Digital forensics investigations and network security issues in tracking the trails of cybercriminals

Digital Forensics Investigations and Network Security Issues in Tracking the Trails of Cybercriminals

1st Oyetunji Oyelakin
School of Computing and Eng
University of West London
London, United Kingdom
lhaking83@gmail.com

1st Abel Ofori-Yeboah
School of Computing and Eng
University of West London
London, United Kingdom
Abel.yeboah-ofori@uwl.ac.uk

2nd Aishat Ganiyu
School of Eng., Phys. and Math.
Royal Holloway University
London, United Kingdom
aishat.ganiyu.2021@live.rhul.ac.u

3rd Oluwole Oguntoyinbo
School of Computing and Eng
University of West London
London, United Kingdom
21516296@student.uwl.ac.uk

***Abstract*—The application of digital forensics investigations (DFI) and the legal implications in network security have become imperative due to increased connectivity and cyberattacks. The DFI process requires investigating computers and their associated media to determine if they have been used to commit a crime or gain unauthorized access. However, in a network environment, attackers can intercept, interrupt, modify content, and modify contents and fabricate the victims. Thus, it is imperative that these cyberattacks are considered from a legal perspective considering the challenges. The paper explores the digital forensics investigations process and its legal implications from network security to assist in determining indicators of compromise, attribution, and prosecution. The contribution of the paper is threefold. First, we explore DFI challenges from a network security perspective, including the legal and the standards. Secondly, we implement attacks on a network and use DFI tools such as Splunk to detect interruptions, modifications, and disruptions during the investigation process. Finally, we discuss some DFI challenges that impinge on national and international law during investigations and prosecutions and recommend improvement. The results show that the DFI process in the network security environment is relevant in detecting, preventing, and prosecuting these threats.**

Keywords—Digital Forensics, Network Security, Cyber Attack, Interception, Interruption, Modification, Fabrication

I. Introduction

The invincibility of cyberattacks has made the use of digital forensics investigations in network security grow exponentially since cyberattacks are inevitable [1]. Cybercriminals break into network systems in several ways to intercept, disrupt, alter, and falsify their victims' data. This leads to data theft, monetary losses, intellectual property theft, reputational harm, and mistrust. Digital forensics Investigations is the process of investigating computers and related media to ascertain whether they were used in a crime or to gain unauthorized access [2]. Digital forensic investigative jurisprudence is the framework a court of law uses to administer justice in the event of cyberattacks and cybercrimes. The legal discipline known as "cyber jurisprudence" connects philosophy and science. It considers the evolving nature of digital and cybernetic assets and any potential legal ramifications. To be admitted in court, digital forensics investigations must meet jurisdictional norms and legal requirements and be genuine, accurate, and convincing to jurors. In digital forensic investigations, evidence is legally binding and typically meant for the court [2]. The three fundamental principles of information security, that is confidentiality, integrity, and availability, are generally violated by certain behaviors, which are considered risks to cyber security. The paper discusses how cybercriminals could breach a secured network and carry out interruption, modification, and fabrication. Figure 1 discusses a network system setup and the various vulnerable spots that cybercriminals could exploit for the DFI process.

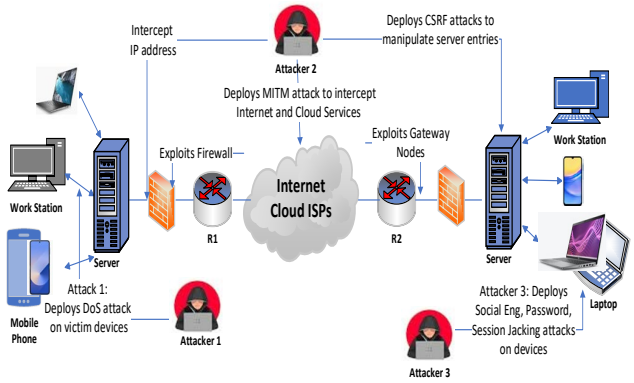

Fig 1. Network Security and Cyberattack Vectors

However, various challenges exist when addressing DF investigations and NS that impact victims. These include inadequate control mechanisms, risk assessment, security misconfigurations, and a lack of third-party auditing, which leads to penetrations and manipulations, thus requiring digital forensics investigations[1].

The paper explores the digital forensics investigations process and its legal implications from network security to assist in determining indicators of compromise, attribution, and prosecution. The contribution of the paper is threefold. First, we explore DFI challenges from a network security perspective, including the legal and the standards. Secondly, we implement attacks on a network and use DFI tools such as Splunk to detect interruptions, modifications, and disruptions during the investigation process. Finally, we discuss some DFI challenges that impinge on national and international law during investigations and prosecutions and recommend improvement [18]. The results show that the DFI process in the network security environment is relevant in detecting, preventing, and prosecuting these threats.

II. State of the Art

This section discusses the state of the art and related literature in network security and digital forensics investigations. For instance, [3] asserts that the prevalence of computer or cyber-related criminal attacks in today's technologically advanced culture has increased the need for and use digital evidence in courts to prosecute criminals. However, there are challenges in law and ethical issues that are crucial facets of investigations but have received less focus. Maheshwari and Sharma proposed a new approach to

Combating cybercrime and discussed several digital forensics techniques and procedures that aid in investigations. The study looked at several cyber forensics technologies and techniques that help improve investigations by creating hard, admissible evidence in cases of cyberterrorism, cyberstalking, spam, and other types of cybercrime [4]. Further, [2] posits that for a case to be admissible at court, digital evidence and DFI jurisprudence must be applied in examining the issues of authenticity, accuracy, correctness, and completeness to avoid complexities in evidence gathering. The author contends that for any evidence to be accepted in court for prosecution, it is crucial to follow legal procedures when gathering evidence at a digital crime scene. However, countless cases have been deemed inadmissible in court due to insufficient evidence gathered and maintained for accuracy, validity, and completeness. Research on the systems, methods, and taxonomy related to network attacks was done by [5]. An attacker may use software services to obstruct routine network operations by exploiting gaps, flaws, and misconfigurations. Attackers could use open-source tools on a host to launch a successful attack, find security gaps, and gather vital information. However, the authors feel that their applicability is restricted. The goal of network defense is to minimize unusual network traffic. While being observed, defenders typically do not disguise their identities, whereas attackers do.

