DNS Poisoning

DNS poisoning, also known as DNS spoofing, involves tampering with the Domain Name System (DNS) information to redirect users to fraudulent websites. Here's a summary of the key points about DNS poisoning:

- Definition: DNS poisoning involves replacing legitimate DNS entries with fraudulent ones, effectively misdirecting users to malicious sites instead of their intended destinations.
- Method: This can be achieved by corrupting the DNS cache on individual client machines (like Windows PCs or MacBooks) or on DNS servers (such as a Windows DNS server).
- Purpose: Attackers use DNS poisoning to redirect users from legitimate websites to malicious ones for purposes such as stealing sensitive information, spreading malware, or conducting phishing attacks.
- Prevention: The primary method to prevent DNS poisoning is through DNSSEC (DNS Security Extensions), which adds a layer of security to the DNS lookup and response process although it is not deeply covered in some basic network security certifications like Network Plus.

Understanding and preventing DNS poisoning is crucial for maintaining the integrity of network communications and protecting users from cybersecurity threats.

ere's a comprehensive step-by-step guide on how to simulate DNS poisoning on a Windows 11 client using the hosts file:

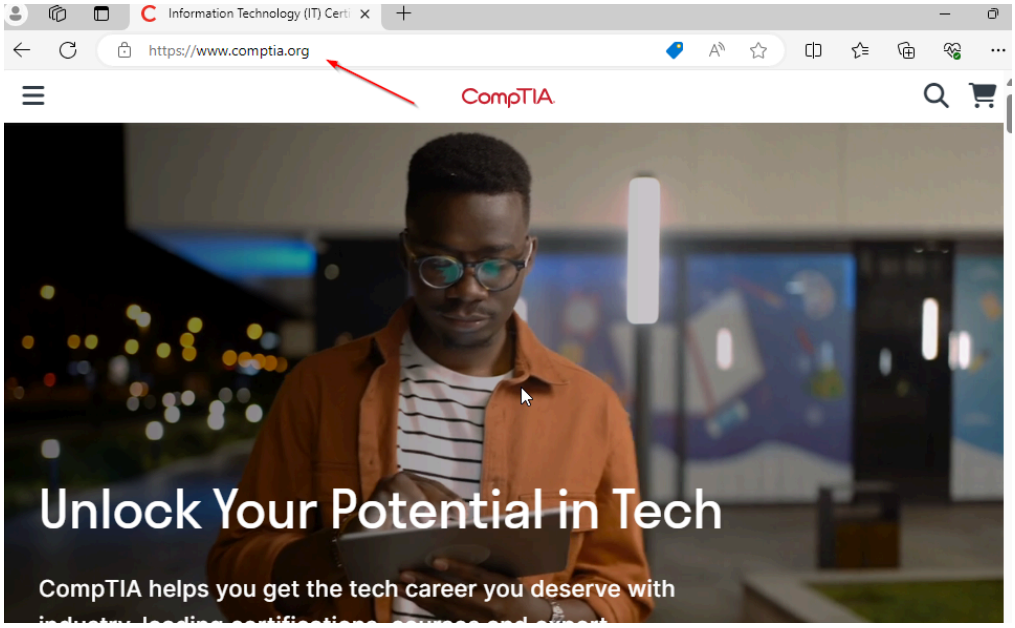
Equipment and Software Needed

- A computer running Windows 10/11
- Administrative privileges on the computer
- Notepad or any text editor with administrative privileges

