Week 3 Splunk Questions - Solution

Key knowledge/skills: common attributes selection & Splunk SPL commands

Exercise 1. Add netw m_2500.csv” in Splunk, and name the index as “tcp_stream_2500”

Q1. Select the comn , they should be able to describe the events in terms of Who, What, Whe app” field is useful in the absence of “protocol”).

Sample answer: app, dest_ip, dest_port, src_ip, src_port, timestamp

Q2. List all the IP addresses that run HTTP over non-standard port (hint: dest_port != 80), with the event counts.

Sample answer:

dest_ip	Count
10.0.1.101	1
10.0.1.120	64
10.0.2.101	2
10.0.2.105	2
10.0.2.108	2

Sample SPL command: index= tcp_stream_2500 earliest=0 app=http dest_port!=80 | chart count by dest_ip

Q3. What’s the Skype server IP address?

Sample answer: 13.107.3.128

Sample SPL command: index= tcp_stream_2500 earliest=0 app=skype | dedup dest_ip | table dest_ip

Exercise 2. Add endpoint data “symantec_ep_trafffic_file.csv” in Splunk, and name the index as “symantec_ep_traffic_file”.

Q1. Select the common attributes/fields, they should be able to describe the events in terms of Who, What, Whe[illegible]

Sample answer: acti[illegible]me, Begin_Time, dest_ip, dest_port, End_Time, Host_Name, Netwo[illegible], dest_port, src_ip, src_port, user

Q2. List all the block[illegible]rc_ip, dest_ip, Network_Protocol, and user information.

Sample answer:

src_ip	dst_ip	Network_Protocol	user
10.0.2.101	10.0.1.100	ICMP	amber.turing
10.0.1.101	10.0.1.100	ICMP	administrator
10.0.2.103	10.0.1.100	ICMP	grace.hoppy
10.0.2.107	10.0.1.100	ICMP	billy.tun

Sample SPL command: index=symantec_ep_trafffic_file earliest=0 action=blocked | dedup src_ip | table src_ip, dest_ip, Network_Protocol, user