**ISEC 500 - Information Security Overview**

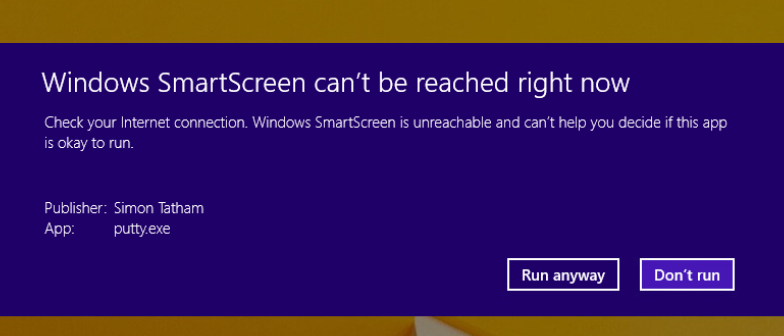
**Assignment 10 – Lab 8: Pentesting and Understanding Vulnerabilities - Incident Response**

The requirements for this lab are to capture the screenshot of the below steps from given sections and submit in the word document.

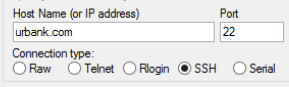
**Part 1**

**PROVISIONING THE VIRTUAL ENVIRONMENT**

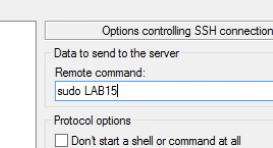
* **step 4**



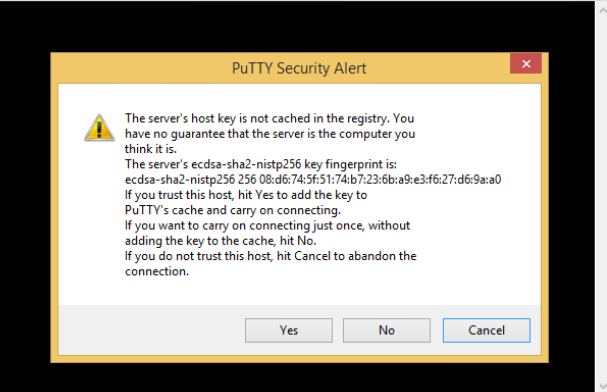
* **step 5**



* **step 6**



* **STEP 7**

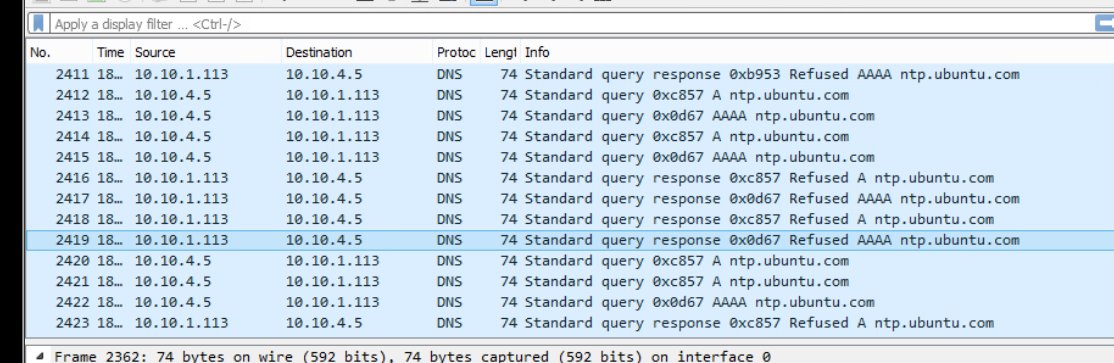


* **STEP 8**

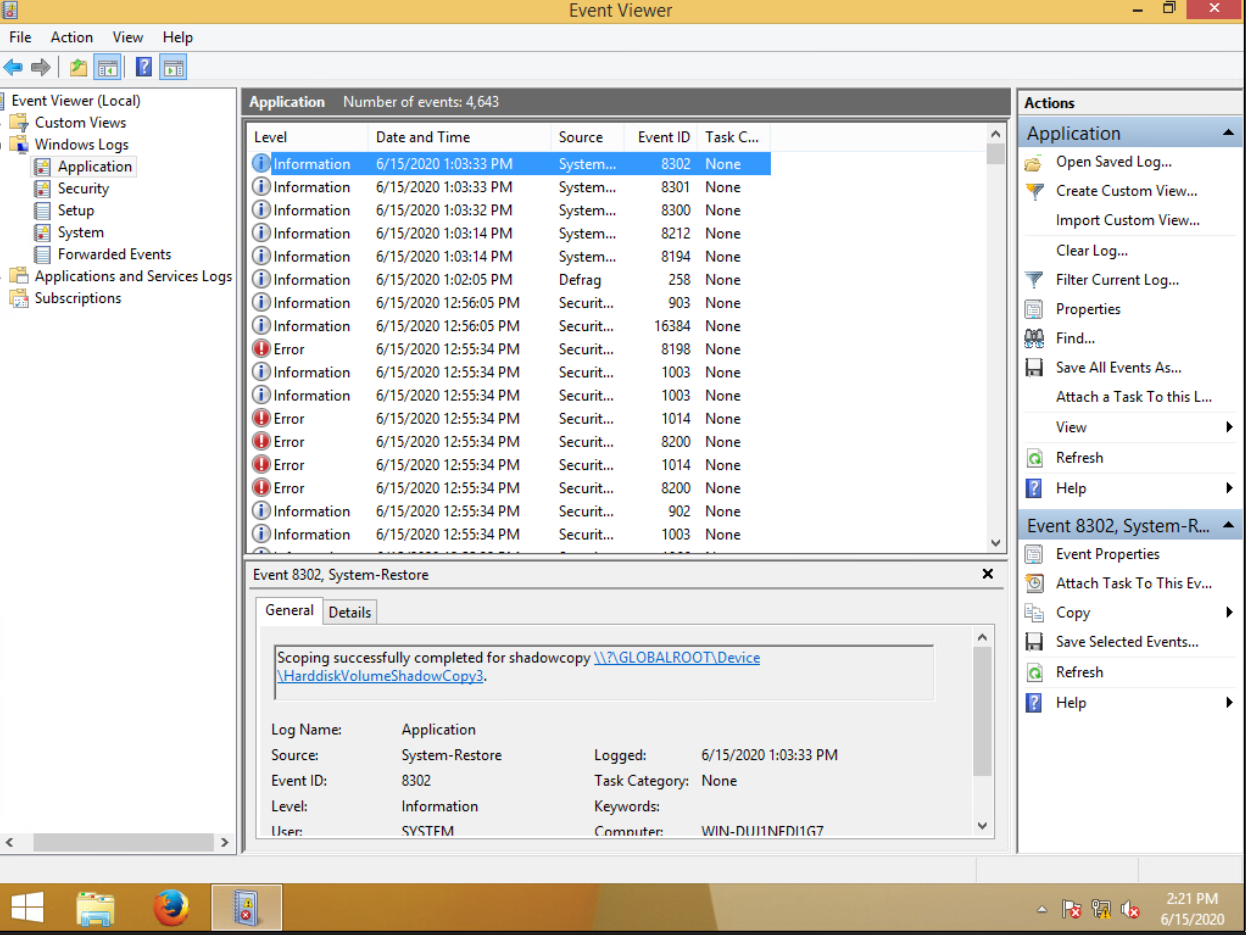


**PART 2**

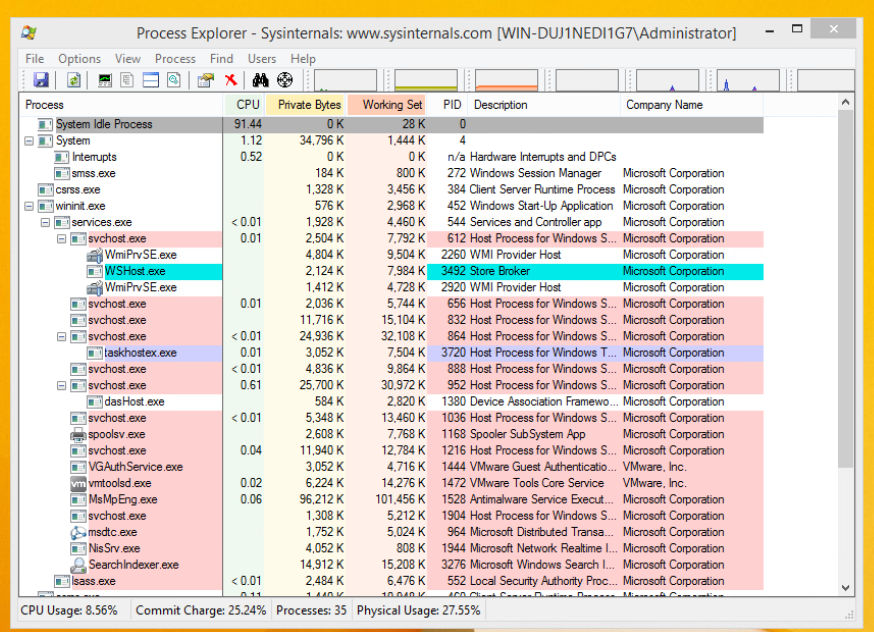
