**SNP – Lab 05**

**Activity 1**

**Use the lab 4 pcap file and answer the questions below**

1. Beside the malware payload what are the other exploits(s) sent by the EK?
   * Application/java-archive
   * Application/x-shockwave-flash
2. How many times was the payload delivered?
   * 3 times
3. Submit the pcap to Virus total and find out what are the EK names are shown in the Suricata alerts?
   * ET CURRENT\_EVENTS GoonEK ET CURRENT\_EVENTS Goon/Infinity URI Struct EK ET CURRENT\_EVENTS RIG EK

**Activity 2**

**Use the pcap file inside the lab 05 to answer these questions**

1. What is the date and time of this activity?
2. What is the IP address of the Windows host that gets infected?
3. What is the MAC address of the infected Windows host?
4. What is the host name of the infected Windows host?
5. What is the domain name of the compromised web site?
6. What is the IP address of the compromised web site?
7. What is the domain name that delivered the exploit kit (EK) and malware payload?
8. What is the IP address that delivered the EK and malware payload?
9. What snorts events are generated by this pcap?
10. What exploit kit is this?
11. How many times was the payload delivered?
12. What browser was used by the infected windows host?
13. What different exploit were sent by the EK during the infection?