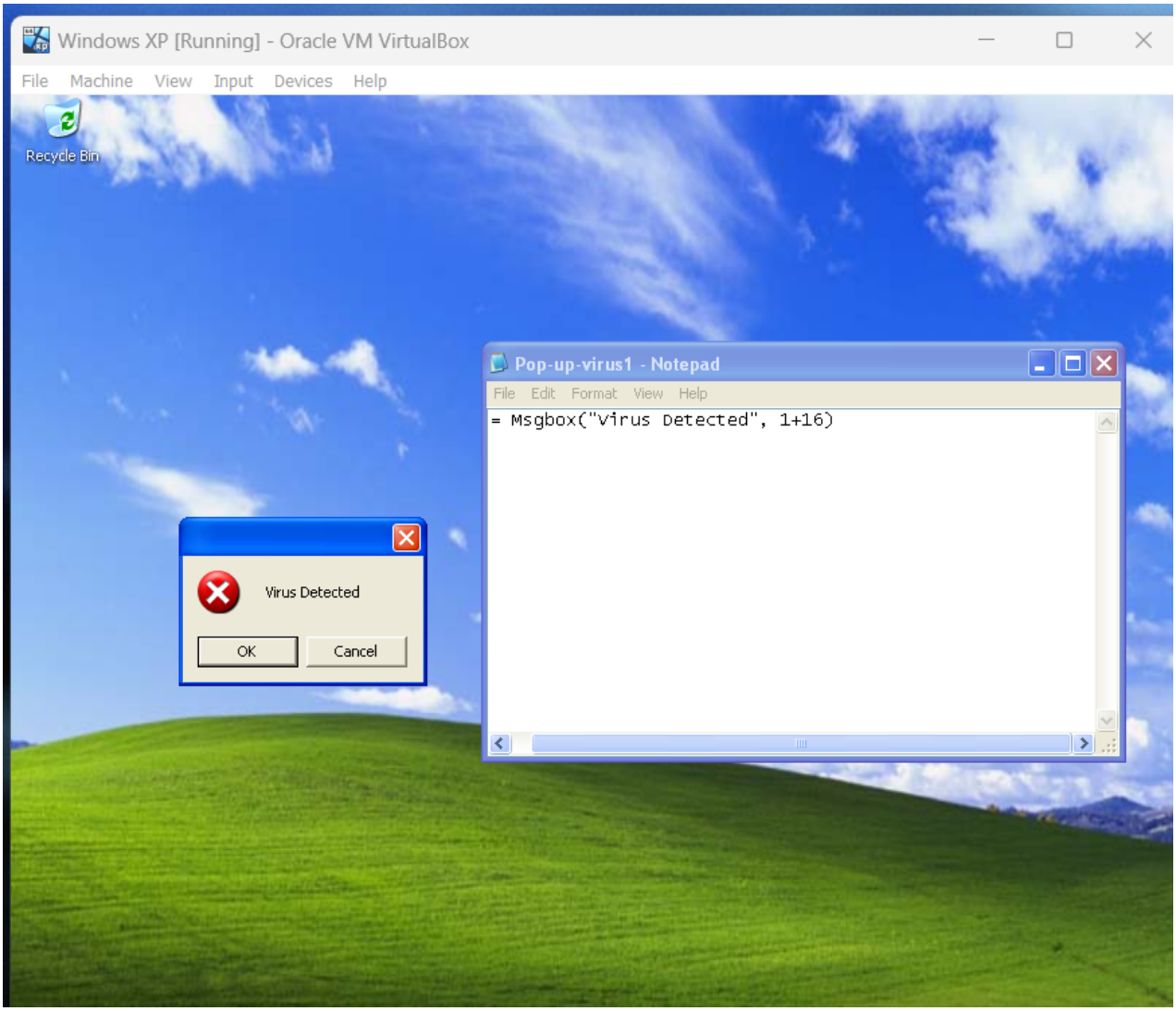
Assignment 5: Malware and Cryptography

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?

   9,000

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

   PlayStation 3s, $20,000

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

   - **Fully sign trusted certificates**
   - **Perfect man-in-the-middle attacks**
   - **A hacker can pick a more realistic CA name.**
   - **Connection Hijacking**

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

   SHA-1

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

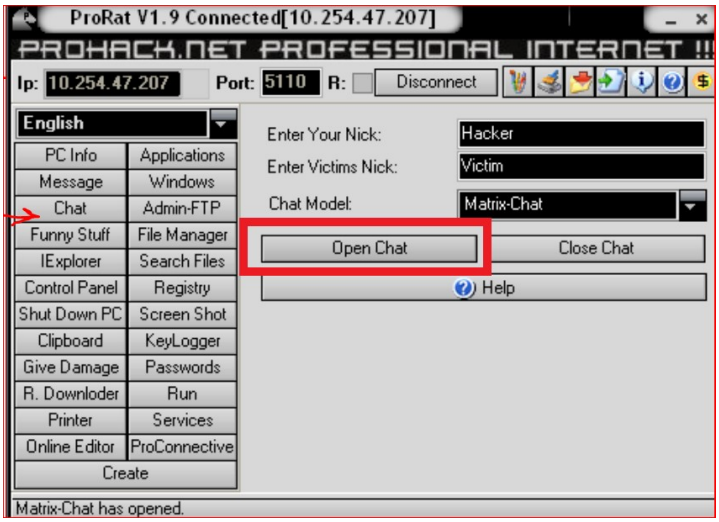
Making the theoretical possible is sometimes the only way to affect change and secure the internet.

