Enhancement of Network-Based Attack Detection Rates using Snort as an Intrusion Detection System
Kutala Mohan Prasad¹, Goddumarri Vijay Kumar²
Student¹, Assistant Professor²
Department of Computer Science & Engineering
Sri Krishnadevaraya University College of Engineering and Technology, Anantapur, A.P, India

Abstract:
In the present era consolidation of virtual applications in cloud computing environment enables a significant chance of energy optimization. Cloud Computing acts as source for provisioning of computer resources to end user by pooling servers which are geographically distributed, in the form of accessible resources. This paper addresses the problem of energy inefficiency in the data centers where the ideal power is wasted when the servers run at low utilization. We present an operational model for the live migration of the Virtual Machines in cloud that uses load balancing algorithm for efficient energy optimization. The simulation results show the efficiency of the operational model when compared with the previous model.

I. INTRODUCTION
As we already know, apart from its benefits in the particular area in which it is implemented, any technical development also has its disadvantages. The same applies to computers that have completely changed & transformed people's lives but at that time they "harm" a lot of the individual components. Since computers are becoming such "private" buddies to humans, with the capacity of virtually everyone using computers, a new type of crime, cybercrime or computer crime also arisen, described as every criminal offense using computer as a weapon, goal, or by any other mechanism for the continuity of crime. Because of pervasive computer networks, network security has now become essential in an online society. Today the majority of them use computers, tablets, and smartphones every day for web-based correspondence, and the use of e-mail, network, and web servers to handle multiple requests. These accesses build sand of information across the web. We've long since gone through the internet to analyze its work and to understand it. Nonetheless, the very fact is that we humans have already built a much more strong and complicated framework, humans could recognize bits and bobs of that too, and generalize widely. During this time a whole new area of study emerged, i.e. network forensic work (usually relates to network-based evidence scientific research). To order to deal with these crimes, investigators have established the Digital Forensic field alongside its branches, each of it deal within a specific area. Both of such essential branches were computer forensics dealing with computer-related crime in several ways, and network forensics analyzing network traffic, usually by collecting packet as well as attempting to examine the files for useful details. Wireshark becomes a famous technique which focusing on packet detection, and Snort is another that focuses on the processing of packets. The forensic network may be a field of research outside any particular civil matter, and can identify several technological advancements, tools , and techniques created again for homicide investigation requirements. The Forensic Network offers a way for the Public to access the facts underneath a crime scene. We will figure out how to discover information that is hidden on the

Abstract:

In the present era consolidation of virtual applications in cloud computing environment enables a significant chance of energy optimization. Cloud Computing acts as source for provisioning of computer resources to end user by pooling servers which are geographically distributed, in the form of accessible resources. This paper addresses the problem of energy inefficiency in the data centers where the ideal power is wasted when the servers run at low utilization. We present an operational model for the live migration of the Virtual Machines in cloud that uses load balancing algorithm for efficient energy optimization. The simulation results show the efficiency of the operational model when compared with the previous model.

I. INTRODUCTION
As we already know, apart from its benefits in the particular area in which it is implemented, any technical development also has its disadvantages. The same applies to computers that have completely changed & transformed people's lives but at that time they "harm" a lot of the individual components. Since computers are becoming such "private" buddies to humans, with the capacity of virtually everyone using computers, a new type of crime, cybercrime or computer crime also arisen, described as every criminal offense using computer as a weapon, goal, or by any other mechanism for the continuity of crime. Because of pervasive computer networks, network security has now become essential in an online society. Today the majority of them use computers, tablets, and smartphones every day for web-based correspondence, and the use of e-mail, network, and web servers to handle multiple requests. These accesses build sand of information across the web. We've long since gone through the internet to analyze its work and to understand it. Nonetheless, the very fact is that we humans have already built a much more strong and complicated framework, humans could recognize bits and bobs of that too, and generalize widely. During this time a whole new area of study emerged, i.e. network forensic work (usually relates to network-based evidence scientific research). To order to deal with these crimes, investigators have established the Digital Forensic field alongside its branches, each of it deal within a specific area. Both of such essential branches were computer forensics dealing with computer-related crime in several ways, and network forensics analyzing network traffic, usually by collecting packet as well as attempting to examine the files for useful details. Wireshark becomes a famous technique which focusing on packet detection, and Snort is another that focuses on the processing of packets. The forensic network may be a field of research outside any particular civil matter, and can identify several technological advancements, tools , and techniques created again for homicide investigation requirements. The Forensic Network offers a way for the Public to access the facts underneath a crime scene. We will figure out how to discover information that is hidden on the

