Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студентки *Маркіної Марії Володимирівни*

академічної групи *125м-19-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *магістр*

на тему *Розробка програмно-методичних ресурсів для лабораторних робіт для теми «Сніфінг»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Флоров С.В.			
розділів:				
спеціальний	к.т.н., доц. Флоров С.В.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Тимофєєв Д.С.			

Дніпро
2020

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студентці *Маркіній Марії Володимирівні* **академічної групи** *125м-19-2*
(прізвище ім'я по-батькові) (шифр)

напряму підготовки *125 Кібербезпека*
(код і назва спеціальності)

на тему *Розробка програмно-методичних ресурсів для лабораторних робіт для теми «Сніфінг»*

затверджену наказом ректора НТУ «Дніпровська політехніка» від 22.10.2020 № 888-с.

Розділ	Зміст	Термін виконання
Розділ 1	*Аналіз актуальності та наукової новизни розробки програмно-методчного комплексу. Аналіз теоретичної складової.*	16.10.2020
Розділ 2	*Підготовка оточення для проведення лабораторних робіт та розробка методичних ресурсів.*	27.11.2020
Розділ 3	*Техніко-економічне обґрунтування доцільності запровадження запропонованих в роботі рішень.*	12.11.2020

Завдання видано _____ Флоров С.В
(підпис керівника) (прізвище, ініціали)

Дата видачі: 03.09.2020р.

Дата подання до екзаменаційної комісії: 11.12.2020р.

Прийнято до виконання _____ Маркіна М.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 74 с., 53 рис., 2 табл., 4 додатка, 21 джерело.

Об'єкт розробки: Розробка програмно-методичних ресурсів для лабораторних робіт з теми «Сніфінг».

Мета проекту: Підготовка програмно-методичних ресурсів для проведення лабораторних робіт в аудиторії 1/72.

У першому розділі обґрунтовано необхідність створення програмно-методичних ресурсів для лабораторних робіт з теми «сніфінг», проаналізовано актуальність питання, проведено планування розробки необхідних ресурсів для відповідних лабораторних робіт: обране середовище для виконання лабораторних робіт, а також інструменти, що будуть використовуватися в лабораторних роботах. Окрім цього, описана теоретична складова сфери кібербезпеки, що розглядається.

В другому розділі підготовлено методичні матеріали для дослідження можливостей інструментів для сніфінгу студентами, отримання ними практичних навичок, а також знань з теми «сніфінг». Також додано вказівки для налаштування оточення в аудиторії, в якій виконуватимуться роботи.

У третьому розділі визначено розмір капітальних витрат на створення програмно-методичного комплексу для лабораторних робіт з теми «сніфінг» та експлуатаційних витрат, які необхідні для проведення сніфінгу спеціалістом, а також величину втрат, яка може бути відвернена. Після чого розраховано загальний ефект від впровадження.

Практичне значення роботи полягає в тому, що розроблена низка лабораторних робіт з теми «Сніфінг», що реалізована на базі комп'ютерної лабораторії НТУ «Дніпровська політехніка», дозволить студентам оволодіти новими навичками та отримати нові знання, які є досить важливими для спеціаліста з інформаційної безпеки.

СНІФІНГ, КІБЕРБЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА, ЕТИЧНИЙ ХАКІНГ.

РЕФЕРАТ

Пояснительная записка: 74 с., 53 рис., 2 табл., 4 приложения, 21 источник.

Объект разработки: разработка программно-методических ресурсов для лабораторных работ по теме «Сниффинг».

Цель проекта: Подготовка программно-методических ресурсов для проведения лабораторных работ в аудитории 1/72.

В первом разделе обоснована необходимость создания программно-методических ресурсов для лабораторных работ по теме «сниффинг», проанализирована актуальность вопроса, проведено планирование разработки необходимых ресурсов для соответствующих лабораторных работ: выбрана среда для выполнения лабораторных работ, а также инструменты, которые будут использоваться в лабораторных работах. Более того, описана теоретическая составляющая сферы кибербезопасности, которая рассматривается.

Во втором разделе подготовлены методические материалы для исследования возможностей инструментов для сниффинга студентами, получения ими практических навыков, а также знаний по теме «сниффинг». Также добавлены указания для настройки окружения в аудитории, где будут проводиться работы.

В третьем разделе определен размер капитальных затрат на создание программно-методического комплекса для лабораторных работ по теме «сниффинг» и эксплуатационных расходов, необходимых для проведения сниффинга специалистом, а также величину потерь, которая может быть предотвращена. После чего рассчитан общий эффект от внедрения.

Практическое значение работы состоит в том, что разработанный ряд лабораторных работ по теме «Сниффинг», реализованный на базе компьютерной лаборатории НТУ «Днепровская политехника», позволит студентам овладеть новыми навыками и получить новые знания, которые являются достаточно важными для специалиста по информационной безопасности.

СНИФФИНГ, КИБЕРБЕЗОПАСТНОСТЬ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ЭТИЧЕСКИЙ ХАКИНГ.

THE ABSTRACT

Explanatory note: 74 pages, 53 figures, 2 table, 4 appendices, 21 sources.

Object of elaboration: creation of software-methodical resources for laboratory works for the topic "Sniffing".

The purpose of the project: Preparation of software and methodological resources for laboratory works in the classroom 1/72.

In the first section has been substantiated the need to create software and methodological resources for laboratory work on the topic of "sniffing", analyzed the relevance of the issue; plans to provide the necessary resources for laboratory works have been described: selected environment for laboratory work, as well as tools to be used in laboratory works. In addition, the theoretical component of the considered cyber security sphere have been described.

In the second section, methodological materials were prepared to explore the possibilities of tools for sniffing, so that students can get practical skills, as well as knowledge on the topic of "sniffing". Also there have been provided instructions for setting up an environment in the audience in which the work will be performed.

The third section defines the amount of capital expenditures for the creation of software and methodological resources for laboratory works on the topic of "sniffing" and operating costs required for sniffing by a specialist, as well as the amount of losses that can be avoided. Then the overall effect of the implementation has been calculated.

The practical significance of the work is that a number of laboratory works on the topic of "Sniffing", implemented on the basis of the computer laboratory of NTU "Dnipro Polytechnic", will allow students to acquire new skills and gain new knowledge that is very important for information security specialists.

SNIFFING, CYBER SECURITY, INFORMATION SECURITY, ETHICAL HACKING.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ПЗ – програмне забезпечення;

ОС – операційна система;

URL – Uniform Resource Locator;

ARP – Address Resolution Protocol;

FTP – File Transfer Protocol;

HTTP – Hypertext Transfer Protocol;

HTTPS – Hypertext Transfer Protocol Secure;

MAC – Media Access Control;

IP – Internet Protocol;

SMTP – Simple Mail Transfer Protocol.

ЗМІСТ

ВСТУП

На теперішній час можна стверджувати, що навчальна програма для спеціалістів з кібербезпеки включає в себе доволі багато теоретичного матеріалу і недостатню кількість певних практичних робіт для ознайомлення студентів з інструментами, які можуть використовуватися спеціалістами з інформаційної безпеки, етичними хакерами, тощо. Таким чином, спеціалісту, що закінчує навчання, бракує певних навичок для подальшої роботи. Наприклад, у навчальній програмі недостатньо матеріалів для вивчення такої теми як сніфінг. У той самий час, подібний аналіз трафіку є дуже важливим як для спеціалістів з кібербезпеки, що захищають інформаційні системи, так і для зловмисників, які здійснюють атаки на мережі, що захищаються спеціалістами. Отже, вивчення інструментів для проведення сніфінгу, може допомогти майбутнім спеціалістам отримати практичні навички з аналізу трафіку, зрозуміти механізми роботи деяких атак хакерів (а також продумати можливі механізми захисту), отримати необхідні знання щодо роботи мережі, а також протоколів, що розповсюджуються у мережі (знання принципів роботи протоколів є важливою для більшої кількості роботодавців у сфері кібербезпеки).

Для того, щоб студенти мали змогу отримати практичні навички а також знання в цій сфері кібербезпеки, необхідно створити низку лабораторних робіт, що дозволять ознайомитись з обраною темою та необхідними інструментами. Створенням методичних матеріалів для проведення таких лабораторних робіт, а також необхідною підготовкою лабораторії (встановленням необхідного програмного забезпечення, налаштуванням оточення – мереж, тощо) повинен займатись фахівець з інформаційної безпеки.

Для того, щоб розробити програмно-методичні ресурсів для лабораторних робіт з теми «Сніфінг», слід, перш за все, обрати оточення, в якому будуть виконуватися ці лабораторні роботи, а також обрати інструменти, що будуть використовуватися для дослідження теми «сніфінг». Після цього можуть бути

сформовані методичні матеріали з цієї теми, а також підготовлена лабораторія для проведення лабораторних робіт.

Таким чином, мета цієї роботи зводиться до розробки методичних матеріалів та підготовки програмного комплексу, а також необхідного оточення для проведення лабораторних робіт. Отримані результати зможуть стати прикладом створення матеріалів для проведення лабораторних робіт, які є більш націленими на практичні навички та вміння та можуть допомогти у реальній роботі спеціаліста з кібербезпеки.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про сніфінг мереж

Сніфінг – це процес моніторингу та захоплення всіх пакетів, що проходять через обрану мережу, за допомогою спеціальних інструментів. Сніфери пакетів, як правило, використовуються адміністраторами мережі для відстеження потоку даних, що проходить через їх мережу. Такі програми називаються аналізаторами мережевих протоколів. Таким же чином зловмисники можуть використовувати це ПЗ для перехоплення пакетів та їх аналізу – для цього їм просто необхідно бути підключеними до цільової мережі (саме тому важливо розмежовувати доступ до мережі, використовувати надійну аутентифікацію для доступу до неї, тощо).

Пакети даних, захоплені з мережі, використовуються для вилучення та викрадення конфіденційної інформації, такої як паролі, ідентифікатори користувачів, дані кредитних карток, тощо.

Після проведення сніфінгу, зловмисник також має змогу провести підміну пакетів та виконати атаку «людина посередині». Для цього зловмисник викрадає дані користувача та використовує їх у системі як законний користувач.

Сніфінг може мати як активний, так і пасивний характер. При пасивному сніфінгу трафік блокується, але він жодним чином не змінюється. Такий спосіб дозволяє лише збирати дані. Зазвичай пасивний сніфінг використовувався у мережах з хабами. У мережі, яка використовує хаби для підключення систем, усі хости в мережі можуть бачити трафік. Тому зловмисник може легко зафіксувати трафік, що проходить. Хороша новина полягає в тому, що хаби сьогодні майже застаріли. Більшість сучасних мереж використовують комутатори та роутери. Отже, пасивний сніфінг не є більш ефективним.

При активному сніфінгу трафік не тільки блокується і контролюється, але він також може бути певним чином змінений, як це визначається атакою. Активний сніфінг використовується для атак на мережі на основі комутатора. Він включає в себе введення пакетів протоколу ARP у цільову мережу для заповнення

таблиці адресованої пам'яті вмісту комутатора (CAM). CAM відстежує, який хост підключений до якого порту.

Протоколи, які є найбільш вразливими при сніффігу і найбільше цікавлять зловмисника при його проведенні:

– HTTP – Використовується для надсилання інформації у вигляді чистого тексту без будь-якого шифрування і, отже, є легкою ціллю.

– SMTP (Simple Mail Transfer Protocol) – в основному використовується для передачі електронної пошти. Цей протокол ефективний, але він не включає жодного захисту від сніфінгу.

– NNTP (Network News Transfer Protocol) - Він використовується для всіх типів комунікацій, але головним його недоліком є те, що дані та навіть паролі надсилаються через мережу як чистий текст.

– POP (Post Office Protocol) – використовується для отримання електронних листів від серверів. Цей протокол не включає захист від сніфінгу.

– FTP (File Transfer Protocol) – FTP використовується для надсилання та отримання файлів, але він не пропонує жодних функцій безпеки. Усі дані надсилаються у вигляді відкритого тексту, який можна легко перехопити.

– IMAP (Internet Message Access Protocol) – IMAP за своїми функціями такий самий, як SMTP, але він дуже вразливий до сніфінгу.

– Telnet – надсилає все (імена користувачів, паролі, натискання клавіш) по мережі як чистий текст, отже, його можна легко перехопити і використати. [1]

1.2 Обґрунтування необхідності створення програмно-методичних ресурсів для лабораторних робіт з теми «сніфінг», актуальність питання

Наукова новизна цієї роботи полягає в тому, що розроблений комплекс програмно-методичних ресурсів запропонує більш практичний підхід до навчання студентів, що дозволить їм отримати реальні навички у сфері кібербезпеки і стати більш кваліфікованими спеціалістами. Отримані знання також допомагатимуть студентам освоювати інші курси, в яких розглядаються атаки та взаємодія пристроїв у мережі.

Сніфінг мережі або аналіз пакетів є цінним вмінням для етичних хакерів і повинен бути частиною набору навичок кожного спеціаліста з інформаційної безпеки. Аналіз пакетів може допомогти зрозуміти, як трафік проходить через мережу, у якій проводиться сканування, які пакети надсилаються та які протоколи при цьому використовуються. Крім того, вміння проводити сніфінг дозволяє спеціалістам зрозуміти, для яких атак може бути вразливою мережа, а також усвідомити важливість захисту мереж. У навчальній програмі на теперішній час є досить мало інформації та лабораторних робіт щодо сканування мереж та відповідного аналізу трафіку. Впровадження таких робіт та відповідна розробка програмно-методичних ресурсів дасть змогу студентам отримати практичні навички зі сканування мереж та аналізу трафіку, ознайомитися з такими важливими протоколами, як ARP, ICMP, тощо. Також це допоможе отримати більше знань про можливі атаки, зокрема, атаку типу «людина посередині» і зрозуміти важливість створення паролів для бездротових мереж, використання протоколів з шифруванням (наприклад, HTTPS замість HHTP), а також виконання інших перевірених практик для захисту мережі від витоків інформації та підміни даних.

Таким чином, практичне значення роботи полягає в тому, що розроблена низка лабораторних робіт з теми «Сніфінг», що реалізована на базі комп'ютерної лабораторії НТУ «Дніпровська політехніка» дозволить студентам оволодіти новими навичками та отримати нові знання, які є досить важливими для спеціаліста з інформаційної безпеки.

1.3 Планування розробки програмно-методичних ресурсів для лабораторних робіт з теми «сніфінг»

1.3.1 Вибір середовища для проведення лабораторних робіт з теми «сніфінг»

Лабораторні роботи з теми «сніфінг» найкраще виконувати на віртуальних машинах, оскільки:

– Після створення та налаштування віртуальних машин, є можливість працювати зі стабільною конфігурацією системи, що означає, що немає

необхідності після зміни конфігурації перелаштовувати встановлене програмне забезпечення, що використовуватиметься у лабораторних роботах;

– Іноді використання програмного забезпечення для сніфінгу та проведення атак типу «людина посередині» може загрожувати безпеці мережі. Щоб ізолювати лабораторію, можна об'єднати віртуальні машини, що використовуються у лабораторних роботах, у необхідній підмережі, ізолювати цю мережу від решти комп'ютерів, які не повинні використовуватися у межах проведення лабораторних робіт;

– При використанні віртуальних машин є можливість використання одночасно декількох операційних систем, а також можлива взаємодія між ними. Таким чином, враховуючи, що більшість розроблених лабораторних робіт передбачатиме атакуючу машину та атаковану, студент зможе виконувати роботу на одному комп'ютері замість двох;

– Потенційно небезпечне програмне забезпечення, що використовується на віртуальних машинах не зашкодить хостовій системі. Це важливо, наприклад, при проведені атаки «людина посередині». Також на віртуальних машинах вимкнення фаєрволів та антивірусів не є таким критичним, як на звичайній робочій станції. При проведенні робіт з теми «сніфінг» може знадобитись вимкнення цих інструментів захисту;

– Більшість менеджерів віртуальних машин пропонують механізми збереження стану віртуальних машин – так звані снапшоти. За допомогою цієї можливості користувач може легко відновити стан віртуальної машини, якщо вона вийшла зі строю або її теперішній стан заважає виконувати роботу належним чином. Отже, навіть якщо при виконанні робіт віртуальна машина перестане функціонувати (наприклад, в результаті дій однієї з програм для проведення атак) – її попередній стан можна буде відновити;

– Також у багатьох менеджерах є можливість імпорту та експорту віртуальних машин, що дозволить налаштувати по одній віртаульній машині кожного типу, експортувати їх та імпортувати на всіх робочих станціях, де вони будуть необхідні;

– На вітруальній машині можна встановити саме необхідну операційну систему необхідної версії, що ніяк не вплине на роботу хостової машини;

– Якщо віртуальні машини стануть більше не потрібні – їх можна буде легко видалити, не ушкодивши жодної конфігурації на хостовій машині;

Слід зазначити, що існують і мінуси віртуальних машин, серед яких: необхідність мати на хостовій машині достатню кількість ресурсів (місця на диску, оперативної пам'яті, тощо), складність налаштування мережі в деяких менеджерах віртуальних машин і менша швидкість роботи однієї машини. Втім, можна стверджувати, що ресурсів на одній робочій станції обраної аудиторії достатньо для двох віртуальних машин – атакуючої і атакованої, а інші складності несуттєві, зважаючи на переваги. Отже, тепер необхідно обрати систему віртуалізації.

Існує два типи гіпервізорів. Гіпервізори першого типу працюють безпосередньо рівнем вище, ніж апаратне забезпечення комп'ютера і не потребують встановлення хостової операційної системи. У цьому випадку, вона працює на тому ж рівні, що й віртуальні машини. Для роботи ж гіпервізорів другого типу необхідна хостова операційна система, через як гіпервізор і буде отримувати доступ до апаратної частини машини. Тобто, гіпервізори другого типу працюють рівнем вище, ніж операційна система хостової машини. Вважається, що для установ чи підприємств краще підходять гіпервізори першого типу, в той час як гіпервізори другого типу частіше використовуються для персонального користування. Це зумовлюється тим, що другий тип простіше у використанні та їм легше керувати, а перший має вищу продуктивність. Зважаючи, що для запропонованого проекту важливіше продуктивність, а також на те, що університет є установою і рішення для корпоративної мережі, а не для домашнього користування, для нього є більш доречними, слід обрати віртуальні машини першого типу.

Найбільш популярними системами віртуалізації на сьогодні є Hyper-V та VMware. Hyper-V – це вбудований гіпервізор, який здатен створювати віртуальні машини в системах під керуванням ОС Windows. Його можна легко активувати на

хостовій машині під керуванням Windows 10, також можливо надавати права на керування гіпервізором певним користувачам або групам користувачів. Через те, що Hyper-V функціонує як роль Windows Server, ним можна керувати за допомогою Active Directory.

VMware vSphere – це платформа віртуалізації, що складається з безлічі компонентів, які потрібно встановити та налаштувати. По суті, vSphere - це набір продуктів для віртуалізації, які в поєднанні дозволяють створити обчислювальну платформу. В основі VMware vSphere лежить VMware ESXi, власний гіпервізор, який використовується для безпосереднього управління хост-серверами та запуску декількох гостьових віртуальних машин.

Згідно з думкою експертів [2], Hyper-V найбільше підходить для роботи коли:

– В інформаційній системі є існуюча платформа на базі Microsoft;

– Необхідна проста платформа для віртуалізації без будь-яких додаткових обчислювальних та функціональних вимог;

– Здійснюється керування сторонньою фізичною інфраструктурою (а не розташованою у хмарі, наприклад);

– Планується запустити віртуальні машини Windows;

З іншого боку, Hyper-V може не бути найкращим варіантом, якщо:

– Виконується багато оркестраційних дій, тобто інфраструктура є досить різноманітною і нею важко керувати без сторонніх інструментів, оскільки робота з Hyper-V у такому випадку буде займати більше часу, ніж з VMware.

– Важливим фактором є параметри віртуальних мереж.

Зі свого боку більш доречним вважається використання VMware, коли:

– Необхідна велика потужність, щоб дозволити велику кількість швидких змін;

– Вартість ліцензування не є проблемою;

– Потрібна інтеграція сторонніх розробників.

– В інформаційній системі потрібні складні параметри віртуальних мереж.

– В організації немає існуючої інфраструктури віртуальних машин та необхідно консолідувати їх усі на одній платформі.

З іншого боку, слід відмовитися від VMware, якщо:

– Інфраструктура в установі насамперед базується на Windows;
– В інформаційній системі вже існує централізоване управління системами Microsoft;
– Ви може виділити на гіпервізор лише низький бюджет.

Отже, роблячи висновок з вищезазначеного для проведення лабораторних робіт в аудиторії 1/72 слід обрати системи віртуалізації Hyper-V, щоб забезпечити цілісність інформаційного середовища та легко та централізовано керувати віртуальними машинами, правами та політиками для них.

