**Name:** Hemant Jain

**Lab Progress Report Due Date:** 04/12/2021

**Current Week Since Start Date:** Week 12 (04/14/2021– 04/20/2021)

**Reporting Week:** From Apr 06, 2021 to Apr 12, 2021

**Summary about the Test Out Module-12 Learning:**

From the Test Out LabSim, I learnt about Incident Response, Forensics and Recovery. It all started with the brief discussion about the Security Incident, Incident Response Processes.

Security Incident was defined as an event or series of events that are a result of a security policy violation. Incident Response is the action taken to stop the incident in process, collect all data and implement appropriate solution.

Discussed about the attack frameworks MITRE ATT@CK, Diamond Model of Intrusion Analysis, Cyber Kill Chain. Discussing about the stakeholder management and the high-level open-ended discussions for the internal Policies in Communication planning, disaster recovery planning, business continuity planning, and incident response team charter. Learnt about the distinguishing factors between whitelisting and blacklisting applications. Using the isolation, quarantine, containment, and segmentation appropriately.

Creating a runbook for a network and identify the various scenarios where to use the playbooks and runbooks.

Endpoint Security Configuration tools like Firewall rules, Mobile device management(MDM)< Data monitoring apps, content filters, URL filters, certificate status databases.

In detail discussion about he three important pillars isolation, containment and segmentation.

Security Orchestration, Automation and Response (SOAR), and the incident plans namely runbooks and playbooks.

Learnt what does the Security Information and event management (SIEM) does and is used for. What are the important trends for network management? Demonstrated the use of vulnerability scan outputs as part of SIEM. Identifying the trends and use them appropriately and identify uses of SIEM. SIEM components which combining contributes towards the complete architecture likely Vulnerability scan output, SIEM dashboards, Sensors, Sensitivity, Trends, Alerts, Correlation. Read about the bandwidth monitors, metadata, and data analyzers likely NetFlow, sFlow, IPfix.

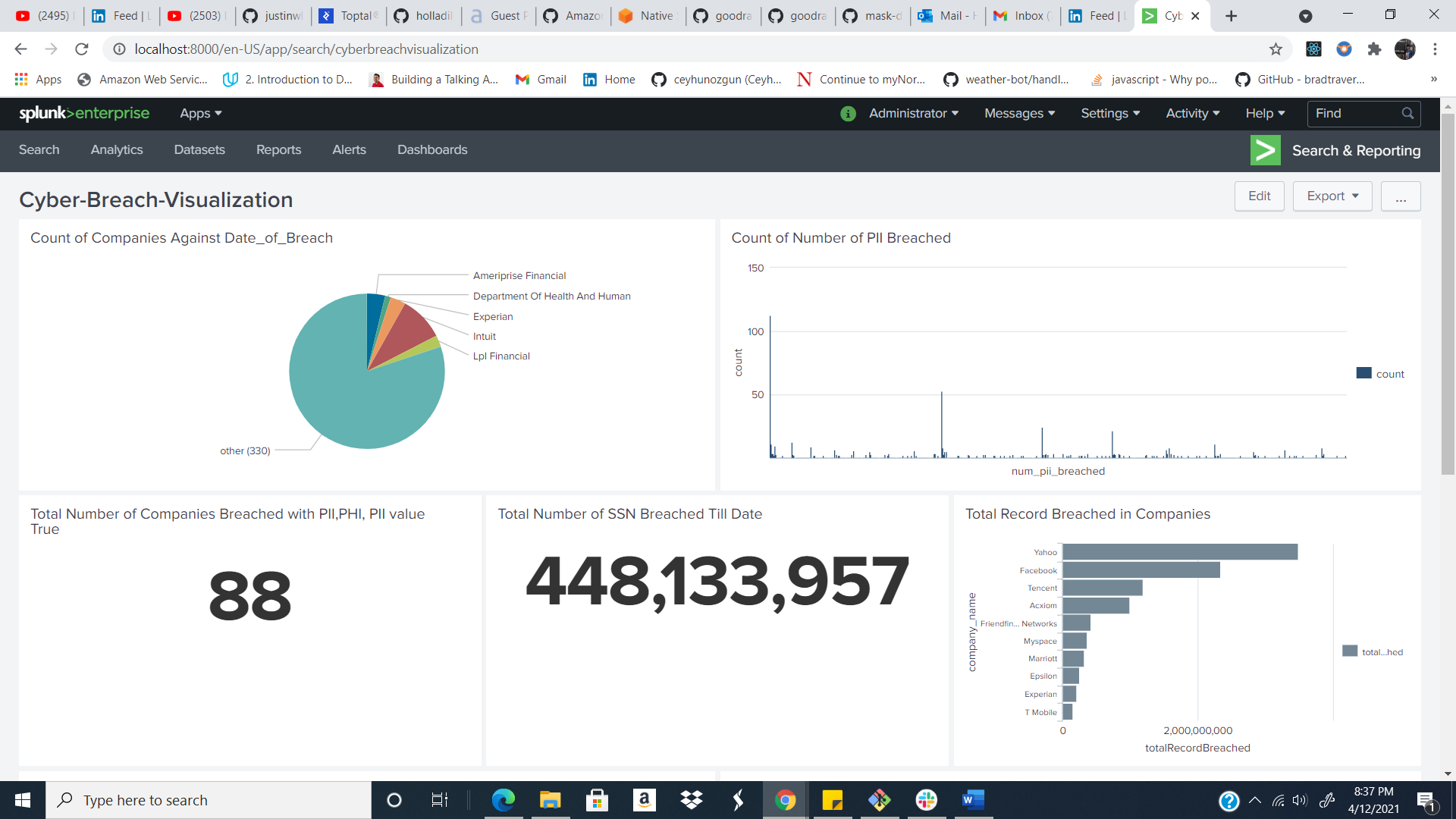
Performed the lab on the configuration of collector-initiated subscriptions, configuring source initiated subscriptions, log events with event viewer. Processes needs to be aware about while implementing the event forwarding and subscriptions. The event-subscription configurations likely Source-initiated subscription, subscription configuration, type of service account, event saving , filters, runtime status.