Additionally, [6] conducted a survey of attacks, defence, and security mechanisms in wireless sensor Networks." According to the authors, the main goal of the research is to investigate various security attack types, their effects, and defense mechanisms in Wireless Sensor Networks, which are susceptible to security assaults and threats because of their features and constraints. Several factors are considered when identifying and categorizing security attacks, including the network layer where the attack occurs, network security fundamentals, the location of the attacker, data transmission, various protocol stack layers, etc., as well as the various security measures that can be applied to defend against multiple attacks. In their analysis of network layer assaults using various survey techniques, the authors concluded that while security attacks are classified according to the various network tiers in which they occur, they are not classified as such. All tiers of the protocol stack are susceptible to some security threats, although there are several ways to defend against them.

Further, [1] explored the application of cryptography in network security for cyberattack prevention by discussing critical factors in guaranteeing the security of information flows by using cryptography and how different encryption techniques are used to encrypt and decrypt data transmitted over the network. In cryptography, secret keys, public keys, and hash functions are used to guarantee data confidentiality, integrity, authentication, and non-repudiation in a secure network environment. The study examined how applied cryptography theories can be used to safeguard information and network systems. compared a range of cyberattacks against several encryption protocols, including symmetric, asymmetric, and hashing functions. Abel et al. proposed a relativism DFI model from existing models and propose a model that will improve the DFI process from the result of the evaluation with inference from international standards [18].

Many encryption algorithms and network systems have been developed and discussed in the literature including [3] [4] [6] [7] [8] [9] [10] [11], but few researchers have taken advantage of the discrepancy. Furthermore, due to significant security flaws, the use of digital forensic investigation tools for security has rapidly increased in the cutthroat technology market. Technologies for digital forensic investigation are necessary to defend networks from deliberate attacks. The fragility of these systems has been well acknowledged, and network information security challenges have been thoroughly investigated. However, in the event of a security breach, it is crucial to be aware of the potential effects of digital forensics, the protocols or procedures that should be followed during an investigation, the tools and techniques that an investigator should use, and the potential locations and methods for collecting forensic data. There are gaps in literature since forensic analysis is typically guided by legal framework, intuition, scientific technique and experience rather than a systematic or. This study aims to close these gaps by focusing on interception, interruption, modification, and fabrication issues.

A. Network Attacks

A computer network asset is the target of an attack if it is attempted to be stolen, destroyed, altered, or used illegally. There are two types of attacks: active and passive. The integrity or availability of the network resource is threatened when an attacker tries to manipulate system resources or their functioning [1] [12]. The four network attacks are interception, interruption, modification, and fabrication.

1) Interception:

Figure 2 discusses how an attacker can penetrate a network and intercept communication on the network. A method for gaining access to information that the attacker is not permitted to see is called interception [6].This form of penetration aims to compromise the information's confidentiality. There's a chance the attacker is a person. Two examples are unauthorized downloading software files and hacking a computer or program to obtain data across a network. An unauthorized entity accesses data, and that indicates a breach of confidentiality. Examples of such interception lead to data capturing on the network through wiretapping, unlawful copies of data or programs, and IP Snooping.

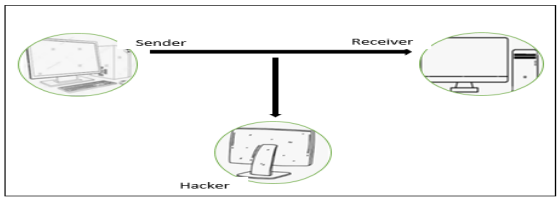

Fig. 2. Interception Attack on a Network

2) Interruption:

Figure 3 shows how an attacker can interrupt communication between two parties in a network environment. This attack occurs when one or more systems' communication channels are obstructed. The unauthorized user attack renders the currently in-use systems useless, causing system inefficiency. An interruption attack is an attack on accessibility. When it occurs, system assets are either lost, rendered unavailable, or rendered useless, which could translate into the destruction of hardware, wireless communication disruption, or removal of file management software [6].

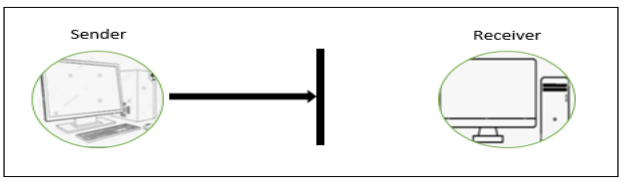

Fig. 3. Interruption Attack on a Network

3) Modification:

Modification attacks refer to attempts to modify the intercepted data authorized. This kind of assault involves the attacker gaining access to an object and tampering with it. Anywhere that information is stored is susceptible to this kind of attack. Data transmission via the internet could likewise be

intercepted using this technique. This kind of assault seeks to compromise the accuracy of the data. Integrity is at risk when an unauthorized person has access to an asset and tampers with it. Examples include distributing software in a new way and altering the content of network connections [1] [6].

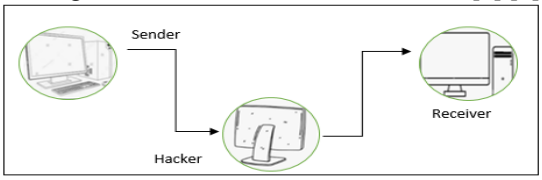

Fig. 4. Modification Attack on a Network

4) Fabrication:

Figure 5 shows an attacker's attempt to access the system using pirated products without authorization. . Data integrity is compromised because of this kind of attack. Usually, an unauthorized party introduces a fake item into the system. Authenticity is challenged, and this is sometimes referred to as impersonating. Two examples include adding records to a file or delivering false information over a network [6].

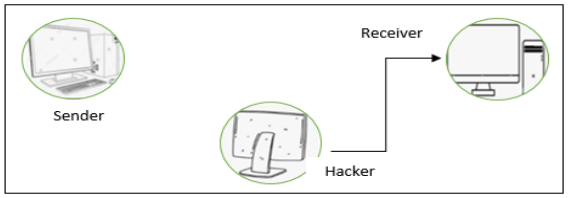

Fig. 5. Fabrication Attack on a Network

B. Network Security And Attacks

Network security refers to measures taken to prevent unauthorized use, abuse, alteration, or denial of the use of information, facts, data, or capabilities [13]. Data could be compromised without security safeguards, and controls may be changed to damage or destroy the data or the network. Many individuals rely on the Internet for much of their work, social lives, and leisure pursuits. Additionally, some people attempt to damage our online-connected computers, invade our privacy, and disable internet services. In the area of computer networking, network security has grown in importance due to the intensity and scale of recent assaults as well as the possibility of new, devastating future attacks. The networks and data are susceptible to any of the attackers.

