Investigating the offense

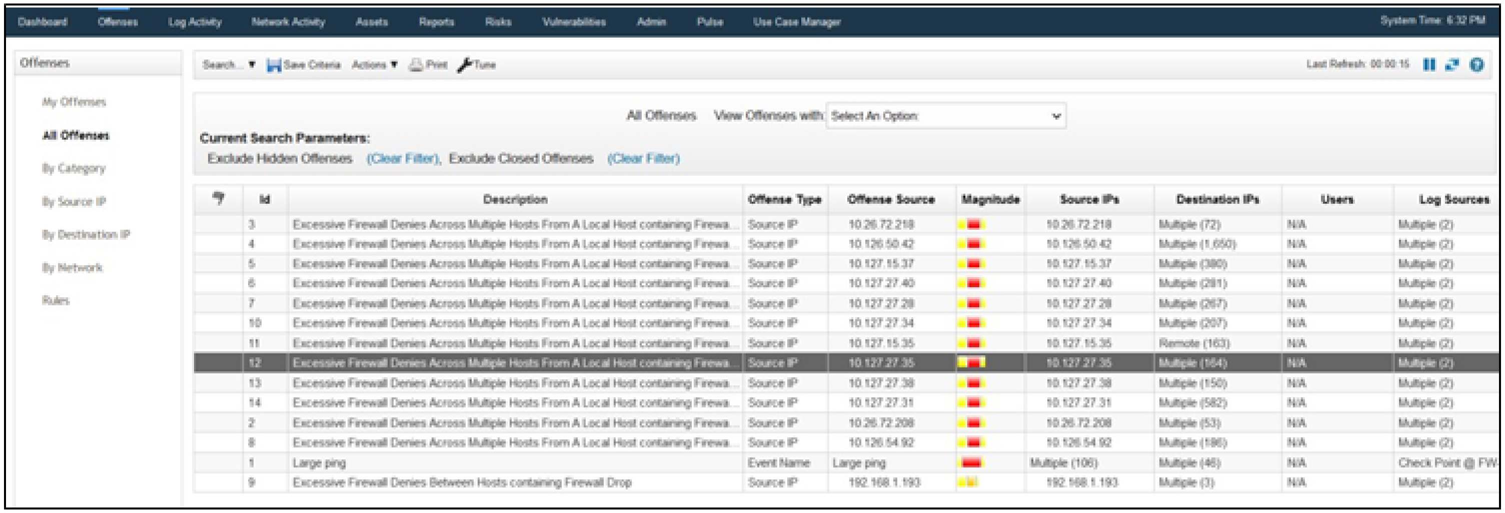
Investigating the offense

In this Lab, We will try to investigate an offense triggered by events, we may have pushed in the last lab.

We will look at the offense named **“Local DNS Scanner containing invalid DNS”** or **“Excessive Firewall Denies”**

Perform the below steps:

1. Login in the Qradar Interface, on the Home page, Click the **Offenses** tab.



All Offenses View Offenses with: Select An Option:

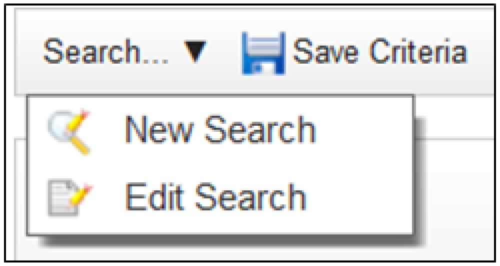
Current Search Parameters:
Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

	Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources
	3	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.26.72.218	🟨🟥	10.26.72.218	Multiple (72)	N/A	Multiple (2)
	4	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.126.50.42	🟨🟥	10.126.50.42	Multiple (1,650)	N/A	Multiple (2)
	5	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.15.37	🟨🟥	10.127.15.37	Multiple (380)	N/A	Multiple (2)
	6	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.40	🟨🟥	10.127.27.40	Multiple (281)	N/A	Multiple (2)
	7	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.28	🟨🟥	10.127.27.28	Multiple (267)	N/A	Multiple (2)
	10	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.34	🟨🟥	10.127.27.34	Multiple (207)	N/A	Multiple (2)
	11	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.15.35	🟨🟥	10.127.15.35	Remote (163)	N/A	Multiple (2)
	12	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.35	🟨🟥	10.127.27.35	Multiple (164)	N/A	Multiple (2)
	13	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.38	🟨🟥	10.127.27.38	Multiple (150)	N/A	Multiple (2)
	14	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.31	🟨🟥	10.127.27.31	Multiple (582)	N/A	Multiple (2)
	2	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.26.72.208	🟨🟥	10.26.72.208	Multiple (53)	N/A	Multiple (2)
	8	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.126.54.92	🟨🟥	10.126.54.92	Multiple (186)	N/A	Multiple (2)
	1	Large ping	Event Name	Large ping	🟥	Multiple (106)	Multiple (46)	N/A	Check Point @ FW
	9	Excessive Firewall Denies Between Hosts containing Firewall Drop	Source IP	192.168.1.193	🟨	192.168.1.193	Multiple (3)	N/A	Multiple (2)

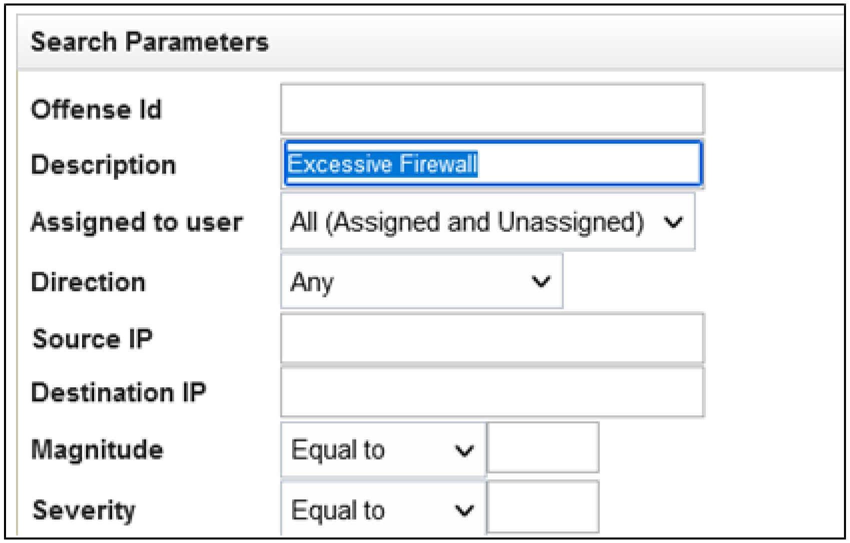
2. Select the Offense with the description **Local DNS Scanner containing Invalid DNS or Excessive Firewall Denies**

a. If you are not able to see the offense with this name, you may search for the offense.

b. From the **Search** list, click **New Search.**



c. In the Search parameters pane, define **Description** as any Keyword.



Search Parameters

Offense Id		
Description	Excessive Firewall	
Assigned to user	All (Assigned and Unassigned)	
Direction	Any	
Source IP		
Destination IP		
Magnitude	Equal to	
Severity	Equal to	