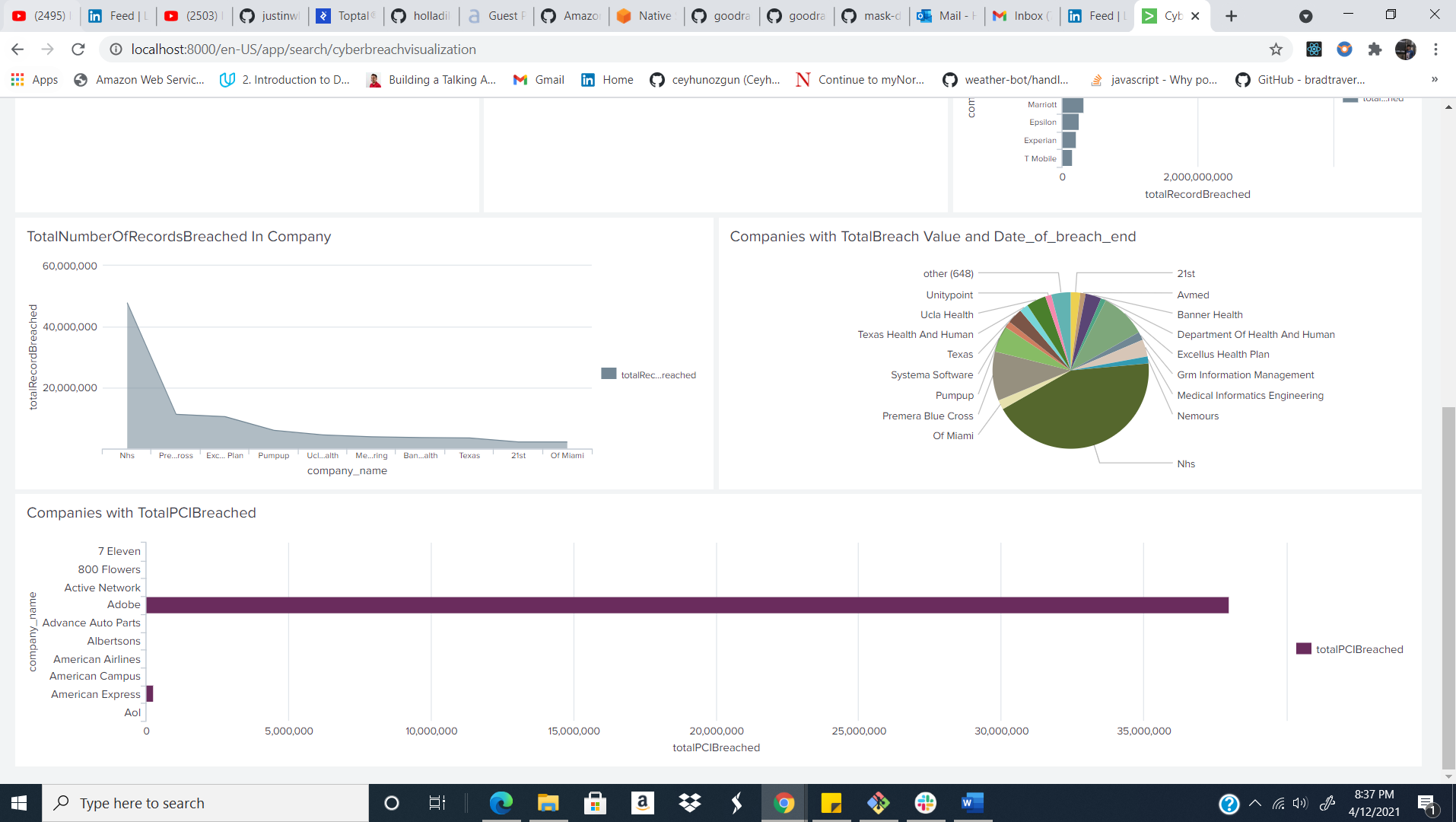
Learnt how to create a forensic drive image with FTK, Guymager and DC3DD and examining a forensic drive image with Autopsy. Learnt how to use TCPDump to capture packet data, Using wireshark to capture network protocol information, Using the TCPReplay to analyze attacks, using the shells and scripting for programming and remote connection, using the Linux commands and utilities, using a logging activity to manipulate and add information to log files.

In-detail description about the SSH(Secure Shell), OpenSSL, Scripting environments. Read about the packet capturing, switched network sniffing , wireshark, tcpdump, tcpreplay and additional sniffing tools.

**Splunk Dashboard Screenshots:**

**Find the PDF of the Splunk Analysis enclosed in the Zip File:**





**Progress Embedded Image of Progress Report from LabSim:**

