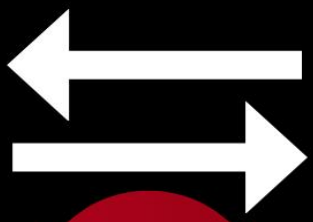


LOG ANALYSIS AND SYSTEMS INTEGRATION WITH WAZUH

PREPARED BY
MEHMOODULHASSAN

Linux log analysis

Logs files:

A log file store events, process, massages and other data from applications, operation system or devices.

They provide information based on the actions perform by the user, playing an important role in monitoring.

So basically, Linux operating systems like kali and ubuntu their logs are stored in the following directory **/var/log.** So basically, there are some important logs file that we need to check and analyze them.

1. Boot
2. Cron
3. Secure
4. maillog
5. Httpd
6. Massages

So here, boot logs are created during the startup of the system. If there is an issue, every single event will be logged.

In the crontab, all logs related to scheduled tasks are created. For example, if we need to update the system, we can schedule the task in crontab. At the specified time, the system will update, and the corresponding event will be logged.

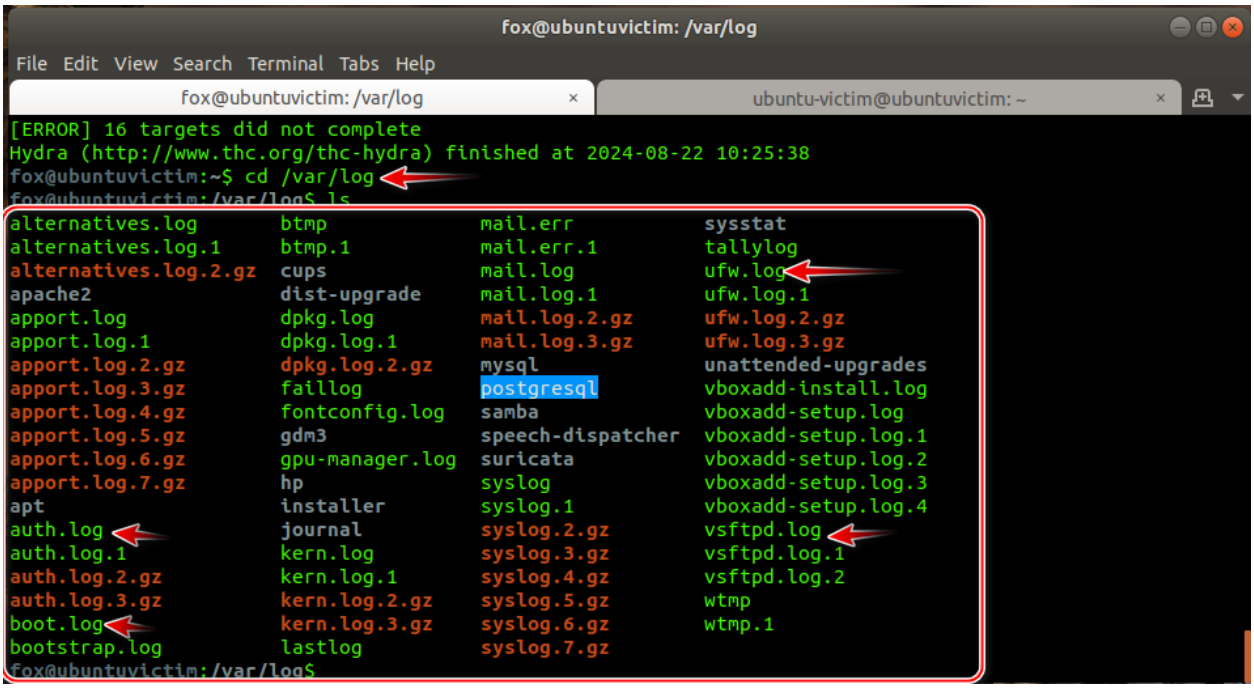
In secure log all the security information are stored like user login activity user logout authentication failure and password related etc.

In Linux, mail logs capture details about email processing, including sender/recipient addresses, delivery status, and errors, as well as connection and authentication attempts.

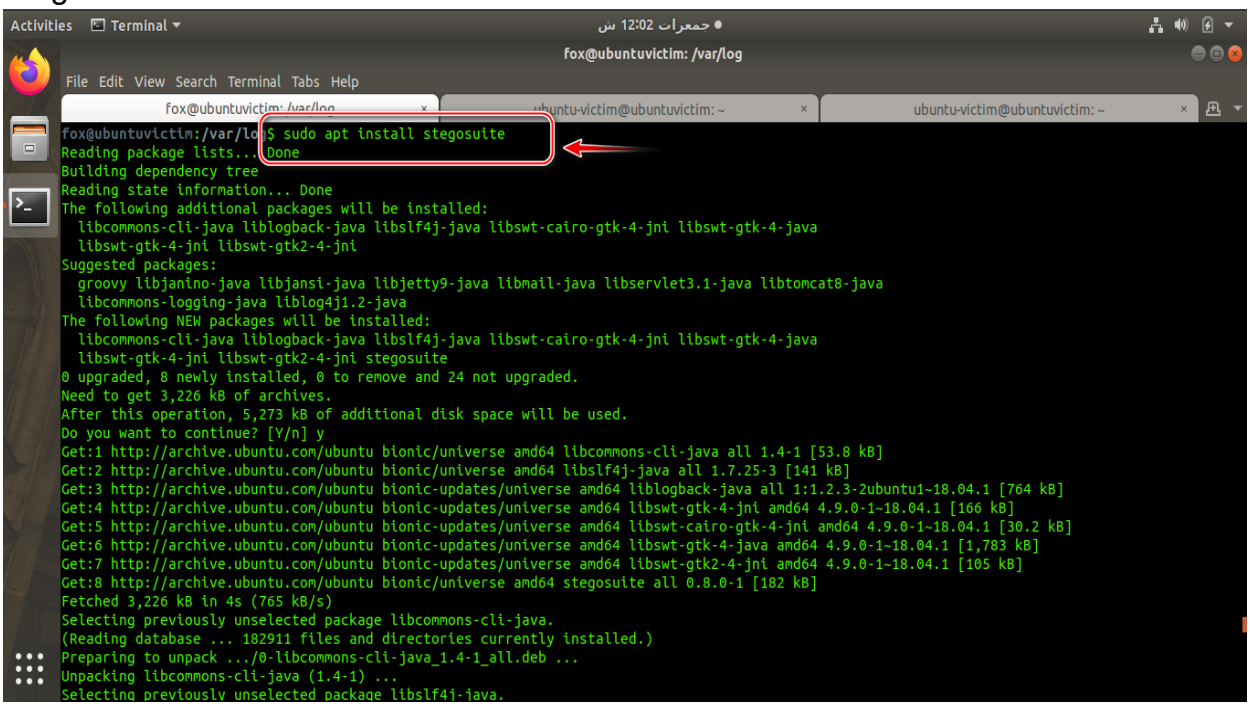
In Linux, httpd logs record details of web server activity, including client requests, URLs accessed, and server response statuses. They also log errors, warnings, and server issues during operation.

In Linux, messages logs store general system activity and diagnostic information, including kernel messages, boot processes, and system events. They help monitor overall system health and troubleshoot issues.

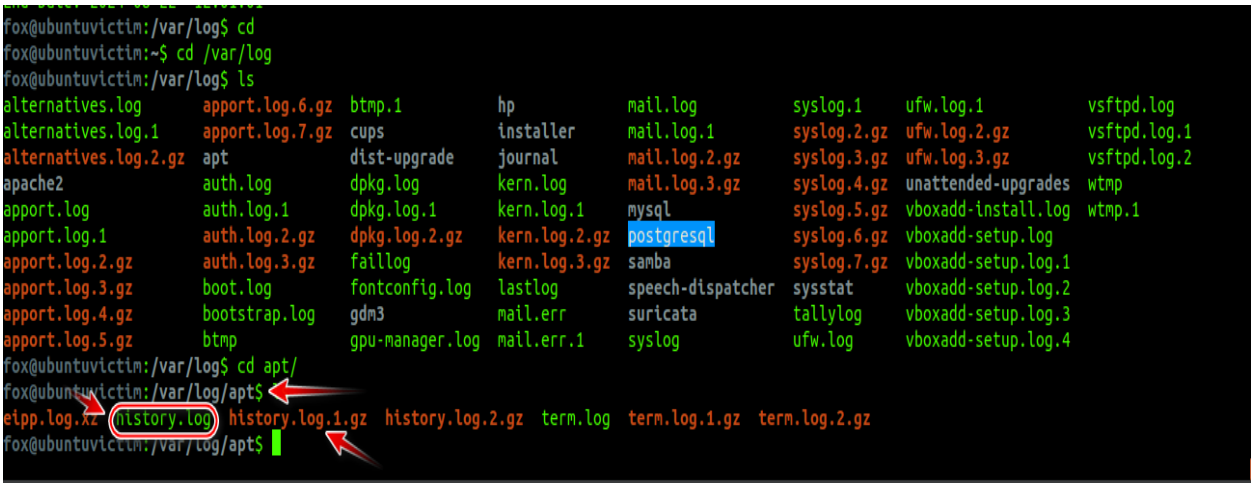
So, these are some short brief of those logs so now let’s check and do some analysis.



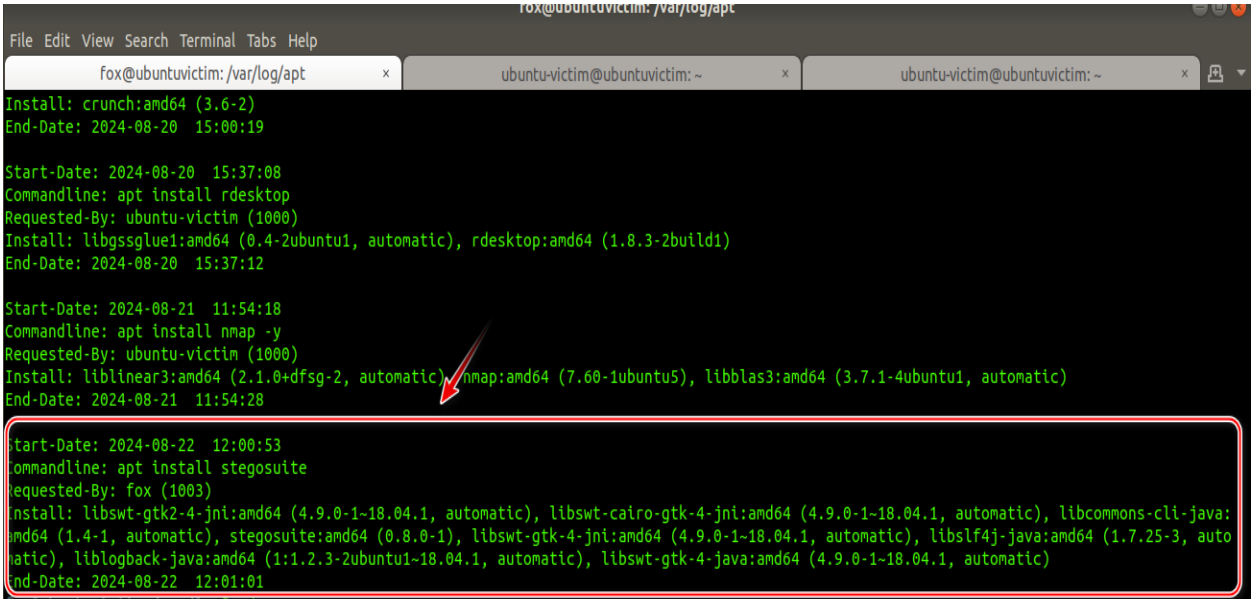
First of all, as we can see, our Ubuntu logs are located in /var/log, where all the log files are stored. We will install a package and then check to see if the logs are being generated..



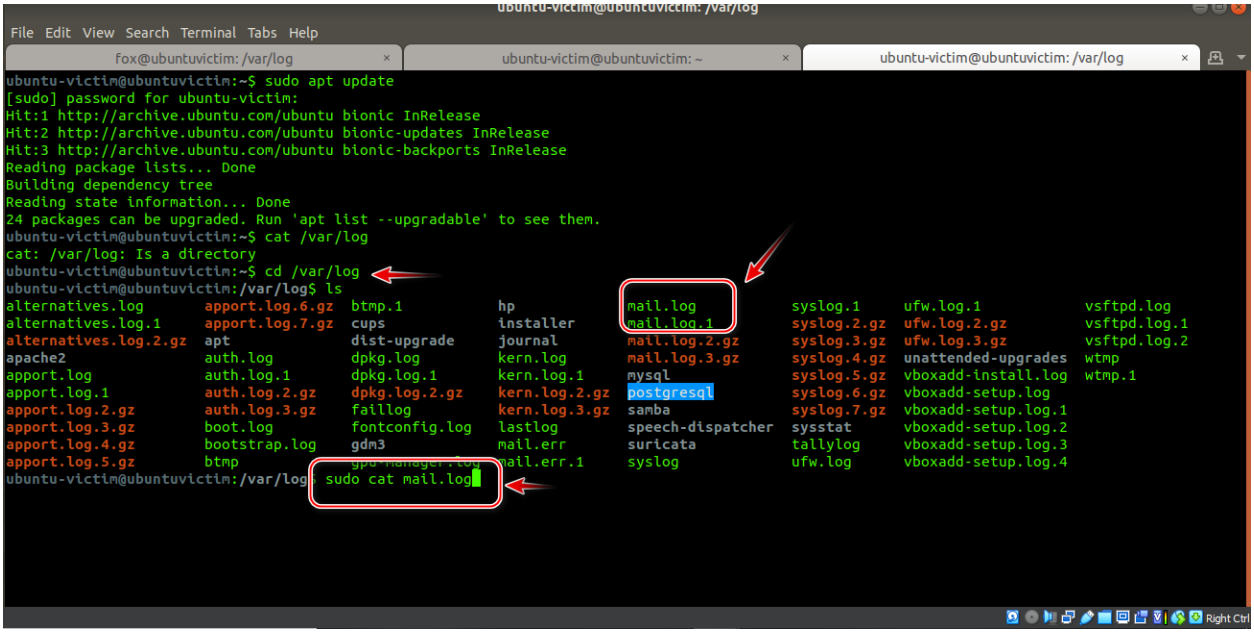
Now here we can see I just run the apt command to install that utility just to check if their logs.



