Tackling Cyber Kill Chain Stages in a lab Environment

MSc Research Project
Cybersecurity

Preetam Shrikar Kolekar
Student ID: X21179352

School of Computing
National College of Ireland

Supervisor: Prof. Michael Pantridge

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: ……. ……Preetam Shrikar Kolekar……

Student ID: ……x21179352…….……

Programme: ……MSc in Cybersecurity ……(MSCCYB1) **Year:** …2023……..

Module: ……Research Project…….……

Supervisor: ……Michael Pantridge…….……

Submission Due Date: ……18th September, 2023…….……

Project Title: ……Tackling The Cyber Kill Chain Stages In A Lab Environment……

Word Count: ……6400…… **Page Count**……24…….……..

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Preetam

Date: ……18/09/23……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Tackling Cyber Kill Chain Stages In A Lab Environment

Preetam Shrikar Kolekar
X21179352

Abstract

This thesis included an in-depth analysis on how to tackle each stage of the Cyber Kill Chain in a lab environment. The hypothesis of this project includes mapping the CIS v8 Controls to the MITRE ATT&CK techniques and implement the mitigation inspired from CIS Controls to provide a mitigation to break the kill chain. The implementation has been performed using a lab setup which server as a generic and secure ecosystem/environment which will demonstrate several security solutions such as SIEM, NIDS, HIDS, Proxy, Firewall, Malware Scanning. By using one or more implemented security solutions, we have created a lab to safeguard itself from attacks by tailoring it specifically to tackle every stage of the Cyber Kill Chain. The lab is setup using a type-2 hypervisor: Oracle Virtual Box. Where the victim machine is a Windows 10 VM and Linux serves as a gateway for security solutions. Wherever possible, we have made use of cloud services such as ELK in the Cloud to reduce the workload on the underlying hardware and provide us high availability of the SIEM service.

1 Introduction

1.1 Background

Cybersecurity comprises of a plethora of techniques, strategies, and technologies to protect systems and information from cyber-attacks. Cybersecurity embodies measures to safeguard data/information from theft, damage or unauthorized access. This encompasses multiple aspects of people, process, and technology (PPT) such information security, network security, data protection and privacy, application security, access control, disaster recovery, user awareness, continuous monitoring and continual improvement.

Cyber attacks include intentional exploit of information systems and networks in order to achieve disruption in services, financial gain, theft or defamation. Although, there are numerous ways using which data breaches can be performed, but some of the common attack types include Malware attack, Phishing, Denial of Service (DoS), Man in the middle attack (MITM), SQL Injection and Zero-Day exploitation. To tackle these threats, several mitigations can be placed to protect the information systems such as Firewall, Intrusion Detection Systems (IDS), Access Control, Security Awareness Training, Antivirus tools, Disaster Recovery (DR), Incident Response Planning, etc. These mitigations are combined together to provide multiple layers of security which is also known as defence-in-depth.

Mitre ATT&CK Framework - Mitre ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) Framework is a vast and in-depth knowledge base that cybersecurity enthusiasts can refer to gain knowledge about the methods and strategies implemented by cyber adversaries. It serves as a tool that maps the enter lifecycle of an attack and provides knowledge

on the various stages an attacker may follow to successfully perform and attack. Below are the key aspects of Mitre ATT&CK Framework:

- Tactics – These are the objectives of an attack, for example: Active Scanning, Account Manipulation, Phishing, Privilege Escalation, Credential Access, etc.
- Techniques – Tactics include specific techniques which define how an attacker can possibly achieve the tactical objective. For example: Initial Access tactic includes spear-phishing and exploiting public facing applications.
- Sub-Techniques – Several techniques are further drilled down into one or more sub-techniques which provides us with a granular aspect of how the attack can take place.
- Procedures – These are the implementation methods inside a techniques or sub-technique.
- Mitigations – For every technique, the framework provides a brief description on how to mitigate these attack types. *(Strom et al.)*

Cyber Kill Chain – Developed by Lockheed Martin, the cyber kill chain is a model which describes the stages of cyber attacks. This kill chain divides an attack into separate stages, each representing a stage in the process of an attack. The stages of Cyber Kill Chain include:

1. Reconnaissance – This is the first phase in the kill chain which includes an attacker gathering information of the target. This entails the attacker tries to gain information of the security posture, publicly available data that can be used to leverage the attack and possible vulnerabilities in the system.
2. Weaponization – In this phase of the kill chain, the attacker builds a weapon such as malware or phishing site which is tailored to lure victims and attack specific vulnerabilities identified in the Reconnaissance stage.
3. Delivery – This stage embodies the process of delivering the weapon to the targeted victim. This can be performed using phishing links, email attachments or USB drives.
4. Exploitation – This phase includes the attacker executing the delivered weapon and exploiting the identified vulnerability in the system and executes the payload.
5. Installation – Post the exploitation phase, the attacker installs malware such as a backdoor on the system which allows them to preserve the control on the system.
6. Command and Control (C2) – Upon installation of the malware, the malware establishes connections to the attackers command and control servers which allows the attacker to have remote access on the infected machine and issue commands.
7. Actions on Objectives – Final stage of the Cyber Kill Chain includes the attacker stealing data or disrupting systems and operations. *(Yadav & Rao, 2015)*

CIS Controls – The Centre for Internet Security (CIS) Controls, is a framework which includes prioritized set of controls which aim to improve the cybersecurity defences. These controls are developed with a motivation to guide organizations in improving their security posture against known cyber threats and are developed by a community of IT experts bases on real attack data. The CIS controls are a framework and not a standard such as ISO 27001. The advantage of referring to CIS controls is that they are freely available on their website if any organization wishes to add robustness into their security by taking inspiration from the controls of this framework.

The CIS Controls v8 are divided into 18 set of controls which include:

Inventory and Controls of Hardware Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defences, Data Recovery, Network Infrastructure Management, Network Monitoring and Defence,

Security awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management and Penetration Testing. *(Groš, 2021)*

1.2 Motivation and Objective

Motivation:

- **Current Landscape -** There are several security standards and frameworks which can either act as a defensive guidebook for the organizations (For example: CIS controls, ISO 27001, NIST) or act as an offensive guide such as Mitre ATT&CK (Mitre ATT&CK can also be used as a defensive guide by understanding the attack techniques which can be used by adversaries), but there is very little information on the internet as to how anyone can map these defensive frameworks against offensive frameworks in order to secure their environment from actual attacks and attack types. Every organization aims to be secure and remain secure against the modern day's cyber-attacks, but several organizations, especially small to medium businesses (SMBs) lack the required resources in terms of knowledge, leadership commitment, finance, and resource competency. *(Bashofi and Salman, 2022)*

- **Relevance of Integration –** By combining offensive and defensive techniques and frameworks together will give us a clearer picture of how we could secure our organization as it would allow us to understand how the offensive strategies work, how the attack is carried out and what are the ways we could implement to mitigate specific type of attacks. Mitre ATT&CK techniques include a knowledge base that cybersecurity enthusiasts and professions can use to understand the techniques which may potentially be used by their adversaries or malicious actors. CIS Controls include several strategies and controls for every aspect of the security structure in order to safeguard organizations from data breaches. By integrating both these frameworks and mapping them against Cyber Kill Chain stages will provide us with a clear understanding on how we could mitigate the attacks and what type of controls are possible to implement in a virtual lab which is limited by a single host and free/open-source tools in order to demonstrate the implementation of the thesis.

- **Need for Implementation** – As a research paper, theoretically, mapping of defensive controls against cyber-attack types is possible but there can be unlimited number of ways on how this can be achieved in reality. The lab implementation will demonstrate how the basic security environment can be setup in order to detect and tackle the data breaches by referring to the mapping of security control and attack types performed.

