Securing the Network with an Intrusion Detection System—IDS

Learning Objectives

In this lab, you will configure **Snort**, an open-source **intrusion prevention and detection system**, on the TargetIDS virtual machine and a Web-based IDS monitoring tool called Snorby. You also will use the **Nessus scanning tool** to scan the TargetIDS virtual machine to test the Snort configuration and see exactly what circumstances trigger an IDS alert.

Tools and Software

• Snort

• Snorby

• Nessus

• vi editor

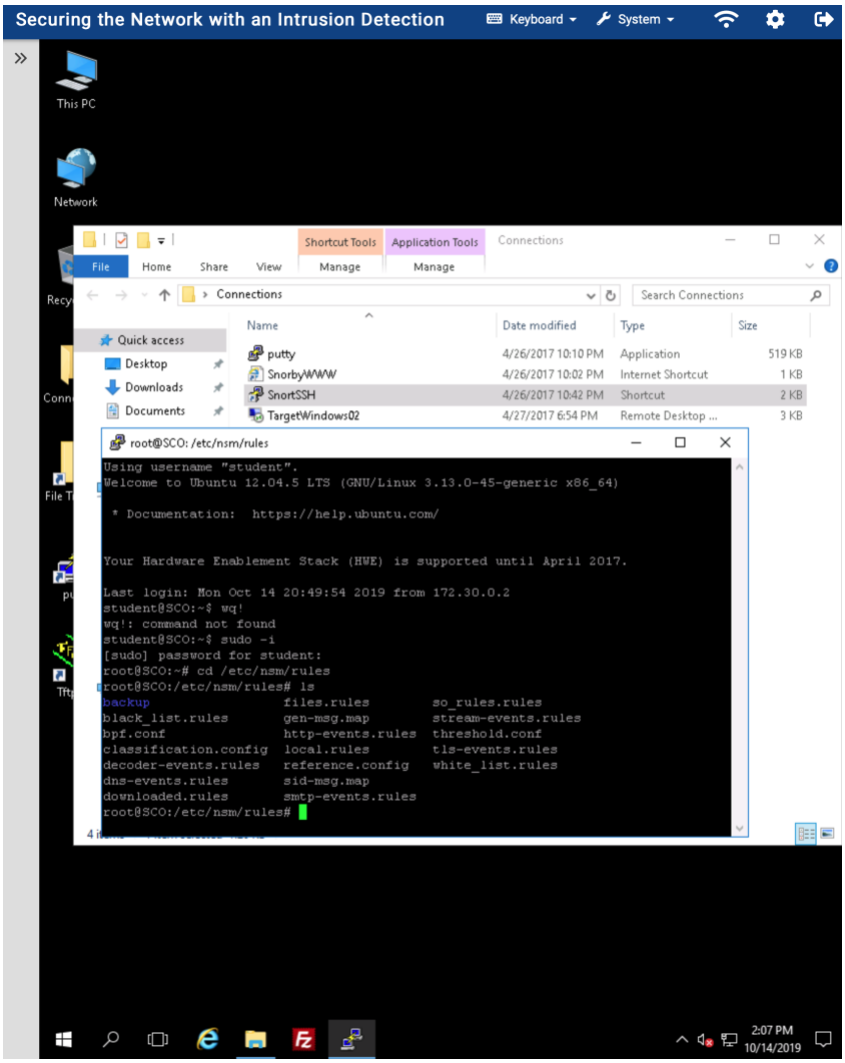
Lab Deliverables

❖ Part 1: Configure an Intrusion Detection System—IDS

1. Intrusion detection is the process of detecting potential misuse or attacks and the ability to respond based on the alert that is provided.

