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,

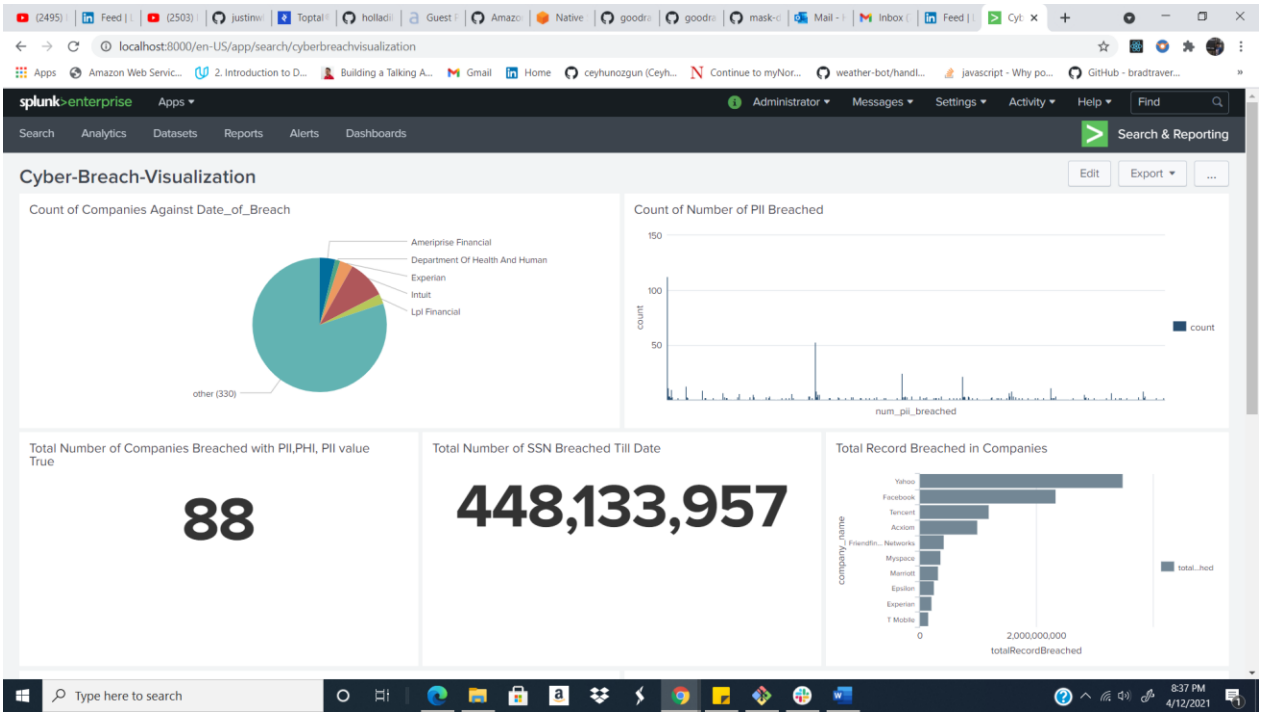
Trends, Alerts, Correlation. Read about the bandwidth monitors, metadata, and data analyzers likely NetFlow, sFlow, IPfix.
Performed the lab on the configuration of collector-initiated subscriptions, configuring source initiated subscriptions, log events with event viewer. Processes needs to be aware 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.