Enhancement of Network-Based Attack Detection Rates using Snort as an Intrusion Detection System
Kutala Mohan Prasad¹, Goddumarri Vijay Kumar²
Student¹, Assistant Professor²
Department of Computer Science & Engineering
Sri Krishnadevaraya University College of Engineering and Technology, Anantapur, A.P, India

Abstract:
In the present era consolidation of virtual applications in cloud computing environment enables a significant chance of energy optimization. Cloud Computing acts as source for provisioning of computer resources to end user by pooling servers which are geographically distributed, in the form of accessible resources. This paper addresses the problem of energy inefficiency in the data centers where the ideal power is wasted when the servers run at low utilization. We present an operational model for the live migration of the Virtual Machines in cloud that uses load balancing algorithm for efficient energy optimization. The simulation results show the efficiency of the operational model when compared with the previous model.

I. INTRODUCTION
As we already know, apart from its benefits in the particular area in which it is implemented, any technical development also has its disadvantages. The same applies to computers that have completely changed & transformed people's lives but at that time they "harm" a lot of the individual components. Since computers are becoming such "private" buddies to humans, with the capacity of virtually everyone using computers, a new type of crime, cybercrime or computer crime also arisen, described as every criminal offense using computer as a weapon, goal, or by any other mechanism for the continuity of crime. Because of pervasive computer networks, network security has now become essential in an online society. Today the majority of them use computers, tablets, and smartphones every day for web-based correspondence, and the use of e-mail, network, and web servers to handle multiple requests. These accesses build sand of information across the web. We've long since gone through the internet to analyze its work and to understand it. Nonetheless, the very fact is that we humans have already built a much more strong and complicated framework, humans could recognize bits and bobs of that too, and generalize widely. During this time a whole new area of study emerged, i.e. network forensic work (usually relates to network-based evidence scientific research). To order to deal with these crimes, investigators have established the Digital Forensic field alongside its branches, each of it deal within a specific area. Both of such essential branches were computer forensics dealing with computer-related crime in several ways, and network forensics analyzing network traffic, usually by collecting packet as well as attempting to examine the files for useful details. Wireshark becomes a famous technique which focusing on packet detection, and Snort is another that focuses on the processing of packets. The forensic network may be a field of research outside any particular civil matter, and can identify several technological advancements, tools , and techniques created again for homicide investigation requirements. The Forensic Network offers a way for the Public to access the facts underneath a crime scene. We will figure out how to discover information that is hidden on the

1. INTRODUCTION
As we already know, apart from its benefits in the particular area in which it is implemented, any technical development also has its disadvantages. The same applies to computers that have completely changed & transformed people's lives but at that time they "harm" a lot of the individual components. Since computers are becoming such "private" buddies to humans, with the capacity of virtually everyone using computers, a new type of crime, cybercrime or computer crime also arisen, described as every criminal offense using computer as a weapon, goal, or by any other mechanism for the continuity of crime. Because of pervasive computer networks, network security has now become essential in an online society. Today the majority of them use computers, tablets, and smartphones every day for web-based correspondence, and the use of e-mail, network, and web servers to handle multiple requests. These accesses build sand of information across the web. We've long since gone through the internet to analyze its work and to understand it. Nonetheless, the very fact is that we humans have already built a much more strong and complicated framework, humans could recognize bits and bobs of that too, and generalize widely. During this time a whole new area of study emerged, i.e. network forensic work (usually relates to network-based evidence scientific research). To order to deal with these crimes, investigators have established the Digital Forensic field alongside its branches, each of it deal within a specific area. Both of such essential branches were computer forensics dealing with computer-related crime in several ways, and network forensics analyzing network traffic, usually by collecting packet as well as attempting to examine the files for useful details. Wireshark becomes a famous technique which focusing on packet detection, and Snort is another that focuses on the processing of packets. The forensic network may be a field of research outside any particular civil matter, and can identify several technological advancements, tools , and techniques created again for homicide investigation requirements. The Forensic Network offers a way for the Public to access the facts underneath a crime scene. We will figure out how to discover information that is hidden on the