C. Digital Forensic

Digital forensics investigation is a process of investigating computers and their associated media to see if they have been used in criminal activity or for illegal purposes [2] [14]. The goal of digital forensics is to conduct forensically sound digital media analysis to identify, protect, recover, analyze, and present information facts and opinions to the court of law, law enforcement, corporations, and individuals. Digital forensics could also be defined as "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for facilitation or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations [2].

To facilitate or further the reconstruction of events determined to be criminal or to help foresee the unauthorized actions shown to be disruptive to planned operations, digital forensics is the use of scientifically derived and proven methods towards preservation, collection, validation, identification, analysis, interpretation, and presentation of digital evidence derived from digital sources. The reliability of digital evidence is a crucial component in digital forensics. Cell phones, digital fax machines, computers, digital audio, and digital video are all examples of digital evidence. Thus, evidence must meet the requirements of the legal system for reproducibility, non-interference, and minimization [14]. DFI has seven linear phases involved including Identification, Preservation, Collection, Examination, Analysis, Presentation, and Decision. The Digital Forensic Investigation Process [14] [15].

D. The Need For Digital Forensic Investigation Model

According to [14] there is a need to understand the digital forensic investigation process because the following are directly affected by how digital forensic science is applied:

- The avoidance of additional malicious actions being taken against the intended "target. "
- The accurate identification of the responsible parties after a successful investigation of the circumstances that gave rise to the crime.
- Punishing the criminals who committed the crime.
- Improving the present preventative measures to ensure that such an incident doesn't happen again.
- enhancing corporate security specialists' benchmarks to protect their respective corporate networks.
- Everyone's "plug" "may raise their understanding of existing vulnerabilities and defenses in this digital environment.

1) Splunk software For data analysis

Splunk is a piece of software that is used to search and examine machine data. This machine data may originate from online applications, sensors, gadgets, or user-generated data. Analyzing the logs produced by various processes meets the demands of the IT infrastructure. However, proper data modeling can also evaluate any structured or semi-structured data. Field separators, data type recognition, and search process optimization are all built-in features. Additionally, data visualization for the search results is provided. In addition to producing graphs, alerts, dashboards, and visualizations, it captures, indexes, and correlates real-time data in a searchable container. Splunk offers simple access to data throughout the enterprise for quick diagnosis and solutions to various business issues [16] such as SIEM (Security Information and Event management). The Splunk Structure includes Search Head, Indexer, and Forwarder are the three critical parts of the Splunk Enterprise SIEM architecture. Each plays a distinct role in developing the entire SIEM solution.

- **Indexer:** This tool analyzes logs and stores them in indexes to facilitate data analysis and searches.
- **Search Head**: When the data has been indexed, the Search Head allows Search Processing Language (SPL) to query for various occurrences. Additionally, it is used to make multiple reports, charts, and dashboards.
- **Forwarders** Gather data and send it to an indexer or another forwarder. They have a negligible impact on the operating performance of the system on which they are installed and use very few of its resources.

III. Approach

This section discusses the approach we used for our implementation. We used a digital forensics investigation process. To conduct a network forensic investigation, we would gather information and investigate various existing standards and procedures. Network forensics aims to identify cyber-attack's origins and effects by capturing, recording, and analyzing network traffic and audit files. Figure 6 illustrates the DF investigation process used [2] [18].

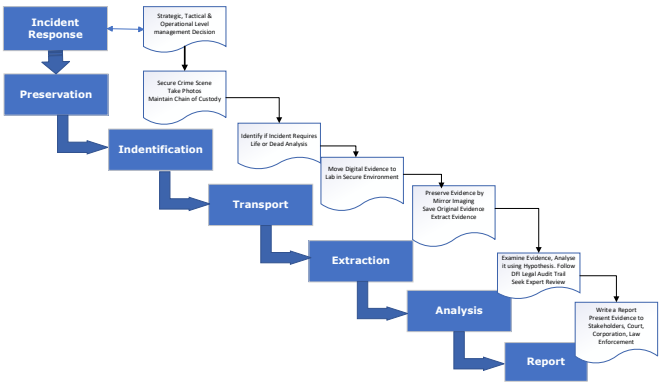

Fig. 6. Digital Forensic Investigation Process Model (Yeboah-Ofori 2020)

A. Network Environment Designed for the Cyberattack

The network diagram is fundamental and must be well organized. Each element of our network architecture will be described using the GNS3 design tool. Our network is set up realistically because it accurately mimics a real network environment using VLANs, a variety of VMs, including Kali (to run the attacks) and Splunk (to investigate those attacks), as well as our Active Directory Server, Rsyslog Server, Web Application (DVWA) Server, Firewall-Router, Admin, and Users.

B. DFI Lab Set Up

We will set up our virtual machines and use Kali Linux and the Burp suite to simulate three attacks on our network. In addition to helping to characterize attacks, the next generation of SIEM may monitor user behavior, business activities, and system performance. Splunk may, therefore, be used to analyze and gather data regarding attack simulations, the attack strategies and tactics deployed, and the duration of the assault. Due to Splunk, businesses can easily prevent security breaches and have financial peace of mind.

C. Choice of Tools, Simulation Attacks, and Results Checked on Splunk

In this section, we will choose the attack simulation and the choice tools that we will be using to observe the results of our investigation on Splunk. Here are the attacks and tools:

- Brute force attack using burp suite.

The Burp Suite is a collection of tools for web application penetration testing. Professional web app security researchers rely on it the most. This tool can perform a login brute force attack. It comes with Kali Linux already installed. First, we'll ensure Burp is set up correctly in our browser. Using a simulation login page from the "Intruder" training tool, this simulation assault shows how to bypass authentication.

- Dos attack using Hpin3:

A fundamental method of preventing access to network services is a denial of service (DOS) attack. This attack involves sending the victim an excessive number of or an overload of large packets. The target can't manage attackers, and the server can't serve legitimate users by sending many packets (in our example, SYN). Since the tool hping3 enables us to transmit modified packets and regulate their size, amount, and fragmentation, we will utilize it to overwhelm the target and get around or through firewalls.