Objective:

This topic aims to combine multiple frameworks which are offensive as well as defensive in order to build an environment which can incorporate certain defensive controls using which modern day cyberattacks can be tackled. This project aims to build a generic and secure lab ecosystem/environment that can be used as a foundation for a secure environment which can be further improved upon by adding more security features and fine-tuning the current security policies and implementations of the lab to accommodate the needs of certain attack types.
The hypothesis of this project includes the mitigation towards Mitre Attack techniques inspired from CIS critical security controls (v8) and tackling the Cyber Kill Chain in order to break the chain. The implementation of this project includes use of these mitigation techniques and deploying several rules, policies, security tools and strategies using virtual machines to serve as a proof of concept for the hypothesis.

1.3 Scope

The Scope of this research paper is to perform analysis and test how the CIS Control mitigations map against Mitre ATT&CK Framework and provide at least one mitigation to break each stages of Cyber Kill Chain in a lab environment with limited resources of a single host machine using free or open-source tools. The implementation of mitigations will be done using a Linux and a Windows virtual machine environment and some cloud services (if required) where Linux system will have control services and policies which will help evade the attack/stages of attacks on the Windows virtual machine.

The overall scope is further divided into below sections:

1. **Research Focus & Scope:**
    a. Mapping Objectives - The research focused on mapping CIS controls as a mitigation against MITRE ATT&CK Framework and Cyber Kill stages.
    b. Cyber Kill Chain Mitigation: Aiming to mitigate the Cyber Kill chain by implementing at least one of the security controls from CIS controls in the virtual lab.
2. **Technical Scope:**
    a. Tools and Technologies – Several tools were used in the lab on Linux and Windows operating system where windows 10 was considered as the victim machine and security tools and strategies were implemented using Linux machine such as ELK Stack for Log and resource monitoring, Snort for NIDS, OSSEC for HIDS, Squid for proxy and URL Blocking, YARA for scanning malicious files, Firewall, Antivirus, Sysmon, Winlogbeat for shipping Sysmon logs.
    b. Virtual Lab Environment – A virtual lab setup using a hypervisor such as Oracle Virtual Box or VMWare.

1.4 Contribution to Scientific Research

This research studies the mapping of offensive and defensive framework and implements the possible outcomes in a lab setup. Ideally, this research will provide its readers with an insight of protecting their organizations from specific attack types such as mentioned in MITRE ATT&CK and help them to understand the required security controls to provide a mitigation on each stage of the Cyber Kill Chain.

1.5 Thesis Outline

2 Related Work

- **MITRE ATT&CK: Design and Philosophy:**

This research paper provides an overall understanding of MITRE ATT&CK. MITRE ATT&CK is a knowledge base of adversarial tactics which adversaries might use to perform cyber attacks. This paper talks about the need to create this framework, its design and philosophy amongst other things. This report emphasised that ATT&CK is being used for

emulating adversary behaviour and red teaming. This paper defines the structure of ATT&CK framework which include tactics, techniques, sub-techniques and procedures. The conclusion consists of statements which point to the use of ATT&CK in multiple security practices and their application across other domains. *(Strom et al.)*

- **Implementing CIS Critical Security Controls for Organization on a Low-Budget:**

This research paper focuses on the approach of implementation of CIS controls with the organizations who do not have access to large funds as small to medium businesses do not have the required resources to spend on implementing high-cost security solutions. This paper shows a potential approach to incorporate most of the CIS Controls without spending large amounts of money. An organization can opt for using several built-in security features in Windows to achieve most of the CIS controls. *(www.proquest.com, 2018)*

3 Research Methodology

The research methodology that was performed for this thesis includes the process followed to gather the required information and knowledge for this report:

Choice of defensive cybersecurity framework:

It was paramount for this thesis to choose a cybersecurity framework which is robust, well-known, formidable, descriptive and relatively easy to adopt. There are several options of cybersecurity & information security frameworks which fit the above description thus more research was required as to which defensive framework has to be chosen.

Below is the comparison of well-known security frameworks: CIS Controls, ISO 27001 & NIST Cybersecurity Framework. *(ISO, 2022) (National Institute of Standards and Technology, 2018) (www.proquest.com, 2018)*

Feature / Framework	CIS Controls v8	ISO 27001	NIST Cybersecurity Framework
Primary Focus	Specific security controls for various threats	Comprehensive Information Security Management System	Risk management across entire cybersecurity lifecycle
Structure	18 Controls with various sub-controls	Various clauses and controls within ISMS	Five core functions with corresponding categories and subcategories
Flexibility	**Practical and adaptable to various sizes of organizations**	Often requires adaptation for small/mid-sized businesses	Scalable and can be tailored to various organization sizes
Implementation Cost	**Low to Moderate**	Can be high, especially for smaller organizations	Moderate to high, depending on alignment with existing practices
Standards Alignment	**Broad alignment with other standards**	International standard recognized globally	Aligned with international standards, but U.S.-centric
Regulatory Recognition	Recognized by various regulatory bodies	Widespread international regulatory recognition	Recognized mainly in the U.S. by various industries and regulators
Guidance Level	Detailed, action-oriented guidance	High-level, management-oriented guidance	High-level strategic guidance with detailed informative references
Industry Focus	Cross-industry	Cross-industry	Primarily U.S. industries but applicable cross-industry
Maintenance & Updates	Regularly updated, community-driven	Regular updates, governed by ISO	Regularly updated by NIST

CIS Controls v8 were chosen as the mitigation framework against MITRE ATT&CK techniques for the following reasons: *(www.proquest.com, 2018)*

1. Practicality – CIS Controls provide specific and actionable guidance on how to implement their controls and certain security measures.
2. Flexibility – The framework is suitable for various sizes and types of organizations, unlike ISO, adapting to this framework does not require a set of highly skilled employees or consultants for implementation as this is not a certifiable standard.
3. Cost Effective – Has much lower implementation cost as the framework can be flexible and adjustable unlike a standard.
4. Alignment with Other Standards – The controls defined in the CIS v8 often align with security controls of multiple standards, thus allowing your organization to ease the compliance achievement with several laws and regulations.
5. Community Driven – Timely updates are driven by a community of cybersecurity experts to ensure effectiveness against modern day threats.

Choice of offensive framework – MITRE ATT&CK

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is basically a knowledge base which is well-known and used to understand several attack techniques, attack phases and understand adversarial behaviour. Below are some of the reasons for opting for this framework for this thesis.

1. Improves Defence Strategies – It is important to understand the behaviour of a cyber attack in order to defend our organization and be able to design a better detection, prevention and response plan.
2. Comprehensive Understanding – MITRE ATT&CK maps the tactics and techniques used by attackers in a detailed way and a granular way. This provides understanding the actual behaviour of attack vectors.
3. Describes complete lifecycle – ATT&CK covers the complete lifecycle of an attack from Reconnaissance to Impact.
4. Supports Red and Blue Team Exercises – Offensive security can use techniques describes in MITRE ATT&CK to simulate an actual attack. Whereas, defensive security can use it to understand the attack types and improve their security strategies. Thus, providing an edge to be used in this thesis.
5. Free and Open – MITRE ATT&CK is available for free for everyone which makes it easy to use for any induvial or organization. *(MITRE, 2023) (Strom et al.)*

Breaking the Cyber Kill Chain – The Cyber Kill Chain defines several stages of attack starting from Reconnaissance to finish at performing Actions on Objectives. It is important to apply security measures to each stage of the Kill Chain to detect or delay or to prevent the attack.

Below is the brief description of the research performed for Kill Chain Mitigations of every stage:

1. Reconnaissance – Detect and block enumeration activities, monitor and analyse the system logs for malicious activities.
2. Weaponization – Web content filtering, malicious URL Blocking, email security.
3. Delivery – Use of HIDS and NIDS, malicious URL Blocking, user awareness.
4. Exploitation – Systems need to be kept updated and patched for mitigating known vulnerabilities.
5. Installation – Implement the principle of Least Privilege and scan actively for changes in the registries. Keep actively scanning the critical files for integrity check.

6. Command & Control (C2) – Monitor for unusual traffic using NIDS that may showcase a communication similar to Command & Control. Keep the virtual lab network segregated from the host network.
7. Actions on Objectives - Monitor critical files and system configuration logs for any changes. Implement access control.

Research on tools – To perform the implementation, I have thoroughly analysed and studied the required strategies and tools which will be required to achieve the goal. Below are the research performed on the required techniques and the specific tools used to be able to meet the goals.

