Управління вразливістю – це процес виявлення, аналізу та управління виявленими загрозами та ризиками організації для запобігання негативних наслідків у разі їх реалізації. Він включає розробку стратегій, планування дій, реалізацію заходів щодо підвищення рівня захисту організації та зниження вразливості до можливих загроз.
- Важливість полягає в забезпеченні захисту від потенційних загроз і ризиків, що можуть призвести до витоку чутливої інформації, втрати даних, порушення функціонування систем і втрати репутації. Ефективне управління вразливістю дозволяє знизити ймовірність виникнення інцидентів безпеки, зменшити їх вплив та забезпечити стійкість організації до нових загроз і вразливостей, що можуть виникнути в майбутньому.

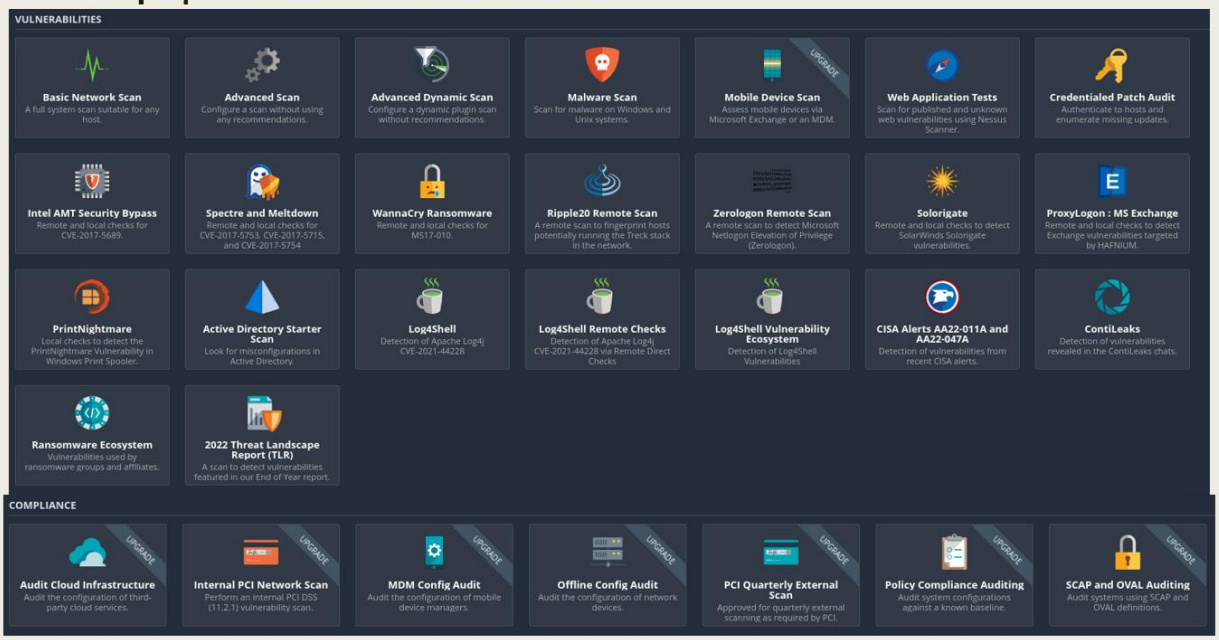
3

# Зростання ринку безпеки кінцевих точок






# Інтерфейс ПЗ Nessus



# Переваги інструментів сканування для керування вразливістю

- Визначає потенційні вразливості безпеки
- Дає комплексну оцінку загального стану безпеки організації
- Економить час і ресурси
- Дозволяє проактивну безпеку
- Допомагає визначити пріоритетність заходів безпеки
- Допомагає відповідати вимогам та аудиту
- Покращує загальну безпеку



# Недоліки інструментів сканування для керування вразливістю

- Може бути обмежений за обсягом і здатністю виявляти певні типи вразливостей
- Потрібна технічна експертиза
- Може бути ресурсомістким
- Може викликати збої
- Сканування вразливостей може надати обмежений контекст щодо фактичного ризику, створеного вразливістю
- Не розглядає основні проблеми, які призвели до вразливостей

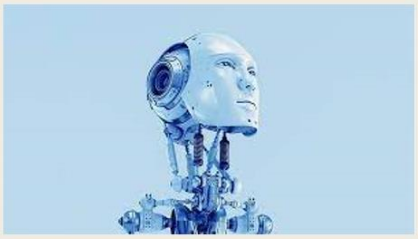
# Найкращі практики використання програми керування вразливістю

- Регулярно виконуйте сканування вашої мережі для виявлення нових вразливостей
- Розставляйте пріоритети вразливостей на основі їхньої критичності та можливості використання
- Використовуйте функцію авторизованого сканування Nessus, щоб отримати більш детальну інформацію про вразливості у ваших системах
- Інтегруйте Nessus з іншими інструментами безпеки, такими як SIEM, щоб оптимізувати вашу програму управління вразливостями.
- Переконайтеся, що ви використовуєте останню версію Nessus і що у вас встановлені найновіші плагіни.



# Нові тенденції в управлінні вразливостями

- Штучний інтелект та машинне навчання дозволяють краще виявляти вразливості та визначати їх пріоритетність
- Хмарне управління вразливостями для зменшення витрат і складності



# Висновки

- Використання Nessus може бути дуже ефективним, якщо дотримуватися таких рекомендацій, як визначення частоти сканування, що відповідає потребам установи, визначення пріоритету активів, що підлягають скануванню, та запуск сканувань у відповідному режимі
- Nessus є цінним інструментом, який можна використовувати для виявлення та керування вразливими місцями в інформаційній системі організації. Його ефективність полягає в його здатності сканувати та визначати вразливості, а також надавати рекомендації щодо виправлення.