1.3.2 Вибір програмного забезпечення для проведення лабораторних робіт з теми «сніфінг»

Проаналізувавши популярні курси на linkedIn learning та pluralsight, рекомендації ec-council та CompTIA, можемо сказати, що найбільш актуальними та використовуваними є такі сніффери як:

– Wireshark – один із найпопулярніших сніфферів, широко використовується мережевими інженерами, підтримується спільнотою, а отже безкоштовна для користувачів. Добре підходить для ознайомлення з мережевими протоколами. Доступний на Windows та linux; [5]
– SMAC – утиліта з графічним інтерфейсом, надає користувачеві можливість змінити фізичну адресу пристрою (MAC). Проста у використанні, допоможе зрозуміти, як можна змінити MAC-адресу для проведення атак; [20]
– Capsa network analyser – простий у використанні мережевий інструмент, який дозволяє контролювати, аналізувати, усувати несправності як в дротових, так і в бездротових мережах. Capsa має інтуїтивно зрозумілий та простий у використанні графічний інтерфейс, який не такий складний для

навчання, як інші подібні мережеві інструменти. Для цього інструмента існує безкоштовна демо-версія; [4]

– Cain and abel – інструмент для збору паролів для Microsoft Windows, найчастіше використовується для зламу паролів та атак типу «людина посередині», має можливості сніфінгу мережі, аналізу протоколів маршрутизації та запису VoIP-розмов. Інструмент розроблений головним чином для для спеціалістів з інформаційної безпеки та адміністраторів мереж, але це також корисний інструмент для тестувальників проникнення, викладачів та консультантів з питань безпеки; [12]

– Xarp tool – це програмне забезпечення, яке використовує передові методи виявлення атак з використанням пртоколу ARP. Використовуючи активні та пасивні модулі, XArp виявляє хакерів у мережі. Проста у використанні, працює з Windows та ubuntu системами. У безкоштовні можливості XArp входять: попередньо визначені рівні безпеки, моніторинг мережі та виявлення підміни ARP-протоколів; [13]

– Paessler PRTG – призначений для відстеження мережевого потоку. Дана програма самостійно може відслідковувати використання полос пропускання, час безвідмовної роботи та інші характеристики різних систем. Також існує функція збору статистики з різних мережевих елементів: комутаторів, маршрутизаторів, серверів та ін. Широко використовується системними адміністраторами. Добре підходить для складних мереж з розгалуженою інфраструктурою; [14]

– Steel Central Packet Analyzer – інструмент, призначений для аналізу мережі, який дозволяє досліджувати великі обсяги записаного трафіку. Повна інтеграція з Wireshark і інтуїтивно зрозумілий інтерфейс дозволяють ефективно і швидко локалізувати необхідний сегмент даних для аналізу. Підходить для роботи з великими та складними мережами. Добре показує себе в задачах, пов'язаних з аналізом роботи додатків (рівень мережі і додатків), веб-додатків, баз даних, IP-телефонії. Може виконувати простий і швидкий аналіз декількох пов'язаних потоків трафіку, захоплених різними пристроями, для швидкого

виявлення сегмента мережі, в якому спостерігаються проблеми з продуктивністю; [15]

– Fiddler – це веб-проксі програма, що використовується для дебагінгу, реєструючи весь трафік HTTP(S) між комп'ютером та Інтернетом. Fiddler включає потужну підсистему сценаріїв на основі подій і може бути розширена за допомогою будь-якої мови .NET. Fiddler є безкоштовною програмою і може налагоджувати трафік практично з будь-якої програми, яка підтримує проксі-сервер, включаючи Internet Explorer, Google Chrome, Apple Safari, Mozilla Firefox, Opera та багато інших. Використовується переважно розробниками та тестувальниками. Fiddler – проксі, який працює з трафіком між вашим комп'ютером і віддаленим сервером. [16]

– SolarWinds Network Packet Sniffer – може фіксувати уповільнення мережі, допомогає запобігти впливу сповільнення на кінцевого користувача, дозволяє зрозуміти, чи основна проблема пов'язана з конкретним додатком чи з мережею в цілому. Ця інформація на рівні пакетів надає адміністраторам найрелевантніші показники, включаючи час відгуку мережі та додатків, обсяг трафіку та кількість трафіку. Підходить для розробників та адміністраторів мереж. [11]

– OmniPeek – інструмент для аналізу протоколів, доступний лише на платформі Windows, за функціоналом схожий на Wireshark. Також у цьому ПЗ є функція відстеження мереж віддалено. Зазвичай застосовується для усунення несправностей у мережі. Існує безкоштовна демо-версія. [19]

– Tcpdump – це інструмент командного рядка, який за замовчуванням прослуховує найменший номер інтерфейсу (як правило, eth0), і повідомляє про весь трафік. Це може бути незручно, і найчастіше це просто занадто багато трафіку для сортування. Також зазвичай непотрібно бачити весь цей трафік. Через це tcpdump має комплексну систему фільтрації, яка дозволяє переглядати лише те, що необхідно, і ігнорувати інші пакети. Утиліта розроблена для unix систем, втім, є її адаптація і для Windows. [17]

– Sniff-o-matic – швидкий і простий інструмент для збору та аналізу мережевого трафіку системи, що більше підходить для досвідчених користувачів. Він фіксує мережевий трафік і дозволяє аналізувати дані. За допомогою цього програмного забезпечення можна продивитися інформацію про захоплені пакети у структурі дерева або в поданні необроблених пакетних даних. Може бути встановлений як безкоштовна пробна версія. [18]

Оскільки у попередньому розділі було обрано гіпервізор, що добре інтегровано з системами Windows, логічніше буде обрати для лабораторних робіт інструменти, що будуть працювати на базі саме цієї операційної системи. Також можна сказати, що інструменти для сніфінгу, розроблені для операційної системи Windows, зазвичай простіші та мають більш зручний графічний інтерфейс ніж програмне забезпечення для сніфінгу на linux. Таким чином, програми, що працюють на ОС Windows, більше підходять для ознайомлення з темою та для початку роботи з подібними інструментами, а отже більше підходять для студентів.

Також, слід відмовитися від інструментів, що розроблені для роботи зі складними розгалуженими мережами та великою кількістю пристроїв, оскільки у лабораторних роботах планується використати мінімальну кількість віртуальних машин. Не будемо використовувати також сніффери, що використовуються розробникми та тестувальниками, оскількі в таких програм інша мета і вони більш складні для розуміння.

Таким чином, із вищезазначеного списку популярного програмного забезпечення для сніфінгу слід обрати наступне: Wireshark, SMAC, Capsa network analyser, Cain and abel, Xarp tool, OmniPeek та Sniff-o-matic.

1.4 Висновок і постановка задач

У першому розділі було обґрунтувано необхідність створення програмно-методичних ресурсів для лабораторних робіт з теми «сніфінг», проаналізовано актуальність питання, після чого було проведено планування розробки необхідних ресурів для відповідних лабораторних робіт.

Було обране середовище для виконання лабораторних робіт – віртуальні машини у віртуальній мережі з використанням гіпервізора Hyper-V. Також було проведено аналіз популярного програмного забезпечення, що використовується при сніфінгу та обрані інструменти, що будуть використовуватися безпосередньо в лабораторних роботах.

Після цього, на основі отриманих даних, необхідно розробити методичні матеріали з використанням обраних інструментів в обраному оточенні, додати завдання для студентів щодо звітності з отриманих лабораторних робіт, що дозволять оцінити виконання завдань студентом та оцінити засвоєнні ним знання. Також, необхідно підготувати аудиторії 1/72 до проведення створених робіт, тобто встановити та налаштувати оточення та відповідне програмне забезпечення.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Підготовка віртуальних машин в аудиторії 1.72 для проведення лабораторних робіт з теми «сніфінг»

Перш за все, на робочій станції адміністратора необхідно дозволити використання засобів Hyper-V з робочих станцій студентів, тобто призначити їм необхідні дозволи. Також, потрібно підключити засоби Hyper-V на всіх робочих станціях. Зробити це можна наступним чином: натиснути правою кнопкою миші на меню Windows, обрати там пункт «програми та функції», натиснути справа вгорі «Пов'язані настройки – програми та засоби»; у меню, що з'явилося, зліва обрати пункт «Увімкнення або вимкнення засобів Windows», далі позначити галочкою пункт «Hyper-V», після цього підтвердити зміни. Потрібні пункти можна побачити на рисунку 2.1. Тепер комп'ютер необхідно перезавантажити. [3]

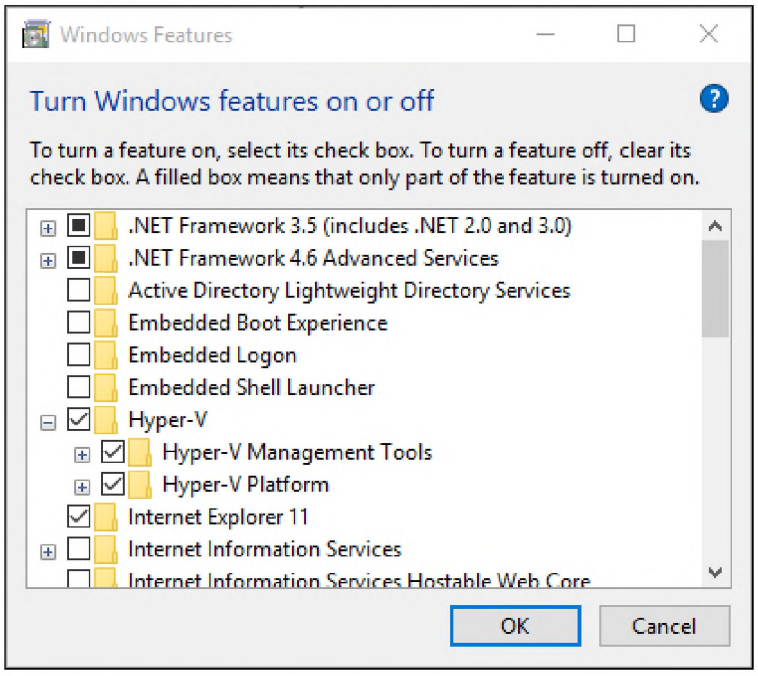


Рисунок 2.1 – Активація компонентів Hyper-V

Студенти виконуватимуть лабораторні роботи на двох віртуальних машинах Hyper-V: Windows 10 та Windows Server 2012. Розглянемо їх налаштування. Файли віртуальних машин розташовані за шляхом D:\Ceh_labs, як це можна побачити на рисунку 2.2.

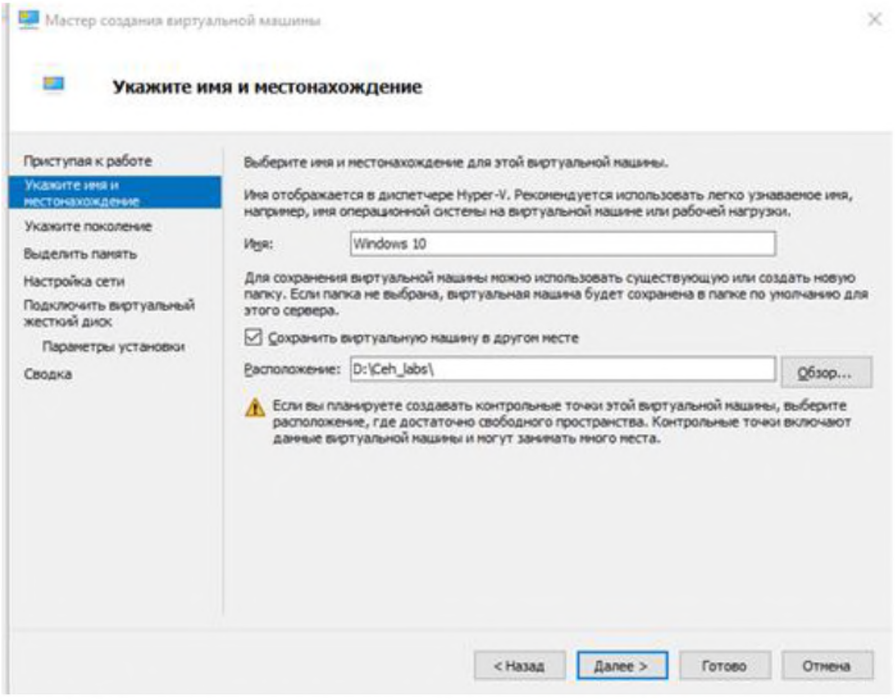


Рисунок 2.2 – Шлях розташування файлів віртуальних машин

Далі необхідно вказати покоління віртуальних машин, кількість ОЗУ та пам’яті на жорсткому диску, після чого вказати образ диску для встановлення ОС. Відповідні налаштування можна побачити на рисунках 2.3, 2.4, 2.5, 2.6 та 2.7. На кожну віртуальну машину виділено по 3 Гб ОЗУ (всього на хостовій машині 8Гб), для того щоб дві машини могли працювати одночасно.

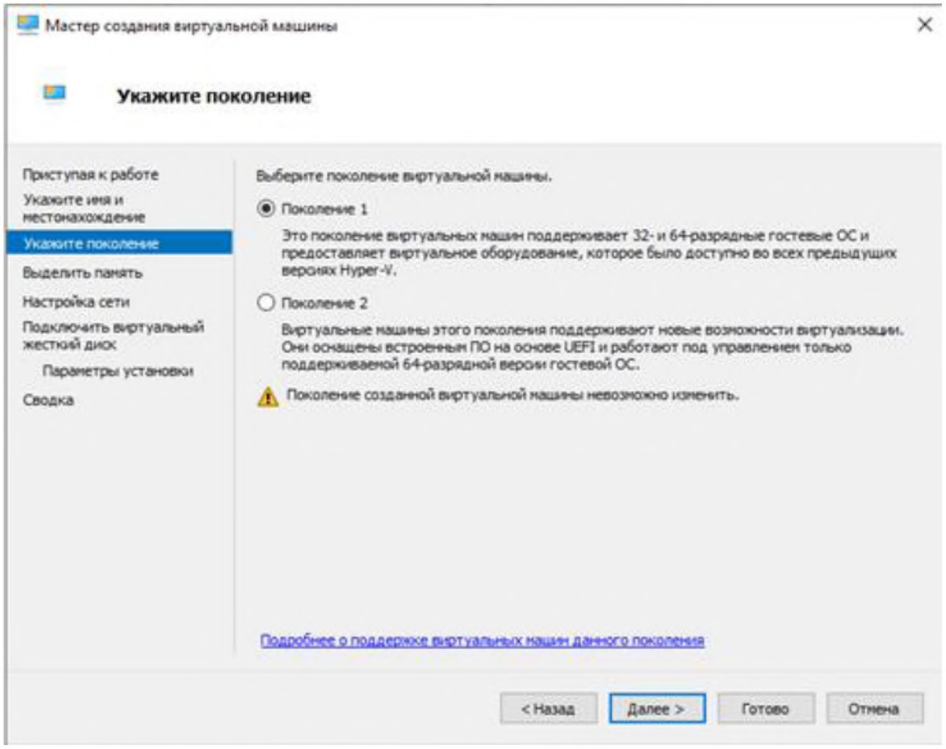


Рисунок 2.3 – Налаштування покоління віртуальної машини

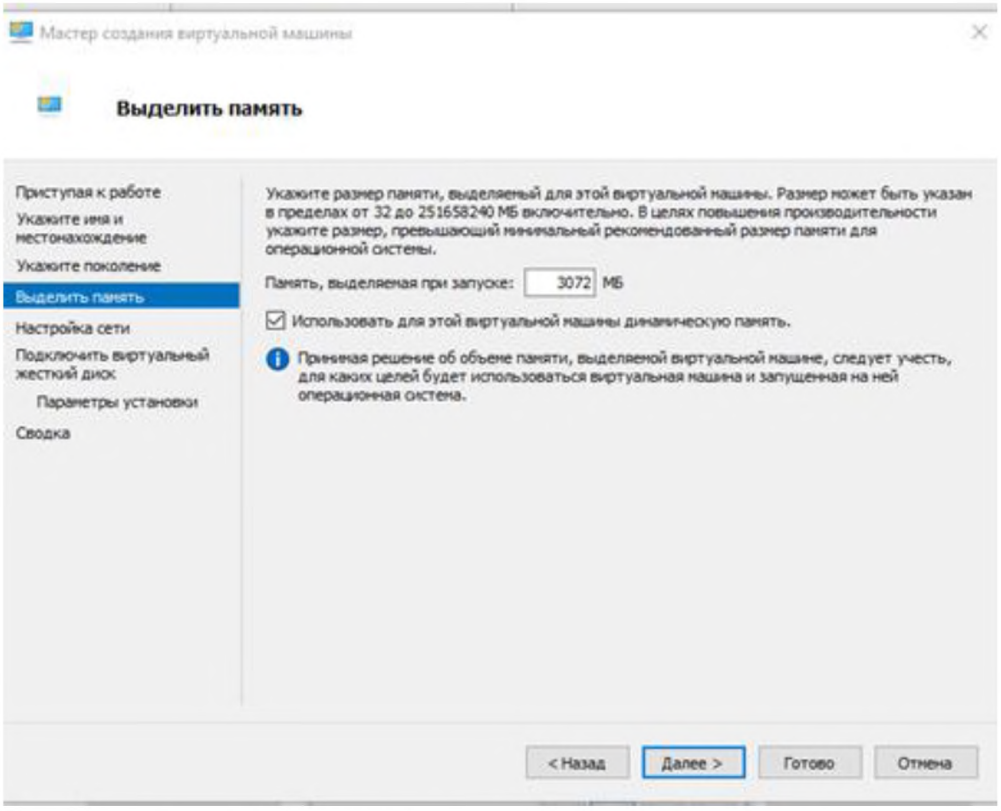


Рисунок 2.4 – Налаштування ОЗУ, що виділяється на одну віртуальну машину

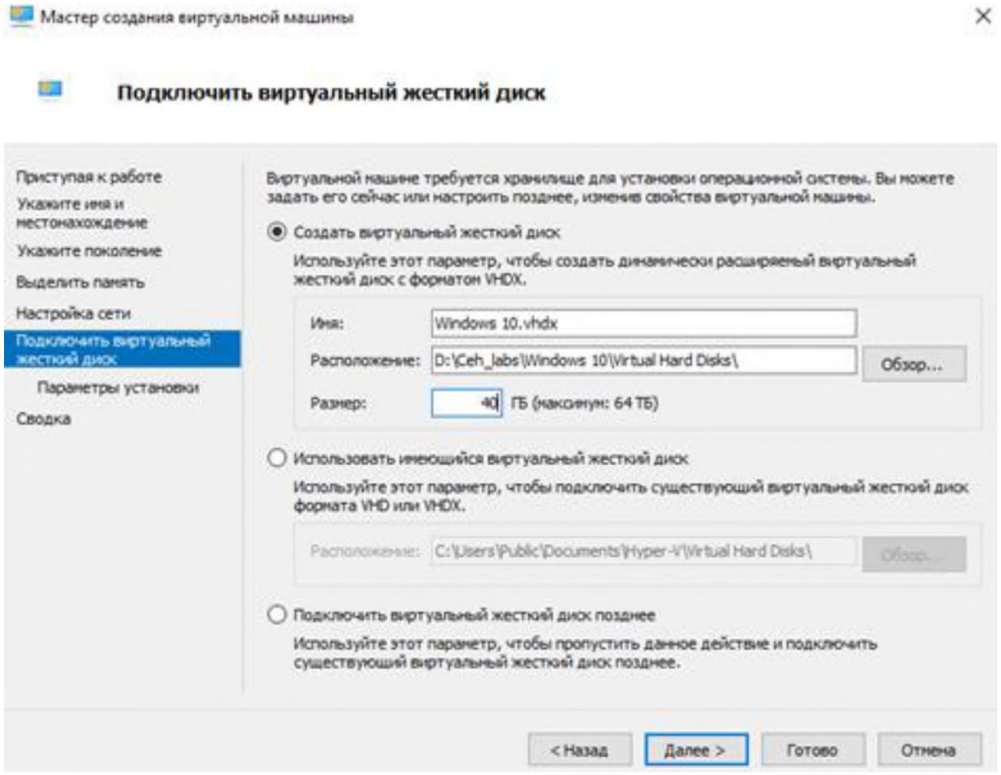


Рисунок 2.5 – Налаштування пам’яті, що виділяється на одну віртуальну машину

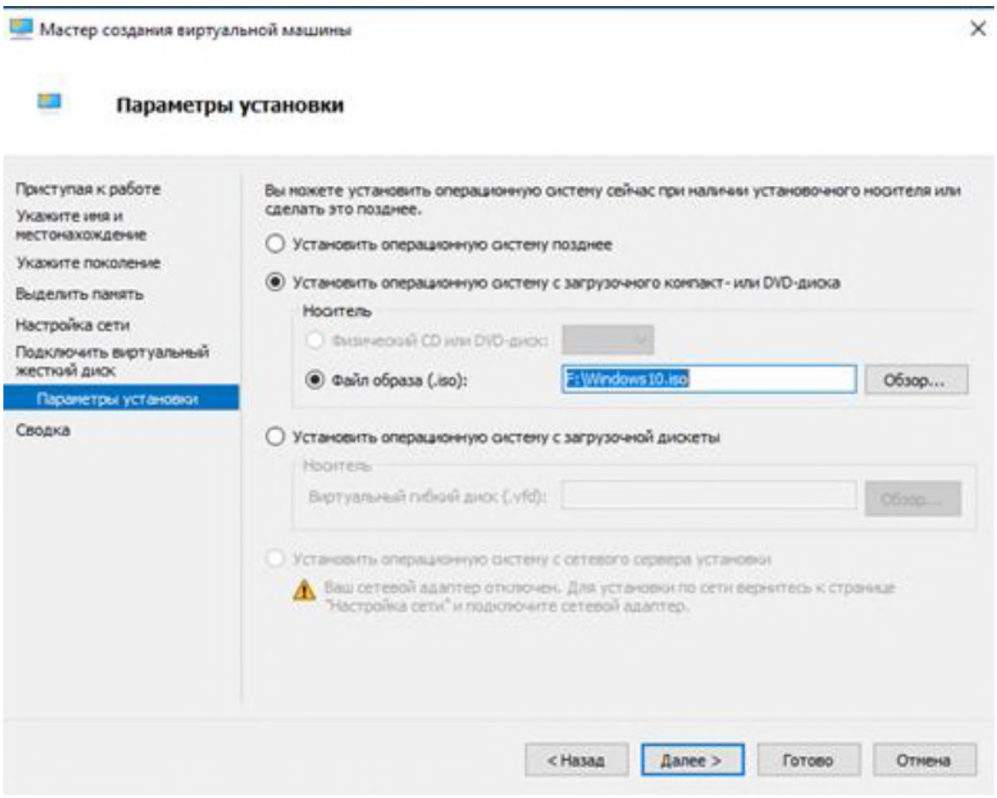


Рисунок 2.6 – Налаштування образу ОС

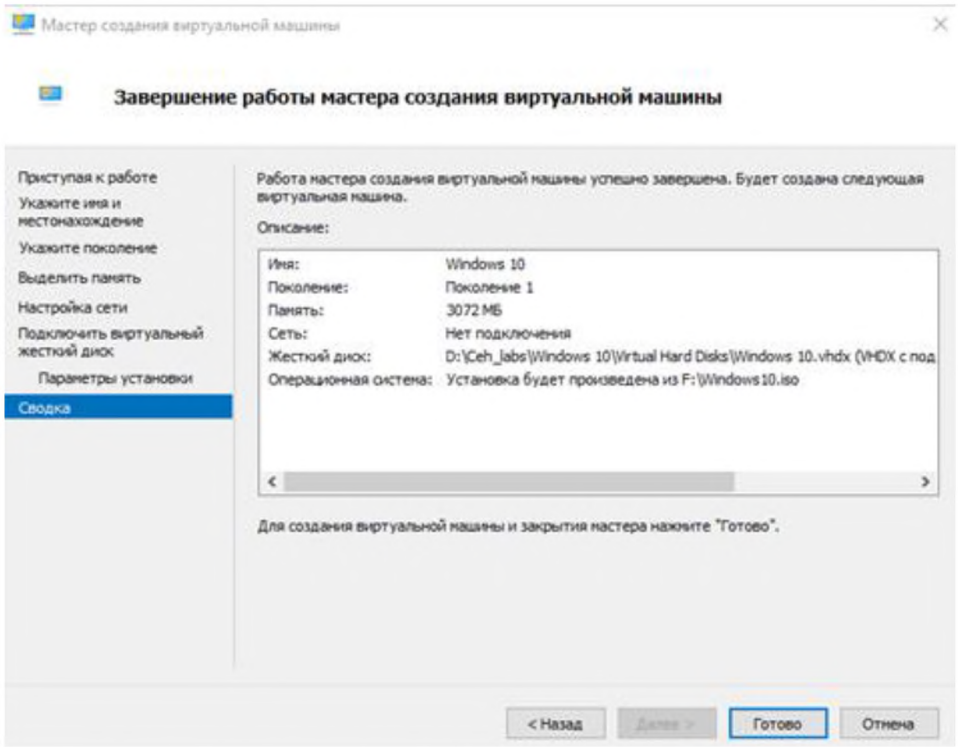


Рисунок 2.7 – Фінальна перевірка налаштувань

Після створення віртуальної машини, необхідно підключити її до віртуального комутатора, для того щоб атакована та атакуюча машина

знаходились в одній мережі. Створення віртуального комутатора та його підключення до віртуальної машини зображені на рисунках 2.8 та 2.9.

