МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

ІМЕНИ СЕМЕНА КУЗНЕЦЯ

Лабораторна робота №7

## Тема: «Аналіз вразливостей в сучасних операційних системах»

з дисципліни «Основи побудови та захисту сучасних операційних систем»

Виконав:

Студент групи 6.04.125.010.21.2

факультету Інформаційних технологій

спеціальності 125

П.І.П. Бойко В.В.

Перевірив:

Леуненко О.В.

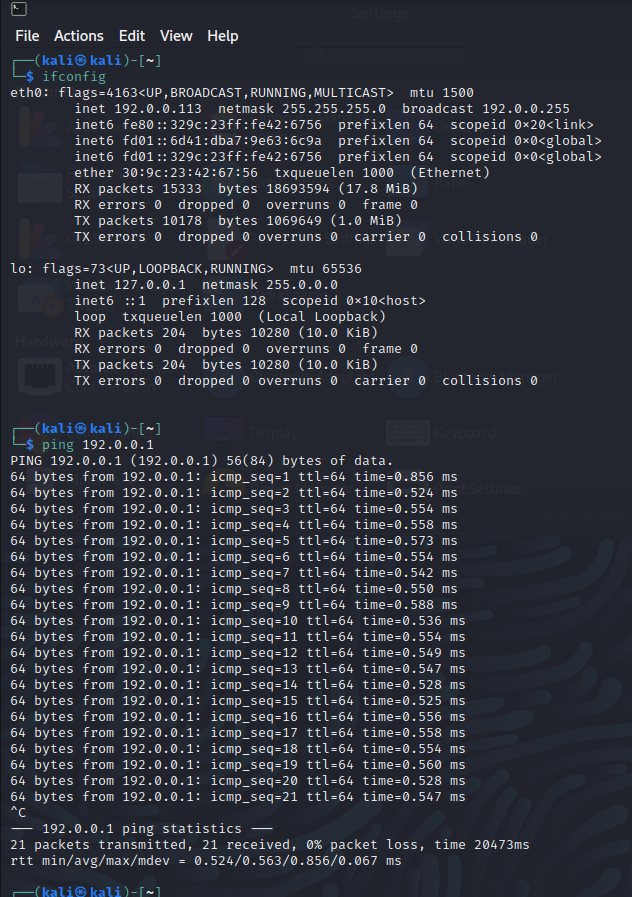
