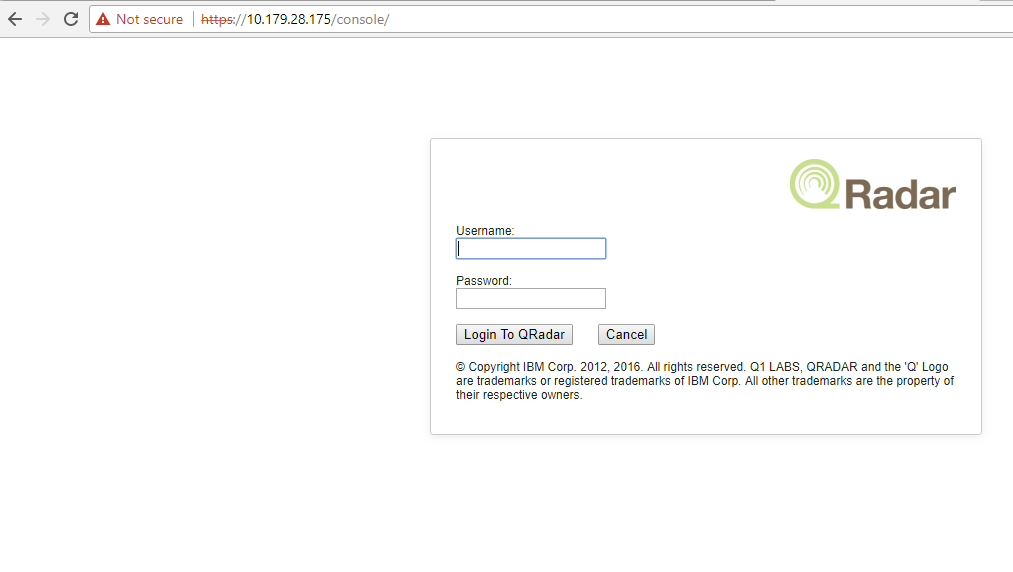
**Case Study Project on QRadar**

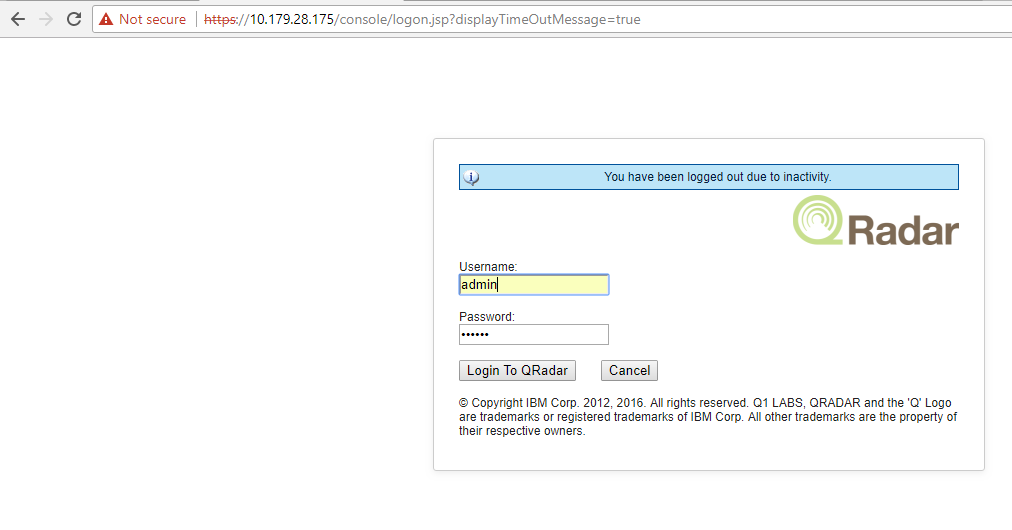
TopGear Project

Step1: Open the web browser and put the URL in search bar and access the QRadar console.

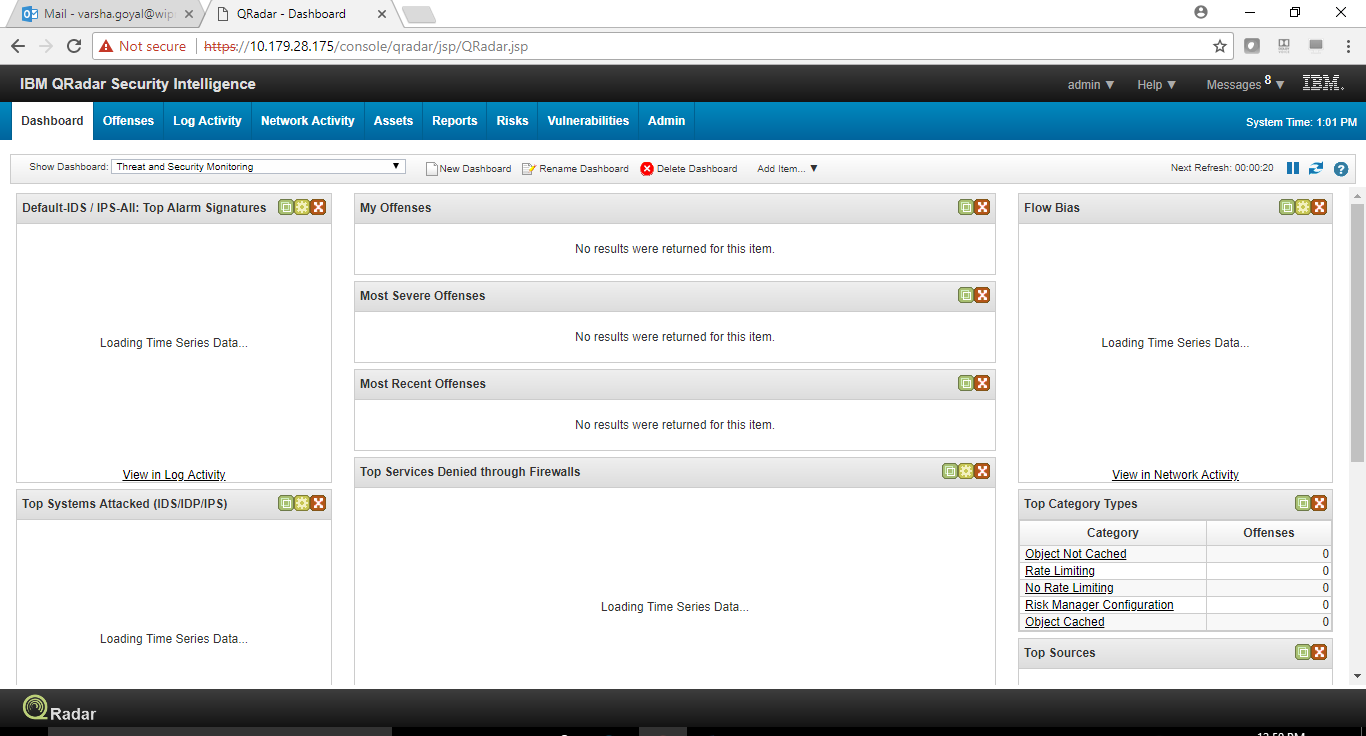
Login page appears.



Put valid login name and password and click on “Login to QRadar”.



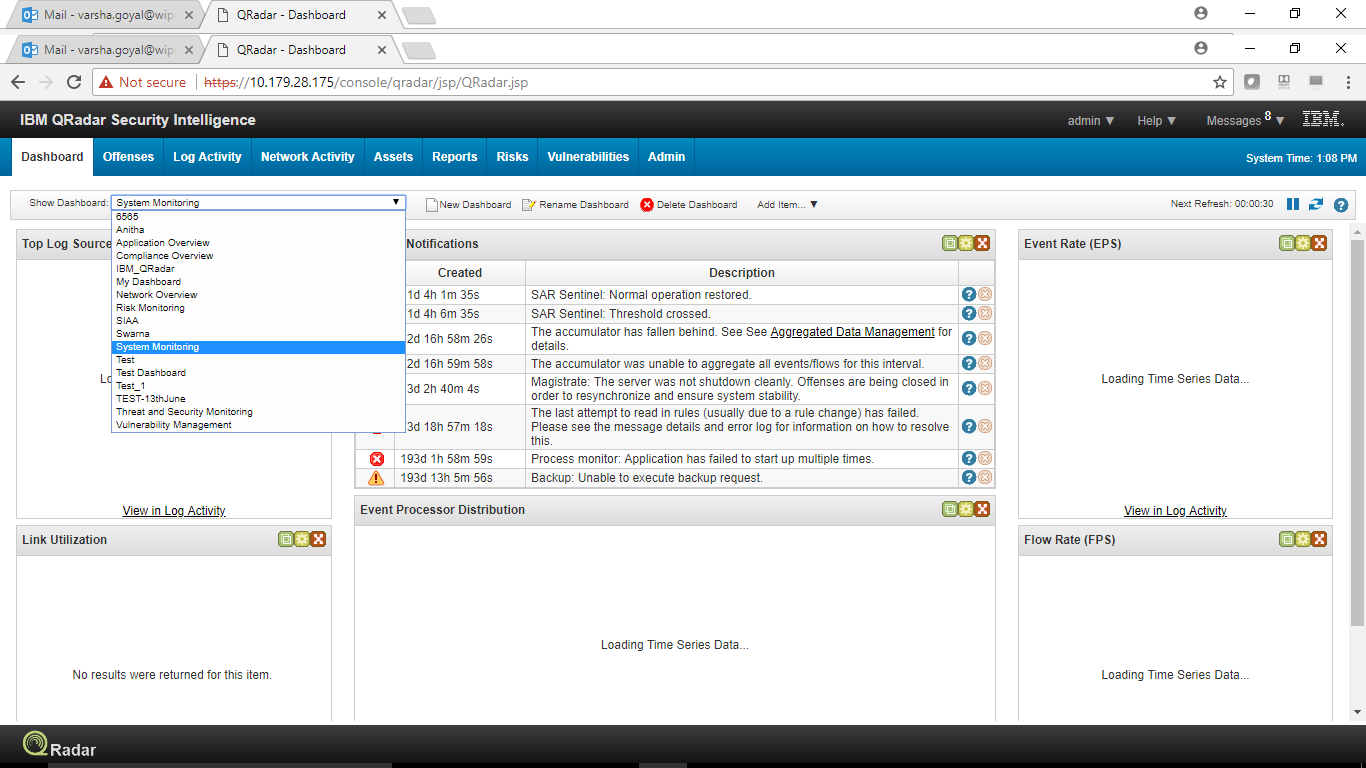
After login, we can see the QRadar console as below-



Step 2:

To see Dashboards menu, click on ‘Dashboard’ tab drop down button.

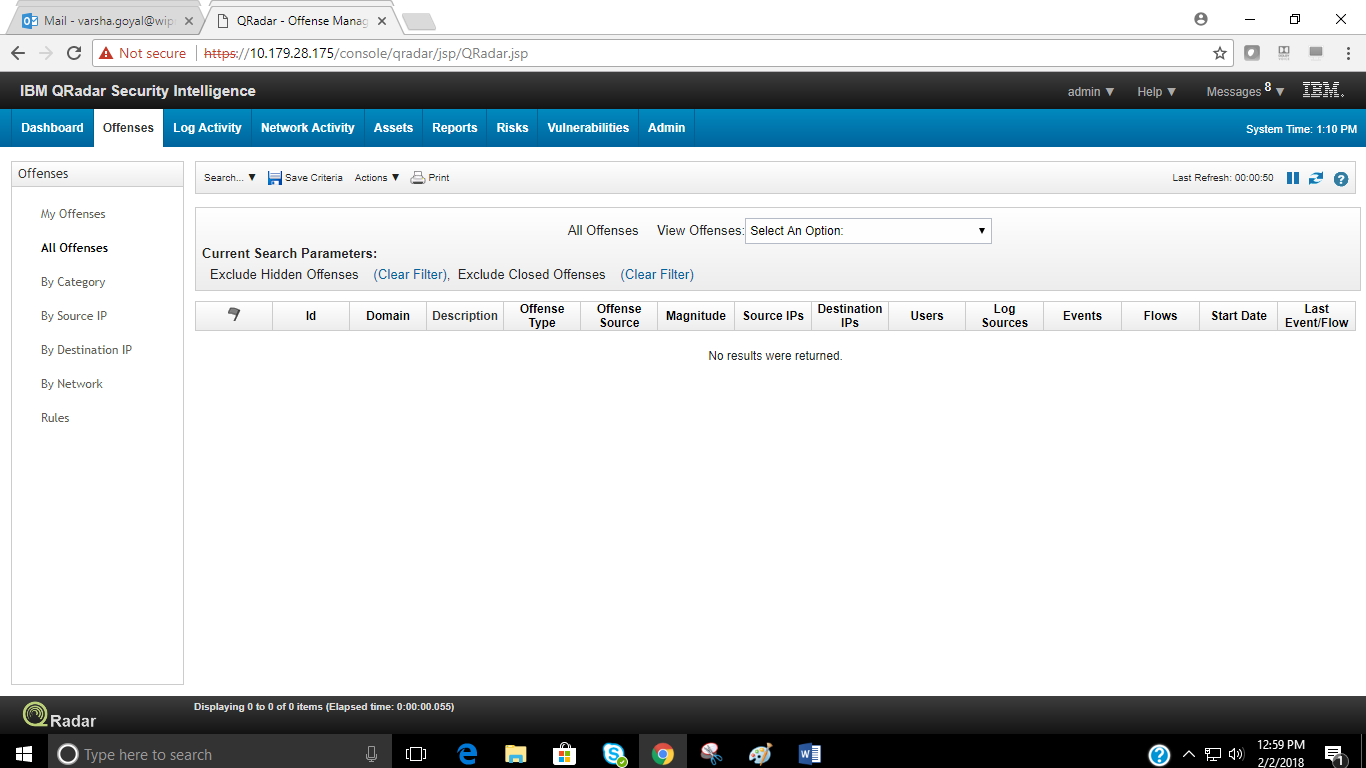
Select any option from drop down Dashboard. E.g. I select ‘System Monitoring’