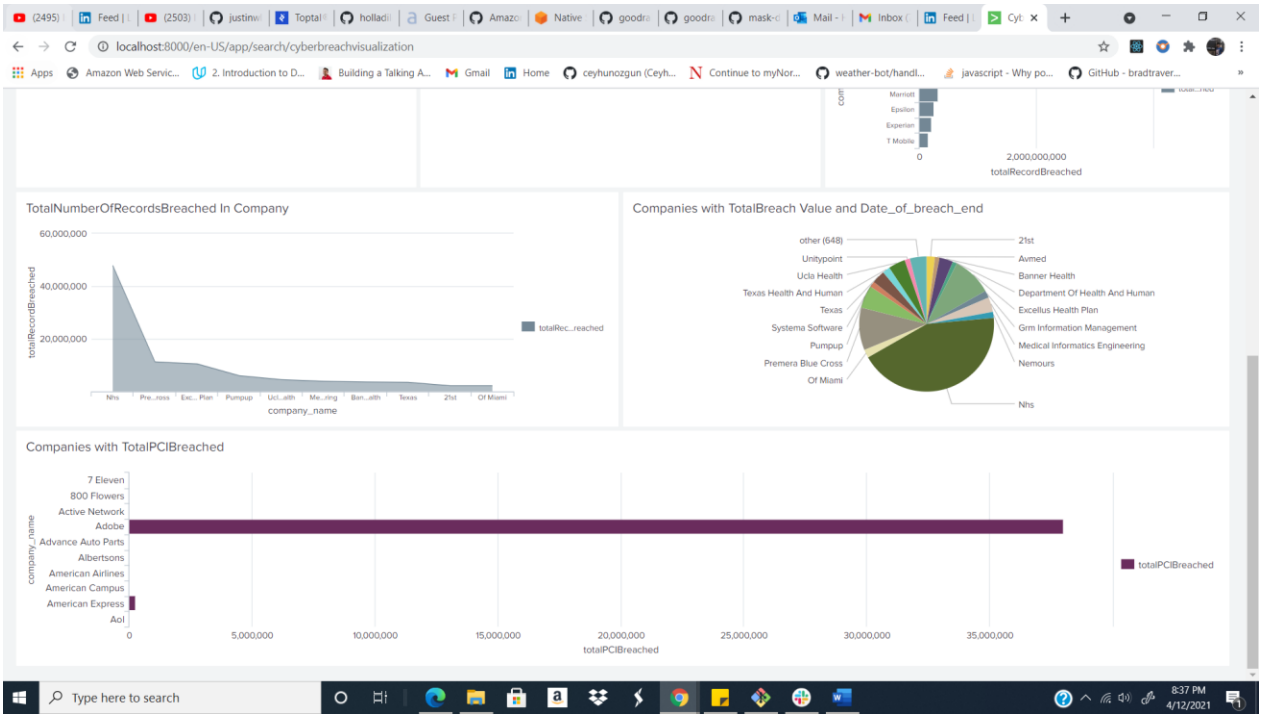
Learnt how to create a forensic drive image with FTK, Guymager and DC3DD and examining a forensic drive image with Autopsy. Learnt how to use TCPDump to capture packet data, Using wireshark to capture network protocol information, Using the TCPReplay to analyze attacks, using the shells and scripting 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.

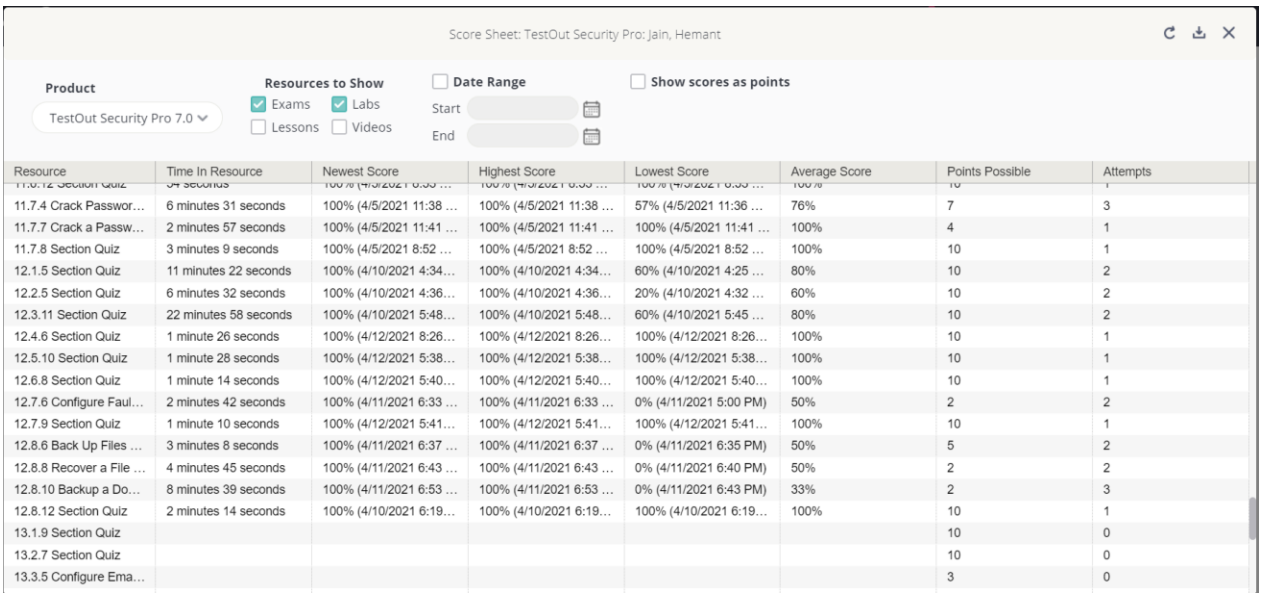
Splunk Dashboard Screenshots:

