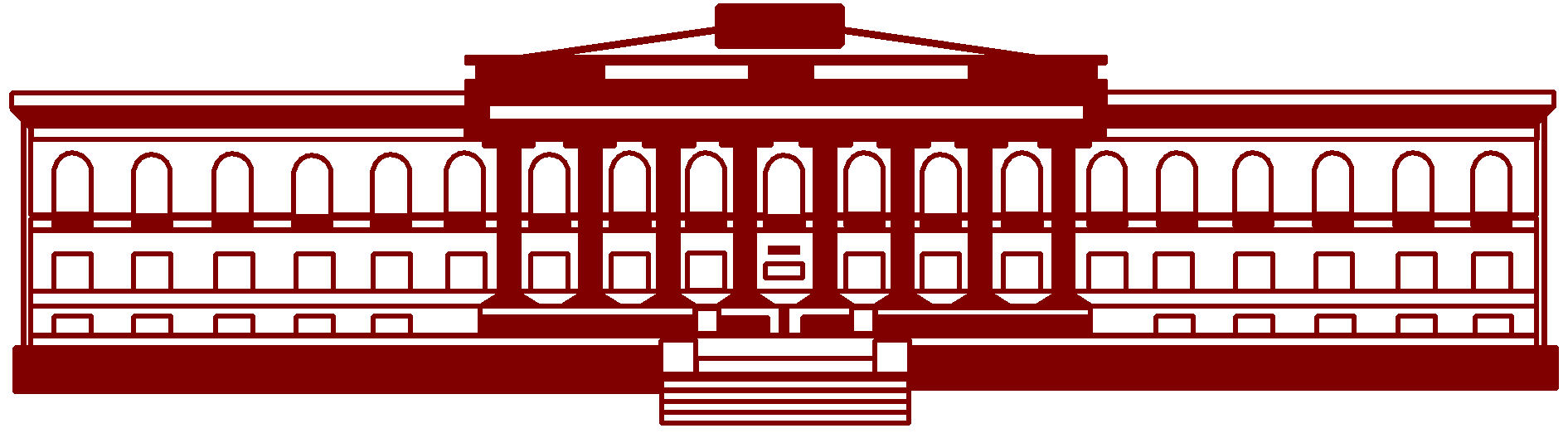
**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

**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-22*

*спеціальності 122 «Комп'ютерні науки»*

*ОП «Прикладне програмування»*

Шевлюк Вікторії Віталіївни

*Перевірив:*

д.т.н, професор

Сайко В. Г.

**Київ 2022**

**Тема:** Моніторинг стану ІС з використанням сканерів безпеки

**Мета роботи:** вивчити поняття сканерів безпеки, їх типи, етапи, рівні та механізми функціонування. Ознайомитися із сучасними додатками сканування мережі

**Завдання:**

1. Здійсніть сканування всіх пристроїв, підключених до локальної  
мережі за допомогою програми Angry IP Scanner. Зафіксуйте у звіті детальну  
інформацію по кожному із підключених до мережі пристрою.