Abstract:
In the present era consolidation of virtual applications in cloud computing environment enables a significant chance of energy optimization. Cloud Computing acts as source for provisioning of computer resources to end user by pooling servers which are geographically distributed, in the form of accessible resources. This paper addresses the problem of energy inefficiency in the data centers where the ideal power is wasted when the servers run at low utilization. We present an operational model for the live migration of the Virtual Machines in cloud that uses load balancing algorithm for efficient energy optimization. The simulation results show the efficiency of the operational model when compared with the previous model.

1.1. Computer as a Weapon(Tool)
Where the user is the primary focus of Cybercrime, a machine could be seen more as weapon than the target. Typically such crimes need less technical abilities, since the damage done in the physical world manifests itself. The person weaknesses are usually exploited. The allegations handled are often emotional and invisible, rendering legal action against the variations more complicated. Such crimes which has occurred since decades on offline. Even before development, bribes, frauds and the like occurred in highly technology equipment. In reality, a certain perpetrator was already provided a tool which expands his/her possible full of targets and makes it much harder to locate & arrest him.

1.2. Computer as a Target:
A limited number of criminals are committing such crimes. Unlike computer-based crimes, such crimes involve the technical expertise of the perpetrators. Such crimes are very modern, because machines still exist, which illustrates how unprepared culture and the world at large are for the war against these crimes. Many such offenses are committed on the Internet every day. However, it is important to note that Africans, as well
as Nigerians, do need to improve their technological skills to handle and commit these crimes.

1.3. Digital Forensics
The usage of methods that have been scientifically validated or established to store, obtain, verify, classify, examine, evaluate, record and apply relevant data obtained from digital media in order to encourage or endorse the investigation of illegal activities or aid to anticipate unlawful steps that are proved destructive. This also involves visual processing, video analysis and audio analysis (both analog and digital). Digital forensics aims mainly at the identification, compilation, storage and analysis of data in ways which safeguard the integrity of the evidence gathered.

1.4. Relations with other digital forensics fields
In forensic research, digital forensics categorized to many branches related to concerned computing technologies. Below is the connection of each of those other sectors.

1.4.1. Computer Forensics
This is the oldest area for digital forensics that host based forensics often use to collect and examine data on personal devices such as phones, laptops and workstations. Usually data remains in non-volatile and central memory on the hard disk. Furthermore, there may be additional proofs of less widely known fields like the storing of hardware (e.g. mainboard or graphics cards) or also digital devices (e.g. DVDs or SD cards) which are left in a drive slot. Also the computer's hardware state and parts may be examples, such as a keylogger attached to the keyboard and USB mainboard(s).

1.4.2. Network Forensics
Network forensics handles data that can be found mainly on inbound and outbound traffic across a network connection. Network forensics tries to examine network traffic logged via IDS or firewalls as well as on n/w devices like hubs, switches and routers. Forensics in the network generally be described as science finding and recovering relevant data from couple of crimes in the networked world and making them appropriate in court. Typically cybercrime investigation includes cases involving Homeland Security Office, spying for companies, pornography, traditional crimes supported by system equipment, technologies on network, tracking of employees or records of medical, in which personal data (privacy) is a crucial issue.

1.4.3. Memory Forensics
It performs computer memory information. This is only tool that is possible because opponents do not write data for non-volatile device storage as they are fighting. Moreover, it makes it possible to examine more sensitive data, i.e. RAM material which is lost following power-off or reboot, such as kernel state of OS or device processes. Forensics on memory supports computer forensics and network forensics it is necessary for the hard disk key retrieval or network link keys to be restored.

1.4.4. Mobile Forensics
Mobile forensics is digital forensics field for retrieval, under forensic circumstances, of data from mobile devices or digital evidence. The term ‘mobile computer’ usually applies to cell phones, which can include ipads, notebooks, wearables and other apps which may be used – the memory and wireless network(s).

