



[Course](#) > [LAB GUIDE](#) > [Lab 4 - Investigatin...](#) > Investigating an off...

## Investigating an offense that is triggered by flows

### Investigating an offense that is triggered by flows

Follow the below steps to investigate an offense that is triggered by flows.

1. Run the following command on SSH Terminal, to access the remote shell to the Qradar.

```
ssh root@allinone742
```

Enter the password as 'p@ssw0rd'

```
root@allinone742:~  
File Edit View Search Terminal Help  
[root@GUIHOST ~]# ssh root@allinone742  
root@allinone742's password:  
Last login: Tue Jun  1 21:35:23 2021 from 10.10.9.29  
This server was upgraded to QRadar 7.4.2 FixPack 2 (Build 20210120225428) on Wed  
May 26 23:37:01 IST 2021.  
[root@allinone742 ~]#
```

2. Run the following commands:

inconfig ens33 promisc

```
[root@allinone742 configurationsets]# ifconfig ens33 promisc
```

cd /labfiles



./startRdp.sh

```
[root@allinone742 labfiles]# ./startRdp.sh
Actual: 311 packets (79977 bytes) sent in 7.86 seconds
Rated: 10163.3 Bps, 0.081 Mbps, 39.52 pps
Flows: 2 flows, 0.25 fps, 311 flow packets, 0 non-flow
Statistics for network device: ens33
    Successful packets:      311
    Failed packets:         0
    Truncated packets:      0
    Retried packets (ENOBUFFS): 0
    Retried packets (EAGAIN): 0
You have new mail in /var/spool/mail/root
[root@allinone742 labfiles]#
```

3. In the Qradar user interface, navigate to the Network Activity tab.

Dashboard   Offenses   Log Activity   Network Activity   Assets   Reports   Risks   Vulnerabilities   Admin   Pulse   Use Case Manager

4. Observe the network activity and verify that a network activity triggers an offense.

Flow Type	First Packet Time	Storage Time	Source IP	Source Port	Destination IP	Destination Port	Source Bytes	Destination Bytes	Total Bytes	Source Packets	Destination Packets	Total Packets	Protocol	Application	ICMP Type/Ct	Source Flags	Destination Flags	Source QoS	Destination QoS	Flow Source	Flow Interface
	Jun 18	Jun 18	192.168.1.1	51716	19	3389	330,330 (C)	311,905 (I)	642,295	1,201	1,238	2,439	tcp_ip	RemoteAccess MStTerminalS...	N/A	F,S,P,A	S,R,P,A	Best	Best	allnone742	allnone742 ems33
	Jun 18	Jun 18	192.168.1.1	51716	19	3389	40,401 (C)	37,061 (C)	77,462	139	142	281	tcp_ip	RemoteAccess MStTerminalS...	N/A	S,P,A	S,P,A	Best	Best	allnone742	allnone742 ems33

5. To investigate the offense, click the red icon in the left-most column. Red Icon in the left most column signifies the flows that contribute to an offense.

6. The Offense Summary page opens.

7. What is the name of the offense, Offense Type, Offense Source and Destination IP?

8. How many events or Flows are associated with this offense?

9. Which Rule added events or flows to this offense?

To investigate the flows that contributed to the offense. Follow the below steps.

1. Click **Flows** on the Offense Summary page toolbar The Flow List page opens.

2. Examine the Flow associated with this offense. Double-Click on the flow listed.

3. Answer the flowing questions:

a. What is the flow direction?

b. What is the Application name?

c. Which Activity triggered this offense?

4. Tune the flow as a false positive.

a. On the Flow details page's toolbar, click **False Positive**.

b. Click **Tune**.

c. Click **Close**.

5. Close the offense.

a. On the **Offense** tab navigation menu, select **All Offenses**.

b. From the **Actions** drop-down list on the toolbar, select **Close**.

c. From the **Reason for Closing** list, select **False-Positive, Tuned**.

d. Click **OK**.

---