There is network activity. But activity doesn’t mean abnormal activity. We need to look for abnormal activity.



System Logs are being kept. Which gives us data to analyze the computer for abnormal activity.



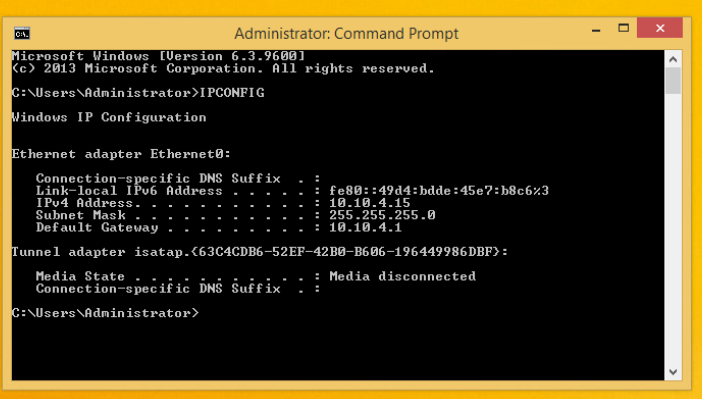
We can also see the processes in the computer using the process explorer.



We can use different types of logs such as process logs, system logs, and network logs for performing event correlation.

As we can see in the network activity, there is NTP traffic. Which is a clock synchronization protocol. It will keep the clocks synchronized.

We can also see our own network details using the ipconfig command.



Then we can use the ping command to test external addresses.

