Security Baseline – Preparatory Exercises

Ifeanyi Uzoukwu

CYB 670

Dr. Reza Solari

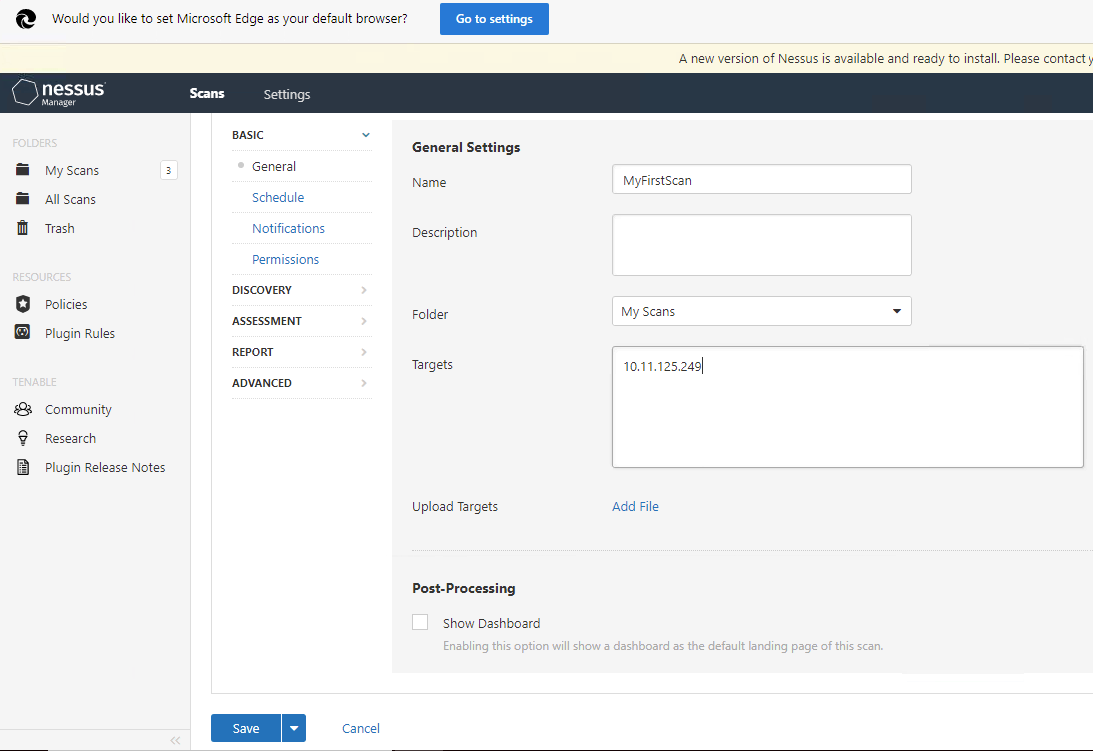
University of Maryland Global Campus

**Introduction**

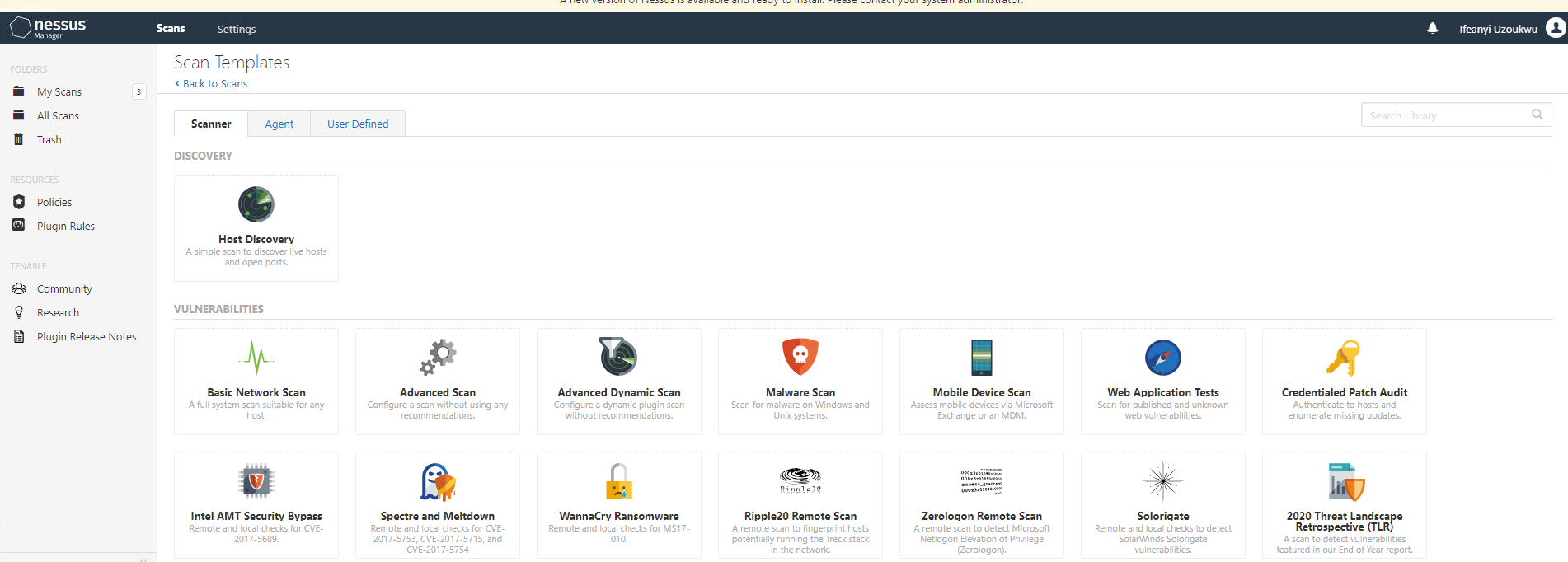
The Preparatory Exercises for this lab required students to perform a security scan using the **Nessus** tool, Scan files to detect signs of Malware using the **Yara** tool, and read email files using the **Mozilla Thunderbird** application. The following images are representative of screenshots I took while performing the various components of the lab.

