Network threats, assessments, and defense

Twinkle Akhilesh Mishra

StudentId:8894858

Conestoga College

INFO8965: Computer and Network Security

Conestoga College

Course	INFO8965: Computer and Network Security
Activity	Network threats, assessments, and defense
Student Name	Twinkle Akhilesh Mishra
Date performed	04-March-2025

Objectives

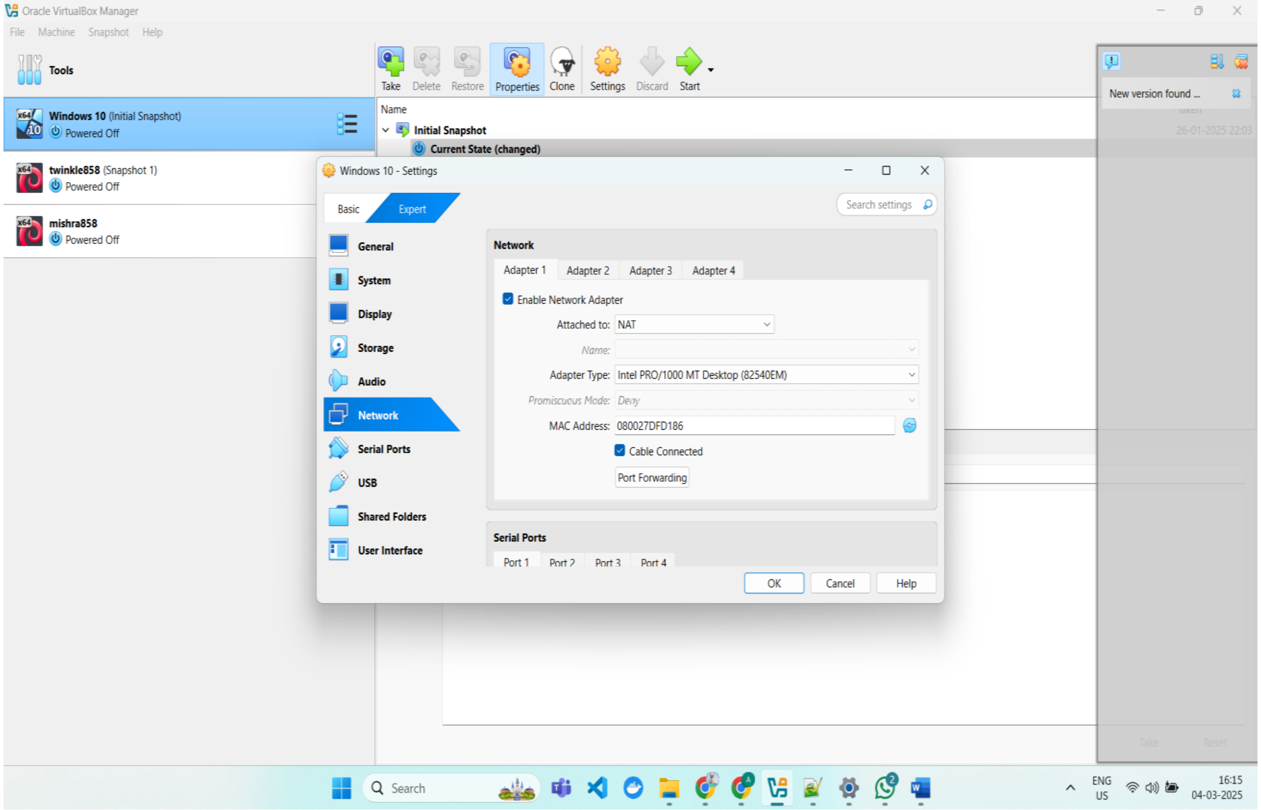
- Understand DNS poisoning and its implications
- Use nmap for port scanning

