LEVERAGING USERS TO BREAK CYBER KILL CHAIN

UNIVERSITY OF TURKU
Department of Future Technologies
Master of Science in Technology Thesis
Security of Networked Systems
December 2019
Charles Kokofi

Supervisors:
Seppo Virtanen
Antti Hakkala

UNIVERSITY OF TURKU
Department of Future Technologies

CHARLES KOFI KOKOFI: Leveraging users to break cyber kill chain

Master of Science in Technology Thesis, 55 p., 6 app. p.
Networked Systems Security
January 2020

Cyber kill chain defined the chronological strategies that attackers follow in invading information system with the hope of reducing the exponential increase in attacks by equipping organizations and technological stakeholders to revise and build a resilient defensive strategy capable of identifying and preventing attack.

Considering how well resourced these attackers, using complicated tools and techniques such as customised attacker vectors and weapons capable of subverting any system or network calls for a counter-productive strategy such as attack surface reduction.

Breaking the cyber kill chain using attack surface reduction involve limiting the success of an attacker at every stage of the cyber kill chain. Attack surface reduction involves controlling user behaviours, use of efficient and robust technologies and implementation of a resilient attack defence model.

Leveraging the cyber kill chain would be released through evaluation and analysis of technologies, defense models to determine the efficiency and robustness, review of related literatures and implementation strategies capable of subverting the success of an attacker.

Keywords: Hacking, cyber kill chain, attack vectors, defense model, perimeter defense, defense in depth, defense in breadth, attack surface reduction

Table of Contents

Abbreviations and Acronyms

ABI	Application Binary Interface
ACL	Access Control List
AES	Advanced Encryption Standard
APT	Advanced Persistent Attack
AV	Anti-Virus
CSRF	Cross-Site Request Forgery
CVE	Common Vulnerability and Exposure
DAC	Discretional Access Control
DBMS	Database Management Software
DES	Data Encryption Standard
DMZ	Demilitarized Zone
DNS	Domain Name Service
DOS	Denial of Service
DSA	Digital Signature Algorithm
ECC	Elliptic-Curve Cryptography
ENISA	European Network and Information Security Agency
FTP	File Transfer Protocol
HIDS	Host-Based Intrusion Detection System
HTTPS	Hypertext Transfer Protocol Secure
IDEA	International Data Encryption Algorithm

IDS	Intrusion Detection System
ISA	Instruction Set Architecture
ISO	International Standard Organization
MAC	Mandatory Access Control
MIT	Massachusetts Institute of Technology
MITM	Man-in-the -Middle Attack
NCSC	National Cyber Security Center
OSI	Open System Interconnectivity
OSNIT	Open Source Intelligence Technique
OWASP	Open Web Application Security Project
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
POP3	Post Office Protocol Version 3
RAT	Remote Access Toolkit
RBAC	Role-Based Access Control
RSA	Rivest-Shamir-Adleman
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol

URL	Universal Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WMD	Weapon of Mass Disruption
WWW	World Wide Web
XSS	Cross Site Scripting
ZED	Zed Attack Proxy

1.Introduction

According to Julian and Surya (2014), the exponential growth of the internet has led to significant cyber-attack incidents with disastrous and grievous consequences such as theft of confidential data as well as personal identity, denial of service, closure of upcoming industries, data breaches and leakages and cyber espionage.

In spite of the attack model introduced by Lockheed et al. in 2011 to exposed hackers' chain of operations, with the hope of affording users the hacker's mindset, technological industries have seen an unprecedented upsurge in attacks over the years resulting in poised accelerated cyber spending of 81 billion 2016, 101 billion 2018 and estimated over 1 trillion 2019 according to Gartner Inc and Symantec report indicate 56% increase in attack, 4800 monthly compromised websites, 3.7million unsuccessful host attacks.

The increase in attack can be attributed to the ever-changing attack vectors coupling the dormant attitude of users towards security. The use of email vector increases by 48%, PowerShell increase by 100%, supply chain 78% and user online participation increase by 100% resulting in significant digital footprint due to introduction of smart home, IOT devices and social networks. A practical example of vector complexity and dynamism is Stuxnet and drone attack on Iran nuclear plant and Saudi-Arabia oil industry respectively.

According to NIST Information Security and Privacy Advisory Board Chairman Dan Chenok, it requires one to turn off his computers to remain protected from attack. This implies cyber-attacks are inevitable and requires a counter-productive measures to protect, detect and monitors one's system.

Designing counter-productive defense requires both explorative and exploitative mindset of a hacker. These attributes afford users in-depth understanding of hacker's chain of operation and choice of technologies and behavior controls that will aid in attack surface reduction. This is what this thesis intends to address by facilitating users understanding of the cyber kill chain and methodologies that could be leveraged to reduce attack surface.

1.1 Statement of purpose

Ever since the introduction of cyber kill chain, different attack prevention defense models emerged but no single one of them prove to be efficient and robust enough to withstand any penetration attack and theft of sensitive information. This is as result of inadequate understanding of the various stages of the cyber kill chain leading to wrong choice of defense models and technologies to implement as well as uncontrolled user behavior towards security.

1.2 Objectives

The main objective of this thesis is to help users build an in-depth understanding of the seven stages of the cyber kill chain thoroughly, available defence models and methodologies that will aid in reducing the attack surface by limiting the stage-by-stage progress of the attacker and thereby breaking the kill chain

1.3 Thesis Structure

This thesis is structured into 7 chapters with chapter 1been introduction. The introduction chapter talks about the problem statement, the thesis objective as well as the thesis organization. Chapter 2 & 3 is about reviews of related literatures and theories.

Chapter 4 explains the existing system that is the cyber kill chain seven stages and technologies and behaviours that can be leveraged to reduce the attack surfaces in each stage.

Chapter 5 talks about the attack surface reduction methodologies whiles chapter 6 is about thesis conclusion and chapter 7 ends the thesis with references.

2. Introduction to Hacking

The critical role of information security such as availability, confidentiality, data integrity and non- repudiation of information has been downplayed by hackers resulting in an unprecedented increase in attacks in recent times. Julian and Surya (2014), the exponential growth of the internet has led to significant cyber-attack incidents with disastrous and grievous consequences.

The internet growth and advancement in technology contributed to changing threat landscape hence changing attack vectors and some limitations in the existing defense model which hackers have taken advantage of to launch attacks in spite of complex firewalls, network monitoring tool and antivirus.

2.1 Hacking

The advent of technology and for that matter internet has impacted humanity in terms of business, production, manufacturing, socialization, collaborative computing, and information distribution as well as information storage. It has transcended geographical borders forming cyber-network. As complexities began to grow, coupling the broad participation and patronage of computer systems and the Internet as a whole, some level of curiosity among experts emerged causing paradigm shift from positivity to negativity. This poses a threat such as theft of information, denial of services, invasion of privacy, identity theft and others. This deviant art is woefully associated with the term “hacking” by the media and has become the hottest topic in the media.

According to Ajinkya A. Farsole et al. (2010) hacking is considered the rapid crafting of programs, effecting changes to existing complicated software aiming to have unrestricted access to run applications of a choice. Deepak Kumar et al. (2015) define hacking as a process that involves controlling an organization’s information system to acquires sensitive and confidential information. Dr. Rasmi and Satapathy (2010) augmented Ajinka and Deepak by defining hacking as the art of modifying certain features of a system, and the one who does this is called a hacker.

John Erickson (2011) also explained that the idea of hacking conjures stylized images of electronic vandalism, espionage that are associated with breaking the law whiles hacking is about following the law. This assertion explains the fact that hacking have both negative and positive impact on the society.

2.2 Hacking Timeline

Hacking time define the significant hacking events from the inception of telegraph breach to the formation of groups fighting for freedom of information till date. One could consider this to be fine-tuned of events that runs through the ages.

1958-1960s :Code Maximization

According to Steven Levy (2010) the MIT railroad club adopted the term "hacking" when members of the club hacked their train sets and modified its working. This clever art resulted in technological curiosity and resourcefulness among club members to innovate, improve and gets old devices that are not working to function.

Program bumming was introduced (the art of reducing code length to perform the same function) also known as maximizing code. This led to most elegant hack , the UNIX operating system from Bell’s lab by Dennis Ritchie and Ken Thompson.

1970 - 1979 :Phreaking

During this era, the technological curiosity was directed towards telephone systems. The exploitation and discovery of inner workings of the telephone switching network was realized by John Draper a veteran. This afford him the ability to make long distance calls for free. This became a movement known as phreakers.

According to Zuley (2003) et al. this movement is an example of anti-establishment subculture. John Draper later built the blue box which facilitated a lot of fraudulent phone call activities. Steve job the co-founder of Apple Inc and Wozniak Steve also makes good utilization of the blue box.

1980 – 1990s :Computer Revolution

Hacking saw an unprecedented increase as a result of the introduction of personal computers by IMB. This led to the introduction of War game which revealed the inner workings of a hacker.

During this time the art of deception is at its pick due to formation of gangs. The inception of 414 gangs, legion of doom and masters of deception. Cybercrime is becoming popular such that the government of America started to punished perpetrators through the enactment of computer fraud and Abuse act.

It is also during this time the world realized hacking could take any form. Robert Morris launches the first Internet worm. Kevin Mitnick a famous hacker now a security consultant was convicted for unauthorized access to federal computers. Other attacks include the Pentagon, FBI websites and Citibank fraud by Vladimir Levin.

2000 -2009: Cyber-Crime Evolution

The upsurge of cybercrime during this era was alarming as electronic commerce is on the rise. In fact, this era registered the most damaging crime ever in the history of cybercrime. This era saw the upsurge of some disastrous virus such as conficker (infiltrate million machine) and "I love you " virus created by Reonel Ramones that sucks the global economy of USD 9 billion from the Philippines.

This period also saw the growth of attacks such as defacing campaign, theft and cracking resulting in massive DOS (denial of service) carried out by script kiddies, carders and the beginning of cyberespionage by a hacker group known as TITAN RAIN (Chinese cyberspies) which specialized in stealing of government information.

2010-2019

The formation of hacktivist LulzSec and Anonymous combine forces to reveal corruption that is ongoing in governments, top industries and banking sector by leaking documents to that effect and 400,000 credit card publication by OxOmar a 19-year student from Israel.

Currently theft of emails and password (65469298 from Tumblr), Bangladesh bank heist ($951million) account details, banks, the WikiLeaks attack, new viruses (WannaCry, Mirai, Ryuk) and the surge of APT attack and recent exploitation of security flaw in TLS-code that impacted 5 million servers.

2.3 Classification of Hackers

According to Kimberly Grave (2007), there are 3 main division of hackers namely white hats, black hats and grey hats. Hackers are also referred to us ethical or unethical hackers based on manner of behavior and motivations.

Talking about motivation, Ryan and Deci (2000) think that some hackers do what they do for the purpose of intrinsic motivation. This motivation is driven by recognition, advancement, achievement, having fun and fulfilling an inherent satisfaction. This, therefore, make hackers selfish and careless about the consequences of their actions on victims.

Again, Grabosky and Peter (2001) argue that there are some who think the life of crime and value for financial rewards are hard to turn down, therefore, sticks to their beliefs and commit crime all the time. This is considered extrinsic motivation. Extrinsic motivated hackers' hacks for financial reward.

Nevertheless, Sterling (1993) mentioned that hackers are not only motivated by extrinsic and intrinsic gains instead some reasons accounted for their activities such as gaining publicity, to protest and also to challenge one's capability. Considering these motivations that determine the intent of a hacker, hackers can be classified as white, grey and black hackers respectively.