Among various factors, handheld forensic systems can be difficult:
The isolation of a computer from the network can be difficult. Some handheld devices have GSM, Ethernet, Near Field Communication (NFC), Infrarot communication as well as WiFi. Therefore, if the main network connection fails, mobile devices will link automatically from a separate network. It can be difficult to switch off a power supply on mobile devices. Batteries may not be reversible or a solar panel may remain in the system. This can go against traditional forensic procedures. Encryption of a whole computer makes it difficult or impossible to access data. There will not be typical hardware interface, i.e. a keyboard or computer. The program data types may be secret (proprietary) or regularly modified. Because of these difficulties, there is a wide range of methods required to obtain information in mobile devices; because no procedure or tool could collect the information in any smartphone type.

2. PROPOSED SYSTEM
Any forensic investigation will begin somewhere, whether in the form of a document (report) or an allegation (human) or an automated warning (computer). There is little to explore, without starting point. This could also come in the form of an IDS alert, abnormal system behavior, strange log entries, (like high cpu Usage), some combination of indicators in practice or a complaint e-mail. When making an complaint or an automatic incident warning, the origins and reliability of data need to be remembered. An person that files a report of abuse due to frequent offensive texts showing on his/her screen may potentially be interacting with a computer virus/worm. An warning mechanism for intrusion detection will only signify an attempted, ineffective intrusion or may even a false alarm. Further more, the capabilities, limitations, and other recognized complexities related to the origins must be weighed and encompasses both human and physical influences.

2.1 Network Forensics using Snort
Snort is often a network-based intrusion detection system (NIDS) designed to capture true internet traffic or before the-captured traffic patterns for pre-intrusion analysis to be replayed. The before the-captured traffic will be kept as normal de facto. The "defacto" specification for communication networks is the libpcap library prototype which is known as pcap (for UNIX/Linux based operating systems). The library design is defined as WinPcap of Microsoft Windows based OSes, but this is the same design as the pcap based on UNIX/Linux.
Network forensic investigation plays an significant role in identifying the network attacks and the architecture of which network forensic investigation relies on methods used for forensic analysis of the network. In general, we also use Snort method for suspicious packet detection. Snort is a free multiplatform open-source software, could be programmed to work in 4 categories. Mode 1st becomes sniff, it acts like a packet sniffer reading a packets it off network. You can configure the second mode, packet logger, to log a packet data to a disk. 3rd mode is, NIDS helps snort system to evaluate decrypt n/w traffic towards already defined preprocessors & rules, and if a similarity is found, executes multiple different actions. The fourth step about inline, allowing snort system to get drops & packets, or to transfer certain packet depending different rule forms of Snort inline.

2.2 Snort Architecture

Rule header was its rule section which recognises how and where to fit the n/w traffic, inclusion criteria were as follows:

Those parameters must be defined by each rule header.

2.3 Network Forensics Using Wireshark

While Wireshark is highly used analyzer of networks and protocols, it is an important tool in network forensics. Of that reason, any Digital Forensic Investigator will be able to use Wireshark of investigating the network and malware. Wireshark (formerly referred to as Ethereal) is often a GUI-based application for analyzing network traffic and even individual packets. To go and get the most of this tool, it is important that you understand TCP/IP or you'll have a huge amount of information without even any interpreting it. Capture, Identify and Analysis Most of the people's perception, network forensics involves the CIA method. CIA stands for Capturing the packets, Identifying date and time of packets and Analyzing both know and unknown packets.

2.3.1 Capturing

A standard role for an analyst during the accident analysis process is the output of a packet Capture, and evaluate the package. It is also popular tools used in Capturing, packet execution and evaluate. Wireshark - Linux, Windows etc. is available. Having captured the flow is created to a pcap file.

2.3.2 HTTP filter

After running the hancitordll, it reflect another infection i.e., Cobalt strike.
Infected traffic

2.3.3 Following stream

Protocol Hierarchy Statistics

2.3.4 Identifying

The analyst must have sturdy knowledge and awareness about the OSI model and packet examination on each layer to finally leverage PCAP as a forensic mechanism. Packet capture (PCAP) is the systematic reporting of data packets passing through capture devices that are characteristic of the network traffic. Frame signifies the section of transferring into a second layer protocol also consists of a second layer header continued on a packet. The network in a computer uses a frame through digital information transmission. During the HTTP request a protocol header is appended to the packet in the seventh application layer. Application layer header payload Transport layer header and network layer header are included within a packet.

