TALLINN UNIVERSITY OF TECHNOLOGY

Faculty of Information Technology

Department of Computer Engineering

ITC70LT

Seyed Morteza Zeinali (IVCM131121)

ANALYSIS OF SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) EVASION AND DETECTION METHODS

(Master Thesis)

Supervisor: Bernhards Blumbergs

Master's Degree

Ph.D. Student at Tallinn University of Technology

Tallinn 2016

Declaration

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

....

(Author's signature) **(Date)**

Abstract:

Security Information and Event Management (SIEM) systems have become today a crucial and essential component of complex enterprise networks. They typically aggregate and correlate incidents from different systems and platforms, and carry out a rule-based analysis to detect advanced threats. The latest reports show that in spite of the fact SIEMs are significantly efficient, but there are still shortcomings and evasion methods that can compromise the integrity of data and forge the data stored and need to improve over prior solutions. This paper evaluates and analyze the SIEM evasion detections, SIEM evasion methods, expresses approaches and the tools that evade security appliances. An attack simulation experiment is performed using multiple Advanced Evasion Techniques (AETs) to demonstrate the capabilities of SIEM in detecting any suspicious behaviour of event logs and alerting them in near real-time. The tested SIEM was able to collect, filter, normalize, correlate, alert, and report network attacks within minutes after attack incidents.

Keywords:

Evasion Detection, Event Management, Security Information, Evasion Techniques, SIEM, Outlier Detection, Information Management, Advanced Threats, AET, incident, Anomaly Behaviour.

Acknowledgements

I would like to appreciate my supervisor Bernhards Blumbergs for his aid and support to make this work appear in the form it is right now throughout the entire period of the research by giving me knowledge and feedback on my work.

I would also like to thank my friends and family who bared with me and continuously motivated me to work on and finish my research paper.

Morteza Zeinali

List of Abbreviations

SIEM	Security Information and Event Management
AET	Advanced Evasion Technique
IDS	Intrusion Detection System
IPS	Intrusion Protection Systems
USM	Unified Security Management
OSSIM	Open Source Security Information Management
APT	Advanced Persistence Technique
BYOD	Bring Your Own Devices
DDoS	Distributed Denial of Services
TCP	Transmission Control Protocol
HIDS	Host-based Intrusion Detection System
NIDS	Network Intrusion Detection Systems
UDP	User Datagram Protocol
PCI DSS	Payment Card Industry Data Security Standard
DLP	Data Loss Prevention
DPI	Deep Packet Inspection
OSI	Open Systems Interconnection model
IP	Internet Protocol
DHCP	Dynamic Host Configuration Protocol
HTTP	Hypertext Transfer Protocol

URI	Uniform Resource Identifier
SQL	Structured Query Language
CSV	Comma Separated Values
SMB	Server Message Block
NetBIOS	Network Basic Input/Output System
RDP	Remote Desktop Protocol
SP2	Service Pack 2
CVE	Common Vulnerabilities and Exposures
IO	Input/Output
ARP	Address Resolution Protocol

Table of Contents

List of Figures

List of tables

1. Preliminaries

1.1. Introduction

Sophisticated cyber threats have been become a significant adversary in the evolving world of the cyberspace. Layered defense technologies still are essential for enterprises. However, the days of relying merely on perimeter controls are elapsed. It is no longer enough to just rely on firewalls, Intrusion Detection Systems (IDSs)/Intrusion Protection systems (IPSs) and antivirus in place. Wide-spreading adoption of a distributed environment that leverages virtualization and cloud, the perimeter no longer exists [1]. Attackers have become nimble at “flying under the radar” concealing from security controls [2]. They use sophisticated and subtle intelligent techniques include zero-day, social engineering tactics, advanced evasion techniques to evade detections [3]. Moreover, today’s technology has accumulated with large-scale data produced by devices that share the massive volume of information organizations with compounds that need an effective tool for control, monitoring and fighting against potential threat. In this way, Security Information and Event Management (SIEM) Systems play a key role at organizations in monitoring both real-time events and a mountain of long-term data to detect anomalous patterns of utilization and alert organizations whenever needed. Even though SIEM solutions bring additional security to the network, but they are not quite bulletproof. As the SIEMs are extremely reliant on event logs, cyber perpetrators can use advanced evasion techniques to penetrate to the victim machines and stop, derail, delete or inject malicious logs to cause unexpected SIEM behaviour and overcome them.

This chapter begins with a brief overview of security information and event management systems. Afterwards, look at the challenges facing with SIEMs and some existing defects. Next, the contribution section explains the goals of this research study, the purpose and motivation to reach and the applied methodology to do the project. Then, problem statement and research questions are pinpointed to specify the current problems. This chapter ends with a brief description to the audience and readers to point out the expected results as well as the research plan.

1.2. Background

The current computers and networks produce huge volumes of security log information. A Security Information and Event Management system is required for handling of the increased level of information security as well as the analysis and management of centralized log [4]. The underlying principle of SIEM system is that the relevant information about the security of an enterprise is produced in diverse sources, and the data is correlated and viewed from one central location. This process makes it easier to study the patterns and trends that are not allowed. SIEM is a combination of Security Information Management (SIM), and the Security Event Management (SEM) functions into a single security management system. In details, SIM segment mainly emphasizes on the analysis of historical data intending to improve the long-term storage performance and efficiency of information security infrastructures. On the contrary, SEM area emphasizes on the aggregation of data into a manageable amount of information with the aid of which security incidents can be dealt with immediately [5].

According to Miller [6], SIEMs provide near real-time monitoring as well as analysis of security events which enables quick remediation before damage is occurred. Further, the systems respond quickly in case of an attack with accuracy up to 90% and speed within 60 seconds of event correlation and have the capability of generating compliance reports [7]. SIEM systems allow users to build content, logic, conditions, and criteria. These are used with correlation rules deployed for faster identification and escalation of a security event or incidence. Data from different sources is collected and aggregated through agents. Noise or unwanted data is filtered and normalized to a proper format for analysis through correlation [8].

Furthermore, SIEM works by deploying different sets of agents in a hierarchical manner with an aim of collecting security-related information and events from the end-user devices, system servers, and the network equipment Also, SIEM gathers security information for specialized security equipment, and tools such as intrusion detection systems, firewalls, and antivirus. The collected information is forwarded to a centralized control and management console. The central console further performs inspections on the logs and flags any anomalies. Altogether, the roles of SIEM product is to collect, consolidate, correlate, communicate and control [9]. First, the log data is collected from different devices and applications, which is then aggregated and normalized, also known as consolidation. Log data is then parsed and correlated, a process that involves putting pieces of an attack together to form a complete picture. In this step that contextual information about a network and common threats becomes more useful. The collected data is first stored locally in organization's the network before it is transferred to a central area for analysis and archiving.

However, it is important to note that an SIEM, cheap or expensive, is not 100% secure. The advancement of cyber threats and techniques makes it possible for some hackers to avoid being detected by SEIM [7]. This paper looks into and analyzes SIEM evasion detection, methods, tools, and approaches.

1.3. The challenge facing with SIEM solutions

Evasion techniques have become possible today as a result of attackers using new exploit to slip by the organizations' perimeter systems. Moreover, attackers are also using social engineering tactics. Those tactics are making it completely possible for the attacker to bypass the security controls that are put in place for the network and systems. On the other hand, an SIEM system cannot pick up or detect an attack that was never logged [10]. At present, attackers are keen to first gather information about the network and understand the target in order to prepare for a later attack, as named the reconnaissance phase of the attack. As a result, the attacker is able to find any vulnerabilities and weaknesses on a system or network before they launch an attack [11]. After understanding the target, the attacker designs an attack "toolkit" that will be deployed into the target system. The attack toolkit establishes ongoing communication and gets into the target network. Finally, the attack toolkit completes the mission by covering tracks and stealing data and information. The research phase of the attack involves activities include reconnaissance attacks (using information lookup tools, ping sweeps, port scanning and packet sniffers) and uses other exploits that make evasion possible.

SIEM system is designed for aggregating and correlating event and log data from diverse sources such as devices and applications throughout the network or system. SIEM is a great and reliable tool for compliance. However, the current evasion techniques are making SIEM to become less ideal for quick detection and thorough investigation of threats. The challenge facing the current day SIEM systems is that of massive amount of alerts and logs (i.e. big data), and their diverse unstructured nature. There is a challenge of getting enough resources to thoroughly investigate all the alerts. Furthermore, there is an increase in false positives[1] that results in missing of critical events. To put it differently, the massive volume of alerts and increase in positive results may case alert fatigue in the SIEM. Moreover, it takes a couple of days to process and analyze these alerts and various events and to finally piece together a critical issue such as a threat [12].

As can be seen, an SIEM system may put too much focus on an individual attack, and as a result forget in the campaigns. Furthermore, there are those attacks that are not alerted at the perimeter wall, such that no data about such attacks is collected. In the same way, there is no particular way of measuring the time between an incident or attack origination and the discovery. In other words, there can be too much time elapsed between when the attack originated, when it was discovered, contained or closed [13].

The current detection systems and methodology should be designed and developed with the focus on campaign of attacks and not an individual event or attack. Effective SIEM intelligence goes beyond a single attack and focuses on a campaign that may be launched by an attacker. Additionally, the solution should have a mechanism and algorithm that understands the actor's history and past behaviors, processes, techniques, and infrastructures. Developing a SIEM solution with the focus on campaign based intelligence and analytics gives the organization an ability to proactively detect attacks on various stages of the deployed exploits kill chain. Such a solution can quickly identify attacks at various stages of the chain and understand the activities and commands of those attacks. The solution can tell how long the attacks have been active in the network and also detect other places that the attacks may have spread.

The basic evaluation parts of an SIEM system involves the evaluation of three elements. First is the central console, second is the monitoring entity, and finally the communication process between the monitoring entity and the central console [14]. For the SIEM to function effectively, its design and development must ensure that the monitoring entity and the communication process supplies complete and integrated information to the central console.

[1] "A false positive is when the system generates an alert about traffic, but that traffic is not Malicious or important as related to the safety of the network" (CCNA Security P.377).

The current SIEM products also lack an information storage facility that is secure enough. For instance, the security events are always available and used for analysis [15]. The forensic storage facility in an SIEM solution is used retaining the digital log data used as evidence while detecting malicious activity and security breach. Moreover, having a forensic storage facility provides an infrastructure capability in which the integrity of events stored as well as availability of system would be preserved. A weakness on the SIEM storage facility may be as a result of the use of the classic RSA algorithm. The classic RSA algorithm commonly used in the present SIEM systems is based on pairs of public and private keys, namely asymmetric key cryptography used in signing security events. The forensic storage using classic RSA algorithms has some limitations that attackers may exploit while launching an attack. The benefit principle behind the RSA algorithm is that it operates quickly and challenges any algorithm in real-time on the problem of factorization of massive numbers. Moreover, it does not involve high usage of memory. However, an attacker could lunch a DoS attack in order to prevent of signing the event only by knowing the logical address of signing module. In this way, the attacker would be able to compromise the availability of system. The attacker also could compromise the integrity of events stored using a malicious software installed on network device that generates RSA signatures and could forge the signatures. Compromising the security used by the forensic storage algorithm will eventually compromise the security provided by an SIEM using an RSA algorithm.

SIEM systems are highly relied on event logs to collect, normalize and analyze them for any suspicious behaviour. On the other hand, incidents are escaping of SIEM because they can be a big evidence in detecting their destructive presence [16]. Attackers attempt to discover subtle ways to avoid their presence being detected. They attempt to disable logging or derail them from the vision of SIEM solutions. Further, Attackers are able to delete any existing local log trails, if log management infrastructure is unsecured or has unreliable log infrastructure. It is possible, just by manipulating symbolic link (also called soft link or symlink) the shell history file to /dev/null on UNIX system. In this way, attacker can conceal all of the shell commands from the vision of the SIEM in order to evade detection.

1.4. Thesis research goals

At the present time, an enterprise is required to deploy a SIEM solution to keep them in business and protect their operations and intellectual property [17]. Ecommerce benefit more from SIEMs as they ensure security levels are people transact business online. Deploying SIEM solution further helps in meeting the compliance obligations. Storing the logs from different sources in a central secured database make the process of consolidation and analysis easy. The main aim of the analysis on the collected data is to help detect any threats that may not be identified by the traditional means such as perimeter walls and signature-based techniques [18].

At the present time, SIEM technologies have evolved from simple point solutions into comprehensive systems that allow organizations to optimize their security related functions such as the collection and management of critical network and system log data. SIEM further helps an enterprise optimize the execution of processes in support for policy and regulatory compliance obligation. SIEM helps identify information security threats and act upon them. Also, the SIEM helps in continuous information security risk management processes. In the long run, it is critical for enterprises to evaluate SIEM vendors, develop the SIEM implementation strategy, understand SIEM considerations and capabilities, and like every tool and technique, understand that SIEM has limitations [19].

The aim of this research thesis is to evaluate and analysis of the SIEM evasion detections, SIEM evasion methods, approaches and the executable tools against different SIEM vendors. Further, this study would give an overview of collected logs from end sources and look whether SIEM solutions were able to detect and alert all launched exploits and evasions in near real-time or not and why the result is as such. It would also possible to compare achieved result from main experiment with an out of scope experiment - the Snort network intrusion detection system deployed - to achieve a solid proof of concept. Moreover, perform detailed comparative performance evaluation and analysis with both SIEM solutions.

To develop a solid understanding of the study topic, this research will experiment on the process of attack evasion and detection. The test-bed based evaluation using the SIEM platform will help demonstrate the research topic and assist in answering the research questions. This study deploys Splunk Enterprise SIEM Platform[1] and AlienVault Unified Security Management (USM). Splunk solution presents a free trial license for 60 days, allowing index up to 500 megabytes of data per day. It has most of the features and functionality of a premium SIEM Enterprise solution. Splunk Enterprise SIEM product provides users with a feature rich open solution complete with log and event collection, correlation, and normalization. The tool provides a central, unified view of critical IT services and utilizes advanced analytics driven by machine learning to highlight anomalies, detect root causes, and pinpoint areas of impact.

This research prefers to use Splunk Enterprise SIEM platform due to a number of reasons including: instant trial, and instant conversion for proof of concept to production, a dedicated environment for each customer, reliability and includes a custom alert trigger that allows users to look at data and create a notice that can detect possible anomalies, Mowlem explained. Thus effectively used for experiment purposes. The tool offers a single and centralized view across all the machine data. An enterprise using Splunk gets flexibility they need at the pace that works for their business[2].

