REAL EXAMPLE OF OFFENSES/ ALERTS INVESTIGATION USING QRADAR

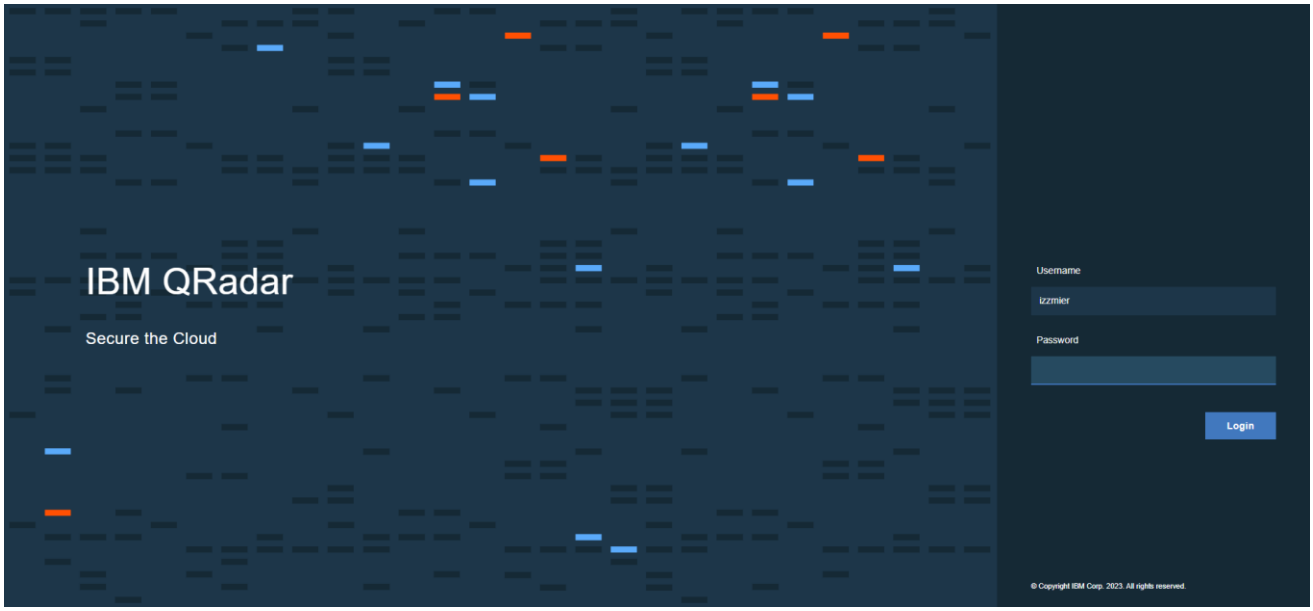
BY: IZZMIER IZZUDDIN ZULKEPLI

INTRODUCTION

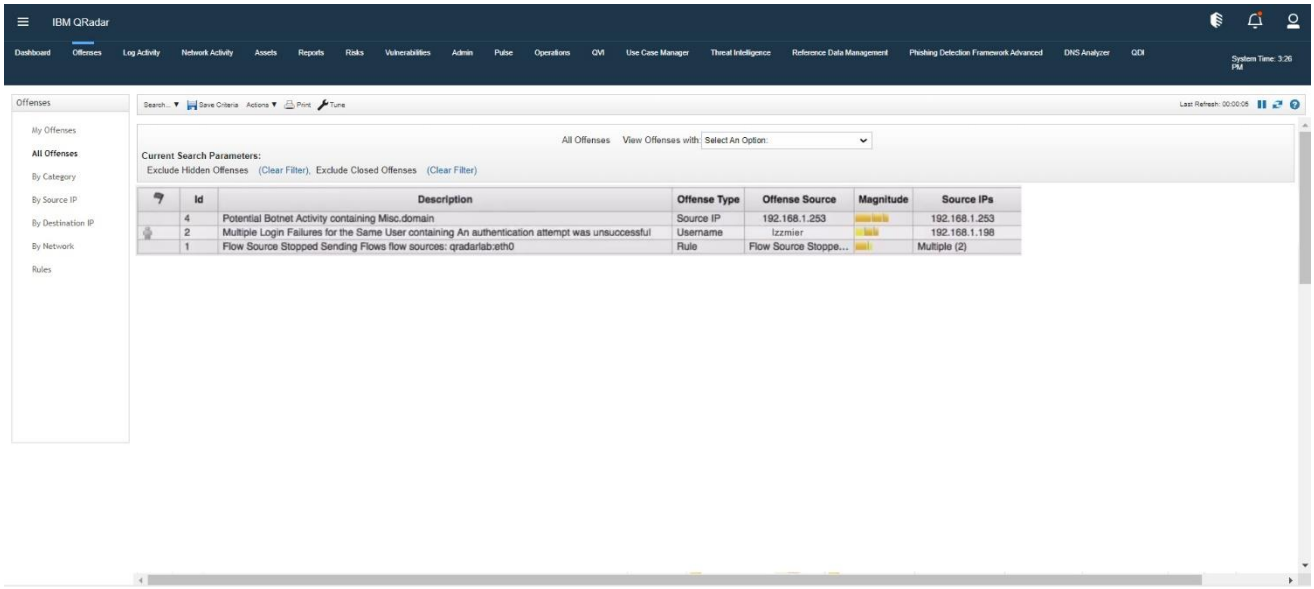
This writeup will show you how to investigate the offenses/alerts using one of the following SIEM, QRadar. Let's go to QRadar and do the offense investigation from start to finish. As we are ready familiar with the brute force attack, let's take it as example and do full offense investigation.

