МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ХАРЧОВИХ ТЕХНОЛОГІЙ

Інститут (факультет)_Автоматизації і комп'ютерних систем_____
Кафедра _Інформаційних систем_____

«До захисту в ЕК»	**«До захисту допущено»**
Директор інституту(декан факультету)	Завідувач кафедри
_____ __Андрій Форсюк_____	_____ __Сергій Чумаченко__
(підпис) (ім'я та прізвище)	(підпис) (ім'я та прізвище)
«___» _____ 2022р.	«___» _____ 2022р.

КВАЛІФІКАЦІЙНА РОБОТА
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ МАГІСТРА

зі спеціальності__122 «Комп'ютерні науки»_____
(код та назва спеціальності)
освітньо-професійної програми_Інформаційні управляючі системи та технології
_____
на тему:_Створення та дослідження системи вибору сканерів безпеки для виявлення вразливостей комп'ютерних систем_____

Виконав: здобувач_2_ курсу, групи ІС-2-3М

_____Андрійчук Тарас Юрійович_____ _____
(прізвище, ім'я, по батькові повністю) (підпис)

Керівник _Гуржій Андрій Миколайович_____ _____
(прізвище , ім'я та по батькові повністю) (підпис)

Консультанти_____ _____
(ім'я та прізвище) (підпис)

_____ _____
(ім'я та прізвище) (підпис)

_____ _____
(ім'я та прізвище) (підпис)

Рецензент Віктор Сідлецький _____
(ім'я та прізвище) (підпис)

Я як здобувач(ка) Національного університету харчових технологій розумію і підтримую політику університету з академічної доброчесності. Я не надавав(-ла) і не одержував(-ла) недозволеної допомоги під час підготовки цієї роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Здобувач_____
(підпис)

Київ - 2022р.

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ХАРЧОВИХ ТЕХНОЛОГІЙ

Інститут (факультет) __Автоматизації і комп'ютерних систем_____
Кафедра __Інформаційних систем_____
Освітній ступінь__магістр_____
Спеціальність__122 «Комп'ютерні науки»_____
(код і назва)
Освітньо-професійна програма __ Інформаційні управляючі системи та технології_____
(назва)

ЗАТВЕРДЖУЮ
Завідувач
кафедри Інформаційних систем

_____
"____" _____2022року

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧА

_____Андрійчука Тараса Юрійовича_____
(прізвище, ім'я, по батькові)

1. Тема роботи __Створення та дослідження системи вибору сканерів безпеки для виявлення вразливостей комп'ютерних систем_____
керівник роботи_Гуржій Андрій Миколайович_____,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від "11" листопада 2022 року №884-кс
2. Строк подання здобувачем роботи__7 лютого 2022 року_____
3. Вихідні дані до роботи *нормативно-правова база діяльності підприємства, інформація про сканери безпеки, дані про комп'ютерні системи*._____
4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)_ Дослідження наявних рішень для вирішення знайдених проблем та вибір наукових методів. Алгоритмізація обраних методів. Автоматизація і тестування методів та аналіз отриманих результатів. Техніко-економічний ефект._____
_____
_____
_____
_____
5. Перелік графічного матеріалу
_Схеми даних**,** системні форми._____
_____
_____
_____
_____
_____

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Гуржій А.М.		
2	Гуржій А.М.		
3	Гуржій А.М.		

7. Дата видачі завдання____11 листопада 2021_____

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів виконання кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Функціональне та концептуальне моделювання вибору сканерів безпеки для виявлення вразливостей комп'ютерних систем.	22.11.2021	
2	Дослідження наукових робіт з рішеннями проблемних задач.	13.12.2021	
4	Опис та порівняння наукових рішень для розуміння їх використання.	12.01.2022	
5	Автоматизація обраних наукових рішень.	22.01.2022	
6	Аналіз отриманих результатів.	27.01.2022	
7	Розрахунок очікуваного економічного ефекту від впровадження розробки.	30.01.2022	
8	Оформлення пояснювальної записки.	31.01.2022	
9	Розробка презентації.	03.02.2022	

Здобувач _____ ____Андрійчук Т. Ю._____
(підпис) (прізвище та ініціали)

Керівник роботи _____ _____Гуржій А. М._____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, загальним обсягом робота складає 91 сторінок, має 44 рисунків, 11 таблиць, 24 сторінки додатків. Список використаних джерел містить 31 найменувань і займає 3 сторінки.

Мета роботи – вирішення проблеми складності вибору сканера безпеки на існуючому різноманітті ринку шляхом реалізації програмного модуля, який допоможе у виборі найбільш підходящого сканера відповідно до параметрів та потреб інформаційної системи.

Важливість роботи - чинне законодавство зобов'язує проходити всіх власників інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, технічних і програмних засобів, які реалізують функції ТЗІ експертизу, тобто тестування системи. Тут стануть у нагоді сканери безпеки, адже їх можна використовувати для аналізу систем, тому і для експертизи і для сертифікації вони допоможуть, а дана дипломна робота допоможе з вибором цього сканера.

Короткий висновок - досліджено існуючі рішення сканерів безпеки інформаційних систем, детально розглянуто їх сильні та слабкі сторони, класифіковано результати. Ґрунтуючись на проведеному дослідженні розроблений програмний додаток вибору сканера безпеки відповідно до технологій та протоколів, які використовуються в інформаційній системі.

Рекомендації по використанню результатів роботи - розроблене програмне забезпечення є прототипом програмного модулю та не може бути використаний у комерційних цілях. Реальний проект потребує матеріальних вкладів та глибших досліджень.

Пропозиції про можливі напрямки розвитку чи продовження виконаних досліджень - програмний модуль є актуальним на момент написання диплому. Для подальшого використання потрібне проведення аналогічних досліджень для оновлення бази даних, адже розвиток інформаційних рішень не стоїть на місці.

Дослідження є тестовим, було порівняно кількість випробовуваних портів та розпізнаних сервісів, але сканери безпеки тестують ще й інші вразливості, тому для покращення слід розширити діапазон досліджень вразливостей.

Ключові слова: ІНФОРМАЦІЯ, БЕЗПЕКА, ВРАЗЛИВІСТЬ, СКАНУВАННЯ, ЗАГРОЗИ, ІДЕНТИФІКАЦІЯ, ПРОГРАМНІ ЗАСОБИ, ОПЕРАЦІЙНА СИСТЕМА, МЕРЕЖІ, ПОРТИ.

ЗМІСТ

УМОВНІ СКОРОЧЕННЯ

КСЗІ - комплексні системи захисту інформації

ІТС - інформаційно-телекомунікаційної системи

ТЗІ - технічний захист інформації

ОТР КСЗІ - організаційно-технічне рішення на розгортання типової складової компоненти КСЗ

СМІБ - системи менеджменту інформаційної безпеки

ЗАЗ - засоби аналізу захищеності

ПЗ - програмне забезпечення

СКБД - система управління базами даних

ВСТУП

Актуальність. Тенденція щодо встановлення мінімального рівня захищеності IT-середовища фактично визначила необхідність комплексного підходу – використання широкого спектра програмних засобів для підвищення рівня захищеності комп’ютерних мереж та систем.[1]

Захист інформації є однією з вічних проблем. Протягом історії людства способи розв'язання цієї проблеми визначались рівнем розвитку технологій. У сучасному інформаційному суспільстві технологія відіграє роль активатора цієї проблеми — комп'ютерні злочини стали характерною ознакою сьогодення. Комп'ютерними називають злочини, пов'язані з втручанням у роботу комп'ютера, і злочини, в яких комп'ютери використовуються як необхідні технічні засоби. Серед причин комп'ютерних злочинів і пов'язаних з ними викрадень інформації головними є такі: швидкий перехід від традиційної паперової технології зберігання та передавання інформації до електронної за одночасного відставання технологій захисту інформації, зафіксованої на машинних носіях; широке використання локальних обчислювальних мереж, створення глобальних мереж і розширення доступу до інформаційних ресурсів; постійне ускладнення програмних засобів, що викликає зменшення їх надійності та збільшення кількості уразливих місць. Сьогодні ніхто не може назвати точну цифру загальних збитків від комп’ютерних злочинів, але експерти погоджуються, що відповідні суми вимірюються мільярдами доларів.[2]

Питання підвищення рівня захищеності IT-середовища є сьогодні актуальним не лише для великих корпорацій, але й для невеликих організацій, як для потреб бізнесу, так і для навчальних установ.[3] Як правило, такі питання вимагають інвестування певної суми коштів на організацію програмно-апаратних засобів підвищення рівня захищеності IT-середовища, причому левова частка тих коштів виділяється на закупівлю ліцензій відповідних програмних продуктів. І якщо раніше організації часто використовували піратське програмне забезпечення (ПЗ), то зараз на фоні загального підвищення

рівня легального використання ліцензійного ПЗ чимала вартість таких програмних засобів є стримувальним чинником для багатьох організацій у їх використанні. У результаті захищеність даних та інфраструктури таких організацій залишається під питанням.

Випробування на проникнення є частиною аудиту безпеки, який повинна пройти кожна компанія, яка має на меті отримати сертифікати відповідності міжнародним стандартам ISO/IEC 27001:2005. [4]

Питання налаштування журналізації подій залежать від багатьох чинників, які впливають на кількість записуваних даних, їх деталізацію, час їх збереження, ранжування за критичністю подій тощо. Зокрема, зазначимо, що відомий міжнародний стандарт в галузі інформаційної безпеки ISO 27001:2005 [4] – прямий нащадок ISO/IEC 17799:2005 (який, своєю чергою, ґрунтувався на Британському стандарті BS 7799), передбачає журналізацію подій у системі, аналіз цих подій та потребу їх збереження. У пункті A.10.10.1 стандарту ISO 27001:2005 [4] вказується лише, що контрольні журнали, які записують діяльність користувачів, винятки та події в системі захисту інформації, повинні генеруватися і зберігатися протягом узгодженого періоду часу з метою допомогти у майбутніх розслідуваннях та в постійному контролі над управлінням доступом.

Дослідження дають зрозуміти, що сканери для багатьох компаній використовуються за принципом: “Купуємо для відповідності нормативним вимогам, використовуємо для підвищення рівня захищеності системи” [5]. Однією з найбільших помилок сьогодні під час використання сканерів є думка організацій про те, що, просто володіючи цим інструментом, організація вже відповідає вимогам стандартів чи вимогам аудиторів.

Тому сьогодні для виконання цього завдання буде доцільне використання найкращого програмного забезпечення. Власники програмних рішення сканування інформаційних систем зазвичай обіцяють повний захист вашої системи, але в дійсності це не зовсім так. Одна й та ж вразливість може бути не знайдена одним сканером, а інший її виявить [6]. Вразливості однакові, але

підходи до їх перевірки у кожного продукту різний, тому можна виділити, які саме сканери якнайкраще справляються з відповідним типом вразливостей. Як обрати найкращий сканер безпеки за мінімальну вартість, наприклад, якщо у вас не велика корпорація та бюджет досить обмежений. На вирішення цього питання й направлене дипломне дослідження.

Мета дипломної роботи - вирішення проблеми складності вибору сканера безпеки на існуючому різноманітті ринку шляхом реалізації програмного модуля, який допоможе у виборі найбільш підходящого сканера відповідно до параметрів та потреб інформаційної системи.

Досягнення мети потребує розв'язання таких **задач**:

1. дослідження застосування сканерів безпеки в інформаційних системах;
2. проведення порівняльного аналізу сканерів безпеки з метою виявлення їх переваг і недоліків;
3. опрацювання результатів, структурування даних та формування відносних коефіцієнтів;
4. створення програмного модуля автоматизованого вибору оптимального сканера безпеки згідно результатів тестування;

Об'єкт дослідження – процес захисту інформації за допомогою сканера безпеки інформаційних систем.

Предмет дослідження – методи та способи роботи сканерів безпеки інформаційних систем.

Оцінка сучасного стану проблеми на основі вітчизняної та зарубіжної літератури. Сьогодні відомо близько 85 продуктів класу SIEM-систем [7], кожна з яких заслуговує окремого аналізу. Серед списку з 85 позицій лише вісім належать до безкоштовних продуктів і тільки два з них належать до продуктів з відкритим кодом. [8]

Ще однією проблемою є те, що насправді ті організації, які переслідували мету лише відповідати нормативним вимогам, виявили, що вони не лише не відповідають цим вимогам, але й не є достатньо захищеними при цьому. Ті ж

організації, які зосередилися на питанні захищеності із використанням SIEM-систем, виявили, що вони підвищили свій рівень захищеності та відповідають нормативам.

Галузь застосування. Даний програмний комплекс має велике значення та значно полегшує життя корпорацій, які прагнуть оцінити ступінь захищеності інформаційних систем як для власного контролю потоку та обробки даних, так і для сертифікації.

Новизна. Запропоновано оцінка ефективності сканерів безпеки шляхом відносних коефіцієнтів та розроблено програмний модуль вибору сканера безпеки.

Практична цінність полягає у тому, що розроблений програмний модуль може бути використаний організаціями задля вибору сканера безпеки для перевірки захищеності інформаційних систем.

РОЗДІЛ 1. СУЧАСНІ ПІДХОДИ ЩОДО ОРГАНІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ

1.1. Сучасний стан використання засобів підвищення рівня захищеності IT-середовища

Сканери вразливостей дають змогу сканувати мережі, комп'ютери та програми на предмет виявлення можливих проблем у системі безпеки, оцінювати і рекомендувати усунення вразливостей.[9] Існує думка, що сканери під час виявлення окремих потенційних вразливостей виконують злам системи, використовуючи отриману інформацію та відповідні програми-експлоїти. Насправді на цьому етапі застосовуються інші системи – системи тестування на проникнення, які на основі знайденої сканерами вразливостей інформації моделюють атаки зловмисників, використовуючи при цьому активний аналіз системи на наявність потенційних вразливостей. Ці вразливості, своєю чергою, можуть спровокувати некоректну роботу цільової системи, або повну відмову в обслуговуванні.[10] Аналіз ведеться з позиції потенційного атакуючого і може включати активне використання вразливостей системи. Результатом роботи є звіт, який містить усі знайдені вразливості системи безпеки, а також може містити рекомендації щодо їх усунення. Мета випробувань на проникнення – оцінити його можливість здійснення і спрогнозувати економічні втрати в результаті успішного здійснення атаки.[11] Випробування на проникнення є частиною аудиту безпеки, який повинна пройти кожна компанія, яка має на меті отримати сертифікати відповідності міжнародним стандартам ISO/IEC 27001:2005, що описує методи захисту та системи менеджменту захисту інформації в інформаційних технологіях.

1.2. Актуальність обраної теми

Під інформацією цей Закон розуміє документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі.

Інформаційна діяльність - це сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави.[12]

Сканери безпеки слугують гарними помічниками для дослідження інформаційних систем. Їх можна використовувати для отримання сертифікації та для проведення державної експертизи, використовуючи звіти, які були сформовані сканерами безпеки. Це значно полегшує процес проходження сертифікації.

Державна експертиза у сфері технічного захисту інформації проводиться з метою дослідження, перевірки, аналізу та оцінки об'єктів експертизи щодо їх відповідності вимогам нормативних документів із технічного захисту інформації та можливості їх використання для забезпечення технічного захисту інформації.[13]

Об'єктами експертизи є:

- КСЗІ, які є невід'ємною складовою інформаційної, телекомунікаційної або інформаційно-телекомунікаційної системи ;
- технічні та програмні засоби, які реалізують функції ТЗІ та/або оцінки стану захисту інформації ;
- організаційно-технічне рішення на розгортання типової складової компоненти КСЗІ в ІТС - задокументоване уніфіковане рішення для багаторазового розгортання складових КСЗІ в ІТС або КСЗІ типової складової компоненти КСЗІ в ІТС, самодостатньої для вирішення певного завдання, що включає проектні рішення програмно-технічного комплексу, організаційно-технічні рішення щодо регламенту функціонування типової компоненти ІТС та опис (алгоритм) процедури впровадження.

Існує декілька видів експертизи:

- Первинна експертиза є основним видом експертизи і передбачає виконання Організатором усіх потрібних заходів, визначених у розділі II цього Положення, для підготовки та прийняття рішення щодо об'єкта експертизи.
- Додаткова експертиза проводиться стосовно об'єктів експертизи, щодо яких відкрилися нові наукові та науково-технічні обставини, а також у зв'язку із закінченням строку дії документів, що засвідчують результати експертизи.
- Контрольна експертиза проводиться іншим Організатором з ініціативи Замовника у разі наявності у нього обґрунтованих претензій до висновку первинної чи додаткової експертизи або з ініціативи Адміністрації Держспецзв'язку для перевірки висновку первинної чи додаткової експертизи. [12]

Суб'єктами експертизи є:

- юридичні та фізичні особи - власники (розпорядники) інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, технічних і програмних засобів, які реалізують функції ТЗІ, - замовники експертизи ;
- Адміністрація Держспецзв'язку;
- територіальні органи Адміністрації Держспецзв'язку, які проводять експертизу шляхом аналізу декларацій про відповідність комплексних систем захисту інформації вимогам нормативних документів із ТЗІ;
- навчальні заклади, науково-дослідні, науково-виробничі установи Державної служби спеціального зв'язку та захисту інформації України, підприємства, установи та організації, які проводять експертизу;
- державні органи, які проводять експертизу у сфері свого управління;
- фізичні особи, які на постійній або професійній основі здійснюють діяльність, пов'язану з наданням експертних послуг, - виконавці експертних робіт з ТЗІ.

Захист даних в комп'ютерних мережах стає однією з найбільш відкритих проблем в сучасних інформаційно-обчислювальних системах.

Стандарт встановлює вимоги до розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та вдосконалення документованої СМІБ в контексті існуючих бізнес-ризиків організації.

Стандарт ISO 27001[14] визначає інформаційну безпеку як: «збереження конфіденційності, цілісності та доступності інформації; крім того, можуть бути включені і інші властивості, такі як справжність, неможливість відмови від авторства, достовірність ».

Конфіденційність - забезпечення доступності інформації тільки для тих, хто має відповідні повноваження (авторизовані користувачі).

Цілісність - забезпечення точності і повноти інформації, а також методів її обробки.

Доступність - забезпечення доступу до інформації авторизованим користувачам, коли це необхідно (на вимогу).

Для розробки СМІБ організація повинна виконати наступні кроки:

1. Визначити область застосування СМІБ.
2. Розробити Політику інформаційної безпеки.
3. Визначити (розробити) підхід до оцінки ризиків.
4. Ідентифікувати ризики.
5. Проаналізувати і оцінити ризики.
6. Прийняти рішення по обробці ризиків:
    a. застосувати до ризику відповідні засоби управління;
    b. прийняти ризик відповідно до розроблених критеріїв прийняття ризиків;
    c. піти від ризику (уникнути ризику);
    d. передати ризик іншій стороні (наприклад, страхової компанії, постачальника).

7. Вибрати засоби управління, які можна застосувати для зменшення ризиків. При виборі засобів управління повинні враховуватися критерії прийняття ризиків, законодавчі вимоги, договірні вимоги.
8. Отримати згоду керівництва по залишковим ризикам.
9. Підготувати Положення про застосовність - один з обов'язкових документів СМІБ.

Першим кроком на шляху до мінімізації реалізації загроз є постійний моніторинг мереж. Його можна здійснювати різними способами і найбільш поширений - це використання відповідних програм. Ці програми отримали назву сканери або ж сканери безпеки. Такий шлях вирішення питання досить зручний, адже сканери досить автоматизовані і економлять наш час.

ЗАЗ або сканери безпеки, призначені для автоматизації роботи адміністратора безпеки шляхом пошуку потенційних порушень політики безпеки та вразливостей ОС. При цьому ЗАЗ можуть виявляти такі види порушень (вразливості)[15]:

·“люки” (back door) в программах и программе типу “троянський кінь”;

·слабкі паролі й неправильні налаштування механізмів автентифікації;

·сприйнятливість до проникнення внаслідок неявних довірчих відносин між системами;

·сприйнятливість до атак на відмову в обслуговуванні;

·неправильні налаштування міжмережевих екранів, мережевих і прикладних сервісів;

·нездатність засобів захисту системи адекватно реагувати на спроби збору інформації;

Левова частка підприємств та організацій не здійснює моніторинг систем цілодобово, 7 днів в тиждень, цілий рік.[16] Ця ситуація може бути неприпустимою у системах з підвищеними вимогами до захисту інформації, до систем з високою відмовостійкістю тощо. Хіба що будуть застосовані найсучасніші системи управління інформацією та повідомленнями безпеки - сканери безпеки. У цьому випадку стає можливим централізований онлайн-

моніторинг подій з різноманітних джерел – операційних систем, прикладних сервісів, мережевих пристроїв тощо у режимі реального часу, кореляція результатів, надання звітів, ранжування за критичністю сервісів, нотифікація/попередження користувачів за настання певних подій, що дає змогу забезпечити відповідальний персонал та користувачів системи повною інформацією про її стан і тим самим забезпечити можливість ефективно управляти ризиками системи. [17]

1.3. Проведення опитування для оцінки актуальності теми

Для кращого розуміння актуальності обраної теми, можна привести таку характеристику, отриману при опитуванні користувачів порталу habr.com. [18]

На запитання про використовувані сканерах безпеки у своїх організаціях, переважна більшість респондентів відповіло, що вони використовують хоча б один сканер безпеки (70%). При цьому в організаціях, які практикують регулярне застосування сканерів безпеки для аналізу захищеності своїх інформаційних систем, воліють використовувати більше одного продукту даного класу. 49% респондентів відповіло, що в їхніх організаціях використовується два і більше сканера безпеки.

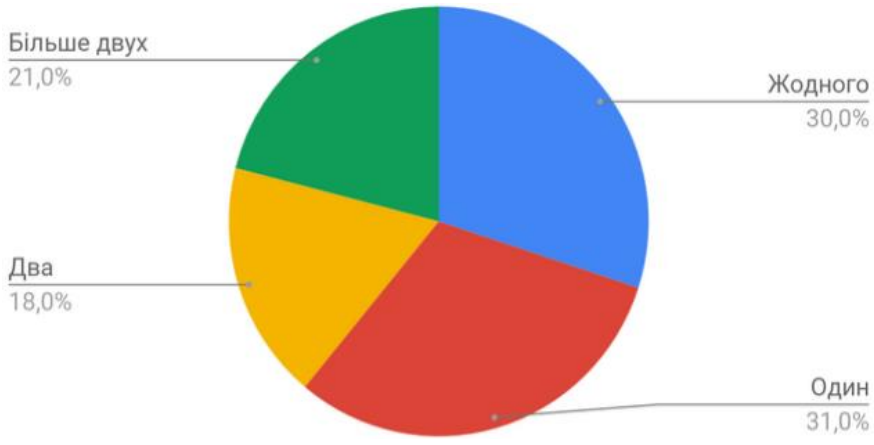


Рис. 1.1. Розподіл організацій опитаних респодентів за кількістю використовуваних сканерів безпеки

Відповідаючи на питання, для яких цілей використовуються спеціалізовані сканери безпеки, більшість респондентів відповіло, що вони використовуються

в якості додаткових інструментів аналізу захищеності Web-додатків (68%). На другому місці, виявилися спеціалізовані сканери безпеки СУБД (30%), а на третьому (2%) утиліти власної розробки для вирішення специфічного кола завдань з аналізу захищеності інформаційних систем.

