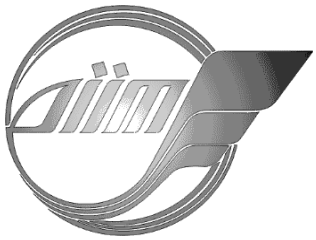
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ



УДУНТ ННІ ДІІТ

Кафедра «Комп'ютерні інформаційні технології»

Лабораторна робота №1

з дисципліни «Безпека програм та даних »

на тему: «Основні ознаки присутності шкідливих програм»

Виконав:
студент гр.ПЗ1911
Сафонов Д.Є.
Прийняв:
Разносілін В.В.

Дніпро, 2022

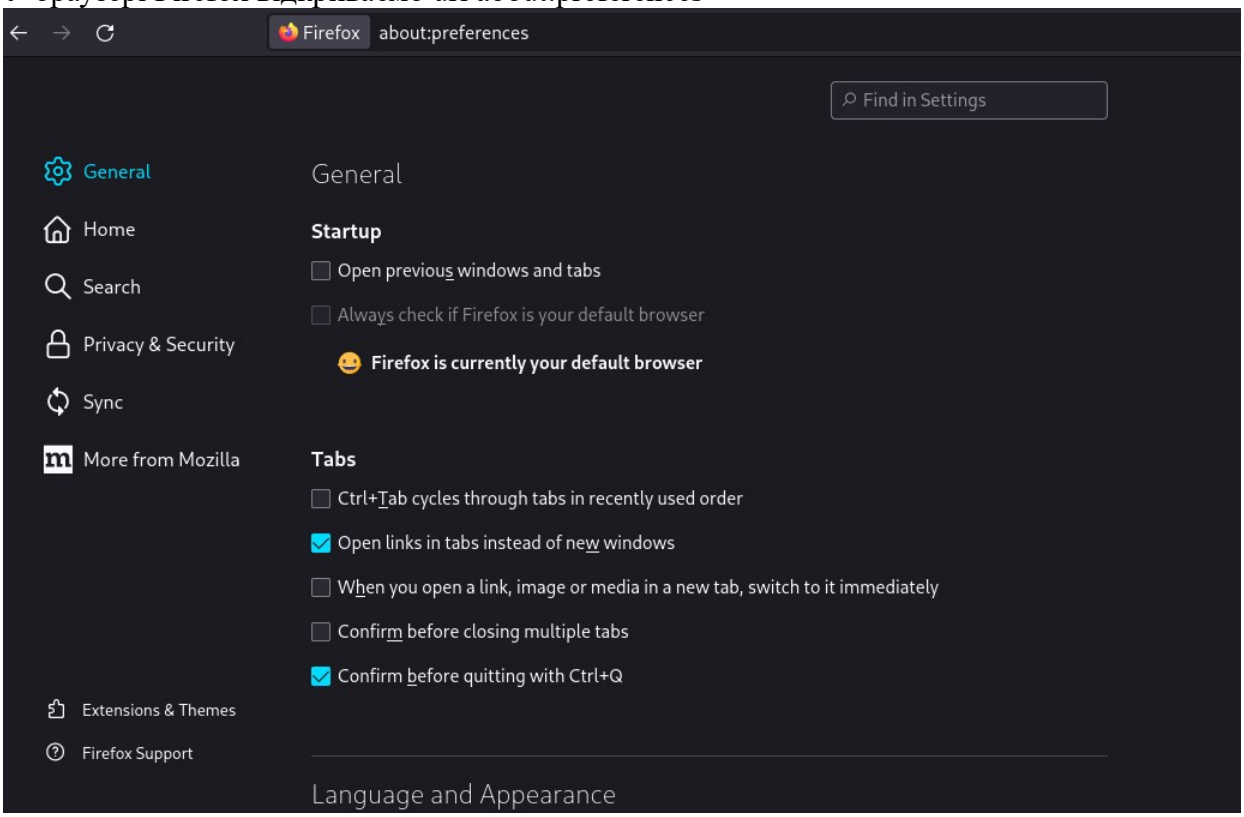
Тема. Основні ознаки присутності шкідливих програм.
Мета.

1. Дослідити явні прояви вірусної активності на прикладі несанкціонованого зміни налаштувань браузера
2. Ознайомитися з основним методом дослідження запущених процесів, а саме отримати навички роботи з Диспетчером завдань Windows, і вивчити його стандартний набір
3. Вивчити елементи операційної системи, що відповідають за автозапуск програм при її завантаженні
4. Вивчити і проаналізувати мережеву активність можна за допомогою вбудованих в операційну систему інструментів або ж скориставшись спеціальними окремо встановлюються додатками

Лабораторна робота виконана на ОС linux тому використане ПЗ відрізняється від наведеного в методичних вказівках, але хід роботи збережено.

