# КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ТАРАСА ШЕВЧЕНКА



## ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

**Кафедра прикладних інформаційних систем**

**Звіт до лабораторної роботи №6**

# з курсу

**«Безпека мереж і комп’ютерних систем»**

*Студента 2 курсу*

*групи ПП-21 спеціальності 122 «Комп'ютерні науки» ОП «Прикладне програмування»*

%username%

*Викладач:*

проф. Сайко В.Г.

## Київ – 202

**1.Назва роботи**

Вивчення брандмауерів, віртуальних приватних мереж і мережевих технологій

виявлення вторгнень і запобігання вторгнень

1. **Тема роботи**

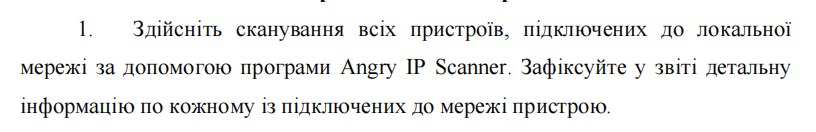
Вивчення брандмауерів, віртуальних приватних мереж і мережевих технологій

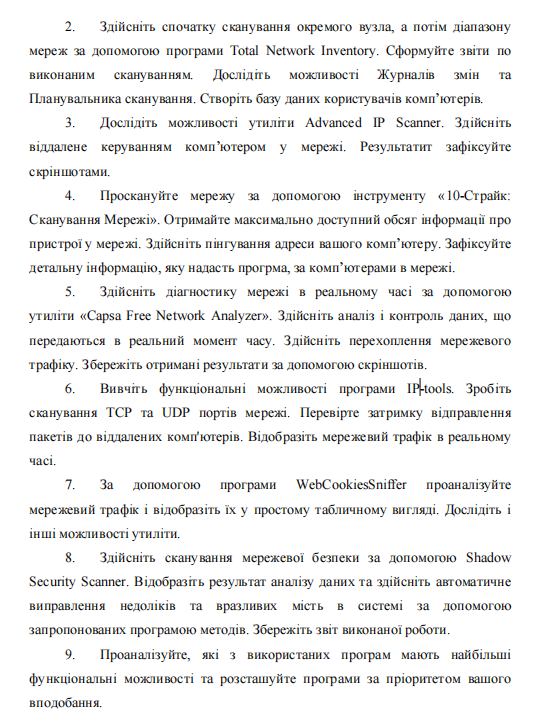
виявлення вторгнень і запобігання вторгнень