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


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Cyber-Breach-Visualization
Edit
Export
Count of Companies Against Date_of_Breach
Ameriprise Financial
Department Of Health And Human
Experian
Intuit
Lpl Financial
other (330)
Count of Number of PII Breached
150
100
50
count
num_pii_breached
Total Number of Companies Breached with PII,PHI, PII value True
88
Total Number of SSN Breached Till Date
448,133,957
Total Record Breached in Companies
Yahoo
Facebook
Tencent
Acxiom
Myspace
Marriott
Epsilon
Experian
T Mobile
company_name
0
2,000,000,000
totalRecordBreached
Type here to search
8:37 PM
4/12/2021


localhost:8000/en-US/app/search/cyberbreachvisualization
Marriott
Epsilon
Experian
T Mobile
0
2,000,000,000
totalRecordBreached
TotalNumberOfRecordsBreached In Company
60,000,000
40,000,000
20,000,000
totalRecordBreached
totalRec...reached
company_name
Companies with TotalBreach Value and Date_of_breach_end
other (648)
Unitypoint
Ucla Health
Texas Health And Human
Texas
Systema Software
Pumpup
Premera Blue Cross
Of Miami
21st
Avmed
Banner Health
Department Of Health And Human
Excellus Health Plan
Grm Information Management
Medical Informatics Engineering
Nemours
Nhs
Companies with TotalPCIBreached
7 Eleven
800 Flowers
Active Network
Adobe
Advance Auto Parts
Albertsons
American Airlines
American Campus
American Express
Aol
company_name
0
5,000,000
10,000,000
15,000,000
20,000,000
25,000,000
30,000,000
35,000,000
totalPCIBreached
totalPCIBreached
Type here to search
8:37 PM
4/12/2021

Progress Embedded Image of Progress Report from LabSim:



Score Sheet: TestOut Security Pro: Jain, Hemant

Product: TestOut Security Pro 7.0

Resources to Show: Exams, Labs, Lessons, Videos

Date Range: Start, End

Show scores as points

Resource	Time In Resource	Newest Score	Highest Score	Lowest Score	Average Score	Points Possible	Attempts
11.7.4 Crack Passwor…	6 minutes 31 seconds	100% (4/5/2021 11:38 …	100% (4/5/2021 11:38 …	57% (4/5/2021 11:36 …	76%	7	3
11.7.7 Crack a Passw…	2 minutes 57 seconds	100% (4/5/2021 11:41 …	100% (4/5/2021 11:41 …	100% (4/5/2021 11:41 …	100%	4	1
11.7.8 Section Quiz	3 minutes 9 seconds	100% (4/5/2021 8:52 …	100% (4/5/2021 8:52 …	100% (4/5/2021 8:52 …	100%	10	1
12.1.5 Section Quiz	11 minutes 22 seconds	100% (4/10/2021 4:34…	100% (4/10/2021 4:34…	60% (4/10/2021 4:25 …	80%	10	2
12.2.5 Section Quiz	6 minutes 32 seconds	100% (4/10/2021 4:36…	100% (4/10/2021 4:36…	20% (4/10/2021 4:32 …	60%	10	2
12.3.11 Section Quiz	22 minutes 58 seconds	100% (4/10/2021 5:48…	100% (4/10/2021 5:48…	60% (4/10/2021 5:45 …	80%	10	2
12.4.6 Section Quiz	1 minute 26 seconds	100% (4/12/2021 8:26…	100% (4/12/2021 8:26…	100% (4/12/2021 8:26…	100%	10	1
12.5.10 Section Quiz	1 minute 28 seconds	100% (4/12/2021 5:38…	100% (4/12/2021 5:38…	100% (4/12/2021 5:38…	100%	10	1
12.6.8 Section Quiz	1 minute 14 seconds	100% (4/12/2021 5:40…	100% (4/12/2021 5:40…	100% (4/12/2021 5:40…	100%	10	1
12.7.6 Configure Faul…	2 minutes 42 seconds	100% (4/11/2021 6:33 …	100% (4/11/2021 6:33 …	0% (4/11/2021 5:00 PM)	50%	2	2
12.7.9 Section Quiz	1 minute 10 seconds	100% (4/12/2021 5:41…	100% (4/12/2021 5:41…	100% (4/12/2021 5:41…	100%	10	1
12.8.6 Back Up Files …	3 minutes 8 seconds	100% (4/11/2021 6:37 …	100% (4/11/2021 6:37 …	0% (4/11/2021 6:35 PM)	50%	5	2
12.8.8 Recover a File …	4 minutes 45 seconds	100% (4/11/2021 6:43 …	100% (4/11/2021 6:43 …	0% (4/11/2021 6:40 PM)	50%	2	2
12.8.10 Backup a Do…	8 minutes 39 seconds	100% (4/11/2021 6:53 …	100% (4/11/2021 6:53 …	0% (4/11/2021 6:43 PM)	33%	2	3
12.8.12 Section Quiz	2 minutes 14 seconds	100% (4/10/2021 6:19…	100% (4/10/2021 6:19…	100% (4/10/2021 6:19…	100%	10	1
13.1.9 Section Quiz						10	0
13.2.7 Section Quiz						10	0
13.3.5 Configure Ema…						3	0