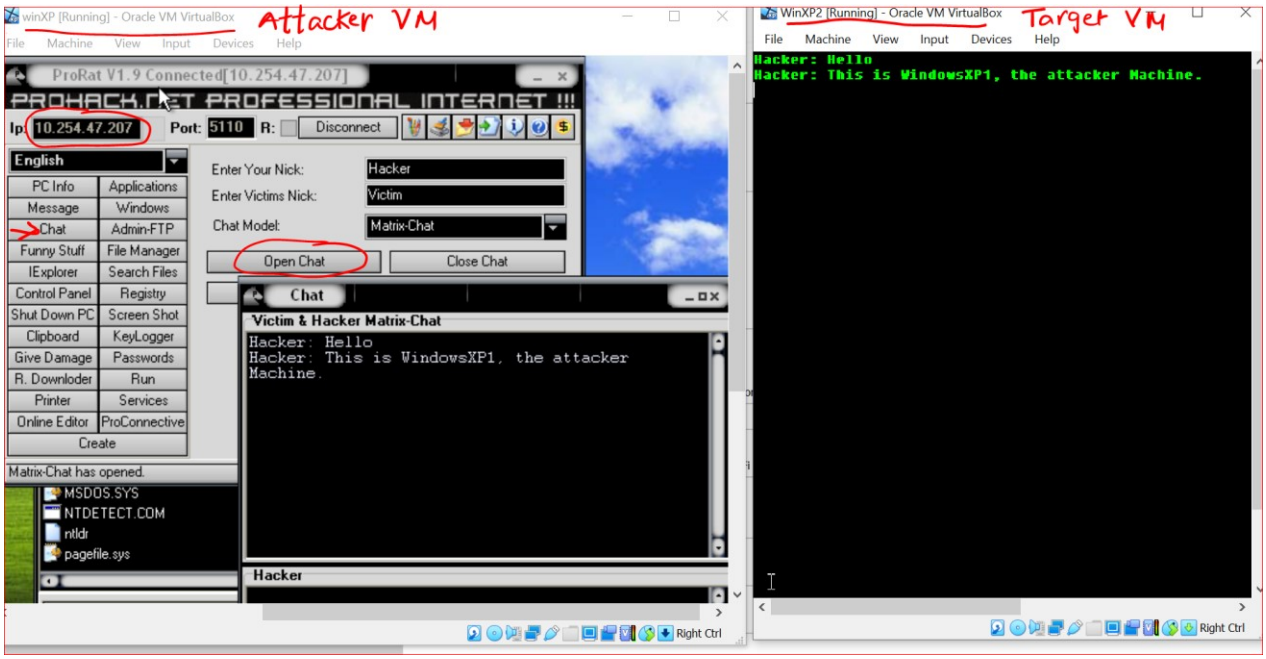
Extra Credit: Creating Trojan to infect the Target Machine (Localhost).

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.


ProRat V1.9 Connected[10.254.47.207]
PROHACK.NET PROFESSIONAL INTERNET !!!
Ip: 10.254.47.207
Port: 5110
R:
Disconnect
English
PC Info
Applications
Message
Windows
Chat
Admin-FTP
Funny Stuff
File Manager
IExplorer
Search Files
Control Panel
Registry
Shut Down PC
Screen Shot
Clipboard
KeyLogger
Give Damage
Passwords
R. Downloder
Run
Printer
Services
Online Editor
ProConnective
Create
Enter Your Nick:
Hacker
Enter Victims Nick:
Victim
Chat Model:
Matrix-Chat
Open Chat
Close Chat
Help
Matrix-Chat has opened.


winXP [Running] - Oracle VM VirtualBox
Attacker VM
File Machine View Input Devices Help
ProRat V1.9 Connected[10.254.47.207]
PROHACK.NET PROFESSIONAL INTERNET !!!
Ip: 10.254.47.207
Port: 5110
R:
Disconnect
English
PC Info
Applications
Message
Windows
Chat
Admin-FTP
Funny Stuff
File Manager
IExplorer
Search Files
Control Panel
Registry
Shut Down PC
Screen Shot
Clipboard
KeyLogger
Give Damage
Passwords
R. Downloder
Run
Printer
Services
Online Editor
ProConnective
Create
Enter Your Nick:
Hacker
Enter Victims Nick:
Victim
Chat Model:
Matrix-Chat
Open Chat
Close Chat
Chat
Victim & Hacker Matrix-Chat
Hacker: Hello
Hacker: This is WindowsXP1, the attacker Machine.
Hacker
Matrix-Chat has opened.
MSDOS.SYS
NTDETECT.COM
ntldr
pagefile.sys
Right Ctrl
WinXP2 [Running] - Oracle VM VirtualBox
Target VM
File Machine View Input Devices Help
Hacker: Hello
Hacker: This is WindowsXP1, the attacker Machine.
Right Ctrl