d. Click **Search.**

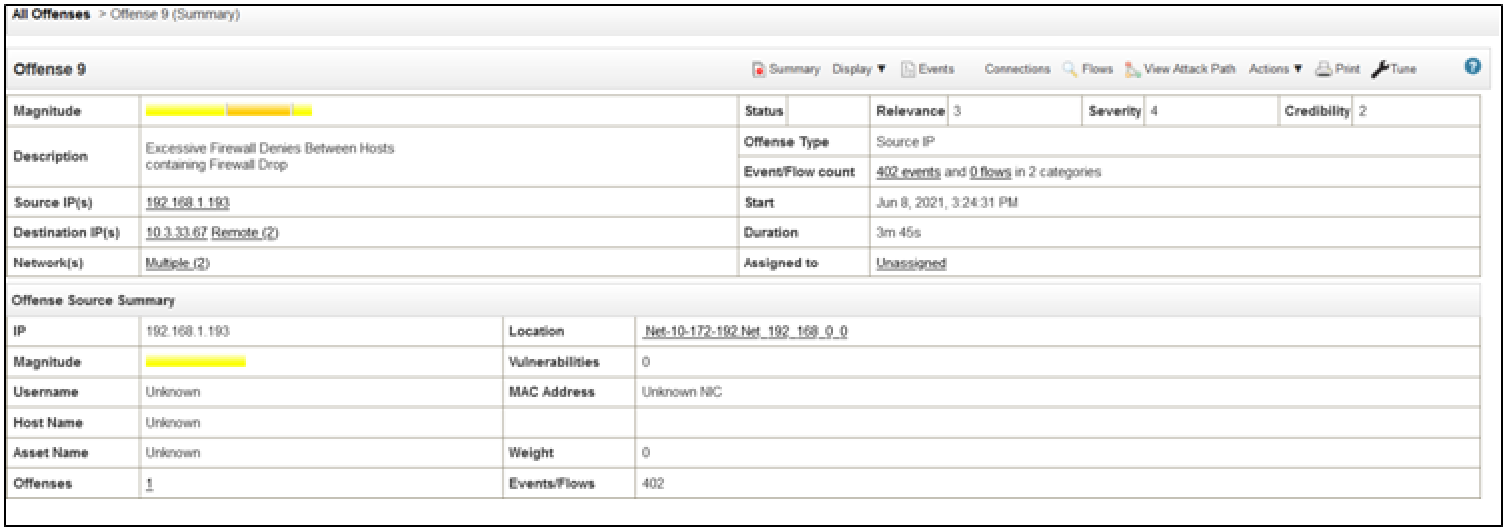
The All Offenses page will show the offenses that meet the search criteria.

3. Answer the following questions for the selected offense.

a. What is the offense type and offense source and magnitude?

b. What Network does the offense source IP belong to?

4. Double click the offense to view the offense Summary page. This summary page provides detailed information about the offense.



Offense 9

Magnitude		Status		Relevance	3	Severity	4	Credibility	2
Description	Excessive Firewall Denies Between Hosts containing Firewall Drop	Offense Type	Source IP						
		Event/Flow count	402 events and 0 flows in 2 categories						
Source IP(s)	192.168.1.193	Start	Jun 8, 2021, 3:24:31 PM						
Destination IP(s)	10.3.33.67 Remote (2)	Duration	3m 45s						
Network(s)	Multiple (2)	Assigned to	Unassigned						

Offense Source Summary

IP	192.168.1.193	Location	Net-10-172-192.Net_192_168_0_0
Magnitude		Vulnerabilities	0
Username	Unknown	MAC Address	Unknown NIC
Host Name	Unknown		
Asset Name	Unknown	Weight	0
Offenses	1	Events/Flows	402

5. Answer the following questions for this offense.

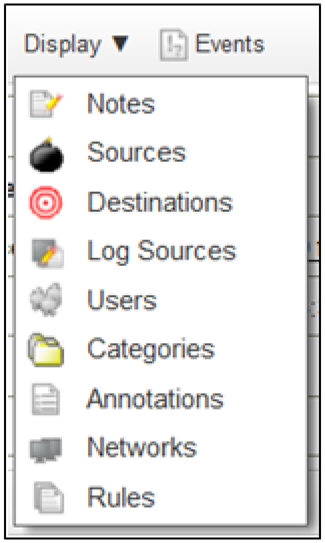
   a. How many events or flows have been added to this offense?

   b. What time did this offense begin?

   c. Is the Source IP involved in any other offenses?

   d. How many destination IPS are targets o the offense? Are the destination Ips local or remote?

   e. List the categories of the events that contributed to this offense. From the **Display** drop-down list on the toolbar, select **Categories** to display the event categories.



f. What do you learn about this offense based on the annotation? From the **Display** drop-down list on the toolbar, select **Annotations.**

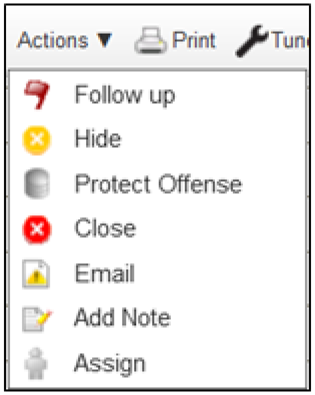
g. What is the event name, event category, and destination port for the events listed in the Last 10 Events list? Click Summary on the toolbar and scroll down to the Last 10 Events list.

h. For which service is the destination port well known?

