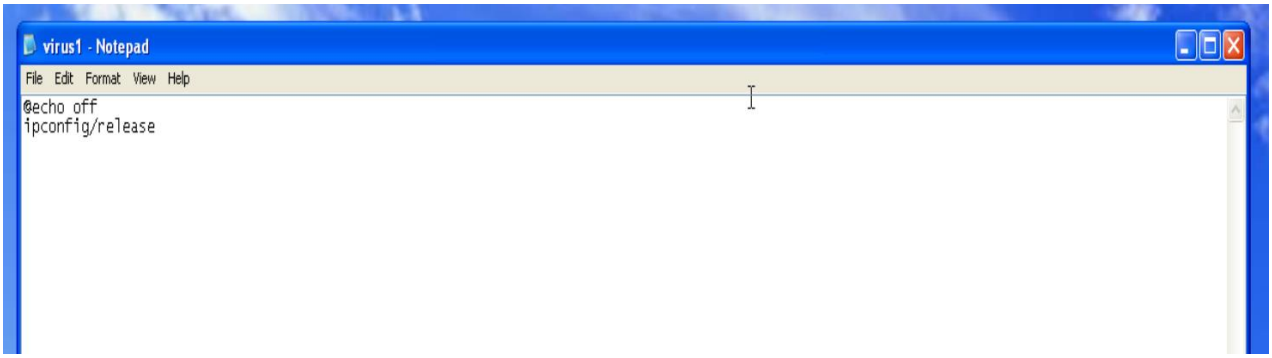
Assignment 5: Malware and Cryptography

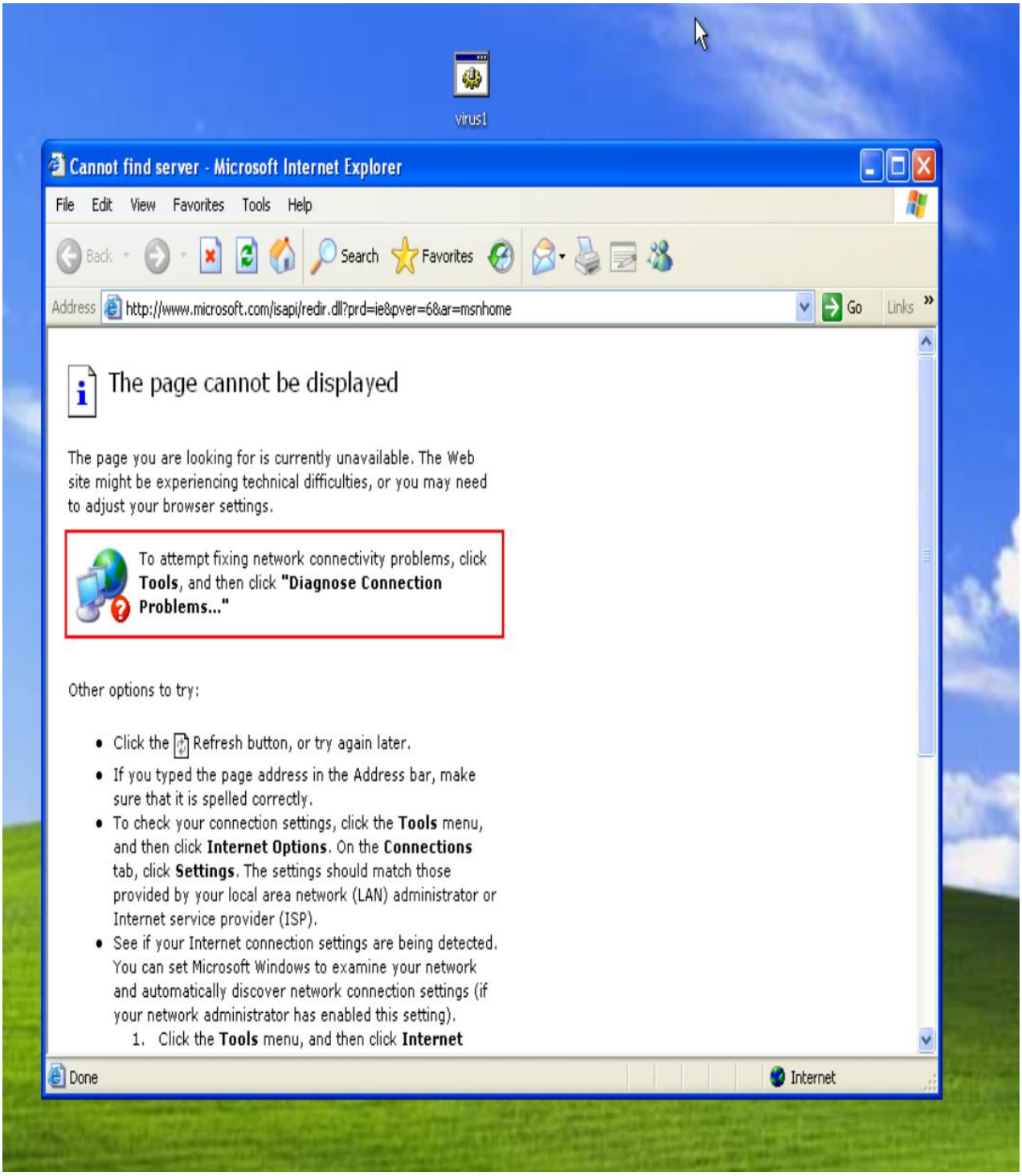
CYSE450 Ethical Hacking and Penetration Testing