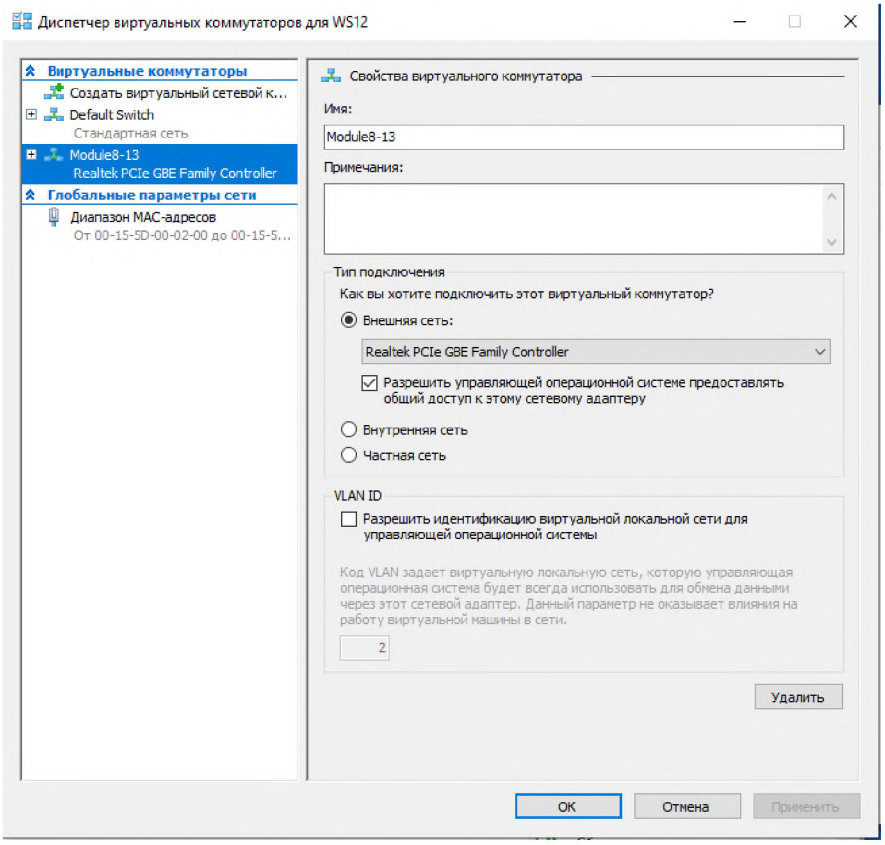


Рисунок 2.8 – Створення віртуального комутатора

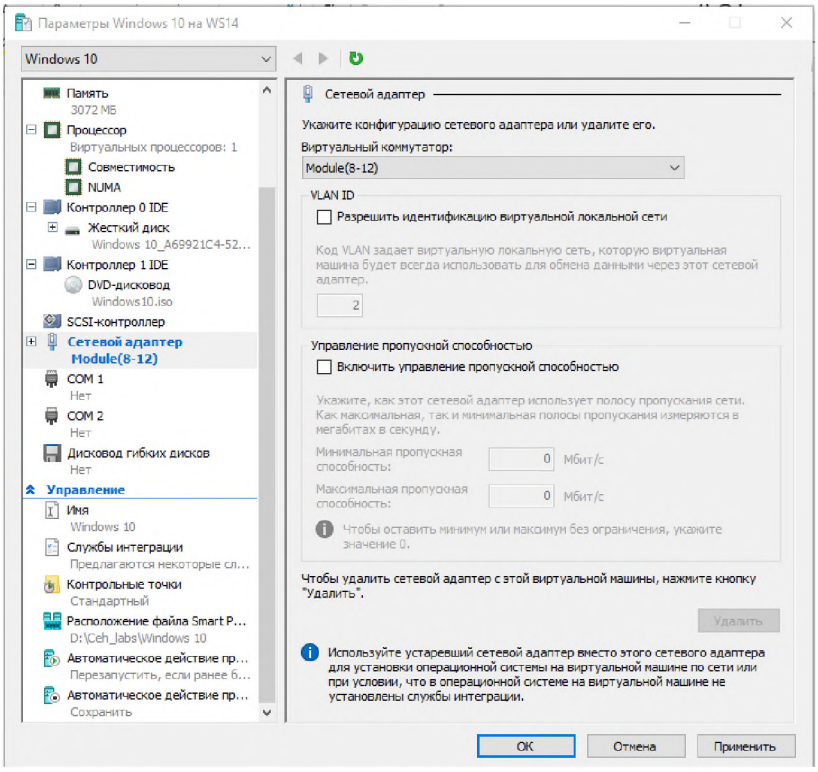


Рисунок 2.9 – Підключення віртуального комутатора до віртуальної машини

Віртуальну машину Windows 10 створено, після цього таким самим чином створюємо віртуальну машину Windows Server 2012. Як можна побачити на рисунках 2.10 та 2.11, на віртуальній машині Windows 10 створено обліковий запис Student, а на машині Windows Server 2012 – Administrator. В обох випадках пароль від облікового запису – Pa$$word.

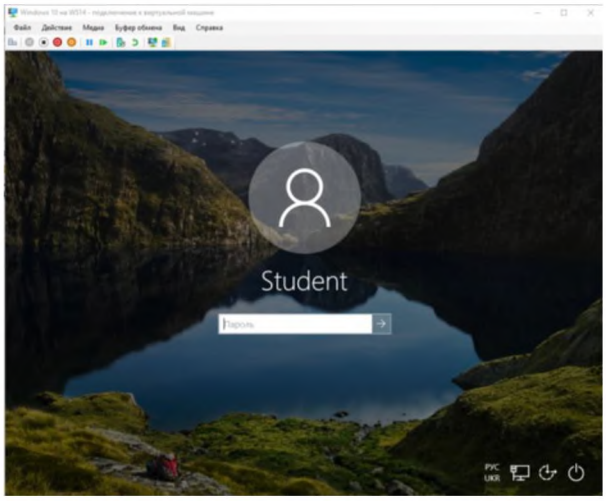


Рисунок 2.10 – Обліковий запис на Windows 10

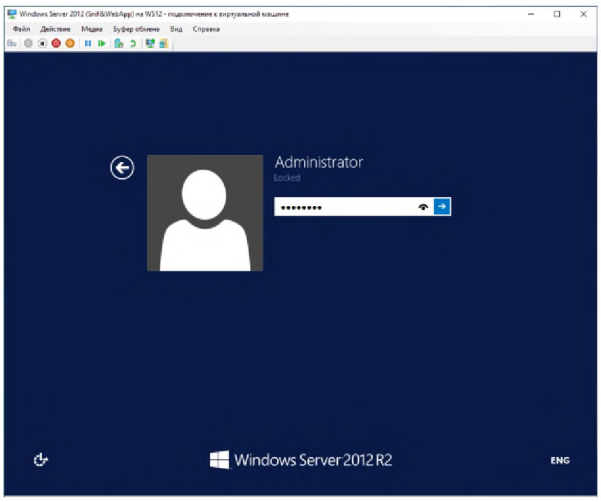


Рисунок 2.11 – Обліковий запис на Windows Server 2012

2.2 Підготовка програмного забезпечення в аудиторії 1.72 для проведення лабораторних робіт з теми «снiфінг»

Програмне забезпечення, необхідне для виконання лабораторних робіт, зазначене у таблиці 2.1. Також вказані джерела завантаження цього ПЗ (для виконання лабораторних робіт студентами вдома або у разі видалення його в аудиторії), номери лабораторних робіт, у яких зазначені програми

використовуються, та віртуальні машини, на які необхідно встановити це програмне забезпечення.

Таблиця 2.1 Програмне забезпечення, необхідне для виконання лабораторних робіт

Назва	Джерело для завантаження	Номери лабораторних робіт	Віртуальні машини	Додатково
OmniPeek	https://www.liveaction.com/products/omnipeek-network-protocol-analyzer/	1	Windows Server 2012	
SMAC 2.7	https://www.klcconsulting.net/smac/	2	Windows 10	Ключ для активації: SMC2U-00C8-4001-0100-F71F-8C4D
capsa natwork analyser	https://www.colasoft.com/capsa/	3	Windows server 2012	Для завантаження ПЗ необхідно зареєструватися
Wireshark	https://www.wireshark.org/download.html	4	Windows server 2012	
Cain and abel	https://qpdownload.com/link.php?name=c ain-and-abel	5, 6	Хостова машина Windows 10*	Для коректної роботи програми необхідно встановити та запустити winpcap
Xarp tool	www.xarp.net/#download	6	Windows server 2012	
Sniff-o-matic	www.softsea.com/download/Sniff-O-Matic.html	7	Windows server 2012	

Для виконання деяких лабораторних робіт та коректної роботи вищезазначеного ПЗ на віртуальних машинах необхідно встановити додаткове програмне забезпечення. Воно зазначено у таблиці 2.2.

Таблиця 2.2 Додаткове програмне забезпечення

Назва	Джерело для завантаження	Віртуальні машини
WinRar	https://www.win-rar.com/start.html?&L=4	Windows Server 2012, Windows 10
.net framework	https://dotnet.microsoft.com/download/dotnet-framework	Windows Server 2012, Windows 10
.net core	https://dotnet.microsoft.com/download/dotnet-core/current/runtime	Windows Server 2012, Windows 10
npcap	https://nmap.org/npcap/	Хостова Windows 10

2.3 Підготовка методичних матеріалів для лабораторних робіт з теми «сніфінг»

2.3.1 Підготовка до проведення лабораторних робіт

Для проведення деяких лабораторних робіт необхідно вимкнути фаєрвол на обох віртуальних машинах. На рисунках 2.12, 2.13, 2.14, 2.15 показано як це зробити. На машині Windows 10 необхідно натиснути «вимкнути» фаєрвол для мережі домену, приватної мережі та загальнодоступної мережі. На машині Windows Server 2012 необхідно перейти до пункту меню «Turn Windows Firewall on or off» та вимкнути захист для приватних та публічних мереж.

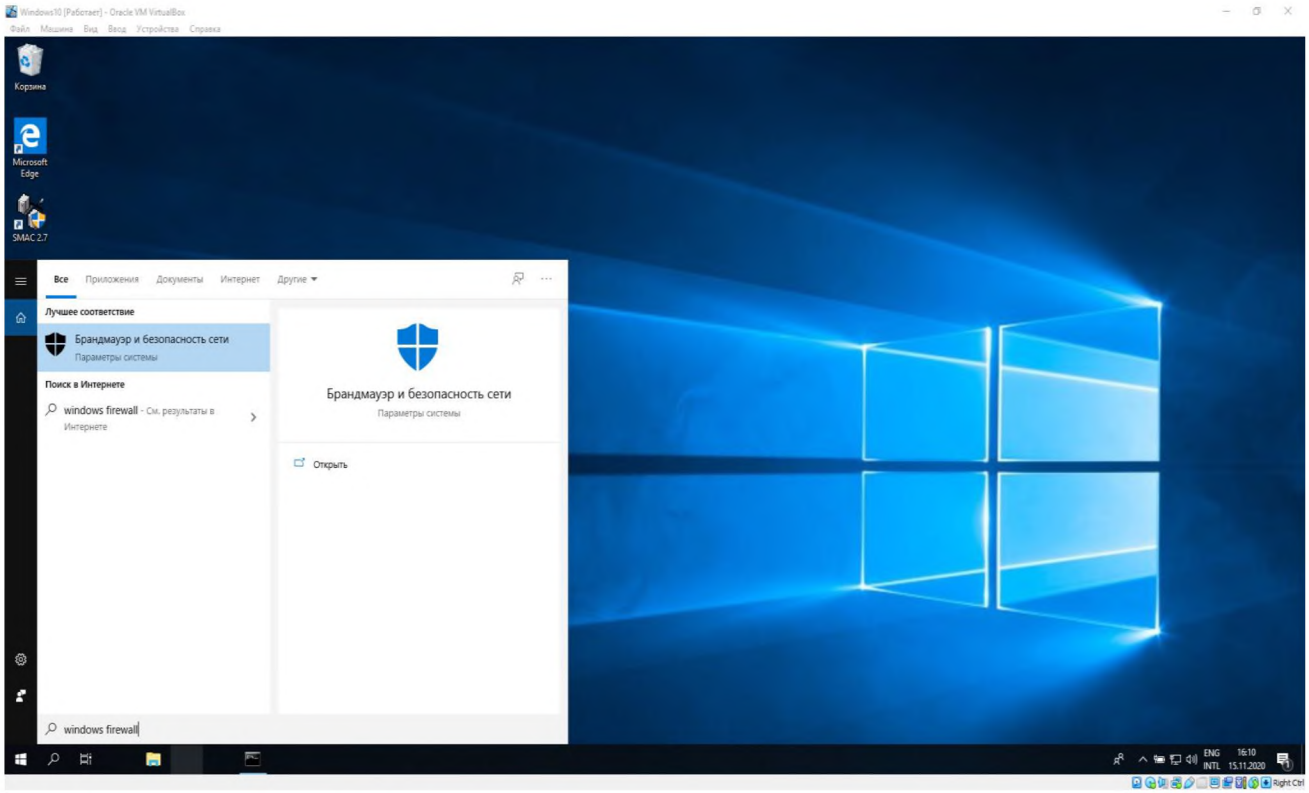


Рисунок 2.12 – Перехід до брандмауеру Windows 10

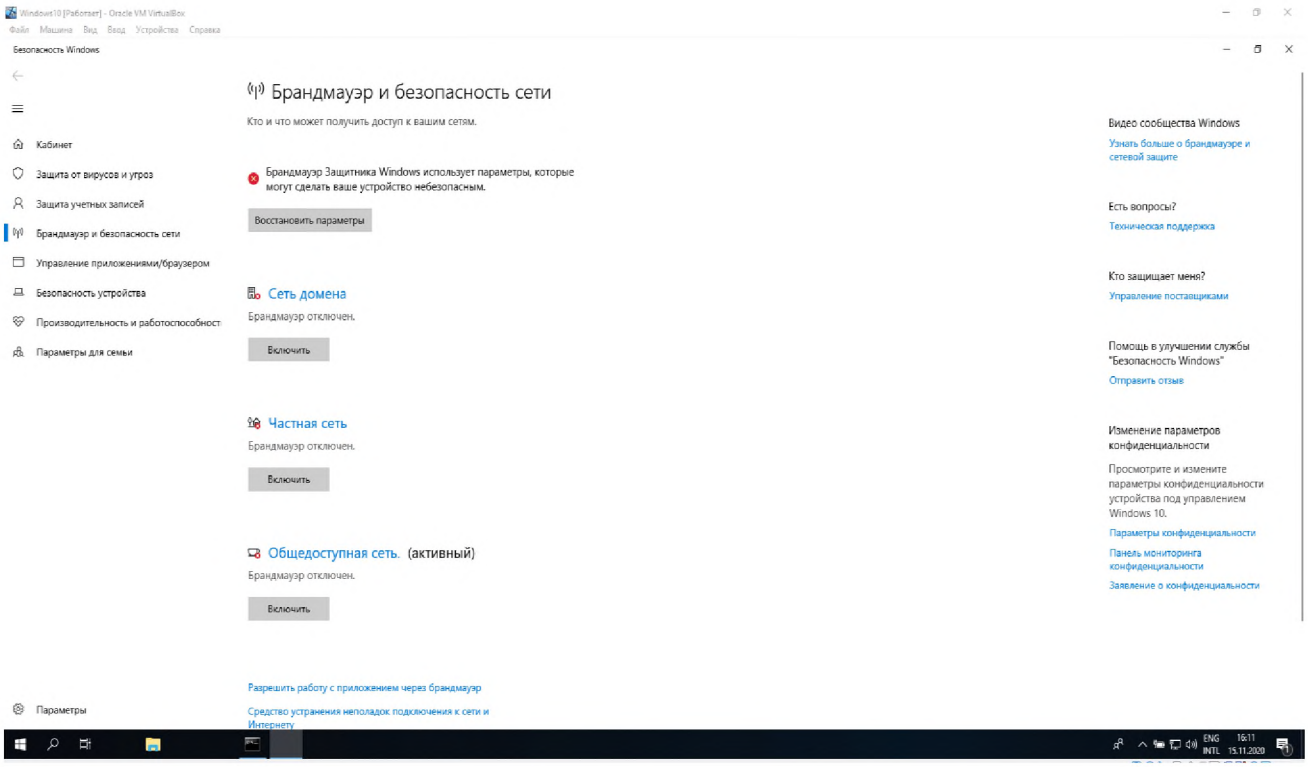


Рисунок 2.13 – Вимкнення брандмауеру

Рисунок 2.14 – Перехід до брандмауеру Windows Server 2012

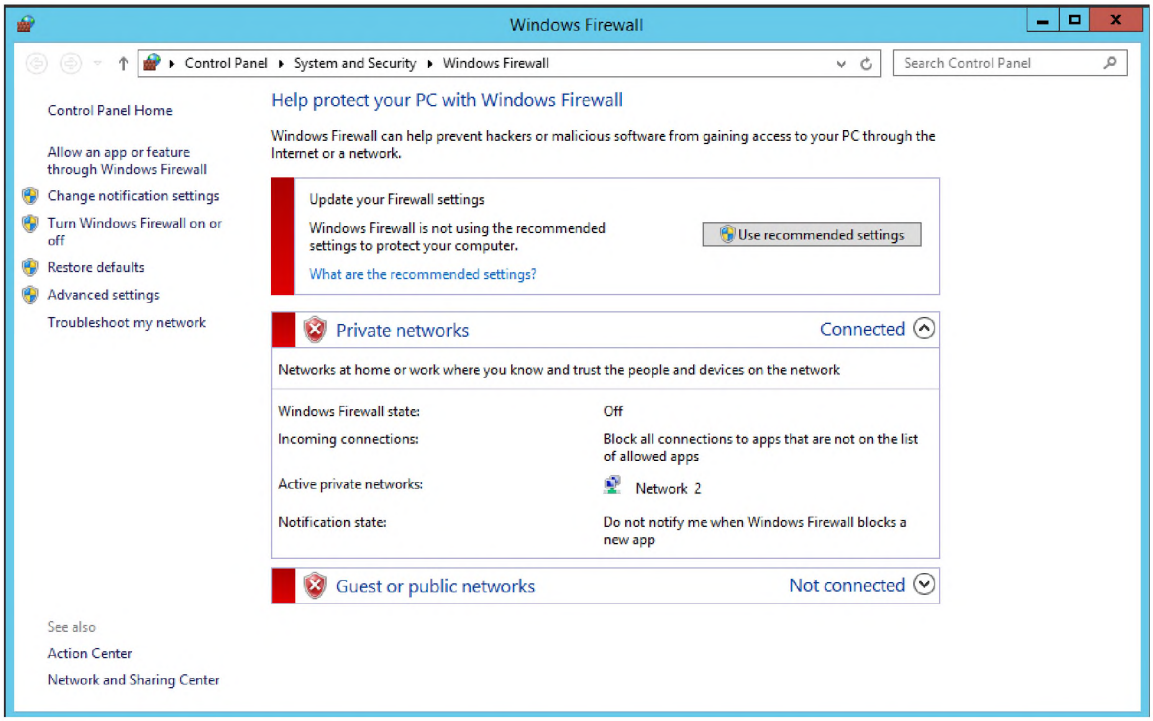


Рисунок 2.15 – Вимкнення брандмауеру Windows Server 2012

2.3.2 Сніфінг мережі за допомогою OmniPeek Network Analyzer

OmniPeek Network Analyzer - це програмне забезпечення, розроблене компанією Savius, яке використовується для моніторингу Інтернет-мереж. Цей аналізатор пакетів здатен перевірити ефективність підключення та виявити

області, які споживають найбільшу пропускну здатність. Дані про бездротові точки доступу, протоколи та багато іншої інформації також легко збираються за допомогою цього програмного забезпечення.

Мета лабораторної роботи: ознайомлення з інструментами для аналізу мережі, вивчення їх можливостей, аналіз захоплених пакетів.

Для цієї лабораторної роботи необхідне наступне:

– OmniPeek Network Analyzer, що знаходиться за шляхом C:\Program Files (x86)\Wild Packets\OmniPeek Demo\omnipeek.exe на віртуальній машині Windows server 2012;
– Windows 10 як цільова (атакована) машина;
– Будь-який інтернет-браузер;
– Встановлений Microsoft .NET Framework 2.0 або новішої версії.

Необхідний час для виконання лабораторної роботи: 20 хвилин.

Хід роботи:

1. Перш за все, необхідно запустити OmniPeek Network Analyzer, що знаходиться за вищезазначеним шляхом. Запущена програма зображена на рисунку 2.16.

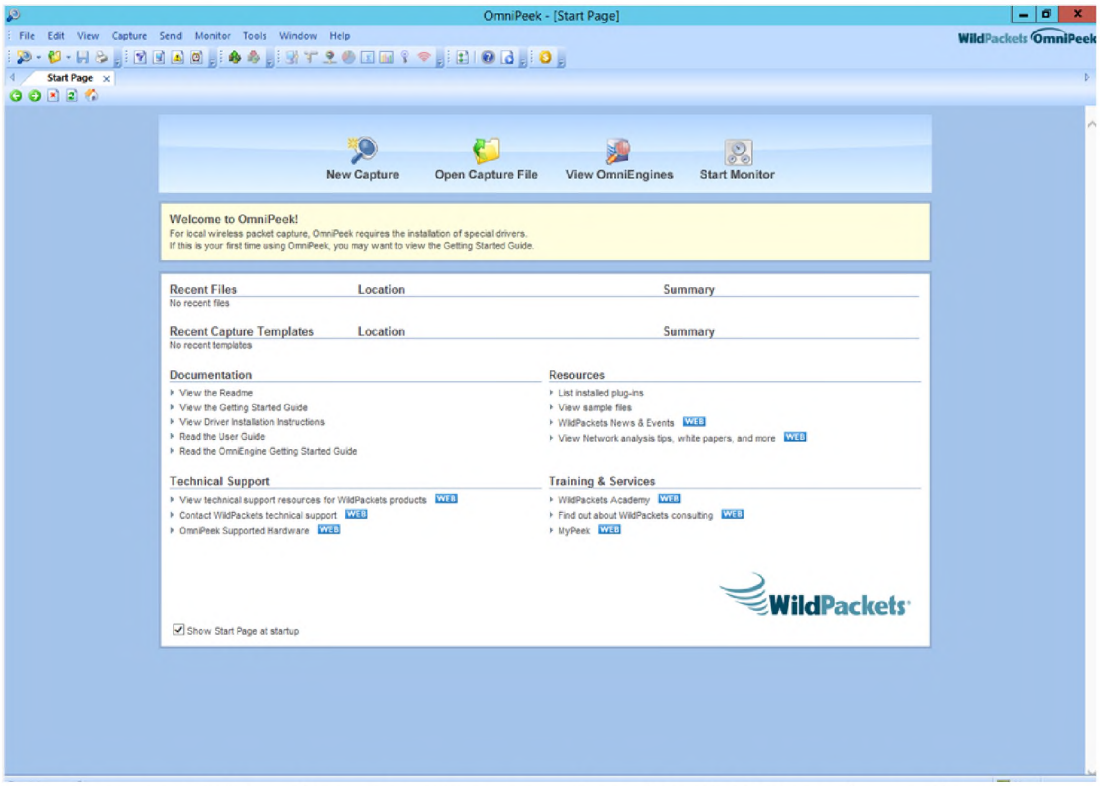


Рисунок 2.16 – Стартовий екран OmniPeek Network Analyzer

2. Увійдіть до віртуальної машини Windows 10. Вимкніть фаєрвол на обох машинах.

