

**Temasek Polytechnic
School of Informatics & IT**

**Introduction to
Security Incident Response & Management**

**(Security Incident Investigation in a SOC Environment
with IBM Security QRadar SIEM)**

**IBM Security QRadar SIEM
Hands-on Lab Exercises**

IBM Security QRadar SIEM Hands-on Lab Exercises

	Hands-on Lab Exercises	Page No.
Investigating an offense that is triggered by events exercise	1. Investigating the Local DNS scanner offense	5
Investigating the events of an offense exercises	2. Looking for events that contribute to an offense 3. Saving search criteria and search results 4. Investigating event details	10 13 15
Investigating an offense that is triggered by flows exercise	5. Investigating an offense that is triggered by flows	19

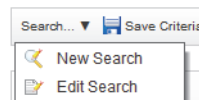


4 Investigating an offense that is triggered by events exercises

Exercise 1 Investigating the local DNS scanner offense

To investigate an offense triggered by events, this exercise looks at the offense named **Local DNS Scanner containing Invalid DNS**. Perform the following steps:

1. In the QRadar SIEM console, double-click the **Offenses** tab.
The All Offenses page opens.
2. Select the offense with the description **Local DNS Scanner containing Invalid DNS**.
 - a. If you do not see the **Local DNS Scanner containing Invalid DNS** offense, search for the offense. From the **Search** list, select **New Search**.



- - b. On the Search Parameters pane, define the search criteria. In the **Description** field, type Local DNS Scanner.



Search Parameters	
Offense Id	
Description	Local DNS Scanner
Assigned to user	All (Assigned and Unassigned)
Direction	Any
Source IP	
Destination IP	



Note: The description search criteria is case sensitive.

- -
 - c. Click **Search**.

The All Offenses page shows the offense that meets the search criteria, **Local DNS Scanner containing Invalid DNS**.

All Offenses View Offenses: Select An Option:					
Current Search Parameters:					
Description contains Local DNS Scanner (Clear Filter) , Exclude Hidden Offenses (Clear Filter) , Exclude Closed Offenses					
 Id	Description	Offense Type	Offense Source	Magnitude	
4	Local DNS Scanner containing Invalid DNS	Source IP	10.152.247.69		

3. Answer the following questions for the **Local DNS Scanner containing Invalid DNS** offense.
- What is the offense type and offense source and magnitude?



Hint: Hold the mouse over the **Magnitude** to obtain the numeric value.

- What network does the offense source IP belong to?



Hint: Hold the mouse over the **Offense Source IP** to obtain the network.

4. Double-click the **Local DNS Scanner containing Invalid DNS** offense to view the Offense Summary page. The Offense Summary page provides detailed information about the offense.

All Offenses > Offense 4 (Summary)

Offense 4

Summary

Display ▼

Events

Magnitude	<div><div></div></div>	Status		Relevance	3	Severity	
Description	Local DNS Scanner containing Invalid DNS	Offense Type	Source IP				
		Event/Flow count	155 events and 0 flows in 2 categories				
Source IP(s)	10.152.247.69	Start	Aug 23, 2013 3:36:37 AM				
Destination IP(s)	Local (153)	Duration	0s				
Network(s)	Net-10-172-192.Net 172 16 0 0	Assigned to	Unassigned				

Offense Source Summary

IP	10.152.247.69	Location	Net-10-172-192.Net 10 0 0 0
Magnitude	<div><div></div></div>	Vulnerabilities	0
User	Unknown	MAC	Unknown NIC
Host Name	Unknown		
Asset Name	Unknown	Weight	0
Offenses	1	Events/Flows	155

5. Answer the following questions for this offense.

a. How many events or flows are associated with this offense?

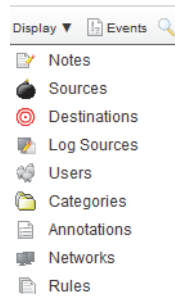
b. What time did this offense begin?

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

d. How many destinations IPs are targets of the offense? Are the destinations IPs local or remote devices?

Exercise 1 Investigating the local DNS scanner offense

- e. List the event categories that contributed to this offense. From the **Display** list on the toolbar, select **Categories** to view the event categories.



