Honeypots as Computer Forensics Tool

Marcos Avilés Lugo
Master in Computer Sciences
Dr. Jeffrey Duffany
Electrical and Computer Engineering and Computer Sciences Department
Polytechnic University of Puerto Rico

Abstract *— Cybercrimes were increase in last years. In a near future majority of crime will be cybercrimes. The new technologies like mobile device and networks permit easy access to electronic devices that have Electronic Stored Information (ESI) in them. These ESI could be potential evidence in a court. For that reason Computer Forensics is and will continue been used to resolve cybercrimes. Honeypots while protect real assets and improve Information System security could be an additional Computer Forensics tool to help gather possible evidence faster and resolve cybercrimes like distribution of child pornography, bank fraud, and network intrusion. Also to recollect, document and study hackers and "cybercriminals" techniques used to gain unauthorized access. In a bigger scale Honeypots could be useful to create a profile of cybercriminals or organized cybercrime organization to fight against terrorism. New crimes requires new tools to be resolved, Honeypots could be a helpful tool in this process.*

Keywords *— Computer Forensics, Cybercrime, Cybercriminals, Honeypots.*

INTRODUCTION

Cybercrimes were increased in United States and Puerto Rico. Cybercrime is a fast-growing area of crime [1]. More and more cybercriminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual. Cybercrimes include but are not limited to identity theft, credit card theft, illegal gambling, child pornography, hack and information system, cyber bulling, unauthorized access to a network and bank fraud. Cybercriminals are people that realize cybercrimes. Alberto Gonzalez was sentenced in March 2010 to 20 years in prison for working with a crime ring to steal 40 million credit card numbers from retailer TJMaxx and others, costing over $200 million [2]. In Puerto Rico since 2012 laws to defeat against cybercrimes were created. For example the New Progressive Party Rep. José Aponte introduced legislation to help in the investigation of cybercrimes in the island [3]. Cybercrimes, such as identity theft and theft of data, have surged in Puerto Rico over the past few years as Internet use has soared. The bills include a measure to create the island's first cybercrime laboratory to allow local law enforcement to analyze electronic evidence. Aponte said that during a recent cybercrime symposium, the lack of such a laboratory was cited as a serious hurdle to cybercrime investigations. Cybercrime is a bigger risk now than ever before due to the sheer number of connected people and devices [4]. You often hear the term 'cybercrime' bandied about these days, as it's a bigger risk now than ever before due to the sheer number of connected people and devices. To resolve these cybercrimes is necessary a science that provide all necessary tools and techniques to gather enough information of electronic devices, networks and/or storage devices related to a crime that could be potential evidence in a case or court trial. This science exits and is called Digital Forensics now Computer Forensics. Computer Forensics needs new tools and techniques to gather potential evidence faster in order to resolve more cybercrimes. The additional tool I suggest is a Honeypot. This is exactly the purpose of my project research and this need to resolve cybercrimes that are increasing is the justification to do this master project article: the use of Honeypot as an additional Computer Forensics tool.

COMPUTER FORENSICS

How Computer Forensics could be defined? For example Ken Zatyko in 2007 answer this question

for Forensics Magazine and said: [5] "the application of computer science and investigative procedures for a legal purpose involving the analysis of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible expert presentation". Forensics is an applied science to solve a legal problem. The forensics science and laws are together and much related. Computer Forensics is this science applied to electronic information and includes the search, discovery, review, validation, analysis, recovery and presentation of any Electronic Stored Information that could be used as evidence in a court case even when it was admissible or not. Because new technology and digital era arrives new technologies to recover and extract digital information stored in new devices are necessary. So Computer Forensics arrive too in order to facilitate the search, techniques and ways to recover information even when hidden or deleted in any devices that serve as storage. Devices include digital cameras, smart phone, SD-cards, pen drives, internal hard drive, external hard drives, server, networks (logs), cloud services, L-tapes and becoming storage devices. Recoverable data with Computer Forensics software includes electronic documents, pictures, videos, music, text messages, voice messages, e-mails, social media content and any ESI.