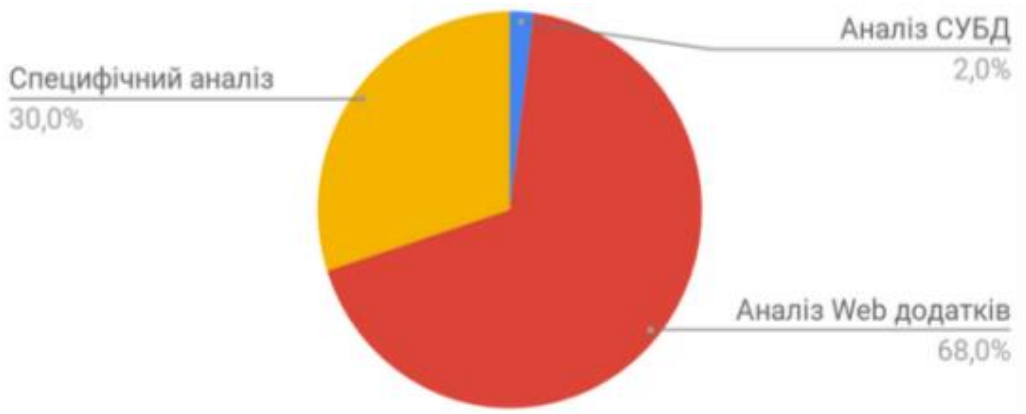


Рис. 1.2. Цілі застосування спеціалізованих сканерів безпеки в організаціях опитаних респондентів

Результат опитування респондентів про кінцеві продукти, які мають відношення до сканерів безпеки, показав, що більшість організацій воліють використовувати продукт Positive Technologies XSpider (31%) і Nessus Security Scanner (17%).

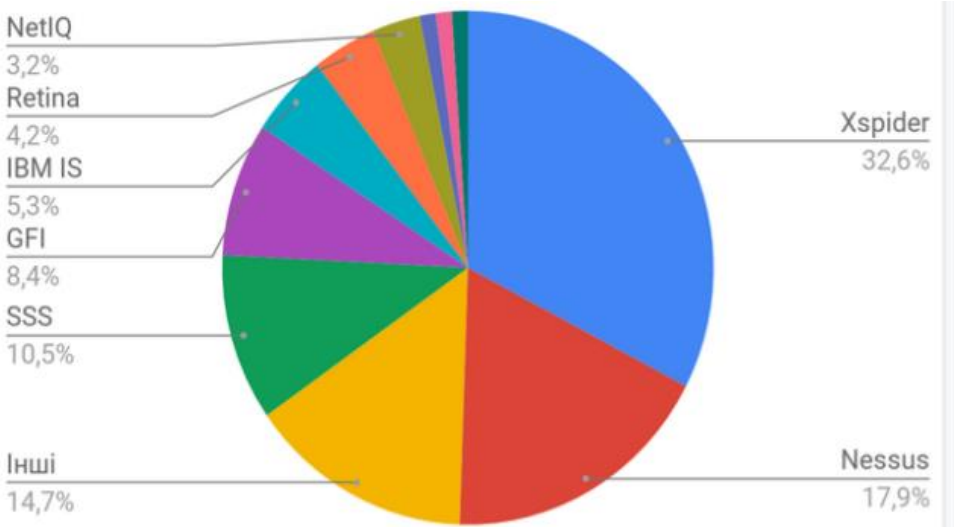


Рис. 1.3. Використовувані сканери безпеки в організаціях опитаних респондентів

Наступне питання, «Які механізми сканування ви застосовуєте?». Відповідь на це запитання дає кругова діаграма, яка показує для вирішення яких завдань застосовуються сканери безпеки.

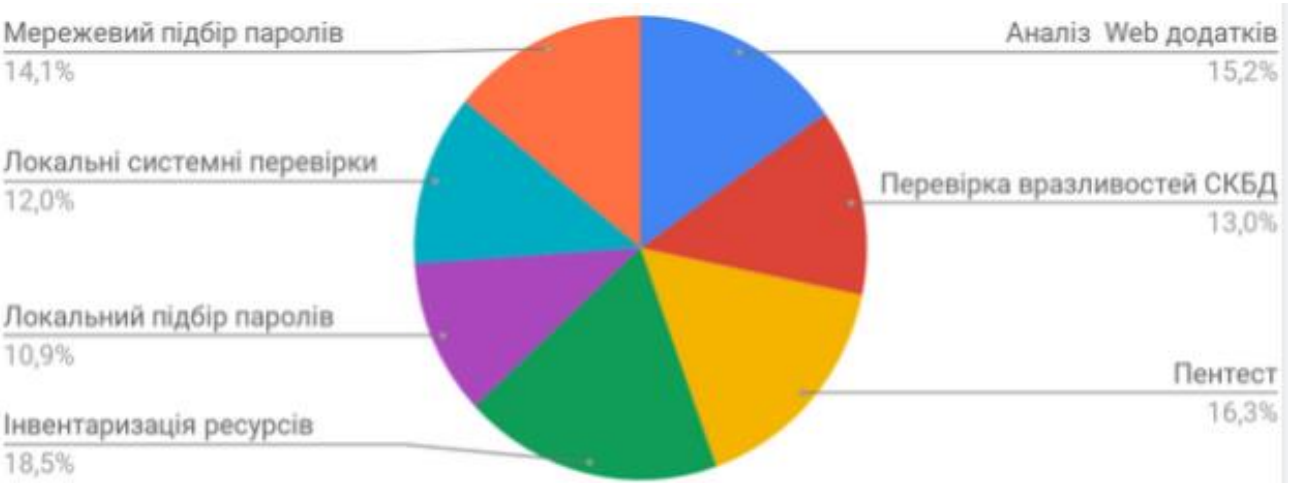


Рис. 1.4. Застосовувані механізми сканування

Нарешті, відповіді на останні два питання характеризують ситуацію із завданням контролю відповідності стандартам (внутрішньокорпоративних або міжнародним). Це завдання поки не типове для сканерів безпеки, але останнім часом все більш і більш актуальне.

Ось як розподілилися відповіді на питання «Чи існують в організації стандарти по безпечному налаштуванню систем і додатків? ».

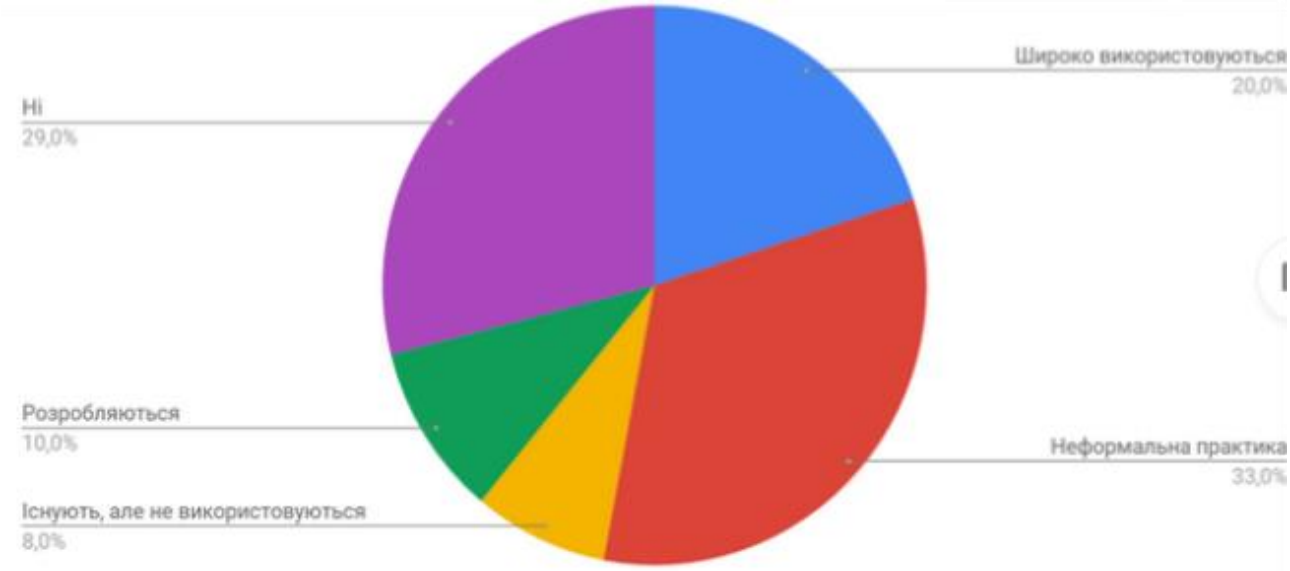


Рис. 1.5. Розподіл організацій за наявності стандартів щодо безпечного налаштування систем і додатків

Тобто в більшості випадків (71%) тобто робляться спроби відповідати хоч якомусь стандарту.

А ось на питання «Чи використовуються в організації засоби автоматизації контролю відповідності стандартам по безпечної налаштування систем і додатків?» більшість респондентів (56%) відповіли негативно.

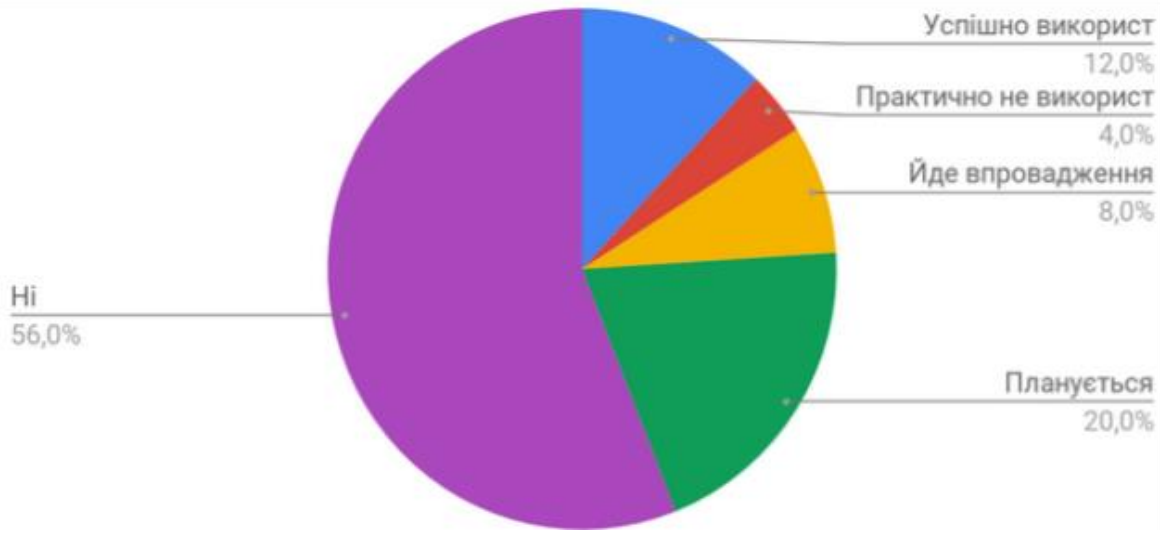


Рис. 1.6. Розподіл організацій за наявності систем контролю стандартів щодо безпечного налаштування систем і додатків

1.4. Принцип роботи сканерів безпеки

ЗАЗ можуть здійснювати сканування системи як “ззовні”, з використанням для доступу до системи мережевих засобів (network-based), так і “зсередини”, працюючи безпосередньо на хості, який аналізують (host-based, application-based). Як правило, мережеві сканери також здатні здійснювати сканування локальної системи через “зворотний” інтерфейс (127.0.0.1).

Для мережевих ЗАЗ існують дві групи способів виявлення вразливостей – сканування й зондування.[19]

Сканування (banner check) – механізм пасивного аналізу, використовуючи який сканер намагається визначити існування вразливості за непрямими ознаками без фактичного підтвердження її наявності. Цей метод є найшвидшим і найпростішим для реалізації. Цей процес ідентифікує відкриті порти, що

знайдені на кожному мережевому пристрої, і збирає пов'язані з портами заголовки (banner), знайдені під час сканування кожного порту. Аналіз заголовків дозволяє ідентифікувати операційну систему й використовувані сервіси аж до конкретної версії. На підставі апріорних знань про наявність вразливостей в тій чи іншій версії ПЗ робиться висновок про наявність або відсутність вразливості в системі, яку аналізують.

Варто зазначити, що певна функціональність щодо аналізу заголовків включається навіть в ПЗ, яке призначене лише для сканування мереж (як розглянутий у попередній роботі Nmap). ПЗ, що спеціально призначене для пошуку вразливостей, обов'язково має базу даних щодо вразливостей, і механізми її оновлення.

Зондування (active check) – механізм активного аналізу, який дозволяє впевнитись, чи присутня вразливість на вузлі, що аналізують. Зондування виконується шляхом емітування атаки, що використовує вразливість, яку перевіряють. Цей метод повільніший, чим сканування, але майже завжди значно точніший. Цей процес використовує інформацію, що була отримана в процесі сканування, для детального аналізу кожного мережевого пристрою.

Наприклад, в ході сканування можна отримати відомості про відкриті TCP порти №№ 135, 139. Це ознака використання в мережі служби NetBIOS. При цьому можна одразу підозрювати численні вразливості, притаманні системам Windows і протоколу NetBIOS. Далі логічною є взаємодія з системою за протоколом NetBIOS для вивчення наявності загальнодоступних (*shared*) ресурсів, захищеності цих ресурсів паролем. При цьому можна отримати відомості про користувачів системи, наявність можливості адміністрування системи через мережу, тощо. За цими даними можна отримати детальні й достатньо достовірні відомості про наявність вразливостей.

Також під час зондування можуть використовуватись відомі методи реалізації атак для того, щоб остаточно підтвердити або спростувати наявність тих вразливостей, які припускаються за результатами сканування, а також виявити інші вразливості, які не можуть бути виявлені пасивними методами, як,

наприклад, нестійкість до атак типу “відмова в обслуговуванні” (“denial of service”).[20]

Серед сканерів вразливостей можна виділити:

- сканер портів
- Сканери, що досліджують топологію комп'ютерної мережі
- Сканери, що досліджують вразливості мережевих сервісів
- Мережеві «черв'яки»
- CGI-сканери («дружні» — допомагають знайти вразливі скрипти)

Необхідною складовою сканера безпеки є система підготовки звітів. Оскільки основним призначенням цього ПЗ є надання інформації системним адміністраторам, доброю ознакою якості програми є її здатність не лише виявляти вразливості, але й надавати рекомендації з їх усунення.

Практично будь-який сканер проводить аналіз захищеності у п’ять етапів.

1. Збирання інформації про мережу. На даному етапі всі активні пристрої ідентифікуються у мережі і визначаються запущені на них сервіси і домени. У випадку використання систем аналізу захищеності на рівні операційної системи даний етап пропускається, оскільки на кожному вузлі, що аналізується встановлені відповідні агенти системного сканера.

2. Виявлення потенційних вразливостей. Сканер використовує описану базу даних для порівняння зібраних даних з відомими вразливостями за допомогою перевірки заголовків чи активних зондувальних перевірок. У деяких системах всі вразливості ранжуються за ступенем ризику. Наприклад, у системах Netsonar вразливості поділяються на два класи: мережеві та локальні. Мережеві вразливості (наприклад, ті, що діють на маршрутизатори) вважаються більш серйозними порівняно з вразливостями, характерними тільки для робочих станцій. Аналогічно і в Internet Scanner всі вразливості поділяються на три ступені ризику: високий (high), середній (Medium), низький (Low).

3. Підтвердження виявлених вразливостей. Сканер використовує спеціальні методи і моделює (імітує) визначені атаки для підтвердження факту наявності вразливостей на вибраних вузлах мережі.

4. Генерування звітів. На основі зібраної інформації система аналізу захищеності створює звіти, які описують виявлені вразливості. У деяких системах (наприклад, Internet Scanner і Netsonar) звіти створюються для різних категорій користувачів, починаючи з адміністраторів мережі і закінчуючи керівництвом компанії. Якщо перших більше цікавлять технічні деталі, то для керівництва компанії треба надати гарно оформлені з застосуванням графіків і діаграм звіти з мінімумом подробиць. Немаловажним аспектом є наявність рекомендацій для ліквідації виявлених проблем. І тут лідером є система Internet Scanner, яка для кожної вразливості вміщує покрокові інструкції з ліквідації вразливостей, специфічні для кожної операційної системи. Часто звіти також містять посилання на FTP- чи Web-сервери, що мають patch і hotfix, які ліквідують виявлені вразливості.

5. Автоматична ліквідація вразливостей. Цей етап зрідка реалізується у мережевих сканерах, але широко застосовується у системних (наприклад, System Scanner). При цьому дана можливість може реалізуватись по-різному. Наприклад, у System Scanner створюється спеціальний сценарій (fix script), який адміністратор може запустити для ліквідації вразливості. Одночасно зі створенням цього сценарію, створюється і інший, який анулює зміни. Це необхідно, коли після ліквідації проблеми нормальне функціонування вузла було порушено. У інших системах можливості „відкату” не існує.

1.5. Методологія тестування на проникність

Один із заходів, що проводяться в ході контролю стану защіщѐнності систем - це так званий тест на проникнення або на стійкість до злому.

Методологія тестування мережі на стійкість до злому (Тестування на проникнення, Penetration Testing або Ethical hacking) має на увазі, що суб'єкт, що виконує оцінку, спирається на власне розуміння того, як реалізована тестована система. він володіє мінімумом інформації про об'єкт тестування, тому іноді такий тест називають «Методом чѐрного ящика». Мета такого тесту - пошук

способів отримання доступу до системи з допомогою інструментів і засобів, використовуваних порушниками.

Докладне обговорення цієї методології виходить за рамки даної дипломної роботи, далі наведені лише короткі коментарі до кожного етапу.

У процесі планування визначаються цілі та завдання тесту. Обумовлюються умови, список допустимих технік, формується перелік об'єктів тестування

Рис. 1.7. Схема тестування на стійкість до злому

Наступний етап - збір інформації. На цьому етапі використовуються різні методи збору інформації про мережу, наприклад, ідентифікація доступних мережевих пристроїв, ідентифікація топології мережі, ідентифікація відкритих портів і т. д.

Далі слідує процес ідентифікації вразливостей. Тут використовується зібрана раніше інформація про вузли, операційні системи, сервіси, додатки. Головним чином використовується інформація про сервіси, їх версіях, а також

про додатки, що реалізують зазначені сервіси. Ця інформація зіставляється з інформацією про відомі вразливості, тобто з будь-якими базами вразливостей.

Останній етап - підтвердження (верифікація) вразливостей, про наявність яких були зроблені припущення на попередньому етапі. Цей етап можна назвати основним у розглянутій методології. По суті, на цьому етапі ілюструється можливість отримання доступу до системи.

Як показує практика, повністю автоматизувати процедуру тестування на стійкість до злому неможливо. Що стосується мережевих сканерів безпеки, то вони можуть бути використані для автоматизації процесів збору інформації та ідентифікації вразливостей. Крім того, звіти сканера безпеки можуть бути включені в загальний звіт по проведеному тесту.

1.6. Висновки до першого розділу.

Отже, було досліджено застосування сканерів безпеки в інформаційних системах, шляхом опитування та опрацювання законодавчих документів, що дало змогу виявити те, що використання сканерів безпеки є досить актуальним на даний час. Проаналізувавши існуючі типи сканерів, принципи їх роботи, особливості та характеристики можна зробити висновок, що сканери безпеки є гарним способом для проведення аналізу захищеності систем, формування звітів. Досить важливою та основною частиною тестування є тестування відкритих портів. Тому далі буде досліджений саме цей тип тестування.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ СКАНЕРІВ БЕЗПЕКИ. ЇХ ПОРІВНЯННЯ ТА АНАЛІЗ ДАНИХ

2.1. Умови порівняння: Налаштування сканерів

2.1.1. Ідентифікація вузлів

Для ідентифікації вузлів були задіяні методи ICMP Ping і TCP Ping.[21] Наприклад, на рис 2.1 наведені відповідні налаштування для сканера Nessus.

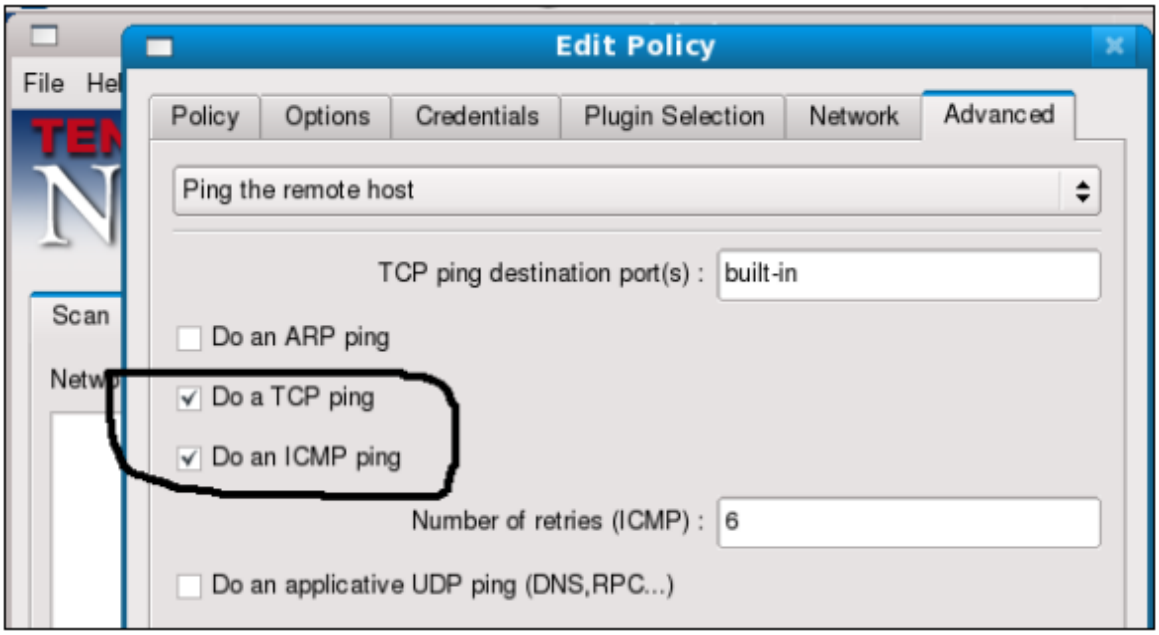


Рис 2.1. Ввімкнення методів ідентифікації вузлів на сканері Nessus

Для методу TCP Ping використовувався наступний перелік портів:

21, 22, 23, 25, 53, 80, 110, 111, 113, 135, 139, 143, 389, 443, 445, 563, 636, 990, 993, 995, 1521, 1723, 1433, 3128, 3306, 3372, 3389, 4899, 5432, 8080.

