HOW TO INSTALL/USE HONEYPOT FOR DOMAIN TAKE-DOWN PROBLEMS

by

Oluwabukunmi Olayiwola

A thesis submitted to the Faculty of the University of Delaware in partial fulfillment of the requirements for the degree of Master of Science in Cybersecurity

Summer 2020

HOW TO INSTALL/USE HONEYPOT FOR DOMAIN TAKE-DOWN PROBLEMS

by

Oluwabukunmi Olayiwola

Approved: _____
Haining Wang, Ph.D.
Professor in charge of thesis on behalf of the Advisory Committee

Approved: _____
Mark S. Mirotznik, Ph.D.
Interim Chair of the Department of Electrical and Computer Engineering

Approved: _____
Levi T. Thompson, Ph.D.
Dean of the College of Engineering

Approved: _____
Douglas J. Doren, Ph.D.
Interim Vice Provost for Graduate and Professional Education and
Dean of the Graduate College

ACKNOWLEDGMENTS

I would like to dedicate this Thesis first of all to God Almighty for the wisdom and strength to successfully complete this thesis.

To my wonderful Parents and Siblings who were always there to encourage and support me. I would also like to thank my Advisor, Professor Haining Wang, for the guidance throughout this work; and to all my Professors, all University of Delaware Staffs and Friends who made this journey a memorable and a productive one.

TABLE OF CONTENTS

LIST OF FIGURES v
ABSTRACT vi

Chapter

1 INTRODUCTION 1

1.1 Motivation 1
1.2 Background 2
1.3 Problem Statement 4
1.4 Objectives/Research Goals 5
1.5 Research Questions 5
1.6 Research Organization 5

2 UNDERSTANDING DOMAIN TAKE-DOWN PROCEDURE 6

2.1 Overview of Domain Registration and Domain Take Down 6
2.2 Reasons for Domain Take-Down and Identifying Domain Take Down Problems 7

2.2.1 Advantages of Domain Take Down 9
2.2.2 Disadvantages of Domain Take Down 10

3 HONEYPOT 11

3.1 Honeypot Overview and Architecture 11

3.1.1 Types of Honeypot 12
3.1.2 Honeypot Classification 13
3.1.3 System Configuration 14

3.2 Using Honeypot to Identify Domain Takedown Problems 15

3.2.1 How Honeypot works 15

3.2.2 Positioning of Honeypot ……. 16
3.2.3 Configuring/Setting of Honeypot …… 18
3.2.4 Honeypot Software Solution ……... 19

4 RELATED WORK ……... 21

4.1 HoneySpam: Honeypots Fighting Spam at the Source ……... 21
4.2 Taking Down Websites to Prevent Crime ……... 22
4.3 Examining the Impact of Website Take-down on Phishing ……... 22

5 DISCUSSION ……. 24

5.1 Advantages …….. 24
5.2 Limitations ……..…… 26
5.3 Importance of Honeypots …… 27
5.4 Best Practices to deploying honeypots – Things to look out for …… 28
5.5 Conclusion …….. 30

REFERENCES ……..…….. 31

Appendix

A ACRONYMS ……..…… 36

LISTS OF FIGURES

Figure 1.1 Honeypot Architecture: From C K Shyamala, N Harini, Dr T R Padomanabhan (2011) ……...….... 12

Figure 3.1 A Honeypot Place at the back of the network: From Mohammadzadeh.e.n, Hamid, Honarbakhsh, Roza, and Zakaria, Omar (2012) …… 17

Figure 3.2 A Honeypot Placed in front of a Network: From Mohammadzadeh.e.n, Hamid, Honarbakhsh, Roza, and Zakaria, Omar (2012) ……..… 18

ABSTRACT

Defense against cyberattacks is a major task that has been actively pursued and conducted in the security community over the years. Likewise, domain takedown procedure is known to be an effective way in defending against common cyberattacks like Phishing. It is also used to restrain various cybercrimes similar to malware, contents including child sexual abuse, human trafficking, etc. Therefore, as the development in hardening systems increases, the attack is also relatively expanding. On the other hand, there are cases where securing a system is usually based on the intrusion that has already occurred, which causes us to speculate the attacker's activities that are usually overlooked. Moreover, due to the increasing level of cyber-attacks and crimes on the Internet, there have been integrity issues relating to domain takedown procedure where some of these illegal domains are being reused, enabling attackers the free access to infiltrate the system.

To better address this problem, this research explores the architecture of honeypot: a security mechanism placed to detect, distract and prevent or restrain illegal attempt/activities against information system. It further describes how to install or use a honeypot to combat domain takedown problems. In addition, this study shows a detailed literature review of previous researcher's view on honeypot and domain takedown problems as well as their solutions, leaving us with the conclusion that no chances should be given in a secure computer system. There should always be active preparation and defense against any sort of such attacks.

Chapter 1

INTRODUCTION

1.1 Motivation

The Internet is known to be of great importance and impact in many fields from education, healthcare, businesses, to government including individuals whose lives have equally been made easy through the access of readily available information in their convenience. Just like common resource, the Internet-based services are subject to a high level of nefarious activities which may have bad consequences for both users and the services providers [2].

Consequently, the development of Domain Name Systems over the years is one of which dominates the internet with the rate of registration increasing drastically giving an increase in the level of cyberattacks as Cyber criminals take advantage of some vulnerabilities associated with the domain names to exploit thereby leaving it compromised. As a result of this, there has been so many actions taken to eradicate domains that have either been created for illegal or have been manipulated. One of which is the domain take down procedure [37].

Domain takedown is one of the most effective ways used to combat/defend against common cyberattacks like phishing and spear phishing. It is also used to alter different cybercrimes by eliminating domains associated with malware, contents including child sexual abuse, human trafficking, money laundering, pharmaceuticals or other illicit goods etc. [7]. This involves steps taken to identify whether a particular domain serves as a threat or a threat itself. After which a decision is made to either suspend the domain or delete it [37].

Due to the rise in the level of nefarious activity noticed on today's Internet, organizations are beginning to employ mechanisms named Intrusion Prevention

Systems (IPS) for identifying and responding to different attacks which are limited to protecting, against already known attacks. As a result, new detection mechanisms are being implemented for use in more powerful reactive-defense systems. One of which is the honeypots [1].

In addition, another technique set in place to monitor illegal activities occurring through the internet by accurately detecting attacks, while relying on an attacker attempt to exploit a vulnerability [1]. Furthermore, within the last few years, there have been recommendation of many different uses of honeypots. Some of them are utilized to waste the attackers time others to decrease malicious activity or to trick attackers while there are some used to examine the intrusion steps of the attackers. Honeypot applications are numerous and there are so many considerations associated with its review [40].