- Port Scan Attack using Nmap:

A Port Scan is a technique widely employed by hackers to discover open entry points or vulnerabilities in a network. The Nmap network reconnaissance and security auditing program, introduced in 1997, is one of the most straightforward and well-liked cybersecurity tools available today. Nmap will be utilized since it can be used to identify the target's port states and detect running services during port scanning, as well as results and recommendations on how to prevent those attacks.

IV. Implementation

This first section will describe the network put in place to run our attacks and to investigate the network. We created a Local Area Network (LAN), utilizing a star topology, using various components as follows:

VLAN: Virtual Local Area Network is one or more local area networks that can be combined to form a bespoke network called a VLAN. It allows for combining and integrating a collection of devices spread across several logical networks. As a result, a virtual LAN that is managed similarly to a physical LAN is created. VLANs limit user access by dividing their network into various segregated LAN segments (VLAN Users, VLAN Admin, VLAN Active Directory, VLAN SIEM (Splunk), Rsyslog, and a DMZ).

Burp suite in our Kali Linux is a set of tools used for penetration testing of web applications. This tool will allow us to intercept packets and run a brute-force attack in our scenario. Figure 7 displays our Network Architecture:

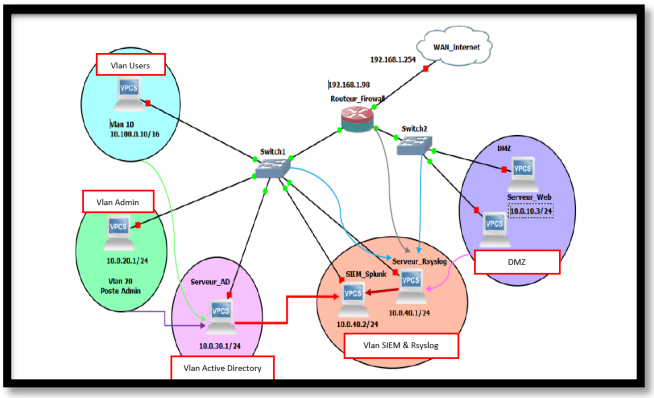

Fig. 7. Network Architecture

A few examples of correlation scenarios would be performed on the above network. Also, the attack that is intended to be identified will be highlighted, and the details of the logging elements that provide the source data will be explained, as well as how they will be correlated on our Splunk SIEM. SPLUNK gives real-time visibility into the condition of the physical and virtual IT infrastructure and manages events and alerts. The platform also offers application and service monitoring. Attackers frequently look for open ports as starting points to launch network attacks. A port scan request is TCP or UDP traffic sent to a range of ports.

A. Description Port Scan Attack

A network scanner like Nmap ("Network Mapper") could investigate problems in a network. It determines which systems are network accessible, as well as what services (applications and versions), operating systems, and filter types are available. This technique is known as the "Port Scan Attack." Hackers widely use a port scan strategy to discover holes or weak points in a network. Using a port scan attack, cybercriminals can find open ports. It is crucial to keep in mind that port scanning by network administrators to generate vulnerability maps that must then be patched is crucial. Arp-scan, Nmap, Zenmap, and Angry IP Scanner stand out among the many port scanning programs.

B. Attack 1: Port Scan Attack Scenario on Rsyslog Server

On Kali Linux, Nmap is open-source software that uses erroneous TCP packets with various flags set to try and fingerprint the open ports, operating system (OS), and versions of the targeted network. In our scenario, an attacker connected to our local network can scan the Rsyslog server by typing this command: #sudo nmap sO 10.0.40.1, as shown in Figure 8. This option—sO show all open ports on our Rsyslog.

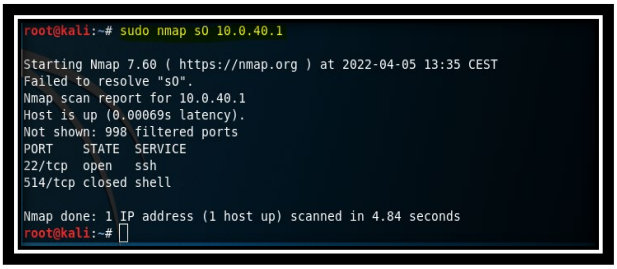

Fig. 8. Port Scan Attack on our Rsyslog server

Figure 7 shows that our Rsyslog has 998 filtered ports, which leads us to believe that our firewall is configured correctly and that only SSH port 22 appears to be open. Thus, an intruder can then perform a brute-force attack to get credentials to access our Rsyslog server.

C. *Results on our SPLUNK*

Network investigations have been conducted using the Splunk tool to check for port scan attacks on the network. To make data analysis and search more accessible, the Indexer tool in Figure 8 analyses logs and stores them in indexes. We can view the firewall logs on our Splunk after adding the index="firewallog" parameter. Figure 9 indicates that although the scan was denied by our Firewall (UFW BLOCK), we can still see multiple TCP Packets attempting to contact our Rsyslog (10.0.40.1) based on our investigation. The Splunk tool's red-highlighted area denotes TCP packets trying to connect to our server. The findings demonstrate that real-time port scan attacks can be detected and analyzed in Splunk for security controls.

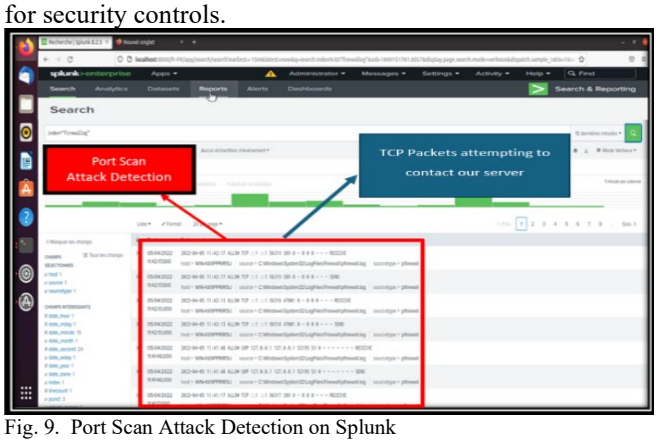

Fig. 9. Port Scan Attack Detection on Splunk

D. *Recommendations to prevent DOS Attacks*

- Filtering packets is one of the steps required to stop a SYN Flood attack. Incoming packets' headers are examined by packet filters, which put them to the test against a set of rules.
- Set up a firewall. Firewalls add an additional line of protection because they are specifically made to manage high traffic volumes. Firewalls can be set up to transmit an acknowledgment to the host or the SYN-ACK to the attacker.
- Include intrusion detection and prevention systems. These gadgets give the network an additional layer of security, like firewalls. They keep a close eye on the network's activity.
- Guard the host. Configuring the TCP order book can avoid a SYN denial of service flood.
- Gather NetFlow records and data.