1. **SIEM – Security Incident and Event Management (SIEM**) tools are an important aspect of any cyber defence strategy. SIEM tools provide a real-time log analysis of security events generated by software as well as hardware components of the Information System infrastructure. SIEM tools are used to centrally collect log data from multiple systems and sources and basically display the output in a structured and readable format. SIEM tools can be used to monitor systems, applications and network devices like firewalls. *(González-Granadillo, González-Zarzosa and Diaz, 2021)*

   CIS Controls which suggest the use of SIEM:
   CIS Controls 13, 8, 3, 4,
   - Control 8. Audit Log Management – Audit Log Management control suggest that we need to collect, alert, review and retain audit logs of security incidents or any event for that matter, to help us detect, analyse, and even recover from the attack.
   - Control 13. Network Monitoring and Defence – This control emphasizes on centralizing security event alerts through the entire organization's assets and correlating the logs for analysis. This control specifically suggests a use of SIEM in order to manage and log security alerts in the organization.
   - Control 4. Secure Configuration of Enterprise Assets and Software – This control suggests the use of secure configuration on the assets and software of the organization and monitoring them in real time. A SIEM tool can be used to collect data on any changes in the system configuration.
   - Control 3. Data Protection – A SIEM tool can be used to protect sensitive data by applying DLP integration. SIEM can also be used to identify unusual access patterns or data movements.

Choice of SIEM tool – ELK Stack

ELK Stack is a combination of three tools known as Elasticsearch, Logstash and Kibana. ELK stack is commonly used for visualizing, searching and analysing data in real-time. These three tools perform separate tasks but work together to provide a comprehensive knowledge on real-time logs.

1. Elasticsearch – This component is used to store and search large volumes of data which can be further analysed. Elasticsearch can analyse structured as well as unstructured data.
2. Logstash – Logstash is used to process the data by taking from several sources and processing it to configured destinations. Logstash can parse logs and perform operations in data ingestion and transformation. *(Saurabh Chhajed, 2015)*

3. Kibana – Kibana works as an interface to communicate with the data stored in Elasticsearch and provide a simple way to do so. It is used to visualize data, create dashboards, build charts on the input data.

Research performed on why to use ELK Stack as a SIEM Solution: *(Saurabh Chhajed, 2015)*

- Cost Effectiveness – As ELK Stack is open-source, this makes it a strong option to be considered for such kind of a thesis where I do not have any access to enterprise grade tools and infrastructure.
- Real-time Analysis and Monitoring – ELK Stack provides real time monitoring and analysis of logs, in this case we require to monitor and analyse Sysmon logs from a Windows 10 VM.
- Scalable – Elasticsearch is created in such a way that it can accommodate data of variable size. ELK stack is capable of handling small set as well as large sets of enterprise data. It is scalable as per your needs, thus making it suitable for implementation of the thesis.
- Easy to deploy and integrate – ELK Stack integrates well with Sysmon to be able to read logs from windows VM and log shipping tools such as winlogbeat are fairly easy to install on the windows system and ship logs to the ELK Stack.

2. **NIDS – Network Intrusion Detection System (NIDS)** is a security feature which is used to monitor the traffic flowing through your network for any malicious activities. The requirement for NIDS here is to actively monitor the traffic flow and provide alerts in case of any suspicious activities based on the defined rules.
   CIS Controls which suggest the use of NIDS:
   - Control 13. Network Monitoring and Defence – This CIS Control motivates the implementation of NIDS to facilitate monitoring of network traffic which helps in detecting potential security threats.
   - Control 12. Network Infrastructure Management – This control suggests implementing NIDS to ensure network devices are securely managed.

Choice of NIDS Tool – SNORT

Snort is an open-source network intrusion detection system (NIDS) which can be configured to monitor network traffic in real-time and provide alerts for any suspicious activity on the network based on defined rules. *(Roesch, 1999)*

Research performed on why to use SNORT for this thesis:

- Cost-Effective – SNORT is an open-source tool, thus it is an ideal choice for this type of thesis where I am limited to use free or open-source variants of security tools.
- Flexibility – SNORT can also be used as a packet sniffer, packet logger along with its complete NIDS capabilities.
- Adaptability – We can configure Snort to use rules based on our needs or we can also find large sets of rules which can be simply imported into its local.rules file to be used for network monitoring without you needing to configure separate rules.
- Frequent Updates – Snort is frequently updated to adapt the modern threat landscape.

3. **HIDS –** Host Intrusion Detection System (HIDS) is a host-based security tool that is used to monitor the system logs and not the network. HIDS is focused on individual systems instead of networks of multiple systems.
   CIS Controls which suggest the use of HIDS:
   - Control 3. Data Protection – HIDS can be configured to identify file integrity changes of critical files and can log modification to data on sensitive files.

- Control 5. Account Management – HIDS can detect privilege escalation attempts and unusual account behaviours.
- Control 8. Audit Log Management – Audit Log Management control suggest that we need to collect, alert, review and retain audit logs of security incidents or any event for that matter, to help us detect, analyse, and even recover from the attack. This control is directly related to HIDS as it aims to implement logging and monitoring at the host side.

Choice of HIDS Tool- OSSEC (Open-Source Security) is an open-source HIDS which is used to perform file integrity checking, log analysis, win registry monitoring, sending real-time alerts, etc.

Research performed on why to use OSSEC for this thesis: ***(Cid, Hay and Bray, 2008)***

- Open-Source – As OSSEC is open-source, it is free and has a major advantage of being community driven which provide timely update against modern threats. Thus, making it suitable for implementation of this thesis.
- Customizable – OSSEC allows to customize its configuration file based on our need to be able to receive the logs as per our convenience.
- Multi-Functional – Has multiple features such as log analysis, file integrity check and rootkit detection which provides convenience for monitoring.

4. **YARA –** YARA is a malware dentification and classification tool which allows researchers to create rules to detect specific malware files that consist Boolean expressions and strings. It can serve as an additional layer of malware detection tool along with traditional anti-malware tools such as Windows Defender, as used in this thesis. (Si et al., 2022)

   CIS Controls which suggest the use of Malware Defense.
   Control 10. Malware Defenses – This involves implementing Anti-Malware tools along with utilizing YARA to scan for malware signatures.

Research performed on why to use YARA and Windows Defender for malware security:

- Free to use – YARA is an open-source tool and Windows Defender works as a free anti-virus tool on the windows host machine.
- Email and Web Browser protection – YARA can be used to filter content to provide security against email and web browsers. YARA can be used to scan Email attachments and download files for malicious signatures.
- Automation – YARA can be automated and scheduled to run and scan for malware signatures to detect malicious files.

5. Squid – Squid is an open-source caching and Proxy service which can be used to cache web contents and increase response time along with performing content filtering and URL blocking.
   These features of Squid can help in blocking malicious URLs in order to reduce the risk of phishing.

4 Design Specification

Hardware Requirements:

Machine	Operating System	RAM	Processor	Storage
Host Machine	Windows 10	16 GB	Inter i7 or i5 (Quad Core)	512 GB
Virtual Machine 1	Kali	4 GB	4 vCPUs	120 GB
Virtual Machine 2	Windows 10	2 GB	2 vCPUs	80 GB

Software Requirements:
Oracle Virtual Box 6.1 or higher

Hypothesis Design Specification:

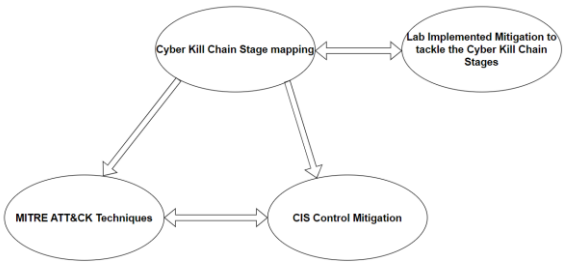


Fig 1. Mapping of Hypothesis Design Architecture

The Hypothesis Design specification includes the mapping of an offensive framework/knowledge base MITRE ATT&CK's attack techniques with the mitigating controls from Centre for Internet Security. The CIS controls are referred to provide a mitigation against the attack which can be in any stage of the Cyber Kill Chain. The CIS mitigation against the attack type describes solutions to break, delay or detect the CKC stage. The mitigation which will be implemented in the lab is then documented in the CKC Mitigation column of the attached excel sheet name "Mapping". Please refer the attached excel sheet "Mapping".