Наприклад, область відповідних налаштувань сканера Internet Scanner приведена на рис 2.2.

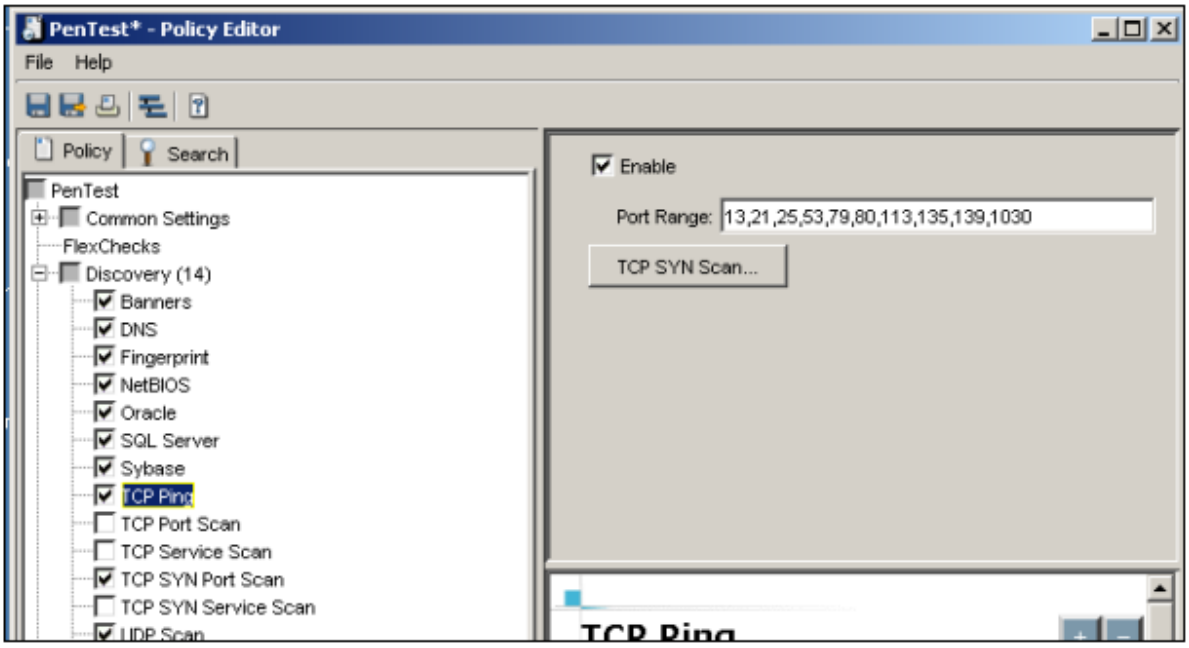


Рис. 2.2. Вибір діапазону портів для методу TCP Ping в сканері Internet Scanner.

2.1.2. Ідентифікація відкритих портів

Для ідентифікації відкритих портів використовувався метод SYNscan, там, де він був відсутній - TCP connect scan.

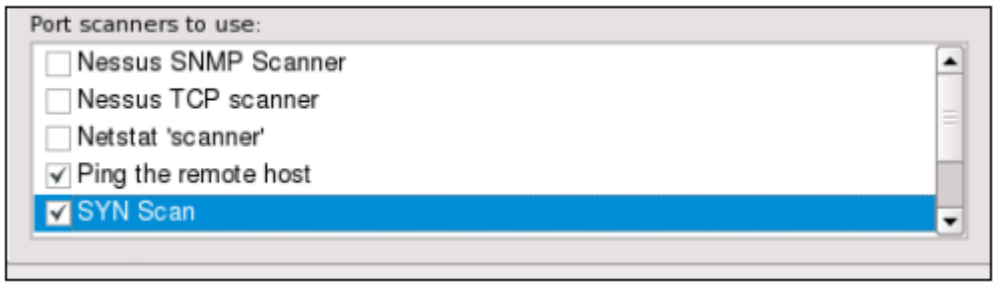


Рис. 2.3. Ввімкнення SYNScan в сканері Nessus

Діапазон сканованих портів TCP- 1: 65535

Діапазон сканованих портів UDP - 1: 65535

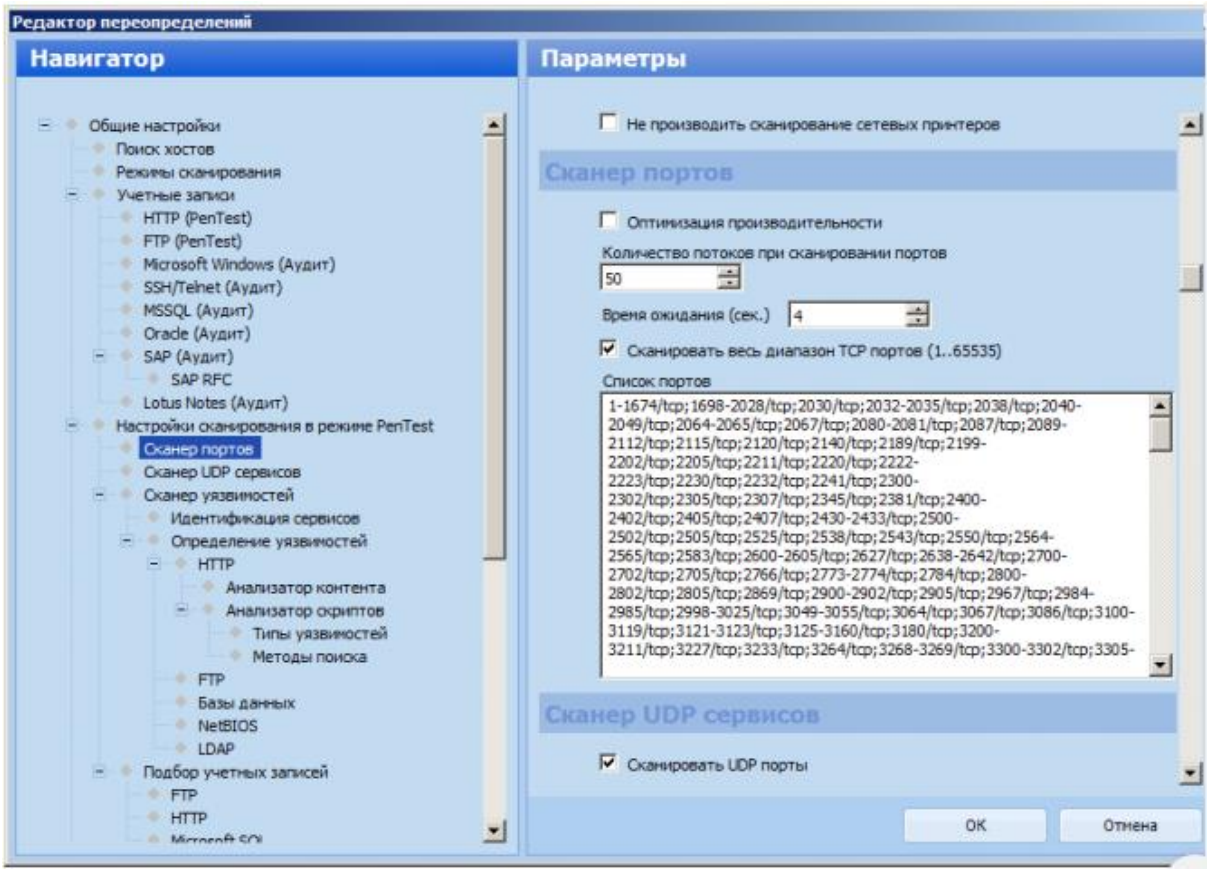


Рис. 2.4.. Налаштування діапазону портів в MaxPatrol

2.1.3. Ідентифікація сервісів і додатків

В даному випадку об'єкт сканування - це «чорний ящик», тому для ідентифікації сервісів і додатків повинні бути задіяні всі методи, які підтримуються сканером.

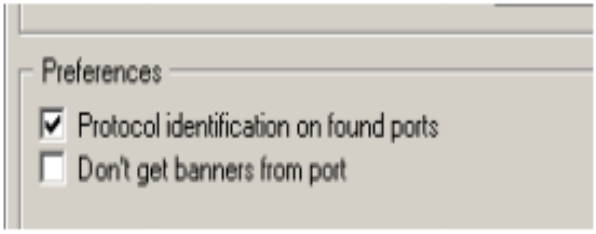


Рис. 2.5. Включення ідентифікації сервісів в сканері Shadow Security Scanner

2.1.4. Ідентифікація операційних систем

Для дослідження було задіяно п’ять вузлів з різними операційними системами.[22-25] Для проведення тестування використовувались вузли з

різними налаштуваннями та різними операційними системами на них. Відповідно до сумісності з ОС було створено таблицю відповідності сканера безпеки та вузла, на якому його було протестовано (табл 2.1).

Таблиця 2.1.

Вузли, які використовувались для перевірок.

Назва вузла	Операційна система	Сканери, які тестувались	Протоколи та технології
host1.test	Windows7	MP, IS, Retina, Nessus, SSS, NetClarity, Xspider, X-scan, MBSA, GFI, NetIQ	● FTP - File Transfer Protocol ● HTTP - HyperText Transfer Protocol ● MSRDP - Microsoft Remote Display Protocol ● POP3 - Post Office Protocol Version 3 ● SMTP - Simple Mail Transfer Protocol
host2.test	Linux Kernel 2.6	SAINT, Qualys, MP, Nessus, GF, NetIQ	● SSH - Secure Shell ● ICMP - Internet Control Message Protocol ● TCP - Transmission Control Protocol ● Traceroute
host3.test	FreeBSD 5.2	MP, IS, Retina, Nessus, SSS, NetClarity	● FTP - File Transfer Protocol ● SSH - Secure Shell ● DNS - Domain Name System ● ICMP - Internet Control Message Protocol ● Traceroute
host4.test	Cisco IOS	MP, IS, Retina, Nessus,	● Telnet - teletype network

	12.2 switch	SSS, NetClarity	• SNMP - Simple Mail Transfer Protocol • Cisco • Traceroute • ICMP - Internet Control Message Protocol
host5.test	Linux	SAINT, Qualys, MP, Nessus, GF, NetIQ	• HTTP - HyperText Transfer Protocol • SSH - Secure Shell • DNS - Domain Name System • ICMP - Internet Control Message Protocol • Traceroute

Для ідентифікації операційних систем були задіяні всі наявні в сканерах методи.

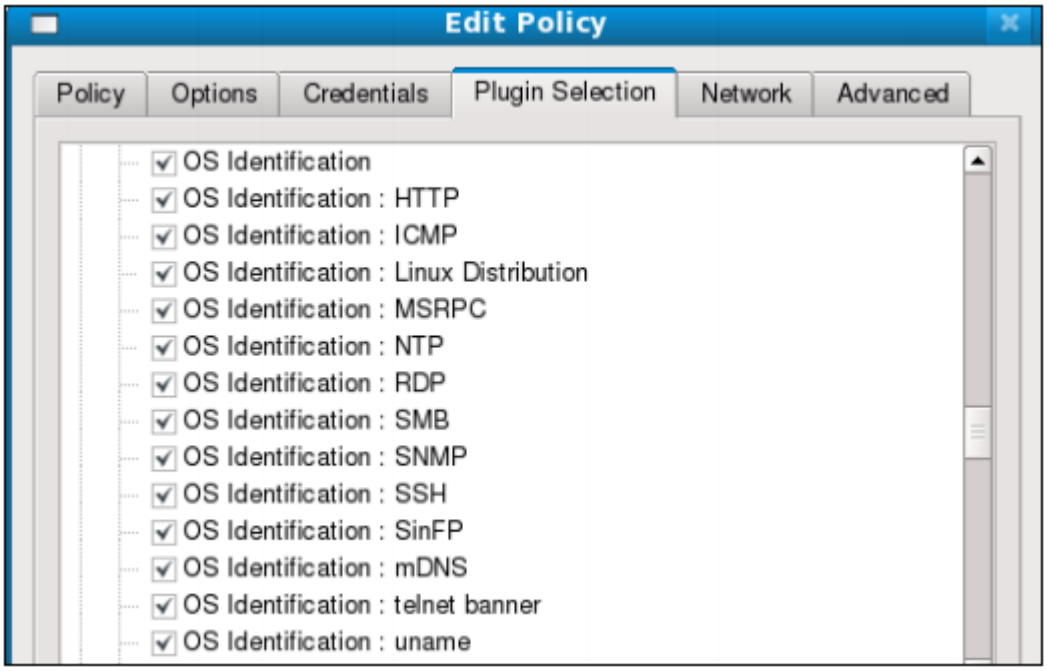


Рис. 2.6. Налаштування ідентифікації ОС в Nessus

2.1.5. Ідентифікація вразливостей

Для дослідження вразливостей було обрано основні протоколи та технології, які є найбільш актуальними на даний момент. Грунтуючись на результатах дослідження на цих протоколах та технологіях можна робити висновки і про інші аналогічні протоколи та технології.

Протоколи та технології, які було задіяно для тестування:

1. SQL (structured query language) - декларативна мова програмування, яку застосовують для створення, модифікації та управління даними в реляційній базі даних, керованої відповідною системою управління базами даних.
2. NFS(Network File System) - протокол мережевого доступу до файлових систем.
3. NNTP(Network News Transfer Protocol) - являє собою мережевий протокол розповсюдження, запиту, розміщення і отримання групи новин при взаємодії між сервером групи новин і клієнтом.
4. LDAP (Lightweight Directory Access Protocol) - протокол прикладного рівня для доступу до служби каталогів X.500, розроблений IETF як полегшений варіант розробленого ITU-T протоколу DAP.
5. FTP (File Transfer Protocol) — протокол передачі файлів по мережі.
6. HTTP (HyperText Transfer Protocol) - протокол прикладного рівня передачі даних використовується для передачі довільних даних.
7. MSRDP (Microsoft Remote Desktop Protocol — протокол віддаленого робочого стола) - пропріетарний протокол прикладного рівня, що використовується для забезпечення віддаленої роботи користувача з сервером, на якому запущений сервіс термінальних підключень.
8. POP3 (Post Office Protocol Version 3 — протокол поштового відділення, версія 3) - стандартний інтернет-протокол прикладного рівня, який використовується клієнтами електронної пошти для отримання пошти з віддаленого сервера по TCP-з'єднання.

9. SMTP (Simple Mail Transfer Protocol — простий протокол передачі пошти) - це широко використовуваний мережевий протокол, призначений для передачі електронної пошти в мережах TCP / IP.

10. SSH Secure Shell — «безопечна оболочка») — мережевий протокол прикладного рівня, що дозволяє виробляти віддалене управління операційною системою і тунелювання TCP-з'єднань.

11. Dos-атака (Denial of Service «отказ в обслуживании») — хакерська атака на обчислювальну систему з метою довести її до відмови, тобто створення таких умов, при яких достовірні користувачі системи не можуть отримати доступ до наданих системних ресурсів (серверів), або цей доступ ускладнений.

12. ICMP (Internet Control Message Protocol — протокол міжмережних керуючих повідомлень) - мережевий протокол, що входить в стек протоколів TCP / IP.

13. TCP (Transmission Control Protocol) – це стандарт, який визначає як встановлювати і підтримувати зв'язок, за допомогою якого дві програми зможуть обмінюватися даними.

14. Traceroute - це службова комп'ютерна програма, призначена для визначення маршрутів пересування даних в мережах TCP / IP.

15. DNS (Domain Name System «система доменних імен») — комп'ютерна розподілена система для отримання інформації про домени.

16. Telnet - teletype network) — мережевий протокол для реалізації текстового термінального інтерфейсу по мережі.

17. Cisco - технологія мережевого обладнання, призначена в основному для великих організацій і телекомунікаційних підприємств.

Для ідентифікації вразливостей були включені всі наявні перевірки, за винятком «Небезпечних» тестів, що призводять до відмови в обслуговуванні. Як відомо, перевірки, що виконуються мережевими сканерами безпеки, можна розділити на дві категорії:

- Логічні висновки (inference) - перевірки, засновані на зібраній інформації, наприклад, на результатах ідентифікації сервісів і додатків.
- Тести - перевірки, що виконуються шляхом явних атак або так званих спеціальних запитів.

Тести, в свою чергу, можна поділити на «небезпечні» і «безпечні». Небезпечні тести можуть призвести до виведення сервісу, що тестується, з ладу, тому в ході порівняння вони не були використані. На рисунку 2.7 наведено відповідні налаштування сканера Nessus.

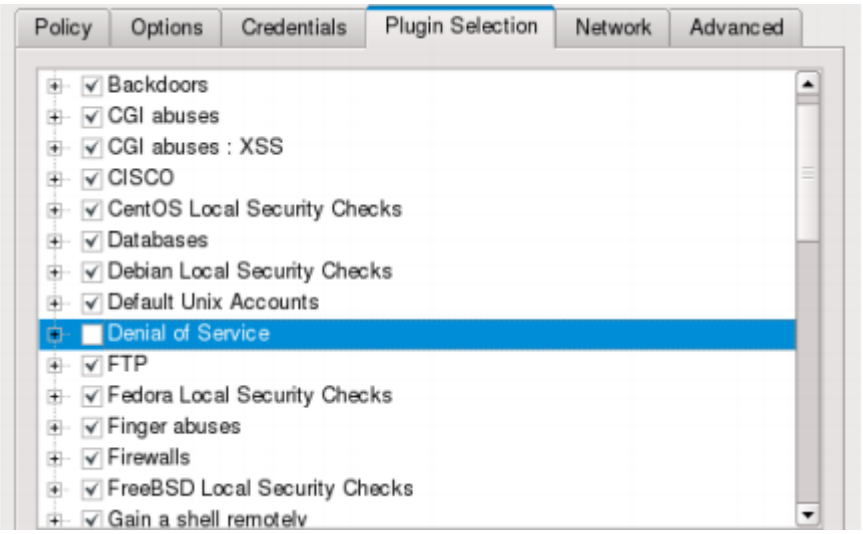


Рис. 2.7. Відключення DoS перевірок («небезпечних» тестів) в Nessus

Таким чином, ідентифікація вразливостей за непрямими ознаками була включена, як і ідентифікація вразливостей за допомогою тестів (якщо сканер надавав можливість вибору, використовувалися тести, рис 2.8).

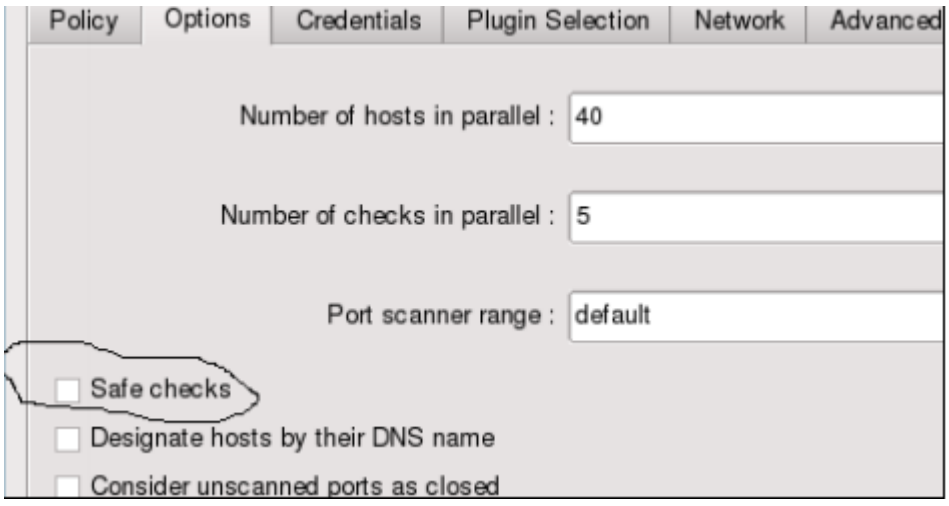


Рис 2.8. Ввімкнення «тестів»

Відстеження взаємозв'язків між перевірками було включено. Для підключення до Windows-систем використовувався «нульовий сеанс» .

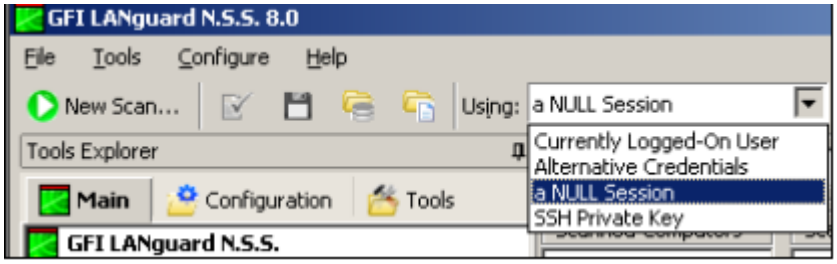


Рис. 2.9. Налаштування аутентифікації в GFI LANguard

Однак якщо сканер підтримує можливість проводити системні перевірки за результатами підбору пароля, то ця опція була задіяна.

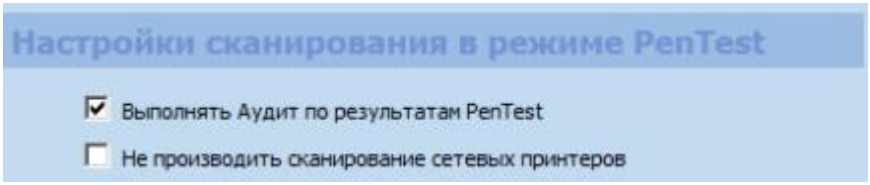


Рис. 2.10. Функція «Аудит по результатам Pentest» в MaxPatrol

Підбір паролів (якщо такі перевірки були, вони були задіяні) передбачав використання тільки словників за замовчуванням (не використовувалися спеціально підключені словники).

Нарешті, для з'ясування причин збоїв та аналізу результатів «ведення журналу» ходу роботи сканера має бути включено.

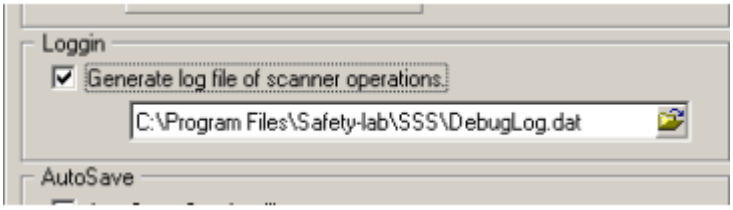


Рис. 2.11. Ввімкнення «журналювання» роботи сканера Shadow Security Scanner

2.2. Аналіз завдання

Оскільки в якості об'єктів сканування виступають реальні «мішені», адекватність результатів роботи сканерів для порівняння не викликає сумнівів. Але при цьому слід розуміти, що робота одного сканера може займати тривалий час (від декількох хвилин до декількох днів). Якщо врахувати, що сканери

запускалися по черзі (одночасне сканування одного і того ж вузла різними сканерами було виключено для «чистоти експерименту»), стан об'єкту сканування вузла міг змінитися. Тому при аналізі результатів були виключені вузли, стан яких сильно змінювався з часом.