E. *Description of a Brute Force attack*

A brute force attack entails a series of trial-and-error steps with the ultimate goal of succeeding in deciphering a password, login, hidden web page, or encryption key. Even though this attack strategy is dated, hackers still use it frequently and significantly. Cracking a password can take anything from a few seconds to several years, depending on its length and complexity. So, we'll employ the Burp Suite tool. We also have automated technologies at our disposal to defend against brute force attacks (e.g., Brutus, Medusa, THC Hydra, Ncrack, John the Ripper, Air-crack-ng, and Rainbow). function, they may be able to own the entire application.

F. *Conceptual Model of Credential Stuffing Brute Force Attack*

Figure 10 shows how to deploy the credential Stuffing Brute Force Attack on our network.
The attacker first performs a port scan attack to identify which packets are susceptible to being intercepted. The "Intruder" option can be used to automate brute force attacks on an online site's login page, fuzz the web application to detect vulnerabilities, and use a tool like the Burp suite. In our scenario, Intruder will also let us continually try to log into different servers. Credential stuffing attacks can have various adverse effects and risks, including releasing credentials on the dark web as payback, for corporate espionage, or to steal data or identities.

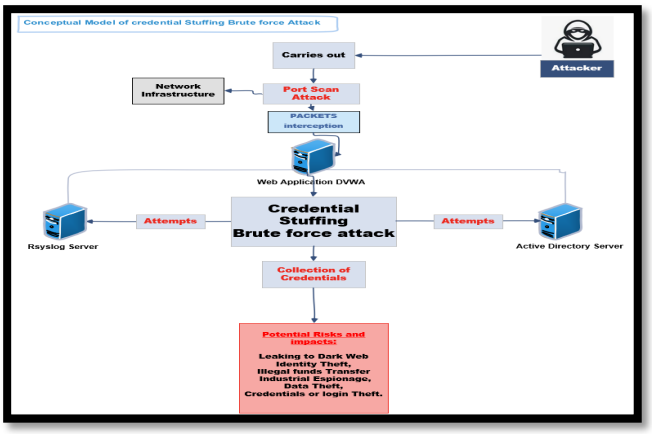

Fig. 10. Conceptual Model of Credential Stuffing Brute Force Attack

We will set up DVWA as a PHP/MySQL web application. The main goal is to aid security professionals in testing their skills and tools in a legal environment. In our DVWA, we go to the brute force tab, where the user's password is guessed as "admin." In the Burp Proxy tab, we will ensure "Intercept is on" and visit the login page of the application we are testing in our browser. Figure 11 shows that we have successfully captured the packet via Burp Suite with the username admin and the password. So, we will now be able to conduct a credential stuffing brute force attack that tries a combo username-password on our web application, which can then be used on our Rsyslog or Active Directory server.

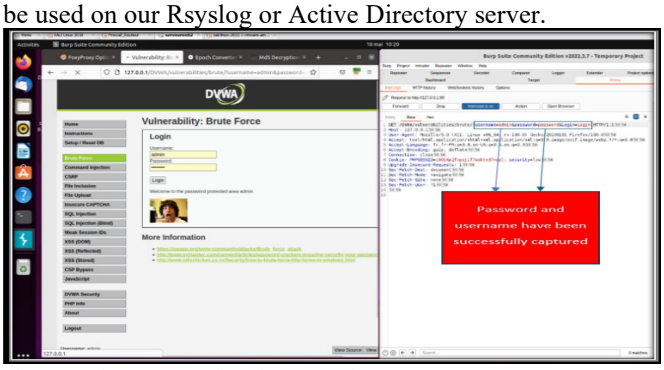

Fig 11. Packets Interception via Burp Suite

Figure 12 shows the setup our environment for the investigation. We use the Hydra tool, that allows us to perform various kinds of brute-force attacks using wordlists. On our Kali Linux machine, we will retrieve the token and the cookie from our original packet interception on burp suite; then we type this command in our hydra tool to crack the password list:

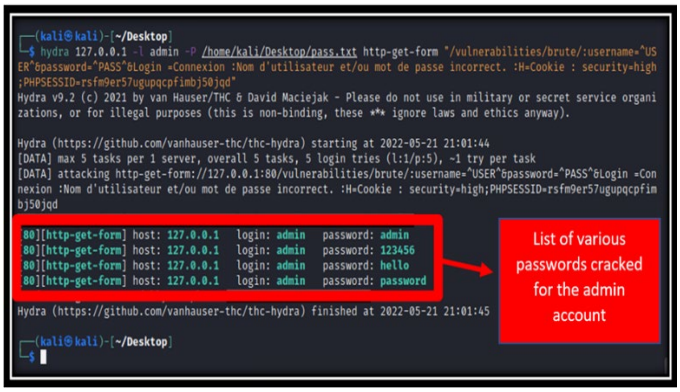

Fig. 12. Commands on Hydra

After getting the list of passwords, we will inject them into the Intruder module, which allows us to repeat an action several times (for example, try our several passwords collected on Hydra). Consequently, we blend outside means with our logical guesses to attempt a break-in via burp suite. In Figure 13, in the intruder module, we choose the variable “payload” we want to test. The word "password" is highlighted in orange on the screen because it is the one we want to test.