Therefore, to better ensure adequate defense against cyber attackers and to address these issues, this research extends from taking down domain mechanism to proposing the use of honeypot which involves revealing ways of installing it to identify and help resolve the domain take-down problems. Honeypot is a known mechanism adopted which shows how security tools cannot be overemphasized giving that they can adequately use to detect and minimize cyber-attacks. Moreover, other research view is being explained relating to the different issues as well as proposing measures to completely eradicating these compromised domains to maintain the privacy and Integrity of both the organizations and individuals. Consequently, this research aims at providing best practices for domains that could be prone to attack, notify those that have been a victim of an attack and warnings to those who are engaging to illegal use of domain.

1.2 Background

Domain Take-Down is one of the widely adopted mechanism to defend again all form of cybercrime by researchers and institutions and a powerful tool against

cybercrime. Previous research showed how takedown is used to disrupt a range of these crimes through removing the domain used. However, domain take-down can only be done at the registrar level which requires the intervention by service providers, both hosting providers and domain name registrars whenever a problem is noticed. The takedown of these domains is achieved in various ways which include the hosting provider taking down the website, having the owners of a compromised machine remove offending pages, suspending the domain name, or seizing the physical server as part of a wider law enforcement initiative. When a domain is involved in illicit activities, such as malware distribution, pharmaceutical, and human trafficking, it can be seized by a law enforcement agency. Domain takedown is an example of situational crime prevention, as it aims to change the environment in which crime occurs.

Moreover, it has been identified by previous research that little or no information is available about the take-down operations and their effectiveness where some have been reused or bought by another party which contradicts the influence of reliability, security and integrity.

Additionally, acts that were relatively accepted in the previous years are now disapproved by Law enforcement agency like the Anticybersquatting Consumer Protection Act (ACPA), World Intellectual Property Organization (WIPO), Internet Corporation of Assigned Names and Numbers (ICANN) etc. For example, cybersquatting also known as domain squatting is one of which involves registering, trafficking in or making use of internet domain name with the intention of selling with a higher price someone else's trademarked domain. It is also found that social networking websites like twitter, Facebook etc. have tried to restrain cybersquatting, thereby making it a violation of their terms of service. [5, 41]. This is so because the rate of cyberattack has significantly increased over the years and some of the activities if support could serve as a threat.

1.3 Problem Statement

Cybercrimes are known to be illicit activities performed through the internet or facilitated by diverse forms of computer technology like the use of online social networks, sending sexual uncensored digital photos with a smart phone or digitally distributing child pornography, Phishing, bullying/harassing others and social engineering or cyberstalking etc. Unfortunately, all these nefarious activities continue to increase drastically as technology evolves.

Similarly, domain names although meant for legal activities has equally been compromised by malicious actors to deceive various individuals. There are situations where some domains have either been deleted, expired, banned or deactivated by the registrars due to illegal actions or dormancy. What these Cyber attackers do is that they create and adopt domain names that are visually similar to that of the legitimate brands to perform their criminal activity. Domain reuse has given attackers leverage/free access to infiltrate the system which has posed a lot of problems on the internet that affects government, organizations and individuals.

Despite the fact that domain take down has been implemented for years, little is known about the importance of website takedown as an intervention technique to disrupt different types of online crime. In particular, websites can quickly reappear, and legitimate websites can be poorly jeopardized [34, 35]. Moore and Clayton examined the effects of website takedown on phishing, and found that it is helpful, but it cannot completely mitigate phishing attacks as it will never be prompt. [19, 34].

Moreover, malicious actors adopt legitimate domains and creates a link in form of an attachment to deceive users to clicking on it thereby redirecting them to a malicious site to get their personal information. Although, it is through a familiar site like file sharing, these individuals unaware of their tactics access the file causing them to become a victim.

Additionally, it has been found that there are those involved in cybersquatting, they are known for their practice in registering domain names that are identical to that

of an existing trademark with the intent of benefiting from it by selling the names to those businesses for a profit.

1.4 Objectives/ Research Goals

The goal of this research is to explain the process involved in installing honeypot and explain how it can be used for domain take-down problems.

1.5 Research Questions

Based on the problems explained, and the objectives, this research aims at answering these questions:

1. What are the reasons for a domain take-down?
2. What is the domain take-down procedure?
3. What are the security gaps associated with domain take-down?
4. What is the best solution that can be implemented for domain take-down problems?
5. How to use honeypot for domain take-down problems?
6. What is the importance of honeypot as technology increases?

1.6 Research Organization

Therefore, this research is organized as follows. Chapter 2 explains the domain take-down procedure, Chapter 3 showed an overview on the architecture of honeypot. Chapter 4 revealed various related research, where Chapter 5 showed a discussion with regards to the advantages and limitations of honeypot as well as best practices that highlights the steps individuals can follow to help protect themselves and prevent them from being exploited, and finally concluded the study.

Chapter 2

UNDERSTANDING DOMAIN TAKE-DOWN PROCEDURE

2.1 Overview of domain registration and domain take down

The TLDs (Top Level Domains) assigns name to websites and in order for a user to setup a website, a TLD needs to be registered with a registrar. Once that has been done, such user becomes the registrant. There are various steps that is required for registration. One of which is that giving the fact that two TLDs cannot be the same, the registrant has to examines the availability of the domain name and once the domain is chosen, the name is submitted to the ICANN accredited registrar by the registrant who then pays the required fee which makes the domain active for a restricted time. Once the domain becomes active, for it to be linked to the internet, a registration record must be created which has to be configured by the registrar. The registrar then configures the Domain Name System (DNS) to enable Internet address resolution. Address resolution facilitates services such as email and website hosting. Once these services are up and active, the registrant may create and operate a website.

Consequently, a status is assigned once the domain is active. The status indicates whether the registration of a domain can be transferred, modified or deleted which preserves the state of information. The status makes data a deed, which saves website information in the case of a system failure. Also, information services called WHOIS that identify the registrar and registrant along with their points of contact becomes available.

However, giving this information, to takedown a domain, the law enforcement may use two different methods which includes to file an Acceptable Use Policy (AUP) complaint. If the AUP complaint method is not available or not successful, then a

court order should be used to change the status of the domain. Moreover, court orders may also be used to change the WHOIS directory or the DNS configuration meaning that a law enforcement agency may be able to compel a registrar to delete, redirect or take control of a domain. If this is successful, these methods may be used to hasten online criminal efforts. [23, 39].

2.2 Reasons for Domain Take-Down and Identifying Domain Take Down Problems

Domain takedown is an important procedure used to defend against any form of attack orchestrated by cyber criminals. These attacks have had a great influence in many entities and government agencies. Some of these reasons are explain below but they are not limited to them. There are so many other tactics attackers adopt. Some of them includes:

1. Phishing:

This is simply the use of illegal domains to steal customers credentials such as username and password. There are some domains that disguises as the actual domain whereas their goal is to trick individuals into divulging important information. This act has affected many companies as theses attackers adopt phishing to deceive their employees thereby infiltrating the whole system. Most of these attacks are seen in financial institutions like banks, credit card companies, etc. due to the kind of information they handle. Additionally, some of these nefarious individuals adopt sophisticated means in attacking their customers. They make use of familiar online file sharing/storage services like google doc, OneNote, OneDrive etc. just to bypass most of the scanning tools in place. Whenever anyone clicks on it, it redirects them to a phishing site which most likely poses a security risk.