3. Тепер на віртуальній машині Windows Server 2012 можна перейти до розділу меню «New Capture» («нове захоплення пакетів»). Меню, що з'явиться, можна побачити на рисунку 2.17. У цьому меню перевірте налаштування та клацніть «ОК». Зверніть увагу на кількість даних, що зараз відображаються при захопленні.

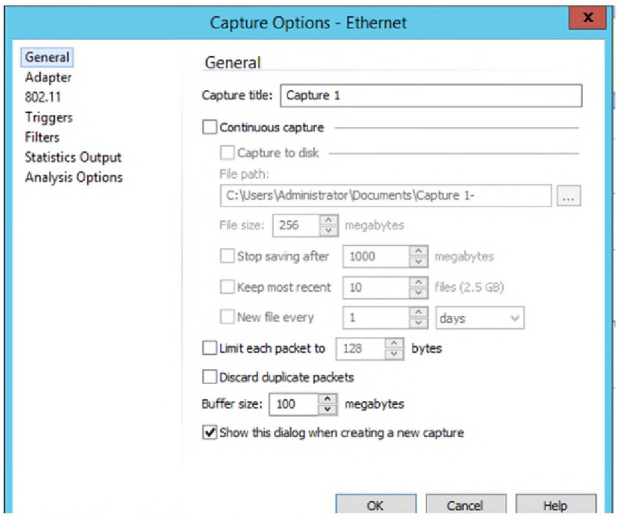


Рисунок 2.17 – Меню нового захоплення пакетів

4. Поверніться Windows 10, зайдіть до браузеру та перейдіть на декілька сайтів. Наприклад, це може бути gde-fon.com. Проаналізуйте зміни, що можна побачити в OmniPeek Network Analyzer. Результат може подібним до того, що зображено на рисунку 2.18. Збережіть скріншот для звіту з лабораторної роботи.

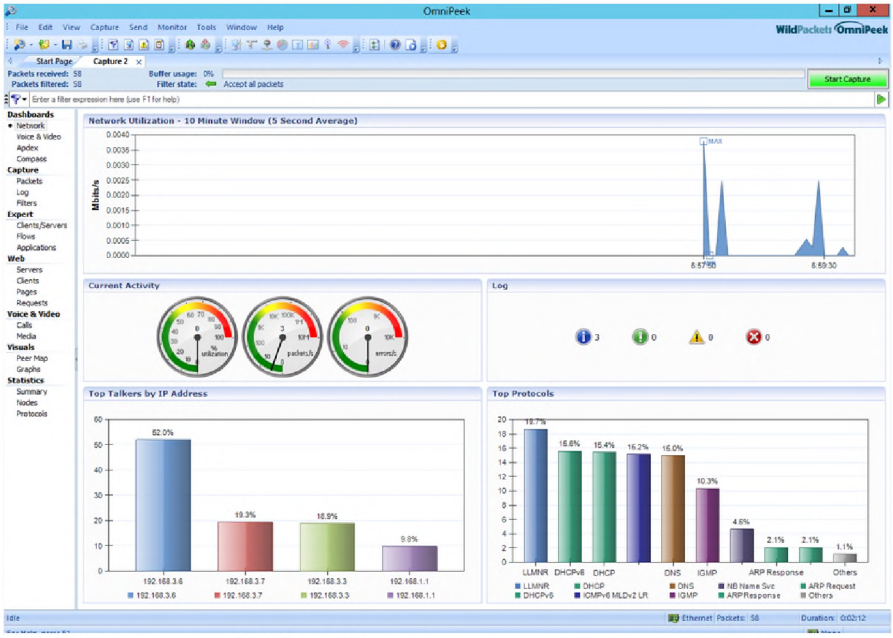


Рисунок 2.18 – Процес захоплення пакетів

5. Щоб відобразити захоплені пакети, оберіть Packets у секції Capture на лівій панелі вікна. На рисунку 2.19 зображена утворена таблиця з пакетами.

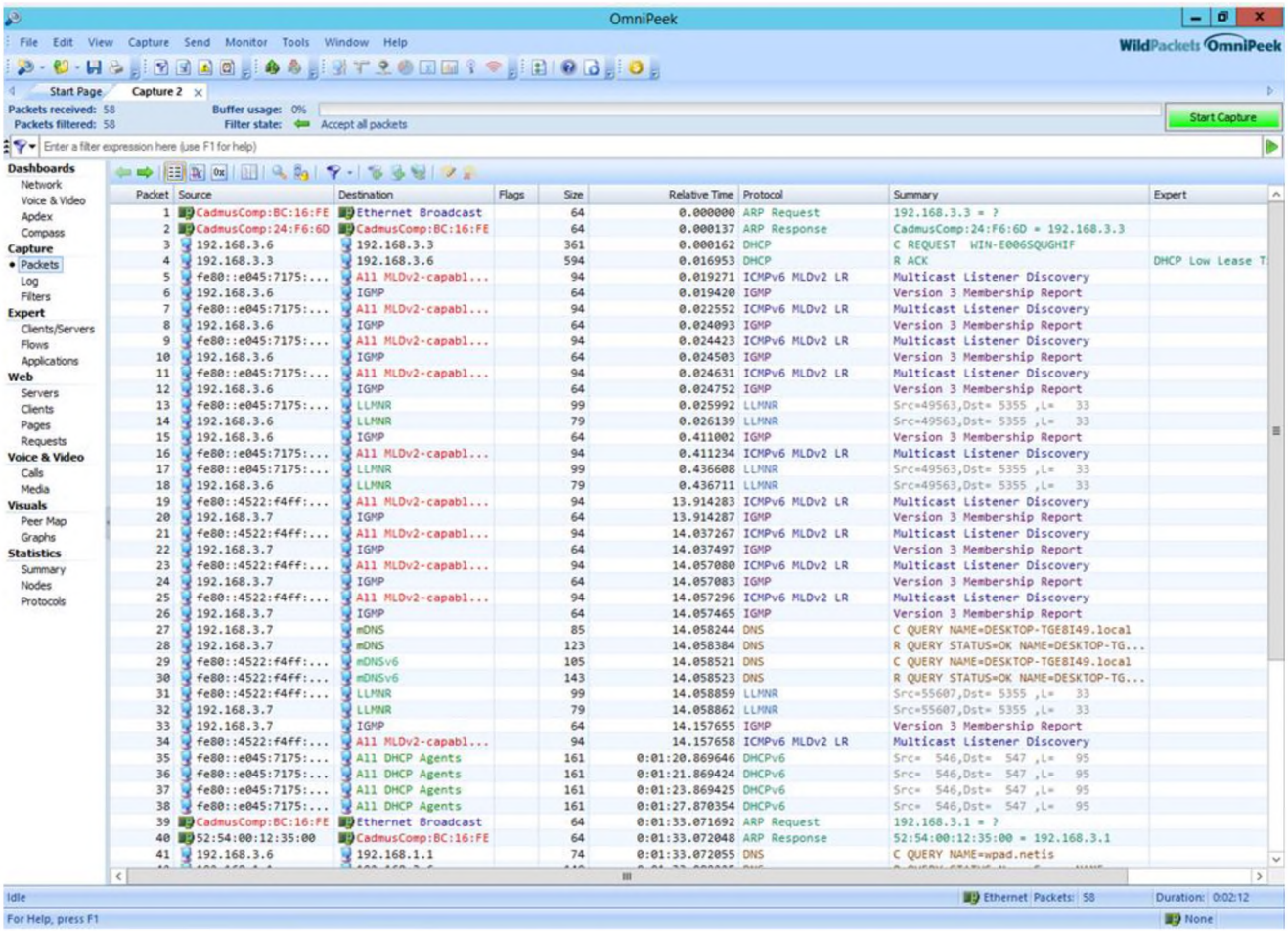


Рисунок 2.19 – Таблиця з захопленими пакетами

Спробуйте відфільтрувати один з протоколів, наприклад протокол ARP, як це показано на рисунку 2.20. Збережіть скріншот для звіту з лабораторної роботи, опишіть обраний протокол у звіті.

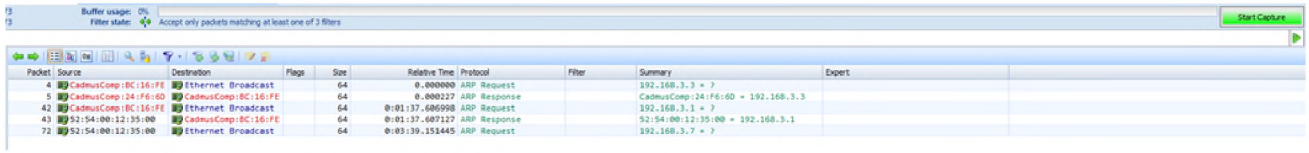


Рисунок 2.20 – Відфільтровані протоколи ARP

6. У цьому ж вікні можна переглянути певний пакет, для цього просто оберіть його і внизу з'явиться його склад, як це зображено на рисунку 2.21. Знайдіть серед цієї інформації номери портів, зробіть скріншот, додайте його до звіту та опишіть, чому один з номерів портів саме такий.

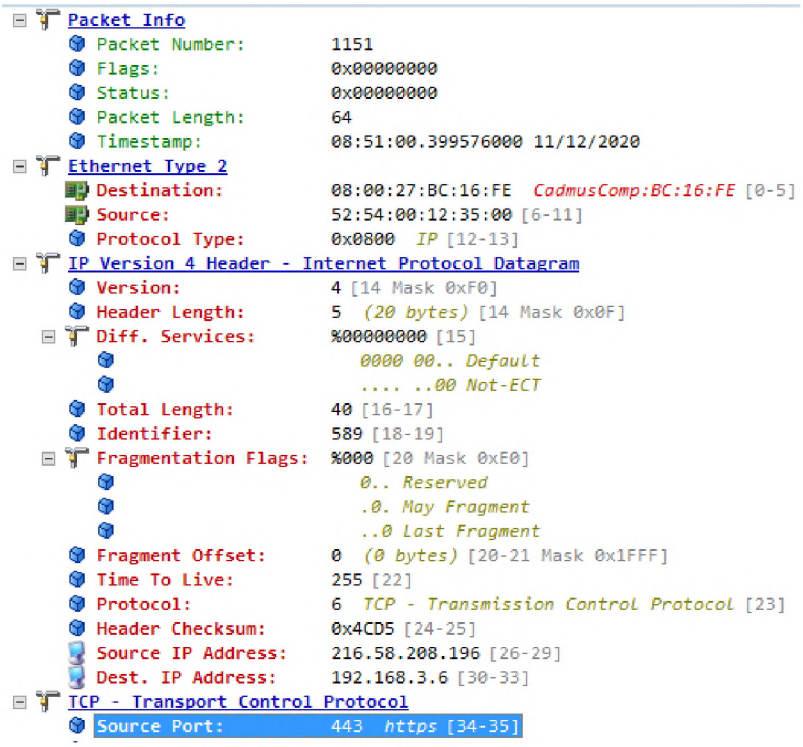
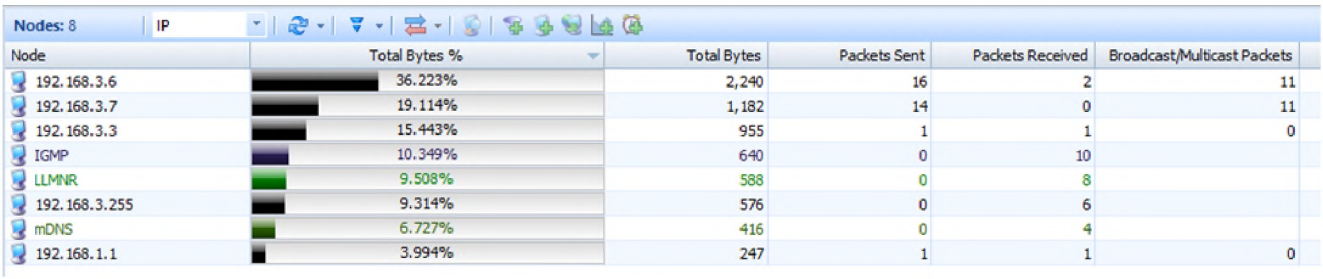


Рисунок 2.21 – Інформація про пакет

7. Таким же чином ви можете відобразити лог (Log), фільтри (Filters), ієрархію (Hierarchy) і мапу пірів (Peer Map), обравши відповідну опцію. Також можна переглянути вузли (Nodes) та протоколи (Protocols) в секції Statistics на лівій панелі вікна. Після цього слід відобразити повний підсумок за вашою мережею із секції Statistics в лівій панелі вікна. Спробуйте знайти кількість отриманих і

надісланих пакетів віртуальними машинами Windows 10 та Windows Server 2012 (для цього дізнайтеся ip-адреси відповідних машин, виконавши команду ipconfig у cmd). Результати можуть виглядати приблизно як на рисунку 2.22. Збережіть скріншот для звіту з лабораторної роботи, опишіть його.



Nodes: 8 | IP

Node	Total Bytes %	Total Bytes	Packets Sent	Packets Received	Broadcast/Multicast Packets
192.168.3.6	36.223%	2,240	16	2	11
192.168.3.7	19.114%	1,182	14	0	11
192.168.3.3	15.443%	955	1	1	0
IGMP	10.349%	640	0	10	
LLMNR	9.508%	588	0	8	
192.168.3.255	9.314%	576	0	6	
mDNS	6.727%	416	0	4	
192.168.1.1	3.994%	247	1	1	0

Рисунок 2.22 – Вкладка «Nodes»

8. Для збереження результатів, оберіть File – Save Report.

Оберіть бажаний формат звіту у вікні Save Report, потім натисніть Save.

Продивіться отриманий програмою звіт. Він виглядає, як зображено на рисунку 2.23.

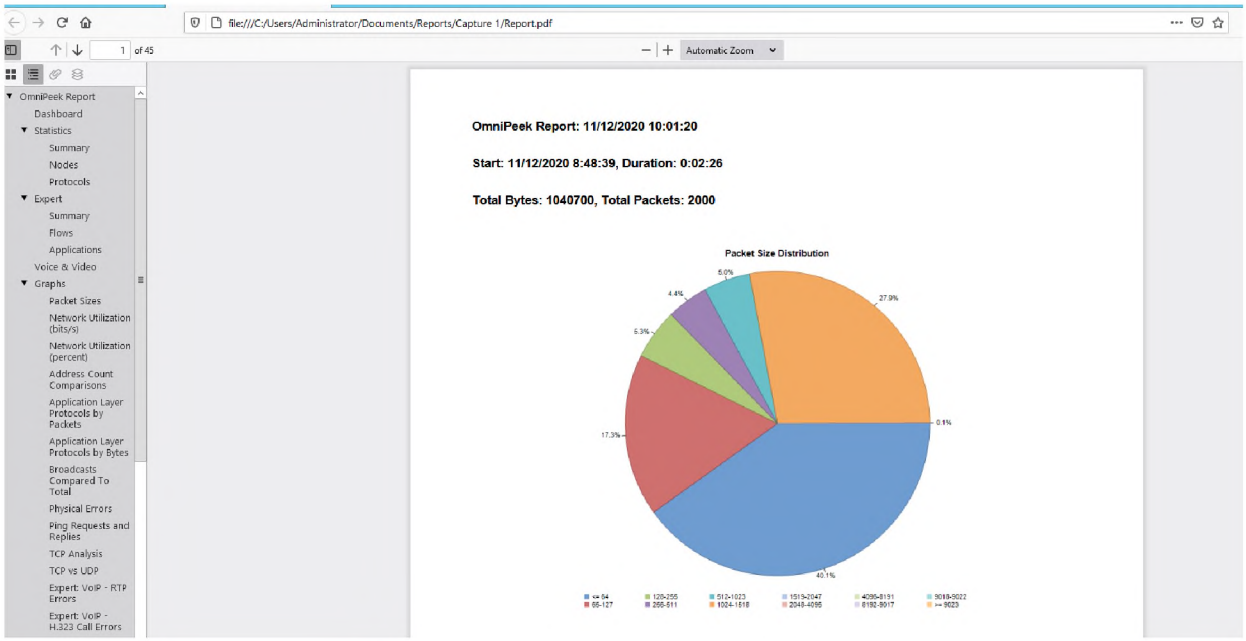


Рисунок 2.23 – Створення звіту

Аналіз лабораторної роботи: проаналізуйте та задокументуйте результати виконаних завдань у звіті.

2.3.3 Спуфінг MAC-адрес за допомогою SMAC

SMAC - це потужний, але простий у використанні програмний продукт для зміни MAC-адрес (спуфер) для систем Windows 10, 8, 7, VISTA, 2008, 2003, XP та 2000, незалежно від того, чи дозволена така функція виробником мережевої карти. SMAC розроблений сертифікованими професіоналами (CISSP, CISA, CIPP та MCSE). Програма також чудово підходить для пошуку MAC-адрес.

Мета лабораторної роботи: ознайомлення з інструментами заміни MAC-адреси, вивчення їх можливостей.

Для цієї лабораторної роботи необхідне наступне:

– SMAC 2.7, що знаходиться за шляхом C:\ProgramData\KLC\SMAC\SMAC.exe на віртуальній машині Windows 10;
– Будь-який інтернет-браузер;

Необхідний час для виконання лабораторної роботи: 10 хвилин.

Хід роботи:

1. Перш за все, необхідно запустити SMAC, що знаходиться за вищезазначеним шляхом. Запущена програма зображена на рисунку 2.24. Оберіть мережевий адаптер для спуфінгу MAC-адреси.

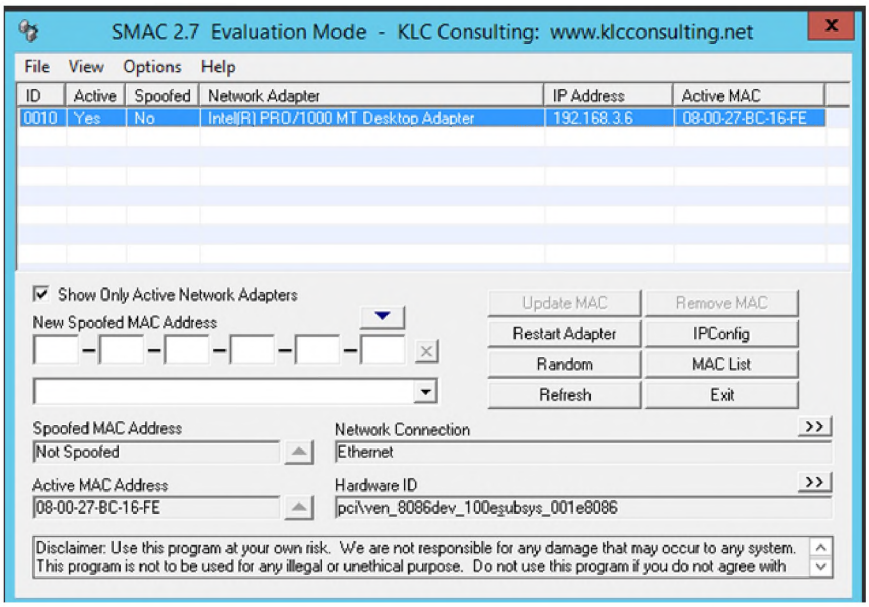


Рисунок 2.24 – головне меню SMAC

2. Натисніть Random, для того щоб згенерувати випадкову MAC-адресу. Приклад результату наведено на рисунку 2.25. Натискання на кнопку Random також вставляє нову підмінену MAC-адресу у поле спуфінгу (заміни) MAC-адреси.

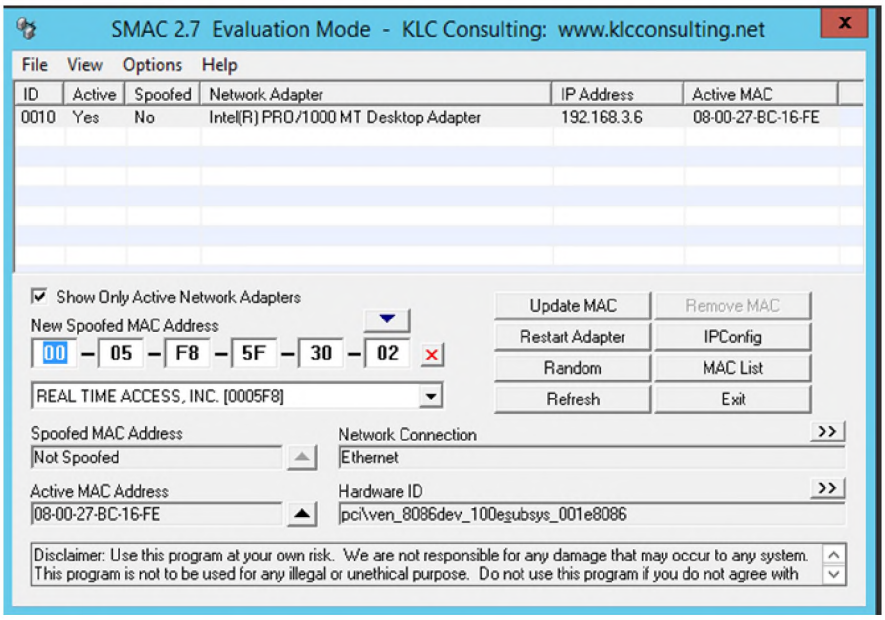


Рисунок 2.25 – генерування випадкової MAC-адреси

3. Мережеве підключення (Network Connection) та адаптер (Network Adapter) відображають відповідні імена. Натисніть кнопку стрілки «вперед» у мережевому підключенні, щоб відобразити інформацію про мережевий адаптер, як на рисунку 2.26. Натискання кнопки зі стрілкою «назад» у мережевому адаптері знову відображатиме інформацію про мережеве підключення. Ці кнопки дозволяють перемикатися між мережевим підключенням та інформацією про мережевий адаптер.

Рисунок 2.26 – Відображення мережевого підключення та адаптера

4. Так само ідентифікатор апаратного забезпечення (Hardware ID) та ідентифікатор конфігурації (Configuration ID) відображають відповідні імена.

5. Для того щоб зібрати інформацію з ipconfig, натисніть IPConfig, з'явиться інформація, подібна до того, що зображена на рисунку 2.27. Коли з'явиться вікно з інформацією, її можна додатково зберегти натисканням на File у верхній частині вікна.

