Intrusion detection systems are utilized to recognize inconsistencies to get programmers before they harm an organization. They can be either organization or host-based. A host-based interruption recognition framework is introduced on the customer PC, while an organization puts together an interruption discovery framework with respect to the organization. Intrusion detection systems work by one or the other searching for marks of known assaults or deviations from typical movement. These deviations or peculiarities are pushed up the stack and analyzed at the convention and application layer. An IDS might be executed as a product application running on client equipment or as an organization security apparatus. Cloud-based intrusion detection systems are likewise accessible to secure information and frameworks in cloud organizations.

Kibana is an open-source information representation and investigation instrument utilized for log and time-arrangement examination, application checking, and operational knowledge use cases. It offers amazing and simple-to-utilize highlights like histograms, line diagrams, pie outlines, heat maps, and implicit geospatial support. In Project 2, we used Kibana to log data based on our findings from Day 1 of the Red vs Blue Team Project. In this project, we were assigned to play two different roles, a security analyst and a penetration tester. On the Red Team, we were assigned to attack a virtual machine, Capstone, using the Kali Machine. On the Blue Team, we used Kibana to insert and log the data found on Day 1. The following vulnerabilities were found:

* Accessible Files
* Brute Force Passwords
* Port 80

Using the brute force tool on Day 1 on for the Red Team, we were able to obtain secret files in the machine. For accessible files, we were to use the IP addresses located on protocol 80 and from there on, we were able to access the server’s usernames and passwords. Since protocol 80 was open, we were able to access private information on the machine. Using **nmap,** we were able to monitor any vulnerable ports in services in the network. The IP address was located, which had an opened port (80). With the open port, we were able to obtain the accessible files. Hydra is a pre-introduced tool in Kali Linux used to savage power username and secret phrase to various administrations like ftp, ssh, telnet, MS-SQL and so on.With **Hydra,** we were able to access the secret files in the Capstone Machine.