Ransomware Workout Instruction

Welcome to the *Ransomware* workout, in which you will experience a very common cyberattack known as ransomware. Ransomware quietly and quickly encrypts a victim's files and spreads rapidly to encrypt other files in a network or organization. Once the damage is complete, the victim is notified and requested to pay a *ransom* to restore the files.

> Don't worry, this workout is free. You won't need to pay any Bitcoin!

This workout guides you through the experience of a user action initiating the cyberattack and the process of recovering your files using open-source ransomware NekRos (https://github.com/PushpenderIndia/nekros). NekRos simulates the process of Ransomware in a safe manner without destroying your files or spreading to other computers.

Your Mission

Attack Mission

Once you are logged in, take note of the items on the desktop. When you are ready to start the attack double click on the 'Free Vacation' application on the desktop. The attack should take place, but if it does not, you may need to wait a few minutes and then click on the Free Vacation application again.

Follow the instructions of the ransomware to decrypt the files on the computer. **Do not close the application prematurely or else you will not be able to unlock your files.**

The attack mission will automatically indicate a completion status when you have successfully performed the attack.

Defense Mission

Once you have completed the attack mission, use Windows Defender to perform the defense mission. Research the Ransomware Protection for Windows Defender at https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/controlled-folders.

Configure the server with Ransomware protection and run the attack again. If you have configured this successfully, then nothing should happen to your files on the Desktop. The defense mission will automatically indicate a completion status when you have successfully configured your server for protection.