Харків – 2022

Мета і завдання: вивчення механізмів акивного збору інформації про мережу

Хід роботи

1. Вивчення засобів для перевірки доступності вузла

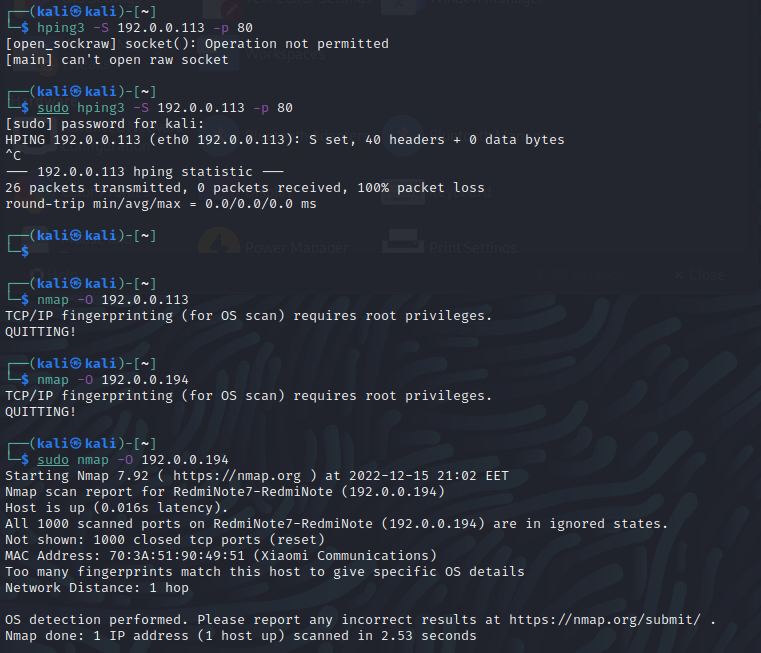
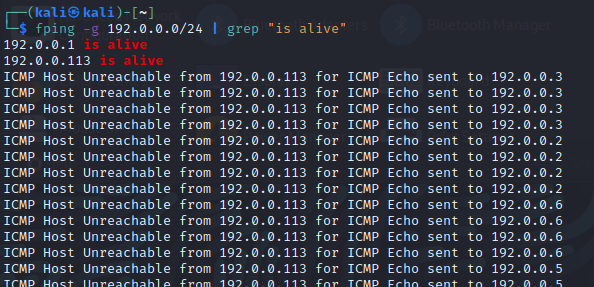
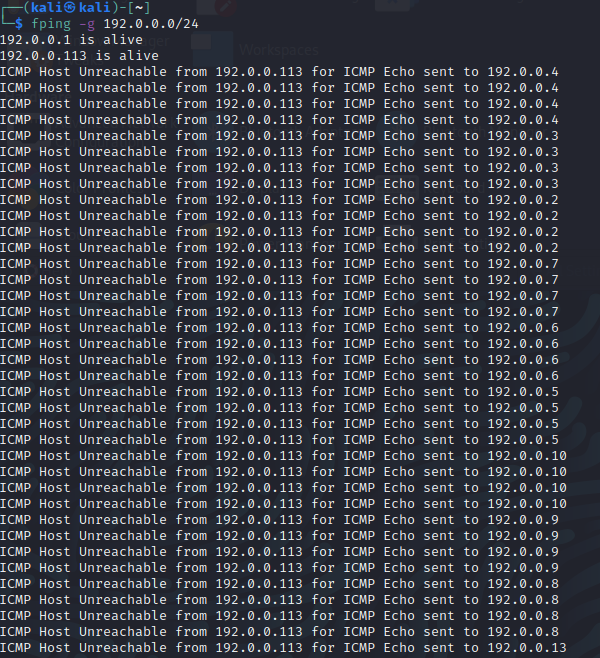
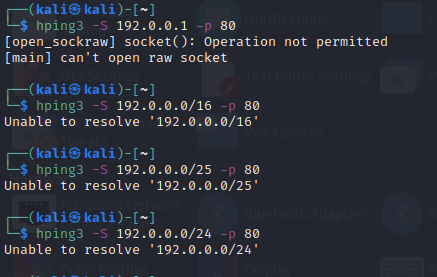
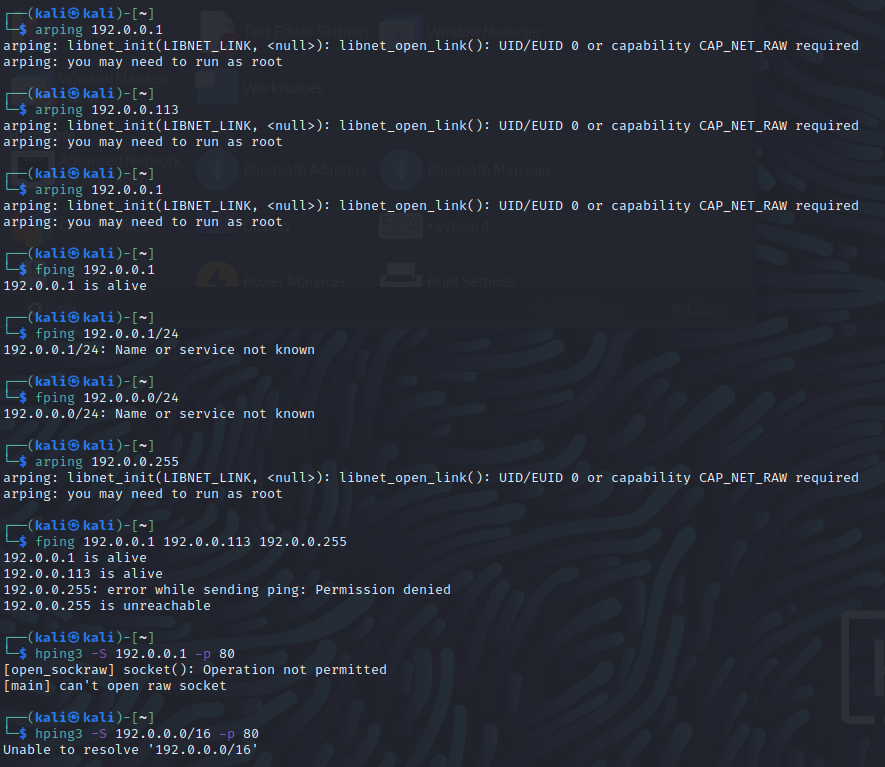
Для визначення ip адреси ввожу команду «ifconfig»