Resources

- Hardware: PC/Laptop
- Software: VirtualBox, Kali Linux VM, Windows 10/11 VM

(A) DNS Poisoning

- **Setting Up the Network Adapter in VirtualBox**
  - Open VirtualBox.
  - Right-click on the Windows 10 VM and select Settings.
  - Navigate to Network settings.
  - Choose one of the following options:
    - NAT (Network Address Translation) Mode (Recommended):
      - Allows the VM to access the internet.
      - Restricts external visibility of the VM.
      - Functions like a physical device connected to the internet via a router.
      - Prevents communication between virtual machines for security.
    - Bridged Adapter Mode (Alternative Option):
      - Allows the VM to directly connect to the host network.
      - VM gets its own IP address, making it accessible within the network.
- Understanding NAT Mode
  - NAT Mode is the default network setting in VirtualBox.
  - It enables internet access for the guest OS (VM) while keeping it hidden from external networks.
  - Works similarly to a router, with VirtualBox acting as an intermediary.
  - Enhances security by isolating VMs from each other.
  - Limitation: The VM is not directly accessible from external devices.



Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter

Attached to: NAT

Name:

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

MAC Address: 080027DFD186

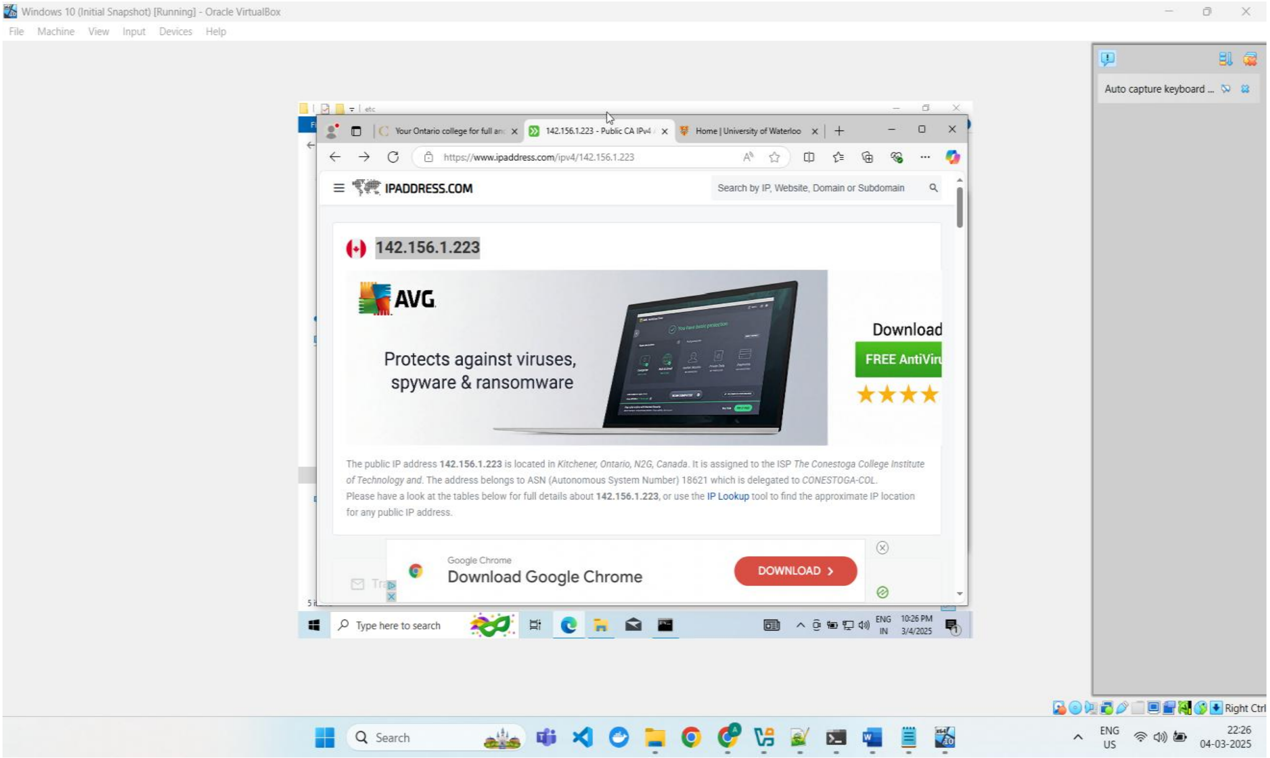
☑ Cable Connected

Port Forwarding

Serial Ports

Port 1 | Port 2 | Port 3 | Port 4

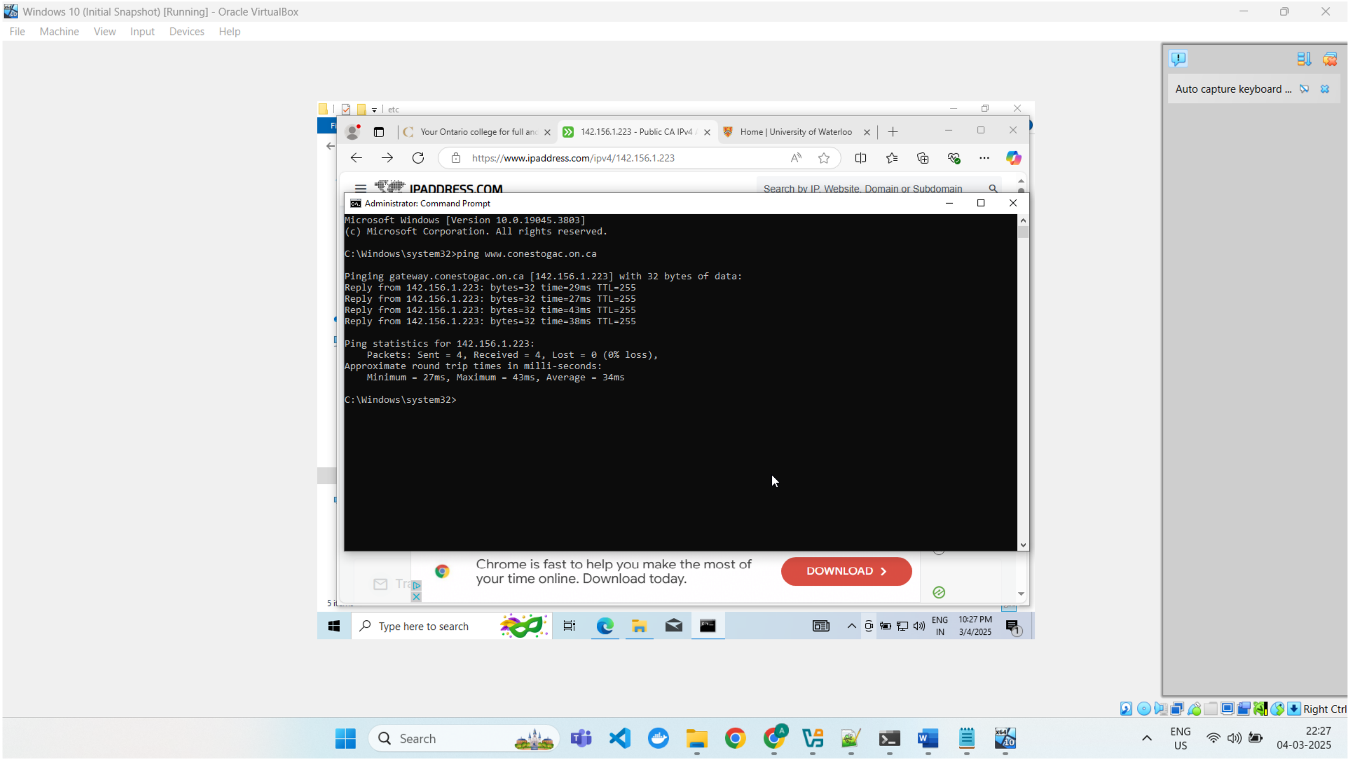
- **Find IP Address**:
  - **Visit the Target Website**:
    - Open a web browser inside the Virtual Machine (VM).
    - Navigate to **www.conestogac.on.ca**
  - **Use the Command Prompt to Find the IP Address**:
    - Open Command Prompt (cmd) as an Administrator.
    - Type the following command and press Enter:
      ping www.conestogac.on.ca -4
    - The output will display the IPv4 address of the website, which in this case is **142.156.1.223**
  - **Verify Using an Online Lookup Tool** (Alternative Method):
    - Open a web browser in the VM and go to www.ipaddress.com/ip-lookup.
    - Enter **www.conestogac.on.ca** in the search bar.
    - The website will display the corresponding IP address (**142.156.1.223**) along with additional details.

