CYBER ATTACK TRENDS ANALYSIS IN EDUCATIONAL SECTOR USING DISTRIBUTED HONEYPOTS

By

Muhammad Haseeb Jalalzai

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Information Security

August 2017

CERTIFICATE

This is to certify that **Muhammad Haseeb Jalalzai** Student of **MSIS-12** Course Reg.No: **NUST201362687MMCS25213F** has completed his MS Thesis titled **“Cyber Attack Trends Analysis in Educational Sector Using Distributed Honeypots”** under my supervision. I have reviewed his final thesis copy and am satisfied with his work.

____

Thesis Supervisor

(Baber Aslam, PhD)

Dated: _____________

ABSTRACT

Cyber attacks are evolving as a sophisticated challenge. Traditional signature based security devices (secure gateways, next generation firewalls, antivirus, IPS etc.) are not sufficient to learn attack's taxonomy. Although such measures are sufficient for identified vulnerabilities with signatures. They fail to protect zero day attacks. Hence a security tool required to spy intruders by deceiving and slowing down their attack. Honeypots or related technologies can be used for this purpose.

Considering this, distributed honeypots reviewed and analyzed the attack patterns on our educational domain (.edu.pk) which is prime focus of this research. Before this we lacked the updated and readily available recent attack trends, which is essential to equip with centralized repositories of attack patterns. The main reason behind this situation is that we have no real world Intrusion Detection Systems (IDS) in place which provides us updated information about attack patterns. The real world IDS means a system having no controlled access but has potential of analyzing and learning about a particular attack. Researcher deployed a detection mechanism consisting of distributed honeypot sensors in different universities to gather maximum data from .edu.pk ccTLD (Country Code Top Level Domain). Extensive study was carried out followed by evaluation of solutions which resulted in screening of tools used in research. Then selected honeypot tools used that fulfills our goal to analyze attack trends faced by our higher educational institutes. The focus is towards active attacks from the internet on university networks and their analysis in the form of updated attack trends.

Research aims at collecting cyber attacks data within our regional internet space and their live trends analysis. The distributed honeypot sensors were placed in between an unmonitored internet connection and firewall. This system design has ability to capture maximum amount of data since the packets are not being filtered. The results are encouraging and prove that honeypot is a demanding tool for today's cyber security world.

Current research has further derived a centralized mechanism to store and present the logs generated by honeypot in a user friendly and meaningful way. The adopted approach resulted in efficient and effective analysis.

ACKNOWLEDGMENTS

My gratitude of appreciation is expressed humbly to my thesis supervisor Dr. Baber Aslam, for all the support, patience and guidance he provided to me. I also appreciate his professional attitude toward people working with him. I would like to thank him too for the quick feedback he provided to me whenever needed.

The lectures delivered by faculty are worth appreciation for knowledge, skill, integrity and comprehensiveness. In this regard, especially Dr. Monis Akhlaq, Dr. Ashraf Masood, Dr. Imran Rashid, Lec. Waleed Bin Shahid and Assistant Professor Mian Muhammad Waseem Iqbal are highlighted for efforts and cooperation extended with kindness and affection. Moreover, the persistent support and motivation rendered by Mr. Shah Fahad, Mr. Hassan Ishfaq, Ms. Narmeen Shafqat and Mr. Irfan Butt contributed significantly in improving the research quality.

At the end, source of the very initial instinct are parents always standing by to assist and help for fulfilling career dreams of mine and infact they have been, they are and will remain inspirational for me. I deeply acknowledge the patience and support of all family in MS studies completion.

TABLE OF CONTENTS

ABSTRACT iv
ACKNOWLEDGMENTS v
TABLE OF CONTENTS vi
LIST OF FIGURES x
LIST OF TABLES xii
ACRONYMS xiii

INTRODUCTION 1
1.1 Introduction 1
1.2 Problem Statement 2
1.3 Research Aim 3
1.4 Research Objective 4
1.6 Thesis Outline 5
1.7 Conclusion 5

THEORETICAL BACKGROUND 6
2.1 Introduction 6
2.2 Honeypots 6
2.3 Types of Honeypots by Deployment 7
2.3.1 Production Honeypots 7
2.3.2 Research Honeypots 8
2.3.3 Analysis of Honeypots by Deployment 8
2.4 Types of Honeypots by Interaction 9
2.4.1 No Interaction Honeypots 9
2.4.2 Low Interaction Honeypots 9
2.4.3 Medium Interaction Honeypots 9
2.4.4 High Interaction Honeypots 10
2.5 Honeypots versus Firewalls 11
2.6 Honeypots versus IDS 11
2.7 Contextual Analysis 12
2.8 Honeypots Advantages 12
2.9 Honeypots Disadvantages 13
3.0 Conclusion 13

LITERATURE REVIEW 15
3.1 Introduction........ 15
3.2 Literature Review 15
3.2.1 ACM Library 15
3.2.2 IEEE Library 16
3.2.3 USENIX Library........ 16
3.3 Honeypot Tools 17
3.3.1 Artillery 17
3.3.2 Web Labyrinth........ 19
3.3.3 Wordpot........ 19
3.3.4 PHP MyAdmin........ 20
3.3.5 HoneyBadger........ 20
3.3.6 Honeyd........ 20
3.3.7 Amun........ 20
3.3.8 Nepenthes........ 20
3.3.9 Kippo........ 21
3.3.10 Suricata........ 21
3.3.11 ROMAN........ 21
3.3.12 Sebek 21
3.3.13 Honey Tokens........ 22
3.3.14 Honeywall........ 22
3.3.15 SpamPot........ 22
3.3.16 HoneySticks........ 22
3.3.17 WebBug 22
3.3.18 Tracker 23
3.3.19 Zip Bombs........ 23
3.4 Analysis of Honeypot Tools........ 23
3.5 Conclusion 23

RESEARCH METHODOLOGY 24
4.1 Introduction........ 24
4.2 Data Collection Techniques 24
4.3 International Honeypot Projects........ 25
4.3.1 Georgia Tech Honeynet Project 25
4.3.2 Spanish Honeynet Project........ 26
4.3.3 Brazil’s Honeynet Project........ 26
4.3.4 Tunisian Honeynet Project 26

4.3.5 UK Honeynet Project 27
4.3.6 Assert Alaskan Honeynet Project 27
4.3.7 Chinese Honeynet Project 27
4.3.8 UNC Charlotte Honeynet Alliance 27
4.3.9 Mexican Honeynet Project 28
4.3.10 Internet Systems Lab Honeynet Project 28
4.4 Analysis of Honeynet Projects 28
4.5 Conclusion 29

DATA ACQUISITION TECHNIQUES AND FRAMEWORKS 30
5.1 Introduction 30
5.2 Design Format 30
5.2.1 Location 30
5.2.2 Configurations 30
5.2.3 Architecture 31
5.3 Honeypots Methodology 31
5.3 Honeypots Frameworks 33
5.3.1 Beeswarm Honeypot Framework 33
5.3.2 OWASP WASC Distributed Web Honeypots Project 34
5.3.3 Project Honeypot 34
5.3.4 Modern Honeypot Network Framework 35
5.4 Distributed Honeypots Framework 35
5.5 Conslusion 36

PROTOTYPE DEPLOYMENT 37
6.1 Introduction 37
6.2 Scope of Research Work 37
6.3 Prototype Design Parameters 37
6.4 Hardware and Software Specifications 38
6.5 Honeypots Details 38
6.5.1 Kippo Honeypot 39
6.5.2 Dionaea Honeypot 39
6.5.3 Shockpot Honeypot 39
6.5.4 ElasticHoney Honeypot 39
6.5.5 SNORT 40
6.5.6 Suricata 40
6.5.7 Pof Honeypot 40

6.6 Distributed Honeypots Architecture 40
6.7 Honeypots Deployment 41
6.7.1 Management Node Deployment 41
6.7.2 Sensor Node Deployment 41
6.7.3 Web Based Analyzer Node Deployment 43
6.8 Conclusion 44

RESULTS AND ANALYSIS 45
7.1 Introduction 45
7.2 Thesis Scope and Research Paradigm 45
7.3 Prototype Evaluation and Testing 46
7.4 Results and Analysis 47
7.4.1 Results of Kippo Honeypot 47
7.4.2 Results of Dionaea Honeypot 54
7.4.3 Results of Shockpot Honeypot 58
7.4.4 Results of ElasticHoney Honeypot 60
7.4.5 Results of SNORT and Surricata Honeypot 65
7.4.6 Results of p0f Honeypot 69
7.5 Conclusion 73

CONCLUSION AND FUTURE WORK 74
8.1 Introduction 74
8.2 Summary of Attack Statistics 74
8.3 Conclusion 80
8.4 Future Work 81

Appendix “A” – Management Node Installation 83
Appendix “B” – Sensor Nodes Installation 85
Appendix “C” – Web Based Analyzer Node Installation 88

BIBLIOGRAPHY 91

LIST OF FIGURES

FIGURE # CAPTION……………………………………………………...……………PAGE

FIGURE 5.1: OVERVIEW OF HONEYPOTS FRAMEWORK 32
FIGURE 5.2: BEESWARM IDS OVERVIEW 34
FIGURE 5.3: NETWORK LAYOUT DIAGRAM FOR PROPOSED HONEYPOTS SETUP 35
FIGURE 6.1: ARCHITECTURE OF PROTOTYPE HONEYPOTS 40
FIGURE 6.2: HIGH LEVEL NETWORK ARCHITECTURE OF HONEYPOTS 42
FIGURE 6.3: WEBBASED DASHBOARD OF HONEYPOT SENSORS 43
FIGURE 6.4: MOBILE APP SCREENSHOT FOR A WEB BASED ANALYZER NODE 44
FIGURE 7.1: HEI HONEYPOT SENSORS INTERCONNECTIVITY 46
FIGURE 7.2: STATISTICS OF SSH ATTACKS 48
FIGURE 7.3: TOP SSH USERNAMES DETECTED 49
FIGURE 7.4: TOP SSH PASSWORDS DETECTED 49
FIGURE 7.5: SSH FAILURE VERSUS SUCCESS RATIO 50
FIGURE 7.6: NO. OF SUCCESSFUL SSH LOGINS PER DAY 51
FIGURE 7.7: TOP 20 SOURCE IP ADDRESSES OF SSH ATTACKERS 51
FIGURE 7.8: TOP SSH ATTACKERS DETAILS 53
FIGURE 7.9: OVERALL ATTACK STATISTICS OF DIONAEA HONEYPOT 55
FIGURE 7.10: NO. OF ATTACKS VERSUS HOURS 55
FIGURE 7.11: SUMMARY OF ATTACK PROBES VERSUS DESTINATION PORTS 56
FIGURE 7.12: OVERALL ATTACK STATISTICS OF SHOCKPOT HONEYPOT 59
FIGURE 7.13: STATISTICS OF SHOCKPOT HONEYPOT 59
FIGURE 7.14: OVERALL STATISTICS OF ELASTICHONEY ATTACKS 61
FIGURE 7.15: SUMMARY OF DAYWISE ATTACK STATISTICS 61
FIGURE 7.16: ELASTICHONEY SIGNATURES VERSUS DETECTION SPECTRUM 62
FIGURE 7.17: TOP ATTACKERS DETECTED BY ELASTICHONEY SENSORS 63
FIGURE 7.18: ATTACK SURFACE FROM DIFFERENT COUNTRIES 64
FIGURE 7.19: TOP CITIES OF ATTACKER’S ORIGIN 64
FIGURE 7.20: OVERALL ATTACK STATISTICS OF SNORT/SURRICATA SENSORS 65
FIGURE 7.21: HOURLY STATISTICS OF SURRICATA/SNORT HONEYPOTS 66
FIGURE 7.22: DETAILS OF OPERATING SYSTEMS USED BY ATTACKERS 69
FIGURE 7.23: OVERALL ATTACK STATISTICS OF P0F HONEYPOTS 70
FIGURE 7.24: SUMMARY OF DATEWISE ATTACK STATISTICS 70
FIGURE 7.25: TOR NETWORK EVENT STATISTICS 73
FIGURE 8.1: OVERVIEW OF OVERALL CYBER ATTACK STATISTICS 74
FIGURE 8.2: WEBBASED DASHBOARD OF HONEYPOTS 75
FIGURE 8.3: SUMMARY OF TOP ATTACKERS LOCATION 75

FIGURE 8.4: TOP HONEYPOT SENSORS WITH DESTINATION PORTS 76
FIGURE 8.5: LIST OF TOP IP ADDRESSES OF ATTACKERS 76
FIGURE 8.6: SUMMARY OF OPERATING SYSTEMS USED BY ATTACKERS 77
FIGURE 8.7: SUMMARY OF USERNAMES AND PASSWORDS USED BY ATTACKERS 77
FIGURE 8.8: SUMMARY OF TOP HASHES, URLS AND SIGNATURES 78

LIST OF TABLES

TABLE 3.1: CUSTOM BANLIST OF IPV4 ADDRESSES 18

TABLE 4.1: LIST OF COUNTRIES IN EUROCOM (LEURRE.COM) PROJECT 24

TABLE 6.1: HARDWARE SPECIFICATONS OF MANAGEMENT NODE 38

TABLE 6.2: HARDWARE OF SEPECIFICATIONS OF SENSOR NODE 38

TABLE 6.3: HARDWARE SPECIFICATIONS OF WEB BASED ANALYZER NODE 38

TABLE 7.1: TOP SSH PASSWORDS COMBINATION WITH ‘ROOT’ USERNAME 50

TABLE 7.2: LIST OF SSH COMMANDS DETECTED BY KIPPO HONEYPOT 52

TABLE 7.3: URLS LIST ACCESSED BY ATTACKERS 53

TABLE 7.4: LIST OF KIPPO SENSORS VERSUS ATTACK COUNTS 53

TABLE 7.5: ATTACKERS SSH VERSION DETAILS 53

TABLE 7.6: TOP PORTS DETECTED BY DIONAEA HONEYPOT 54

TABLE 7.7: DETAILS OF TOP ATTACKERS DETECTED BY DIONAEA HONEYPOT 56

TABLE 7.8: LIST OF URLS DETECTED BY DIONAEA HONEYPOT 57

TABLE 7.9: TOP MD5S DETECTED BY DIONAEA HONEYPOT 57

TABLE 7.10: LIST OF DIONAEA SENSORS VERSUS ATTACK COUNTS 58

TABLE 7.11: LIST OF SHOCKPOT HONEYPOT SENSORS VS NO. OF EVENTS RECORDED 60

TABLE 7.12: DETAILS OF SHOCKPOT ATTACKERS 60

TABLE 7.13: LIST OF URLS ACCESSED BY SHOCKPOT HONEYPOTS 60

TABLE 7.14: DETAILS OF HASHES DETECTED BY SHOCKPOT HONEYPOTS 60

TABLE 7.15: ELASTICHONEY SENSORS VERSUS ATTACK COUNTS 62

TABLE 7.16: PAYLOADS DETECTED BY ELASTICHONEY SENSORS 63

TABLE 7.17: SNORT SENSOR DETAILS WITH INDIVIDUAL ATTACK COUNTS 66

TABLE 7.18: LIST OF SNORT SENSORS 66

TABLE 7.19: SIGNATURE DETAILS WITH NO. OF ATTACK COUNTS 67

TABLE 7.20: SOURCE PORTS VERSUS NO. OF EVENTS OCCUR 67

TABLE 7.21: DESTINATION PORTS VERSUS NO. OF EVENTS DETECTED 68

TABLE 7.22: SNORT TOP ATTACKERS DETAILS 68

TABLE 7.23: LIST OF P0F HONEYPOT SENSORS 71

TABLE 7.24: LINK TYPE VERSUS NO. OF CONNECTIONS 71

TABLE 7.25: NMAP VERSUS NO. OF EVENTS 72

TABLE 7.26: TOP ATTACKER’S DETAILS WITH NO. OF EVENTS 72

TABLE 7.27: DESTINATION PORTS WITH NUMBER OF EVENTS 72

TABLE 8.1: SUMMARY OF TOP ATTACKERS 79

ACRONYMS

APNIC	Asia Pacific Network Information Centre
APT	Advanced Persistent Threat
ccTLD	Country Code Top Level Domain
CERT	Computer Emergency Response Team
CMS	Content Management System
CSIRT	Computer Security Incident Response Tem
CVE	Common Vulnerabilities and Expoures
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
FJWU	Fatima Jinnah Women University
HEIs	Higher Education Institutes
HTTP	Hyper Text Transfer Protocol
ICT	Information and Communication Technologies
IDS	Intrusion Detection Systems
IS	Information Security
IT	Information Technology
KUST	Kohat University of Science and Technology
MSSQL	Microsoft Structured Query Language
MTTD	Mean Time To Detect
MTTR	Mean Time To Respond
PERN	Pakistan Education and Research Network
QAU	Quaid-i-Azam University
RDP	Remote Desktop Protocol
RPC	Remote Procedure Call
SIP	Session Initiation Protocol
SSH	Secure Socket Shell
TFTP	Trivial File Transfer Protocol
URL	Uniform Resource Locator
WAN	Wide Area Network

Chapter 1

INTRODUCTION

1.1 Introduction

The exponential growth of IT industry innovation has increased the use of computers, technology and information systems from last few decades. In addition the security of IT assets is now a top most issue for all organizations including government, ministries, academia and financial sectors. The technology expansion and over dependency of various businesses and governments agencies have given exponential rise in the number of cyber interception. However, on the other hand very little attention is paid to this issue of cyber attacks as we rarely observe organized analysis and investigation. This generates a requirement of trained information security professionals [1] and the efforts of academia who can jointly do the analysis of attack trends which are being faced by most of the organization over our cyberspace.

Although, there are universities that are offering information security programs but they lack the updated readily available recent attack trends and daily based analysis reports to their students, which is essential to equip specifically academia and universities community with centralized repositories of attack patterns. The main reason behind this situation is the absence of a real world intrusion detection systems (IDS) which can provide us updated attack patterns specific to each attack [2]. Here real world IDS means those systems which do not have controlled or closed access but they have potential for analysis and learning of particular attack. Normally IT admins and university management discourage these sort of systems which are considered to be a security risk or potential threat for a campus network even prefer to deploy Information Security (IS) labs inside campus network. So universities normally have security parameters in place and they usually block or discourage the usage of port scanners, sniffers or malwares to be tested inside these networks. While there is a requirement and demand for IS professionals to learn through readily available updated attack trends. Considering this in our thesis, we have deployed distributed honeypot sensors at WAN links of different universities to review and analyze attack trends on our regional country level educational domain “.edu.pk” (ccTLD). These distributed honeypot sensors are strategically placed outside of campus network and separated from production environment, so that maximum data is gathered from internet cyberspace.

In this way InfoSec professionals are not only able to analyze live attack patterns but they can also utilize this setup to launch different attack probes, correspondingly honeypots will keep the tracks of all attacks in their log files. Here it is important to mention that by reviewing and analyzing honeypot attack data, IT security awareness and education can be enhanced. Furthermore, the production information systems can be harden by keeping in view of these attack patterns. As far as our implementation strategy is concerned we used database to parse honeypot logs, to further present them in a user-friendly interface we used log management application for effective analysis and outlines of honeypots log data. The proposed prototype will be a baseline for honeynet setup that comprises of various distributed honeypot sensors to be enhanced for further research and various cyber-attacks analysis.

1.2 Problem Statement

Now a days ICT systems are not just used for automation of the operations of working environment. They have become an integral part of our society. Conversely, proliferation of cyber attacks is also increasing day by day. Hence, government organizations, financial sectors, telecommunications, power and defense organizations etc. are among the main target of cyber attacks. These attacks are launched in hunt of military or financial gains and are originated by intruders or black hat community or even by a state agent. It has been noticed that not only the numbers of attacks have increased but the sophistication of attacks is another important issue of concern is more challenging due to rapid development of technology. Because of this, organizations are lacking in safeguarding their critical assets and failing to cope with latest cyber-attacks. Therefore, it is important to have mechanism through which latest cyber-attacks can be learned and gathered for further analysis.

The distributed honeypots setup needs to be designed to analyze latest cyber-attacks trends and live patterns of our regional internet space. Such deployment will not only gather latest attack trends but it will also provide adequate information about adversaries which are being blocked by various security controls in enterprise networks. By blocking various threats through traditional security devices we save our ICT environment to some extent but rately someone notices the type and soure of the attack. So, to learn about recent attack patterns, this sort of setup is essential to learn about the actual threats, which provides us accurate and updated information about the attack surface to which our information systems are connecting. By using honeypots for attack analysis, we not only learn attacker’s actions but we further correlate this information to protect our production systems. The data gathered by using this tool can help us in alarming infosec professionals regarding upcoming threats and attack patterns.

1.3 Research Aim

The aim of this research work is to implement honeypot sensors through which latest threats, their respective types and live statistics can be gathered for analysis. So, the research questions that motivate to work in this thesis are:

- Is there any mechanism that exists in Pakistan to check latest cyber attack statistics and its types?
- Can we have any readily available data which shows trends of these attacks and their characteristics, through which we can collect cyber-attack statistics and their trends in our region’s cyber space? “As a case study we will focus on universities internet space for attack trends and their analysis”.
- How the distributed honeypots logs can be stored centrally at one location and then presented in a easy user-friendly format for security analysts?

All attacks are sniffed by honeypots through emulated services and corresponding traces are saved in log files. As, with the passage of time data in log files grows, it becomes too difficult to extract information of an attack. In our prototype scenario, all honeypots are placed on WAN links and there is no restriction of access as they are meant to be accessed at optimum level, so the size of the log files are expected to be high. As a result, large data sets are generated and their analysis will be tedious and time consuming activity, if not organized properly. In our case of implementation, we focused on presenting honeypots logs in a user friendly and organized way. This research project is aimed to address this problem by deploying honeypots prototype with ease of access and efficient log analysis capabilities. We mean that security analysts can easily extract desired information from these large data sets log files with less efforts and time consumption. This design also has features of various outlines of graphs for quick review, different types of reports with summarized data sets and meaning full representation of logs are accessible through a web based interface. This setup can be enhanced further by launching different attack probes to our distributed honeypot sensors and then analyzing this approach apart from conventional method of studies.

Following our research questions of thesis, first we review the literature how our research questions can be addressed. Then we deployed distributed honeypots prototype keeping in view the research questions and ease of access. Finally, results were evaluated through tested prototype to confirm our research contribution in selected field.

1.4 Research Objective

Although there are variety of honeypot tools available in the market and honeypots technology is existing for the many of years. But keeping in view the scope of our research, financial constraints and time limitations, we only focus on selected honeypots with distributed architecture that addresses typical attack surface area of our case study. In our case study universities or Higher Educational Institutes (HEIs) mainly have live services like SSH, HTTP, FTP, MSSQL, MYSQL etc. So, we have selected corresponding honeypots that emulate these services like Kippo [3], SNORT [4], Suricata [5], Glastopf [6], p0f [7], Dionaea [8]. Further in this prototype deployment attributes like security appliances, network equipment, internet bandwidth, IP Scheme etc. are out of scope. This prototype consist of 19 honeypot sensors deployed at WAN links of three different geographical locations of universities with one management node whose results are furnished in this thesis report. However, we can have additional sensor nodes in our design but storage and other computation of management node must be aligned with additional load of sensor nodes.

1.5 Risk Assessment

Any hardware or software change with respect to the business needs of an organization is a continuous operation. Implementing any information system change almost always results in some change in the configuration of the information system, which changes overall security posture of Information Systems.

In this way system becomes vulnerable as it is very easy for a malware to change the registry values. For example, a famous 2008 worm Conficker. On execution, the worm replicates using a random fuction to the system directories folder. It manipulates registry settings of windows XP SP1 and SP2 by running named service through random function on affected machine. Hence making a deliberate change to the already available configurations, which otherwise need to be tested first before actual implementation in a production environment [9].

1.6 Thesis Outline

The structure of this thesis is comprised of eight chapters. The first chapter contains the need of this research work along with problem statement, aims of thesis, research questions, the methodology and research objectives. Chapter 2 presents the honeypots theoretical foundation to have better understanding of this technology and discusses the strengths of honeypots. Chapter 3 discusses literature review to learn how previous work addressed our research questions and aims. How the available literature will be utilized to address our aims and identify those areas where our prototype can bring improvements. Chapter 4 discusses the international level honeypot projects to evaluate and finalize research methodology for this research work. In Chapter 5 various honeypot frameworks are illustrated and then selective approach of distributed honeypots framework is adopted that will be used for this research project. Chapter 6 focuses on design architecture, its components and actual implementation of this thesis work. Chapter 7 contains the results of thesis work along with detailed reports. The Chapter 8 concludes the research work with the outcome and related discussion followed by the road map for future research work.

1.7 Conclusion

This chapter has covered the scope and significance of this research and how the research has been conducted. So far, Pakistan has no reporting mechanism for active attack trends analysis. This work is a milestone towards the centralized reporting of attack patterns with respect to selected information system services of our region. It will enhance the ability to detect the events of active attacks and their trend analysis specifically for the academic cyber space.

Chapter 2

THEORETICAL BACKGROUND

2.1 Introduction

The definition for honeypots is generally accepted in information security research community was defined by Spitzner, L, back in 2002. Spitzner defined “a honeypot is a security resource whose value lies is being probed, attacked or compromised” [10]. It is similar to any other computer machine, however it is placed by purpose and build to be compromised so that it provides information about the attackers [10].

2.2 Honeypots

Honeypots are low cost but high value security measures. Honeypots are network connected computer software, a device or computer system which appears to be attractive and vulnerable. It holds some good information, it sits on our network and it is not well protected realistically only exists to be attacked. In fact, it may be considered as a trip wire with a strategic objective to trap intruders using an outdated machine. When hacked, this machine is porgammed to generate an alert that some unusual activity has occured and hackers are attempting to exploit this particular machine.

Honeypots can be deployed for different purposes for achieving specific results, as defined in [10] and [11]. Most common uses of honeypots are given below.

- To distract attacker or attacks from a production environment to safeguard more valuable resources on a network.
- Honeypots are widely used to learn attacks and their tactics, actions, origin and many other associated attributes of attacks.
- Honeypots have capability to capture zero day attacks and most of the security firms are using them for this purpose from decades. So, they provide adequate information about new exploits and attacks.
- Honeypots are very useful for in-depth analysis of attacks once they are compromised or exploited.

Honeypots are highly flexible tools and they are also used to catch something called Advanced Persistent Threats (APT), the name sounds similar to hacking activity performed by Chinese hackers group in 2013 to steal US Military information [12]. Advanced Persistent Threats are very slow and long attacks with an objective to steal intellectual property and other information from the organizations. There are many other uses of honeypots, it is cost effective with high value security measures depending on the meaningful way of deployment with continuous monitoring.

2.3 Types of Honeypots by Deployment

The author of [1,10] classified honeypots into two major groups regarding their deployment methods, these are (a) production honeypots and (b) research honeypots. This major categorization is based on the purpose of its usage. Honeypots are further categorized by the author [13] with respect to their purposes and level of interaction with the attackers.

2.3.1 Production Honeypots

Production honeypots are easier to deploy, build and maintain as their functionality requirement is less than the research honeypots. Productions honeypots are valuable because they provide value to the organizations in saving their information assets. Production honeypots are used by the organization to mitigate risks and protect their production systems [14]. Production honeypots provide less information like they may provide source of attacks, which usually is exploited to perform attacks etc. But we may not know who the attackers are, how organized they are, their level of expertise and what tools they have used or are using. However, production honeypots provide us the attack patterns with limited information details. Production honeypots are designed in a way to build a replica of production systems or any specific vulnerability is exposed in the network to trap attackers. Then these alerts and indicators are helpful in reducing the risk of being intruded [15]. The information extracted from the honeypots is useful in engineering better defense systems. Moreover, the information is used to take counter measures to protect production systems against future threats. Basically, production honeypots are used to deal with attackers or the guys with malicious intentions. The commercial organizations mostly use these honeypots for strengthening their defensive systems.

2.3.2 Research Honeypots

Research honeypots are mainly used by the research firms, government agencies, defense organizations, universities and large security firms to collect maximum information about cyber attacks. They do not add any value to the organizations, instead they are used to collect maximum information about Black Hat community [14]. Mainly research honeypots are not emulated services, so necessary precautions are required to deal with these threats. The main purpose of research honeypot is to gather intelligence and to understand the behavior of attacks i.e. different ways and means used during the attack by the attackers. This information is important to learn the attacker's motives, their actions and even the attackers themselves. Research honeypots are complex to maintain and deploy. They have deeper insights and generate large data so they are time consuming from organization's perspective [13]. They are primarily used to study cyber threats and to do extensive research on available data. So, the intelligence gathering is one of the core, unique and substantial aspect of research honeypots [16]. These are very useful in detecting new forms of attacks and for network forensics.

2.3.3 Analysis of Honeypots by Deployment

These high-level categorization of honeypots is just a guideline; otherwise same honeypot tool can be used for production or research purposes. It does not matter how the tool is build but it matters how actually it is used [1]. For instance, a honeypot captures all the activities of attack and even records keystroke of attackers. If this honeypot is used by production organization, then their interest is to detect the attacker, blocking their access to the production network and further to prosecute the individuals who are involved. However, if in case it is used by research organization then the same honeypot will focus on and gather intelligence related to origin of attack, what tools or techniques are used and the detailed set of activities once they have compromised the honeypot. As we see same honeypot with same information captured is dealt differently. The only difference behind is its purpose. So, various honeypots can be used for either research or production solution.