Lab Architecture:

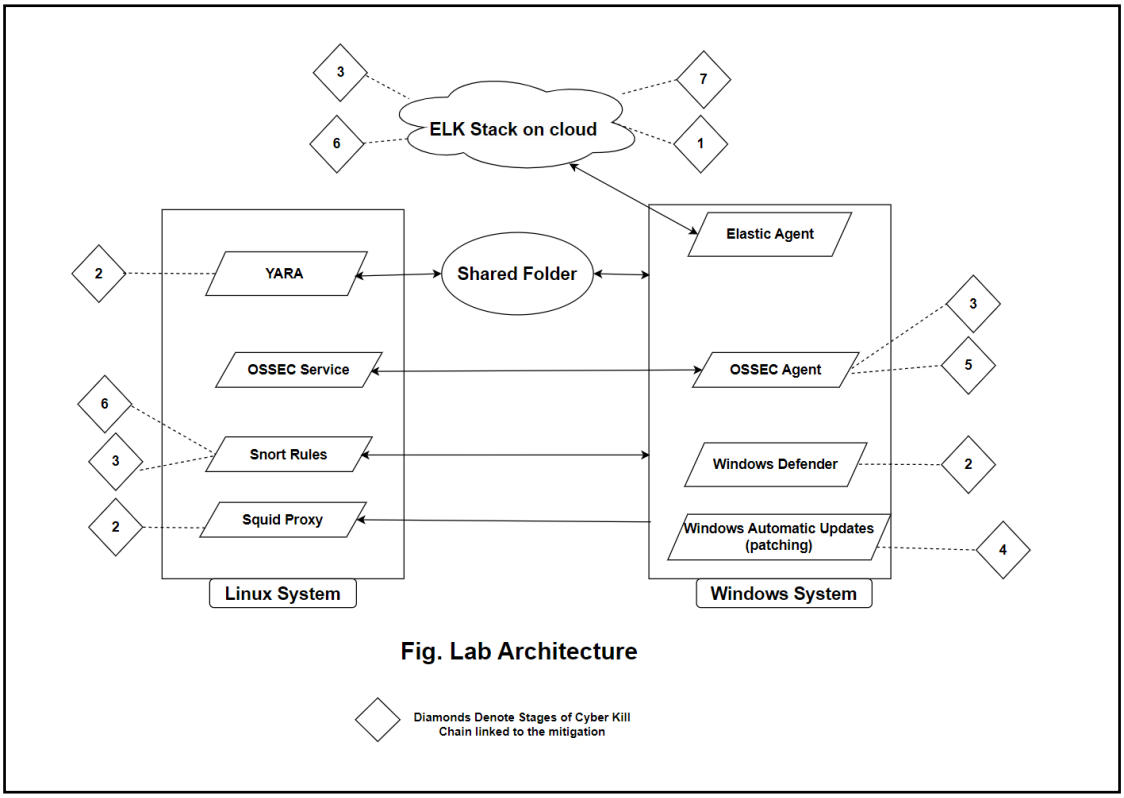


Fig 2. Implementation Lab Architecture

Inside the Lab Architecture, several strategies and tools inspired from the CIS Mitigation column from the attached excel sheet "Mapping" (refer the attached excel sheet "Mapping") are implemented to detect, delay or possibly break the Cyber Kill Chain stage.

Below are the specifications of implemented strategies to tackle the cyber kill chain stage:

1. **Reconnaissance –** This stage talks about enumerating and gathering information about the victim. This stage is tackled using the ELK Stack SIEM which monitors the victim machine (Windows 10 VM) logs for any suspicious activities. The collected logs can be analysed and once a suspicious activity is detected, further action can be taken to block it.
2. **Weaponization –** In this stage the attacker creates a weapon such as a malware or a phishing link, we have implemented Squid as proxy and performed URL blocking for known malicious websites, this will help in blocking the malicious sites and denying the phishing attack. Windows Defender on the Windows VM will help in keeping the malicious files in check, whereas additionally, YARA rules have been set to detect files with malicious signatures.
3. **Delivery –** In this stage, the attacker delivers the weapons using something like a phishing link, thus malicious URL are blocked using Squid tool and OSSEC for HIDS and Snort for NIDS and ELK Stack for SIEM are implemented to scan for any changes in the file integrity of critical files and any suspicious network activity, respectively.
4. **Exploitation –** Windows system has automatic updates enables in order to stay updated against latest vulnerabilities, thus patching is taken care of.
5. **Installation –** OSSEC and SIEM will actively scan for any integrity changes of critical files. The principle of least privilege can also be used where the user of the system will not have rights to install any unauthorized software.

6. **Command and Control (C2)** – Snort can be used to continually monitor the network for any suspicious activity or communication to and from the victim and the attacker using SIEM and Snort. The Virtual Labs need to be segregated from the host and they should not be able to directly communicate.
7. **Actions on Objective** – Once the attacker has reached this stage, it is quite difficult to evade the attack in an environment such as this where I am limited by several constraints such as lack of enterprise tools, automated software, host resource limitations, etc. However, SIEM tool can help by detecting the system configuration logs for any suspicious changes. OSSEC can also be helpful in this. *(Yadav and Rao, 2015) (Groš, 2021)*

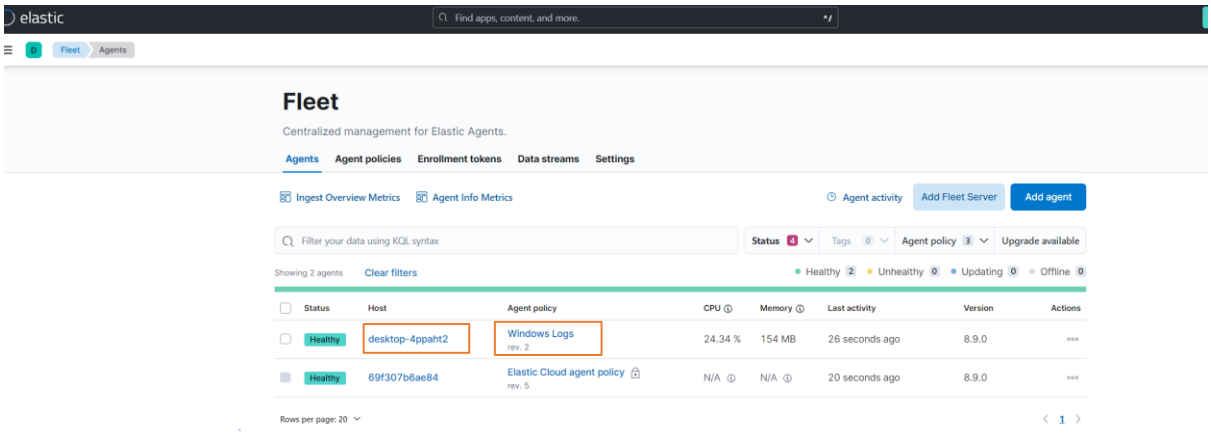
5. Implementation

The implementation of this thesis is performed in terms of the lab, where we have taken inputs from the excel sheet which we used to produce mappings of CIS Controls mitigation against MITRE ATT&CK techniques and then took at least one of the mitigations to be able to detect, delay or possibly break the cyber kill chain. The implementation of this thesis is a secure, generic lab environment which will include the required foundation of security requirements for this project and it can be further improved to harden the present security controls by adding more specific rules to the strategies implemented based on the attack scenarios.