2. Spam, Malware and Viruses:

Over the past years, there has been a drastic increase with the rate at which spam is being sent. Spamming is another common tactic attacker's use. They send out

unwanted bulk emails to various individuals with the aim of them clicking on an embedded link that will redirect them to a site hosting a malware. Moreover, the actual senders jeopardize end-user's machines on broadband links, which are functioning as a part of a 'botnet'. However, the compromised machine launching the botnet can be ordered to forward spam, also to inspect for security vulnerability or to send a great amount of traffic as a DDOS attack giving that botnets can be used to not only send spam to advance their services, it can steal data as well as allow attacker to access the device and its connection.

Consequently, attackers, has lately employed using botnet to send email viruses which involves a code that is implemented when a user who has been tricked opens an email attachment. This virus gets recreated by itself and then emails everyone associated to that particular organization or address book. However, the main infection vector at present appears to be placing malware onto websites in such a way as to affect those visiting most especially those who do not have the necessary security patches to their systems, or people who can easily be tricked into executing code provided by the website. These attackers mainly target the most vulnerable entity and people who have little or no knowledge about tactics of nefarious individuals.

3. Typosquatting:

This is also called URL hijacking, or a fake URL, a string site or mimicking domain and it is a form of cybersquatting which involves an illegal registration and use of internet domain names that are identical or similar to a particular company, trademark or personal names with the intent to profit from the goodwill of the actual owners. Typosquatting simply involves manipulation. It takes advantage of typographical errors known as typos which involves targeting users who incorrectly type a website address in their web browser for example, Yahooo.com instead of Yahoo.com. Attackers frequently creates fake websites that imitate actual website which have the look and feel of the intended destination so that one may not realize they are at a different site.

These sites are most likely dangerous because they malicious software could be downloaded to one's device just by visiting the site. You don't necessarily have to click on a link or accept a download for dangerous code to install on your computer or smartphone which is also a drive-by download and many typosquatters adopt this method as a way to distribute malicious software with the aim of stealing one's personal information. Additionally, typosquatters sometimes adopt phishing as a means to get you to visit their fake websites. [31]

2.2.1 Advantages of Domain Take Down

Explained below are the advantages of domain take-down.

1. It helps reduce targets becoming a victim. This includes domains that are used for phishing, domain take-down help prevent people who normally would fall for phishing attacks have less malicious domains to access [36].
2. Reduction in the existence of attackers. Constantly taking down domains helps minimize the use of domains for malicious activities. It also discourages nefarious individuals in creating such malicious domains.
3. Increases the protection of brands. Taking down malicious domains helps ensure that the actual brand have the necessary protection. It ensures that organizations worry less about look-alike domains that greatly affect their organization.
4. It also helps reduce the cost of maintenance. Giving the fact that many organizations has been affected by this, there will be a decrease in addressing attacks that could damage a company's reputation. For example, if there is a leak in the credentials of users within an organization or malware infection, the company would not have to pay to get tools that can minimize the risk but also pay to retrieve the information that has been leaked. With domain take -down, there will be a decrease in have to make double payments [19].

2.2.2 Disadvantages of Domain Take Down

1. There could be a misuse of domain take-down. Giving that there is no real legal or economic cost for submitting illegal domains, people might misuse this option where without proper investigation, they assume that a domain is used for nefarious activities. This could affect taking down the actual malicious domain. This could also affect legitimate site which has been taken down.
2. There could also be an advancement in spreading malware. One thing about attackers is that they always find ways of engaging in their malicious acts.
3. It could affect intelligence gathering activities where the law enforcement has little to no idea of the activities of these attackers giving there are not enough malicious domains to monitor [33].

Chapter 3

HONEYPOT

3.1 Honeypots Overview and Architecture

Honeypot has emanated as an essential tool which gives awareness into new attacks and latest trends attackers use to manipulate. There has been diverse explanation relating to what honeypot means giving by different individuals and research. According to Lance Spitzner, founder of the Honeynet Project, a honeypot is a system designed to learn how attackers examines for and exploit vulnerabilies in an IT system. A honeypot is also said to be "an information system resource whose value lies in unauthorized or illicit use of that resources" [21].

Consequently, honeypots are, in their most basic form, information servers that look like the actual one which are deliberately placed in a test network they are then provided with erroneous information that are concealed as files of classified nature. Successively, these servers are originally configured in a way that is hard to penetrate into by attackers although, not impossible. This intentionally reveals them and ensuring that they are very appealing for an attacker in search of a target. In the long run, the server is stacked with monitoring and tracking tools so that it traces every step and activity of an attacker which is also well recorded in a log for reference reasons [29, 49].

Additionally, honeypot is the proactive defense technology, where resources are positioned in a network with the sole purpose of observing and capturing new attacks [24], In other words, a honeypot is a bait, set on a network to draw the attention of attackers. They are also virtual machines, created to imitate the actual machines, thereby creating the impression of running full services and applications,

with open ports that might be found on a typical system or server on a network. However, the main goals of honeypot are to distract the attacker and to gain the information about the attack and the attacker [45].

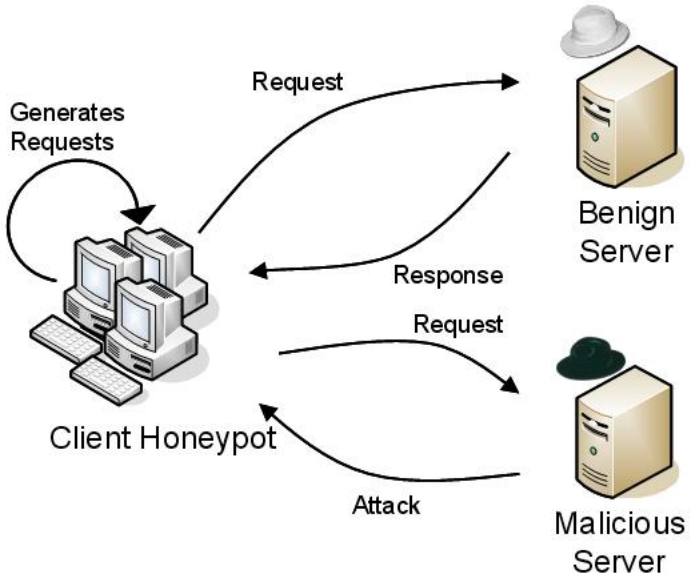

Figure 1.1: Honeypot Architecture: From C K Shyamala, N Harini, Dr T R Padomanabhan (2011).

3.1.1 Types of Honeypot

There are two (2) types of honeypot or basic uses. They are:

1. **The Production /Corporate honeypot** – this type of honeypot is configured in a production environment and serves as a tool for investigating attacks with the aim of using the information to harden the network's security [55]. Moreover, this can be used to identify typosquatting domains relating to an organization where some of these domains might contain malicious contents.
2. **The Research honeypot** – On the other hand, this type is a honeypot that is utilized by researchers and with the purpose of studying attack techniques and other traits like reasons for attacks or idea behind an attack. The information gotten is further used to create defense solutions (such as antiviruses, anti-malware, etc.) that can prevent similar attacks that may arise in the future [55].