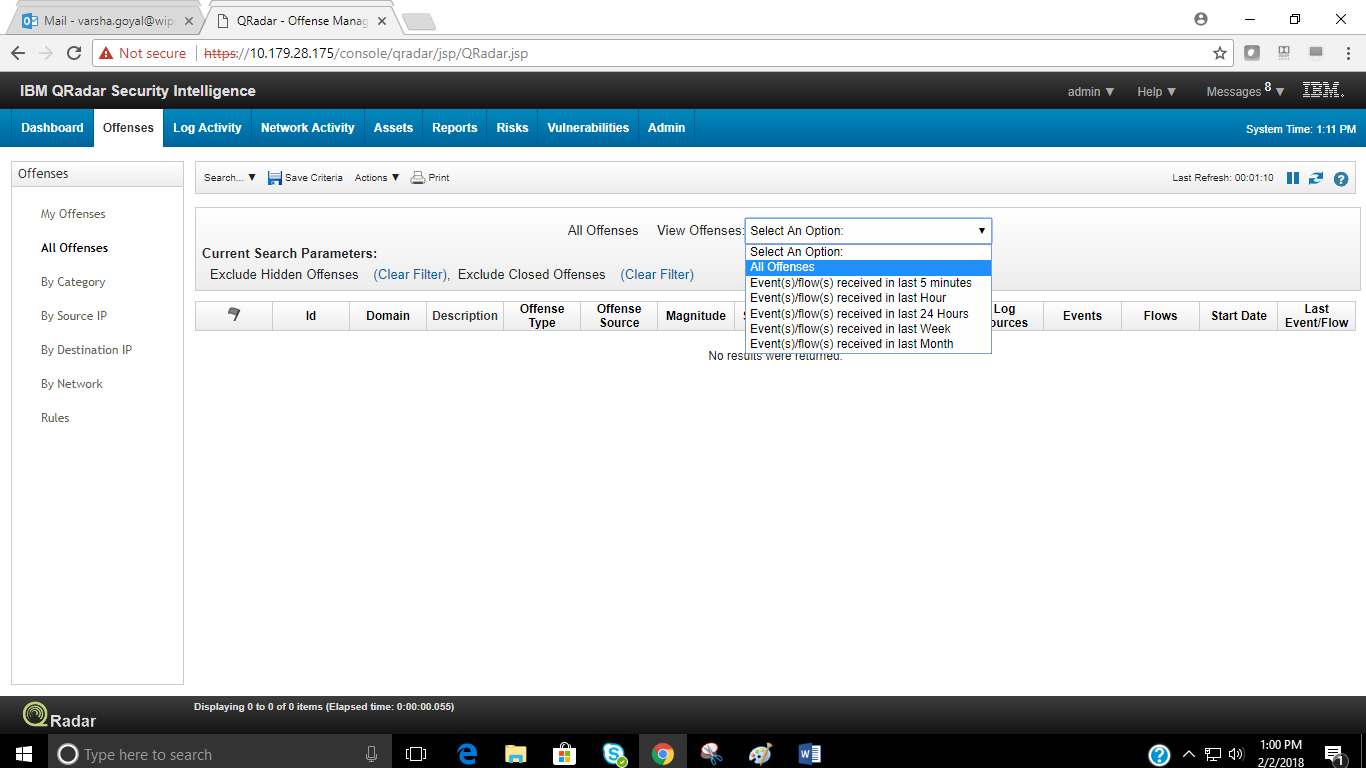
Step 3:

Click on the ‘Offenses’ tab to see offense page.

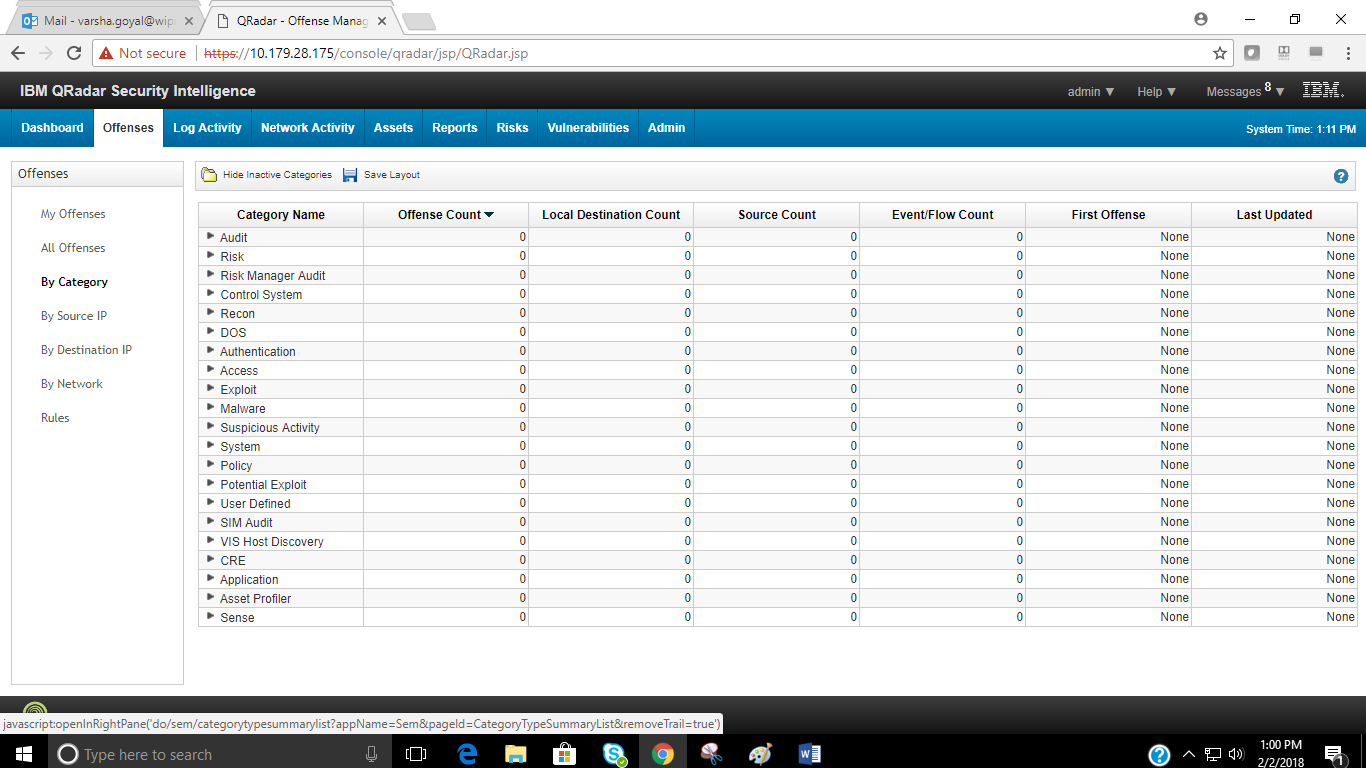
Click on ‘All Offenses’ in the left hand side of offense page to see all generated offenses in console.



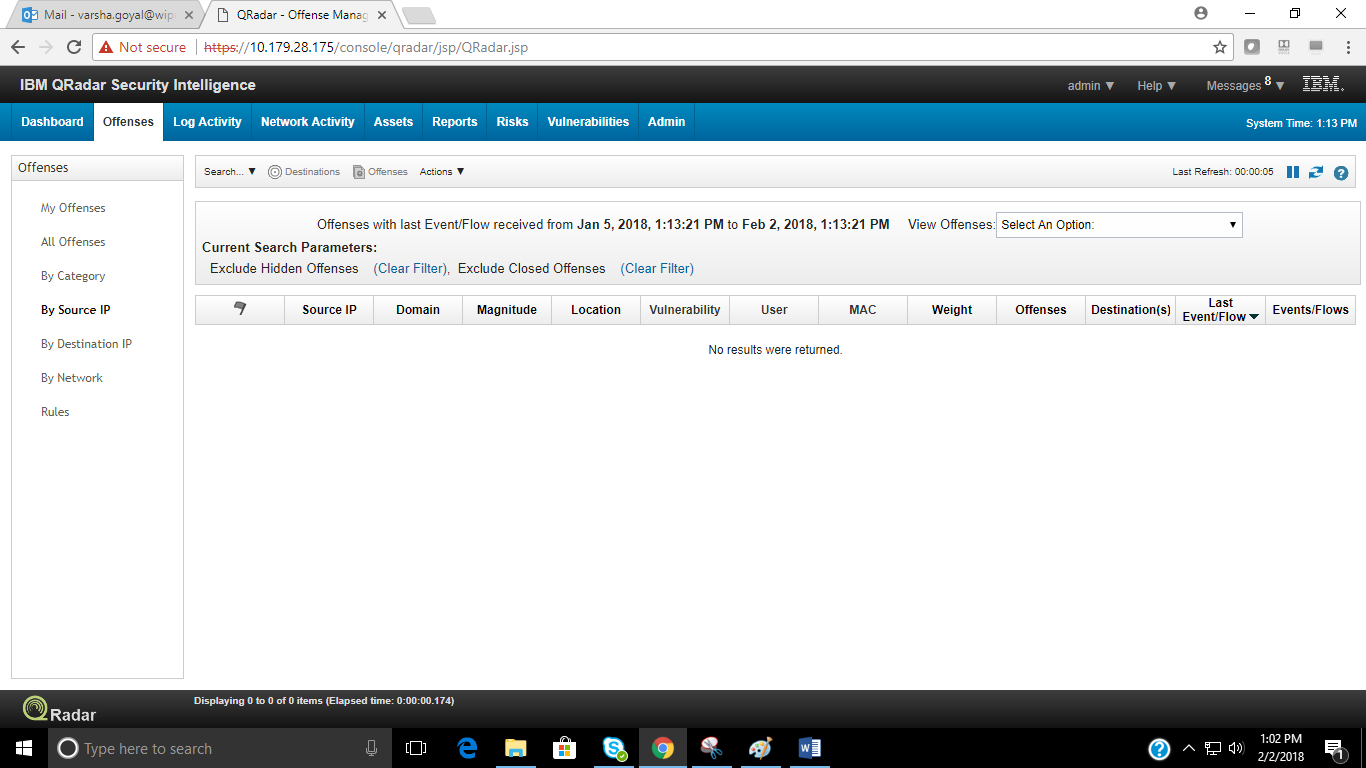
To Short-out offenses in page for convenient, click on ‘View Offenses’ option on page and select accordingly.



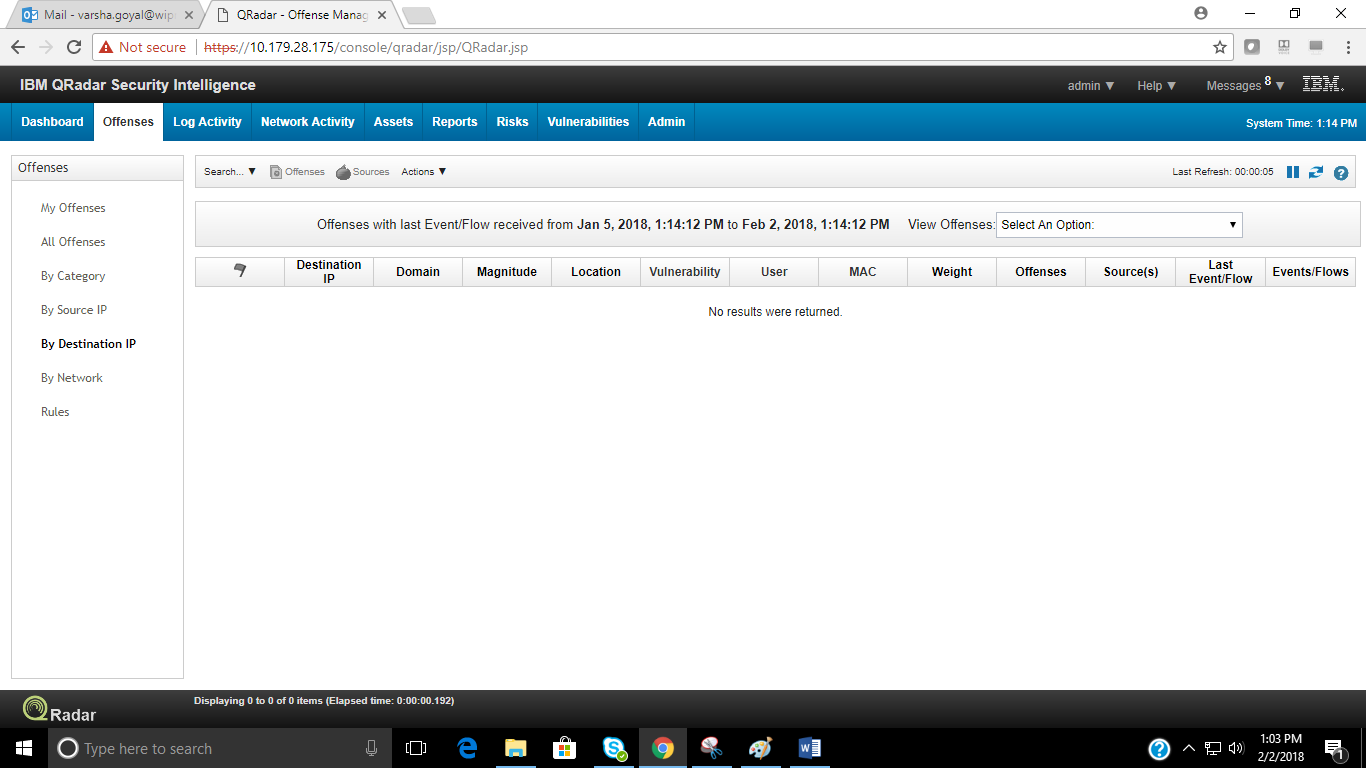
Click on ‘By Category’ link in left hand side of page to see offenses grouped by category.