BRUTE FORCE

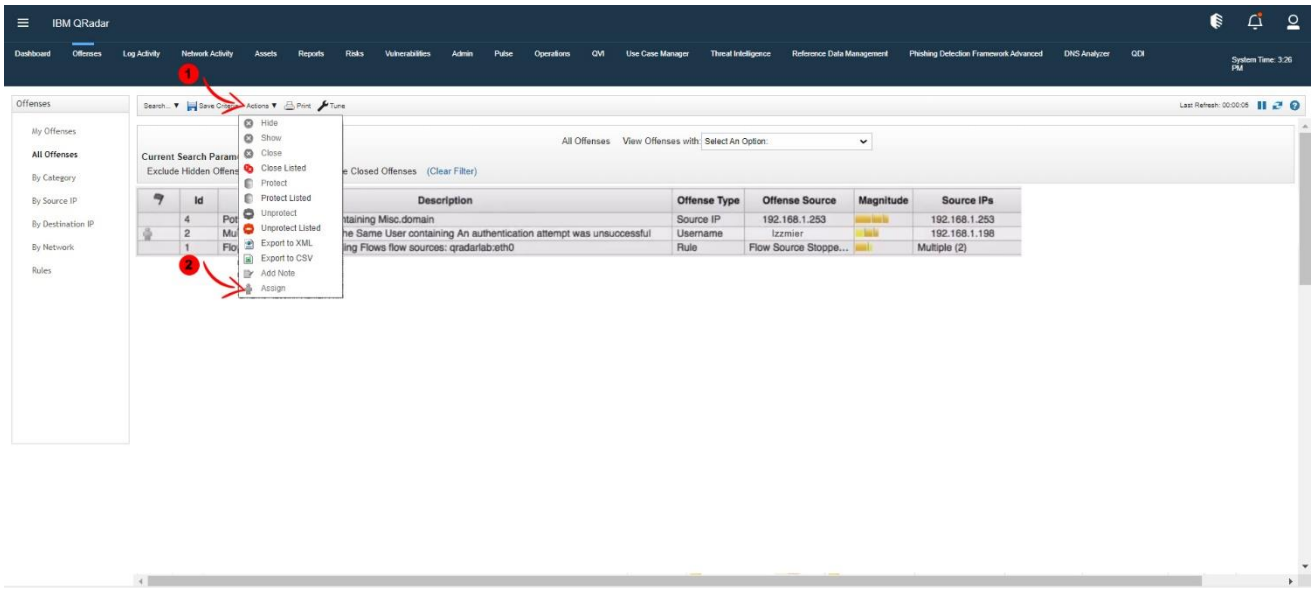
Login the QRadar with our own credentials. Every time we do the investigation make sure using our own account.



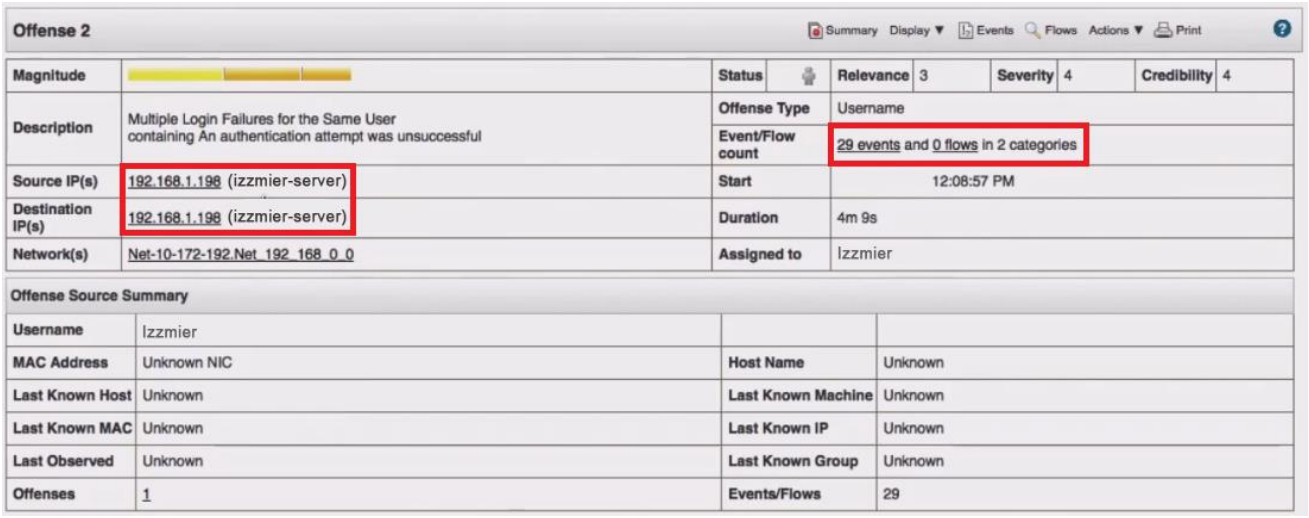
After login, click offenses tab and you can see list of the new offense. We choose offense no 2, **Multiple Login Failures for the Same User containing An authentication attempt was unsuccessful**.