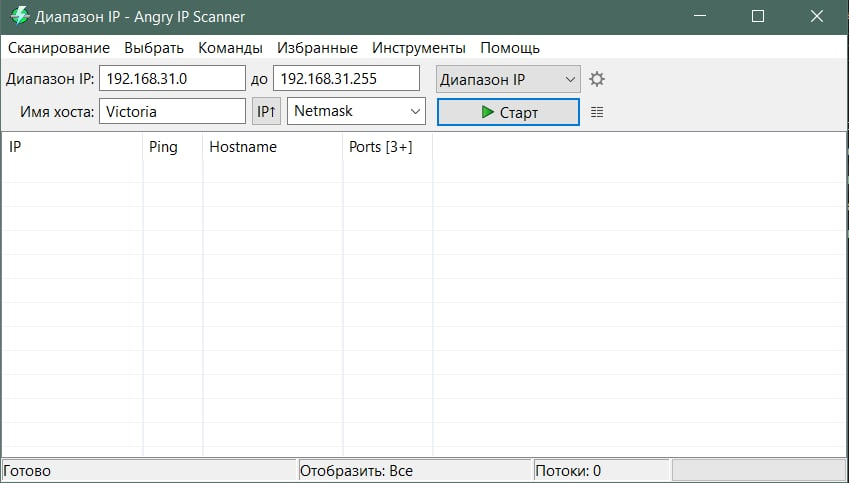
2. Здійсніть спочатку сканування окремого вузла, а потім діапазону  
мереж за допомогою програми Total Network Inventory. Сформуйте звіти по  
виконаним скануванням. Дослідіть можливості Журналів змін та  
Планувальника сканування. Створіть базу даних користувачів комп’ютерів.  
3. Дослідіть можливості утиліти Advanced IP Scanner. Здійсніть віддалене керуванням комп’ютером у мережі. Результатит зафіксуйте скріншотами.  
4. Проскануйте мережу за допомогою інструменту «10-Страйк:  
Сканування Мережі». Отримайте максимально доступний обсяг інформації про пристрої у мережі. Здійсніть пінгування адреси вашого комп’ютеру. Зафіксуйте детальну інформацію, яку надасть прогрма, за комп’ютерами в мережі.  
5. Здійсніть діагностику мережі в реальному часі за допомогою  
утиліти «Capsa Free Network Analyzer». Здійсніть аналіз і контроль даних, що  
передаються в реальний момент часу. Здійсніть перехоплення мережевого  
трафіку. Збережіть отримані результати за допомогою скріншотів.  
6. Вивчіть функціональні можливості програми IP-tools. Зробіть сканування TCP та UDP портів мережі. Перевірте затримку відправлення пакетів до віддалених комп'ютерів. Відобразіть мережевий трафік в реальному часі.  
7. За допомогою програми WebCookiesSniffer проаналізуйте мережевий трафік і відобразіть їх у простому табличному вигляді. Дослідіть і інші можливості утиліти.  
8. Здійсніть сканування мережевої безпеки за допомогою Shadow  
Security Scanner. Відобразіть результат аналізу даних та здійсніть автоматичне виправлення недоліків та вразливих мість в системі за допомогою запропонованих програмою методів. Збережіть звіт виконаної роботи.  
9. Проаналізуйте, які з використаних програм мають найбільші функціональні можливості та розсташуйте програми за пріоритетом вашого  
вподобання.

**Хід роботи:**

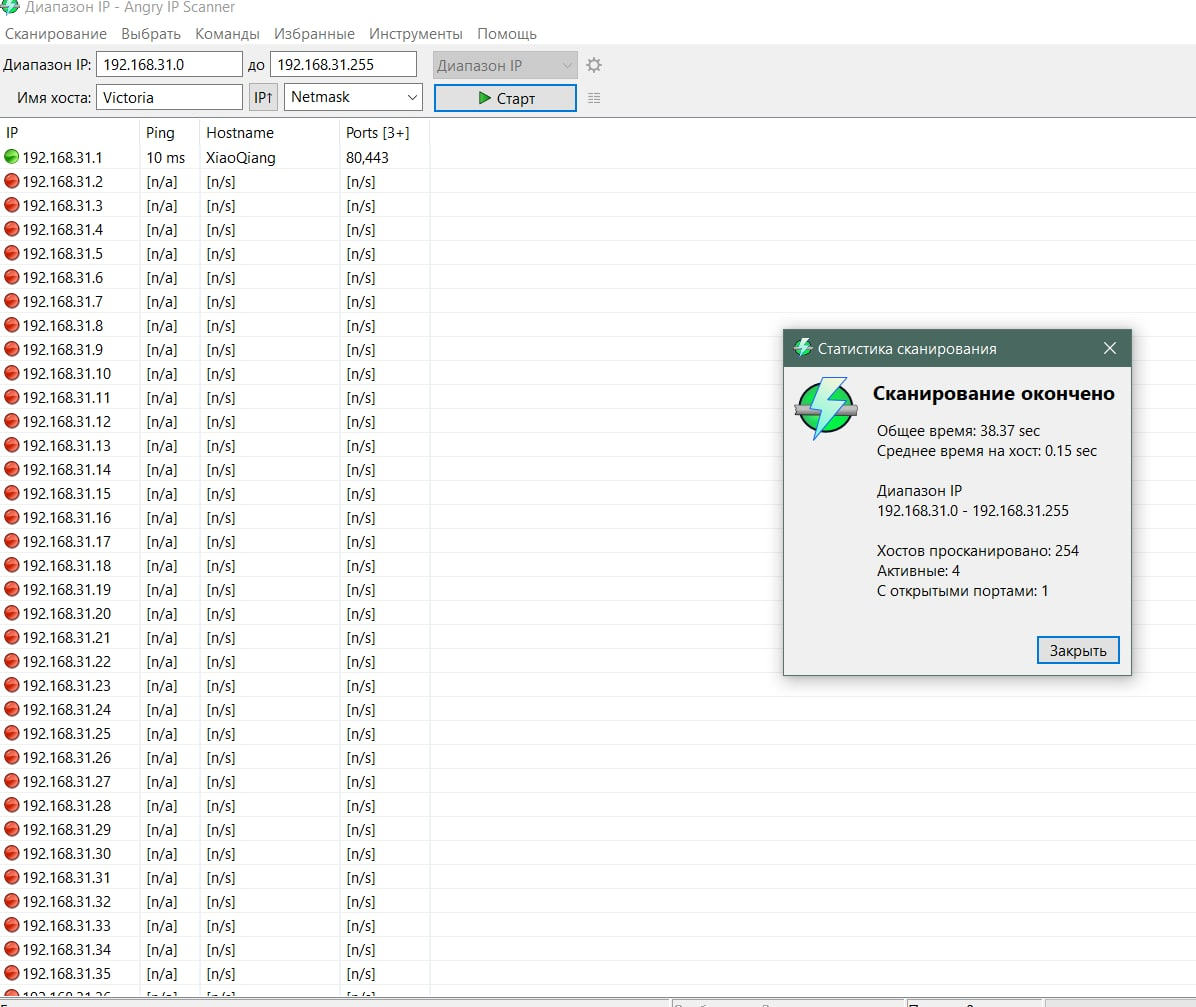
Встановимо Angry IP Scanner:

Angry IP Scanner – програма для сканування всіх пристроїв підключених до локальної мережі. Програма здатна сканувати мережу на предмет активних хостів за вказаними IP-адресами або в заданому діапазоні. Angry IP Scanner надає достатньо інформації щодо кожної виявленої адреси, а саме MAC-адресу, відкриті порти, повне ім’я комп’ютера і його робочу групу в мережі. Програма дає можливість отримати швидкий доступ до FTP, Telnet, SSH або web-сервера перевіреного комп’ютера. Angry IP Scanner дозволяє зберігати результати сканування у файлах TXT, CSV, XML або IP-Port. Також програма здатна розширити власну функціональність завдяки підключенню сторонніх або власноруч створених плагінів.  
Основні особливості:  
• Багатопоточне сканування;  
• Сканування IP-адрес у заданому діапазоні;  
• Підтримка UDP і TCP запитів;  
• Перегляд відкритих портів;  
• Збереження результату в різних форматах файлів.





Проскануємо цим сканером мою мережу:

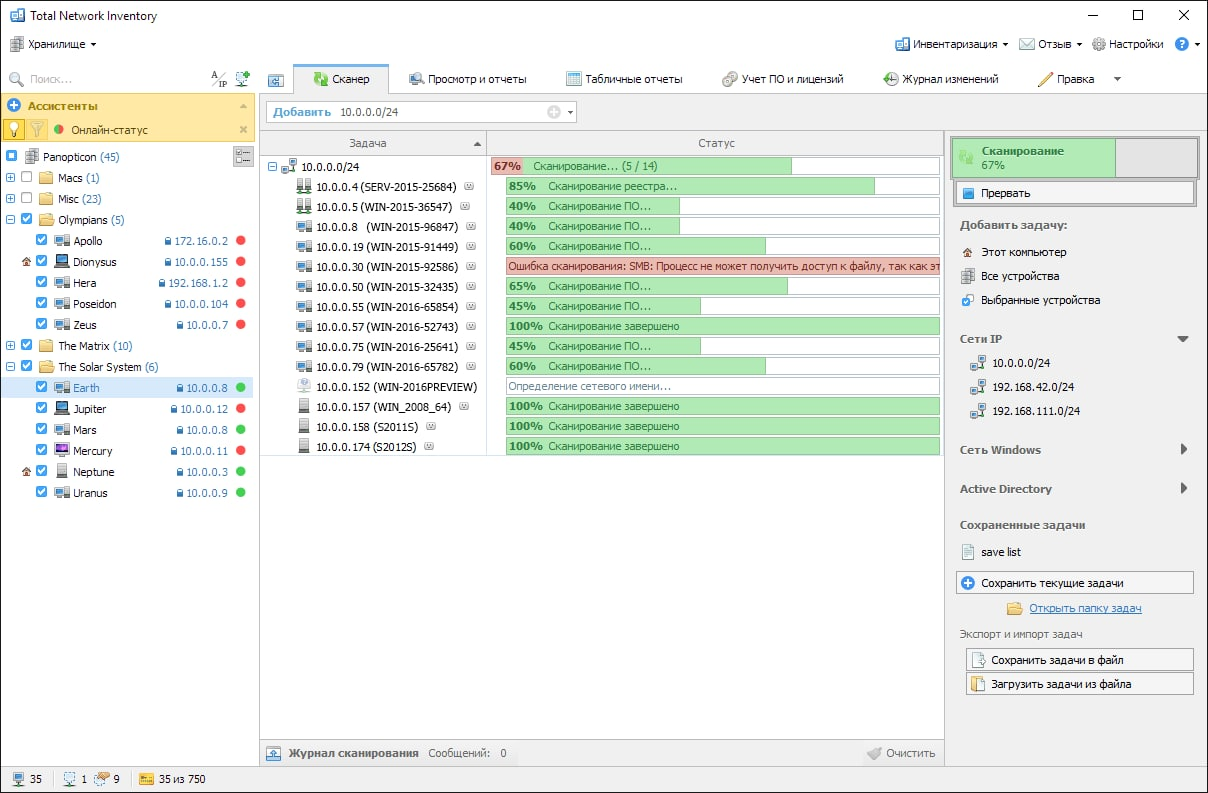


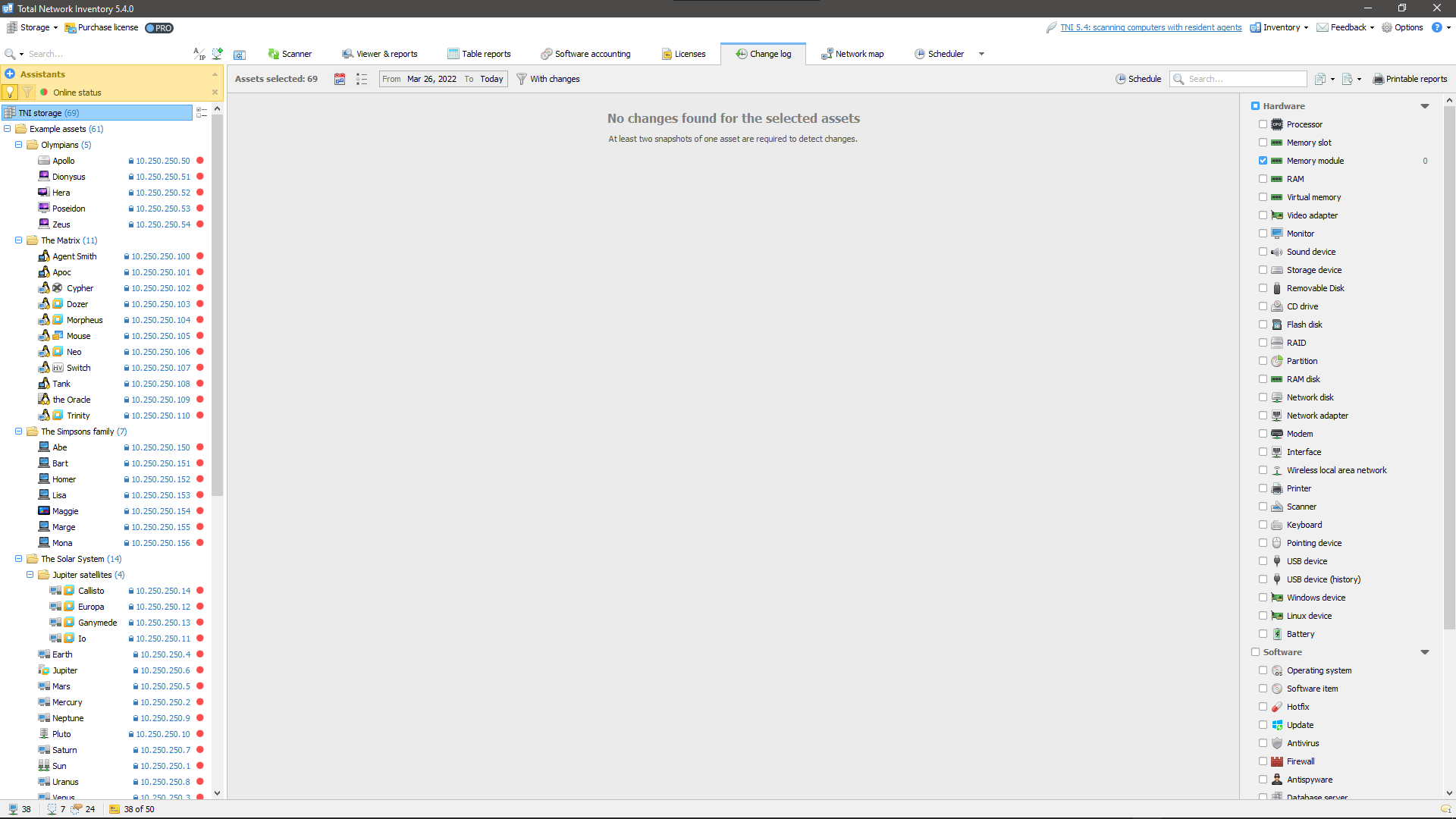
Ми можемо побачити айпі-адреси пристроїв, що з’являлись у цій мережі у заданому діапазоні. Якщо сканер знаходить хост з відкритим портом, він може надати про нього детальну інформацію, щодо всіх інших – можна продивитись лише айпі-адресу.