2.4 Types of Honeypots by Interaction

Below is further categorization of honeypots with respect to level of interaction with adversaries. These types are discussed below along with corresponding tools overview that has been learned during this research work one by one.

2.4.1 No Interaction Honeypots

No interaction or in other words referred honey ports, are primarily used for log or block on full TCP connections. Basic honey ports are very simple to setup like “NetCat”, “NetSh”, “IPTABLES” on Linux etc. This is a little script of blacklisted IP Addresses and block them by pushing them out from network. In Microsoft Windows “windows PowerShell honey port” is very simple and good to block unwanted hosts.

2.4.2 Low Interaction Honeypots

Low interaction honeypots run the emulated services and they are designed in such a way that attacker will not gain the complete access once compromised. These honeypots do not have real operating system to interact with adversaries. Their deployment and maintenance is comparatively easy and simple then the medium and high interaction honeypots. Because of this reason their functionality is limited with minimized risks. Essentially these honeypots are providing basic services. For example, serving basic content and are not interactive once breached. In low interaction honeypots “Web Labyrinth” [17] is very good tool to detect people trying to scan and spying on web apps or other stuff similar. It contains random web links within the content. Another famous low interaction honeypot is “Honeyd” which is a daemon to provide front end services by simulating large network layout on a single network interface. Basically, unused space is used by the “Honeyd” [18] for publishing fake computer nodes that provides only front end service to be attacked. In addition, “Conpot” [19] is another low interaction honeypot specifically designed to capture attacks against Industrial control systems.

2.4.3 Medium Interaction Honeypots

Medium Interaction Honeypots are less sophisticated and their interactivity is fewer than high interaction honeypots. These types of honeypots do not have full-fledge operating system unlike High Interaction Honeypots but they run complicated emulated services for attackers to interact with. Although the services configured and emulated in medium interaction honeypot give impression of real operating system. Actually, they simulate something real but still it is not quite there. Medium interaction honeypots are resemblance of real services with limited functionality once breached. There are range of Medium honeypots like Honeytrap [20], Nepenthes [21], Shockpot and MwCollect [22]. Malwares can easily be collected and detected by Nepenthes and MwCollect tools. Honeytrap emulates port listeners dynamically to listen to TCP connections generated from local network streams. Shockpot honeypot is purposely designed to expose the WebApp specific vulnerability “CVE-2014-6271” and capture attacks against this vulnerability.

2.4.4 High Interaction Honeypots

This could be either an exact simulation of operating system or even a real operating system that will allow someone to compromise. In high interaction honeypots copy real systems or modify real hosts to act as honeypots to verbosely log attacker activity and capture all network and related flow data.

Essentially imitate real systems, real hosts, real services or real devices because purpose is to act as honeypots that collects data. So that it can be learned, what attacker will do together with the system or service or data. This requires a lot of dedicated monitoring to run high interaction honeypots then it need to have someone watching them because these are real systems. If someone compromises them and uses them to attack other hosts then it is a big responsibility because attacker can attack back to real production systems. This can be stopped by different techniques e.g. limiting or blocking outbound traffic or diverting their traffic to black holes etc. There must be a security control layers so that it can be monitored.

High interaction honeypots should not be built using standard image because intelligent attackers after compromising honeypot may dump them and then calculate the hash of it. Then place that hash into compromised systems. In this way, they will easily trace their work and identify the compromised systems so it is a weaker end in Honeypots which eventually brings lots of risks.

2.5 Honeypots versus Firewalls

As mentioned earlier, firewalls are basically used to block the unauthorized access to computer networks by controlling inbound and outbound traffic. So, they are placed in production networks by customizing their configurations to allow specific traffic of network and rest is blocked. In this way in case of excessive traffic firewall will completely block the traffic while in case of honeypots it has only malicious traffic so it is a rare chance that it will collapse or in case it goes down then it does not affect core business or accessibility to the production systems. Similarly, firewall generates large data of its log files due to production network and adversaries access as well, so it is difficult for network administrators to search for a specific event. While in case of honeypots it only logs attacker’s activity so it has minimal data sets and easy to utilize this information to safeguard our networks. Another aspect of firewalls is that it blocks all unnecessary traffic but it doesn’t provide indications of blocked traffic so organizations are unaware about the malicious users who are probing or attempting to penetrate the production network. Whereas honeypots not only trigger and provide alerts of attacks, they also provide the insight of attacks and probes launched against our network.

2.6 Honeypots versus IDS

The core feature of honeypot is attack detection by providing alerts and warnings. Because of its simplified design it easily fulfills and addresses the challenges which are faced by other intrusion detection systems. As in Honeypots there is rare chance of false positives and false negatives issues faced in IDS. As honeypots only have malicious traffic and only accessed by unauthorized users, while in case of IDS it is placed in production environment it has production as well as unwanted users access. Due to this reason like firewalls it generates larger size of logs which is again cumbersome to trace specific event. Another problem in IDS is it works based on known signatures or available vendor’s database, so zero day attacks cannot be detected by IDS. While in case of Honeypots all traffic is suspicious and so it records each and every event which is quite helpful in detecting zero day attacks. As in IDS large amount of data is passing, there is chance that in case of excessive traffic it can be by passed, which is very damaging and alarming for the organizations. In case of honeypots everything received is attack so definitely have lesser traffic load as compared to IDS and in case it collapses it will not affect real environment. In administrative point of view for detailed investigations and insight of attacks learning we can easily offload honeypots device for further investigations and forensics but for IDS we cannot afford this to pull offline. In this way production organizations, can derive most direct benefit from honeypots [23].

2.7 Contextual Analysis

Honeypots are very flexible and adaptative tools used for purpose based on the context. Honeypots have been used mainly for data collection regarding the adversaries and their tools in addition to origin. But it can be used for learning purposes to learn the techniques (old & new) to gather maximum information to enrich our security portfolio. Depending on the context they may be used to enhance the security for smooth functionining of the production environment i.e. organizational IT infrastructure.

2.8 Honeypots Advantages

There are many advantages to use honeypots as security tool in security arsenal, some of the key advantages are given below.

- Honeypots are good to detect zero day attacks while other security solutions which work based on signatures are unable to detect these attacks. Honeypots record each and everything that they receive, hence they are capable enough to discover new tools and tactics that are not used before.
- Honeypots have small data set value, while traditional security appliances have a lot of alerts and warnings generated on daily basis due to huge amount of production data that has to pass through them.
- Capable to capture advanced attack patterns for instance IPv6 attacks, while firewalls and other security appliances which do not have these feature sets are unable to detect these attacks.
- Using honeypots reduces the problem of false positive and false negative as they are built for Black Hats and not to be used by ordinary persons. Only blacklisted traffic will be handled by honeypots.
- Honeypot is a cost effective and minimal resource consuming device because they are only used to capture harmful and malicious activity so any low-end computer can be used with limited processing capabilities.

- Most of the honeypots are purpose built with simplicity and flexible tools. They do not have requirement for complex algorithm to be used for developing updates and signatures.
- Have capability to learn hidden or covert channel attacks because they are at end points and have potential to capture encrypted data.

2.9 Honeypots Disadvantages

The disadvantages of honeypots are also highlighted below.

- As honeypots are meant and build to be compromised, in case of lack of continuous monitoring if these compromised honeypots are placed unattended for long time. Then there is risk that attackers can take control of these machines and launch attacks to other production machines specifically in case of highly interactive honeypots where complete operating system is available for attackers to interact.
- Honeypots view the scope of attack in a microscopic way, which detects only those attacks which directly interacting with this honeypot. So, honeypots will be unable to detect other systems being compromised.
- Experienced hackers can identify honeypots either by fingerprinting the simplest mistake or error in emulated services is a signature of honeypot [1], so in result it is failure of honeypots itself. However, script kiddies or worms are not very likely to identify these types of emulated honeypots but experienced hacker can determine honeypots by their fingerprints.

The above demerits are the only reasons of failure, thus reducing their utility as a security tool. This is the main reason that changes and completely deviates present security mechanisms [12].

3.0 Conclusion

As per above information we conclude that where we use honeypot term there our intention of that honeypot system is to be compromised, attacked or to be investigated. If the honeypot system is not compromised or attacked, then it might not have any value. That is exactly opposite to our real-world production systems where we keep on trying to protect them so that they will not be probed or attacked. So, the honeypots are different from other traditional security tools, as these tools are designed and placed to address a specific problem. Like Firewalls are placed to control the inbound and outbound network traffic flows. Same is the case with Antispam engine, they are used to detect spam or junk mails and block those mails based on available database signatures. These tools are normally placed at the organization's perimeter network or inside the premises of an organization. So, that any unauthorized access to these resources be blocked immediately after detection of breach. Honeypots differ from other traditional security controls in the aspects of being a general solution to detect security loopholes and their flexibility and usability in many situations. As it can be used like a firewall to deter attacks or attackers, likewise it is also used to detect attacks as IDS works. Honeypots can be used to capture automated worms or bots and can provide an early warning of indications. It is purely up to the user what they want to achieve and get from honeypots. User can use and customize them as per requirement. But honeypots are not so easy to setup as it seems, they need a complete understanding of this technology, purpose of deployment and finally the network placement otherwise if judged then they can be more destructive.

Chapter 3

LITERATURE REVIEW

3.1 Introduction

This chapter includes the literature review of honeypots. In this chapter focus is towards honeypot technology and its variety of use cases in research work. In this regard not only the word “honeypot” is searched through the published work. There are also discussions about numerous honeypot tools.

3.2 Literature Review

For literature review, we accessed relevant researches and literature to build theoretical framework (to further extend this study). In this regard, we searched relevant literature to assess honeypot tools and their deployment approaches to collect cyber-attacks for further analysis. The most of the literature work we searched was found in ACM, IEEE, USENIX and other honeypot projects executed at international level. We used the keyword “Honeypot” in search tabs to find relevant stuff for theoretical understanding and to address our research questions. We found ACM with 80 results, IEEE Computer Society showed 416 results and 56 from USENIX publications were accessed. The literature review is further summarized into three different themes based on ACM, IEEE and USENIX selected publications in further sections. The international honeypot projects will discuss with details in Chapter 4.

3.2.1 ACM Library

From ACM library, the author Roya Ensafi, Philipp Winter and David Fifield used localize honeypot sensors to detect that China is using active probing to block the privacy-tools using hidden circumvention servers like Tor [24] . Another article from ACM is “Detecting Malicious Activity with DNS Backscatter” in which researcher [25] uses honeypots to detect malicious network activity using DNS reverse queries. The OpenSSL Heartbleed vulnerability using Amazon EC2 honeypot sensors. The author Zakir Durumeric and his other colleages analyzed various aspects of Heartbleed vulnerability like which sites are vulnerable, impact on Certificate Authority ecosystem and patching behavior [26]. Another interesting publication of ACM is regarding detection of fake likes using stealthier approach of well organized network and operated by bots. This detection was noticed by deploying a set of honeypot pages by the author Emiliano De Cristofaro and his other colleageus [27].

3.2.2 IEEE Library

From IEEE publications, the author Naomi Kuze deployed multiple honeypots in real networks to detect vulnerable websites [28]. Another interesting survey paper published in IEEE library is regarding use of honeypot as a research tool providing an opportunity for detecting different types of network attacks [29]. The honeypots usage is not only limited to legacy network attacks but also useful for advanced attacks like detection of ransomware attacks. To detect ransomware activity the researchers used the file screening service of Microsoft File Server Resource Manager feature along with EventSentry for manipulating windows security logs [30]. Another advanced usecase of honeypots is in detecting attacks for Body Area Network, where using cryptographic primitives in wearable technologies is considered as a performance overhead. For this, researchers are using fake base station along with a decoy of wearable sensors to detect malicious traffic and to provide adaptive security for BANs [31].

3.2.3 USENIX Library

In 22nd USENIX Security Symposium, a very interesting article was published in which researchers implemented a set of honeypots to identify Pay Per View (PPV) networks. The statistics show that hundred of million of fraudulent impressions were deliverd per day using PPV network, consequently a heavy loss to advertising agencies [32]. The researchers of Brazil’s CERT have deployed a network of 50 low interaction honeypots to emulate SIP servers. They are successful in tracking SIP servers abuse traffic and advice in preventing these attacks against VoIP networks [33].

Above literature review clearly illustrates that honeypot technology is massively used in research community to learn variety of attacks targeted to data networks. The objective is to learn about attacks with other associated details and collection of their data for further analysis purposes. Although after reviewing this literature we conclude that honeypots architecture is effectively used to detect and gather data of cyber-attacks. But as per our review such methodologies are not implemented in Pakistan to collect live attack statistics of regional internet space. This clearly strengthens our research question and motivate us in a way forward to carry out this research work to address this problem.

The output of honeypots data is collected in form of corresponding log files. These log files generate large data sets in case of high attack traffic and these log files consumes most of the disk space. As the size of log files increases it slows the processing time and requires extra efforts for analysis. To address this problem, the author has proposed a system which is comprised of logging and analysis module [34]. The logging module showed significant results in saving the disk space by reducing size of log file.

In this research work for effective log management, large log files are parsed at regular intervals. The parsed information is then stored in the database and this database is accessed through a friendly web interface. Hence the researchers will access the honeypot's output data through the web interface for better analysis purposes. The author has introduced another method of transferring log files from honeypot server to a central database location using scripts [35].

3.3 Honeypot Tools

Some of the honeypot tools that are commonly used for data collections are briefly reviewed in this section. Most of the tools are developed by honeynet project [36], whereas others are developed by different information security groups and most of these tools are used as part of honeynet technology understanding.

3.3.1 Artillery

Linux “Artillery” is a great tool, it takes seconds to setup very simple and useful tool [37]. The logging of Artillery is very simple we can extract logs to syslog or it has remote syslog options. We can correlate “Artillery ban list” to protect other systems. It is said to be a very simple and great tool. It also has some added feature sets e.g. it has built-in file integrity monitoring, this is a great feature to monitor data integrity by logging when file has changed on the system. We have extracted a ban list while configuring it externally on the internet, the table 3.1 on next page exhibited a view of ban lists. It is a glimpse of one-day collection after running the honeypot on the internet.

IP Addresses of Ban List			
5.141.204.17	23.21.193.217	46.22.173.133	59.157.4.2
5.143.214.67	23.62.6.137	46.50.183.70	59.175.234.194
5.175.147.196	23.62.7.139	46.102.246.202	60.10.134.50
5.175.226.248	23.62.7.154	46.105.168.204	60.12.21.162
5.196.45.103	23.66.230.19	46.108.16.114	60.13.186.5
5.196.147.120	23.94.156.184	46.118.147.179	60.32.68.243
5.196.147.122	23.94.190.146	46.149.111.39	60.154.184.44
5.196.238.108	23.95.12.234	46.149.111.40	60.191.19.185
5.196.238.112	23.95.103.243	46.151.52.48	60.191.98.3
5.196.243.187	23.102.232.112	46.151.52.61	60.191.250.71
5.206.73.17	23.227.196.23	45.151.52.191	60.206.40.81
5.231.198.67	23.227.196.206	46.151.54.46	60.210.22.136
5.254.98.54	23.227.196.219	46.151.54.56	60.213.190.98
8.23.233.115	23.227.199.72	46.166.131.154	60.250.188.9
8.254.73.28	23.227.199.91	46.155.145.113	60.250.204.147
12.21.179.99	23.227.199.93	46.242.145.95	61.8.65.109
12.201.204.248	23.235.201.32	49.156.156.99	61.19.247.71
14.17.75.3	23.249.163.114	49.212.64.102	61.19.249.88
14.17.102.168	23.249.167.202	49.236.204.180	61.40.192.56
14.23.153.98	23.254.131.223	49.238.42.139	61.60.4.27
14.140.179.62	27.34.244.186	50.23.7.242	61.132.161.130
15.126.217.94	27.102.206.54	50.57.47.17	61.150.115.126
18.111.52.125	27.112.8.214	50.250.226.178	61.152.91.20
27.123.168.210	27.123.168.210	52.0.228.224	61.153.250.118

Table 3.1:Custom Banlist of IPv4 Addresses

This is the reason why it is not recommended RDP (Remote Desktop Protocol) to open it on the internet directly because it receives hits from internet constantly whether we know or not. This one is just for FTP service port 21, mostly we see hits on port 22 and 80. As we know that port 22 and 80 are very common. So, we deployed honeypots for these services in our research project which we discussed in detail in upcoming chapter of Results and Analysis.

So, learning and gaining from attackers even from this basic honeypot when someone is trying to connect to this, just from this banlist we can learn significantly from it. It can be wrapped this into tcpdump command, use this command to run tcpdump listening on port 80. Then we put file “http.pcap” and then executed netcat on port 80 and writing all the output or whatever comes out of it to http.txt file. So, we can learn a lot from someone who tries to launch random access to our network. The Table 1 contain source IPv4 addresses from which one can build their own ban-list to their network.

3.3.2 Web Labyrinth

In low interaction Honeypots “Web Labyrinth” is very good tool to detect people trying to scan and spy web apps or other related stuff [38]. So good thing about this is it contains random web links within the content. Whenever spider sees this it clicks on these links by diving in and when the upcoming next pages open they again contain different tags and links, this keep going on going, in this way intruder gets wrapped up, it triggers that someone is spying our web apps. Hence it ends up basically on a Tor page and this will never finish crawling, correspondingly it logs and leaves footprints to a database which can be used in web scans.

3.3.3 Wordpot

The very interesting honeypot web application is “Wordpot” also configured in our prototype, actually it simulates the fake WordPress application [39]. This honeypot has significant value because WordPress is often targeted by its various exploits and it is one of the most popular CMS (Content Management System) in terms of exploits. If recent CMS exploits database is observed, it would be evident that there are a lot of exploits just in a near past. Additionally, very good and customizable honeypot as by default it comes with version 2.5, which can further be customized for latest version to download

WordPress themes, even add our own themes into it. Once it is setup and customized to a certain extent it looks very realistic.

3.3.4 PHP MyAdmin

“PHP MyAdmin” is another exciting honeypot tool, it is very simple emulator of PHP MyAdmin suite [40]. The valuable aspect of this honeypot is its configuration which uses weak passwords. Ultimately, the bots will login into it by collecting a huge amount of data from them. It triggers every single event in logs and is very helpful in learning brand new attacks against PHP MyAdmin exploits. This honeypot tool provides us an idea that we can design any fake login panel of our indigenous production app and then it can be used for reverse phishing by making the intruders feel as logged into our own portal.

3.3.5 HoneyBadger

Another useful honeypot is “Honeybadger”, this is good tool to play with. It grasp most of the data from its logs. It uses different techniques (one of the method is using Java) trying to determine the actual location of attackers by simply setting up a system having honey badger. It works accurately and pin points the exact location [41].

3.3.6 Honeyd

Honeyd [16] is used to simulate the hosts using a single computer. It is a low interaction honeypot with capability of services emulation as well as to emulate OS of different IP stack.

3.3.7 Amun

Amun [42] is older honeypot and it simulates different services and modifies the configuration. It gives us liberty regarding ports modification and then usage for listening purpose to act as honeypot.

3.3.8 Nepenthes

Nepenthes is another low interaction honeypot used to capture worms and malwares [43]. It provides the emulation of known windows vulnerabilities and when an attacker will exploit any vulnerability it downloads the payload. Through nepenthes tool the collected data contains the attacker source, shell codes with hex dumps used for exploits and the worms that was downloaded.

3.3.9 Kippo

The one we deployed in this project is Kippo, Kippo simulates SSH service. It is very tiny with python script customizable SSH service emulator [44]. It is adaptable, portable and highly configurable to look like a real SSH service at least for outside world. It logs the flat file and stores the full TTY sessions which enables it to replay the attacker activities in real time which is one of its great feature. It is the most popular honeypot on which a lot of research has already been done. That is the reason that experienced attacker can identify and differentiate between this and real Linux host. It is a very useful tool to be used as a pentest.

3.3.10 Suricata

Suricata IDS is used to catch malware files, it is customizable and very powerful tool for malware analysis. BRO IDS is also power tool. Another good tool for malware sample analysis is Cuckoo Sandbox.

3.3.11 ROMAN

ROMAN (Router Man) hunter is high interaction honeypot for Router and Switches. Basically, it acts as a real router but it can be configured as honeypot, it is very useful and easy thing to setup to learn by monitoring how attacker play with routers after gaining access to it. In this MAC addresses are grabbed and correlated to a real environment with organizational blacklist.

3.3.12 Sebek

Sebek is a kind of high interaction honeypot, which provides the rootkits of kernel modules and can be patched to Linux, Solaris and FreeBSD or Windows 32 platforms [45]. It has another feature of hiding its own presence to hide the monitoring of traffic from attacker is very useful. It is used to record the keystrokes of an attacker with read/write access capabilities to the files. It is also useful where host level data capturing is required and attacker is using some encrypted network channel.

3.3.13 Honey Tokens

Honey Tokens are easy to deploy. These are used to monitor anything that happened with the files that is file access, file modification or overall integrity. As it not only ensures integrity of files it can also be used for strings, directories or drives. Then it generates the unique logs whenever something happens.

3.3.14 Honeywall

Honeywall comes into .ISO file used to build through bootable CD ROM, it provides the high interaction level to the attacker [45]. It forms the transparent layer between two network bridges to collect data and online analysis. It is highly configurable through IPTABLES, SNORT rules, fingerprinting through p0f, keystrokes like Sebek and binary dumps can be collected using this tool.

3.3.15 SpamPot

SpamPot [46] is used to detect, collect and analyze spam emails.

3.3.16 HoneySticks

HoneySticks [47] is a bootable USB stick containing honeywall and associated Honeypots. This simplifies the honeypot deployment process, contains the bootable USB based on virtual honeynet.

3.3.17 WebBug

For Document Bugging, WebBug server [48] is easy to use tool that allows us to check the document’s bugs and track them, it is very useful tool for document tracking. The very popular way of document tracking used in emails is through images, in fact that does not have an image but a blank white box. It is tracking whether the message was opened or not. If the users allow call back then it gives location, IP Address and other necessary information. This is the reason why download of external images within the email are discouraged. This technique can be used to track attacker.

3.3.18 Tracker

Tracker [49] honeypot is used for DNS vulnerabilities; it detects the malicious traffic of DNS activity. It can find open DNS resolver and find domains which are resolving large number of hosts. Malicious DNS often collapse major part of internet traffic, keeping in view vulnerabilities of DNS it is highly recommended by Information Security researchers. So that secure mechanisms must be adopted to deploy a secure DNS. To deploy a secure DNS, another paper has been published during this research work in which various DNS security challenges are discussed and a secure approach used to deploy a PKI based DNS server [50].

3.3.19 Zip Bombs

Zip Bombs [51] are tiny little files which are expanded in to 1MB to 5 GB, used to exploits computer’s storage or consumes available free space.

3.4 Analysis of Honeypot Tools

Above mentioned honeypot tools help in identifying required feature sets of honeypots to be used in our research work. Keeping in view of research scope, where our core requirement is distributed honeypots. The single honeypot can be deployed in multiple locations and their statistics will be collected at central location, the tools like Kippo and Surricata fulfill our needs. So, above tools enables us to understand behavior of each tool.

3.5 Conclusion

The above mentioned literature concludes that honeypot technology is around for many years. This identifies the solid understanding of its use cases in research work. The chapter concludes that Pakistan is lagging behind in detection mechanism of cyber attack statistics. So, this clearly strengthens a way forward to take an initiative to gather a live attack statistics of our region. This chapter has covered the literature of honeypot and also discussed various honeypot tools used worldwide for detecting anomalies in ICT environment.

Chapter 4

RESEARCH METHODOLOGY

4.1 Introduction

In this chapter, we will discuss the available methodologies and practices that are useful in designing our new system. First we elaborate data collection techniques and then we discuss the list of international honeynet projects that have been deployed to collect the attack statistics of their corresponding cyber internet space. Next, we discuss the related projects with some details of their architecture and data collection mechanisms. In the last section, we discuss the similar level of deployments done for gathering data which strengthens the research methodology used for this work.

4.2 Data Collection Techniques

The researchers have established various monitoring techniques to observe attacker's activities on the internet. One of technique is to use dark nets or global telescope to learn global trends of internet attacks. Another existing solution is to centralize the Intrusion Detection alerts and firewalls to extract some valuable information. Although these logs will provide good overview of attack trends, but have limited information and lack accuracy. The third technique is the most useful way to get more precise information about attacks i.e distributed deployment of honeypots. With this solution, the authors F. Pouget, M. Dacier and V.H. Pham [52] have deployed distributed platform of honeypots in eleven different countries, names of countries are mentioned in table 4.1.

S. No.	Countries	S. No.	Countries
1	Australia	7	Ivory Coast
2	USA	8	Lithuania
3	Belgium	9	Poland
4	France	10	Taiwan
5	Germany	11	Colombia
6	Italy		

Table 4.1: List of Countries in Eurocom (Leurre.com) project

This large scale deployment of honeypots was done in 2005, in which CERTs (AusCERT, CERTcc) are reporting centers for all internet security incidents [50,53]. These CERTs

(Computer Emergency Response Team) disseminate information to other communities, they provide technical advises, conduct trainings, provide technical documents, coordinate responses, find and analyze product vulnerabilities. They named this large scale setup of honeypots with leurre.com [49,54] and they encourage for rest of the world to become a part of this international level honeynet project.

4.3 International Honeypot Projects

Below are some of the honeynet projects deployed to gather attack intelligence of their regional internet space.

- The Georgia Tech HoneyNet Project
- Spanish HoneyNet Project
- Brazil's HoneyTARG Honeypots Project
- Tunisian HoneyNet Project
- UK HoneyNet Project
- ASSERT Alaskan US HoneyNet Project
- Chinese HoneyNet Project (ICST)
- UNC Charlotte HoneyNet Alliance
- Mexican HoneyNet Project
- Internet Systems Lab HoneyNet Project

The above mentioned projects are initiated at national level to learn the attacks initiated around the globe to their regions. Most of these honeypots are managed by CERT and others are managed by research institutes. The overview of these projects will present in upcoming lines.

4.3.1 Georgia Tech Honeynet Project

This honeynet project is sponsored by Professor Henry L Owen from School of Electrical and Computer Engineering in Georgia Institute of Technology Istanbul, Turkey. His lab namely Network Security and Architecture (NSA) is an alliance of Honeynet project. The focus of this is towards network security, forensics and data analysis. They have collected 5 years' statistics through this honeynet and captured malware, incident traces for further dissemination to fellow researchers [55]. They developed tools for firewall, network attack trace forensics, DNS tracking, P2P network tracking, honeynet report generation and live-cd for honeymole.

4.3.2 Spanish Honeynet Project

The Spanish HoneyNet project [56] is managed by dedicated information security professionals. This honeynet project does not belong to any research institute or organization, it is non-profit research organization run by volunteers. Their aim is to learn the latest tools and tactics used by blackhat community and then share the lessons learned. Most of work belongs to opensource and they share various handy scripts for incident handling. This group engages to raise awareness by sharing the lessons learned in form of training or by sharing useful scripts. They have also published their research work in form of papers. The latest paper published in 2008 created awareness and helped to guide about deployment of wireless honeypots, based on 802.11 (WiFi) technologies. This paper provides a design and architectural overview for the deployment of wireless honeypots, coined as HoneySpot [57].

4.3.3 Brazil’s Honeynet Project

The HoneyTARG honeynet project is maintained by CERT.br i.e Brazil’s Computer Emergency Response Team (CERT). This project is meant to increase the capacity of incident detection, event correlation and trend analysis in the Brazilian Internet space [58]. This honeynet is comprised of 27 low interaction honeypots (Honeyd) sensors deployed in 27 different cities to gather threat intelligence regarding Brazil’s attack surface. This organized system will publish attack statistics related to TCP/UDP ports, AS numbers, country codes, source OS against these honeypots and notify to CSIRT (Computer Security Incident Response Team).

4.3.4 Tunisian Honeynet Project

The Tunisian honeynet project [59] developed a framework of Saher-HoneyNet which is based on collection of opensource tools used to detect attacks and their analysis is presented in friendly graphical interface. This project is maintained by tunCERT to provide trend analysis of Tunisian attack surface which includes information about malicious activities like attack trends, destination ports, malware stats, globe map with an outlined dashboard and alert mechanisms. This project is backed by experienced information security professionals and active alliance of Honeynet organization.

4.3.5 UK Honeynet Project

This project was founded in 2002 by non-profit volunteer research organization to observe the attack patterns in UK internet space [60]. Their purpose is to provide information about vulnerabilities and security incidents occurred in UK networks. This project was active till Dec 2012 and after that they are not as much active as they were before.

4.3.6 Assert Alaskan Honeynet Project

This honeynet project is established in Advanced System Security Education, Research and Training (ASSERT) lab located in Computer Science Department of University of Alaska at Fairbanks, AK, United States [47]. The goals of this lab is to provide an isolated controlled computing environment for computer security and information assurance education which includes isolated virtual machines, digital Forensics and physical SCADA lab.

4.3.7 Chinese Honeynet Project

The Chinese Honeynet project is maintained by Institute of Computer Information Security Engineering Research Center in Peking University China under China CERN “CNCERN” [61]. This project was established in 2004 and it is also member of international Honeynet Research alliance. This project is actively involved in data collection of cyber-attacks and develop tools to enhance the honeypot technology. Unfortunately, Chinese honeynet does not provide statistics and related information to the public.

4.3.8 UNC Charlotte Honeynet Alliance

This project is maintained in the University of North Carolina at Charlotte, United states [62] to improve computer security measures with the help of honeynets and other associated network tools. This setup is part of university research of network security group in Laboratory of Information and Infrastructure Security. This setup was also used to deliver information assurance trainings to the Cyber Corps of US Government.

