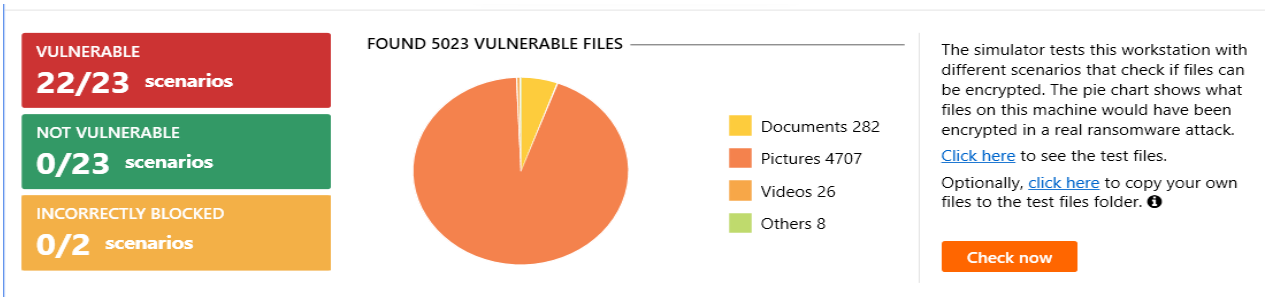
Lab #1 Understanding Ransomware Simulator

Last Name_____ First Name_____

Objectives: Hands-on Lab to carry out phishing analysis on several case studies and ransomware simulator. The aim is to determine the level of vulnerabilities that computer users are exposed to daily and answer questions based on ransomware simulation.

Scenario: Ransomware is a form of malware designed to encrypt files on a device. Making the files and the systems that rely on the device unusable. A ransom is then demanded to provide access. Ransomware is often designed to spread across a network and target database and file servers and can thus quickly paralyze an entire organization. Cybercriminals place organizations in a position where paying the ransom is the easiest and safest way to regain access to their files. If not, the organizations will lose all their data which will cause the organizations to face different consequences. There are many popular ransomware variants. Some examples of ransomware variants are Ryuk (spear-phishing emails or by using compromised user credentials), maze (file encryption and data theft), Lock bit (data encryption), and more.

During a ransomware attack, an individual who is facing this attack will have no clue of what they are facing during that attack. Individuals facing that attack will not know what is happening to their computers and why they can't gain access to their files and systems. To solve this problem, ransomware simulators such as KnowBe4 and others are used to simulate how ransomware attacks happen and show how vulnerable their computers are. Ransomware simulator (KnowBe4's) is a type of simulator that simulates twenty-two infection scenarios and one crypto mining infection scenario and shows how vulnerable your workstation is. This hands-on lab exercise gives you how a ransomware simulator such as KnowBe4's and others is used to simulate how ransomware attacks happen and show how vulnerable their computers are. By checking the result of the simulation of the attack, they will understand this type of attack process better. Moreover, they will learn about what ransomware is and the vulnerabilities of their workstation.



Goals:

The students will:

- Learn what ransomware is
- Learn how the ransomware simulator works
- Understand how vulnerable your workstation is

– Learn what is happening during a ransomware attack

Tools:

– Ransomware Simulator
– Laptop/Desktop
– Windows 11/10 Operating System
– Case Studies

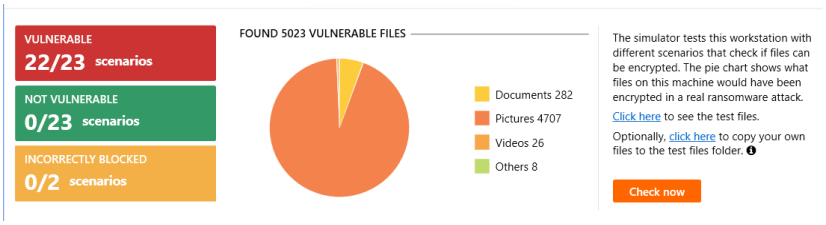
Steps:

Task #1: Installation Guideline/ Running of the Simulator

1. Go to the KnowBe4 website and fill out the form that is placed there to receive the knowbe4 Ransomware simulator.
2. Download the knowbe4 Ransomware simulator from the website.
3. Disable your real-time settings on your current laptop/desktop.
4. Extract the knowbe4 Ransomware simulator files.
5. Install the Ransomware simulator on your desktop/laptop.
6. Open the Ransomware simulator on the desktop
7. When the simulator is open, press the Check now button.
8. When the button is pressed, the simulator will run different ransomware scenarios on your laptop/desktop.