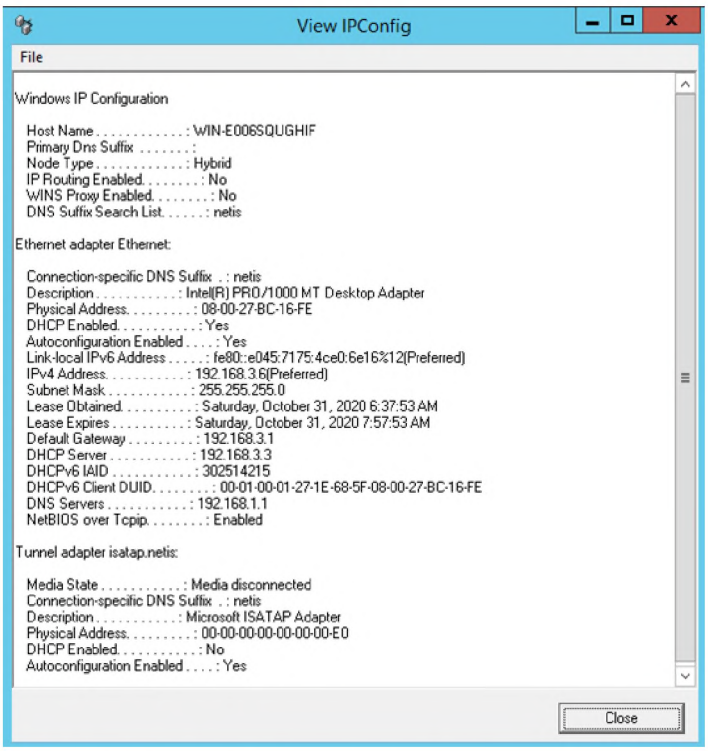


Рисунок 2.27 – Відображення інформації ipconfig

6. Ви також можете імпортувати список MAC-адрес в SMAC натисканням на MAC List. Якщо в полі MAC-адреси немає адреси, можна натиснути кнопку Load List, щоб вибрати файл списку MAC-адрес. Далі можна обрати файл Sample_MAC_Address_List.txt з вікна Load MAC List. Список MAC-адрес буде доданий до MAC List у SMAC. Виберіть MAC-адресу та натисніть Select. Ця MAC-адреса буде скопійована до New Spoofed MAC Address на головному екрані SMAC. Змініть MAC-адресу цим способом, або згенеруйте випадкову MAC-адресу, як було зазначено вище.

7. Щоб перезапустити мережевий адаптер, натисніть кнопку Restart Adapter, що перезапустить вибраний мережевий адаптер. Перезапуск адаптера спричиняє тимчасову проблему відключення мережевого адаптера. Це зображено на рисунку 2.28.

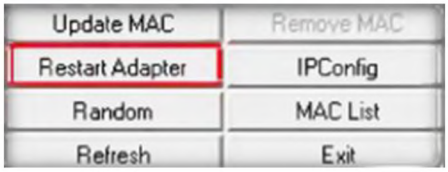


Рисунок 2.28 – Кнопка перезапуску адаптера

8. Перевірте інформацію ipconfig, зробіть скріншот для звіту зі зміненою ip-адресою. Після цього натисніть Remove mac та restart adapter, щоб повернути попередні налаштування та знову зробіть скріншот зі стандартною MAC-адресою для звіту. Після цього обов'язково перевірте, що на віртуальній машині є інтернет-підключення.

Аналіз лабораторної роботи: проаналізуйте та задокументуйте результати виконаних завдань у звіті, опишіть що таке MAC-адреса і у яких атаках її заміна може використовуватися.

2.3.4 Аналіз мережі за допомогою Capsa Network Analyzer

Capsa - це назва сімейства аналізаторів пакетів, розроблена Colasoft для мережевих адміністраторів для моніторингу, усунення несправностей та аналізу дротових та бездротових мереж. Це програмне забезпечення може виконувати збір пакетів в режимі реального часу, цілодобовий моніторинг мережі, вдосконалений аналіз протоколів, поглиблене декодування пакетів та автоматичну експертну діагностику. [4]

Мета лабораторної роботи: ознайомлення з інструментами для аналізу мережі, вивчення їх можливостей, аналіз мережевих протоколів та мережевого трафіку.

Для цієї лабораторної роботи необхідне наступне:

– Capsa Network Analyzer, що знаходиться за шляхом C:\Program Files\Colasoft Capsa 11 Free Edition\Capsa.exe на віртуальній машині Windows server 2012;
– Windows 10 як цільова (атакована) машина;
– Будь-який інтернет-браузер;

Необхідний час для виконання лабораторної роботи: 20 хвилин.

Хід роботи:

1. Перш за все, необхідно запустити Capsa Network Analyzer, що знаходиться за вищезазначеним шляхом. Запущена програма зображена на рисунку 2.29.

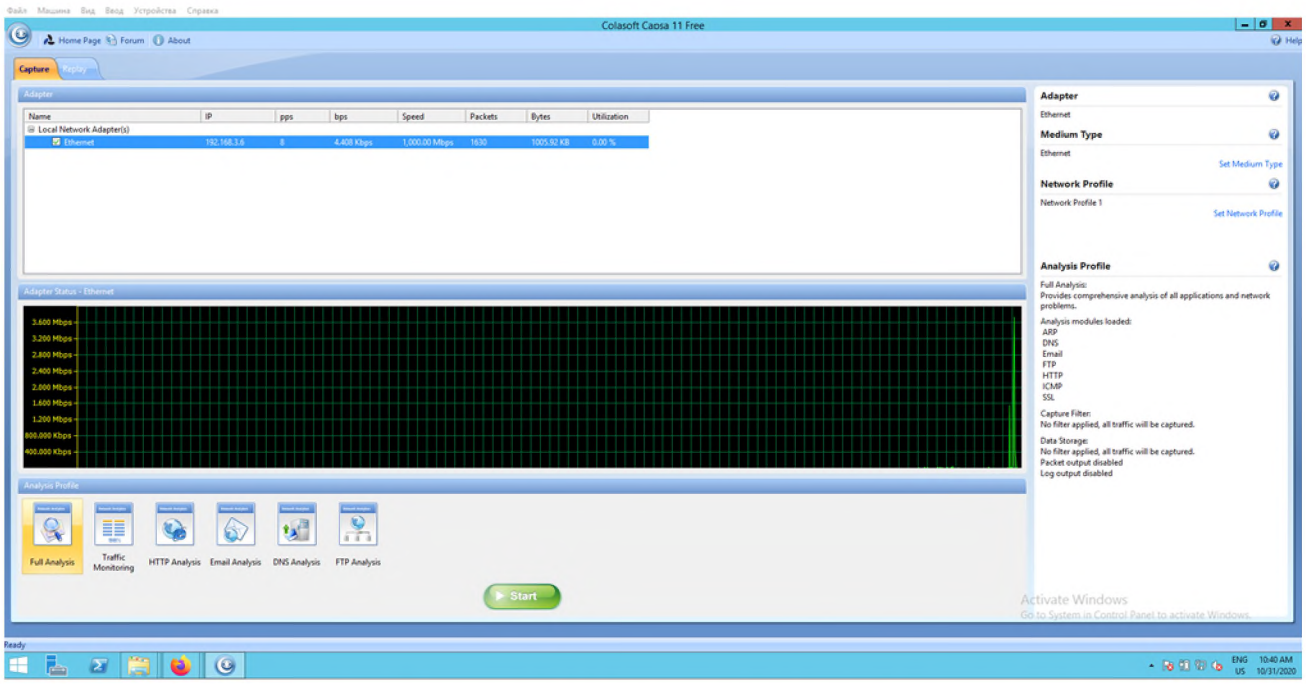


Рисунок 2.29 – Стартове меню Capsa Network Analyzer

2. У нижній частині вікна натисніть кнопку «Start», щоб розпочати захоплення пакетів.

3. Вимкніть фаєрвол на обох віртуальних машинах. Перейдіть до віртуальної машини Windows 10, зайдіть до командної строки cmd (її можна знайти через пошук поряд з меню пуск). Введіть команду ping та додайте ip-адресу Windows Server 2012 (її можна дізнатися за допомогою ipconfig). Збережіть скріншот команд ping та ipconfig для звіту з лабораторної роботи.

4. Поверніться до Capsa Network Analyzer, перейдіть до вкладки «packet» та знайдіть запит та відповідь ping (протокол ICMP). Опишіть у звіті, для чого потрібен протокол ICMP та додайте свої скріншоти, як показано на рисунках 2.30 та 2.31. Повний перегляд пакету можна відкрити натиснувши на нього двічі.

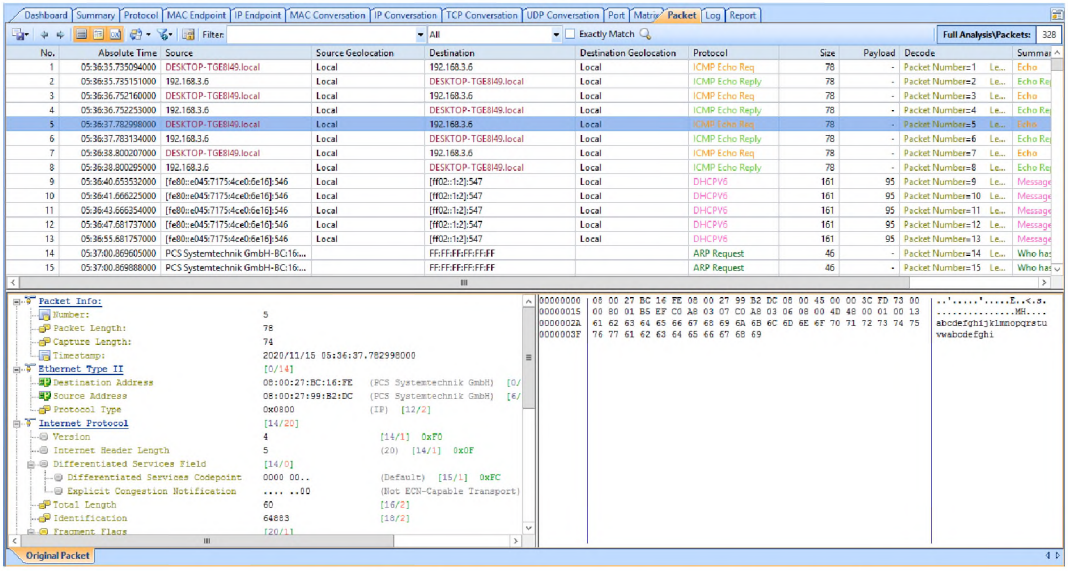


Рисунок 2.30 – Перегляд захоплених пакетів

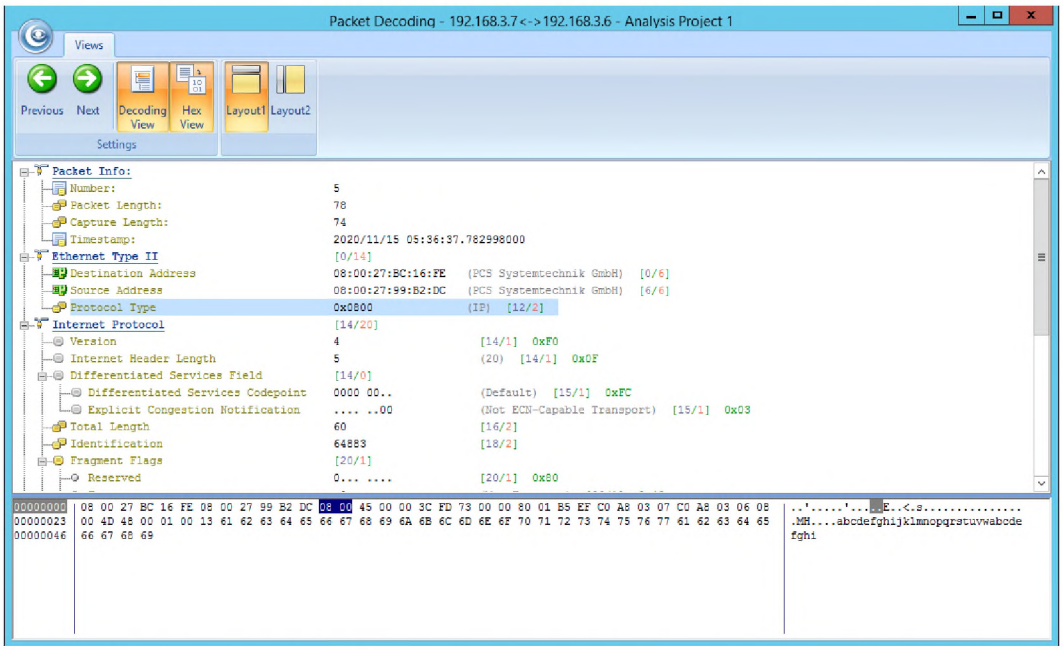


Рисунок 2.31 – Повний перегляд захопленого пакета

5. Збережіть скріншоти для звіту з лабораторної роботи з панелей Dashboard, Protocol, IP, TCP та UDP Conversation та ще з однієї вкладки на Ваш вибір. Коротко опишіть отримані скріншоти у звіті.

Аналіз лабораторної роботи: проаналізуйте та задокументуйте результати виконаних завдань у звіті.

2.3.5 Сніфінг мережі за допомогою Wireshark

Wireshark - провідний аналізатор мережевого трафіку у світі та важливий інструмент для будь-якого фахівця з безпеки або системного адміністратора. Це безкоштовне програмне забезпечення дозволяє аналізувати мережевий трафік у режимі реального часу і часто є найкращим інструментом для вирішення проблем у мережі.

Wireshark може допомогти усунути неполадки, такі як: втрачені пакети, проблеми із затримками та шкідлива активність у мережі. Він також надає інструменти для фільтрації та детального аналізу трафіку. [5]

Мета лабораторної роботи: ознайомлення з інструментами для аналізу мережі, вивчення їх можливостей, аналіз захоплених пакетів.

Для цієї лабораторної роботи необхідне наступне:

– Wireshark, що знаходиться за шляхом C:\Program Files\Wireshark\Wireshark.exe на віртуальній машині Windows server 2012;
– Windows 10 як цільова (атакована) машина;
– Будь-який інтернет-браузер;

Необхідний час для виконання лабораторної роботи: 20 хвилин.

Хід роботи:

1. Перш за все, необхідно запустити Wireshark, що знаходиться за вищезазначеним шляхом. Запущена програма зображена на рисунку 2.32.

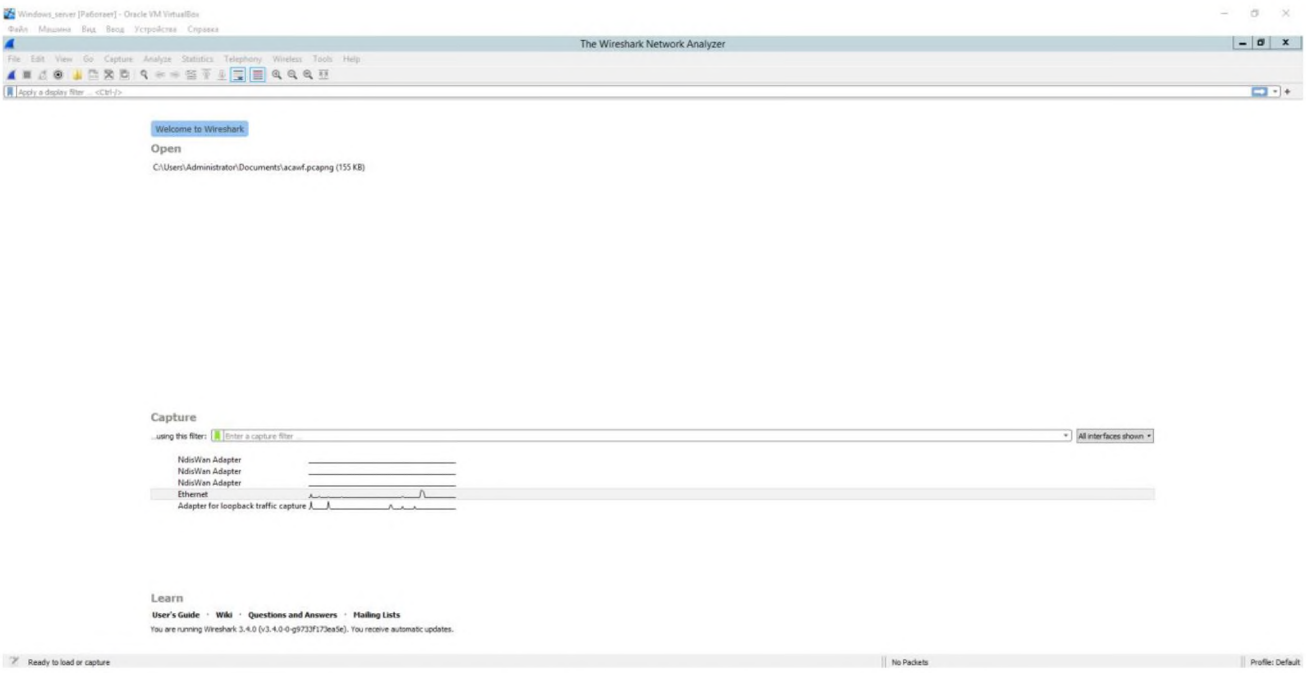


Рисунок 2.32 – Стартовий екран Wireshark

2. Увійдіть до віртуальної машини Windows 10.

3. Тепер на віртуальній машині Windows Server 2012 необхідно обрати адаптер, оберіть «Ethernet», щоб розпочати захоплення пакетів. Після цього на віртуальній машині Windows 10 виконайте команду ping для адреси Windows Server 2012 у cmd. Поверніться до Wireshark.

4. Знайдіть результати команди ping – для цього можна скористатися фільтром під меню вгорі, обравши icmp протокол. Нижче можна буде побачити знайдені пакети, а ще нижче – склад обраного пакета. Зробіть скріншот для звіту з лабораторної роботи, як це показано на рисунку 2.33. Після цього приберіть фільтр з протоколом та відфільтруйте пакети за довжиною, від найменшого до найбільшого. Зробіть скріншот для звіту.

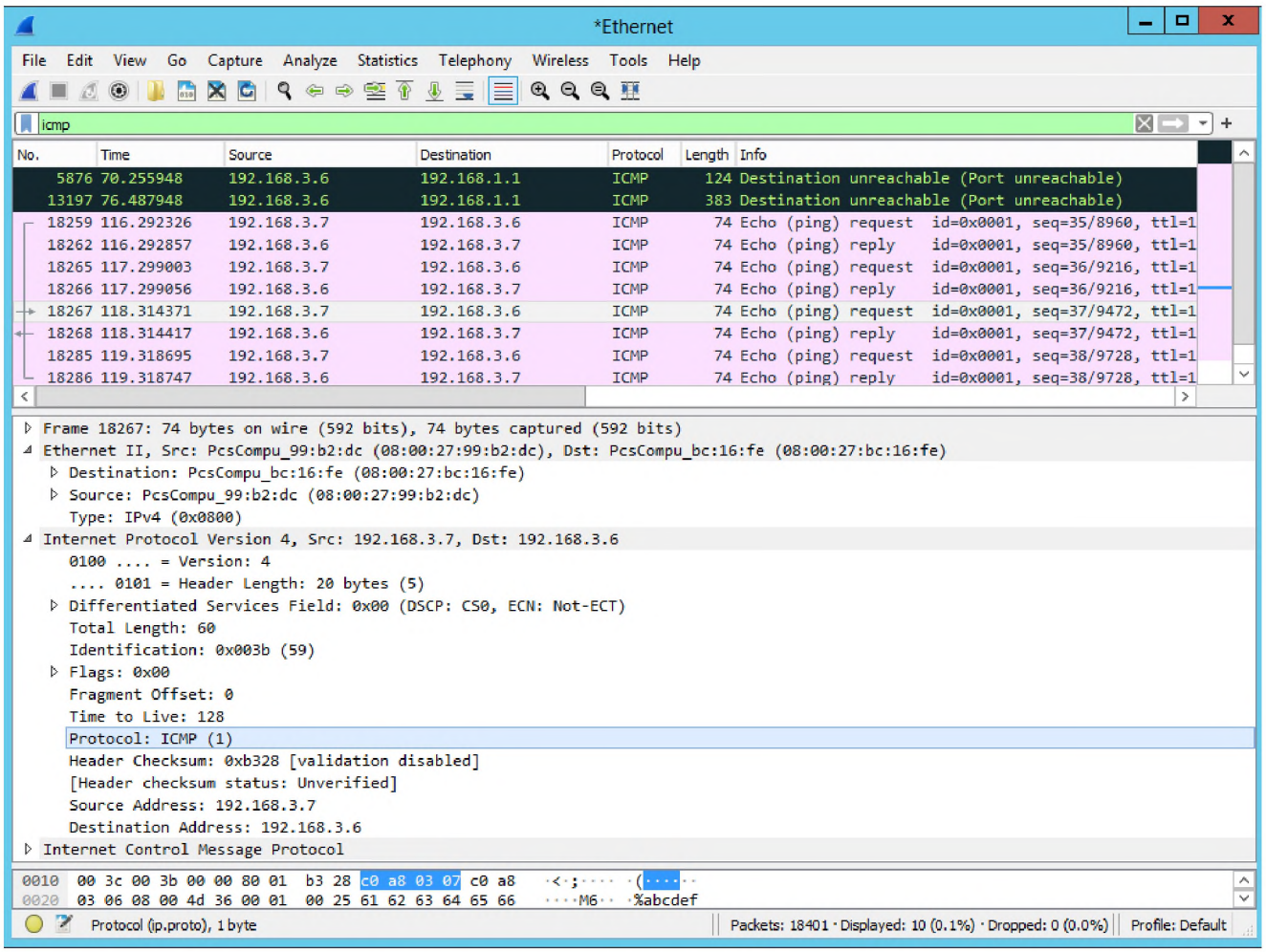


Рисунок 2.33 – Меню захоплення пакетів з фільтром

5. На віртуальній машині Windows Server 2012 перейдіть на сайт gde-fon.com та збережіть декілька рисунків. Знов поверніться до Wireshark, перейдіть до меню File – export objects – http. Відкриється меню, подібне до того, що зображене на рисунку 2.34. Продивіться, які об’єкти можна зберегти. Зробіть скріншот для звіту.