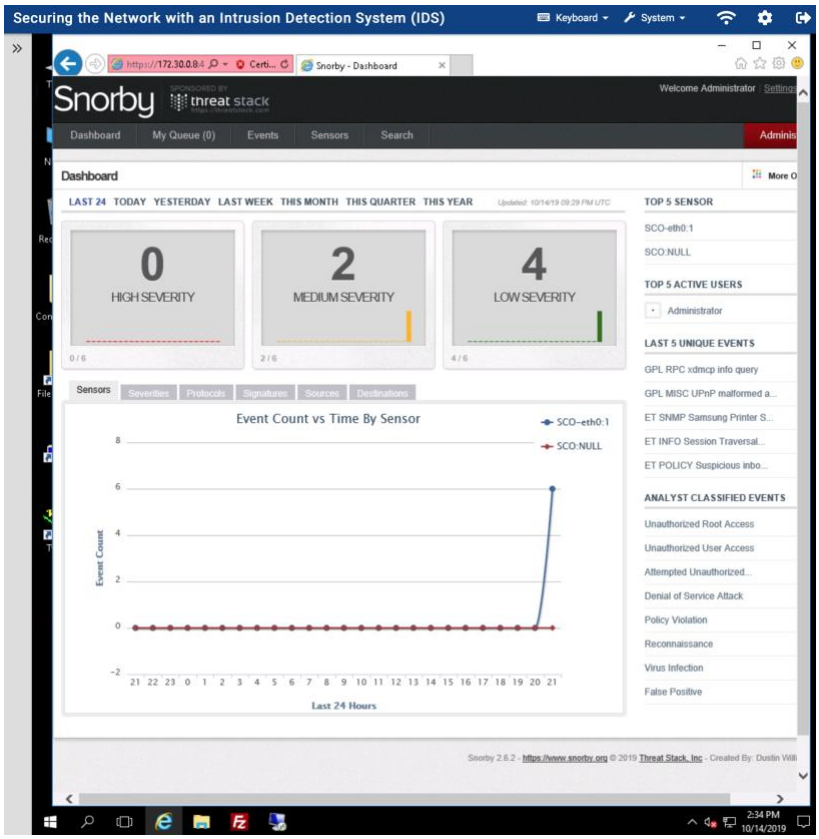
2. Best practice in a network environment is to have host-based intrusion detection systems enabled on critical servers and workstations to provide your network and security organization with real-time alerts and alarms pertaining to potential system compromise and/or unauthorized access.