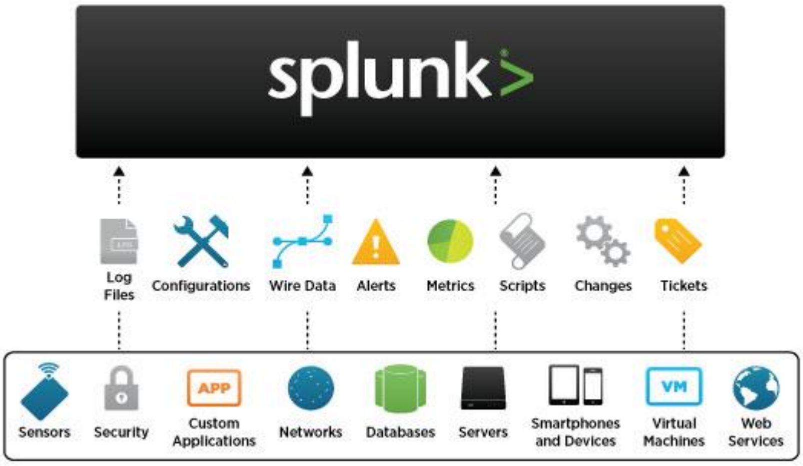


Figure 1: Splunk Enterprise SIEM Overview[3]

[1] http://www.splunk.com/en_us/download/splunk-enterprise.html

[2] http://www.splunk.com/en_us/products/splunk-cloud/hybrid.html

[3] http://www.philiplay.com/2014/10/how-splunk-is-playing-for-power-in-big-data/

AlienVault was selected as second solution for this experiment. It is composed of a unified framework, which is available as Open Source Security Information Management (OSSIM) and also as a commercially supported product called AlienVault Unified Security Management (USM). According to AlienVaut website[1] it is claimed to be the world's most widely used open source SIEM solution. It offers open-source SIM (OSSIM), a free, open-source version of its solution with a restricted feature set, but its commercial product - AlienVault USM - extends OSSIM with scaling advantages, consolidated administration and reporting, log management. OSSIM SIEM product provides users with a feature rich open solution complete with log and event collection, correlation, and normalization. This product was launched by a group of security engineers who saw the need for a reliable open source security product. OSSIM SIEM was developed specifically to address the challenges faced by security professionals. This project deploys a SIEM solution of AlienVault that is capable of asset discovery, intrusion detection, behavioral monitoring, vulnerability assessment, and security information and event management. Additional description is presented in the chapter 6.1.2.

1.5. Problem Statement

The latest reports show that in spite of the fact threat detection platforms like SIEM are significantly efficient, but there are still shortcomings and evasion methods that can compromise the integrity of data and forge the data stored and need to improve over prior solutions. Moreover, "Reports from a new study by market research firm, reveals [20] that the current security threats includes: Advanced Persistence Techniques (APTs) [21], Advanced Evasion Techniques (AETs) [22]" used in sophisticated attacks harm the business and make them vulnerable. With the projection of 5billion internet of things devices by the end of this decade and growing 'bring your own devices' trends and development in mobile technology, SIEMs are expected to tackle the latest and emerging security breaches and challenges with advanced analysis. Furthermore, enterprises are

[1] https://www.alienvault.com/products/ossim

required to comply with the regulatory standards that leverage multiple types of use cases and different data types

1.6. Research Questions

Thesis will address the following research questions:

i. What are the available SIEM evasion detections techniques?
ii. What are the common types of SIEM evasion methods, approaches and tools to execute them?
iii. Is SIEM able to produce a response in near real-time?
iv. Which evasion approaches can be used to overcome SIEM solution detection?

1.7. Expected Results

At the end of this thesis, it will be possible to determine whether SIEM solutions were able to detect and alert all launched exploits and evasions in near real-time or not and why the result is as such. It would also possible to compare achieved result from main experiment with an out of scope experiment - the Snort network intrusion detection system deployed - to achieve a solid proof of concept. Moreover, an experimental approach will help answer the research questions and also assist in getting a deeper practical understanding of SIEM through the use of a real experiment environment.

1.8. Research Plan

This thesis and related research involves a thorough evaluation and analysis of SIEM evasion detection, SIEM evasion methods and represents approaches and the usable tools to execute them against SIEM vendors, and review of other research projects in the area of SIEM systems. This research reviews on other journal articles, product review articles, SIEMs conferences, websites and books in respect to SIEM evasion detection, methods, tools, and approaches. Additionally, the research covers government and corporate findings that provide critical content and information in regards to SIEMs. The primary information research methodology deployed in this paper involves review and analysis of relevant and related literature. The resources required include access to peer-reviewed journal articles sourced from the internet and academic research paper online databases.

2. Attacks and SIEMs grow in complexity

The two critical systems that form a SIEM system include the firewalls and the Intrusion Detection Systems[1] (IDSs). Information from firewalls and IDSs form a fundamental source of log and event data for the SIEM system. At present, vendors are producing and supplying firewalls and IDSs that are well sophisticated and are capable of detecting and blocking malicious activities from an attacker[17].

Distributed denial of services (DDoS) and other attacks are harming businesses around the world [23]. Just as the organization adoption of technology changes constantly, cyber-attacks are also evolving. At the present, there has been an emergence of some of the most dangerous threats such as the growth of advanced targeted attacks, advanced persistence threats and advanced evasion techniques. Through these attacks, the perpetrators are using crafted techniques to penetrate a company's system or network for different goals. At the same time, the traditional network perimeter protection and other tools such as cryptography and signature-based are becoming less effective.

As the threats advance over the years, network and system defenses has also evolved. Organizations now deploy firewall platforms at the network boundaries to audit the inbound and outbound traffic while blocking any malicious connections. Intrusion detection systems and tools are used to inspect the traffic allowed by the first layer and look for matches to the signatures of common attacks. There are various vendors who offer SIEMs that can correlate log events from devices and applications. Any anomaly is recorded and used in ranking the risk, from low to the highest level [24].

SIEM system is deployed between detection and actionable intelligence. Originally, SIEM systems were designed and developed as a central console for gathering and storing security data, including event info and log. An SIEM system is composed to two main parts. One is a central entity involved in the gathering, correlating, aggregating, and analyzing the information[4]. Second, the system is composed of independent monitoring agents or entities that are involved in supplying the central console with the relevant log data and event information[14]. The relevant information collected by the agents and

[1] Many commercial IDS products are also known as Intrusion Prevention (or Protection) Systems, to highlight their counteraction capability. In fact, such devices perfectly fit in our general definition of IDS.

supplied to the central entity includes log data on system logs and intrusion alerts. The security data collected is used to streamline compliance reporting and threats incident investigation. With the emergence of advanced persistent threats (APTs) and advanced evasion techniques (AETs), traditional SIEM systems have indicated to have device and information limitations, blind spots and assessment gaps [25].

The modern SIEM solutions can deliver faster response times and persuasive situational awareness by integrating different capabilities [26]. Big data scalability is one capability integrated with SIEM, making the solution more reliable and effective. The present day SIEM solutions have the extensibility, capability and speed. The integration enables faster and better threat detection. Current SIEM solutions are developed for volume requirements and big data analysis speed. The systems have the capability to expand data capture with additional feeds from diverse sources. The systems can process large, diverse and dynamic sets at larger event rates and capture and store the billions of logs, events, and flows for both real-time and historical data[25].

The figure below shows an SIEM with a central console used in monitoring an organization and the intranet. The principle behind the design of this system involves receiving and distributing external traffic using a router. The firewall and network IDS filters and inspects the traffic while the switch is used to organized the allowed traffic over different sources that are connected to the LAN. The monitoring process occurs through allowing all devices to collect audit data such as system logs and firewall alerts. Such data is sent to the central console in the SIEM system where it is aggregated, correlated, analyzed, and reported in case of an anomaly detection [14]

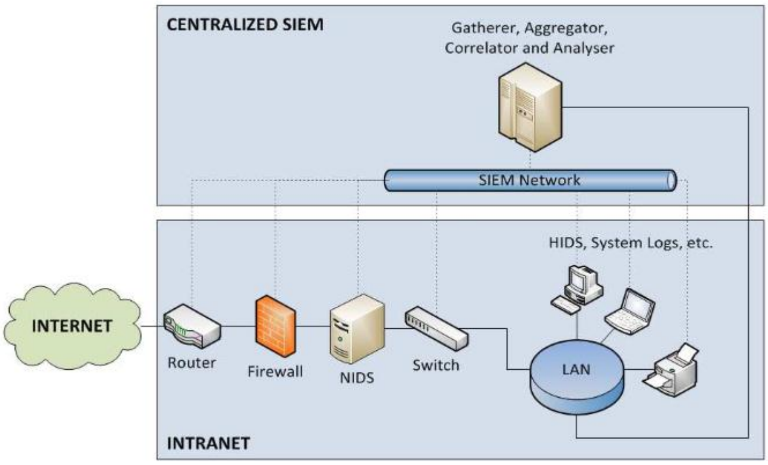


Figure 2: Architecture of a centralized SIEM Monitoring on Intranet [14].

A proper evaluation of an SIEM solution helps prevent an attacker from evading the system. There are three main steps that should be involved in a proper SIEM evaluation. First, the entities collecting, aggregating, correlating, and analyzing the audit log data from the monitoring entity should be evaluated thoroughly to ensure that the SIEM solution is efficiently detecting the majoring number of attacks and generating a minimum number of false events and alarms. Secondly, the audit data collector or agent should independently be evaluated to guarantee that all information and data collected by the agent is correct and real. Finally, all communications between SIEM entities should be evaluated and secured to guarantee that there are no attacks that occur in the communication channels such as packet injections and packet modification. Attacks on the communication channels can compromise the core role of the SIEM solution, which involves the analysis and detection of incidents in the system.

3. Fundamental Log Data Sources and Information Transmission

3.1. Intrusion Detection Systems

According to Shon Harris [27], Intrusion detection is defined as ’’the process of detecting an unauthorized use of, or attack upon, a computer, network, or telecommunications infrastructure’’. An IDS system is capable of analyzing data and detect malicious and dangerous exploit. The system then reports an alert if an anomaly is detected. The IDS is made up of a decoder, preprocessor, detection entity, and the alert module[14]. In an IDS system, the function of the decoder is to receive the raw audit data from a collection agent and to transform the data into a format that can be handled by a set of preprocessors. Next, the set of preprocessors receives the data in the right format form the decoder. The function of the preprocessor is to analyze the received data to determine which parts are dependent on each other and handles those pieces in a way that can easily be scrutinized by the detection entity of the IDS. TCP preprocessor is one example of a typical preprocessor used in IDS. In particular, TCP preprocessor is involved in composing session flows from different TCP segments. This process involves perpetual fragmenting, reordering, and assembling of TCP segments. IDS’s detection entity function involves receiving the data from the preprocessor and examining it to detect any intrusion. If the detection entity discovers any intrusion, it sends a signal to the alert console so that an alarm can be raised. Finally, the alert console is responsible for raising alerts as per the request by the detection engine. The alert may be in the form of a logging into a local file shared via email with the responsible authorities [14].

Based on the source of the logo data, an IDS can be either host-based (HIDS) or network-based (NIDS). A host based IDS, referred to as HIDS, analyses data in a single host device. The data analyzed by a HIDSs include systems calls of the systems running in the monitored host device. The HIDSs analyze data from system call arguments, stack skates, user behaviors, system logs, and memory registers. On the other hand, a NIDS is used for analyzing the network traffic. The level of detection varied between one NIDS and another. A NIDS is responsible for analyzing network traffic, and data from the application and the transport layer [14].

Intrusion detection systems utilize multiple detection methods including signature based detection, statistical anomaly-based detection and stateful protocol analysis.

- **Signature based** – the anomalies are modeled such as rules known as signatures. The intrusion detection is accomplished through the process of comparing the signatures with a behavior taking place in the system or network being monitored either by the HIDS or NIDS.

- **Anomaly based –** the anomaly-based IDS presents the normal behaviors of a system in a certain model. Any other activity that falls out this agreed model is considered abnormal and is alerted.

- **Hybrid** – the Hybrid IDS uses both signature and anomaly-based models to detect a security incident. In this case, the set of preprocessors is involved in the anomaly-based technique while the detection entity is in charge of signature-based technique [14].

3.2. Firewalls

A firewall is a security module, either software or hardware, deployed to prevent the access of a trusted network by an untrusted source. A trusted network is also used to present a single device such as a laptop or PC. On the other hand, the term is used to present a set of heterogeneous devices such as those that form an enterprise network. An untrusted source is used to refer to the internet and any other source that may cause harm to the trusted network. A firewall is responsible for examining data packets that pass from a trusted network to an untrusted one, and vice versa. The firewall is designed in a way that enables it to automatically discard that are considered unacceptable according to the firewall security policy. The firewall security policy is composed of a set of rules. A packet must meet these rules for it to be either accepted or discarded based on the rules. A firewall is evaluated through the penetration testing technique. The penetration testing technique evaluates the firewall through the process of simulating different attacks and analyzing their effects.

4. SIEM Threat Detection and Alerting

SIEM solutions are capable of real-time monitoring of the network at all time to detect and alert in case it identifies an incident and a critical security issue. The main roles of the SIEM solution in an organization's network are to monitor the log data, collect and store it in a central console. The next step involves analyzing the log data, filtering alerts and build correlation rules.

SIEM log management finds all the log sources. As indicated earlier, log sources include applications, systems and devices that are in a network[19]. SIEM collects the logs data securely in a way that non-repudiation can be proven. To have a secure chain of custody, the logging data process must be automated, consistent and clearly apparent. They use factors and methodologies that secure the data using collection technologies. For example, to collect log data from sources over UDP, the collection device preferably hasto be located near to source in order to mitigate the risk of data being lost. This can be possible by reducing the number of packet hops to zero that need travel before reaching its destination [28]. Often, SIEM systems collect large volumes of log data. Thus, the system should be capable of collecting this data without getting overwhelmed. A common construction approach for an SIEM system is the hierarchical approach that enables the system to collect log data at multiple levels[19]. In other words, the system is designed in a way that an agent is deployed in different location levels. These agents communicate to back the SIEMs central management console in charge of data storage and analysis. The process has no impact on the performance or running of the network. Traditionally, the SIEM system focused more on collecting the device or structure related log data and events. For instance, the traditional SIEM implementation required that the operating systems running on both the servers and end user devices send log data such as log in events, antivirus application alerts, and communication subsystem information. Some of the log data collected for OS includes successful or unsuccessful logins, admin login, user information- readable or encrypted, and other conventional events. Other log data may include antivirus updates, repair and infection details. The communication subsystem information collected by the SIEM edge collectors and agents includes blocked and successful port connections, all port connections attempts, and information on a network's IP addresses. In addition to these events, SIEMs are fed with log data from other critical network devices such as routers, intrusion prevention systems, and firewalls.

The log data from these sources help the SIEM system in building a profile of the network when the organization's system is operating under the allowed event conditions. The process of creating an allowed event profile is vital for the SIEM system to detect an anomalous event after comparing it with the normal event profile.

The log data collected from different sources is stored in their raw and enriched format for a long period. Storing the log data in its raw format optimizes the time taken to access the data in future. Ultimately, the most critical function of an SIEM application is the analysis of the log data. SIEM system is required to look into the different logs stored and notify the user about the network environment based on the information insights deducted from the log data. An ideal SIEM solution can correlate both the new data and data that is similar to another set of logs that the system had collected previously.

Using a set of distributed intelligence features and algorithms, SIEM solutions can detect and alert the analysts in case of any threats. SIEMs notifies the analysts in case of any anomalies in the logs collected. The system is designed in a way that is called well situational awareness, where the incident happened, what other areas of the system will be affected by the incident, and also gives insights that could help establish the source of the threat. This allows solutions to detect attacks in most cases as soon. In addition to situation awareness, they can operate as a solution to orchestrate responses and stop attacks well ahead of become breaches [29]. Out of the analysis process, the SIEM system will activate automated actions, real-time user notifications, historical log data analysis, and compliance analysis. Consequently, the analysis process should take place without interfering with the performance of the network or the system that is being acted on by the SIEM tool.