Наприклад, в ході сканування був знайдений вузол з порожнім паролем адміністратора. Неважко здогадатися, що стан цього вузла сильно змінився в ході сканування.

Сканери безпеки, які тестувались, їх вартість та операційна система, яка підтримується, знаходяться у таблиці 2.2.

Таблиця 2.2.

Сканери безпеки, які досліджувались в ході тестування

	ОС	Ціна	Link
Positive Technologies Xspider	Win	Free	www.ptsecurity.ru/xs7download.asp
Nessus Security Scanner	Win/*nix/ Mac	2394$	www.nessus.org/plugins/index.php
SafetyLab Shadow Security Scanner	Win	499$	http://www.safety-lab.com/en/products/securityscanner.htm
GFI LANguard N.5.5.	Win/*nix/ Mac	30$	www.gfi.com/lannetscan
IBM Internet Scanner	Win	600$	https://secuniaresearch.flexerasoftware.com/community/
EEYE Retina Network Security Scanner	Win	1950$	https://www.beyondtrust.com/search?ss360Query=Retina

NetIQ	Win/*nix/ Mac	675$	https://www.microfocus.com/ru-ru/products
Qualys	Unix	295$	https://www.upguard.com/articles/tenable-vs-qualys
X-scan	Win	Free	https://x-scan.apponic.com/
SAINT	Unix	Free	https://www.saintcorporation.com/
MBSA	Win	799$	https://www.microsoft.com/en-us/download/
MaxPatrol	Unix, Win	899$	https://www.anti-malware.ru/products/maxpatrol-siem
NetClarity	Win	995$	https://www.scmagazine.com/review/netclarity-nacwall-micro/

2.3. Обробка результатів

2.3.1. Ідентифікація сервісів і додатків

Як говорилося вище, методологія тестування на стійкість до злому розглядає об'єкт сканування як «чорний» ящик, тому достовірність результатів сильно залежить від точності ідентифікації сервісів і реалізації цих сервісів додатків. Крім того, оскільки об'єктом сканування в даному випадку були вузли мережевого периметра, завдання ідентифікації сервісів і додатків ускладнювалася фільтрацією трафіку, навмисної підміною банерів і іншими настройками, що утруднюють визначення сервісів.

Якщо відкритий порт був знайдений не всіма сканерами, він і пов'язані з ним уразливості (якщо вони були знайдені іншими сканерами) просто вилучались з результатів. Ось, наприклад, результат збору інформації по вузлу host1.test (табл. 2.3).

Таблиця 2.3.

Результати ідентифікація сервісів і додатків по вузлу host1.test

	ОС	TCP:21	TCP:25	TCP:110	TCP:1000	TCP:1723	TCP:3000	TCP:3389	Оцінка
Реально	Windows 7	Gene6 FTP Server	SMTP, Mdaemon	POP3, Mdaemon	HTTP, Mdaemon	PPTP, Microsoft	Mdaemon/WorldClient	RDP	14
Xspider	не визнач.	FTP	SMTP	POP3	HTTP	PPTP	Mdaemon	RDP	10
Nessus	AIX 5.2,	Gene6 FTP	SMTP	POP3	HTTP, Mdaemon	PPTP, Microsoft	HTTP, Mdaemon	MsRDP	11
SSS	не визнач.	FTP	SMTP	POP3	HTTP, Wdaemon	1	HTTP, Wdaemon3.0	RDP	8
GFI	не визнач.	FTP	0	Mdaemon 9.6.5	HTTP, Mdaemon	PPTP, Microsof	Mdaemon/WorldClient	RDP	6
IBM IS	не визнач.	FTP	SMTP, Mdaemon	POP3, Mdaemon	1	PPTP	1	1	6
Retina	не визнач.	FTP	SMTP	POP3	HTTP	PPTP	HTTP	MsRDP	7
NetIQ	Windows 7	FTP, Gene6	SMTP, Mdaemon	POP3, Mdaemon	HTTP	1	0	RDP	7
X-scan	Windows 2003	FTP	SMTP	1	HTTP, Mdaemon	0	Web service for Mdaemon	RDP	8
MBSA	Solaris	FTP	SMTP	POP3	HTTP	PPTP	0	1	7
MaxPatrol	Windows 2007	FTP	SMTP	POP3, Mdaemon	HTTP, Mdaemon	PPTP, Microsof	HTTP, Mdaemon	MsRDP	11

На цьому вузлі було знайдено 7 відкритих портів TCP. При цьому всі 7 портів були знайдені кожним з сканерів. Якщо сканер зміг ідентифікувати сервіс, у відповідній клітинці записано назву сервісу. Якщо ідентифіковано додаток - його назва вказана через кому після назви сервісу. Якщо сканер не зміг ідентифікувати сервіс, то в клітинку заноситься просто «одиничка».

Наприклад, 21-й порт використовується сервісом FTP, і всі сканери це визначили. сканер Nessus та NetIQ змогли ідентифікувати додаток - Gene6 FTP Server. Відповідно, в кожному осередку цього рядка вказано назву сервісу - FTP, а в клітинку, відповідну сканера Nessus та NetIQ, внесено також назва програми. Правильно ідентифікований сервіс оцінювався в 1 бал, правильно ідентифікований додаток - ещѐ 1 бал. Якщо сканер помилився, то 1 бал віднімається.

Наприклад, в даному випадку сервіс SMTP (порт 25) правильно ідентифікували всі сканери, крім GFI LANguard N.5.5. (Це +1 бал). Сканер Internet Scanner та NetIQ ідентифікував додаток (MDaemon). Це ещѐ +1 бал. Сканер GFI LANguard N.5.5 визначив, що порт є відкритим, але не визначив ні сервіс, ні додаток, тому бали ні додаються, ні вираховуються.

Далі можна аналогічно аналізувати наступні сервіси та порти, що було протестовано в нашій системі. Отже, практично аналогічна ситуація з сервісом POP3, який всі сканери змогли ідентифікувати як відкритий, проте сканер X-scan не визначив сервіс, тому бали залишаються незмінні. Іншим сканерам нараховується плюс бал за визначений правильно сервіс. А сканерам MaxPatrol, NetIQ,

Дал порт 1000 - це Web-сервіс для MDaemon. Сканер Internet Scanner визначив, що порт відкритий, але не зміг ідентифікувати ні сервіс, ні додаток - у відповідному полі варто просто «одиничка» (при цьому бали не нараховуються). Сканер NetClarity не визначив, що даний порт відкритий - в полі відображається «нуль».

У підсумку, за визначення сервісів і додатків сканери MaxPatrol і Nessus отримують по 11 балів, Shadow Security Scanner - 8 балів, Internet Scanner - 6 і т.д. У таблиці 3 наведені відповідні значення

2.3.2. Ідентифікація вразливостей

Після того як всі знайдені (всіма сканерами) уразливості були занесені в таблицю, по кожній з них проводилася перевірка: чи існує дана уразливість в дійсності.

За результатами перевірки був заповнений стовпець «реально». Далі були заповнені стовпці окремо по кожному сканеру. Якщо сканер знайшов вразливість і її наявність було підтверджено вручну (в стовпці «реально» стоїть одиничка), то у відповідній клітинці - одиниця. якщо сканер знайшов вразливість і її наявність НЕ було підтверджено вручну (в стовпці «реально» стоїть нуль), то це «помилкове спрацювання (False Positive), воно позначається одиницею на червоному тлі.

Решта ситуації - це пропуски (False Negatives). Пропуски можуть бути з різних причин:

- Сканер не виконує такої перевірки (перевірка відсутня в базі сканера)
- Помилка реалізації (перевірка є в базі, але зроблена «недбало», в деяких випадках можуть бути пропуски)
- Потрібна автентифікація (для виконання перевірки сканера необхідно підключення з використанням облікового запису)
- Інші причини

З'ясувати причини пропусків - завдання досить тродоємне. В даному порівнянні виявлялися тільки ситуації пропусків через відсутність перевірки в базі сканера.

Такі пропуски позначені «нулем» на жовтому тлі. Пропуски з інших причин позначені «нулем» на червоному тлі. Таким чином, використовувалася наступна система позначень

1 — Вразливість знайдена правильно

1 — Хибна тривога (false positive)

0 — Вразливість не знайдена, та її дійсно немає

0 — Пропуск вразливості (false negative) по причині відсутності перевірки в базі

0 — Пропуск вразливості (false negative) по іншим причинам

2.3.2.1. Вузол 1 (host1.test)

Далі в якості прикладу, що ілюструє використання відповідних позначень, знову використовується вузол host1.test (табл 2.4).

Таблиця 2.4.

Результати сканування вузла host1.test

Збір інформації		MP	IS	Retina	Nessus	SSS	NetClarity	Xspider	X-scan	MBSA	GFI	NetIQ	реально
Операційна система		Windows7	не визнач	не визнач	AIX 5.2, Catalist OS 6.3, SCO OpenServer 5.0.7	не визнач	не визнач	не визнач	не визнач	Windows7	не визнач	не визнач	Windows7
Відкриті порти, сервіси, додатки	TCP:21	FTP	FTP	FTP	FTP,Gene6 FTP Server	FTP	FTP	FTP	FTP	FTP,Gene6 FTP Server	FTP	FTP	Gene6 FTP Server v3.6.0
	TCP:25	SMTP	SMTP, Mdaemon	SMTP	SMTP	SMTP	SMTP	SMTP, Mdaemon	SMTP	SMTP	SMTP	SMTP	
	TCP:110	POP3, Mdaemon	POP3, Mdaemon	POP3	POP3	POP3	POP3	POP3, Mdaemon	POP3	POP3	POP3	POP3	Pop3, Mdaemon, 9.6.5
	TCP:1000	HTTP, Web service for Mdaemon	1	HTTP	HTTP, Web service for Mdaemon	HTTP, Wdaemon 3.0	0	1	HTTP	HTTP, Web service for Mdaemon	HTTP, Wdaemon 3.0	0	HTTP, Web service for Mdaemon
	TCP:1723	PPTP, Microsoft	PPTP	PPTP	PPTP, Microsoft	1	PPTP	PPTP	PPTP	PPTP, Microsoft	1	PPTP	PPTP, Microsoft
	TCP:3000	HTTP, Web service for Mdaemon	1	HTTP	HTTP, Web service for Mdaemon	HTTP, Wdaemon 3.0	0	1	HTTP	HTTP, Web service for Mdaemon	HTTP, Wdaemon 3.0	0	MDaemon/ WorldClient
	TCP:3389	MsRDP	1	MsRDP	MsRDP	RDP	RDP	1	MsRDP	MsRDP	RDP	RDP	RDP
		11	6	7	11	8	5	6	7	11	8	5	
Вразливості		**MP**	**IS**	**Retina**	**Nessus**	**SSS**	**NetClarity**	**Xspider**	**X-scan**	**MBSA**	**GFI**	**NetIQ**	**реально**
Some POP3 server banners providing information to attacker		0	0	0	0	0	1	0	0	0	0	0	1
FTP: Переповнення буфера		0	0	0	1	0	0	0	0	0	1	0	1
FTP: Знайден логін(guest/guest)		1	1	0	0	0	0	0	0	0	1	0	1
SMTP:EXPN		1	0	0	0	0	0	0	1	0	0	1	0
SMTP daemon supports EHLO		0	1	0	0	0	0	1	1	0	0	1	1
HTTP: Знайдені директорії		0	0	0	1	0	0	0	0	0	0	0	1
HTTP: Незахищена передача даних		1	0	0	1	0	0	0	0	1	0	0	1
HTTP:Файл robots.txt		1	0	0	1	0	0	0	0	0	0	0	1
HTTP:Unknown CGIs arguments torture (підозра на XSS)		0	0	0	1	0	0	0	0	1	0	0	1
MsRDP: Віддалене керування		1	0	1	1	0	0	0	1	0	1	0	1
MsRDP: Невідповідність стандарту FIPS-140		0	0	0	1	0	0	1	0	0	0	0	1
SQL: allows remote authenticated users to gain privileges via unknown vectors		0	0	0	0	0	0	0	0	0	0	1	1
NNTP: uses port 123 even for modes where a fixed port number is not required		0	0	0	0	0	0	0	1	0	0	0	1
NFS: remote attackers to bypass intended access		0	0	0	0	0	0	0	0	0	1	0	1

Всього на даному вузлі усіма сканерами було знайдено 41 вразливостей, потім підтверджено ручною перевіркою 38 вразливостей. При цьому, наприклад, сканер MaxPatrol знайшов 5 вразливостей, і один раз він «помилився» (в таблиці

помилкові спрацьовування позначені «одиницею» на червоному тлі). Отже, сканером MaxPatrol було пропущено 9 вразливостей з 13.

Проаналізуємо причини помилкових спрацьовувань і пропусків.

Помилкове спрацьовування сталося в ході визначення підтримки команди EXPN. Ось як виглядає результат ручної перевірки:

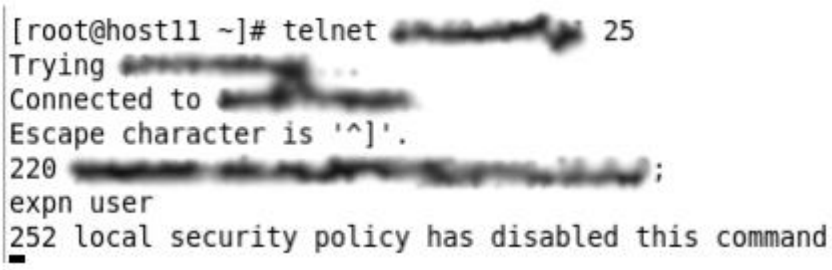


Рис. 2.12. «Ручна перевірка» підтримки команди EXPN

Цілком можливо, що MaxPatrol не зовсім коректно обробляє код відповіді 252, яка повідомляє про заборону даної команди локальною політикою.

Тепер проаналізуємо причини пропусків. П’ять пропуску з дев’яти були допущені через відсутність перевірок в базі сканера, а саме:

- Надання сервісом POP3 «зайвої» інформації
- Помилка реалізації (переповнення буфера) сервера FTP
- Підтримка команди EHLO
- Невідповідність стандарту FIPS

Ці перевірки сканером MaxPatrol просто не виконуються (такі пропуски позначені «нулем» на жовтому тлі). Причини двох пропусків, що залишилися (підозра на XSS і каталоги на Webсервере) - це вже помилки реалізації. Такі перевірки сканер виконує, але в даній ситуації відповідних вразливостей знайдено не було (такі пропуски позначені «нулем» на червоному тлі).

Internet Scanner знайшов дві вразливості, помилкових спрацьовувань при цьому зафіксовано не було. Що стосується пропусків, то їх було 8, з них 7 - через відсутність в базі відповідних перевірок. Цікаво, що факт наявності на вузлі віддаленого управління (RDP) не був виявлений, тому що для виконання відповідної перевірки (RdpEnabled) потрібні адміністративні привілеї.

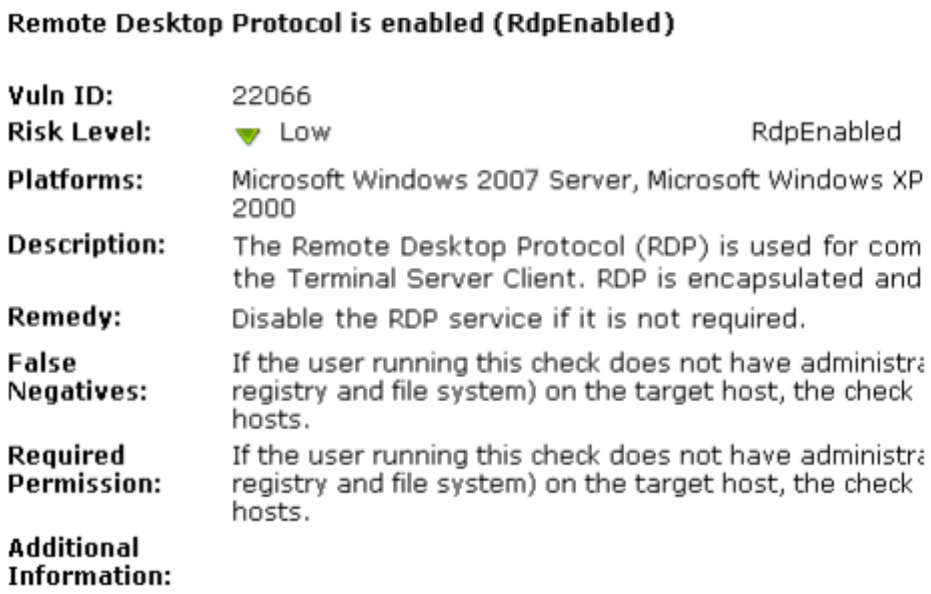


Рис. 2.13. Перевірка «RdpEnabled» в сканері Internet Scanner

Сканер Retina знайшов тільки одну вразливість з 13 можливих, інші перевірки відсутні в його базі, Nessus виявив 7 вразливостей, пропустив 3 через відсутність перевірок в базі, .

Shadow Security Scanner НЕ знайшов жодної уразливості, 9 пропусків було допущено через відсутність перевірок в базі, один - через реалізацію самої перевірки. Зупинимося детальніше на пропуску даними сканером уразливості сервера FTP Gene6. Така перевірка дійсно мається на сканері SSS.

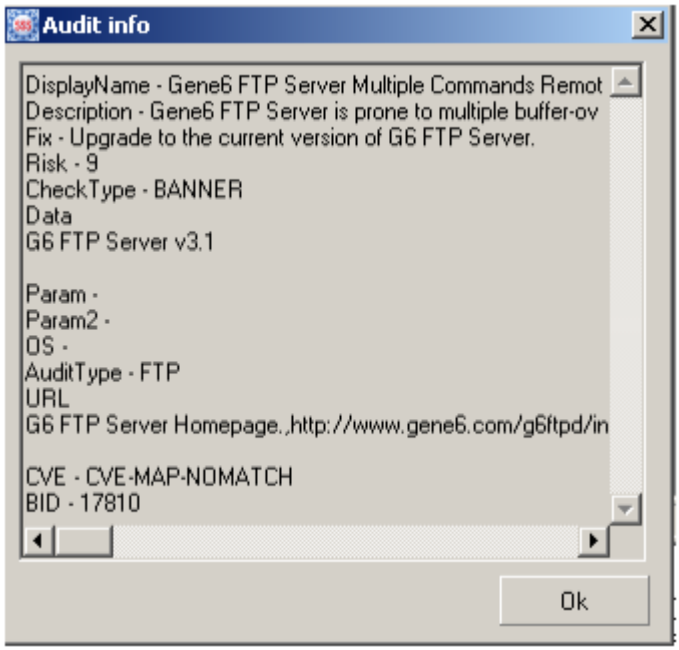


Рис. 2.14. Перевірка FTP Server Buffer Overflow Vulnerabilities в сканері SSS

З її опису можна зрозуміти, що перевірка знаходить вразливість, якщо версія сервера, вилучена з банера - 3.1. В даному випадку «дійсна» версія сервера FTP - 3.6.0. Зрозуміло, сканер SSS НЕ знайшов даної вразливості.

На рисунку 2.15 представлено опис цієї вразливості в базі SecurityFocus. Дійсно, там згадується саме версія 3.1.

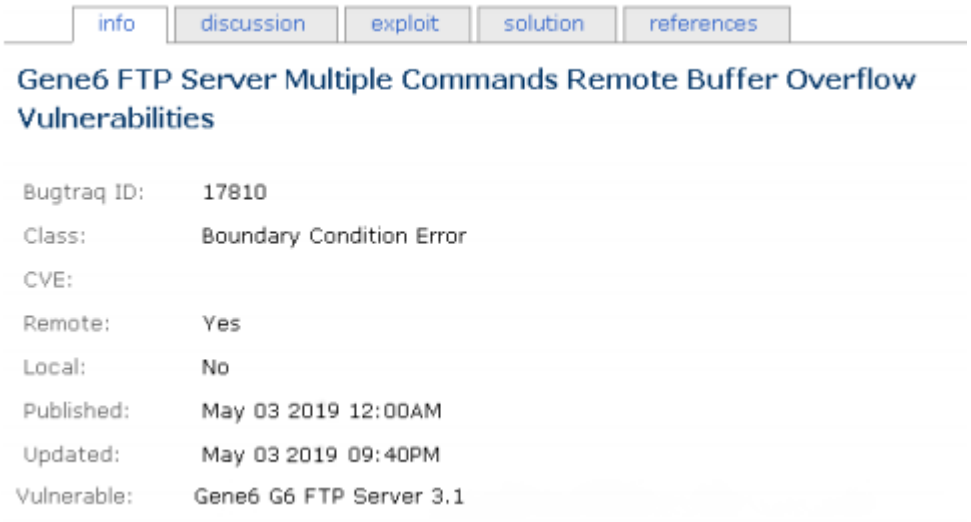
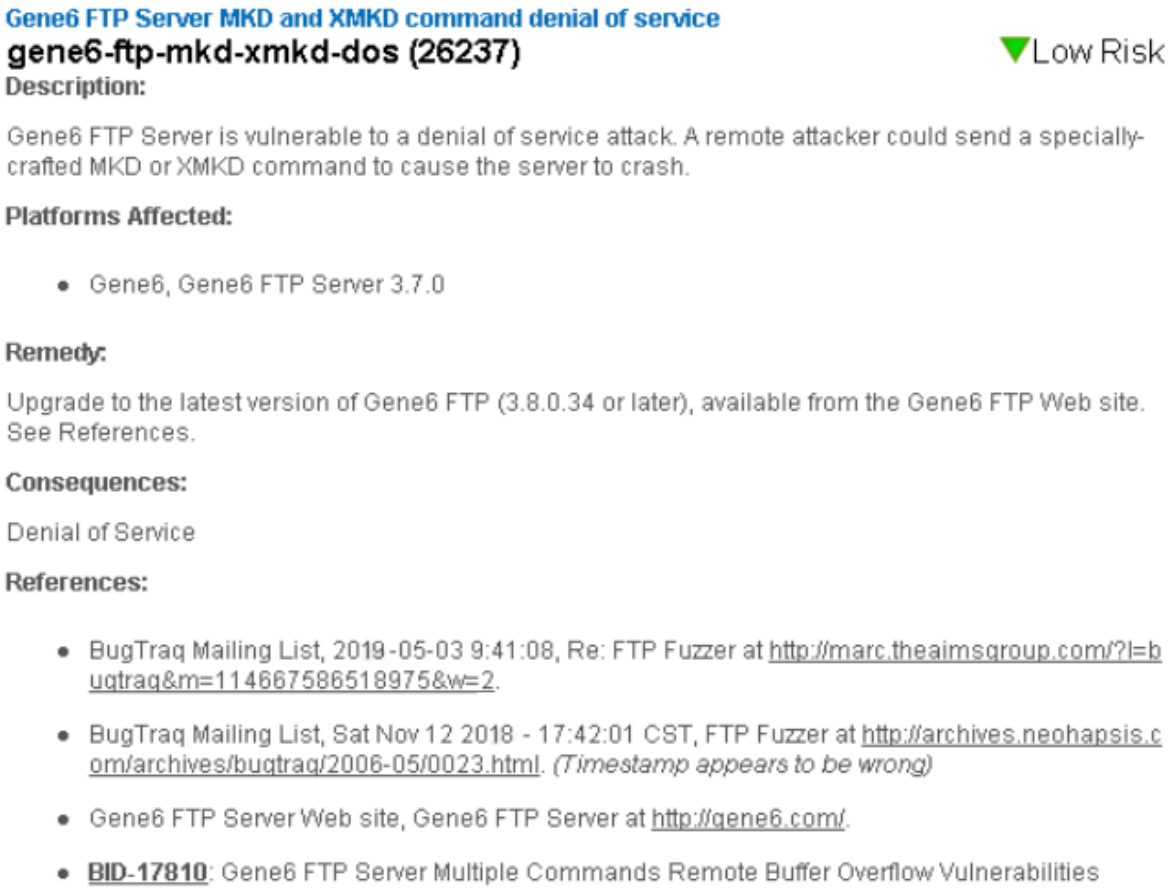


Рис. 2.15. Опис уразливості FTP Server Buffer Overflow Vulnerabilities

З іншого боку, опис цієї ж уразливості в базі XForce відрізняється від приведеного вище опису.