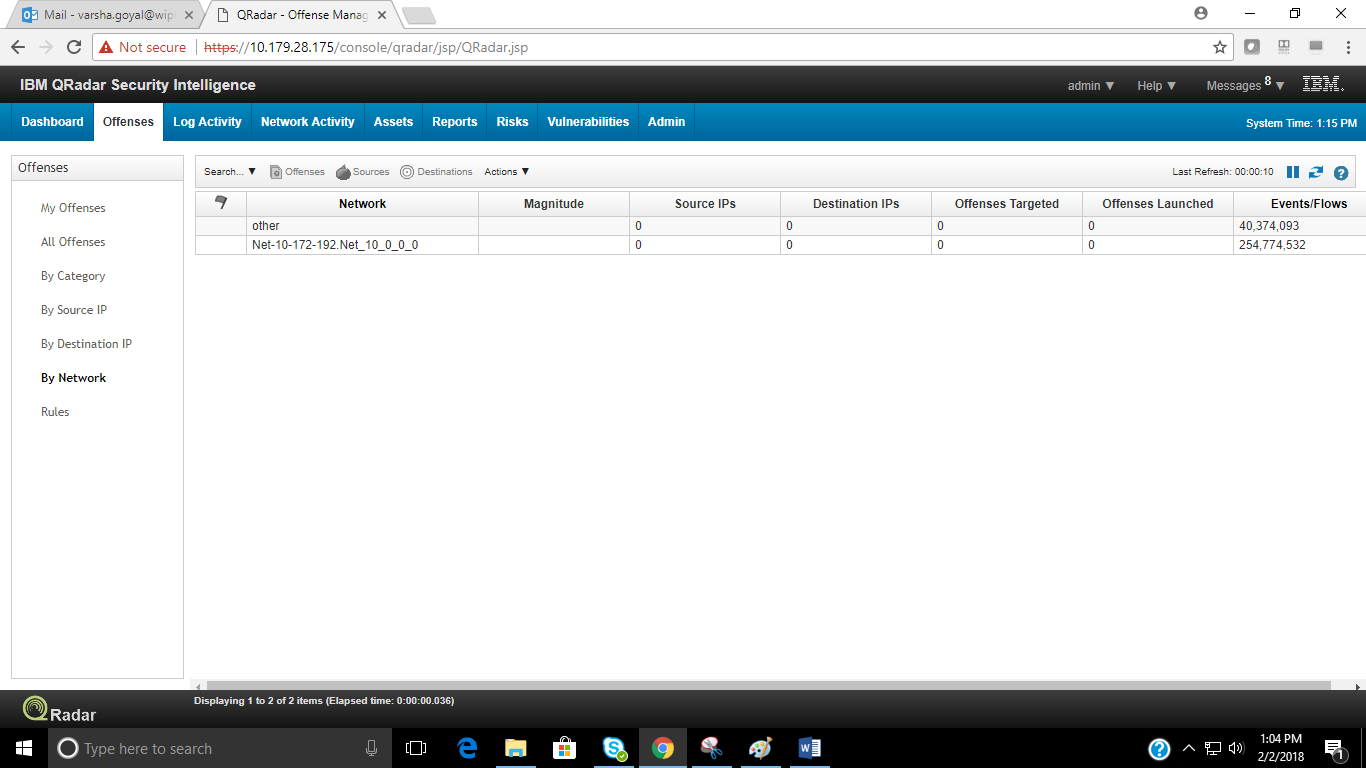
Click on ‘By Source IP’ link in the left hand side of page to see offenses grouped by source IP.



Click on ‘By destination IP’ link in the left hand side of the page to see offenses grouped by destination IP.

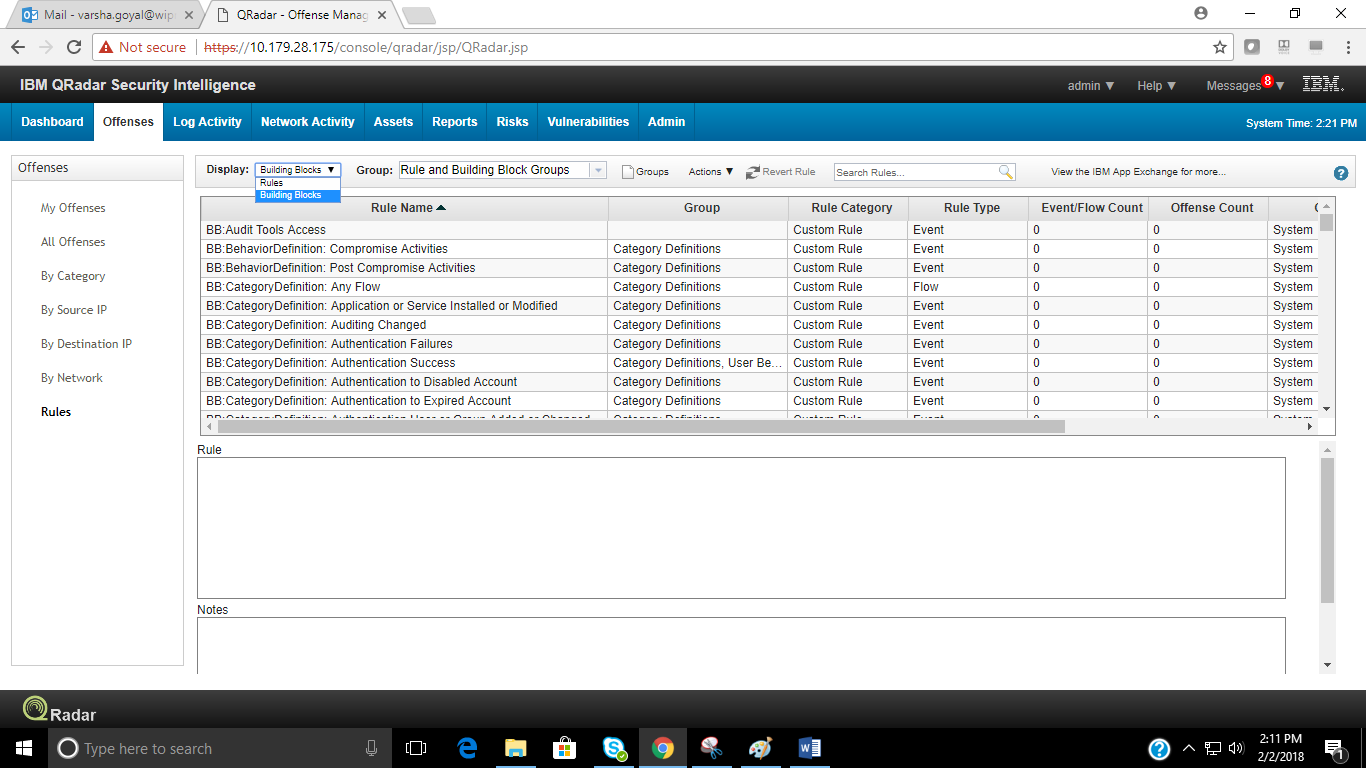


Click on ‘By Network’ link to see offenses grouped by network as defined in network hierarchy.

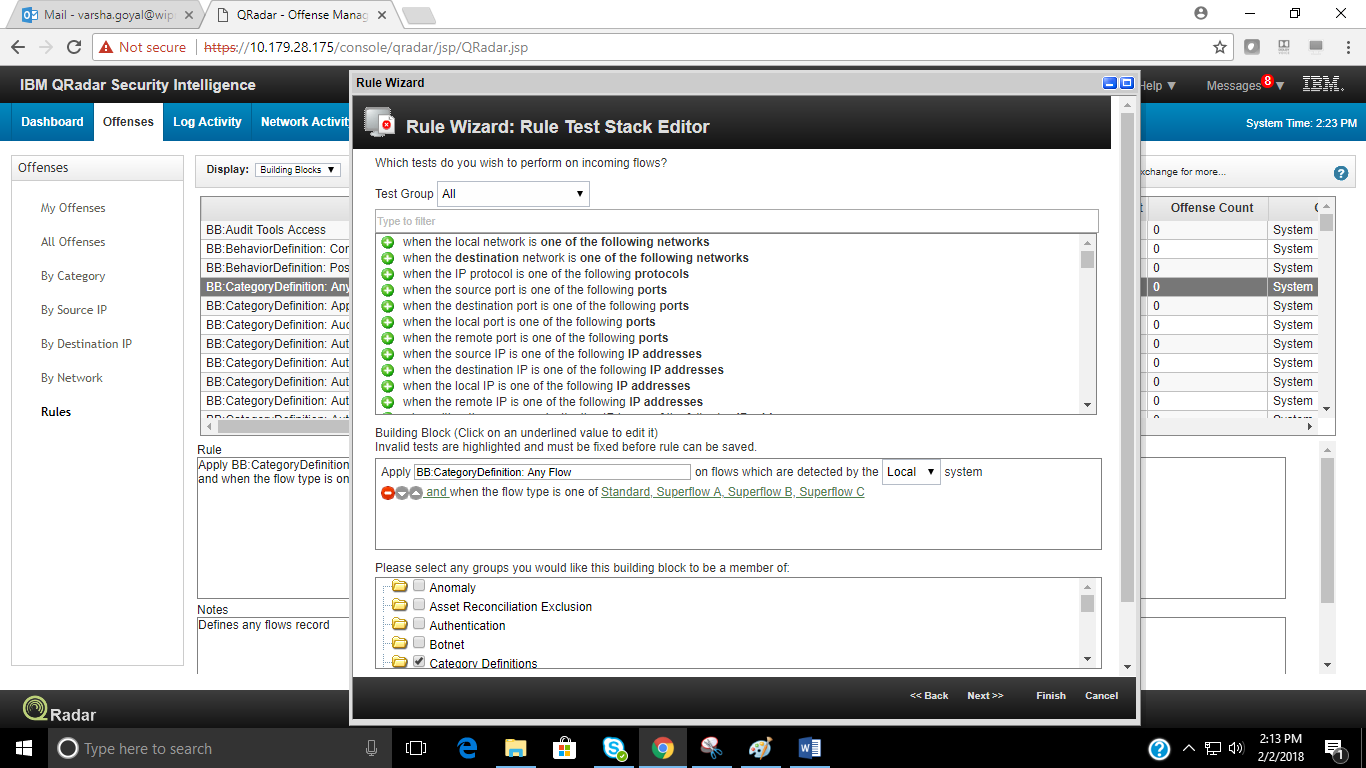


Click on ‘Rules’ to see all the rules.

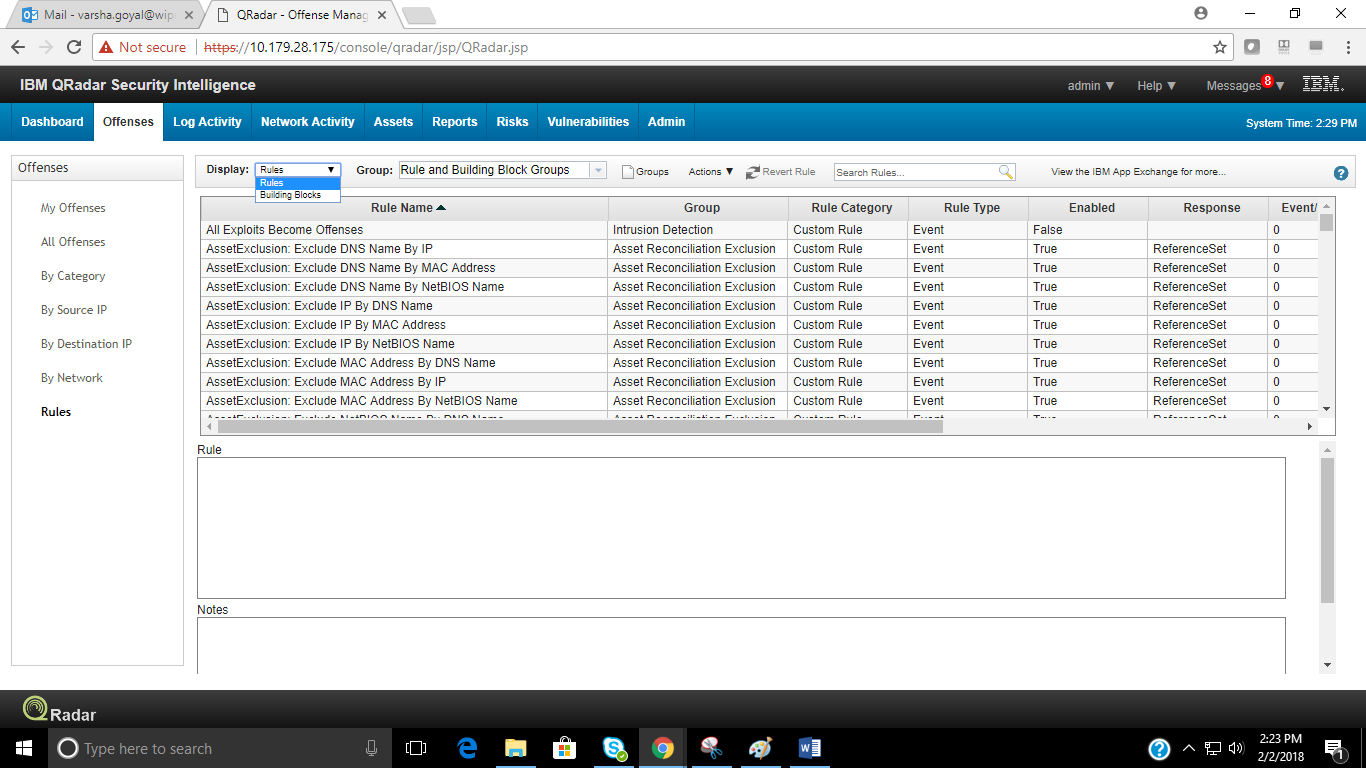
Click on ‘Display’ drop down button and select ‘Building Block’ option to see all building blocks.