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

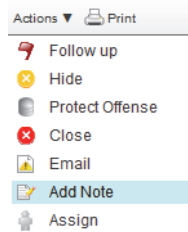
- g. What is the event name, event category, and destination port for the events listed in the **Last 10 Events** list? Click **Summary** on the toolbar and scroll down to the **Last 10 Events** list.

h. The destination port is well known for what type of server communications?

6. Perform the following actions on this offense.

a. Add a note:

i. From the **Actions** toolbar, select **Add Note**.



ii. Type This offense was investigated in the QRadar SIEM Foundations course.

iii. Click **Add Note**.



Note: The note is displayed in the Last 5 Notes pane on the Offense Summary page. A **Notes** 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. Hold the mouse over the **Notes** icon to view the note.

b. Protect the offense. From the **Actions** toolbar on the Offense Summary page, select **Protect Offense**. 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.

Offense 4				Summary		Display ▼		Events		Flows	
Magnitude		<div><div></div><div></div><div></div></div>		Status				Relevance		2	
Severity				Offense		This offense has been protected					
Description		Local DNS Scanner containing Invalid DNS		Event/Flow count		155 events and 0 flows in 2 c					

Why do you protect an offense?



5 Investigating the events of an offense exercises

Exercise 1 Looking for events that contribute to an offense

In [Unit 4, "Investigating an offense that is triggered by events exercises,"](#) on page 5, you investigated the offense by analyzing the offense summary information. In this exercise, you use the log events that are viewed in the **Log Activity** tab to further analyze the offense.

1. In the QRadar SIEM console, double-click the **Offenses** tab.
The All Offenses page opens.
2. Find and double-click the **Local DNS Scanner containing invalid DNS** offense.
3. Show the low-level categories of the offense's events by selecting **Display > Categories** on the toolbar.

Offense 4 (All Categories) ?

Offense 4 Summary Display ▾ Events Flows Actions ▾ Print

Magnitude	■■■	Notes	3	Severity	3	Credibility	3
Description	Local DNS Scanner containing Invalid DNS	Sources					
Source IP(s)	10.152.247.69	Destinations	s and 0 flows in 2 categories				
Destination IP(s)	Local (153)	Log Sources	013 3:34:20 AM				
Network(s)	Net-10-172-192.Net 172.16.0.0	Users					
		Categories					
		Annotations					
		Networks					
		Rules					

List of Event Categories Events Flows

Name	Magnitude	Local Destination Count	Events/Flo	First Event/Flov	Last Event/Flow
DNS Reconnaissance	■■■	2	2	Aug 23, ...	Aug 23, ...
DNS Protocol Anomaly	■■■	153	153	Aug 23, ...	Aug 23, ...

4. To investigate the events that are associated with this offense in the low-level category DNS Protocol Anomaly, right-click the table row that shows **DNS Protocol Anomaly** and click **Events**.



Note: Alternatively, you can select **DNS Protocol Anomaly** and click **Events** in the title bar above the table.

List of Event Categories					
Name	Magnitude	Local Destination Count	Events/Flo	First Event/Flov	Last Event/Flov
DNS Reconnaissance	<div><div></div><div></div><div></div></div>	2	2	Aug 23, ...	Aug 23, ...
DNS Protocol Anomaly	<div><div></div><div></div><div></div></div>	153	153	Aug 23, ...	Aug 23, ...

The List of Events page opens.

- Create a filter to exclude the source IP that contributed to the **Local DNS Scanner** offense. Select an event. Right-click **10.152.247.69** and select **Filter on Source IP is not 10.152.247.69**.

Viewing events from Aug 23, 2013 3:34:23 AM to Aug 23, 2013 3:34:26 AM

View: Select An Option:

Display: Default (Normalized)

Completed

Current Filters:

Offense is Local DNS Scanner (Clear Filter), Low Level Category is DNS Protocol Anomaly (Clear Filter)

► Current Statistics

Records Matched Over Time

Reset Zoom

8/22/13 6:34 PM - 8/22/13 6:34 PM

100

50

0

6:34:26 PM

6:34:26 PM

6:34:26 PM

6:34:26 PM

6:34:26 PM

6:34:26 PM

6:34:26 PM

6:34:26 PM

6:34:26 PM

6:34:26 PM

Update Details

(Hide Charts)

