

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ



**УДУНТ ННІ ДІТ**

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.

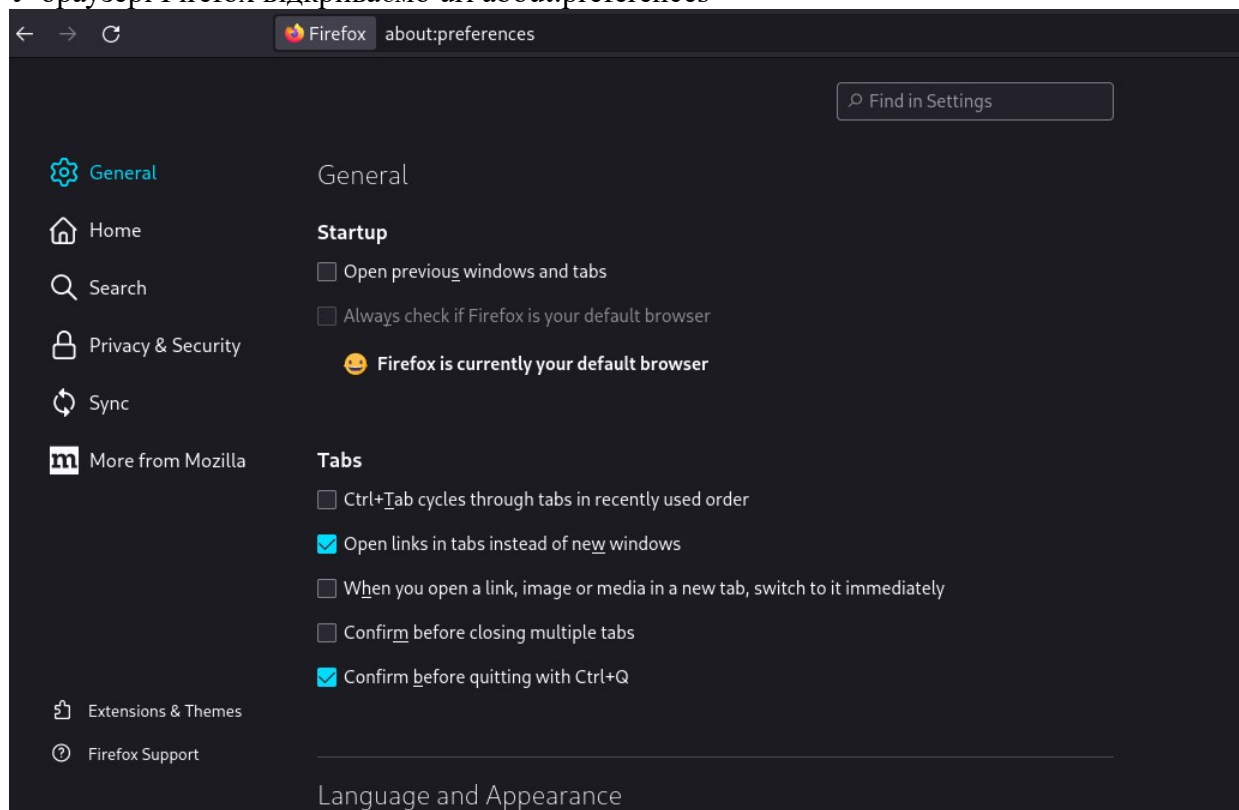
**Мета.**

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 відкритті нового вікна браузера відкриється ця сторінка.