**Part 1: Using the Nessus Tool**

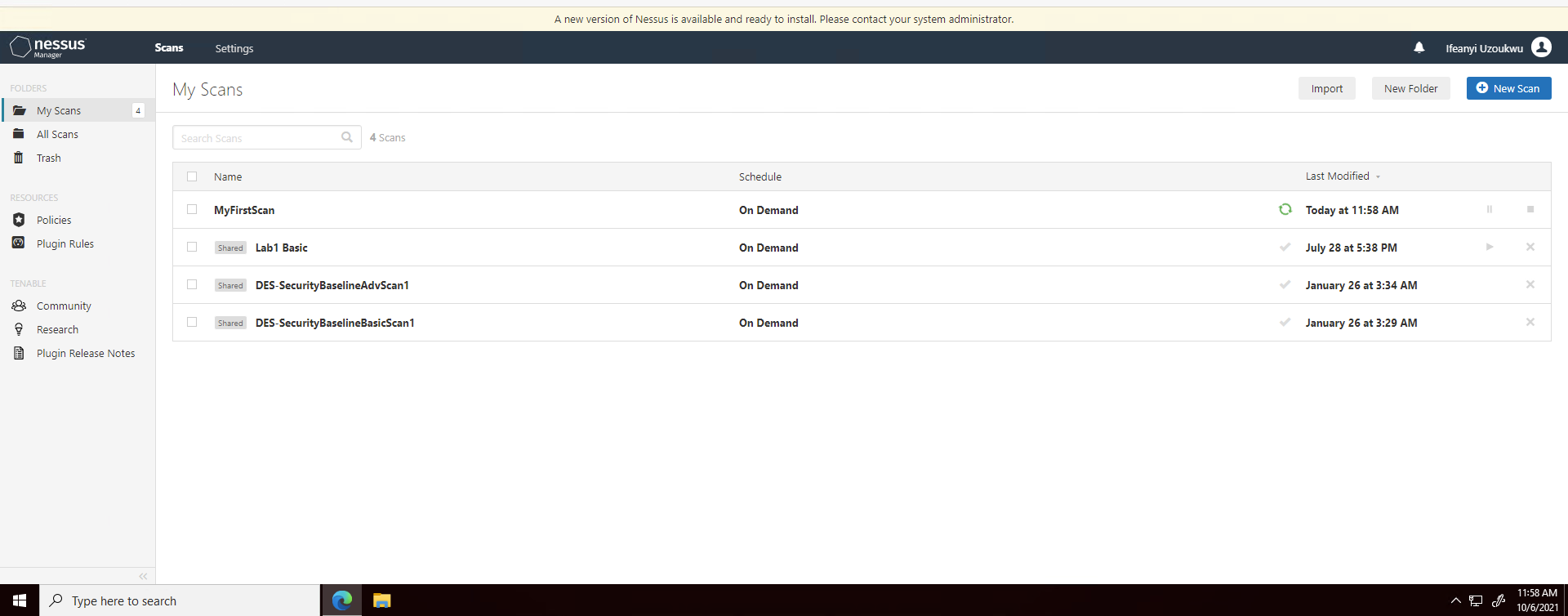
1. **Opening the Nessus Tool**



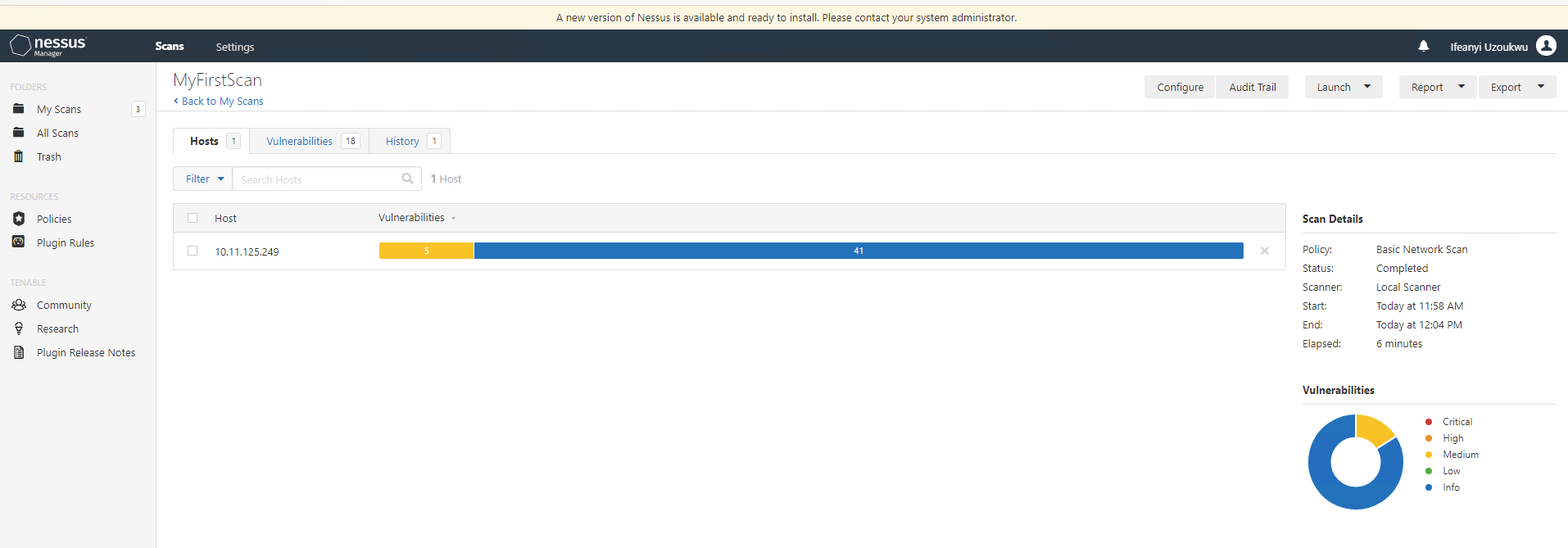
1. **Running a Basic Network Scan on the WINTGT01 Virtual Machine IP: 10.11.125.249**