Event Name	Log Source	Eve Cou	Time	Low Level Category	Source IP	Source Port	Destination IP	Dest Port	Use	Magnitude
Invalid DNS	CheckPoint @ FW-1...	1	8/23/13 ...	DNS Protocol Anomaly	10.152.247.69	58571	172.17.0.162	53	N/A	<div><div></div><div></div><div></div></div>
Invalid DNS	CheckPoint @ FW-1...	1	8/23/13 ...	DNS Protocol Anomaly	10.152.247.69	58571	172.17.0.162	53	N/A	<div><div></div><div></div><div></div></div>
Invalid DNS	CheckPoint @ FW-1...	1	8/23/13 ...	DNS Protocol Anomaly	10.152.247.69	58571	172.17.0.162	53	N/A	<div><div></div><div></div><div></div></div>
Invalid DNS	CheckPoint @ FW-1...	1	8/23/13 ...	DNS Protocol Anomaly	10.152.247.69	58571	172.17.0.162	53	N/A	<div><div></div><div></div><div></div></div>
Invalid DNS	CheckPoint @ FW-1...	1	8/23/13 ...	DNS Protocol Anomaly	10.152.247.69	58571	172.17.0.162	53	N/A	<div><div></div><div></div><div></div></div>
Invalid DNS	CheckPoint @ FW-1...	1	8/23/13 ...	DNS Protocol Anomaly	10.152.247.69	58571	172.17.0.162	53	N/A	<div><div></div><div></div><div></div></div>
Invalid DNS	CheckPoint @ FW-1...	1	8/23/13 ...	DNS Protocol Anomaly	10.152.247.69	58571	172.17.0.162	53	N/A	<div><div></div><div></div><div></div></div>
Invalid DNS	CheckPoint @ FW-1...	1	8/23/13 ...	DNS Protocol Anomaly	10.152.247.69	58571	172.17.0.162	53	N/A	<div><div></div><div></div><div></div></div>
Invalid DNS	CheckPoint @ FW-1...	1	8/23/13 ...	DNS Protocol Anomaly	10.152.247.69	58571	172.17.0.162	53	N/A	<div><div></div><div></div><div></div></div>
Invalid DNS	CheckPoint @ FW-1...	1	8/23/13 ...	DNS Protocol Anomaly	10.152.247.69	58571	172.17.0.162	53	N/A	<div><div></div><div></div><div></div></div>

Displaying 1 to 40 of 94 items (Elapsed time: 0:00:00.622)

© Copyright IBM Corp. 2012, 2013. All rights reserved.

Page: 1 Go < 1 2 3 >

- What results are returned?

- What do the results of this search indicate?

8. To look for similar DNS requests unrelated to the offense, click **Clear Filter** for the **Offense is Local DNS Scanner** filter.

Viewing events from Aug 23, 2013 3:34:23 AM to Aug 23, 2013 3:34:26 AM View:

Display:

Original Filters:
 Offense is Local DNS Scanner [\(Clear Filter\)](#), Low Level Category is DNS Protocol Anomaly

Current Filters:
 Source IP is not 10.152.247.69 [\(Clear Filter\)](#)

► Current Statistics

Event Name	Log Source	Eve Cou	Time ▼	Low Level Category	Source IP
No results were returned.					

9. What results are returned? Why?

10. To view events from the last 24 hours, in the **View** list, select **Last 24 Hours**.

Viewing events from Aug 23, 2013 3:34:23 AM to Aug 23, 2013 3:34:26 AM View:

Display:

Current Filters:
 Low Level Category is DNS Protocol Anomaly [\(Clear Filter\)](#), Source IP is not 10.152.2