After the analysis of the log data, SIEM should present the results and conclusions in a manner that is dependent on the user roles. The information presentation should be consistent with the different user's roles such as those of the operator, analyst, engineer, to the organization executive. In most cases, SIEM vendors provide a solution that features a graphical user interface that is interactive. The information is presented in a format that is user-readable and understandable for all the log sources connected to the SIEM. In some cases, SIEM reporting functionality gives the user the rights and ability to customize the log information reports, and extracts only what is relevant for their roles.

Apart from the real-time monitoring, analysis of log data, and interactive visual information reporting, SIEM solutions have compliance reporting feature that generate a detailed and actionable audit log records. This feature of the SIEM is in line with the acceptable security frameworks such as Payment Card Industry Data Security Standard (PCI DSS). Compliance firms and information auditors can use SIEM tool reports to validate and prove that an organization is compliant with any relevant regulation that guides and monitors the operations of the organization. The auditor may check collected log data, information reports, and other regulation specific content while auditing the organization for assurance that they comply with regulations.

As a result of the complex design requirements and the need for better performance while handling large volumes of data, vendors are designing SIEM platforms that are purposely built to provide adequate performance and that can easily scale [30]. These current SIEM systems have been able to overcome the challenges that traditional log applications faced such as unreliable and clunky log aggregators, analytic components and system connectors. The system has features that make big data collection relatively straightforward, complex and reliable log data analysis and easily understandable information reporting. With attention to advanced evasion techniques, SIEM solutions are reliable and effective as compared to other traditional security techniques used to provide security for an enterprise. Further, the advancement in the design of today’s SIEM makes them perform better despite the coordinated and comprehensive view of the security status and requirements in the enterprise information technology environment.

The motivation for the advancement in the design the current SIEM systems is as a result of the requirements that the security tool remains ahead of the resourceful and experienced attackers who are aiming at compromising networks through the use of AETs. If the SIEM is designed and implemented well, the technology can offer a reliable and powerful tool that can detect and alert the administrators in case of threats from malicious technologies. Additionally, SIEMs are not strongly capable to detect APTs attacks unless they are used along with Data Loss Prevention (DLP) and Deep Packet Inspection (DPI). According to Ed Tittel [31], DLP solution is a system that aids to identify and prevent the unauthorized utilization of critical information and transmission of them to outside an organiazation and DPI inspects the payload of a packet data passing through the security defence technologies.

SIEMs can overcome the challenge of big data storage by enabling preprocessing to take place at the edge collectors[31]. In this case, only specific log and event data is allowed to pass through to the centralized management console. This process is reliable in reducing the volume of log and event data that is communicated, stored, and further analyzed at the central management node. However, this approach introduces a critical security issue if, for instance, the pre-processing at the edge collectors and agents wrongly filters out the relevant log data and events before a thorough analysis takes place. This challenge requires the SIEM developers and designers to come up with a way to handle the large log data and events volumes and reliability of the edge collector’s roles.

5. Evasions

5.1. Advanced Evasion Techniques (AETs)

There are different methods and techniques that aimed to evade the log data collectors. Mostly, these are attacks that evade firewalls and IDSs[14]. An experienced and motivated attacker may combine a set of techniques and tools to disguise an attack through multiple protocols[1] AETs as defined is "any evasive hacking techniques that allow an intruder to bypass security detection during a networkbased attack" [32]. Common security techniques can easily detect and prevent the well-known threats and exploits. On the contrary, it is hard for the tools to detect the advanced evasion techniques. In this case, the security tools should be capable of carrying out a thorough traffic analysis to detect any exploits by the AET. Vendors such as McAfee are developing newer tools such as the Next Generation Firewall that has the capability to analyze the traffic, detect and act on the exploits before they attack a system or network. A solution that can detect AETs should be able to decode and normalize the traffic for thorough analysis[4]. This process should happen on all the protocol layers in the network.

Internet protocols are complex, and there exist many interpretations that can be created while implementing them, giving the advanced attackers a chance to exploit the less common protocol properties to disguise an attack [33]. Furthermore, information security system may not detect an attack if the experienced attacker deliberately crafts network traffic that disregards the existing protocols. The exploit can freely penetrate the network up to the attacker's desired destination without the security system detection. Altogether, these kinds of attacks are referred to as advanced evasion techniques.

The idea behind AETs is to combine different evasion techniques possibly at multiple OSI layers with various protocols, and deliver exploit to a targeted victim. Changing evasion parameters in each attack, it would be possible to create a massive amount of different evasion combinations [34]. Thus, if the attacker can be able to exploit a weakness in one of the devices or system, the same approach could succeed on the other security devices. AETs takes advantage of the complicated internet protocols that are not

[1] http://www.mcafee.com/us/products/network-security/next-generation-firewall-technologies/anti-evasion.aspx

well implemented and understood. The attacker makes use of a rare combination of the protocol combination, resulting in the design of an attack that cannot be easily detected. In the same way, the attacker understands that there exists inspection and technical limitations on the security systems deployed for a network. AETs can exploit some weaknesses in the security system storage capacity, design flaws or speeds[34]. In the past, AETs have given attackers a chance to attack vulnerable networks without being detected by the existing information security systems. As can be seen, network security systems become ineffective against an advanced evasion technique that has a low level of traceability.

5.2. Evasion Techniques

There are a number of different approaches and techniques that can be utilized when it comes to evade security defense technologies. There are five main types of evasion techniques namely: denial of service (DoS), payload mutation, packet splitting, shellcode mutation, and duplicate insertion [35]. This chapter provides an overview of the different categories. This chapter provides an overview of categories.

5.2.1. Denial of Service

DoS attack aims at overwhelming a system resources or network bandwidth. DoS attack overwhelms resources such as the central processing unit and the intrusion prevention system memory space. The attack usually generates a large volume of packets and network traffic. Further, DoS attack usually weakens the detection algorithms. Such an attack can significantly slow down the rule matching algorithm of intrusion detection systems, such as Snort. A DoS attack manipulates and modifies the input network packet traffic exploiting the worst case execution of a rule matching algorithm. This uses backtracking and attempts to cover the possible pattern matches in the rule [39].

5.2.2. Packet splitting

Packet splitting includes TCP segmentation and IP fragmentation. This attack chops TCP stream and UDP datagrams into segments or non-overlapping fragments. The intrusion prevention system should try and reassemble those segments and fragmentations and restore them back to their original application content[14]. However, if this reassembling process fails, then the IDS may neglect a particular attack that may be embedded in the content that targets to exploit the host. Ideally, an intrusion detection system should reassemble fragmentation to detect and prevent any evasion attack. An IDS system is required to do the same as it monitors all the outgoing and incoming traffic in a host network under its supervision. However, an IDS may face challenges while monitoring and reassembling the segments and fragmentation back to their original application content. For instance, an IDS may face the challenge of limited system resources that are abundantly required to keep track of all per connection information. Some of the resources needed by the IDS for optimum functioning include the space allocated to the reassembly buffer for collecting all IP fragmentations and TCP states as well as the resulting reassembled content in a large host network [39].

5.2.3. Duplicate Insertion Technique

Duplicate insertion is an evasion technique in which an attacker inserts an overlapping or duplicate segments, or IP fragmentations to confuse the intrusion prevention system. Duplicate insertion technique depends on the intrusion prevention system supervising a host network. In effect, the host network or the victim may handle the overlapping segments inconsistently since the supervising IDS lacks relevant and related information such as the network topology. The figure below is a simple demonstration of how duplicate insertion evasion technique works.

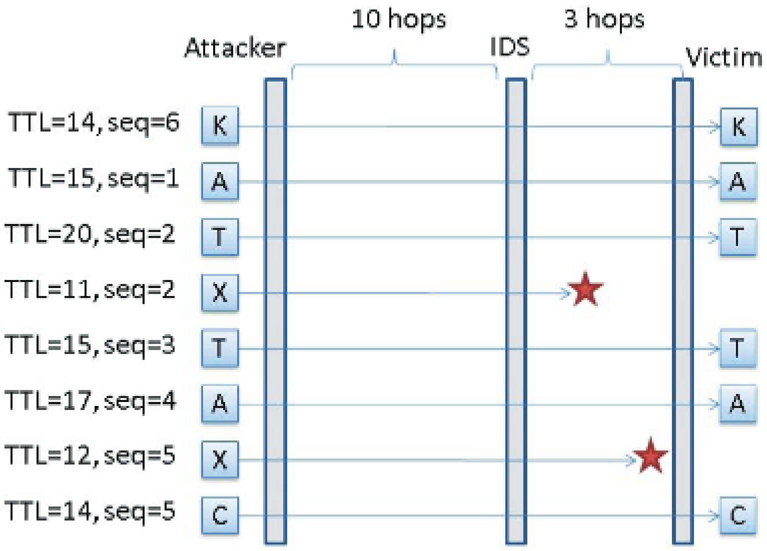


Figure 3: Duplicate insertion technique with small TTL values [39].

In the above trivial example, an attack is launched through inserting small Time to live values. The values are represented by letter X in the figure. The attacker aims to drop the values before reaching the host/target. The IDS is required to detect if the segments will reach the target for it to be able to reliably reassemble the segments and observe the same original application content as the victim. Overlapping segments are often ambiguous to the IDS. For instance, suppose that a segment bears the sequence at number ten with the content ATTXYZ. Further, another overlapping segment or fragment in the same connection has the sequence number 13 bearing the content ACK. Thus, a victim host might interpret the original application content as either ATTXYZ or ATTACK after receiving the two overlapping segments from the same connection and depending on the operating system running on the host[39].

However, a system administrator can reconfigure the operating system policy and set how the host in the internal network to interpret the packets in a way that overcomes the ambiguity. The reconfiguring process may help improve consistency between the victim and the IDS. To avoid errors while doing manual configuration, a study proposes the use of active mapping method that actively tests all hosts to derive the policy. However, there are factors that affect he mapping. Such factors arise since the mapping of the IP addresses to the victim is not one to one with use of DHCP. Further, the active testing on IP association may be imprecise and inconsistent if the firewall and other IDS filter the packets. On the other hand, there can be unexpected packet drops in the network router if the traffic volume passing the router is high.

5.2.4. Payload Mutation

Payload mutation is an evasion technique where the attacker transforms a malicious packet payload into a semantically equivalent one. A transformed payload appears different from the common signatures that an IDS expects and the attack easily can evade detection. The semantics of the transformed malicious attack remains the same, thus, the attack remains effective to a host/victim. For instance, an attacker may target a uniform resource identifier (URI) of the HTTP request. The attacker may transform the request into different mutated expression with the application of libwhisker library. The attacker applies self-reference directories, URI hexadecimal encoding, and reverse traversal directories. The techniques enable the attacker to manipulate and represent the URIs in different semantically equivalent forms. Normalization for payload mutation is often ambiguous since the host and the IDS may differ in the way they process the content. Like for duplicate insertion, payload mutation can be controlled by if the administrator configures the IDS policy to enable the IDS detect the applications on the host and improve consistency on the view of the original application payload content between the IDS and the victim host[39].

5.2.5. Shell Code Mutation

In shell code mutation evasion technique, the attack principle involves encoding a shell code into a polymorphic form. A shell code is a piece of code that exploits a host software vulnerability. The polymorphic form helps the attacker evade IDS detection that relies on signatures extracted from variants of the shell code. There are different forms that an attacker uses to achieve polymorphism[14]. For instance, shell code polymorphism can be achieved through encrypting and compressing the shell code. Further, the attacker prepend an additional piece of code that is used to decompress and decrypt the encrypted shell code to launch an exploit[14]. On the other hand, an original shell code can be replaced with a different but semantically equivalent code and instructions [39].

There are different ways of shellcode mutation such as polymorphic encodings and Alternate Encodings [36]. In effect, shellcode mutation becomes very tricky for an IDS to detect the polymorphic codes in a shell code mutation evasion attack. Furthermore, an IDS may be required to have the capability to decrypt and decompress an encrypted and compressed shell code to restore it to the original content and signature for detection purposes. On the other hand, the IDS may be required to emulate the execution of the code execution to detect a malicious behavior. Therefore, it is quite expensive to detect this evasion attack and restore the code semantics online [37].

5.3. Evasion Tools

The table below represents the evasion techniques and the tools to carry out the attack against security defence technologies [38].

Evasion Technique	Tool Name
Packet Splitting	Fragroute, Sploit, Evader[1]
Duplicate Insertion	Fragroute, Sploit, Evader
Payload Mutation	Nikito, Sploit, Havij, Evader
Shellcode Mutation	ADMutate, Sploit, Metasploit, Evader

Table 1: Evasion techniques and tools.

5.3.1. Evader

Evader[2] Launches controlled advanced evasion technique (AET) - borne attacks on the security devices installed at network, and tweaks evasions and combinations to demonstrate if the attack was successful. This tool is useful to test if a known exploit can be handovered using AETs through the current defense technology to a target host. It is an educational tool that allows network administrators, an opportunity to evaluate the resistance of their own security devices against AETs [39].

5.3.2. Fragroute

Fragroute[3] exploits TCP/IP protocols. This tool is good at duplicate insertion and packet splitting evasion techniques. It operates at the TCP/IP layer. The tool enables the attackers to evade IDS's signature matching mechanisms. In most cases, an attacker develops a simple code script that arranges the sequence of the evasion technique that will be launched and then runs Fragroute. The tool is responsible for transforming the

[1] Educational Tool

[2] http://evader.mcafee.com/

[3] http://www.monkey.org/~dugsong/fragroute/

attacker’s traffic into a format that is specified in the new script, hence successfully cheating and evading detection at the IDS.

5.3.3. Nikto

Nikto[1] transforms and modifies URI requests. This Open Source tool web scanner performs comprehensive tests against web servers for various items. The web scanning tool is capable of generating several malicious URI requests. The tool is used by developers and network administrators to test the web servers to ensure that they are secure. Additionally, Nikto helps check for server configuration items such as the multiple index files, and HTTP server options. The tool identifies the installed software and web servers and scans plugins and items to frequently and automatically update them. Moreover, Nikto provides attackers with a way of developing evasion methods used in payload mutation and help web scanner evade detection. Mostly, attackers leverage Nikto’s methods for evasion using the payload mutation technique.

5.3.4. ADMmutate

ADMmutate[2] transforms shell code to polymorphic form. The tool attempts to obfuscate the detection of the shell code by the IDS system. The principle between ADMmutate tools is fundamentally simple. The development of the tool involves building an encoding engine that wraps and compresses the exploit prior to launching an attack over a host network. Once the encoded exploit has triggered on a remote machine, it jumps to the decode engine that is sent together with the exploit. The decode engine unwraps the real exploit, and executes the original script of the shell code. To prevent this tool from launching an attack, the host system should look for the decode engine in the network. However, a decode engine may also be in a polymorphic form and appear differently each time an exploit is run.

[1] http://sectools.org/tool/nikto/

[2] https://www.sans.org/security-resources/idfaq/polymorphic_shell.php

5.3.5. Sploit

Sploit[1] is a tool for generating mutant attacks and provides a framework for the evasion techniques discussed above. The framework is designed to evaluate and test the misuse detection models in intrusion detection systems used in a network. The tool is based on an engine that applies a set of transformation techniques to the attacker's exploit script. The tool is capable of automatic generation of high number of diverse attack mutations that are executed against the victim to test the detection capability of the IDS. Furthermore, Sploit represents the perfect environment for the design, implementation, and evaluation of new evasion and mutation techniques.