1. **Мета роботи**

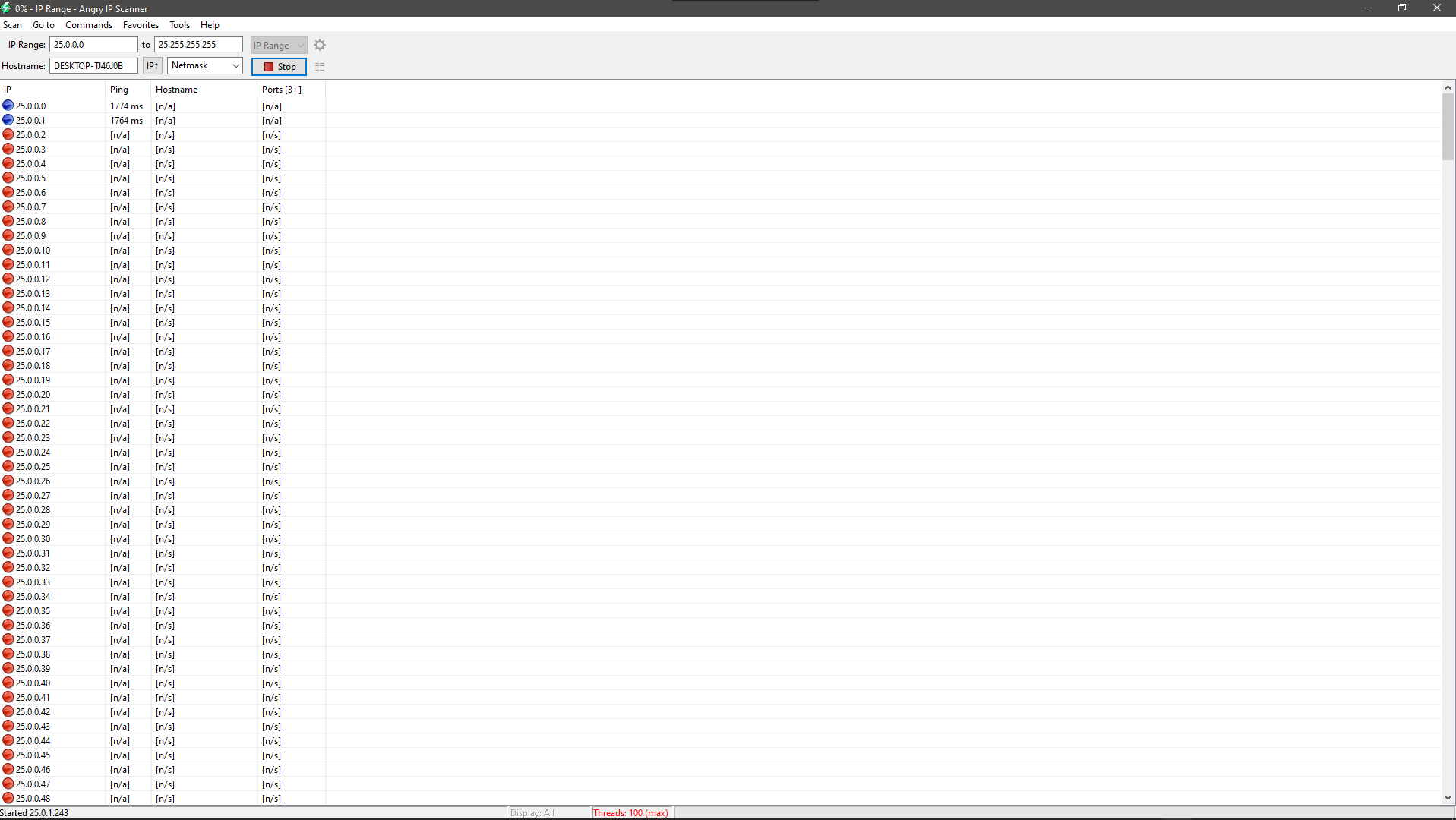
За допомогою інтернет-ресурсів проаналізувати загрози мережевій безпеці.