3.1.2 Honeypot Classification

However, there are categories in which honeypot is classified based on their level of interaction [12, 50]. There are two popular classification of honeypots available today, they are the low-interaction and the high-interaction. They are defined based on the services, or interaction level, provided by the honeypot to prospective attackers [39]. These classification enables us to understand not just the type of honeypot employed, but also assist in explaining diverse possibilities relating to the vulnerabilities intended for the attacker to manipulate [29].

For the Low-Interaction, they are defined as anything from an open port to a fully simulated network service [11]. The execution procedure of a low interaction honeypot includes installing any kind of operating system emulation software (such as VMWare Workstation or Server), then selecting the operating system and services needed to be imitated, also, setting up a monitoring plan and allow the software function by itself in a typical way. Functional examples of Low Interaction Honeypots are: Honeyd and KFSensor as they are all existing honeypot products [15]. Moreover, the advantages of Low interaction honeypots are that it rests upon its simplicity and they are simple to configure, use and maintain due to its limited capabilities and minimum risk. They are also relatively reliable. The limitation is that they are relatively easy and simple to be identified by attackers, because the service's response is not entirely executed, an experienced attacker can observe how good the imitation capabilities are as long there is enough time to verify [12, 29].

The High-Interaction are actual services that are implemented normally in a secured environment. They are rather more sophisticated than the low interaction honeypots due to the fact that it involves the use of operating systems and factual applications performed in real hardware, without the need to utilize emulation software, running in a normal process. They are many times directly related to services such as databases and shared folders. They present the attackers with a better imitation

of an operating system, so that the attacker can interact without having an idea of what is happening [48]. A very good example of a High Interaction Honeypot is illustrated by Honeynets. One advantage of this is that it is not easy to unmask [12] as there is the feasibility of capturing huge sum of information about the technique of attackers because the intruders are linked with an actual system. This helps organizations to learn about the full extent of the attacker's activities. However, the disadvantage of this is that they are high to maintain, they require the need of a professional and the use of additional technologies like virtual machines to ensure that attackers cannot access the system [29].

3.1.3 System configuration

Honeypots can either work solitary or as a group. A group of honeypots is commonly referred to as a honeynet. Honeynet is simply a bait network which comprises of one or more honeypot that looks like the actual network and it contains several systems that is hosted on one or few servers each representing an environment for example a Windows, Linux and a Mac honeypot machine. Although, one separate honeypot may be simpler to set up, but they are essentially not robust and are more susceptible to unplanned breakdown than honeynet because they lack the load balancing capabilities and redundancy of a group of cooperating servers [14].

Any system on the honeynet may serve as a level of access for attackers. The honeynet collects information on the attackers and redirect them from the actual network. The advantage of a honeynet is that it feels more like an actual network than a honeypot and it has a huge collection space which makes it a preferable solution for enormous, and complicated networks. It also provides attackers with a substitute corporate network which can represent an attractive alternative of the actual one [20].

However, it is important to be conscious of the degree of the hacking hassle you intend to reveal to the attackers while configuring the honeypot because If it's too simple to break, it can be less attractive. Also, if they notice that they are not in contact with the real production system. The main idea is to trick them rather than

being tricked by them. On the other hand, if the system is so difficult to break in, you will really impede any attacks and will not be able to collect any information. Note that, experienced attackers can perceive some signals that they are moving into a honeypot area. The best thing to do is that enticing an attacker with something in the middle of easy and hard will help in replicating a real-life system [8].

3.2 Using Honeypot to Identify Domain Takedown Problems

The custom security solutions, such as Intrusion Detection Systems, may not be sufficient taking into consideration a more complex attack. Moreover, Honeypots provide a mechanism for detecting unique attack vectors, even in a concealed setting. The advent in technology such as virtualization have made honeypots even more useful. Honeypots have limitations, so it is important to understand how honeypots work in order to make the best use of them [39].

3.2.1 How Honeypot works

A honeypot is a mainly a detecting tool as opposed to a preventating solution which works best when matched with endpoint security, an Intrusion Detection System, or SIEM (Security Information and Event Management) [8]. Giving that a honeypot is a trap system, these trap systems are usually structured in a VM or cloud server connected to a network, but they are secluded and severely observed by system and network teams. In order for them to be detected by the attackers, honeypots are formulated to deliberately be at risk with flaws an attacker will identify and attempt to manipulate.

These flaws could be part of a security gap within an application, or system weaknesses like unimportant ports that are opened, out of date software versions, or a bad password. Immediately the attacker finds the victim that is at risk, he will attempt to initiate an attack and increase the advantage until he can secure a definite control of the application.

However, the attackers are oblivious to the fact that all their activities are being is observed carefully. This can rightly be adopted to help solve domains that are created for malicious activities. Giving that one of the disadvantages of domain takedown involves lack of law enforcement or agencies to properly monitor the activities of attacker as there are less domains to work with. Using honeypot, it will help breach this gap as organizations can easily monitor the activities of these attackers where data is being gathered from the attacker's tactics to help strengthen prevalent security policies. These attackers' action can also be reported to legal authorities immediately, which is what often happens with high-end corporate networks. On the other hands, some organizations can tell in particular what domains they need to flag and block within their environment. Honeypot can easily help to identify the domains that needs to be blocked immediately.

3.2.2 Positioning of Honeypot

Honeypot can be placed in two different location either at the back of the firewall or in front of the firewall.

1. At the back of the Firewall:

The substantial part of honeypots is mainly placed inside the Firewalls shown in the figure 2 below. In order for it to be properly managed. Placing honeypot inside firewall will elevate the threat in internal network, particularly if the internal network was not secured against the honeypots by extra firewall. The advantage of placing honeypot inside the firewall is to properly examine internal attackers as most organization overlook that which also can have great influence on the organization. The issue arises when the internal honeypot is compromised by an external attacker, giving this scenario, the traffic will be unstopped as honeypot traffic; thereby, the attacker has the access to the internal network through the honeypot [29, 35]. It is also possible to place them outside the firewalls.