Step 1: Verify Normal Website Access

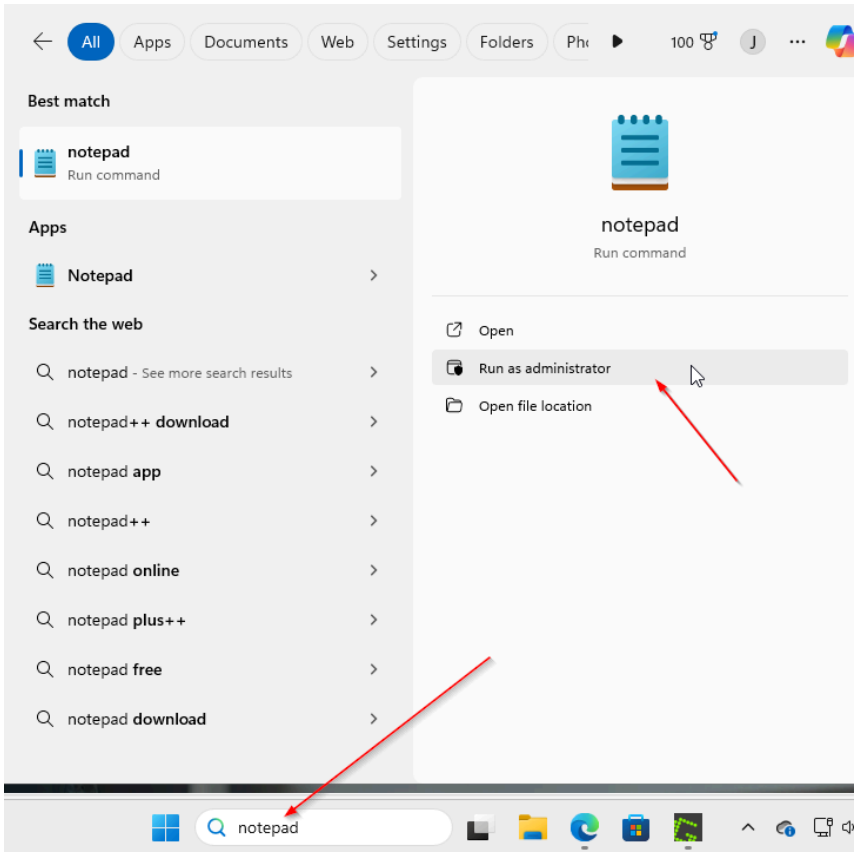
1. Open a Web Browser: Launch your preferred web browser I'm using Edge.

2. Visit a Legitimate Website: Navigate to a legitimate website, such as Comptia.org, to ensure it loads correctly and there are no existing issues with DNS resolution.

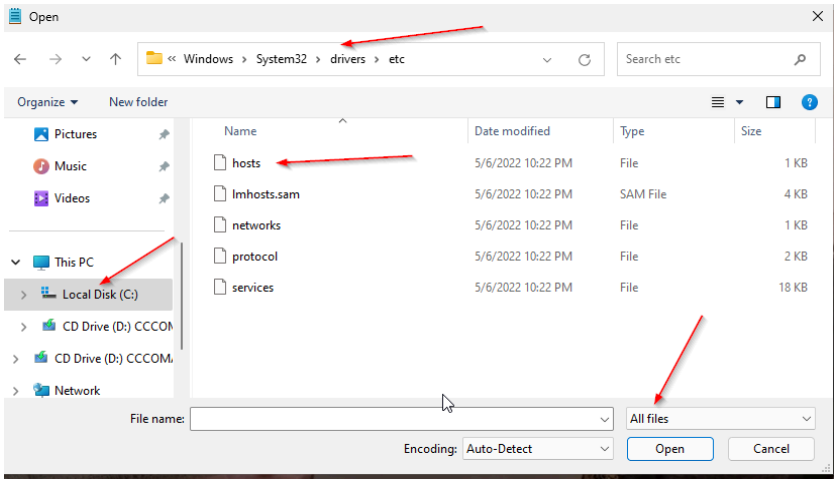


Step 2: Access and Modify the Hosts File

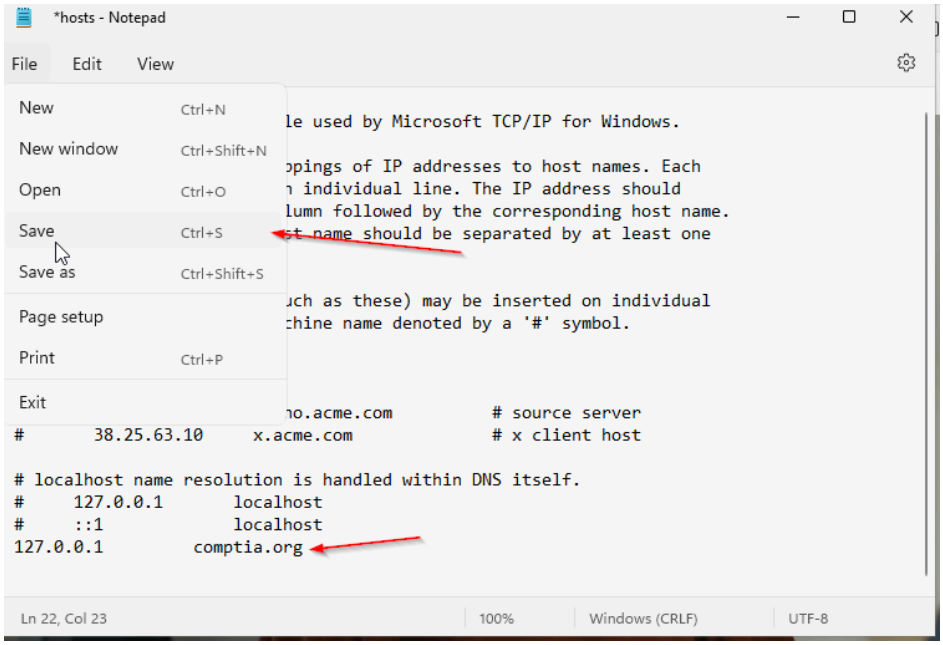
1. Open Start Menu: Click the Start button on your Windows 11 taskbar.
2. Open Notepad as Administrator:
    - Type “Notepad” in the search bar.
    - Right-click on Notepad in the search results and select “Run as administrator”.
    - Click “Yes” on the User Account Control (UAC) prompt to grant administrative privileges.