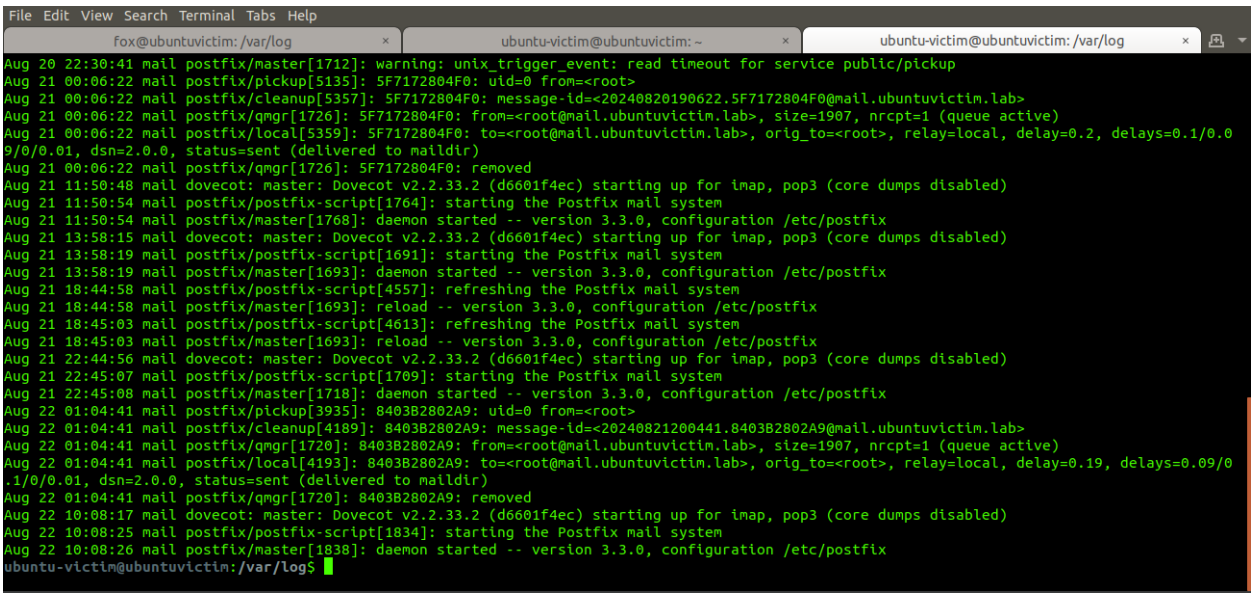
So, since we ran the apt command, we are now checking its logs. Navigate to the location /var/log/apt as mentioned in the figure, and you will find the history.log file. Open it using the nano command



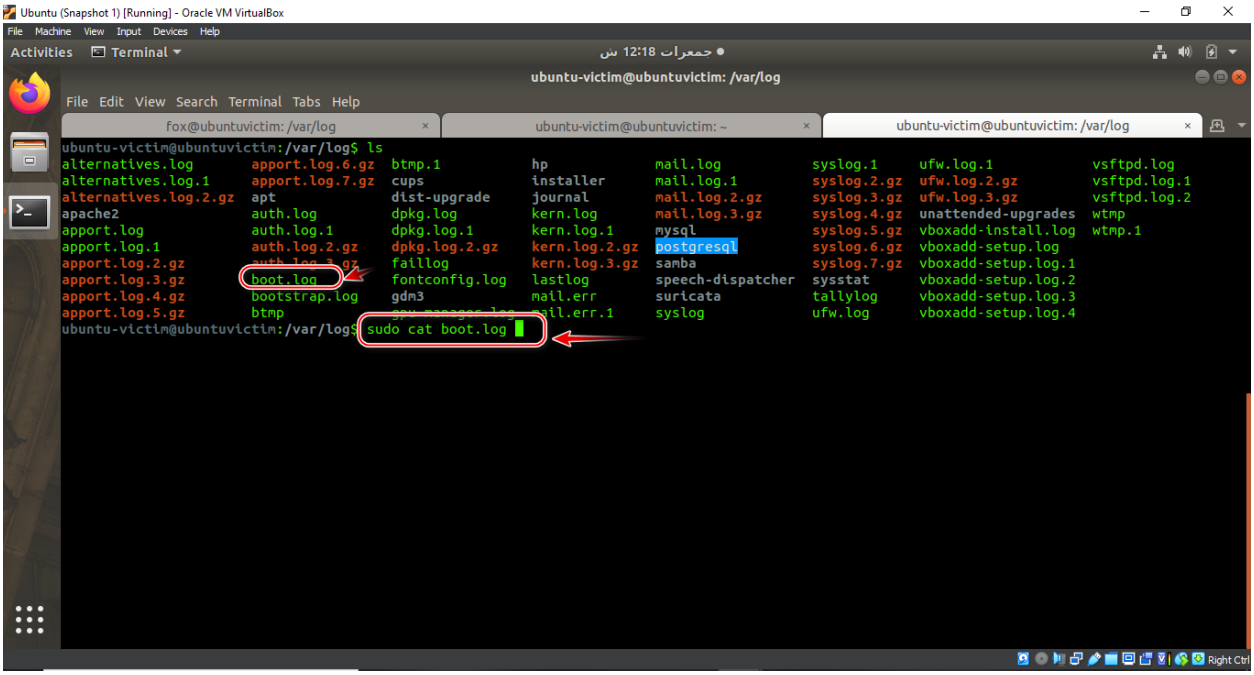
Here the log of that installation is being created which mean our system logs are monitoring fine.



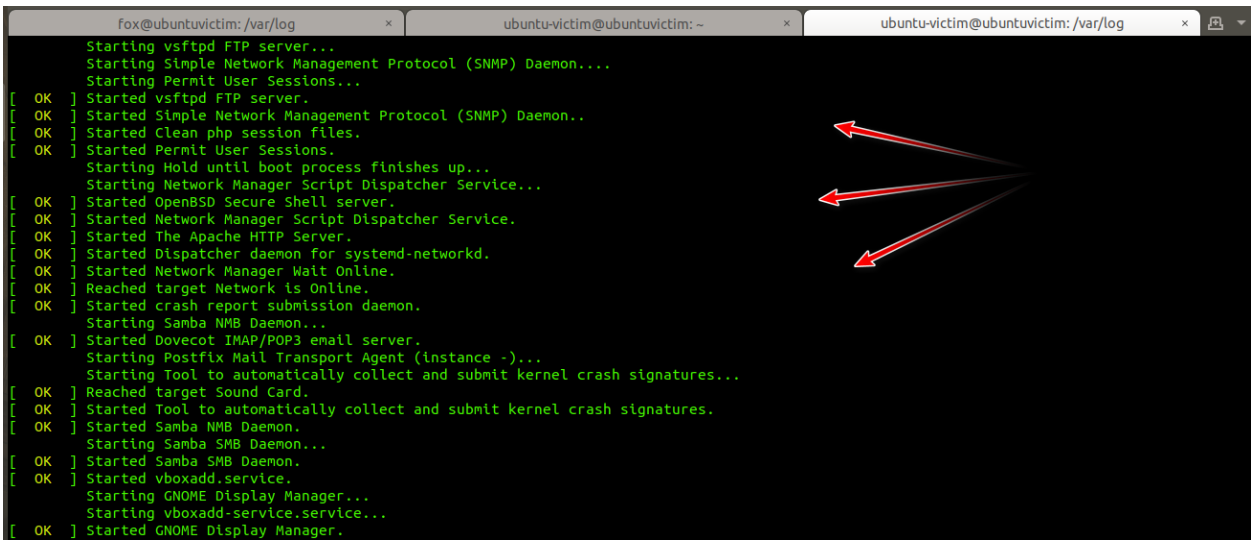
Now, here is another log file named mail.log. This file contains all logs related to mail, including information about sent and received emails, as well as any failures on the network



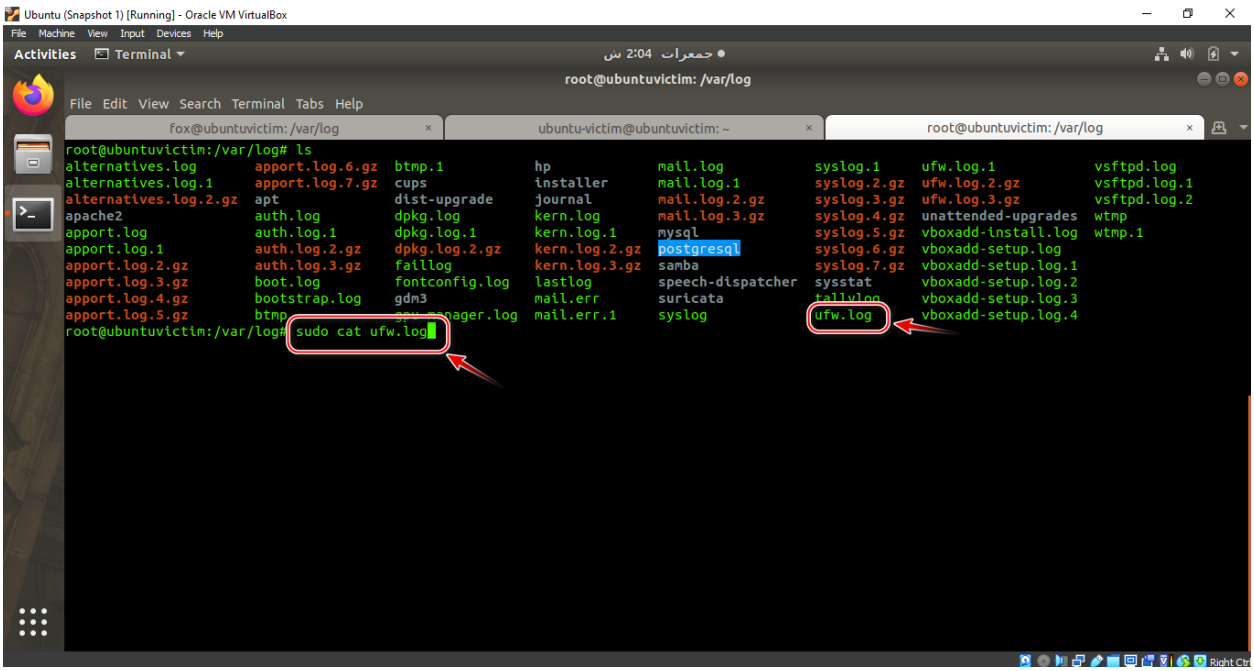
Here are the mails all of the mail logs are showing in the figure.



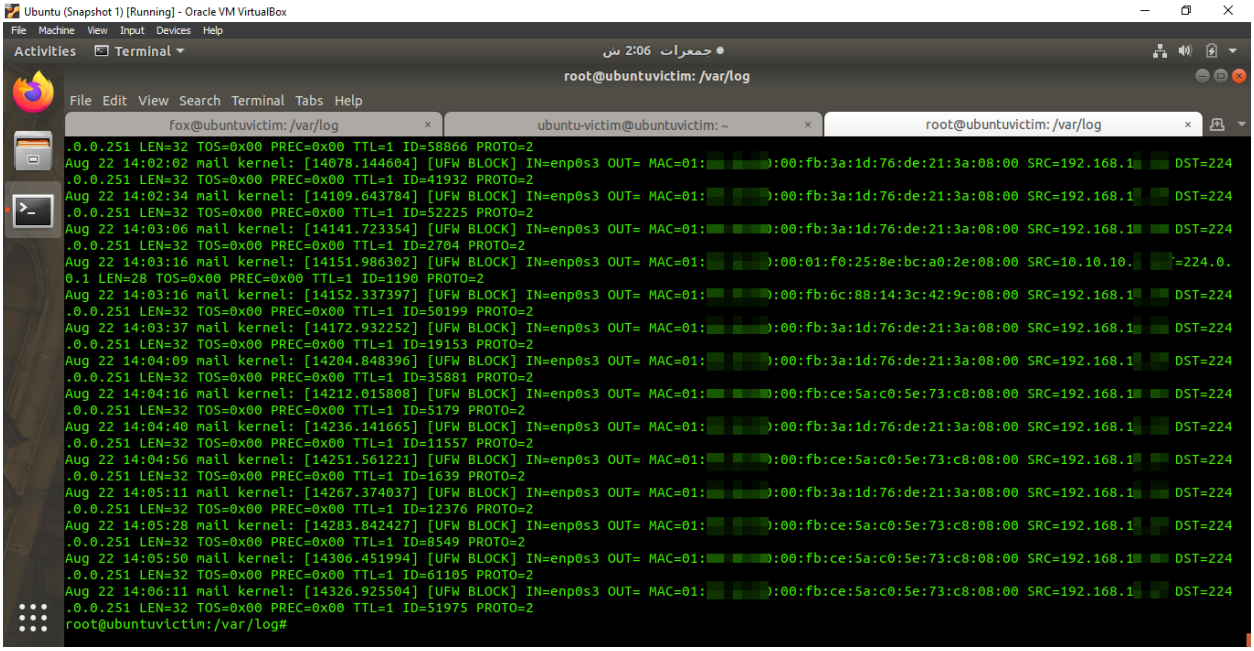
Now, here is another log file named boot.log. This file contains all the logs related to the system startup, including information about services, programs, and network activities.



Here is the log file opened so here we can see all file and programs related to the startup of the system.

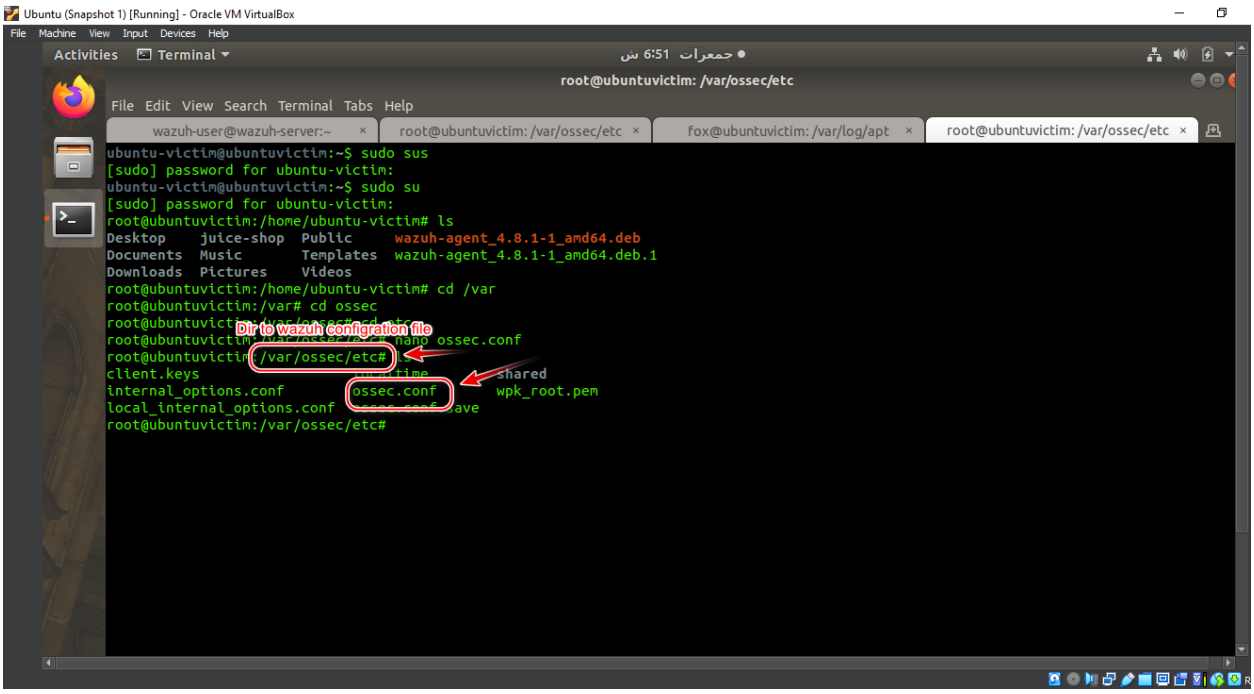


As shown in the figure, this is the Ubuntu firewall log file. It stores all the information related to UFW, such as which services are enabled or blocked.

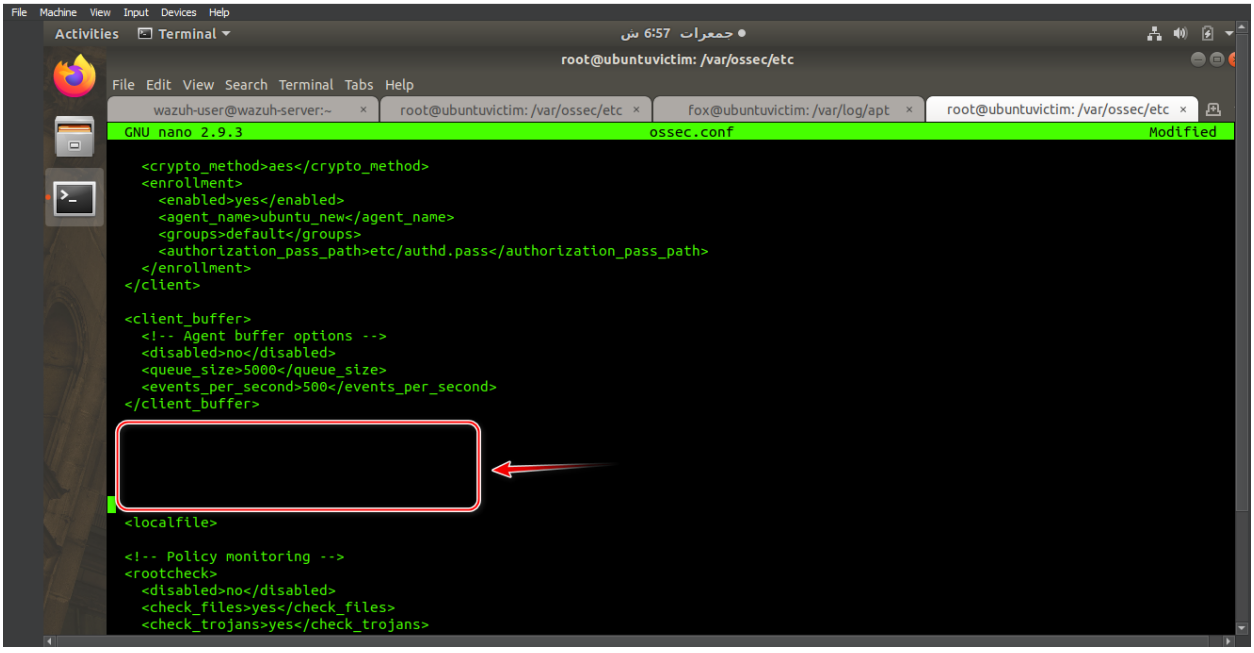


Now as we open the UFW file so here our all details we can see that some service are blocked by UFW and some are allowed according to the rules.