5.3.6. Metasploit

Metasploit[2] provides several shell mutation encoders. Metasploit is one of the most used penetration testing software also for determining the capabilities of the supervising IDS. Thus, the tool is critical in IDS signature development and network and system exploit research. The tool supports the development of exploit scripts against a host. Further, a Metasploit Framework provides a polymorphic encoder for shell codes. The tool provides an encoder that allows a tester to exploit the scripts for evasion testing.

5.3.7. Havij

Havij [3] launches SQL injection attack and mutates the attack to avoid detection. This is an automated SQL injection tool that assists in testing and exploiting SQL injection vulnerabilities in the web page. The tool takes advantage of a vulnerable application. The tool enables a penetration tester to perform a back-end database fingerprinting. The tool enables retrieval of Database Management Systemv(DBMS) password hashes and login names, dump columns and tables, execute SQL statements against a server, fetching data from the database, accessing the file system, and executing the operating system shell commands. The tool has unique methods of SQL injection and has a success rate of attack on a vulnerable target above 95%. Further, Hajiv has a friendly

[1] https://seclab.cs.ucsb.edu/academic/projects/projects/sploit/

[2] http://www.metasploit.com/

[3] http://onhax.net/havij-adv-sql-injection-tool

graphical user interface, automated configuration, and heuristic detections that make it easy for use by amateur users. Attackers use Hajiv since it supports evasion by manipulating the white space in an attack string. Further, the tool replaces the white space with a comment syntax for a C language.

Apart from the tools discussed above, there are other tools deployed in generating evasion traffic. For example, there are multiple tools such as sqlmap, FTester, idsprobe, and AGENT. The evasion technique tools enable several combinations of evasion techniques based on methods such as payload mutations, duplicate insertion evasion, and packet splitting technique to avoid detection.

5.4. SIEMs and Advanced Evasion Techniques (AETs)

At present, the AETs are crafted and developed to penetrate a network even in cases where an organization has deployed the conventional security tools and technologies. Thus, it is becoming mandatory for enterprises to deploy an SIEM solution that aids in meeting the compliance and security requirements [40]. The commonly deployed security solutions today, such as UNIX Syslog and firewall logs are not fully effective in detecting and notifying AETs threats. Today, vendors are providing SIEM solutions that help an organization achieve all their log management needs. The current SIEM vendors can overcome the traditional beliefs and notions that made SIEM solutions be seen as complex and a service that required expertise to install and operate. In the past, organizations expressed disappointments and failures resulting from their effort of implementing SIEM solution for monitoring security in their networks.

The first SIEM solutions were not fully optimized to be able to handle more data despite their capabilities [41]. SIEMs are tasked with the requirement of collecting raw input and reducing the petabytes of raw data to a few megabytes that is more significant and can easily be understood. At present, an effective SIEM solution has an expanded raw data collection, storage, analysis, and, information reporting capabilities [42]. To reduce and filter the huge volumes of raw input further requires the solution to have distributed intelligence features. The design and development of the new SIEM solutions are also putting into account that the current technology environment is characterized by virtual and cloud features. Thus, the SIEM is capable of full and effective functioning in the emerging technology environments. Moreover, SIEM developers are incorporating new and complex algorithms that enable an SIEM solution to perform both real-time and historical analysis of log data. The solutions are capable of monitoring all event data ensuring that the data is properly collected, normalized and analyzed. Also, compliance reporting is a critical role of SIEM [43]. This next chapter discusses on the methods and implementation of a SEIM system by simulating an experiment and how it can be used to detect threats.

6. Methods and Implementation

This chapter describes the SIEM solutions and testing tool used for experiment. This study also presents the used methods to make a reliable experiment as possible, and attempts to follow an overview and explains the implementation of experiment.

6.1. The Test-bed Environment

The test environment of the study requires to match some criteria in order to evaluate and produce a desirable result of applying evasion techniques using SIEM solution. Some SIEM solutions were reviewed for the purpose of this experiment. Splunk Enterprise and AlienVault open source SIEM solutions were selected for the purpose of this experiment. The following sections presents with a brief description of SIEM solutions and its connector agent and the selected reasons behind of them, network structure and software testing tool respectively.

6.1.1. Splunk SIEM solution

Splunk SIEM was selected for this experiment due to the solution's availability and extensibility in a wide range of event log analysis and add-ons. Splunk offers support for both 32 and 64-bit architectures with capability of deploying on most of platforms [44]. Further, the solution offers a widespread range of products to convert machine data into precious data by monitoring and analyzing all system activities. This is well-known as Operational Intelligence and is the unique worth proposition of solution. Splunk allows the user easy and basic log analysis for event sources, and easy manipulation. The vendor is the most Gartner 2015, leader and challenger (Magic Quadrant for Security Information and Event Management) [45]. The latest updated version of available solutions was utilized for the experiment.

In Splunk SIEM, log data is capable to be added in two ways: uploading files from the computer (local log files, such as .CSV) and secondly, forwarding data from Splunk forwarder (SIEM agents). SIEMs provide different collector agents depends on the need. Collector agents or Forwarders represent a much more powerful solution for data forwarding rather than raw network feeds. They are capable to use SSL security and usage of any available network port, data compression, configurable buffering and tagging of metadata like source type, source, and host. The forwarding and receiving capability makes solution possible to manage functions such as load balancing, data consolidation and data routing. Splunk provides three types of forwarders: Universal forwarder, heavy forwarder and light forwarder. This experiment utilizes Universal Forwarder of Splunk SIEM as collector agent because it is free of use and has minimum features required to this experiment.

6.1.2. AlienVualt USM solution

Unified Security Management (USM) platform from AlienVault[1] of was selected as second solution for this experiment, as it provides more advanced functionality than OSSIM with single user server and deducted feature set. Further, USM supports additional capabilities like robust log management, log search for SIEM events, single/multiple server with multiple sensors that are limited on OSSIM solution. USM allows the users a free 30 days trial usability and test of its capabilities. AlienVault is recognized by Gartner as the only visionary vendor in Quadrant for SIEM in terms of simplicity and affordable approach to security [46].

Furthermore, the choice of using AlienVault is due to the fact that the solution leverages the robust ability of open source by allowing users to contribute and receive real-time data and information about malicious hosts. This is important for the study since it allows people to share ideas and information that aids improve the solution and makes it more capable to detect threats even from advanced evasion techniques. Additionally, vendor provides users with ongoing development for the product, which gives users access to the sophisticated technologies. The product is reliable and effective for both enterprises and researchers who need a SIEM solution for experimentation. The version requires to deploy on VMWare version 4.x or higher [47].

AlienVault USM uses OSSEC open source host based intrusion detection system (HIDS) as one of its base agent technologies [48]. OSSEC has a log analysis engine that is able to correlate and analyze logs from several devices and formats. The agent is a small program mounted on the systems in order to be monitored. It collects information and

[1] https://www.alienvault.com/

forward it to the manager for analysis and correlation. It also provides integrity checking, rootkit detection, Windows registry monitoring and active response.

6.1.3. Network Structure

The test-bed network consists of the attacker machine, the SIEM platforms, which collect, normalize and analyze the event logs to detect anomalies, and the target victim machine, which is included with some software vulnerabilities. The attacker and the target victim machines were connected to each other. The attacker and the target victim machines have assigned fixed IP addresses. In this experiment, it is assumed that an intruder try to misuse a network internal system (here called attacker machine) and exploits along with using multiple evasion techniques to reach victim target machine. SIEM solutions support collector agents to forward data from event sources to SIEM manager system. Universal forwarder of Splunk and OSSEC for AlienVault were configured to collect and forward event logs. VMware vSphere Hypervisor was used as virtual machine software for all systems, and promiscuous mode was enabled. The figure 4 illustrates the network structure.

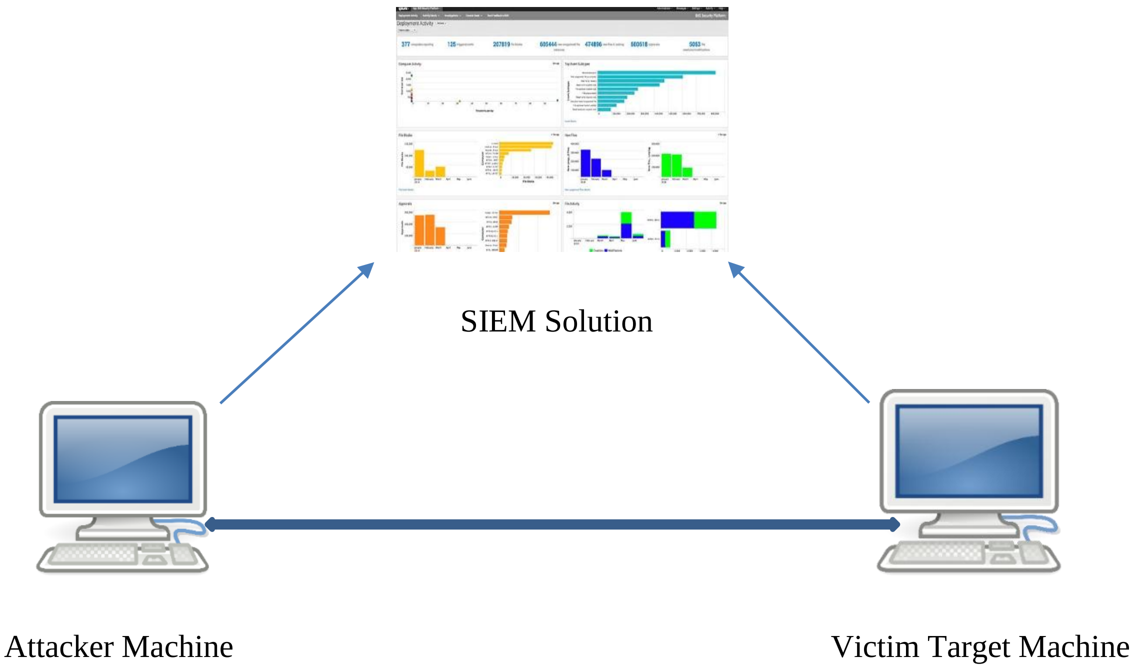


Figure 4: The used network structure

6.1.4. Software Testing Tool

Evader

This study uses free tool of Evader, automated with another tool called Mongbat - with an updated version of 2.01, from Stonesoft - as an advanced evasion software testing tool in order to test of the capabilities of security devices such as IDS/IPS or SIEM systems in detecting, alerting sophisticated different targeted attacks. The tool was released by Stonesoft at Black Hat security conference in June 2012. Evader contains both command line as well as graphical user web interface to improve ease of use. It is a ready-made test lab, providing multiple evasion techniques and can be applied in any test environment. It enables researchers and network administrators to run and assess automatically or manually a variety of AET combinations, which conceal the following of well-known exploits, delivering them through the network security devices to a vulnerable target host in an undetected way [49]. The Evader tool was used for this experiment simulation with the aim of achieving the proof of concept.

It should be noted that the tool uses combined and automatic evasion techniques in order to be undetected against security defense technologies anyhow. Further, tool implements its own TCP/IP stack that makes it possible to generate network traffic to possibly penetrate the target host without detection.

At the present, Evader uses three well known exploits including:

- **CVE-2008-4250:** MSRPC Server Service Vulnerability, which exploits windows server service vulnerability used by Conficker worm.
  Protocols used: 11 evasions for TCP, IP, SMB, NetBIOS and MSRPC.

- **CVE-2004-1315**: HTTP phpBB highlight that utilizes the arbitrary PHP code injection vulnerability in viewtopic.php, caused by insufficient validation of ‘highlight’ argument (the vulnerable server included in the evader Linux image).
  Protocols used: HTTP, TCP, IP

- **CVE-2012-0002**: Windows RDB denial of Service, which exploits the Remote Desktop vulnerability in order to produce of denial of service. There are no additional atomic evasions available.
  Protocols used: TCP, IP, RDP

Both atomic (single) and also different evasions combination were utilized to evaluate SIEM solutions and acquiring a reliable result. The evasions are applicable to variant and same OSI layers simultaneously. Further, Evader supports 18 various evasions usable for the whole three exploits using transport and network layers.

This study employed two different, Conficker and HTTP phpBB Highlight exploits versus Windows XP and Ubuntu respectively. The used principle behind of these two exploits were because they are sufficient to obtain required result and observation of the capabilities of the SIEM solutions in detecting and alerting attacks in real-time at as many as possible.

Evader provides the possibility of payload obfuscation, which means the used shellcode encoder[1] is different for each attack. Otherwise, security devices would be able to detect shellcode. Thus, tool makes effort to use randomly a new shellcode encoder at each attack execution. The tool routinely utilizes well-known shellcode encoders when obfuscation is deactivated. For instance, the Conficker exploit utilizes Fnstenv/mov Dword XOR shellcode encoder, which is a known shellcode encoder for security defense devices and uses signature-based detection [50].

Automated Mongbat

Mongbat is an accompanier fuzz testing tool for evader [51], also called the brain of Evader [52]. It allows users to make test cases in which it execute the evader over and over again, so that the weaknesses of the middle-box are discovered. In the other words, it can run multiple evader instances of evader while using specified evasion parameters for each attack versus the target host. The attacks might use either a single evasion technique at the time or a combination of different evasion techniques, in which each

[1] All exploits containing shellcode can be run 'obfuscated' – Generates a different shellcode encoder and possible NOP sled for each execution. – Makes exploit based detection harder.

attack will has its own parameters. For example, a pair of attacks with similar evasion combinations are quite different due to different parameters in the attacks. The main reason behind the choice of Stonesoft Evader and Mongbat is because they include all of the aforementioned evasion techniques, therefore making it the best option for this experiement.

6.2. Methods

In the following sections, the methods of building the experiments are discussed.

6.2.1. Statistics of used evasions

This study tested with attacks with specified evasions and evasion combinations against target victim machine in order to collect the statistics of evasion detection success while using SIEM solution under test. Several testIn detail, 18 of them can be applied against both victim machines. 11 different evasions were utiliszed against Windows XP and 9 evasions against Ubuntu.

It should be noted that during each single experiment the selected exploit remained the same, and only the evasions were changed. To achieve comparable results for specific SIEM vendor, the similar set of evasions were performed against target victim machines. It is worth noticing that this study assumed that attacker was successful to evade security devices like IDS/IPS. For example, because sophisticated attacker has either successfully compromised an inside host or has a malicious insider.

There were failures while the attack process was considered, it occurred while establishing a TCP connection without success due to a network error, or the target victim machine being under a heavy load and unable to process all the requests. Thus, in these cases, it was needed to re-execute or troubleshoot the failed attack, and then to re-execute it again.

6.2.2. SIEM Configurations

As the purpose of the experiment simulation is to examine SIEM solutions' reliability. Thus, a set of standard configurations were needed to achieve the experiment objectives. Moreover, reliable results would not be produced if the solution be configured for attack detection distinctly. Therefore, this is achievable if the solution is configured to operate properly. Naturally, all the solutions have their own specific software features and properties. Hence, having a proper standard configuration will decrease the implications caused by the different systems. There are a lot of challenges for setting up a correct and the most accurate configuration and settings for each SIEM solution. For example, different SIEM systems have their own specific log collector agents, needed to install on nodes to forward events through the network traffic. Additionally, even each solution has its own particular configuration interfaces in applying different inputs and rule policies. It is worth noticing that the lack of a common language among the different solutions by itself is not an issue, but the implementation of specific functionalities might differ much between the solutions, which means that it takes weeks to familiarize with a specific SIEM settings. There are time and index limitations to test the commercial SIEM system. For example, Splunk allows users index up to 500 MegaByte of data per day[1]. Further, the most of solutions need to be deployed on a dedicated server with specific system requirements. It is important to note that the tested SIEMs never obtain commercial benefits for the author, which is not the purpose of this work.