Task #2: Seeing and Exporting Files/Results from Running the Simulator

1. After each task is executed on the desktop/laptop, results from the tasks are displayed on the top of the simulator.



a) What is the total number of vulnerabilities found?

b) What percentage of your files were vulnerable, not vulnerable, or not blocked from the different scenarios?

Vulnerable	Not Vulnerable	Not Blocked

c) Plot a pie chart for the files were vulnerable, not vulnerable, or not blocked from the different scenarios?

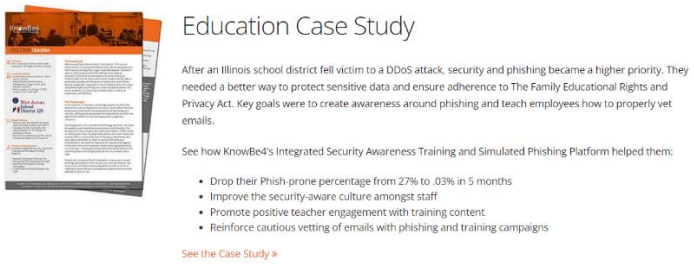
2. Files from the scenarios can also be exported to your computer.
3. Results from running the simulator can be exported to your computer.

From the results exported, how many files were vulnerable, exutable and not exutable

Vulnerable	Exutable	Not exutable

Task #3: Reading/Analyze Different Case Studies

1. After running the simulator, there are different websites that an individual can read and analyze.



2. These case studies are based on companies using the simulator to solve different problems at their companies. Some names of these cases were Commercial Bank Case Study, Data Management Case Study, Financial Services Case Study, and more case studies.

a) What were the different key goals from each of the case studies?

b) In one sentence what was the Data Management Case Study?

c) What were the results of the Data Management Case Study?

d) How long does it take to run a complete simulation on the financial case study profile?

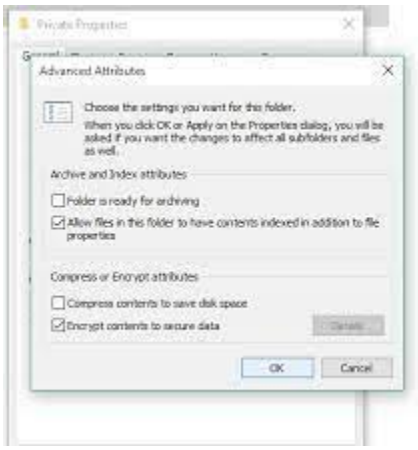
e) What was the conclusion of the financial case study profile?

f) In different case studies, what was the main reason why companies install the Ransomware simulator for their companies?

g) What were the different results from each case study?

3. Read and analyze the different cases that are on the website.

Task 4: **Encrypting Files on a Device**



1. Right-click (or press and hold) file or folder and select Properties.
2. Select the Advanced button and select the encrypted contents to secure the data check box. An "The Advanced Encryption Standard" (AES) is used to encrypt this file.
3. Select Ok to close the Advanced Attributes window, select Apply and then select Ok.

(a) . What type of files did you encrypt from this device?

(b) What are the vulnerabilities of the encrypting file system?

(c) What are the pros and cons of this encrypting file system?

Pros	Cons

(d) What type of AES keys are used to encrypt and decrypt data?

(e) Does AES use symmetric key or asymmetric key algorithms?

(f) Does AES use public or private keys?

(g) In your own words, explain the procedure of encrypting and decrypting a file using the AES method?