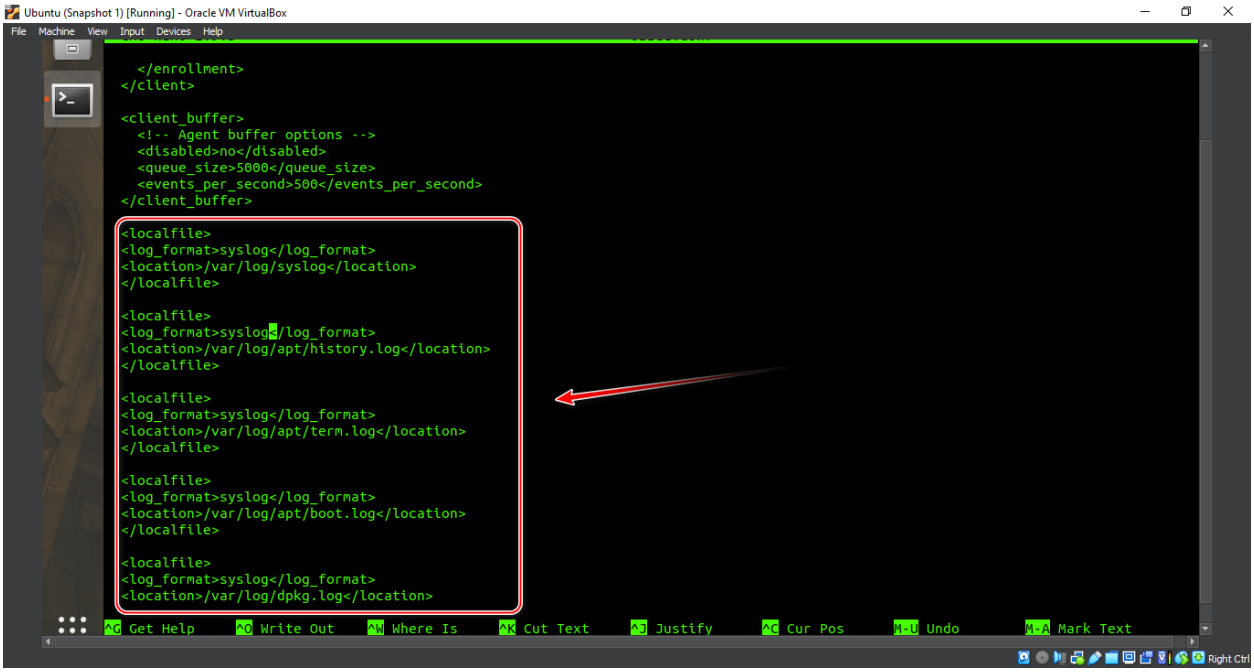
Now after all that let's do integration mean to integrate our ubuntu with Wazuh to monitor all the logs and traffic there on Wazuh(siem).



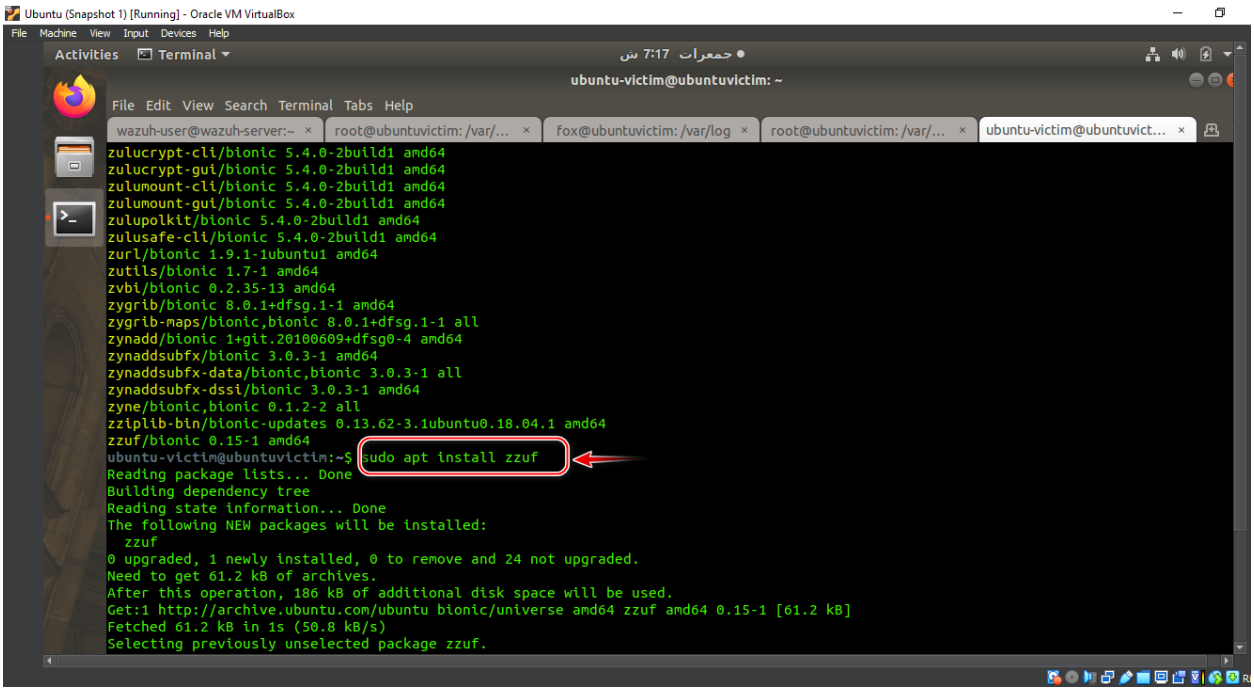
To perform this integration, first navigate to the **/var/ossec/etc** directory. There, you will find the **ossec.conf** file, which is the configuration file for Wazuh.



So, here at this underlined place here we have to write our ubuntu logs file integration details.

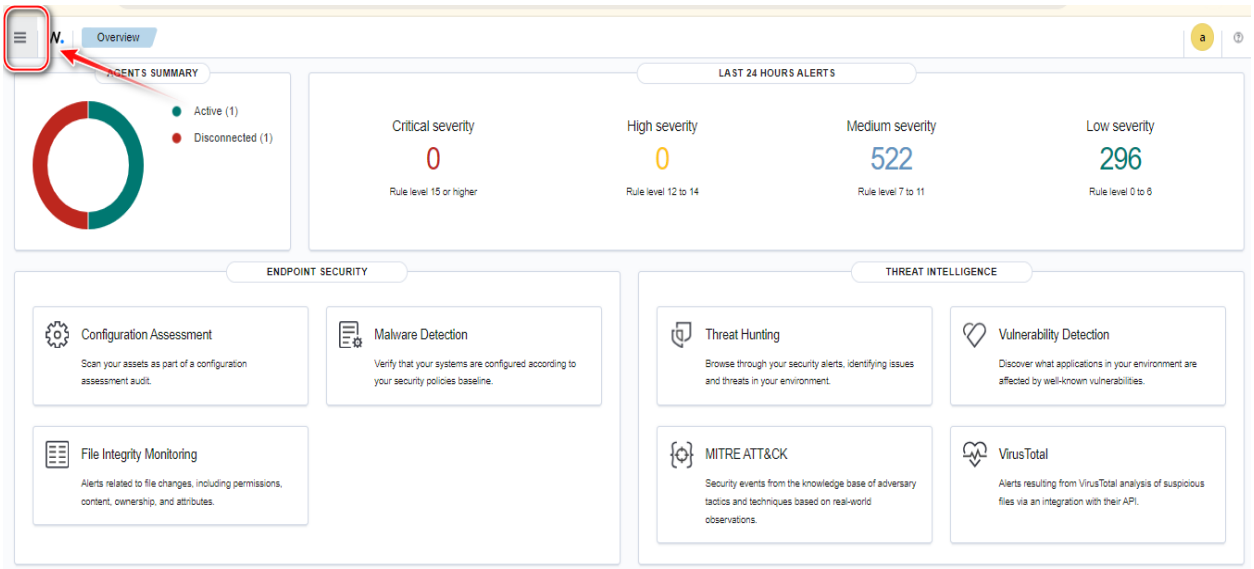


I have described how to integrate Ubuntu log files into the Wazuh server for monitoring.

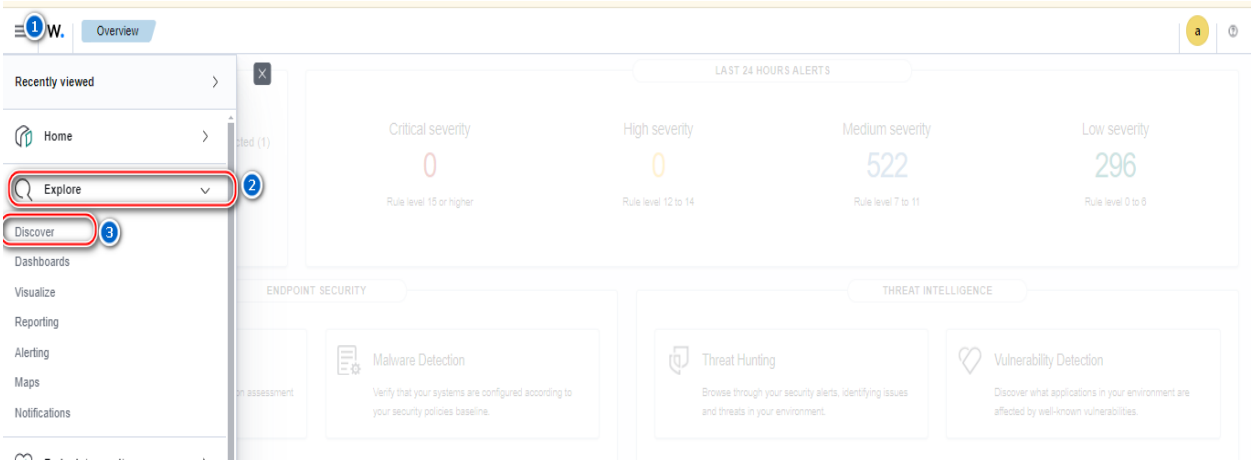


Now for checking it we have here just for checkup installed a zzuf package with apt to monitor that log on the Wazuh server.

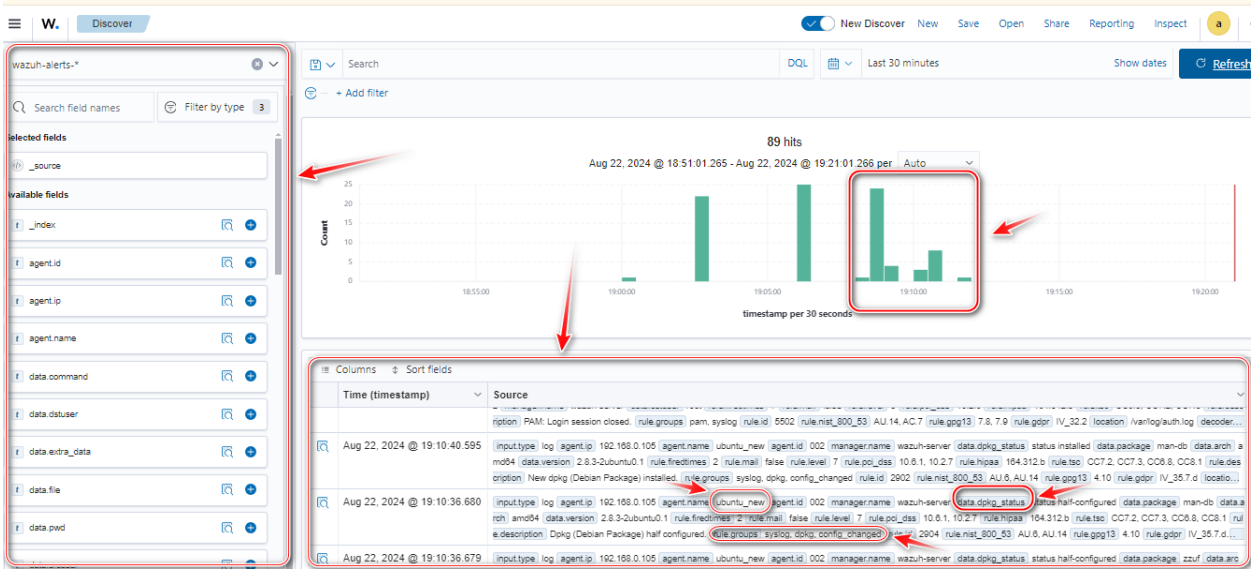
So, after running the command to monitor the logs just open your Wazuh server and make sure your agent is active there.



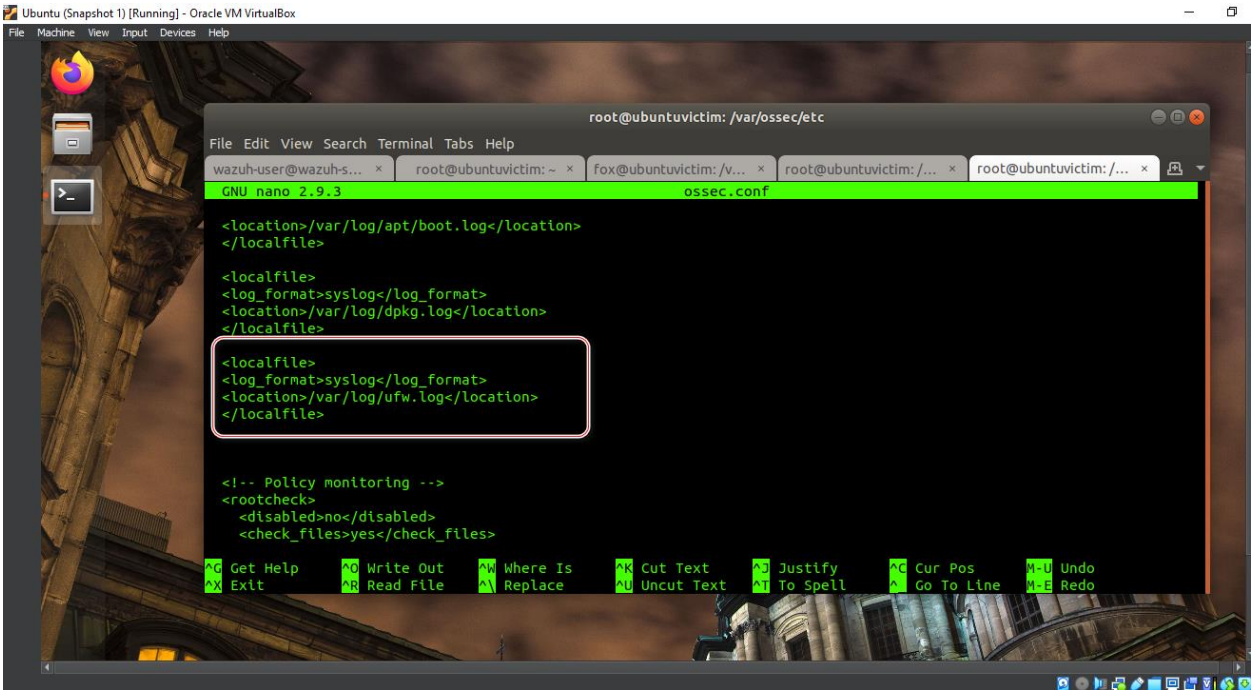
So here in the above figure our Wazuh dashboard is opened and agent is active so now just click on the three dots on the right-hand side.



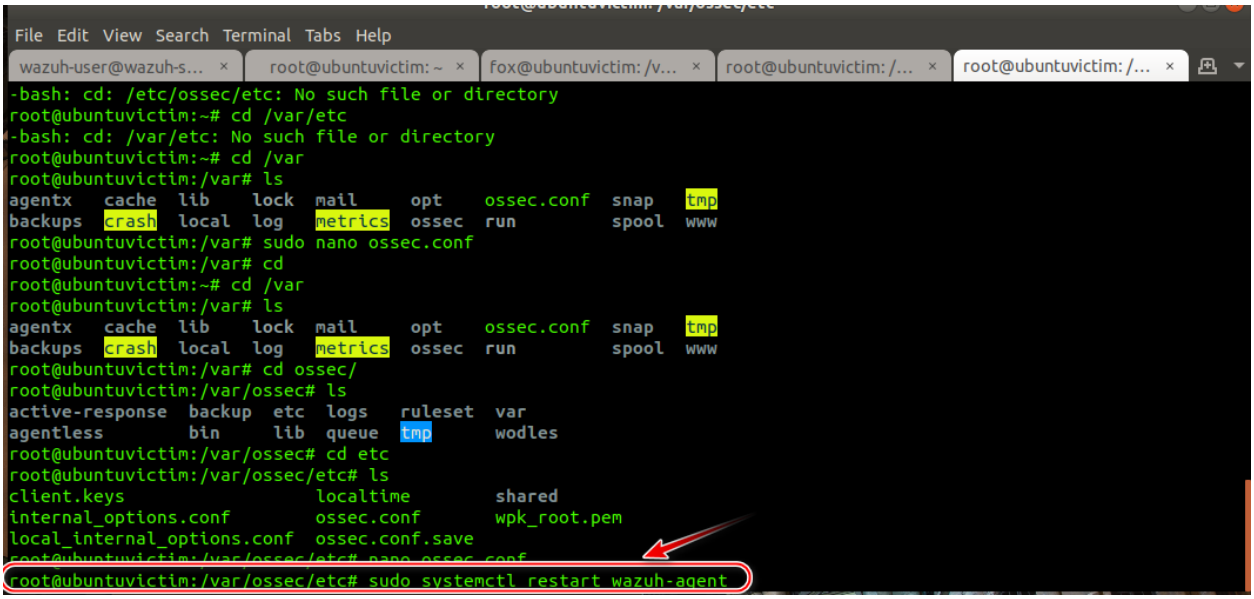
So, after clicking the three dots, a new tab will open, as shown in the above figure. In this tab, you will see several options, including one labeled **Explore**. Within the **Explore** section, click on the **Discover** option to proceed.