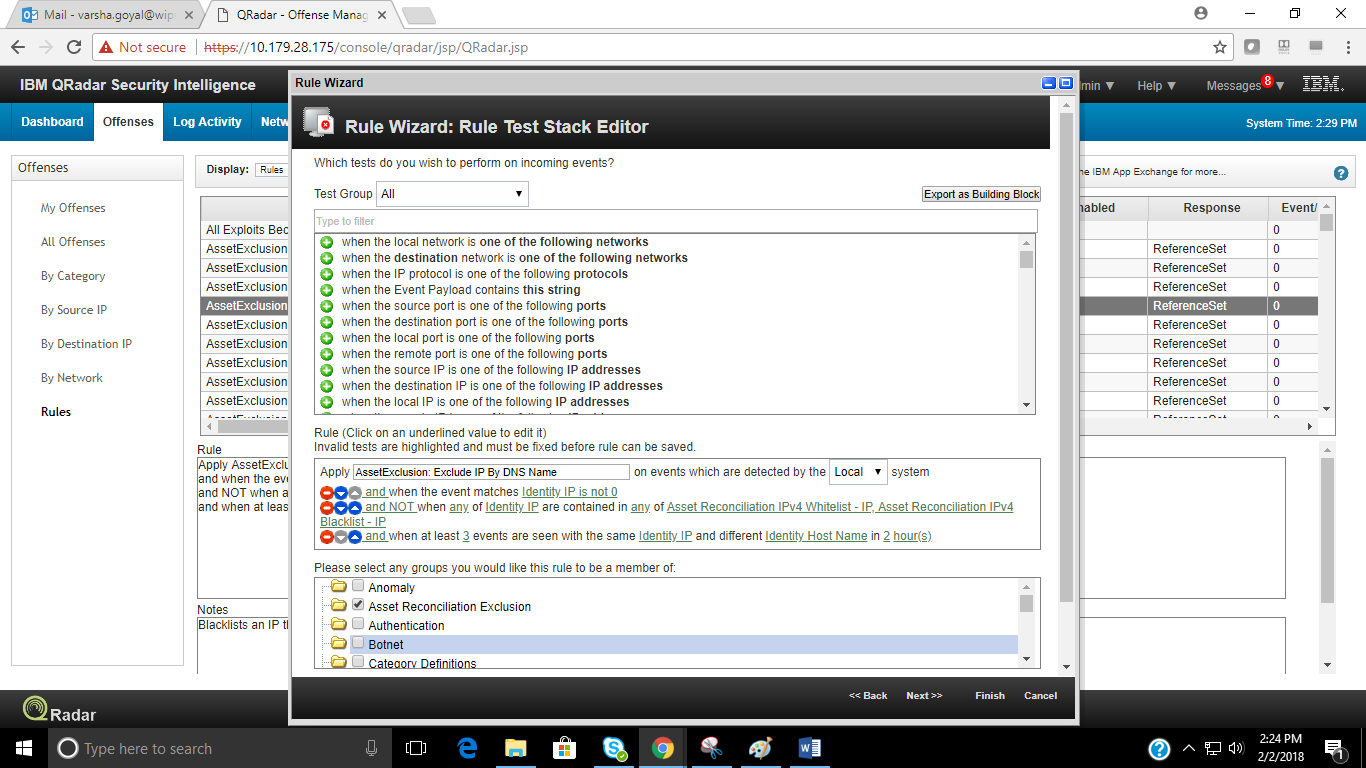
Double click on any of the building block to see its definition.



Now, Again click on ‘Rules’ link on left side of the page and select ‘Display’ drop down button from where select ‘rules’ option to see all defined rules.

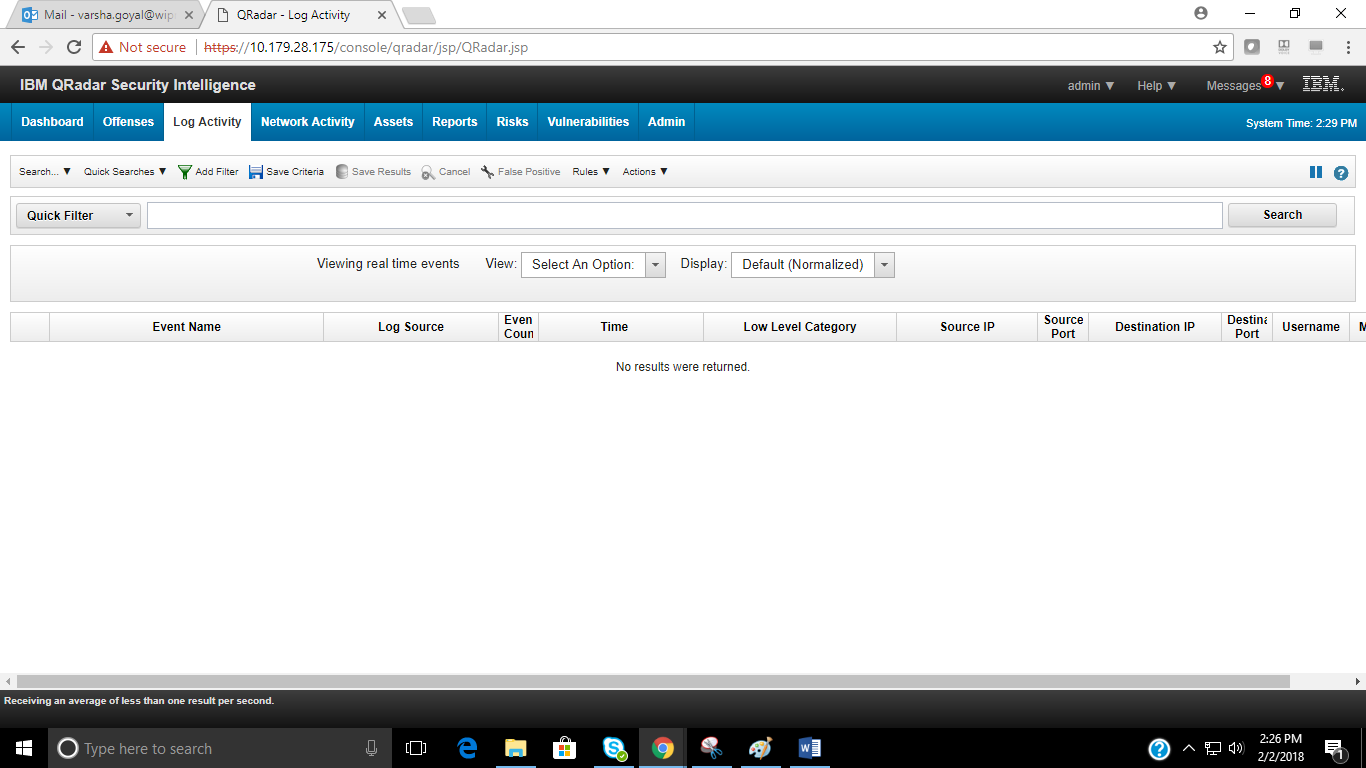


Double click on any one of the listed rules to see and modify its definitions.

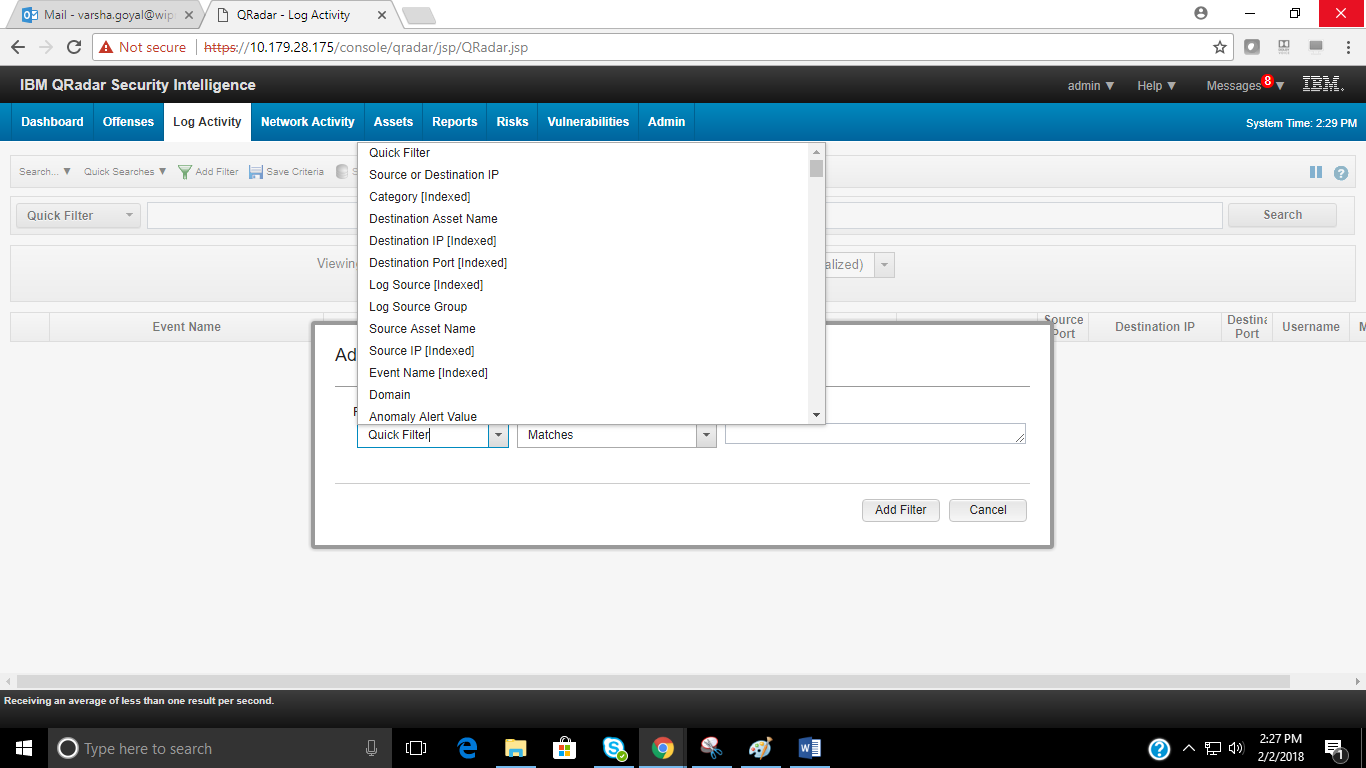


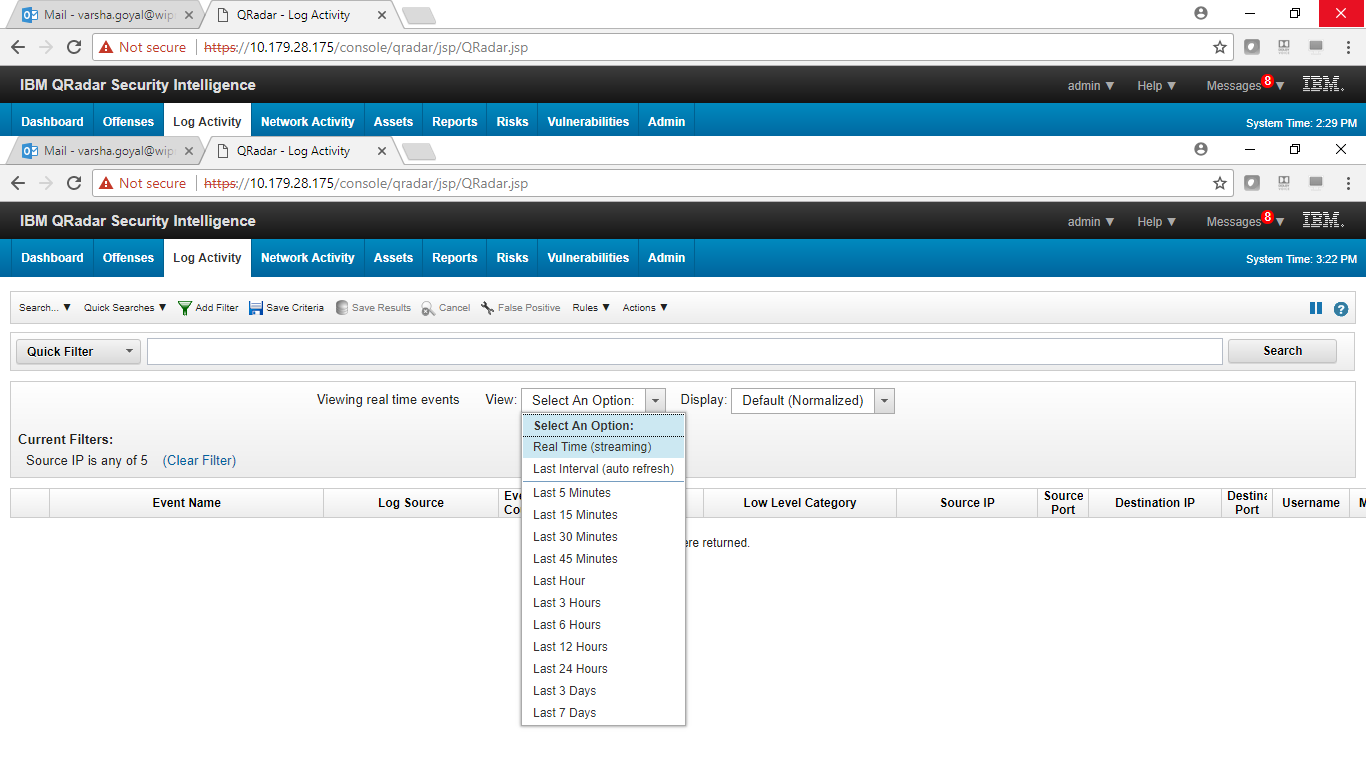
Step 3:

Click on the ‘Log Activity’ tab to see the log activity page.