- 

Windows 10 (Initial Snapshot) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Your Ontario college for full an
142.156.1.223 - Public CA IPv4
Home | University of Waterloo
https://www.ipaddress.com/ipv4/142.156.1.223
IPADDRESS.COM
Search by IP, Website, Domain or Subdomain
Auto capture keyboard ...
Type here to search
10:26 PM
3/4/2025
Search
22:26
04-03-2025
Right Ctrl

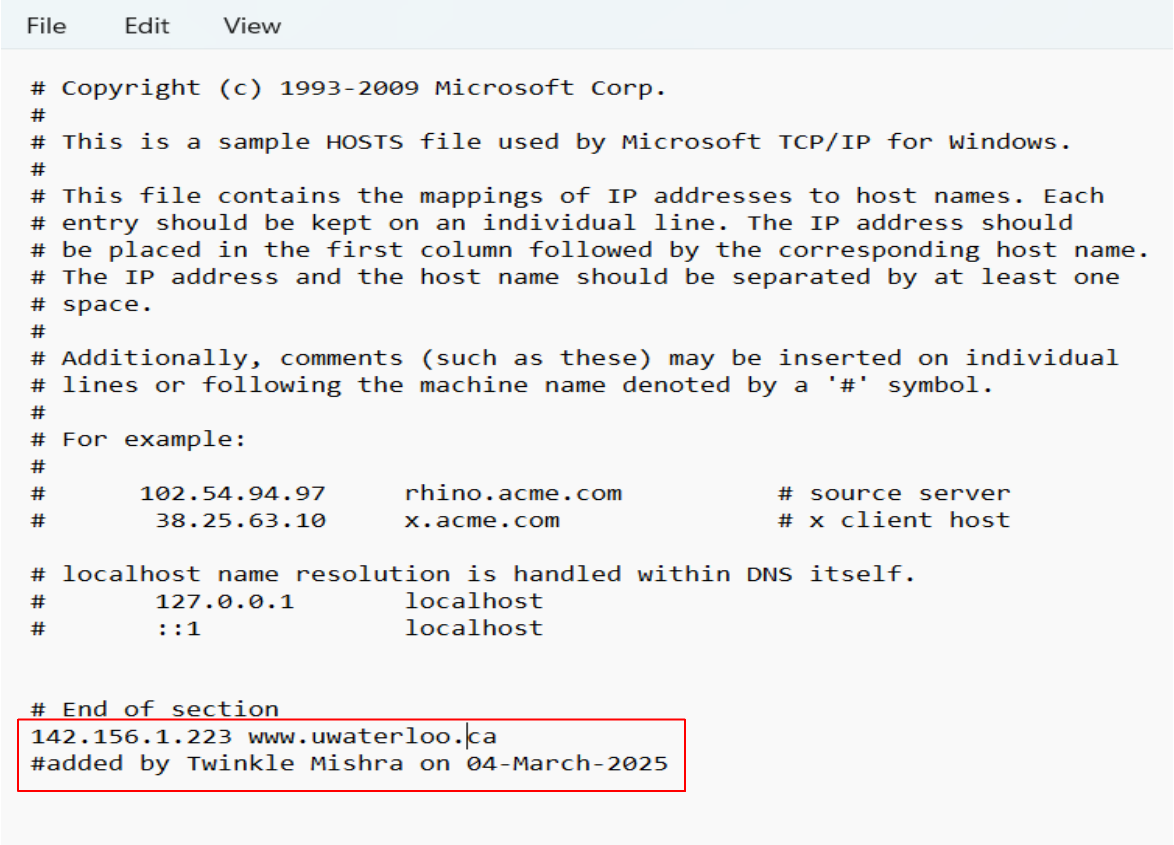
142.156.1.223

The public IP address **142.156.1.223** is located in *Kitchener, Ontario, N2G, Canada*. It is assigned to the ISP *The Conestoga College Institute of Technology and*. The address belongs to ASN (Autonomous System Number) 18621 which is delegated to *CONESTOGA-COL*. Please have a look at the tables below for full details about **142.156.1.223**, or use the IP Lookup tool to find the approximate IP location for any public IP address.