To see how useful Computer Forensics is in the resolution of cybercrimes is good to read the preface of this book: *"The Basic of Digital Forensic"*. The author John Sammons said that Digital Forensics helps to combat the massive increase of cybercrimes because child pornographers, and "old school" criminals are now using the technology to facilitate their illegal activities. Computer Forensics is not limited to search (e-discovery) and found something, carefully analyses, check for authenticity and comparisons is extremely necessary in order to use as evidence in a court and proof that the content was not modified. This science is actually used in criminal investigations, civil litigations, intelligence and administrative matters. Forensic examiners are the guys that use this science to resolve cybercrimes. To continue resolving cybercrimes Computer Forensics examiners need new tools like Honeypots to gather Electronic Stored Information that could serve as evidence.

Computer Forensics software are daily tools used by forensics examiners. The role of the forensics examiner is critical in a case or litigation. The forensics examiner is the person responsible to make part of the digital forensics process. Not necessarily includes the seizure of the electronic device. But following the chain of custody the forensic examiner continue it been responsible of making the e-discovery after the seizure device and so far. Using forensics tools an examiner is able to see, search, found and retrieve information like e-mail addresses, names, phone numbers, keywords, web addresses, web browsing history, network logs of incoming and outgoing traffic, file types, date ranges, system logs, picture information and so far. These tools are helpful when realizing forensics jobs but could have limitations so a combination of various tools could be necessary to found all desire electronic information or looking file. There are software to recover information or ESI that could be potential evidence but this evidence could be seen after crime happens. There are real needs to obtain potential evidence in real time. For example there is a need to obtain the IP address of the device used for the cybercriminal while cybercrime happens or almost as fast as possible. Here Honeypots could be one additional tool to obtain evidence in real time while crime happens. Also this potential evidence is stored is this "fake" system so Computer Forensics analyst and other law enforcement employees could study and analyze this information in the future because is stored in the Honeypot.

HONEYPOTS

A Honeypot is a computer system on the Internet that is expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems [6]. My simple definition of a Honeypot is a simulated system in a controlled environment that looks like a real one asset with

enough vulnerabilities to take the attention of an attacker or cybercriminal but with enough controls to avoid putting in risk real assets in the network. The setup of the Honeypot could not be too much vulnerable because then it be too suspicious for the cybercriminal and it could go out without leaving enough traces to try to discover the identity of the attacker or create a profile of him. The Honeypot help to improve the security of an Information System and the use of an Intrusion Prevention System because in a control environment it should be easier to study the way an attacker or cybercriminal gain unauthorized access and the techniques used to break security and firewall. For example on December of 2014 Next Gov website said that: USPS to improve security use "Honeypot technique". "The White House, State Department and U.S. Postal Service each deliberately delayed fully squelching malicious activity after suffering a data breach [7]. USPS has acknowledged using the Honeypot technique, after detecting an intrusion in September 2014". Jasper Graham, a 15-year National Security Agency veteran said about Honeypot: "Let the adversaries break out all their sophisticated malware and poke around in government files for a few weeks, then document every technique they use [7]". In the Honeypot, Forensic Analysts could use traces leaved by a cybercriminal or cybercrime organization to make a profile that include the behavior, basic acts and techniques used to commit an organized cybercrime. Thinking in that way I said that forensics analyst could see a Honeypot like "Honeydrive3"as a Cybercrime Prevention System. See figure 1.

A Honeynet is a vulnerable and simulated computer network using a decoy server designed to test network security [8]. Honeynets are developed in order to help computer security experts to improve security for networks and systems. A Honeynet is various Honeypot connected in a network. In other words is a network of fake interconnected systems in a controlled environment to take attention of an attacker or cybercriminal. Also could be a group of additional workstation in the LAN where suspicious traffic in the network is rejected to. This suspicious network traffic or the activity executed by an attacker/cybercriminal in this interconnected Honeypot will be stored and log created to study and analyze it.