First thing we need to do after choosing the offense to investigate is assign the offense to ourselves. Click action then click assign. Now the offense assigned.



Let's double click the offense to open the details. The first thing I want to check is original data.



There are 29 events related to offense. At event/flow count tab, click the "29 events" and you can see all the events.

By taking a quick look at the events list, it seen the non-automated brute force because of two things:

I. Long number of attempts
II. There is no pattern between attempts

For example, if an attacker used the automatic script, you would see 5 or 10 attempts per second. We have the first clue here; there is non- automated attack. Note that the source and destination at the same IP address mean someone direct access to the machine trying password, most likely not remote access. We got a second clue here; the person was on the machine.

(Hide Charts)

Event Name	Log Source	Even Coun	Time	Low Level Category	Source IP	Source Port	Destin
An authentication attempt was unsuccessful	(izzmier-server)	1	12:13:06 PM	General Authentication Failed	192.168.1.198	0	192.168
An authentication attempt was unsuccessful	(izzmier-server)	1	12:13:06 PM	General Authentication Failed	192.168.1.198	0	192.168
An authentication attempt was unsuccessful	(izzmier-server)	1	12:12:43 PM	General Authentication Failed	192.168.1.198	0	192.168
An authentication attempt was unsuccessful	(izzmier-server)	1	12:12:43 PM	General Authentication Failed	192.168.1.198	0	192.168
An authentication attempt was unsuccessful	(izzmier-server)	2	12:11:30 PM	General Authentication Failed	192.168.1.198	0	192.168
An authentication attempt was unsuccessful	(izzmier-server)	2	12:11:30 PM	General Authentication Failed	192.168.1.198	0	192.168
An authentication attempt was unsuccessful	(izzmier-server)	2	12:11:15 PM	General Authentication Failed	192.168.1.198	0	192.168
An authentication attempt was unsuccessful	(izzmier-server)	2	12:11:15 PM	General Authentication Failed	192.168.1.198	0	192.168
An authentication attempt was unsuccessful	(izzmier-server)	2	12:10:59 PM	General Authentication Failed	192.168.1.198	0	192.168
An authentication attempt was unsuccessful	(izzmier-server)	2	12:10:42 PM	General Authentication Failed	192.168.1.198	0	192.168
An authentication attempt was unsuccessful	(izzmier-server)	1	12:10:28 PM	General Authentication Failed	192.168.1.198	0	192.168
An authentication attempt was unsuccessful	(izzmier-server)	1	12:10:28 PM	General Authentication Failed	192.168.1.198	0	192.168
Multiple Login Failures for the Same User	Custom Rule Engine-8 :: qra...	1	12:10:26 PM	User Login Failure	192.168.1.198	0	192.168
An authentication attempt was unsuccessful	(izzmier-server)	1	12:10:15 PM	General Authentication Failed	192.168.1.198	0	192.168
An authentication attempt was unsuccessful	(izzmier-server)	1	12:10:15 PM	General Authentication Failed	192.168.1.198	0	192.168
An authentication attempt was unsuccessful	(izzmier-server)	1	12:10:01 PM	General Authentication Failed	192.168.1.198	0	192.168
An authentication attempt was unsuccessful	(izzmier-server)	1	12:10:01 PM	General Authentication Failed	192.168.1.198	0	192.168
An authentication attempt was unsuccessful	(izzmier-server)	1	12:09:22 PM	General Authentication Failed	192.168.1.198	0	192.168
An authentication attempt was unsuccessful	(izzmier-server)	2	12:09:07 PM	General Authentication Failed	192.168.1.198	0	192.168
An authentication attempt was unsuccessful	(izzmier-server)	1	12:09:03 PM	General Authentication Failed	192.168.1.198	0	192.168
An authentication attempt was unsuccessful	(izzmier-server)	1	12:08:59 PM	General Authentication Failed	192.168.1.198	0	192.168
An authentication attempt was unsuccessful	(izzmier-server)	1	12:08:57 PM	General Authentication Failed	192.168.1.198	0	192.168

Next, check for other suspicious behavior from the user on that day. Scroll down to the same page then you can see another detail. Right click on the username and click view events.