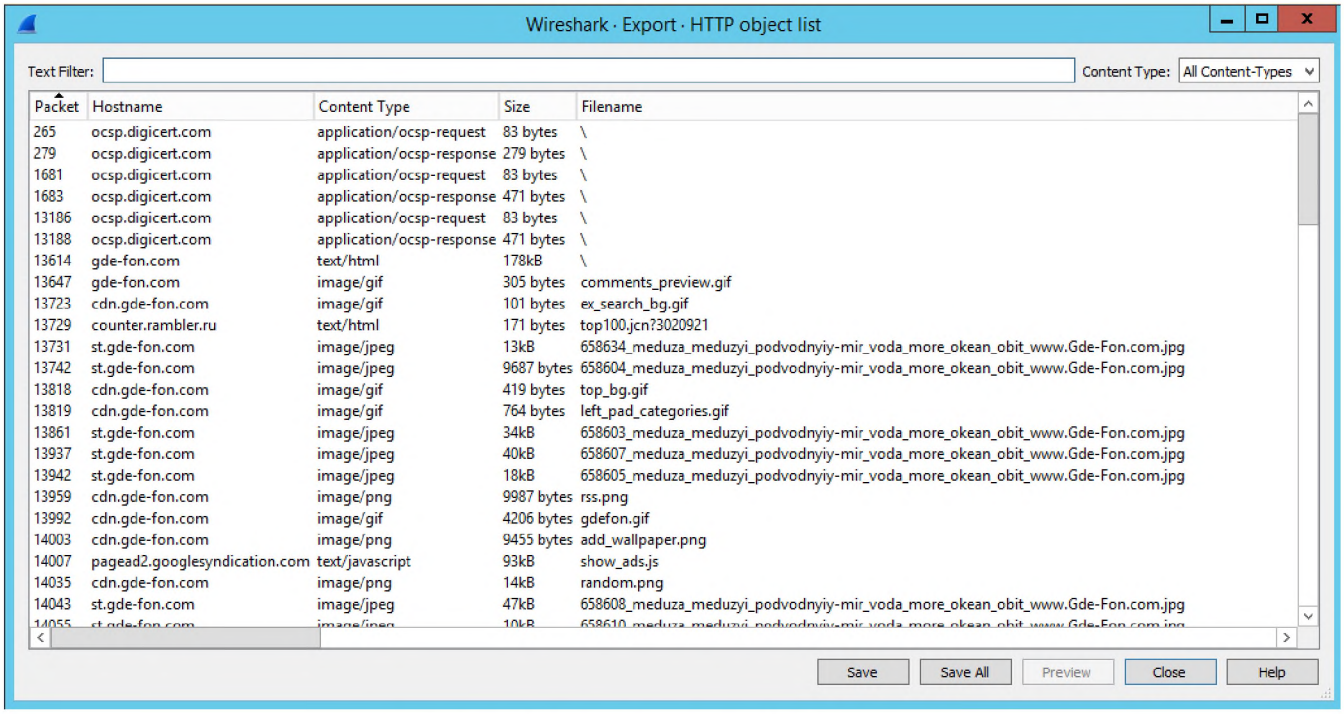


Рисунок 2.34 – експорт HTTP пакетів

6. Перейдіть до Analyze – expert information. Збережіть скріншот до звіту, подібний до того, що вказано на рисунку 2.35.

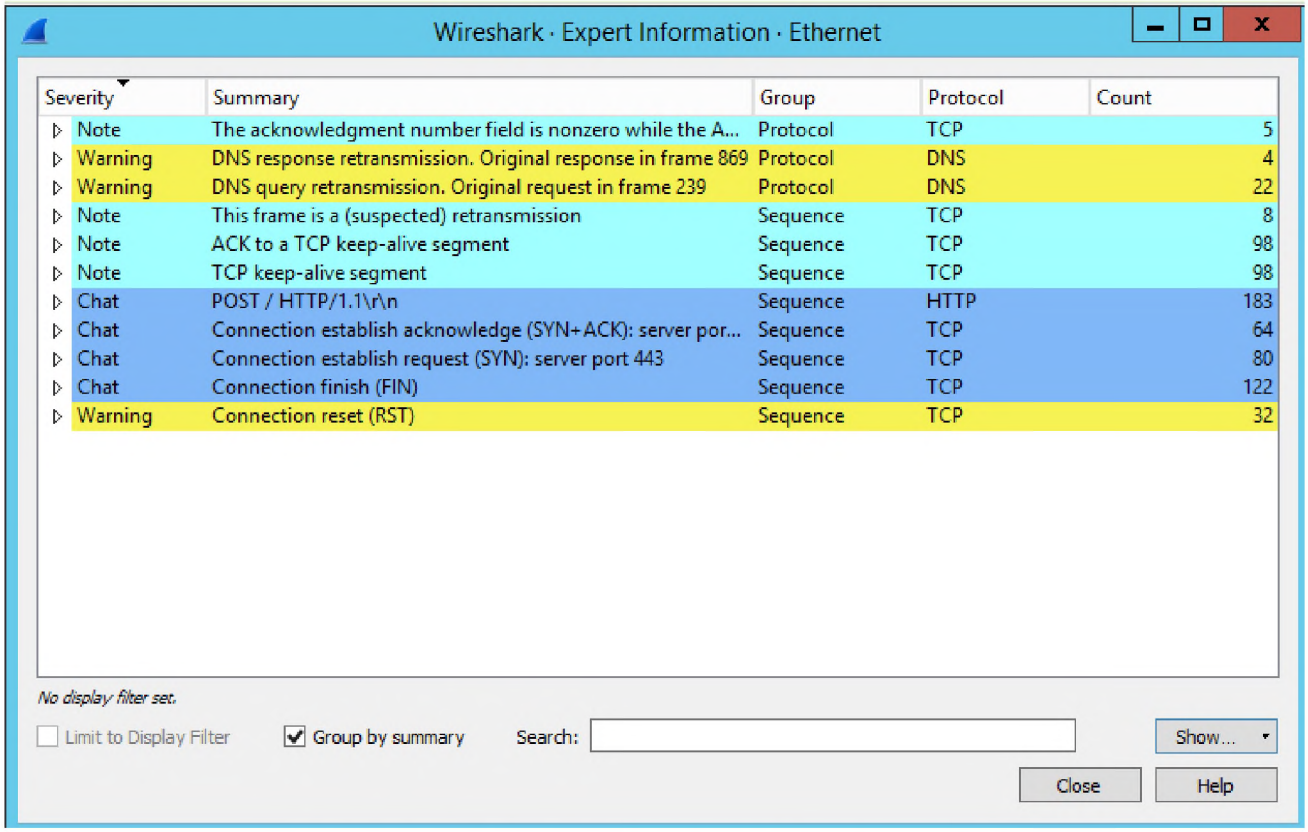


Рисунок 2.35 – Виявлення проблем у мережі

7. Коротко опишіть можливості Wireshark у звіті.

Аналіз лабораторної роботи: проаналізуйте та задокументуйте результати виконаних завдань у звіті.

2.3.6 Атака Man-in-the-Middle за допомогою Cain & Abel

Згідно з офіційним веб-сайтом, Cain & Abel - це інструмент відновлення паролів для операційних систем Microsoft. Він дозволяє легко відновлювати різні види паролів, перехоплюючи пакети у мережі, зламуючи зашифровані паролі за допомогою атак Dictionary, Brute-Force та Cryptanalysis, записуючи VoIP-розмови та аналізуючи протоколи маршрутизації.

Остання версія містить багато нових функцій, таких як APR (ARP Poison Routing), що дозволяє проводити розвідку у локальних мережах та проводити атаки типу "Людина посередині". У цій версії також можна аналізувати зашифровані протоколи, такі як SSH та HTTPS. [6][7]

Мета лабораторної роботи: ознайомлення з інструментами для проведення атак Man-in-the-Middle («людина посередині»).

Для цієї лабораторної роботи необхідне наступне:

– Cain & Abel, що буде знаходитися за шляхом C:\Program Files (x86)\Cain\Cain.exe на хостовій машині (Windows 10);
– Віртуальні машини Windows Server 2012 та Windows 10 як цільові (атаковані) машини;
– Будь-який інтернет-браузер;

Необхідний час для виконання лабораторної роботи: 30 хвилин.

Хід роботи:

1. Перш за все, необхідно вимкнути захисник Windows на хостовій машині Windows 10. Для цього необхідно перейти до Windows defender (його можна знайти за допомогою пошуку поряд із пуском), у ньому зайти до меню «Захист від вірусів та загроз» зліва, та у цьому меню обрати «Параметри захисту від вірусів та інших загроз» – «Керування налаштуваннями». З'явиться меню, що зображене на рисунку 2.36. У ньому необхідно вимкнути усі параметри.

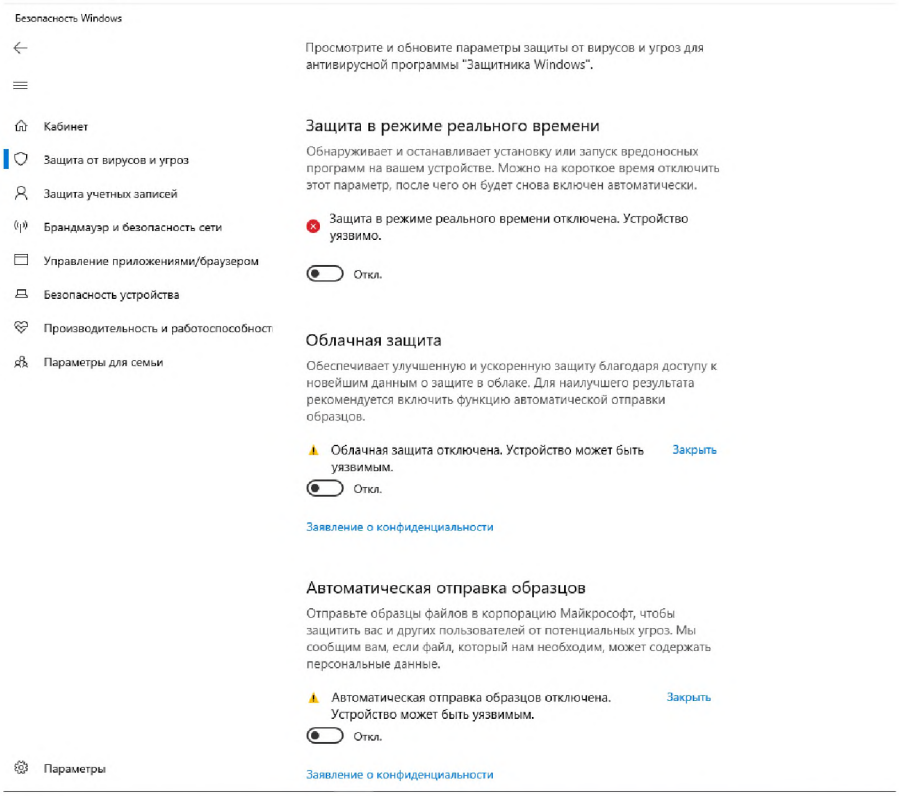


Рисунок 2.36 – Вимкнення антивірусу Windows 10

2. Завантажте Cain & Abel на хостову машину з посилання https://qpdownload.com/link.php?name=cain-and-abel. Встановіть та запустіть її. За необхідності (якщо для роботи програми не вистачає певних бібліотек), завантажте та встановіть npcap, який знаходиться за посиланням https://nmap.org/npcap/. Запущена програма зображена на рисунку 2.37. Запустіть також віртуальні машини Windows 10 та Windows Server 2012.

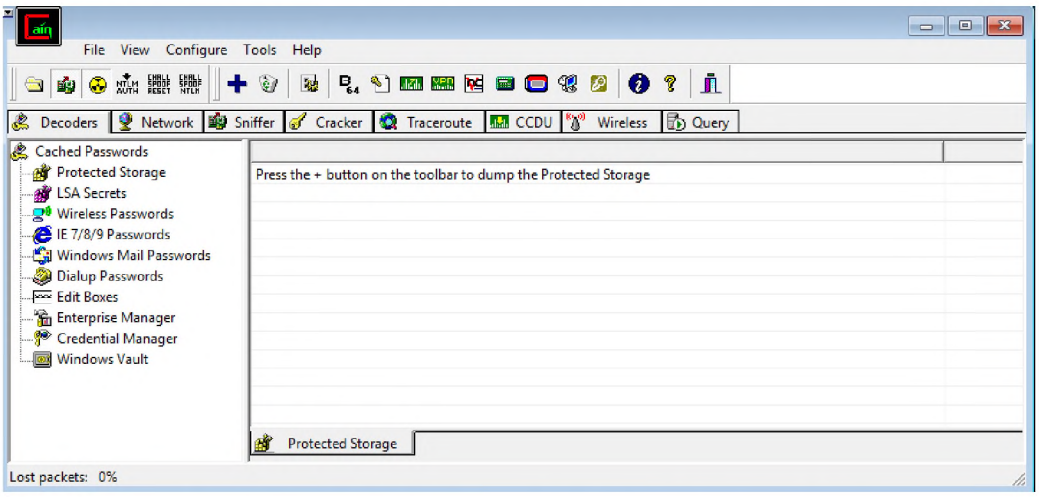


Рисунок 2.37 – Стартове меню Cain & Abel

3. Натисніть «Configure» у головному меню, щоб продивитися налаштування. Перевірте, що обрано необхідний Вам мережевий адаптер, як це зображено на рисунку 2.38.

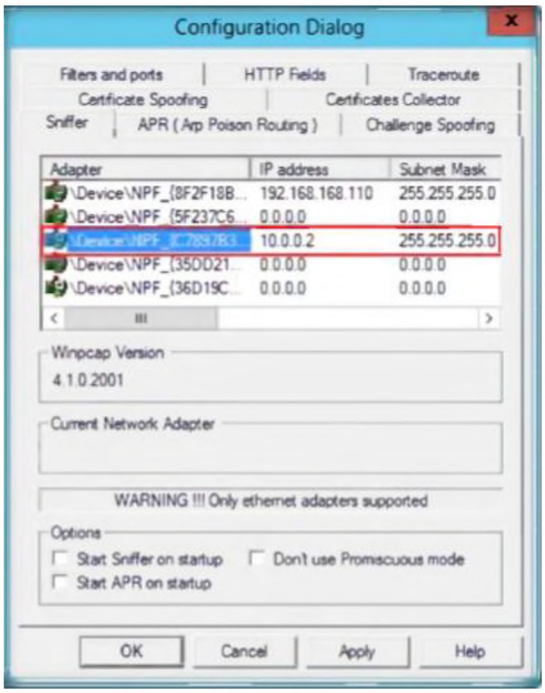


Рисунок 2.38 – Меню вибору адаптера

4. Натисніть кнопку «Start sniffer», щоб розпочати захоплення пакетів, як це показано на рисунку 2.39. Потім перейдіть до вкладки сніфферу (рисунок 2.40). Натисніть «+» вище, оберіть сканування своєї підмережі та відмітьте галочкою «всі тести». Після цього можна підтвердити налаштування. Це зображено на рисунку 2.41.

Рисунок 2.39 – Увімкнення сніфферу

Рисунок 2.40 – Вкладка сніфферу

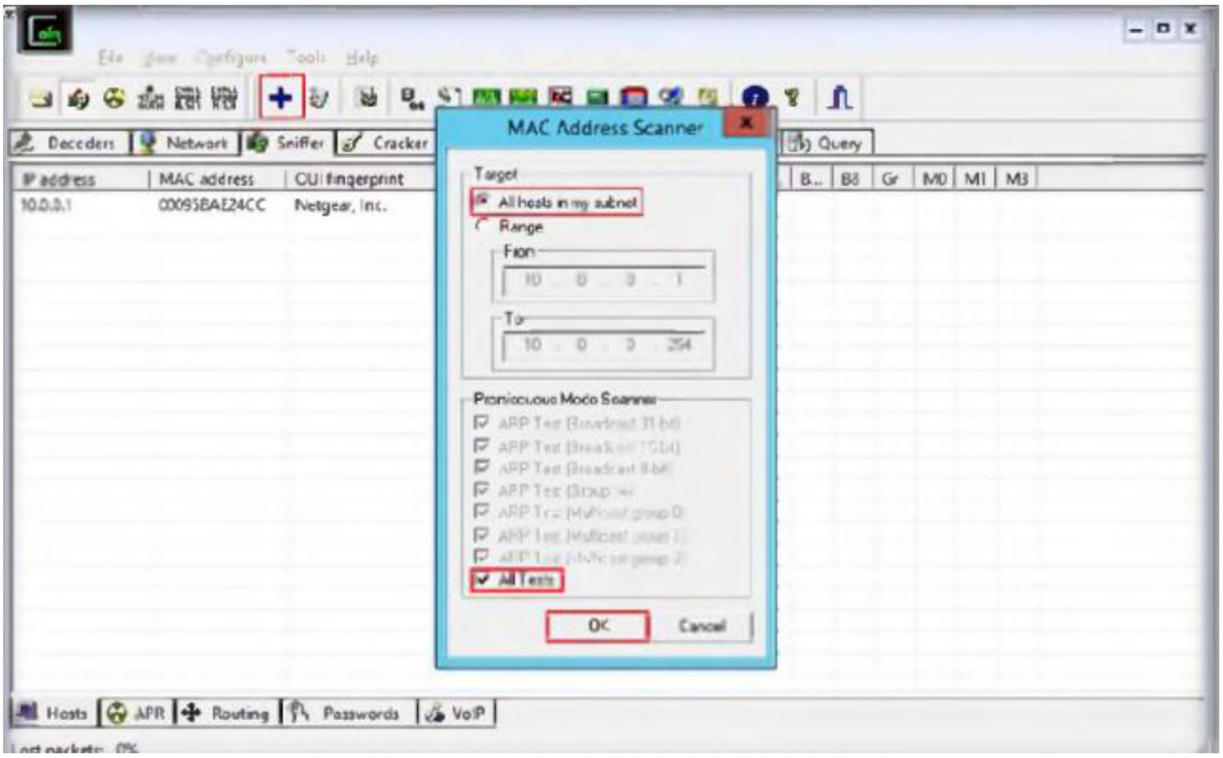


Рисунок 2.41 – Сканер MAC-адрес

5. Програма розпочне сканування фізичних адрес та перерахує усі знайдені MAC-адреси. Зробіть скріншоти для звіту з лабораторної роботи. Натисніть вкладку APR у нижньому меню.

6. Натисніть будь-де у полі «Configuration/Routed Packets» для активації позначки «+», що можна побачити на рисунку 2.42. Натисніть цю позначку.

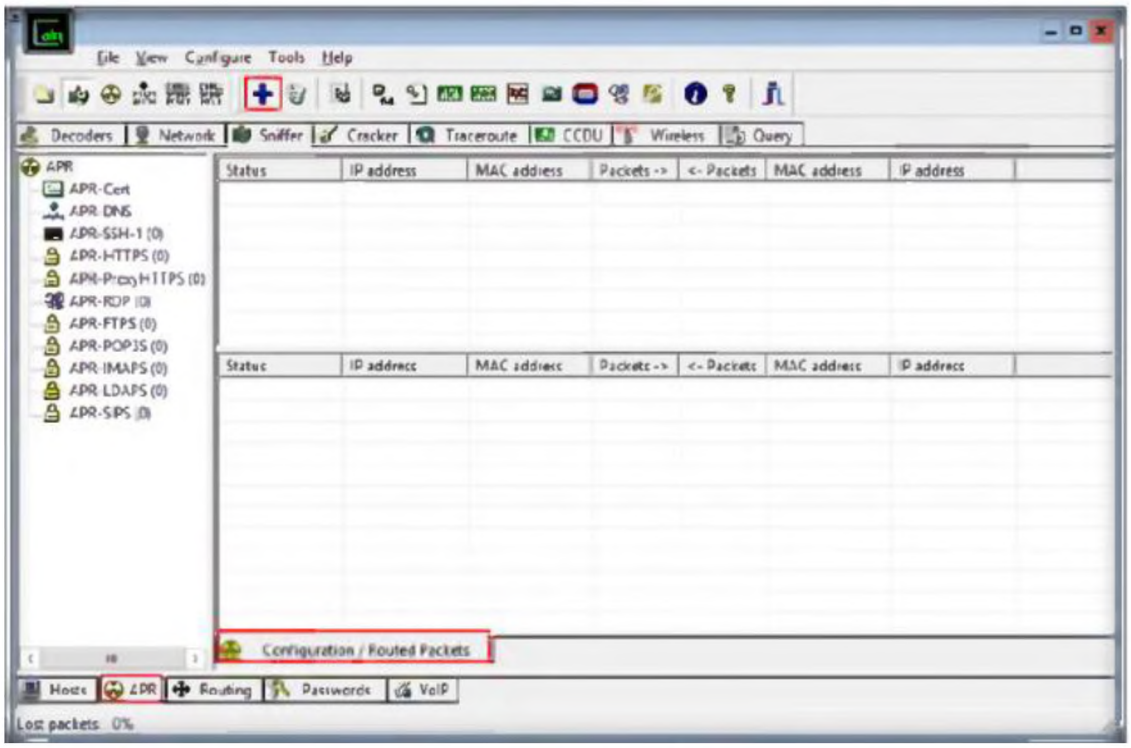


Рисунок 2.42 – Меню APR

6. Для аналізу трафіку між двома віртуальними машинами, оберіть їх IP-адреси. Їх можна дізнатися за допомогою команди ipconfig у cmd. Вікно вибору IP-адрес зазначено на рисунку 2.43. Зробіть скріншот для звіту. Після підтвердження натисніть іконку «Start/Stop APR», що можна побачити на рисунку 2.44.

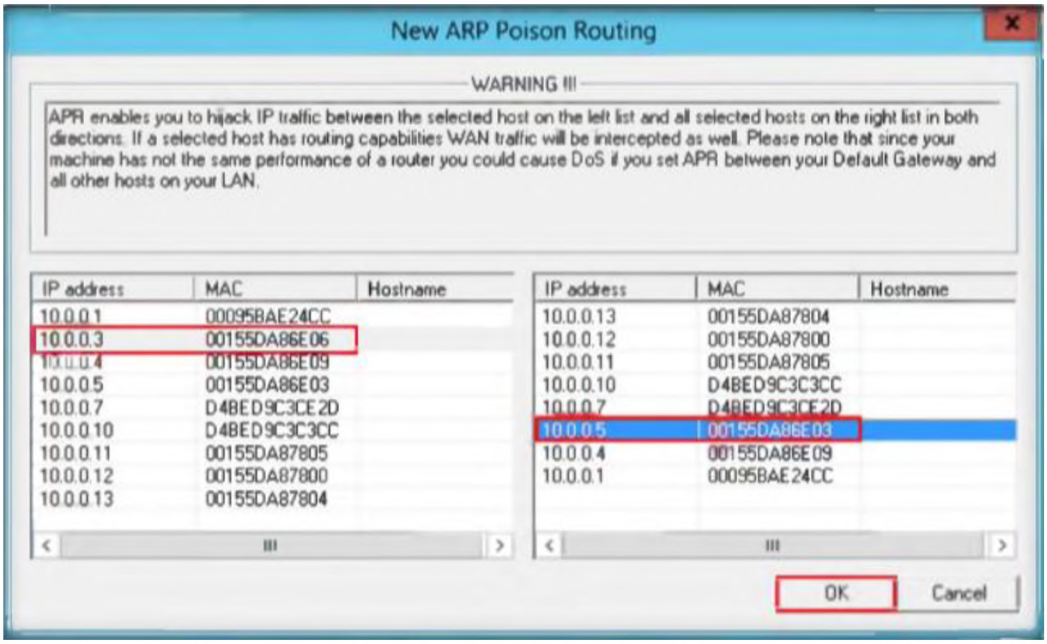


Рисунок 2.43 – Вікно вибору IP-адрес

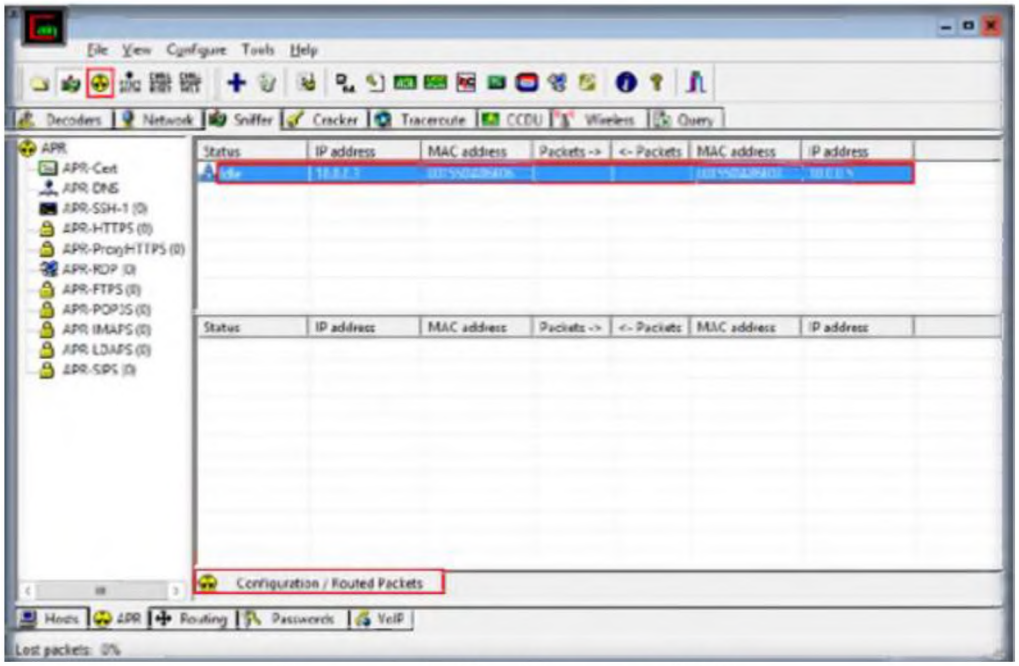


Рисунок 2.44 – Початок APR

7. Тепер перейдіть до віртуальної машини Windows Server 2012 і в командному рядку cmd введіть ftp та додайте ip-адресу віртуальної машини Windows 10 (у даному прикладі це 10.0.0.3) та натисніть enter. Як це виглядає – показано на рисунку 2.45. Введіть ім'я користувача та пароль – Student та Pa$$word.