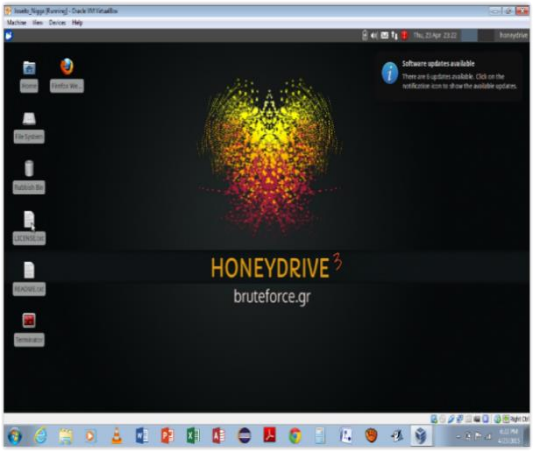

Figure 1
Honeypot Honeydrive3 Default Desktop

An IPS generally sits in-line and watches network traffic as the packets flow through it [9]. It acts similarly to an Intrusion Detection System (IDS) by trying to match data in the packets against a signature database or detect anomalies against what is pre-defined as "normal" traffic. In addition to its IDS functionality, an IPS can do more than log and alert. It can be programmed to react to what it detects. An Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) are used to prevent and detect attacks to networks from inside or outside of an organization' network. They work almost every time with the firewall and could be hardware of software based. It's possible to use an IPS to detect a threat or suspicious traffic in a network and reject this traffic to a fake environment that is the Honeypot. Using the logs stored in the Honeypot and thanks to the Intrusion Prevention is possible to prevent future intrusion to a network or a system by studying the activity executed by the cybercriminal in the Honeypot. Activity includes login attempts, command executed in the Honeypot, areas of interest into the Honeypot and other attacks deploy against the Honeypot. Here we see how this system combination acts and improve security while it permits Forensics Analysts to gather evidence,

study anti-forensics techniques and tools used by attackers and cybercriminals to do cybercrimes. In this way Honeypots function as a kind of Cybercrime Prevention System. A Honeypot alone is not the best defense but when it's combining with a firewall and IPS I'm sure that supports and increases the security of the whole system, secure the information and devices and permits to realize investigation in the Honeypot logs, gather potential evidence, know more about a cybercriminal and prevent future cybercrimes.

Possible information that could be obtained of a Honeypot or Honeynet using it as forensic tool includes the IP address, MAC address, username or nickname used in login attempts, Internet Service Provider, date/time, location of device or mobile if a relocation service is available, possible location of cybercriminal, a log of activities executed by cybercriminal inside the Honeypot and where it is or where it was while the cybercrime happens. In other words a Honeypot help Forensic Specialist and/or detective to track or gather traces of a cybercriminal. But how, where and when the evidence were collected is very important. Without evidence there are no case and no possible guilty. During a court case as much evidence is found and show to the jury more probability to proof that someone is a criminal and guilty. If Forensics Examiner and seizure personnel does not collect the evidence correctly attorneys could fail in the court to proof guilty of someone because the accused' defense will talk to the jury about the incorrect steps during the collection of evidence. Collecting the evidence is very crucial in Computer Forensics. For that reason: all the procedures during the seizure process and the collection of evidence need to be documented well. It includes the documentation related to the Honeypot, the implementation, stored logs with the activity of the cybercriminal and how this possible evidence is related to the cybercriminal. Any notes, papers and reports could be evaluated by the defense or by other people during the case.

The success implementation of the Honeypot as a Computer Forensics tool and how much evidence could be acquire from it depends on its set up and configuration. After the implementation and cybercriminal get access to the Honeypot the activity log is created registering all command and activities executed in it. At this point the Computer Forensics analyst in collaboration with the detective could create a profile of the attacker, possibly a pedophile, gather his possible location, device' IP address, mac address, ISP, analyze a picture or send attachment to obtain more information about him. For example, from a picture send by the criminal, which is, now stored in the Honeypot, Computer Forensics analyst could using other Forensic software can know what kind of smart phone was used to take the picture, the OS of the device, when the picture was taken and where the picture was taken if the GPS of the smart phone was enable. In the case not exits a clear profile of whom is been wanted, Honeypot help to create one. Here we see how much information could be stored in a Honeypot that Computer Forensics analyst could use. From an email now store in the Honeypot, forensic analyst could start gathering evidence like possible email send location, time zone, date and more. All stored in the Honeypot could be analyzed as fast as law resources permit and tool for analyses were available.