► Current Statistics

Records Matched Over Time

Reset Zoom
 0.05

0.025

0

6:34:26 PM 6:34:26 PM 6:34:26 PM 6:34:26 PM 6:34:26 PM 6:34:26 PM 6:34:26 PM 6:34:26 PM 6:34:26 PM 6:34:26 PM 6:34:26 PM

Update Details

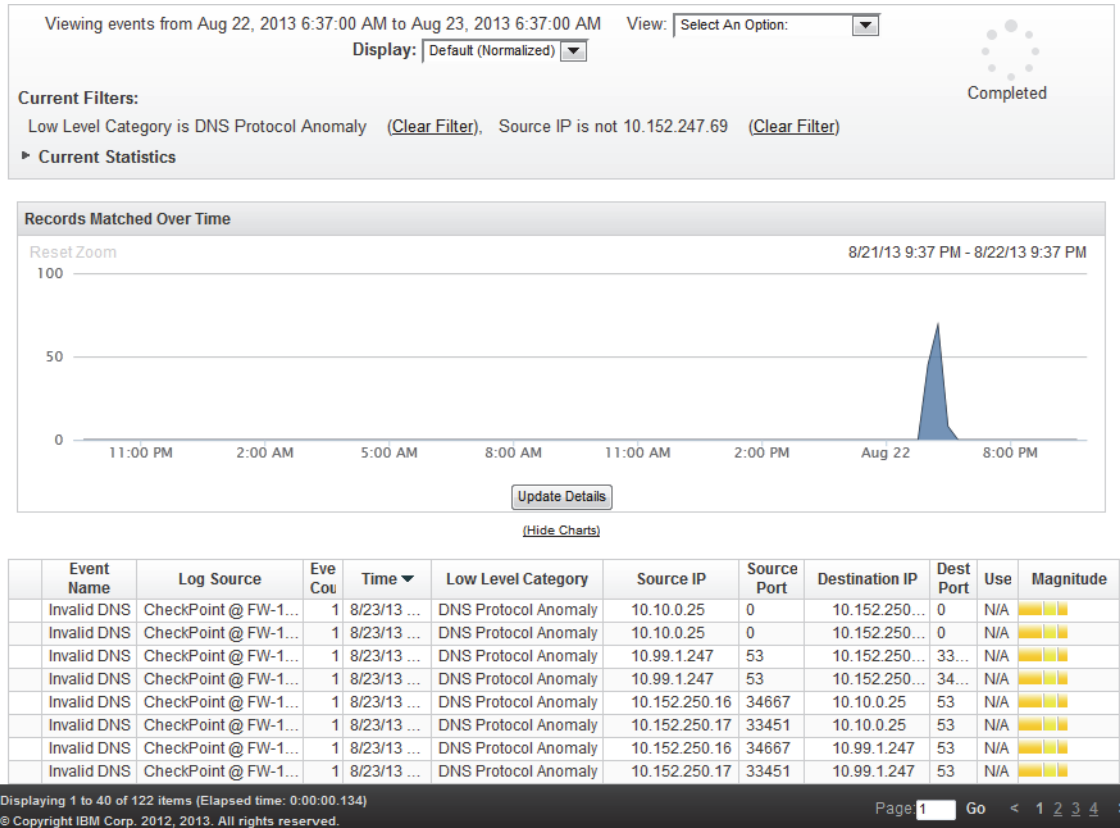
(Hide Charts)

2/13 6:34 PM - 8/22/13 6:34 PM

Event Name	Log Source	Eve Cou	Time ▼	Low Level Category	Source IP	Source Port	Destination IP	Dest Port	Use	Magnitude
No results were returned.										

QRadar SIEM shows events of the low-level category DNS Protocol Anomaly that do not originate from the IP address 10.152.247.69, which is the source IP address of the offense triggered by DNS scanning.

11. Review the suspicious DNS requests from other sources.

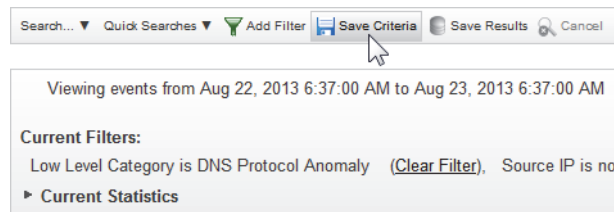


Exercise 2 Saving search criteria and search results

To save the search criteria and search results for future reference, perform the following steps:

1. Save the current search criteria.
 - a. On the toolbar, click **Save Criteria**.

The Save Criteria window opens.



- b. Configure the Save Criteria window as shown in the following table:

Field / Option	Setting
Search Name	Dept - DNS Protocol Anomaly without 10.152.247.69
Assign Search to Group(s)	CheckPoint
Timespan options	Recent Last 24 Hours
Include in my Quick Searches	Enable
Set as Default	Disable
Share with Everyone	Disable

c. Verify that the Save Criteria settings look like the ones in the graphic.