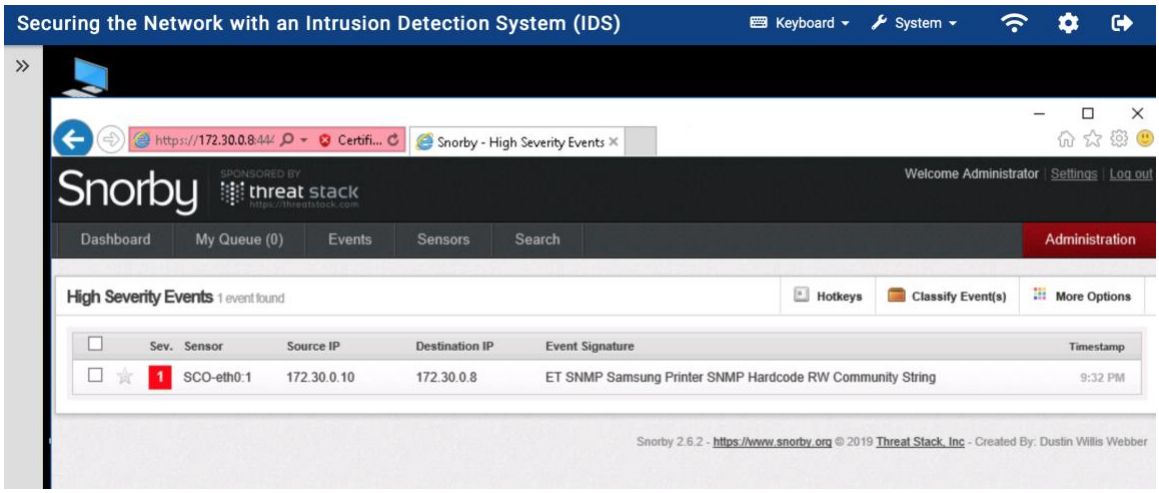
3. **Step: #14**



❖ Part 3: View the Scan Results

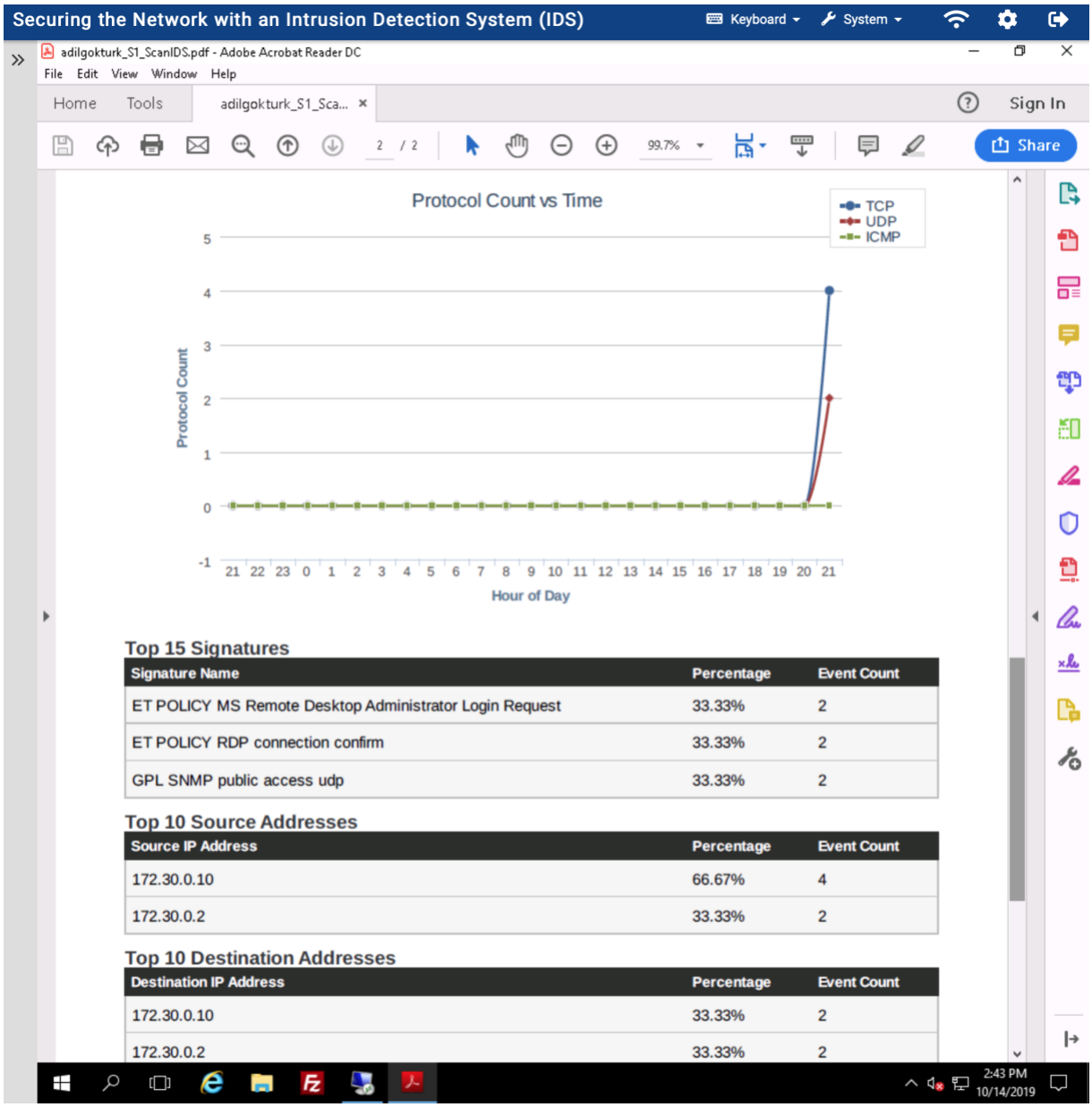
1. Steps: #3





❖ Part 3: Top 15 Signatures

1. Steps: #13



❖ Part 4: Challenge Questions

1. **Discuss the trade-offs (i.e., pros and cons) between the signature-based and anomaly-based IDS approaches. (in 300 words).**

   - Signature-based IDS works like antivirus scanners. Almost all of the malicious behaviors or traffics from the previous attacks or detection experiences are well-known and recorded. The Signature-based IDS easily detects and red-flags the malicious activity. The accuracy of Signature-based IDS is pretty high and its false positive rate is pretty low. However, there is some limitation regarding new methods or pattern those actually haven't been recorded or recognized/defined by the Signature-based IDS, which means that the new attack attempt will not be detected by the Signature-based IDS.
   - In order to detect these new attacks, **anomaly-based IDS approach** would be a better solution than the Signature-based IDS. Anomaly-based IDS analyze current activity of the system and compare it with baseline that already defined in the system. If the anomaly-based IDS detects any unusual activity, which is different than the normal pattern as an outlier, anomaly-based IDS red-flags the activity. However, there is also some limitation on this

approach. The reg-flagged, unusual activity could be either malicious activity or a non-malicious normal activity which is totally new and unclassified or unknown by the anomaly-based IDS, which normal activity could be detected as a malicious activity which is a false signal. Significant number of false signals would be a serious problem for the system administration, which is the major tradeoff between the signature-based and anomaly-based IDS approaches.

2. Discuss at least three limitations in Snort (in 100 words each).

1. SNORT is a Signature-based IDS which works like antivirus scanners. SNORT could easily detect and red flags the malicious activity. The accuracy of SNORT as a Signature-based IDS is pretty high and its false positive rate is pretty low. However, one of its limitation is unrecognized or unrecorded new methods or pattern which are actually haven't been recorded or recognized/defined by the IDS yet.

2. SNORT needs some time to maximize its usefulness. It takes at least 12 months to train itself to detect intrusion as a trained operator and it takes 24-36 months to become an "expert" intrusion detection system.

3. SNORT also requires an experienced network operator/manager who should collect necessary information to make decision without asking clients what to do regarding new trends, traffic and patterns.