Honeypot are not intended to be a magic solution to resolve cybercrime, I said they could be used as real time Computer Forensics tool that could help resolve cybercrimes faster. There are some obstacles while trying to obtain and analyze information stored in the Honeypot. For example the anonymity browsing, hidden profiles. The forensics examiners need to know how to detect it because a lot of cybercriminals will use browsing anonymity. Maybe international efforts could be necessary to catch a cybercriminal that use servers located in foreign countries.

A basic Honeypot could include a device with a hard drive, memory ram, connected to a Local Area Network or Wide Area Network and an OS with an interface set up to store logs of activity like login attempts or get into tries. See Figure 2.

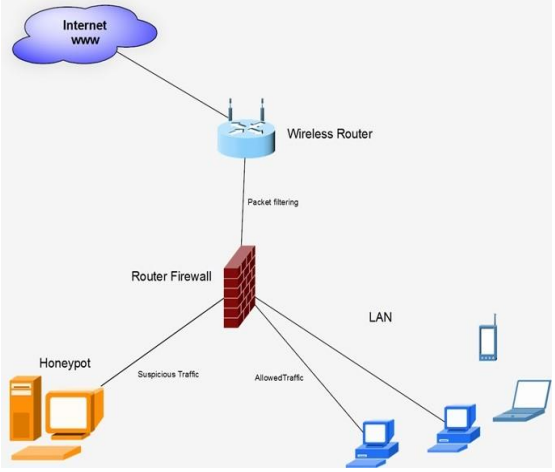

Figure 2
Honeypot Basic Network Configuration

It could be a virtual machine with an OS configured to look like a real system not necessarily equals to the victims system but with the weakness that attacker and cybercriminals looks for. There are a lot of possible Honeypot implementations that could be modified to take attention of a cybercriminal. Computer Forensics Analysts, detectives and law enforcement personnel should know in deep about the cybercrime and if possible about the cybercriminal in order to prepare the environment with the correct set up with enough weakness to keep the attention of the cybercriminal but with good methods to control the environment in order to avoid the cybercrime affect more victims or that the cybercriminal discover that is a fake system. The configuration and set up will vary depending on case needs, cybercrime type, laws resources, applicable country privacy laws, and subpoenas. I think there is not a universal Honeypot for all cybercrimes. I'm sure that the setup of a specific cybercrime should be explained to a judge also the basic functionally in order that they understand how the information that is presented as evidence was capture and stored in the Honeypot.

Legal Aspects

What about the 4th amended of the US constitution and Honeypot implementation? [10] The Fourth Amendment originally enforced the notion that "each man's home is his castle", secure from unreasonable searches and seizures of property by the government. It protects against arbitrary arrests, and is the basis of the law regarding search warrants, stop-and-frisk, safety inspections, wiretaps, and other forms of surveillance, as well as being central to many other criminal law topics and to privacy law. The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. The definition published by Law Cornell web page about 4th amended of the US constitution said that this amended could affect directly the implementation and use of Honeypot and/or Honeynets in criminal and civil cases. In cybercriminal cases there should be reasonable cause in other to use a Honeypot implementation to store information of a possible cybercriminal and start gathering potential evidence. To begin the use of in addition of reasonable cause a subpoena could be necessary.

What about the Patriot Act after 9/11 and Honeypot implementation justification? [11] The Patriot Act is a U.S. law passed in the wake of the September 11, 2001 terrorist attacks. Its goals are to strengthen domestic security and broaden the powers of law-enforcement agencies with regards to identifying and stopping terrorists. The passing and renewal of the Patriot Act has been extremely controversial. Supporters claim that it's been instrumental in a number of investigations and arrests of terrorists, while critics counter the act gives the government too much power, threatens civil liberties and undermines the very democracy it seeks to protect. The Patriot Act's full title is Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. The definition said by Ed Grabianowski about the Patriot Act on How Stuff Works web page could affect Honeypots in a good way. The implementation of Honeypot to be used to obtain evidence of cybercrimes related to terrorism or national security could be backup because national security thread exits or an attacker

even foreign or local is an existing flag. In other words if government is been threat by terrorism or someone that affect the national security they could use Honeypot-Honeynet without a search warrant or subpoena thanks to Patriot Act of 2001.