Gene6 FTP Server MKD and XMKD command denial of service

gene6-ftp-mkd-xmkd-dos (26237)

Low Risk

Description:

Gene6 FTP Server is vulnerable to a denial of service attack. A remote attacker could send a specially-crafted MKD or XMKD command to cause the server to crash.

Platforms Affected:

- Gene6, Gene6 FTP Server 3.7.0

Remedy:

Upgrade to the latest version of Gene6 FTP (3.8.0.34 or later), available from the Gene6 FTP Web site. See References.

Consequences:

Denial of Service

References:

- BugTraq Mailing List, 2019-05-03 9:41:08, Re: FTP Fuzzer at http://marc.theaimsgroup.com/?l=bugtraq&m=114667586518975&w=2.
- BugTraq Mailing List, Sat Nov 12 2018 - 17:42:01 CST, FTP Fuzzer at http://archives.neohapsis.com/archives/bugtraq/2006-05/0023.html. *(Timestamp appears to be wrong)*
- Gene6 FTP Server Web site, Gene6 FTP Server at http://gene6.com/.
- **BID-17810**: Gene6 FTP Server Multiple Commands Remote Buffer Overflow Vulnerabilities

Рис. 2.16. Опис уразливості FTP Server Buffer Overflow Vulnerabilities в базі XForce

Тут мова йде вже про версії 3.7.0. Те ж саме, до речі, говорить і база вразливостей osvdb.

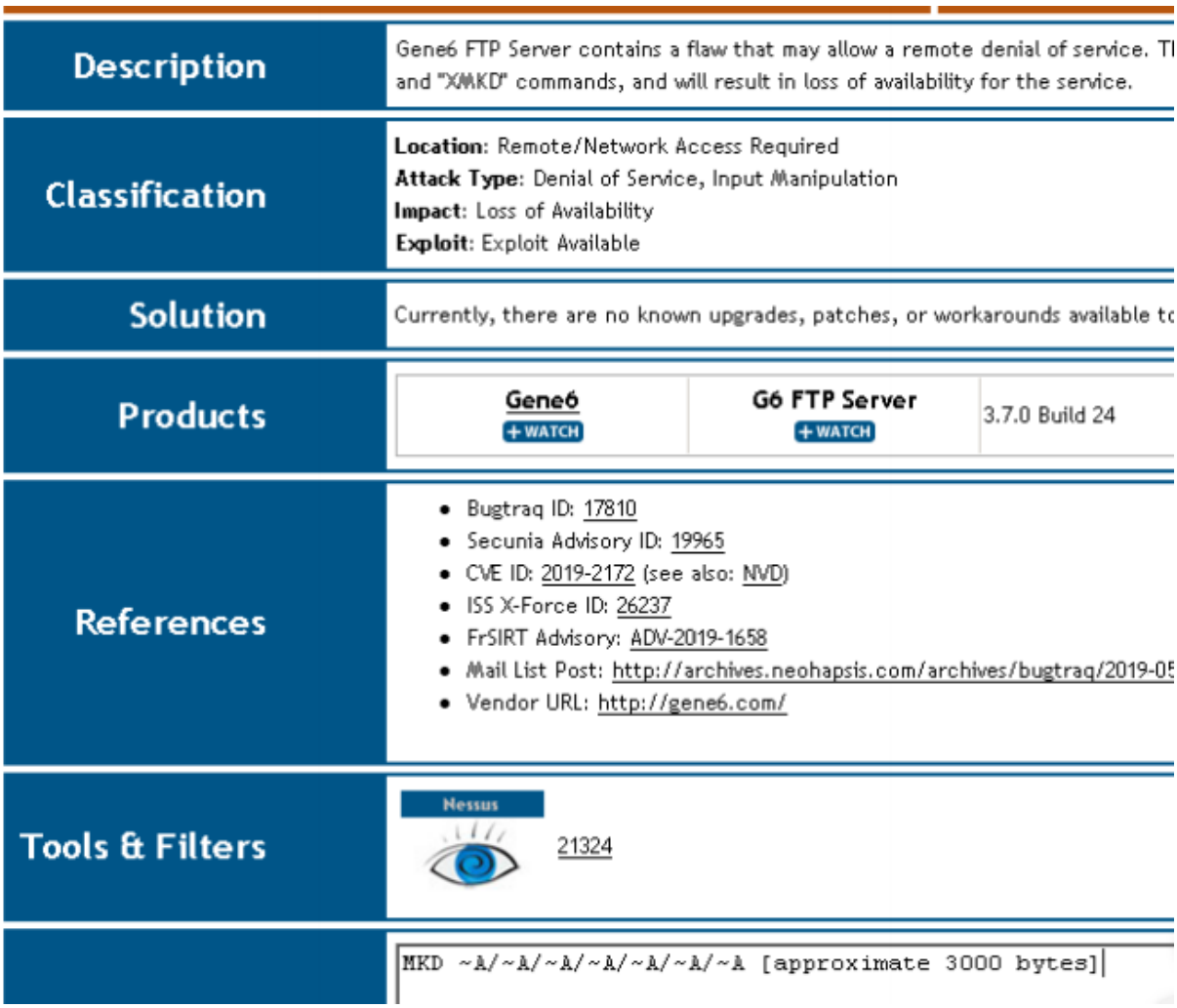


Рис. 2.17. Опис уразливості FTP Server Buffer Overflow Vulnerabilities в базі osvdb

Тому в даній ситуації розумніше «повірити» сканеру Nessus, ніж SSS. Ну і, нарешті, в базі сканера NetClarity більшості перевірок немає, тому його результат - одна знайдена вразливість.

2.3.2.2. Вузол 2 (host2.test)

Роль вузла очевидна - сервер SSH, з ідентифікацією сервісу та додатків всі сканери впоралися однаково (табл. 2.5).

Таблиця 2.5.

Результати сканування вузла host2.test

Збір інформації		MP	SAINT	Qualys	Nessus	GFI	NetIQ	реально
Операційна система		не вияв	не вияв	не вияв	Linux Kernel 2.6	не вияв	не вияв	
Відкриті порти, сервіси, додатки	TCP:22	SSH, OpenSSH_4.3	SSH, OpenSSH_4.3	SSH, OpenSSH_4.3	SSH, OpenSSH_4.3	SSH, OpenSSH_4.3	SSH, OpenSSH_4.3	SSH, OpenSSH_4.3
		2	2	2	2	2	2	
Вразливості		**MP**	**IS**	**Retina**	**Nessus**	**SSS**	**NetClarity**	**реально**
SSH: Відмова в обслуговуванні		1	0	0	0	1	0	1
SSH: Перевищення повноважень		1	0	0	0	0	0	1
SSH: Розголошення інформації		1	0	0	0	0	0	1
SSH: Підміна даних у log-файлі		1	0	0	0	0	0	1
SSH: Розголошення інформації		1	0	0	0	1	0	1
SSH: Відмова в обслуговуванні		1	0	0	0	0	0	1
SSH: Доступ до імен користувача		1	0	0	0	0	0	1
SSH: Обхід обмежень безпеки		1	0	0	0	0	0	1
SSH: DoS-атака		1	0	0	0	1	1	1
SSH: SSH Servers : OpenSSH SKey Remote Information Disclosure Vulnerability		0	0	0	0	1	0	0
IcmpTstamp: ICMP timestamp requests		0	1	1	1	0	0	1
WinXP IP vulnerability		0	0	0	0	0	1	0
The remote host does not discard TCP SYN packets which have the FIN flag set		0	0	0	0	0	1	1
Traceroute:		0	1	1	1	0	1	1
Всього знайдено		**9**	**2**	**2**	**2**	**4**	**4**	**12**
З них виявлено		0	0	0	0	1	1	
Пропусків		3	10	10	10	9	9	
З них по причині відсутності у базі		3	10	9	1	3	9	
Через необхідність аутентифікації		0	0	1	5	0	0	

А ось далі, власне, починається зіставлення версії SSH і переліку відомих вразливостей.

Як видно з таблиці, найбільш коректно і якісно це зіставлення виконано сканером MaxPatrol. Якщо проаналізувати результати інших сканерів, то, виходить, що Internet Scanner і Retina просто не виконують більшості відповідних перевірок («нулі» на жовтому тлі). Пропуск уразливості “SSH: перевищення повноважень” сканером Retina пояснюється тим, що для виконання цієї перевірки потрібно аутентифікація.

Сканер GFI знайшов три уразливості в сервісі SSH, при цьому було зафіксовано одне хибне спрацювань і декілька пропусків.

Причини пропусків вразливостей сканером GFI дві:

- «Недбала» побудова перевірки (рахується обмежене число версій, аналогічно розглянутій вище перевірці сервера FTP)
- Використання тільки однієї бази вразливостей (www.securityfocus.com/bid)

Ось, наприклад, перевірка “SSH: Розголошення інформації” в сканері GFI.

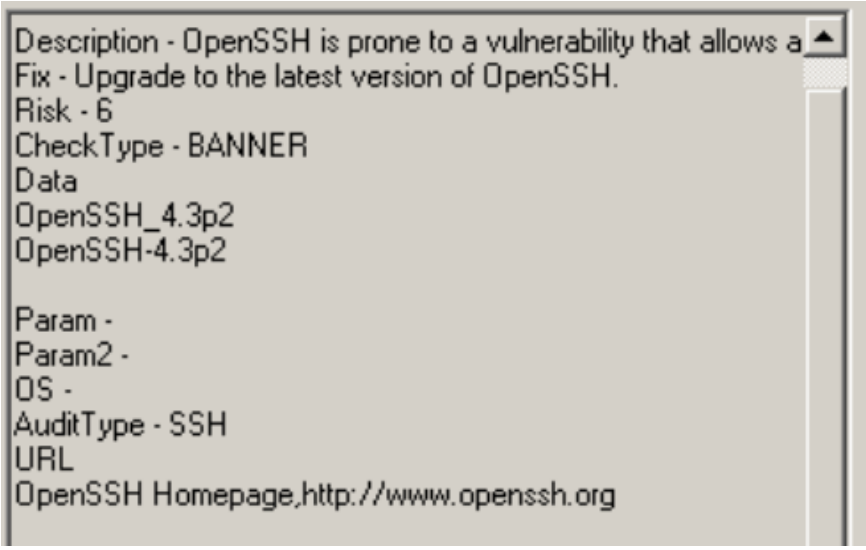


Рис. 2.18. Перевірка CVE-2020-1483 в сканері GFI

Як і в розглянутому вище випадку з FTP, видно, що перевірка враховує тільки окремі версії, хоча швидкий перегляд каталогу CVE[27] вже говорить про те, що й інші версії також можуть містити дану вразливість.

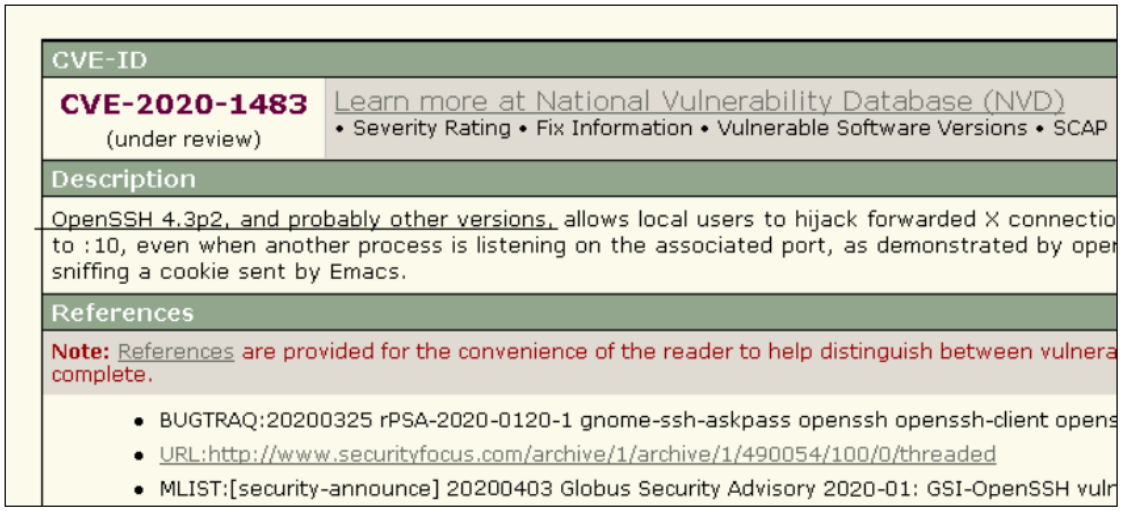


Рис. 2.19. Перевірка “SSH: Розголошення інформації” в каталозі вразливостей

Частина пропусків Nessus-а пов'язана з тим, що для виконання перевірки потрібна автентифікація (таких пропусків було зафіксовано 5), інші пропуски можна пояснити неповнотою самої перевірки (як і в сканері GFI).

2.3.2.2. Вузол 3 (host3.test)

Цей вузол це FreeBSD з рядом сервісів, в процесі ідентифікації яких сканери зіткнулися з деякими труднощами (табл. 2.6).

Таблиця 2.6.

Результати сканування вузла host3.test

Вразливості	MP	IS	Retina	Nessus	SSS	NetClarity	Реально
FTP: Анонімний FTP	1	1	1	1	1	1	1
FTP: Анонімний FTP на запис	1	0	1	1	1	0	1
FTP: файл .rhosts на сервері FTP	0	0	0	1	0	0	1
FTP: VisNetic and Titan FTP Server traversal	0	0	0	1	0	1	0
FTP: ST FTP traversal	0	0	0	1	0	1	0
FTP: Generic FTP traversal	0	0	0	1	0	1	0
SSH: DoS-атака	1	0	0	0	1	1	1
SSH: Перевищення повноважень	1	0	0	0	1	0	1
SSH: OpenSSH GSSAPI Credential Disclosure Vulnerability	1	0	0	0	1	0	0
SSH: OpenSSH-portable PAM Authentication Remote Information Disclosure Vulnerability	0	0	0	0	1	0	1
SSH: Відмова в обслуговування	1	0	0	0	1	0	1
SSH: Розголошення інформації	1	0	0	0	0	0	1
SSH: Сканування портів	1	0	0	0	0	0	1
SSH: Ввімкнення переадресації	1	0	0	0	0	0	1
SSH: Розголошення інформації	1	0	0	0	0	0	1
SSH: Відмова в обслуговування	1	0	0	0	0	0	1
SSH: Відмова в обслуговування	1	0	0	0	0	0	1
SSH: Доступ до імен користувачів	1	0	0	0	0	0	1
SSH: Обхід обмежень безпеки	1	0	0	0	0	0	1
SSH: Перевищення повноважень	1	0	0	0	0	0	1
SSH: Розголошення інформації	1	0	0	0	0	0	1
DNS: Підміна DNS-даних	1	0	0	0	0	0	1
DNS: Відмова в обслуговуванні	1	0	1	0	0	0	1
DNS: Відправка кешу	1	0	1	1	1	1	1
DNS: Відправка кешу	1	0	1	0	0	0	1
DNS: bind-hostname-disclosure (18836)	0	1	0	0	0	1	0
IcmpTstamp: ICMP timestamp requests	0	1	1	1	0	0	1
Traceroute: можливе визначення топології мережі	0	1	1	1	0	1	1
Всього знайдено	20	4	7	9	8	8	23
З них хибних спрацювань	1	1	0	3	0	4	
Пропусків	4	20	16	17	15	19	
З них через відсутність у базі	2	18	14	4	10	18	
Визвані потребою аутентифікації	0	2	0	6	0	0	

Перш за все, сервіс SSH в даному випадку використовує два порти: 22 і 443. Internet Scanner НЕ впорався із завданням ідентифікації SSH, що використовує порт 443. Це сталося через те, що він не намагається виконувати ідентифікацію сервісу SSH, що використовує порт, відмінний від 22-го. Друга складність - пакет Quagga Routing Software Suite. Демони Quagga мають власний віртуальний інтерфейс або VTY (Virtual TeletYpe). Це означає, що можна з'єднатися з демоном, використовуючи протокол telnet. Краще за інших з ідентифікацією даного програмного забезпечення впорався Nessus, сканер MaxPatrol обмежився тільки ідентифікацією сервісу.

Сервіс NNTP був помилково ідентифікований обома сканерами як Skype і FTP. Чи варто говорити, що інші сканери взагалі не впоралися з ідентифікацією зазначених сервісів.

В ході ідентифікації вразливостей також виник ряд цікавих моментів.

Результати пошуку вразливостей в сервісі SSH, взагалі то, аналогічні попереднім вузлам, за винятком перевірки OpenSSH GSSAPI Credential Disclosure Vulnerability. Це вразливість, експлуатація якої можлива тільки

при включеній підтримці аутентифікації gssapi. Оскільки в даному випадку вона вимкнена, то вона не була зарахована як знайдена уразливість. Тільки сканер Nessus, виконуючи дану перевірку, з'ясовує, чи включена аутентифікація GSSAPI. Дуже цікавий момент, у всякому разі, на користь сканера Nessus.

2.3.2.3. Вузол 4 (host4.test)

Це маршрутизатор CISCO, цікавий з точки зору сканування вузол (табл. 2.7).

Мабуть, тут варто «похвалити» результати сканерів MaxPatrol, Internet Scanner і Nessus. але перемога тут, все таки, за MaxPatrol. Nessus «відзначився» тим, що перевірки щодо CISCO побудовані на основі бази securityfocus, а в ній помічені явні розбіжності з CVE і вже тим більше - з списками вразливостей Cisco. Internet Scanner, в цілому, виконав сканування досить якісно, але з пропусками. До речі, тут помічена досить нетипова причина пропуску вразливості CVE-2004-0054. Ця перевірка виконується шляхом явної атаки, до того ж є ймовірність виведення вузла з ладу. За умовами порівняння такі перевірки були відключені.

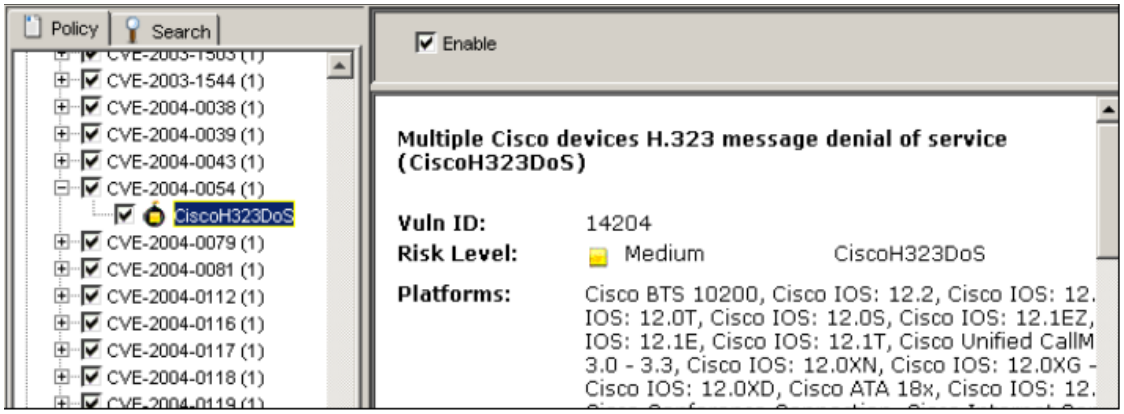


Рис. 2.20. Перевірка CVE-2004-0054 в Internet Scanner

Таблиця 2.7.

Результати сканування вузла host4.test

Збір інформації		MP	IS	Retina	Nessus	SSS	NetClarity	реально
Операційна система		Cisco C1700-K9O3SV3Y7-M, IOS 12.2(15)T8	Cisco IOS C1700-K9O3SV3Y7-M	Cisco 2960G switch (IOS 12.2)	CISCO IOS 12.2(15)T8	не визн	0	CISCO IOS 12.2
Відкриті порти, сервіси та додатки	TCP:23	Telnet	Telnet	Telnet	Telnet	Telnet	Telnet	Telnet
	UDP:161	SNMP	SNMP	SNMP	SNMP	SNMP	SNMP	SNMP
		2	2	2	2	2	2	
Вразливості		**MP**	**IS**	**Retina**	**Nessus**	**SSS**	**NetClarity**	**реально**
Telnet: Незахищений протокол		1	0	1	1	0	1	1
SNMP: Витік інформації		1	0	0	0	0	0	1
SNMP: Відмова в обслуговуванні		1	0	0	0	0	0	1
SNMP: Відмова в обслуговуванні		1	0	0	0	0	0	1
SNMP: Відмова в обслуговуванні		1	0	0	0	0	0	1
SNMP: Розголошення інформації		1	0	0	0	0	0	1
SNMP: Переповнення буфера		1	0	0	0	0	0	0
SNMP: Несанкціонований доступ		1	0	0	0	0	0	1
SNMP: Неавторизований доступ		1	0	0	1	0	1	1
SNMP: Відмова в обслуговуванні		1	0	0	0	0	0	1
SNMP: Відмова в обслуговуванні		1	0	0	0	0	0	1
SNMP: Обліковий запис користувача(public)		1	1	1	1	1	1	1
SNMP: Відмова в обслуговуванні		1	0	0	0	0	0	1
SNMP: Відмова в обслуговуванні		1	0	0	1	0	0	1
SNMP: Відмова в обслуговуванні		1	0	0	0	0	0	1
SNMP: Відмова в обслуговуванні		1	0	0	0	0	0	1
SNMP: Перевантаження пристрою		1	0	0	0	0	0	1

Таблиця 2.7.