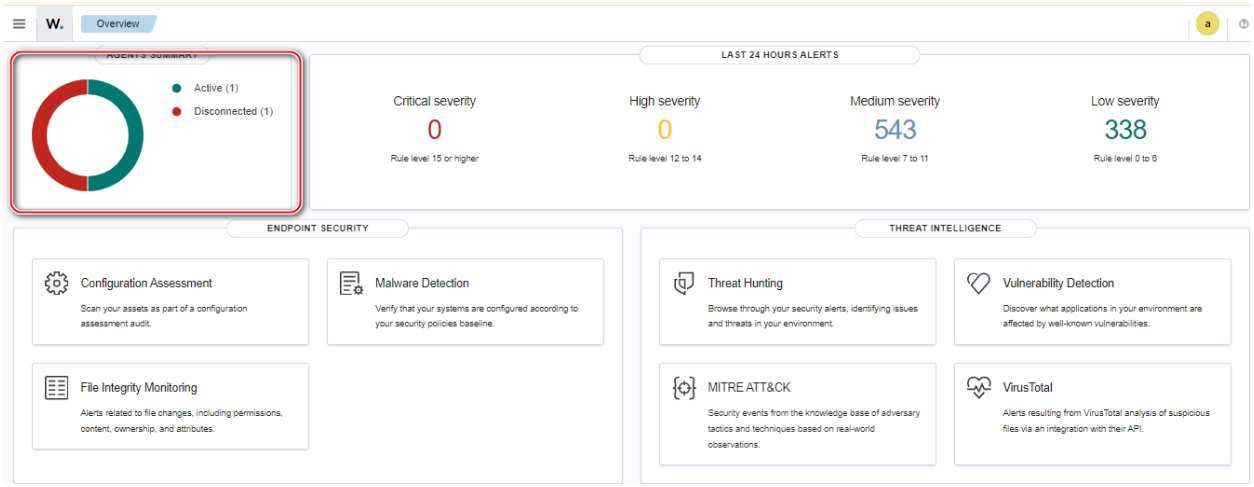
So, you will notice that, as we have integrated Wazuh with Ubuntu and ran the command **sudo apt install zzuf** to install the package, all related logs are being monitored and displayed here, as shown.



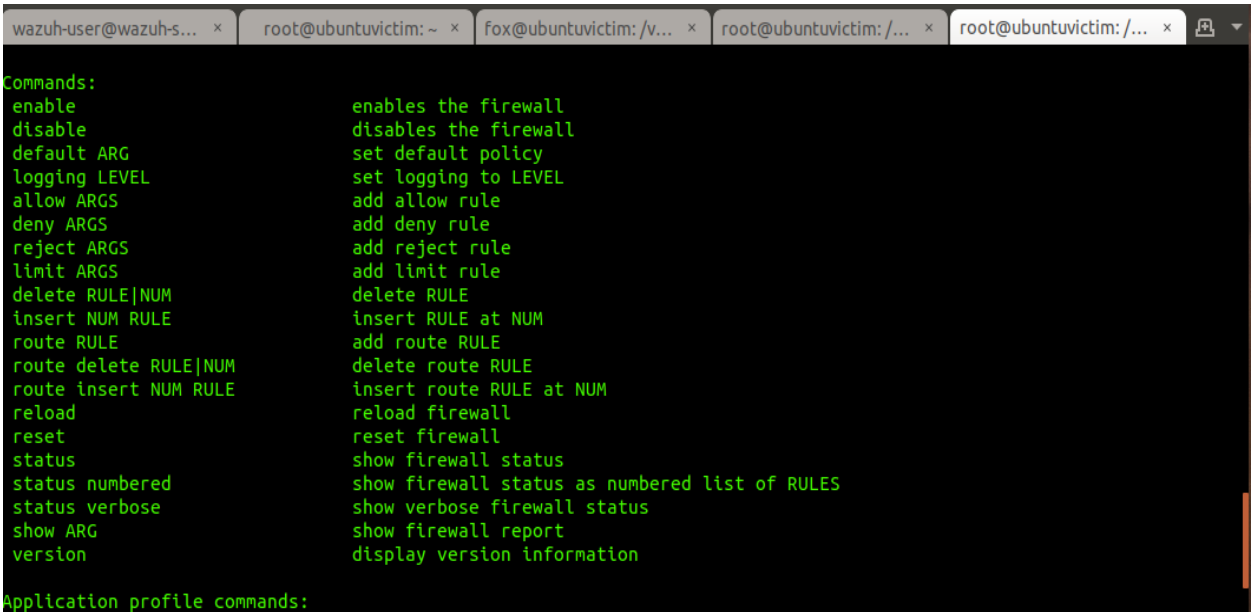
Now here as I added one another **ufw** log file in ossec.conf, so now we have to check their logs.



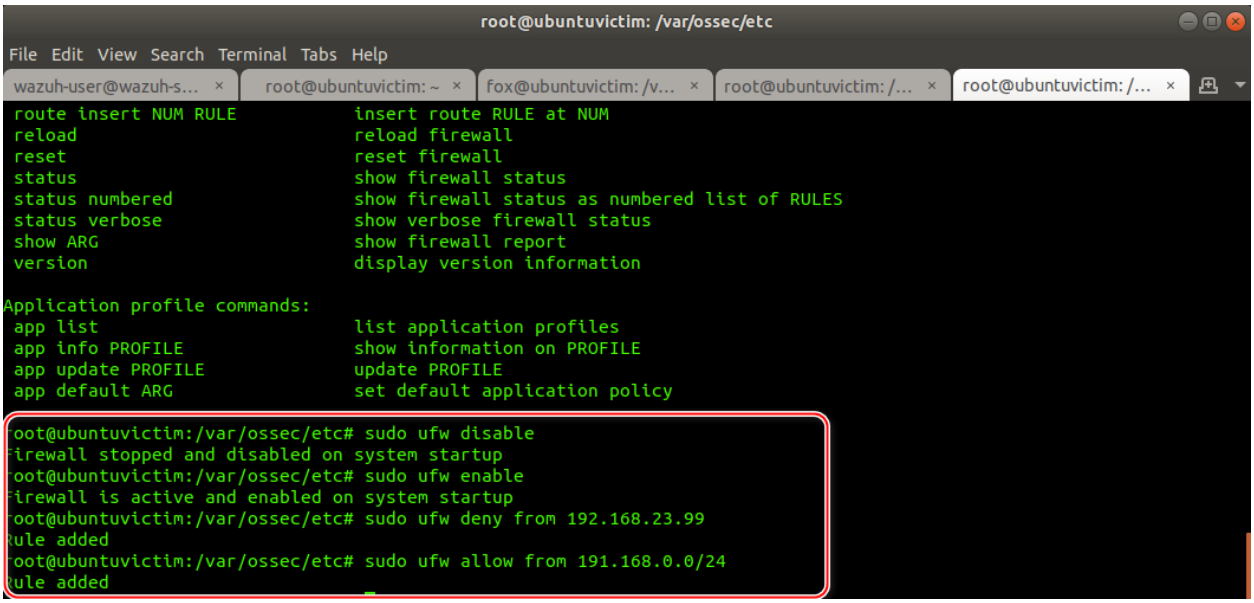
Now let's restart Wazuh agent.



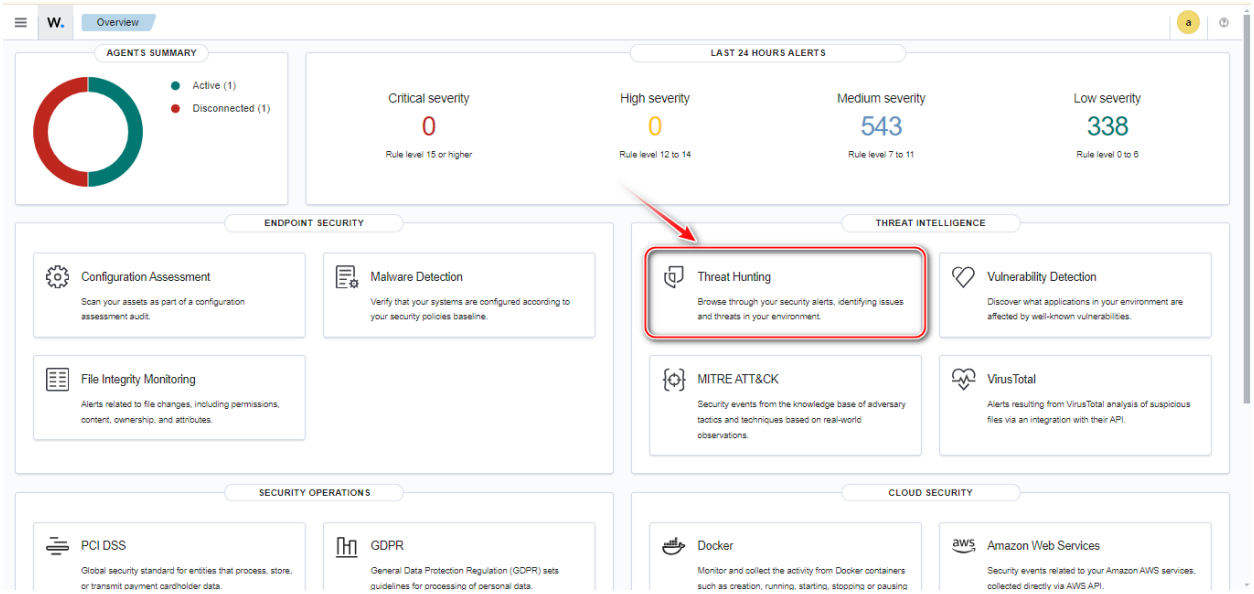
So then after restarting as we can see our agent is active.



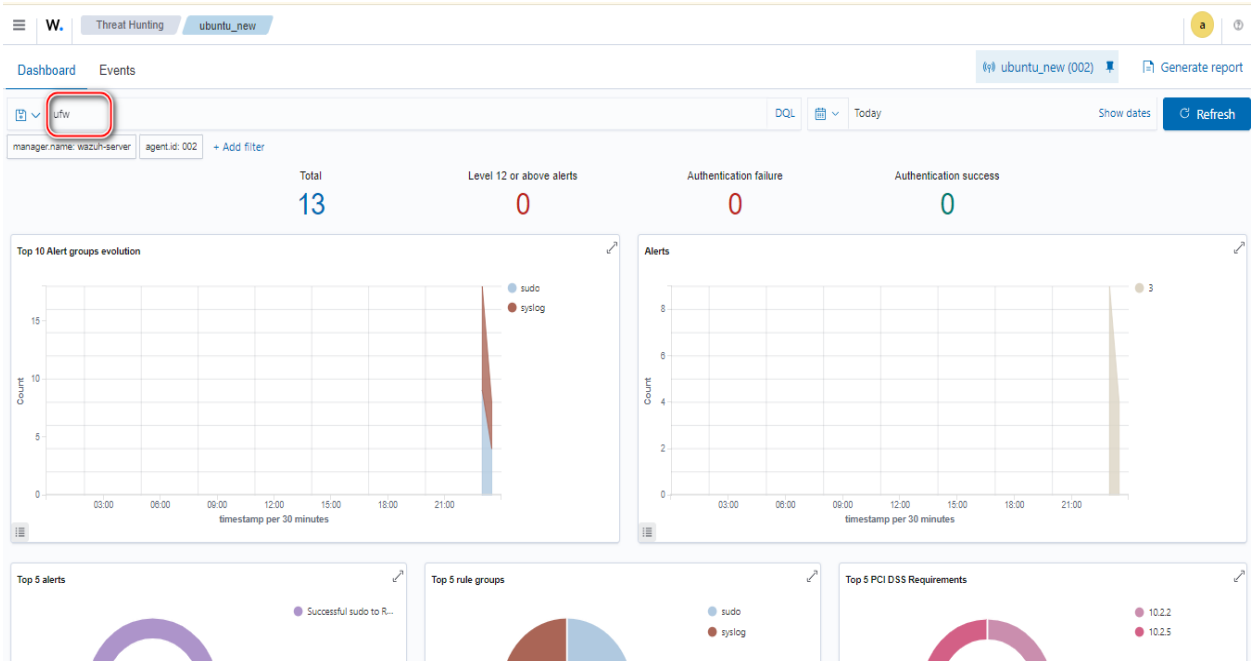
So our agent is active so let's do something to monitor their logs there on ubuntu. So all these commands are used in ufw which I opened with sudo ufw –help.



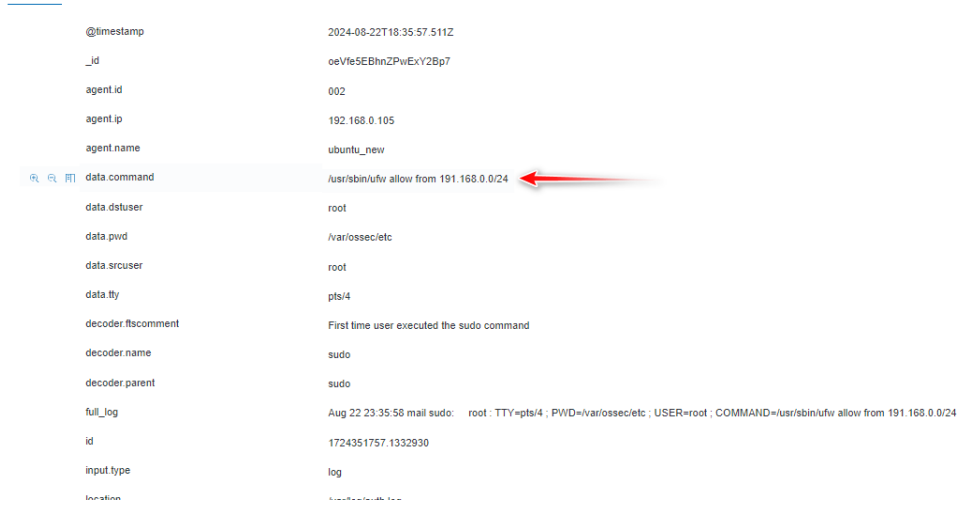
Then here I used some basic commands like disabled enable status allow the specific network deny the specific ip etc. so now let's check their logs.



So for logs go to your dashboard and check your agent is active or not then click on threat hunting tab.



Then here in search bar I typed **ufw** to monitor ufw logs.



@timestamp	2024-08-22T18:35:57.511Z
_id	oeVfe5EBhnZPwExY2Bp7
agent.id	002
agent.ip	192.168.0.105
agent.name	ubuntu_new
data.command	/usr/sbin/ufw allow from 191.168.0.0/24
data.dstuser	root
data.pwd	/var/ossec/etc
data.srcuser	root
data.tty	pts/4
decoder.ftscomment	First time user executed the sudo command
decoder.name	sudo
decoder.parent	sudo
full_log	Aug 22 23:35:58 mail sudo: root : TTY=pts/4 ; PWD=/var/ossec/etc ; USER=root ; COMMAND=/usr/sbin/ufw allow from 191.168.0.0/24
id	1724351757.1332930
input.type	log

Then here the logs are monitored as I allow the network.