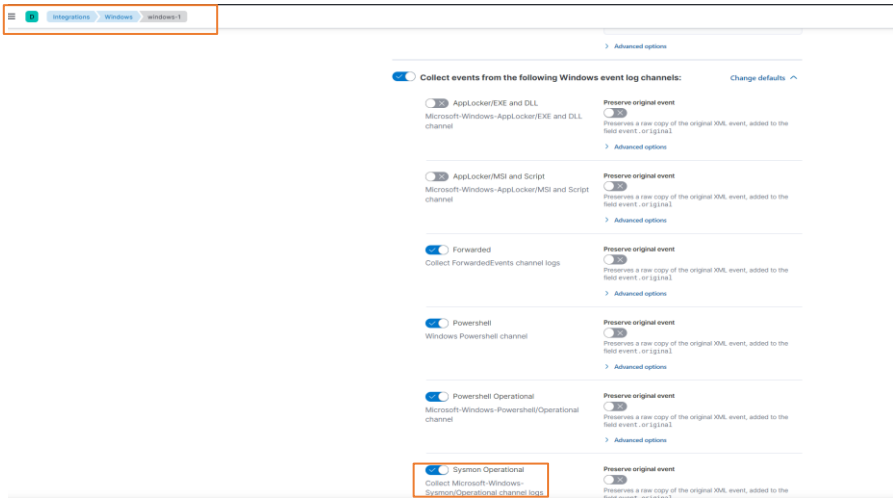
1**. Implementing SIEM: ELK Stack.** ***(Strand, 2022)***

As we are using a cloud hosted ELK Stack, we will be proceeding with reading the Sysmon logs from our Windows Virtual Machine to be able to tackle the Cyber Kill Chain stages: Reconnaissance, Delivery, C2 and Actions on Objectives as described in the Design Specification stage.

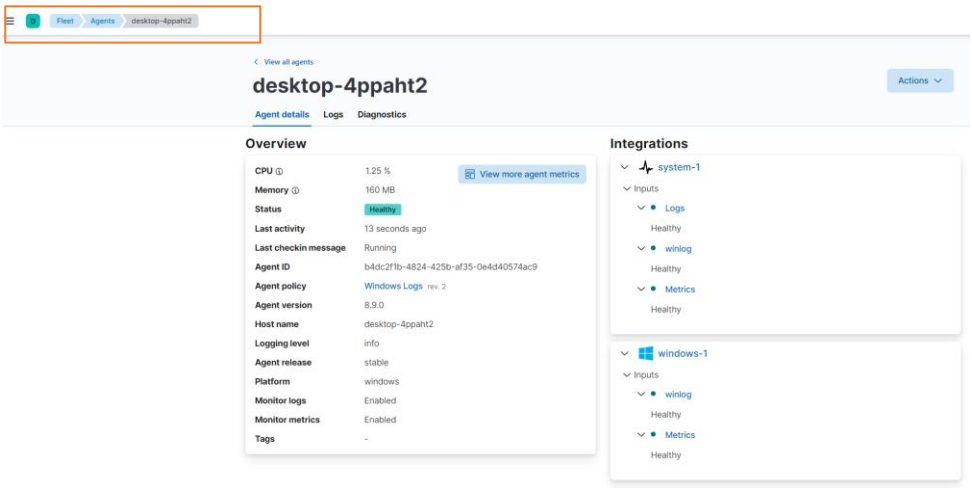
We have logged into the ELK stack. Now, lets verify if the Windows Agent is added and alive by visiting: Management > Fleet > Agents



As we can see, that the Windows system “desktop-4ppaht2” is being monitored through the SIEM using an agent policy that was configured “Windows Logs”

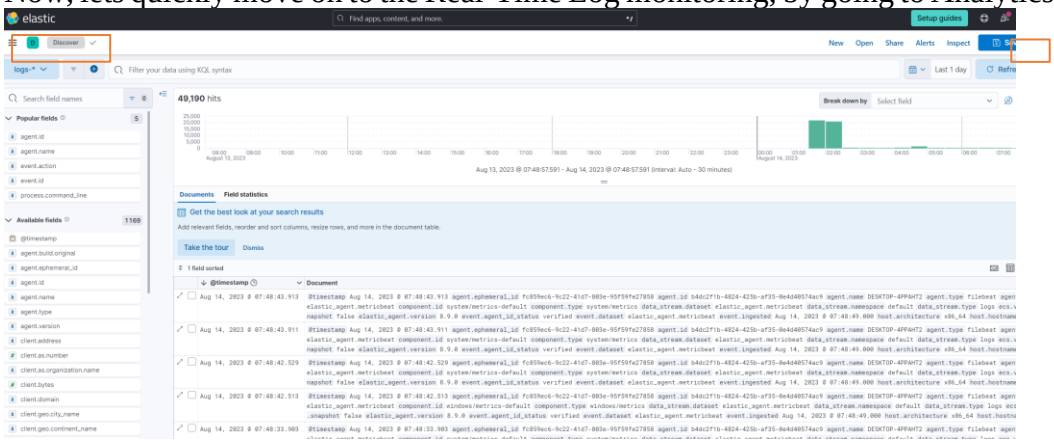


We can verify the agent policy, it is actively pulling and collecting events from Windows event log channels such as Powershell, Forwarded and most importantly **Sysmon Operational.** We are interested in reading the Sysmon logs because when windows event logs are collected by any SIEM, they are not so easy to read. Sysmon provides a much better and easier way to read the logs through this tool.

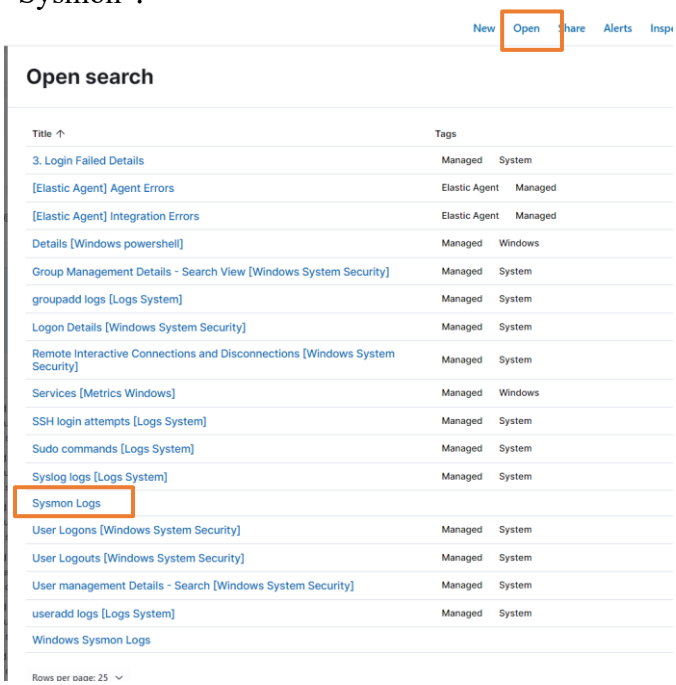


Once, we enter the Agent Details we can see further details of the Agent related to our Windows VM.

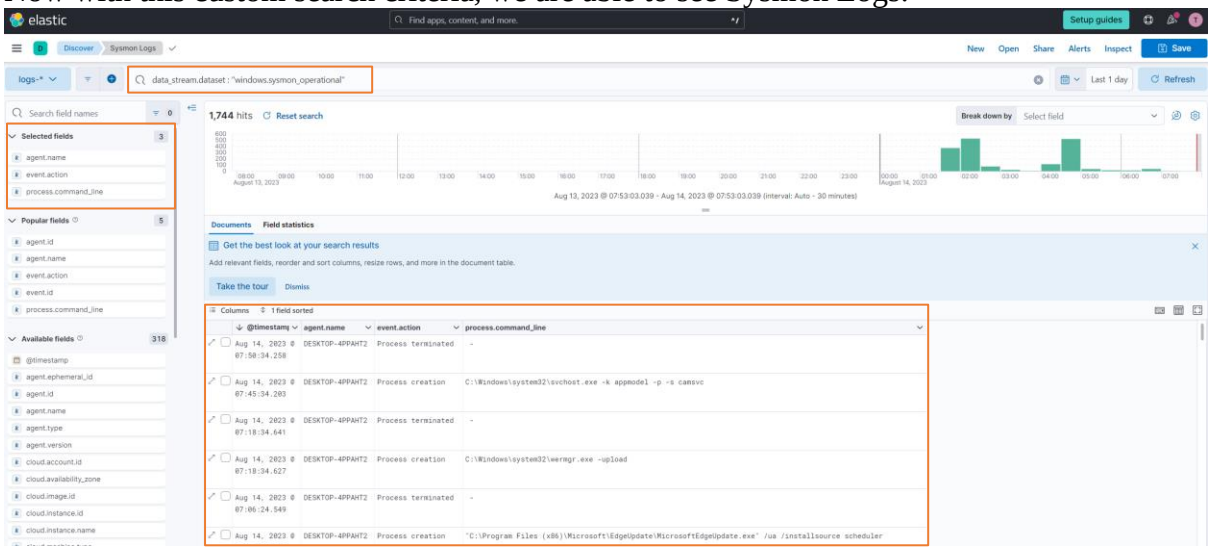
Now, lets quickly move on to the Real-Time Log monitoring, by going to Analytics > Discover.