White hat hackers are defined by Kimberly Grave (2007) as good guys and ethical because the intention for their activities is benevolent. This group of hackers render protective services by protecting and testing systems for weaknesses or vulnerabilities and helping organizations to mitigate those vulnerabilities. white hackers provide organizations with realistic attack simulation that enhance security through early discovery and mitigation Engebretson (2011), augmented Kimberly's assertion.

According to Chiesa et al. (2008), black hackers acts are backed by criminal intents and lack any element of "love for hacking." Engebretson (2011) mentioned that black hackers hack information system for the extrinsic purpose. Kimberly grave (2007) summed it up by defining black hackers as bad guys, malicious in natures and who use their skills set for illegal purpose.

Grey hat hackers are the type of hackers whose acts and intentions can be both benevolent and malevolent. They play a dual role and have the capability of protecting, discovering vulnerability, mitigation and also breaking into the systems. S. Tulasi (2014) augmented this explanation by defining grey hat hackers as hackers who may work offensively and defensively based on confronting situations.

2.4 Hacking Techniques

According to John Mariotti, we worried for decades about WMD (Weapons of mass destruction), Now it's time to worry about a new WMD (Weapons of mass disruption)

2.4.1 Social Engineering

Mike Chapple and David Seidl (2014) defined social engineering as the art of manipulating human behavior through social influence tactics in order to achieve a desired behavior.
Christopher Hadnagy (2011) considered social engineering as the manipulative act that persuades people into taking action that may or may not be in the targets best interest. Kevin Mitchnick (2002) coined social engineering as getting people to do things they wouldn't ordinarily do for a stranger and get paid for it.

Social engineering is therefore the use of psychological weapon of influence techniques by hackers to take advantage of human relations, users' inattention, emotions to elicit vital information without them knowing.

According to Mike Chapple and David Seidl, the three main social engineering tools include pretexting, phishing and baiting.

Pretexting involve creating false sets of circumstances to convince a target to take an action. For this to be true enough, the social engineer assumes an identity of authority. Pretexting includes phone calls, text messages and email messages. Pretexting make use of shoulder surfing, dumpster driving to gather information.

Phishing is now the most prevalent means of stealing information. The user is tricked into clicking a malicious URL or opening an email with attachment which either launches a background RAT(malware giving the attacker a remote access to victims device), redirects user to an infected sites or in the worst scenario users data and equipment get encrypted, and fee is required in exchange for decryption key or code.

Baiting is when an attacker craftly attach malicious codes to flash drives or CD-ROM and leave it in a place such as parking lot, lobby, in the target car or in an open area that the target can pot it. Baiting could also be achieved through tailgating.

2.4.2 Bait and Switch

It is deceptive and diversionary techniques employed by hackers to embed malicious programs in marketing content such as adverts. Hackers hide in marketing content malicious programs so that when a user clicks, download or mouseover these adverts programs, the hidden content get downloaded and installed onto the users' device. These hidden programs redirect users to a malicious website. This advertising links many often are bought and owned by hackers for this purpose. Bait and switch are known for publications of unrelated topics on popular sites.

2.4.3 SQL Injection

According to OWASP (Open Web Application Security Project), SQL injection involves the insertion and injection of SQL statements via the input data-plane to the web application. The SQL statement has the capability of reading, modifying, executing database and operating system contents and operations.

In Lau, S. etc. (2007) classification of SQL injection attack indicates that SQL injection is an exploitation method of using string input to have unauthorized access to a database by shafting the DBMS into running harmful codes.

With regard to both explanations, one could deduce that SQL injection is a form of attack that manipulates the DBMS into revealing confidential information using harmful SQL statements such as “OR 1=1”, “=,”. Considering hacker injecting or 1=1, logic proves that the statement is true. Therefore, the content of the table or database will be displayed. Should this table have other columns such as names, addresses, social security numbers, credit card information, the hacker now has access to sensitive information.

2.4.4 Fake Access Point

Access Point (AP) is a wireless accessing hardware device that enables devices without an inbuilt-wireless interface to have a wireless network. It also facilitates wireless network sharing at home or the offices. Access points come in USB form and also mostly built into routers. Hackers use this access point to lure users into connecting to free wireless. Fake AP enables hackers to hack into connected devices. Again, employees also use this access point on company’s network to share wireless network at the office without pass wording it known as rogue access point. Hackers use this rogue access point to hack into the company’s system stealing and causing a denial of service attack.

2.5 Hacking Motivations

The individuals who are taking the path of hacking are motivated by a series of reasons convincing enough to do so. The famous one-time hacker now a consultant Kevin Mitnick was driven by curiosity, pursuits of knowledge and seduction of adventure whiles Emanuel Goldstein was driven by seeking knowledge, discovering new things and been the first to identify weaknesses in systems.

Levy S. (1984) argues in his thesis that many hackers wish to make cyberspace and information sharing non-monopolistic and free of control from governments and other cooperation. Taylor and Jordan (1998) identified thrill for information, addiction, peer recognition among others.

A thoughtful analysis of the mentioned drives reveals the primary reasons for attacking and stripping information and its resources of its objectivity of confidentiality, availability, and integrity are too complex to unearth.

Nevertheless, Eric Maiwald (2003) categorized hacking motivation into three groups namely greed, challenge and intention(malevolent). Attack drives are limitless based on different schools of thought. One of such is Donald L. Pipkin (2002). Pipkin argued that hackers are driven by experiment, fun, stalking, ego, anger, political, social, cyber terrorism and warfare

Hacking motives are also fuel by nationalism and patriotism Denning (1999). Considering the above-mentioned motives, it is clear hacking drives transcends cultural, ethnicity, religious boundaries. This is augmented by Woo et al. (2000) research findings established 20% of defaced attacks are as a result of religion, ethnicity, and nationalism.

One common motivation that account for many attacks identified by many scholars is Ego. Many hackers possess high ego and always desires to show off their cyber smartness and make information organization to feel their technical prowess. This is often seen in disgruntle, unemployed and sacked employees. This assertion is augmented by Woo et al. (2000); many hackers leave traces as to why they attack an organization. This comes in the form of after hacking statement, notes or remarks. Below are some discussions on motivations that hackers considered their driving force.

2.5.1 Curiosity

Curiosity is a force that makes young learners to experiment and discover the impossible. Curious people are never satisfied with the amount of information they have acquired. They desire to be ahead of every other person. Hacker’s curiosity to know everything about information systems results in playing cat and mouse games with software, hardware, infrastructures, and users leading to getting accustomed to the exploitable vulnerabilities in these resources. Curiosity is not malevolent intent just as Kevin Mitnick put it. It is about seeking and acquiring new knowledge. According to Ryan Russell (2000), the fact that the hacking concept goes beyond information systems is an indication of curiosity. Ryan made an analogy using a hacker learning how door locks works and how to bypass it to impress his friends illustrates the extent of curiosity.

2.5.2 Rewards

Opposed to gaining new knowledge is gaining rewards be it financial, material or satisfaction. Rewards motivate some famous hackers to come to the spotlight of the world and security sector. Kevin Poulsen infiltrates to win a radio contest for Porsche rewards. Astra, a Greek mathematician, hacks France's Dassault Group and sell the information for financial reward. Parker (1998) argues that information and its resources are valuable assets because these are the bedrock of financial and production sectors.

2.5.3 Recognition or Publicity

A growing development that the media has labeled celebrity has become a driving force for committing crimes on information systems. Hackers want to gain fame in the technological industry as well as the cooperate world in the likes of Kevin Mitchnick, Albert Gonzales, LulzSec and other groups like Anonymous. Ryan Russell (2000) explained the hunger for fame has compelled many hackers to become a crime or advisory authors. Ryan went on by saying fame comes with financial rewards because public exposure will make security companies hire you. This compelled hackers to draw fame.

2.6 Hacking Laws

According to ITU, hacking laws are also known as cybercrime laws. These laws cover a variety of criminal conduct such as offences against confidentiality, availability, integrity of data and systems. Rhode Mark Ousley explained that hacking laws protect systems and network intrusion that results into fraud, theft, abuse, damage to data and systems. The most common hacking laws aside country by country cybercrime laws include Computer Fraud and Abuse law (CFAA), Electronic Communication Privacy Act (ECPA) and General Data Protection Regulation 2016/679 (GDPR)

2.6.1 Computer Fraud and Abuse Law (CFAA)

Computer Fraud and Abuse Law (CFAA), This is one of the oldest and most recognized hacking laws that emanated from the United State of America section 1030. The essence of CFAA is to protect confidentiality, integrity and availability of data and systems. CFAA prohibit and deal with unauthorized access to information systems that inflicts some damage such as denial of service, malware and other security threats. The main criminal conduct CFAA prohibit include unauthorized access and damage. These two conducts are central to all other criminal violation of information systems.

According to CFAA explanation of unauthorized access to systems and data could be view from two different spectrum. The first is access without authorization where an outsider breaks into a system without permission. The second is excess authorization where an authorized person elevate the permission and is able to have access to restricted data or systems.

Damage is any impairment to data integrity, programs, systems or information. Damage to data or system involves loss of data, program modification, physical injury or a threat to public safety. The Stuxnet attack on Iranian nuclear power as well as recent drone attack on south Arabia oil company are practical example of attack damage.

2.6.2 Electronic Communication Privacy Act (ECPA)

ECPA protect systems and networks against traffic (emails, keystrokes, message) interception, disclosure and retrieval either in transit or not in transit. ECPA is a federal statute that ensures communication remains confidential and the traffic integrity remains intact. ECPA revolve around two main concepts and understanding of these concepts aids an organization in determination when they fall a victim.

First is the interception also known as eavesdropping. ECPA prohibit wiretapping. Wiretapping involves real-time interception of traffics whiles in transit using versatile tools such as packet sniffers and keystrokes recorders. This intentional act is illegal, unlawful and perpetrators of such act are in violation of ECPA law section 2511(a) and are subject to severe and deterrent punishment.

Again, ECPA does not only prohibit interception but also disclosure of electronic stored information. Information accessed on server also violate ECPA law section 2701. Stored communication could be access through unauthorized means or by excess authorization. Any of this is in violation of ECPA.

Never the less, the ECPA also considers monitoring an integral practice in ensuring information security therefore permit service providers and security professionals to monitor electronic communication for the greater good of the society and their organization.

2.6.3 General Data Protection Regulation 2016/679 (GDPR)

GDPR also refer to as privacy compliance policy has been enacted and approved by the European parliament on 14th April 2016 and enforced 25th May 2018. The primary objective of GDPR is to ensure the privacy of all European citizens as well as protect them against data breaches considering the upsurge in attack in this data-driven era. GDPR protects the data subject right by defining compliance practices that data controller or processor must adhere to. Violation of these compliance practices will results penalties and sanctions.

GDPR data subjects' rights includes breach notification, right to access, right to be forgotten, right to portability. Violation of any these rights might result in 4% annual turnover fine.

The scope of GDPR includes all companies that process personal data and are residing in European union regardless of their location. Organizations outside the EU that process EU citizens information must also oblige by the law through representative appointment.

2.7 Hacking Tools

The daily advent of new complicated hacking tools makes hacking a challenge to combat with. This possess a great threat to many organizations who especially suffered some level of intrusion in the past or do not have proper protection mechanisms in place. Some of the hacking tools include

- Debuggers are tools deign to aid developers in auditing their codes and also identify any problem in the code. Attackers use the same tool to identify exploitable bugs that exist in applications. These tools enable attackers to crack software in order to evade inbuilt protection mechanism such as copy right, digital right management and also to embed malware into them. Examples includes GNU Project Debugger, IDA Pro, Immunity

- Vulnerability and Port Scanners are tools that specify the concise state analysis of a system, network and a device. It enlists all possible flaws or weakness in a system.