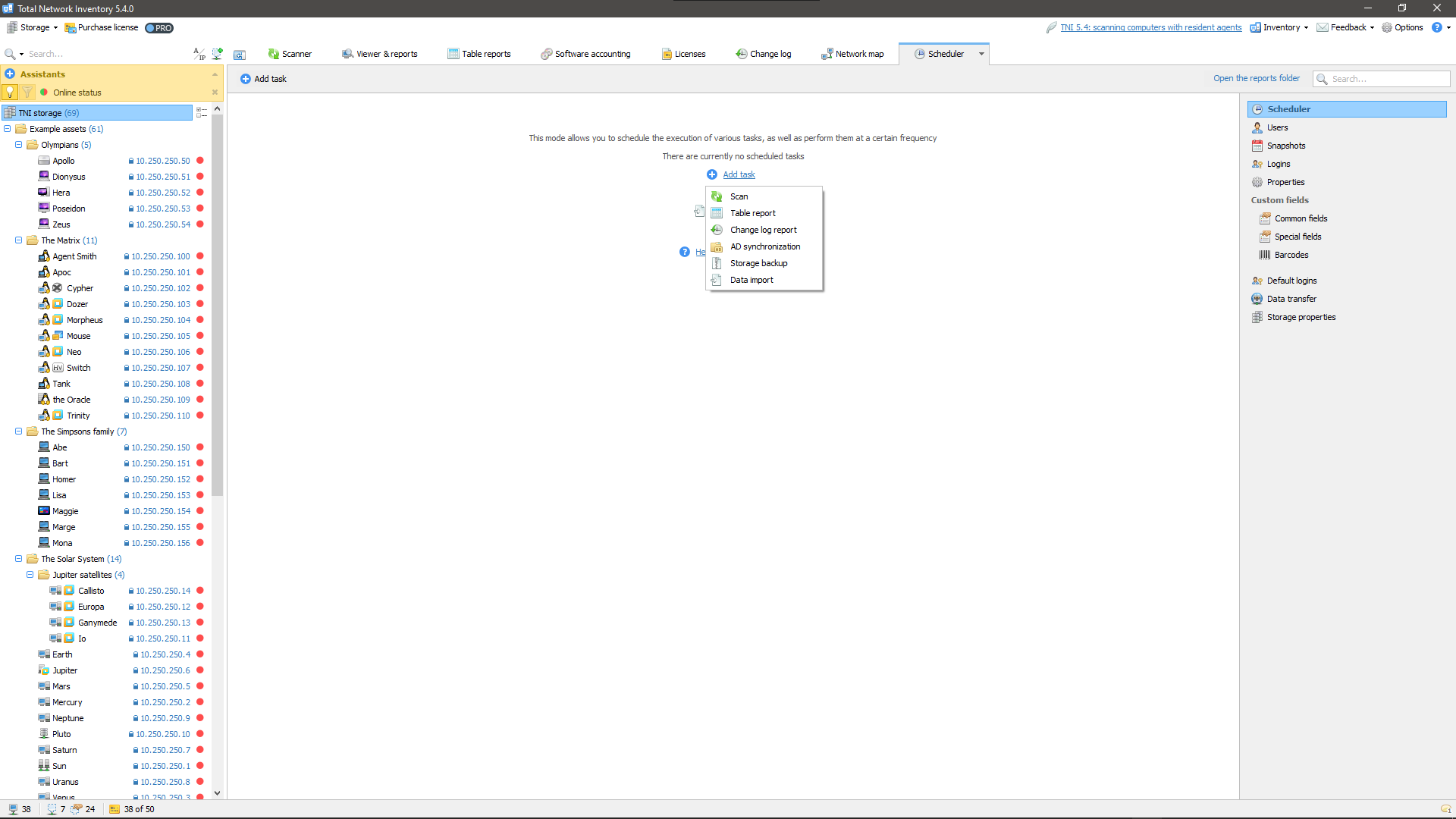
Далі протестуємо Total Network Inventory (сканування вузла, мережі):