Top 5 Source IPs

Source IP	Magnitude	Location	Vulnerability	User	MAC	Weight	Offenses	Destination(s)	Last Event/Flow	Events
192.168.1.198		Net-10-172-19...	Yes	Unknown	Unknown NIC	0	2	1	4h 13s	31

Top 5 Destination IPs

Destination IP	Magnitude	Location	Vulnerability	Chained	User	MAC	Weight	Offenses	Source(s)	Last Event/Flow	Events
192.168.1.198		Net-10-172-1...	Yes	No	Unknown	Unknown NIC	0	1	1	3d 5h 36m 31s	29

Top 5 Log Sources

Name	Description	Group	Events	Offenses	Total Events
ricardo-server			28	1	28
Custom Rule Engine-8 :: qra...	Custom Rule Engine		1	4	9

Top 5 Users

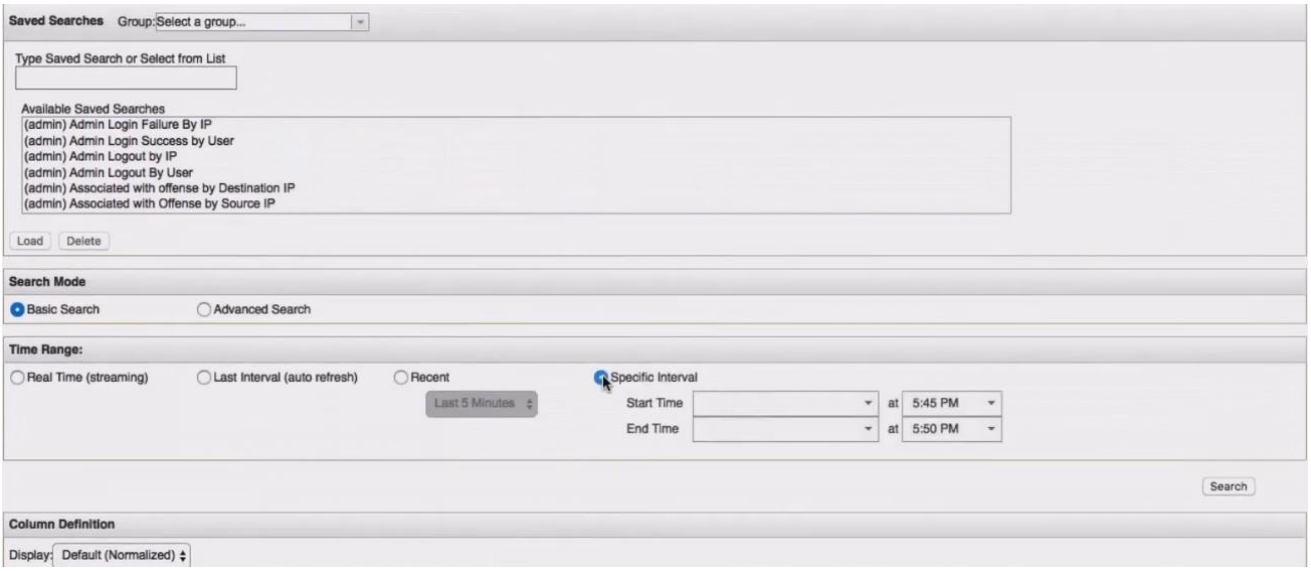
Name	Events/Flows	Offenses	Total Events/Flows
Izzmier	29	1	29

View Assets
View Events

Top 5 Categories

Name	Magnitude	Local Destination Count	Events/Flows	First Event/Flow	Last Event/Flow
User Login Failure		1	1		
General Authenticati...		1	28		

Select the time frame and click search.



Saved Searches Group: Select a group...

Type Saved Search or Select from List

Available Saved Searches
(admin) Admin Login Failure By IP
(admin) Admin Login Success by User
(admin) Admin Logout by IP
(admin) Admin Logout By User
(admin) Associated with offense by Destination IP
(admin) Associated with Offense by Source IP

Load Delete

Search Mode

Basic Search Advanced Search

Time Range:

Real Time (streaming) Last Interval (auto refresh) Recent Specific Interval

Last 5 Minutes

Start Time at 5:45 PM

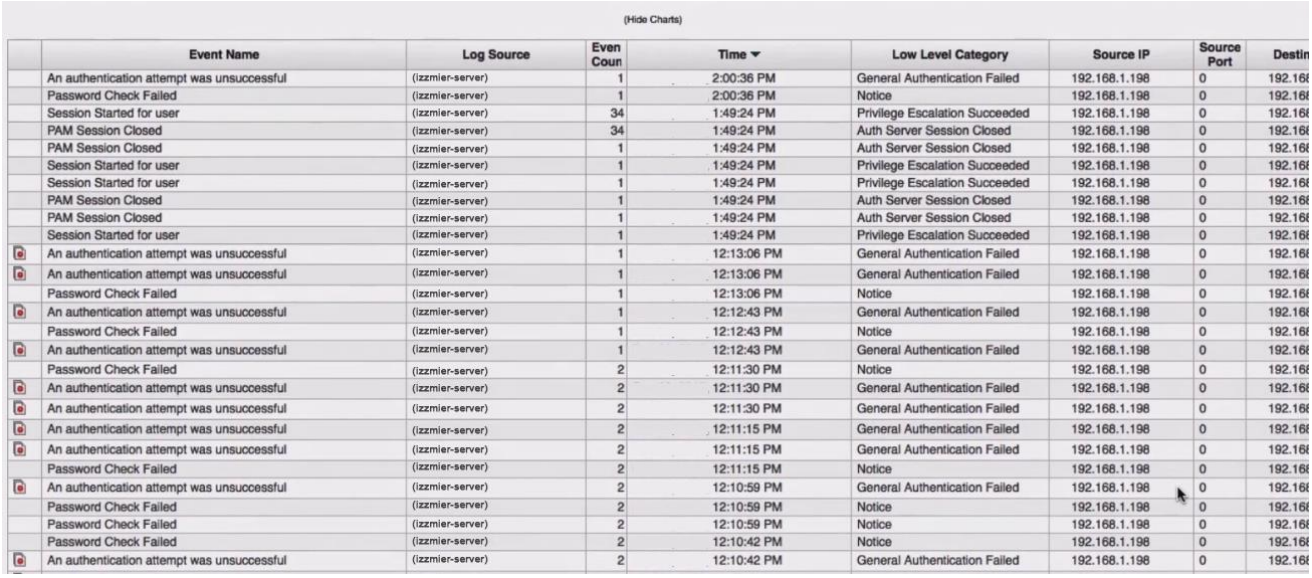
End Time at 5:50 PM

Search

Column Definition

Display: Default (Normalized)

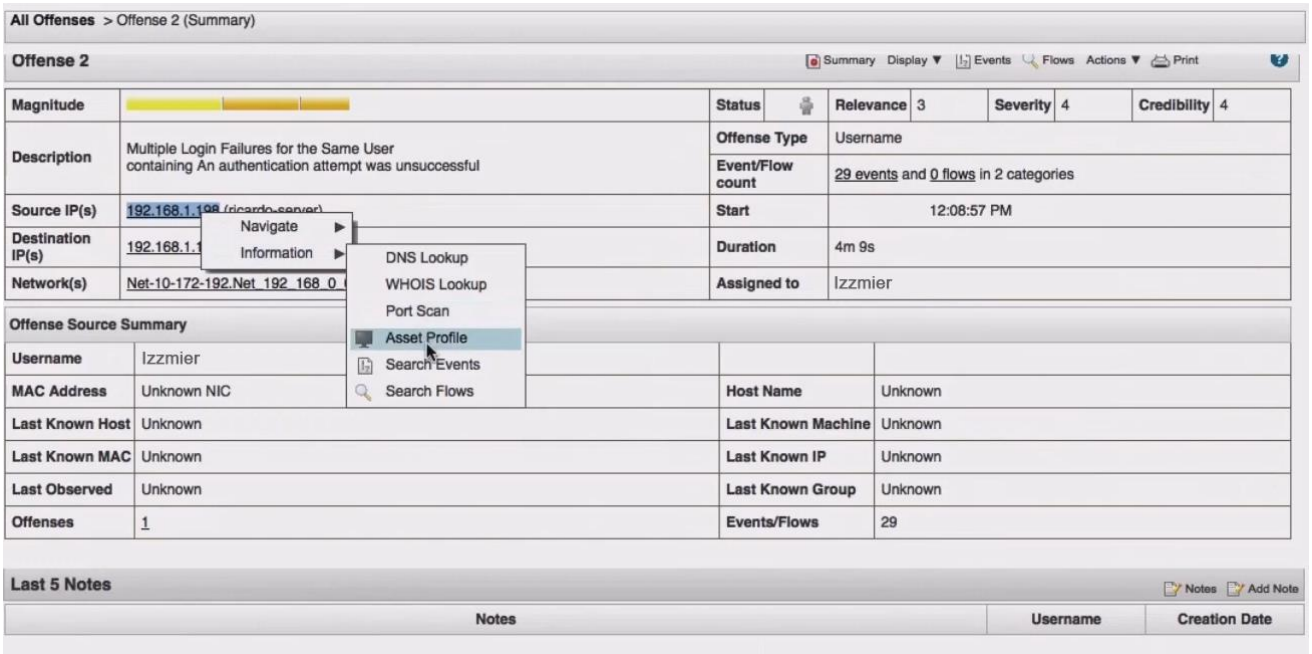
So, we have a list of events between the time frame. Take a quick look at the result, it's seen no other malicious behavior other than failed authentication. We can't yet close the case even if we don't see other malicious behavior.



(Hide Charts)