6.3. Implementation

This section of the paper presents discussions on the implementation of the experiment. All of the needed modifications and adjustments for the software tool and operation systems are demonstrated and explain how the process of testing and running of experiments throughout the section.

Different log sources are used in this experiment (Ubuntu and Windows XP). In this experiment, events are generated to enable the experimentation. A collector agent of SIEM solutions were installed and configured on both attacker and victim machines to collect that data into SIEM managers for indexing and consolidation. Unfortunately, Splunk does not support an agent like many other SIEM solutions for Windows XP system. Even this expeiment reviewed HP Arcsight ESM to deploy, but it is focused on the large companies and only its solution and Arcsight SmartConnector agent, support RedHat and CentOS platforms. This experiment requires to support Debian based platforms to suceed. However, OSSEC agent of AlienVault is effectively able to mount

[1] http://www.splunk.com/en_us/products/splunk-enterprise/free-vs-enterprise.html

on Windows XP SP2, identified and configured for collecting any suspisious log event and incident. The following configuration are needed to be added on Splunk Universal Forwarder outputs.conf file as an agent installed on Ubuntu attacker machine, to forward any incidents to Splunk SIEM manager on the other side:

/opt/SplunkForwarder/etc/system/local/outputs.conf

```
[tcpout]
defaultGroup = defualt-autolb-group
[tcpout: defualt-autolb-group]
Server = 172.16.120.22:9997
[tcpout-server://172.16.120.22:9997]
```

The following configuration are needed to be added and modified on OSSEC agent ossec.conf, /var/ossec/etc/ossec.conf:

```
<ossec_config>
  <client>
    <server-ip>192.168.200.129</server-ip>
  </client>
  <syscheck>
    <!-- Frequency that syscheck is executed - default 15 seconds -->
    <frequency>15</frequency>

    <!-- Directories to check  (perform all possible verifications) -->
    <directories check_all="yes">/bin,/sbin</directories>
   <directories check_all="yes">/opt,/var,/root,/usr,/home</directories>
```

The collected events from operation systems are stored into SIEMs those were forwarded by collector agents. The solutions used in this research allow the user to have a web-based control panel where the user can access a list of system settings, instances or subscribed products.

The simulated attacker system performs the Evader and the Mongbat on Ubuntu 12.04 with kernel version 2.01. The experiments will be carried out against two different Windows XP (en-US) SP2 without patches with activated remote descktop and Ubuntu

12.04 target operating systems. A minor changes were needed to perform experiment on operation systems. The following sections cover the needed modifications to the target victim operation systems.

6.3.1. Windows XP SP2

To test evasions with Conficker (CVE-2008-4250) attack, a Windows XP (en-US) SP2 without patches system was installed as a victim target machine. Some small changes were carried out into Windows registry in order to reduce requests for network work items that were queued by the network layer of the input/output (IO) stream. It occurs when the server service is unable to process the demanded network I/O items quickly enough to the hard disk and exhausts available resources. The following of DWORD registry values were needed to be added into:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanman server\parameters windows registry [53]:

Description: Maximum Free Connections

Value Name: MaxFreeConnections

Data Type: REG_DWORD

Value data: 0x1000 or 4096 (decimal)

Description: Minimum Free Connections

Value Name: MinFreeConnections

Data Type: REG_DWORD

Value data: 0x100 or 256 (decimal)

6.3.2. Ubuntu 12.04

The Ubuntu Linux of Stonesoft was used as a target victim including below vulnerabilities[1] to control following services.

- Apache HTTP Server version 2.0.64
- MySQL 4.1.22
- PHP 4.2.2
- phpBB 2.0.10 (CVE-2004-1315)

To ensure connectivity to the target victim machine, it was needed to modify some variables of “sysctl.conf” system file. The reasons behind of modifications was to avoid of filling out the server’s Address Resolution Protocol (ARP) table persistently and neighbour table overflow warnings. This amend increases the threshold values.

Additionally, it was needed to reduce interval, keep-alive time and TCP keep-alive message number in order to ensure of establishing TCP connections. The following of modifications were applied in this way [54]:

```
net.ipv4.tcp_keepalive_intvl = 1
net.ipv4.tcp_keepalive_time = 2
net.ipv4.tcp_keepalive_probes = 1


net.ipv4.neigh.default.gc_thresh2 = 8192
net.ipv4.neigh.default.gc_thresh1 = 4096
net.ipv4.neigh.default.gc_thresh3 = 65536
```

[1] http://www.mcafee.com/us/resources/misc/guides/evader-users-guide.pdf

7. Lab Observations and Discussions

This chapter of the paper presents the experimental exploration of the applicability of SIEMs in detecting suspicious events in near real-time. It presents all the actual results from experiments. Further, it gives a description of the experiment analysis flow and the data detections from the results. An experimental approach will help answer the research questions and also assist in getting a deeper practical understanding of SIEM capabilities and its performance through the use of a real experiment environment.

In general, 38 different single available evasions were tested with Evader against victim machines, and using SIEM solutions to collect, analyze and alert suspicious behavior of log sources and evaluating detections. The HTTP phpBB Highlight exploit was used against Ubuntu and Conficker exploit was used against only Windows XP SP2. Each attack was masked with various evasion techniques or evasion combinations.

The deployed SIEM solutions were set on real-time mode to prove evidence of concept and observation of SIEM capabilities in detecting the advanced threats. To this, Splunk resides all security and non-security raw information in a single repository. This creates a large amount of data and will make a repository to a common user baseline and traffic activity. This baseline can help the real-time analytics to detect the outliers and anomalies that might be potential threats. Further, statistics can play an important role with this detection, by looking for incidents that are unusual standard deviations. Correlations can also aid by detecting combinations of incidents those are scarcely observed and are suspicious [55].

On the other side, AlienVault utilizes detectors to ship the large number of devices and application events generated. The events are collected and normalized before being handed overed to a central server (AlienVault Collector). Then, AlienVault SIEM server correlates and stores the events in a SQL database. The AlienVault in this expeiment, stores the events in its pre-defined mysql storage [56].

It was verified that the SIEM solution is able to interact with collector agents in receiving log events from sources before running each attack.

7.1. Experiment Results

The experiments were run with obfuscations enabled. As already mentioned the set of evasions remained the same in the experiments that were carried out against the same operation system. For example, for Windows XP exactly applied the same evasions with specified parameters when obfuscation was enabled. After performing attack, the next step is to use Search view to run a search. The search on both solutions can contain words, phrases, wildcards (*), field-value pairs, and Boolean operators such as AND, OR, and NOT. Splunk allows users to choose a smaller time range to increase the speed of the search as well as to narrow down the search results. Further, a portion of an event can be highlighted to include or exclude it from the search.

The following pie charts illustrate the results of selected experiments. In this experiment, attacks with multiple evasion combinations were performed against each victim machine under test (five minutes was enough to get results). The primary target host was Windows XP. The well-known exploit of Conficker (CVE-2008-4250) was tested with multiple combined evasions. The bellow Figures illustrate the result of applied attack and the used number of them into attacks. For example, only one Conficker exploit was deployed that was detected and it can be observable on Figure 5.

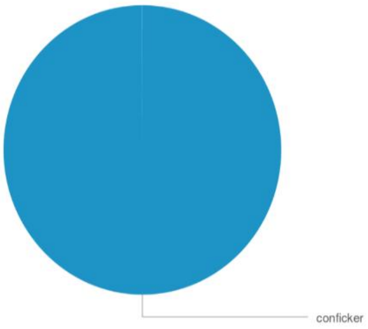


Figure 5: The detected Conficker exploit

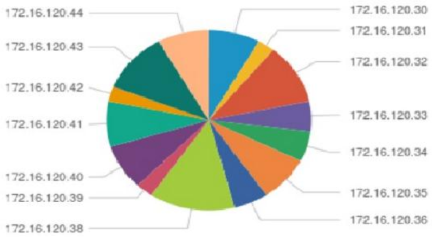


Figure 6: The detected source IP addresses

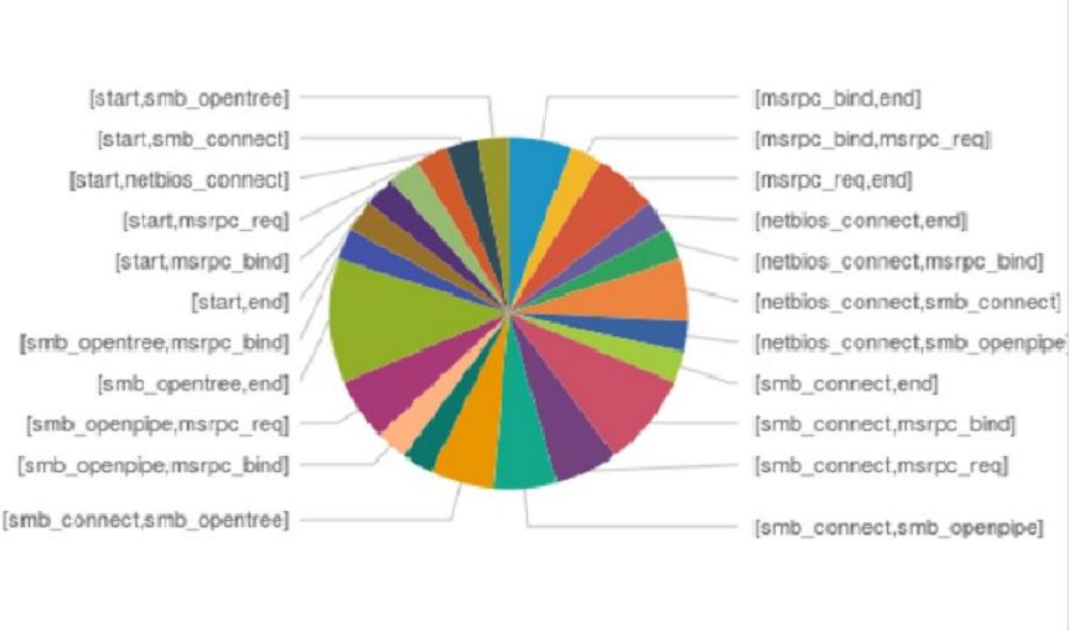
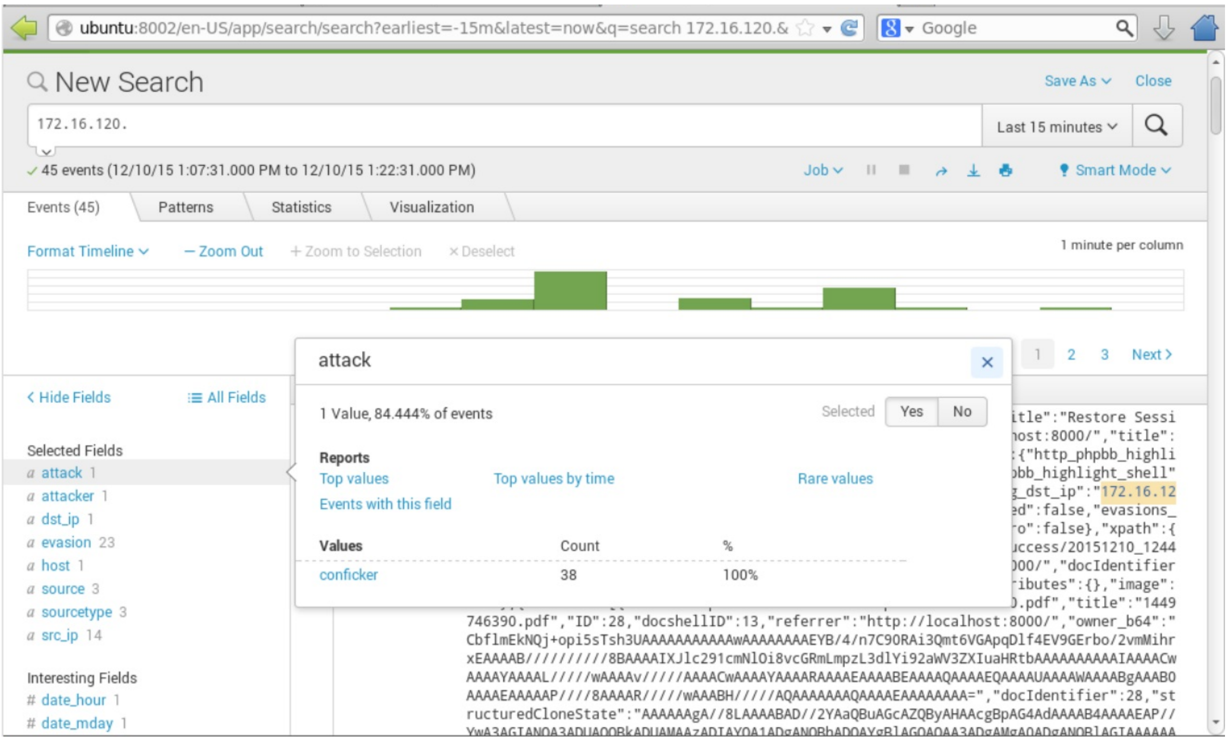


Figure 7: The detected evasion combination

The screenshot abow indicates the results of applying multiple evasion combination and the number of used evasions in this attack.