4.3.9 Mexican Honeynet Project

The Mexican Honeynet project is initiated by UNAM-CERT called Honeynet UNAM [63], they deployed honeypot sensors across data networks of Mexico to identify malicious activities. They named the toolkit with SMART (Sensor Monitoring, Analysis and Collection of Traffic) which includes honeypot tools like honeytrap, IDSmod, Sensorview and Dionaea. This honeynet comprises of three sensors deployed in three different universities and they are planning to increase further sensors by adding more universities in this network. Through this network they have detected many attacks and malware activities in universities network space.

4.3.10 Internet Systems Lab Honeynet Project

This honeynet lab is established in a research organization in Athens, Greece [64]. Their focus is towards internet systems knowledge. It is initially a part of European Project COSINE and this lab's significant component work is based on free software opensource. This honeynet project is playing a major role in Greece education and research network. They have deployed IDS to observe reconnaissance scan activities, DDoS like Stacheldraht and malware. Their purpose is to study the attack surface of Greece in a controlled environment with the help of honeypots.

4.4 Analysis of Honeynet Projects

Above mentioned projects are being undertaken by different countries to gather cyber attack statistics of their cyber space. After reviewing all these, a storng motivation is induced to have such a setup of cyber space surveillance. In next chapter, distributed frameworks are discussed which have already been utilized to generate attack trends and provide cyber intelligence. On the basis of learning and evaluating existing frameworks, a proposed distributed honeypot model of data acquisition fits for scenario of HEIs in Pakistan will be finalized. So for, such type of setup is not existing in Pakistan and the research is going to contribute significantly in this regard.

4.5 Conclusion

The above mentioned honeynet projects suggest the number of implementations of distributed honeypots for trends analysis of specific attack surface. But most of them are deployed to learn the malicious activities of their own data networks. So, according to our review such environment is not implemented in any of the Pakistan's data network to study the trend analysis of Pakistan's internet space. The above mentioned deployments add values to this research by strengthening research question and give us the motivation for carrying out research work to address this area.

Chapter 5

DATA ACQUISITION TECHNIQUES AND FRAMEWORKS

5.1 Introduction

As presented in chapter 4 that major honeypots deployment to learn and collect cyber-attack statistics of different regional internet spaces. These honeypot projects are substantial in designing the architecture of prototype that is going to be used for this thesis work. In this research work our focus is to learn the attack patterns that are being launched specifically in our region's internet space.

5.2 Design Format

We have designed this platform based on three key elements; location, configuration and an architecture. These three elements are defined by the researchers in deploying honeypots. The analysis of honeypots data is critically affected by these factors. Therefore, selection of honeypots requires keen knowledge before actual deployment. These elements are briefly described one by one in further sections.

5.2.1 Location

In computer networks location is identified through IP addresses and here it represents the IP addresses which are used by the honeypots to collect attacks data. So, the honeypots location greatly affects the amount of data they will capture. The nature of attacks and volume is different for one IP address to others. Moreover, not only the location of honeypots is important but the size of honeypots also matters in significant collection of attacks. Keeping this element in our design we have used distributed honeypots concept which we will discuss in detail in upcoming chapters.

5.2.2 Configurations

Configurations means the honeypots services or ports that it offers for luring attacks. Different honeypots tools have different configurations with different behaviors. Some have emulated services and others have real services. They may have specific vulnerabilities to learn specific type of attack. So, there is no single solution available that can be used to detect optimal level of malicious attacks. The configuration also ensures that honeypots fingerprint is small enough that it prevents adversaries in detecting them. In this research work we have customized the default behavior of honeypots configuration at certain level, so that the deployed honeypots are hard to detect by the attackers.

5.2.3 Architecture

The architecture of honeypot refers to the kind of honeypot. We discussed different types of honeypots in previous sections and saw that these honeypots have different attributes in terms of level of interaction, security and scalability. Researchers mentioned that there is no solution available that offers both high level of interaction and scalability [67]. In resultant, it is difficult for researchers to collect larger data sets from large size of honeypots network. The opensource framework that we have established for our prototype is scalable and provides adequate level of interaction, which will be discussed further in later sections. The honeypots architecture used in this research work is comprised of selective distributed honeypots, which is designed in a way that fulfills these elements.

5.3 Honeypots Methodology

The purpose of our research work is to collect cyber-attack statistics and their trends analysis in Pakistan’s internet space. There is no existing mechanism to check attack statistics and its types that are being launched against our region’s internet space. As there are sufficient number of internet users which are increasing day by day, the cyber-attacks are also happening frequently in our region. But at this stage we do not have any readily available data which shows trends of these attacks and their characteristics. For this purpose, in this research work we have deployed honeypots based on distributed architecture to collect attack statistics faced by our region. As a case study we will focus on universities internet space, so our prime study of attack surface is Pakistan’s Higher Education Institutes which is under .edu.pk educational domain. (ccTLD)

The focus is to design an efficient solution which addresses honeypots limitations. In this aspect, we addressed the issue of size and location by segregating honeypots network from production network. Along with this it also depicts live services of the typical production network. Special attention was paid to solve the problem of scalability in our honeypots network by implementing distributed honeypot sensor nodes at different locations. The architecture is designed in such a way that it can accommodate additional sensor nodes for maximum coverage of data networks. This solves the problem of deploying honeypots at larger scale, which is one of our key requirement to collect attack statistics from internet space of educational domain.

Finally, we also addressed the challenge of analyzing large volume of honeypots log data by implementing centralized management node that stores all sensor nodes data in a centralized database. Through this management node, centralized reports are generated and these reports can be analyzed from one interface. Hence the proposed solution is integrated into a complete framework that facilitates honeypots deployment and malicious data analysis. So, the overall goal is to introduce an advanced honeypot framework to the security community that can organize attack statistics and can correlate all sensors data to provide a centralized dashboard for attack analysis. The low level design of proposed honeypot framework is depicted in figure 5.1.

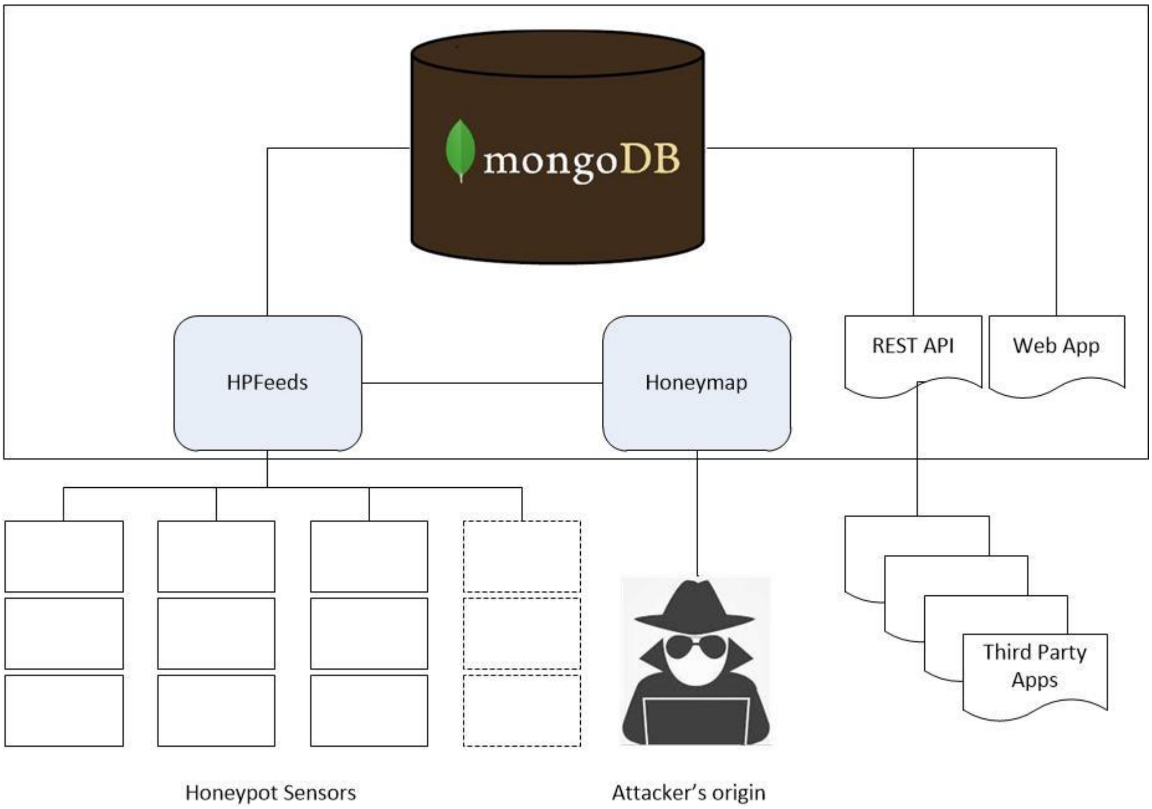


Figure 5.1:Overview of Honeypots Framework

In above figure 5.1 depiction of adopted honeypot framework is presented. To keep all honeypot sensors data in a centralize location “monogDB” is used. “HPFeeds” is used to integrate all dispersed sensor nodes with a management node. Honeymap focuses on information regarding the location of adversaries and plot their origin on a threat map. This information is also transmitted via “HPFeeds” to centralize database. For effective analysis REST API is used to integrate third party analyzer tool; in our scenario we have used “Splunk” tool to analyze and visualize honeypots data.

5.3 Honeypots Frameworks

The above mentioned approach will be used for our actual implementation and the idea is extended from several honeypots research projects. These are distributed frameworks developed for collection of malicious data at larger scale. In this respect, we explore different approaches and before proceeding further for actual deployment we discuss these projects one by one in below sections.

5.3.1 Beeswarm Honeypot Framework

Beeswarm framework supports honeypots that lure services like SSH, Telnet, HTTP, VNC and PoP3. They launched their beta version and expected to be stable in near future, the project is being led by Johnny Vestergaard under the umbrella of The Honeynet Project [68]. They provide easy configuration to deploy and manage honeypots. This system works on infrastructure in which Beeswarm server communicates with Beeswarm client through Beeswarm Drone honeypot to collect data of adversary, the overview of Beeswarm IDS is shown below in Figure 5.2.

Beeswarm framework is having a server node, which is connected with node known as Drone honeypot. Information in the form of reports is communicated to server from Drone honeypot and Drone client. The attacks are launched at Drone honeypot while the information of account activity and plaintext credentials are intercepted by Drone clients.

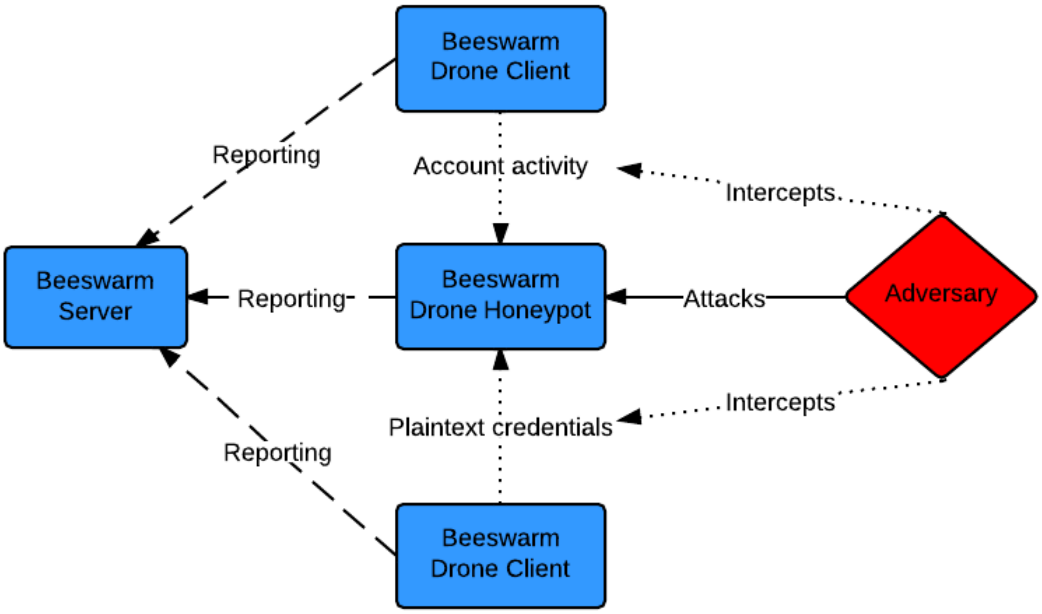


Figure 5.2: Beeswarm IDS Overview

(Image Source: Johnny Vestergaard, http://www.beeswarm-ids.org/images/beeswarm_overview.png)

5.3.2 OWASP WASC Distributed Web Honeypots Project

This project is initiated by OWASP to learn emerging attacks against various web applications. This provides awareness about web application security flaws and statistical incidents against web applications. OWASP released the preconfigured VMware image for WASC distributed honeypot. OWASP community release this collected data in form of OWASP top 10 vulnerabilities [69]. This distributed framework of honeypots is useful to learn vulnerabilities and attack trends about web applications only.

5.3.3 Project Honeypot

Project honeypot is the only distributed honeypots framework used to identify spammers and the spambots that harvest the email addresses from websites. Using this framework, enable infosec professionals to detect the time and IP address of a visitor on a particular website, it uses the custom tagging to detect spammers. The community declares that messages are spam if one of these custom tagged addresses will begin to receive emails.

The Project Honeypot is used by Unspam Technologies, Inc [70], which is an anti-spam company that builds next generation anti-spam engines to combat against spammers.

5.3.4 Modern Honeypot Network Framework

MHN is completely opensource honeypots framework which supports to build a fully functional active defense network. This framework is stable and have larger community that enables it to be used at enterprise level. The data collected is used by the Threatstream for their commercial product Threatstream optic [71].

5.4 Distributed Honeypots Framework

The low-level honeypots architecture used for our research work is shown in figure 5.1. It is divided into three parts: a management node, a set of honeypots sensor nodes and web based interface. The network architecture of established setup is designed in a way such that it monitors large number of IP space using the scalable distributed honeypots, details of network architecture is illustrated in figure 5.3.

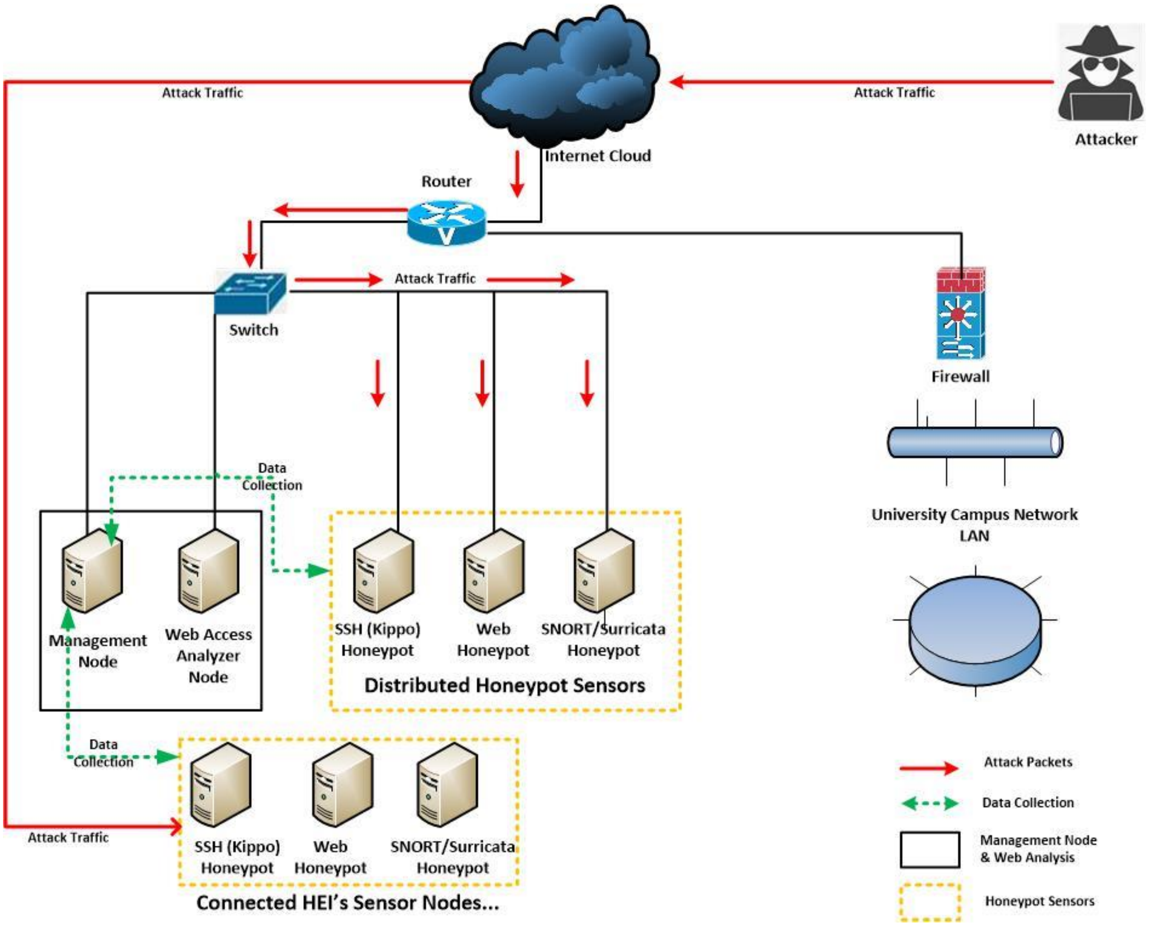


Figure 5.3:Network Layout Diagram for Proposed Honeypots Setup

Figure 5.3 explains the network layout model of the current research. As obvious, the amber dotted lines are representing honeypot sensor nodes and they are placed directly on WAN links. The honeypots sensors are connected through internet with a management node. In this way data collected through honeypot sensors are stored in a management node. The data collection of honeypot sensors through a Management node is represented through a green color dotted lines. Red color arrows depict the attack packet flow. Diagram shows that attack packets are diverted towards honeypot sensors only and restricted from entering the production network due to the presence of firewall.

The all incoming traffic is handled by honeypots, receiving malicious data of attacks and loging all information in centralized location. We deployed one management node through which other distributed sensor nodes are deployed at different locations and all remote sensor nodes are integrated with a management node. Through this management node, centralized reports are collected and these reports can be analyzed from one web based interface.

5.5 Conslusion

As it is observed that some of the projects are designed to capture specific type of attacks. So, they are dedicated solutions to learn a particular type of application attacks. But here we go for more advanced solution that covers variety of attacks at larger scale to address our scope of work that will not target to detect attacks against particular application. For this purpose our prototype will comprise of multiple honeypot decoys to fulfill our requirements, which is further described in detail in next chapter.

Chapter 6

PROTOTYPE DEPLOYMENT

6.1 Introduction

This chapter includes the actual implementation of prototype which covers hardware, OS, software, installation and design architecture used for actual implementation of distributed honeypots used for research work. First we discuss the scope of research work, then prototype architecture followed by hardware and honeypots details. Next we discuss the prototype design and its associated modules. At the end of sections installation of honeypots packages are summarized.

6.2 Scope of Research Work

The main objectives of this research work is to analyze attack patterns specifically within educational sector of our region Pakistan's cyber space. For this purpose, first we studied and evaluated available options, then selected opensource tools that are used and modified to fulfill our goal to analyze attack trends faced by our higher educational institutes. The focus is towards active attacks from the internet on university networks and these cyber-attacks are analyzed in form of updated attack trends.

The focus of proposed honeypots prototype is to enhance the tendency of detecting active attacks and their trend analysis in the academic (PERN) [72] network space. By using honeypots we get information about attacks and logs the data about all attacks in a centralized location. This is achieved by deploying one management node through which other universities sensor nodes are integrated, then the centralized reports are generated from central node and can be analyzed from one interface.

6.3 Prototype Design Parameters

The proposed real world intrusion detection system comprises of distributed honeypots, which is designed in a way that it remains scalable as well as dislocated over a dispersed geographical area of selected higher education internet space. The distribution nature of honeypots carries one master node through which honeypots sensor nodes are deployed at designated locations.

6.4 Hardware and Software Specifications

The hardware and operating system details of Master node, Sensor nodes and Web Based Analyzer Node are given in below table 6.1, table 6.2 and table 6.3 respectively.

Management Node

RAM (Memory)	4 GB
CPU (Processor)	Dual Core Processor
Storage	80 GB
Operating System	Ubuntu Server 14.04 LTS (64 bits)
Network Connectivity	Pubic IP

Table 6.1: Hardware Specificatons of Management Node

Sensor Node

RAM (Memory)	512 MB – 1 GB
CPU (Processor)	Dual Core Processor
Storage	40 GB
Operating System	Ubuntu Server 14.04 LTS (64 bits)
Network Connectivity	Pubic IP

Table 6.2:Hardware of Sepecifications of Sensor Node

Web Based Analyzer Node

RAM (Memory)	12 GB
CPU (Processor)	Dual Core Processor
Storage	300 GB
Operating System	CentOS 7.0 (64 bits)
Network Connectivity	Pubic IP

Table 6.3:Hardware Specifications of Web Based Analyzer Node

6.5 Honeypots Details

Keeping in view the university infrastructure and research scope of cyber attacks analysis specifically for education domain. Specific honeypots have been selected which are compatible with university information systems services. The details of selected honeypots used specifically for this prototype is described in next sections.

6.5.1 Kippo Honeypot

KIPPO is an emulator for SSH service. As SSH is another key service used within universities for secure remote access. Kippo was massively deployed in this research project, Kippo simulates SSH service. It is a very tiny with python script customizable SSH service emulator. It is adaptable and portable, the most importantly highly configurable to look like a real SSH service atleast for outside world. Basically, it logs the flat file and it also stores the full TTY sessions which enables us to replay the attacker activities with real time which is one of its great feature. It is the most popular honeypot on which a lot of research has already been done. That is the reason that experienced attacker can identify and differentiate between this and real Linux host. It is a very useful tool to be used as a pentest.

6.5.2 Dionaea Honeypot

This honeypot is developed under The Honeynet Project 2009 Google Summer of Code (GSOC). It is used to capture malware by exploiting vulnerabilities of a series of services over a network like HTTP, MySQL, MS SQL, FTP, TFTP, SIP, RPC etc. These all services are mainly used within the universities premises. The goal of DIONAEA is to capture a malware copy.

6.5.3 Shockpot Honeypot

It is a standalone web honeypot application exposing the specific exploit CVE-2014-6271 which has Bash Remote Code vulnerability. Another common service used within academia community is web services. So, it is selected to detect attacks against this sort of vulnerability.

6.5.4 ElasticHoney Honeypot

An ElasticSearch honeypot that emulates servers with the goal of capturing servers with exploitation attempts which are vulnerable to CVE-2015-1427 vulnerability. This honeypot works in a simple way it emulates ElasticSearch API and listens on the “/”, “$/\_nodes$ endpoints”, “$/\_search$” and returns response in from of JSON which is very similar to a vulnerable ElasticSearch instance.

6.5.5 SNORT

SNORT is basically an IDS/IPS which is very supportive to detect attacks, it is a powerful intrusion detection system with a stronger community. SNORT is an opensource product, although creator of SNORT was now acquired by Cisco.

6.5.6 Suricata

Suricata is a specialized IDS/IPS suite, it is not much popular as SNORT but has countless contribution from its community. Suricata IDS is used to catch malware files, it is customizable and very powerful tool for malware analysis.

6.5.7 Pof Honeypot

Pof is another powerful honeypot tool used for fingerprinting to detect Operating System (OS) details behind a TCP connection.

6.6 Distributed Honeypots Architecture

The honeypots architecture used for our research work is shown in below figure 9. It is divided into three parts: a set of honeypots sensor nodes, a management node and web based interface. The network architecture of established setup is designed in a way such that it monitors large number of IP space using the scalable distributed honeypots, details of network layout as given in figure 6.1.

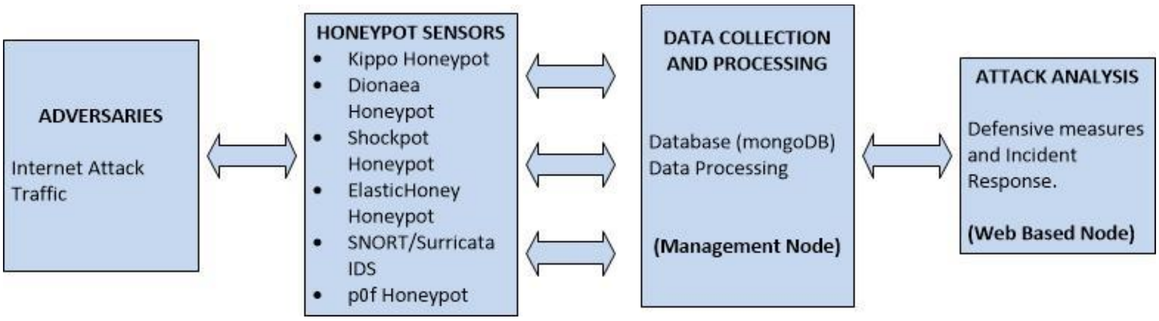


Figure 6.1: Architecture of Prototype Honeypots

The all incoming traffic is handled by honeypots, receiving malicious data of attacks and loging all information in centralized location. We deployed one management node through which other distributed sensor nodes are deployed at different locations and integrated.

Through this management node, centralized reports are collected and these reports can be analyzed from one web based interface.

6.7 Honeypots Deployment

This section involves the actual deployment of honeypots which contains installation of software and related packages to build the proposed design of real world Intrusion Detection System.

6.7.1 Management Node Deployment

First of all, management node is deployed, as it is core node of the honeypots architecture. The following components are configured on a Management node.

- GIT installation and configuration for Distributed Honeypots Framework
- Installation and configuration of MongoDB
- Installation and configuration of HPFeeds for inter-connectivity of Sensor nodes
- Installation and Configuration of Honeymap for global foot printing of attackers

At the end, we run the server completion script to finalize the configuration of management node. A complete step by step details of management node installation is given in Appendix A.

6.7.2 Sensor Node Deployment

Installation of sensor node involves SSH installation, network connectivity in order to reach the management node. Once basic configuration is complete first of all run the updates to have update packages on the sensor node from Ubuntu update repository. Then configure the SSH client to listen on a custom port, so that default port of SSH can be assign to SSH honeypot. After this run the scripts for actual honeypot deployments by coping up with a management node under Deploy tab. For every honeypot, there is designated script containing Management node API key so that sensor node is securely integrated with a management node. In this way, we deploy all honeypots as sensors on each sensor node. The only thing required is connectivity of sensor node to a management node. These steps will be repeated for the other sensor nodes and in this way, we can add as many sensors as we want to a management node. So, that maximum number of data can be collected from the larger scale of sensor nodes. For enterprise deployment management node hardware specifications need to be adjusted as per size of the honeypot sensors. Eventually this design will make the honeynet comprises of several honeypot sensors. High level network architecture diagram is shown below in figure 6.2. This covers whole region (Pakistan) educational internet space to be monitored using distributed honeypots framework. A data collection site is dedicated to keep track of on going attacks. From figure it can be seen that all educational institutes are connected through the internet having honeypot sensor nodes. All senosrs are placed outside the firewall, so that it will not effect the production network of university. In this way all attacks launched from internet to these honeypots will be recorded and analyzed. The detail steps for installation of sensor nodes are mentioned in Appendix B.

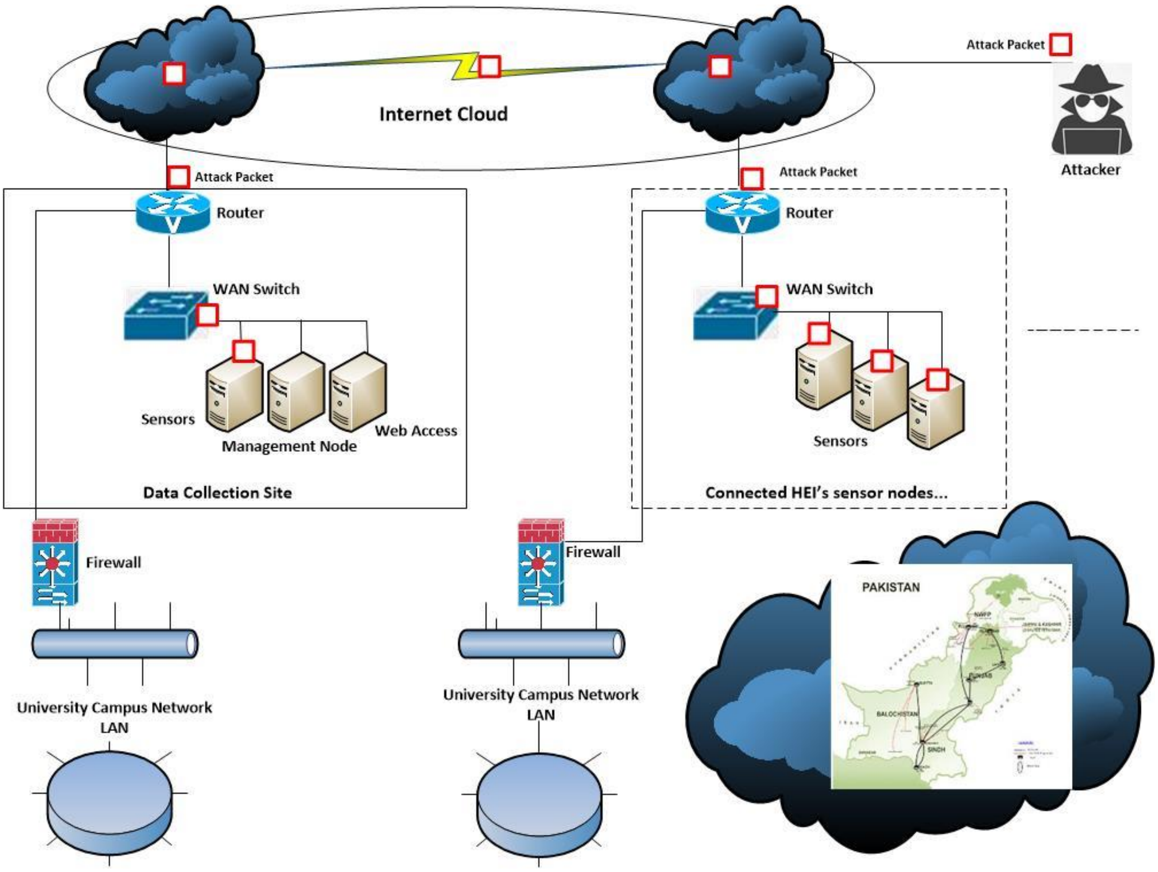


Figure 6.2: High Level Network Architecture of Honeypots

6.7.3 Web Based Analyzer Node Deployment

Once management node and sensor nodes are deployed, then installation and configuration web based analyzer is paid attention. After installation of OS for internet connectivity, update the server for latest packages. Details of installation is mentioned in Appendix C.