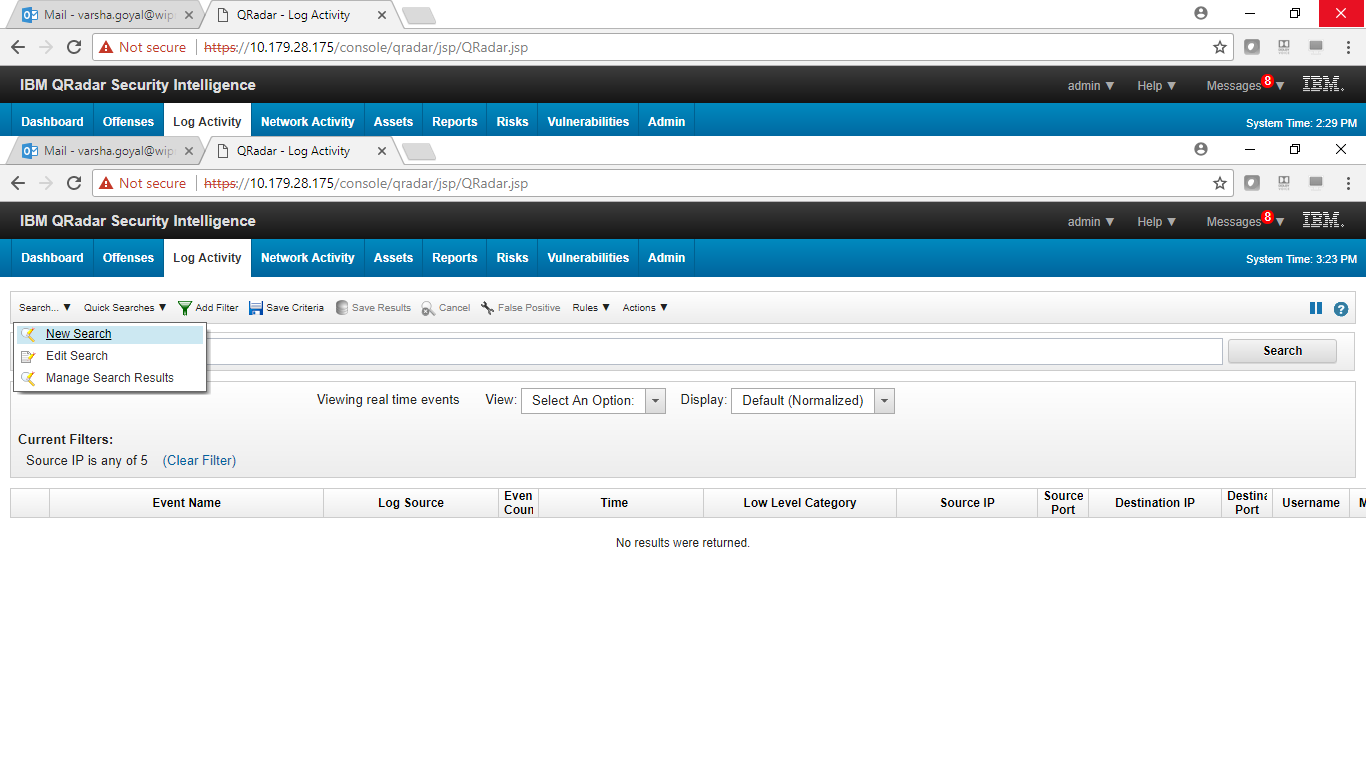


To filter the events, click on ‘add filter’ to select filters for viewing the events.

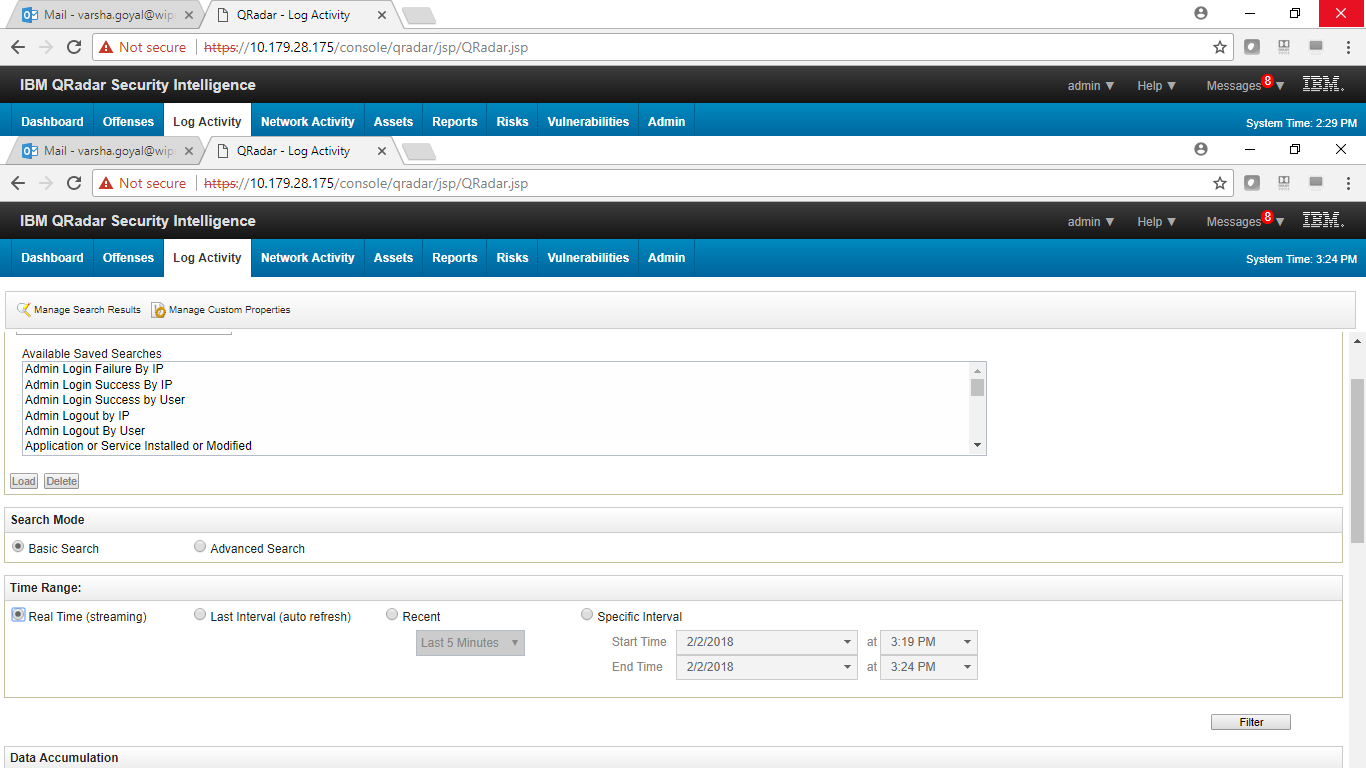
Select any one of the filters available and specify its value, click on ‘add filter’ button to start filtering the events. Select time frame for displaying the events for specified time frame. By default real time events are displayed.



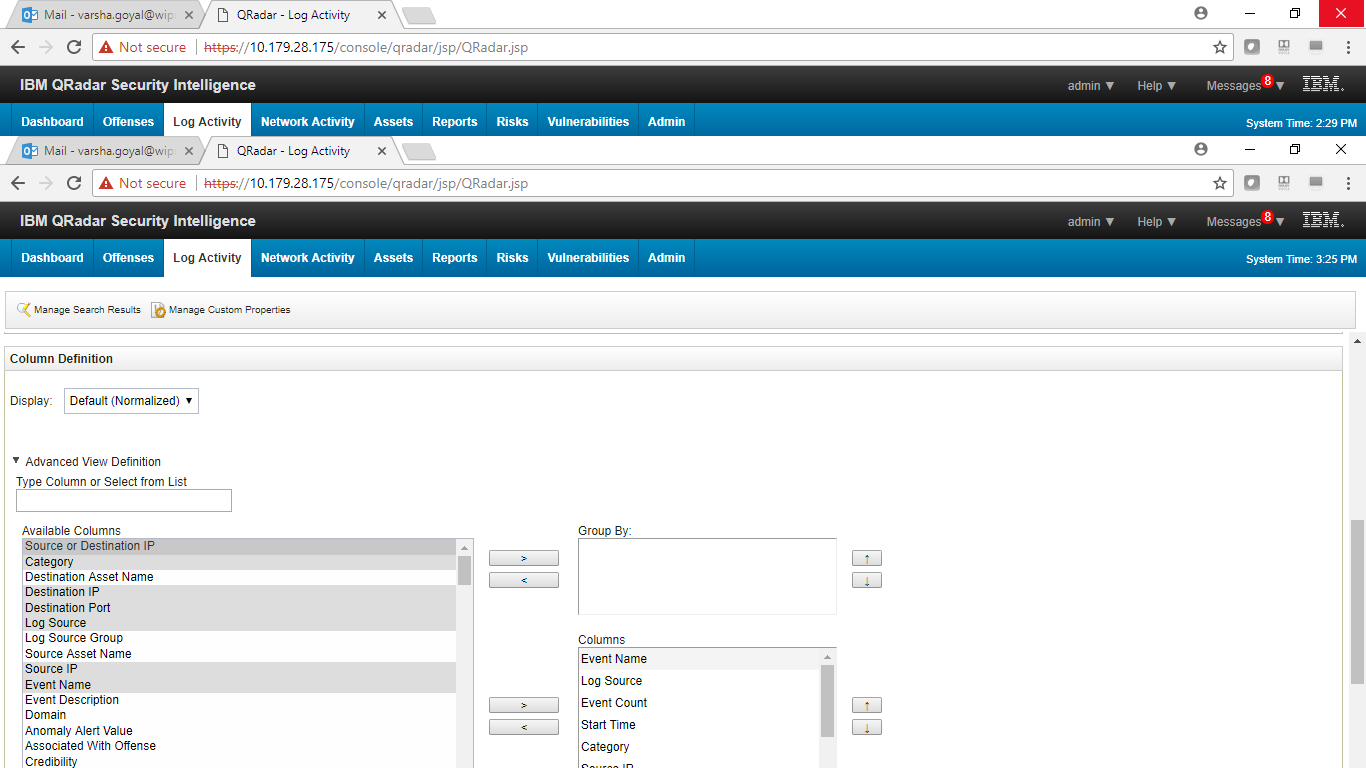
To create a new search, click on ‘log activity’ tab and select ‘search’ drop down button, click on new search.



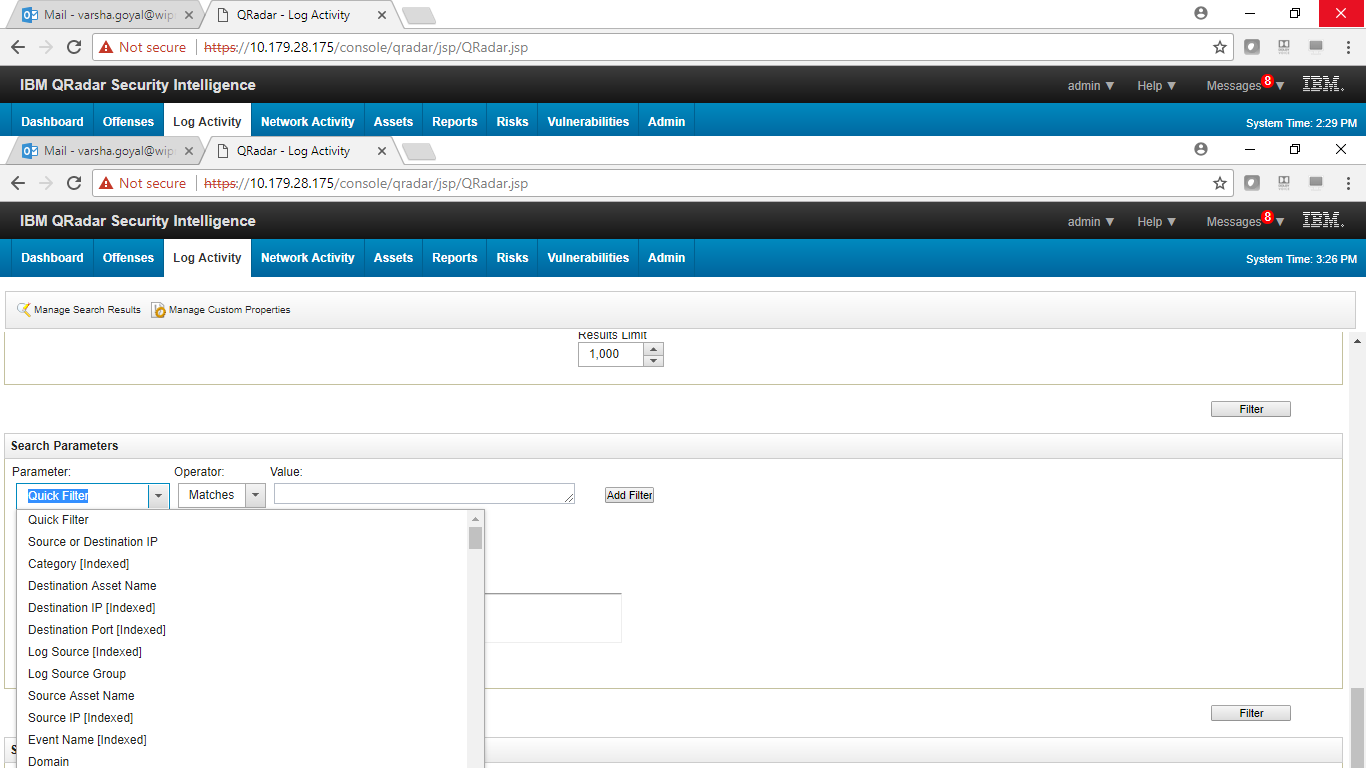
Specify the ‘Time Range’ for which you want to search for the events.