	Event Name	Log Source	Even Coun	Time ▾	Low Level Category	Source IP	Source Port	Destin
	An authentication attempt was unsuccessful	(izzmier-server)	1	2:00:36 PM	General Authentication Failed	192.168.1.198	0	192.168
	Password Check Failed	(izzmier-server)	1	2:00:36 PM	Notice	192.168.1.198	0	192.168
	Session Started for user	(izzmier-server)	34	1:49:24 PM	Privilege Escalation Succeeded	192.168.1.198	0	192.168
	PAM Session Closed	(izzmier-server)	34	1:49:24 PM	Auth Server Session Closed	192.168.1.198	0	192.168
	PAM Session Closed	(izzmier-server)	1	1:49:24 PM	Auth Server Session Closed	192.168.1.198	0	192.168
	Session Started for user	(izzmier-server)	1	1:49:24 PM	Privilege Escalation Succeeded	192.168.1.198	0	192.168
	Session Started for user	(izzmier-server)	1	1:49:24 PM	Privilege Escalation Succeeded	192.168.1.198	0	192.168
	PAM Session Closed	(izzmier-server)	1	1:49:24 PM	Auth Server Session Closed	192.168.1.198	0	192.168
	PAM Session Closed	(izzmier-server)	1	1:49:24 PM	Auth Server Session Closed	192.168.1.198	0	192.168
	Session Started for user	(izzmier-server)	1	1:49:24 PM	Privilege Escalation Succeeded	192.168.1.198	0	192.168
	An authentication attempt was unsuccessful	(izzmier-server)	1	12:13:06 PM	General Authentication Failed	192.168.1.198	0	192.168
	An authentication attempt was unsuccessful	(izzmier-server)	1	12:13:06 PM	General Authentication Failed	192.168.1.198	0	192.168
	Password Check Failed	(izzmier-server)	1	12:13:06 PM	Notice	192.168.1.198	0	192.168
	An authentication attempt was unsuccessful	(izzmier-server)	1	12:12:43 PM	General Authentication Failed	192.168.1.198	0	192.168
	Password Check Failed	(izzmier-server)	1	12:12:43 PM	Notice	192.168.1.198	0	192.168
	An authentication attempt was unsuccessful	(izzmier-server)	1	12:12:43 PM	General Authentication Failed	192.168.1.198	0	192.168
	Password Check Failed	(izzmier-server)	2	12:11:30 PM	Notice	192.168.1.198	0	192.168
	An authentication attempt was unsuccessful	(izzmier-server)	2	12:11:30 PM	General Authentication Failed	192.168.1.198	0	192.168
	An authentication attempt was unsuccessful	(izzmier-server)	2	12:11:30 PM	General Authentication Failed	192.168.1.198	0	192.168
	An authentication attempt was unsuccessful	(izzmier-server)	2	12:11:15 PM	General Authentication Failed	192.168.1.198	0	192.168
	An authentication attempt was unsuccessful	(izzmier-server)	2	12:11:15 PM	General Authentication Failed	192.168.1.198	0	192.168
	Password Check Failed	(izzmier-server)	2	12:11:15 PM	Notice	192.168.1.198	0	192.168
	An authentication attempt was unsuccessful	(izzmier-server)	2	12:10:59 PM	General Authentication Failed	192.168.1.198	0	192.168
	Password Check Failed	(izzmier-server)	2	12:10:59 PM	Notice	192.168.1.198	0	192.168
	Password Check Failed	(izzmier-server)	2	12:10:59 PM	Notice	192.168.1.198	0	192.168
	Password Check Failed	(izzmier-server)	2	12:10:42 PM	Notice	192.168.1.198	0	192.168
	An authentication attempt was unsuccessful	(izzmier-server)	2	12:10:42 PM	General Authentication Failed	192.168.1.198	0	192.168

Next, we check the asset details of the server. Right click on the source IP then click information the asset profile.



All Offenses > Offense 2 (Summary)

Offense 2

Summary Display ▾ Events Flows Actions ▾ Print

Magnitude		Status		Relevance	3	Severity	4	Credibility	4
Description	Multiple Login Failures for the Same User containing An authentication attempt was unsuccessful	Offense Type	Username						
		Event/Flow count	29 events and 0 flows in 2 categories						
Source IP(s)	192.168.1.198 (ricardo-server)	Start	12:08:57 PM						
Destination IP(s)	192.168.1.1	Duration	4m 9s						
Network(s)	Net-10-172-192.Net_192_168_0_	Assigned to	Izzmier						

Navigate ▶
Information ▶
DNS Lookup
WHOIS Lookup
Port Scan
Asset Profile
Search Events
Search Flows

Offense Source Summary

Username	Izzmier		
MAC Address	Unknown NIC	Host Name	Unknown
Last Known Host	Unknown	Last Known Machine	Unknown
Last Known MAC	Unknown	Last Known IP	Unknown
Last Observed	Unknown	Last Known Group	Unknown
Offenses	1	Events/Flows	29