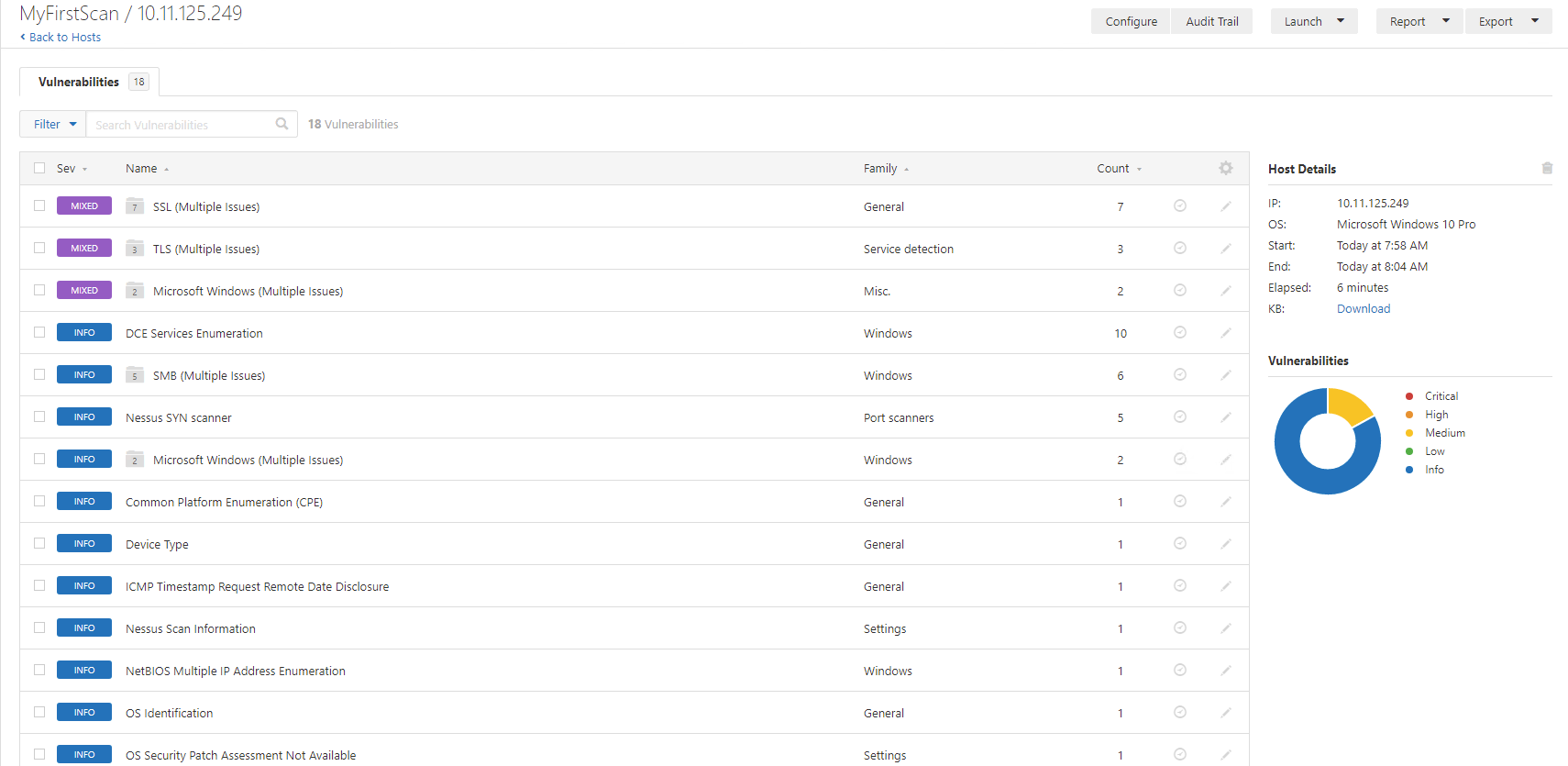
1. **“MyFirstScan” has been completed and is listed amongst the scans on Nessus**



1. **Viewing the results of “MyFirstScan”. The analysis of the scan revealed 41 Information Vulnerability Alerts and 5 “Medium” Vulnerability Alerts.**