Select the normalized columns/ fields that you want to display in the search results.

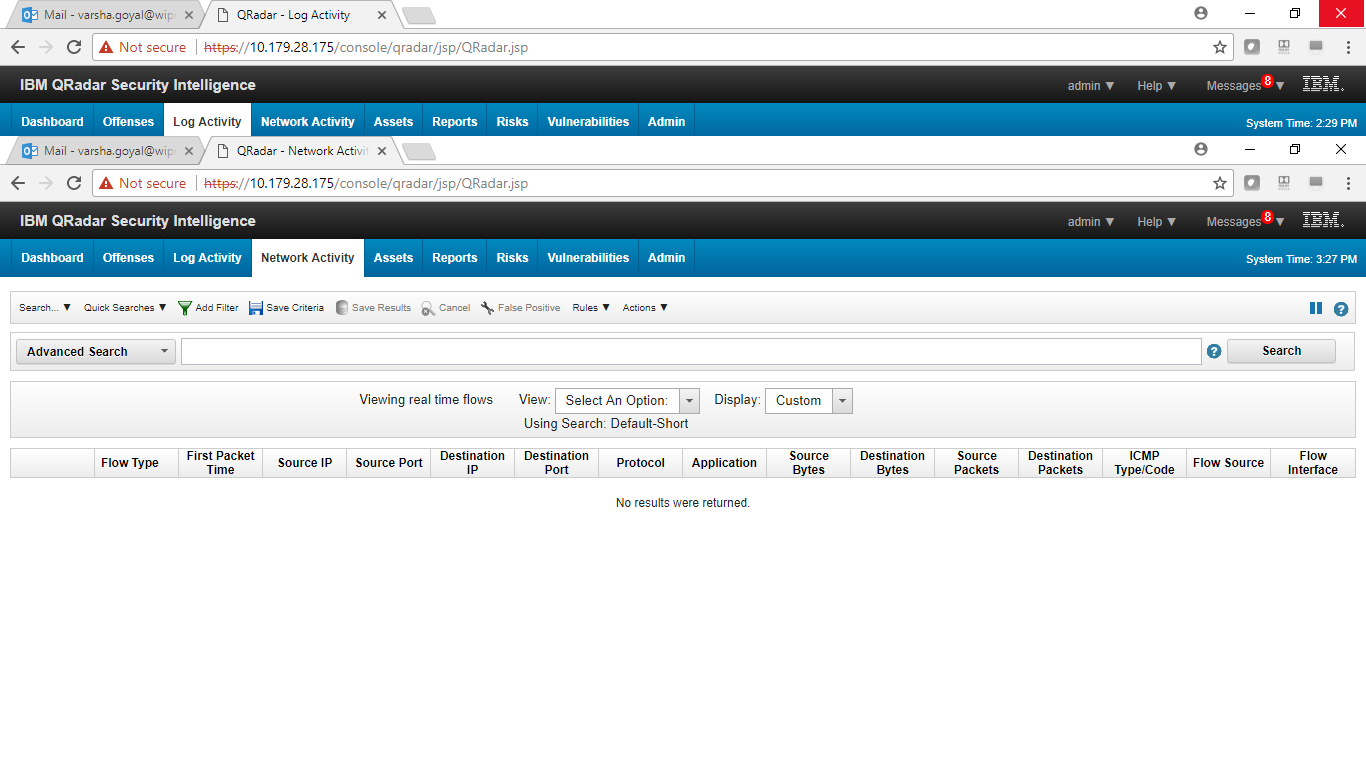


Select the ‘search Parameters’ and specify their value to include filtered events in the search results. Then click on the ‘Filter’ button to begin the search.

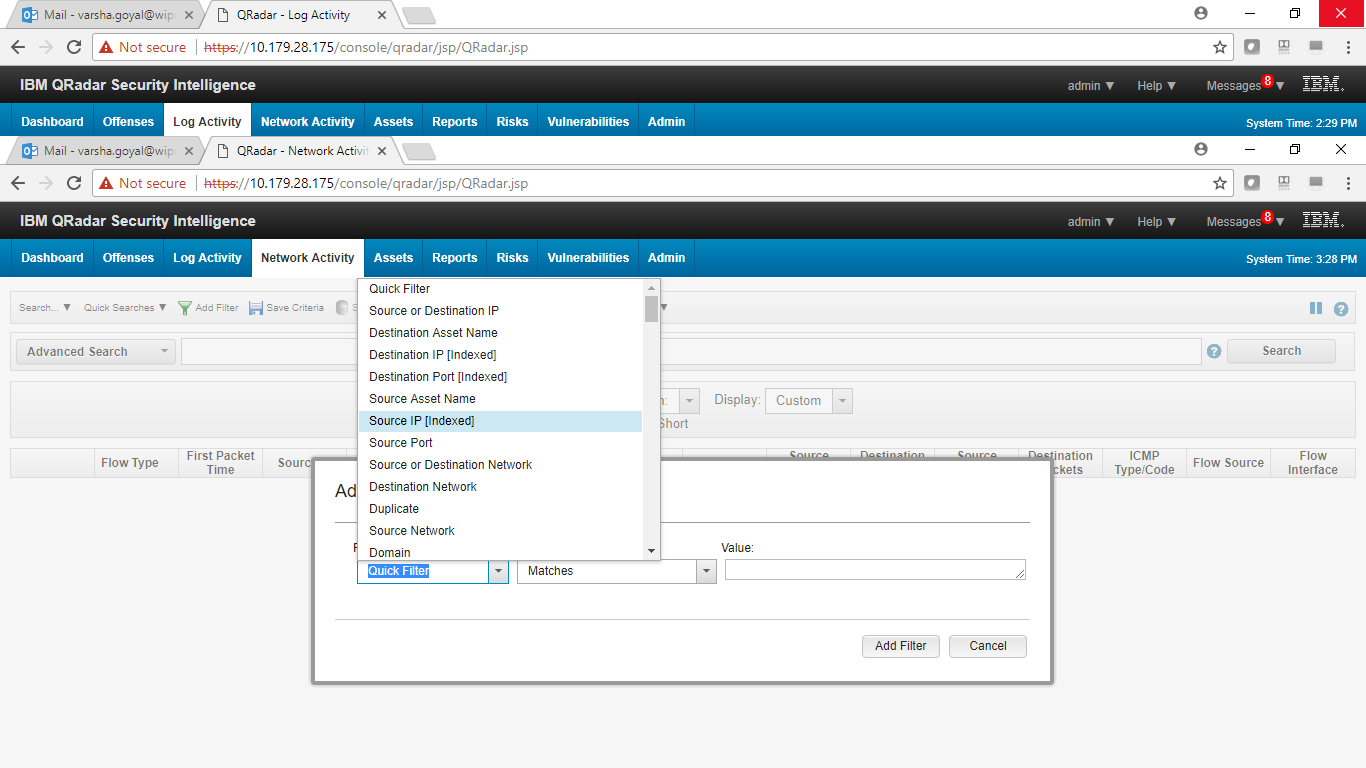


Step 4:

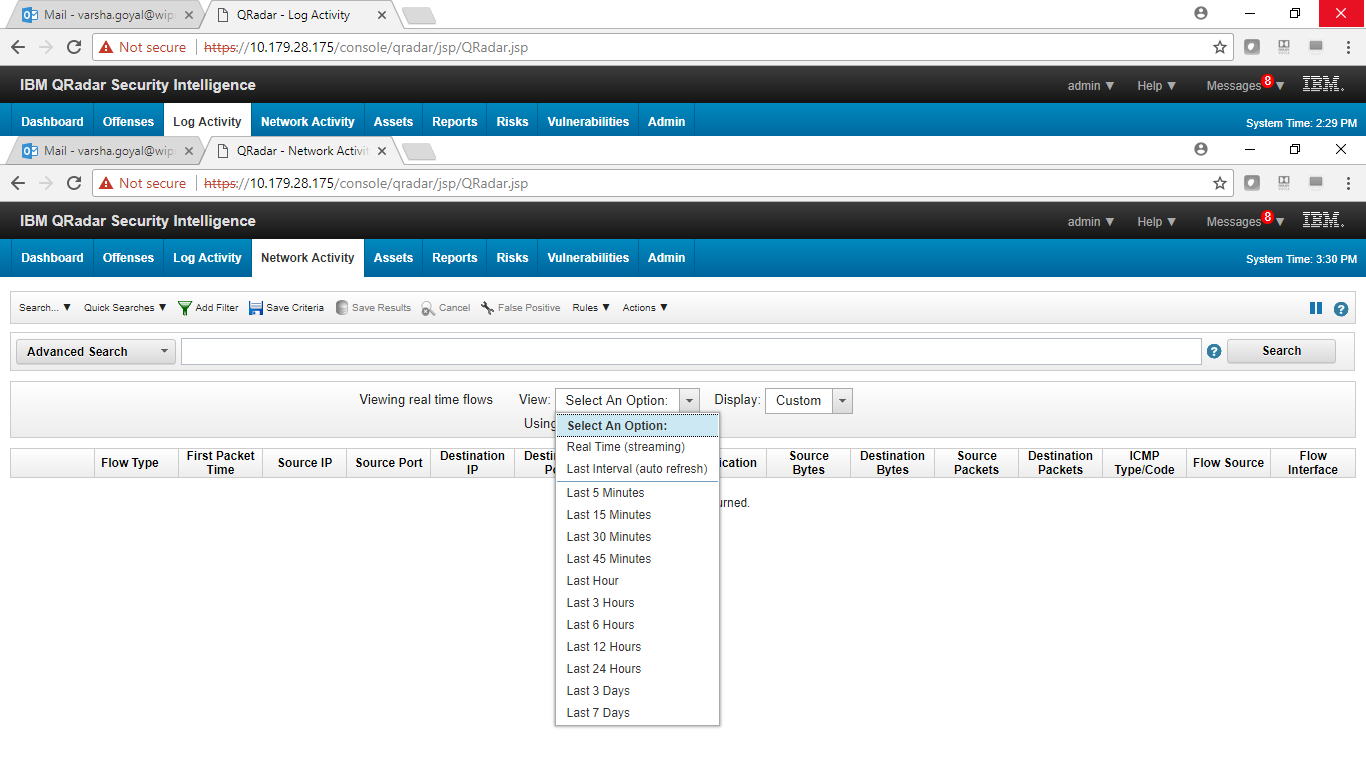
Click on the ‘Network Activity’ tab to see the network activity page.



Click on the ‘add filter’ button and select the filter parameter. Specify the value of filter parameter and click on ‘add filter’ button to begin the filtration of packets.

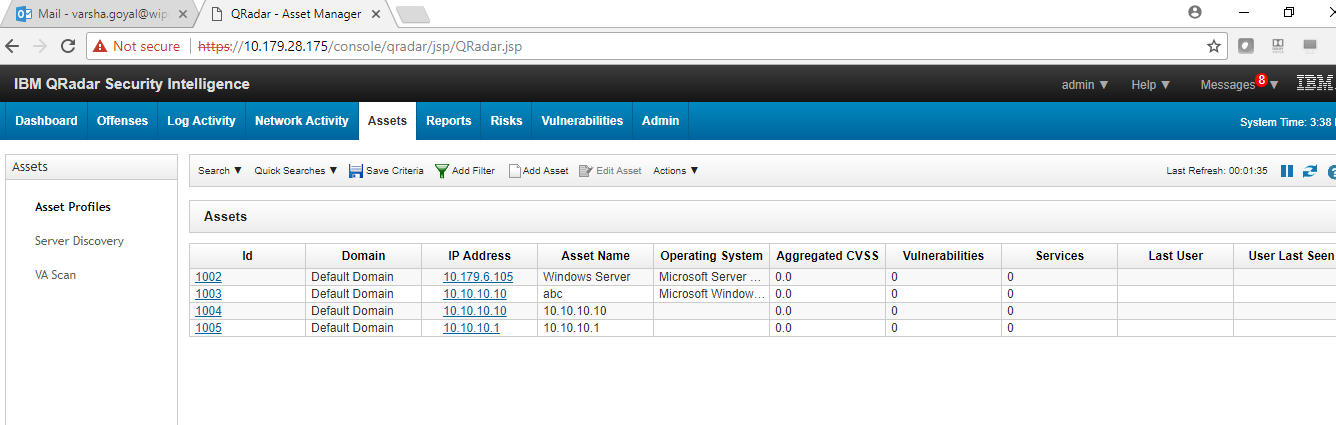


Click on the ‘View’ drop down button to select the desired time frame to filter the packets.