Total Network Inventory – програма для інвентаризації комп’ютерів та  
мережевого устаткування.

Вона дозволяє здійснювати сканування комп’ютерів на базі Windows,  
Linux, FreeBSD та ін. без використання наперед встановлених агентів –  
потрібно знати лише адміністраторський пароль. Можна сканувати окремі  
вузли, діапазони мережевих адрес або структуру Active Directory.  
У централізованому сховищі TNI 4 кожний комп’ютер займає усього  
лише декілька десятків кілобайтів. Тому можна групувати пристрої,  
коментувати їх та прикріпляти додаткову інформацію до них.  
Програма дозволяє формувати гнучкі звіти за різноманітними  
категоріями даних, будувати табличні звіти, використовуючи сотні полів  
моделі даних Total Network Inventory 4. Звіти можна скопіювати, експортувати або роздрукувати, а функція пошуку показує результати раніше, ніж завершиться робота виводу запиту. Журнал змін дозволяє відстежувати зміни в апаратному та програмному забезпеченні. Це дає можливість точно встановити, коли були інстальовані, видалені або оновлені програми на будь-якому комп'ютері у мережі. Таким чином, можна стежити за підключенням і відключенням пристроїв, динамікою використання дискового простору і багатьом іншим. Планувальник сканування дозволяє автоматизувати збирання даних. З його допомогою можна створити одноразові відкладені задачі або розклади для періодичного сканування комп'ютерів. Також можна скласти базу даних користувачів комп’ютерів у мережі, зберігати безліч паролів для різних пристроїв та протоколів, слідкувати за онлайн-статусом пристроїв в реальному часі та багато іншого.