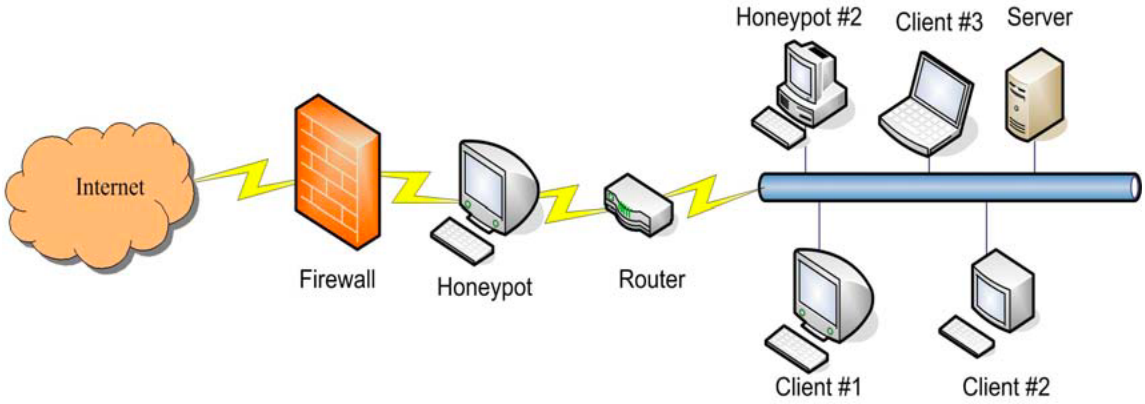

Figure 3.1: A Honeypot Place at the back of the network: From Mohammadzadeh.e.n, Hamid, Honarbakhsh, Roza, and Zakaria, Omar (2012).

2. In Front of the Firewall:

Making use of compromised system in front of firewall decreases the internal network threat shown in figure 3 below. One of the major functions that firewall in a honeypot plays, is that the honeypot firewall confines the things the system returns out and allows all traffic to come in from the internet rather it limits the things that enters into a system from the Internet. By enticing an attacker, into a system, the administrator can observe the activities of the attacker and using the information to create a more secured system that is feasibly inaccessible to future attackers. The main advantages of placing honeypot in front of firewall is that it is not limited by any firewall rule or IDS. The disadvantage is that the internal attackers cannot be easily lured particularly when the outbound traffics of the firewall is limited [29, 32].

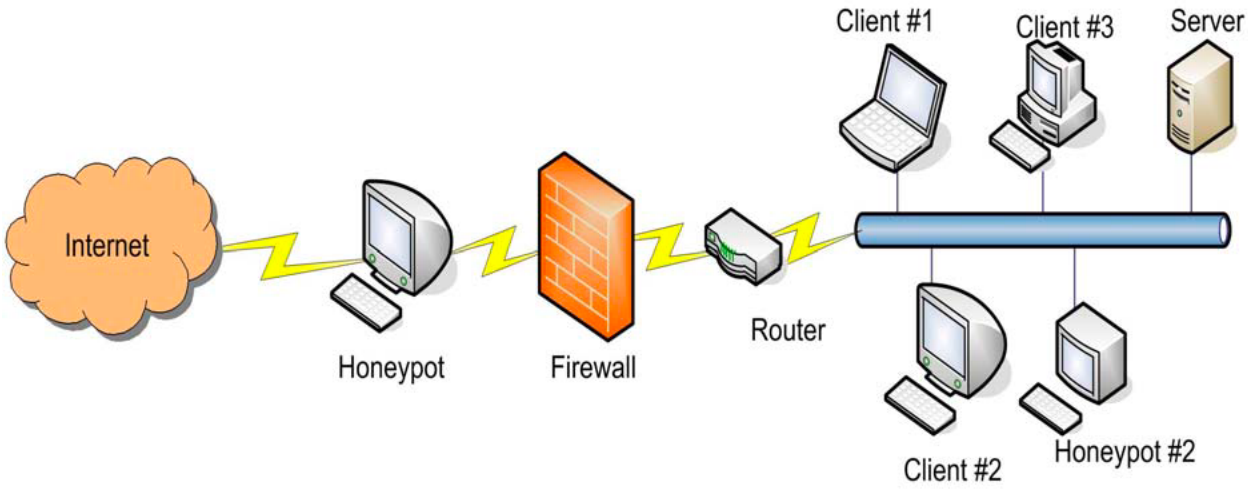

Figure 3.2: A honeypot place in front of a network: From Mohammadzadeh.e.n, Hamid, Honarbakhsh, Roza, and Zakaria, Omar (2012).

3.2.3 Configuring/Setting up of Honeypot

There are diverse kind of public domain tools and software available that can be useful as well as numerous sites that can guide you through the process of configuring a Honeypot. Nearly all the tools seem to have been developed on the Unix platform, where many have been transferred to Microsoft NT. In order to design or develop your own honeypot system, what you will need are a some of the following listed items and a reasonable configuration time:

- A PC which emerges as though an Intel-based PC is fine.
- An operating system. Preferably BSD Unix or RedHat because there are more tools available for the UNIX platform than that of the Microsoft NT.
- Sniffer tool/package. Sniffer tools provide the ability of viewing all of the packets passing between the firewall and the Honeypot system. Making use of a sniffer tool helps you to cross-examine packets in a more thorough way in order to decide which methods the attacker is trying to use in a comprehensive manner than firewall. Consequently, sniffer tools can generate and store log files which can be reserved and utilized for forensic reasons [13].

Another process in setting up honeypot is to generate set of Virtual Machines which are configured on a private network with the host operating system. In order to accelerate data control, a stateful firewall like IP tables can be utilized to log connections. This firewall would typically be configured in Layer 2 bridging mode, making it obvious to attacker. The last action is to seize data, where tools like Sebek and Term Log can be used. Immediately data has been captured, analysis on the data can be performed using tools like Honey Inspector, PrivMsg and SleuthKit [45].

3.2.4 Honeypot Software Solution

To get the best honeypot software, when it comes to honeypot solutions, there are a lot of software solutions to choose from. Below, we have three of the more popular one's for you to choose from:

1. KF Sensor - this is a Windows-based honeypot IDS that begins to observe your network immediately it has been configured. It is a completely developed toolkit that was created to imitate a honeypot aside from the other amazing features. By imitating, it can redirect attacks from systems that are risky and provide a high level of information that can be attained from making use of firewalls and NIDS alone. It is a system installed in a network in order to redirect and learn an attacker's behavior.
2. Glastopf – This is a Python web honeypot which is a low-interaction network emulator and the good thing about this honeypot is that it is an open-source software solution which implies that, like all other alternative solutions with collaborative effort, it includes the effort of numerous experts while will also continue to advance and become better overtime. Another great feature is that it can even imitate applications that are vulnerable to attacks like SQL injection.
3. Ghost USB – This is a USB honeypot and the thing that makes this honeypot unique is that it particularly focuses its attention on malware that spreads

through USB storage devices. This is a big concern giving that USB drives are normally used by employees and authorized users where this continue to cause serious problems. Immediately it gets installed, Ghost USB imitates a USB storage device and spread itself over the network, with the plan of deceiving any malware that circulates using similar devices into corrupting it and once detected, and silently monitored, it becomes easy for administrators to take the necessary measure and precautions.

However, there are other great honeypot solutions for various networking and security need that are not limited to these. Make sure that you select based on your needs and have the necessary resources to build a good honeypot [55].

Chapter 4

RELATED WORK

This chapter focuses on various research view relating to honeypot and domain take down.