Результати сканування вузла host4.test

SNMP: Відмова в обслуговуванні		1	0	0	0	0	0	0
SNMP: Відмова в обслуговуванні		1	0	0	0	0	0	0
SNMP: Витік інформації		1	0	0	0	0	0	0
SNMP: Перевантаження пристрою		1	0	0	0	0	0	1
SNMP: Відмова в обслуговуванні		1	0	0	0	0	0	1
SNMP: Відмова в обслуговуванні		1	0	0	0	0	0	1
SNMP: Відмова в обслуговуванні		1	0	0	0	0	0	1
SNMP:SNMPv1Discovery: SNMP version 1 detected		0	1	1	0	0	0	1
SNMP:SNMPv2Discovery: SNMP version 2 detected		0	1	0	0	0	0	1
CiscoIosAccountBruteforce: Cisco IOS could allow an attacker to determine valid accounts (12745)	8292	0	1	0	0	0	0	0
CiscoIosIpv6Type0Dos: Cisco IOS IPv6 Type 0 routing header denial of service (31715)	22210	1	1	1	0	0	0	1
CiscoIosBgpPacketDos: Cisco IOS BGP packet denial of service and gain full control (19074)		0	1	0	0	0	0	1
CiscoIosIpv6Dos: Cisco IOS IPv6 denial of service and gain full control (19072)	12368	1	1	0	0	0	0	1
CiscoIpOptionCodeExecution: Cisco IOS and IOS XR IP option code execution (31725)	22211	1	1	1	1	0	0	1
CiscoTcpIpv4Dos: Cisco IOS TCP listener IPv4 memory leak denial of service	22208	1	1	0	1	0	0	1
Perimeter Router: SNMP perimeter router identification		0	1	0	1	0	0	1
snmp: SNMP can reveal possibly sensitive information about hosts		0	1	0	1	0	1	1
SNMPShowInterface: SNMP agents reveal information about network interfaces		0	1	0	1	0	1	1
SNMPShowRMON: SNMP RMON agents can monitor network and application activity		0	1	0	1	0	1	1
SNMPShowRoutes: SNMP agents reveal information about network routing		0	1	0	1	0	1	1
SnmpSysdescr: SNMP SysDescr variable can be returned from remote system		0	1	0	1	0	1	1
Cisco IOS Telnet Service Remote Denial of Service Vulnerability	11060	0	0	1	0	0	0	0
Traceroute: можливе виявлення мережевої топології		0	1	1	1	0	1	1
IcmpTstamp: ICMP timestamp requests		0	1	1	1	0	0	1
CISCO : Cisco IOS HTTP Service HTML Injection Vulnerability	15602	0	0	0	0	1	0	1
CISCO : Cisco IOS Multiple Unspecified EIGRP Vulnerabilities	14877	0	0	0	0	1	0	1
Cisco IOS AAA RADIUS Authentication Bypass Vulnerability	14092	0	0	0	1	0	0	1
CISCO: IOS has flaw in its telephony service	12307	0	0	0	1	0	0	1
Cisco IOS TCLSH AAA Command Authorization Bypass Vulnerability	16383	0	0	0	1	0	0	1
Всього знайдено		28	17	9	17	3	9	40
З них хибних спрацювань		4	1	2	0	0	0	
Пропусків		16	24	33	23	37	31	
З них через відсутність у базі		16	23	25	19	33	31	
Визваних необхідністю автентифікації		0	1	5	1	0	0	

2.3.2.4. Вузол 5 (host5.test)

Це гібридний вузол (табл. 2.8), що підтримує відразу кілька сервісів (DNS, HTTP, FTP, SSH).

Таблиця 2.8.

Результати сканування вузла host5.test

Збір інформації		MP	SAINT	Qualys	Nessus	GFI	NetIQ	реально
Операційна система		Unix	UNIX	Buffalo TerraStation	не визнач	не визнач	0	Unix
Відкриті порти, сервіси та додатки	TCP:21	FTP	FTP	FTP	FTP	FTP	FTP	FTP, Pure-FTPd
	TCP:53	DNS, ISC BIND	DNS, ISC BIND	DNS, ISC BIND	DNS, ISC BIND	DNS	DNS, ISC BIND 9.3.0	DNS, ISC BIND 9.3.0
	TCP:80	HTTP, Nginx HTTP Server	HTTP	HTTP, Nginx HTTP Server	HTTP, nginx	HTTP, nginx	HTTP	HTTP, Nginx HTTP Server
	TCP:35752	SSH, OpenSSH_4.6	1	1	SSH, OpenSSH_4.6	1	0	SSH, OpenSSH_4.6
	UDP:53	DNS, ISC BIND	DNS, ISC BIND	DNS, ISC BIND	DNS, ISC BIND	0	0	DNS, ISC BIND
		7	4	5	7	4	3	
Вразливості		**MP**	**SAINT**	**Qualys**	**Nessus**	**GFI**	**NetIQ**	**реально**
HTTP: Знайдені email адреси на web-сайті		1	0	0	1	1	0	1
HTTP: Помилка в скрипті		1	0	0	0	0	0	1
HTTP: Міжсайтовий скриптинг		1	0	0	0	0	0	1
HTTP: Файл robots.txt		1	0	1	1	0	0	1
SSH: Перевищення повноважень		1	0	0	0	0	0	1
SSH: Розголошення інформації		1	1	0	0	0	0	1
SSH: Доступ до імен користувачів		1	1	0	0	0	0	1
DNS: ISC BIND DNSSEC Validation Multiple RRsets Denial of Service		0	0	1	0	0	1	0
HTTP:Plain Text Authentication Forms		0	0	0	1	0	0	1
IcmpTstamp: ICMP timestamp requests		0	1	1	1	0	1	1
Traceroute: можливе виявлення топології мережі		0	1	1	1	0	1	1
LDAP: creates a PID file after dropping privileges to a non-root account		0	1	0	0	0	0	1
LDAP: both the nops module and the memberof overlay are enabled		0	1	0	0	0	0	0
Всього знайдено		7	2	2	5	1	3	10
З них помилкових		0	0	0	0	0	2	
Пропусків		3	8	8	5	9	9	
З них через відсутність у базі		3	8	7	2	6	9	
Викликані необхідністю автентифікації		0	0	0	0	0	0	

На цьому вузлі для сервісу SSH використовується нестандартний порт (35752). Правильно ідентифікувати сервіс вдалося тільки сканерам MaxPatrol і Nessus. Як наслідок, MaxPatrol правильно ідентифікував 3 уразливості в сервісі SSH. А ось сканер GFI через те, що не ідентифікував даний сервіс, пропустив ці вразливості, хоча відповідні перевірки є в його базі. Це ще раз підтверджує той факт, що для даного завдання вкрай необхідна якісна ідентифікація сервісів і додатків.

2.4. Аналіз результатів

Ототожнюючи всі перевірки на 5 вузлах, можна переглянути сумарний результат у таблиці 2.9.

Таблиця 2.9.

Результати всіх перевірок.

	AINT	Qualys	MP	Xspider	SSS	IS	Retina	X-scan	MBSA	NetCarity	Nessus	GFI	NetIQ
	UNIX		Win/UNIX	Win							UNIX/Win/Mac		
host indows7			FTP 0.5 HTTP 0.5 MSRDP 0.5 POP3 0 SMTP 0 NNTP 0 SQL 0 NFS 0	FTP HTTP MSRDP 0.3 POP3 SMTP 1 NNTP SQL 0 NFS	FTP 0 HTTP 0 MSRDP0 POP3 0 SMTP 0 NNTP 0 SQL 0 NFS 0	FTP 0.5 HTTP 0 MSRDP 0 POP3 0 SMTP 0.5 NNTP 0 SQL 0 NFS 0	FTP 0 HTTP 0 MSRDP 0.5 POP3 0 SMTP 0 NNTP 0 SQL 0 NFS 0	FTP 0.5 HTTP 0 MSRDP 0.5 POP3 0 SMTP 0 NNTP 1 SQL 0 NFS 0	FTP 0 HTTP 0.5 MSRDP 0 POP3 0 SMTP 0 NNTP 0 SQL 0 NFS 0	FTP 0 HTTP 0 MSRDP 0 POP3 1 SMTP 0 NNTP 0 SQL 0 NFS 0	FTP 0.5 HTTP 1 MSRDP 1 POP3 0 SMTP 0 NNTP 0 SQL 0 NFS 0	FTP 1 HTTP 0 MSRDP 0.5 POP3 0 SMTP 0 NNTP 0 SQL 0 NFS 1	FTP 0 HTTP 0 MSRDP 0 POP3 0 SMTP 0.5 NNTP 0 SQL 1 NFS 0
host inux Kernel	SH 0 CMP 1 CP 0 raceroute 1	SH 0 CMP 1 CP 0 raceroute 1	SSH 1 ICMP 0 TCP 0 Traceroute 0					-			SSH 0 ICMP 1 TCP 0 Traceroute 1	SSH 0.3 ICMP 0 TCP 0 Traceroute 0	SSH 0.1 ICMP 0 TCP 1 Traceroute 1
host FreeBSD			FTP 0.5 SSH 1 DNS 1 ICMP 0 Traceroutr 0		FTP 0.5 SSH 0.5 DNS 0.2 ICMP 0 Traceroutr 0	FTP 0.2 SSH 0 DNS 0.1 ICMP 1 Traceroutr 1	FTP 0.2 SSH 0 DNS 0.1 ICMP 1 Traceroutr 1	-		FTP 0.5 SSH 0.1 DNS 0.5 ICMP 0 Traceroutr 1	FTP 1 SSH 0 DNS 0.1 ICMP 1 Traceroutr 1	-	-
host isco IOS			Telnet 1 SNMP 1 Cisco 0.4 Traceroute 0 ICMP 0		Telnet 0 SNMP 0.1 Cisco 0.2 Traceroute 0 ICMP 0	Telnet 0 SNMP 0.1 Cisco 1 Traceroute 1 ICMP 1	Telnet 1 SNMP 0.2 Cisco 0.3 Traceroute 1 ICMP 1	-		Telnet 1 SNMP 0.2 Cisco 0.6 Traceroute 1 ICMP 0	Telnet 1 SNMP 0.3 Cisco 0.7 Tracerou te 1 ICMP 1	-	-
host NIX	TTP 0 SH 0.3 NS 0 CMP 1 raceroute 1 DAP 1	TTP 0.2 SH 0 NS 1 CMP 1 raceroute 1 DAP 0	HTTP 1 SSH 1 DNS 0 ICMP 0 Traceroute 0 LDAP 0		-	-	-	-		-	HTTP 0.6 SSH 0 DNS 0 ICMP 1 Traceroute 1 LDAP 0	HTTP 0.2 SSH 0 DNS 0 ICMP 0 Traceroute 0 LDAP 0	HTTP 0 SSH 0 DNS 0 ICMP 1 Traceroute 1 LDAP 0

Оцінка виставляється за тим принципом, що якщо відбулося декілька перевірок на вузлі на один і той самий протокол, то результативна оцінка це кількість правильних спрацювань до загальної кількості вразливостей по даній технології. Так сканер Max Patrol отримав одиницю, тобто кількість спрацювань дорівнює кількості існуючих вразливостей насправді по протоколу SSH, а ось сканер SAINT виявляє лише дві з трьох вразливостей, тому йому зараховується 2\3 бала, тобто 0.6 балів.

Підсумовуючи, можна виділити такі протоколи та технології з високим коефіцієнтом якості визначення вразливості, який в майбутньому буде використовуватись для створення програмного модуля вибору сканера безпеки для інформаційної системи. Загальна оцінка по технологіям у таблиці 2.10, 2.11.

Таблиця 2.10.

Підсумкові оцінки по технологіям

Nessus	MP	SSS	IS	Retina	NetClarity
SQL: 0, NFS: 0, NNTP: 0, LDAP: 0.5, FTP: 0.75, HTTP: 0.8, MSRDP: 1, POP3: 0, SMTP: 0, SSH: 0, ICMP: 1, 'TCP': 0, Traceroute: 1,	'SQL': 0.1, 'NFS': 0, 'NNTP': 0, 'LDAP': 0.1, 'FTP': 0.5, 'HTTP': 0.75, MSRDP: 0.5, 'POP3': 0, 'SMTP': 0, 'SSH': 1, 'ICMP': 0, 'TCP': 0, 'Traceroute': 0,	SQL': 0, 'NFS': 0, 'NNTP': 0, 'FTP': 0, 'HTTP': 0, 'MSRDP': 0, 'POP3': 0, 'SMTP': 0.1, 'SSH': 0.5, 'ICMP': 0, 'Traceroute': 0,	SQL': 0, 'NFS': 0, 'NNTP': 0, 'FTP': 0.4, 'HTTP': 0, MSRDP: 0, 'POP3': 0, 'SMTP': 0.1, 'SSH': 0, 'ICMP': 1, 'Traceroute': 1,	'SQL': 0, 'NFS': 0, 'NNTP': 0, 'FTP': 0.25, 'HTTP': 0, MSRDP: 0.5, 'POP3': 0, 'SMTP': 0, 'SSH': 0, 'ICMP': 1, 'Traceroute': 1,	'SQL': 0.1, 'NFS': 0.2, 'NNTP': 0, FTP: 0.25, 'HTTP': 0, MSRDP:0 'POP3': 1, 'SMTP': 0, 'SSH': 0.1, 'ICMP': 0, 'Traceroute': 1,

DNS 0.1, Telnet': 1, 'Cisco': 0.7	'DNS': 1, 'Telnet': 1, 'Cisco': 0.4	'DNS': 0.2, 'Telnet': 0, 'Cisco': 0.2	'DNS': 0.1, 'Telnet': 0, 'Cisco': 1	'DNS': 0.9, 'Telnet': 1, 'Cisco': 0.3	DNS: 0.5, 'Telnet': 1, 'Cisco': 0.6

Таблиця 2.11.

Підсумкові оцінки по технологіям

X-scan	MBSA	Xspider	GFI	NetIQ	QUALIS	Saint
'SQL': 0, 'NFS': 0, NNTP: 1 FTP: 0.5 HTTP: 0 MSRDP: 0.5, 'POP3': 0 'SMTP':0	'SQL': 0, 'NFS': 0, 'NNTP': 0 'FTP': 0, HTTP:0.5 'MSRDP': 0, 'POP3': 0, 'SMTP': 0	'SQL':0.1 'NFS': 0, 'NNTP': 0, 'FTP': 0, 'HTTP': 0, 'MSRDP': 0.5, 'POP3': 0, 'SMTP': 1	'SQL': 0, 'NFS': 1, NNTP: 0, 'FTP': 1, HTTP:0.1 'MSRDP': 0.5, 'POP3': 0, 'SMTP': 0, 'SSH': 0.2, 'ICMP': 0, 'Traceroute': 0, 'TCP': 0,	SQL': 1, 'NFS': 0, NNTP:0, 'FTP': 0, HTTP:0, MSRDP: 0, POP3: 0, SMTP:0, SSH:0.1, ICMP:0.5 'Traceroute': 1, 'TCP': 1,	HTTP: 0.2, 'DNS': 1, 'LDAP': 0 'SSH': 0, 'ICMP':1, 'Traceroute': 1,	'HTTP': 0, 'DNS': 0, 'LDAP':1 'SSH':0.6 ICMP: 1, Traceroute: 1,

Визначення оцінки відбувається наступним чином. Наприклад, у сканера MaxPatrol перевірка вразливості по протоколу FTP відбувалась на першому та третьому тестовому хості з результатом і там і там по 0.5 балів, отже і оцінка в підсумковій таблиці за FTP у MaxPatrol буде 0.5 балів, як середнє арифметичне. А ось сканер Retina на першому вузлі отримав нуль балів за FTP, а на третьому

0.5 балів, тому сумарний коефіцієнт зараховується 0.25 балів. Далі за аналогією було сформовано таблицю.

2.5. Висновки до другого розділу

Отже, підводячи підсумки тестування можна заявити, що певні вразливості були виявлені найкраще одним зі сканерів, тому можна виділити сильні сторони кожного сканера, що і було зроблено у таблицях 2.9, 2.10 та 2.11. Якщо потрібно обрати сканер з обмеженим бюджетом, не обов'язково брати найдорожчий сканер Nessus. Хоча він насправді є досить непоганим, обширним сканером, який покриває багато аспектів, тому для великої компанії з необмеженим бюджетом буде гарним рішенням.

Було виявлено найсильніші сторони кожного сканера та доведено, що одну й ту ж саму вразливість сканери, маючи різні механізми виявлення, опрацьовують по різному.

РОЗДІЛ 3. ОПИС ПРОГРАМНОГО СЕРЕДОВИЩА

3.1. Загальна характеристика середовища

Як програмний модуль було розроблено сайт з можливістю ввода параметрів, оброблюючи які програма видасть найкращий сканер із описом та посиланням на сайт виробника, та ще три альтернативні варіанти.

Параметри, які вводить користувач це : операційна система, максимальна вартість, на яку розраховує користувач, технології та протоколи, які застосовуються у інформаційній системі.

Вибір протоколів здійснюється за пріоритетністю тобто, користувач проставляє важливість протоколу у своїй системі за шкалою від одного до десяти. Якщо якась технологія не використовується, її можна відключити, просто натиснувши на назву протоколу. Також вибір на результат вибору сканера впливає не мало важливий показник - вартість сканера.

Для написання програмного модуля було обрано мову програмування - Node js[28], яка є досить об’єктно орієнтованою і зручною для написання подібної програми з такими об’єктами як сканери безпеки. Найкращим варіантом було обрано створення саме сайта[29], який надаватиме результат з коротким описом найбільш підходящого сайту та з посиланням на сайт виробника, де можна його одразу придбати. Для зовнішнього вигляду використовувався звичайний html та задля дизайну стилі CSS[30-31].

Принцип вибору сканера безпеки полягає в тому, що програмний модуль має базу даних сканерів з відповідними протоколами та технологіями та відносним коефіцієнтом, де 1 означає повне виявлення у тестувальному середовищі, з якої програма бере інформацію та далі обробляє її.

Основний метод, який виконує функцію вибору сканера є:

```
req_protocols.forEach((protocol) => {
    scanners.forEach((scanner) => {
```

```
            if (scanner.values[protocol.name] != undefined){
                if (protocol.value == 10) {
                        protocol.value *= 2;
                        if (scanner.values[protocol.name] == 1)
                                scanner.values[protocol.name] *= 2;
                }
               scanner.rate += scanner.values[protocol.name] * protocol.value;
            }
        })
    })
```

Суть якого полягає в тому, що подвійний бал отримує сканер, якщо користувачем була надана перевага певній технології та було встановлено максимальний бал, а саме 10 балів. Також додатково, якщо сканер має по цьому параметру максимальну ефективність, тобто його коефіцієнт якості одиниця, то бали також подвоюються. Це дає можливість зробити акцент саме на тих технологіях, які ставить в пріорітет користувач і на тих сканерах, які найкраще впорались у тестувальному середовищі, та виділити такі сканери.

Надавати лише один результат було не цілком правильно, тому було вирішено надавати один найкращий з детальним описом сканер, та ще три альтернативні варіанти для більш широкого вибору також зі ссилками на сайт виробника.

3.2. Інтерфейс користувача

Потрапляючи на сторінку, користувач бачить таке вікно як на рисунку 3.1.

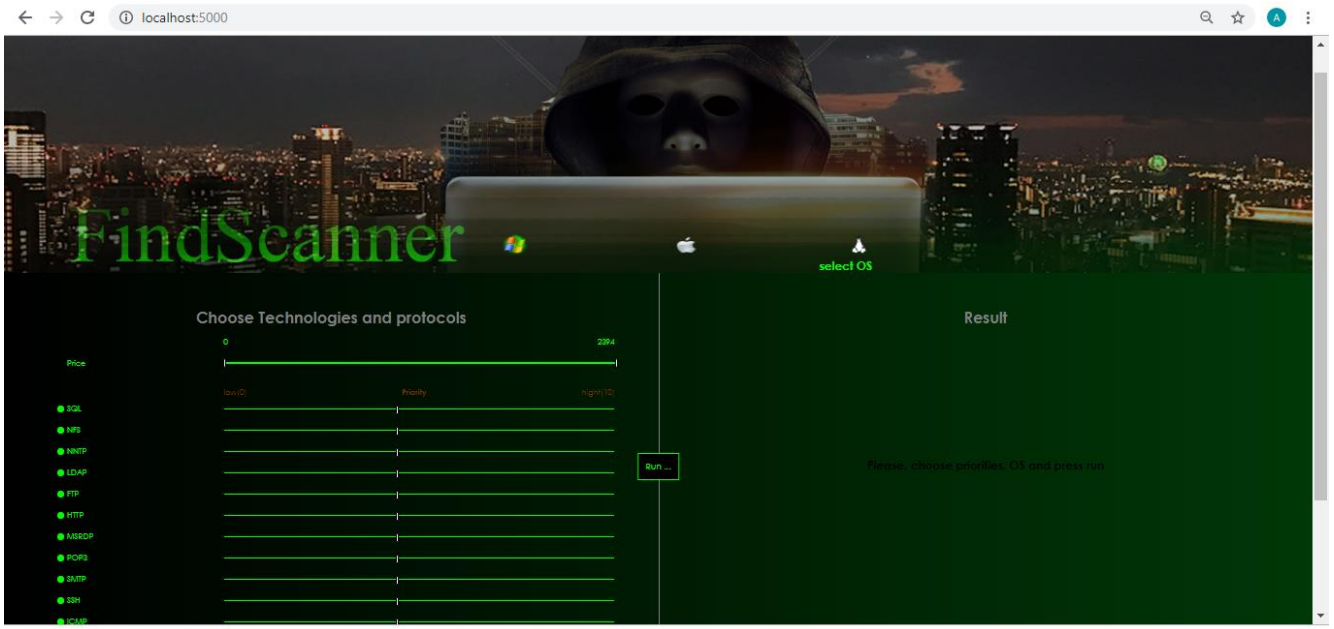


Рис. 3.1. Головна сторінка програмного модулю

Після цього користувач має можливість обрати потрібні технології у лівій частині вікна. Зверху можна вибрати операційну систему, для якої здійснюватиметься пошук сканера. Потім натиснути кнопку “Run” та отримати результат у правій частині вікна.