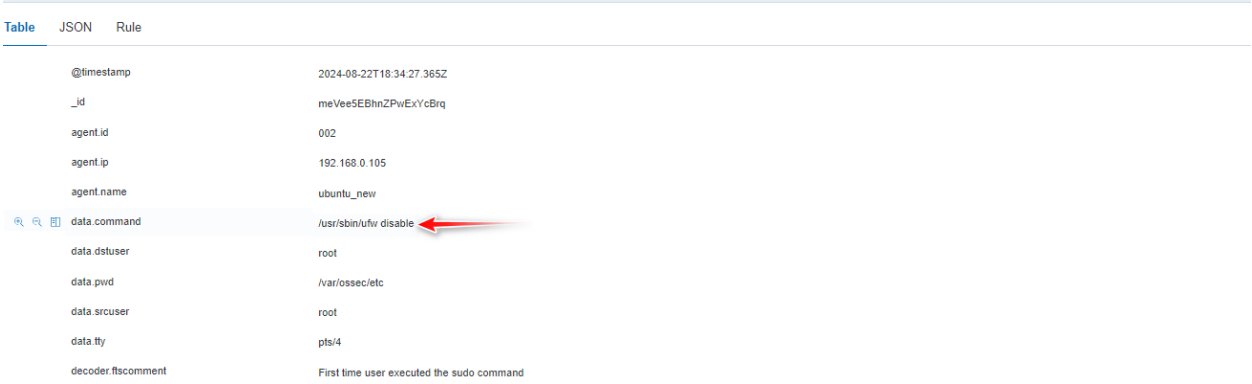
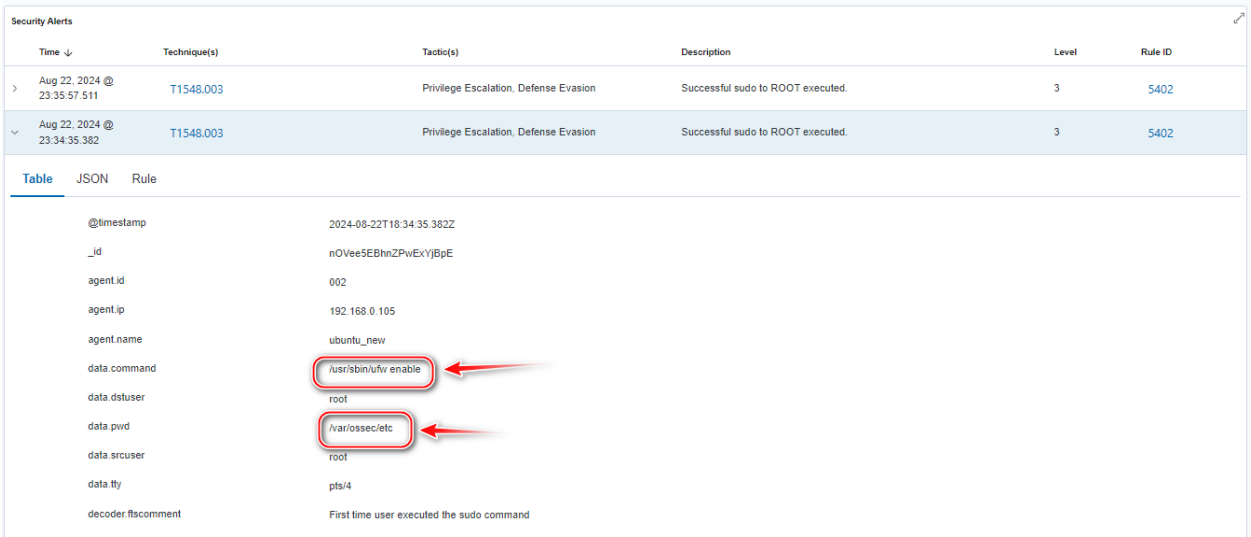


Table JSON Rule

@timestamp	2024-08-22T18:34:27.365Z
_id	meVee5EBhnZPwExYcBrq
agent.id	002
agent.ip	192.168.0.105
agent.name	ubuntu_new
data.command	/usr/sbin/ufw disable
data.dstuser	root
data.pwd	/var/ossec/etc
data.srcuser	root
data.tty	pts/4
decoder.ftscomment	First time user executed the sudo command

Then here is another log of disabling the ufw.



Security Alerts

Time	Technique(s)	Tactic(s)	Description	Level	Rule ID
Aug 22, 2024 @ 23:35:57.511	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402
Aug 22, 2024 @ 23:34:35.382	T1548.003	Privilege Escalation, Defense Evasion	Successful sudo to ROOT executed.	3	5402

Table JSON Rule

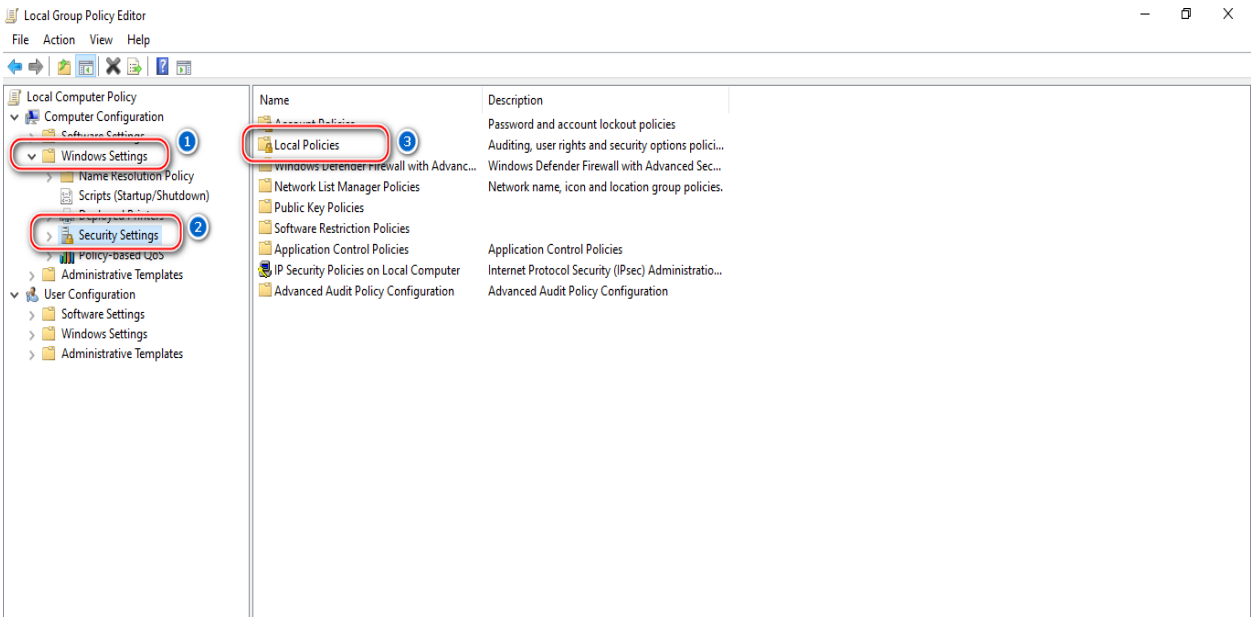
@timestamp	2024-08-22T18:34:35.382Z
_id	nOVee5EBhnZPwExYjBpE
agent.id	002
agent.ip	192.168.0.105
agent.name	ubuntu_new
data.command	/usr/sbin/ufw enable
data.dstuser	root
data.pwd	/var/ossec/etc
data.srcuser	root
data.tty	pts/4
decoder.ftscomment	First time user executed the sudo command

The here is another log of enabling the ufw.

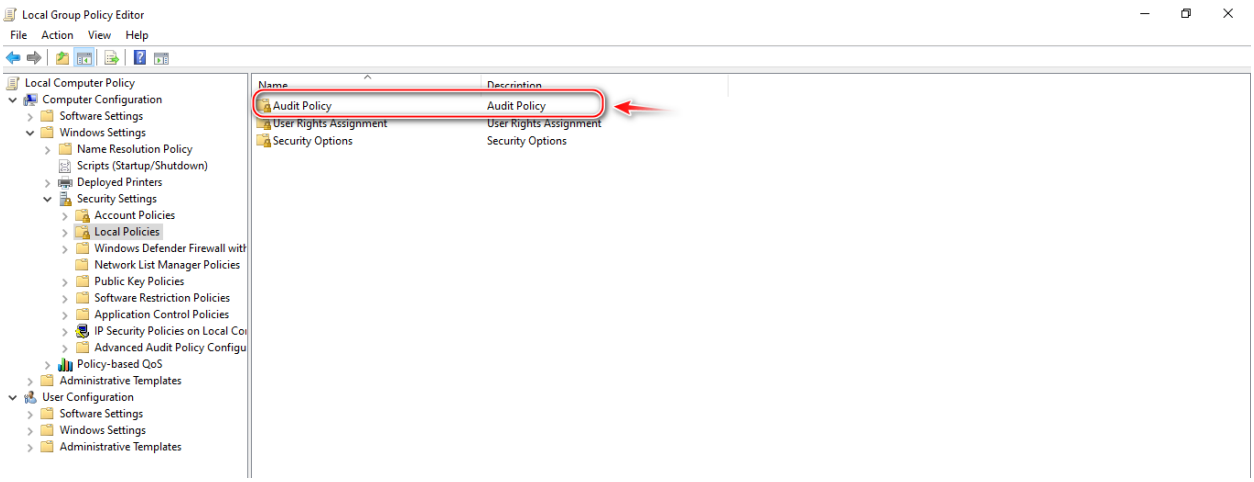
So in short words we can monitor here all the logs here in wazuh as we integrated.

Windows logs analysis

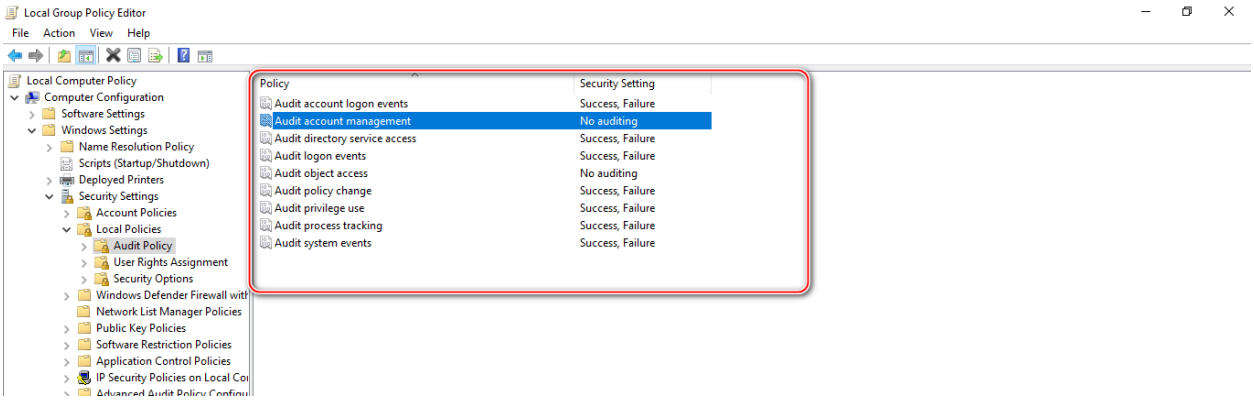
Windows log analysis involves examining various logs generated by the operating system and applications to monitor system activity, identify security events, and troubleshoot issues. Key logs include the Security, Application, and System logs found in the Event Viewer, which record events like user logins, application errors, and system warnings. By analyzing these logs, administrators can detect unauthorized access, track changes, and ensure system integrity. Tools like Wazuh can centralize and automate this analysis, making it easier to identify patterns, anomalies, and potential threats across multiple systems.



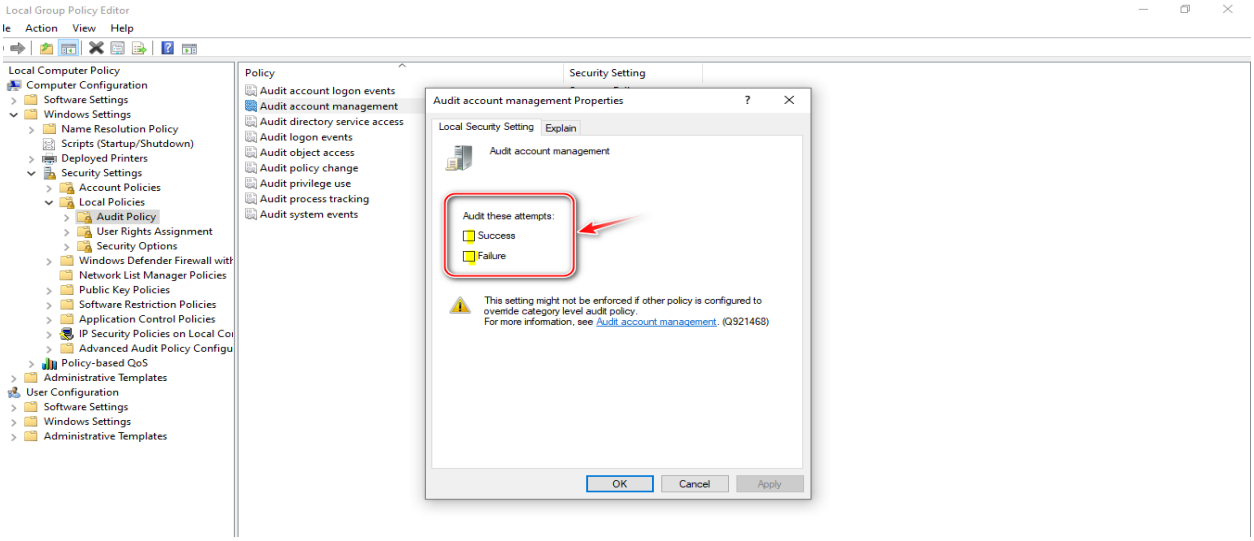
So for first of all in windows type local group policy and then in windows settings click on security settings as we want to monitor first security logs then click on local policies.



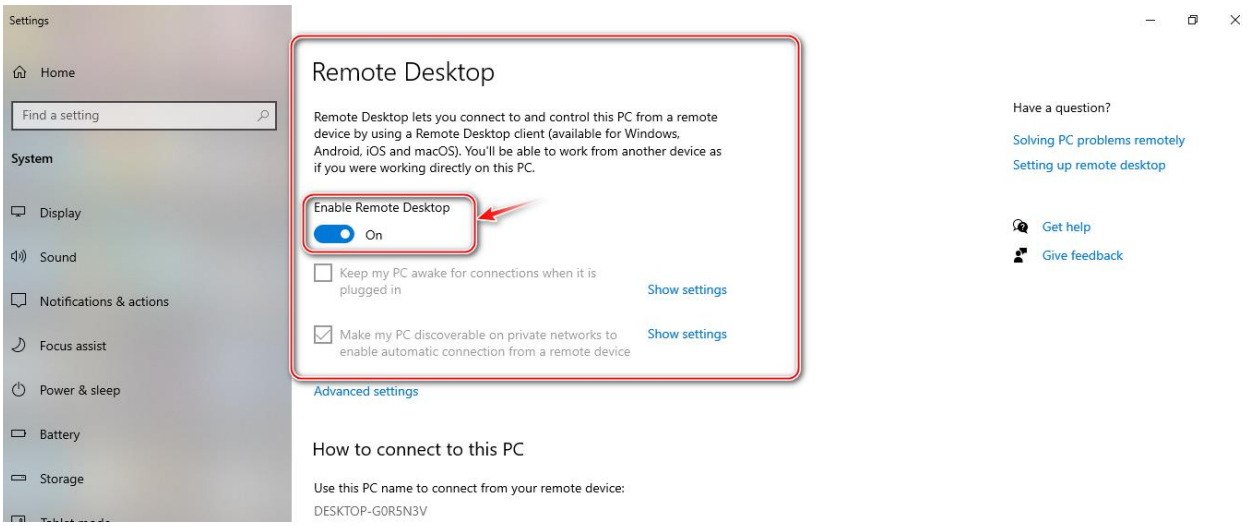
Then in local policy click on audit policy.



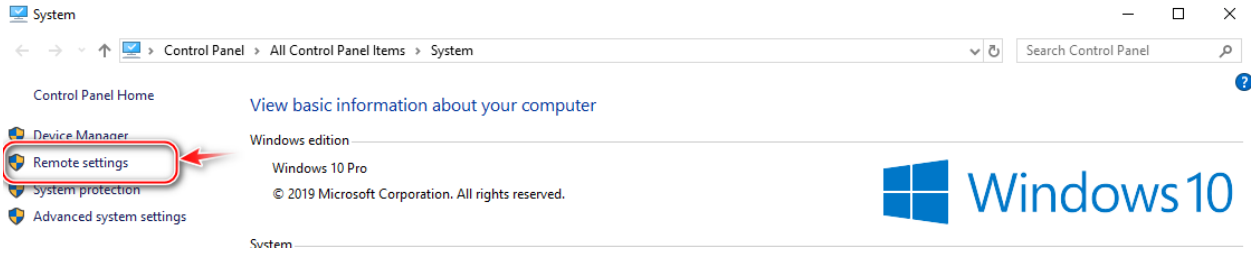
Now here enable this event policy which you want to monitor.