Windows 10 (Initial Snapshot) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Your Ontario college for full and
142.156.1.223 - Public CA IPv4
Home | University of Waterloo
https://www.ipaddress.com/ipv4/142.156.1.223
IPADDRESS.COM
Search by IP, Website, Domain or Subdomain
Administrator: Command Prompt
Chrome is fast to help you make the most of your time online. Download today.
DOWNLOAD
Type here to search
Auto capture keyboard ...
Right Ctrl
Search
ENG IN 10:27 PM 3/4/2025
ENG US 22:27 04-03-2025

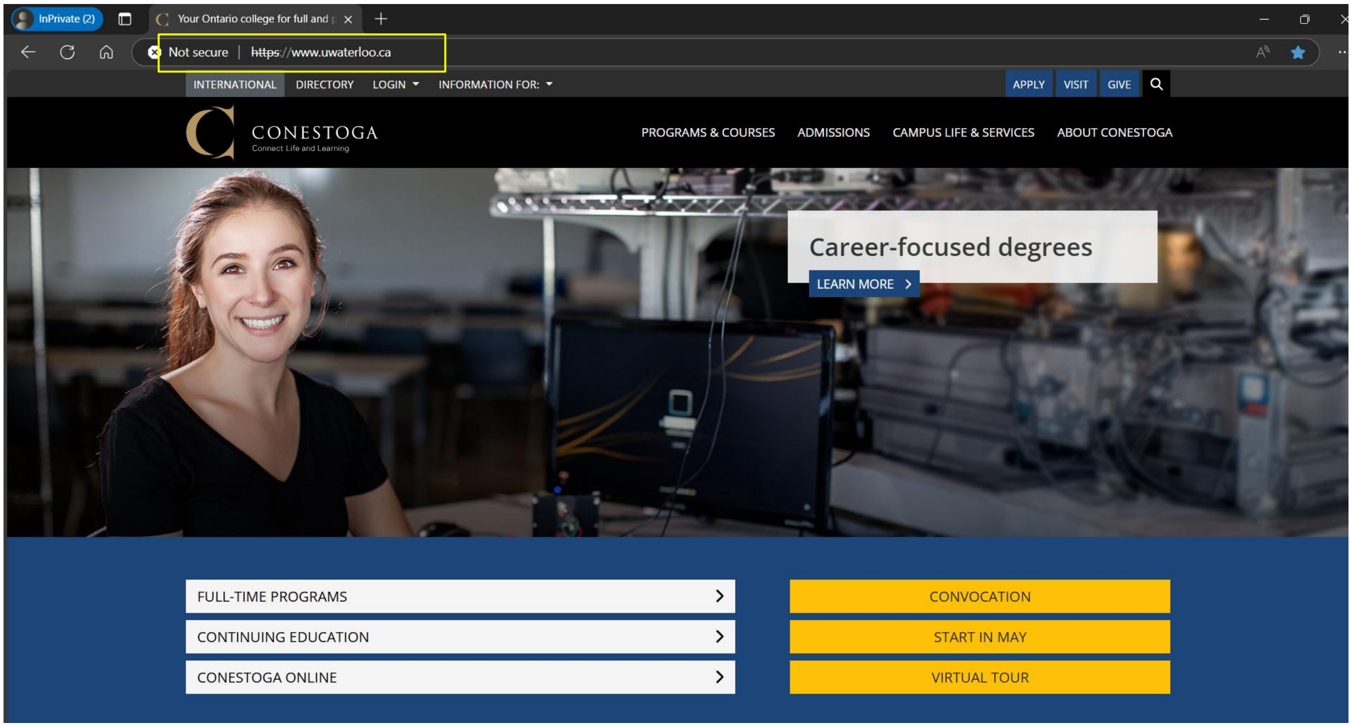
```
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping www.conestogac.on.ca

Pinging gateway.conestogac.on.ca [142.156.1.223] with 32 bytes of data:
Reply from 142.156.1.223: bytes=32 time=29ms TTL=255
Reply from 142.156.1.223: bytes=32 time=27ms TTL=255
Reply from 142.156.1.223: bytes=32 time=43ms TTL=255
Reply from 142.156.1.223: bytes=32 time=38ms TTL=255

Ping statistics for 142.156.1.223:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 27ms, Maximum = 43ms, Average = 34ms

C:\Windows\system32>
```

1. **Edit Hosts file**:
   Open Notepad as Administrator, go to C:\Windows\System32\drivers\etc\hosts. Add a new entry with the IP address from step 2, followed by www.conestogac.on.ca. Add a comment with your name and the date. Save the file and capture a screenshot of these changes as part of **Output #1** (2 Marks).