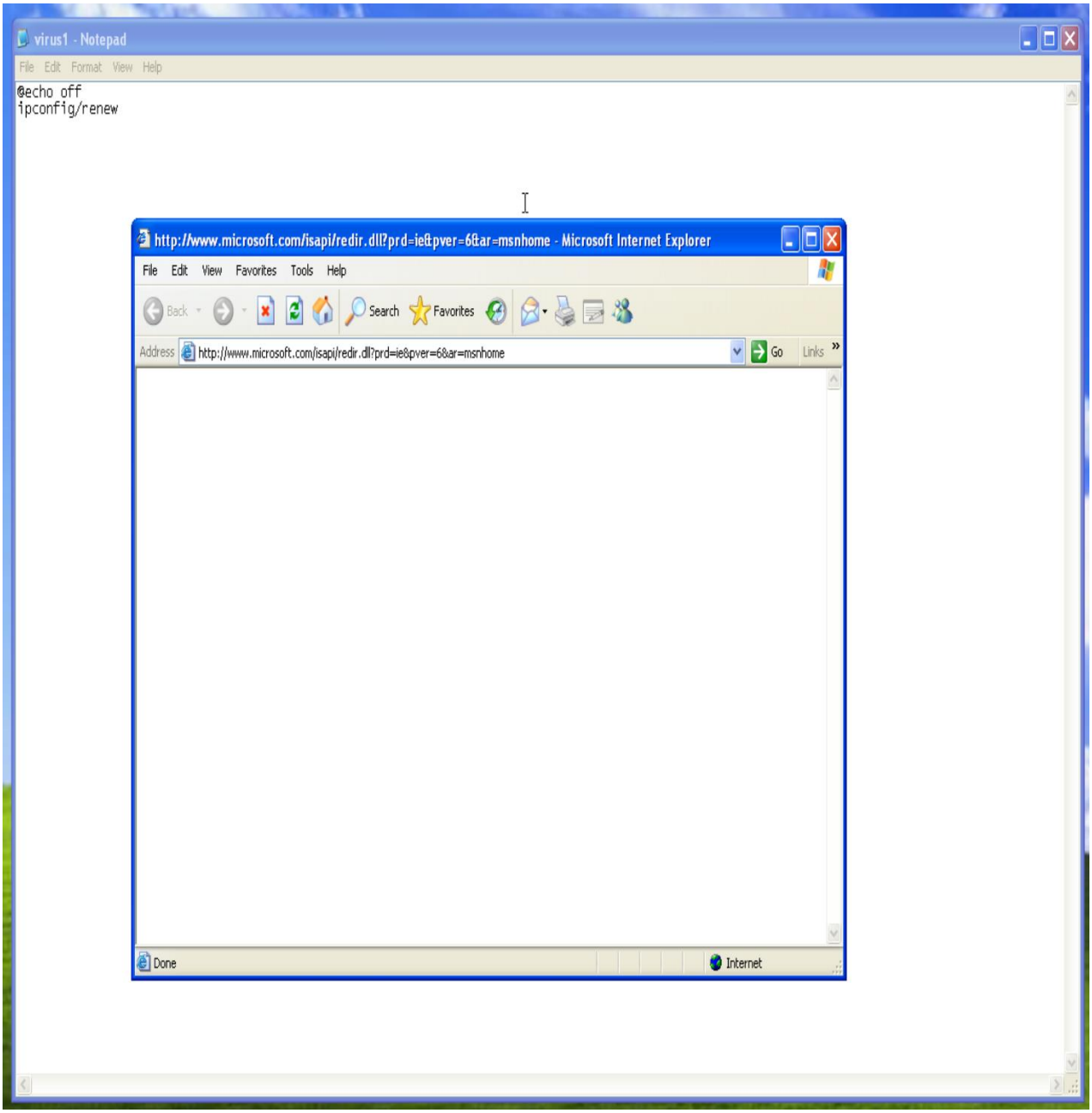
Task-A (50 Points): Creating virus in Windows VM