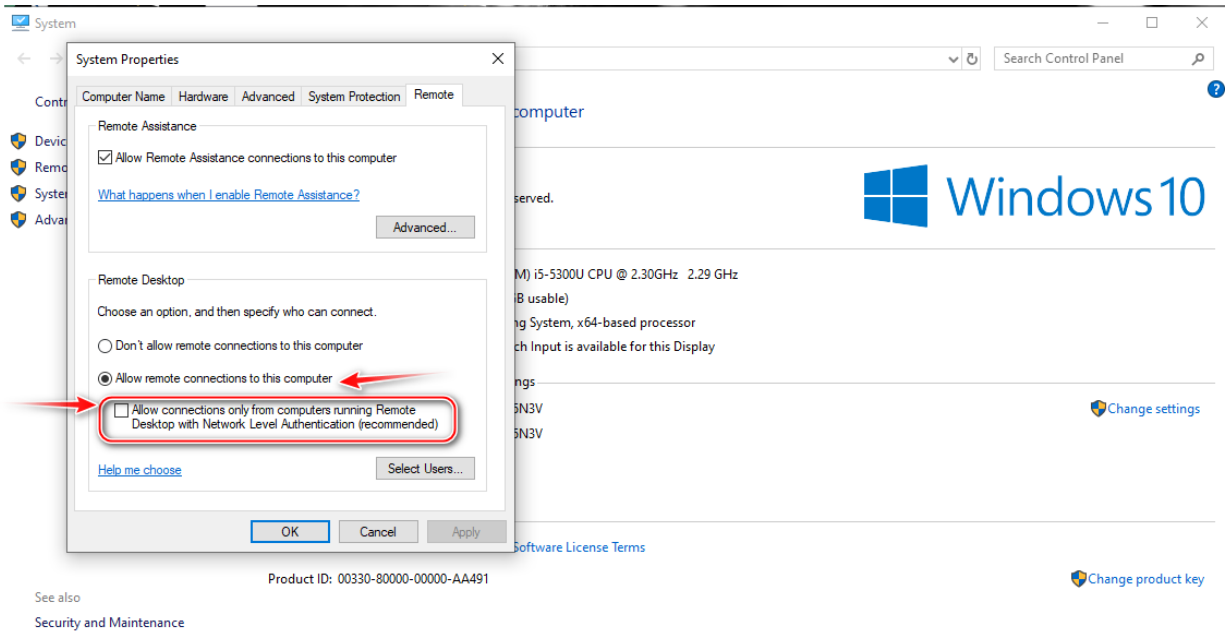
For enabling right click on the policy you want to enable and click on these dialog boxes.



Now all monitoring environment is set so we first on our remote desktop for practice demo.

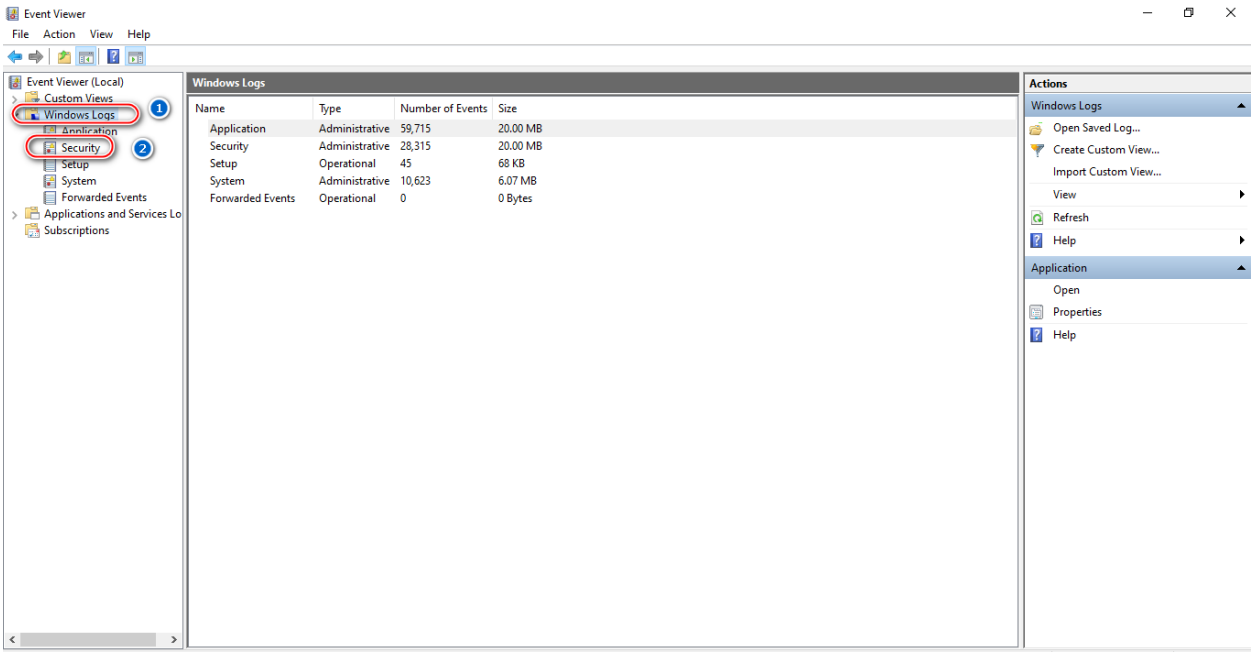


Now one more setting for enabling rdp is right click on this pc and then click properties so you will see this window interface. Then click on remote settings.

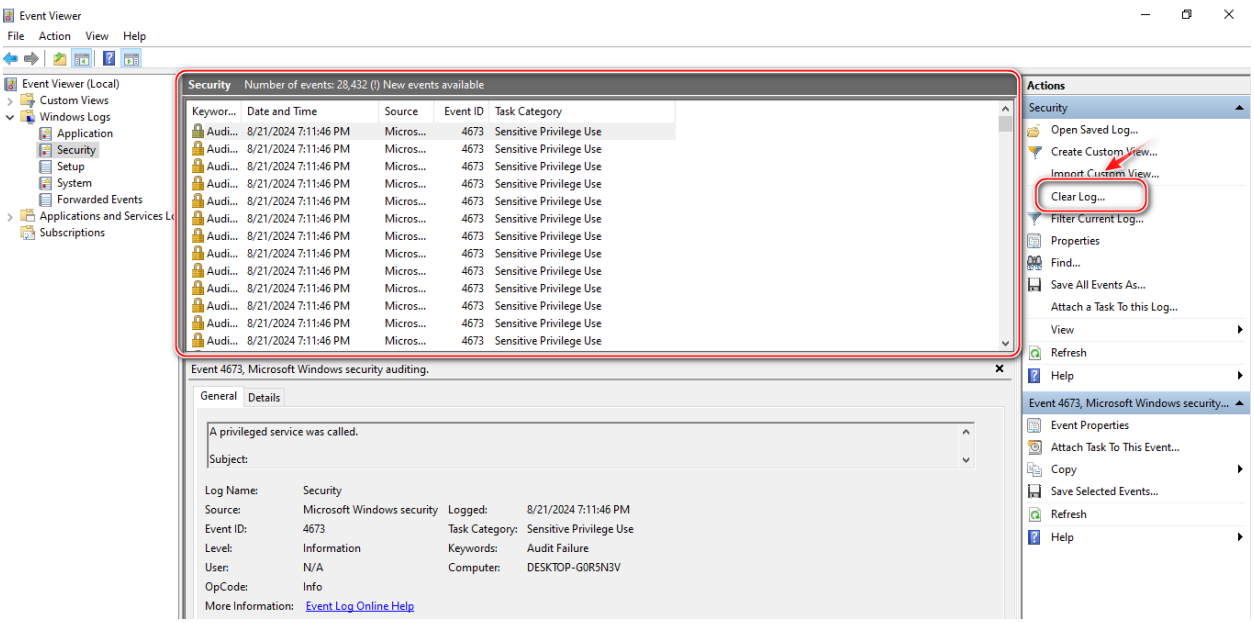


Then make sure that your setting look like same it is uncheck because this option only allow same level authentication like this is windows10 so the other one will same it is.

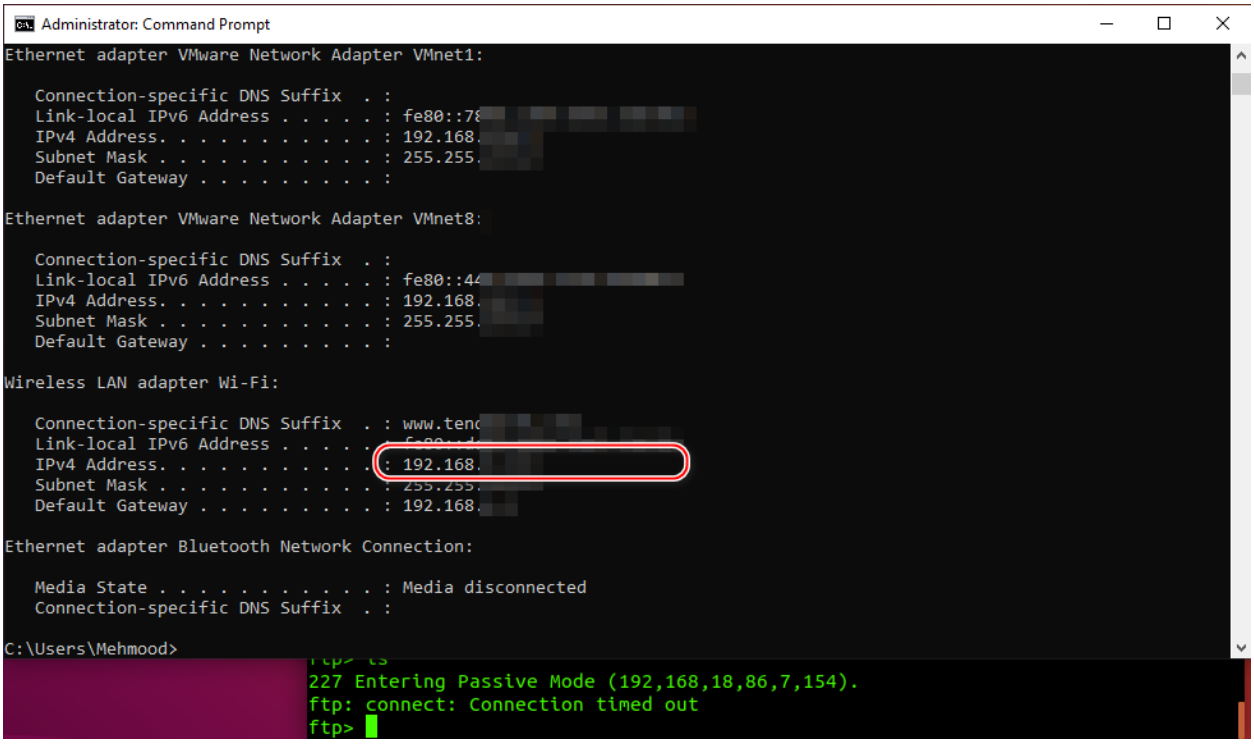
Then after that in search bar search the event viewer and open it.



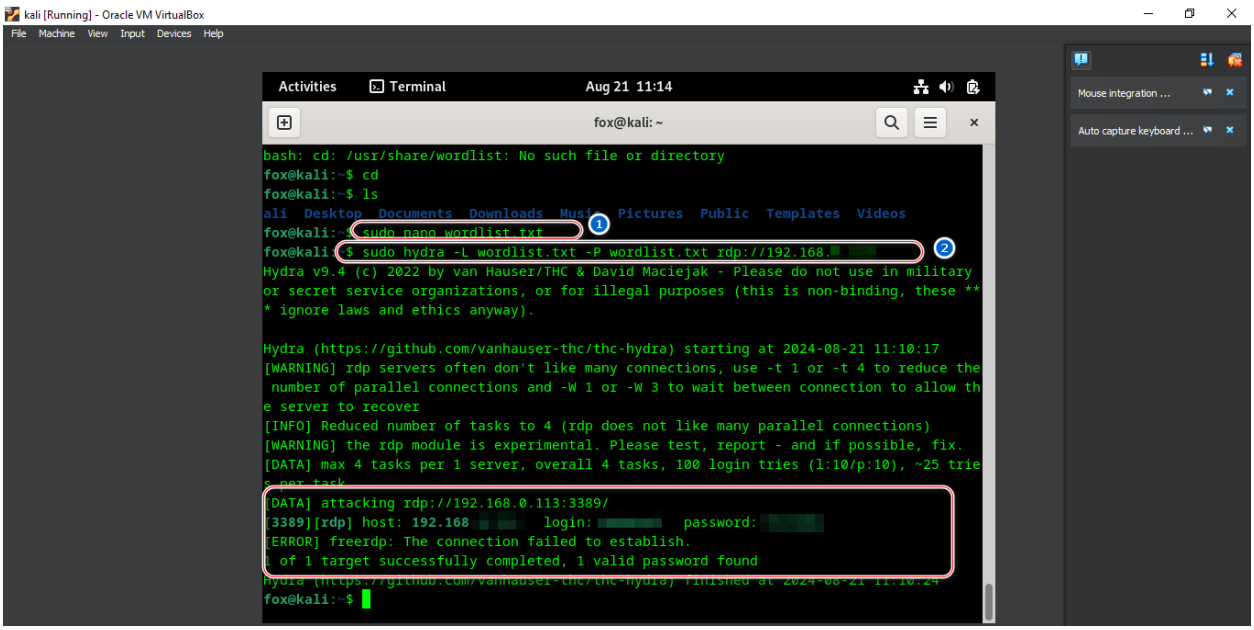
After opening that click on windows logs and then security to check the security logs.



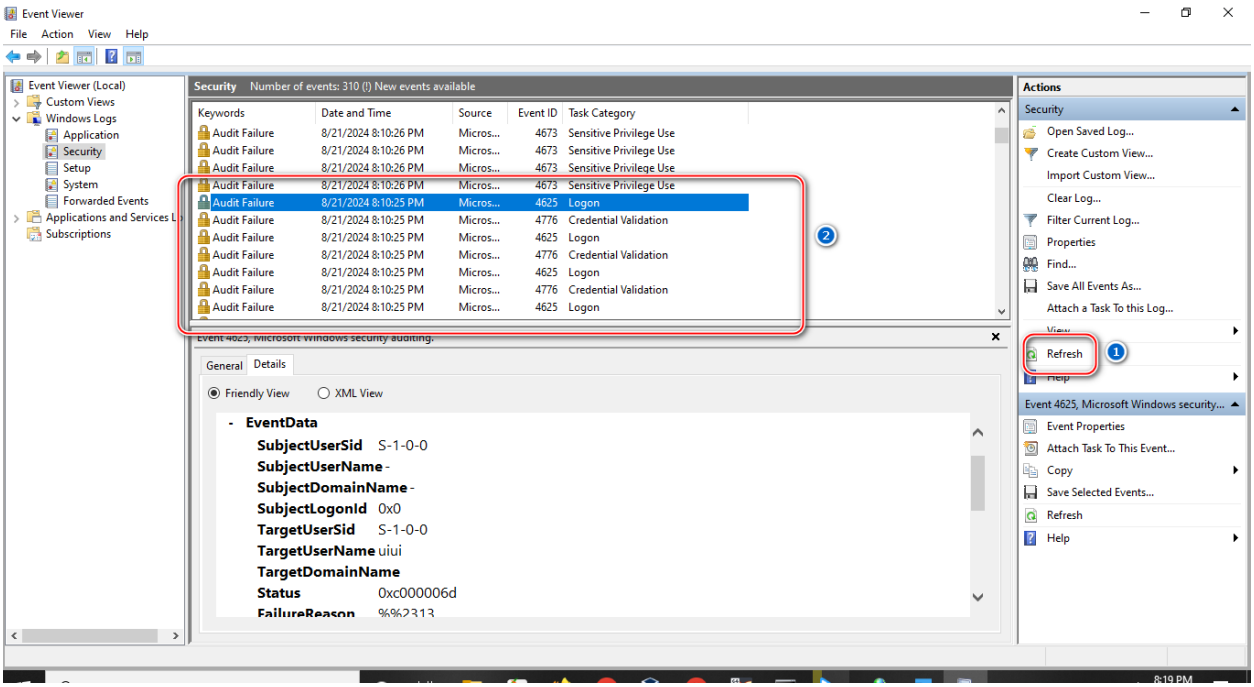
So here as we can see there are some normal default logs of the system so let's clear the logs.