4.1 HoneySpam: Honeypots Fighting Spam at the Source

This paper focused on the design and implementation of HoneySpam, a fully operating framework that is based on honeypot technologies which has the ability to tackle the most common malicious spammer activities. The main concept is reducing unwanted traffic by fighting spamming at the source rather than at the receivers. The attributes of HoneySpam involves the slowdown of the e-mail harvesting process the addresses databases are polluted with special e-mail addresses, which directs the spammer to interact with other honeypot services (destination SMTP servers) which enhances spammer traceability. Other attributes include corrupting of e-mail databases through apparently functioning addresses, improved spammer's traceability through the use of a fake open proxies and open relays.

Moreover, the authors installed honeypot open proxies and relays, with the aim of interrupting and blocking unwanted traffic. They also ensured that all interactions were logged with investigation reasons to improve the spammer traceability. Consequently, they took into account the main attacks spammers could operate against their framework, and how they can face them. They tried the implementation of the HoneySpam framework and running honeyd on a few machines to test the functionality and effectiveness of the implemented services.

4.2 Taking Down Websites to Prevent Crime

Website takedown has been utilized to distort attackers' activities for so long where there are still few information/resources on the total effectiveness of website takedown most especially the fact that many websites can easily be replaced with little price. The researchers of this study conducted an extended interview with a range of people who are solely involved in website takedown, which includes commercial/specialist companies, organizations targeted by attackers, UK law enforcement and service providers who answers to takedown demands. Their principal findings are that law enforcement agencies are not really good at website takedown compared to the commercial firms that eradicates bad website at their root.

However, they mentioned that for takedown to be done, policymakers need to seek to regard the point of view of service providers, who must respect the rights of their users. Moreover, takedown is easier for some kind of content than others such as phishing pages, malware, or explicit child sexual abuse images which is usually straight forward to verify complaints compared to the alternative websites that appears to be legitimate which needs more caution in taking care of putting in consideration, the correct respect for due process. The authors therefore concluded that the police must either enforce a specialized unit who is trained, or contract to commercial firm who are expert in it because having to allow untrained officers to handle takedown is not a good practice and not a right use of resources.

4.3 Examining the Impact of Website Take-down on Phishing

Giving that phishing involves the process of luring people into accessing fraudulent websites and making them to enter their credentials, most organizations are still fighting this attack and until they are eradicated, the attacker will not stop getting the peoples credentials. The authors examined real data on phishing website removal times and the number of visitors that the website attract. The data showed that experienced attackers can extend website lifetimes where the rock-phish gang has

revealed ways for adjusting to regular removal where they created a comparable successful solution with fast-flux. The authors concluded that website removal is part of the answer to phishing, which is not quick to easily combat the issue, but it does reduce the damage that is done. They also disclosed relating to removing sites, some bank work faster than others where some web-hosting companies does a great job. However, enhancing the exposure of attacker's plan and the defender's performance is crucial to decreasing the success of phishing scams.

Chapter 5

DISCUSSION

This section explains the advantages of using honeypot for domain take down problems, the disadvantages, highlighting the importance of honeypot, the best practices to follow and the conclusion.

5.1 Advantages

Honeypots are exceptionally easy concepts that provide great benefit and several advantages over other security solutions, including Network Intrusion Detection Systems. They can also function properly in areas where a typical IDS would not. Below advantages shows reasons why honeypot is a good tool to adopt by organizations to help them solve domain take-down problems. What a great way to monitor one's enemy closely:

- Latest tools and procedure: They are formulated to seize anything that interacts with them like up to date virus or worms, including tools or strategies which has not been seen before, also known as "zero-days". All these strategies or techniques that helps to distract and reroute the attacker's attention from the actual network, in a such way that there is no jeopardy of major resources can be used for subsequent research. It can also be used to properly identify malicious domains and help provide better mechanism to harden system against such. [27, 29].
- Limited Resources: This means that information can be limited and be sufficient to run on a strong platform to work at full scale [29, 30] An IDS needs resource-intensive hardware to meet organization's network traffic and

the more the network increases in speed and creates more data, the IDS have to expand to meet up unlike honeypots that requires limited resources and can be sufficient to work on large networks. This rightly provides the necessary resources needed to monitor illegal domains that tends to penetrate the system.

- Detailed Information gathering: Honeypots can gather detailed information, unlike other security incident analysis tools. Honeypot also gathers smaller, useful, datasets since they only log illegitimate activities. With this, honeypot provides the capability of ensuring that the right information is collected which will help in the process of blocking or taking down actual illegitimate domains thereby limiting the takedown of real domains.
- Simplicity/ease of use: Because of their architecture, Honeypots are easy to implement. The more it Is easy to use the more it helps in getting the job done quickly and blocking out domains that are intended for nefarious reasons. Every organization can train their employees or at most employee expert to monitor the honeypot rather than spending additional money to employ organizations that will monitor it [29].
- Honeypots provide lesser false positives giving that legitimate traffic do not use honeypot. Also, the biggest disadvantage of IDS is that numerous alerts that are created are false. These false positives pose big issues for organizations that invest a lot of time in tuning their system. Moreover, honeypots help to avoid this issue due to its capabilities which help organizations effectively identify actual malicious domains rather and lower or eradicate any false positives.
- They also help to lessen false negatives where IDS technologies have issues recognizing unknown attacks or actions, with honeypot, every action is an anomaly, making advanced or preceding undisclosed attacks unique. This can help organizations better hone their security tools and policies based on the trends and the result gotten.

- Encryption: They work in an encrypted environment. A lot of organizations are progressing towards encrypting all their data due to security issue or regulations in place which hinders an IDS's ability to observe the network traffic whereas with a honeypot, the activities can even be recorded when an attacker is making use of encryption [13].
- Cost- Effective: It requires an inexpensive defensive measure that could generate great value of information about your attackers. The lesser the cost, the more organizations including startups can utilize without having to worry about the expense. It will also be very good for these startups because integrating the right security measure at an early stage helps protect against unknown risk. Likewise, investing in security safes a lot of time, money and resources in the long run [55]
- It helps to develop a profile for attackers just to determine to identify their tactics which is related to that of the lawbreaker’s profiles utilized by the law enforcement agencies in order to recognize their strategy and it determines various unprotected and at-risk operating systems, environments and programs [3,5]. This helps organizations to easily identify malicious domains due to the familiarity and pattern of the result gotten from honeypot.

5.2 Limitation

Just like any other technology, Honeypots also have notable flaws intrinsic to their configuration and performance since Honeypots do not substitute the latest technologies, rather it works along with other existing technologies. The limitation includes:

- Restricted View/Insight: Honeypots can only scan and seize events intended to directly interact with them. They do not seize information associated to attacks intended around close systems, except the attacker interacts with the Honeypot at the same time. They can be used by attacker to infiltrate other systems [16],

because they only track and capture activity that directly interacts with them, they cannot detect attacks against other systems in their network. This could be endangering as attackers involved in reusing domains or typo squatting can monitor the network thereby honing their attacks [8,23].