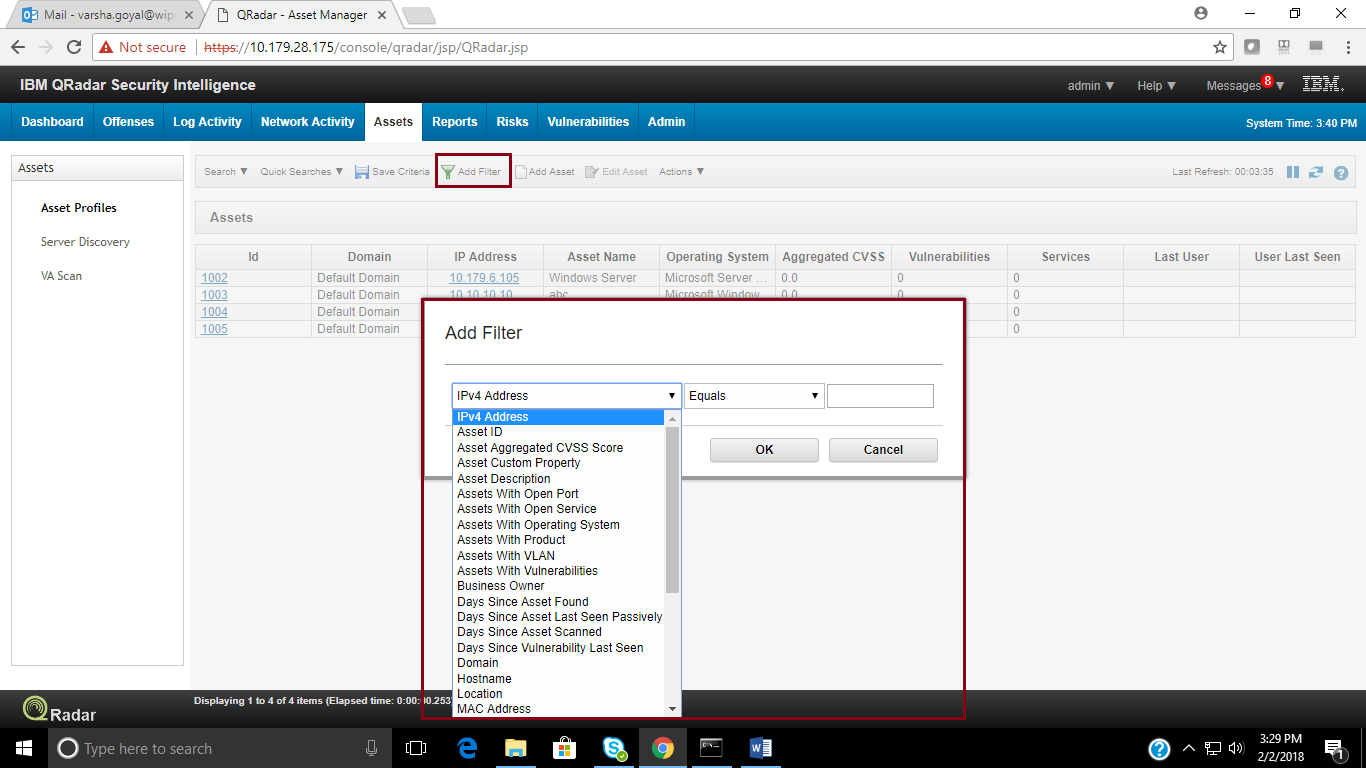


Step 4:

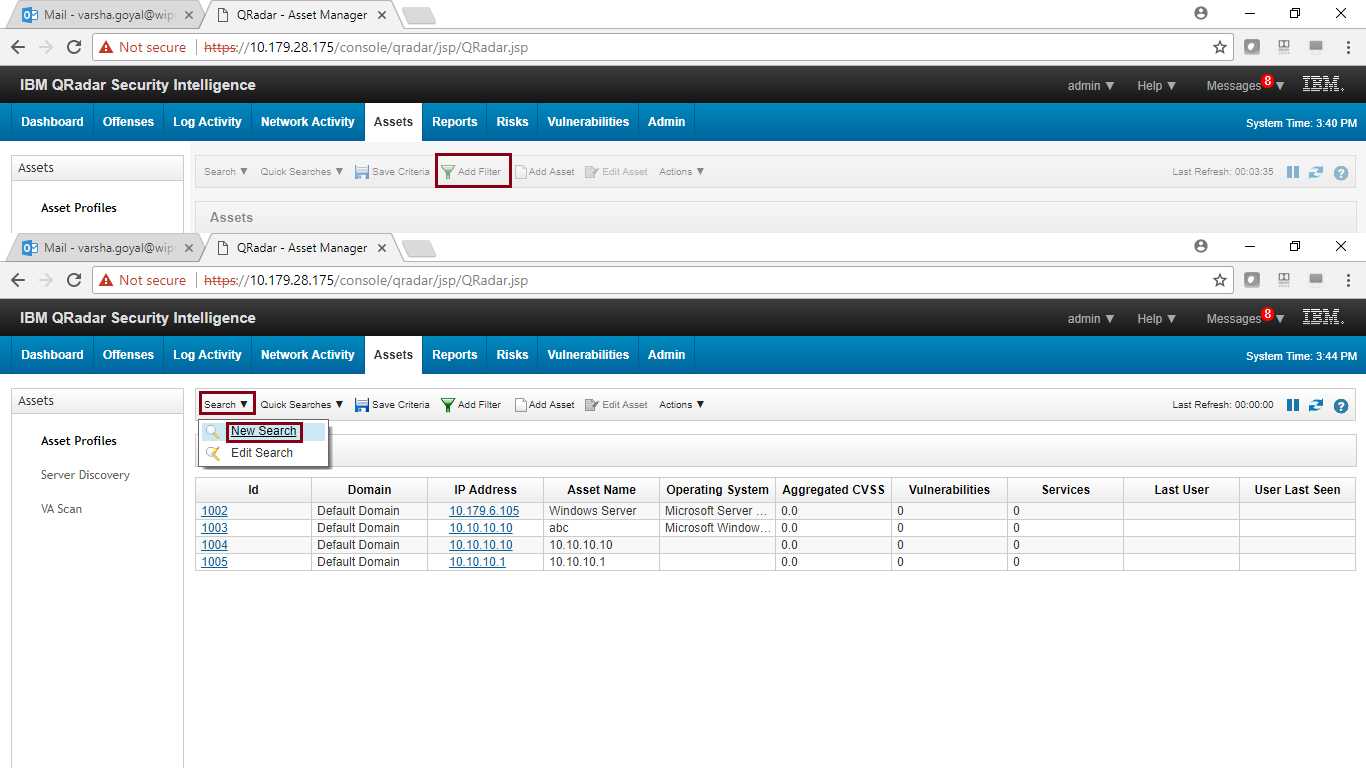
Click on ‘asset’ tab to see asset profile page.



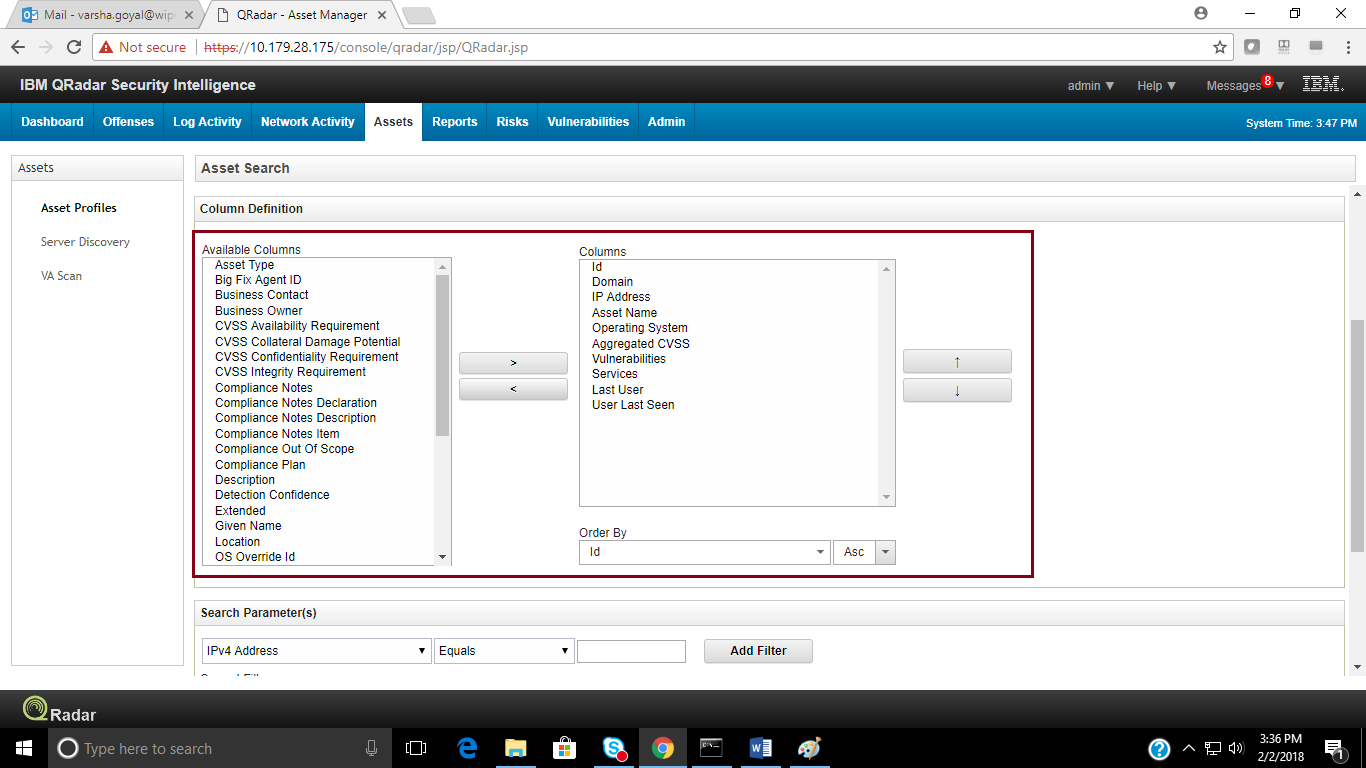
Click on ‘add filter’ button to filter the desired asset and then click on “OK” button.



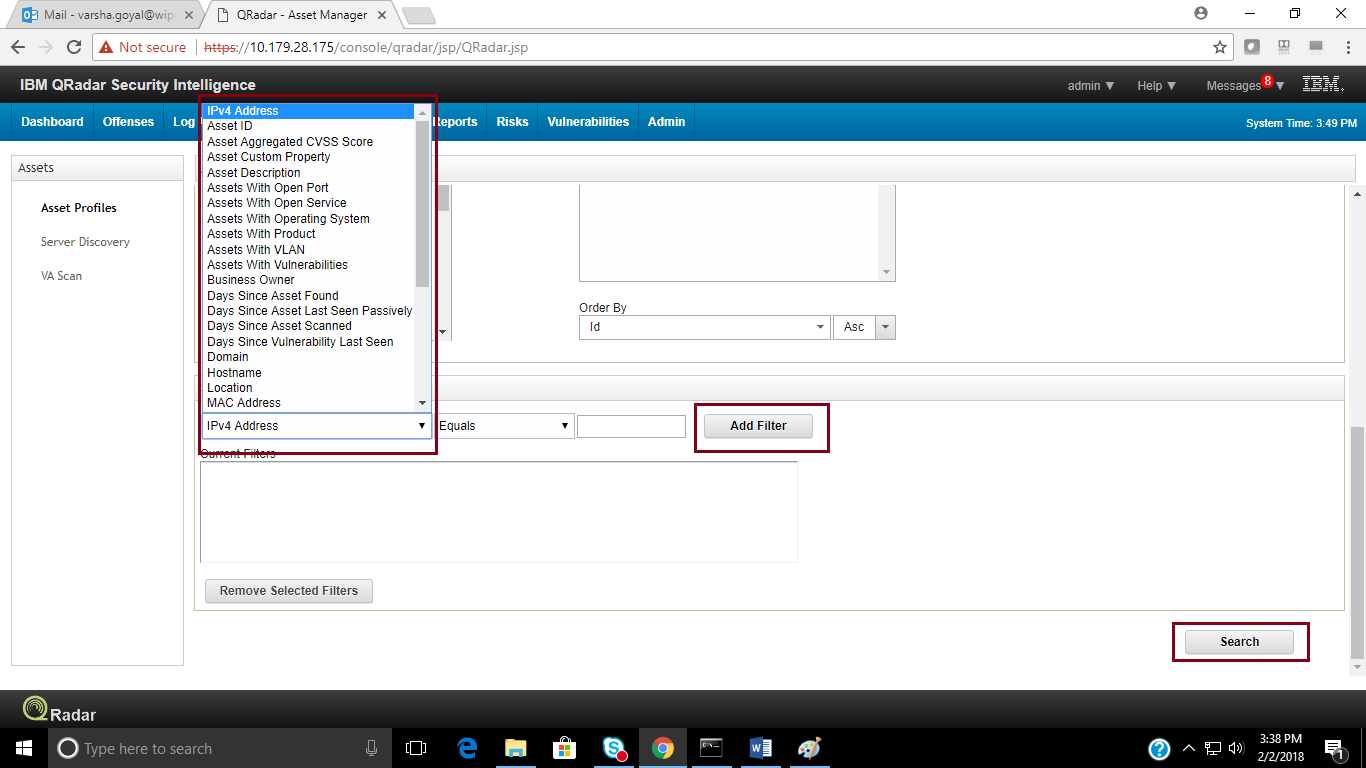
To create a new search for the Assets, In the Asset tab, Click on the ‘Search’ drop down button and click on ‘New Search’.