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost


# End of section
142.156.1.223 www.uwaterloo.ca
#added by Twinkle Mishra on 04-March-2025
```

2. **Verify DNS Poisoning:** Open Internet Explorer and visit www.conestogac.on.ca. Note which website appears? Explain your observation and its reason(s) in **Output #2** (2 Mark).



Not secure | ~~https~~://www.uwaterloo.ca

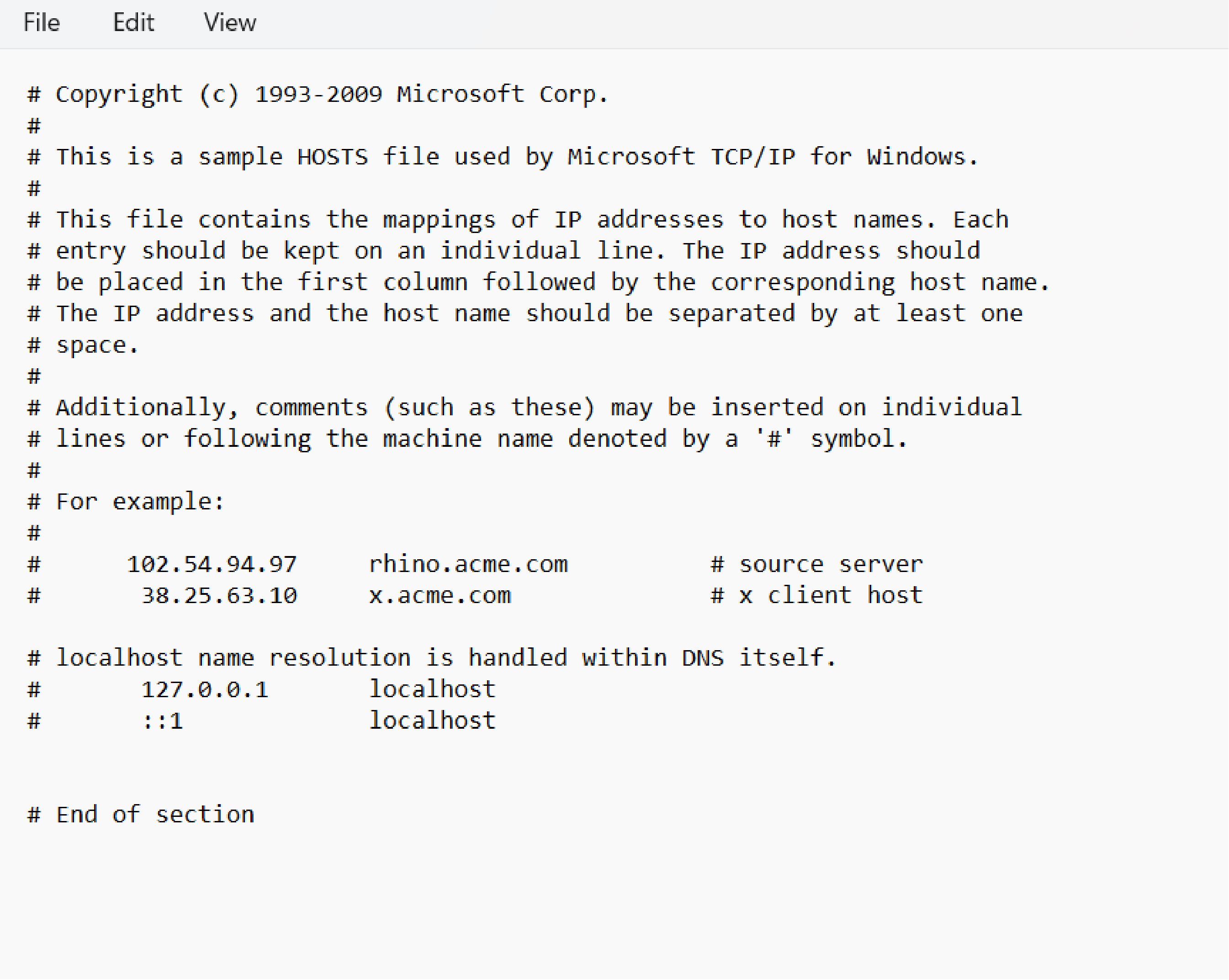
Explanation: The redirection of www.uwaterloo.ca to www.conestogac.on.ca occurs due to **DNS manipulation**, often caused by **hosts file modification** or **DNS cache poisoning**. In this case, the system resolves www.uwaterloo.ca to the IP address of Conestoga College's website instead of its actual server. This is a form of **DNS spoofing**, where attackers alter domain resolutions to mislead users. Such attacks can be used for **phishing**, misinformation, or unauthorized access. To prevent this, users should verify their hosts file, **flush DNS cache**, and use a trusted DNS server.

3. What is **zone transfer**? How is it used as an attack tool? Explain this in **Output # 3** [1 mark].

- The zone transfers as a way for one DNS server to share its list of domain names and IP addresses with another DNS server. This is usually done to keep backup servers updated and ensure everything runs smoothly online.
- How Can Hackers Take advantage of zone transfer?
  - If a DNS server is not set up correctly, the attackers can request a zone transfer and get access to all the internal DNS records. This gives them a map of the company's digital infrastructure also including subdomains, email servers, and other important network details.
- Why Is This Dangerous?
  - Hackers Get a Blueprint of the Network : They can see how everything is connected.
  - More Effective Phishing Scams : Attackers can target employees using real subdomains to make fake login pages look legit.
  - Easier Hacking Attempts : If they find an old or weak system in the DNS records, they can try to break in.

- How to Prevent This?
  - Restrict Zone Transfers – Only allow trusted servers to access DNS records.
  - Keep an Eye on DNS Logs – Watch for suspicious zone transfer requests.
  - Use a Firewall – Block unauthorized zone transfer attempts from outside your network.
- By securing DNS zone transfers, companies can prevent hackers from gathering valuable information and keep their systems safe.

4. Return to the hosts file and remove this entry. Click **`File`** and then click **`Save`**.



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost


# End of section
```