Before choosing Splunk as a logging and analyzer engine for log analysis we checked different options. As large data sets are generated from sensors nodes and their analysis will be tedious and time consuming, if not organized properly. It was tried to address this problem by integrating Splunk with centralize database for ease of access and efficient log analysis capabilities. In this way security analysts can easily extract desired information from these large data set files with less efforts and time consumption. For this we use big data analysis tool Splunk Rest API with honeypots which provides us very useful information by building dashboards along with different types of reports with summarized data sets. Otherwise to see bunch of logs and extract valuable information is a nightmare for analysts. The figure 6.3 contains the screenshot of web based analyzer node’s dashboard.

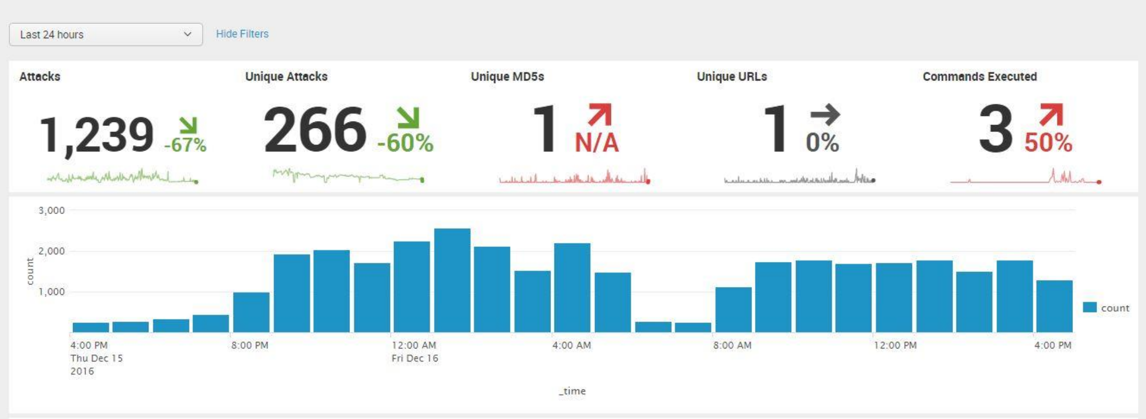
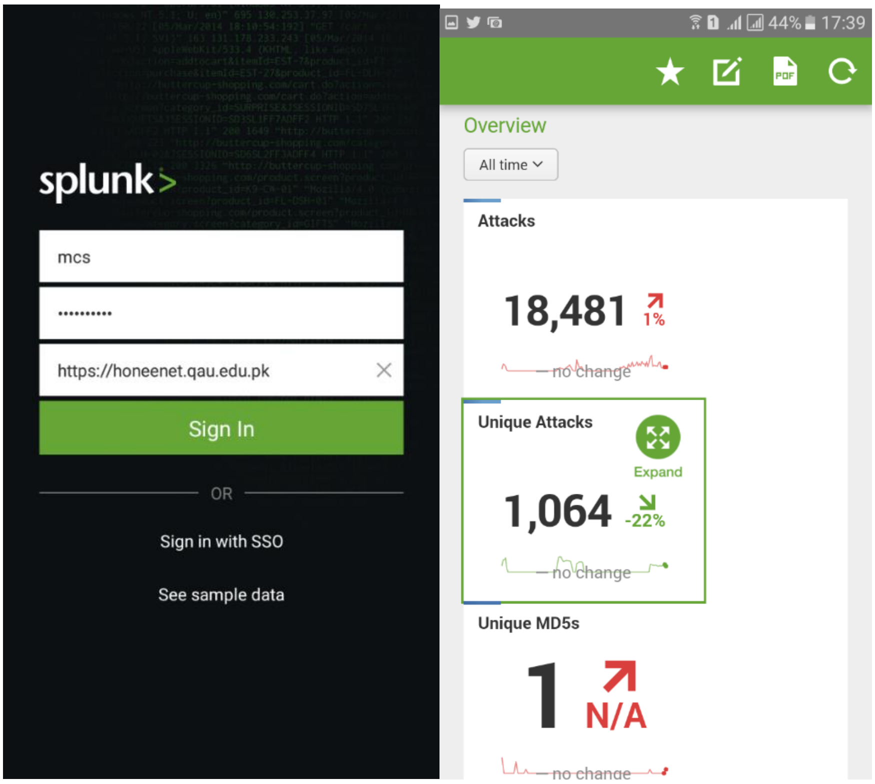


Figure 6.3: Webbased Dashboard of Honeypot Sensors

This analyzer node also has mobile app so that analysts are always keeping in touch and get updates of attack statistics. Another figure 6.4 is exhibited mobile app of log analyzer we used in our setup.



mcs

••••••••••

https://honeenet.qau.edu.pk

Figure 6.4: Mobile App Screenshot for a Web Based Analyzer Node

Splunk is good for bubbling up the interesting stuff up to the top. Our distributed honeypots prototype is not only having this dashboard quality as exhibited in figure 6.3 but its design is also prefect in terms of scalability and security where we just push up services to real hosts and hide them in a way it is leave able.

6.8 Conclusion

This chapter depicted the overall deployment model of distributed honeypots framework used for this research work. The honeypots architecture has been designed keeping in mind that all the dimesnions of research work fulfilled. The overall design parameters are defined in detail so that complete understanding of adopted system can be established in terms of hardware, software, honeypots used, installation and network architecture. In this way this chapter contains the major part of its actual implementation and configuration of overall honeypots environment used for this research work.

Chapter 7

RESULTS AND ANALYSIS

7.1 Introduction

Here design validation is discussed by reviewing and analyzing results extracted from honeypots. To evaluate our prototype in terms of its scope, does this prototype fulfills our research objectives? In first section, the scope of research needs are elaborated and how it can proceed further to achieve the desired results. Then in further sections results are presented which is analyzed based on data collected from honeypots.

7.2 Thesis Scope and Research Paradigm

In this research work it is focused to analyze the cyber-attacks in this region i.e. Pakistan’s cyber space. For this purpose, considering Higher Educational Institutes (HEI) as a case study and deployed distributed sensors at their WAN links to collect cyber-attack statistics. Till now there is not any readily available data which provides information about the live trends of cyber-attacks and their origin. This research work will be a major milestone and a step towards in determining live trends and patterns of cyber-attacks for this region Pakistan’s internet space.

The focus is towards active attacks from the internet on university networks and their analysis in a form of updated attack trends. To test the desired scope of cyber-attack analysis, the experiments were performed in which a group of honeypots were studied, then low-interaction honeypots were selected based on open source software which is configured on a network outside campus firewall at WAN link of each university.

The different configurations of ports and service scripts were run and simulated open source decoys to check which configurations were most useful as distributed honeypots and which were most useful as decoys to protect other network users. The most common attacks were observed, the most common ports used by attackers are identified and degree of success of decoy service scripts, which are discussed in details in next sections.

7.3 Prototype Evaluation and Testing

Honeypots are deployed and placed strategically outside of the production network. First, testing was done of this setup by placing a sensor node at Quaid-i-Azam University (QAU). This sensor node is placed outside of their campus protected network. In this way, these honeypots will not only detect active attacks from the internet but this design will also safeguard their production services to some extent. Once the environment is tested in all aspects, then additional sensor nodes are added from other universities namely Fatima Jinnah Women University (FJWU) Rawalpindi and Kohat University of Sciences and Technology (KUST) Kohat which are also placed on WAN links outside of their campus network protected by a firewall. In this way, this prototype is comprised of three sensor nodes, first one QAU sensor node is in Federal region of Pakistan, other one FJWU is in Punjab province and the third one KUST is in KPK province. In this way, these three sensors nodes geographically dispersed nodes over the internet as shown in Figure 7.1.

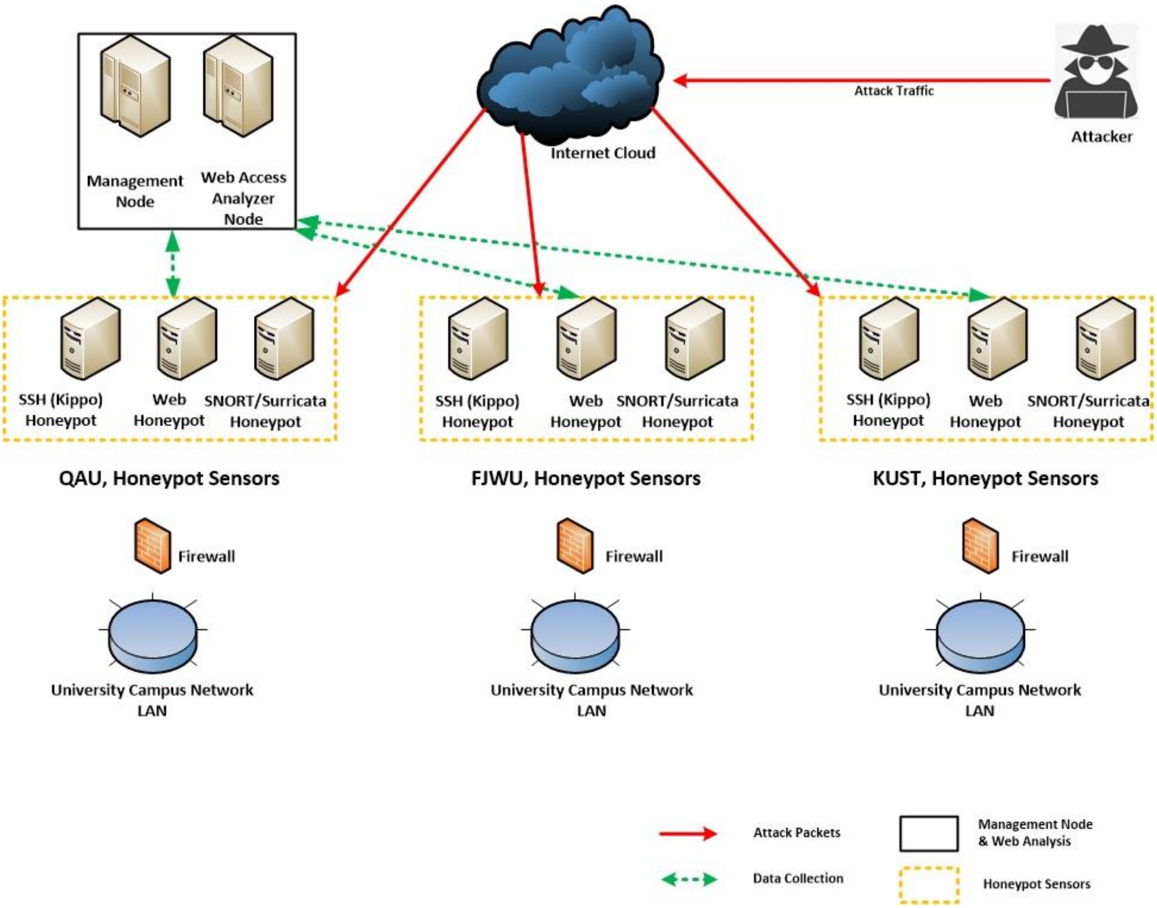


Figure 7.1: HEI Honeypot Sensors Interconnectivity

From above Figure 7.1, it is very clear that this design will not affect normal operations of the universities network. They are silently detecting the active attacks from the internet towards universities network. The data of attack patterns is stored back at a central management node and all universities sensor nodes are integrated with central node. Through this management node, centralized reports are generated and these reports can be analyzed using big data analysis tool Splunk from one interface of logging unit based on a web interface.

7.4 Results and Analysis

In this section, the more detailed view of the established honeypots detection system will present. The time duration of collected results is varied from Dec, 2015 to Nov, 2016. All collected data of attacks are recorded by our system as soon as they are detected. Details of results for each deployed honeypot are discussed one by one in next sections.

7.4.1 Results of Kippo Honeypot

As mentioned in section 6.5.1 KIPPO honeypots are used to detect attacks on SSH service, so for real environment, have customized all sensors nodes to use their default service for SSH access is KIPPO. As soon as we deployed KIPPO honeypot we noticed very frequent attacks on SSH port i.e 22. The figure 7.2 shows the attack patterns and statistics of KIPPO honeypot from Dec, 2015 to Nov, 2016. The below graph illustrates the number of attack probes are on x-axis from Dec, 2015 to Nov, 2016 and on y-axis number of attack attemps are mentioned. It can be seen that the maximum number of SSH attack probes are recorded on April 26, 2016 with 9600 hits. These hits are recored against three SSH sensors deployed in three different universities Quaid-i-Azam University located in Islamabad, Fatima Jinnah Women University in Rawalpindi and Kohat university of Science and Technology located in Kohat of KPK province.

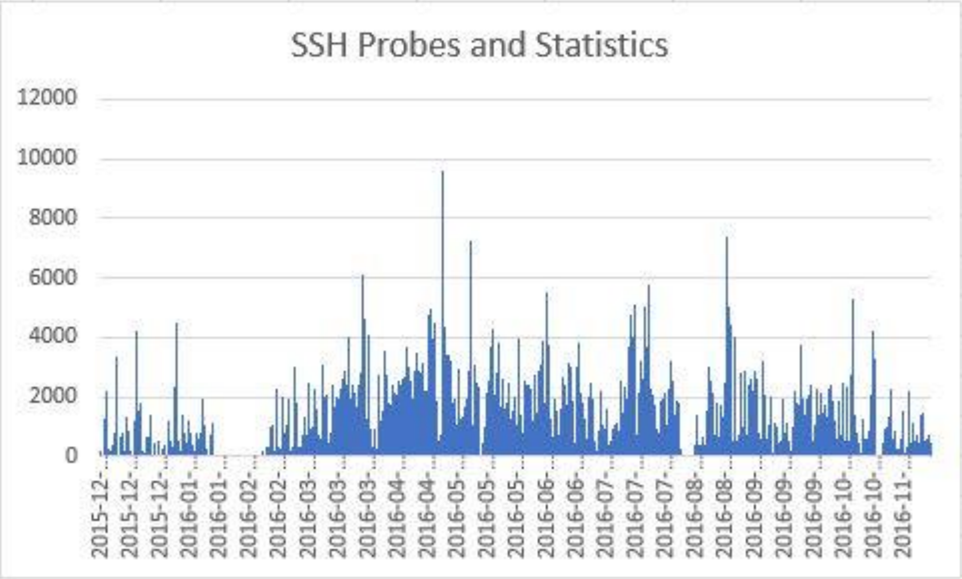


Figure 7.2: Statistics of SSH Attacks

The above results in figure 7.2 clearly illustrates that on our educational internet space SSH service is vulnerable if not securely configured. Furthermore, it is to find out what other valuable information our prototype system can extract from Kippo honeypot nodes for analysts of which origin of attacks, commands executed, username and password combinations, SSH version etc. are some valuable information usually looked for.

In below figure 7.3, SSH usernames and their number of attempts are exhibited. At x-axis usernames are mentioned and on y-axis number of attempts are mentioned. As per statistics collected top most usernames used by attackers are “root’ and “admin”. On the other hand the least most usernames used by attackers are “postgres” and “guest”. These statistics are collected from five different SSH honeypots nodes at geographically dislocated locations of different universities.

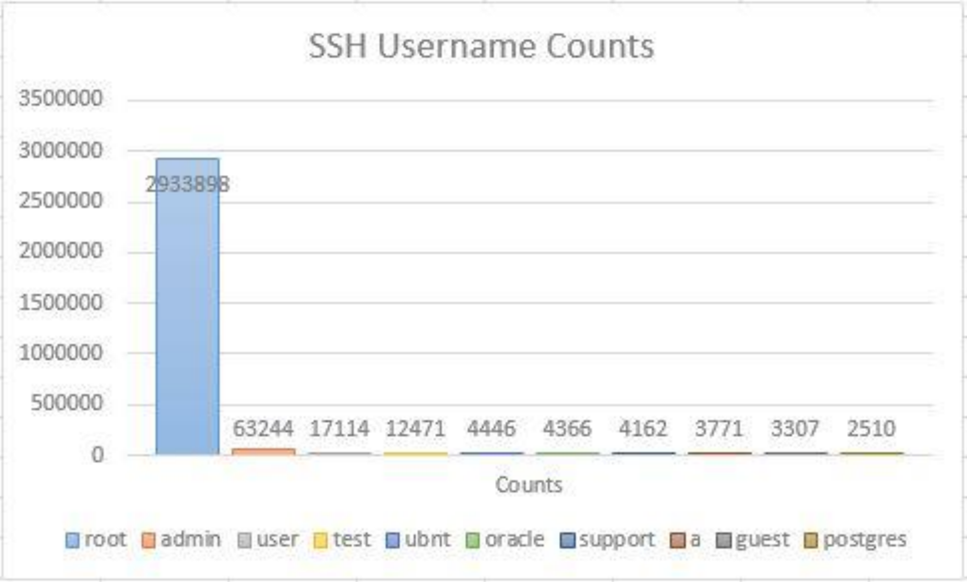


Figure 7.3: Top SSH Usernames Detected

The below graph contains the top SSH passwords along with the number of occurences each password was attempted is shown on y-axis. As it can exhibited from figure 7.4 that the top most password used is "root" and then second largest password count is "123456". At the bottom side, password "wubao" has least counts with 11634 attempts.

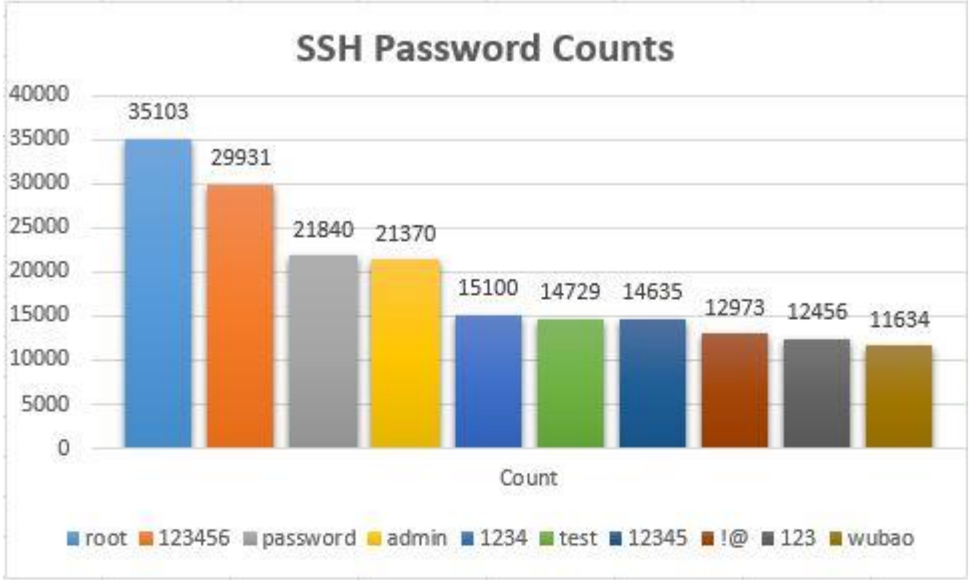


Figure 7.4: Top SSH Passwords Detected

Another statistics of "root" username along with password combinations and corresponding number of counts for eash password is shown below in table 7.1. As it is noticed that the table below the maximum number of password used with 'root' username is "123456".

ssh_username	ssh_password	counts
Root	123456	15963
Root	Admin	14838
Root	password	14705
Root	root	14343
Root	!@	12968
Root	1234	11730
Root	wubao	11632
Root	12345	11427
Root	jiamima	11136
Root	123	10913

Table 7.1: Top SSH Passwords combination with 'root' username

Another valuable result in figure 7.5, which illustrates overall success ratio of login attempts. As per statistics successful logins versus failure is relatively low. Overall, we can see clear upward trend in the number of failure attempts.

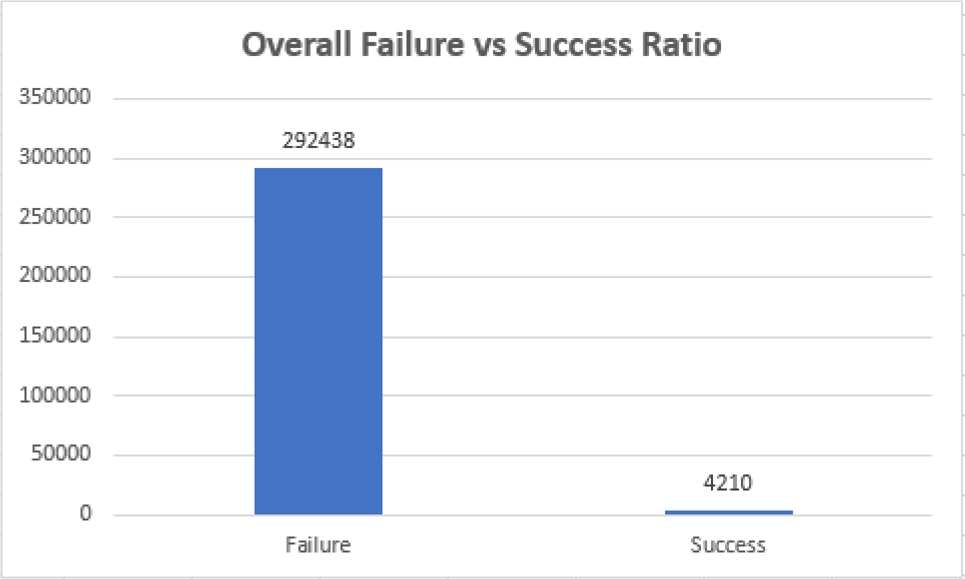


Figure 7.5: SSH Failure versus Success Ratio

Next in figure 7.6, we have statistics of successful logins on per day basis. From this we can see that in one-day maximum turnout of successful login is around 362 times. Average successful logins for whole duration is around 4 attempts per day. It would be fair to say that intruders are capable enough to breach SSH service and gain access to the systems if not properly secured.

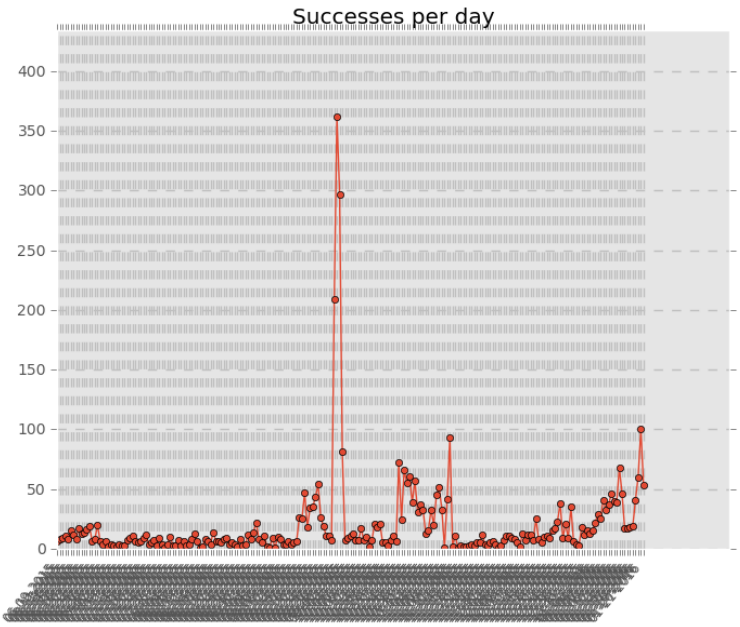


Figure 7.6: No. of Successful SSH Logins per day

The next graph of successful logins from top 20 source IP addresses is shown in figure 7.7. The horizontal axis on below graph shows the source IP addreses. The vertical axis shows the number of successful login attempts performed against each IP address. As it can be seen that the top most IP address is 80.82.64.194 with 1072 successful attempts and least one is 162.248.79.66 with 22 successful attempts.

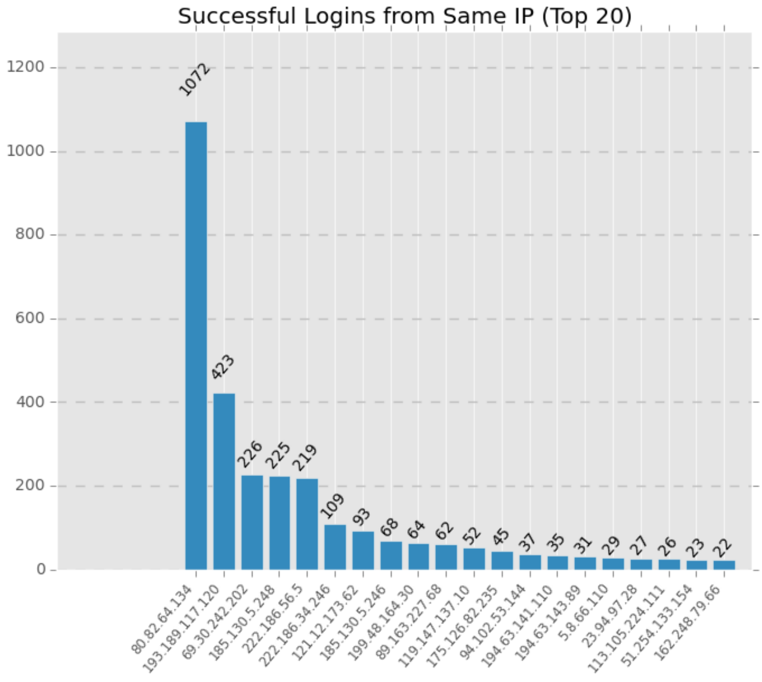


Figure 7.7: Top 20 Source IP Addresses of SSH Attackers

The below Table 7.2 we can see the series of commands that was attempted by the attackers after successful login along with number of each command is executed. From statistics it is noticed that top most command that attackers used is “echo” and they have executed 62 times this command.

SSH Shell Commands	No. of Counts
echo \	62
service iptables stop	45
cd /tmp	25
1 &amp	20
/dev/null 2&gt	20
&amp	20
free -m	17
Ls	10
Exit	8
chmod u+x dage	8

Table 7.2: List of SSH commands detected by Kippo Honeypot

Next table 7.3 contains the URLs accessed by the attackers on SSH emulator and their corresponding number of attempts they have performed. As we can see that attackers have tried to invoke mail utility by entering mailto:!@#$% and mailto:!@#$ with 9 attempts each utility. Other statistics show that they have tried to download malware and infected codes using different URLs as mentioned below in table 7.3.

URLs Accessed using Kippo Shell	No. of Counts
mailto:!@#$%	9
mailto:!@#$	9
http://173.254.203.116:123/Linux-syn25000	7
http://www.hongcherng.com/bc/bc.sh	4
http://222.186.34.180:456/syn	4
http://222.186.34.180:456/keeplive	3
http://173.254.203.116:123/xudp	3
http://173.254.203.116:123/888	3
http://www.hongcherng.com/rd/rd.sh	2
http://180.97.215.150:809/winsx	2

Table 7.3: URLs List accessed by Attackers

The total number of SSH probes on each deployed sensor node is summarized in table 7.4. There are total five sensors used to collect maximum data from different educational universities. The increased number of SSH sensors are used in order to collect maximum number of attack counts and to establish clarity in collected results. Here it can be seen that each sensor has collected handsome amount of attack attempts against SSH honeypots.

Kippo Sensors	Attack Counts
Quaid-i-Azam University Islamabad	2981094
Fatima Jinnah Women University Rawalpindi	1195535
KUST, Kohat KPK	254485
LCWU, Lahore Punjab	163137
Air University, Islamabad	356

Table 7.4: List of Kippo Sensors versus Attack Counts

The list of top KIPPO attackers with details of their country of origin from where attacks were initiated and their corresponding number of attempts are summarized in below figure 7.8. From below statistics, its evident that most of the attacks are orginated from China.