These flaws include open ports, misconfigurations, missing patches, default password, open Wi-Fi. Examples of tools that detect system flaws includes
Nmap, Unicorn Scan, Angry IP Scanner, Nexus, BeEf, Metasploit, Dradis

- Password Cracker tools aid identification and disclosure of password through dictionary or brute force attack. Success of password cracking depends on the how secure is the to be cracked system and the processing power of the attacker. Most popular tools include Air Crack, Hydra, Crowbar, John the ripper. Air Crack use most used on wireless devices and it also has an inbuilt packet sniffer.

- Packet Sniffer are powerful tools that is used in stealing sensitive information. It is most used in man-in-the-middle attack. These tools have the capability of intercepting a packet, modifying it and send it back. Examples include Scapy, DSniff, Cain and Abel, Wireshark

2.8 Attack

With reference to RFC 2828, When a security system suffers an assault through a deliberate attempt that compromises services and violates systems policies is an attack. William and Brown (2015) define attack as any action conscious enough that tries to break and evade the security and procedures of an organization. Attack therefore includes any activity of a user or from an external source that will jeopardize the integrity, confidentiality and the availability of information and information infrastructures. Attacks can be categorized as passive and active.

2.8.1 Passive Attacks

Passive attack is characterized by monitoring and eavesdropping of transmitted information. In this sort of attack, the attacker intercepts the message on transmission but do not alter its contents. In this way, it becomes hard to detect an ongoing attack. The main types of passive attacks include

Message content released, many often users transmit information deemed confidential with the hope that only the receiver will learn the content. But it is rather unfortunate; attackers employ various mechanism that enable them to intercept and determine the content of the information without the sender or the receiver knowing.

Traffic analysis, in an attempt to prevent access to sensitive information, users employ mechanisms such as encryption to encode the content of their messages so that only the intended receiver can learn the content. An attacker in this regard can determine the pattern of a transmitting traffic and based on that could guess the sort of message with the help of other mechanisms such as decoding.

Key-loggers are yet another scheme adopted by attackers. Key-loggers are background process that records every keystroke press by the user and later forward it to the attacker. The attacker then identifies username, passwords, credit card numbers, email messages, and other sensitive information out of the keystrokes recorded. Key-loggers can be considered as surveillance tool.

2.8.2 Active attacks

In contrast to passive attack, active attacks are characterized by message alteration and creation of false messages. The nature of this attack is complex and very difficult to detect as well as preventing it from occurring. The primary forms of this attack include fabrication, modification, and interruption, and these are further explained below.

Modification attack, this attack involves insertion, deletion, and alteration of transmitted information which appears to the intended user as genuine. This sort of attack results in loss of data integrity as well as confidentiality. Modification attack includes replay and man-in-the-middle attack.

Man-in-the-Middle Attack (MITM) is a sort of complex attack. It involves having access to information on transit from sender to receiver. Attackers make use of special hardware or software that intercept data streams and send it to the attacker's servers or computer where the message is modified and later forwarded to the receiver. Because the receiver cannot determine the message time to live, the delay is accepted, and this makes this attack hard to determine.

Replay attack occurs when an intruder eavesdrops a valid authentication token during transmission. Because this message contains a valid authentication key, the intruder at a later time can resend this message to the receiver. If the sender is asking the receiver to perform a transaction, it means that as many times the intruder sends this message, the receiver will perform the necessary transaction. Other types of active attack include Dos and repudiation

2.9 Threat Landscape

Computer threat has captured the limelight of the media over the century because of its impact on businesses, industries, organizations, governments as well as countries. The impact of threats can never be underestimated ranging billions of dollar losses and many often-woeful closures of some future ground-breaking industries.

According to ISO/IEC 270001, a threat is an event that has the potential to cause harm to the computing system which may result in a security breach and is capable of compromising business operations. NIST.SP.800-160, threat is an event has the potential for causing asset loss and the undesirable consequences or impact from such loss. This loss includes confidentiality, unavailability and integrity of system resources to legitimate users and denial of access.

Mark Rhodes-Ousley (2015), threat agent is any entity that cause or contribute to an accident. With regards to NIST SP 800-30 , threat agent is considered any intent and method targeted at intentional exploitation of vulnerability or situation and methods that may accidentally trigger a vulnerability.
Threat vector is used to describe where a threat originates and the path it takes to reach a target by Mark Rhodes-Ousley (2015). Every day sees new emergence of variant threats and threat vectors. According to Kaspersky Lab, 360,000 threats are detected daily whiles Symantec detects 24000 pertaining to mobile applications. These threats vary in complexity, advancement, and impact on systems.

In order to help enterprises to understand and prepared to face cyber threats, anti-virus and firewall laboratory such as Kaspersky, Symantec, Juniper, Force point and other security-oriented organizations provide an overview on current and emerging cyber threats, threat agents and attack and impact of these threats on enterprises. This is often known as the threat landscape.

2.10. Emerging and Threat Vectors

According to 2019 Data Breach Investigation Report (DBIR), no organization is too large or too small to fall victim to data breach and no matter the amount of data in an organization , somebody is planning to steal it.

According to information collected, analyzed and made available in the public domain, there are a new insurgence of threats on a daily basis example AV-TEST security report shown an exponential growth of malware recording 48 million in 2017. There are various threat reports produced by various organizations such as the FBI, open source intelligence (OSINT), ENISA, Kaspersky, Avast. The interesting side is that many of the attack methods remain the same. This section is going to explore the leading threat categories, description, trends and the vectors used in launching an attack.

2.10.1. Malware

Sikorski M Honing (2012), considered malware as any piece of software that is capable of causing harm to the detriment of the user, systems or networks. Over the year's malware has proven to be frequently and cumbersome cyber threats. McAfee laboratory recorded a 32% increase in malware in 2017. There are different types of malware attributing to the purpose and intentions of the adversary such as backdoor, botnet, downloader, root-kit, worm or virus. The August report 2018 by NCSC (National Cyber Security Centre) revealed the return of the Mirai botnet which was used in the French Telecom DDOS attack 2016. Other malware making a wave on the cyberspace include Qakbot trojan, trickbot, NotPetya, IceID, WannaCry, EternalBlue, and Emotet. The main vectors through which the infection spread include Phishing, Malvertising, Exploit Kit and spam email.

2.10.2. Denial of service (DOS)

DOS attack is a situation where an adversary denies legitimate users' access to system resources and services. This occurs when the adversary sends more traffic than the network bandwidth can handle leading to buffer overflow and eventually resulting in a system crash. Distributed denial of service (DDOS) is the pervasive variant of the DOS attack. This attack is alarming from 17% in 2016 to 33% in 2017. The DDOS variant includes APDOS (Advance persistent denial of service), SSL-base attack, PDOS (Permanent denial of service) and IOT Botnets. The main attack vectors include UDP, DNS, TCP, NTP, and HTTP. Mirai catches the world attention in Dyn attack in 2016

2.10.3. Ransomware

This threat proved to be a seamless, automated means of a profit-oriented venture, unlike normal malware. This threat is always in the limelight and has titled the headlines many often. Ransomware encrypts files, and other devices and demanded payment in a form of bitcoin for the decryption key to be released to the victim. This has taken a different dimension when the RainMaker lab introduced "Ransomware -as a-service". This gave way to variant and incessant attacks. The new trend "MED-JACK" which targets medical devices. Ransomware is on the increase this is evident when 6 in every 10 payloads detected in 2017 prove to be ransomware as well as the damage exceeding 5 billion dollars. The most dangerous as well as the wave making ransomware includes MongoLock, Gandcrab, SamSam, Ryuk

2.10.4. Crypto-mining

Cryptocurrency is a digital asset and is govern by nobody because it resides in the personal wallet and this promotes decentralization as well as anonymity. It is produced by solving complex mathematical problems refer to as Mining. This mining is energy inefficient due to the huge amount of processing power required for single mining. Due to its profit margin, hackers now integrate crypto-miners into malware. The infection is spreading and alarming such that security laboratories had detected 28 million crypto-mining malware incidents out of 300 million malwares detected and 7000 compromised crypto-mining websites. The lucrativeness of crypto-mining is facilitated by the introduction of monero (foster crypto privacy by hiding crypto accounts and transactions).

Sandiford Oliver, security researcher at Proofpoint, reiterated considering the high level of profit as well as the resilience of the botnet, it becomes difficult to control due to its potential impact and infrastructure. The new twist to this development is “crypto mining-as-Service”. Some of the abuse CVE’s include CVE-2017-01444, CVE-2017-10271

2.10.5. AI weaponization

A new paradigm in an attack in which the impact is considered to be more disastrous than any other forms of attack. Currently referred to as “new Dogs of war”. The pace of development and growth of an intelligent automation system is beyond imagination. It has cut across all boundaries and become a critical component in almost all technologies of today. Search engines, biometric applications, spam filters, drones, medical robots are examples of AI applications. These technologies have the tendencies to be maliciously exploited to become a threat to digital security, physical and political security of which there is less or no way of stopping the attack. The main AI threats identified include Surveillance and Coercion, AI weapon factory and Careless destabilization of national Security according to the threat-casting Laboratory report 2017.

2.10.6. IOT Botnet

The staggering growth of IoT devices on the Internet is amazing and is becoming the new attacking field for hackers. According to Gartner, 6.5 billion IoT devices are connected in 2016 and by 2021 20 billion devices will be on the Internet. IoT Botnet attack involves a collection of IoT devices such as wearables, cameras, watches, refrigerators, routers, embedded technologies that have been infected. These infected devices are turned into zombies and are control by the operator to achieve his/her intended purpose. It can be considered disastrous taking into consideration the large scale of interconnected devices. Examples include TheMoon, mylobot, satori botnet.

3. Attack Prevention Models

According to CISSP guide, security defense model is a statement or a graphical representation that outline the necessary requirement to support and implement a security policy. It explains, the essence of security model is to fortify, detect, react, monitor and maintain security.

Hypothetically, a security must be centered around three main elements namely people, technology and operations. Every end-to-end defense model must define the people, technology and operation aspects of ensuring confidentiality, integrity and availability of services.

Every strategic and efficient model ensures there are defined and articulate policy and procedures that ensure people do the right thing based on the training accorded them and the provision of a supportive environment that aid them in dissemination of their duties and responsibilities. An efficient model also defined how technology is design, acquired, configured , managed and maintain to enhance network security solidification. Testing and validation, updates and patching, risk assessment are some of the daily operations that are not exempted from defensive model.

Mark Rhode Ousley (2015) suggests that defending against threats on information assets requires three main famous approaches. These approaches serve as the main building blocks upon which organizations defines their security prevention model to preserve and ensure security of a systems

- Perimeter defense
- Defense in-depth approach
- Defense in breadth

3.1 Perimeter Defence

Michael J. Arata Jr (2006) defined perimeter security as a protection accorded the outer boundary of a network. He explained that perimeter defense starts at the property line and

involve the introduction of fence line such as wall, alarm systems, gates and sometime intrusion detection systems.
Mark Rhode Ousley (2015) reference perimeter security as lollipop model that involves the building of virtual or physical structures around an object of value. This object of value includes data, people, property and network resources. These objects are so important, sensitive to the organization and must be protected.

According to Ousley, perimeter security has two layers namely a hard-crunchy outer shell also known as perimeter barrier and soft chewy center that is likened to lollipop also knowns as the protected asset. This is subject to attack by a determined attacker through break-in or weakness exploitation.

Michael Arata (2006) also state that in designing perimeter security, perimeter fences, barriers and access control points are the main aspects that is considered in perimeter defense. Perimeter barriers uses CCTV cameras and sensors to enhance perimeter fences whiles access control make use of access control list, PIN, ID, biometrics, badges to enhance both perimeter fences and barriers.