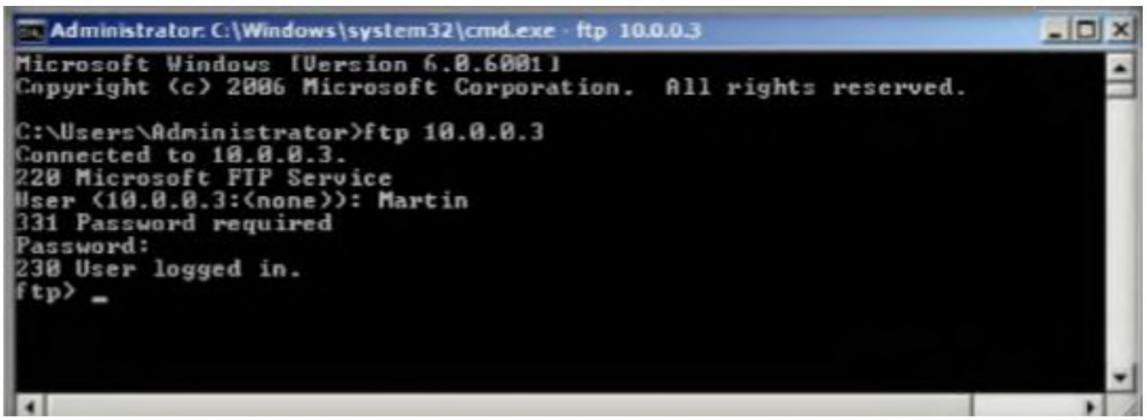


Рисунок 2.45 – Підключення по протоколу ftp

8. Поверніться до Cain & Abel на хостовій машині та продивіться передачу пакетів (рисунок 2.46). Зробіть скріншот для звіту з лабораторної роботи.

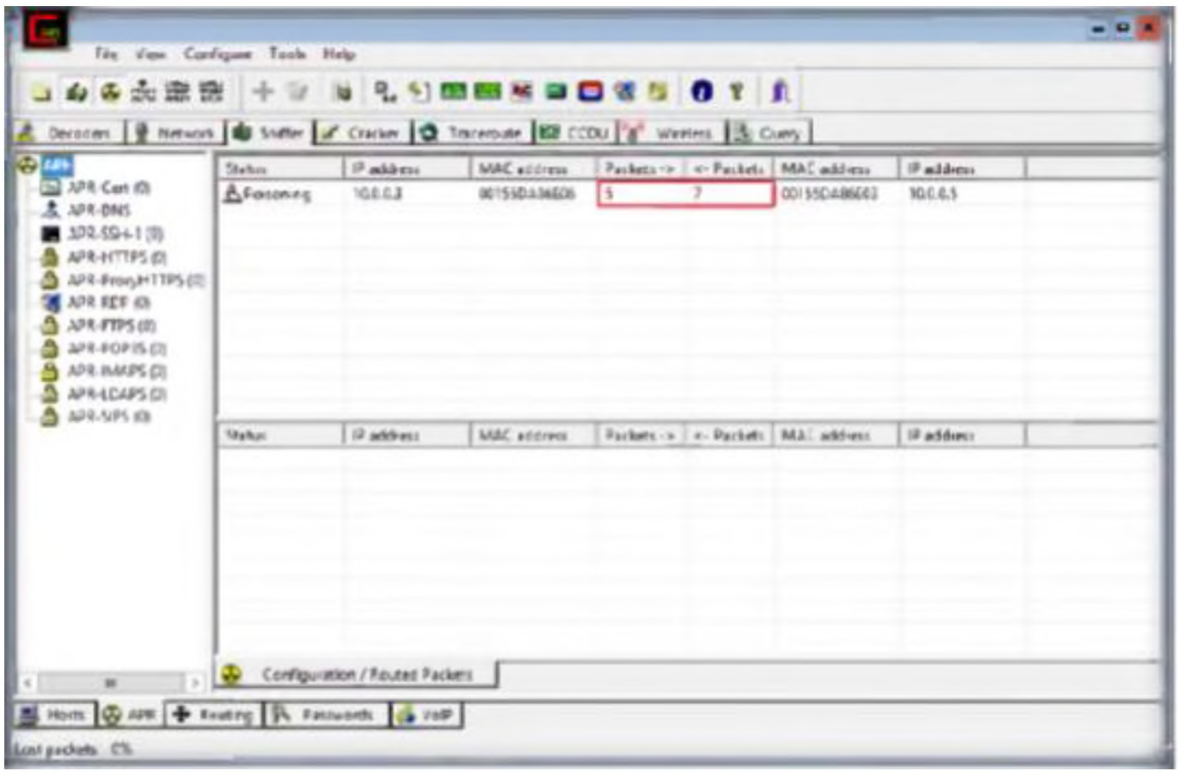


Рисунок 2.46 – Передача пакетів

9. Перейдіть до вкладки з паролями, як показано на рисунку 2.47, щоб побачити виявлений пароль. Зробіть скріншот для звіту, додайте опис протоколу ftp, поясніть, у чому небезпека його використання та які ще протоколи вважаються недостатньо безпечними. Додайте інформацію про альтернативи для них.

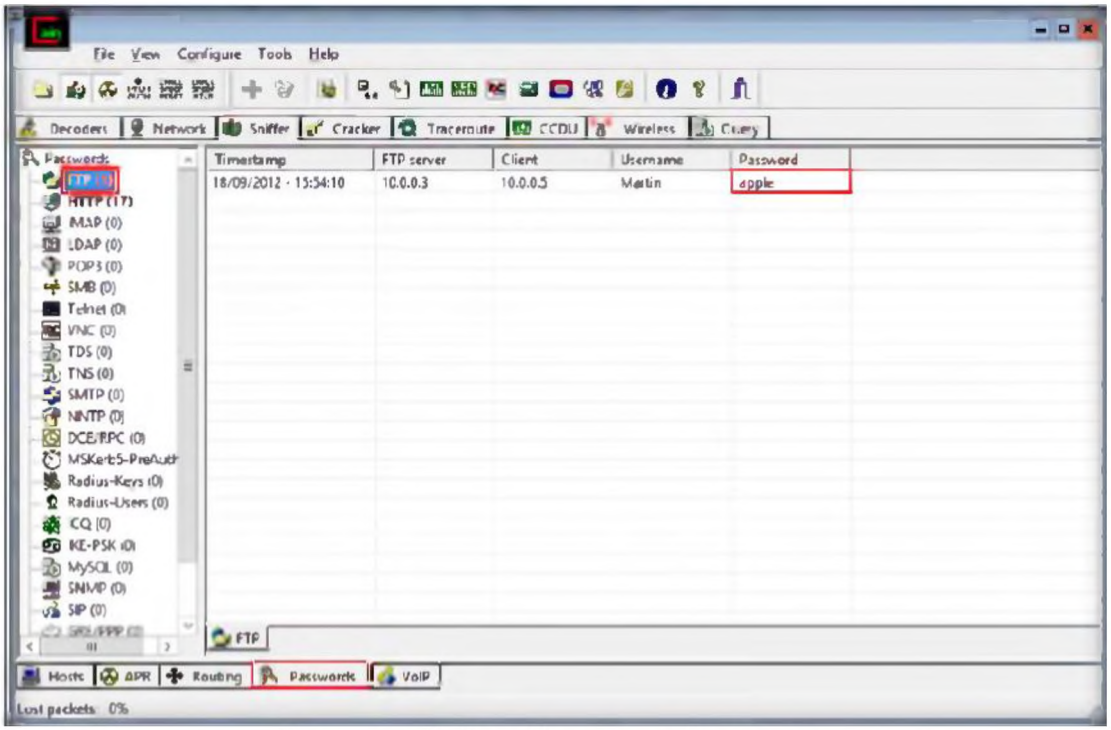


Рисунок 2.47 – Виявлений пароль

Аналіз лабораторної роботи: проаналізуйте та задокументуйте результати виконаних завдань у звіті.

2.3.7 Виявлення ARP-атак за допомогою XArp Tool

XArp - це програмне забезпечення для підтримання належного рівня безпеки, яке використовує передові методи виявлення атак типу ARP. Використовуючи активні та пасивні модулі, XArp виявляє атаки у мережі. Атаки ARP дозволяють зловмисникові збирати дані, що надсилаються через мережу, не виявляючи при цьому себе. Атаки підробки ARP часто не виявляються брандмауерами та безпекою операційної системи.

Мета лабораторної роботи: ознайомлення з інструментами для захисту для ARP атак.

Для цієї лабораторної роботи необхідне наступне:

– XArp Tool, що знаходиться за шляхом C:\Program Files (x86)\XArp\xarp.exe на віртуальній машині Windows server 2012;

Необхідний час для виконання лабораторної роботи: 10 хвилин.

Хід роботи:

1. Перш за все, необхідно запустити – XArp Tool, що знаходиться за вищезазначеним шляхом. Запущена програма зображена на рисунку 2.48.

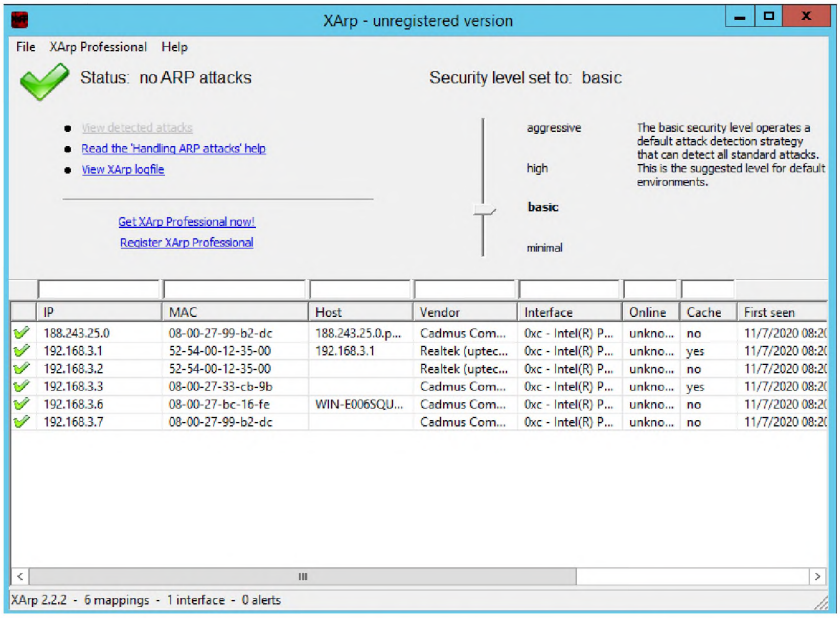


Рисунок 2.48 – Стартовий екран XArp

2. Зробіть скріншоти для звіту з лабораторної роботи. Зазвичай, рівень безпеки встановлено на «basic». Змініть рівень на «aggressive» та знов зробіть скріншот. При виявленні ймовірної атаки з'явиться повідомлення. Зробіть його скріншот також. Він може виглядати як на рисунку 2.49. Опишіть у звіті, на Вашу думку, який рівень безпеки в XArp tool є оптимальній у якій ситуації.

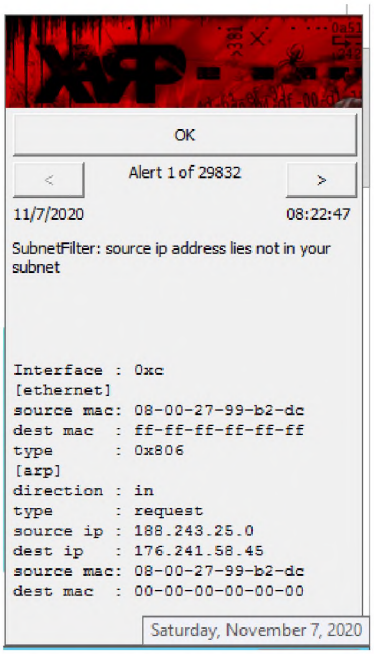


Рисунок 2.49 – Повідомлення про ймовірну атаку

Аналіз лабораторної роботи: проаналізуйте та задокументуйте результати виконаних завдань у звіті.

2.3.8 Перехоплення паролів за допомогою Sniff-o-Matic

Sniff-o-Matic – це простий аналізатор мережевих протоколів та інструмент для розпізнавання пакетів з простим у користуванні та нехитрим інтерфейсом. Він відображає дерево захоплених даних, а також шістнадцяткове відображення необробленого захоплення. Програма також включає параметри фільтрації для обмеження захоплення на основі IP-адреси, протоколу, тощо. Інші функції включають відображення статистичної діаграми та простий варіант пошуку. [21]

Мета лабораторної роботи: ознайомлення з інструментами для аналізу мережі, вивчення їх можливостей, аналіз мережевих протоколів та мережевого трафіку.

Для цієї лабораторної роботи необхідне наступне:

– Sniff-o-Matic, що знаходиться за шляхом C:\Program Files\Kwakkelfrap\Sniffer\SniffOM.exe на віртуальній машині Windows server 2012;

– Будь-який інтернет-браузер;

Необхідний час для виконання лабораторної роботи: 20 хвилин.

Хід роботи:

1. Перш за все, необхідно запустити Sniff-o-Matic, що знаходиться за вищезазначеним шляхом. Запущена програма зображена на рисунку 2.50.

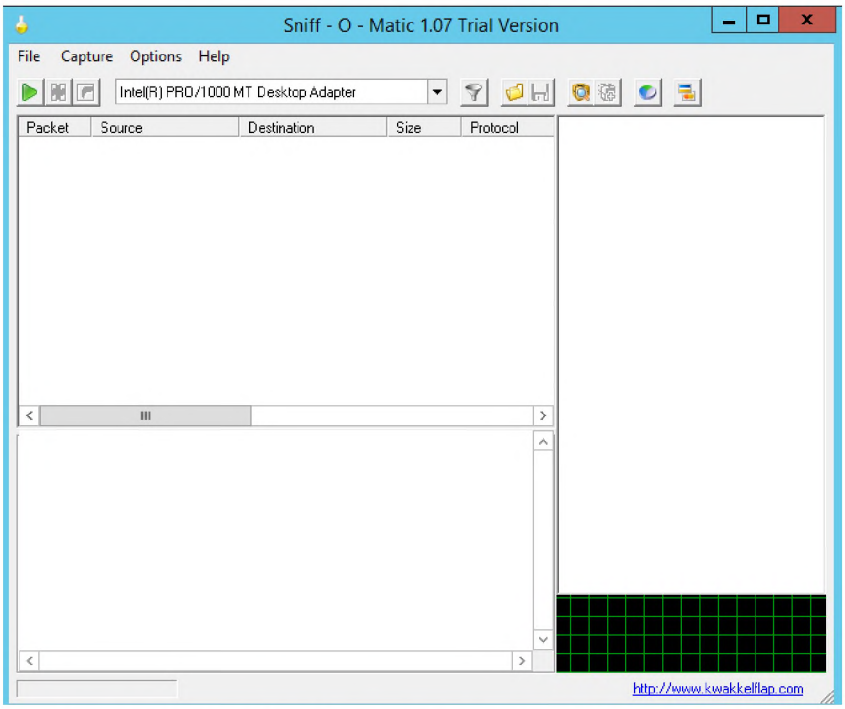


Рисунок 2.50 – Стартове меню Sniff-o-Matic

2. Оберіть необхідний мережевий адаптер та розпочніть захоплення пакетів, натиснувши зелену кнопку.

3. Коли захоплення розпочнеться, перейдіть до браузера та увійдіть до свого email аккаунта. Через деякий час після цього припиніть захоплення пакетів.

4. У вікні захоплених пакетів натисніть на один з них, щоб продивитися детальну інформацію. Вікно із захопленими пакетами зображено на рисунку 2.51. З правого боку оберіть один із пунктів і співпадіння будуть виділені червоним. Зробіть скріншот для звіту з лабораторної роботи.

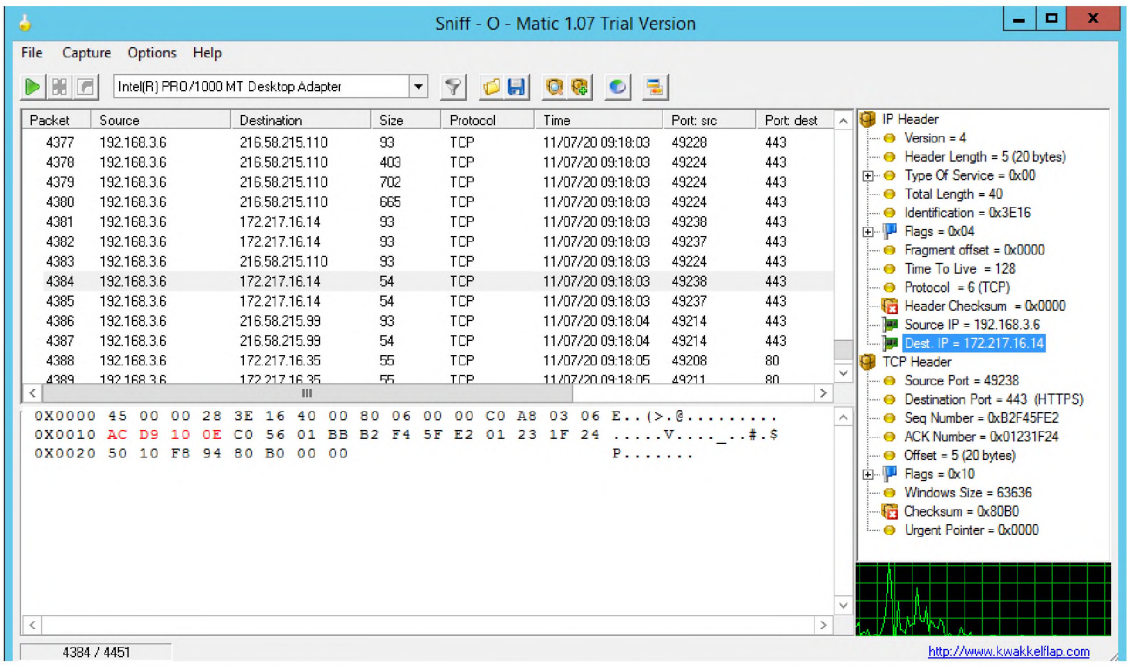


Рисунок 2.51 – Вікно захоплених пакетів

5. Для того, щоб виконати пошук серед захоплених пакетів перейдіть до пункту меню Options – Find. Коли відкриється нове меню, введіть pwd, як зображено на рисунку 2.52.

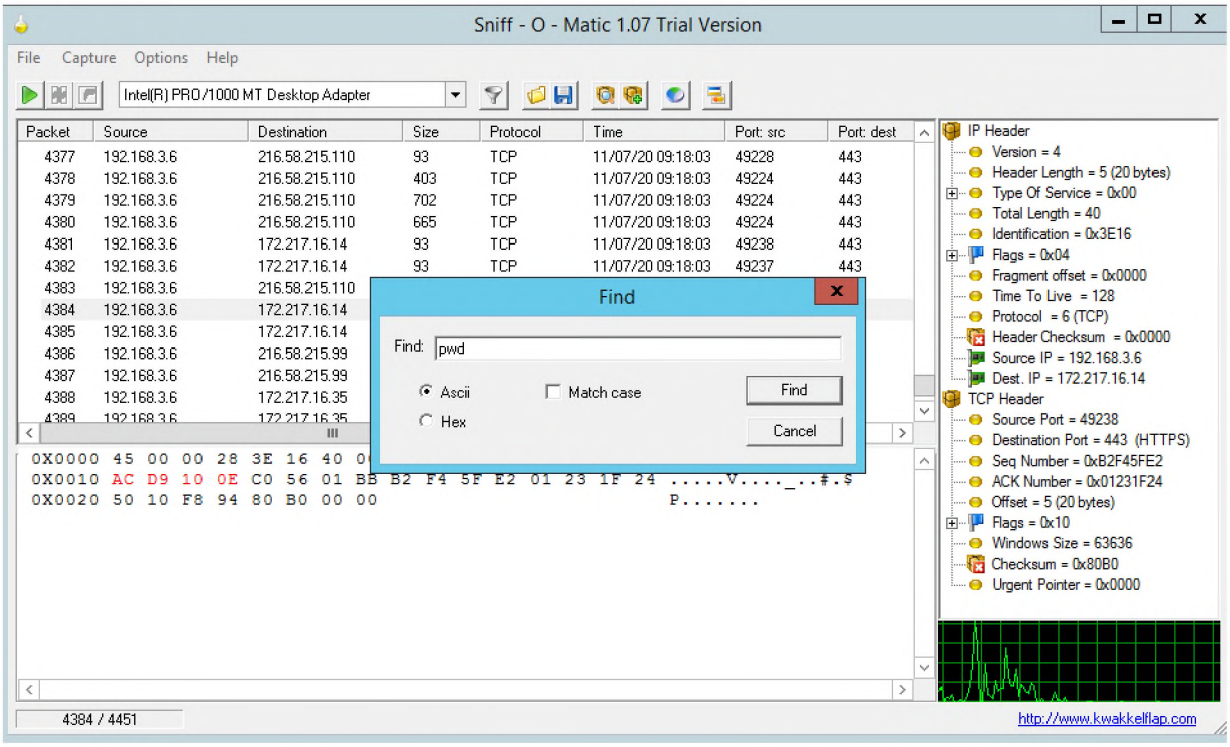


Рисунок 2.52 – Пошук пакета із паролем

5. Поряд зі знайденими пакетами з'явиться позначка бінокля та пакетів. Оберіть знайдений пакет та у нижній частині екрану знайдіть текст, що виділено синім. Додайте скріншот для звіту з лабораторної роботи. Опишіть, як знайдений пакет може використовуватись зловмисником. Додайте до звіту інформацію про те, як можна захиститися від атак Man-in-the-Middle.