The selected screenshots bellow shows the instances of evasion combination used, identified by SIEM solutions. The following instances illustrate used evasion combinations in the attack.



ubuntu:8002/en-US/app/search/search?earliest=-15m&latest=now&q=search 172.16.120.&

New Search

Save As ∨ Close

```
172.16.120.
```

Last 15 minutes ∨

✓ 45 events (12/10/15 1:07:31.000 PM to 12/10/15 1:22:31.000 PM)

Job ∨ Smart Mode ∨

Events (45) Patterns Statistics Visualization

Format Timeline ∨ — Zoom Out + Zoom to Selection × Deselect 1 minute per column

1 2 3 Next ›

‹ Hide Fields ☰ All Fields

Selected Fields
- a attack 1
- a attacker 1
- a dst_ip 1
- a evasion 23
- a host 1
- a source 3
- a sourcetype 3
- a src_ip 14

Interesting Fields
- # date_hour 1
- # date_mday 1

attack

1 Value, 84.444% of events

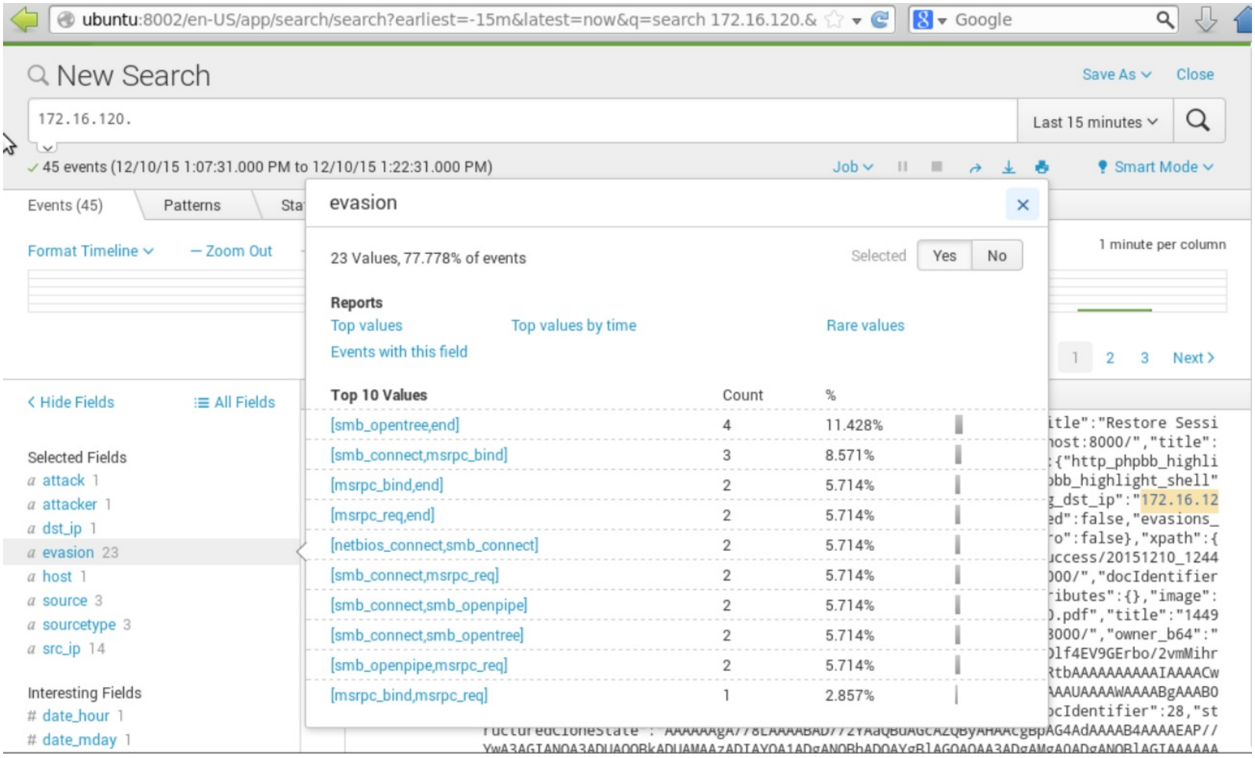
Selected Yes No

Reports
Top values Top values by time Rare values
Events with this field

Values	Count	%
conficker	38	100%

```
itle":"Restore Sessi
host:8000/","title":
:{"http_phpbb_highli
bbb_highlight_shell"
_dst_ip":"172.16.12
ed":false,"evasions_
ro":false},"xpath":{
uccess/20151210_1244
000/","docIdentifier
ributes":{},"image":
).pdf","title":"1449
746390.pdf","ID":28,"docshellID":13,"referrer":"http://localhost:8000/","owner_b64":"
CbflmEkNQj+opi5sTsh3UAAAAAAAAAAAwAAAAAAAAEYB/4/n7C90RAi3Qmt6VGApqDlf4EV9GErbo/2vmMihr
xEAAAAB/////////8BAAAAIXJlc291cmNlOi8vcGRmLmpzL3dlYi92aWV3ZXIuaHRtbAAAAAAAAAAIAAAACw
AAAAYAAAAL/////wAAAAv/////AAAACwAAAAYAAAARAAAAEAAAABEAAAAQAAAAEQAAAAUAAAAWAAAABgAAAB0
AAAAEAAAAAP////8AAAAR/////wAAABH/////AQAAAAAAAQAAAAEAAAAAAAAA=","docIdentifier":28,"st
ructuredCloneState":"AAAAAAgA//8LAAAABAD//2YAaQBuAGcAZQByAHAAcgBpAG4AdAAAAB4AAAAEAP//
```

Figure 8: An overview of scanning the event logs in Splunk.



ubuntu:8002/en-US/app/search/search?earliest=-15m&latest=now&q=search 172.16.120.&

New Search

Save As ∨ Close

```
172.16.120.
```

Last 15 minutes ∨

✓ 45 events (12/10/15 1:07:31.000 PM to 12/10/15 1:22:31.000 PM)

Job ∨ Smart Mode ∨

Events (45) Patterns Sta

Format Timeline ∨ — Zoom Out 1 minute per column

1 2 3 Next ›

‹ Hide Fields ☰ All Fields

Selected Fields
- a attack 1
- a attacker 1
- a dst_ip 1
- a evasion 23
- a host 1
- a source 3
- a sourcetype 3
- a src_ip 14

Interesting Fields
- # date_hour 1
- # date_mday 1

evasion

23 Values, 77.778% of events

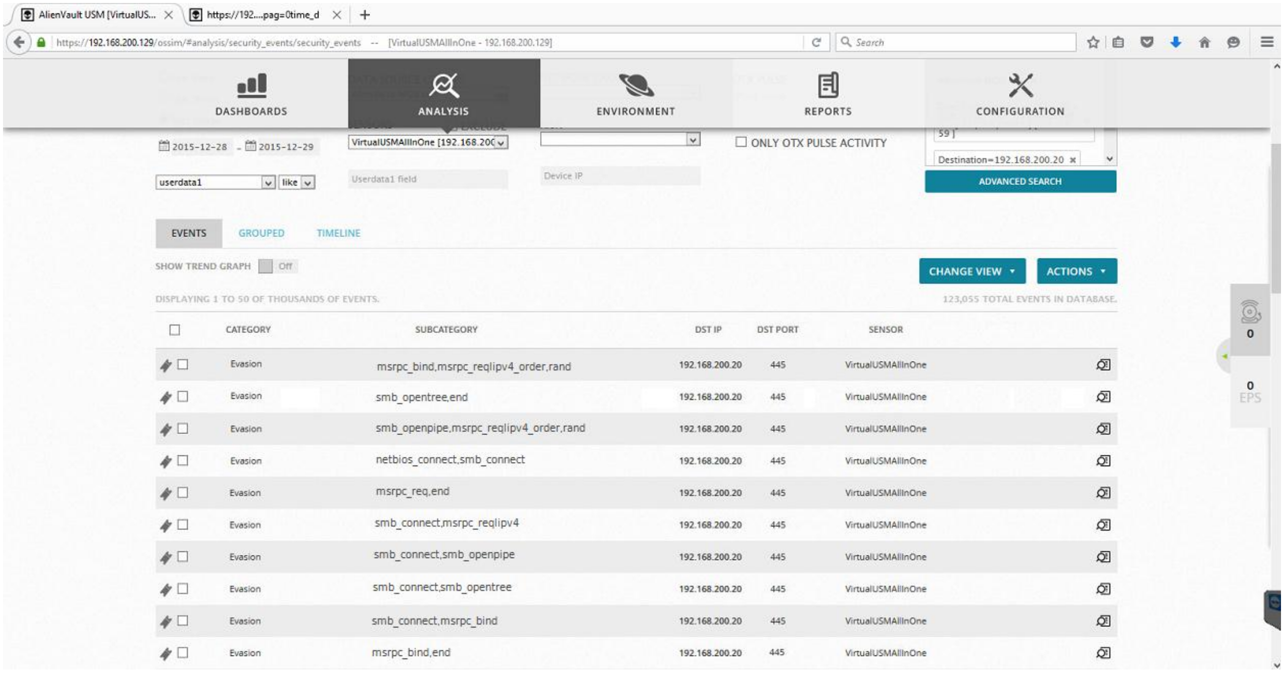
Selected Yes No

Reports
Top values Top values by time Rare values
Events with this field

Top 10 Values	Count	%
[smb_opentree,end]	4	11.428%
[smb_connect,msrpc_bind]	3	8.571%
[msrpc_bind,end]	2	5.714%
[msrpc_req,end]	2	5.714%
[netbios_connect,smb_connect]	2	5.714%
[smb_connect,msrpc_req]	2	5.714%
[smb_connect,smb_openpipe]	2	5.714%
[smb_connect,smb_opentree]	2	5.714%
[smb_openpipe,msrpc_req]	2	5.714%
[msrpc_bind,msrpc_req]	1	2.857%

```
itle":"Restore Sessi
host:8000/","title":
:{"http_phpbb_highli
bbb_highlight_shell"
_dst_ip":"172.16.12
ed":false,"evasions_
ro":false},"xpath":{
uccess/20151210_1244
000/","docIdentifier
ributes":{},"image":
).pdf","title":"1449
3000/","owner_b64":"
Dlf4EV9GErbo/2vmMihr
RtbAAAAAAAAAAIAAAACw
AAAUAAAAWAAAABgAAAB0
ocIdentifier":28,"st
```

Figure 9: An overview of scanning the event logs in Splunk.



AlienVault USM [VirtualUS...
https://192....pag=0time_d
https://192.168.200.129/ossim/#analysis/security_events/security_events -- [VirtualUSMAllInOne - 192.168.200.129]
Search
DASHBOARDS
ANALYSIS
ENVIRONMENT
REPORTS
CONFIGURATION
ADVANCED SEARCH
EVENTS
GROUPED
TIMELINE
CHANGE VIEW
ACTIONS

2015-12-28 - 2015-12-29

VirtualUSMAllInOne [192.168.20(

□ ONLY OTX PULSE ACTIVITY

59]

Destination=192.168.200.20

userdata1 like

Userdata1 field

Device IP

SHOW TREND GRAPH Off

DISPLAYING 1 TO 50 OF THOUSANDS OF EVENTS.

123,055 TOTAL EVENTS IN DATABASE.

0

0 EPS

□	CATEGORY	SUBCATEGORY	DST IP	DST PORT	SENSOR
□	Evasion	msrpc_bind,msrpc_reqlipv4_order,rand	192.168.200.20	445	VirtualUSMAllInOne
□	Evasion	smb_opentree,end	192.168.200.20	445	VirtualUSMAllInOne
□	Evasion	smb_openpipe,msrpc_reqlipv4_order,rand	192.168.200.20	445	VirtualUSMAllInOne
□	Evasion	netbios_connect,smb_connect	192.168.200.20	445	VirtualUSMAllInOne
□	Evasion	msrpc_req,end	192.168.200.20	445	VirtualUSMAllInOne
□	Evasion	smb_connect,msrpc_reqlipv4	192.168.200.20	445	VirtualUSMAllInOne
□	Evasion	smb_connect,smb_openpipe	192.168.200.20	445	VirtualUSMAllInOne
□	Evasion	smb_connect,smb_opentree	192.168.200.20	445	VirtualUSMAllInOne
□	Evasion	smb_connect,msrpc_bind	192.168.200.20	445	VirtualUSMAllInOne
□	Evasion	msrpc_bind,end	192.168.200.20	445	VirtualUSMAllInOne

Figure 10: An overview of the event logs in AlienVault SIEM.

To the second victim, the same different evasion combinations were performed against Ubuntu. The well-known exploit of HTTP phpBB Highlight (CVE-2004-1315) was tested with the same multiple evasion combinations. The bellow Figures illustrate the result of applied attack:

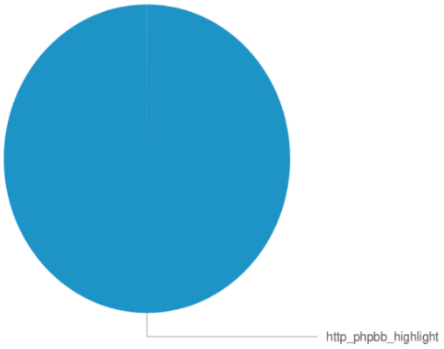


Figure 11: The detected HTTP phpBB exploit

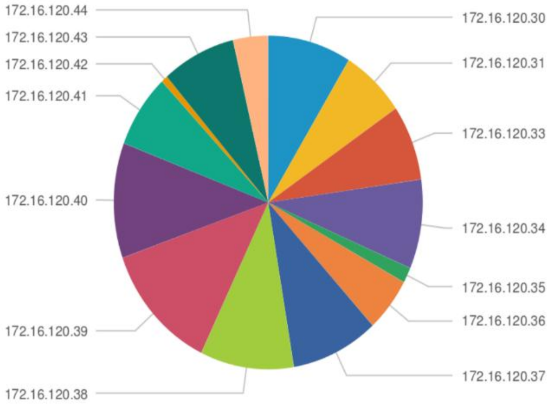


Figure 12: The detected source IP addresses

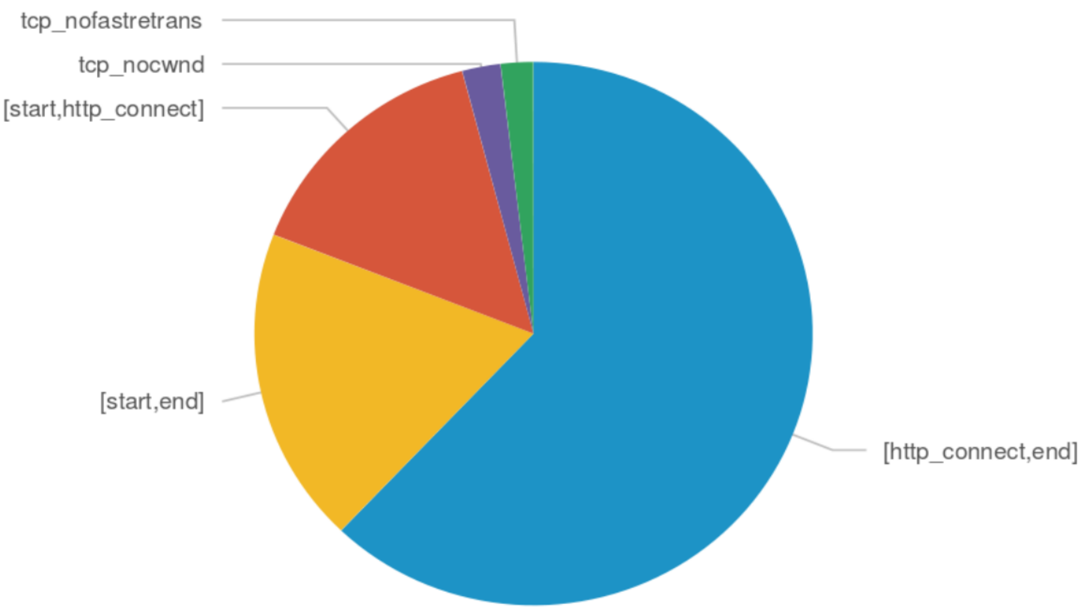
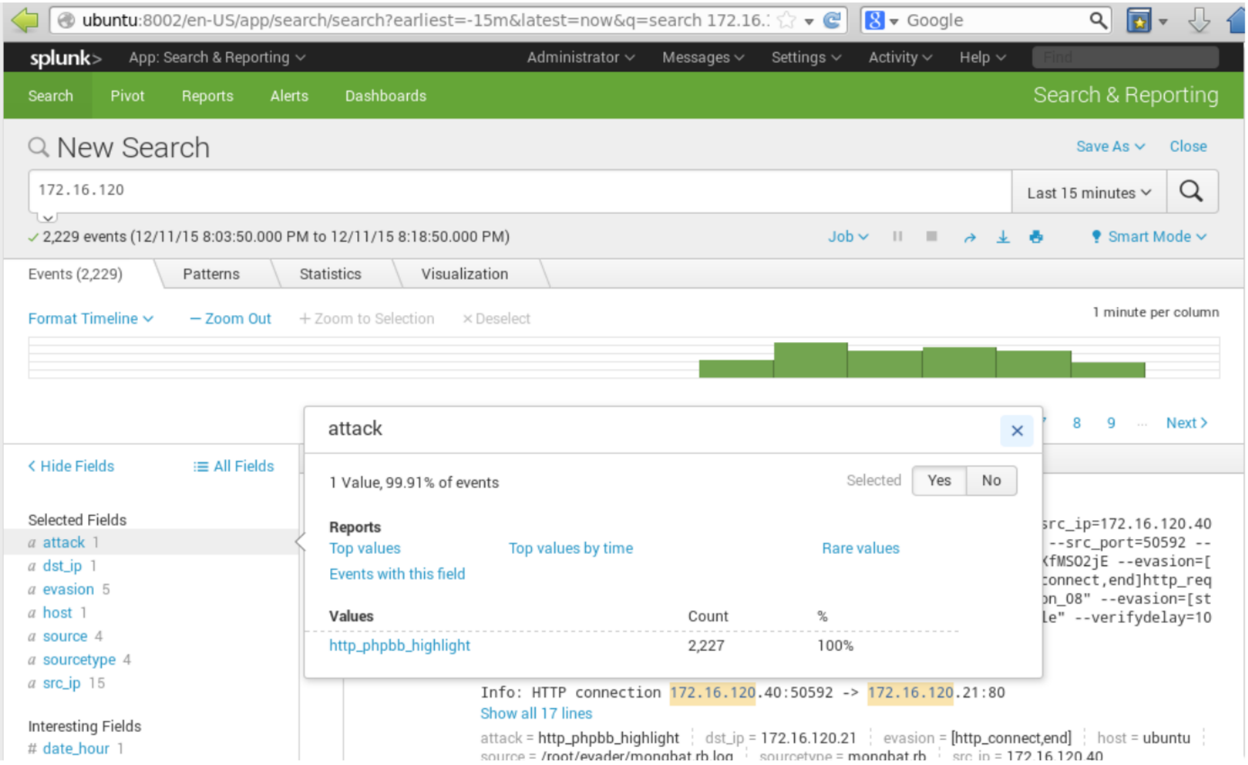