Normally perimeter security creates a false sense of security due to its limitations such as

- Once the attacker breaches the perimeter, all valuable become exposed
- Perimeter security does not protect against insider threats and attack because the firewall which is the main protection mechanism control only outside access.
- Perimeter security does not enforce different levels of security protection.

Perimeter defense is a necessary requirement in securing the outer layer of a network especially when fences, barriers and access control are combinatory implemented, the outer layer become a force to battle with by invaders and attackers.

3.2 Defence-in-Depth Approach

Defense in depth unlike perimeter firewall requires a self-protection architecture of a network. Defense in depth also known as layered security is considered by Michael Arata (2006) as an all-encompassing multi-layered security approach that enforce total security by assuring confidentiality, integrity and availability of data and services. One daunting fact that network designers must take into consideration during design and adoption of defense in depth model is that all security can be compromise by those with experience and right equipment. Though in layered security, there is a possibility of one layer offering the needed protection despite the attackers' expertise.

According to Joel Synder, a defense in depth involve the use of multiple security measures with each protecting against a specific attack vector. These multiple security measures include firewall, IDS/IPS, scanners to deter, detect, delay and response to any form of attack.

Mark Rhode Ousley (2015) also accorded layered security approach the onion reference. Mark explains that for an invader to succeed requires peeling of several layers which necessitates experience, expertise and time before exposing the core which is the organizational assets. Ousley further his explanation by saying the essence of the onion model is not to increase attackers work-level to succeed instead to reduce the risk of unintended failure of any single technology.

Defense in depth strategy cannot be considered a silver bullet because it suffered some limitations that give rise to new defense model known as defense in breadth. Some of the defense in depth limitations that gave birth to defense in breadth includes

- Human factors such as administrative overhead and trusted insider attack
- Changes in technology
- CIA tradeoffs during implementation
- Design flaws
- Lack of experience and expertise

Defence in depth has become the defacto model that is adopted and implemented by many organizations due to its adaptability, scalability, heterogeneity and above all is a proven model despite its limitation.

3.3 Defence in Breadth

This is a non-cost-effective methodology that is making wave into the security industry. Defence in breadth methodology is a patch to the shortcomings of defence in depth architecture. According to Jin-Cho and Ben Archer (2018), defence in breadth involves a collection of selected defence techniques, deploying them together to ensure total security. Having considered the sophisticate nature of recent attack, it is impossible to maintain security using a single silver bullet solution.

Lance Cleghorn (2013) view defence in breadth as layering of heterogeneous technologies in a common attack vector is impractical because the network becomes complex. Complexity been the bane of network security rendered the network difficult to secure by Lewley and Lowry (2004).

Network complexity is as result of clustering technologies. Clustering most often does not reduce attack surface neither does it prevent vulnerabilities such as zero-day attack instead increase administrative overhead and network oversight exposing the network to attack as a result of negligence.

Defence in breadth implementation has started. F5 security industry company integrated defence in breadth methodologies into their products and their products are permeating the security industry gradually. One advantage of using defence in breadth products is that the integrated firewall defines new rule to prevent any new vulnerability upon discovery and if there exist no patch.

3.4 Attack Reduction Model

Thorough analysis of the perimeter model, defense in depth and defense in breadth limitations and advantages should be leveraged to offer network infrastructure comprehensive defense to withstand the emergence of diverse attacks and attack vectors

Comprehensive defense strategy involves the integration of the three models so that each limitation of each preventive model could be complemented by the advantages of each model.

Comprehensive defense strategy aims to detect, deter, delayed, monitor and defend the activities that goes on in a network there breaking the cyber kill chain.

The integration of the three models to define new counter -productive network defense solution involves the formulation of a strategic mechanisms such as

- Hardening the operating system
- Implementation of system isolation mechanism
- Application and file control mechanism
- Exploit Prevention
- Network security mechanism
- Implementation of security awareness program

The next chapter explores the strategic mechanism in detail and how it is capable of reducing the attack surface of the cyber kill.

4. Existing System: Cyber Kill Chain

Cyber kill chain according to Martin Lockheed (2011) is an intelligence-driven defense framework that will aid in the identification and prevention of intrusion activities. The kill chain serves as the penetration path into information systems to execute an attack Marcus J. Ranum (2015).This thesis considers the cyber kill chain an awareness program that provides insight, motivation, an overview of possible cyber-attack strategies map by attackers in launching cyber-attacks of all forms.

The cyber kill chain has come under criticism due to increasing attack after its introduction. One of such criticism is that the cyber kill chain is an old fashion attack method that focuses on malware prevention. Considering the evolving nature of technology and the dynamism with which attackers are modifying attack vectors and adopting new strategies of deploying vectors, the strategic kill chain stages has become unproductive to many.

4.3 Stages of Attack

Considering the destructive and dangerous nature of recent attacks, the breakdown of possible complicated stages will not only aid in identification and prevention but enhance understanding and analysis. There are varying and diverse stages presented but this thesis will dwell on the one presented by Martin Lockheed in figure 1 below.

Attack stages is a chain and non-static method which is mostly based on try and error until one succeeds. If the installation fails, it is trace backwards until the cause is found and resolved then next stage is initiated.

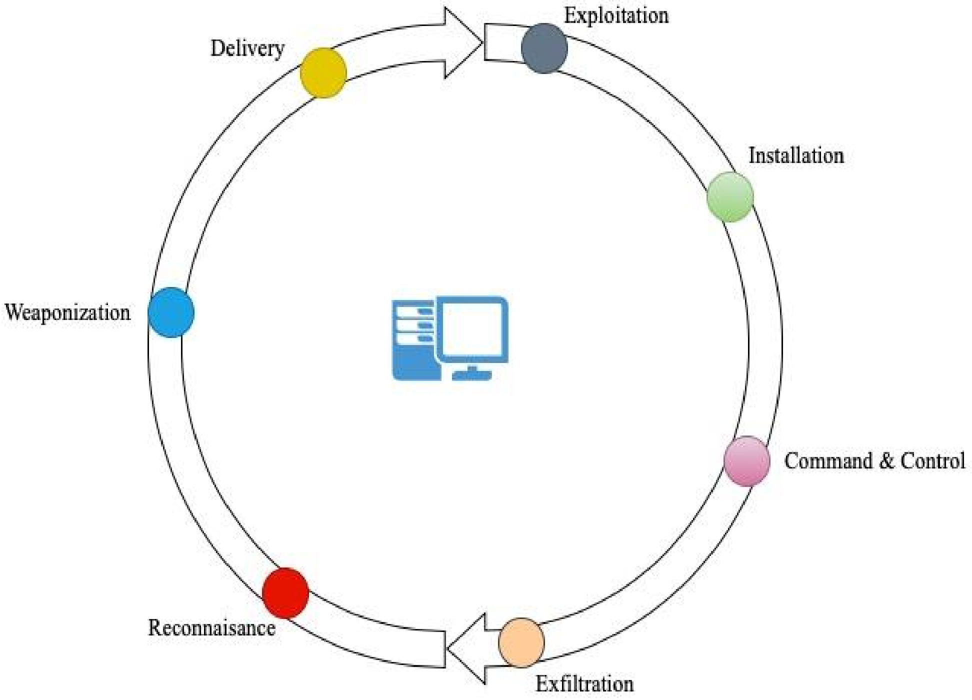

Figure 1: Cyber Kill chain

Figure 1 illustrate the seven stages of cyber kill chain in chronological order starting from Reconnaissance and ends with Ex-filtration. One thing that is evident from the diagram is that the stages are interdependent. This figure 1 is distinct and complete because the seven stages covered pre-hacking and post-hacking activities in real time.

4.3.1. Reconnaissance

Reconnaissance also refer to as information gathering stage of planning attack can be categorize as active and passive reconnaissance Jeremy Faircloth (2011). Active reconnaissance involves engaging the target directly in order to gather the necessary information. The disadvantage of using active reconnaissance is the target is able to records IP address and log activities. Examples of modern active reconnaissance include EyeWitness designed to take screenshots and identify systems using default credential. EyeWitness syntax : ./EyeWitness.py -f filename –timeout optional timeout

The use of a single tool is not enough to gather all necessary information to launch attack. In reality penetration professionals use combine tools in order to gather required information. One powerful framework that all pen testers employs is datasploit. Datasploit is OSNIT framework capable of performing reconnaissance on domains / phone numbers/ usernames/ emails/ credential/ tokens / api-keys / and generate JSON report using text file.

Passive reconnaissance includes the use of complex tools like TheHavester to collect information on the target without any form of direct interaction. Passive reconnaissance is impossible for the target to know or record any activity on the attacker. TheHavester is an excellent and effective python script capable of cataloging email, names, URL, IP address and subdomain names pertaining to the target.
Theharvester Syntax: theharvester -d [domain] -l [number_of_results] -b [source_of_search_query]

The main sources of active and passive reconnaissance information include search engines (google, bing, CerSpotter, dogpile), social media (Facebook, Twitter, LinkedIn), stakeholders (suppliers, service providers, employees), Domain name sites (DNS servers, whois).

Active and passive reconnaissance can be detected and prevented if users employ the right tools and methods such as collecting site visitors logfiles, bowser behavior detection tools, use of browser analytics and collaborating with web and ISP administrators. Users must also limit their online fingerprints as well as their browser fingerprints.

4.3.2. Weaponization

Upon acquiring all necessary information on a target's weakness and vulnerabilities, an exploit is developed to help the attacker leverage the vulnerabilities. Exploit development is based on the intelligent gathered. Exploit takes different forms; web exploit, off-the-shelf or customized malware. The two main exploits this thesis would like to explore include supply chain and heap spray.

Supply chain exploit involve leveraging compound document and free downloadable applications. The attacker downloads and embed payloads into documents and application When the target opens or install the application the payload get downloaded on the target's system. The main weaponization tools on Kali Linux includes Metasploit (MSF venom), veil Framework, Fat Rat.

Practical example of preparing supply chain exploit on Metasploit's MSF venom using putty.exe to leverage window vulnerability

```
$:msfvenom -p windows/meterpreter/reverse -f exe x86/shikata -e- x/desktop/putty.exe LHOST=192.168.1.1 LPORT=443.
```

Upon installation of this infected putty.exe, a connection through port 443 is connected to attacker's machine 192.168.1.1. enabling the attacker an access into the target's machine.

Heap spray is a technique that enable the attacker to duplicate a shellcode into different memory address to increase the chances of the exploit getting it executed. Once the shellcode is dropped into the heap, NOP (no operation) instruction is executed which arbitrarily direct the CPU to exploit address to execute it. The heap is actually a memory location where datafiles are loaded. Heap spray is mostly implemented using the browser.

Weapons are hard to determine but with malware artifact analysis users get to know which payload leverage which vulnerability. Based on this, users will adopt resilient defense mechanism.

4.3.3. Delivery

Delivery involves the transmission of the payload onto the target's domain. Delivery of an exploit is achieved using two major techniques

- adversary-controlled technique
- Adversary -release technique

Adversary-controlled technique involved direct exploitation of the target systems' weakness such as hacking into open ports and protocols and uploading the payload. This is done with the help of Metasploit.

Adversary-released which ensures the conveyance of the payload onto the target system by luring and coercing the user's interaction with the exploit. Delivery is possible through emails, downloadable files (adobe, word, excel, movies), websites, benign links, WinSCP, USB drives or DNS poisoning.

Delivering payload using Metasploit to achieve adversary-controlled method is the most effective technique. Meterpreter is an advance and extensible payload that uses in-memory DLL injection stager and communication is done using stager socket. Meterpreter also has the capability of hiding from antivirus and Intrusion Detection System using memory and process migration.