HTTP

In order to download the websites or web pages on the host system, web browsers utilize the HTTP to interact with this remote server. The HTTP is unprotected because it transfers the data without encrypting them in plain text. That increases the attacker's possibilities of data theft. we can use the HTTP header to analyze the client details and the server details. It is likely to identify the website which the user accesses at the client system. By carrying out the HTTP packet analysis, the forensic investigator will be able to recognize the evidence of the Internet activities carried out. The application layer within the OSI model utilizes the HTTP to interact with these remote servers. The resulting forensic details from the intercepted HTTP packets can be identified.

a. Features of the client system:

Through examining the HTTP packets, one can learn about the different client system specifics like the type of web browser being used, the client-side configured operating system and the client device language package. Figure 2 displays the picture of the HTTP packet recorded with the specifics of the client device. While the client device is claimed to give the features thereof to the server of which the data is to be retrieved and this message exists in plain text.

HTTP GET request

b. About Port

During the information is transmitted across the system the transport layer joins its header being displayed in fig 1. The transport layer header is made up of the sender port number and the recipient. Through understanding the port number of the packet and a forensic investigator may determine the kind of services that the server offers in communication. The server's source port number equals 80 which means the web service of HTTP.

c. Examining the Web Site

The host websites can be detected by analyzing the header of HTTP protocol in a LAN. To access a specific website of the server the client utilizes the HTTP protocol GET request form. Using the HTTP protocol POST form the server replies to the client's web page. HTTP is the headline of the website concerned. Figure 2 displays the HTTP GET request method.

d. IP address

As presented in figure 1 the Bottom layer of the OSI model is effective adding the IP header to every layer and the information moved off to the top layer. This IP header provides source and destination information. The forensic investigator will find the devices that are section of the interaction by knowing certain addresses.

e. Attached Document

The malicious threats can send via e-mail and grabs the sensitive documents in an organization, which can be detected by packet analysis. Figure 3 explains the document attached to the mail. The links in the mail are redirected to a different URL.
TCP stream

DNS
The Domain Name System (DNS) is composed of messages including request (query) and response. Through examining request messages, the sites accessed can be identified using the secure (https) protocol. The server's IP address that hosts the website together with the client's IP address that accesses the website is known for the response message.

TLS
Transport layer security (TLS) observes and secure every interaction between a client and a server. The root and target IP address and using port information is given by the TLS packet. While the TLS packet is carried across the network HTTPS is resolved based upon the port number. TLS is encrypted while the application data is being transferred and data is secure.

Malicious threat

Analysis
The Forensic Network is a category of digital forensics. Forensic investigation involves investigations into network packets info captures, network log files and n/w-related event analyzing among others. Work should be conducted if an incident still is going through, or if an incident has been resolved. When an accident is already ongoing, a tap of the network could be useful. One can save live traffic data for inquiries.

The log files containing information can be collected for further study, because the incident has already occurred. Capturing, collecting or submitting information, the information is neither unstructured nor structured. The goal is to address forensic case research queries depending on what data is available. In forensic cases specific research queries are defined as the six or five W's: Why, When, Who, where, What, and How. Such queries are similar to forensic cases, for both optical & analog. We are taking a fictitious case to clarify that. "A corporation learns that an attacker is abusing its web server and deliberately abussingit."A variety in log-files were compiled and stored safely in our fictitious scenario.

Examples of potential log-files obtained are:
- The Web server compromised- application logs.
- Logs on firewall.
- The compromised Web server- system logs.
- Switch- Network Traffic Logs.
- Router -network traffic logs.

Not all of those logs are specifically linked to forensic network, but may be used as in enquiry. The Scientific research carried out should not be limited to forensic network only. The queries about the investigation are attempted to answer below, in accordance with the publicly accessible log files.

Who would interact?
An MAC address, IP address, or other metadata information from captured packets in network forensics may result in the identifying of the person(s) or devices involved. Whom did compromise the webserver in our fictitious case?

What would have happened?
The logs would give details on exactly what would have happened. Through ours fictional example, whether the server has been compromised or not can be investigated on the basis of the traffic data.

Where does this occur?
The topic discusses where the attack happened or where it turned out. For our fictional example, when and how the murder investigation was being committed.