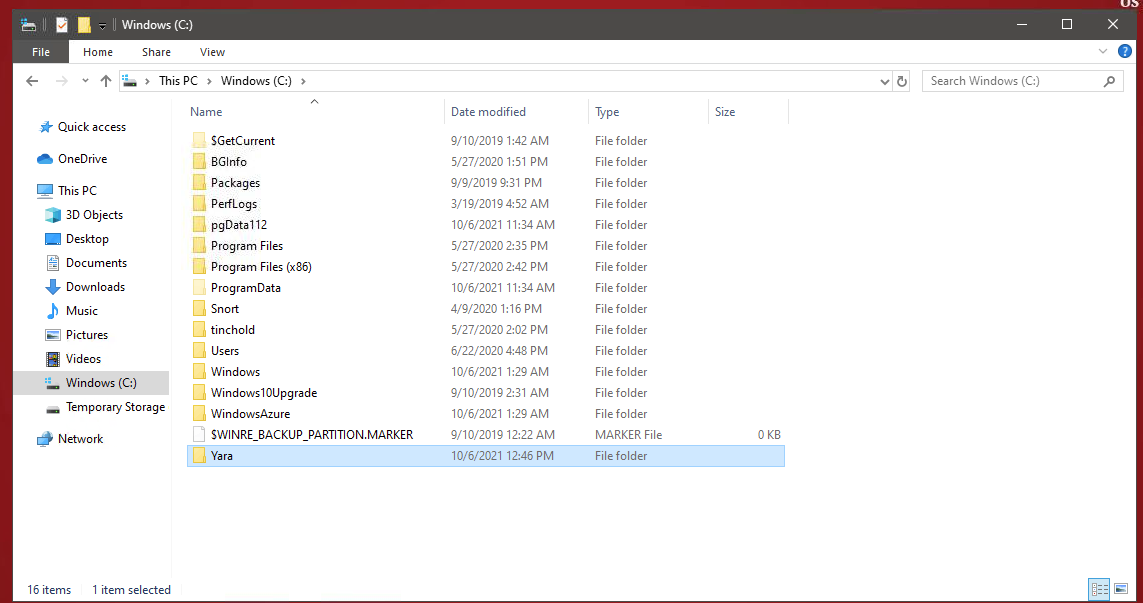


1. **18 Vulnerabilities were found in total during the scan of the WINTGT01 Virtual Machine.**

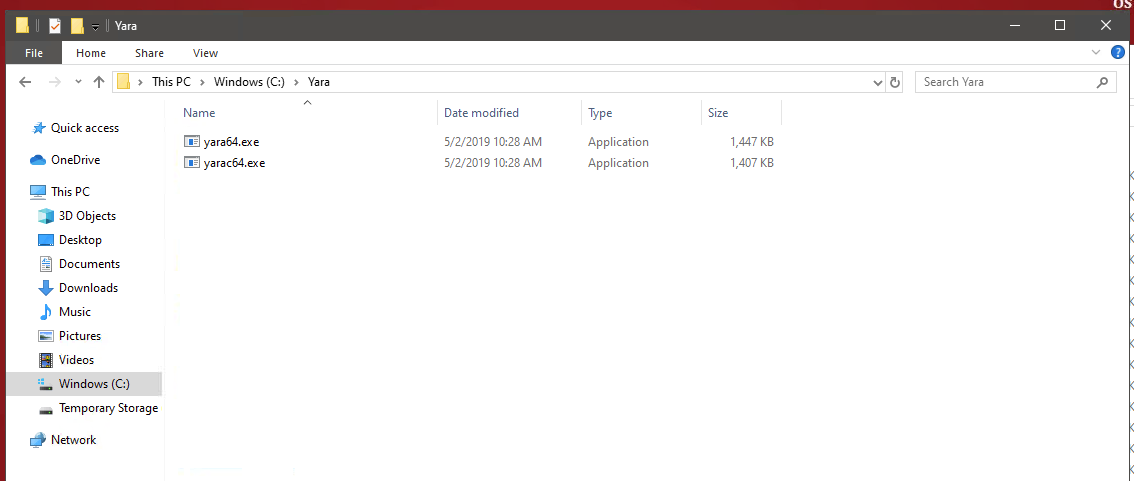


**Part 2: Using the Yara Tool**

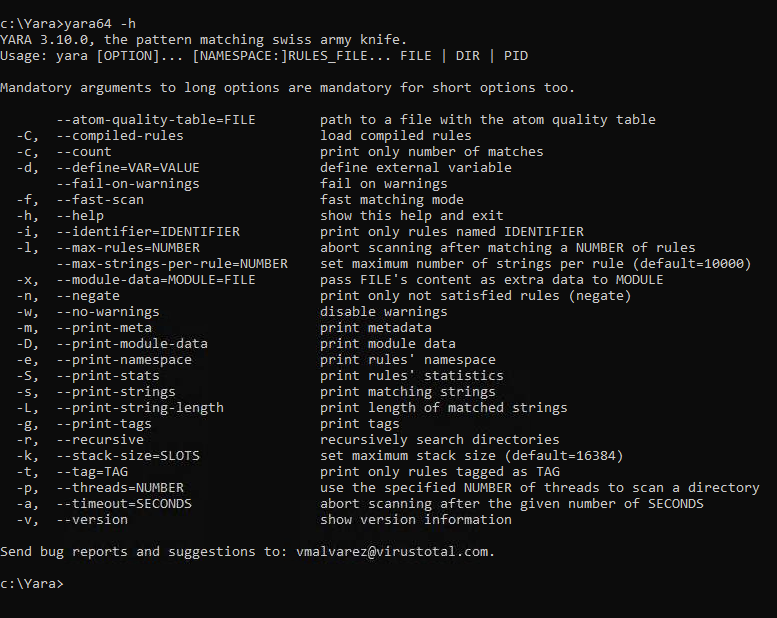
1. **Creating and Opening Yara File Folder**