Та для перевірки статусу вузла ввожу команду «ping та адреса вузла»

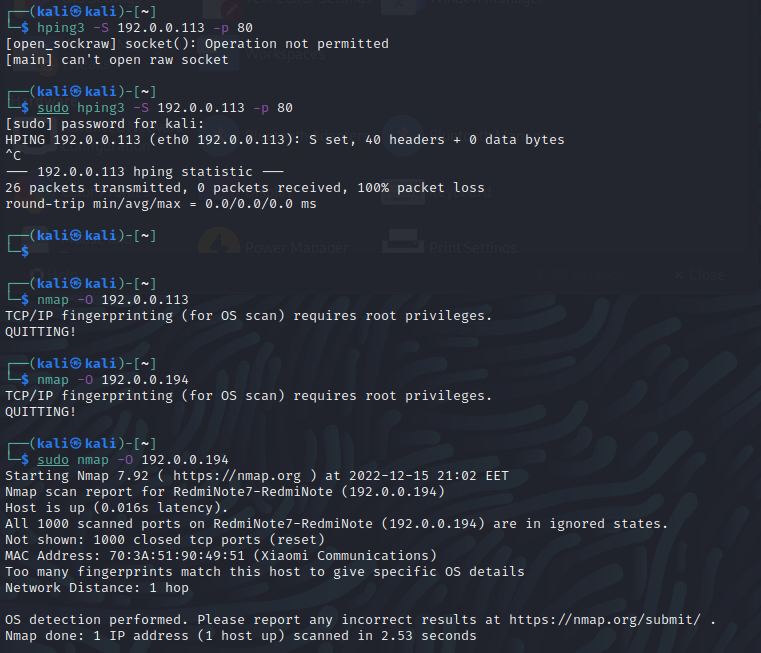
Як результат бачу, що 21 пакет було відправлено, та 21 отримано, отже вузол працює

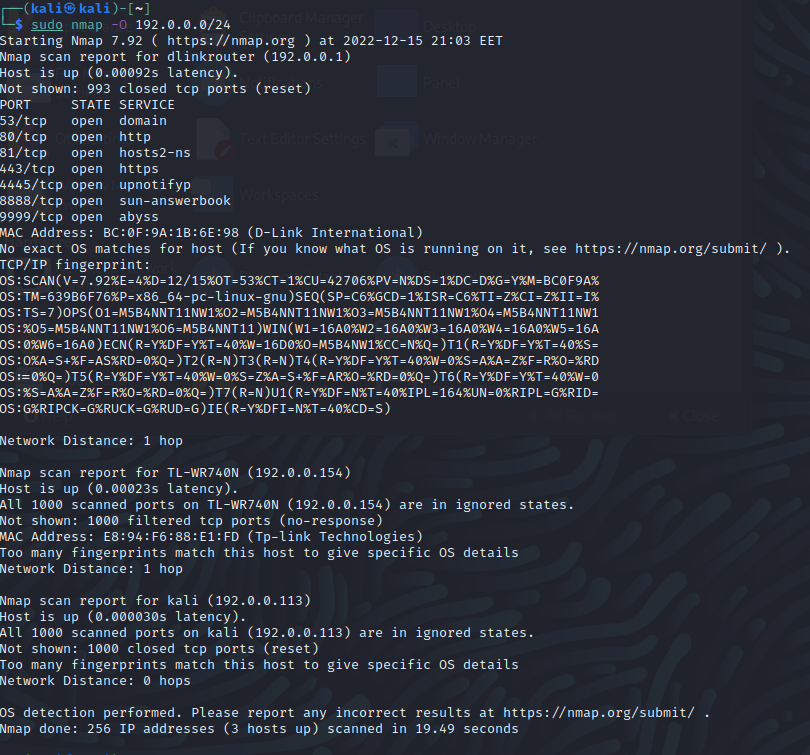
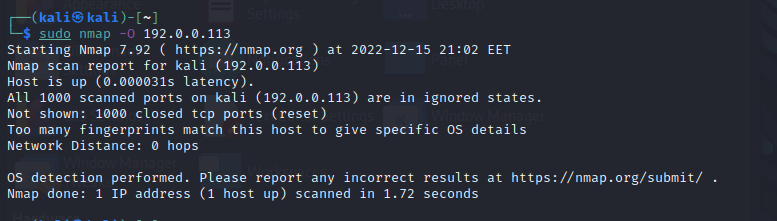
Завдяки «arping» перевіряю вузол завдяки протоколу ARP  
Завдяки «fping» перевіряю доступність декількох вузлів  
Завдяки «hping3» - утіліта для генерації та аналізу пакеів