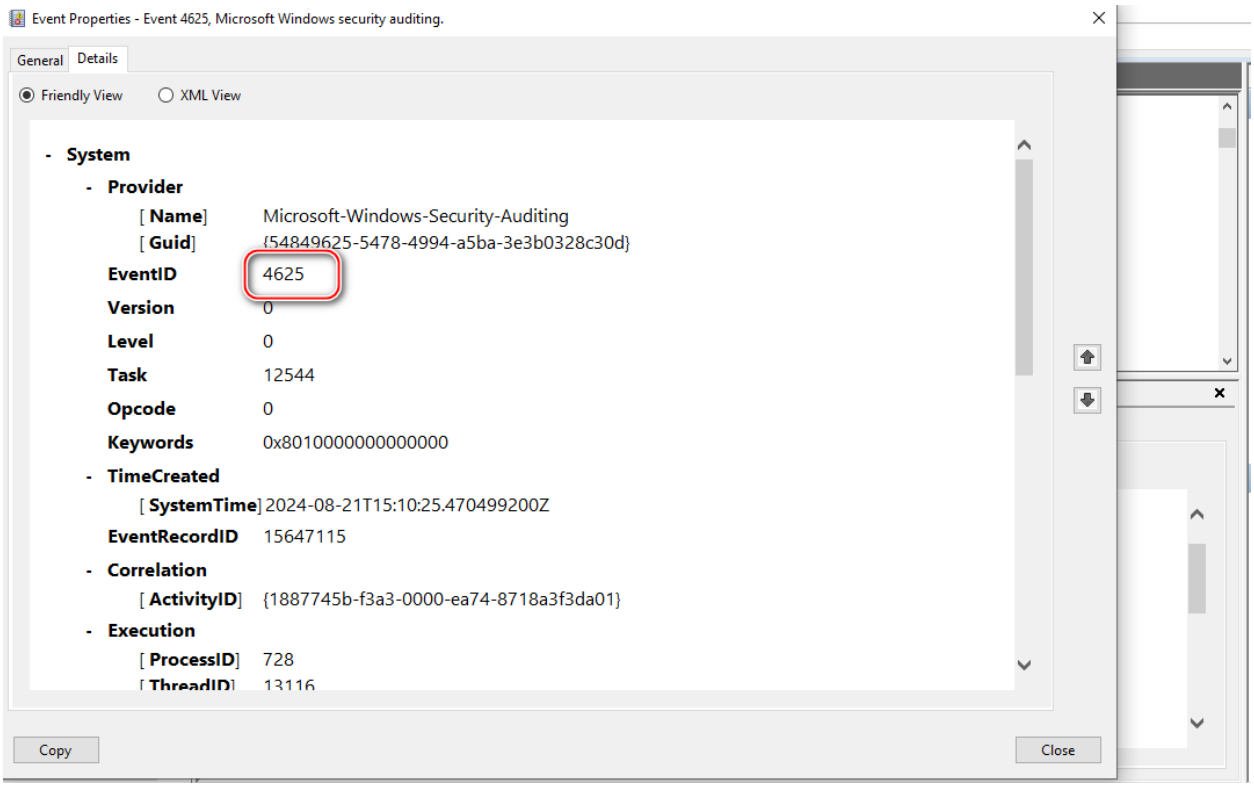
Now to monitor security logs we are just trying brute force attack so for now this window is our victim machine so check windows ip in cmd.



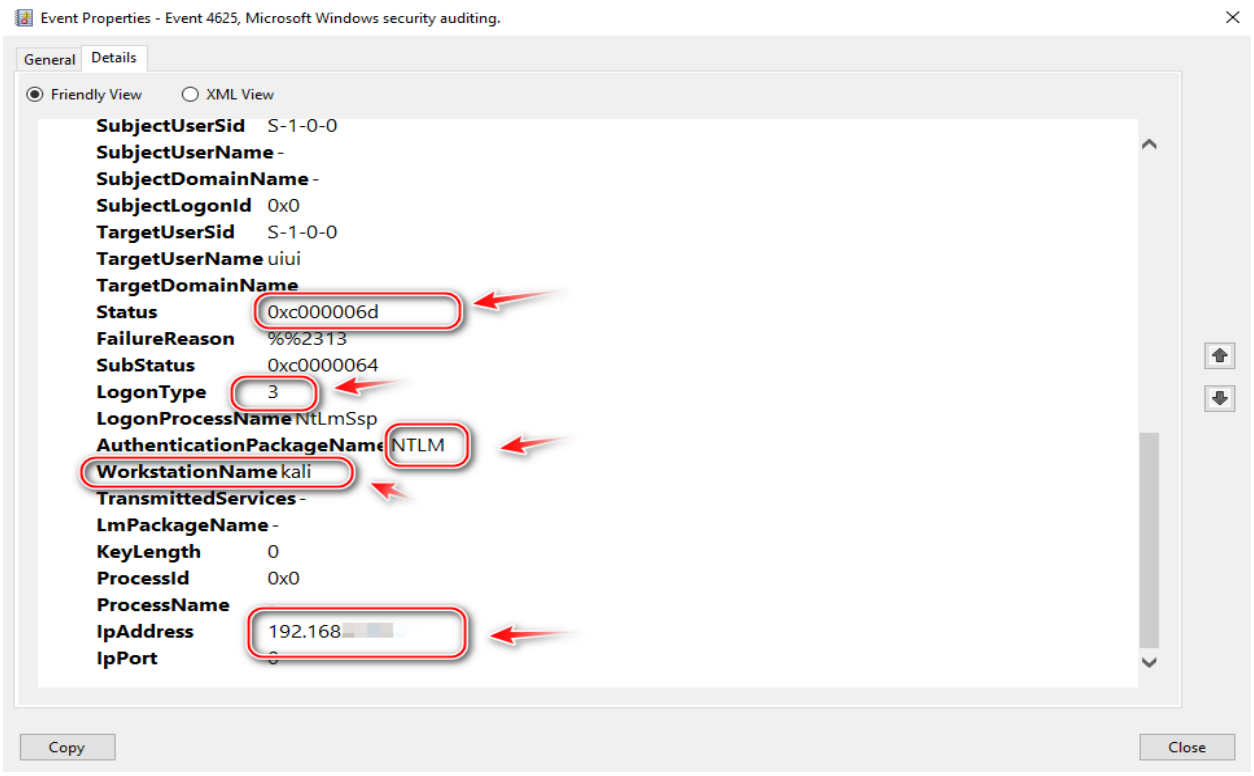
So here as we can see first, I had created a wordlist that include some usernames and passwords. And then I had tried brute force attack on my victim machine with hydra tool so in the end their username and are matched.



So as in that wordlist there are some random usernames and password so here we can see logs are monitored in event viewer so double click on it to check what info is there.



As we can see this is our event id monitored there.



And these are some attacker info and status etc is include in this event.

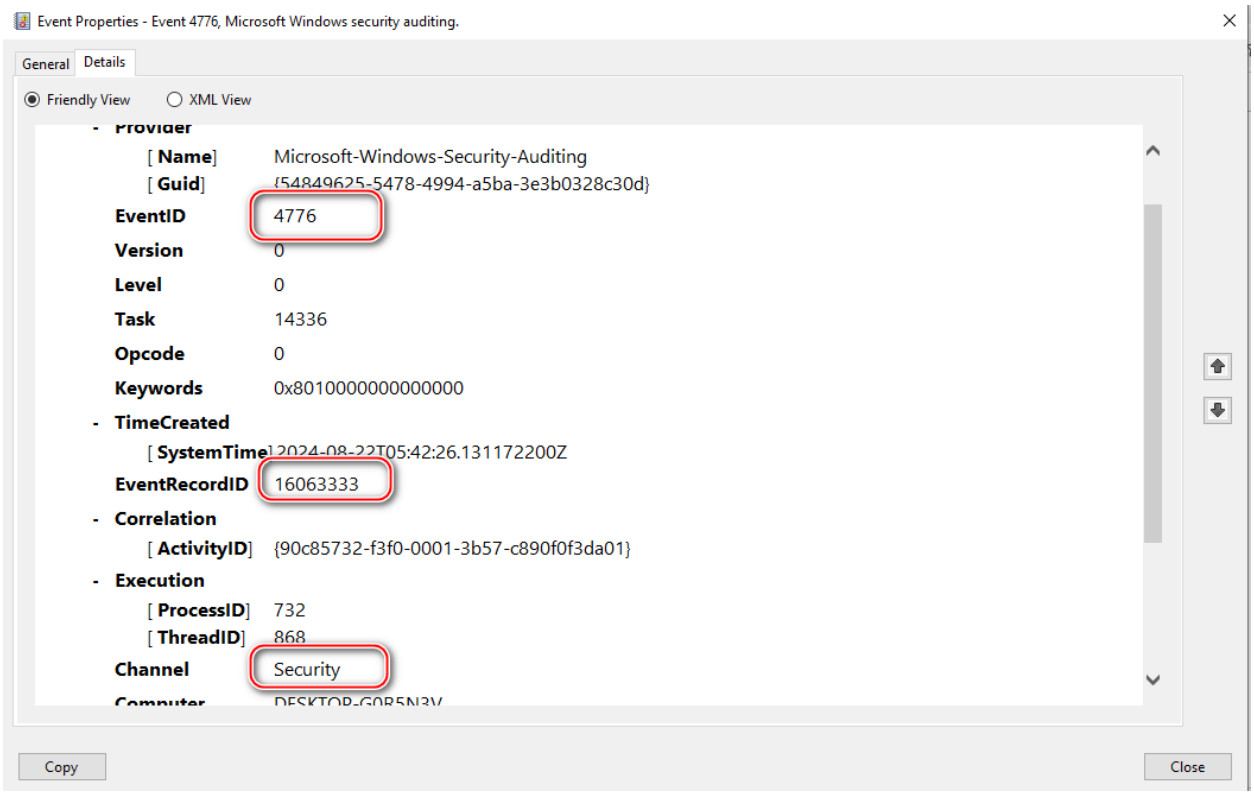
Event ID	Description
4625	A failed logon attempt. Large numbers of these throughout a network may be indicative of password guessing or password spraying attacks. Again, the Network Information section of the event description can provide valuable information about a remote host attempting to log on to the system. Note that failed logons over RDP may log as Type 3 rather than Type 10, depending on the systems involved. You can determine more about the reason for the failure by consulting the Failure Information section of the event description.

So here event id 4625 had some description that user had tried some random password as I tried wordlist ant trying to guess the password and username.

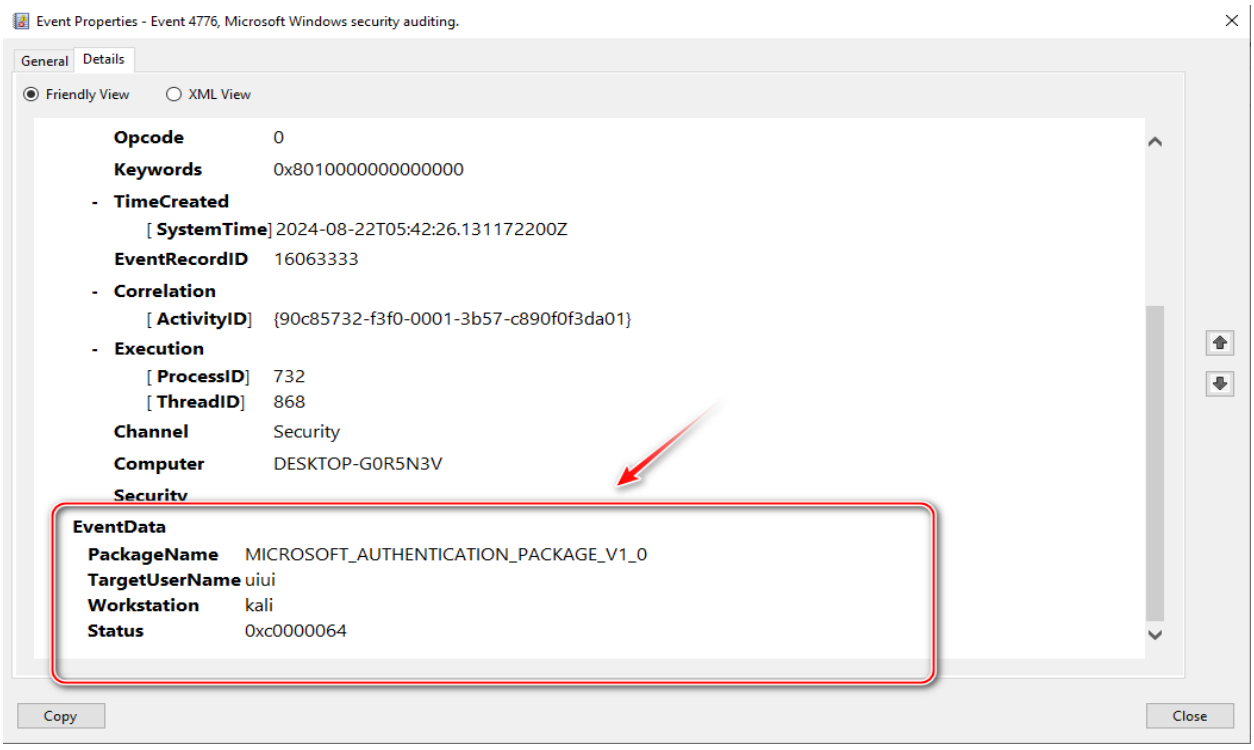
Common logon failure status codes

Status code	Description
0XC000005E	Currently no logon servers are available to service the logon request.
0xC0000064	User logon with misspelled or bad user account.
0xC000006A	User logon with misspelled or bad password.
0XC000006D	This is either due to a bad username or incorrect authentication information.
0XC000006E	Unknown username or bad password.
0xC000006F	User logon outside authorized hours.
0xC0000070	User logon from unauthorized workstation.
0xC0000071	User logon with expired password.
0xC0000072	User logon to account disabled by administrator.
0XC00000DC	Indicates the Server was in the wrong state to perform the desired operation.
0XC0000133	Clocks between domain controller and other computer too far out of sync.
0XC000015B	The user has not been granted the requested logon type (also known as logon right) at this machine.

The event failure status code is that mean the bad user is trying wrong passwords.



Now I have another event there occurred with event id 4776 and event record is that etc.



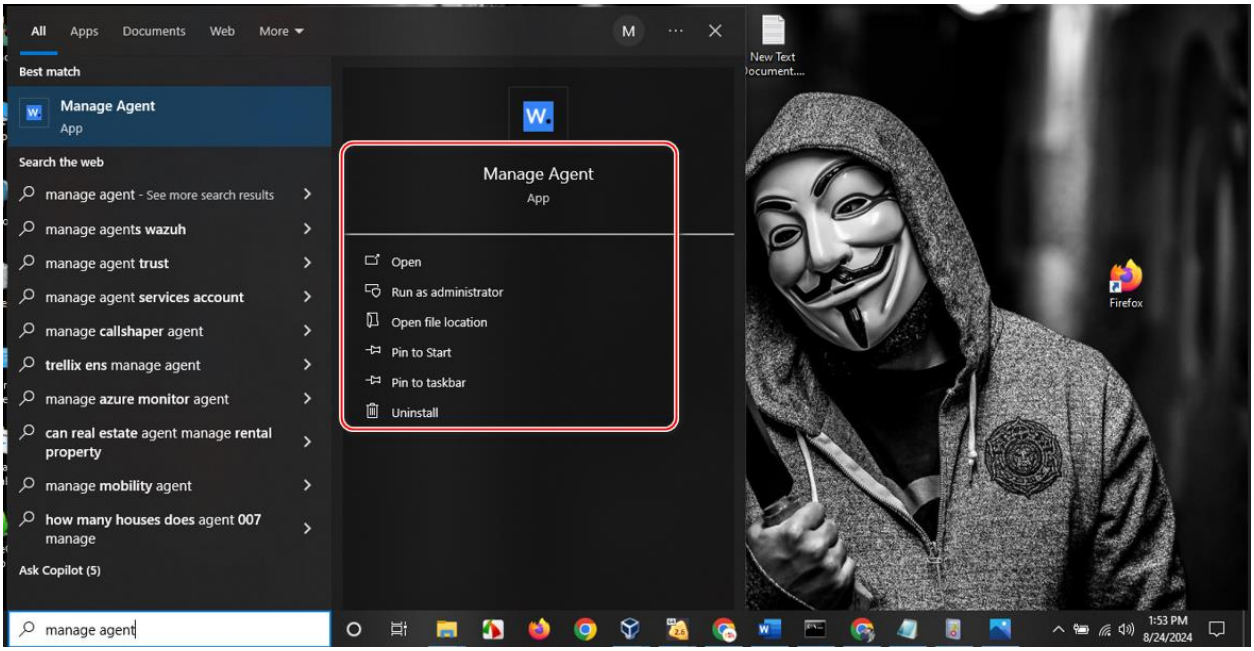
Here is the attacker information and status code.

4776	This event ID is recorded for NTLM authentication attempts. The Network Information section of the event description contains additional information about the remote host in the event of a remote logon attempt. The Keywords field indicates whether the authentication attempt succeeded or failed. In the event of authentication failure, the error code in the event description provides additional details about the failure, as described in Table 8.3. A series of failed 4776 events with Error Code C000006A (the password is invalid) followed by an Error Code C0000234 (the account is locked out) may be indicative of a failed password guessing attack (or a user who has simply forgotten the account password). Similarly, a series of failed 4776 events followed by a successful 4776 event may show a successful password guessing attack. The presence of Event ID 4776 on a member server or client is indicative of a user attempting to authenticate to a local account on that system and may in and of itself be cause for further investigation.