Вивчення налаштувань браузера

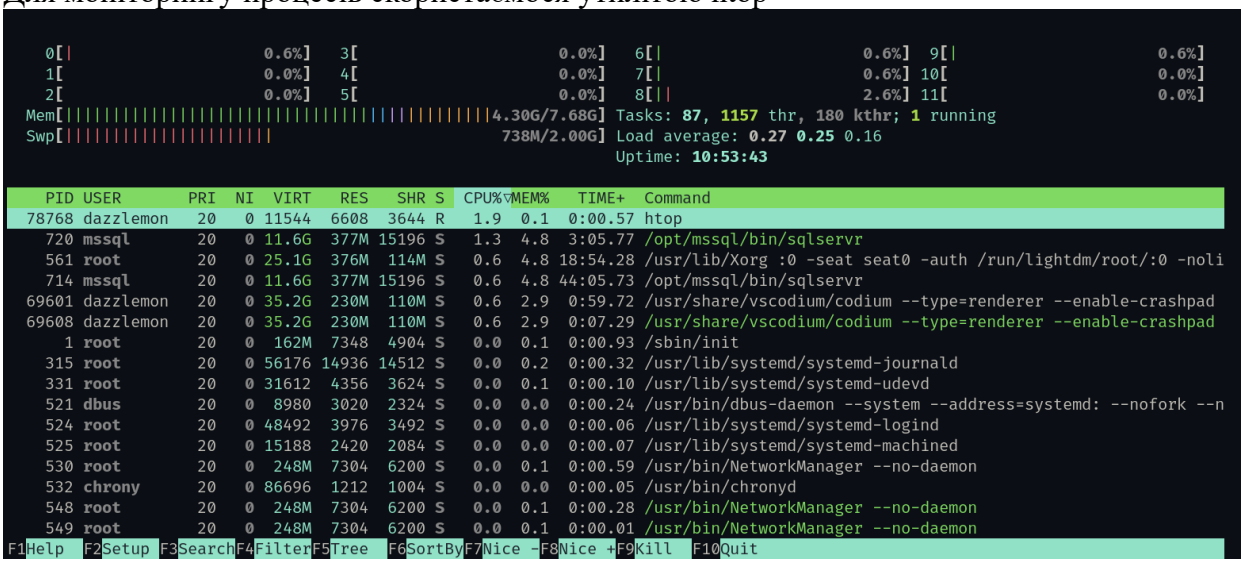
1. У браузері Firefox відкриваємо url about:preferences



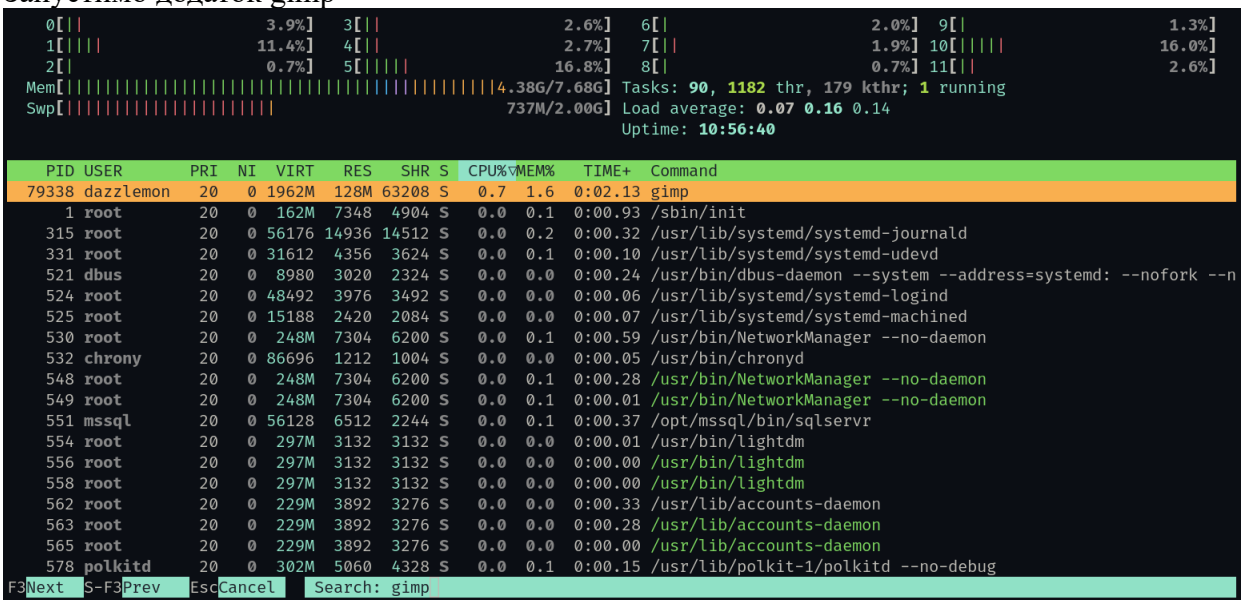
2. В рядку пошуку пишемо new tab
3. В налаштуванні Homepage and new windows обираємо Custom URLs... та вводимо наприклад speedtest.net — при відкриті нового вікна браузера відкриється ця сторінка.

Дослідження підозрілих процесів

1. Для моніторингу процесів скористаємося утилітою htop



2. Запустимо додаток gimp



3. На зараз не існує стандартного способу подивитись графік навантаження але можна приблизно побачити рівень стабільності за допомогою Load average.
На попередньому скринщоті він показує шо процесор завантажений на 7, 16 та 14 відсотків за 1, 5 та 15 останніх хвилин відповідно.

Вивчення елементів автозавантаження

Існує декілька варіантів:

- При ввімкнені комп’ютера — systemd — щоб подивитись активні сервіси треба скористуватися командою systemctl

  Щоб подивитись ввімкнені - systemctl list-unit-files | grep enabled
- При початку користувацької сесії — systemd/User — те саме шо й попередній пункт тільки з прапором --user
- При початку термінальної сесії — треба додати команди в скрипт /etc/profile або додати окремі скрипти до /etc/profile.d/
- При початку графічної сесії X11 - достатньо додати виклик команди до файлу ~/.xprofile або ~/.xinitrc.
- Для запуску графічних додатків треба налаштувати віконний менеджер xmonad - ~/.xmonad/xmonad.hs.

Мережева активність

Для моніторингу мережевого трафіку можна скористатися nethogs