(B) Network reconnaissance and discovery tool

1. **Legality of Port Scanning**: Read the white paper, "The Ethics and Legality of Port Scanning." Summarize your understanding in **Output #4** [2 Marks].
   `"The Ethics and Legality of Port Scanning" by Shaun Jamieson, URL: https://sansorg.egnyte.com/dl/FcsG6IOGwU/? (Access Date: 02/10/2024)`

   Port scanning is a technique used to find open ports on a network, which helps identify potential security weaknesses. While it is useful for assessing vulnerabilities also it can be perceived as invasive and unauthorized if done without permission. The key ethical issue lies in the intent behind the scan—if the purpose is to explore a system without causing harm and it may be acceptable in certain cases. However, without proper consent, port scanning can break laws depending on the region and might even be seen as a precursor to a malicious attack.

2. Using nmap: Do internet research and find out about `nmap` tool of Linux Kali and http://scanme.nmap.org/. On Kali Linux, use `nmap` to scan for open ports `scanme.nmap.org`. Capture the output as
Output #5. Also, explain this output. [3 Marks].

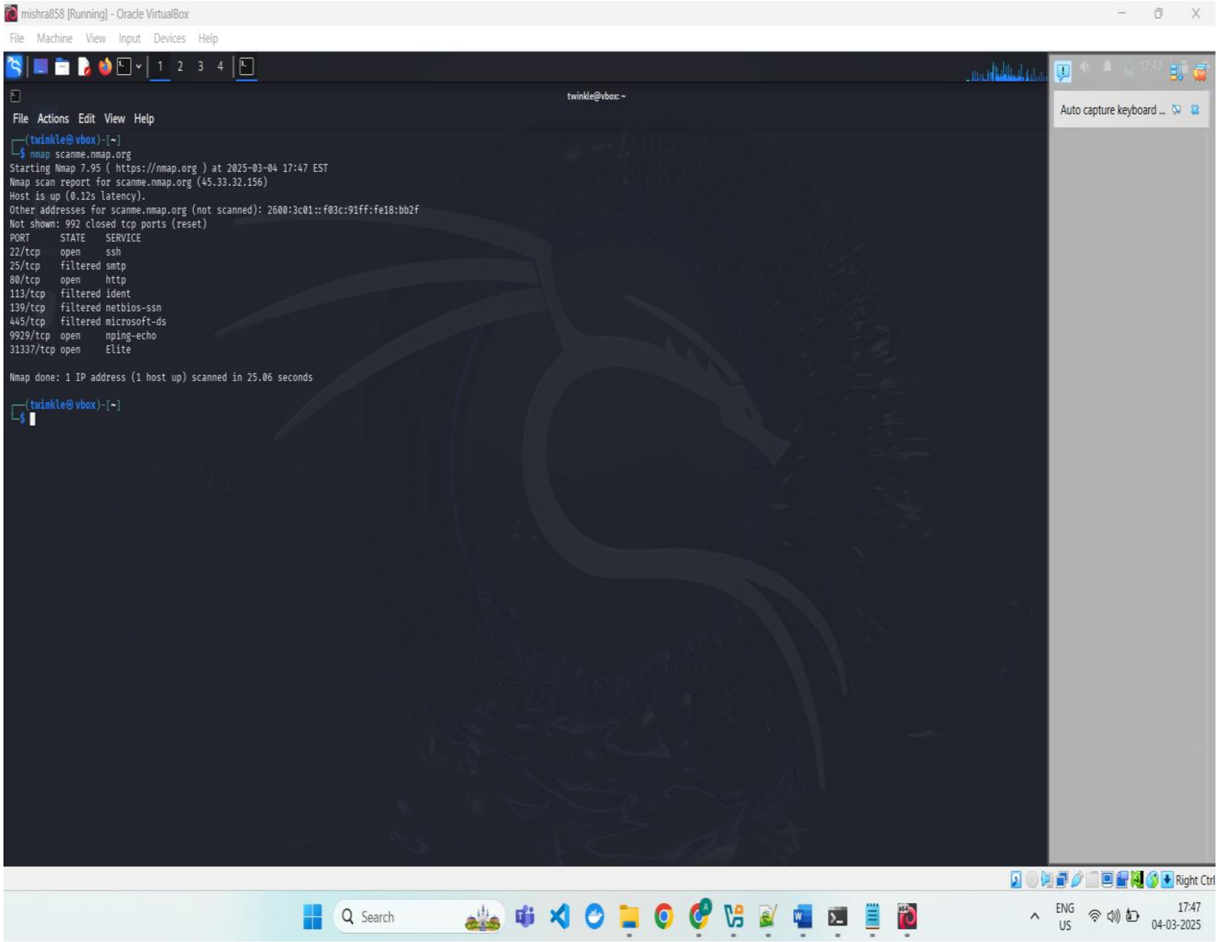
➢ **Nmap** (Network Mapper) is a powerful open-source tool used for network discovery and security auditing. It helps identify active hosts also open ports and running services on a network. Ethical hackers, system administrators and cybersecurity professionals use Nmap to analyze network security.

➢ What is scanme.nmap.org?