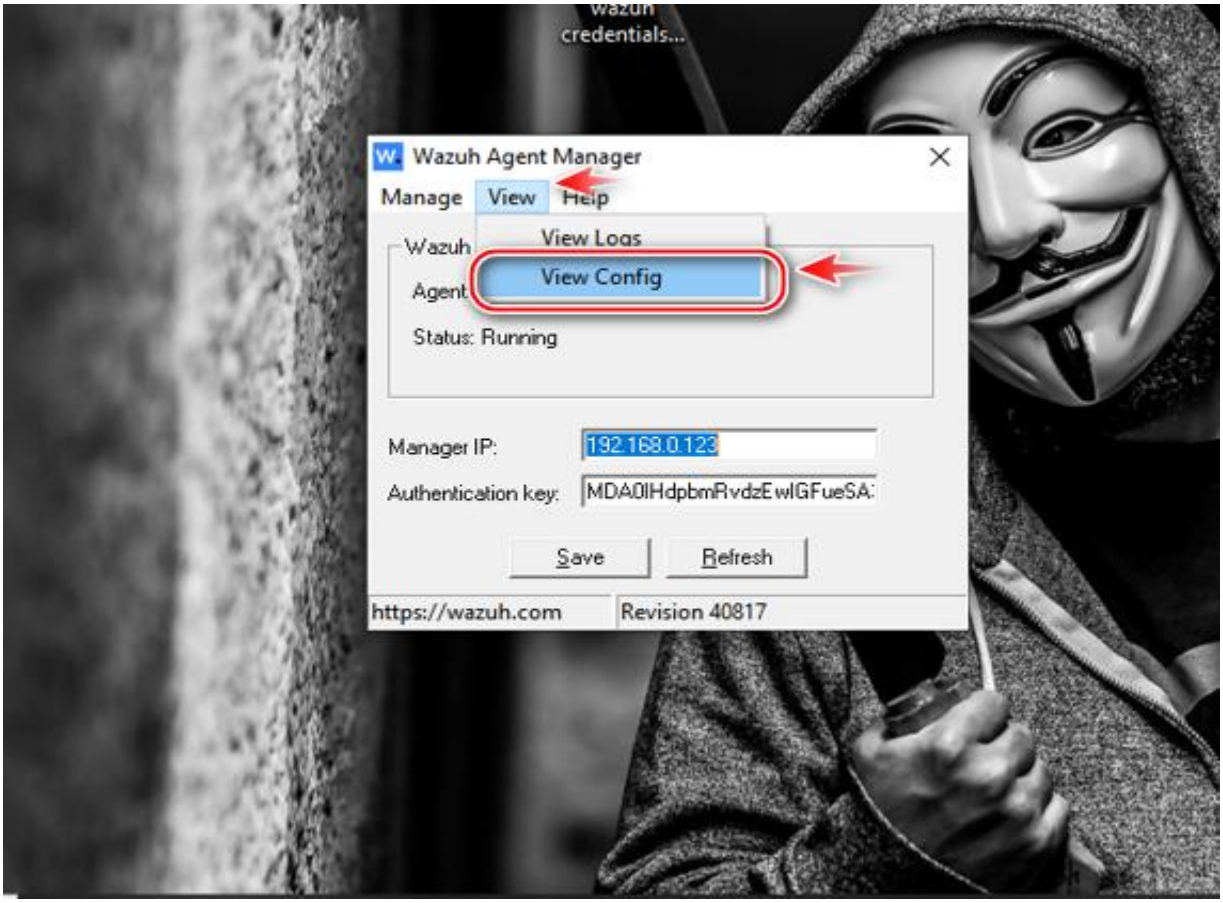
So according that information like event id the user had tried many attempts remotely. But attacker failed.

Now this is all the information about the windows log analysis in event viewer so we have to integrate these events of window to Wazuh to monitor there.

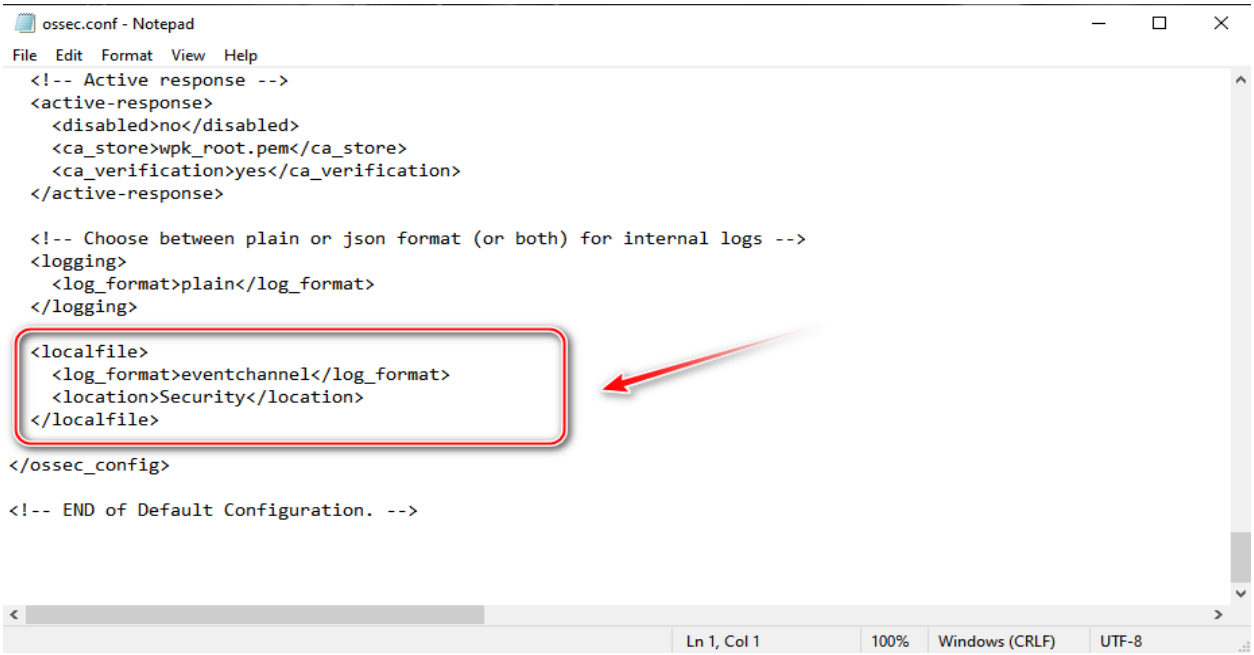
so first of all make sure that you Wazuh agent is installed in your windows machine. As I installed.



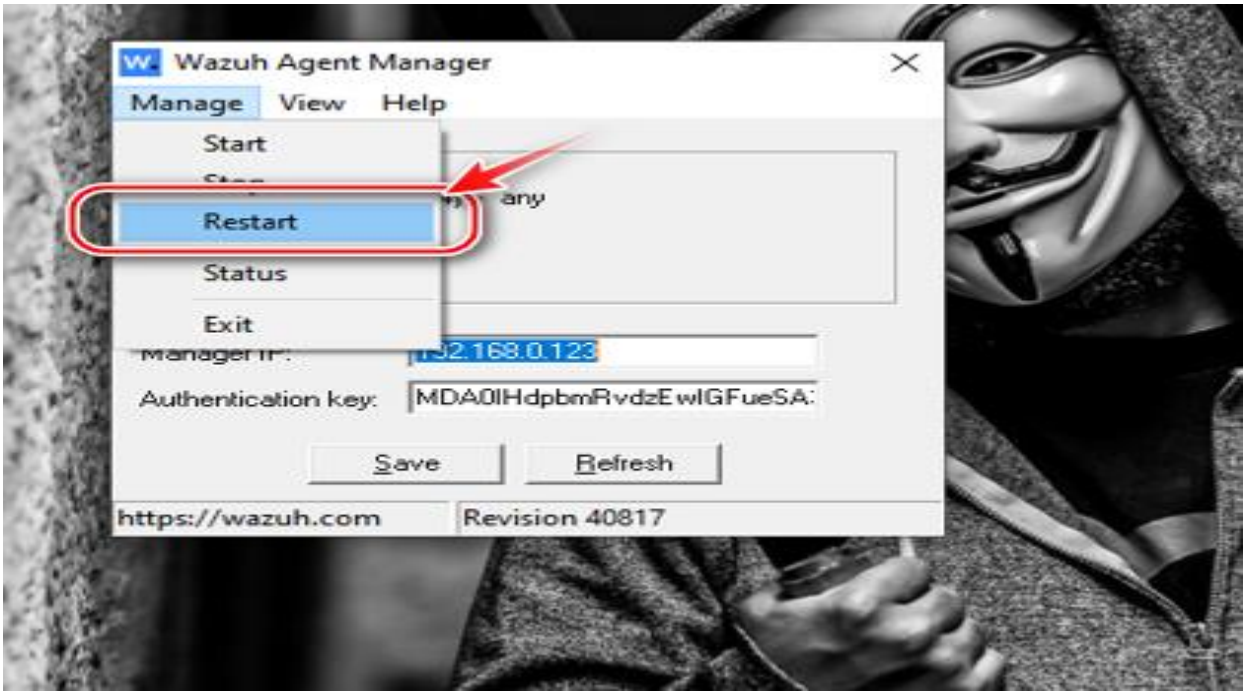
In search bar of Window you can find your Wazuh agent manager.



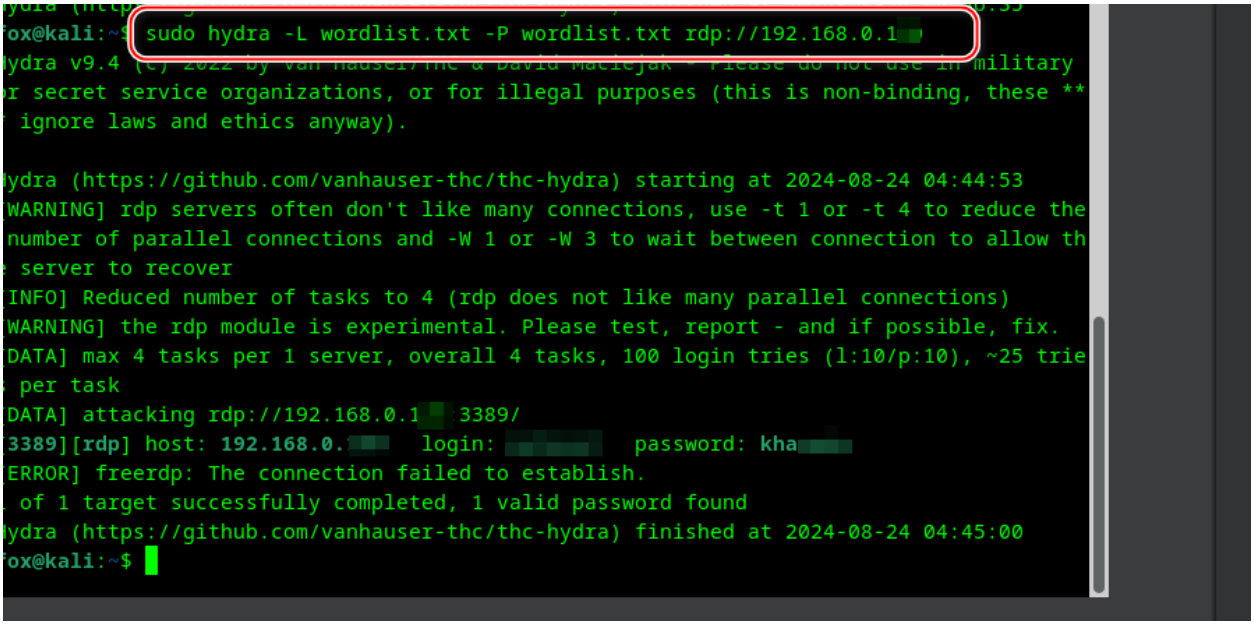
Then in view tab clink view config file to open the Wazuh configuration file.



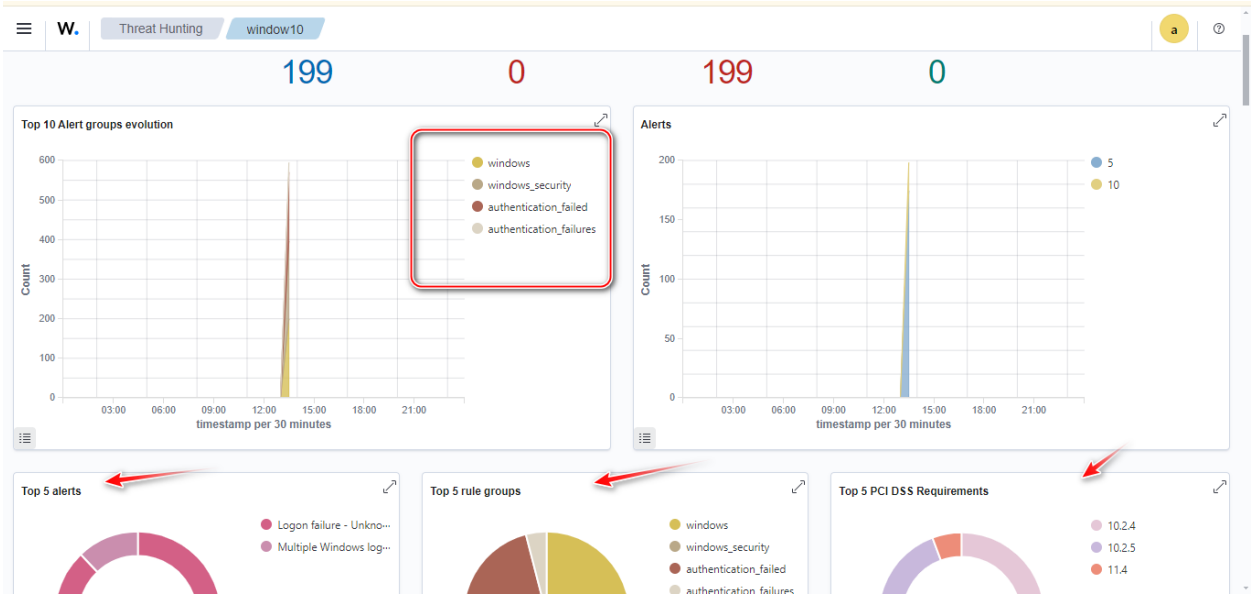
In configuration as I added this file to monitor the security events.



After that you will need just to restart your Wazuh agent.

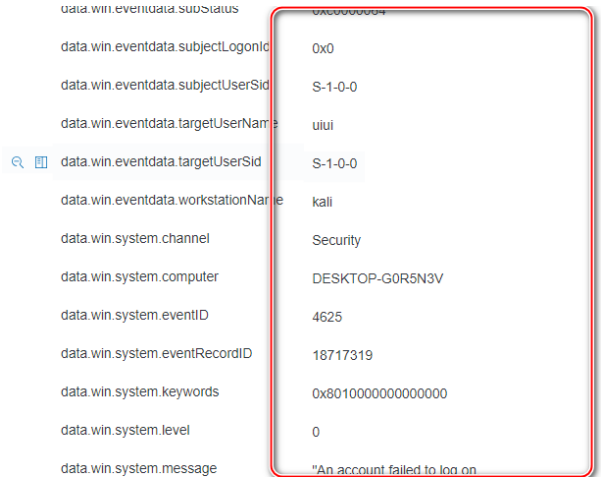


Then after all setting up, I just open my kali which is my attacker machine this time and tried the brute force attack.



Here now open your Wazuh dashboard and select your machine and go to threat hunting section. So here you can see all events.

Here are some details of the attacker machine and status codes which I explained earlier in this lecture.



Here is how some more information of this event like event id attacker system name event type security etc.

Linux and Windows Log Analysis Summary

Linux Logs:

Logs in Linux systems, such as boot.log, cron.log, secure.log, mail.log, httpd.log, and messages.log, are stored in the /var/log directory and are essential for monitoring system activity and diagnosing issues. Each log serves a specific purpose: boot.log records startup events, cron.log logs scheduled tasks, secure.log tracks security-related information, mail.log covers email processing, httpd.log details web server activity, and messages.log captures general system events. To analyze these logs, utilities can be used to review their contents and integrate them with Wazuh for centralized monitoring.

Windows Logs:

In Windows, logs such as Security, Application, and System logs are accessed through the Event Viewer and are crucial for monitoring system activity, detecting security events, and troubleshooting issues. Monitoring these logs helps identify unauthorized access and track system changes. Integrating Windows logs with Wazuh involves configuring the Wazuh agent to capture and send logs to a central server, where they can be analyzed for potential threats using the Wazuh dashboard