Here, we are able to see some logs with timestamps, but they are hard to read. Thus, I have created a search template that can be used to view just the Sysmon logs with only relevant search fields.
Once we click “Open” and scroll down, we will be able to see a search template called “Sysmon”.



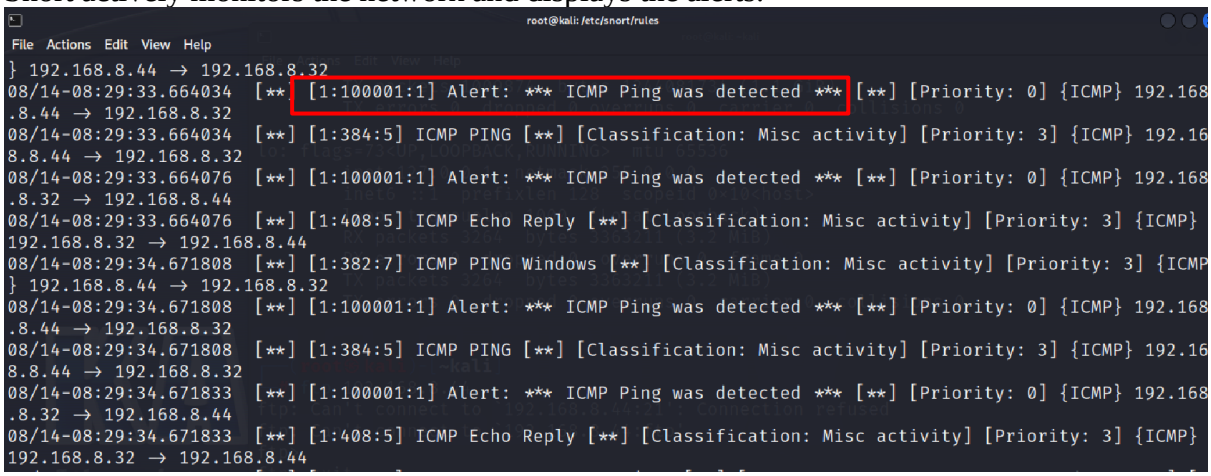
Now with this custom search criteria, we are able to see Sysmon Logs.



2. Snort Implementation – *(Roesch and Cisco, 2013)*
Snort is installed on the Linux virtual machine which can be used to actively monitor network traffic. Let’s try to send some ICMP packets and verify if they are being captured in the Snort.
Snort alerts can be started using this command: sudo snort -q -l /var/log/snort -i eth0 -A console -c /etc/snort/snort.conf
We have sent some pings inside the network:

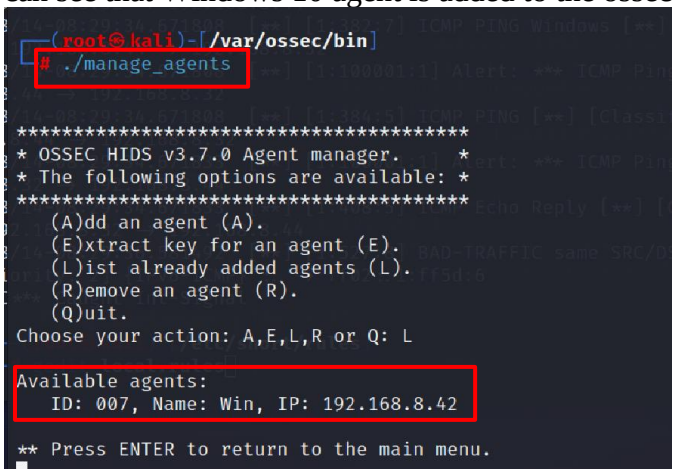
```
^C
C:\Windows\system32>ping 192.168.8.32

Pinging 192.168.8.32 with 32 bytes of data:
Reply from 192.168.8.32: bytes=32 time<1ms TTL=64
Reply from 192.168.8.32: bytes=32 time<1ms TTL=64
Reply from 192.168.8.32: bytes=32 time<1ms TTL=64
Reply from 192.168.8.32: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.8.32:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\system32>_
```

Snort actively monitors the network and displays the alerts:



The snort rule file inside: /etc/snort/rules/local.rules file can be edited to monitor and alert the activities on the network traffic. A file with thousands of rules is also present inside the "snort3-community-rules" folder from which rules can be simply copied into local.rules file and even altered as per your needs. (Talos Detectio Team, n.d.)

3. OSSEC Implementation – OSSEC is installed and present inside the "/var/ossec" folder. When you go inside the "/var/ossec/bin" folder and run the ./manage_agents command, you can see that Windows 10 agent is added to the ossec service.



We can also see that the agent is active by going into: "sudo /var/ossec/bin/agent_control -lc"

```
┌──(root㉿kali)-[/var/ossec/bin]
└─# sudo /var/ossec/bin/agent_control -lc

OSSEC HIDS agent_control. List of available agents:
   ID: 000, Name: kali (server), IP: 127.0.0.1, Active/Local
   ID: 008, Name: Win10, IP: 192.168.8.44, Active
```

We can also see that OSSEC is configured to perform file integrity checks.

Below configuration file of OSSEC agent shows that OSSEC is configured to monitor windows event logs: *(www.ossec.net, n.d.)*

ossec - Notepad

File Edit Format View Help

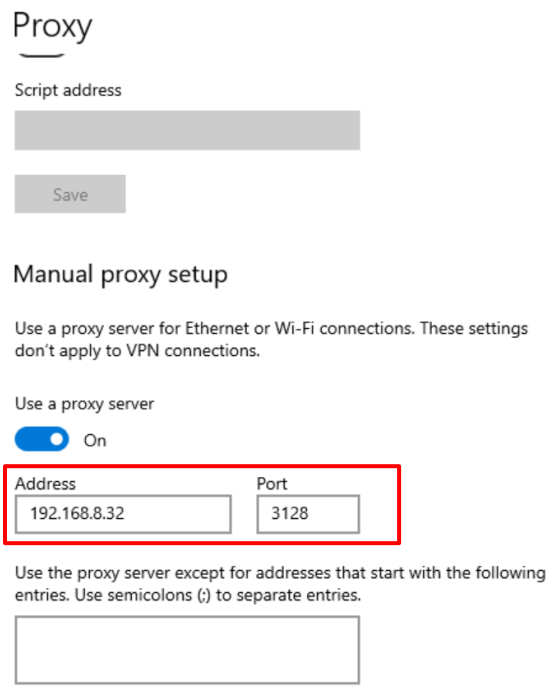
```
  -->

<ossec_config>

  <!-- One entry for each file/Event log to monitor. -->
  <localfile>
    <location>Application</location>
    <log_format>eventlog</log_format>
  </localfile>

  <localfile>
    <location>Security</location>
    <log_format>eventlog</log_format>
  </localfile>

  <localfile>
    <location>System</location>
    <log_format>eventlog</log_format>
  </localfile>

  <localfile>
    <location>Windows PowerShell</location>
    <log_format>eventlog</log_format>
  </localfile>
```