1. Boot your Windows VM
2. Open the Notepad editor
3. Write the script using VBA to create a virus which opens a pop-up dialog box using the correct values to display the **Critical Message icon**, **OK** and **Cancel** buttons. (You may refer to slide# 7 for the description).
4. Save the file as XXXX**.vbs** in Desktop folder. [NOTE: Replace XXXX with your choice for filename]
5. Now navigate to the Desktop folder and open the .vbs file.

Submit the screenshot of the code written in Notepad and the output window after opening the .vbs file.




virus1
Cannot find server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome
Go Links
The page cannot be displayed
The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.
To attempt fixing network connectivity problems, click Tools, and then click "Diagnose Connection Problems..."
Other options to try:
Click the Refresh button, or try again later.
If you typed the page address in the Address bar, make sure that it is spelled correctly.
To check your connection settings, click the Tools menu, and then click Internet Options. On the Connections tab, click Settings. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).
See if your Internet connection settings are being detected. You can set Microsoft Windows to examine your network and automatically discover network connection settings (if your network administrator has enabled this setting).
1. Click the Tools menu, and then click Internet
Done
Internet



Task-B: Case Study (50 Points): Creating a Rogue Server Certificate by Breaking a Hashing

Answer the following questions:

1. The researchers collected 30,000 website certificates in 2008. How many were signed with MD5?

   9,000 of them were signed with MD5

2. What kind of hardware was used to generate the chosen-prefix collision? How much money did the researchers spend on certificates?

RapidSSL was used to generate the chosen prefix collision. The cost was $69 for a new certificate, renewals are only $45, up to 20 free reissues of a certificate, and $2.25/query-and-increment operation. Total cost of certificates: USD $657.

3. What was the impact of generating a rogue CA certificate? What would this certificate allow someone with malicious intentions to do?

   The impact of generating a rogue CA certificate is that we can sign fully trusted certificates • Perfect man-in-the-middle attacks. A malicious attacker can pick a more realistic CA name and fool even expert. MITM requires connection hijacking: • Insecure wireless networks • ARP spoofing • Proxy autodiscovery • DNS spoofing • Owning routers

4. Which hashing algorithm were CAs forced to use after their signing method was demonstrated as not secure?

CAs switched to SHA-1

5. According to the researchers, what's the only way you can effect change and secure the Internet?

   The affected CAs are switching to SHA-1