## Дослідження підозрілих процесів

1. Для моніторингу процесів скористаємося утилітою htop

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
78768	dazzlemon	20	0	11544	6608	3644	R	1.9	0.1	0:00.57	htop
720	mssql	20	0	11.6G	377M	15196	S	1.3	4.8	3:05.77	/opt/mssql/bin/sqlservr
561	root	20	0	25.1G	376M	114M	S	0.6	4.8	18:54.28	/usr/lib/Xorg :0 -seat seat0 -auth /run/lightdm/root/:0 -noli
714	mssql	20	0	11.6G	377M	15196	S	0.6	4.8	44:05.73	/opt/mssql/bin/sqlservr
69601	dazzlemon	20	0	35.2G	230M	110M	S	0.6	2.9	0:59.72	/usr/share/vscodium/codium --type=renderer --enable-crashpad
69608	dazzlemon	20	0	35.2G	230M	110M	S	0.6	2.9	0:07.29	/usr/share/vscodium/codium --type=renderer --enable-crashpad
1	root	20	0	162M	7348	4904	S	0.0	0.1	0:00.93	/sbin/init
315	root	20	0	56176	14936	14512	S	0.0	0.2	0:00.32	/usr/lib/systemd/systemd-journald
331	root	20	0	31612	4356	3624	S	0.0	0.1	0:00.10	/usr/lib/systemd/systemd-udev
521	dbus	20	0	8980	3020	2324	S	0.0	0.0	0:00.24	/usr/bin/dbus-daemon --system --address=systemd: --nofork --n
524	root	20	0	48492	3976	3492	S	0.0	0.0	0:00.06	/usr/lib/systemd/systemd-logind
525	root	20	0	15188	2420	2084	S	0.0	0.0	0:00.07	/usr/lib/systemd/systemd-machined
530	root	20	0	248M	7304	6200	S	0.0	0.1	0:00.59	/usr/bin/NetworkManager --no-daemon
532	chrony	20	0	86696	1212	1004	S	0.0	0.0	0:00.05	/usr/bin/chronyd
548	root	20	0	248M	7304	6200	S	0.0	0.1	0:00.28	/usr/bin/NetworkManager --no-daemon
549	root	20	0	248M	7304	6200	S	0.0	0.1	0:00.01	/usr/bin/NetworkManager --no-daemon

2. Запустимо додаток gimp

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
79338	dazzlemon	20	0	1962M	128M	63208	S	0.7	1.6	0:02.13	gimp
1	root	20	0	162M	7348	4904	S	0.0	0.1	0:00.93	/sbin/init
315	root	20	0	56176	14936	14512	S	0.0	0.2	0:00.32	/usr/lib/systemd/systemd-journald
331	root	20	0	31612	4356	3624	S	0.0	0.1	0:00.10	/usr/lib/systemd/systemd-udev
521	dbus	20	0	8980	3020	2324	S	0.0	0.0	0:00.24	/usr/bin/dbus-daemon --system --address=systemd: --nofork --n
524	root	20	0	48492	3976	3492	S	0.0	0.0	0:00.06	/usr/lib/systemd/systemd-logind
525	root	20	0	15188	2420	2084	S	0.0	0.0	0:00.07	/usr/lib/systemd/systemd-machined
530	root	20	0	248M	7304	6200	S	0.0	0.1	0:00.59	/usr/bin/NetworkManager --no-daemon
532	chrony	20	0	86696	1212	1004	S	0.0	0.0	0:00.05	/usr/bin/chronyd
548	root	20	0	248M	7304	6200	S	0.0	0.1	0:00.28	/usr/bin/NetworkManager --no-daemon
549	root	20	0	248M	7304	6200	S	0.0	0.1	0:00.01	/usr/bin/NetworkManager --no-daemon
551	mssql	20	0	56128	6512	2244	S	0.0	0.1	0:00.37	/opt/mssql/bin/sqlservr
554	root	20	0	297M	3132	3132	S	0.0	0.0	0:00.01	/usr/bin/lightdm
556	root	20	0	297M	3132	3132	S	0.0	0.0	0:00.00	/usr/bin/lightdm
558	root	20	0	297M	3132	3132	S	0.0	0.0	0:00.00	/usr/bin/lightdm
562	root	20	0	229M	3892	3276	S	0.0	0.0	0:00.33	/usr/lib/accounts-daemon
563	root	20	0	229M	3892	3276	S	0.0	0.0	0:00.28	/usr/lib/accounts-daemon
565	root	20	0	229M	3892	3276	S	0.0	0.0	0:00.00	/usr/lib/accounts-daemon
578	polkitd	20	0	302M	5060	4328	S	0.0	0.1	0:00.15	/usr/lib/polkit-1/polkitd --no-debug