- Potential Risk: Essentially, making use of any security tool involves a possible threat likewise honeypots, because they are subject to threats an attacker can confiscate, manage and utilize it as a means for future attacks.
- It is not straight forward to configure and it would be totally risky to configure without involving a professional. This can cause a huge damage and could expose a network to severe attacks. In other words, installing honeypots with little or no planning and examination may instigate additional risks to an existing network, because honeypots are created to be exploited, and there is always a risk of them being controlled by attackers, using them as an advantage to gain access to different systems within the network [13, 55].
- Technically, honeypot cannot trap internal attackers and it all depends on where it is placed.

5.3 Importance of Honeypots

Honeypot is meant to ensure that the confidentiality, the integrity and accessibility of data is not compromised. The main reason a honeypot is essential in organizations is because of the information it provides. They are equipped with important information, and based on the alerts they record, organizations will become well informed of the kind of techniques adopted by the attacker giving them an advantage to accurately identify the necessary things needed to strengthen their defenses. [55] Domain misuse is one of the biggest threats because people can easily be deceived and manipulated but with the right tools in place, it can help limit the risk and attack cause by this.

When utilized with productive basis, Honeypots equips and organization to be protected through prevention, detection and response to an attack likewise, when utilized with research basis, information is collected relating to the situation in which the Honeypot was executed.

Protection against nefarious individuals: Giving that the idea behind this measure is to distract the attacker and make them waste their time and resources while relating with the Honeypot. This helps in properly identifying attacker's motives and having enough time to respond as well as stop the attack. In other words, using honeypot for domain take down problems can help identify illegal domains based on the level they are used for attack, they can also rank the severity and eliminate where necessary.

Based on the amount of information received from the honeypot, they can be used alongside other security tools to flag when similar incidents arise.

5.4 Best Practices to deploying honeypots – Things to look out for

The principal basis for setting up a honeypot is to deceive the attacker into believing that they are in the actual network. The danger now happens if/when the attacker discovers that they are relating with a honeypot rather than the actual network. This could motivate them to find ways of breaking in the main network. Therefore, it is important to note the listed best practices in order to properly enjoy the use of honeypot. First thing to do is to have a written goal and adhere to the following points.

- Do not use real data – it doesn't matter kind, make sure you create junk data that resembles the real one and use it to lure. You have to be aware that a real attacker is involved and is relating with a fake system. You don't want to create any loophole.

- Do not connect your honeypot to your main network – Make sure that the attacker does not have access to your main network through your configured honeypot. Ensure that it is isolated and secluded.
- Be certain that your network is not too easy to attack or gain access to. This will make the attackers skeptical.
- Adopt the use of virtual machines – the secured hardware you can put on your honeypot is one that is virtual; if you get affected, you simply have to restart and create again.
- Make sure there are not many unnecessary services active or numerous ports open. This would not align to what happens in the real instance where only what is require is open.
- Utilizing Firewalls and Routers - make sure that the only way to access your honeypot is through firewalls and routers. All the incoming traffic should go through them before they get on the network that's being imitate. Also, to point to the honeypot, all port numbers should be configured on the firewall and router.
- The design/layout of the working software solutions are not in their default settings as this never happens in the actual network configuration.
- Ensure that there isn't little-to-no traffic passing through the network or that the servers connected to the network is empty because this will be unattractive for the attackers to view as there is nothing interesting on it.
- The usernames and roles should be distinctive to the honeypot – generate new credentials and use them strictly for the honeypot.
- Always examine the honeypot repeatedly– do not allow a honeypot to be active without putting everything you have at it. You can also, request the assistance of experts to try to crack it and onto your main network before you allow it to active on the Internet. [53].

- Privacy – setting up a honeypot needs to be done with great care. Just a miscalculation of leaving one port open significantly affect your main network and could endanger the personal data of any of your clients [55].
- Honeypots should generally be used as defensive detective tool, not an offensive approach to luring intruders [45].

5.5 Conclusion

Honeypot is a great tool that should be deployed by organizations including startups giving its wide range of capabilities. A honeypot will help in defending attacks by understanding the motives of your attackers and the tactics they might use to set out a breach. Also, placing it in the right position and setting it up well will help strengthen your network's security. Moreover, any mistake can cause a great danger.

However, using honeypot, this study with the detailed review of different research work has highlighted the important things needed to properly configure a honeypot and how to use it to address domain take down problems. This study also showed various honeypot that can be configured and some best practices, highlighting the things that one need to look out for before configuring the honeypot. Based on the various literature review, this study concludes that honeypot is a good tool that can help identify domain take down problems and help organizations take immediate actions to eradicating the issues. It also shows how all the gathered information from the honeypot can be used to enhance and harden their system.

REFERENCES

[1] Anagnostakis, K.G., Sidiroglou, S., Akritidis, P., Xinidis, K., Markatos, E., and Keromytis, A.D. *Detecting Targeted Attacks Using Shadow Honeypots*. USENIX Security 2005.

[2] Andreolini, Mauro, Bulgarelli, Alessandro, Colajanni, Michele, and Mazzoni, Francesca. *HoneySpam: Honeypots fighting spam at the source*. Modena, Italy, SRUTI 2005.

[3] Ashour, A.A. *Designing High Interaction Windows Honeynets*. Kentucky: United States, 2006.

[4] Bailey, M., Cooke, E., Jahanian, F., Nazario, J., and Watson, D. "The Internet Motion Sensor: A Distributed Blackhole Monitoring System." *In Proceedings of the 12th ISOC Symposium on Network and Distributed Systems Security (SNDSS).* pages 167–179, February 2005.

[5] Borges, Esteban. Best Honeypots for Detecting Network Threats. *https://securitytrails.com/blog/top-20-honeypots*, October 15 2019.

[6] Bridy, Annemarie. "Notice and Takedown in the Domain Name System: ICANN's Ambivalent Drift into Online Content Regulation." *Washington and Lee Law Review*, 2017.

[7] Camp, Jean L. "Reliable, Usable Signaling to Defeat Masquerade Attacks." T*he Fifth Workshop on the Economics of Information Security*. WEIS, 2006.

[8] Canner, Ben. The Cybersecurity Honeypot: What You Need to Know *https://solutionsreview.com/security-information-event-management/cybersecurity-honeypot-need-know/,* April 19 2018.

[9] Chiba, Daiki, Akiyama, Ayako, Koide, Takashi, Sawabe, Yuta, Goto, Shigeki, and Akima, Mitsuaki. *DomainScouter: Understanding the Risks of Deceptive IDNs*. Tokyo: Japan, RAID 2019.

[10] Dagon, D., Qin, X., Gu, G., Lee, W., Grizzard, J., Levine, J., and Owen, H. "HoneyStat: Local Worm Detection Using Honepots." *In Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection*. RAID, pages 39–58, October 2004.

[11] Deception Tool Kit, DTK, Fred Cohen & Associates. http://www.all.net/dtk/dtk.html.

[12] Diebold, P., Hess, A., and Schaefer, Guenter. *A Honeypot Architecture for Detecting and Analyzing Unknown Network Attacks*. Berlin: Germany, 2005.