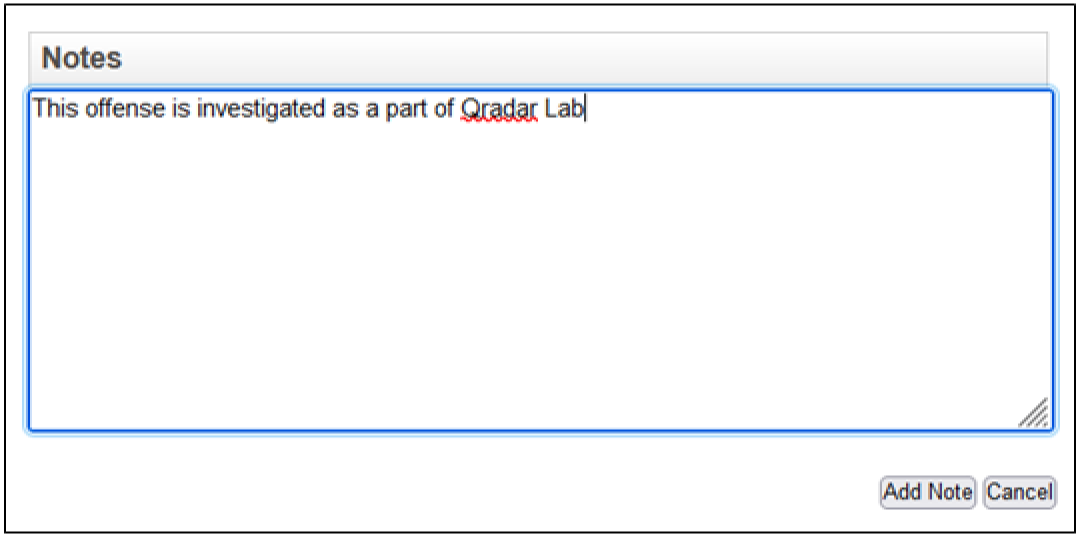
6. Perform the following actions on this offense.

a. Add a note:

i. From the **Actions** drop-down list, select **Add Note.**



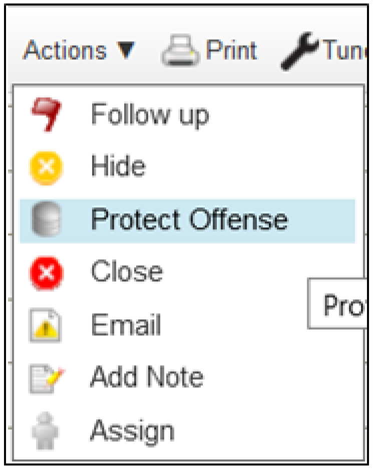
ii. Enter “This offense is investigated as a part of Qradar Lab”



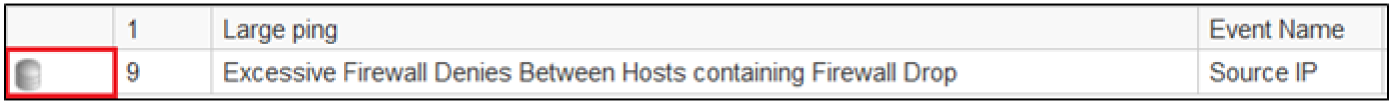
This offense is investigated as a part of Qradar Lab

iii. Click **Add Note.**

b. Protect the offense. From the **Actions** drop-down list on the Offense Summary page, select **Protect Offense.**



c. As a result, the **Protected** icon is displayed in the **Status** field on the Offense Summary page and in the flag column for the offense on the All Offenses page.



	1	Large ping	Event Name
	9	Excessive Firewall Denies Between Hosts containing Firewall Drop	Source IP