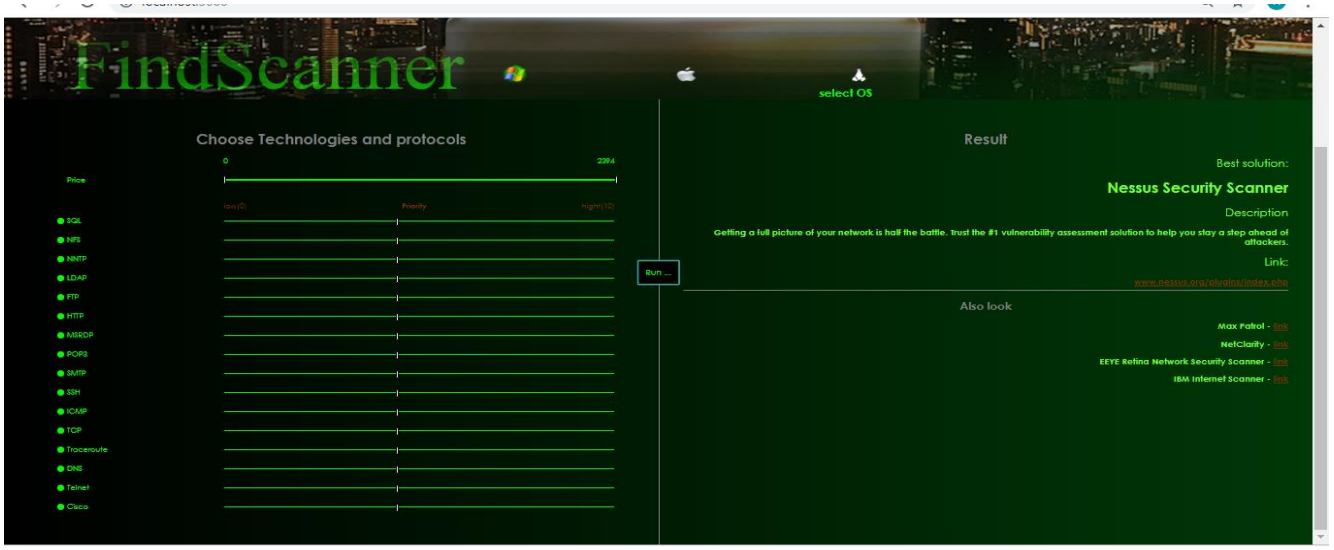


Рис. 3.2.. Результат сканування

Як бачимо при обраних за умовчанням протоколів та технологій як результат отримаємо сканер Nessus. Потім, якщо нам потрібні специфічні технології або протоколи, наприклад NFS, то результат - GFI(рис 3.3), NNTP - Xscan (рис 3.4). Виставляємо всі інші протоколи менш пріоритетними, а один протокол на максимум.

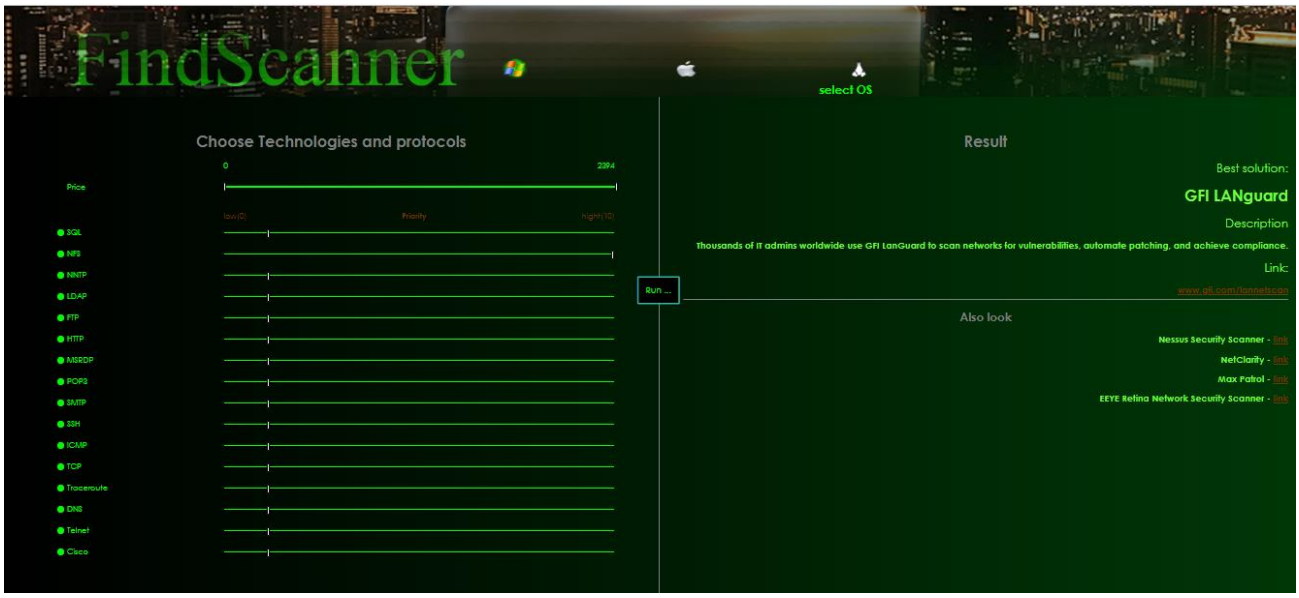


Рис. 3.3. Результат сканування по протоколу NFS

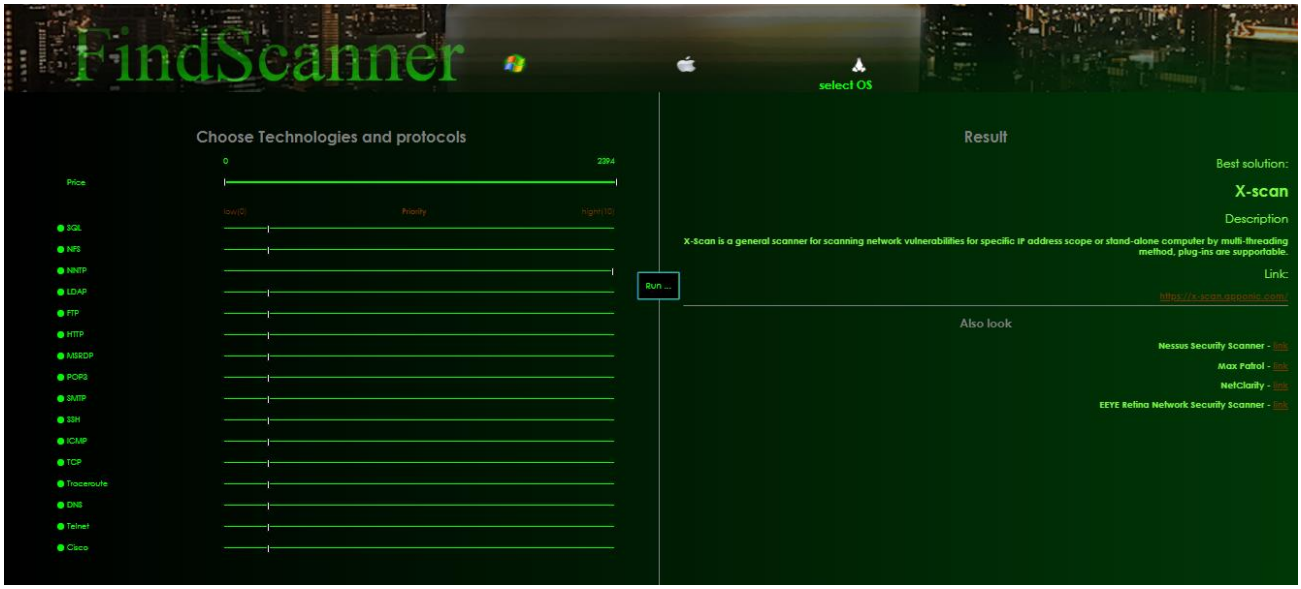


Рис. 3.4. Результат сканування по протоколу NNTP

Якщо обрати технологію Cisco то отримаємо пораду встановити сканер Nessus(рис 3.5), зменшивши ціну - сканер IS(рис 3.6), а обравши операційну систему Linux - MaxPatrol(рис 3.7).

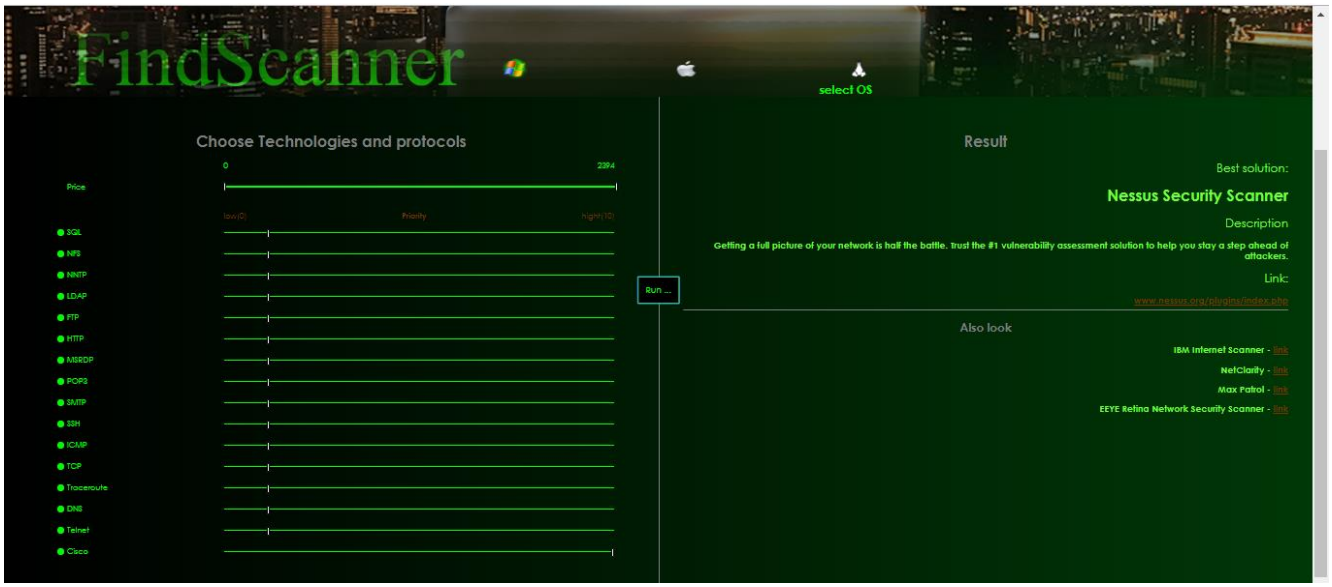
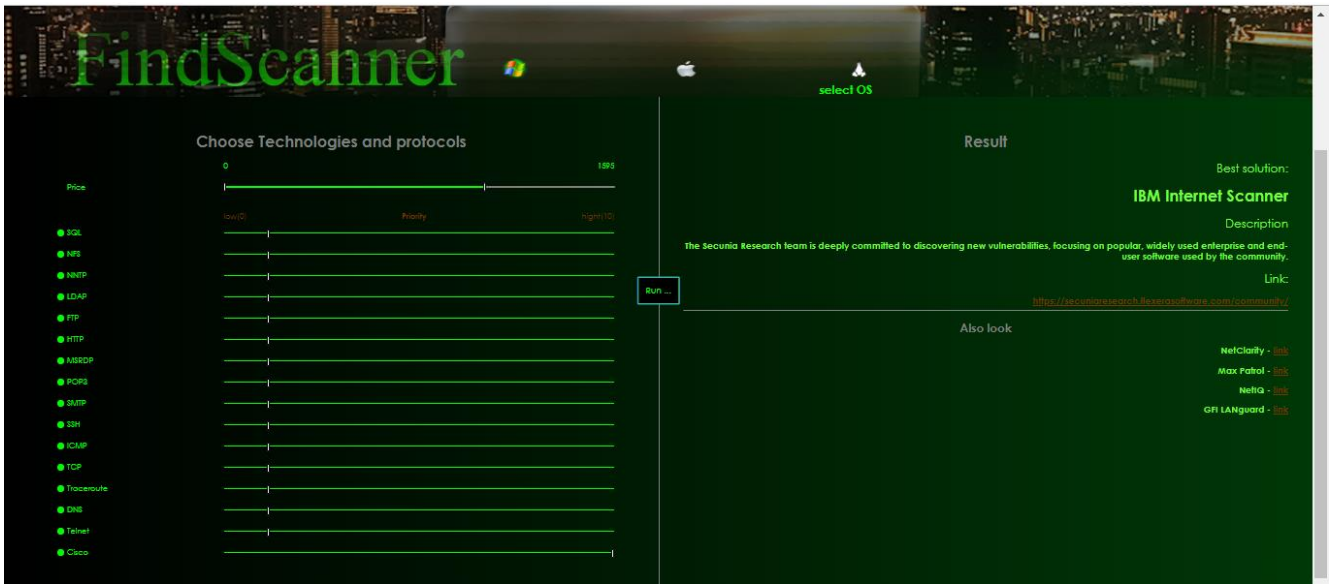


Рис. 3.5. Результат сканування по протоколу Cisco



Рисю 3.6. Результат сканування по протоколу Cisco

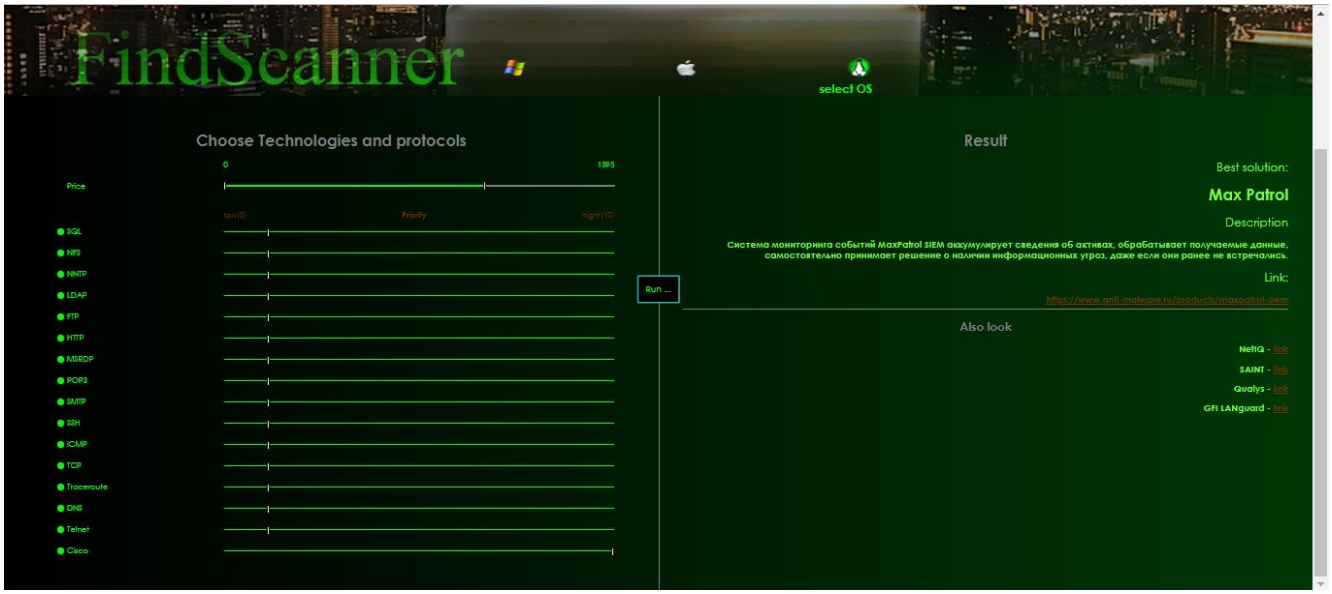


Рис. 3.7. Результат сканування по протоколу Cisco

3.3. Висновки до третьому розділу

Завдяки проведеному дослідженню було розроблено програмний модуль, який полегшує для користувачів процес вибору сканера безпеки інформаційних систем, що є досить складним процесом на великому різномаїтті ринку.

Отже, після проведеного дослідження можно підбити підсумки, що найкращий сканер все ж таки є Nessus, але його захмарна ціна не дає змогу встановити його маленьким компаніям. Тому потрібно визначитись, які протоколи будуть використовуватись у компанії, які технології. А вже потім вибрати сканер безпеки, який підходить для індивідуального підприємства. А це справді можливо і як можна побачити в ході тестування, що справді, один сканер не може охопити всі області однаково добре, тому існують сканери, які досить непогані в певних областях. Так, сканер NetClarity чітко спрацював з вразливістю протокола POP3, а сканер Xspider - SMTP.

ВИСНОВКИ

Вибір сканера безпеки є досить не легким, адже на ринку виробники вказують майже однакові можливості сканера. Під час виконання дипломної роботи було розроблено програмний комплекс, який допоможе користувачам обрати найкращий сканер для їх системи.

Підсумовуючи, можна зазначити, що було:

1. Досліджено застосування сканерів безпеки в інформаційних системах. Спочатку було вивчено нормативно-правову базу та закони, які зобов'язують компанії проходити сканування. Далі було проведено опитування для оцінки ситуації на ринку потенційних користувачів програмного модуля, що було розроблено у межах дипломної роботи.

2. Проаналізовано типи сканерів безпеки, вивчено принципи роботи. На цьому етапі було вирішено проводити лише тестування, яке не шкодить системі, тому тестування Dos атак було виключено.

3. Проведено порівняльний аналіз сканерів безпеки з метою виявлення їх переваг та недоліків.

Що дало змогу виконати:

1. Опрацьовання результатів, всі дані було зведено у таблиці та структуровано. Вирахувано відносні коефіцієнти, які потім було використано у програмному модулі.

2. Потім була створена база сканерів безпеки з ваговими коефіцієнтами та розроблено методи, які сортуватимуть сканери по відносним коефіцієнтам та видаватимуть результат - найкращий сканер безпеки.

3. На заключному етапі було обрано програмне забезпечення та розроблено шаблон сторінки сайту, за яким було створено сторінку для вибору сканера безпеки. Таким чином, було здійснено програмну реалізацію вибору оптимального сканера безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. IT право: проблеми і перспективи розвитку в Україні: збірник матеріалів науково-практичної конференції / Т.В. Бачинський, Д.С. Лозовицький, Р.І. Радейко, Н.П. Бортник – Львів: НУ «Львівська політехніка», 2016. – 396 с.

2. Кондратьєва Я. Ю. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій / Я.Ю.Кондратьєва - Наук.-практ.посіб, 2004 - 545 с

3. Піскозуб А. З. До питання підвищення рівня захищеності комп'ютерних мереж та систем / Піскозуб А. З.- Піскозуб А.З., 2012 - 183 с.

4. ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements.

5. Dr. Anton Chuvakin. A Pragmatic Approach to SIEM: Buy for Compliance, Use for Security. White Paper- URL: http://www.infosec.co.uk/exhibitorlibrary/829/Tripwire_Pragmatic_SIEM_WP_20.pdf.

6. Gartner: marketscope for Vulnerability Assessment 2011 - URL: http://www.gartner.com/technology/media-products/reprints/qualys/article1/article1.htm

7. Mosaic Security Research. Log Management & Security Information and Event Management (SIEM) - URL: https://mosaicsecurity.com/categories/85-log-management-security-information-and-event-management.

8. Протидія злочинам у сфері інтелектуальної власності / Ніколаюк С.І., Никифорчук Д.Й., Томма Р.П., Барко В.І. – К., 2006

9. Сканери уразливості - URL: https://uk.wikipedia.org/wiki/%D0%A1%D0%BA%D0%B0%D0%BD%D0%B5%D1%80%D0%B8_%D1%83%D1%80%D0%B0%D0%B7%D0%BB%D0%B8%D0%B2%D0%BE%D1%81%D1%82%D1%96

10. Аналіз вразливостей корпоративних інформаційних систем - URL: http://jrnl.nau.edu.ua/index.php/ZI/article/view/12453

11. Тест на проникнення - URL: https://uk.wikipedia.org/wiki/%D0%A2%D0%B5%D1%81%D1%82_%D0%BD%D0%B0_%D0%BF%D1%80%D0%BE%D0%BD%D0%B8%D0%BA%D0%BD%D0%B5%D0%BD%D0%BD%D1%8F

12. Про Інформацію: Закон України від 02 жовтня 1992 р. № 2658-XII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/ show/2657-12/ed20110106.

13. Про затвердження Положення про державну експертизу в сфері технічного захисту інформації від 16.05.2007 URL: https://zakon.rada.gov.ua/ laws/show/z0820-07

14. Про міжнародний стандарт ISO/IEC 27001:2005- urlhttp://www.confident.org.ua/index.php/zakonodatelstvo/145-mezhdunarodnyj-standart-iso-iec-27001-2005.htm

15. Захист інформації - Форум https://solar-eclipse.at.ua/forum/11-40-1

16. Безпека та захист інформації - Integrity Systems - URL: http://integritysys.com.ua/solutions/security/

17. Методи і способи захисту інформації- URL: https://pidruchniki.com/1801051351329/ekonomika/metodi_sposobi_zahistu_informatsiyi

18. Реальне використання сканерів безпеки в нашому житті - URL: https://habr.com/ua/post/455662.

19. Использование сканеров безопасности в процессе тестирования сети на устойчивость к взлому, Лепихин В. Б., Гордейчик С. В./ 2005, Учебный центр "Информзащита", Москва – 2006.

