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.

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

TIME REQUIRED: 30 minutes

 OBJECTIVE: Investigate what attackers can do with the results of an MD5 collision.

DESCRIPTION: Collisions for hashing algorithms have historically been a theoretical threat, though recent increases in computing power have made collisions a reality. In 2017, academics from France and Singapore demonstrated a successful SHA-1 collision attack. Collisions in MD5 have been demonstrated for more than a decade. Until recently, even some well-known CAs used MD5 to generate web server SSL certificates. In this activity, you research what's possible when smart researchers decide to call attention to a major security problem on the Internet.

Step-1: Start your web browser in Windows and go to www.google.com

.

Step-2: Type creating a rogue CA certificate and press Enter. Click the first link in the search results, which should take you to the Rogue CA research page at the **Phreedom.org** website. (If not, go to www.phreedom.org and search for rogue CA.)

Step-3: Read the paragraphs summarizing the researchers' findings, and then click the Slides from the 25c3 presentation link to download the PowerPoint presentation, which you use to answer the following questions. Note: You may have to click through a security warning, depending on the browser you are using.

Answer the following questions:

1. The researchers collected 30,000 website certificates in 2008. How many 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?
3. What was the impact of generating a rogue CA certificate? What would this certificate allow someone with malicious intentions to do?
4. Which hashing algorithm were CAs forced to use after their signing method was demonstrated as not secure?
5. According to the researchers, what's the only way you can effect change and secure the Internet?

Extra Credit: Creating Trojan to infect the Target Machine (Localhost).

Required Tool:

Windows XP/7 - Two VMs are preferred.

1. Open the browser in windows VM (prefer Firefox if using winXP in VirtualBox or UTM).
2. Download ProRat 1.9, using the source link: https://prorat.software.informer.com/
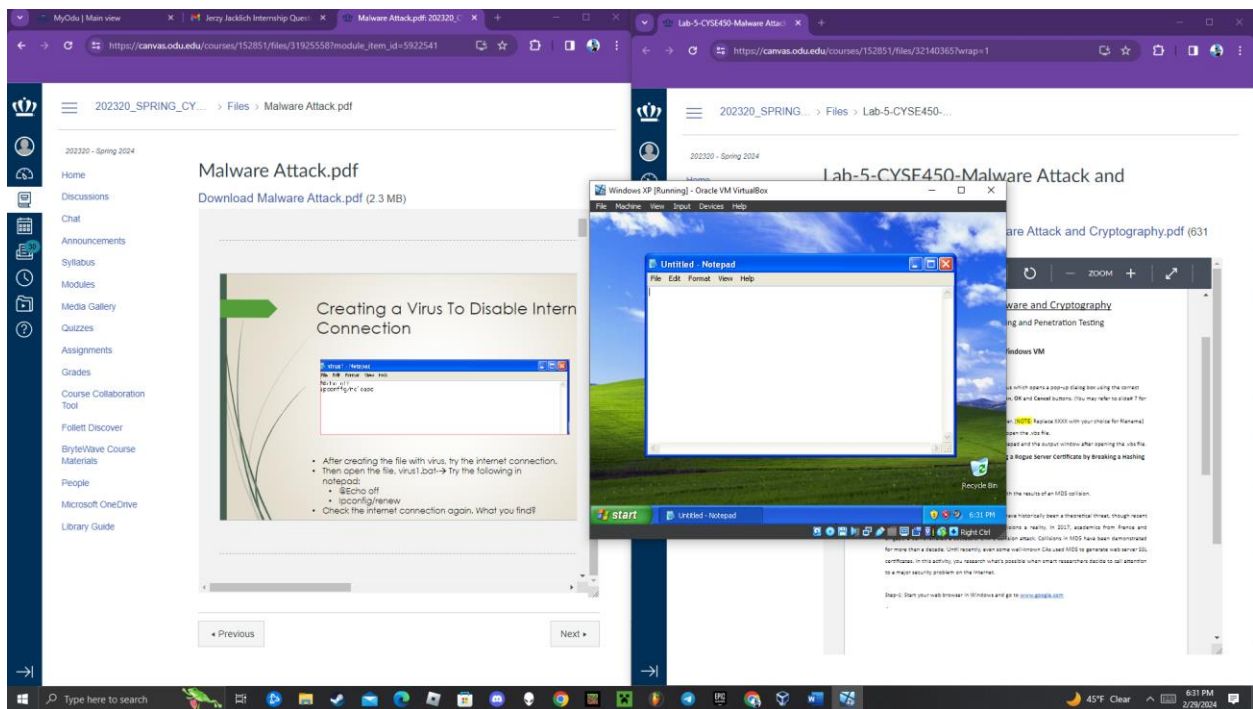
3. Using the instructions demonstrated in the slide, extract the compressed folder for ProRat.