When does it begin?
The analysis purpose deals with the issue of when the accident took place. In our situation, when did this incident happen, when did the machine get infected and then when did the real harassment begin?

Why does this happen to transfer?
There is only one explanation for an incident or situation. In our situation, for example, the web browser could be used to distribute ransomware, the website can be taken down for political purposes, or may it have been included as parts of a DDoS attack.

How does it start?
Using an exploit will hack a compromised computer, or when it's small, it can guess the password. Any port numbers & protocols utilized during the attack will provide insight about whether the attack was successful. To use a vulnerability, a
packet capture including its exploit is important. In our situation the question is about how they come through. To answer questions above, the tool has to chosen for analyzing. There are tools that can be used for selecting or visualizing specific data from log files.

**The importance and value of Forensics Network**

The Network forensics gives insight into an incident or event's network traffic. Also the entire payload of the data packet can be available, depending on the log stage. Whenever an intrusion occurs in digital way, forensics in network may support the questions in the company might have:

- How long did this activity actually occur (When does an intrusion normally start)?
- Was this activity still currently in progress?
- How much those systems will have been affected?
- What details is taken from that?
- Have you taken any classified, proprietary or important information?

**Many useful Network forensics additions are:**

- Hunting (for suspicious or unusual Network activity).
- Metrics / Understanding of network.
- Intelligence
- Passive / DNS
- DNS
- Intelligent Alerting.

If a system gets hacked, the machine 's system capabilities are no longer reliable. The displayed information will purposely show incorrect values by the machine software. By using rootkits, the compromised device can hide information. The suspicious traffic that goes via a router or switch, and at particular point remains visible. A particular network traffic, visual peak, or a regular traffic study may provide additional details on the problem.

**Where does one find forensics for the Network?**

Whenever everyone likes to think a forensic network, typically one wants to think of such a criminal investigation or hacking. Furthermore, in addition to law enforcement and private investigative agencies, CERT / CSIRT teams, security experts, and network administrators may also perform the network forensic investigation. Sources for Network forensics have already been explored in "Collecting network-based evidence."

**Possible Network Data Sources are:**

**Switches**

The switch may have span port function. Span port often process of transferring to scan all kinds of packets from a port switching to the next port switching.

**Routers**

For NetFlow data tracking traffic in network can be provided by routers.

Layer 2-7 devices

Through layer 2-7 system is capable of capturing data in the network, just not only devices but also provide services and also endpoint.

**Network Tap**

It duplicate entries of pieces of data packets & can transfer stream(s) of data to the next storage medium or physical network port.

**Logging and monitoring**

Logging is passive network traffic saving, so logged attacks aren't immediately detected. In fact a recognized trend is observed by tracking the system logs or observing live network activity, notifications may be generated to submit notices. In the context of an mistake or incident, (particular) network traffic may also be saved manually for analysis or examination in the log files.

**Flow diagram of malicious threat:**

**II. CONCLUSION**

In this project, we tried to improve network-based attack detection rates using the new 1.Rules. We had seen that it had the full capacity to recognize all of the attacks, which have a defined rule for the matching signature after the usage of SNORT as an intrusion detection system. The hackers of today are really innovative and create the latest sign for multiple attacks and sometimes, but not always, they can be effective because we have a gun like rules and snort. We introduced network forensics and compared them with network security. Forensic networks were often systematically established, and different varieties of forensic network structures were identified. Through network forensics the impetus for testing is elucidated. The latest developments in this emerging area are discussed, demonstrating the analysis complexities of network forensics. Our purpose to detect stubborn TCP, ICMP and UDP malicious packets during snorting. As a result of this, we have found snort to be capable of detecting attacks and of producing warnings...
based on installation guidelines. Therefore, we need to use the new guidelines to identify and create warnings based on a rule-based intrusion prevention system so that you all can also trigger network attacks based on zero-days.

Future Scope
We intend to develop an automatic data system in the future that we can identify some of these cyber threats which the configuration file doesn't mention any rule. Using the machine learning principle, we would develop our application to recognize the nil-day-based network attacks using the warning generating file as just a practice data collection. We are still planning to integrate different methods of detecting network intrusion (i.e. anomaly-based, rule-based and behavior-based) along the same data but also monitor whether or not the integrated approach works much better than individual method.

III. REFERENCES