- **scanme.nmap.org** is a public test server provided by the Nmap project. It allows users to practice Nmap scanning legally without violating security policies.

➢ **Explanation of the Nmap Output:**

- **Scan Target:** The scan was performed on scanme.nmap.org (45.33.32.156).
- **Filtered and Open Ports:**
- **Ports marked as "filtered":** These ports are blocked by a firewall, meaning no response was received.
- **Ports marked as "open":** These services are actively running and can accept connections.
- **Notable Open Ports in the Scan:**
- **9929/tcp (nping-echo)** : Likely used for network testing.
- **31337/tcp (Elite)** : Traditionally associated with certain hacking tools but could also be used for legitimate applications.
- **Scan Duration**: The scan completed in **25.06** seconds, meaning the network responded efficiently.
- This scan provides insight into which services are accessible on scanme.nmap.org. The presence of filtered ports suggests security measures like firewalls are in place. Open ports indicate active services that could be potential attack vectors if not properly secured.



mishra858 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
twinkle@vbox: ~
File Actions Edit View Help
Auto capture keyboard ...
Right Ctrl
Search
ENG
US
17:47
04-03-2025

```
┌──(twinkle㉿vbox)-[~]
└─$ nmap scanme.nmap.org
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-04 17:47 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.12s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
113/tcp   filtered ident
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 25.06 seconds

┌──(twinkle㉿vbox)-[~]
└─$ 
```