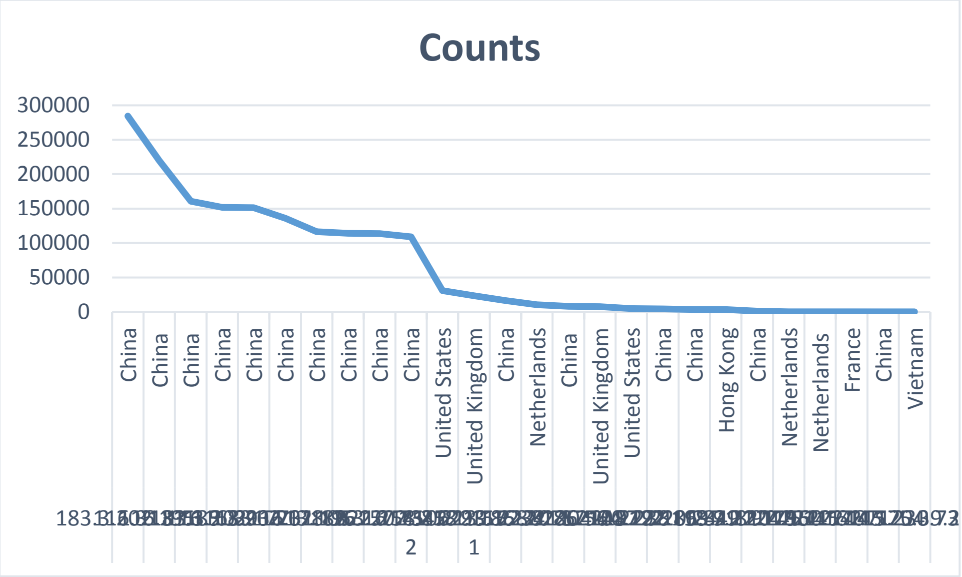


Figure 7.8: Top SSH Attackers Details

In table 7.5, it contains the information regarding SSH client versions that attackers have used to launch the attack on academic internet space. From this it was extracted that top most SSH client verion used by attackers are SSH-2.0 Putty.

Attacker's ssh_version detected	No. of counts
SSH-2.0-PUTTY	2124063
SSH-2.0-libssh2_1.4.3	867829
SSH-2.0-libssh-0.1	655761
SSH-2.0-nsssh2_4.0.0032 NetSarang Computer, Inc.	162117
SSH-2.0-OpenSSH_6.2p2 Ubuntu-6	114898
SSH-2.0-PuTTY	104538
SSH-2.0-OpenSSH_5.3	99212
SSH-2.0-libssh-0.6.0	40472
SSH-2.0-libssh2_1.6.0	38956
SSH-2.0-libssh2_1.7.0	25948

Table 7.5: Attackers SSH version Details

From the above results of Kippo Honeypot, it was noticed that it generates the huge amount of valuable information in the form of graphs and statistics. As it can be observed from statistics that once Kippo is properly configured, it logs every information like username and password that attacker tries to login, if access is successful it will log and track whole session along with commands history. In this way, one can track and trace motive of attackers by analyzing the statistics collected from Kippo sensor. It also collects information about attacker like origin of attacker, IP address from which attack is launched and SSH client details. Kippo is highly customizable to give closer look to the real SSH service and lure the attacker to the greater degree as long as this honeypot is detected by the experienced attacker.

7.4.2 Results of Dionaea Honeypot

In section 6.5.2 we mentioned details about Dionaea honeypots, here we will see the honeypot's behavior like what type of attacks Dionaea logs and how it helps to get valuable information against attacks. The summary of services and ports monitored by Dionaea honeypot sensor is mentioned in following table 7.6 and their corresponding attack patterns will be discussed in upcoming lines with details.

Network Service	Protocol (TCP/UDP)	Ports
SIP	TCP and UDP	5060
SIP	TCP	5061
Microsoft RPC	TCP	135
FTP	TCP	21
MySQL	TCP	3306
Microsoft SQL Server	TCP	1433
Microsoft WINS	TCP	42
Microsoft SMB	TCP	445
TFTP Server	UDP	69

Table 7.6: Top Ports detected by Dionaea Honeypot

The below figure 7.9 shows the attack patterns and statistics of Dionaea honeypot from Dec, 2015 to Nov, 2016. The horizaontal axis represents the days-wise duration of statistics collected. The vertical axis represents the number of attacks performed and is measured in numbers which go up by 5000 at each level. Here it is observed that top most attack attempts are collected on Mar 25, 2016 with around 43385 attack counts from all deployed Dionaea honeypot sensors at different universities.

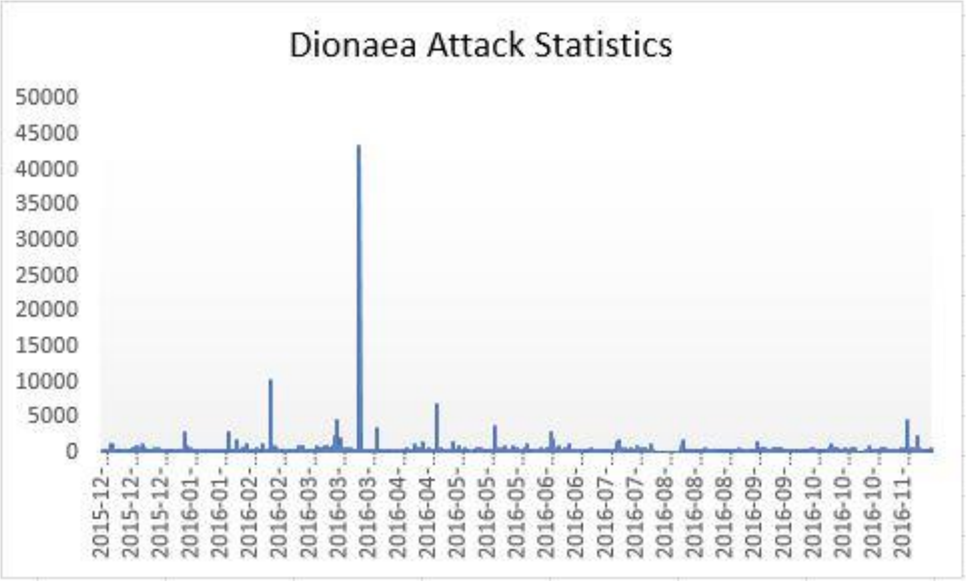


Figure 7.9: Overall attack statistics of Dionaea Honeypot

The next figure 7.10 shows the statistics of number of attacks versus total number of hours these attack statictics are collected from all Dionaea honeypot sensors. Here it is extracted that average attack packets in one day is around 141 packets from all Dionaea honeypots. The attack volume shows that our universities network is continuously under attack and needs to be enahanced.

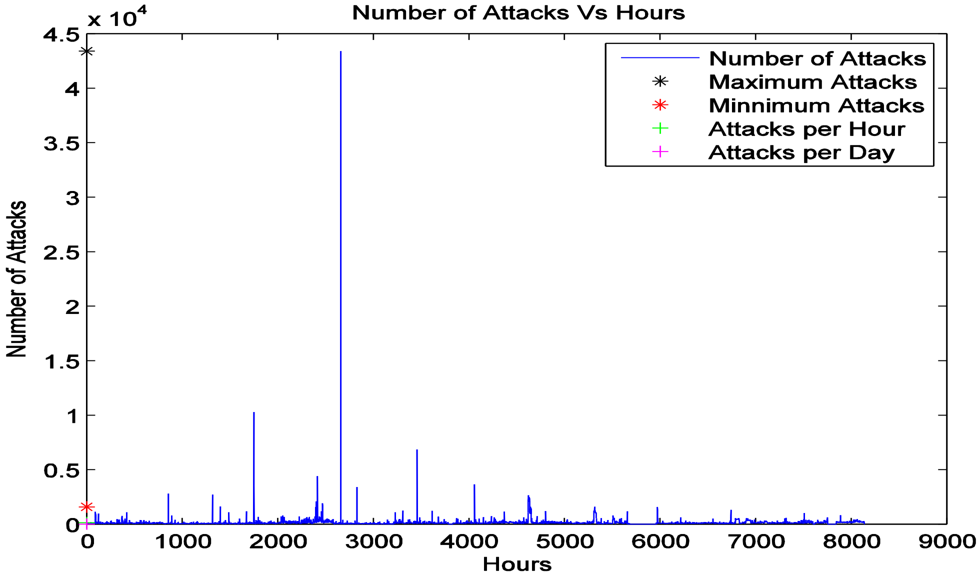


Figure 7.10: No. of Attacks versus Hours

From the above graphs in Figures 7.9 and 7.10, it is quite clear that top most attack value is around 44000 extracted from all Dionaea honeypot sensors. In next figure 7.11, the statistics of port wise attack volume is presented. From this it is noticed that maximum number of attacks performed against port 5060 is around 243619 followed by 3306. This shows that most of attacks are launched against SIP telephony protocol, then opensource MySQL and Microsoft MSSQL database services.

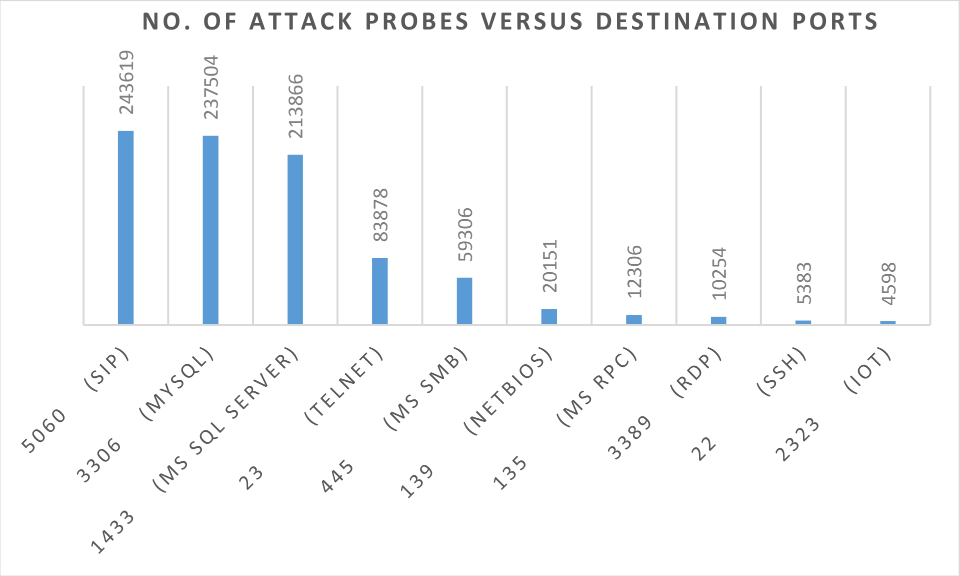


Figure 7.11: Summary of Attack probes versus Destination Ports

The next table 7.7, the details of attackers from top most IP Addresses, their country of origin and number of attempts are shown. As per statistics top most countries from which attacks were launched against network services mentioned in table 7.7 are United States and China. Then next coutnries from which most of attacks collected are United Kingdom and France, their complete details is mentioned in below table 7.7.

Source IP Address	Country	No. of Attempts	Detection Mechanism
216.117.130.133	United States	43353	DShield
::ffff:61.147.103.137	China	32037	DShield
::ffff:74.208.112.7	United States	30227	DShield
::ffff:109.228.57.254	United Kingdom	27068	DShield
::ffff:61.147.103.106	China	19543	DShield
::ffff:74.208.12.240	United States	15478	DShield
::ffff:109.228.57.55	United Kingdom	14538	DShield
::ffff:158.69.73.4	United States	11862	DShield
::ffff:195.154.50.44	France	11729	DShield

Table 7.7: Details of Top Attackers detected by Dionaea Honeypot

The table 7.8 contains the top most URLs detected by all Dionaea sensors along with number of time it was accessed by the attackers. From below statistics it was noticed that attacker has attempted to access SMB shares by invoking custom dialcets. From below results the IP addresses are also collected to which attacker wants to make the session for client server communication.

URLs	No. of Counts
smb://::ffff:187.216.131.254	25
smb://::ffff:190.149.250.46	18
smb://::ffff:119.148.33.125	16
smb://::ffff:66.85.239.82	14
smb://::ffff:216.240.143.112	14
smb://::ffff:195.158.22.7	14
smb://::ffff:61.218.135.130	12
smb://::ffff:122.114.103.149	12
smb://::ffff:120.38.40.55	12
smb://::ffff:117.135.239.43	12

Table 7.8: List of URLs detected by Dionaea Honeypot

Next table 7.9 contains the MD5 Hash value of the malwares captured by deployed honeypot sensors and their corresponding number of counts are also mentioned. The malwares were detected using VirusTotal anlayzer.

MD5s	Counts	Hash Source	Detection Source
d41d8cd98f00b204e9800998ecf8427e	87	TotalHash	VirusTotal
7867de13bf22a7f3e3559044053e33e7	67	TotalHash	VirusTotal
64b4345a946bc9388412fedd53fb21cf	34	TotalHash	VirusTotal
5122974d7c3192a0272b483d7950e92a	18	TotalHash	VirusTotal
ee6896f483387c618156a44aef4a6143	15	TotalHash	VirusTotal
f18d10439daaa8a760fcfedc39d4bfcd	14	TotalHash	VirusTotal
786ab616239814616642ba4438df78a9	12	TotalHash	VirusTotal
f8cde83edd5a34c3d32fbf0e867cbe21	10	TotalHash	VirusTotal
4d56562a6019c05c592b9681e9ca2737	10	TotalHash	VirusTotal
e45ebb90984080e6e7beb7974f1699c6	8	TotalHash	VirusTotal

Table 7.9: Top MD5s detected by Dionaea Honeypot

In last table 7.10 of Dionaea honeypot results, the individual sensors and their corresponding value of Dionaea events are mentioned. As per statistics the QAU sensor has collected large mangnitued of attack packets, the reason behind this is probably the larger network and IP space than among othe universities. Moreover the overall results and events recorded prevailed that universities cyber space is continuously under attack.

Sensors	No. of Events Detected
Quaid-i-Azam University, Islamabad	507843
FJWU, Rawalpindi Punjab	246611
KUST, Kohat KPK	179679
LCWU, Lahore Punjab	68972
Air University, Islamabad	40510

Table 7.10: List of Dionaea Sensors versus Attack Counts

Dionaea results are also very appealing as we expected in terms of its usage, it is noticed that there are number of attacks attempted from internet against academic networks. The results of malware capturing are clear, standing that this prototype system is designed and aligned with strong detection mechanisms to track attackers.

By using these signatures and other associated information of attackers HEIs (Higher Educations Institutes) can be safeguarded from these sorts of attacks.

7.4.3 Results of Shockpot Honeypot

In section 6.5.3, the detail of Shockpot honeypot is given and now in this section its results will be collected and statistics data will also be presented from all Shockpot honeypot senors. First of all, examination of the overall Shockpot events trends from Dec, 2015 to Nov, 2016 is summarized in figure 7.12. From graph below, on horizontal axis we have time duration in terms of hours and on vertical axis magnitude of attacks are mentioned in numbers. From statistics below it is learned that the shockpot honeypots have collected Bash Remote Code vulnerability attacks but not at larger scale.

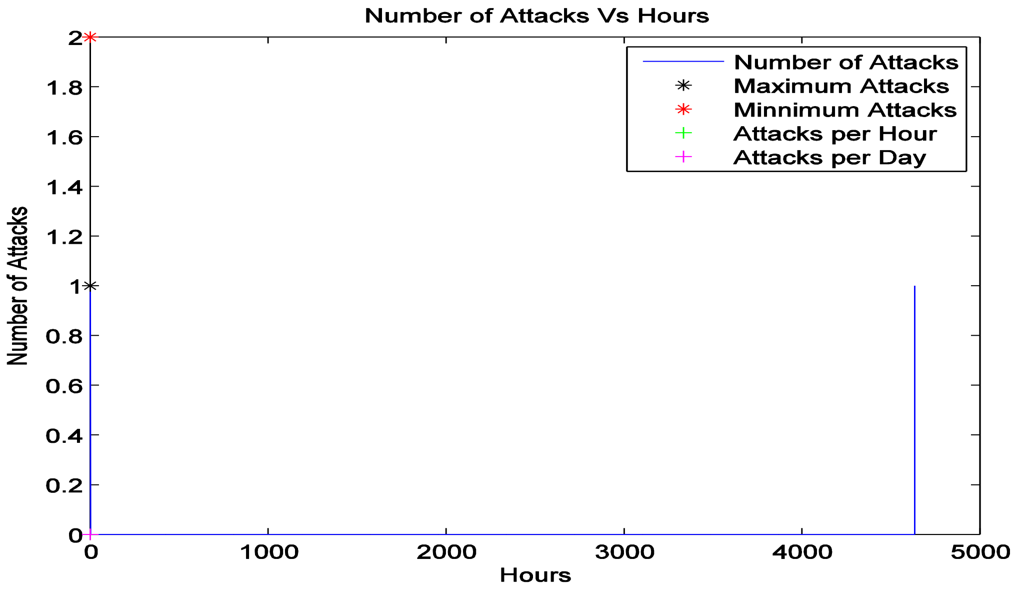


Figure 7.12: Overall Attack statistics of Shockpot Honeypot

From figure 7.13, the most of attack attempts performed against mentioned vulnerability is in the month of February and August, 2016. The details along with time stamps are mentioned in the figure below.

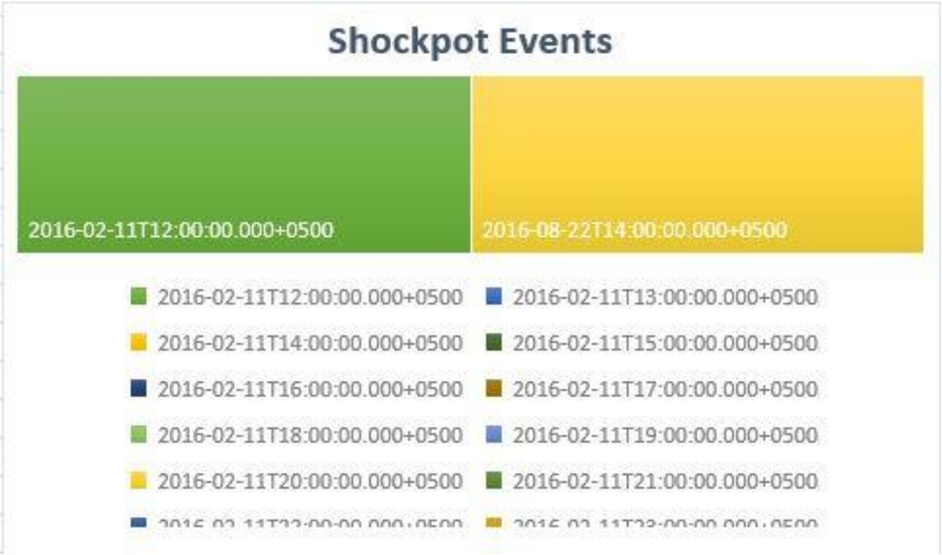

Shockpot Events
2016-02-11T12:00:00.000+0500
2016-08-22T14:00:00.000+0500
2016-02-11T12:00:00.000+0500
2016-02-11T13:00:00.000+0500
2016-02-11T14:00:00.000+0500
2016-02-11T15:00:00.000+0500
2016-02-11T16:00:00.000+0500
2016-02-11T17:00:00.000+0500
2016-02-11T18:00:00.000+0500
2016-02-11T19:00:00.000+0500
2016-02-11T20:00:00.000+0500
2016-02-11T21:00:00.000+0500

Figure 7.12: Statistics of Shockpot Honeypot

As per statistics in figure 7.13, the least No. of attacks detected on honeypot sensors is Shockpot. One of the reasons may be that the only two sensors of Shockpot are deployed in this prototype design. The details of two sensors along with individual attack patterns are shown in table 7.11.

Shockpot Honeypot Sensors	Event Counts
Quaid-i-Azam University, Islamabad	1
Fatima Jinnah Women University, Rawalpindi	1

Table 7.11: List of Shockpot Honeypot Sensors vs No. of events recorded

Next table 7.12 contains the details of attackers along with their country of origin, IP addresses and number of attempts. From the results its clear that attacks launched against shockpot honeypots are from Ukraine and China.

Source	Country	Counts	Detection Src
195.140.168.158	Ukraine	1	DShield
123.249.45.170	China	1	DShield

Table 7.12: Details of Shockpot Attackers

In table 7.13, the list of URLs downloaded to inject CVE-2014-6271 vulnerability on honeypots is mentioned in below table along with their web address and number of attempts.

URLs	Counts
http://qupn.byethost5.com/gH/S0.sh	1
http://houmen.linux22.cn:123/houmen/linux223	1

Table 7.13: List of URLs accessed by Shockpot Honeypots

The details of MD5, SHA1 and SHA256 signatures of files that was detected by Shockpot honeypot sensors are summarized in below table 7.14. The detection mechanism of these hashes are verified through VirusTotal database.

Hash Value	Hash Type	Counts	DB
805fd8d488cb2e059e425e07b69d9cad	MD5	1	VirusTotal
101bb71e77d4367b006f2d79168ad09b5cac1ae4	SHA1	1	VirusTotal
4572ad159a22359bf889f22611f387a8df42785478e8a0232aa723902948a5ec	SHA256	1	VirusTotal

Table 7.14: Details of Hashes detected by Shockpot Honeypots

7.4.4 Results of ElasticHoney Honeypot

The description of ElasticHoney is mentioned in section 6.5.4, Elastichoney honeypot is used to emulate servers with RCE vulnerability and it is heavily exploited. The statistics collected through honeypots are shown in figure 7.14 from time period Feb, 2016 to Nov, 2016. The whole time duration in terms of hours on x-axis and y-axis represents the number of attacks performed and is measured in numbers which go up by 50 at each level.

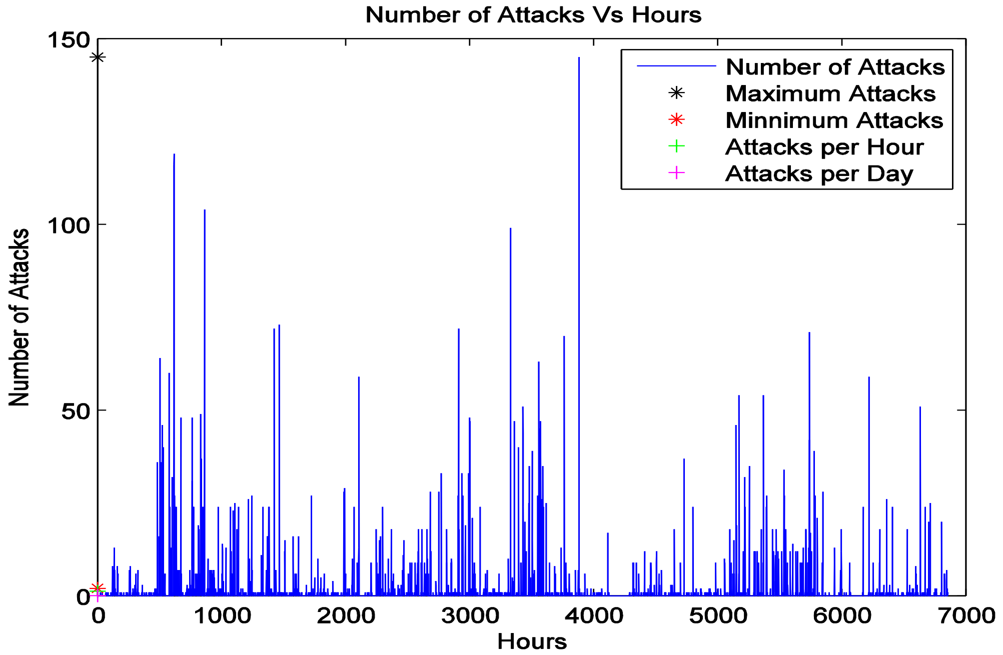


Figure 7.14: Overall Statistics of ElasticHoney Attacks

Another similar graph for ElasticHoney attack statistics is mentioned below in figure 7.15. In this graph the time duration is mentioned in date format from Feb, 2016 to Nov, 2016 and on vertical axis number of attack attempts are present. From this figure it is clear that the maximum number of attack attempts are 145, recorded on July 24, 2016.

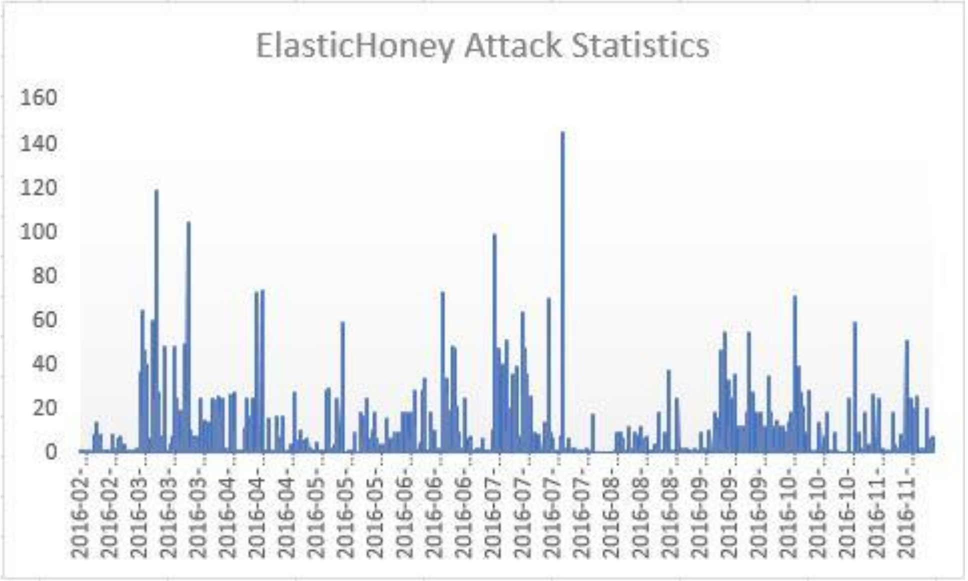


Figure 7.15: Summary of Daywise Attack Statistics

The ElasticHoney honeypot sensors and their individual attack statistics collected from these honeypots are given below in Table 7.15. Although there are only two sensors used for ElasticHoney honeypot in our Honeynet setup but we saw that their results statistics are at larger scale and provide us reasonable data about cyber attacks.

Sensor ID	Honeypot	Counts
Quaid-i-Azam University, Islamabad	elastichoney	6656
Fatima Jinnah Women University, Rawalpindi	elastichoney	1726

Table 7.15: ElasticHoney Sensors versus Attack Counts

The below figure 7.16 contains the spectrum of ElasticHoney signatures used to identify and detect attacks. From pie chart in figure 7.16 there are two type of signaturs used for detecting attack packets. From which the portion of signature for "ElasticSearch Recon Attempted" is negligible around 14% as compared to other signatures who covered the rest attack surface for detecting ElasticHoney honeypot attack traffic.

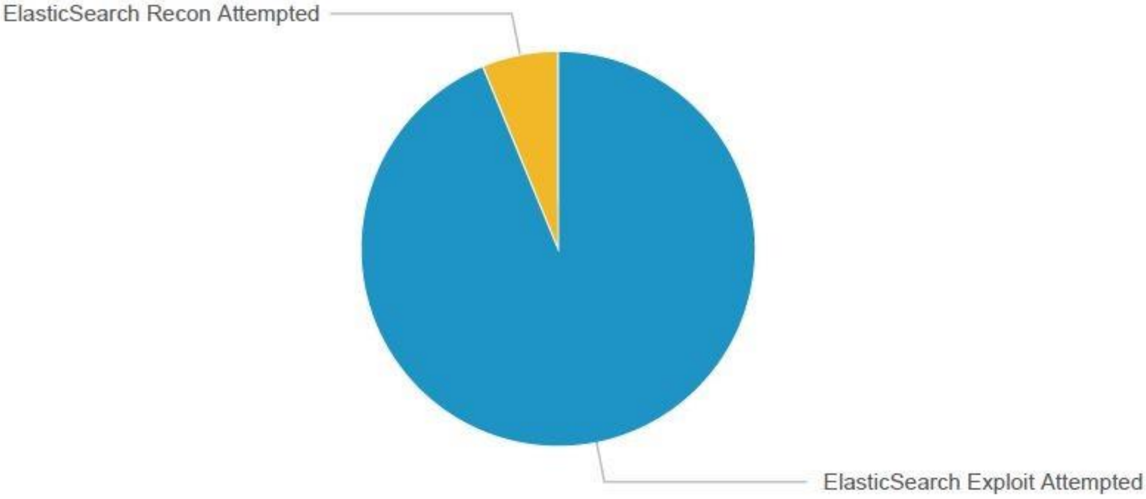


Figure 7.16: ElasticHoney Signatures versus Detection Spectrum

The list of payloads detected and their corresponding number of counts are mentioned in table 7.16. From this, it is observed that the payload mention in first line of table has maximum number of hits i.e. 272.

Decoded Payloads	No. of Counts
\\"echo qq952135763\\"	272
\\"/tmp/nb.Dc\\"	105
\\"/tmp/bbQ.xm\\"	55
\\"/tmp/QQ.MF\\"	45
\\"/tmp/xx.oo\\"	40
\\"/tmp/hf.lp\\"	40
\\"/tmp/cmd.x\\"	40
\\"/tmp/fg.ls\\"	34
\\"/tmp/nudc\\"	30
\\"/tmp/vb.ip\\"	25

Table 7.16: Payloads detected by ElasticHoney Sensors

The figure 7.17 contains the top attackers detected by ElasticHoney sensors with details of their source IP addresses and corresponding number of attack probes. From this source of IP addresses, it is learnt that the GeoLocation of top most IP address is from Jiangsu region in China with 755 attack attmepts. Then the GeoLocation for second highest source IP address is from California, United States. From bottom side, the GeoLocation of IP address "27.100.254.62" is from Korea with 225 attack attempts recorded on prototype setup of honeypots.