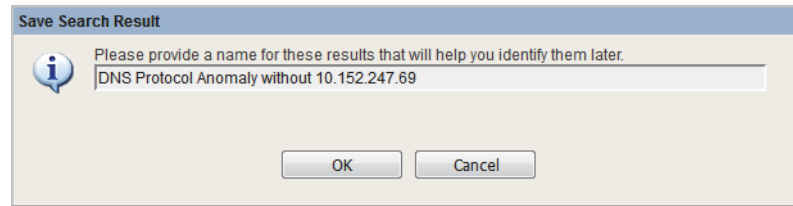
d. Click **OK**.

2. Save the current search results.

a. On the toolbar, click **Save Results**.

The Save Search Result window opens.

- b. In the **name** field, type DNS Protocol Anomaly without 10.152.247.69.

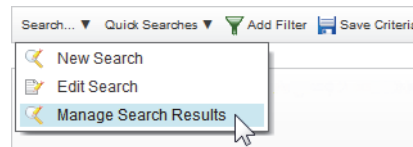


A dialog box titled "Save Search Result" with a blue header bar. It contains an information icon on the left and a text input field on the right. The text input field contains the text "DNS Protocol Anomaly without 10.152.247.69". Below the input field are two buttons: "OK" and "Cancel".

- c. Click **OK**.

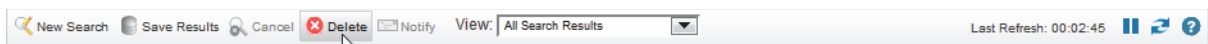
3. Revisit or delete your saved search results.

- a. On the List of Events page's toolbar, click **Search > Manage Search Results**.



The Search Results Management page opens.

- b. Select your search results and click **Delete**.



A screenshot of the Search Results Management page toolbar. It includes buttons for "New Search", "Save Results", "Cancel", "Delete", and "Notify". The "Delete" button is highlighted with a mouse cursor. To the right of the buttons is a "View:" dropdown menu set to "All Search Results" and a "Last Refresh: 00:02:45" timestamp.

F...	User	Name	Started On	Ended On	Duration	Expires On	Status	Size
	admin	DNS Protocol Anomaly without 10.152.247.69	Aug 23, 2013 9:51:12 AM	Aug 23, 2013 9:51:12 AM	346ms	Never	COMPLETED	100.7 KB
	admin	Default (Normalized) / Low Level Category is...	Aug 23, 2013 9:51:00 AM	Aug 23, 2013 9:51:00 AM	6ms	Aug 24, 20...	COMPLETED	4.3 KB
	admin	Default (Normalized) / Offense is Local DNS ...	Aug 23, 2013 9:50:55 AM	Aug 23, 2013 9:50:55 AM	19ms	Aug 24, 20...	COMPLETED	4.3 KB
	admin	Default (Normalized) / Offense is Local DNS ...	Aug 23, 2013 9:50:45 AM	Aug 23, 2013 9:50:45 AM	47ms	Aug 24, 20...	COMPLETED	80.7 KB
	admin	Default (Normalized) / Source IP is not 10.15...	Aug 23, 2013 6:37:38 AM	Aug 23, 2013 6:37:39 AM	315ms	Aug 24, 20...	COMPLETED	100.7 KB
	admin	Default (Normalized) / Low Level Category is...	Aug 23, 2013 6:35:42 AM	Aug 23, 2013 6:35:42 AM	6ms	Aug 24, 20...	COMPLETED	4.3 KB
	admin	Default (Normalized) / Offense is Local DNS ...	Aug 23, 2013 6:33:52 AM	Aug 23, 2013 6:33:52 AM	3ms	Aug 24, 20...	COMPLETED	4.3 KB
	admin	Default (Normalized) / Offense is Local DNS ...	Aug 23, 2013 6:17:29 AM	Aug 23, 2013 6:17:29 AM	23ms	Aug 24, 20...	COMPLETED	80.7 KB
	admin	Default (Normalized) / Associated With Offen...	Aug 23, 2013 4:19:24 AM	Aug 23, 2013 4:19:24 AM	70ms	Aug 24, 20...	COMPLETED	6.7 KB

- c. Close the Search Results Management page.