****

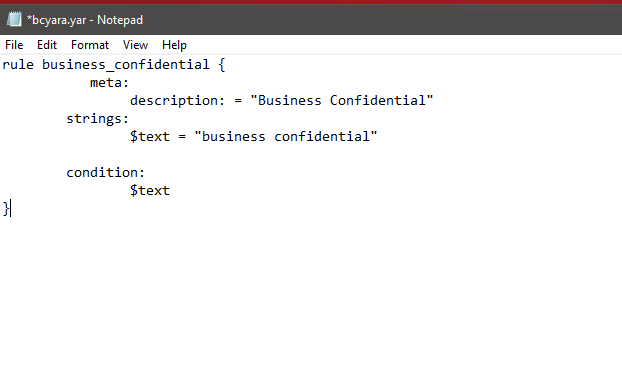
1. **“Yara64.exe” and “yarac64.exe” files moved into Yara File on C: drive**

****

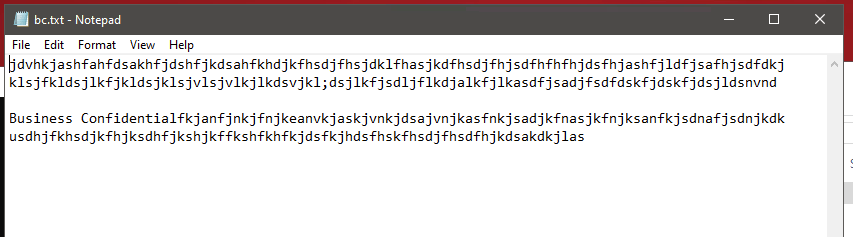
1. **Displaying the Yara help information in the command prompt application**

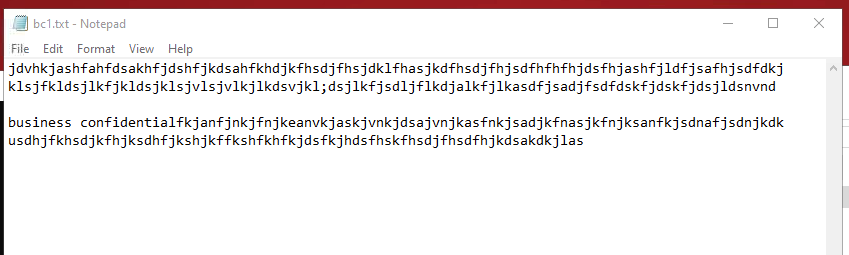
****

1. **Yara Rule Set: “Business Confidential”**

****

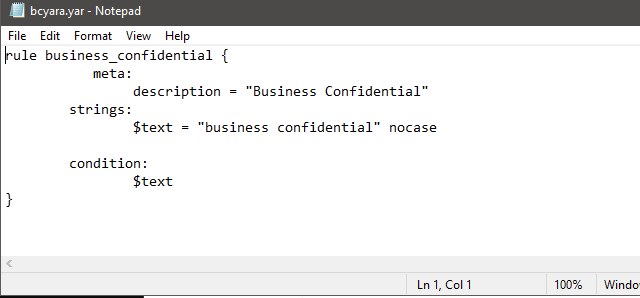
1. **Bc.txt and Bc1.txt files**

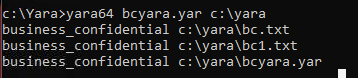
****

****

1. **Running Yara under current ruleset, which returns the bc1.txt and bcyara.yar files**

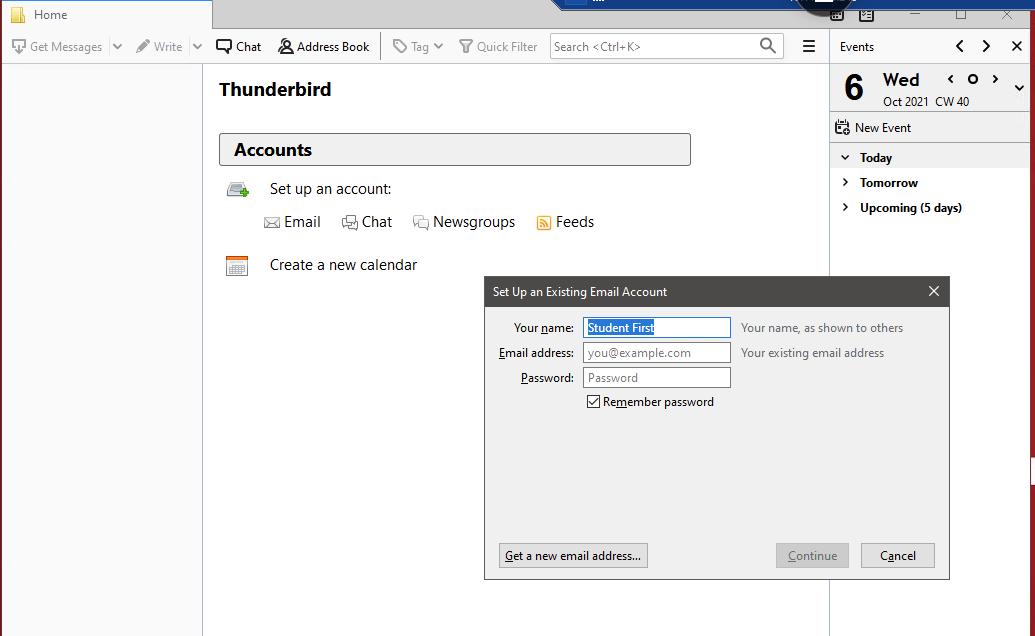
****

1. **Adjusting Yara Ruleset to include “nocase” **
2. **Running adjusted Yara ruleset within the command prompt application**