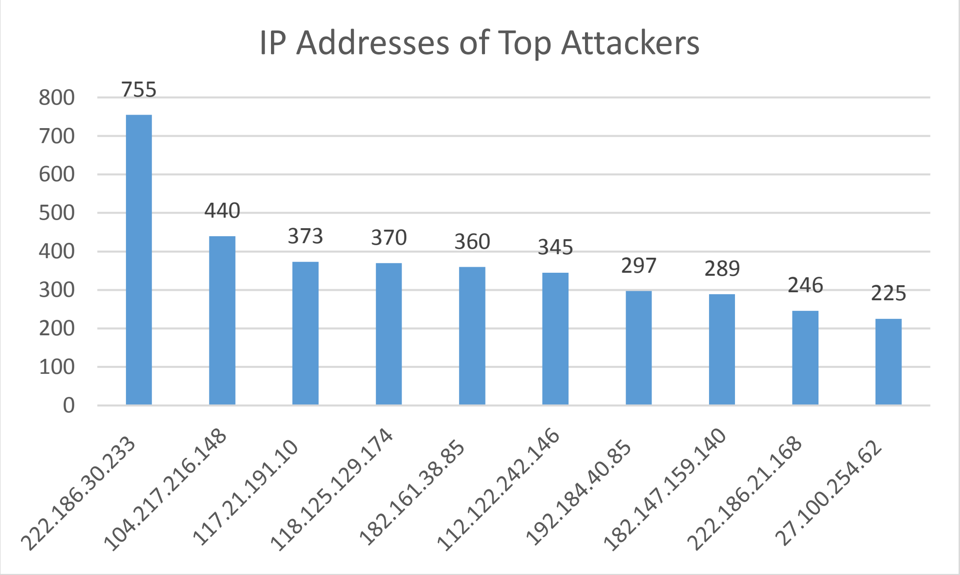


Figure 7.17: Top Attackers Detected by ElasticHoney Sensors

In figure 7.18, the information contains the list of top countries from where attacks detected by these honeypots. From this, it is learned that the name of top three countries is China, United States and Republic of Korea from where attacks are generated.

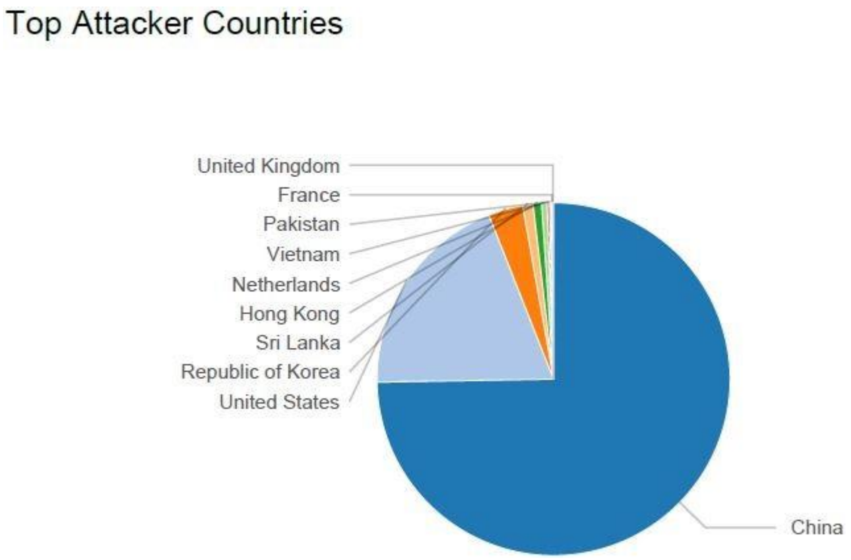


Figure 7.18: Attack surface from different Countries

Next figure 7.19 have names of cities from where these attacks are originated and being launched. As per below pie chart the top most city is Nanjing, then Walnut followed by Chengdu, Beijing, Nanchange, Guangzhou, Hefei, Los Angeles, Fremont and Jeju-si.

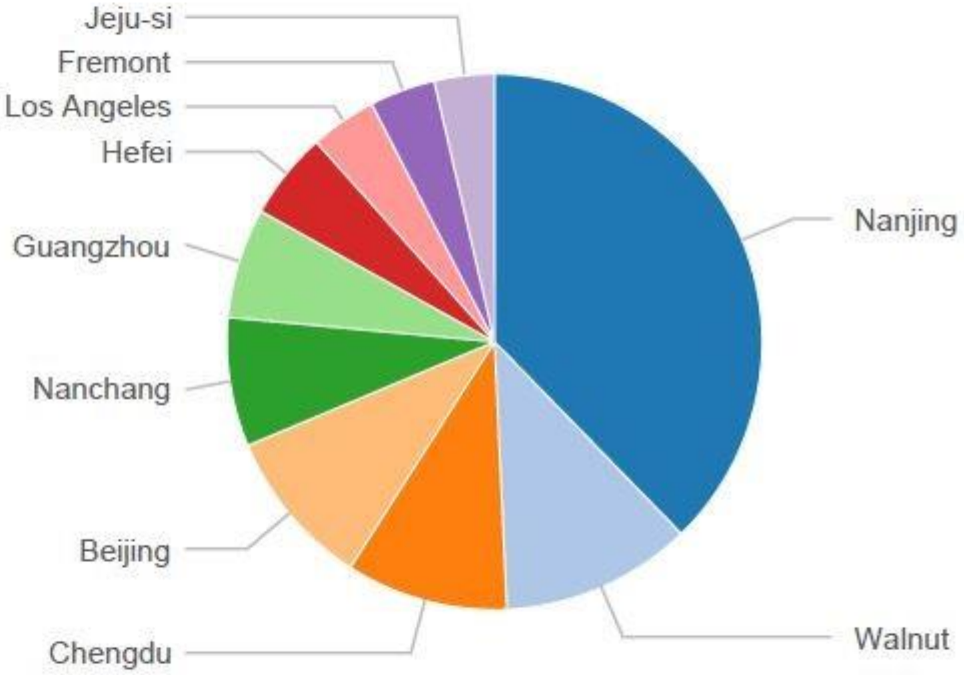


Figure 7.19: Top Cities of Attacker's origin

Here the results clearly indicate that our universities internet space is not only targeted from China and United States but there are number of other countries involved in targeting our regional internet space. It is also noticed that attacks being launched within Pakistan as well but negligible in volume. Hence this is ascertained, without these sort of honeynets setup, it is unable to identify the cyber attacks, their motives and other associated attributes.

By viewing and correlating these attack trends, this can not only secure educational internet space but also design a broader strategy for safeguarding Pakistan’s internet space.

7.4.5 Results of SNORT and Surricata Honeypot

The brief description of SNORT and Surricate Honeypot is already mentioned in section 6.5.5 and 6.5.6. In short, SNORT and SURRICATA are Intrusion Detection Systems and their results statistics from Dec, 2015 to Nov, 2016 are summarized in Figures 7.20 and 7.20. The line graph in Figure 7.19 clearly shows the maximum number of attack probes detected by these IDS is “7103” attempts on 26th April, 2016 at 18:00.

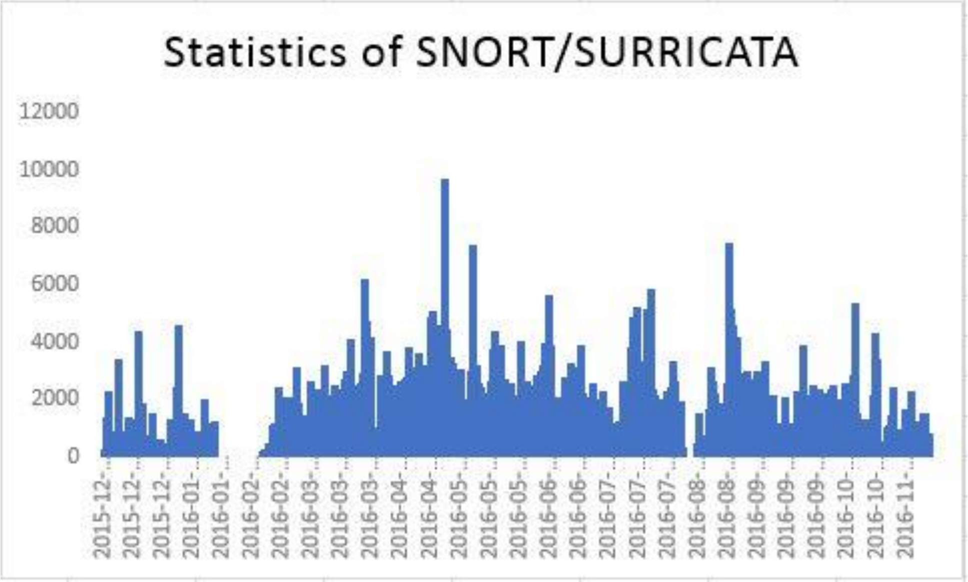


Figure 7.20: Overall attack statistics of SNORT/SURRICATA Sensors

Another customized verion of line graph designed in Matlab specifically for visualization on hour basis is shown in below figure 7.21. In this line chart, hours are mentioned on horizontal axis and number of attacks are represented on vertical axis. As it is clear statistics from below that the average attacks in one hour is around 45 attacks. This means approximately 0.75 attack attempt in one second.

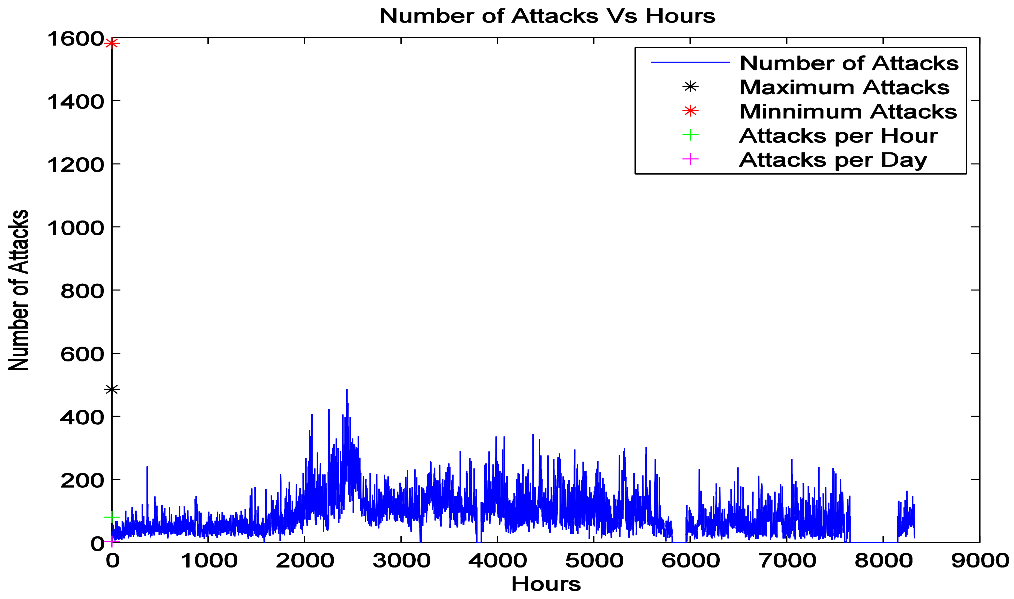


Figure 7.21: Hourly statistics of SURRICATA/SNORT honeypots

The list of Snort/Suricata sensors are mentioned in table 7.17. This table contains the information of Snort and Surricata IDS sensors like their unique ID, honeypot type and number of intruder's packet detected by each sensor.

Sensor ID	Honeypot	Events
Quaid-i-Azam University, Islamabad	SNORT	328885
Fatima Jinnah Women University, Rawalpindi	SNORT	172463
KUST, Kohat KPK	SNORT	120381
LCWU, Lahore Punjab	SNORT	51438
Air University, Islamabad	SNORT	462

Table 7.17: SNORT Sensor details with individual attack counts

Next is the list of top destination sensors along with their corresponding IP Addresses and number of probes detected by each destination. As per statistics, the top most detection is collected through Qaid-i-Azam University sensor. The reason behind this is logical as QAU has larger IP space among other universities.

Destination IP Address	Sensor Location	Events
111.68.96.41	Quaid-i-Azam University Islamabad	449266
121.52.146.163	Kohat University of Sciences & Technology	172463
111.68.96.13	Fatima Jinnah Women University Rwp	51900

Table 7.18: List of SNORT Sensors

Top signatures and their ratio of occurrence is mentioned in table 7.19. This tables contains the list of signatures used to detect malicious internet traffic. As it is noticed that the top most malicious activity is detected against Microsoft and opensource SQL database. Then next is SSH service followed by NOOP, VOIP and SNMP.

Signature Description	Count
ET POLICY Suspicious inbound to MSSQL port 1433	217105
ET POLICY Suspicious inbound to mySQL port 3306	184055
ET SCAN Potential SSH Scan	81936
GPL SHELLCODE x86 inc ebx NOOP	71869
ET SCAN SipCLI VOIP Scan	51511
ET SCAN Sipvicious User-Agent Detected (friendly-scanner)	14319
ET SCAN Sipvicious Scan	13914
ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 54	12020
ET DROP Dshield Block Listed Source group 1	11962
GPL SNMP public access udp	5844

Table 7.19: Signature details with No. of Attack Counts

Next table have the statistics of occurrence ratio for top source ports given in table 7.20. As per the table below, the top most events detected against a source port is “6000” with 79230 counts. On bottom end, the source port is 5001 with “1652” events.

Source ports	No. of Events Detected
6000	79230
5070	15855
5071	11801
5074	7455
43272	4950
5076	4712
5078	2947
42159	2394
5080	1847
5001	1652

Figure 7.20: Source ports versus No. of events occur

The next table 7.21 contains the No. of events detected against destination ports. The top most port is “3306” a MySQL port belongs to opensource MySQL database with “258036” events.

Destination Ports	Events Detected
3306	258036
1433	218980
22	85771
5060	80156
8080	12165
161	6147
111	1378
53	523
3389	512
2222	462

Table 7.21: Destination ports versus No. of Events detected

From above destination ports results it is extracted that most of the attack sessions are established with port 3306 which belongs to MySQL database system, then with Microsoft SQL Database port 1433 and third number is SSH service at port 22. In this way top most targeted services are MySQL Database, Microsoft SQL Database and SSH service.

Next in table 7.22 is the list of source of attackers, country of origin and their corresponding number of attack counts with honeypots. The results clearly illustrate that most of the attack sources originate from China.

Source	Country	Attacks Detected	Detection Mechanism
61.147.103.137	China	12869	DShield
58.218.205.83	China	11936	DShield
183.3.202.195	China	7532	DShield
116.31.116.5	China	5609	DShield
111.68.100.155	Pakistan	5324	DShield
183.3.202.178	China	4685	DShield
61.147.103.106	China	4613	DShield
183.3.202.177	China	3854	DShield
125.46.58.43	China	3769	DShield
74.208.112.7	United States	3655	DShield

Figure 7.22: SNORT Top attackers details

As per statistics collected against Snort and Surricata honeypots, the most of the attacks targeted against common services like databases, SSH, HTTP, SNMP, DNS and RDP. It was also noticed that a larger volume of attacks were orginated from China and United States.

7.4.6 Results of p0f Honeypot

P0f honeypots are used to detect the fingerprints of operating systems that are used by attackers to launch attacks. Following bar chart in figure 7.21 shows the statistics of operating systems detected by these honeypots.

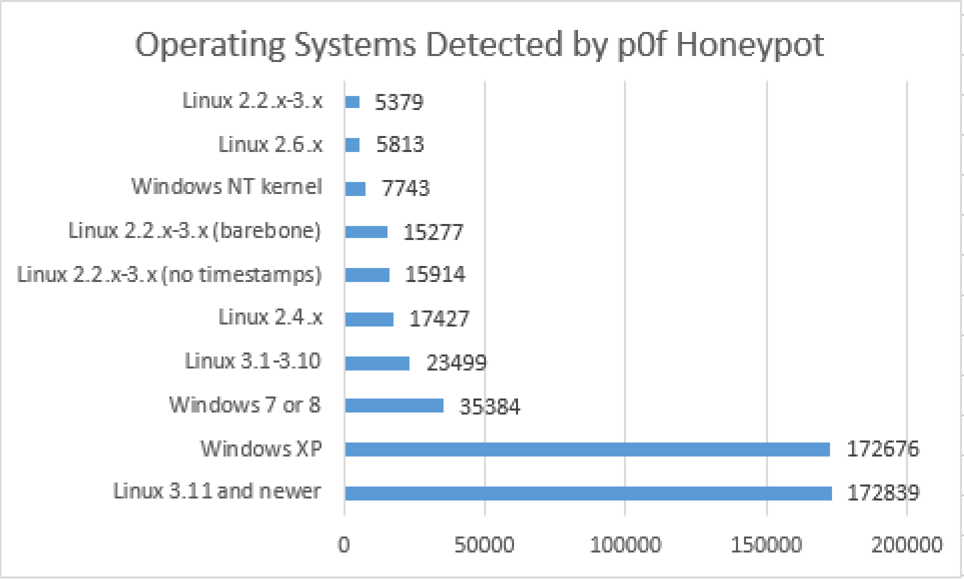


Figure 7.21: Details of Operating Systems used by Attackers

As per above statistics the top most operating system used by attackers are Linux 3.11 or newer version and Windows XP. The older linux kernel has minimum in numbers then a new one as per statistics colledted through p0f honeypot.

The trends of events occurred against p0f honeypot is represented below in figure 7.22 for the whole duration of its deployment. The graph statistics are reperensted using total number of hours on x-axis and number of probes detected on y-axis.

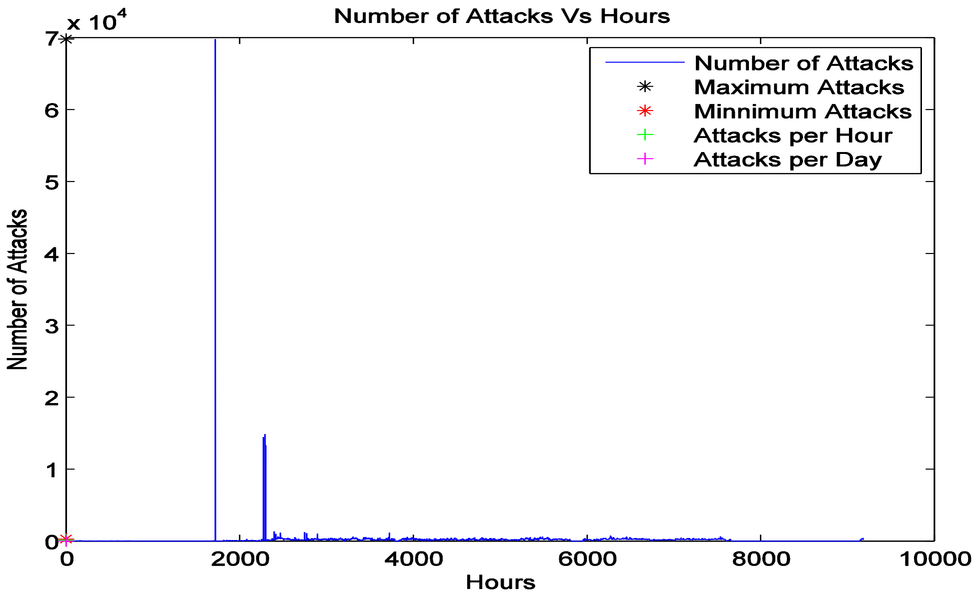


Figure 7.22: Overall attack statistics of p0f Honeypots

The figure 7.23 contains the same data but on horizontal axis time duration is measured in terms of days instead of hours. It clearly indicates that the maximum number of attack probes were around 69783 recorded on February 15, 2016. Here, this behavior also indicates that probably on this day attackers had launched automated attack using some sort of bots. As the number of hits are very large and this can only be possible if the attacker is using some sort of automatic script or the nature of attack is a sort of distributive.

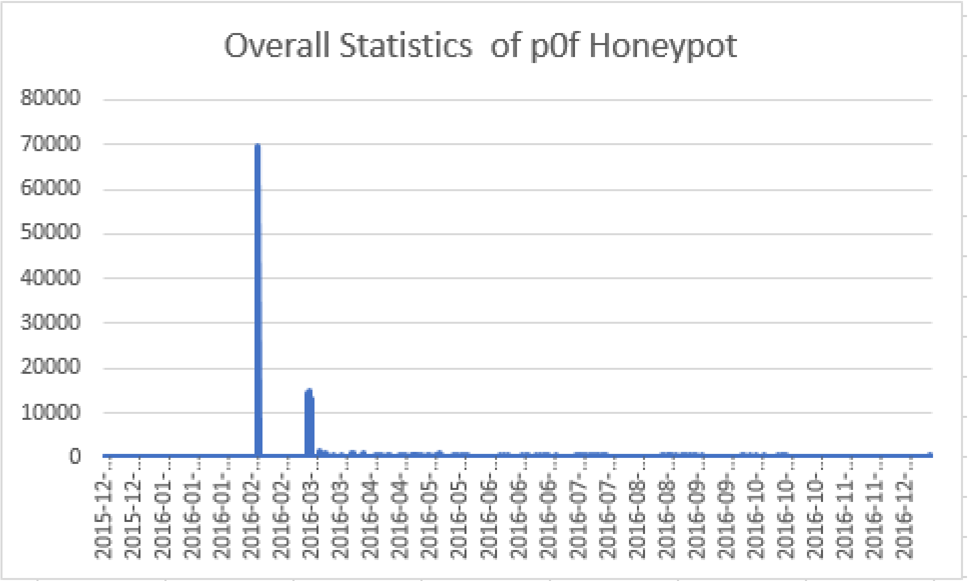


Figure 7.23: Summary of Datewise attack statistics

The below table 7.23 contains the p0f sensor IDs and number of events that each sensor has detected to collect Operating System details of Attackers. From this table one can see sensor's unique ID and their corresponding value in terms of events or attack probes recorded by individual sensor.

Sensors ID	No. of Events Detected
Quaid-i-Azam University, Islamabad	1053883
Fatima Jinnah Women University, Islamabad	216739
KUST, Kohat KPK	173263
LCWU, Lahore Punjab	18831
Air University, Islamabad	611

Table 7.23: List of p0f honeypot sensors

Other valuable information that p0f honeypots collected is type of connectivity link used by the attackers. The list of top media links used by the attackers to our honeypot sensors are listed below in table 7.24. This link category used to establish connectivity with honeypot sensors is mostly via Ethernet or Cable. Another result from below stats is detecting VPN or encrypted secure tunnel used for launching attacks. The attackers used encrypted channel to hide their presence within network. As it is observed from results that reasonable amount of probes are detected against VPN and IPsec or GRE tunneling by establishing secure connection with services offered by honeypot sensors. Hence, here the key point is that the encrypted links can only be detected at last level and honeypots are best source to detect such traffic, otherwise its hard to detect encrypted packets.

Link Type	No of connections
Ethernet or modem	441175
DSL	39319
IPIP or SIT	20427
Generic tunnel or VPN	15509
IPSec or GRE	2523
VLAN	433
GIF	293
Google	50
PPTP	23
jumbo Ethernet	19

Table 7.23: Link type versus No. of Connections

The below table 7.25 contains the p0f events detected through NMAP, below are the results in which NMAP SYN scan detects 1275 events and type of operating systems used by attackers are detected through NMAP is around 98.

p0f APPs and NMAP Details	No. of Events
NMAP SYN scan	1275
NMAP OS detection	98

Table 7.25: NMAP versus no. of Events

List of Top attackers with their origin of country and number of attempts are shown in table 7.26. From this table it is clear that most of the attacks are originating from China and Republice of Korea. Both countries are involve in launching various nature of attacks specifically to educational institutes network.

Source	Country	No. of Attempts	DShield
116.31.116.5	China	50878	DShield
116.31.116.39	China	48332	DShield
183.3.202.195	China	46186	DShield
116.31.116.16	China	40261	DShield
116.31.116.15	China	36057	DShield
150.150.33.72	Republic of Korea	32569	DShield
150.150.1.39	Republic of Korea	28930	DShield
116.31.116.7	China	25723	DShield
183.3.202.178	China	22908	DShield
183.3.202.196	China	21274	DShield

Table 7.26: Top Attacker's details with No. of Events

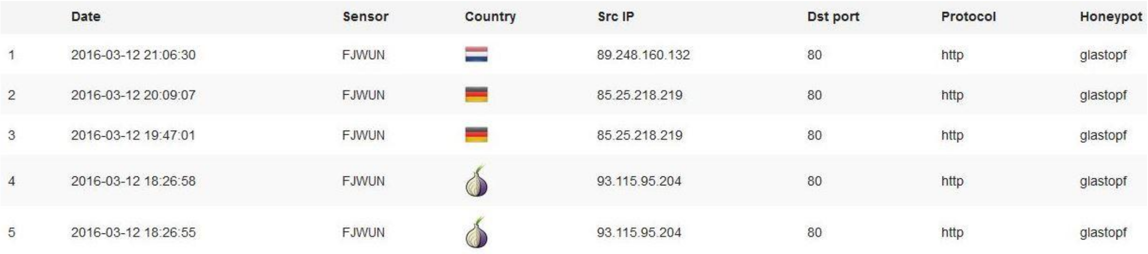
The list of top ports against which p0f statistics are collected are exhibited in below table 7.27. Here it clearly indicates that top most service port on which most of the attack probes are received is SSH port with port number 22.

Destination Ports	No. of Events
22	681123
445	155706
1433	142793
23	134692
3306	127001
80	80501
8080	40509
135	11197
3389	8674
139	8097

Table 7.27: Destination ports with number of Events

From the table 7.27, it is clear that most of services are common internet services that are heavily used on academic or any enterprise networks. Here the list contains the port 22 for SSH service, then we have SMB protocol on port 445 for File and print services sharing another TCP/IP protocol, 1433 is the port for Microsoft SQL Server, 23 is for Telnet services, 80 is HTTP protocol used for Web Services, then 8080 port is mostly used for HTTP alternate like Web proxy or caching services. In list, next port number is 135 which is used for DCE/RPC Locator service like DHCP, DNS, WINS etc, port 3389 is used for Microsoft Terminal Services for Remote Login and the last port in this list is 139 which is used for NetBIOS session service.

During attack analysis phase, it was noticed that some attackers are also using TOR network space to hide and launch attacks, following figure 7.24 exhibits the attack probes of No. 4 and 5 launched from TOR network to honeypot sensors placed in FJWU at port 80 of Glastopf Honeypot sensor.



	Date	Sensor	Country	Src IP	Dst port	Protocol	Honeypot
1	2016-03-12 21:06:30	FJWUN	🇳🇱	89.248.160.132	80	http	glastopf
2	2016-03-12 20:09:07	FJWUN	🇩🇪	85.25.218.219	80	http	glastopf
3	2016-03-12 19:47:01	FJWUN	🇩🇪	85.25.218.219	80	http	glastopf
4	2016-03-12 18:26:58	FJWUN	🧅	93.115.95.204	80	http	glastopf
5	2016-03-12 18:26:55	FJWUN	🧅	93.115.95.204	80	http	glastopf

Figure 7.24: TOR Network Event Statistics

7.5 Conclusion

The results of research work presented in this chapter reveals that HEIs cyber space is continuously under attack. As it is noticed in this research that there are numerous type of attacks launched by adversarires to the internet space of educational network. Hence, securing information system is a continuous process and without learning adversaries' skills it is hard to provide adequate level of security to our network. As result indicates that once we learn the nature of cyber attacks, we will be in better position to provide required level security to our valuable IT assets. Cyberscurity is a complex topic, for complete understanding it requires complete understanding of a latest security posture. It is perceived from results of this research work that it is including but not limited to information security policies, it is important to have expertise from multiple disciplines. It is evident that without knowing insight of each attack we are not able to provide stringent level of security to our information systems. However, with more advancement in technology trends, brings more challenging risks and new threats. So, our research work proves that honeypots are best arsenal toolset to cope up with adavaced cyber attacks. Therefore, reshaping the security posture and resized accordingly is deemed necessary in order to provide a real world security to our information assets.

Chapter 8

CONCLUSION AND FUTURE WORK

8.1 Introduction

In this chapter, to conclude our research work summarized outcomes of research conducted are discussed. It also discusses honeypots conducive role in detecting and gathering cyber-attacks information to build a threat intelligence framework. The chapter ends with prototype conclusion and further utilization of this honeypots technology.

8.2 Summary of Attack Statistics

In previous chapter, various results strengthen our research work to collect live attack trends of educational internet space of Pakistan. If all attacks are concluded on a single page, then the overall statistics of attacks collected from December, 2015 to November, 2016 tenure is shown in Figure 8.1. As per below statistics, the average attack ratio of this tenure is around 1000 multiple type of attack probes in a day. These are the statistics collected only from Educatonal internet space of deployed honeypots. In this way, these attack trends reveals that our regional internet space is facing different form of cyber attacks and we need to have this sort of mechanism to learn and safeguard our information systems from cyber attacks.