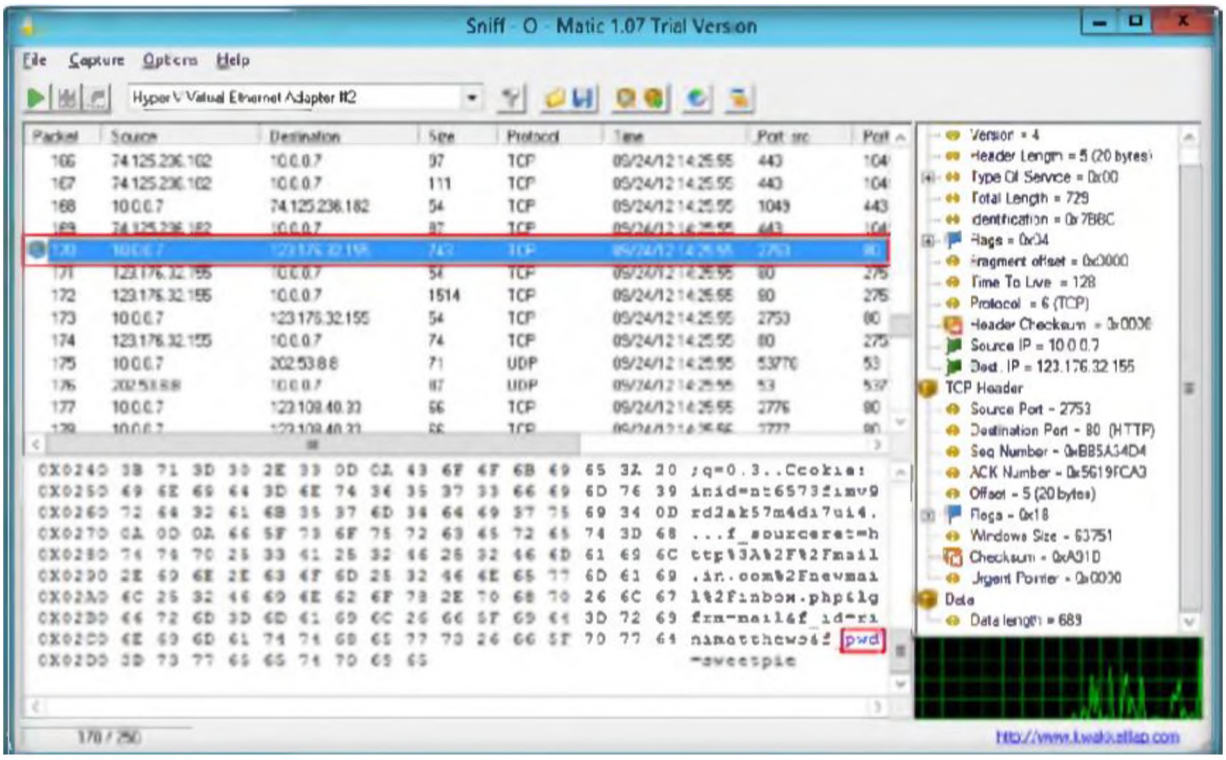


Рисунок 2.53 – Знайдений пакет із паролем

Аналіз лабораторної роботи: проаналізуйте та задокументуйте результати виконаних завдань у звіті.

2.4 Висновки

В другому розділі було підготовлено оточення для проведення практичних занять з теми «сніфінг» – створено та налаштовано віртуальні машини в аудиторії 1.72: Windows 10 та Windows Server 2012, що знаходяться в одній мережі. На відповідні віртуальні машини було встановлено необхідні програми для проведення захоплення пакетів, атак типу «людина посередині» та захисту від таких атак, а також необхідне додаткове програмне забезпечення для коректної роботи вищезазначених програм. Після цього було створено методичні матеріали для дослідження можливостей цих програм студентами, отримання ними

практичних навичок, а також знань з теми «сніфінг». У кожному пункті другого розділу студенту пропонується запустити одну з встановлених програм, дослідити її можливості, дотримуючись інструкції, а також створити звіт з лабораторної роботи. У звіті зазвичай пропонується додати декілька скріншотів, що засвідчуватимуть виконання лабораторної роботи, при необхідності додати короткий опис (що буде свідчити про розуміння студентом виконуваних дій) та додати інформацію про певний протокол або атаку, для того щоб поглибити знання студента про механізми роботи деяких атак, а також програмного забезпечення, що можуть у них використовуватися. Відповідну інформацію студент легко зможе знайти у всесвітній мережі Інтернет.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Розрахунок капітальних витрат на розробку програмно-методичних ресурсів для лабораторних робіт з теми «сніфінг»

Метою виконання економічного розділу є визначення того, чи буде доцільним розробляти програмно-методичний комплекс для проведення лабораторних робіт з теми «сніфінг» для НТУ «Дніпровська політехніка». Щоб з'ясувати це, необхідно провести розрахунки за формулами. На основі розрахованих показників можна буде визначити розмір капітальних витрат на навчання спеціалісту кібербезпеки, що проводитиме сніфінг та експлуатаційних витрат, які необхідні для проведення сніфінгу спеціалістом. Також необхідно буде розрахувати величину втрат, яку зможе відвернути спеціаліст, що проводитиме сніфінг та, на основі цього, розрахувати загальний ефект від впровадження комплексу лабораторних робіт. На основі розрахованих показників можна бути зробити висновок, чи є навчання студента за допомогою розроблених матеріалів вигідним.

3.2 Розрахунок капітальних витрат на розробку програмно-методичних ресурсів для лабораторних робіт з теми «сніфінг»

До фіксованих (капітальних) варто відносити наступні витрати для НТУ «Дніпровська політехніка»:

– витрати на залучення працівника, який розроблюватиме програмно-методичні ресурси для лабораторних робіт;

– витрати на електроенергію, яку споживає апаратне забезпечення за час роботи працівника, що розробляє програмно- методичні ресурси.

Для підрахунку заробітної платні працівника, який розроблює програмно-методичні ресурси для лабораторних робіт з теми «сніфінг», необхідно розрахувати трудомісткість розробки. Вона визначається тривалістю кожної робочої операції цього працівника:

$$t = t_{\text{тз}} + t_{\text{кнк}} + t_{\text{ааз}} + t_{\text{спз}} + t_{\text{по}} + t_{\text{до}} \quad , \text{ годин}, \qquad (3.1)$$

де:

$t_{\text{тз}} = 5$ – тривалість складання технічного завдання на розробку програмно-апаратних ресурсів;

$t_{\text{кнк}} = 8$ – тривалість розробки концепції навчального комплексу;

$t_{\text{ааз}} = 3$ – тривалість процесу аналізу апаратного забезпечення аудиторії;

$t_{\text{спз}} = 21$ – тривалість визначення складу необхідного програмного забезпечення та вимог щодо програмного забезпечення;

$t_{\text{по}} = 5$ – тривалість підготовки оточення в аудиторії (розробка програмних ресурсів);

$t_{\text{до}} = 26$ – тривалість документального оформлення методичних матеріалів;

$$t = 5+8+3+21+5+26=68 \text{ годин.}$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальні потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) та визначається за формулою:

$$З_{\text{зп}} = t \cdot З_{\text{іб}}, \quad \text{грн}, \qquad (3.2)$$

де:

t =68 – загальна тривалість розробки;

$З_{\text{іб}} = 56$ – средньогодинна заробітна плата спеціаліста, грн/годину. У даному випадку вважатимемо, що роботи по створенню програмно-методичних ресурсів виконує викладач. Середня заробітна плата викладача на годину становить 56 грн.

$$З_{\text{зп}} = 68 \cdot 56 = 3808$$

У даному випадку, витрати на розробку програмно-методичних ресурсів для лабораторних робіт з теми «сніфінг» включають в себе заробітну плату робітника, а також витрати на електроенергію – при розробці працівник використовує одну робочу станцію в аудиторії, отже необхідно також розрахувати

витрати електроенергії для одного комп'ютера на увесь вище розрахований час (оскільки при усій вищезазначеній роботі використовується комп'ютер).

$$З_{мч} = t \cdot С_{мч}, \quad грн, \tag{3.3}$$

Щоб розрахувати вартість 1 годинного часу, скористаюсь формулою:

$$С_{мч} = Р \cdot t_{нал} \cdot С_е + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}, \quad грн \tag{3.4}$$

де:

P = 1,1 – встановлена потужність ПК, кВт;

C_e = 1,68 – тариф на електричну енергію, грн/кВт·година;

$Ф_{зал}$ = 0 – залишкова вартість ПК на поточний рік, грн.;

$Н_а$ =1/3 – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ = 1 – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ = 0 – вартість ліцензійного програмного забезпечення, грн;

$F_р$ = 1920 – річний фонд робочого часу (за 40-годинного робочого тижня $F_р$ = 1920).

$$С_{мч} = 1{,}1 \cdot 1{,}68 = 1{,}9 \text{ грн.}$$

$$З_{мч} = 68 \cdot 1{,}9 = 129 \text{ грн.}$$

Вартість придбання програмного забезпечення дорівнює нулю, оскільки в аудиторії 1/72 вже придбана та встановлена необхідна операційна система (Windows 10), а усі програми, що використовуються у розроблених лабораторних роботах, є вільним програмним забезпеченням, або мають демо-версію, якої вистачає для проходження розробленого курсу. Таким чином, Крп – вартість розробки проекту та залучення для цього фахівців становить:

$$К_{пр} = З_{зп} + З_{мч}, \quad грн, \tag{3.5}$$

$$К_{пр} = 3808 + 129 = 3937 \text{ грн}$$

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = K_{пр}, \text{ грн}, \quad (3.6)$$

де:

$K_{пр}$ – вартість розробки проекту та залучення для цього фахівців.

$$К = 3937 \text{ грн}.$$

3.3 Розрахунок річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (рік), що виражені у грошовій формі.

Для організації, у якій проводиться сніфінг, актуальними можуть бути експлуатаційні витрати на електроенергію, що буде споживатися комп'ютерами під час виконання відповідних робіт, а також заробітна платня, яка буде виплачуватися спеціалісту з кібербезпеки за проведення сніфінгу.

Вартість електроенергії, що споживається апаратурою протягом року ($С_е$), визначається за формулою:

$$С_е = Р_к \cdot F_р \cdot Ц_е, \text{ грн}, \quad (3.7)$$

де:

$Р_к = 1,1$ – встановлена потужність ПК, кВт;

$F_р = 120$ – річний фонд робочого часу спеціаліста, год;

$Ц_е = 1,68$ – тариф на електроенергію, грн/кВт·годин.

Таким чином:

$$C_е = 1{,}1 \cdot 1{,}68 \cdot 120 = 221{,}76 \text{ грн.}$$

Також, до експлуатаційних витрат слід додати заробітну платню спеціаліста, що проводитиме сніфінг в організації:

$$C_з = t \cdot З_{іб}, \text{ грн,} \qquad (3.8)$$

де:

$З_{іб}$ = 124 – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину;

t = 120 – час, необхідний для виконання сніфінгу в організації спеціалістом з кібербезпеки, год.

$$C_з = 124 \cdot 120 = 14880 \text{ грн}$$

Отже, річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$C = C_е + C_з = 222 + 14880 = 15102 \text{ грн.} \qquad (3.9)$$

3.4 Визначення економічного ефекту від впровадження запропонованих у роботі рішень

Виконавши запропоновані лабораторні роботи, методично-програмне забезпечення до яких було розроблено у цій роботі, студент у майбутньому зможе протидіяти атакам типу «людина посередині» та сніфінгу, тобто сприятиме захисту від певних загроз інформаційній безпеці. Або він зможе виконувати тестування на проникнення, використовуючи ці технології, допомагаючи, таким чином, компанії захиститися від цих загроз. Отже, у будь-якому випадку, можна розрахувати величину потенційно відвернених збитків для компанії, з якою працюватиме студент, виходячи з імовірності виникнення відповідного інциденту інформаційної безпеки й можливих економічних втрат від нього.

Далі буде визначено можливі збитки від загрози сніфінгу та атак типу «людина посередині». Внаслідок їх реалізації може буде викрадено персональні дані працівників або клієнтів компанії, можуть бути розкриті ідентифікаційні та аутентифікаційні дані.

Станом на 2019 рік, середня кількість вкрадених персональних даних для середньої компанії у світі становить 25575 записів, а середня вартість запису – 150 доларів. [8]. Величина середньої вартості запису розраховувалася Інститутом Понемона, враховуючи втрату довіри споживачів після інциденту кібербезпеки та зменшення кількості клієнтів, як наслідок. Отже, для загрози, пов'язаної з втратою персональних даних внаслідок сніфінгу та атаки «людина посередині», збиток становить:

$$B = 25575 \cdot 150 \cdot 28{,}37 = 108834413 \text{ грн.}$$

Розкриття ідентифікаційних та аутентифікаційних даних може призводити до різних наслідків, залежно від того, пароль та ідентифікатор від якої саме системи було розкрито. Найчастіше розкриття такої інформації також веде до втрати персональних даних, або до втрати доступності інформаційної системи. Оскільки розмір збитків від цього випадку дуже залежить від специфіки компанії, не розглядатимемо його.

Хоча атаки MitM не настільки поширені, як атаки-вимагачі чи фішинг, вони постійно загрожують організаціям. Наразі, ймовірність подібних атак зменшено, оскільки більше половини всього інтернет-трафіку у світі зараз зашифровано (за даними Electronic Frontier Foundation), а такі браузери як Chrome і Firefox попереджатимуть користувачів про ризик атак MitM. Втім, загальноприйнятим є використання принципалів MitM у більш складних атаках. Атаки типу «людина посередині» були задіяні у 35% атакованих компаній, згідно з Індексом розвідки X-Force від IBM IBM 2018. [9]

Також, згідно з дослідженнями 2020 року, 50% компаній, що відносяться до малого та середнього бізнесу повідомили, що зазнали щонайменше однієї кібератаки за останній рік. [10]

Отже, можна стверджувати, що ймовірність атаки типу «людина посередині» становить:

$$R = 0{,}35 \cdot 0{,}5 = 0{,}18$$

Таким чином, ймовірні збитки становлять:

$$B \cdot R = 108834413 \cdot 0{,}18 = 19590194 \text{ грн.}$$

3.5 Визначення та аналіз показників економічної ефективності запропонованого рішення

Загальний ефект від впровадження становить:

$$E = B \cdot R - C = 19590194 - 15102 = 19575092 \text{ грн.} \qquad (3.10)$$

де:

B – загальний збиток від атаки корпоративну мережу, грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на підтримку комплексу, грн.

3.6 Висновок про економічну доцільність проектного рішення

В цьому розділі було визначено розмір капітальних витрат на створення програмно-методичного комплексу для лабораторних робіт з теми «снiфінг», тобто величину витрат на навчання спеціалістів кібербезпеки, що будуть застосовувати снiфінг (3937 грн) та експлуатаційних витрат, які необхідні для проведення снiфінгу спеціалістом (15102 грн), а також величину втрат, яку може відвернути студент, працюючи у майбутньому і володіючи при цьому навичками, які він отримає під час виконання лабораторних робіт (108834413 грн) та, на

основі цього, розраховано загальний ефект від впровадження (19575092 грн). На основі розрахованих показників можна зробити висновок, що навчання студента за допомогою розроблених матеріалів є досить вигідним. Окрім цього, можна зазначити, що впровадження розроблених матеріалів підвищить конкурентоспроможність НТУ «Дніпровська політехніка», оскільки навички, отримані студентом завдяки розробленому програмно-методичному комплексу допоможуть студентові бути більш конкурентоспроможним на ринку праці. Однак, такий показник, а також вигоду для держави (більш кваліфікований працівник буде отримувати більшу заробітну плату та, відповідно, виплачувати більше податків) у межах цієї роботи не розраховуємо, оскільки такі розрахунки є досить складними і для них потребується більше інформації.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було обґрунтовано необхідність створення програмно-методичного комплексу для лабораторних робіт з теми «сніфінг» та проведено аналіз теоретичної частини щодо сніфінгу, після чого було обране необхідне оточення для проведення таких робіт в НТУ «Дніпровська політехніка» (віртуальні машини у віртуальній мережі), а також обрані інструменти, тобто програмне забезпечення, що буде використовуватися у лабораторних роботах з теми «сніфінг». Цими інструментами стали: OmniPeek, SMAC, Capsa network analyser, Wireshark, Cain and Abel, Xarp tool, Sniff-o-matic. Оточення та програмне забезпечення було встановлено та налаштовано в аудиторії 1/72. Також були підготовлені методичні матеріали для виконання лабораторних робіт.

Таким чином, було розроблено матеріали для семи лабораторних робіт. У кожній такій роботі пропонується дослідити можливості певного інструменту зі сніфінгу згідно запропонованих пунктів, а також створити звіт з лабораторної роботи. У звіті студенту необхідно додати декілька скріншотів, що засвідчуватимуть виконання лабораторної роботи, при необхідності додати короткий опис та інформацію про певний протокол або атаку, для того щоб поглибити знання студента про механізми роботи деяких атак, а також програмного забезпечення, що можуть у них використовуватися.

Наприкінці було також проведено аналіз економічної доцільності створення цих програмно-методичних ресурсів для лабораторних робіт в НТУ «Дніпровська політехніка».

ПЕРЕЛІК ПОСИЛАНЬ

1. Ethical Hacking – Sniffing. URL: https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_sniffing.htm (дата звернення: 2.12.2020).
2. Virtualization and Cyber Security: Arming Future Security Practitioners. URL: https://www.researchgate.net/publication/279941493_Virtualization_and_Cyber_Security_Arming_Future_Security_Practitioners (дата звернення: 10.11.2020).
3. Установка Hyper-V в Windows 10. URL: https://docs.microsoft.com/ru-ru/virtualization/hyper-v-on-windows/quick-start/enable-hyper-v (дата звернення: 10.11.2020).
4. Colasoft Capsa Network Analyzer. URL: https://colasoft-capsa.en.softonic.com/?ex=CORE-117.0 (дата звернення: 21.11.2020).
5. What is Wireshark? What this essential troubleshooting tool does and how to use it. URL: https://www.csoonline.com/article/3305805/what-is-wireshark-what-this-essential-troubleshooting-tool-does-and-how-to-use-it.html (дата звернення: 17.11.2020).
6. Password Cracking Using Cain & Abel. URL: https://resources.infosecinstitute.com/topic/password-cracking-using-cain-abel/ (дата звернення: 18.11.2020).
7. PenTest Edition: Creating A Man-in-the-Middle Attack using Cain & Abel [Tutorial]. URL: https://thecybersecurityman.com/2017/12/06/creating-a-man-in-the-middle-attack-using-cain-abel-tutorial/ (дата звернення: 17.11.2020).
8. Loss of business: the largest cost of a data breach. URL: https://www.pandasecurity.com/en/mediacenter/security/cost-of-a-data-breach/ (дата звернення: 27.11.2020).

9. What is a man-in-the-middle attack? How MitM attacks work and how to prevent them. URL: https://www.csoonline.com/article/3340117/what-is-a-man-in-the-middle-attack-how-mitm-attacks-work-and-how-to-prevent-them.html (дата звернення: 24.11.2020).
10. 30 Surprising Small Business Cyber Security Statistics (2020). URL: https://www.fundera.com/resources/small-business-cyber-security-statistics (дата звернення: 24.11.2020).
11. Automatically monitor and measure network and application performance with network sniffer software. URL: https://www.solarwinds.com/network-performance-monitor/use-cases/network-sniffer-tool (дата звернення: 25.11.2020).
12. Attempt to recover lost passwords for various offline and network services through decryption, powerful decoding algorithms, and extra tools. URL: https://www.softpedia.com/get/Security/Decrypting-Decoding/Cain-and-Abel.shtml (дата звернення: 30.11.2020).
13. XArp – Advanced ARP Spoofing Detection. URL: http://www.xarp.net/ (дата звернення: 30.11.2020).
14. Моніторинг. Візуалізація. Контроль. URL: https://www.ru.paessler.com/prtg (дата звернення: 2.12.2020).
15. SteelCentral Packet Analyzer Plus. URL: https://bakotech.ua/product/141/ (дата звернення: 3.12.2020).
16. Fiddler — помічник в дебаггінгу JavaScript. URL: https://habr.com/ru/post/140147/ (дата звернення: 29.11.2020).
17. Advanced System Administration and Troubleshooting. URL: https://www.sciencedirect.com/topics/computer-science/tcpdump (дата звернення: 24.11.2020).

18. Sniff-O-Matic. URL: https://download.cnet.com/Sniff-O-Matic/3000-2094_4-10542029.html
(дата звернення: 24.11.2020).
19. Omnipeek Network Protocol Analyzer. URL: https://www.liveaction.com/products/omnipeek-network-protocol-analyzer/
(дата звернення: 28.11.2020).
20. SMAC – FREE MAC Address Spoofing Tool. URL: https://www.klcconsulting.net/smac/
(дата звернення: 24.11.2020).
21. Sniff - O – Matic. URL: http://www.softsea.com/review/Sniff-O-Matic.html
(дата звернення: 16.11.2020).

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі	11	
6	А4	Спеціальна частина	37	
7	А4	Економічний розділ	8	
8	А4	Висновки	1	
9	А4	Перелік посилань	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

- Маркіна М.В._125м-19-2.docx
- Маркіна М.В._125м-19-2.pptx

ДОДАТОК В. Відгук керівника економічного розділу

Керівник економічного розділу к.е.н., доц. Пілова Д.П.

Дата: _____ Підпис: _____

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

Розробка програмно-методичних ресурсів для лабораторних робіт для теми «Сніфінг»

студентки групи 125м-19-2 Маркіної Марії Володимирівни

Кваліфікаційна робота за спеціальністю 125 Кібербезпека Маркіної М.В. представлена пояснювальною запискою на 74 с., 53 рис., 2 табл., 4 додатка, 21 джерело.

Мета кваліфікаційної роботи – розробка програмно-методичних ресурсів, ціллю яких є підвищення рівня кваліфікації та функціональності спеціалістів з кібербезпеки.

У ході виконання кваліфікаційної роботи були вирішені наступні питання: обґрунтовано необхідність створення програмно-методичних ресурсів, проаналізовано актуальність питання, проведено планування розробки необхідних ресурсів для відповідних лабораторних робіт, описана теоретична складова сфери кібербезпеки, що розглядається. Окрім того, підготовлено методичні матеріали для лабораторних робіт з теми «Сніфінг», описано процес налаштування оточення в аудиторії, в якій виконуватимуться роботи.

У економічному розділі були розраховані витрати на впровадження комплексу, доведена економічна доцільність його впровадження.

До недоліків проекту слід віднести окремі незначні невідповідності вимогам оформлення. Рівень запозичень у кваліфікаційній роботі не перевищує вимог «Положення про систему виявлення та запобігання плагіату».

Кваліфікаційну роботу виконано у відповідності до вимог, які пред'являються до кваліфікаційної роботи магістра і заслуговує оцінки "відмінно", а Маркіна Марія Володимирівна – присвоєння їй кваліфікації професіонала із організації інформаційної безпеки.

Керівник кваліфікаційної роботи к.т.н., доц. Флоров С.В.

Дата: _____ Підпис: _____