Meterpreter is an interactive shell that facilitate download/upload of password hashes, backdoor installation, privilege escalation. Metasploit attach payload to exploit, using the listener and execute command

- Payload: set payload windows/meterpreter/ reverse_tcp
- Listener: set LHOST 192.168.0.241
- Execute: exploit

Understanding delivery methods and leveraging weaponizer artefacts to detect malicious payload is one method of prevention. Analyse emails, logs and traffic as well. Equipping users through training to be able to identify phishing, USB, browser delivery method is an effective prevention strategy

4.3.4. Exploitation

Exploitation stage ensures environmental conditions that will facilitate the exploit to trigger installation are fulfilled. Some conditions that facilitate launching installation includes

- the exploit acquiring the right privileges
- the exploit evading detection from anti-virus scanner, and IDs to prevent deletion
- the platform (Linux, Mac, windows) matched.

These three conditions constitute adversary command execution. Recent exploits have adopted metamorphic characteristics. A metamorphic exploit is an exploit having the ability to change its form in order to evade detection by anti-virus. Exploits are designed to exploit several aspects of the target systems such as kernel-level exploit, protocol level exploit, application level exploits, system drivers. Some exploit includes CVE-2010-3333(MS office), CVE-2014-4114(pdf), CVE-2013-3245(audio file)

The main prevention strategies include the use of genuine operating system, installation of updates and patches, constant log analysis and password updates. The use of host-based intrusion detection system (HIDS) such as Snort or Suricata is recommended.

4.3.5. Installation

With exploit installation, a payload is executed, and changes are being made to the target file system and libraries. Privileges are escalated. Exploit file format is also changed. Polymorphic and metamorphic malware have the capability of evading detection by making changes to their memory footprint. This stage also enables remote access into the target's system. This is facilitated by the installation of RAT (remote access Trojan) onto the target system after exploitation is complete. This aids the attacker to deploy as many exploits as possible in order to maintain continuous access to the target's environment and also ensure persistent communication with the target system.

The use of intrusion detection systems, HIDS technology will prevent the installation and human sensors will serves as spies for identification and reporting.

4.3.6. Command and control

This stage is characterized by two main purposes namely stealing of sensitive information (patents, password, finance data) from victims' system and communicating with the malware residing on the victim's machines. Command & control ensure a persistent communication channel with the attacker's server and the victim's system in order to give the attacker hands-on keyboard access to the target system. Exploits must be interacted with, controlled and modified to perform its function.

The use of data encryption, Firewall, IDs, human sensors, system virtualization are potential tools for breaking this stage of the kill chain.

4.3.7. Ex-Filtration

This stage is also referred to in other books as “action on objective”. The motive of attack differs from adversaries, but it could be one of the following:

- steal information be it personal or intellectual property
- cause destruction in the system (denying services to customers, overwriting transaction)
- exposing an organization
- escalating privileges (CVE-2015-002) making system unusable
- using systems as weapon to kill.

Access on keyboard could be dangerous to the victim yet it's the stage that attackers start to release their mission. Upon the completion of the mission, an attacker shutdown the RAT and remove all traces

Breaking the cyber kill chain stages displayed in figure 1, it will involve the use of encryption, unique and strong passwords, human sensor and securing sensitive data.

5. Attack Surface Reduction Methodologies

According to Tom Olczak's Enterprise security: practitioners guide, attack surface includes all vulnerabilities and controls across networks and systems owned by an organization that are exposed to attack. Majeed and Quadri (2016) define attack surface as all the different points where an attacker could get into a system and where they could get data out.

Recent attack surface increase is due to emerging system weaknesses that make the system's behavior deviates from its intended purpose. This system's behavioral deviation becomes a risk to the system owner. This risk could be made acceptable by minimizing, monitoring and managing the attack surface known as attack surface reduction.

Considering the vast proposals both from academic and industry on how to prevent attack, this thesis would like to propose the six means by which attack surface reduction strategies could leverage the cyber kill chain strategies.

- Hardening the operating system
- System Isolation
- Application and File control
- Network Protection
- User-behavior and Policy

5.1 Hardening the operating system

The operating system also known as system software according to Power and Ford (2009) controls all part of a computing system and manages resources such as CPU scheduling, process management, memory, I/O, storage and files management.

These resources are critical to the functioning of any information system and any vulnerability identified and leverage by attacker would result in disaster for such an organization. It is therefore essential that the operating system must be hardened to decrease any attack surface such as browser associated attacks since many OS comes with browsers. The OS hardening has the capability of breaking the cyber kill chain from different stages.

Petteri Siik (2017) defined operating system hardening as a method of removing or disabling certain system features to reduce attack surface in order to improve operating system security.

5.1.1 Patch Management

Patch management involves addressing system update and system maintenance issues. The operating system contains different packages that increases its attack surface area. These packages have vulnerabilities such as zero-day exploit, buffer overflow issues that could be exploited by an attacker.

Patch management decreases these attacks surfaces through constant and as at when available installation of updates that fixes system identified bugs. System maintenance enhance the OS functionalities and decrease attack surface through the use of automated tools for daily or weekly scanning of the system for any weakness.

5.1.2 Configuration Management

Configuration management involves system planning, implementation, controlling and monitoring of system changes due to patch management. Considering series of update of the operating system as well as hardware system calls for security-minded configuration management to avert the adverse effect these constant changes could pose.

Configuration management planning ensures the development of policies , procedures and standard for updating the system whiles implementation and controlling prioritized update installation based on risk and impact of any identified threat. Monitoring ensure configuration is identical with the defined baseline and also enhances system maintenance.

5.1.3 Disabling Redundant Services and Ports

Disabling unnecessary services and ports takes into account redundant services and ports that are not in use by the operating system or programs.
Services are programs that runs to aid the functionalities of the operating system whiles ports are open communication channels used by the operating system when the operating starts.

Many of these services get loaded into memory and waste CPU time. Identification and disabling of these services free up system resources and prevent denial of service attack emanating from memory overflow. Closing unneeded ports also prevent port scan attack.

5.2 Systems Isolation

According to Rui Shui et al. (2016), security isolation is a foundation of computing systems that enable resilience to different forms of attack. The importance of security isolation can be traced back to computing technology planning report by James Anderson.

This report identifies that security and privacy issues are mainly caused by resource sharing between users. This idea was built into operating system known as Reference monitor. Reference monitor validate all references made by programs in execution and ensure resource sharing. Isolation techniques for attack prevention includes

5.2.1 Language-based Isolation (LBI)

LBI ensures that security of an application is strengthen using the properties of a programming language. LBI enforces application level security by preventing vulnerabilities that the operating system is unable to prevent.

According to Sergio and Ankur (2009), many websites in cooperate untrusted content that allows for page altering, theft of sensitive information. Sergio and Ankur categorically state that these sites must enforce language-based isolation technique to prevent browser-related vulnerabilities that allows for information theft.

Arun and Neuman (2009), classified language-based isolation into

- Type System : Type system enforce isolation using language semantics , compilers and runtime systems. Type system ensures programs access only appropriate memory location and control transfer happens to appropriate program point.

The main responsibility of type system lies on the programmer by ensuring the codes conform to type system policies. Type system examples includes java, Modular-3 , ML

- Certifying compilers: According to Torben(), Compiler translate a high-level programming language to low-level machine language that is understandable by the computer and also report obvious programmer mistakes in the process.

  The compiler ensures any given source code satisfy a define security policy and produces a certificate. This certificate comes in the form of machine-checkable evidence that a bytecode follows a defined policy.

5.2.2 Sandbox Based Isolation

Sandbox is a specific address space that untrusted codes or applications are transformed to run. The pioneer of sandbox technology. Wahbe et al.(1994) defined sandbox as technique for encapsulating untrusted code so that it may not escape its fault domain.

Wahbe et al adopt this technique and implemented it by introducing checks into program binary so that the program could only make writes, jumps and store into its own segment. This implies that sandbox could be considered a container that untrusted application could run in.

Never the less Arun and Neuman simplified sandbox definition as a technique for creating a confined execution environment for running untrusted programs on the same machine. In order for a program to be restricted to run in a confined environment , three main techniques could be implored

- Instruction Set Architecture based (ISA): According to Bhunia et al. (20019), ISA serves as an intermediary between the software and the hardware of a computer. sandboxing technology implements ISA by restricting a programs activity at the instruction level.

ISA sandboxing implementation is based on introduction of additional instruction to the existing binary to check for memory access violation. This implies ISA provides a mechanism by which the software tells the hardware what should be done.

- Application Binary Interface(ABI): Wikipedia defined ABI as a low-level interface between an application and the operating system and it involves data type , size , alignment and calling convention.

  Any sandbox that controls the ABIs of an application falls within application binary interface. Application uses the ABI to restrict their behavior and is achieve through the configuration file of the application. ABI prevent systems call.

- Access control-based : Access control-based sandboxing ensures program activities are based on explicit permission. This includes files, processes, pipes , network Unix chroot-jail, FreeBSD jail are practical examples of access control sandboxing where a user's view is restricted to a permitted directory. Other sandbox applications include window sandbox, Shade sandbox, Shadow sandbox, BitBox sandbox

5.2.3 Virtual Machine based Isolation

According to Sigh and Yip (2017), virtual machines are software computers that enable the user to perform the same function just like physical computer. This is to aid the performance of specific tasks that are considered risky to perform in a host environment e.g. accessing malware-infected sites or data and also testing the behavior and performance of an applications such as operating system.

Arun and Neuman defined virtual machine as software abstraction of a real machine that enable emulation , optimization, translation, isolation and replication. Smith and Nair (2005) explained that virtual machines can support individual processes, a complete system, flexible hardware usage , software isolation and translation from one instruction set to another.

Based software isolation, there are different categories of virtual machine such as process VM, system VMs, hosted VMs and hardware VMs

- Process Virtual Machine platform enable execution of individual processes and is process dependent. This implies that the virtual machine is created when a process is created and terminated when a process is terminated.

- System Virtual Machine provides a full system environment that support an operating system and its processes with access to all virtual hardware resources. This environment allows for running of multiple isolated guest operating system.

- Hosted Virtual machines are implemented when a virtual machine is built on an existing operating system known as the host. This virtual machine is actually seen as an application process by the host and the host provides the necessary resources such as device driver and other lower-level services.

5.2.4. OS-Kernel based Isolation

According to Paulo Shakarian et. al (2013), the kernel of an operating system manage access to the protected hardware and responsible for how resources are accessed and used by the various processes. The kernel determines the appropriate actions that a process must take such as accessing files, view config file

Since the kernel serves as the intermediary between the hardware and the applications, it enforces policies that ensure that all applications run smoothly and all processes access necessary resources without interference thereby guaranteeing isolation.

5.2.5 Hardware based isolation

Hardware Virtual machine also known as server virtualization. Its implementation is based on abstraction of a hardware platform using a control program known as hypervisor. Hypervisor actually create a computer environment for a guest software through simulation. Access to resources are restrictively managed and is more secure and isolated compared to the other virtual machines.

5.3 Application and File Security Control

Applications are customized programs design specifically to aids in the execution of various task by the end user. These programs can be standalone or web-based application , most of which are designed by amateur programmers   that contain exploitable vulnerabilities that hackers, script kiddies and pen testers exploits.

Common application vulnerability exploits include SQL injection, insecure cryptographic storage, lightweight directory access protocol injection(LDAP) and cross-site scripting among many others. These exploits are commonly referred to as Zero-day vulnerability.

Securing application is a daunting task that involve two main processes namely secure design and application behavior control. Reducing attack surface deeply depend on the mentioned processes and this constitutes application security practices. These secure practices will equip users not to do things that will compromise any system.