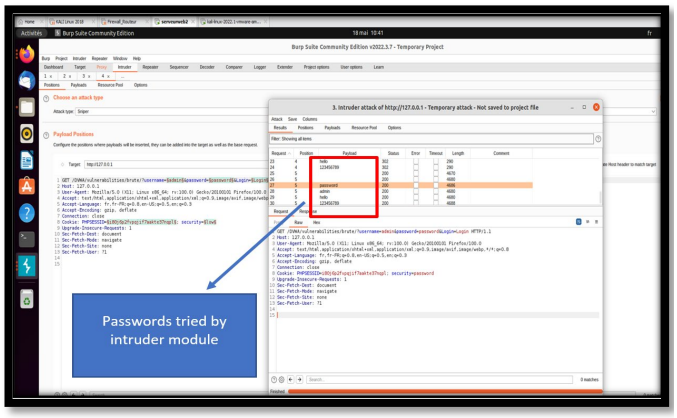

Fig. 13 Intruder Option on Burp Suite

Finally, in Figure 14 we analyze the password by its length and test it live via the render option on Burp Suite. As shown on the welcome screen, the correct password is the password.

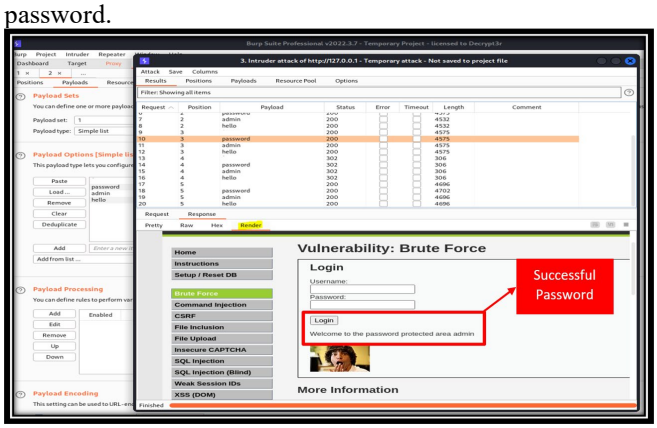

Fig. 14. Welcome screen after trying the correct password

G. *Results for Using Splunk for Digital Forensic Investigations*

The Splunk tool has been used to conduct network investigations to detect credential stuffing and brute force attacks on our network. To make data analysis and search more accessible, the Indexer tool analyzes logs and stores them in indexes. We can retrieve the web server DVWA logs on our Splunk after adding the index="auth.log" parameter. Based on our investigation, Figure 15 indicates the number of failed attempts that the attacker has made to exploit the system by deploying a credential-stuffing brute force attack. The area highlighted in red in the Splunk tool indicates that there have been numerous unsuccessful attempts on our DVWA Server to extract credentials using our admin account. The results show that credential stuffing attacks can be captured in Splunk in real time for detection and analysis for security controls.

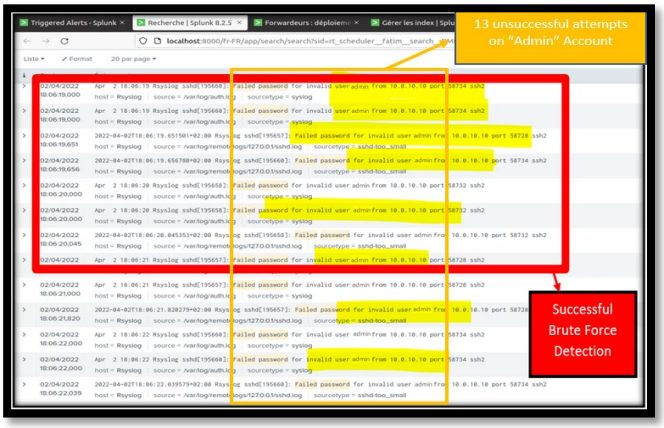

Fig. 15. Failed Attempts on Splunk

H. *Recommendations to prevent Brute Force Attacks*

- System administrators must protect their system passwords using strong ciphers, like 256-bit encryption and a strong password policy.
- Administrators must also use a salt value and a hash or add a random letter string to password hashes to randomize them.
- Administrators can also set up an intrusion detection system that recognizes brute force attempts, uses a CAPTCHA, and mandates two-step authentication.
- The likelihood of brute force attacks is decreased by limiting the number of attempts.
- Implement a security campaign against phishing and social engineering.
- Make use of Web Application Firewalls (WAF).

Figure 16 displays IoCs for the three attacks: To conclude this phase, after our investigation on Splunk, we gathered all the information about our three suspicious attacks to create our IoC with the Mandiant IoC tool, an editor for Indicators of Compromise (lOCs). Information discovered on a computer that shows a network's security has been hacked is referred to as an "Indicator of Compromise" (IOC).

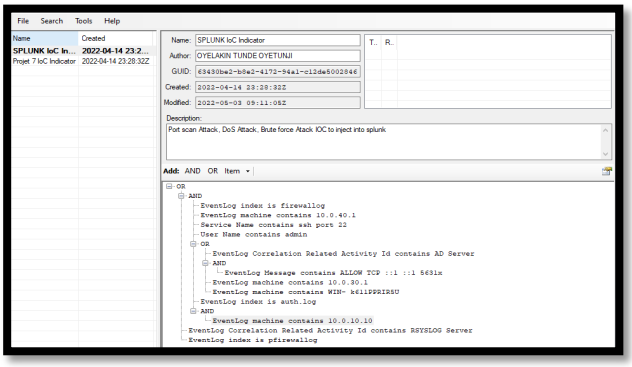

Fig. 16. Indicators of Compromise

After developing our IoCs, we re-inject them into Splunk to recognize and predict new attacks. The ultimate goal of gathering this data is to produce "smarter" programs that can later identify and quarantine questionable files. The Splunk Enterprise Security Threat Intelligence framework gathers, prioritizes, and manages various threat intelligence streams. Select Configure > Data Enrichment > Intelligence Downloads from the menu below. Then we checked out the Threat Intelligence Uploads menu and manually pasted threat intelligence on an as-needed basis, such as Figure 16.