Last 5 Notes

Notes Add Note

Notes	Username	Creation Date

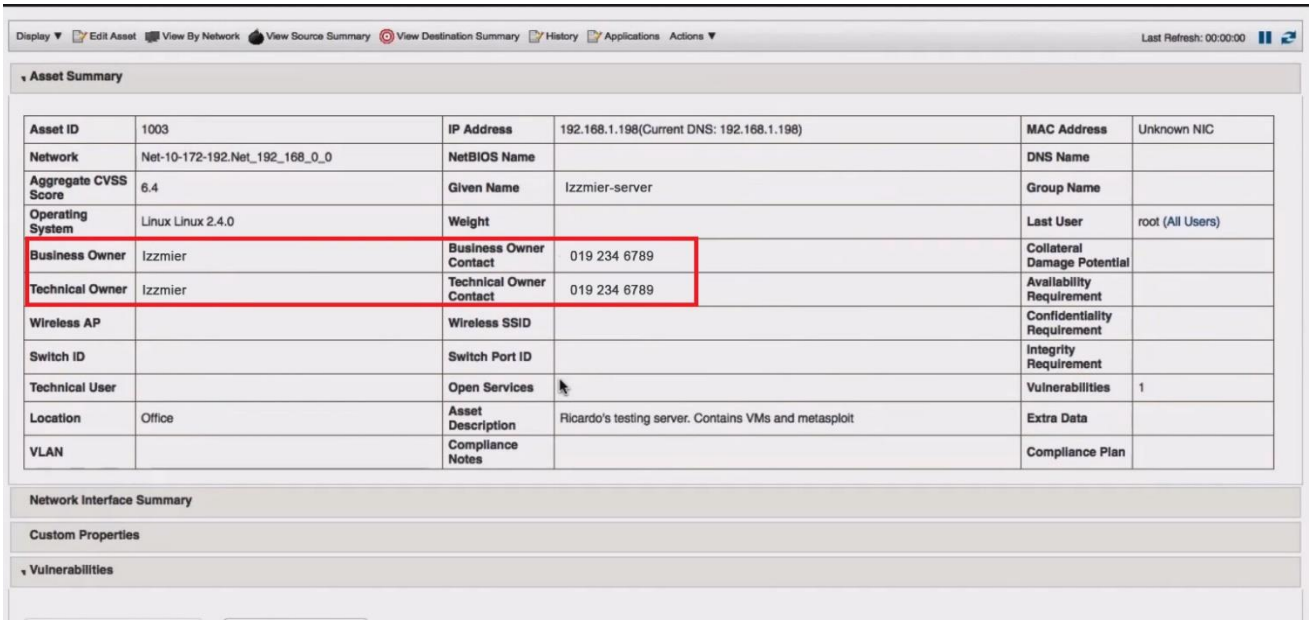
Nice! We got more information about this server. We found ore more clues, this server located inside the office based on the detail of location. Chances of someone get into/breaking someone office to just try to put password manually is not that high. Still, we can't close the offense and move to the next step.

Based on the asset details, we have business owner details. So, in this case I will call that person and ask about the case (Actual incident response plan we must send an email to IT team to get this confirmation). We must get confirmation from him. Fortunately, he confirms that he forgot the

password on that day and later called an IT to get his password reset. We make sure what the user told us matches with what we got in the logs.

So, we need to double check to make sure what the user told us matches with the logs:

I. Make sure the attack is manual not automated
II. Make sure we ask the user how many attempts he makes and compare with the logs
III. We make sure the user has direct access to server, which in this case true since user has server in the office



Display ▼ Edit Asset View By Network View Source Summary View Destination Summary History Applications Actions ▼ Last Refresh: 00:00:00

Asset Summary

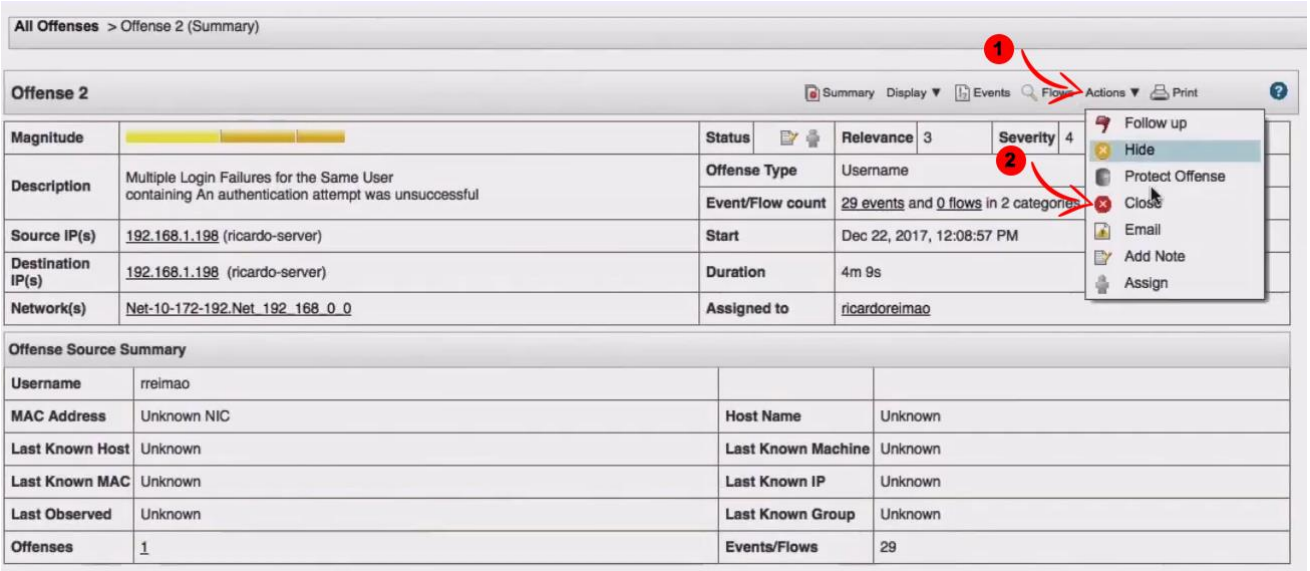
Asset ID	1003	**IP Address**	192.168.1.198(Current DNS: 192.168.1.198)	**MAC Address**	Unknown NIC
Network	Net-10-172-192.Net_192_168_0_0	**NetBIOS Name**		**DNS Name**	
Aggregate CVSS Score	6.4	**Given Name**	Izzmier-server	**Group Name**	
Operating System	Linux Linux 2.4.0	**Weight**		**Last User**	root (All Users)
Business Owner	Izzmier	**Business Owner Contact**	019 234 6789	**Collateral Damage Potential**	
Technical Owner	Izzmier	**Technical Owner Contact**	019 234 6789	**Availability Requirement**	
Wireless AP		**Wireless SSID**		**Confidentiality Requirement**	
Switch ID		**Switch Port ID**		**Integrity Requirement**	
Technical User		**Open Services**		**Vulnerabilities**	1
Location	Office	**Asset Description**	Ricardo's testing server. Contains VMs and metasploit	**Extra Data**	
VLAN		**Compliance Notes**		**Compliance Plan**	