5.3.1 Securing application design

Designing any application follows system development methodology also refer to as application life-cycle. This life-cycle defines the various stages that an application goes through before it is finally ready for aiding end-user in performance of a task. Waterfall model, agile development, spiral model are examples of application development life-cycle.

Building security into applications and application development life-cycle are of paramount importance in reducing attack surface. According to Rhode Mark Ousley (2015), application life-cycle commences with data gathering and ends with deployment but does not include security practices that will ensure secure design and secure application.
Reducing attack surface in application design process must involve integration of security practices such as threat modeling, security training and secure code review

- Threat modeling techniques enable developers to review the security properties of any design application. It involves identification and mitigation of exploitable vulnerabilities in the application's architecture.

  Threat modeling methodologies that guarantee secure application design include STRIDE(Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privileges), PASTA(Process for Attack Simulation and Threat Analysis) and VAST(visual, Agile and Simple Threat modeling) among others. Programmers endeavoring to integrate threat modeling into development process is a means of leveraging the application from attack.

- Threat modeling can only be achieved through security training. Security training is an awareness program that will equip application development team on new application vulnerabilities and security practices such as threat modeling methodologies that could be used and how to use them.

- Secure code review involves the use of manual or automated tools to inspect, analyzed and identified security issues in an applications source code. Manual code review is done by expert programmer other than the writer. Though manual review is effective, it is time consuming. Some recommended code review tools include collaborator, Code Scene, Codebrag, Review Assistant, Phabricator and Gerrit

  Review Assistant is a simple and lightweight process for visual studio. It allows the programmer to flexibility, defect fixing, in code discussion, gives emails notification, support post commit code review, present report and statistics.

5.3.2 Application Behavior Control

Application behavior is dependent on the purpose of design. The purpose of design enlists the functions and the required resources needed to complete task execution. Considering the vast amount of free applications on the web, it become imperative to control applications installed to prohibit unwanted behaviors such as privilege escalation, remote access , port opening, fingerprint collection and transfer of files to remote servers.

Controlling applications be it standalone or web-based application could be achieved through access control, application whitelisting and file monitoring

- Access control is a very critical topic in computer security because it defines the allowable actions, operations and users in any information system. Access control is not only limited to applications instead it also involves hardware, network, operating systems, middleware as well.

  Access control can be seen as a security compliance component that ensures physical and logical access to system resources comply by the defined policies. This protect against abuse of application features by users and processes from making changes to the system data.

  Access control identify, authenticate and authorized users, processes and machines by evaluating their credential. The main types of access control includes Discretionary Access Control (Access to files and directories are at the discretion of the file owner upon the file creation), Mandatory Access Control (Access to system resources are defined by the system) and Role-Based Access Control list (Access is not based on objects rather authorization)

  The efficacy of Access control is greatly influence by system policy and defined access control list. System policy is a set of documents defining acceptable use of resources. It includes standards and guidelines. Every policy document should take into consideration general issues (password construction and guidelines, email policy, disaster response plan, ethics policy), Network security (acquisition, remote access, router, and wireless policy, use of personal devices on the network, Bluetooth and plugs and plays device policies), Server security(database policy, logging policy, equipment disposal policy, application installation policy) and Application security application signature policy, application requirement and features policy, web interface policy)

- Application whitelisting is the compiled list of applications and their components (configuration files) that are authorized by the application designer to be active on a system or host. Whitelisting technologies are intended to prevent the execution of malicious programs and applications on a host NIST SP 800-167.

  A whitelist entity includes a host, email, process, application, port numbers, OS, interfaces and the main technologies include airlock digital, lumension, carbon black, digital guardian, SELinex

  Whitelisting is an effective tool for ensuring file integrity, memory protection, access control, software inventory and incident response purposes. Whitelisting technologies installed to leverage application control.

- Proper file management and monitoring is essential in preventing attack on systems. File management involves organization , administering and monitoring of files on a system to support business workflow.

  File administration ensures access to a file is based on privilege and job role. Proper file administration prevents unauthorized reading, modification and deletion of sensitive files by users.

  File monitoring identify changes made to the file by who and at what time. Based on file monitoring, different forms of attack could be identified and prevented before the attacker gets his hands-on keyboard. Some modern technologies for file monitoring include Samhain and Tripwire.

  Samhain and Tripwire are form of host-based intrusion detection systems that keep different versions of file and also alert the user about changes that is ongoing by who, which process and file location. Identification of changes is based on file's signature hashes store in a configure file.

5.4 Network Security

The role of networks infrastructure in today's business is so critical that network protection must be accorded priority and urgency. Network facilitate end-to-end communication among devices, transfer of data and facilitates online transactions around the globe. These possess a challenge and requires a defensive mechanism in place to protect network against attack.

The pursuit of network protection is a necessary requirement because attackers have the capability of subverting network to access data, cause denial off services, disable systems and exploit vulnerabilities in the connected devices. The network protection commences with design choice. There exist different types of networks having its own advantages and disadvantages. The network design choice translates the purpose of the network and the sort of protective mechanisms defenders must strive for.

- Local Area Network (LAN), local area network is a kind of small network limited to a building. The nature of this network affords defenders the opportunity to exercise control in terms of choice of technology, its implementation and management policies and procedures to secure the network.

- Metropolitan Area Network (MAN), it is a kind of network that span a geographic. Due to disperse nature of this network, security and management is handled by service provider.

- Wide Area Network (WAN), involves interconnection of LANs and MANs managed by service provider. The service provider is responsible for securing the network and the devices therein.

Stringent mechanism and technologies have to be employed in securing the network and they include network Segmentation, Firewall, IDS/IPS, Encryption, Secure protocol and SIEM.

5.4.1 Encryption

Encryptions involve the use of sophisticated mathematical algorithms to transform plaintext into a seemingly unintelligible form using an encryption key. This becomes a necessity due to the sensitivity, confidentiality and the value of information. To prevent unauthorized persons from reading or accessing sensitive data encryption becomes necessary. There are different encryption algorithms classified as symmetric and Asymmetric. These are the popular modern encryption algorithms mostly used. With the symmetric cryptosystem, one key does both encryption and decryption while the asymmetric cryptosystem makes use of different keys namely public and private keys.

The choice of encryption algorithms is influence by the processing time, memory usage, power consumption, and throughput. The most popular in terms of symmetric algorithm include AES-128, AES-192, AES-256, DES, Blowfish and RC6 whiles Asymmetric includes RSA and PKCS

Some simple open-source yet effective host-based encryption algorithm that users must employed to secure their data include Ax Crypt, VeraCrypt, Cypherix

- Ax Crypt is an open source (GNU general public license) software that enables users to encrypt a file to self-decrypting executable and it is based on 128-bit AES algorithm. It also makes use of SHA-1 for password hashing and file verification.

  Ax Crypt's amazing features include file shredding, auto-key generation, and its portability. Ax Crypt neither creates volumes(containers) nor does it encrypt folders. The key file generated by Ax Crypt can encrypt as many files as the user desired.

- VeraCrypt, is also an open source software that encrypts volume (storage devices) on the fly (encryption and decryption are done whiles in memory) without any user intervention. Encrypted data can only be accessed or read using a password or key file.

  The security of VeraCrypt is one of a kind because it has the capability of hiding data in data. VeraCrypt usually creates two volumes namely standard and hidden. The hidden volume keeps sensitive data such that unauthorized user when forcefully break into standard volume may not be able to access the hidden volume.

VeraCrypt encryption and decryption speed depend on the number of processors the server or the computer have. VeraCrypt put data into chunks according to the number of the processors available and run parallel encryption and decryption. VeraCrypt encryption algorithm includes AES, Camilla, Two fish, and Kuznyechik. VeraCrypt does not protect files and directories against malware infections especially using VeraCrypt on an infected PC.

- Cypherix, is a window-based encryption software that affords users the opportunity to create a secure container using 448 blowfish and 26 AES algorithm to secure files, emails, images, text and many more. Cypherix encryption is considered secure because an average hacker can’t break the 448 blowfish algorithm.

  Cypherix is user-friendly due to the ease of use such as drag and drops feature. Encryption is done on the fly and mostly mounted drive is label S. Documents can only be accessed providing a password. When drive is unmounted, the receiver of Cypherix encrypted documents do not need Cypherix installation to decrypt. There are different versions such as Cypherix LE, SE, and PE

5.4.2 Network Segmentation (NS)

Network Segmentation ensures a network is partition into smaller and manageable systems that enforces network segregation (controlled communication between the various small networks using ruleset). Network segmentation restricts access to specific information, services and hosts thereby ensuring continues operation amid disaster. This is because if a hacker accesses and infect one segment of the network, it will not affect the other segments. The infected network segment can be taken off. Implement network segmentation through the use of modern technologies and physical isolation, minimize user privileges and implement least privilege principles.

Separation of a network should be done taking into consideration sensitivity, criticality and business need and network access should be based on duties, functions and operational requests. In network segmentation, implementing whitelisting of network traffics is advisable compared to blacklisting.

5.4.3 Network monitoring

Monitoring system and network resources for malicious events should be a basic priority of a user or system administrator and could be achieved using both hardware and software . Monitoring ensures discovery of bad or malformed traffic, over memory usage, CPU hijack, open ports exploitation, network.

Monitoring using hardware involve the use of physical equipment's such as CCTV cameras, Sensors, Motion detectors , infra or laser detectors, id scanners, biometric access, locks devices whiles software monitoring tools include

- Tcpdump, t shark, wind dump, Wireshark (analyzing protocol)
- ARPWatch (monitors MACSec ARP traffic 802.1AE/ 802.1X)
- Task manager (Microsoft tool)
- Syslog (for Linux, configure using "set syslog port")
- Wi-Fi-inspector (display anybody on one's network)
- Nexus and Qualys free scan (free vulnerability scanner)
- MBSA (Microsoft Baseline Security Analyzer)

Monitoring involves detecting intrusion, discovering attacks and reporting vulnerabilities. Combine use of hardware and software monitoring tool leverage the physical perimeter of an organization. Physical perimeter protection is as important as network protection.

5.4.4 Security Protocols

Networks facilitate communication , file sharing among connected devices on the other ends. The main goal of security protocols is to prevent a third-party from intercepting and modifying the communication calls for implementation of security protocol that can secure the medium.

Mohsen Toorani (2015), Security protocols are the foundation for secure communication. Protocols are set of conventions that defines the mechanics of message exchange on network. These protocols are not silver-bullets because most often they come under attack by hackers.

The most widely used network protocols that has the capability of securing data integrity and privacy includes

- IPSec and VPNs, is defined by Internet Engineering Task Force (IETF) to enforce cryptographic key sharing, agent authentication, data integrity and privacy between networked entities. IPSec enforces secure communication known as secure association using VPN to protect sensitive data.

  Security association key management is managed using IETF defined key management protocol called Internet Key Exchange (IKE). Currently are there two main version of IPSec IKEv1 and IKEv2 that are responsible for encrypting, decrypting, authenticating of packets.

- TLS (Transport Layer Security) is responsible for data encryption, agent origin authentication and message integrity. TLS is also responsible for client-server authentication using X.509 certificates. Examples of applications that employs TLS includes web browser, email and voice over IP (VOIP).

  TLS evolved from SSL defined by IETF RFCs 2246, 4346, 5246 and 8446 as a result of identified cryptographic flaws such as RC4 weakness and POODLE attack.

  The TLS cryptographic algorithm is composed of cipher suit that is acquired during the process of handshake. The cipher suit includes AES and other algorithms and session key.