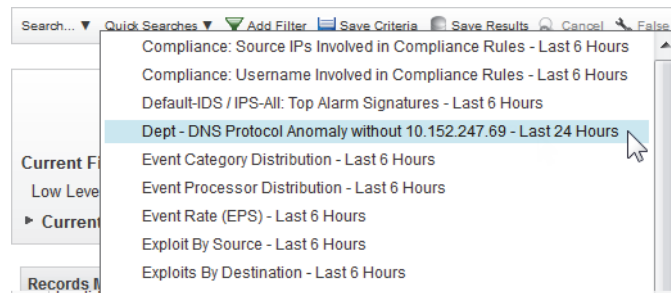
Exercise 3 Investigating event details

The details of an event, particularly its payload, can provide further insights. To investigate the details of an event, perform the following steps:

- Find and run your saved search.
 - In the QRadar SIEM console, double-click the **Log Activity** tab.
 - On the **Log Activity** tab toolbar, click **Quick Searches**.
 - Select **Dept - DNS Protocol Anomaly without 10.152.247.69 - Last 24 Hours**.



Hint: If you do not see your saved search, double-click the **Log Activity** tab and click **Quick Searches** again.



d. In the search result, double-click an event.

The Event Details page opens in the **Log Activity** tab.

2. Verify with the firewall and DNS experts of your organization whether the log message that is displayed in the payload is a concern.

Return to Event List
Offense
Map Event
False Positive
Extract Property
Previous
Next
Print

Next Item (Shift + >)

Event Information

Event Name:	Invalid DNS				
Low Level Category:	DNS Protocol Anomaly				
Event Description:	DNS cache poisoning occurs when false DNS records are injected into a DNS server's cache tables. Once the cache tables have been altered, a remote attacker may inspect, capture or corrupt any information exchanged between hosts on the network. By poisoning a DNS server, a remote attacker could, for example, direct users to malicious sites or prevent them from accessing web sites of their choice.				
Magnitude:	<div><div></div><div></div><div></div></div> (5)	Relevance:	6	Severity:	3
Credibility:	5				
Username:	N/A				
Start Time:	Aug 23, 2013 3:34:26 AM	Storage Time:	Aug 23, 2013 3:34:26 AM	Log Source Time:	Jul 7, 2009 10:21:47 AM
Policy:	N/A				

Source and Destination Information

Source IP:	10.152.247.69	Destination IP:	172.17.0.161
Source Asset Name:	N/A	Destination Asset Name:	N/A
Source Port:	51316	Destination Port:	53
Pre NAT Source IP:		Pre NAT Destination IP:	
Pre NAT Source Port:	0	Pre NAT Destination Port:	0
Post NAT Source IP:		Post NAT Destination IP:	
Post NAT Source Port:	0	Post NAT Destination Port:	0
IPv6 Source:	0:0:0:0:0:0:0:0	IPv6 Destination:	0:0:0:0:0:0:0:0
Source MAC:	00:00:00:00:00:00	Destination MAC:	00:00:00:00:00:00

Payload Information

utf
hex
base64

☒ Wrap Text

```
<182>Aug 23 03:34:26 FW-1Machine <13>Jul 07 10:21:47 checkpoint.firewall-1.test.com 07Jul2009
10:21:47 drop 10.152.246.249 product: SmartDefense; src: 10.152.247.69; s_port: 51316; dst:
172.17.0.161; service: 53; proto: udp; rule: ;Attack Info: Illegal number of Resource
Records;__policy_id tag: product=VPN-1 & FireWall-1[db tag={C8518DA6-6A76-11DE-
8CAA-0A98F6F93F3F};mgmt=MNET_CMA;date=1246916926;policy_name=Standard];attack: Invalid
DNS;has_accounting: 0;i/f_dir: outbound;i/f_name: CRMN.1004;orig_name:
MNET7_MNETVS;origin_sic_name: CN=MNET7_MNETVS,O=MNET_CMA..aobkgn;
```



Note: Use **Previous** and **Next** on the Events Details toolbar to browse the events.

3. To return to the list of events, on the toolbar, click **Return to Event List**.

(This page intentionally left blank)



7 Investigating an offense that is triggered by flows exercises

Exercise 1 Investigating an offense that is triggered by flows

To investigate an offense that is triggered by flows, perform the following steps:

1. Generate network traffic. In the PuTTY command line, type the following command:

```
./startRdp.sh
```

```
[root@COE labfiles]# ./startRdp.sh
sending out eth0
processing file: /labfiles/flows/extrdp.pcap
Actual: 311 packets (79977 bytes) sent in 7.98
ated: 10022.2 bps, 0.08 Mbps, 38.97 pps
Statistics for network device: eth0
    Attempted packets:      311
    Successful packets:     311
    Failed packets:         0
    Retried packets (ENOBUFS): 0
    Retried packets (EAGAIN): 0
[root@COE labfiles]#
```

2. In the QRadar SIEM console, click the **Network Activity** tab.
3. Observe the network events and verify that a network event triggers an offense.

9/11/13 12:05:50 AM	9.9.8.42	51716	192.168...	3389	tcp_ip	RemoteAccess.MSTerminalServices	41,488 (C)	39,733 (C)
---------------------	----------	-------	------------	------	--------	---------------------------------	------------	------------



Note: QRadar SIEM shows a red icon in the left-most column for network events that contribute to an offense.

4. To investigate the offense, click the red icon in the left-most column.



Note: There is a delay between the time the red icon is shown next to the network event and when the offense is created on the All Offenses page in the Offenses tab.



Note: Disable block pop-up windows in Firefox. On the Firefox toolbar, select **Tools > Options > Content > Disable block pop-up windows > OK**.

The Offense Summary page opens.

Offense 1

Summary

Display ▼


Events

Flows


Actions ▼

Print

?

Magnitude	<div><div></div></div>	Status		Relevance	6	Severity	5	Credibility	3
Description	Remote Desktop Access from the Internet containing RemoteAccess.MSTerminalServices	Offense Type	Source IP						
		Event/Flow count	1 events and 1 flows in 2 categories						
Source IP(s)	 9.9.8.42	Start	Sep 11, 2013 12:06:49 AM						
Destination IP(s)	192.168.10.12 (192.168.10.12)	Duration	0s						
Network(s)	Net-10-172-192.Net 192 168 0 0	Assigned to	Unassigned						

Offense Source Summary

IP	 9.9.8.42	Location	UnitedStates
Magnitude	<div><div></div></div>	Vulnerabilities	0
User	Unknown	MAC	Unknown NIC
Host Name	Unknown		
Asset Name	Unknown	Weight	0
Offenses	1	Events/Flows	2

5. What is the name of the offense?

6. What is the offense type and offense source?

7. What is the destination IP?

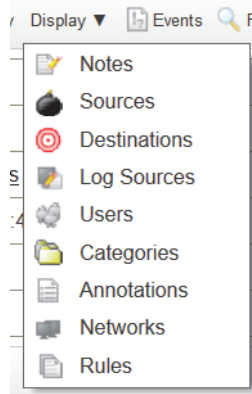
8. How many events are associated with this offense?

How many flows are associated with this offense?

9. What rule contributed to this offense?

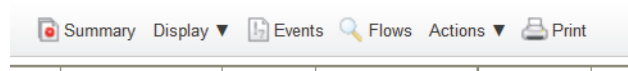


Hint: To determine which rule triggered the offense, click the **Display** list and select **Rules**.