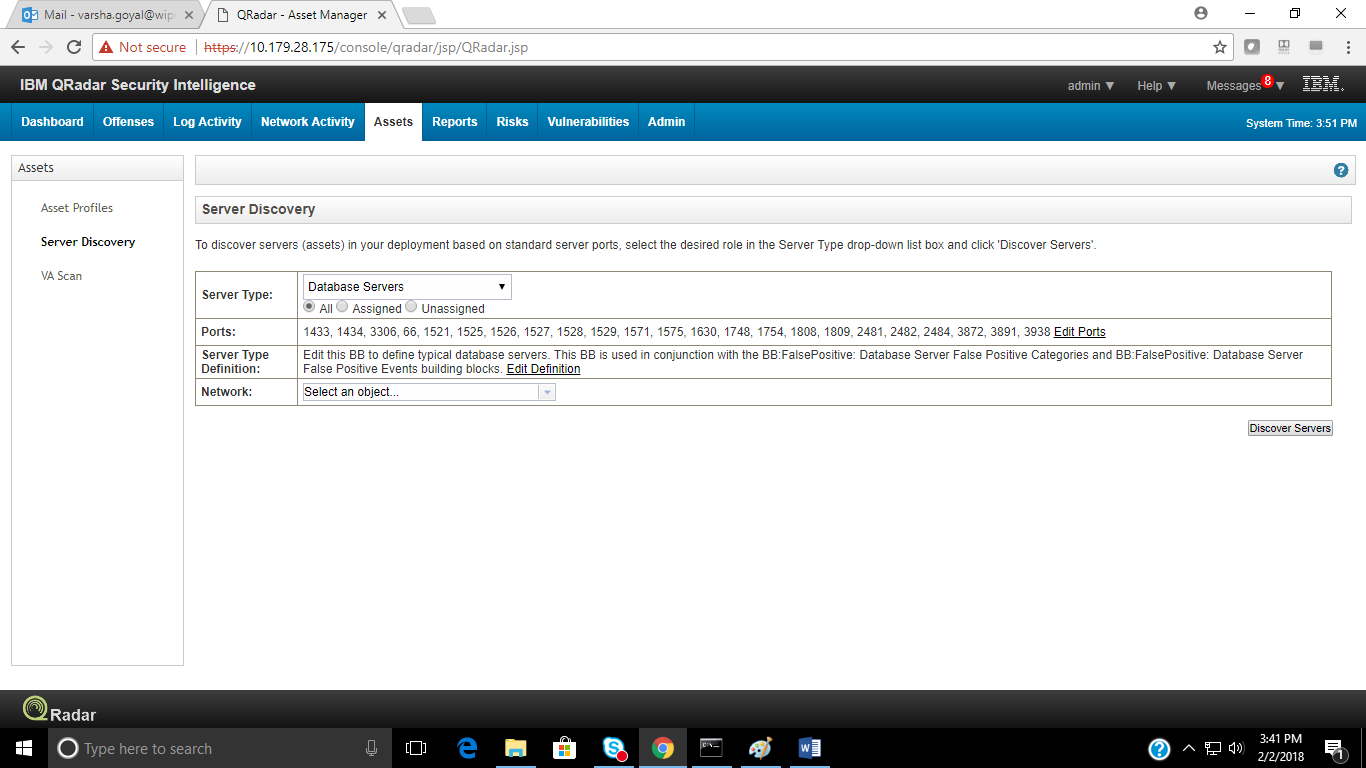
Enter the column definition/ fields what we would like to see in the search results.



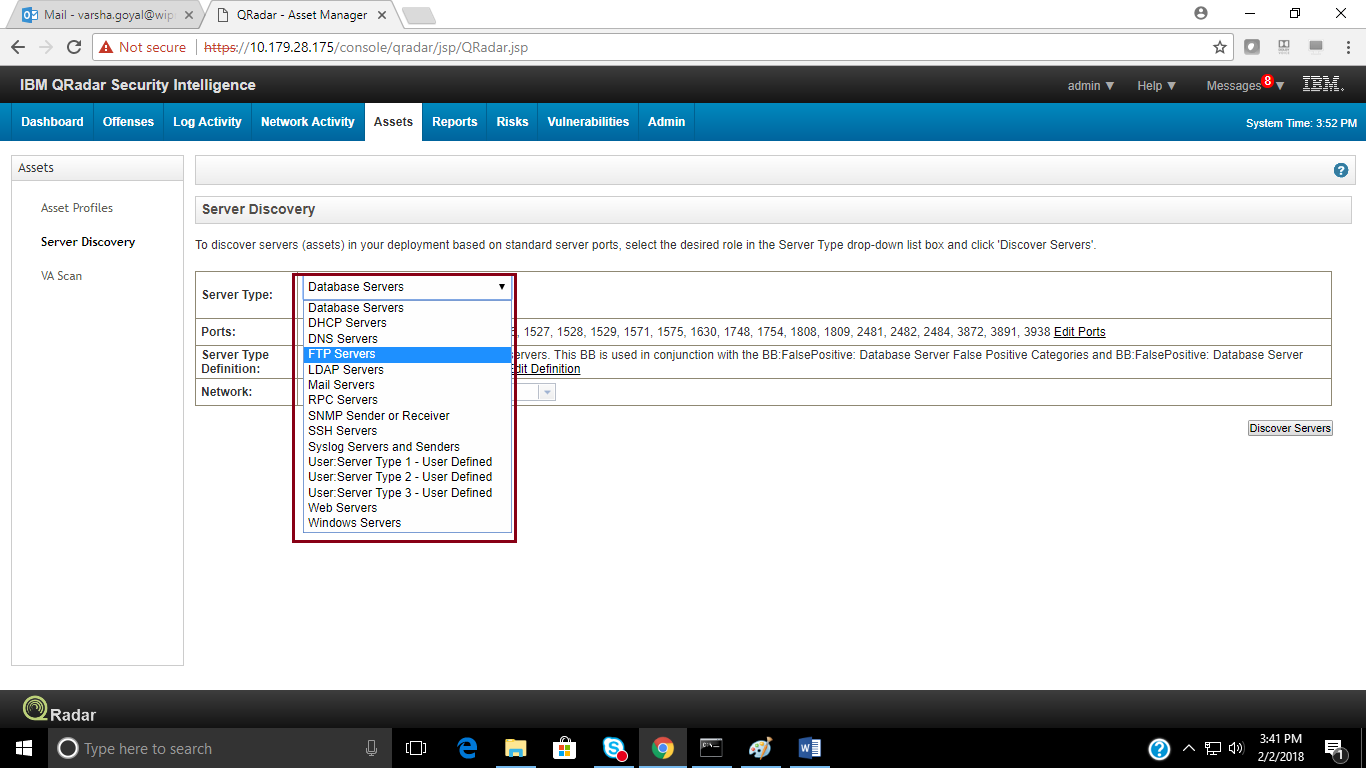
Select the ‘Search Parameter’ and specify their values, then click ‘Add Filter’ button. Now, click on ‘Search’ button to begin the search.



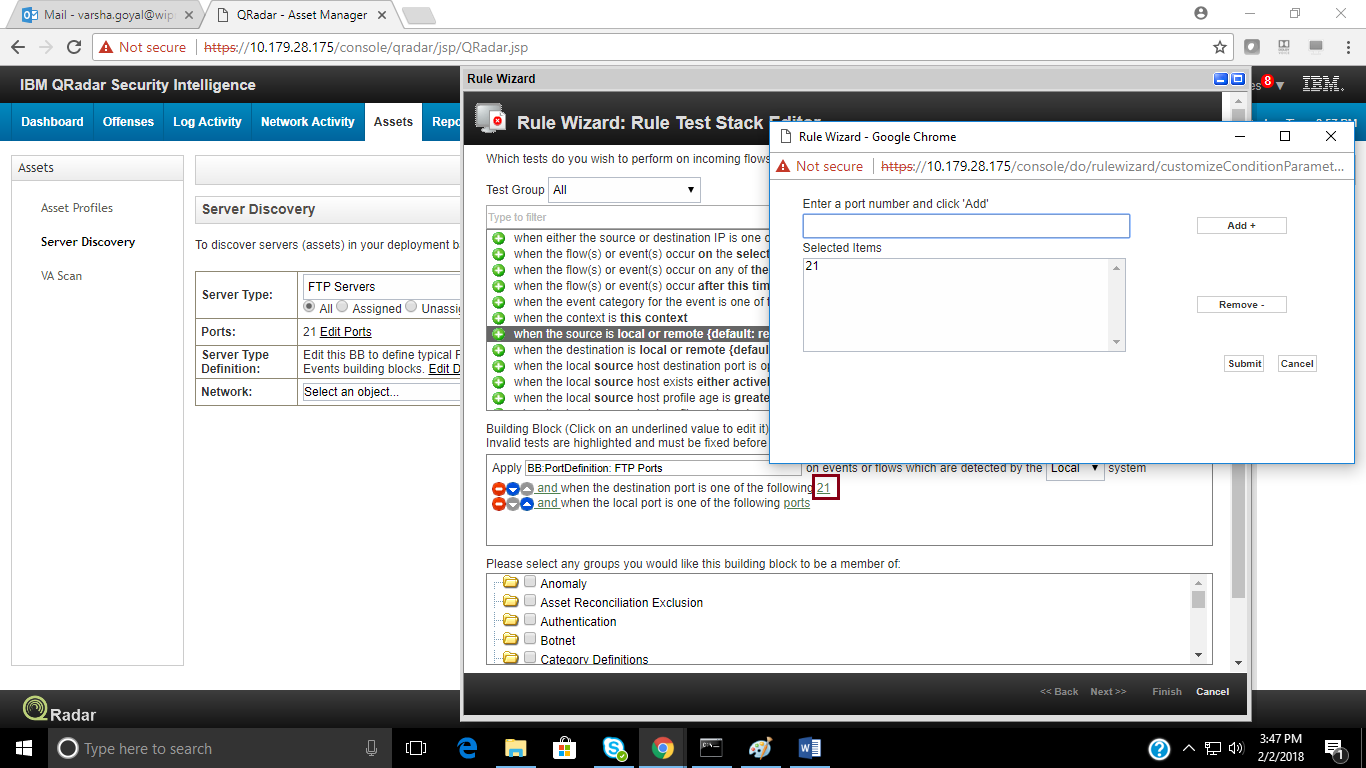
Again click on the ‘Assets’ tab then click on ‘Server Directory’ on the left hand side of the page.



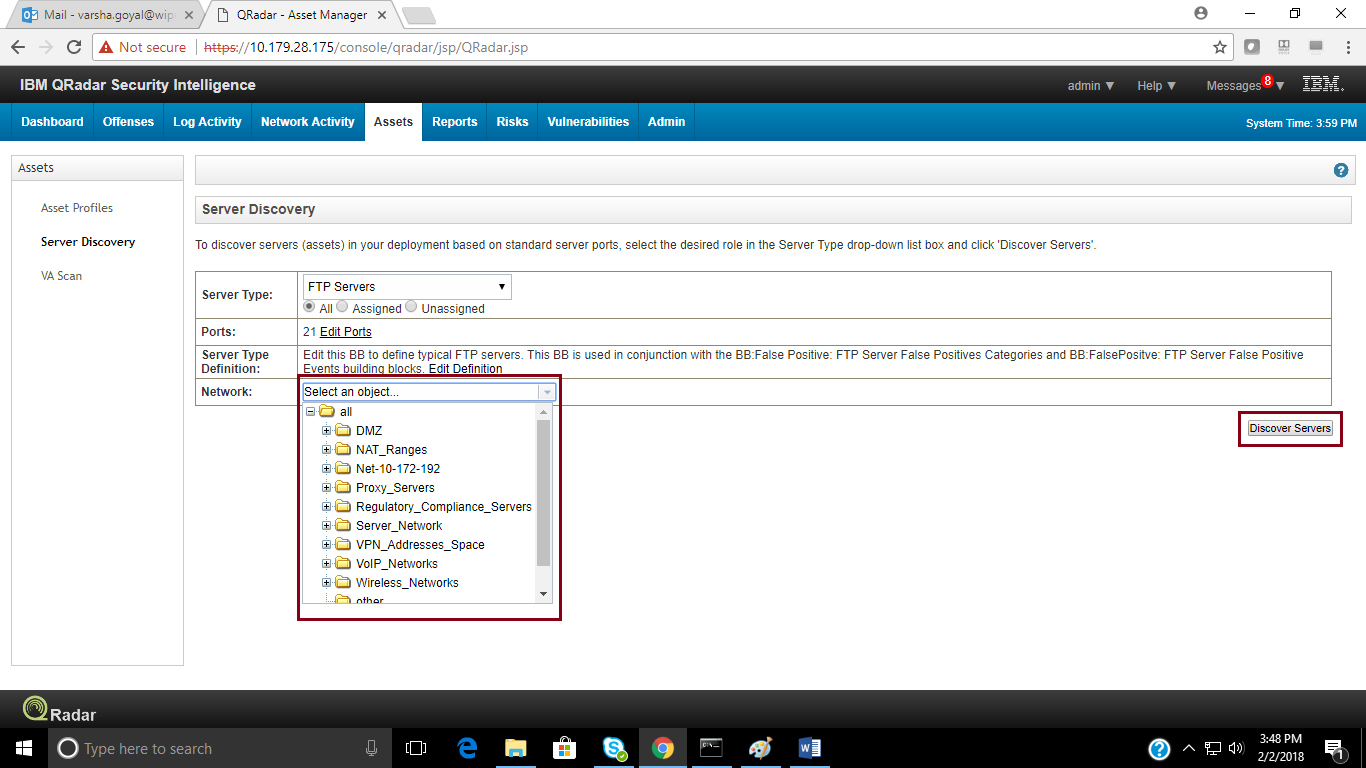
Click on ‘Server Type’ drop down button to select the Server/Asset type to be discovered.



Click on ‘Edit Port’ to specify the ports other than standard port for any specific type of server/asset for discovery.



Select the ‘Network’ as defined in Network Hierarchy to search for the specified Servers/Assets and click on ‘Discover Servers’.



To log out of QRadar console, click on drop down box on top-right side of the console as shown:

