Hosts File Attack

Time required: 30 minutes

How to Create Screenshots: Please use the Windows Snip and Sketch Tool or the Snipping Tool. Paste a screenshot of just the program you are working on. If you are snipping a virtual machine, make sure your focus is outside the virtual machine before you snip.

1. Press and hold down the **Windows key** & **Shift**, then type **S.** This brings up the on-screen snipping tool.
2. Click and Drag your mouse around whatever you want to snip.
3. Release the mouse button. This places the snip into the Windows Clipboard.
4. Go into Word or wherever you want to paste the snip. Hold down **CTRL**, then type **V** to paste the snip.

Lab Description

This lab can be done on a Windows virtual machine.

DNS host name resolution works in the following order.

1. Checks to see if the host name is its own name
2. Local resolver cache
3. Hosts file
4. DNS server

Substituting a fraudulent IP address can be done by either attacking the Domain Name System (DNS) server or the local host table. Attackers or malware can target a local hosts file to create new entries that will redirect users to their fraudulent site or prevent the user from going to a legitimate anti-malware site. In this project, you will add a fraudulent entry to the local hosts file to simulate a malware attack.

1. Start your web browser.
2. Go to www.google.com.
3. **Insert a screenshot:**

Click or tap here to enter text.

4. Click **Start**, type **Notepad**.

5. Right-click Notepad and then select **Run as administrator**.
6. Click **File** and then **Open**. Click the File Type drop-down arrow to change from Text Documents (*.txt) to All Files(*.*).
7. Navigate to file **C:\Windows\System32\drivers\etc**
8. Open the **hosts** file.
9. At the end of the file on a new line, type **127.0.0.1** → Press **Tab** and enter **google.com**
10. On a new line, type **127.0.0.1** → Press **Tab** and enter **www.google.com**
11. Add the following 2 lines to the hosts file. These lines will redirect wncc.edu to the outside IP address of the D1 classroom.
    198.206.239.241 wncc.edu
    198.206.239.241 www.wncc.edu

In this hosts file, google.com is now resolved to the IP address 127.0.0.1, which is the local host. This should prevent your computer from reaching google. wncc.edu will go to D1.

12. Click **File** → **Save**.

Make sure the name you are saving is hosts. Notepad should ask you if you are replacing hosts. If you add .txt to the extension of the file, hosts.txt, this lab will not work.

13. **Paste a screenshot of the contents of your hosts file:**

Click or tap here to enter text.

14. Open an administrative command prompt.
15. Type **ipconfig /flushdns** and press Enter. (This will flush your DNS cache.)
16. Ping **google.com** (Notice the IP address returned.)
17. Ping **wncc.edu** (Notice the IP address returned.)
18. **Insert a screenshot:**

Click or tap here to enter text.

19. Type **ipconfig /displaydns** (Notice the ip addresses of wncc.edu and google.com)
20. **Insert a screenshot:**

Click or tap here to enter text.

21.

22. Go to **google.com**

23. **What website appears? (You should receive an error.) Why did you receive this error?**

Click or tap here to enter text.

24. Go to **wncc.edu**

25. Click Advanced → Go to the web site anyway.

26. **Paste a screenshot of the resulting web site:**

Click or tap here to enter text.

27. **Why is google.com disabled?**

Click or tap here to enter text.

28. Return to the hosts file and remove the entry you added.

29. Click **File** → **Save**.

30. Close all windows.

31. Confirm internet access to google.com and wncc.edu

Assignment Submission

Attach this completed document to the assignment in Blackboard.