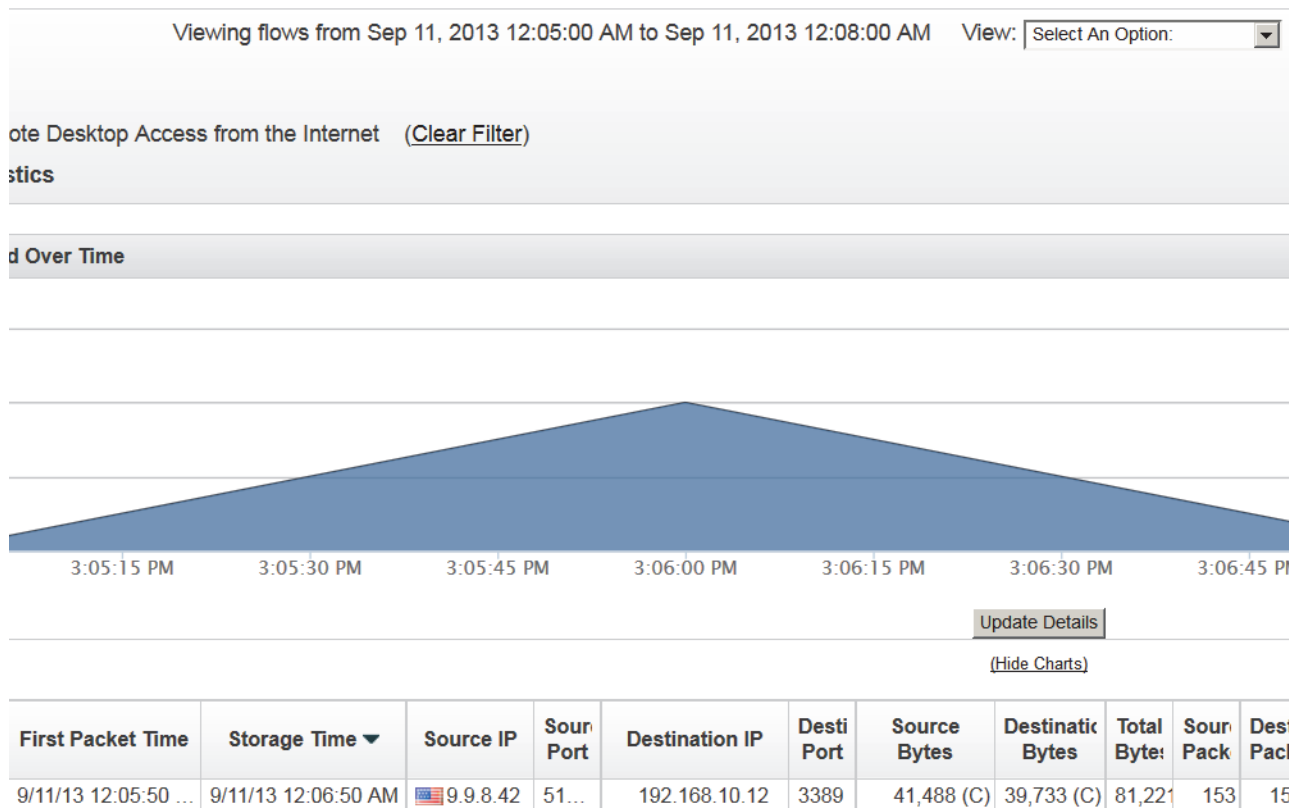


Note: The *Policy Remote: Remote Desktop Access from the Internet* rule that triggered this offense is one of the default rules in the Enterprise tuning template. The rule evaluates Remote Desktop Access from external IP addresses to internally hosted Microsoft Windows servers.

10. To investigate the flows that contributed to the offense, click **Flows** on the Offense Summary page toolbar.



The Flow List page opens.



11. Examine the flow associated with this offense. Double-click the network event listed.

The Flow Details page opens.

12. Answer the following questions:

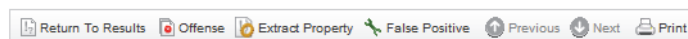
a. What is the flow direction?

b. What is the application name?

c. Based on your investigation, what behavior triggered this offense?

13. Tune the network event as a false positive.

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



The False Positive page opens.

False Positive

False positive tuning allows you to prevent event/flow(s) from correlating into offenses.

Event/Flow Property

- ☒ Event/Flow(s) with a specific QID of 53265624 (*RemoteAccess.MSTerminalServices*)
- ☐ Any Event/Flow(s) with a low level category of *Remote Access*
- ☐ Any Event/Flow(s) with a high level category of *Application*

Traffic Direction

- ☒ 9.9.8.42 to 192.168.10.12
- ☐ 9.9.8.42 to Any Destination
- ☐ Any Source to 192.168.10.12
- ☐ Any Source to any Destination

Cancel Tune

- b. Click **Tune**.
- c. Click **Close**.



Note: Tuning an event or flow as a false positive updates the **User-BB-FalsePositive: User Defined False Positives** building block.

- 14. Close the Flow Details page.
- 15. Close the offense.
 - a. On the **Offense** tab navigation menu, select **All Offenses**.
 - b. From the **Actions** list on the toolbar, select **Close**.
 - c. From the **Reason for Closing** list, select **False-Positive, Tuned**.
 - d. Click **OK**.