1. **Умова завдання**

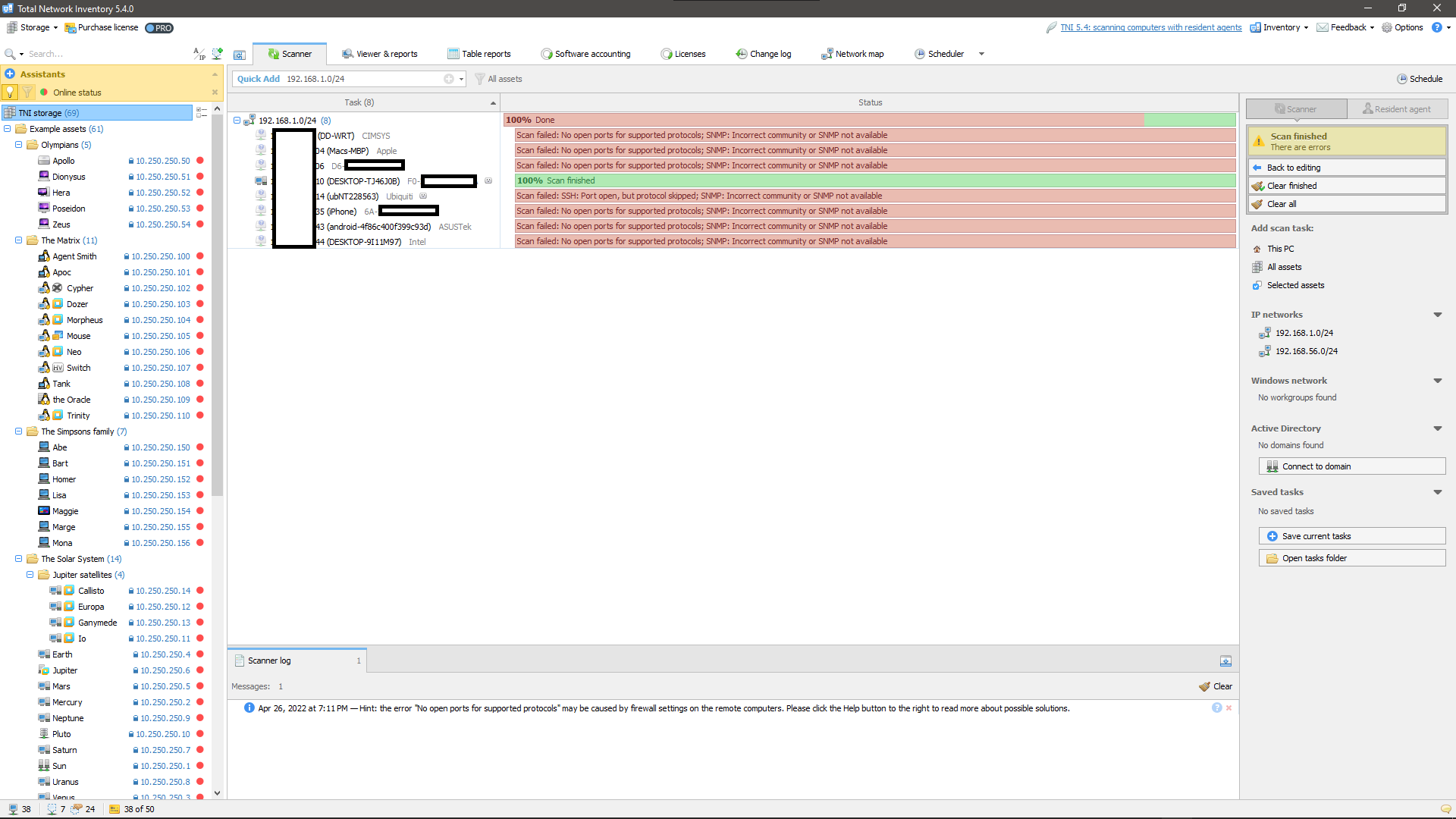


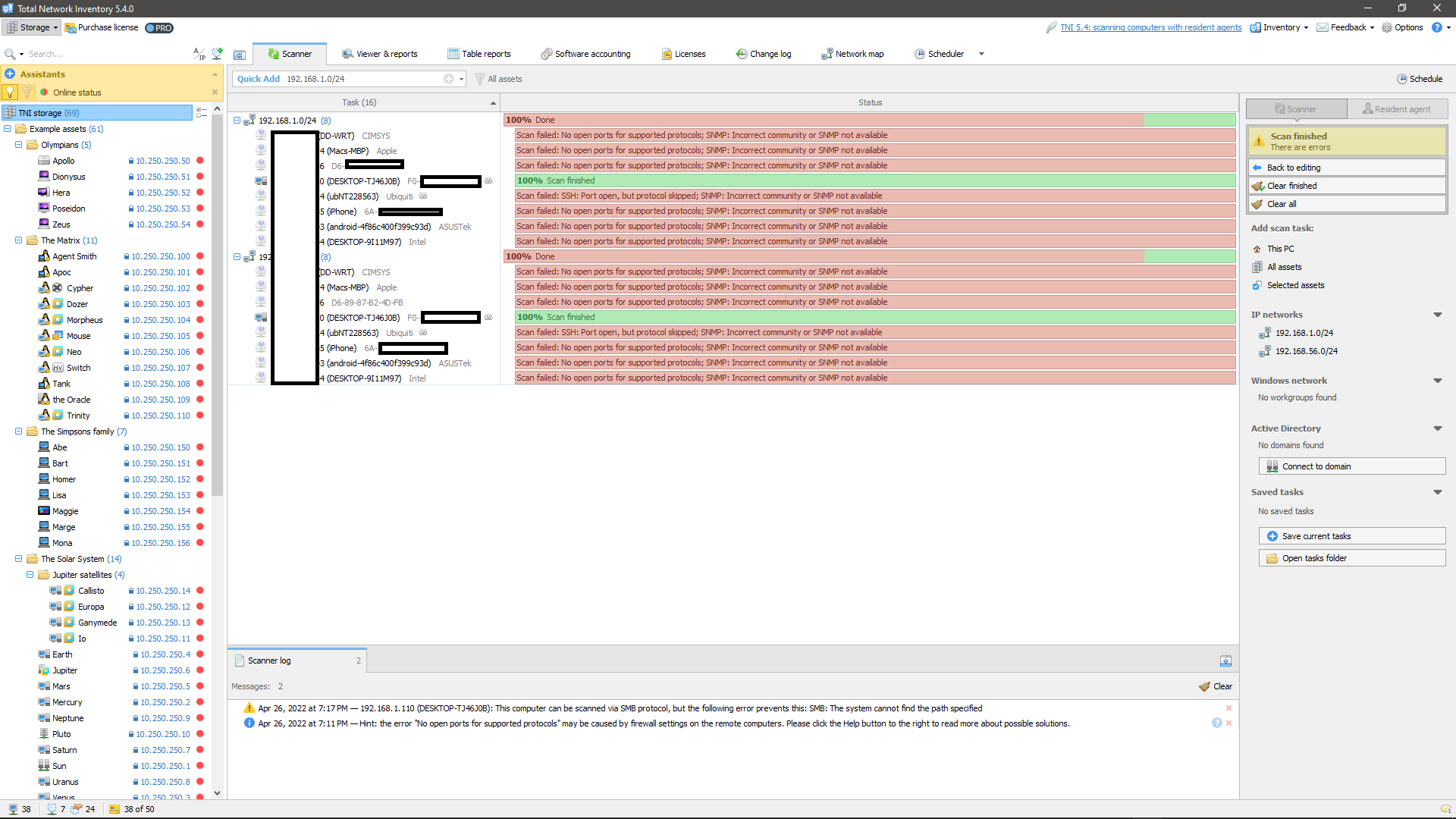


1. **Рішення**

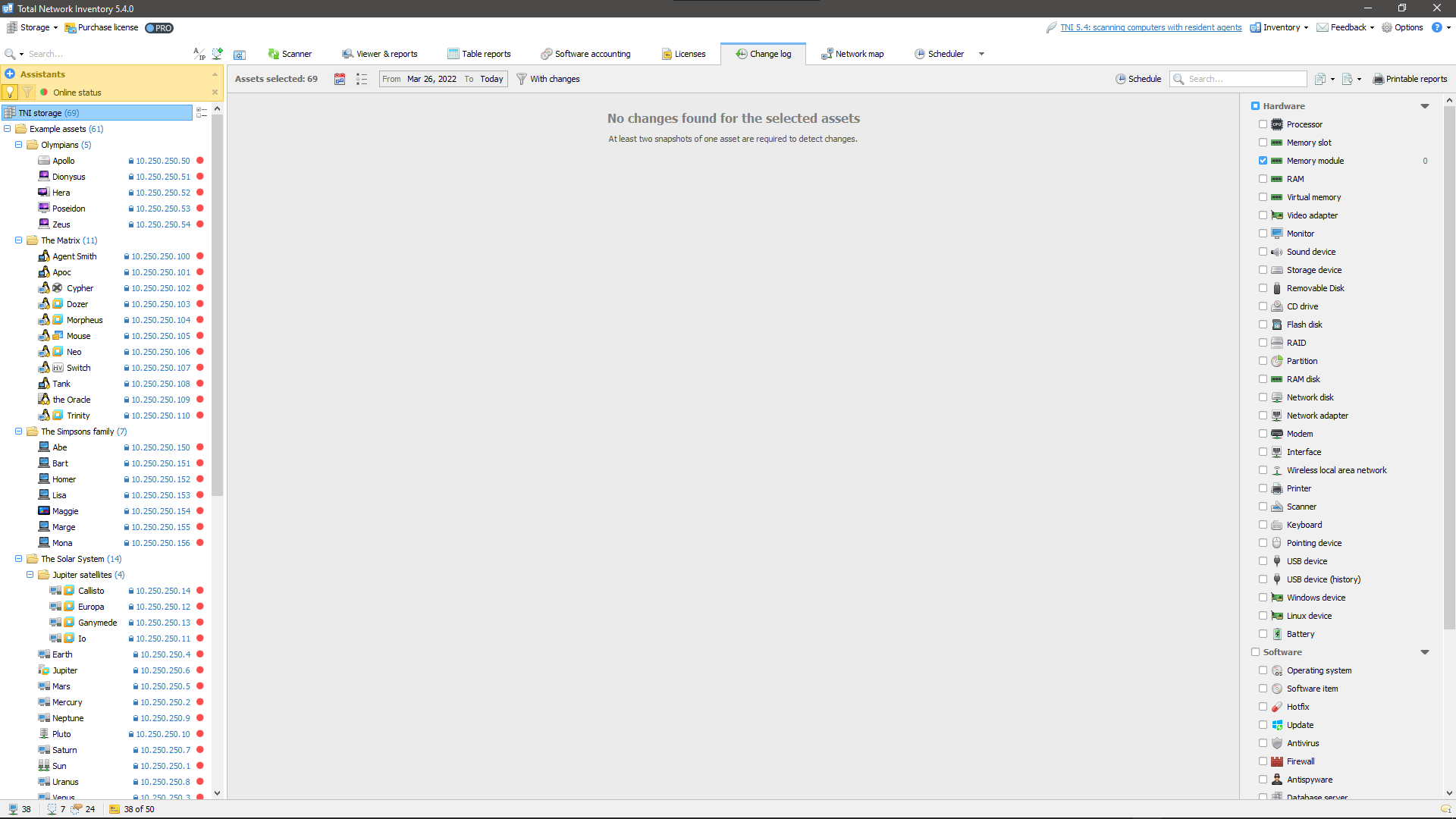


Angry IP scanner

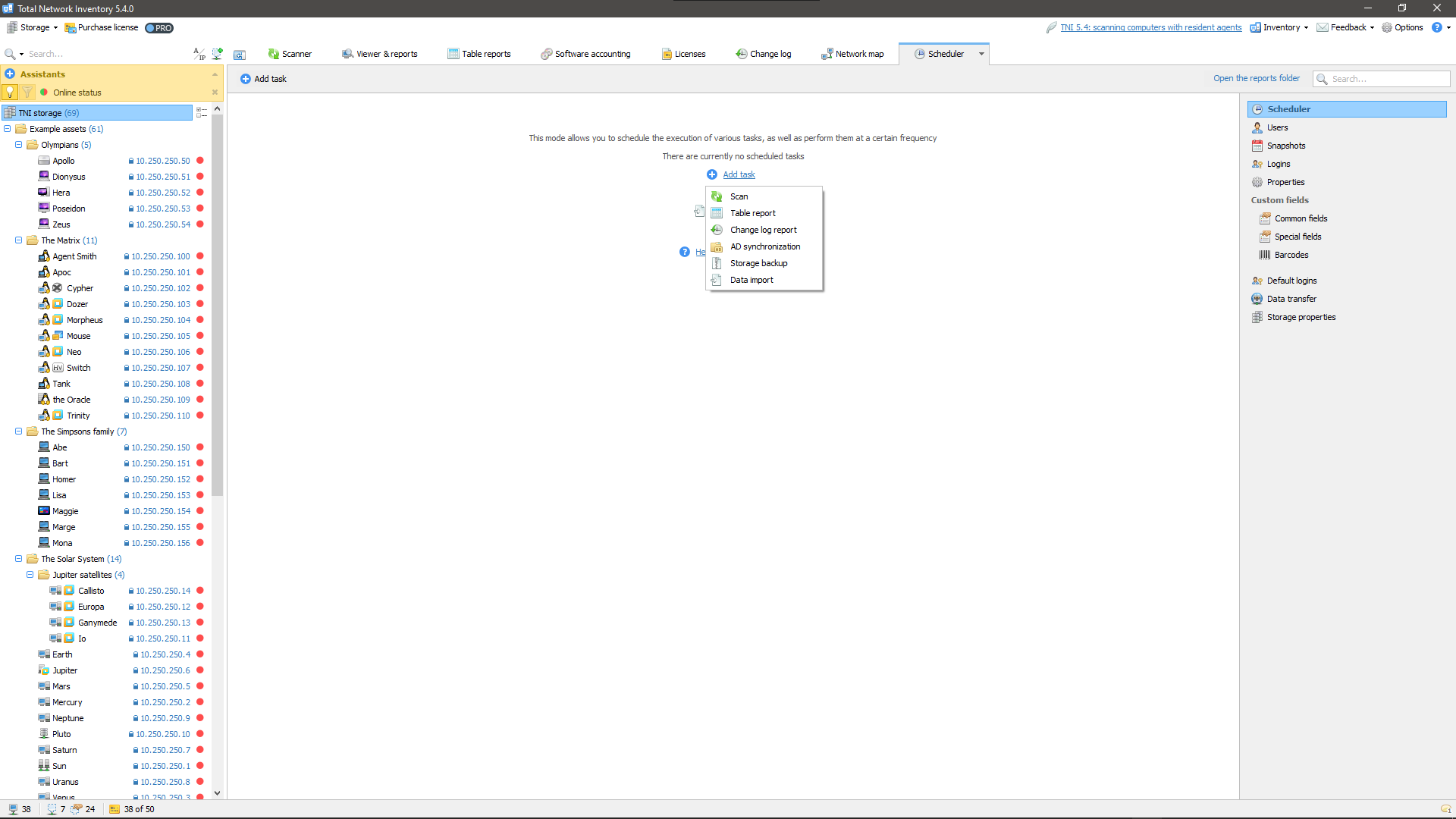




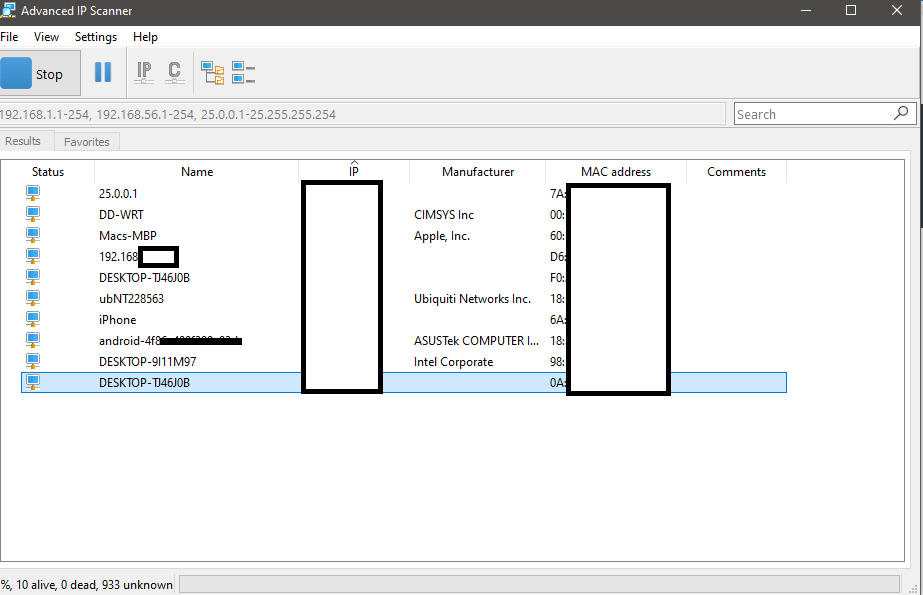
Total Network Inventory (сканування вузла, мережі)



TNI (журнал змін - дозволяє переглянути зміни в обладнанні та порівняти різні версії)



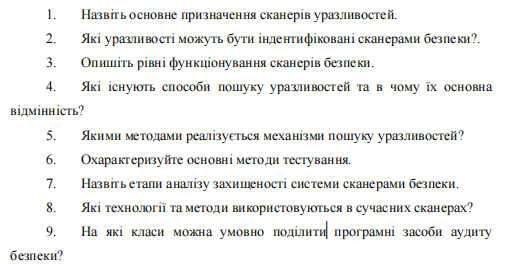
TNI (планувальник - дозволяє відкласти будь-яку функцію програми на заданий час)



Advanced IP Scanner