The Federal Rules of Civil Procedure (FRCP) that governs the conduct of all civil actions brought in Federal District Courts also have an impact in the way the information obtained in the Honeypot could be used. While they do not apply to suits in state courts, the rules of civil procedure for many states have been closely modeled on these rules of civil procedure [12]. The FRCP are promulgated by the United States Supreme Court pursuant to the Rules Enabling Act, and then approved by the United States Congress. The Court's modifications to the rules are usually based on recommendations from the Judicial Conference of the United States, the federal judiciary's internal policy-making body. Although federal courts are required to apply the substantive law of the states as rules of decision in cases where state law is in question, the federal courts almost always use the FRCP as their rules of procedure. Some legal aspects included in the FRCP like Rule 24 and Rule 45 that affect Honeypots are: subpoenas, search warrant, evidence acquisition methods, preservation and documentations that will convert evidence acquire in the Honeypot as admissible or not in a court trail.

How useful could be a Honeypot? Useful depends on how you see them. Honeypots always improve security of a System but are useful for other things. Its use and implementation will show how useful could be them. It is possible to acquire evidence not before but it's possible while a crime is happening? Yes, this is the main idea behind the implementation of a Honeypot. Be a kind of a real time evidence acquisition tool. That's the way Honeypot contributes to Computer Forensics area and contributing to law enforcements personnel to help resolve investigation faster. Helping to resolve cybercrime and avoid other possible victims is a contribution to society and people of Puerto Rico. It's important to clarify that real time evidence acquisition tool is a relative term. This because what is evidence and what isn't depends in law and the court not in Computer Forensics analyst or tools. In other words I said Honeypots could act like a real time Computer Forensics tool not like a magic tool that all obtain and stored in the Honeypot will be accepted like admissible evidence in a court trial. There are a lot of variables and possibilities in the way of a criminal case and during a court trail that could affect the "evidence" acquired thanks to the Honeypot.

Configuration and Implementation of Kippo Honeypot

After download the Honeydrive3 OVA file from www.bruteforce.gr, I import the OVA file to Virtual Box. I don't change the default configuration I just import it and start the basic installation of a virtual machine. The import process and installation take like 25 minutes. After installation was done I connect the virtual machine to the Internet by Ethernet cable and using a DHCP IP address of my TP-link router and download all available updates. The updates installation process takes about 50 minutes to 1 hour. There were a lot of updates, including the installation of the python service which is necessary to use the SSH service of Kippo Honeypot. So it's extremely necessary to download all available updates before configure the Honeypot. It's highly important to understand that Honeydrive3 is bistro of various Honeypot for different purposes not a single tool and that the OVA file is just pre-configured not configured. You need to understand the Honeypot you want and configure to satisfy your requirements.

- For purposes of a control environment Honeypot, I connect my laptop to my router TP-link and other laptop computer with Kali Linux Virtual Machine cabled both. The router have an exception to allow traffic through port 22 (TCP) for Virtual Box. The IP at this moment is DHCP and have Internet connection.
- After install updates of the Virtual Machine I configure the network connection of the Virtual Machine as a LAN (Internal Network- cable connected) for purposes of my Honeypot

(kippo). Kali Linux have the same configuration, so both were in the same LAN.

- After configure Virtual Machine network connection I download and install the firewall. So open the terminal console, login as root typing sudo write password which is Honeydrive and write in the console the command: apt –get install gufw.
- Then add the exception of allow traffic through port 22 in the virtual machine that is the default port for SSH traffic, using the command: iptables –A INPUT –p tcp –dport 22 –j ACCEPT. Then type: iptables –L to verify that the exception was added to the firewall (for this reason we look to iptables) or use the alternate command: nmap localhost –p22 and you should see this in the terminal console that the port is open: PORT STATE SERVICE 22/tcp open ssh.
- Type in the terminal console to see that the service SSH that uses python is running, type: -netstat -ip –inet and you will all services running and its port. See figure 3.