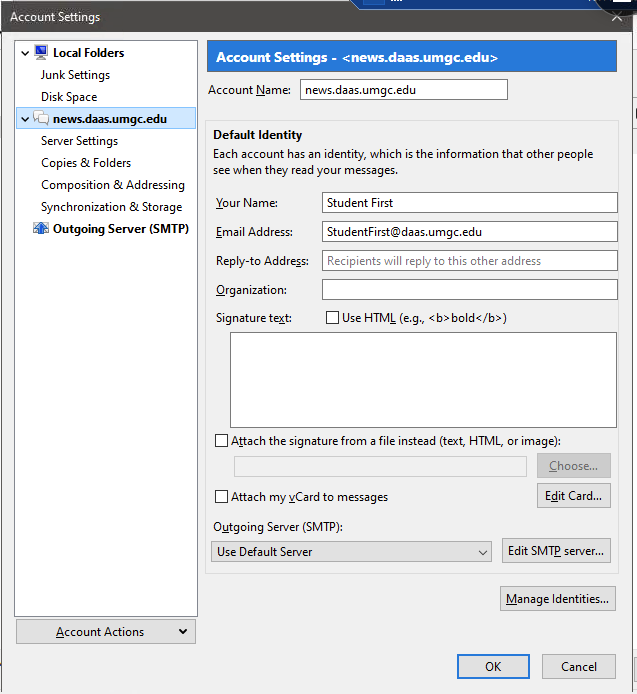
****

**Part 3: Using Mozilla Thunderbird Email Application**

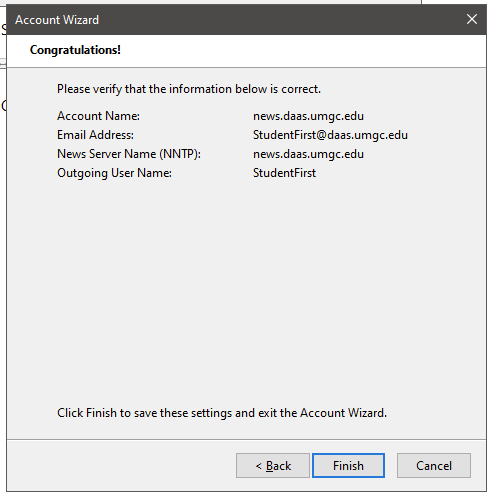
1. **Setting Up a new account within Mozilla Thunderbird**