- Kerberos is a free open-source application designed by MIT. Kerberos is a client-server network authentication protocol that make use of strong secret-key cryptography. Considering the unsecure nature of the network, Kerberos enable a client to prove its identity to a server over unsecure connection MIT Kerberos Consortium (2019)

Kerberos not only ensure authentication but encourage data integrity and privacy through message encryption using strong crypto. Kerberos works at the transport layer of the TCP/IP protocol stack using port 88.

Kerberos authentication implementation involve the client a request key distribution center(KDC) for authentication key (TGT). Upon satisfied verification of client's credential TGT alongside session key encrypted using TGT granting service (TGS)secret key. The client stores the TGT and upon expiration a new request is made by local session manager.

- OSPF Authentication ensures router update information is exchange in a secure manner using password or MD5 hash algorithm. This prevents rogue router from injecting routing information into the network thereby preventing denial of service attack and eavesdropping.

  OSPF authentication implementation is based on configuring network routers to authenticate each other to prevent man-in-the-middle devices. On cisco router configuration is

  ```
  ip address 192.17.64.2 255.255.254.0
  ip ospf authentication-key malo@1
  ```

5.4.5 Firewall

A firewall can be considered as a software or hardware that has the capability of filtering network traffics (ingress/ egress connections) between one system and the internet. Since organizations varies in terms of size, services, type of data, so is the firewall.

Firewalls are built to serve and meet the need of different groups. A personal firewall is to protect a single computer and helps a single user. An organizational firewall is to provide protection for small size organization's information and information structure. Enterprise firewall serves the need of a large organization that are geographically distributed.

Firewall be it personal, organizational or enterprise performs the following functions include blocking inbound and outbound traffic, content filtering (embedded virus or attack signatures), network address translation, log keeping, reporting and ensure availability.

Though the firewall is responsible for protecting networks and information resources, some threats could subvert the function of the firewall such as social engineering, insider attack, specific malware and inexperience administrators. The choice of the right firewall

Packet filters; the primary example of this firewall is the router and Unix kernel. Packet filters are responsible for network traffic analysis using the source and destination IP address, port number, and packet headers.

- Packet filters such as the router are not secure because hackers could bypass it using IP spoofing, source routing, and tiny fragment attack. Packet filtering takes place at layers 3 and 4 of the OSI layer (transport and network). Packet filter permit or deny traffic based on ACL (Access Control Lists) defined in the router or the UNIX kernel.

- Circuit-level gateway, this type of firewall can be considered as resource-efficient. The processing of a packet does not require many resources since it only checks the legitimacy of a TCP handshake to conclude. This firewall works at the session layer of the OSI model and completely abides by session rules. The major problem with this firewall is malware, and other attack vectors hidden in the packet and remote connections whether valid or invalid are considered legitimate sessions.

- Application Layer gateway, this type of firewall act as a proxy (application service access code) in connecting the client’s request to application servers. It is responsible for content screening, authentication and ensures connection and usage of a specific service. Traffics are generated from applications such as HTTP, FTP, SMTP or POP3, DNS for the web, file transfer, emails, and domain name resolution respectively. Attacks may occur as a result of using pirated OS, wrong configuration and disclosure of authentication information.

- Stateful Packet Inspection, Cisco PIX, Reflexive ACL, Checkpoint Firewall-1 GX are typical examples of a modern firewall in the market. It works at the network and application layer of the OSI. It maintains active state connections (IP address, Headers, Protocols, Seq number, ports) in its dynamic state table. Stateful firewall matches traffic with rules defined in the system as well as using a state table to allow or reject traffic. Current stateful firewalls have the capability of content and deep packet inspection.

- Next Generational firewalls, these are firewalls designed to meet the current and the future needs considering advancement in technology and its related threats. Features of these firewalls include deep-packet inspection, signature identification, web filtering, encrypted SSL packet inspection, third-party application verification, IPS/IDS. The fantastic thing about this firewall is it detects and stops any attack instantly. Examples include ASA5500-X Firepower series 2100, 4100, 9000.

5.5. Intrusion Detection and Prevention System

Antivirus and firewalls are developed to detect malicious activities within a network, but their limitations are incapacitating their functions and require a more complex tool that can process, and monitor traffics for malicious events Mark Rhode (2015).

Intrusion detection (IDs) are hardware or software applications that are responsible for monitoring and identifying malicious activities that goes on in a network. IDS are firewall compliments that is capable of determining hostile network activities originating externally or internally Tiwari et al (2017).

IDs provides system administrator information on any suspicious event termed as alert. Alert can be true positive, false positive, true negative and false negative.

- True positive, malicious event is ongoing
- False positive, event identify is not malicious but there is alert
- True negative, event is not malicious but there is alert

- False negative, malicious event is been ignored but no alert

The alert is on whiles the event is not malicious and the system overlooking malicious event constitute IDs limitations.

The two main type of ID/IPS include Host-based IDS (HIDS), and Network-based IDS (NIDS). Whiles the HIDS monitor single computer, workstation, server or a device whiles NIDS provide a protection for all devices on a network.

IDS ability to identify malicious event is based on anomaly detection (event profile, behaviour, heuristics and statistic) or signature detection (pattern of code collected into a database). Anomaly and signature detection are effective IDS mechanism.

The combine use of HIDS and NIDS to compliment firewall and antivirus render a network more secure. Examples of common IDS include Snort, Suricata, Segan, security onion, OSSEC could be used to reduce attack surface area at no cost.

Snort is the most recommended and used network intrusion detection system (NIDS). Snort is an open source tool capable of monitoring packets in real-time to detect suspicious payload. Snort is based on TCP/IP traffic sniffer and analyser tool called libpap. Based on this protocol analysis and matching tool, Snort detects and prevents attacks such as denial of service, Server Message Block (SMB) probes, buffer overflow, stealth scan of ports, Common Gateway Interface attack (CGI).

Due to the drawback of snort acting dump, it’s always recommended to configure snort to interact with other services like firewall, iptables to detect and blocks suspicious hosts. Detecting and blocking suspicious packets and host is determined by the placement location of snort in a network.

5.6 Security and Event Management System (SIEM)

According to Subhalakshmi Ganapathy (2018), SIEM is a threat detection and incident response technology that gathers and correlate network activities (events) occurring across a network. SIEM involve real-time event analysis as well as historical event analysis.

Though organizations deploy intrusion detection system (IDs), intrusion prevention system (IPs), anti-malware as well as firewall to detect and prevent anomalies, due to some limitation in these technologies, some sophisticated attacks could bypass them and compromise the network.

SIEM technology solution have different inbuilt capabilities that works independently whiles providing network security visibility. The main capabilities of SIEM technology include

- Log Management: Network infrastructure generates different log data. SIEM technology like IBM Qradar collect ,process and store all logs across different platforms applications and devices. The log management perform forensic analysis on all collected logs by normalizing them to gain meaningful insight.

- Vulnerability Management: Cyber security report have it that an attack takes about 175 days to detect known as the dwell time. IBM Qradar integrate forensic analytical tool that searches logs and other network activities to detect attack patterns and its impact. Detected attack patterns are investigated by security operations and vulnerability manager provide them with graphical view to facilitate investigation

- Real-time Monitoring facilitate early detection and response to attack indicators. IBM Qradar real-monitoring comprise of event response system, event correlation engine and intuitive analytics. Whiles event response system detects discrete events and determine if the event matches predefined attack alert profile, the correlation engine detects attack pattern using collected logs.

- Security Intelligence is an integral part of IBM Qradar and it involve aggregating threat feeds from trusted source like anti-virus companies, common vulnerability exposure(CVE) database, FBI, recognized platform developers like Microsoft or third parties. Analyze associated incidents with attack vectors provided by threat feeds and alert when similar incident is detected.

- Incident management using IBM Qradar involves provision of rea-time event response system, correlation engine, forensic analysis, event alert, automated scripts to seal loopholes, and incident tracking. All these important features are built into IBM Qradar to facilitate the work of SOC

Successful implementation of SIEM solution depends choice of architecture and solution checklist. The two main architecture include all-in-one or distributed. Security experts should also take into consideration scalability, log data compatibility, off-the-shelf or customized components, security harmony of tools and predictive intelligence when selecting SIEM solution.

SIEM technologies are incredibly useful and provide organizations benefit such as increase efficiency, threat prevention, reducing breach impact, cost, log analysis and retention, security compliance and better reporting.

5.7 User-Behaviour Control

The deployment of sophisticated, complex and state of the art technologies in the bid of safe guarding data and information infrastructures could hardly prevent internal attacks such as gaining excess access, deleting production and back up data, system crashing, misuse and stealing. Mechanism that can leverage internal attack is effective user-centered security control program.

The importance of effective and on-going security awareness program in an organization has the potential of reducing attack surface by 45%. According to Henry Dalziel (2015), security awareness enables employees to detect social engineering attacks and respond to it appropriately and also gathered the confidence to report any suspicious activity.

The importance and the role of security awareness is of paramount in achieving confidentiality, data integrity and availability of services. This is why security awareness standards such as ISO 27002, NIST special publication 800-100 and SANs have developed security awareness guideline.

Security awareness involve implementation of training, motivation and sanction to improve employee's behavior such as making employees accountable for their actions, reducing liabilities their behavior may cause and increase regulation compliance by employee. Reducing attack surface through security awareness involves the adoption of the following stringent strategies.

5.7.1 Reducing digital footprint

Technology has downplayed the sense of responsibility on the part of users online. It is no doubt users concern not about what goes on online. The only thing that matters to them is the perceived enjoyment of chatting, sharing and socializing with friends. Out of this perceived enjoyment, users leave behind traceable behaviors which adversely affect them later. This effect includes identity theft, data breaches, stolen credential (credit card, password, pin codes, certificates). This information's are given actively (intentional shared) or passively (unintentionally shared). This critical information is collected using search engines, social media, third-party cookies and used to their benefit. Social media has become the primary information gathering place for hackers. Hackers select and collect information on their targets using social media. Hacked institution discovered that their system's compromise is due to an employee's post on Facebook. This is the level of exposure of one's profile, employer's information, GPS location, shared Wi-Fi information, family, religion and medical records

Users must endeavor to reduce the amount of information and online exposure. Disabling JavaScript in the browser as well as third-party cookies will limit hackers-user online activities. Users must endeavor to make use of multi-factor authentication for online logins and to verify site security in terms of data collection. Tuning browser security settings as well as social media privacy settings protect users online.

A successful attack is based on the amount of target's information available to the attacker. Limiting the amount of information users placed online could hinder the attacker's success and this can only be accomplished if users can

- stop broadcasting their router SSID
- use ID cards with only user name

- minimize data on websites instead dwell on the intranet
- reduce dumpster information by shredding, burning documents with vital information use biometrics to authenticate to prevent shoulder onlookers from stealing your password and pins

The ability of a user capable of adhering to reducing digital footprint makes the reconnaissance stage in figure 1 impossible to gather enough information capable of laughing attack.

5.7.2 Signature Verification

Every application comes with a signature in a form of embedded certificate that could be used to detect if an application is genuine or not especially in the case of supply chain attack it becomes a necessity to check application certificates before running them.

The most commonly web-based tool for checking the genuity of any application is Virus Total. Virus Total is a powerful web-application that is connected to more than 70 antivirus scanners. It helps users to inspect all applications, documents, process to verify the source, detect virus and hidden malwares based on the antivirus databased.

5.7.3 Education and Training

Training and education, according to William stalling (2015), security training and education provide users the necessary skills to perform their duties. Training affords users the opportunity to know actions that could compromise security, identify possible attack vectors and report to appropriate personnel.

Some required training for users includes equipment and working environment protection, password protection and reporting. Training should also be tailored to suit individual expertise.