4. Create the ProRat Server with the **icon** of your choice and bind with some downloadable software (for example, Notepad++)

5. To infect the Target System, First, run the software in the Client/attacker windows XP or 7 Machine.

6. Then, connect with the Target system using the IP address of the second windows VM (If you can install the second windows VM) or you can use the local host machine (which should be there as with IP as 127.0.0.1) and the default password.

7. Once connected to target VM, Complete the following tasks:

    a. Open the IExplorer and disable the close button so that the target machine cannot use the close button to close the Internet Explorer.

    b. Open the chat option, as shown below, to send any message to the target Machine.

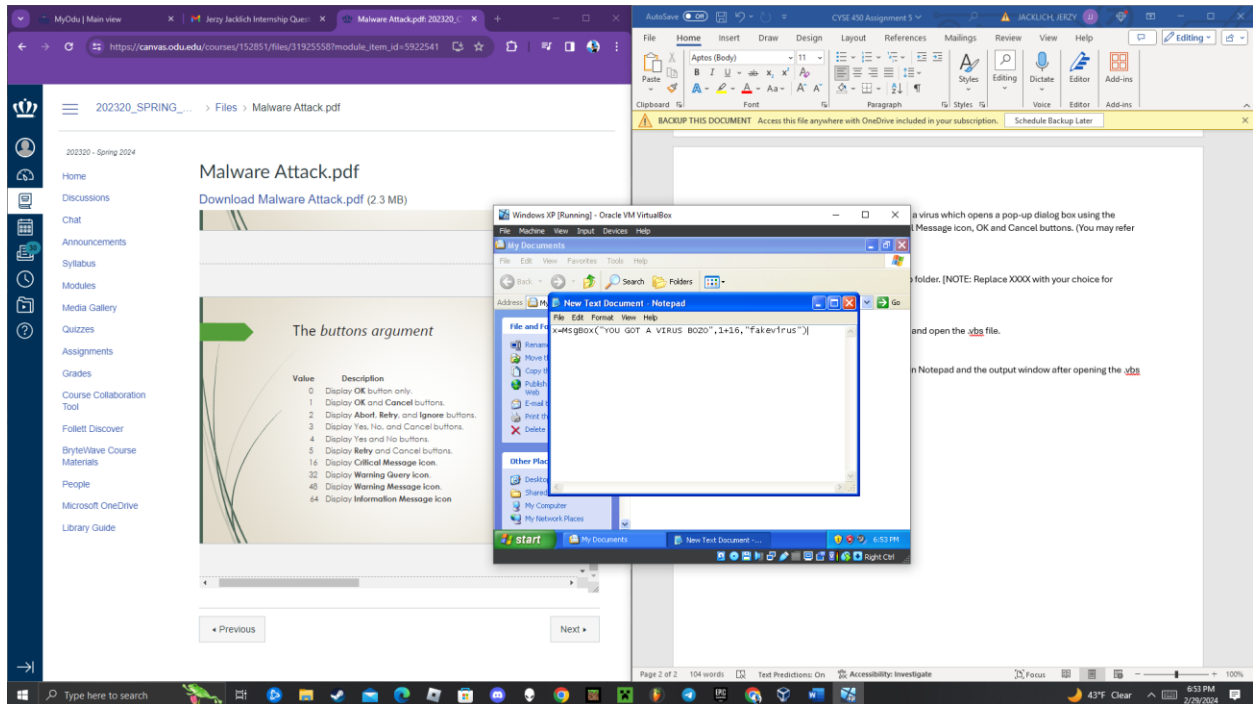Task-A (50 Points): Creating virus in Windows VM
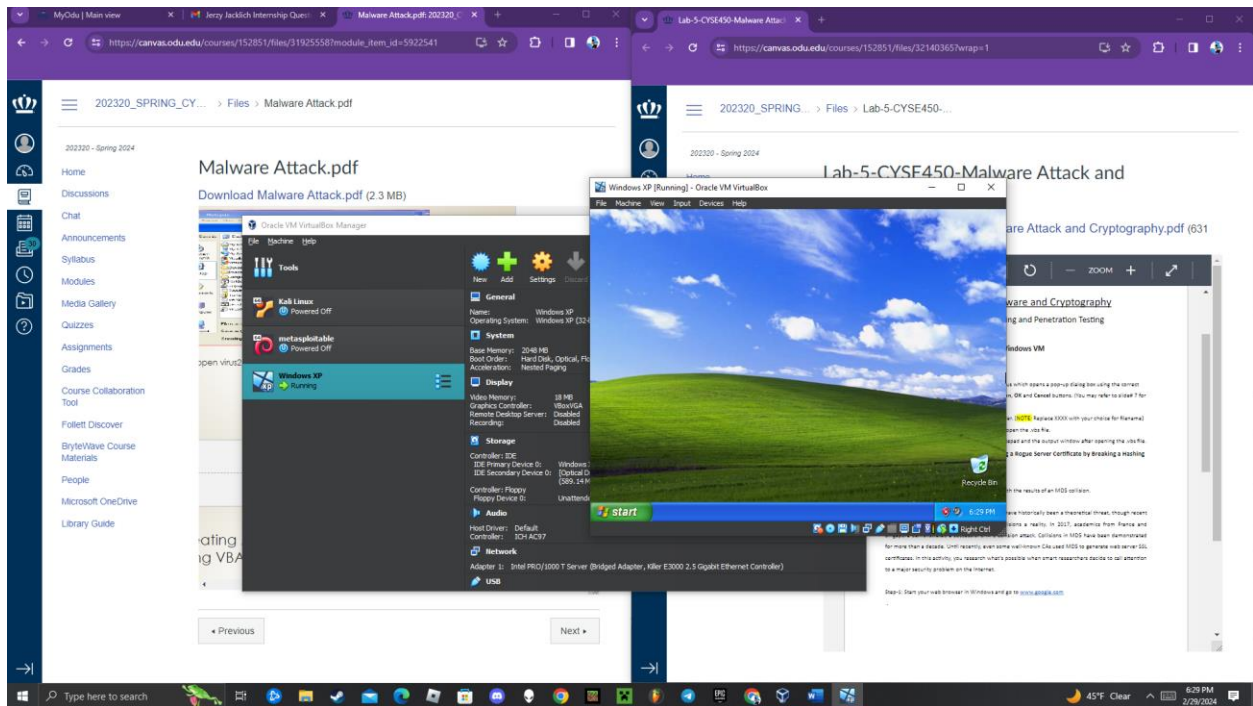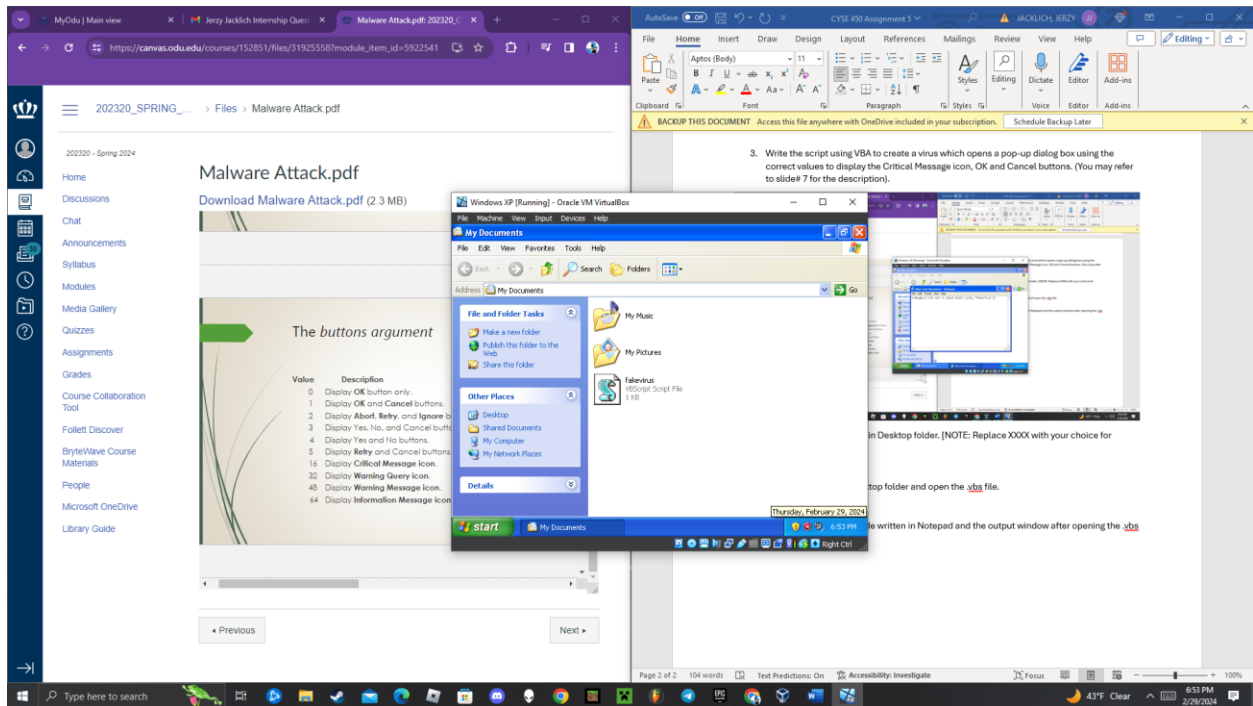
1. Boot your Windows VM
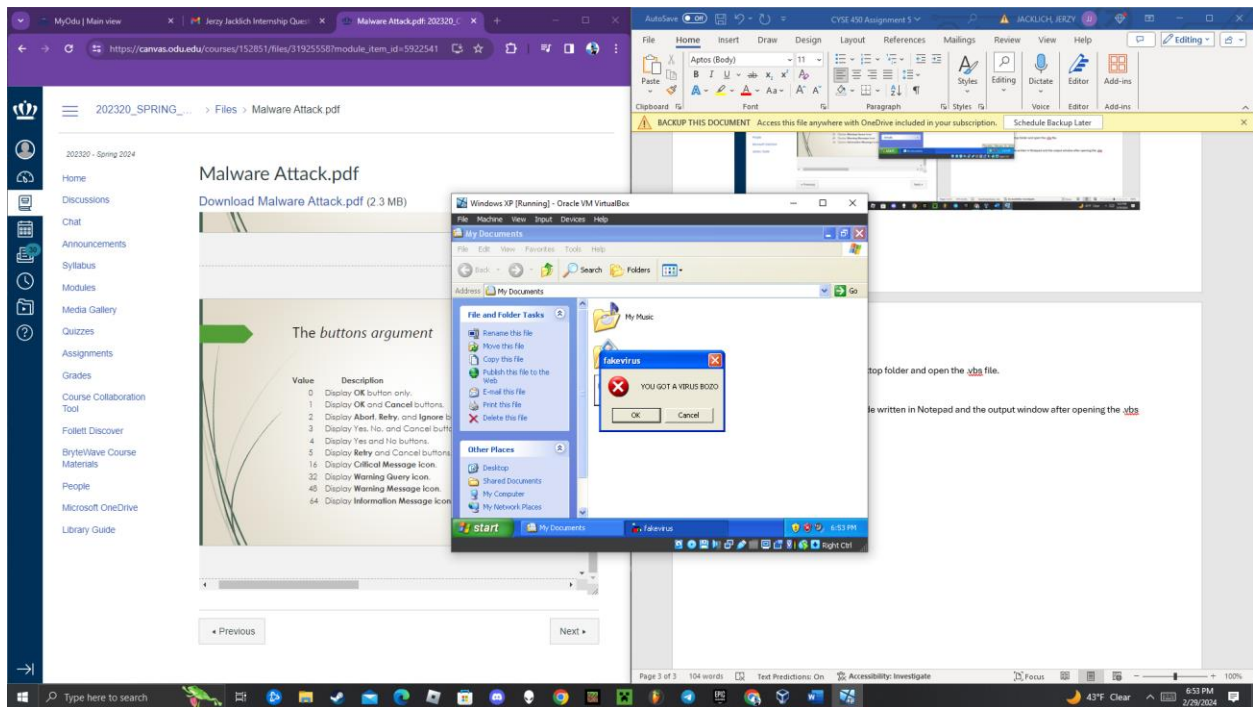

2. Open the Notepad editor

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

x=MsgBox("YOU GOT A VIRUS BOZO",1+16,"fakevirus")

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

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

9,000 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?

200 Playstation 3's were used to generate the chosen-prefix collision over the course of 1-2 days. The researchers spent a total of $657 on certificates.

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

With this attack you can sign fully trusted certificates and execute perfect man in the middle attacks.

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

They had to switch to SHA-1 after MD5 was proven to be vulnerable.

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

"Making the theoretical possible"