[13] Er. Padda, Sheilly, Er. Gupta, Sonali, Er. Apoorva, Er. Lofty, and Er. Kaur, Amandeep. "Honeypot: A Security Tool in Intrusion Detection." *International Journal of Advanced Engineering, Management and Science (IJAEMS),* Vol-2, Issue-5. Mohali: India, 2016.

[14] Gibbens, Mathias, and Rajendran, Harsha V. *Honeypots*.

[15] HoneyD. http://www.honeyd.org, 2007.

[16] Honeynet Project. "Know Your Enemy: Honeynets." *http://old.honeynet.org/papers/honeynet/An overview of honeypots with a good discussion of their advantages and disadvantages*, March 24, 2008.

[17] Honeynet Project. "Know Your Enemy: GenII Honeynets." *Retrieved 2 September 2007 from* http://www.honeynet.org/papers/gen2/, 2007.

[18] Honeynet Project. "Know your enemy: Honeynets." *Retrieved on 7 October 2007 from* http://www.honeynet.org/papers/honeynet/index.html, 2007.

[19] Hutchings, Alice, Clayton, Richard, and Anderson, Ross. *Taking Down Websites to Prevent Crime*, IEEE 2016.

[20] Imperva. "Honeypot." https://www.imperva.com/learn/application-security/honeypot-honeynet/.

[21] Karthikeyan, R., Dr. Geetha, T., Shyamamol, K.S., and Sivagami, G. "Advanced Honey pot Architecture for Network Threats Quantification." *International Journal of Engineering and Techniques*, 2017.

[22] Khosravifar, Babak, and Bentahar, Jamal. *An Experience Improving Intrusion Detection Systems False Alarm Ratio by Using Honeypot*, IEEE 2008.

[23] Knight, Jason. *Domain Takedowns A Step by Step Analysis for Law Enforcement*. Cambridge: United Kingdom, January 4, 2017.

[24] Kondra, J. R., and Bharti, S. K. *Honeypot-Based Intrusion Detection System: A Performance Analysis*, 2016. 15

[25] Krawtez, N. "Anti-Honeypot Technology", *IEEE Security and Privacy.* Vol 2, Nb 1, pages. 76-78, 2004.

[26] Labrea Tarpit Project, *http://labrea.sourceforge.net/*.

[27] Leita, C., Dacier, M., and Massicotte, F. *Automatic handling of protocol dependencies and reaction to 0-day attacks with ScriptGen based honeypots*. Berlin, Heidelberg: Springer-Verlag, RAID 2006.

[28] Levine, J.G., Grizzard, J.B., and Owen, H.L. "Using Honeynets to Protect Large Enterprise Networks". *IEEE Security & Privacy*, 2(6):73–75, November/December 2004.

[29] Lopez, Miguel H., and Reséndez, Carlos F.L. "Honeypots: Basic Concepts, Classification and Educational Use as Resources in Information Security Education and Courses." *Proceedings of the Informing Science & IT Education Conference*, 2008.

[30] Man, Y. R. Internet security: *Cryptographic principles, algorithms and protocols*. Wiley, 2003.

[31] McAfee. "What is Typosquatting." *https://www.mcafee.com/blogs/consumer/family-safety/what-is-typosquatting*, July 3 2013.

[32] Mohammadzadeh.e.n, Hamid, Honarbakhsh, Roza, and Zakaria, Omar. "A Survey on Dynamic Honeypots." International Journal of Information and Electronics Engineering, Vol. 2, No. 2, March 2012.

[33] Moore, T., and Clayton, R. "Ethical dilemmas in take-down research." *Second Workshop on Ethics in Computer Security Research.* WECSR, 2011.

[34] Moore, T., and Clayton, R. "Ethical dilemmas in take-down research." *Second Workshop on Ethics in Computer Security Research*. WECSR 2011.

[35] Moore, T., and Clayton, R. "Evil searching: Compromise and recompromise of Internet hosts for phishing." *13th International Financial Cryptography and Data Security Conference,* 2009.

[36] Moore, T., and Clayton, R. “Examining the impact of website take-down on phishing.” *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit*, 2007.

[37] Moore, T., and Clayton, R. “Examining the impact of website take-down on phishing.” *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit*, 2007.

[38] Moore, Tyler, and Clayton, Richard. *The Impact of Incentives on Notice and Take-down*. Cambridge: United Kingdom, June 13 2008.

[39] Peter, Eric, and Schiller, Todd. *A Practical Guide to Honeypots*, 2018.

[40] Pouget, F., and Dacier, M. *Honeypot-based Forensics*. Sophia-Antipolis: France, October 2011.

[41] Pouget, F., and Holz, T. “A pointillist approach for comparing honeypots”. *In K. Julisch & C. Kruegel*, 2005.

[42] Pouget, F., Dacier, M., and Debar, H. “Honeypot: a comparative survey.” *Eurecom Report, RR-03-81*, September 2003.

[43] Provos, N. “A Virtual Honeypot Framework.” *In Proceedings of the 13th USENIX Security Symposium*, August 2004.

[44] Provos, Niels, and Thorsten Holz. Virtual Honeypots: From Botnet Tracking to Intrusion Detection. Addison-Wesley Professional. *A comprehensive book about honeypots, including ethical and legal issues. Has a perfect "5 star" rating on Amazon.com at the time of writing*, 2007.

[45] Sharma, Abhishek. “Honeypots in Network Security.” *International Journal of Technical Research and Applications*. Vol. 1. Issue 5. Punjab: India, 2013.

[48] Silva, Danny V., and Rodriguez Rafael, Glen D. “A Review of the Current State of Honeynet Architectures and Tools.” *International Journal of Security and Networks*, 2017.

[49] Spitzner, L. Honeypots: Tracking hackers. Addison-Welsey: Boston, 2002.

[50] Spitzner, Lance. *Honeypots: Tracking Hackers*. Addison-Wesley, 2003.

[51] The Honeynet Project Member. “*Know Your Enemy: GenII Honeynets Easier to deploy, harder to detect, safer to maintain*”, June 2003.

[52] Tiny Honeypot home page. *http://www.alpinista.org/thp/.*

[53] Wahid, Adli. *Honeypots & Honeynets Overview.*

[54] Yegneswaran, V., Barford, P., and Plonka, D. "On the Design and Use of Internet Sinks for Network Abuse Monitoring." *In Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection*. RAID, pages 146–165, October 2004.

[55] Zelleke, Liku. "How to establish a honeypot on your network." https://www.comparitech.com/net-admin/how-*to-establish-a-honeypot-on-your-network/*, September 25 2019.

Appendix A

ACRONYMS

ACPA – Anticybersquatting Consumer Protection Act

AUP – Acceptable Use Policy

DDOS – Distributed Denial of Service

DNS – Domain Name System

ICANN – Internet Corporation of Assigned Names and Numbers

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

NIDS – Network Intrusion Detection System

SIEM – Security Information and Event Management

TLD – Top Level Domain

VM – Virtual Machine

WIPO – World Intellectual Property Organization