****

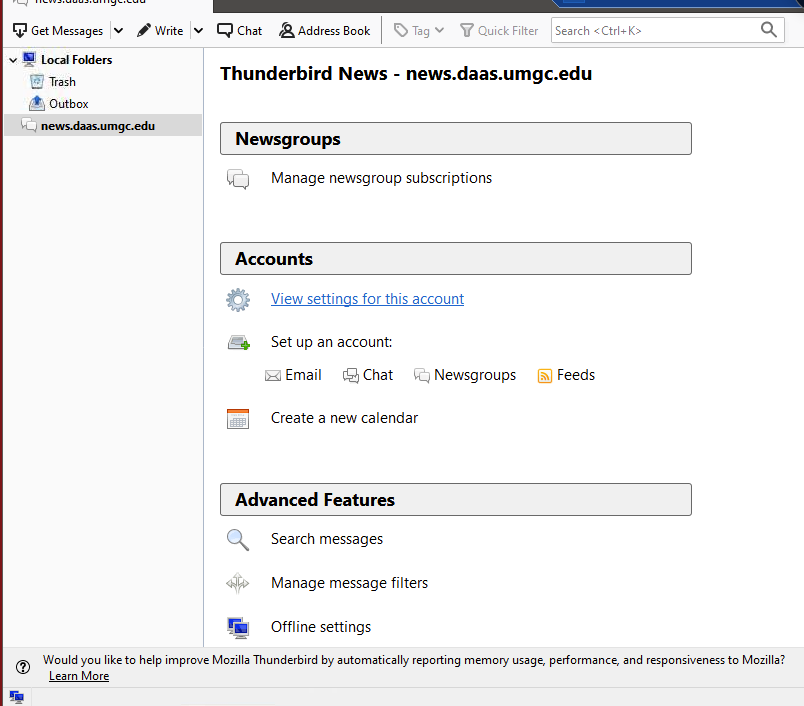
1. **Editing Newsgroup Settings**

****

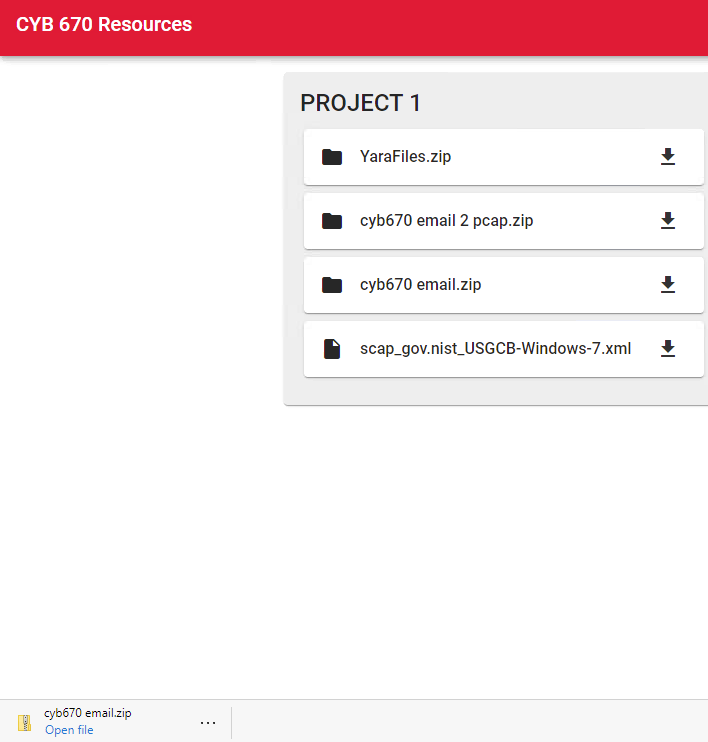
1. **Confirming New Newsgroup Settings**

****

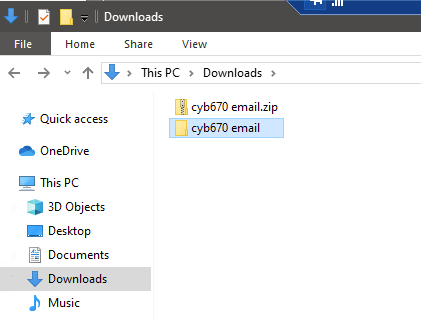
1. **Viewing news.daas.umgc.edu newsgroup**

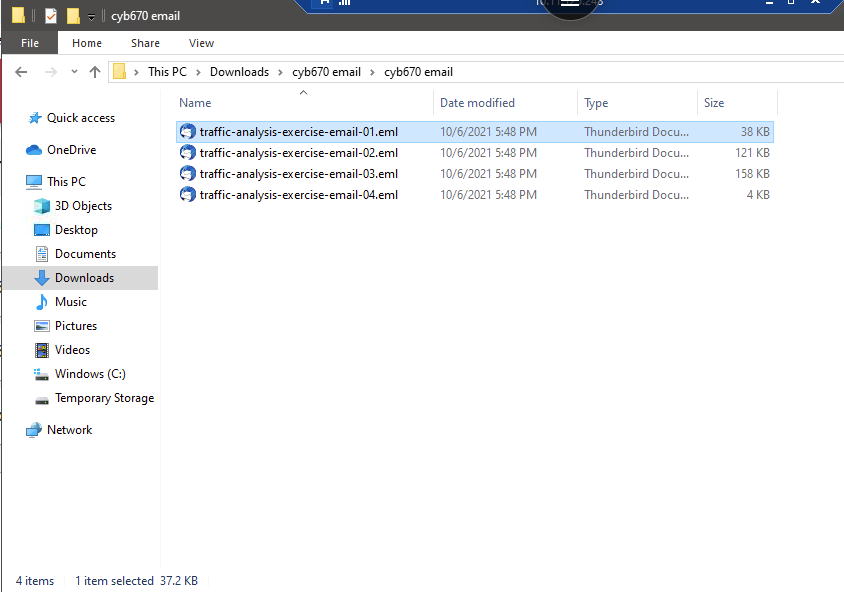
****

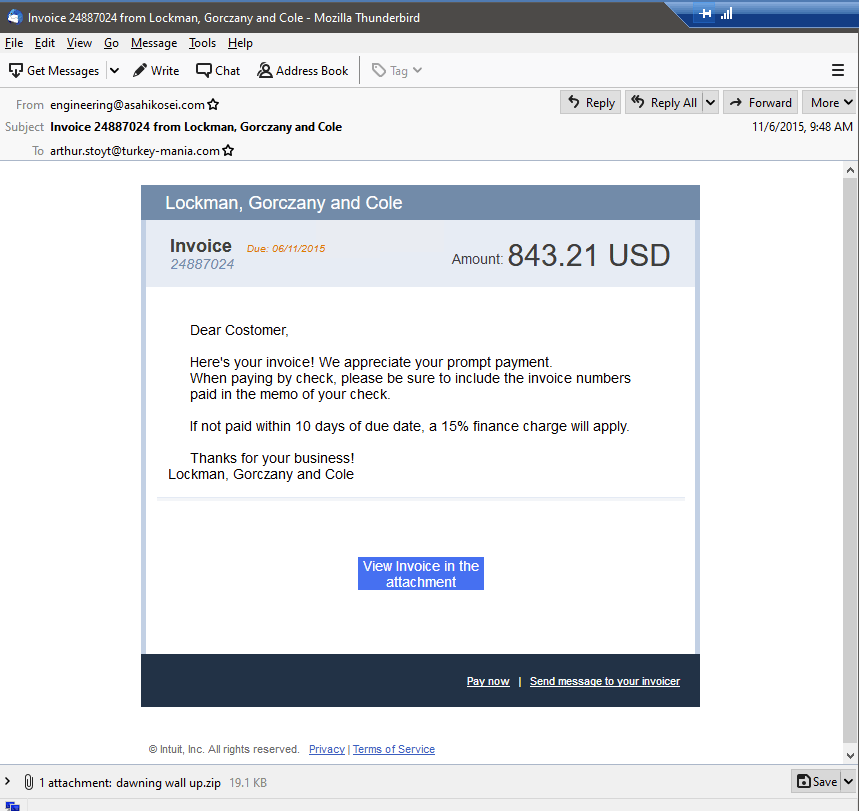
1. **Downloading cyb670email.zip file from resources page**