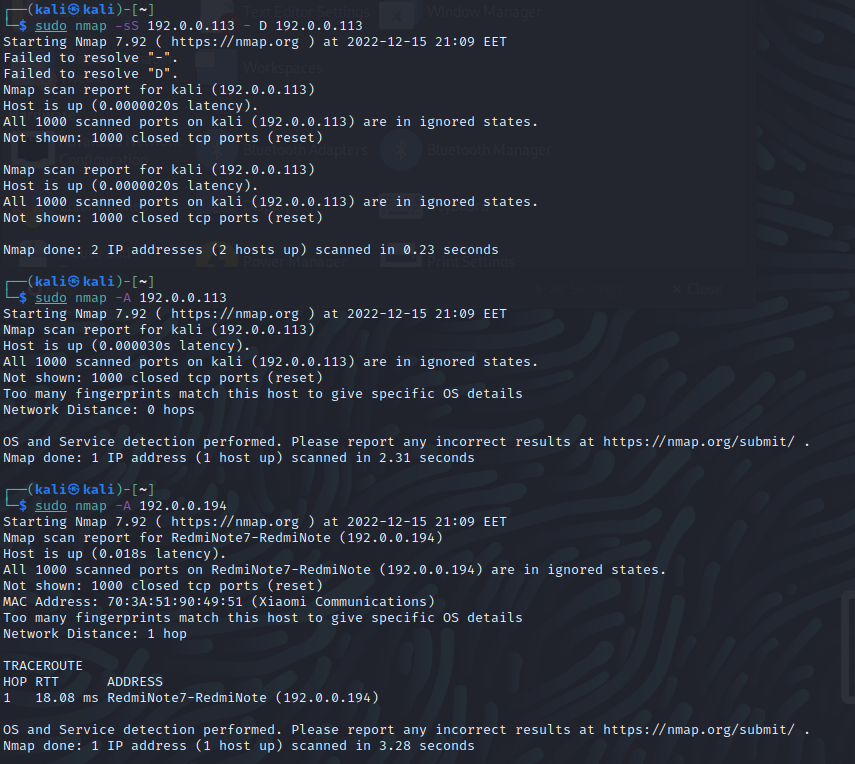
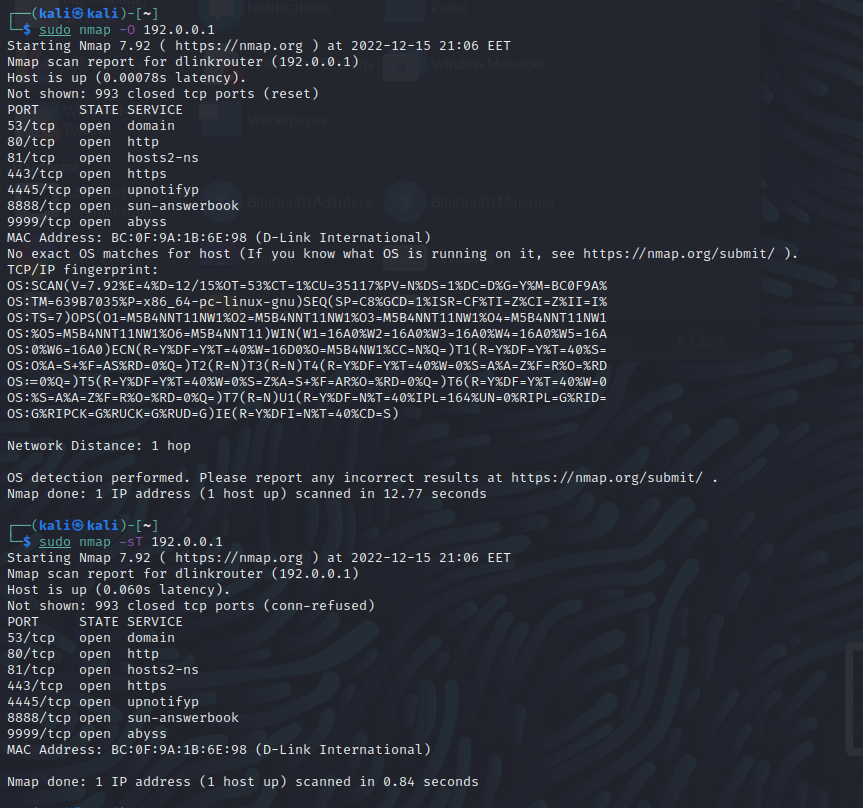
2. Визначення засобів для визначення ОС