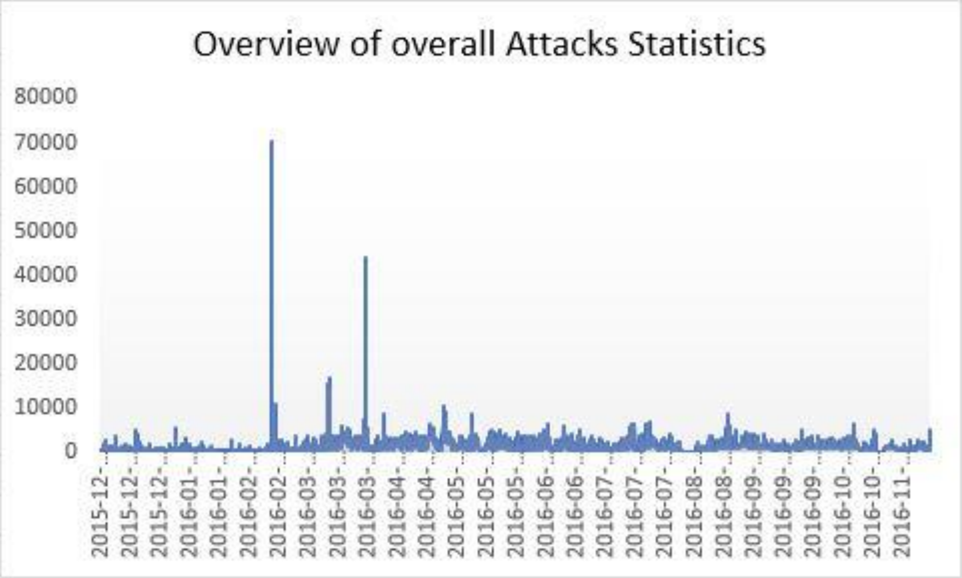


Figure 8.1: Overview of overall Cyber Attack statistics

The Figure 8.2 contains a dashboard of web based analyzer system that shows collective view all sensors that bubbles up current attack surface of selected educational cyber space. This dashboard shows the crisp information regarding recent attack trends of selected cyber space collected from all honeypot sensors. Here, it shows last 24 hours total learnt attacks out of which how many attacks are unique. Then next trends are unique MD5s, Unique web addresses and commands executed from all deployed honeypot sensors.

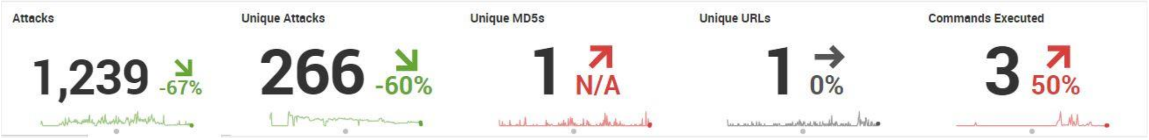


Figure 8.2: Webbased Dashboard of Honeypots

The figure 8.3 shows the list of countries with corresponding name of cities and their surface area of attacks launched to all honeypot sensors. From below stats it is concluded that most of the attacks launched to selected internet space are from China, USA, Korea, Germany, Netherlands, UK, India, Hong Kong and Taiwan.

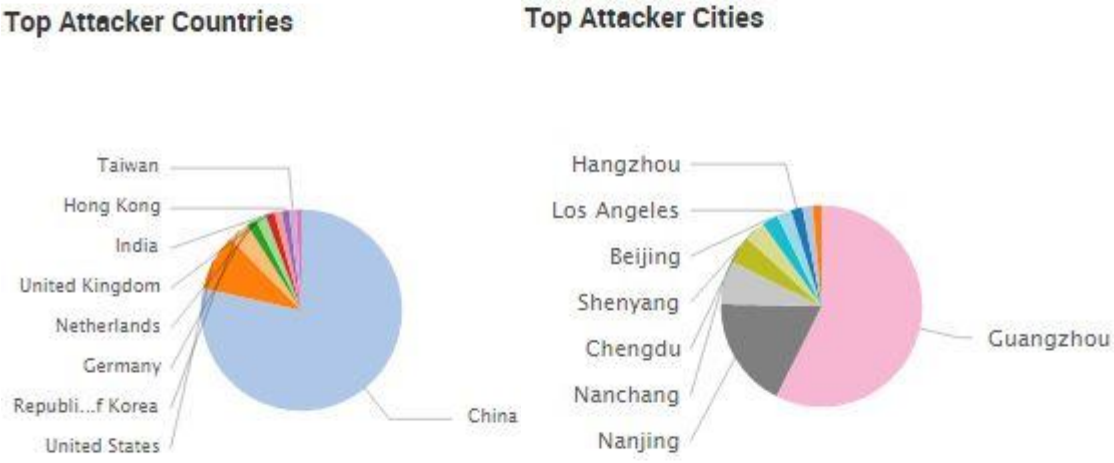


Figure 8.3: Summary of Top attackers Location

In next Figure 8.4 summary of top honeypots used for this prototype in detection and collection of active attacks, followed by corresponding attack surface of destination ports on which most of the top attacks detected are depicted in pie charts. The overall collection and attack trends revealed that most of the attacks are launched against SSH port, then on MySQL database system, Microsoft SQL Server database system, SIP port (5060), Microsoft SMB and AD services on port 445, telnet, Web, Web proxy and cache Services.

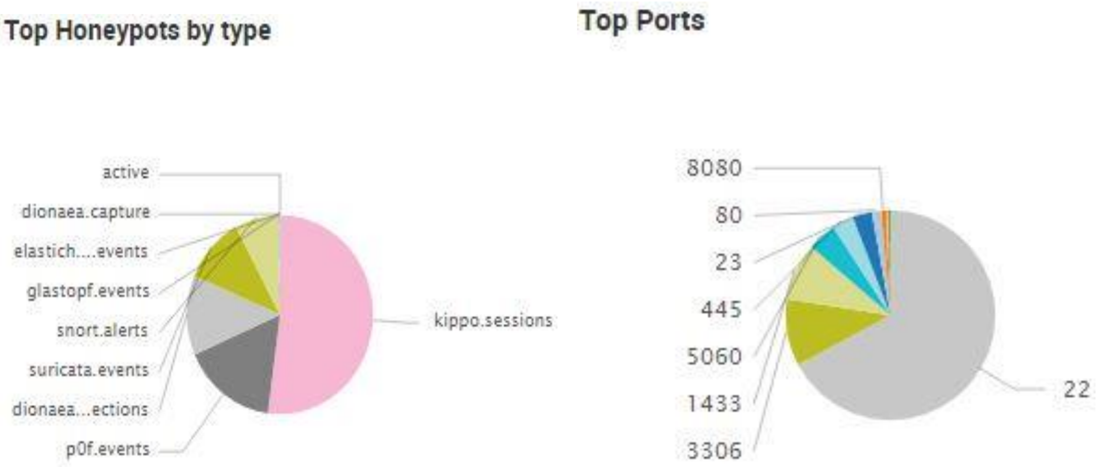


Figure 8.4: Top Honeypot Sensors with Destination ports

The next figure 8.5 contains overview of top attacker's source IP addresses and their equivalent number of attack probes across all honeypot sensors. The top most IP Address used is "183.3.202.195", the geolocation of top most IP address is from Guangdong region of China.

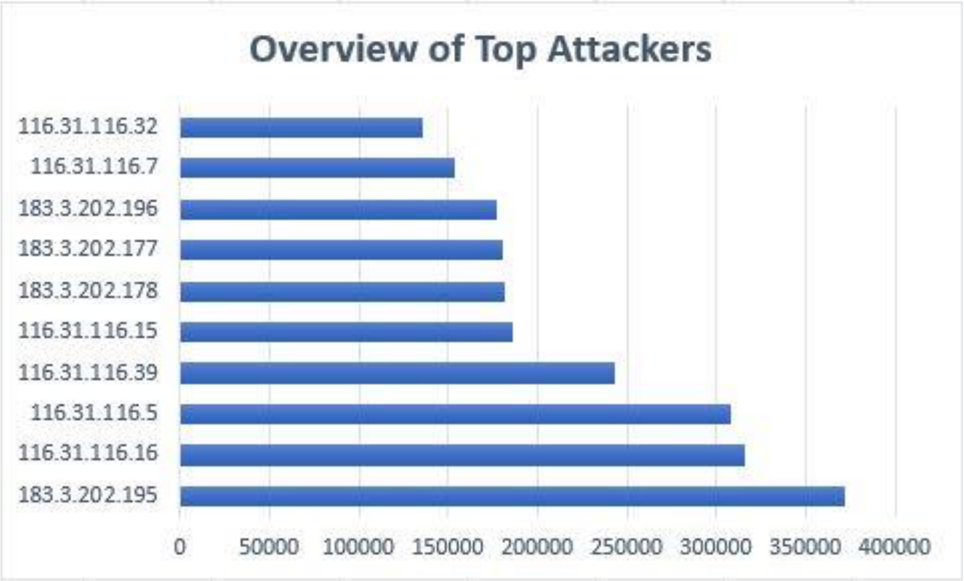


Figure 8.5: List of Top IP addresses of Attackers

The next result in Figure 8.6 shows the percentage usage of operating systems by attackers to launch attacks on our distributed honeypot nodes. As per graph the top most operating system is Linux 3.11 or above and Windows XP with overall 37% and 36% ratio respectively.

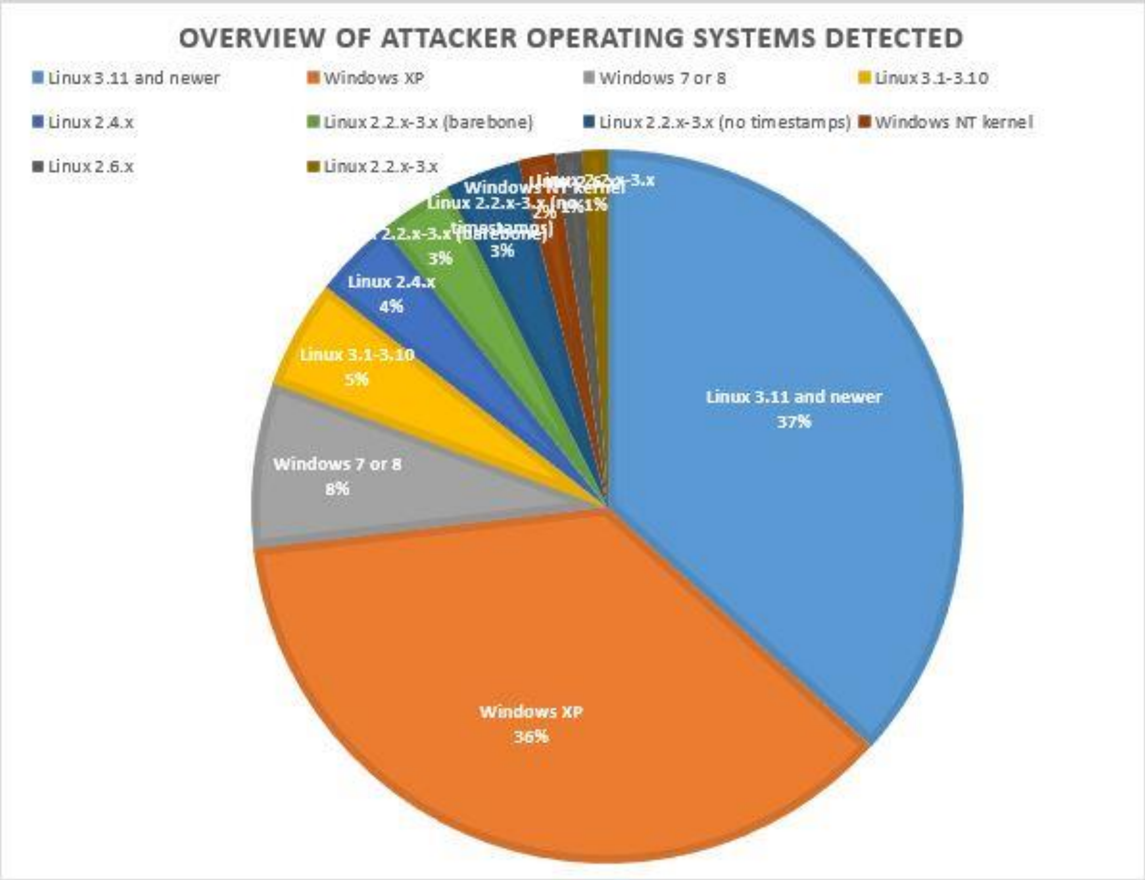
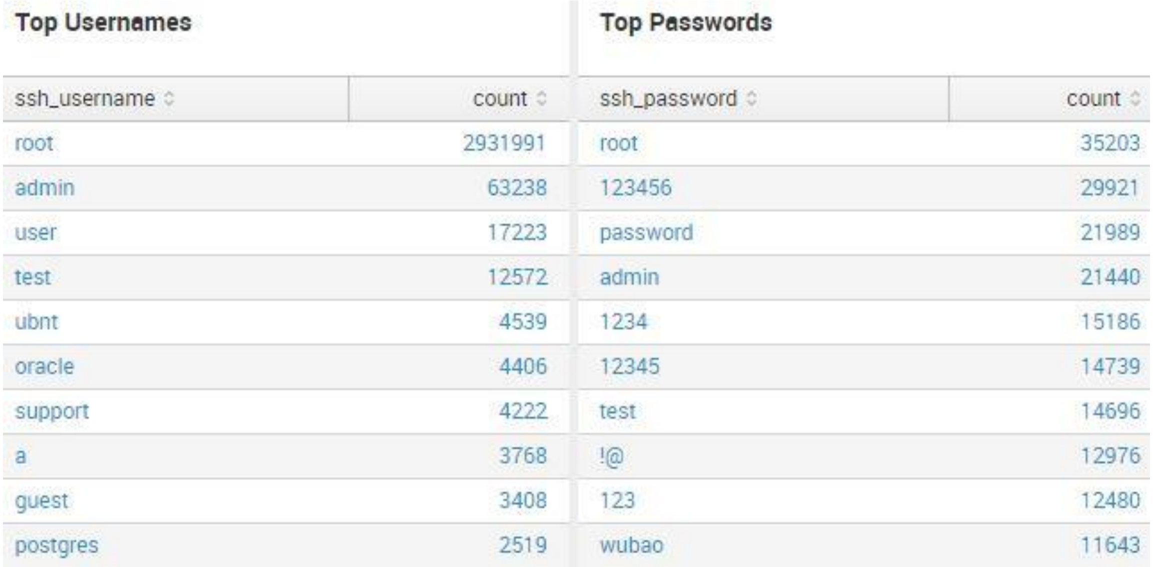


Figure 8.6: Summary of Operating Systems used by Attackers

Next in figure 8.7, the collective summary of top usernames/passwords along with number of attempts used to access all honeypot nodes. From stats below the top most usernames in top to down list are “root”, “admin”, “user” and “test”. Then results for summary of top most password are “root”, “123456”, “password” and “admin”.



Top Usernames

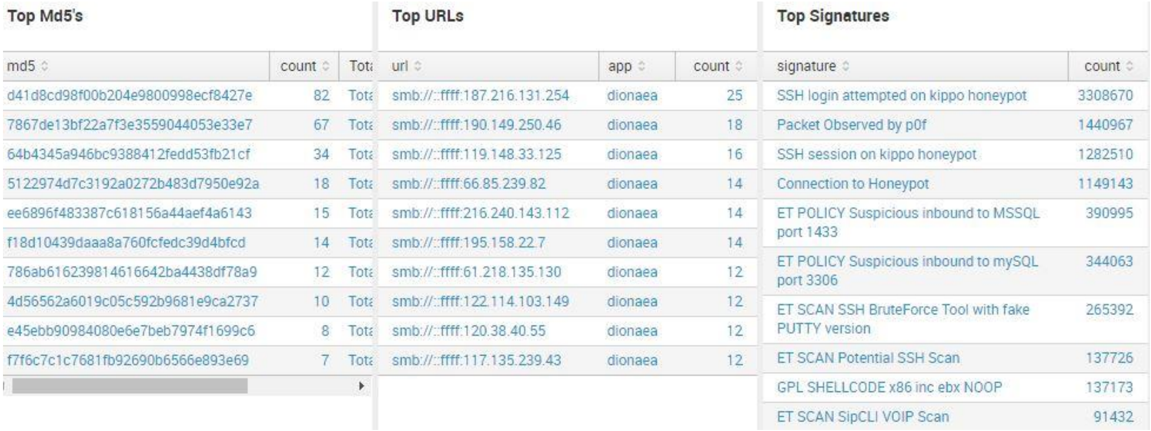
ssh_username	count
root	2931991
admin	63238
user	17223
test	12572
ubnt	4539
oracle	4406
support	4222
a	3768
guest	3408
postgres	2519

Top Passwords

ssh_password	count
root	35203
123456	29921
password	21989
admin	21440
1234	15186
12345	14739
test	14696
!@	12976
123	12480
wubao	11643

Figure 8.7: Summary of Usernames and Passwords used by attackers

Next statistics in Figure 8.8 contains summary of top malware collected along with details of their MD5 hashes, top URLs and top signatures used in detecting cyber attacks. The results also provide other information like number of counts detected, honeypot app and other associated information.



Top Md5's

md5	count	Tot
d41d8cd98f00b204e9800998ecf8427e	82	Tot
7867de13bf22a7f3e3559044053e33e7	67	Tot
64b4345a946bc9388412fedd53fb21cf	34	Tot
5122974d7c3192a0272b483d7950e92a	18	Tot
ee6896f483387c618156a44aef4a6143	15	Tot
f18d10439daaa8a760fcfedc39d4bfcd	14	Tot
786ab616239814616642ba4438df78a9	12	Tot
4d56562a6019c05c592b9681e9ca2737	10	Tot
e45ebb90984080e6e7beb7974f1699c6	8	Tot
f7f6c7c1c7681fb92690b6566e893e69	7	Tot

Top URLs

url	app	count
smb://::ffff:187.216.131.254	dionaea	25
smb://::ffff:190.149.250.46	dionaea	18
smb://::ffff:119.148.33.125	dionaea	16
smb://::ffff:66.85.239.82	dionaea	14
smb://::ffff:216.240.143.112	dionaea	14
smb://::ffff:195.158.22.7	dionaea	14
smb://::ffff:61.218.135.130	dionaea	12
smb://::ffff:122.114.103.149	dionaea	12
smb://::ffff:120.38.40.55	dionaea	12
smb://::ffff:117.135.239.43	dionaea	12

Top Signatures

signature	count
SSH login attempted on kippo honeypot	3308670
Packet Observed by p0f	1440967
SSH session on kippo honeypot	1282510
Connection to Honeypot	1149143
ET POLICY Suspicious inbound to MSSQL port 1433	390995
ET POLICY Suspicious inbound to mySQL port 3306	344063
ET SCAN SSH BruteForce Tool with fake PUTTY version	265392
ET SCAN Potential SSH Scan	137726
GPL SHELLCODE x86 inc ebx NOOP	137173
ET SCAN SipCLI VOIP Scan	91432

Figure 8.8: Summary of Top Hashes, URLS and Signatures

In the table below (Table 8.1), the list of overall top attacker's details like source IP Addresses (IPv4 and IPv6), Country and their number of attack probes initiated towards deployed honeypot nodes are given. It is clear that most of the attacks are launched from outside Pakistan region, in which top most countries are China, United States, India, Korea, UK and Chile. From these trends a recommendation arises that educational internet space can be secured if collected IP addresses are banned through blacklist enteries used in firewall or related security controls.

Source IP Addresses	Country	Counts
183.3.202.195	China	371520
116.31.116.16	China	316001
116.31.116.5	China	308529
116.31.116.39	China	243691
116.31.116.15	China	224185
183.3.202.178	China	181128
183.3.202.177	China	180808
183.3.202.196	China	176848
69.60.116.97	United States	44282
216.117.130.133	United States	43431
106.51.255.21	India	36495
211.228.17.137	Republic of Korea	36462
210.68.57.135	Taiwan	36434
182.100.67.248	China	34358
218.87.109.247	China	33600
182.100.67.62	China	33489
158.85.2.157	United States	33024
150.150.33.72	Republic of Korea	32569
221.229.172.119	China	32292
::ffff:61.147.103.137	China	32037
::ffff:74.208.112.7	United States	30227
58.218.205.83	China	29188
150.150.1.39	Republic of Korea	28930
175.23.30.37	China	27685
118.33.89.167	Republic of Korea	27632
218.65.30.92	China	27097
109.228.57.254	United Kingdom	27068
111.68.96.41	Pakistan	26712
134.213.152.201	United Kingdom	24769
218.87.109.245	China	24767
218.189.13.155	Hong Kong	24548
115.248.186.3	India	22631
201.238.207.34	Chile	22258
150.150.32.245	Republic of Korea	21121

Table 8.1: Summary of Top Attackers

From the above summary of attack statistics, it is concluded that there a huge number of attack probes launched on our regional internet space. Based on results produced by this prototype, it is not clear that all attacks are automated, but these results and attack statistics set solid grounds that multiple types of cyber attacks are happening on our internet space.

So, usage of honeypots proved that honeypot technology is a great tool to detect, collect and examine the attack patterns. They not only provide information regarding attack patterns but they are very useful in collecting details of attacks like nature of attack probe, origin, username/password along with methodology adopted to perform attack and all other associated information.

8.3 Conclusion

As noticed from results of prototype, the honeypot nodes collect bundles of information regarding attacks, so consent monitoring is one of the core requirement in safeguarding production systems. For this there is a requirement to have dedicated people for watching logs, watching honeypots actually see what's going on. Essentially honeypots valuable information can only be achieved once keen monitoring is performed so that taking the information and then use this information to safeguard real environment. Once the proper monitoring is achieved honeypots will build its own threat intelligence for that network and will provide the real value of active defense using trends data. Based on this custom IDS and SIEM rules can be build, all this is based on event correlation and continuous event monitoring actually taking the data and using it to learn from attackers.

Using honeypots one can extract and normalize the data to build more interesting metadata in the form of a dashboard as mentioned earlier. As a result, the use of distributed honeypots for gathering and analyzing latest cyber attacks trends definitely fulfills the research work goal. The discussed results clearly represent the latest trends of cyber attacks faced by educational network of Pakistan internet space. In this way by event correlation and keen analysis of data e.g. analysis conducted to detect IP addresses, their connected Autonomous System, username and passwords leave bunch of information, collectively concrete information can be provided to track the attacker. What else the attacker is doing in past? what they did yesterday? What they did in previous week? in this way it builds complete picture of an attacker. Thus enabling us to understand the risk, indeed a real risk. This research gathered and hashed malware samples, then used this hash to correlate in real environment to check it shows up valuable information or not, which provides us very interesting results in the form of their presence in real network.

So, honeypots provide an active defense approach, it comes how to approach threat space, related environment and tools. What already have at disposal to annoy attackers, to trap them, bother them, distract them from the environment of our control? It requires a robust monitoring setup, from where one can watch them, learn from them, gathering data and actually trying to learn from adversaries. In other words, it is done to shield cyber space so that attackers will not be able to attack back. Attackers do have right to their privacy. Infact by reducing the Mean time to Detect (MTTD) and Mean Time to Respond (MTTR) is to close this gap. The effort of closing gap will ensure no damage or little damage which can be recovered very quickly.The recent report initmated that the average time to detect an attack within a network and respond is 205 days, so the effort is to close the gap in between MTTD and MTTR. Honeypots are definitely one of the way to reduce this gap.

8.4 Future Work

Future work can be an expansion of honeypot sensors, so that maximum statistics of attack data can be gathered for better understanding of attack motives. In our design, there are four different locations based distributed deployment of honeypot sensors. This deployment has limited resources and other constraints. Another thing that has used in prototype is IP address for detection techniques. Mostly single public IP Address is shared by different users, so to trace back actual system some extra effort is required. Additionally, this setup can be utilized for learning actual and live behavior of attacks, which is an added advantage for infosec academics community. Moreover, based on collected data, indigenous block lists can be built and integrated with existing SIEM solution in order to safeguard production systems. As a case study, we only targeted the educational internet space. This sort of setup can be established for enhancing cyber attacks surveillance of a whole country's cyber space.

In short the lesson learned from this research work is that it is necessary to keep a consistence eye over a cyber space in order to safe guard our valuable data and IT assets. As technology swift is at its peak level and almost everything is going to be digitized. So, this overwhelming usage of internet systems has changed the trends, now battles are fought on digital fields. Now traditional wars are transforming into cyber war, where bombs have been replaced by botnets, bits used in the form of bullets and malwares used in sort of paramilitries for cyber attacks. This technological shift is expected to become World War C, where C means Cyber that demands everyone must be well-prepared to safeguard their systems from attacks of troops of adversaries. So, for this purpose it is observed that results produced by honeypots play an improtant role in learning and monitoring attack surface to which we are consistently connected, directly or indirectly. Computer worms and viruses emanate with full anonymity but the “ballistic missile” reaches along with its return address. Keeping in view the complex nature of cyber warfare, our research shows that skillful team and deep understanding is required to detect these attacks. Though many precautionary measures are taken by placing the valuable systems behind traditional security controls like firewall, antivirus and IPS etc. but still attackers may gain access, so we are still behind the attacker’s curve. But in reality, there is no robust security product or tool or anything like that actually going to protect us.

Often, CIOs focus on getting the right IT workforce with the right or best tools available in market. But, HRM may train whatever workforce is available in IT department and give them tools they need for keep secure functioning of IT services over information highway. Tools like honeypot does play this role at certain extent and plays pivotal role in defending cyber space.

This research gave insight of infosec scenario. Least attention may be paid which does not solve the problem of intrusion detection. Future plan is to mobilize resources to create a pool of all intrusions, malwares, IPs used for attacks and other relevant data which can be used in a national firewall at the main internet gateway to safe cyber space from most of the attacks as well as zero day attacks.

So, future work will focus on whole of the regional cyber space from the perspective of information security. Future scope will involve public sector, private organizations, academia and non-profit ogranizations on a platform of NUST to build a safer cyber space. As a healthy regional cyber space is going to contribute in a healthy Digital World for altruistic globalization.