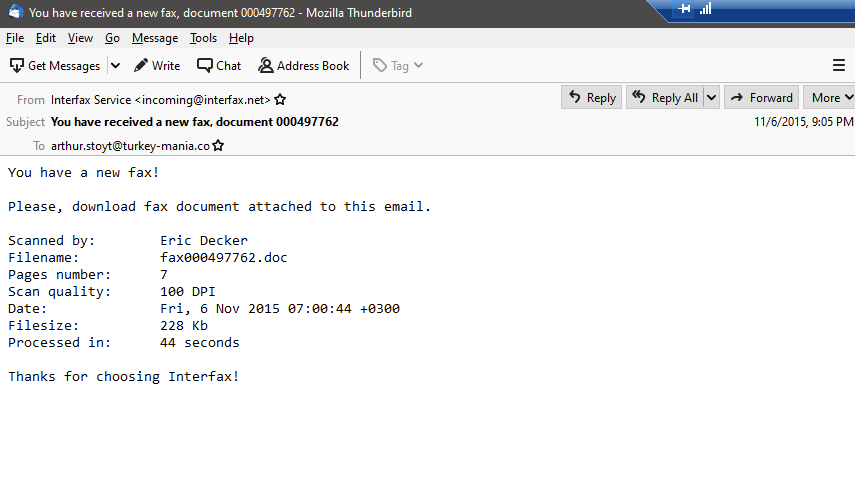
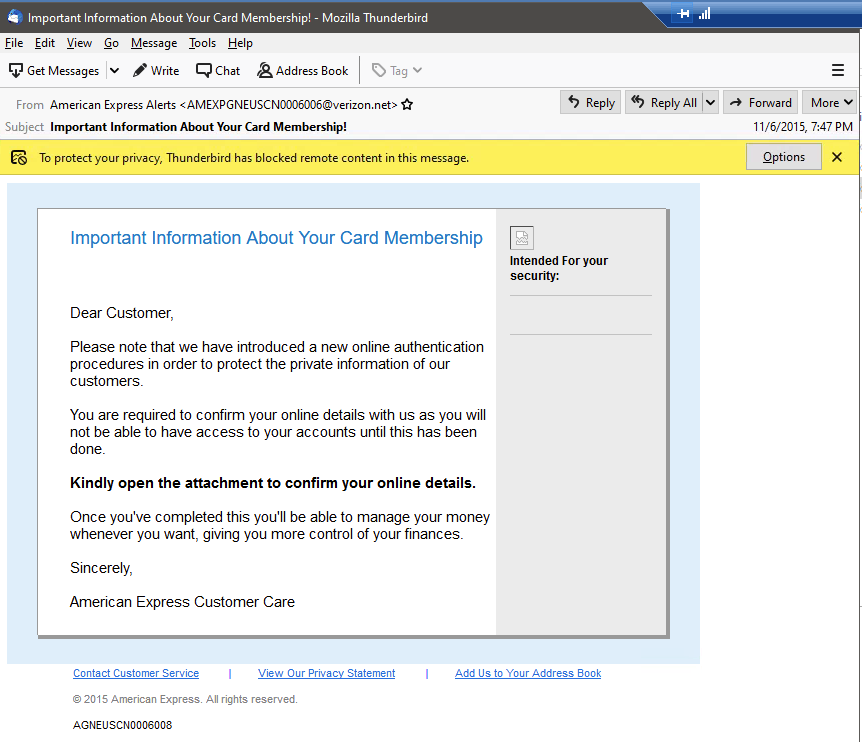
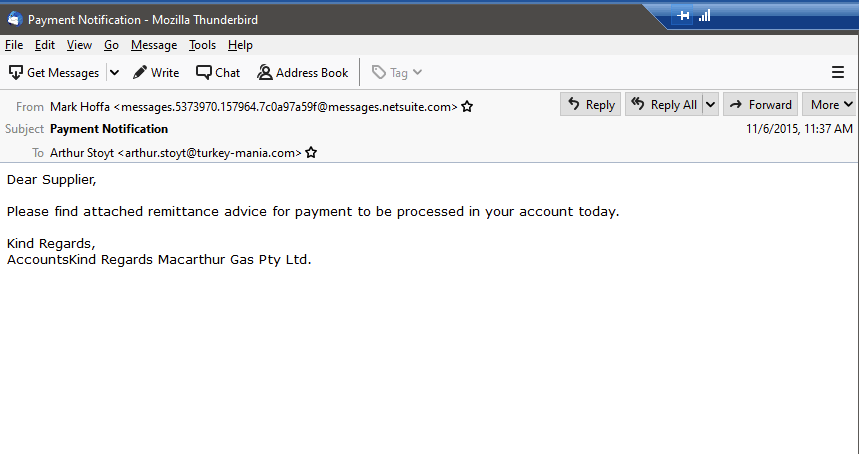
****

1. **Both Zipped and Unzipped versions of cyb670email.zip files downloaded**

****

1. **Viewing contents of unzipped cyb670 email file**
2. **Using Mozilla Thunderbird to open attachments from cyb670email.zip file**

****

****