«nmap»

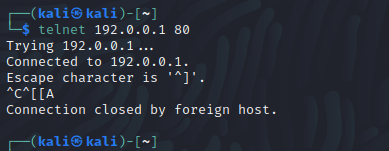




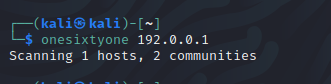
3. Сканування портів



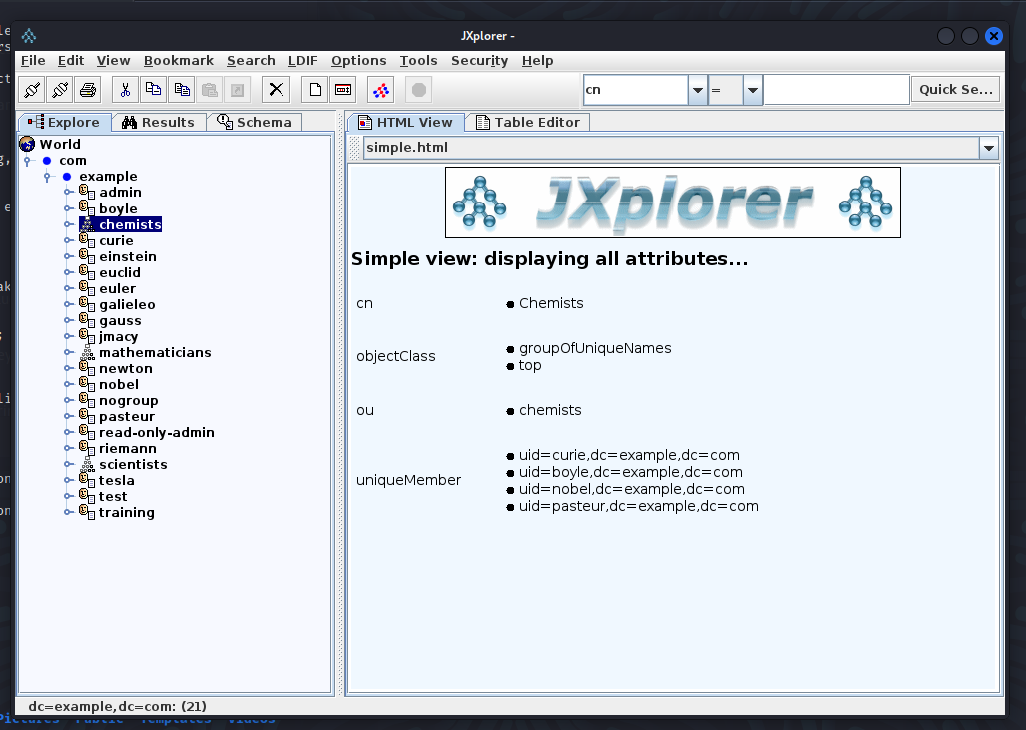
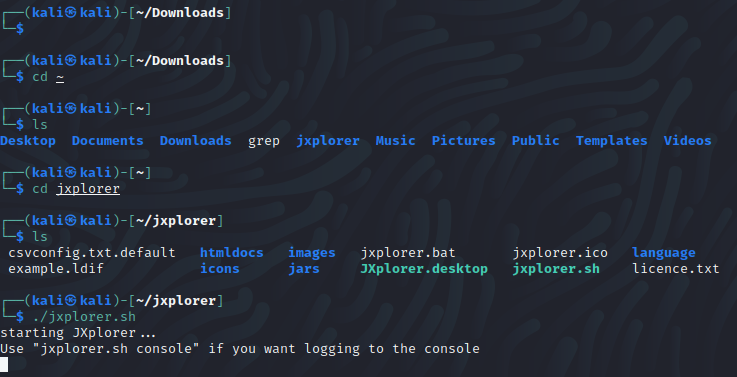
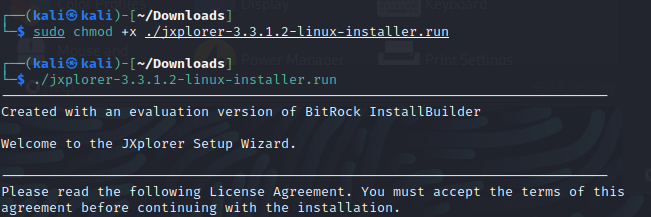
4. Перехоплення банерів



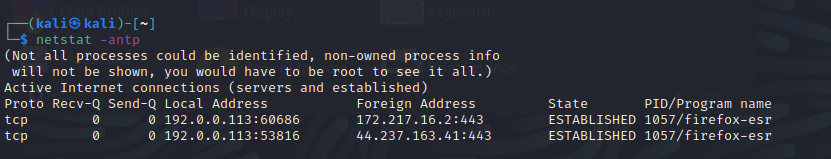
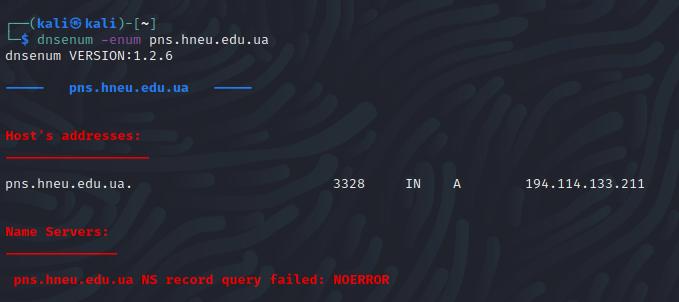
6. Отримання інформації з NetBIOS



7. Отримання інформації з LDAP



9. Отримання інформаціїїз DNS



Контрольні питання

1. ping and ip of point
2. p0f nmap nbtscan
3. actually nmap using for analizing open ports, network, OS type
4. zenmap is GUI nmap
5. talnet <ip>
6. nbtscan утиліта для пошуку NetBIOS імен. Вона відправляє запити до кожного вузла з IP-адресами у заданному діапазоні
   1. SNMP
      1. Onesixtyone
      2. snmp-check
      3. nmap
   2. LDAP
      1. JXplorer
      2. Ldapsearch
      3. Nmap
   3. SMTP
      1. smtp-user-enum
      2. nmap
   4. DNS
      1. Dnsenum
      2. Dnsrecon
      3. Nmap
7. nmap, openvas