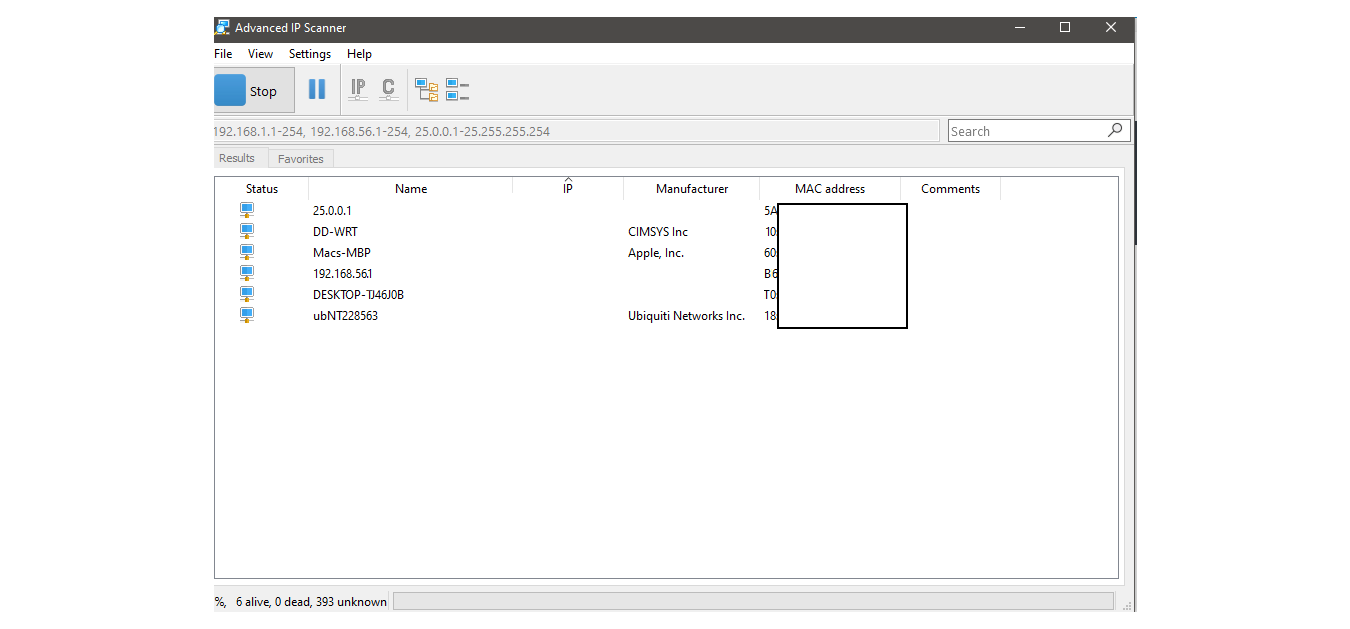






Далі протестуємо Advanced IP Scanner:

Надійний і безкоштовний сканер для аналізу локальних мереж. Ця  
програма шукає всі пристрої в мережі, надає доступ до спільних папок, дає  
змогу віддалено керувати комп’ютерами (через RDP та Radmin) і навіть може  
віддалено вимикати їх. Її легко використовувати та запускати як портативну  
версію. Це рішення повинен мати кожен адміністратор мережі.



**Висновок:** у ході даної лабораторної роботи ми протестували різні мережеві сканери і їх функції. Серед усіх вищепротестованих сканерів мені найбільше сподобався Advanced IP Scanner. Зручний і дуже простий інтерфейс, можливо не дуже широкий функціонал – проте, як на мене, для звичайного користувача – більш ніж достатньо.

**Контрольні питання:**

1. ***Назвіть основне призначення сканерів уразливостей.***

Збір інформації про мережу, визначення потенційних уразливостей, підтверження існуючих вразливостей, генерування звітів

***2. Які уразливості можуть бути індентифіковані сканерами безпеки?.***

Це залежить від типу сканеру - спеціально пристосовані сканери шукають більш спеціалізовані вразливості.

***3. Опишіть рівні функціонування сканерів безпеки.***

► Збір інформації про мережу;

► Визначення потенційних уразливостей;

► Підтверження існуючих вразливостей;

► Генерування звіту

***4. Які існують способи пошуку уразливостей та в чому їх основна  
відмінність?***

Сканування, зондування, імітація атак, експлойт

***5. Якими методами реалізується механізми пошуку уразливостей?***

Вищевказаними способами пошуку уразливостей (іноді автоматизованими, іноді ручними)

***6. Охарактеризуйте основні методи тестування.***

Сканування - найбільш простий та пасивний метод, зондування - більш агресивний підхід, але менш агресивний за імітацію атак, експлойт - найрезультативніший та найскладніший метод.

***7. Назвіть етапи аналізу захищеності системи сканерами безпеки.***

Етапи аналізу захищеності корелюють з алгоритмом роботи сканеру - аналіз уразливостей, їх видалення та перевірка результатів. ***8. Які технології та методи використовуються в сучасних сканерах?***

Багатопоточне сканування, сканування у діапазоні, перегляд портів, виявлення МАС-адрес, доступ до мережевих папок, трасування маршруту, керування службами, перевірка заголовків.

***9. На які класи можна умовно поділити програмні засоби аудиту  
безпеки?***

Локальні (діють на безпеку одного ПК) та мережеві (діють на безпеку мережі)