CSC427 Tutorial - Ransomware

Tuesday, January 14, 2020

# Tutorial Objectives

The objective of today’s tutorial is to practice identifying phishing emails and to understand ransomware.

## Getting Started

Open the VM, CSC427 - Ransomware Tutorial. To log in to the VM, select user **csc427** and enter the password **dh2020**.

### Exercise: Phishing Emails

On the VM, there is a folder called Phishing Emails and this is where the email images are. Try to identify the phishing emails and explain how you identified that they were phishing emails. Are they all phishing emails?

### Exercise: Simple Encryption Ransomware

Write a simple Ransomware Encryption Malware that changes the extension of the files located on the computer. **Use the encryption pass:Y3NjNDI3ZnVu**

Note: **Do not run the ransomware in root.** This will likely encrypt all files and prevent access to important applications like ls.

Hint: There is already an encryption program installed on the VM called ccrypt

### Exercise: Build a Decrypt File

Now, build a decryption file to decrypt the encryption program that you built above.

### Exercise: Advanced Ransomware Encryption

Now, change the simple encryption ransomware, so that it hides the directories on the computer.**Use the encryption pass:Y3NjNDI3ZnVu**

Hint: Google how to hide directories.

### Exercise: Customize your Ransomware

At a minimum change the background picture, create a pop up message, and encrypt the files.

Alter the decryption algorithm, to account for the changes from the advanced ransomware encryption exercise.

Hint: you might want to use the programs Zenity and Gsettings to help customize the ransomware

### 