На мою думку, найбільш перспективна програма з вищевказаних - це Total Network Inventory. Вона має найбільший функціонал, найзручніший інтерфейс та гнучкі налаштування, що робить її накращим вибором для будь-якого використання - комерційного, навчального чи особистого.

**Контрольні запитання:**



1. Збір інформації про мережу, визначення потенційних уразливостей, підтверження існуючих вразливостей, генерування звітів.
2. Це залежить від типу сканеру - спеціально пристосовані сканери шукають більш спеціалізовані вразливості.
3. Збір інформації про мережу;

визначення потенційних уразливостей;

підтверження існуючих вразливостей;

генерування звіту

1. Сканування, зондування, імітація атак, експлойт
2. Вищевказаними способами пошуку уразливостей (іноді автоматизованими, іноді ручними)
3. Сканування - найбільш простий та пасивний метод, зондування - більш агресивний підхід, але менш агресивний за імітацію атак, експлойт - найрезультативніший та найскладніший метод.
4. Етапи аналізу захищеності корелюють з алгоритмом роботи сканеру - аналіз уразливостей, їх видалення та перевірка результатів.
5. Багатопоточне сканування, сканування у діапазоні, перегляд портів, виявлення МАС-адрес, доступ до мережевих папок, трасування маршруту, керування службами, перевірка заголовків.
6. Локальні (діють на безпеку одного ПК) та мережеві (діють на безпеку мережі)

**Висновки**

В результаті виконання даної лабораторної роботи я оволодів практичними навичками використання Angry IP scanner, користувався програмою Total Network Inventory для перевірки параметрів безпеки мережі та мого комп’ютера. Налаштував декілька інших програм, зокрема Advanced IP Scanner, WebCookiesSniffer, скориставшись різними клієнтами. Вважаю дану лабораторну роботу виконаною в повному обсязі.