Figure 13: The detected evasion combination in running on Ubuntu.



```
172.16.120
```

✓ 2,229 events (12/11/15 8:03:50.000 PM to 12/11/15 8:18:50.000 PM)

1 Value, 99.91% of events

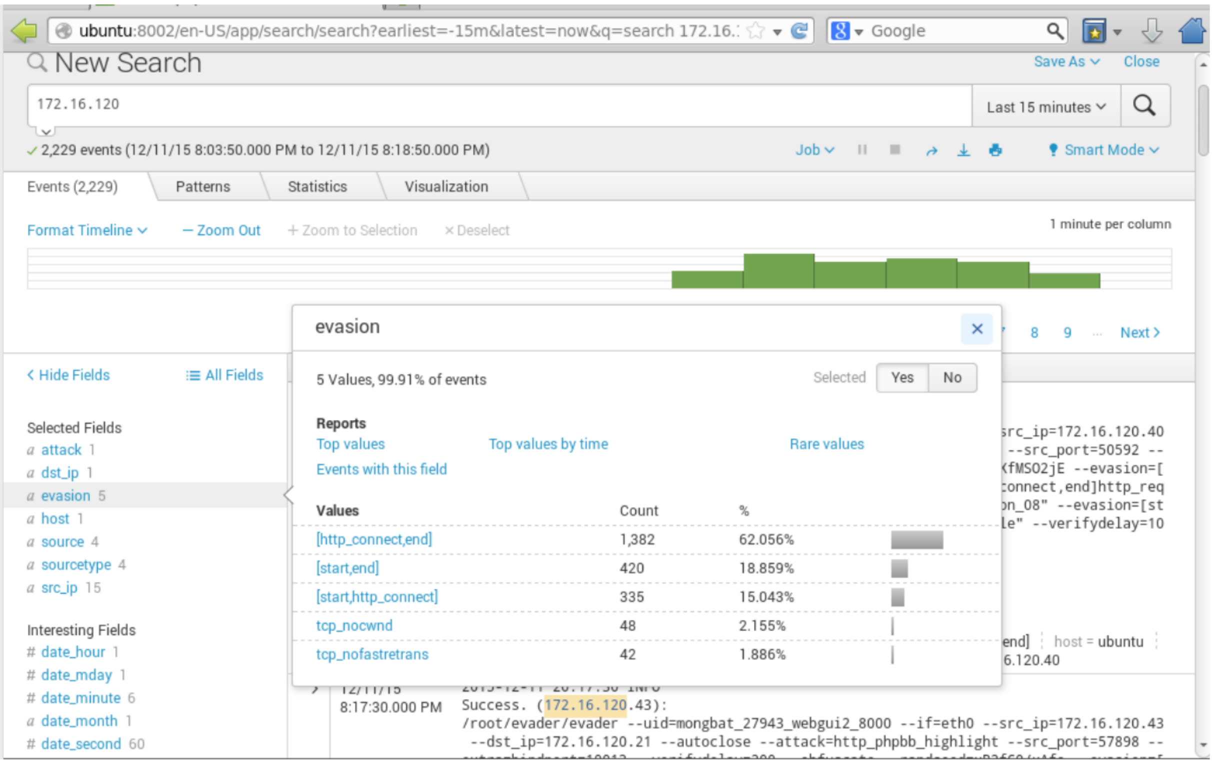
Values	Count	%
http_phpbb_highlight	2,227	100%

```
src_ip=172.16.120.40
 --src_port=50592 --
(fMSO2jE --evasion=[
connect,end]http_req
on_08" --evasion=[st
le" --verifydelay=10
```

```
Info: HTTP connection 172.16.120.40:50592 -> 172.16.120.21:80
```

attack = http_phpbb_highlight | dst_ip = 172.16.120.21 | evasion = [http_connect,end] | host = ubuntu
source = /root/evader/mongbat.rb.log | sourcetype = mongbat.rb | src_ip = 172.16.120.40

Figure 14: An overview of the event logs in Splunk.



172.16.120

✓ 2,229 events (12/11/15 8:03:50.000 PM to 12/11/15 8:18:50.000 PM)

Selected Fields
- a attack 1
- a dst_ip 1
- a evasion 5
- a host 1
- a source 4
- a sourcetype 4
- a src_ip 15

Interesting Fields
- # date_hour 1
- # date_mday 1
- # date_minute 6
- a date_month 1
- # date_second 60

evasion

5 Values, 99.91% of events

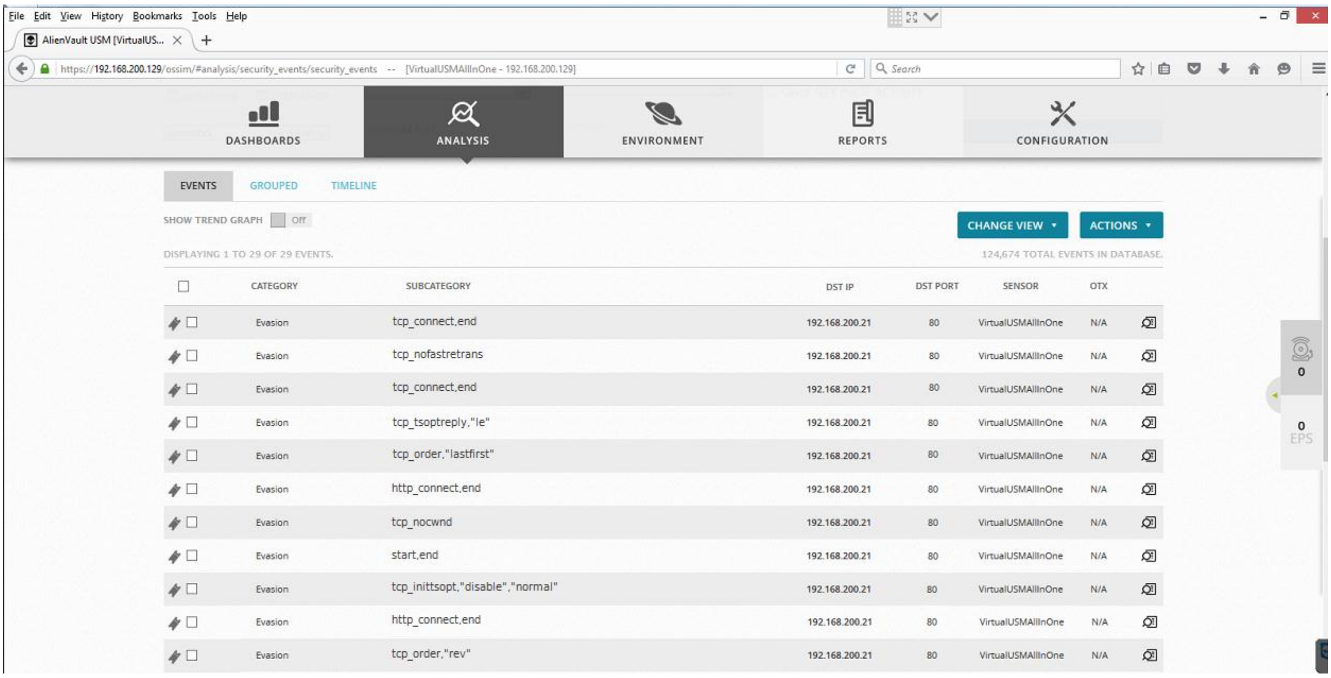
Values	Count	%
[http_connect,end]	1,382	62.056%
[start,end]	420	18.859%
[start,http_connect]	335	15.043%
tcp_nocwnd	48	2.155%
tcp_nofastretrans	42	1.886%

```
src_ip=172.16.120.40
 --src_port=50592 --
(fMSO2jE --evasion=[
connect,end]http_req
on_08" --evasion=[st
le" --verifydelay=10

end]  host = ubuntu
6.120.40
```

```
12/11/15          2015-12-11 20:17:30 INFO
8:17:30.000 PM    Success. (172.16.120.43):
                  /root/evader/evader --uid=mongbat_27943_webgui2_8000 --if=eth0 --src_ip=172.16.120.43
                   --dst_ip=172.16.120.21 --autoclose --attack=http_phpbb_highlight --src_port=57898 --
```

Figure 15: An overview of the event logs in Splunk.


File Edit View History Bookmarks Tools Help
AlienVault USM [VirtualUS...
https://192.168.200.129/ossim/#analysis/security_events/security_events -- [VirtualUSMAllInOne - 192.168.200.129]
Search
DASHBOARDS
ANALYSIS
ENVIRONMENT
REPORTS
CONFIGURATION
EVENTS
GROUPED
TIMELINE
SHOW TREND GRAPH
Off
CHANGE VIEW
ACTIONS
0
0
EPS

DISPLAYING 1 TO 29 OF 29 EVENTS.

124,674 TOTAL EVENTS IN DATABASE.

□	CATEGORY	SUBCATEGORY	DST IP	DST PORT	SENSOR	OTX
□	Evasion	tcp_connect,end	192.168.200.21	80	VirtualUSMAllInOne	N/A
□	Evasion	tcp_nofastretrans	192.168.200.21	80	VirtualUSMAllInOne	N/A
□	Evasion	tcp_connect,end	192.168.200.21	80	VirtualUSMAllInOne	N/A
□	Evasion	tcp_tsoptreply,"le"	192.168.200.21	80	VirtualUSMAllInOne	N/A
□	Evasion	tcp_order,"lastfirst"	192.168.200.21	80	VirtualUSMAllInOne	N/A
□	Evasion	http_connect,end	192.168.200.21	80	VirtualUSMAllInOne	N/A
□	Evasion	tcp_nocwnd	192.168.200.21	80	VirtualUSMAllInOne	N/A
□	Evasion	start,end	192.168.200.21	80	VirtualUSMAllInOne	N/A
□	Evasion	tcp_inittsopt,"disable","normal"	192.168.200.21	80	VirtualUSMAllInOne	N/A
□	Evasion	http_connect,end	192.168.200.21	80	VirtualUSMAllInOne	N/A
□	Evasion	tcp_order,"rev"	192.168.200.21	80	VirtualUSMAllInOne	N/A

Figure 16: An overview of the event logs in AlienVault SIEM.

7.1.1. Snort deployment

To have a solid experiment, this study also deployed Snort as an open source intrusion detection system to examine and compare achieved result of different log sources. To do this in Splunk, Snort[1] software with the last version of 2.9.8.0 and its last updated rules with v2.980 were installed in the located Splunk SIEM system. Some few changes were required into snort.conf file located at this path C:\Snort\etc:

```
# Setup the network addresses you are protecting

ipvar HOME_NET 172.16.120.0/25

# Set up the external network addresses. Leave as "any" in most
situations

ipvar EXTERNAL_NET !$HOME_NET

var RULE_PATH c:\Snort\rules

var PREPROC_RULE_PATH c:\Snort\preproc_rules

var WHITE_LIST_PATH c:\Snort\rules

var BLACK_LIST_PATH c:\Snort\rules

config logdir: c:\Snort\log

output alert_full: alert.full

Dynamic Modules
###################################################

# path to dynamic preprocessor libraries
dynamicpreprocessor directory
c:\Snort\lib\snort_dynamicpreprocessor

# path to base preprocessor engine
dynamicengine c:\Snort\lib\snort_dynamicengine\sf_engine.dll

# path to dynamic rules libraries

# dynamicdetection directory \usr\local\lib\snort_dynamicrules

preprocessor reputation: \
   memcap 500, \
   priority whitelist, \
   nested_ip inner, \
   whitelist $WHITE_LIST_PATH\white.list, \

   blacklist $BLACK_LIST_PATH\black.list

And in the local.rule file located at path:

# LOCAL RULES
```

[1] https://www.snort.org/

```
#-------------
alert icmp 172.16.120.32/27 any -> 172.16.120.21/30 any
(msg:"testing ICMP"; sid:1000001;)
alert tcp 172.16.120.32/27 any -> 172.16.120.21/30 any
(msg:"testing tcp"; sid:1000002;)

alert ip 172.16.120.32/27 any -> 172.16.120.21/30 any
(msg:"testing IP"; sid:1000003;)
```

The Splunk for Snort[1] Application was needed to integrate Snort with Splunk. It is a free application available to download and extract into:
C:\ProgramFiles\Splunk\etc\apps. Further, it was required to define an input in "files & directories" in Splunk:

C:\Snort\log with a sourcetype of snort_alerts_full

Here is the command to start snort:

```
c:\snort\bin\snort –I <NIC Number> -d -e -v -c c:\snort\etc\snort.conf
```

AlienVault USM SIEM provides several ready make detectors like Snort, Suricata, Kismet and so on. It was needed to active it from AlienVault GUI menu: Configuration → Development → Sensor Configuration → Collection

7.2. Findings and discussions

The results of experiment indicated that conducting a search on logs to find signs of launched attacks were successfull and all of the tested SIEMs including Splunk and AlienVault USM SIEM solutions were effectively able to identify attacks in near real-time correlation of networking events, report them and alert within minutes after occurring specific attacks. In detailed, comparing launched attacks with detected incidents by SIEM solutions, Splunk is able to highlight them during less than two minutes, while it is three minutes for AlienVault on average. Multiple factors can be involved in this time difference such as agent capabilities in collecting and forwarding log data and also solution’s programming structure. As already mentioned, the collected log data from heterogeneous sources such as Windows systems and Linux systems were major sources of this experiment to test detectabilities of SIEMs, due to several reason

[1] https://splunkbase.splunk.com/app/340/

intended. First, creating a clear picture between log managment and SIEM solutions. SIEMs utilize a same framework to log management, but much more unique with key features include: correlation involving both real-time and historical monitoring and analysis of event incidents, as enterprises requires real-time monitoring and notifications during anomalous activity occuring on their network hosts and systems. Prioritization by highlighting critical security events which is much more important. Regularly, scanning reports from vulnerabilities. Real-time identification and notification of incidents. Second reason can be that SIEMs are efficient in cases of feeding with logs of layered security defences or end host logs in anyway, using only end host logs were suficiant to prove evidence of concept. Third reason is that the attackers use end hosts as the first target using social tactics to penetrate other parts of enterprises' network.