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

## Вивчення елементів автозавантаження

Існує декілька варіантів:

- При ввімкненні комп'ютера — `systemd` — щоб подивитись активні сервіси треба скористуватися командою `systemctl`

UNIT	LOAD	ACTIVE
proc-sys-fs-binfmt_misc.automount	loaded	active
sys-devices-pci0000:00-0000:00:01.1-0000:01:00.0-nvme-nvme0-nvme0n1-nvme0n1p1.device	loaded	active
sys-devices-pci0000:00-0000:00:01.1-0000:01:00.0-nvme-nvme0-nvme0n1-nvme0n1p2.device	loaded	active
sys-devices-pci0000:00-0000:00:01.1-0000:01:00.0-nvme-nvme0-nvme0n1-nvme0n1p3.device	loaded	active
sys-devices-pci0000:00-0000:00:01.1-0000:01:00.0-nvme-nvme0-nvme0n1-nvme0n1p4.device	loaded	active
sys-devices-pci0000:00-0000:00:01.1-0000:01:00.0-nvme-nvme0-nvme0n1-nvme0n1p5.device	loaded	active
sys-devices-pci0000:00-0000:00:01.1-0000:01:00.0-nvme-nvme0-nvme0n1-nvme0n1p6.device	loaded	active
sys-devices-pci0000:00-0000:00:01.1-0000:01:00.0-nvme-nvme0-nvme0n1-nvme0n1p7.device	loaded	active
sys-devices-pci0000:00-0000:00:01.1-0000:01:00.0-nvme-nvme0-nvme0n1.device	loaded	active
sys-devices-pci0000:00-0000:00:01.2-0000:02:00.0-usb1-1\x2d9-1\x2d9:1.0-bluetooth-hci0.device	loaded	active
sys-devices-pci0000:00-0000:00:01.2-0000:02:00.1-ata1-host0-target0:0:0-0:0:0-block-sda-sda1.device	loaded	active
sys-devices-pci0000:00-0000:00:01.2-0000:02:00.1-ata1-host0-target0:0:0-0:0:0-block-sda.device	loaded	active
sys-devices-pci0000:00-0000:00:01.2-0000:02:00.2-0000:03:08.0-0000:29:00.0-net-wlo1.device	loaded	active
sys-devices-pci0000:00-0000:00:01.2-0000:02:00.2-0000:03:09.0-0000:2a:00.0-net-enp42s0.device	loaded	active
sys-devices-pci0000:00-0000:00:03.1-0000:2b:00.1-sound-card0-controlC0.device	loaded	active
sys-devices-pci0000:00-0000:00:08.1-0000:2d:00.3-usb3-3\x2d1-3\x2d1.1-3\x2d1.1:1.0-sound-card2-controlC2.device	loaded	active
sys-devices-pci0000:00-0000:00:08.1-0000:2d:00.3-usb3-3\x2d1-3\x2d1.4-3\x2d1.4:1.0-sound-card3-controlC3.device	loaded	active

lines 1-18

Щоб подивитись ввімкнені - `systemctl list-unit-files | grep enabled`

- При початку користувацької сесії — `systemd/User` — те саме що 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](#)

NetHogs version 0.8.7					
PID	USER	PROGRAM	DEV	SENT	RECEIVED
1046	dazzle..	/usr/lib/firefox/firefox	enp42s	1.059	2.107 KB/sec
6916	dazzle..	/opt/discord/Discord --type=utility --utility-sub-type=network.mojom.Ne..	enp42s	0.355	1.112 KB/sec
?	root	unknown TCP		0.000	0.000 KB/sec
TOTAL				1.414	3.219 KB/sec