Network Interface Summary

Custom Properties

Vulnerabilities

Finally, we can close this offense. Click action and then click close. Don't forget to put closer notes, for example like this "Called the user and he informed he was having trouble with the password. The password was reset by IT, case can be closed.



All Offenses > Offense 2 (Summary)

Offense 2

Summary Display ▼ Events Flows Actions ▼ Print

1

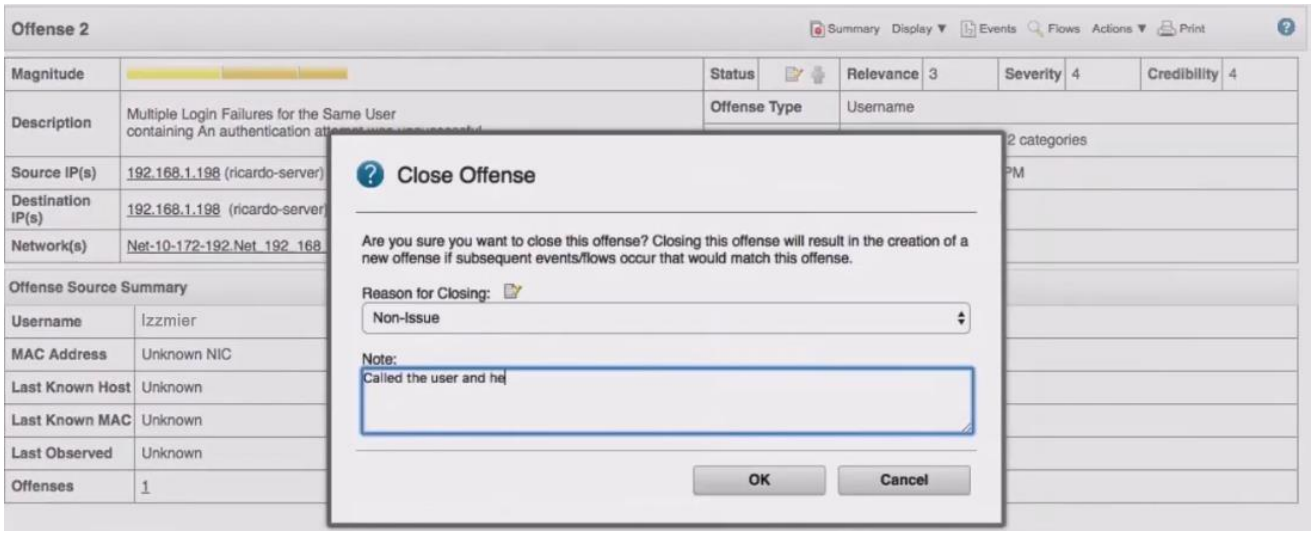
2

Follow up
Hide
Protect Offense
Close
Email
Add Note
Assign

Magnitude		**Status**	**Relevance** 3 **Severity** 4
Description	Multiple Login Failures for the Same User containing An authentication attempt was unsuccessful	**Offense Type**	Username
		Event/Flow count	29 events and 0 flows in 2 categories
Source IP(s)	192.168.1.198 (ricardo-server)	**Start**	Dec 22, 2017, 12:08:57 PM
Destination IP(s)	192.168.1.198 (ricardo-server)	**Duration**	4m 9s
Network(s)	Net-10-172-192.Net_192_168_0_0	**Assigned to**	ricardoreimao

Offense Source Summary

Username	rreimao		
MAC Address	Unknown NIC	**Host Name**	Unknown
Last Known Host	Unknown	**Last Known Machine**	Unknown
Last Known MAC	Unknown	**Last Known IP**	Unknown
Last Observed	Unknown	**Last Known Group**	Unknown
Offenses	1	**Events/Flows**	29


Offense 2
Summary
Display
Events
Flows
Actions
Print
Magnitude
Status
Relevance 3
Severity 4
Credibility 4
Description
Multiple Login Failures for the Same User
containing An authentication
Offense Type
Username
2 categories
Source IP(s)
192.168.1.198 (ricardo-server)
PM
Destination IP(s)
192.168.1.198 (ricardo-server)
Network(s)
Net-10-172-192.Net_192_168
Offense Source Summary
Username
lzzmier
MAC Address
Unknown NIC
Last Known Host
Unknown
Last Known MAC
Unknown
Last Observed
Unknown
Offenses
1
Close Offense
Are you sure you want to close this offense? Closing this offense will result in the creation of a new offense if subsequent events/flows occur that would match this offense.
Reason for Closing:
Non-Issue
Note:
Called the user and he
OK
Cancel