This thesis examined Snort IDS as out of scope to achieve a solid proof of concept. It was observable that both solutions were feasible to detect the launched evasion combinations on the screen of SIEM solutions. They were presented with the titles such as shellcode for TCP attacks and IP fragmentation. Findings indicate that even using the prevention rules of Snort, it was able to block attacks coming from attacker machine. This can be due to the ability of Snort with being real-time intrusion detection features including reassembly of overlapping segments such as a stand-alone application component [57].

The reasons behind of these effective reactions of SIEMs can indicate that the capabilities of the correlation engines have been developed, and the researchers developing such solutions better understand attack patterns. It was possible to determine source and destination of originating attacks quickly and easily. Specially, Splunk is effectively capable to produce alerts, whenever a specific incident is detected.

The current day SIEM comes with an agent manager deployment model. Under this model, all the log sources have a light weight SIEM agent software that is installed to collect log data and forward to the manager for analysis. An attacker who gains control of a system via a compromised account for local events, or a compromised machine in a network will attempt to stop the SIEM agent services so that the attacker's unauthorized and illegitimate activities will go unnoticed.

Splunk SIEM used in the experiment counters such a malformed actions by reporting the anomaly. The advanced search will help identify the anomaly. Further, the Splunk SIEM is configured to trigger an alert if a host forwards logs with anomalies or stops forwarding the log data after the threshold limit. After an alert is received, the source is marked under attack and an incident response team starts mitigating the issue.

On the other side, OSSEC agent of AlienVault used in this experiment, performs periodically to inspect if any configured file has changed and send back the relevant logs in encrypted form to the server over UDP. Then, the logs are parsed with decoders and interpreted with rules that generate security alerts [58].

Furthermore, an attacker may forward a lot of irrelevant files after compromising the agents in case of the SIEM using files as an event source. The attacker may cause a bandwidth choke by sending a lot of the files from the event source to the manager. Such an incident affects the performance of the real-time search that is configured, as well as the storage capacity of the index used for storing logs. Such unusual and suspicious behaviors can easily be detected by search and reporting SIEM solutions. In Splunk, the field sidebar will help indicate the anomalies based on the number of values in the fields. If the number is alarming and high, the user can click on the field and start checking on the source and take mitigation measures. It also illustrates that human analyst is effective in picking out the patterns required to spot advanced attacks.

8. SIEM Future Works

At present, the internet is driving a paradigm shift whereby enterprises are deploying and managing their services and infrastructure [59]. The current enterprise is characterized by outsourced services in the cloud, infrastructures revolving to both real and virtual (hybrid), and increased use of a meshed wireless communication environment. Based on the knowledge gained from this research, it is clear that SIEM has become over time more of an information platform. The deployment of services and infrastructure in clouds has increased the deployment of SIEMs [59]. However, in the past, the technology is complex and hard to tune and identify attacks and anomalies. Notably, there has been an evolution of the SIEM solutions [60]. The current SIEM solutions are built as data stores with high input velocities and a great focus on usability, with most of the platforms offering friendly web-based user interfaces. Enterprises need to make maximum use of the SIEM tool all time to scan the data, analyze and alert in case of anomalies. However, there are still some challenges and constraints facing SIEM solution's capabilities.

The future of SIEM shows a higher deployment of the SIEM cloud solutions[59]. The future SIEM is needed to be highly scalable due to inter-organizational features of companies. The future of SIEM predicts a period of increased expectations and requirements for the SEIM. The SIEM will be required to have increased reliability to ensure increased data fidelity. The future SIME will be required to have full packet capture[60]. Further, the requirement of full packet capture is important at an age where big data will be the foundation of an effective SIEM solution.

A critical challenge that will arise as a result of cloud-based SIEM solutions that meet inter-organizational requirements will be the issue of ensuring integrity and privacy of the events in the company. Thus, security, privacy, and resilience will have an effect on the future of SIEM.

9. Conclusion

This research paper ought to discuss on SIEMs and advanced evasion techniques. The paper reviewed on the common AETs and the tools used to accomplish such attacks. This paper provides a relevant background on the evolution of information landscape and the increasing recognition of event management, log data, and a multidimensional approach to information security using the traditional methods such as firewalls and also SIEM solutions. According to the research, SIEM is considered as an advanced solution for log management as it offers features that are relevant to addressing the demands placed on the big data, dynamic and advanced nature of security threats, and the regulatory compliance. The experiment performed in this research shows how SIEM collects, filters, and normalizes, correlates, alerts, and reports any suspicious behavior of the systems flow. Therefore, this research concludes that SIEM solutions, if rightly identified and deployed, can help in the identification and alerting of advanced evasion techniques and other critical attacks.

References

[1] Mcafee, „SIEM Advanced Threat Detection, Look beyond the perimeter to stop attacks targeting data,“ 2015. [Võrgumaterjal]. Available: www.mcafee.com/us/resources/solution-briefs/sb-esm-vormetric.pdf.

[2] A.Raitz, D.Goldburt, M.Seward, „Extracting More Value from SIEM Deployments: Integrating Splunk with ArcSight,“ Splunk, San Francisco, 2010.

[3] Rafał Leszczyna, Michał R. Wróbel, „Evaluation of Open Source SIEM for Situation Awareness Platform in the Smart Grid Environment,“ %1 *Factory Communication Systems (WFCS), IEEE World Conference on,* 2015.

[4] H. Karlzen, „An Analysis of Security Information and Event Management Systems: The Use of SIEMs for Log Collection, Management, and Analysis.,“ p. 45, January 2009.

[5] A. Williams, „Security Information and Event Management Technologies,“ kd. 10, nr 1, p. 34, February 2006.

[6] D.Miller, S. Harris, A.Harper, S. VanDyke, Ch. Blask, Security Information and Event Management (siem) Implementation., McGraw-Hill, 2011.

[7] J. M. Butler, „Benchmarking Security Information Event Management,“ SANS, 2009.

[8] Igor Anastasov, Danco Davcev, „SIEM implementation for global and distributed environments,“ %1 *Computer Applications and Information Systems (WCCAIS), 2014 World Congress*, 2014.

[9] Guillermo Suarez-Tangil, Esther Palomar, Arturo Ribagorda, Ivan Sanz, „Providing SIEM systems with self-adaptation,“ %1 *IEEE*, 2015.

[10] J. Glenn, „Security beyond the SIEM,“ 2015. [Võrgumaterjal]. Available: http://pages.arbornetworks.com/BeyondtheSIEMOnDemand-View.html.

[11] Tsung-Huan Cheng, Ying-Dar Lin, Yuan-Cheng Lai, and Po-Ching Lin, „Evasion Techniques: Sneaking Through Your Intrusion Detection/Prevention Systems,“ kd. 14, nr 4, pp. 1011 - 1020, FOURTH QUARTER 2012.

[12] A. Kibirkstis, „Role of a SIEM in Detecting Events of Interest,“ November 2009. [Võrgumaterjal]. Available: https://www.sans.org/security-resources/idfaq/siem.php.

[13] Mandiant, „M-Trends 2015: A VIEW FROM THE FRONT LINES,“ Mandiant, 2015.

[14] S. Pastrana, J. Montero-Castillo, and A. Orfila, „Evading Idss And Firewalls As Fundamental Sources Of Information In Siems,“ p. Chapter 7, 2013.

[15] N. Neves (editor) (FFCUL), N. Kuntze (Fraunhofer), C. Di Sarno (CINI), V. Vianello (UPM), „D5.1.4 - Resilient SIEM Framework Architecture, Services and Protocols,“ p. 153, Sep. 2013.

[16] I. Tibble, Security De-Engineering: Solving the Problems in Information Risk Management, CRC Press, 2012, p. 332.

[17] „Can Security Information And Event Management Tools Deliver Security Benefits And Business Value," Security, NTT Com, 2014.

[18] Raydel Montesino Stefan Fenz Walter Baluja, „Information Management & Computer Security - SIEM-based framework for security controls automation," kd. 20, nr 4, pp. 248 - 263, 2012.

[19] „Vendor Landscape plus: Security Information & Event Management.," p. 78, 2011.

[20] „DON'T BE FOOLED," McAfee, 2014.

[21] „M-Trends A view from the front lines," Mandiant,a FireEye Company.

[22] „The Security Industry's Dirty Little Secret," McAfee, 2014.

[23] A. Wang, „How Distributed Are Today's DDoS Attacks?," *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security,* pp. 1511-1513 , 2014 .

[24] J. Pescatore, „How DDoS Detection And Mitigation Can Fight Advanced Targeted Attacks," *A SANS Whitepaper,* 2013.

[25] Mcafee, „Advanced Evasion Techniques & Advanced Persistent Threats," Jan 2014. [Võrgumaterjal].

[26] A. Kibirkstis, „Role of a SIEM in Detecting Events of Interest," SANS, 2009.

[27] S. Harris, Certified Information Systems Security Professional (CISSP) All-In-One Exam Guide, McGraw Hill, 2013.

[28] D. Thomas, „Optimize Log Management, How to collect and store loges securely," 2013. [Võrgumaterjal].

[29] S. A. M. Scott Taschler, „Best Practices Guide: SIEM Orchestration," [Võrgumaterjal].

[30] M. Rothman, „SIEM Best Practices for Advanced Attack Detection.," SearchSecurity, [Võrgumaterjal]. Available: http://searchsecurity.techtarget.com/tip/SIEM-best-practices-for-advanced-attack-detection.

[31] E. Tittel, Unified Threat Management for DUMMIES, Hoboken, New Jersey: John Wiley & Sons, 2012.

[32] Stonesoft, „http://www.stonesoft-security.co.uk/solutions/aets/," [Võrgumaterjal].

[33] O.-P. Niemi, „Protect Against Advanced Evasion Techniques: Essential Design Principles," 2014.

[34] Stonesoft, „AETs," [Võrgumaterjal].

[35] Thomas H. Ptacek and Timothy N. Newsham, „Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection,“ 1998. [Võrgumaterjal].

[36] V. Robertson et al. 1, „Testing Networkbased-based Intrusion Detection Signatures Using Mutant Exploits,“ 2004.

[37] Tsung-Huan Cheng et al. 3, „Evasion Techniques: Sneaking through Your Intrusion Detection/Prevention Systems,“ *Communications Surveys & Tutorials, IEEE,* kd. 14, nr 4, pp. 1011 - 1020, 2012.

[38] Cheng, Tsung-Huan. et al. 3, „Evasion Techniques: Sneaking through Your Intrusion Detection/Prevention Systems,“ *Communications Surveys & Tutorials, IEEE,* kd. 14, nr 4, pp. 1011 - 1020, FOURTH QUARTER 2012.

[39] McAfee, „Evader,“ [Võrgumaterjal]. Available: http://evader.mcafee.com/.

[40] „Cyber Security Taken to the Next Level,“ eiqnetworks, 2015. [Võrgumaterjal]. Available: https://www.eiqnetworks.com/hybrid-saas/overview.

[41] A. Chuvakin, „Next-generation SIEM,“ 2012. [Võrgumaterjal]. Available: http://searchsecurity.techtarget.com/opinion/Marcus-Ranum-chat-Next-generation-SIEM.

[42] S.Taschler, „SIEM Orchestration, How McAfee Enterprise Security Manager can drive action, automate remediation, and,“ 2013. [Võrgumaterjal]. Available: http://www.mcafee.com/jp/resources/misc/siem-best-practices-guide.pdf.

[43] A. Kibirkstis, „Role of a SIEM in Detecting Events of Interest,“ SANS, 2009. [Võrgumaterjal]. Available: https://www.sans.org/security-resources/idfaq/siem.php.

[44] „Installation Manual,“ Splunk, [Võrgumaterjal]. Available: http://docs.splunk.com/Documentation/Splunk/6.2.0/Installation/Systemrequirements.

[45] G. a. P. J. M. q. f. S. I. a. E. M. Young, „Gartner,“ 2015. [Võrgumaterjal].

[46] „Magic Quadrant for Security Information and Event Management,“ 2015. [Võrgumaterjal]. Available: http://www.gartner.com/technology/reprints.do?id=1-2JNVI05&ct=150720&st=sb.

[47] alienvault, [Online]. Available: alienvault.com.

[48] „OSSEC,“ [Võrgumaterjal]. Available: http://ossec.github.io/index.html.

[49] Stonesoft, „Stonesoft Releases Evader 2.01 Advanced Evasion Testing Tool,“ 26 February 2013. [Võrgumaterjal].

[50] „libemu: Detecting selfencrypted shellcode in network streams,“ [Võrgumaterjal]. Available: https://www.honeynet.org/node/313.

[51] „Evader users guide,“ Stonesoft, Retrieved 27.06.2013. [Võrgumaterjal]. Available: http://evader.mcafee.com/.

[52] „Evader User's Guide,“ [Võrgumaterjal]. Available: www.mcafee.com/us/resources/misc/guides/evader-users-guide.pdf.

[53] „How to troubleshoot Event ID 2021 and Event ID 2022,“ [Võrgumaterjal]. Available: https://support.microsoft.com/en-us/kb/317249.

[54] „/proc/sys/net/ipv4 parameters (see sysctl) (LONG, can be ignored),“ 2005. [Võrgumaterjal]. Available: https://www.redhat.com/archives/redhat-install-list/2005-October/msg00105.html.

[55] „Splunk,“ [Võrgumaterjal]. Available: https://www.splunk.com/web_assets/pdfs/secure/Splunk_as_a_SIEM_Tech_Brief.pdf.

[56] AlienVault, „AlienVault Instalation Guide,“ 2011. [Võrgumaterjal]. Available: C:\Users\Mehraz\Downloads\Documents\AlienVault_Installation_Guide.pdf.

[57] ScriptRock, „Top Free Network-Based Intrusion Detection Systems (IDS) for the Enterprise,“ 2015. [Võrgumaterjal]. Available: https://www.scriptrock.com/articles/top-free-network-based-intrusion-detection-systems-ids-for-the-enterprise.

[58] „How to enable File Integrity Monitoring (FIM),“ 2014. [Võrgumaterjal]. Available: https://www.alienvault.com/doc-repo/usm/threat-detection/AlienVault_HIDS_File_Integrity_Configuration.pdf.

[59] R. Rieke, „SIEM Systems of the Future,“ 2011. [Võrgumaterjal]. Available: http://www.massif-project.eu/sites/default/files/dissemination/2011-03-31_Effectsplus-Roadmap-MASSIF.pdf.

[60] Mike. Rothman, „The past, present and future of SIEM technology,“ Searchsecurity, 2014. [Võrgumaterjal]. Available: http://searchsecurity.techtarget.com/video/The-past-present-and-future-of-SIEM-technology.

[61] „Best Practices to Make BYOD, CYOD and COPE Simple and Secure,“ Citrix, 2014.