And OSSEC is also configured to scan for file integrity changes every 1 hour:

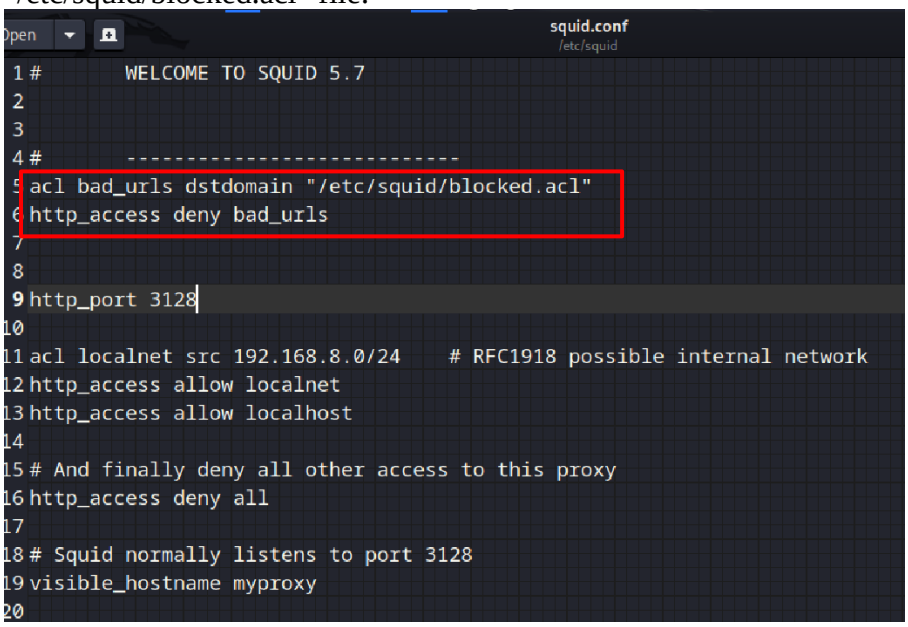
```
 <!-- Syscheck - Integrity Checking config. -->
<syscheck>

  <!-- Default frequency, every 20 hours. It doesn't need to be higher
    -  on most systems and one a day should be enough.
    -->
  <frequency>3600</frequency>

  <!-- By default it is disabled. In the Install you must choose
    -  to enable it.
    -->
  <disabled>no</disabled>

  <!-- Default files to be monitored - system32 only. -->
  <directories check_all="yes">%WINDIR%/win.ini</directories>
  <directories check_all="yes">%WINDIR%/system.ini</directories>
  <directories check_all="yes">C:\autoexec.bat</directories>
  <directories check_all="yes">C:\config.sys</directories>
  <directories check_all="yes">C:\boot.ini</directories>
```

4. Proxy & URL Blocking –

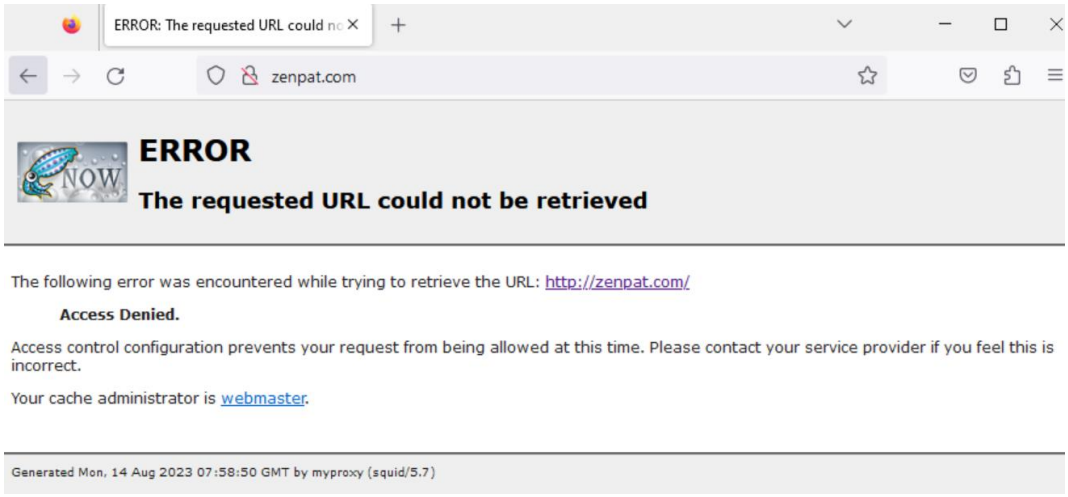
Manual Proxy is setup and it is ensured that all the data traversing from Windows 10 VM is routed through the Kali Linux VM.



Malicious URL Blocking – Malicious URLs are blocked using Squid to be able to tackle phishing attacks and avoid malicious links. "etc/squid/squid.conf" file includes the configuration of the Squid service. Here we can see malicious URLs are being blocked using "/etc/squid/blocked.acl" file.



Below is the example of the same:



5. Windows Defender and YARA – Windows system is enabled with Windows Defender in order to safeguard itself from malicious files.
We have also installed YARA on Linux to be able to detect files which include malicious signature: Below is an example of the test.
Command: yara myrules.yar "/location of files" can be used to scan files with malicious signature using the rules configured in "/yara-4.3.2/myrules.yar" file.

As we can see in the above screenshot, files with CryptoLocker hash are detected, but file with no malicious hashes "new.txt" when scanned, does not display any hash detection message.
Yara is configured to perform automatic scans every 1 hour using set of rules to detect for hash signatures configures in the rules of Yara.

Thus, the above implementation is performed to meet the Design Specification requirements mentioned in the above section in order to tackle the Cyber Kill Chain stages to atleast detect, delay or possibly break the chain during an attack.

As mentioned before, the above implemented lab is Generic and includes some of the control which satisfy the minimum requirements of the project aim as we are limited due to several constraints such as not having access to well-developed enterprise tools, Lab hosted on a single machine (laptop), time constraints, individual knowledge.

6. Evaluation

The evaluation of this thesis is based on the application of the hypothesis which falls under the implementation.

The requirements of the evaluation criteria can be the amount of security controls implemented on each stage of the Cyber Kill Chain.

1. Reconnaissance – To tackle this phase, we have implemented 1 major control that is a SIEM Tool. This stage is tackled using the ELK Stack SIEM which monitors the victim machine (Windows 10 VM) logs for any suspicious activities.

2. Weaponization – In this stage the attacker creates a weapon such as a malware or a phishing link, we have implemented Squid as proxy and performed URL blocking for known malicious websites, this will help in blocking the malicious sites and denying the phishing attack. In this phase, we have implemented 2 controls which are Windows Defender and YARA.

3. Delivery – In this stage, the attacker delivers the weapons using something like a phishing link. To tackle this phase, we have 3 effective solutions that is HIDS (OSSEC), NIDS (Snort) and SIEM (ELK Stack) to be able to block malicious link access, verify for file integrity check and verify malicious network activity.

4. Exploitation – Windows system has automatic updates enables in order to stay updated against latest vulnerabilities, thus patching is taken care of.

5. Installation – HIDS and ELK stack, 2 solutions are effective against this stage. OSSEC and SIEM will actively scan for any integrity changes of critical files. The principle of least privilege can also be used where the user of the system will not have rights to install any unauthorized software.

6. Command and Control (C2) – Snort can be used to continually monitor the network for any suspicious activity or communication to and from the victim and the attacker using SIEM and Snort. The Virtual Labs need to be segregated from the host and they should not be able to directly communicate. 3 solutions are effective against this attack stage.

7. Actions on Objective – SIEM solution can be helpful in this stage by detecting the system configuration logs for any suspicious changes. OSSEC can also be helpful in this.