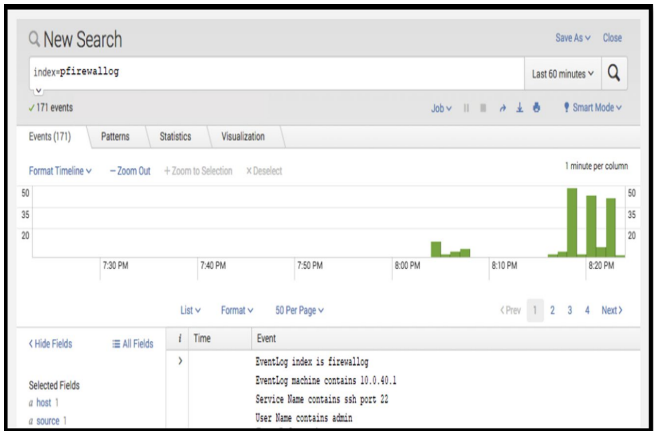

Fig. 16. Threat Intelligence uploads

V. Findings and Recommendations

This section examines the findings and suggestions from the diverse attacks' simulation performed and the CF investigation conducted on the Splunk tool during the implementation phase. First, we created a lab infrastructure that is as similar to a production environment as possible. This study used attack simulation on our local network, which provided a valuable method for identifying and resolving particular network issues. Splunk was chosen because it is an analytics-driven SIEM platform that gathers, examines, and correlates massive amounts of network and other machine data in real time. It also helps us keep track of and browse logs. It correlates and indexes data into a searchable container, enabling the creation of alerts, reports, and visualizations.

The first attack was a Port Scan Attack on our Rsyslog server using Nmap, a potent tool capable of carrying out several scans, including port scans and OS fingerprinting. Initially, the command nmap -sO 10.0.40.1 was used to scan the open ports on our Rsyslog server. According to the scan results, our Rsyslog has 998 filtered ports, and only SSH port 22 appeared to be open, which allowed us to conclude that our firewall appeared to be correctly configured. As a result, a hacker can use a brute force attack to obtain login information for our Rsyslog server. We could see the firewall logs on our Splunk after adding the index="firewallog." Based on our investigation, We have demonstrated that even though the scan was rejected by our firewall (UFW BLOCK), we could still notice several TCP Packets trying to contact our Rsyslog (10.0.40.1). It is advised not to enable unnecessary ports, to use tools to check open ports, to use a firewall and IPS to prevent or detect intruders on the network. Finally, to constantly update all available patches to fix any issues that may already be present to prevent a port scan attack.

The second attack was a DoS Attack on our Active Directory server using the open-source testing tool Hping3 on Kali Linux, which manages fragmentation and also transfers encapsulated packets in a quiet mode. (Tigner et al., 2021). Due to the diversity of DoS attacks, the attacks in this study were mainly modeled using TCP flooding to reduce the complexity of the generated data. We have entered the following command on port 21 of our Windows server (AD): *hping3 -c 500 -d 120 -S -w 64 -p 21 -flood -rand-source 10.0.30.1*. This command will send a SYN flag to start a TCP connection as quickly as possible without presenting any responses. To swiftly identify assaults and anticipate new threats, we analyzed the data generated by the attacks using the Splunk platform. We could see the firewall logs on our Splunk after adding the index="pfirewallog" parameter. The traffic results show how the network has been inundated with multiple TCP packets originating from various faked IP addresses and displaying the filter: ALLOW TCP::1 ::1 5631x. This attack deliberately depletes the site's resources, preventing authorized users from accessing our Active Directory Server. Configuring a firewall and adding intrusion prevention systems IDS/IPS to gather NetFlow data and logs are just a few of the activities that must be taken to prevent a SYN Flood assault.

Further, the final attack performed was a brute force on our Web server DVWA using Hydra and the Burp suite. DVWA was used because it is a PHP/MySQL web application created to assist security experts in testing their knowledge and equipment in a legal setting. Testing the brute-force attack on this server would be easier in our scenario. A brute force is used to decode login credentials, passwords, and keys. The goal of brute force attacks is to be the easiest, least expensive, and most direct method of accessing a website. We went to the brute force tab in our DVWA, where the user's password to guess would be "admin." We checked that "Intercept was on" in the Burp Proxy tab and navigated to the login page of the application we tested in our browser. After using the burp suite to capture the connection successfully, we conducted a brute-force attack using credential stuffing that tries a username-password combination on our web application that can subsequently be utilized on our Rsyslog or Active Directory server. First, we used the open-source Hydra tool in Kali, enabling us to carry out various brute-force attacks using wordlists. As illustrated in Figure 10, we entered the command into the Hydra tool to break the password list after retrieving the token and cookie from our initial packet interception on the burp suite. After obtaining the list of passwords, we injected them into the Burp Intruder module, which is used for automated assaults, including brute-forcing login pages for online applications, dictionary attacks, and fuzzing the web application to uncover vulnerabilities. The intruder option allowed us to find the correct password. Splunk could display the results now that the Active Directory server logs have been included in indexes. According to our investigation, we have shown how often the attacker tried to use a credential-stuffing brute-force assault to exploit the system. The findings demonstrate that real-time Splunk capture of credential stuffing assaults for detection and analysis of security policies. To prevent credential stuffing brute force attacks, System administrators should make sure that their system passwords are encrypted with strong ciphers, such as 256-bit encryption, a strong password policy, salt the hash, and possibly require two-step authentication.

The study has demonstrated that to handle an attack properly, the type of attack must first be determined, and a suitable handling mechanism must be selected. Therefore, network investigation is required to determine how to take preventative measures to minimize damage, such as using IoCs and what response strategies to employ during an assault. Using Splunk made capturing, searching, and analyzing log data more accessible in real-time. Security events can be discovered by analyzing logs as well as numerous other sources of system information. A log file, which describes the events that have taken place in the application's environment and the server on which it runs, is an essential piece of data. We could pinpoint the three attacks on these systems by analyzing and comparing this data. The experimental findings contributed to a better knowledge of various attack types and developing a warning system for security issues. This proved that the suggested methodology revealed information about our network's security under attacks.

VI. Conclusion

This study shows the usefulness of digital forensic tools such as Splunk (SIEM tools) in predicting network issues .(Modification, Interception, Interruption, and Fabrication). In the first phase, we designed and configured a network that could prevent problems using firewalls and other mechanisms

such as VLAN, DMZ, and the deployment of Splunk. During the second phase, Port scan, Brute Force, and DoS attacks were run on our locally designed network to determine if the network configuration was adequate to prevent these attacks and to test Splunk's ability to detect security breaches in a timely manner. It was shown that the correct application of Splunk helps analyze significant issues that occur in real-time on the network. After successfully implementing the network and carrying out different assaults on the networks, various security measures were suggested for implementation to help strengthen our networks further. This work demonstrates the usefulness of assault simulation and elaborates on a Splunk-based digital forensics investigation. Moreover, a response model and prediction technique were implemented, allowing intelligence collection to anticipate the results.