Appendix “A” – Management Node Installation

1. Prerequisites.

Operating System: Ubuntu 14.04 LTS

```
sudo apt-get update
```

```
sudo apt-get install python2.7 python-openssl python-gevent libevent-dev python2.7-dev build-essential make liblapack-dev libmysqlclient-dev python-chardet python-requests pythonsqlalchemy python-lxml python-beautifulsoup mongodb python-pip python-dev python-numpy python-setuptools python-numpy-dev python-scipy libatlas-dev g++ git php5 php5-dev gfortran
```

```
sudo apt-get install libxml2-dev libxslt1-dev python-dev python-lxml libffi-dev
```

2. Cloning the Repository with Threatstream

```
cd /opt
```

```
sudo git clone https://github.com/threatstream/mhn
```

3. Installing Mnemosyne script

```
cd /opt/mhn/scripts
```

Edit the line CHANNELS and add at the end of the line and inside the single quote:

```
shockpot.events
```

The line should look like this:

```
CHANNELS=’amun.events,conpot.events,thug.events,beeswarm.hive,dionaea.capture,dionaea.connections,thug.files,beeswarn.feeder,cuckoo.analysis,kippo.sessions,glastopf.events,glastopf.files,mwbinary.dionaea.sensorunique,snort.alerts,wordpot.events,p0f.events,suricata.events,shockpot.events’
```

4. Management Node Core Components installation inclusive of MongoDB using following three scripts

cd /opt/mhn/scripts

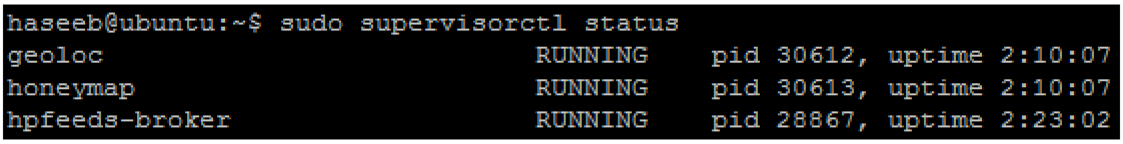
sudo ./install_hpfeeds.sh

sudo ./install_mnemosyne.sh

sudo ./install_honeymap.sh

Once all three scripts run successfully, we will check the status of installation.

sudo supervisorctl status

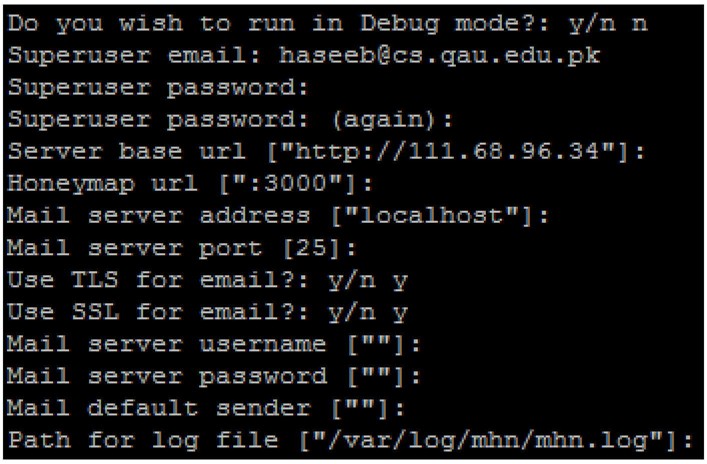


```
haseeb@ubuntu:~$ sudo supervisorctl status
geoloc                          RUNNING    pid 30612, uptime 2:10:07
honeymap                        RUNNING    pid 30613, uptime 2:10:07
hpfeeds-broker                  RUNNING    pid 28867, uptime 2:23:02
```

5. To finish the installation run the last script by issuing the command:

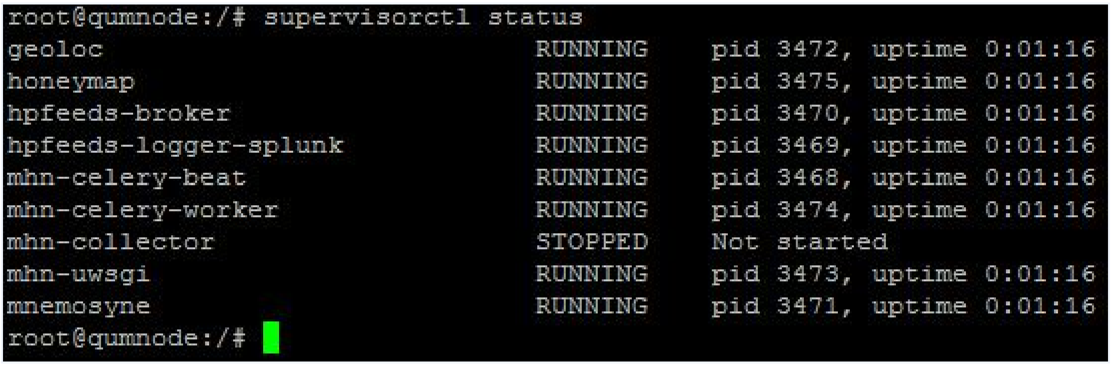
sudo ./install_mhnserver.sh

At one point it prompted to enter some configuration, just configure it with our own preferences and let the script do his job:



```
Do you wish to run in Debug mode?: y/n n
Superuser email: haseeb@cs.qau.edu.pk
Superuser password:
Superuser password: (again):
Server base url ["http://111.68.96.34"]:
Honeymap url [":3000"]:
Mail server address ["localhost"]:
Mail server port [25]:
Use TLS for email?: y/n y
Use SSL for email?: y/n y
Mail server username [""]:
Mail server password [""]:
Mail default sender [""]:
Path for log file ["/var/log/mhn/mhn.log"]:
```

Below is a screenshot of Management node running with all required services.



```
root@qumnode:/# supervisorctl status
geoloc                          RUNNING    pid 3472, uptime 0:01:16
honeymap                        RUNNING    pid 3475, uptime 0:01:16
hpfeeds-broker                  RUNNING    pid 3470, uptime 0:01:16
hpfeeds-logger-splunk           RUNNING    pid 3469, uptime 0:01:16
mhn-celery-beat                 RUNNING    pid 3468, uptime 0:01:16
mhn-celery-worker               RUNNING    pid 3474, uptime 0:01:16
mhn-collector                   STOPPED    Not started
mhn-uwsgi                       RUNNING    pid 3473, uptime 0:01:16
mnemosyne                       RUNNING    pid 3471, uptime 0:01:16
root@qumnode:/#
```

Appendix “B” – Sensor Nodes Installation

1. Prerequisites.

Operating System: Ubuntu 14.04 LTS

```
sudo apt-get update
```

```
sudo apt-get upgrade
```

2. SSH Installation

```
sudo apt-get install openssh-server
```

The configuration file for sshd is located at /etc/ssh/sshd_config, search for the port directive and change it to the port that we want for example 2233, then restart the service by issuing the command:

```
sudo service ssh restart
```

3. SENSORS DEPLOYMENT

Installing Kippo Honeypot on a Sensor Node by entering following command.

```
wget "http://mnode.qau.edu.pk/api/script/?text=true&script_id=11" -O deploy.sh && sudo bash deploy.sh http://mnode.qau.edu.pk uLDDxj7L
```

4. Installing Dionaea Honeypot

```
wget "http://mnode.qau.edu.pk/api/script/?text=true&script_id=4" -O deploy.sh && sudo bash deploy.sh http://mnode.qau.edu.pk uLDDxj7L
```

5. Installing Shockpot Honeypot

```
wget "http://mnode.qau.edu.pk/api/script/?text=true&script_id=15" -O deploy.sh && sudo bash deploy.sh http://mnode.qau.edu.pk uLDDxj7L
```

6. Installing ElasticHoney Honeypot

wget "http://mnode.qau.edu.pk/api/script/?text=true&script_id=6" -O deploy.sh && sudo bash deploy.sh http://mnode.qau.edu.pk uLDDxj7L

7. Installing SNORT and SURRICATA Honeypot

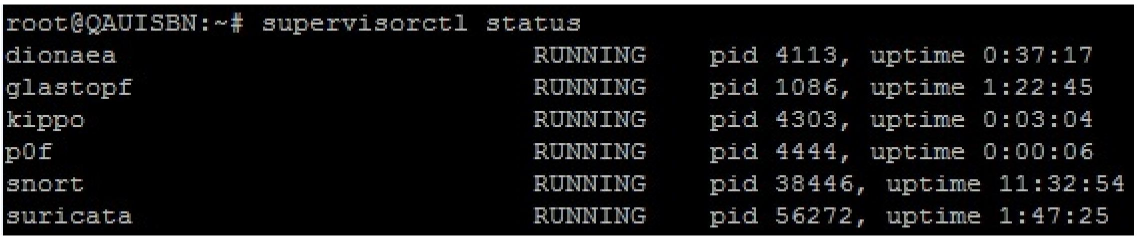
wget "http://mnode.qau.edu.pk/api/script/?text=true&script_id=3" -O deploy.sh && sudo bash deploy.sh http://mnode.qau.edu.pk uLDDxj7L

wget "http://mnode.qau.edu.pk/api/script/?text=true&script_id=13" -O deploy.sh && sudo bash deploy.sh http://mnode.qau.edu.pk uLDDxj7L

8. Installing p0f Honeypot

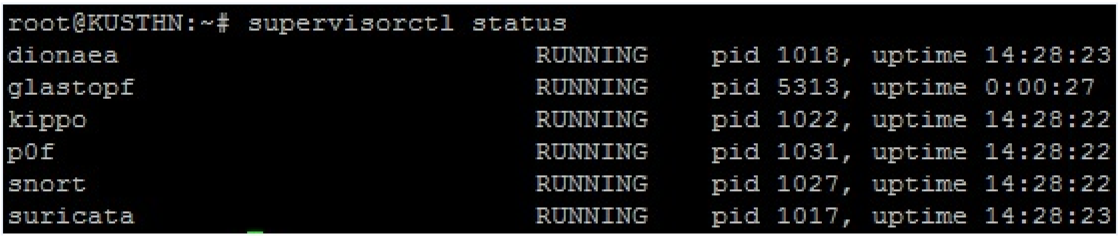
wget "http://mnode.qau.edu.pk/api/script/?text=true&script_id=16" -O deploy.sh && sudo bash deploy.sh http://mnode.qau.edu.pk uLDDxj7L

Screenshot of Quaid-i-Azam University (QAU), Islamabad sensor node with status of honeypots running on this sensor.



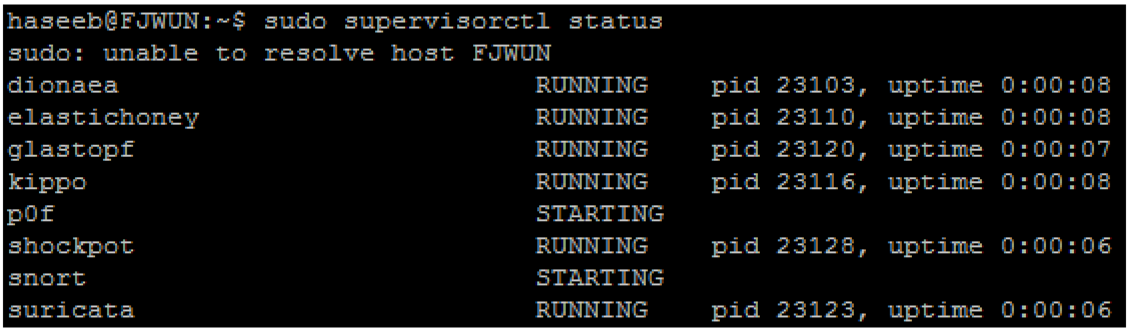
```
root@QAUISBN:~# supervisorctl status
dionaea                          RUNNING    pid 4113, uptime 0:37:17
glastopf                         RUNNING    pid 1086, uptime 1:22:45
kippo                            RUNNING    pid 4303, uptime 0:03:04
p0f                              RUNNING    pid 4444, uptime 0:00:06
snort                            RUNNING    pid 38446, uptime 11:32:54
suricata                         RUNNING    pid 56272, uptime 1:47:25
```

Screenshot of Kohat University of Sciences and Technology (KUST), Kohat sensor node with status of honeypots running on this sensor.



```
root@KUSTHN:~# supervisorctl status
dionaea                          RUNNING    pid 1018, uptime 14:28:23
glastopf                         RUNNING    pid 5313, uptime 0:00:27
kippo                            RUNNING    pid 1022, uptime 14:28:22
p0f                              RUNNING    pid 1031, uptime 14:28:22
snort                            RUNNING    pid 1027, uptime 14:28:22
suricata                         RUNNING    pid 1017, uptime 14:28:23
```

Screenshot of Fatima Jinnah Women University (FJWU), Rawalpindi sensor node with status of honeypots running on this sensor.



```
haseeb@FJWUN:~$ sudo supervisorctl status
sudo: unable to resolve host FJWUN
dionaea                          RUNNING    pid 23103, uptime 0:00:08
elastichoney                     RUNNING    pid 23110, uptime 0:00:08
glastopf                         RUNNING    pid 23120, uptime 0:00:07
kippo                            RUNNING    pid 23116, uptime 0:00:08
p0f                              STARTING
shockpot                         RUNNING    pid 23128, uptime 0:00:06
snort                            STARTING
suricata                         RUNNING    pid 23123, uptime 0:00:06
```

Appendix “C” – Web Based Analyzer Node Installation

1. Prerequisites.

Operating System: CentOS 7

```
sudo yum update
```

2. Installing splunk for web based analyzing.

```
sudo wget -O splunk-6.5.0-59c8927def0f-linux-2.6-x86_64.rpm 'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=linux&version=6.5.0&product=splunk&filename=splunk-6.5.0-59c8927def0f-linux-2.6-x86_64.rpm &wget=true'
```

3. Installing Apache web server for web based access.

```
sudo yum -y install httpd
sudo systemctl start httpd
sudo systemctl enable httpd
```

4. Allowing splunk, splunk forwarder and HTTPS port on server.

Below are the ports that we used on Web Based Analyzer server:

Web port: 443 (SSL enabled)

Splunkd port: 8089

Splunk Forwarder: 9997

Open port for https (Splunk website)

```
iptables  -A INPUT -i eth0 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
```

Open port for splunkd services

```
Iptables -A INPUT -i eth0 -p tcp --dport 8000 -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp --sport 8000 -m state --state NEW,ESTABLISHED -j ACCEPT
```

6. Open port for Splunk Forwarders

```
iptables -A INPUT -i eth0 -p tcp --dport 9997 -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
iptables -A OUTPUT -o eth0 -p tcp --sport 9997 -m state --state NEW,ESTABLISHED -j ACCEPT
```

7. Verifying by issuing below command.

```
iptables -L
```

8. Allowing ports from firewall.

```
sudo firewall-cmd –permanent –ad-port=443/tcp
```

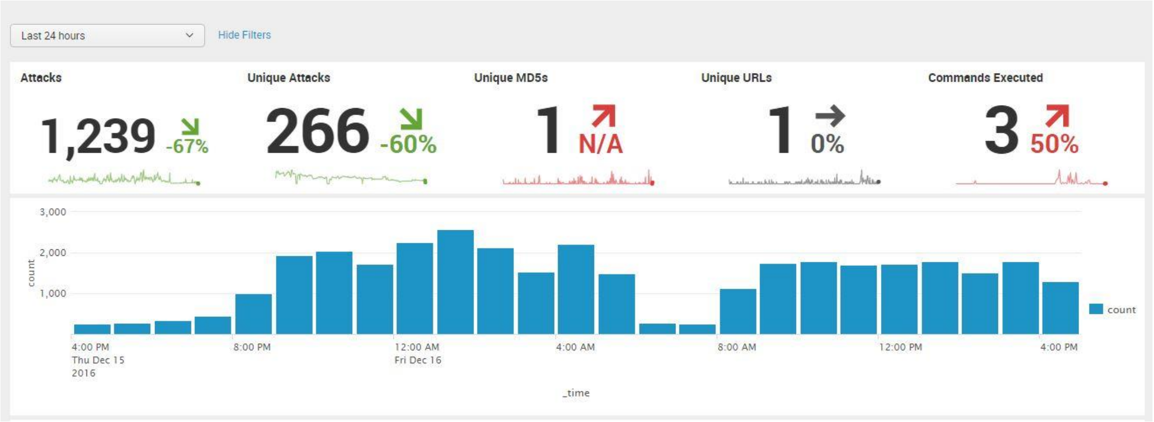
```
sudo firewall-cmd –permanent –ad-port=8000/tcp
```

```
sudo firewall-cmd –permanent –ad-port=9997/tcp
```

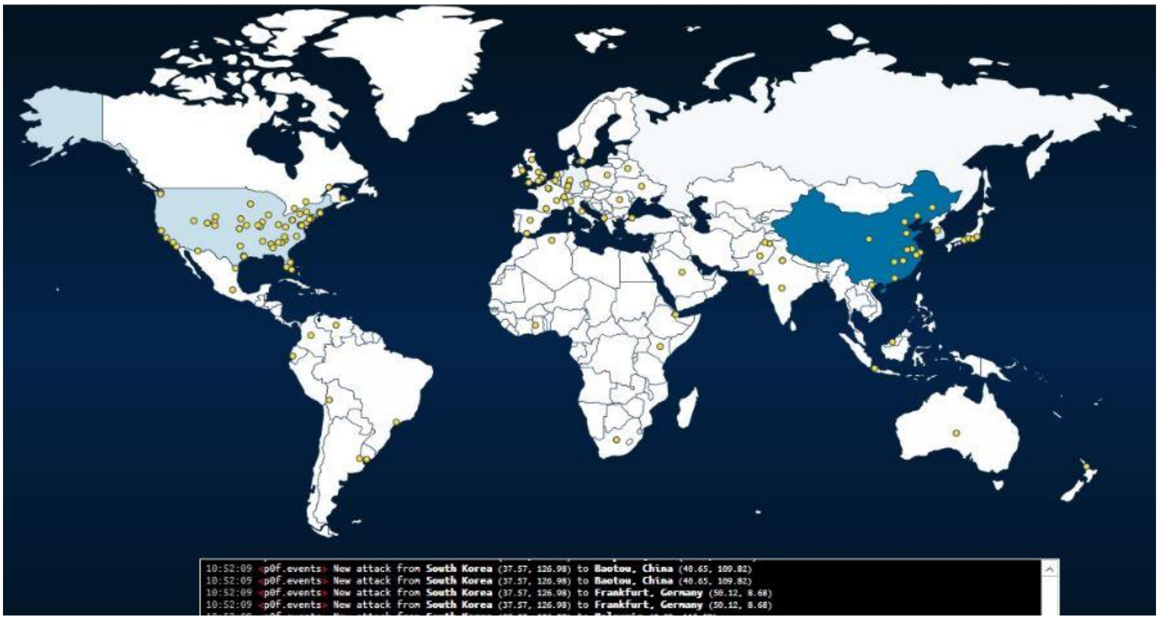
And reload the firewall

```
Sudo firewall-cmd reload
```

Below is a screenshot of Web Based Dashboard for Cyber Attack analysis.

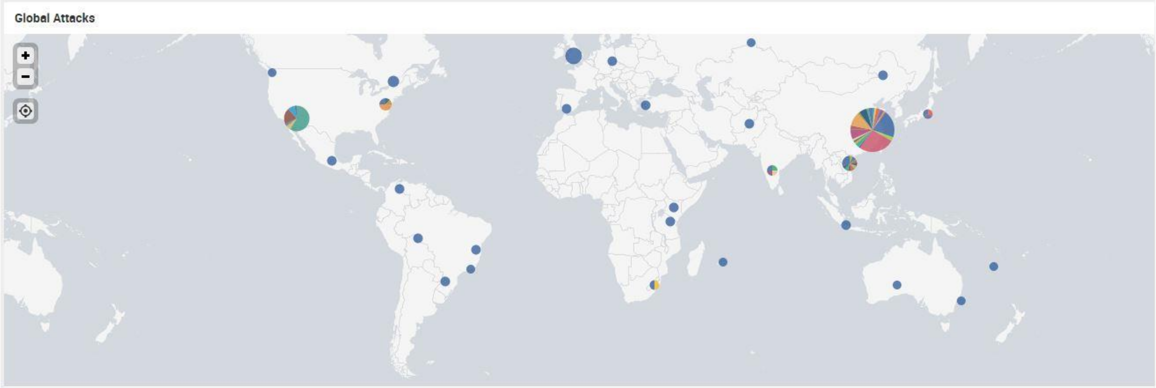


Below figure shows graphical representation of attacker's origin using HPFeeds of our prototype over a global map.



```
10:52:09 <p0f.events> New attack from South Korea (37.57, 126.98) to Baotou, China (40.65, 109.82)
10:52:09 <p0f.events> New attack from South Korea (37.57, 126.98) to Baotou, China (40.65, 109.82)
10:52:09 <p0f.events> New attack from South Korea (37.57, 126.98) to Frankfurt, Germany (50.12, 8.68)
10:52:09 <p0f.events> New attack from South Korea (37.57, 126.98) to Frankfurt, Germany (50.12, 8.68)
```

GeoTagging of cyber attacks spectrum is plotted using Splunk in below figure of web based node.



BIBLIOGRAPHY

[1] L. Spitzner, Honeypots: Tracking Hackers, Boston, MA: Addison-Wesley Longman Publishing Co., Inc., 2002.

[2] C. L. a. M. D. a. F. Massicotte, "Automatic handling of protocol dependencies and reaction to 0-day attacks with ScriptGen based honeypots," vol. 4219 LNCS, 2006, pp. 185-205.

[3] M. Oosterhof, "Kippo Honeypot Desaster," [Online]. Available: https://github.com/desaster/kippo. [Accessed 11 2016].

[4] L. Rist, "Glastopf The Honeynet Project," 27 5 2009. [Online]. Available: https://www.honeynet.org/taxonomy/term/61.

[5] R. MacTiernan, "http://www.academia.edu/1074906/Honeypot_IDS_SNORT_Intrusion_Detection_System," Academia, vol. B00029564, pp. 1-153, 2015.

[6] M. D. V. P. F. Pouget, "Leurre.com: on the Advantages of Deploying a Large Scale Distributed Honeypot Platform," in E-Crime and Computer Conference, MONACO, 2005.

[7] K. Gary, "Analysis of Attacks Using a Honeypot," in CyberForensics 2014, Greenwich, 2014.

[8] P. P. T. B. Pavol Sokol, "Data Collection and Data Analysis," in Institute of Computer Science, Kosice Slovakia.

[9] C. L. a. M. D. a. F. Massicotte, "Automatic handling of protocol dependencies and reaction to 0-day attacks with ScriptGen based honeypots," in Lecture Notes in Computer Science including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics, 2006, pp. 185-205.

[10] L. Spitzner, Honeypots: Tracking Hackers, Boston, MA USA: Addison-Wesley Longman Publishing Co., Inc., 2002.

[11] T. J. H. a. M. Kilger, "Know Your Enemy: The Social Dynamics of Hacking," The Honeynet Project, Michigan State University USA, 2012.

[12] D. B. a. N. P. DAVID E. SANGER, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," The New York Times, 18 02 2013. [Online]. Available: http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?_r=0. [Accessed 03 12 2015].

[13] I. a. A. M. Mokube, "Honeypots: Concepts, Approaches, and Challenges," in ACM - Proceedings of the 45th Annual Southeast Regional Conference, NewYork USA, 2007.

[14] K. a. S. B. a. Y. T. A. Sadasivam, "Design of Network Security Projects Using Honeypots," J. Comput. Sci. Coll., vol. 20, no. 1047890, pp. 282-293, 2005.

[15] M. Pickett, "A Guide to the Honeypot Concept," in GIAC, 2003.

[16] L. Spitzner, "Symantec Connect The Value of Honeypots, Part One: Definitions and Values of Honeypots," 03 11 2010. [Online]. Available: http://www.symantec.com/connect/articles/value-honeypots-part-one-definitions-and-values-honeypots.

[17] H. Willkommen, "Honeytrap Low Interaction Honeypot," [Online]. Available: http://books.gigatux.nl/mirror/honeypot/final/ch06lev1sec3.html.

[18] G. W. Janet Casey, "MwCollect' collects worm-like malware in a non-native environment," [Online]. Available: https://directory.fsf.org/wiki/Mwcollect.

[19] J. Fielding, "Create a simple honeypot Nepenthes," TechRepublic, [Online]. Available: http://www.techrepublic.com/blog/data-center/create-a-simple-honeypot-with-debian-and-nepenthes/

[20] N. Provos, "Development of the Honeyd Virtual Honeypot," Niels Provos, 2008. [Online]. Available: http://www.honeyd.org/

[21] dawuud, "HoneyBadger," 2016. [Online]. Available: https://readthedocs.org/projects/honeybadger/.

[22] B. Jackson, "Mayhemic Labs WebLaybrinth," Mayhemic Labs , 2009. [Online]. Available: https://github.com/mayhemiclabs/weblabyrinth.

[23] D. F. P. W. N. F. N. W. a. V. P. Roya Ensafi, "Examining How the Great Firewall Discovers Hidden Circumvention Servers," 2015

[24] K. F. a. J. Heidemann, "Detecting Malicious Activity with DNS Backscatter," ACM, 2015

[25] J. K. D. A. A. H. M. B. Zakir Durumeric, "The Matter of Heartbleed," ACM, 2014.

[26] A. F. G. J. M. A. K. M. Z. S. Emiliano De Cristofaro, "Paying for Likes? Understanding Facebook Like Fraud Using Honeypots," ACM, 2014.

[27] S. I. T. Y. D. C. a. M. M. Naomi Kuze, "Detection of Vulnerability Scanning Using Features of Collective Accesses Based on Information Collected from Multiple Honeypots," IEEE, pp. 1067-1072, 2016.

[28] K. P. a. T. M. Ronald M. Campbell, "A Survey of Honeypot Research: Trends and Opportunities," IEEE, pp. 208-212, 2015.

[29] C. Moore, "Detecting Ransomware with Honeypot techniques," in 2016 Cybersecurity and Cyberforensics Conference, Jordan, 2016.

[30] H. C. K. K. V. M. A. T. E. A. M. Leonard, "A Honeypot System for Wearable Networks," IEEE, pp. 199-201, 2016.

[31] P. B. Kevin Springborn, "Impression Fraud in Online Advertising via Pay-Per-View Networks," in 22nd USENIX Security Symposium, Washington DC, USA, 2013

[32] K. s.-J. a. C. H. Joao M. Ceron, "Anatomy of SIP Attacks," USENIX, pp. 25-32, 2012.

[33] B. G., "BitBucket PhpMyAdmin-Honeypot," BitBucket, 2015. [Online]. Available: https://bitbucket.org/gbence/phpmyadmin-honeypot.

[34] dawuud, "HoneyBadger," 2016. [Online]. Available: https://readthedocs.org/projects/honeybadger/.

[35] R. K. S. R. K. Saurabh Chamotra, "Data Diversity of a Distributed Honey Net Based Malware Collection," in Emerging Trends in Networks and Computer Communications (ETNCC), 2011 International Conference on, 2011.

[36] K. K. Lavenya, "HoneyComb : Enhancement to Honeypot Log Management," International Journal of Engineering Research & Technology, vol. Vol.1, no. Issue 6 (August- 2012), pp. 1-6, 2012.

[37] D. Kennedy, "Project Artillery TrustSec Information Security," 2016. [Online]. Available: htthttps://www.trustedsec.com/artillery/.

[38] K. N. R. D. T. K. S. F. S. Felix Leder, "The Honeynet Project," Honeynet Project, 2017. [Online]. Available: https://www.honeynet.org/.

[39] N. Quist, "Active Defense Through Deceptive Configuration," SANS Institute Reading Room Site, USA, 2016.

[40] G. Brindisi, "A WordPress Honeypot," Brindi.si, 2012. [Online]. Available: http://brindi.si/g/projects/wordpot.html.

[41] J. Riden, "Using Nepenthes Honeypots to Detect Common Malware," Symantec Connect, 2006. [Online]. Available: https://www.symantec.com/connect/articles/using-nepenthes-honeypots-detect-common-malware.

[42] J. D. Lukas, "Conpot ICS SCADA Honeypot," Conpot, [Online]. Available: http://www.conpot.org

[43] L. Spitzner, "Sebek | The Honeynet Project," The Honeynet Project, 14 8 2008. [Online]. Available: http://www.honeynet.org/project/sebek.

[44] Q. M. a. B. Shirley, "Honeypots and Honey-Wall Implementation and Analysis," Jacksonville State University, 2010.

[45] R. MacTiernan, "http://www.academia.edu/1074906/Honeypot_IDS_SNORT_Intrusion_Detection_System," Academia, vol. B00029564, pp. 1-153, 2015.

[46] J. Trost, "ThreatStream," Anomali, 2016. [Online]. Available: https://www.anomali.com/platform/threatstream. [Accessed 15 02 2017].

[47] J. Riden, "Using Nepenthes Honeypots to Detect Common Malware," Symantec Connect, 2006. [Online]. Available: https://www.symantec.com/connect/articles/using-nepenthes-honeypots-detect-common-malware

[48] G. H. Project, "Honeynet Project," 18 05 2007. [Online]. Available: http://www.islab.demokritos.gr/honeynet/.

[49] A. Center, "ASSERT - University of Alaska Fairbanks," ASSERT, Fairbanks, AK, 2010.

[50] B. G., "BitBucket PhpMyAdmin-Honeypot," BitBucket, 2015. [Online]. Available: https://bitbucket.org/gbence/phpmyadmin-honeypot.

[51] dawuud, "HoneyBadger," 2016. [Online]. Available: https://readthedocs.org/projects/honeybadger/

[52] N. Provos, "Development of the Honeyd Virtual Honeypot," Niels Provos, 2008. [Online]. Available: http://www.honeyd.org/

[53] J. Fielding, "Create a simple honeypot Nepenthes," TechRepublic, [Online]. Available: http://www.techrepublic.com/blog/data-center/create-a-simple-honeypot-with-debian-and-nepenthes/

[54] E. Tan, "KIPPO - A SSH Honeypot," EDGIS, 27 3 2016. [Online]. Available: https://www.edgis-security.org/honeypot/kippo-updated/.

[55] L. Spitzner, "Sebek | The Honeynet Project," The Honeynet Project, 14 8 2008. [Online]. Available: http://www.honeynet.org/project/sebek

[56] J. Beal, "Network and Information Security," SecDSM, 2016. [Online]. Available: https://www.secdsm.org/archives/2016/10/CyberDeceptionSlideDeck.pdf.

[57] W. B. S. M. I. Muhammad Haseeb Jalalzai, "DNS security challenges and best practices to deploy secure DNS with digital signatures," in Applied Sciences and Technology (IBCAST), 2015 12th International Bhurban Conference on, Islamabad Pakistan, 2015.

[58] E. Williams, "Dropping Zip Bombs on Vulnerability Scanners," HackaDay, 2017. [Online]. Available: http://hackaday.com/2017/07/08/dropping-zip-bombs-on-vulnerability-scanners/

[59] M. D. V. P. F. Pouget, "On the Advantages of Deploying a Large Scale Distributed Honeypot Platform," in Institute Eurocom, France, 2007.

[60] E. -. e.-c. a. c. e. 2006, "Monaco," in ECCE-Conference, Monaco, UK, 2006.

[61] "AusCERT a leading Cyber Emergency Response Team (CERT) in Australia and Asia/Pacific Region," 2007. [Online]. Available: https://www.auscert.org.au/main. [Accessed 02 2016].

[62] R. L. H. O. D. C. B. C. John Levine, "The Use of Honeynets to Detect Exploited Systems Across Large Enterprise Networks," in IEEE SMC Information Assurance Workshop, West Point, NewYork, 2003.

[63] "Spanish Honeynet Project," [Online]. Available: https://honeynet-es.org/.

[64] R. Siles, "HoneySpot: The Wireless Honeypot, Monitoring the Attacker's Activities in Wireless Networks," in The Spanish Honeynet Project (SHP), Spain, 2007.

[65] "CERT.br - Distributed Honeypots Projects," honeyTARG Honeynet Project, [Online]. Available: https://honeytarg.cert.br/honeypots/#porto-velho.

[66] "Tunisian Honeynet Project SAHER HoneyNet," tunCERT Tunisian Computer Emergency Response Team, [Online]. Available: http://www.honeynet.tn/.

[67] A. C. J. R. S. M. David Watson, "UK Honeynet Project," [Online]. Available: http://www.ukhoneynet.org/.

[68] "Chinese Distributed Honeynet deployment with CNCERT/CC," [Online]. Available: http://www.honeynet.org.cn/index.php?option=com_content&task=view&id=80&Itemid=33.

[69] "UNC Charlotte Honeynet Alliance," Center of Academic Excellence in Information Assurance Education, [Online]. Available: http://honeynet.uncc.edu/.

[70] M. B. R. A. P. L. Roberto Sanchez, "Proyecto Honeynet National Autonomous University of Mexico UNAM," 2015. [Online]. Available: https://www.honeynet.unam.mx/en.

[71] T. H. P. Bruce Schneier, "The Honeynet Project®…improving the global security of the Internet," in IEEE Security Tracking the Wild Hacker, Greece, 2003.

[72] H. E. Commission, "PERN," HEC, 2 August 2017. [Online]. Available: http://www.pern.edu.pk/.