Education most often referred to as career development involves domain expertise tailored training that is provided to an employee from external source like college. Effective training and education have the tendency of equipping employees and making them security conscious thereby reducing attack surface and creating sound security environment.

Education and training should be cantered

- Password usage
- Data encryption
- Reducing online fingerprints
- System configuration
- Vulnerability identification(social engineering, phishing, malware) and reporting also known as human sensors.

5.7.4 Employee Compliance Motivations

Motivation, with reference to Davis et al (1992) employees are driven by intrinsic and extrinsic motivational factors. Intrinsic motivation involves pleasure and satisfactions reward that an employee enjoys as a result of job engagement. Extrinsic motivation includes monetary rewards, promotions and recognitions that an employee is accorded as a result of performance outcome.

Studies have revealed that insider threat been the result of employee non-compliance could be attributed to intrinsic and intrinsic motivational factors Guo et al (2011). Organizations are thereby advised to implement and integrate intrinsic and extrinsic motivation factors such as monetary reward, recognitions, awards, promotions and engagement into their organizational culture in order to motivate employees for policy compliance. Offering an employee, a ticket for an international conference for been security vulnerability identification will motivate the others. Better still, having the employee picture on the company's magazine for a month is a plus.

5.7.5 Sanctions

Sanctions are to serve as deterrence to employees. Deterrence should be considered a means of discouraging unacceptable or non-security compliance behaviour of employees. The severity of sanctions normally has the ability to deter or encourage employee to comply with security policies or not Seppo et al (2007)

There are different forms of sanctions such as counselling, oral warning, written reprimand, suspension, contract termination and imprisonment. The role of sanctions cannot be neglected to effectively tackle the issue of insider attack.

A practical means of implementing a sanction when an employee violate security policy should be depending on severity instant contract termination, publication of his name in the newspaper and legal action against him. This will send message to stakeholders on the level of extent their information is protected and will deter other employees from non-compliance behaviours.

6. Conclusion

Whiles cyber kill chain concept has become a hot topic and discussed in most papers, it is worthwhile noting previous works do not address the issue of leveraging users to be able to reduce the attack surface thereby limiting the attacker's stage-by-stage progress. Most papers do not thoroughly explain each stage with practical demonstration on tools to use and how to harness those tools to achieve the objective of preventing attack. Others cited some prevention technologies, but citing is inadequate to equipping a user to prevent an attack.

Considering the recent upsurge in attack and its effect on individuals, organizations and institutions, a resilient and counter-productive approach is required. This involves a step by step understanding of the cyber kill chain stages as illustrated in figure 1and how to limit attack surface in each stage to reduce the chances of an attacker launching attack.

This is exactly what this thesis achieved by thoroughly exploring the cyber kill chain stages from reconnaissance to ex-filtration in detail broadening, enhancing the understanding of users on different forms of attack vectors, exploits and how they are technically used in leveraging vulnerabilities in the systems and networks.

This thesis also demonstrated and explained how various technologies as well as user behavior control will aid in fostering a counter-productive defense against attack vectors, exploits thereby reducing the attack surface and finally breaking the cyber kill chain.

This thesis not only contribute to the in-depth understanding and breaking of the cyber kill chain instead it also explored and evaluates the advantages and disadvantages of the variant attack prevention models. This is to enable users to be able to select and implement the model that will foster a counter-productive security against modern attack actors.

This thesis also establishes the fact that no single attack model or technology is a silver bullet, efficient and robust enough to providing that secure environment for data confidentiality, integrity, availability and non-repudiation, instead recommends model integration and layering of multiple technologies for security assurance.

In conclusion this thesis after exposing users to the technical details of the cyber kill chain stages, present also a kill chain leveraging strategy known as attack reduction mechanism. This Attack reduction strategy involves hardening the OS, enforcing System Isolation, Application and File control, Network Protection and Security Awareness.

6.1 Future Research

This area of cyber-attack within information security is so acritical and not fully explored. It requires constant and thorough investigation to understand the new threats, vulnerabilities and exploits domain in order to foster counter-productive defense mechanisms.

The main force to battle with when it comes to cyber-attack is the advancement in technology. This empowers attackers and give them the edge in developing exploits and vectors to launch an attack because it takes an organization about 206 days to determine and contain an attack.

This thesis only explored the seven stages and how to reduce attack surface to limit the progress of an attacker. Each stage of the cyber kill chain is daring and explorable area that researchers should take into consideration.

References

Baumard, P. (2017). Cybersecurity in France. SpringerBriefs in Cybersecurity, MIP Conservatoire national des arts/ metiers, Paris, France

Beaver, K. (2010). Hacking for Dummies; 3rd Edition. Indianapolis: John Wiley & Sons.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Anderson, H. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv preprint arXiv:1802.07228.

Chiesa, R. (2010). Hackers profiling: Who are the attackers? Freedom from Fear, 2010(7), 4-4.

Costoya, J., Flores, R., Gu, L., & Mercês, F. (2017). Securing Your Home Routers Understanding Attacks and Defence Strategies. Retrieved from https://documents.trendmicro.com/assets/wp/wp-securing-your-home-routers.pdf
[accessed on 18.9.2019]

Daimi, K. (2018). Computer and network security essentials. Cham, Switzerland: Springer.

Denning, D. (1998). Information Warfare and Security. 27(9), 1-2. Addison-Wesley Longman Ltd. Essex, UK

ENISA Threat Landscape Report. (2018). 15 Top Cyberthreats and Trends. Retrieved from https://www.enisa.europa.eu › publications › at_download › fullReport [accessed 4/11/2019]

Erickson, J. (2011). Hacking: The art of exploitation. San Francisco, CA: No Starch Press.

Farsole, A. A., Kashikar, A. G., & Zunzunwala, A. (2010). Ethical Hacking. International Journal of Computer Applications, 1(10), 14-20, Wardha, India.

Grabbosky, P. N. (June 2001). Virtual criminology, old wine in new bottle. SAGE Publications, London, Thousand Oaks, CA and New Delhi, Vol. 10(2), 243–249; 017405
Hadnagy, C. (2011). Social engineering: The art of human hacking. Indianapolis, IN: Wiley.

Harrison, R. (2004). Microsoft Solutions for Security: The Antivirus Defense-in-Depth Guide. Retrieved from https://documento.mx/preview/antivirus-defense-in-depth-guide-5c1166e496b7c [accessed 18.9.2019]

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defence informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research, 1(1), 80.

John Mariotti Quotes (Author of The Chinese Conspiracy). (n.d.). Retrieved from https://www.goodreads.com/author/quotes/1078971.John_Mariotti
[accessed on 18.9.2019]

Jordan, T., & Taylor, P. (1998). Sociology of Hackers. The Sociological Review,46(4), 757-780.

Kahate, A. (2006). Cryptography and Network security, 2003. Tata Magraw-Hill publishing Company Limited, Eighth reprint, India

Komar, B., Beekelaar, R., & Wetter, J. PhD. (2003). Firewall for Dummies (2nd ed.), Wiley Publishing Inc, New York.

Leeson, P. T., & Coyne, C. J. (2005). The economics of computer hacking. JL Econ. & Poly, 1, 511.

Levy, S. (2010). Hackers: Heroes of the computer revolution: 25th Anniversary Edition. Sebastopol, CA: O'Reilly.

Maiwald, E (2001). Network security: a beginner's guid*e*. McGraw-Hill Professional.

Mitnick, K. D., & Simon, W. L. (2011). The art of deception: Controlling the human element of security. John Wiley & Sons.

Ozalk, T. (2015). Attack Surface Reduction – Chapter 4. Retrieved from https://resources.infosecinstitute.com/attack-surface-reduction/#gref [accessed 20.5.2019]

Parker, D. (1999). Fighting Computer Crime. A New Framework for Protecting Information.

Ranum, M. J. (2014). Breaking Cyber Kill Chains. Tenable Network Security

Russell, R. (2002). Hack proofing your network. Rockland, MA: Syngress Media.

Ryan, R. M., & Deci, E. L. (2000). Intrinsic and extrinsic motivations: Classic definitions and new directions. Contemporary educational psychology, *25*(1), 54-67.

Saili Waichal, S., & Meshram, B. B. (2013). Router Attacks-Detection and Defense Mechanisms. International journal of scientific & technology, (2). Retrieved from http://www.ijstr.org/final-print/june2013/Router-Attacks-detection-And-Defense-Mechanisms.pdf [accessed 8/8/2019]

Satapathy, S., & Patra, R. R. (2015). Ethical Hacking. International Journal of Scientific and Research Publications, 5(6).

Schneier, B. (2011). Secrets and lies digital security in a networked world. John Wiley & Sons, Indianapolis, Canada

Shimeall, T., & Spring, J. (2013). Introduction to information security: a strategic-based approach. Newnes.

Sikorski, M., & Honig, A. (2012). Practical malware analysis: the hands-on guide to dissecting malicious software. no starch press.

Stallings, W. (2015). Computer security: principles and practice 3d edition/W. Stallings, L. Brown.

Sterling, B. (1993). The Hacker Crackdown: Law and Disorder on the Electronic Frontier Part.

Sucuri.net, Cryptocurrency Mining Malware. (2018). Trends & Threat Predictions. Retrieve from https://sucuri.net/documentation/Sucuri-eBook-Cryptomining-Malware.pdf [accessed 18/9/2019]

Sun, S. T., Wei, T. H., Liu, S., & Lau, S. (2007). Classification of SQL injection attacks. University of British Columbia, Term Project.

Tsu, S. (2017 translated). The Art of War. Arcturus Publishing Limited, London

Vokorokos, L., Baláž, A., & Madoš, B. (2015). Application Security through Sandbox Virtualization. 83-99. Retrieved from https://www.citationmachine.net/apa/cite-a-journal/manual [accessed 6/10/2019]

Yadav, T., & Rao, A. M. (2015, August). Technical aspects of cyber kill chain. In International Symposium on Security in Computing and Communication (pp. 438-452). Springer, Cham.

Prasad, S. T. (2014). Ethical hacking and types of hackers. International Journal of Emerging Technology in Computer Science Et Electronics (IJETCSE111, no. 2: 24-27.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973-993.

Shu, R., Wang, P., Gorski III, S. A., Andow, B., Nadkarni, A., Deshotels, L., ... & Gu, X. (2016). A study of security isolation techniques. ACM Computing Surveys (CSUR), 49(3), 50.

Mogensen, T. Æ. (2009). Basics of compiler design. Copenhagen, Denmark.

Smith, J. E., & Nair, R. (2005). The architecture of virtual machines. Computer, 38(5), 32-38.

Power, R., & Ford, R. (2009). Operating system fundamentals, North Atlanta
Arata, M. J. (2006). Perimeter security. McGraw-Hill. New York, America.

Pahnila, S., Siponen, M., & Mahmood, A. (2007, January). Employees' behavior towards IS security policy compliance. In 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07) (pp. 156b-156b). IEEE.

Tiwari, M. M., Kumar, R., Bharti, A., & Kishan, J. (2017). Intrusion detection system. International Journal of Technical Research and Applications, 5(2), 38-44.

Subhalakshmi Ganapathy (2018), The Absolute Guide to SIEM, Retrieved from
https://www.manageengine.com/log-management/the-absolute-guide-to-siem.pdf
[accessed 4/ 11/2019]

Viswanathan, A., & Neuman, B. C. (2009). A survey of isolation techniques. Information Sciences Institute, University of Southern California, America

Wahbe, R., Lucco, S., Anderson, T. E., & Graham, S. L. (1994, January). Efficient software-based fault isolation. In ACM SIGOPS Operating Systems Review (Vol. 27, No. 5, pp. 203-216). ACM.