20. Internet Security Systems, Inc. Аналіз захисту. Мережевий чи системний рівень Керівництво з вибору технології аналізу захищеності. - URL: (http://www.infosec.ru/themes/default/publication.asp?Folder=1988&matid=1670)

21. How to view the list of open ports in Windows - URL: https://support.kaspersky.com/us/common/windows/

22. Linux* kernel - URL: https://mirrors.edge.kernel.org/pub/linux/kernel/v2.6/

23. Get Ubuntu | Download - URL: https://ubuntu.com/download

24. Software Download - Cisco Systems - URL: https://software.cisco.com/download/home

25. Установка freebsd - URL: https://www.freebsd.org/ru/where.html

26. Common Vulnerabilities and Exposures - URL: https://cve.mitre.org/

27. CVE security vulnerability database- URL: https://www.cvedetails.com/

28. Node.js - URL: https://nodejs.org/uk/

29. ИЗУЧАЕМ NODE.JS - URL: https://learn.javascript.ru/screencast/nodejs

30. CSS- URL: https://ru.wikipedia.org/wiki/CSS

31. Как работает CSS- URL: https://developer.mozilla.org/ru/docs/Learn/CSS/Introduction_to_CSS/How_CSS_works

Додаток А

Вихідний код програмного комплексу

index.js

```
const express = require('express');
const path = require('path');
const PORT = process.env.PORT || 5000;
let app = express();
const bodyParser = require("body-parser");
const data = require('./data');
app.use(express.static(path.join(__dirname, 'public')))
   .set('views', path.join(__dirname, 'views'))
   .set('view engine', 'ejs')
   .use(bodyParser.json())
   .use(bodyParser.urlencoded({extended: true}));
app.get('/', (req, res) => {
   const max_price = Math.max.apply(Math, data.scanners.map(o => o.price));
   res.render('pages/index', {data: data.protocols, max_price: max_price})
});
app.post('/submit',  (req, res) => {
   const req_os = req.body.os;
   const req_price = req.body.price;
   const req_protocols = req.body.protocols;
   let scanners = data.scanners.filter(el =>
      (el.os.includes(req_os)
      && el.price >= req_price.from
      && el.price <= req_price.to)
   );
   scanners.forEach((scanner) => {
      scanner.rate = 0;
   })
   req_protocols.forEach((protocol) => {
      scanners.forEach((scanner) => {
         if (scanner.values[protocol.name] != undefined){
                  if (protocol.value == 10) {
                           protocol.value *= 2;
                           if (scanner.values[protocol.name] == 1)
                                    scanner.values[protocol.name] *= 2;
                  }
            scanner.rate += scanner.values[protocol.name] * protocol.value;
         }
      })
   });
   scanners = scanners.map(scanner => {
      return {
         name: scanner.name,
         rate: scanner.rate,
         url: scanner.url,
```

```
            price: scanner.price,
            description: scanner.description,
        }
    });
    scanners = scanners.sort((a, b) => b.rate - a.rate);
    res.status(200).send(scanners);
})
app.listen(PORT, () => console.log(`Listening on ${ PORT }`));
```

data.js

```
module.exports = {
    protocols: [
        'SQL',
        'NFS',
        'NNTP',
        'LDAP',
        'FTP',
        'HTTP',
        'MSRDP',
        'POP3',
        'SMTP',
        'SSH',
        'ICMP',
        'TCP',
        'Traceroute',
        'DNS',
        'Telnet',
        'Cisco',
    ],
    scanners: [
        {
            rate: 0,
            name: 'Nessus Security Scanner',
            os: 'win|unix|mac',
            url: 'www.nessus.org/plugins/index.php',
            description: 'Getting a full picture of your network is half the battle. Trust the #1
vulnerability assessment solution to help you stay a step ahead of attackers.',
            price: 2394, //price in dollars
            values: {
                'SQL': 0,
                'NFS': 0,
                'NNTP': 0,
                'LDAP': 0.5,
```

```
            'FTP': 0.75,
            'HTTP': 0.8,
            'MSRDP': 1,
            'POP3': 0,
            'SMTP': 0,
            'SSH': 0,
            'ICMP': 1,
            'TCP': 0,
            'Traceroute': 1,
            'DNS': 0.1,
            'Telnet': 1,
            'Cisco': 0.7,
        }
    },
    {
        rate: 0,
        name: 'Max Patrol',
        os: 'win|unix',
        url: 'https://www.anti-malware.ru/products/maxpatrol-siem',
        description: 'Система мониторинга событий MaxPatrol SIEM аккумулирует сведения об активах, обрабатывает получаемые данные, самостоятельно принимает решение о наличии информационных угроз, даже если они ранее не встречались.',
        price: 899,
        values: {
            'SQL': 0.1,
            'NFS': 0,
            'NNTP': 0,
            'LDAP': 0.1,
            'FTP': 0.5,
            'HTTP': 0.75,
            'MSRDP': 0.5,
            'POP3': 0,
            'SMTP': 0,
            'SSH': 1,
            'ICMP': 0,
            'TCP': 0,
            'Traceroute': 0,
            'DNS': 1,
            'Telnet': 1,
            'Cisco': 0.4,
```

```
        }
    },
    {
        rate: 0,
        name: 'SafetyLab Shadow Security Scanner',
        os: 'win',
        url: 'http://www.safety-lab.com/en/products/securityscanner.htm',
        description: 'Safety Lab Shadow Security Scanner is a Proactive Computer Network Security Vulnerability Assessment Scanner with over 5000 audits.',
        price: 499,
        values: {
            'SQL': 0,
            'NFS': 0,
            'NNTP': 0,
            'FTP': 0,
            'HTTP': 0,
            'MSRDP': 0,
            'POP3': 0,
            'SMTP': 0.1,
            'SSH': 0.5,
            'ICMP': 0,
            'Traceroute': 0,
            'DNS': 0.2,
            'Telnet': 0,
            'Cisco': 0.2,
        }
    },
    {
        rate: 0,
        name: 'IBM Internet Scanner',
        os: 'win',
        url: 'https://secuniaresearch.flexerasoftware.com/community/',
        description: 'The Secunia Research team is deeply committed to discovering new vulnerabilities, focusing on popular, widely used enterprise and end-user software used by the community.',
        price: 600,
        values: {
            'SQL': 0,
            'NFS': 0,
            'NNTP': 0,
```

```
            'FTP': 0.4,
            'HTTP': 0,
            'MSRDP': 0,
            'POP3': 0,
            'SMTP': 0.1,
            'SSH': 0,
            'ICMP': 1,
            'Traceroute': 1,
            'DNS': 0.1,
            'Telnet': 0,
            'Cisco': 1,
        }
    },
    {
        rate: 0,
        name: 'EEYE Retina Network Security Scanner',
        os: 'win',
        url: 'https://www.beyondtrust.com/search?ss360Query=Retina',
        description: 'All features, including SCAP support, audit and customization dialogs, PowerShell integration and reporting, and the guided user interface, using the Microsoft .NET framework require Microsoft .NET 4.5.2 and higher.',
        price: 1950,
        values: {
            'SQL': 0,
            'NFS': 0,
            'NNTP': 0,
            'FTP': 0.25,
            'HTTP': 0,
            'MSRDP': 0.5,
            'POP3': 0,
            'SMTP': 0,
            'SSH': 0,
            'ICMP': 1,
            'Traceroute': 1,
            'DNS': 0.9,
            'Telnet': 1,
            'Cisco': 0.3,
        }
    },
    {
```

```
            rate: 0,
            name: 'NetClarity',
            os: 'win',
            url: 'https://www.scmagazine.com/review/netclarity-nacwall-micro/',
            description: 'It would be in the best interest of many organizations looking for network access control to start by evaluating the NACwall Micro device.',
            price: 995,
            values: {
              'SQL': 0.1,
              'NFS': 0.2,
              'NNTP': 0,
              'FTP': 0.25,
              'HTTP': 0,
              'MSRDP': 0,
              'POP3': 1,
              'SMTP': 0,
              'SSH': 0.1,
              'ICMP': 0,
              'Traceroute': 1,
              'DNS': 0.5,
              'Telnet': 1,
              'Cisco': 0.6,
            }
          },
          {
            rate: 0,
            name: 'X-scan',
            os: 'win',
            url: 'https://x-scan.apponic.com/',
            description: 'X-Scan is a general scanner for scanning network vulnerabilities for specific IP address scope or stand-alone computer by multi-threading method, plug-ins are supportable. ',
            price: 0,
            values: {
              'SQL': 0,
              'NFS': 0,
              'NNTP': 1,
              'FTP': 0.5,
              'HTTP': 0,
              'MSRDP': 0.5,
```

```
            'POP3': 0,
            'SMTP': 0,
          }
        },
        {
          rate: 0,
          name: 'MBSA',
          os: 'win',
          url: 'https://www.microsoft.com/en-us/download/details.aspx?id=19892',
          description: 'The Microsoft Baseline Security Analyzer provides a streamlined method to identify missing security updates and common security misconfigurations.',
          price: 799,
          values: {
            'SQL': 0,
            'NFS': 0,
            'NNTP': 0,
            'FTP': 0,
            'HTTP': 0.5,
            'MSRDP': 0,
            'POP3': 0,
            'SMTP': 0,
          }
        },
        {
          rate: 0,
          name: 'Positive Technologies Xspider',
          os: 'win',
          url: 'www.ptsecurity.ru/xs7download.asp',
          description: 'Основная задача сканера XSpider – обнаружить уязвимости в сетевых ресурсах до того, как это будет сделано злоумышленниками, а также выдать чёткие и понятные рекомендации по устранению обнаруженных уязвимостей.',
          price: 0,
          values: {
            'SQL': 0.1,
            'NFS': 0,
            'NNTP': 0,
            'FTP': 0,
            'HTTP': 0,
            'MSRDP': 0.5,
            'POP3': 0,
```

```
            'SMTP': 1,
        }
    },
    {
        rate: 0,
        name: 'GFI LANguard',
        os: 'win|mac|unix',
        url: 'www.gfi.com/lannetscan',
        description: 'Thousands of IT admins worldwide use GFI LanGuard to scan networks for vulnerabilities, automate patching, and achieve compliance.',
        price: 30,
        values: {
            'SQL': 0,
            'NFS': 1,
            'NNTP': 0,
            'FTP': 1,
            'HTTP': 0.1,
            'MSRDP': 0.5,
            'POP3': 0,
            'SMTP': 0,
            'SSH': 0.2,
            'ICMP': 0,
            'Traceroute': 0,
            'TCP': 0,
        }
    },
    {
        rate: 0,
        name: 'NetIQ',
        os: 'win|mac|unix',
        url: 'https://www.netiq.com',
        description: 'NetIQ Corp. (Nasdaq: NTIQ), a leading provider of integrated systems and security management solutions, has been recognized by top industry research groups and publications.',
        price: 675,
        values: {
            'SQL': 1,
            'NFS': 0,
            'NNTP': 0,
            'FTP': 0,
```

```
            'HTTP': 0,
            'MSRDP': 0,
            'POP3': 0,
            'SMTP': 0,
            'SSH': 0.1,
            'ICMP': 0.5,
            'Traceroute': 1,
            'TCP': 1,
        }
    },
    {
        rate: 0,
        name: 'Qualys',
        os: 'unix',
        url: 'https://www.upguard.com/articles/tenable-vs-qualys',
        description: 'Continuous security and vulnerability detection—both Tenable and Qualys have built industry-leading suites around these two cybersecurity disciplines.',
        price: 295,
        values: {
            'HTTP': 0.2,
            'DNS': 1,
            'LDAP': 0,
            'SSH': 0,
            'ICMP': 1,
            'Traceroute': 1,
        }
    },
    {
        rate: 0,
        name: 'SAINT',
        os: 'unix',
        url: 'https://www.saintcorporation.com/',
        description: 'Protect your most critical business assets.Enterprise-power vulnerability management is now for everyone.',
        price: 0,
        values: {
            'HTTP': 0,
            'DNS': 0,
            'LDAP': 1,
            'SSH': 0.6,
```

```
                'ICMP': 1,
                'Traceroute': 1,
            }
        },
    ]
};
```

views/pages/index.ejs

```
<!doctype html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport"
        content="width=device-width, user-scalable=no, initial-scale=1.0, maximum-scale=1.0, minimum-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">

    <link href="https://fonts.googleapis.com/css?family=Roboto" rel="stylesheet">

    <link rel="stylesheet" href="//code.jquery.com/ui/1.12.1/themes/base/jquery-ui.css">
    <script src="https://code.jquery.com/jquery-1.12.4.js"></script>
    <script src="https://code.jquery.com/ui/1.12.1/jquery-ui.js"></script>
    <script>
        $( function() {
            const price_range_selector = '#price-range';
            $(price_range_selector).slider({
                range: true,
                min: 0,
                max: '<%= max_price %>',
                values: [ 0, '<%= max_price %>' ],
                slide: function( event, ui ) {
                    $("#price-from")[0].innerHTML = $(price_range_selector).slider( "values", 0);
                    $("#price-to")[0].innerHTML = $(price_range_selector).slider( "values", 1);
                }
            });
            $("#price-from")[0].innerHTML = $(price_range_selector).slider( "values", 0);
            $("#price-to")[0].innerHTML = $(price_range_selector).slider("values", 1);
        } );
    </script>

    <link rel="stylesheet" href="/css/app.css" >
```

```
</head>

<body>
<main>


  <header>
    <img src="/images/header.png">
    <div class="os-controls">
      <div class="os-controls-item active" data-os="win">
        <img src="/images/win.png">
      </div>
      <div class="os-controls-item " data-os="mac">
        <img src="/images/apple.png">
      </div>
      <div class="os-controls-item " data-os="unix">
        <img src="/images/linux-logo.png">
      </div>
      <h2 class="os-controls-label">select OS</h2>
    </div>

  </header>
  <div style="position: relative;">
    <div class="d-flex">
      <div class="w50" style="padding: 50px  90px">
        <h1 class="text-center color-grey">Choose Technologies and protocols</h1>


        <ul class="protocols-list">
          <li  class="protocol-item-wrapper">
            <label></label>
            <div>
              <span id="price-from" class="clr-main">0</span>
              <span><b></b></span>
              <span id="price-to" class="clr-main">0</span>
            </div>
          </li>
          <br>
          <br>
```

```
                    <li  class="protocol-item-wrapper" style="display:flex;align-items: center;">
                      <label style="display:flex;align-items: center;" class="clr-
main">Price</label>
                      <div id="price-range" ></div>
                    </li>
                    <br><br>

                    <li  class="protocol-item-wrapper">
                      <label></label>
                     <div>
                       <span>low(0)</span>
                       <span><b>Priority</b></span>
                       <span>hight(10)</span>
                     </div>
                    </li>
                    <br>

                    <% data.forEach(function(protocol) { %>
                    <li  class="protocol-item protocol-item-wrapper active">
                      <label><%= protocol %></label>
                      <input name="<%= protocol %>"  type="range" min="1" max="10"
value="5">
                    </li>
                    <% }); %>
                  </ul>
                </div>
                <div class="w50" style="padding: 50px; border-left: 1px solid grey;">
                  <h1 class="text-center color-grey">Result</h1>
                  <h2 class="no-result">
                    Please, choose priorities, OS and press run
                  </h2>
                  <div class="result hidden clr-main-light">
                    <h2 class="w-400">Best solution:</h2>
                    <h1 class="result-name">Name</h1>
                    <h2 class="w-400">Description</h2>
                    <h3 class="result-description">Description</h3>
                    <h2 class="w-400">Link:</h2>
                    <h3> <a class="result-url">link</a><hr></h3>
                  </div>
                  <div class="extra-result hidden">
```

```
                    <h2 class="text-center color-grey">Also look</h2>
                    <div class=" clr-main-light extra-result-template extra-result-item hidden">
                        <h3 class="text-right"><span class="d-unset extra-result-name">Name</span> - <a class="d-unset extra-result-url">link</a></h3>
                    </div>
                </div>

            </div>
        </div>
        <button class="btn btn-run" onclick="submit()">Run ...</button>
    </div>

</main>
</body>

<script src="/js/app.js"></script>

</html>
```

resources/scss/app.scss

```
 :not(head){
  box-sizing: border-box;
  font-family: inherit;
  display: block;
}
html {
  font-family: 'Century Gothic', sans-serif;
}
html, body, main {
  height: 100%;
  min-height: fit-content;
  background: black;
  margin: 0;
}
h1 {
  font-size: 32px;
}
.clr-main {
  color: #00ff03;
```

```
}
.clr-main-light {
  color: #77ff42;
}
a, a:visited {
  color: #7a3600;
}
.w-400 {
 font-weight: 400;
}
hr {
  border-color: grey;
}
main {
  width: 100%;
  background: linear-gradient(to right, #000, #003807);
}
header {
  width: 100%;
  position: relative;
  .os-controls {
    padding-bottom: 35px;
    position: absolute;
    bottom: 0;
    left: 38%;
    display: flex;
    justify-content: space-between;
    width: 28vw;
    img {
      padding: 5px;
      width: 55px;
      height: 45px;

    }
    .os-controls-item {
      cursor: pointer;
      &.active {
        background: url("/images/green_cloud.png");
        background-size: 100% 100%;
      }
```

```
    }
    .os-controls-label {
      position: absolute;
      bottom: 0;
      right: 0;
      color: #00ff03;
      margin: 0;
    }
  }
}
img {
  width: 100%;
}
.d-flex {
  display: flex;
}
.d-unset {
  display: unset;

}
.w50 {
  width: 50%;
}
.m-auto {
  margin: auto;
}
.text-center {
  text-align: center;
}
.text-right {
  text-align: right;

}
.color-grey {
  color: grey;
}
ul.protocols-list li.protocol-item {
  position: relative;
  display: flex;
  align-items: center;
```

```
  justify-content: space-between;
  color: grey;
  &:before {
    content: '';
    cursor: pointer;
    position: absolute;
    top: calc(50% - 7px);
    left: -20px;
    background: grey;
    width: 14px;
    height: 14px;
    border-radius: 100%;
  }
  label {
    cursor: pointer;
  }
  &.active {
    color: #00ff03;

    &:before {
      background: #00ff03;
    }
  }
  &:not(.active) {
    input {
      visibility: hidden;
    }
  }

}

//input range
.protocol-item-wrapper {
  display: flex;
  justify-content: space-between;

  label:first-child {
    width: 40%;

  }
```

```
  div:last-child {
    color: #7a3600;
    width: 100%;
    display: flex;
    justify-content: space-between;
  }
}

input[type=range] {
  -webkit-appearance: none; /* Hides the slider so that custom slider can be made */
  width: 100%; /* Specific width is required for Firefox. */
  height: 40px;
  cursor: pointer;
  background: transparent; /* Otherwise white in Chrome */
}

input[type=range]::-webkit-slider-thumb {
  -webkit-appearance: none;
}

input[type=range]:focus {
  outline: none; /* Removes the blue border. You should probably do some kind of focus styling for accessibility reasons though. */
}

input[type=range]::-ms-track {
  width: 100%;
  cursor: pointer;

  /* Hides the slider so custom styles can be added */
  background: transparent;
  border-color: transparent;
  color: transparent;
}


/* Special styling for WebKit/Blink */
input[type=range]::-webkit-slider-thumb {
  -webkit-appearance: none;
  border: 1px solid #000000;
```

```
  height: 18px;
  width: 6px;
  border-radius: 3px;
  background: #ffffff;
  cursor: pointer;
  margin-top: -6px; /* You need to specify a margin in Chrome, but in Firefox and IE it is automatic
*/
  box-shadow: 1px 1px 1px #000000, 0px 0px 1px #0d0d0d; /* Add cool effects to your sliders! */
}


input[type=range]::-webkit-slider-runnable-track {
  height: 3px;
background: #00ff03;
}

input[type=range]:focus::-webkit-slider-runnable-track {
  background: #00ff03  ;
}
//range input

.btn {
  background: black;
  color: #00ff03;
  border: 2px solid #00ff03;
  padding: 15px;
  font-size: 18px;
  cursor: pointer;
}
.btn-run {
  position: absolute;
  top: 400px;
  left: 50%;
  transform: translate(-50%, -50%);
}

.no-result {
padding-top: 250px;
  text-align: center;
  margin: auto;
```

```
}
.result {
  text-align: right;
}

.hidden {
  display: none;
}
.ui-widget-content {
  background: grey;
}
.protocol-item-wrapper div:last-child {
  height: 3px;
  border: 0;
}
.ui-slider-horizontal .ui-slider-range {
  background: #00ff03;
}
.ui-slider-horizontal .ui-slider-handle {
  -webkit-appearance: none;
  border: 1px solid #000000;
  height: 18px;
  width: 6px;
  border-radius: 3px;
  margin: 0;
  top: 50%;
  transform: translateY(-50%);
  cursor: pointer;
  &:focus {
    outline: 0;
    background: #fff;
  }
}

* {
  animation: fadein 2s;
  -moz-animation: fadein 2s; /* Firefox */
  -webkit-animation: fadein 2s; /* Safari and Chrome */
  -o-animation: fadein 2s; /* Opera */
}
```

```
@keyframes fadein {
  from {
    opacity:0;
  }
  to {
    opacity:1;
  }
}
@-moz-keyframes fadein { /* Firefox */
  from {
    opacity:0;
  }
  to {
    opacity:1;
  }
}
@-webkit-keyframes fadein { /* Safari and Chrome */
  from {
    opacity:0;
  }
  to {
    opacity:1;
  }
}
@-o-keyframes fadein { /* Opera */
  from {
    opacity:0;
  }
  to {
    opacity: 1;
  }
}
```

public/js/app.js

```
// Check / uncheck protocols
const protocol_item_selector = '.protocol-item';
const protocol_not_input_selector = '.protocols-list .protocol-item :not(input)';
const active_class = 'active';


document.querySelectorAll(protocol_not_input_selector).forEach((protocol_item) => {
```

```
    protocol_item.addEventListener('click', () => {
        protocol_item.closest(protocol_item_selector).classList.toggle(active_class);
    });
})
//////////


// Check OS
const os_controls_items_selector = '.os-controls .os-controls-item';

let os_controls_items_node = document.querySelectorAll(os_controls_items_selector);
os_controls_items_node.forEach((clicked_item) => {
    clicked_item.addEventListener('click', () => {
        os_controls_items_node.forEach((item) => {
            item.classList.remove(active_class);
        });
        clicked_item.classList.add(active_class);
    })
})
//////////




//send "run" request
const protocol_input_selector = '.protocols-list .protocol-item.active input';
const os_selector = '.os-controls .os-controls-item.active';
const no_result_selector = '.no-result';
const result_selector = '.result';
const result_name_selector = '.result .result-name';
const result_description_selector = '.result .result-description';
const result_url_selector = '.result .result-url';
const price_range_selector = '#price-range';
const extra_result_selector = '.extra-result';
const extra_result_template_selector = '.extra-result-template';
const extra_result_template_class = 'extra-result-template';
const extra_result_item_selector = '.extra-result-item';
const extra_result_name_selector = '.extra-result-name';
const extra_result_url_selector = '.extra-result-url';
```

```
const hidden_class = 'hidden';

function submit() {
    let data = {
        price: {
            from: 0,
            to: 0,
        },
        os: '',
        protocols: []
    };

    data.price.from = $(price_range_selector).slider( "values", 0 );
    data.price.to = $(price_range_selector).slider( "values", 1 );

    const os = document.querySelector(os_selector).dataset.os;
    data.os = os;

    document.querySelectorAll(protocol_input_selector).forEach((protocol) => {
        const name = protocol.getAttribute("name");
        const value = protocol.value;
        data.protocols.push({name: name, value: value});
    });

    /////////
    document.querySelector(no_result_selector).classList.remove(hidden_class);
    document.querySelector(result_selector).classList.add(hidden_class);
    document.querySelector(result_name_selector).innerHTML = '';
    document.querySelector(result_description_selector).innerHTML = '';
    document.querySelector(result_url_selector).href = ' ';
    document.querySelector(result_url_selector).innerHTML = '';
    /////////

    /////////
    document.querySelector(extra_result_selector).classList.add(hidden_class);
    document.querySelectorAll(extra_result_selector + ' '
        + extra_result_item_selector
        + ':not(' + extra_result_template_selector + ')').forEach((node) => {
```

```
    node.parentNode.removeChild(node);
  });
  /////////


  fetch('submit', {
    method: 'POST',
    headers: {
      "Content-Type": "application/json",
    },
    body: JSON.stringify(data)
  }).then((json_response) => {
    json_response.json().then((response) => {
      const best_result = response[0];
      if (best_result) {
        document.querySelector(no_result_selector).classList.add(hidden_class);
        document.querySelector(result_selector).classList.remove(hidden_class);
        document.querySelector(result_name_selector).innerHTML = best_result.name;
        document.querySelector(result_description_selector).innerHTML =
best_result.description;
        document.querySelector(result_url_selector).href = best_result.url;
        document.querySelector(result_url_selector).innerHTML = best_result.url;
        if (response.length > 1) {
          document.querySelector(extra_result_selector).classList.remove(hidden_class);



          for (let i = 1; i < response.length && i < 5; i++) {
            let node = document.querySelector(extra_result_template_selector).cloneNode(true);

            node.querySelector(extra_result_name_selector).innerHTML = response[i].name;
            node.querySelector(extra_result_url_selector).href = best_result.url;
            node.classList.remove(extra_result_template_class);
            node.classList.remove(hidden_class);

            document.querySelector(extra_result_selector).append(node);
          }
        }

      }
```

```
        })
    }).catch((error) => {
        console.log(error);
    })
}
```