3. Navigate to the Hosts File:
    - In Notepad, click `File > Open`.
    - Browse to `C:\Windows\System32\drivers\etc`.
    - In the filename box, change the filter from “Text Documents” to “All Files” to view all types of files in the directory.
    - Select and open the “hosts” file.

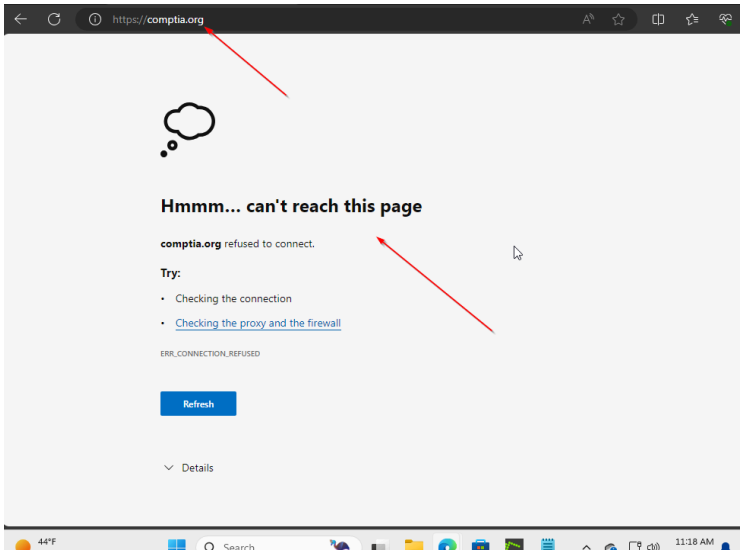


4. Modify the Hosts File:
    - Scroll to the bottom of the file.
    - Add a new line: `127.0.0.1 compTIA.org`
    - This entry redirects all traffic intended for `compTIA.org` to the localhost IP address, effectively blocking the site.
    - Save the changes by clicking `File > Save`.



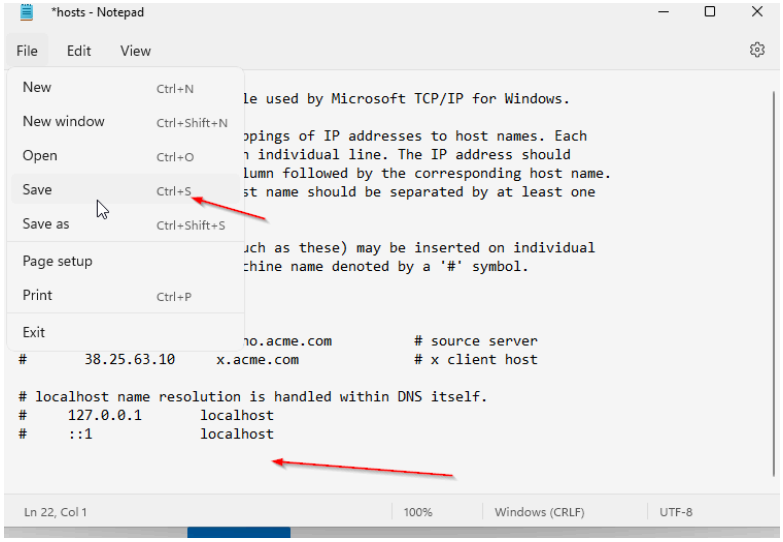
Step 3: Test the Changes

1. Open a Private Browsing Window:
    - Right-click on your browser icon and select “New private window” or “New incognito window” to ensure that the session is free from caching issues that might affect the test.
2. Attempt to Access the Blocked Site:
    - Type `compTIA.org` in the browser’s address bar and press Enter.
    - Observe that the website does not load, confirming that the DNS resolution is being redirected to the localhost (127.0.0.1), which is not a web server.