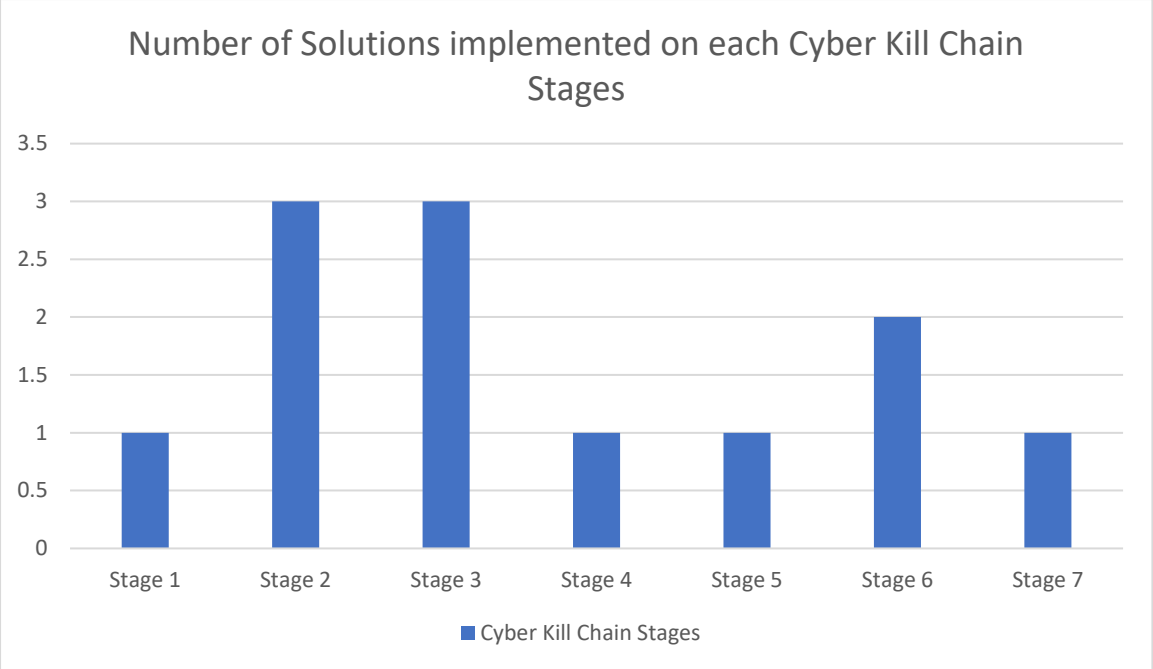


Fig 3. Number of Solutions implemented on each Cyber Kill Chain Stages

7. Conclusion & Future Work

Conclusion: We have performed in-depth analysis of how the MITRE ATT&CK describes techniques and tactics which are commonly followed by adversaries. MITRE ATT&CK knowledge base consists of multiple stages in which attack types are divided. Each attack type has a mitigation which is already defined by the framework. But, to tackle these attack techniques or stages of MITRE we have used a sophisticated defensive framework that is CIS v8 controls which is a community driven set of security control which anyone can study and incorporate in their organization for improving their security posture.
We have taken the controls provided by CIS v8 and mapped them against the MITRE ATT&CK stages in order to understand a sophisticated mitigation which is inspired from a well-reputed cybersecurity framework, such as CIS. We have performed analysis on how we could use the mitigations suggested by CIS v8 and implement them in a lab environment, consisting of a Linux and a Windows virtual machine and be table to tackle the cyber kill chain stages using one or more security solutions.
For the practical implementation, we have implemented SIEM (ELK Stack), NIDS (Snort), HIDS (OSSEC), Malware Detection (YARA), Proxy (Squid), URL filtering. Using these solution, we have implemented one or more than one way to tackle the cyber kill chain stages.

Limitations: Although not the hypothesis, but the implementation of this project was limited due to multiple constraints such as not having access to enterprise grade tools which could have improved the implementation and would have been better effective in real time, lack of infrastructure: this project faced a significant lack of hardware and software resources as it was developed on a single host (laptop) and I was forced to use free/open-source solutions which require a lot of expert configuration to be called as enterprise grade.

Future Work: This thesis can be further improved upon by performing additional analysis on how to implement better tweaked and more fine-tuned security solutions to be able to handle

the cyber attacks. Further study can be done on implementing even more solutions provided by CIS v8 Controls to improve the quality of the thesis and the lab.

References

Bashofi, I. and Salman, M. (2022). *Cybersecurity Maturity Assessment Design Using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002*. [online] IEEE Xplore. doi:https://doi.org/10.1109/CyberneticsCom55287.2022.9865640.

Cid, D., Hay, A. and Bray, R. (2008). *OSSEC Host-Based Intrusion Detection Guide*. [online] *Google Books*. Syngress. Available at: https://books.google.ie/books?hl=en&lr=&id=h37q2q3wvcUC&oi=fnd&pg=PP1&dq=OSSEC&ots=Uc_kOQQlzZ&sig=ERYGlsPS3d8qXhkMNX2UJ66JS2A&redir_esc=y#v=onepage&q=OSSEC&f=false [Accessed 14 Aug. 2023].

González-Granadillo, G., González-Zarzosa, S. and Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*, 21(14), p.4759. doi:https://doi.org/10.3390/s21144759.

Groš, S. (2021). *A Critical View on CIS Controls*. [online] IEEE Xplore. doi:https://doi.org/10.23919/Con%E2%84%A152528.2021.9495982.

ISO (2022). *ISO/IEC 27001 standard – information security management systems*. [online] ISO. Available at: https://www.iso.org/standard/27001.

MITRE (2023). *MITRE ATT&CK™*. [online] Mitre.org. Available at: https://attack.mitre.org/.

National Institute of Standards and Technology (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. *Framework for Improving Critical Infrastructure Cybersecurity*, [online] 1.1(1.1). doi:https://doi.org/10.6028/nist.cswp.04162018.

Roesch, M. (1999). *Snort -Lightweight Intrusion Detection for Networks*. [online] Available at: https://www.usenix.org/legacy/publications/library/proceedings/lisa99/full_papers/roesch/roesch.pdf.

Roesch, M. and Cisco (2013). *SNORT Users Manual 2.9.15*. [online] Amazonaws.com. Available at: http://manual-snort-org.s3-website-us-east-1.amazonaws.com/.

Saurabh Chhajed (2015). *Learning ELK Stack*. Packt Publishing.

Si, Q., Xu, H., Tong, Y., Zhou, Y., Liang, J., Cui, L. and Hao, Z. (2022). Malware Detection Using Automated Generation of Yara Rules on Dynamic Features. *Science of Cyber Security*, pp.315–330. doi:https://doi.org/10.1007/978-3-031-17551-0_21.

Strand, J. (2022). *IntroLabs*. [online] GitHub. Available at: https://github.com/strandjs/IntroLabs/blob/master/IntroClassFiles/Tools/IntroClass/md/elk_in_the_cloud.md.

Strom, B., Applebaum, A., Miller, D., Nickels, K., Pennington, A. and Thomas, C. (2018). *MITRE ATT&CK®: Design and Philosophy*. [online] Available at: https://www.mitre.org/sites/default/files/2021-11/prs-19-01075-28-mitre-attack-design-and-philosophy.pdf.

Talos Detectio Team, C. (n.d.). *Snort 3 Rule Writing Guide - Snort 3 Rule Writing Guide*. [online] docs.snort.org. Available at: https://docs.snort.org/.

Tarnowski, I. (n.d.). *How to use cyber kill chain model to build cybersecurity?* [online] Available at: https://tnc17.geant.org/getfile/tnc17_paper_TNC17-IreneuszTarnowski-HowToUseCyberKillChainModelToBuildCybersecurity_-En.pdf.

www.ossec.net. (n.d.). *Centralized agent configuration — OSSEC*. [online] Available at: https://www.ossec.net/docs/docs/manual/agent/agent-configuration.html.

www.proquest.com. (2018). *Implementing Cis Critical Security Controls for Organizations on a Low-Budget - ProQuest*. [online] Available at: https://www.proquest.com/openview/35c1afabcb51e016995318e859762f96/1?pq-origsite=gscholar&cbl=18750&diss=y.

Yadav, T. and Rao, A.M. (2015). Technical Aspects of Cyber Kill Chain. *Communications in Computer and Information Science*, pp.438–452. doi:https://doi.org/10.1007/978-3-319-22915-7_40.