The attacks that Splunk identified are discussed in depth, along with an introduction to network investigation, digital forensics tools, and several potential network attacks. How to protect their network and stay on top of attacks. This experiment also illustrated how networks or systems for digital forensics could be successfully tested using free and open-source software such as DVWA, Kali Linux, Hydra, Nmap, Hping3, and Burp-suite. Additionally, we've established a secure network to monitor activity for irregularities and practice assaults. These preventative and proactive steps will help followers use and develop methods for investigating cyberattacks.

Table 1 discusses the challenges of tracking the trails of cybercriminals have been challenging due to the invincibility nature of cyberattacks, the changing threat landscape and the changing attack surface. We trust that implement the recommended coordinated approaches, including legal integration, expertise and applying standard DFI model during investigation process. We recommend Afripol, that could potentially formulate policies in cyber security and digital forensics from Africa perspective.

Future work will consider challenges in exploiting cryptographic algorithms on digital logs during evidence extraction. We will further explore Afripol concepts.

Table 1: Challenges of Tracking the Trails of Cybercriminals

Factors Impacting DFI	Cyber Crimes	DFI Challenges	Recommendations in tracking the trails	Standards
Complex Cryptography Algorithms	Criminals exploit encryption algorithms on network systems, VPN, Blockchains, ToR systems	Having required tools to investigate crimes in VPN and ToR environment	Lack of expertise and understanding of the Tactics, Techniques and Procedures used by criminals.	ISO/IEC 27042 provides a comprehensive guide to ensure that tools, techniques, and methods applied
Advance Persistent Attacks	Criminals from nation states are deploying sophisticated APT attacks on other nations	Investigating life systems from nation states is unlikely as criminals	Investigators and law enforcement agencies having challenges with global legal and jurisdictional laws	ISO/IEC 17020 and 17025 ISO/IEC 27043 provides guidelines for pre-incident to post-incident preparations
Deep and Dark Web Crimes	Cybercriminals are deploying botnet attacks, and spoofing exploits to exploit the deep web cryptosystems	Understanding Cyberattacks, cybercrimes and forensics nature in crime scene investigations	The use of pseudonyms to transfer monies globally and hide their trails.	ISO/IEC 27037 is designed for incident responses. To maintain the integrity and authenticity of digital evidence
Jurisdictional Laws	Nation States have their Cyber Crime Groups such as APT28, APT29	Coordinating jurisdictional laws across nations to track the trails of cyber criminals	Proper global coordination of resources among agencies, cyber threat information sharing and expertise	Agencies such as Interpol, Europol, ACPO, CEE, ILAC and other. We recommend Afripol

REFERENCES

[1] A. Yeboah-Ofori, C. Agbodza, F. Opoku-Boateng, I. Darvishi and F. Sbai, "Applied cryptography in network systems security for cyberattack prevention," in *2021 International Conference on Cyber Security and Internet of Things (ICSIoT)*, 2021.

[2] A. Yeboah-Ofori, "Digital Forensics Investigation Jurisprudence: Issues Of Admissibility Of Digital Evidence," *Journal of Forensic, Legal & Investigative Sciences.,* no. 6, pp. 1-8, 2020.

[3] M. Hewling, "Digital forensics: an integrated approach for investigating cyber/computer related crimes," University of Bedfordshire, 2013.

[4] S. Maheshwari and N. Sharma, "Cyber Forensic: A New Approach to Combat Cyber Crime," *Acclaims,* vol. 15, pp. 2,4,6, 2021.

[5] N. Hoque, M. Bhuyan, R. Baishya, D. Bhattacharyya and J. Kalita, "Network attacks: Taxonomy, tools, and systems.," *Journal of Network and Computer Applications,* no. 40, pp. 307-324, 2014.

[6] S. Biswas and S. Adhikari, "A Survey of Security Attacks, Defenses and Security Mechanisms in Wireless Sensor Network.," *International Journal of Computer Applications.,* no. 131, pp. 28-35, 2015.

[7] J. Andress, The basics of information security: understanding the fundamentals of InfoSec in theory and practice, Syngress, 2014.

[8] U. Karabiyik, N. Celebi, F. Yildiz, J. Holekamp and K. Rabieh, "Forensic analysis of scada/ics system with security and vulnerability assessment," in *ASEE Annual Conference & Exposition.*, 2018.

[9] B. Sharma, M. Joseph, B. Jacob and B. Miranda, "Emerging trends in digital forensic and cyber security-an overview.," *2019 Sixth HCT Information Technology Trends (ITT),* pp. 309-313, 2019.

[10] K. Sharma, M. Makino, G. Shrivastava and B. e. Agarwal, "Forensic investigations and risk management in mobile and wireless communications.," 2019. [Online].

[11] P. Murthy and V. Nagalakshmi, "Database Forensics and Security Measures to Defend from Cyber Threats," in *3rd International Conference on Intelligent Sustainable Systems (ICISS)*, 2020.

[12] N. Mangrulkar, A. Patil and A. Pande, "Network Attacks and Their Detection Mechanisms: A Review," *International Journal of Computer Applications,* vol. 90, no. 9, 2014.

[13] P. Murthy and V. Nagalakshmi, "Database Forensics and Security Measures to Defend from Cyber Threats," in *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, 2020.

[14] A. Agarwal, M. Gupta, S. Gupta and S. Gupta, "Systematic digital forensic investigation model," *International Journal of Computer Science and Security (IJCSS),* vol. 5, no. 1, pp. 118-131, 2011.

[15] R. Ajetunmobi, C. Uwadia and F. Oladeji, "A Survey and Critique of Digital Forensic Investigative Models.," *Int. Journal of Computer Science and Information Security,* vol. 14, no. 12, p. 496, 2016.

[16] M. Hristov, M. Nenova, G. Iliev and D. Avresky, "Integration of Splunk Enterprise SIEM for DDoS Attack Detection in IoT," *2021 IEEE 20th International Symposium on Network Computing and Applications (NCA),* pp. 1-5, 2021.

[17] Y. Zhao, "Implementing Virtual Local Area Networks," Dakota State University, 2002. [Online].

[18] A. Yeboah-Ofori, E. Yeboah-Boateng and H. Gustav Yankson, "Relativism Digital Forensics Investigations Model: A Case for the Emerging Economies," *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)*, Accra, Ghana, 2019, pp. 93-100, doi: 10.1109/ICSIoT47925.2019.00023.