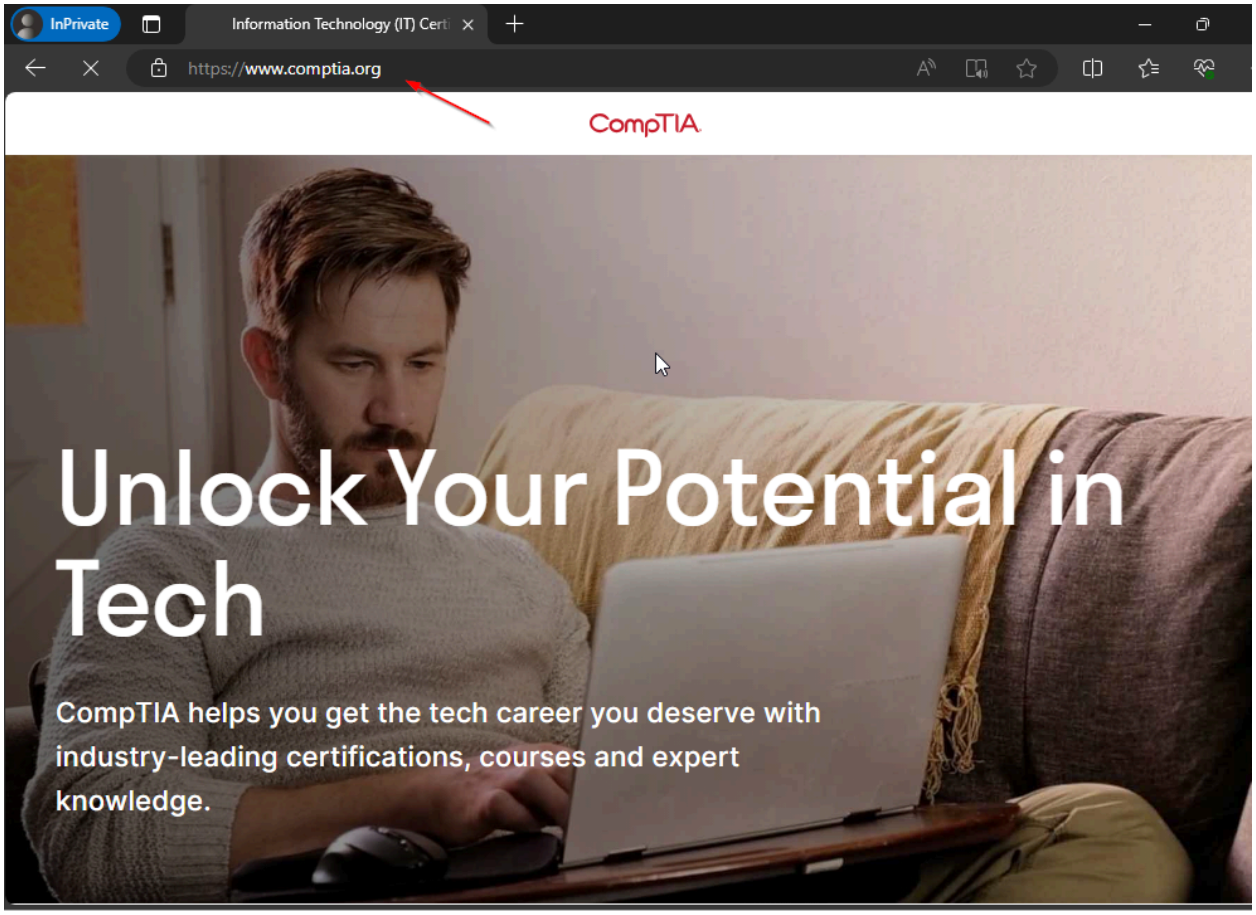
Step 4: Revert Changes

1. Open Notepad as Administrator Again and navigate to the hosts file as described in Steps 2.1 to 2.3.
2. Remove the Entry you added:
    - Delete the line `127.0.0.1 compTIA.org`.
    - Save the file.



3. Verify Website Access:

- Refresh or reopen the private window and navigate to `compTIA.org` again.
- The site should now load normally, demonstrating that the DNS resolution is functioning correctly after reverting the changes.



Conclusion

This exercise demonstrates how modifications to the hosts file can simulate DNS poisoning by redirecting DNS queries locally. It's a powerful demonstration of how easily DNS can be manipulated on a client machine, underscoring the importance of securing and monitoring DNS settings to prevent malicious activities.