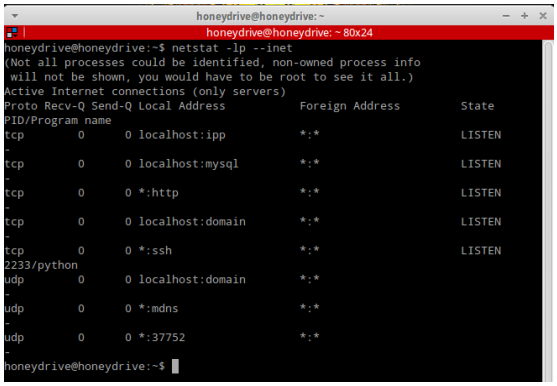

Figure 3
SSH and Mysql Running

- This is not the same as see the port open, this to assure that the service SSH is running in order to start the Honeypot kippo and start catching info by the traffic through this port.
- After that I disable the DHCP service of my router and configure (edit) the network connection of the Honeydrive, and assign a static IP address. I do the same to kali virtual machine. I do this assuring that both machines were in the same location address: 192.168.0.2 and 192.168.0.3 and a subnet mask in the same location.
- I assure that the kippo configuration file (kippo.cfg) have as default the port 22 for SSH connections in order to catch all un authorized login attempts through this port. This file could be edited and save it by terminal console or manual looking its folder path. Then I log out as an administrator (root log out). See figure 4.

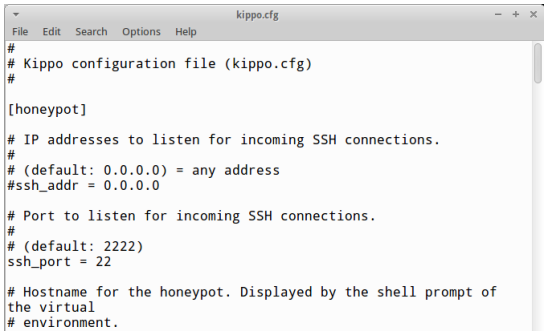

Figure 4
Kippo Configuration File

- Then as normal user I start the kippo Honeypot using the command: sh ./start.sh. See figure 5.

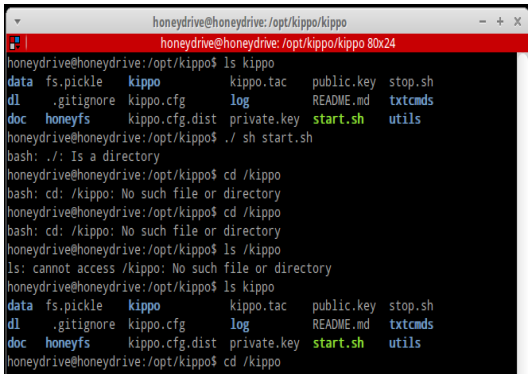

Figure 5
Starting Kippo Honeypot

- After that you will see that kippo and its sql database were started. After that the Honeypot start catching login attempts and attacks that were received through port 22. At this point kippo is emulating a SSH (Secure Shell – a network protocol that enables encrypted communication between two computers).
- I open the terminal console on Kali Linux and type the command: nmap –A 192.168.0.2 to see

if my Honeypot (Kippo virtual machine) is in the same LAN and have connectivity (also you could do ping to the desired IP address. Then I write the command: ssh -l root 192.168.0.2. The failed login attempts were registered in the Honeypot including hour, date and IP address.

- I open the Firefox web browser while my Honeypot is running I type: (IP address of Honeypot) 192.168.0.2/kippo-graph/kippo-ip.php and see the graphics of log-in attempts and/or attacks and received in the Honeypot. This means the Honeypot successfully detects attacks, unauthorized log-in attempts and traffic through firewall and port 22.

Firewall/IPS Monitoring and Intrusion Basic Protocol with Honeypot

Traffic from Internet and Internet Service Provider pass throw firewall software or Next Generation Firewall hardware based and is filtered by IPS rule that allow and send traffic throw port 80 and 8080 from known and allowed connections to the wireless router. Then wireless router send it to the WLAN devices. If traffic is suspicious or not allowed like login attempts to SSH throw port 22 or 2222 is automatic rejected to the Honeypot. Honeypot always have port 22 open to receive any SSH login attempts. In figure 6 a Bruteforce SSH login attack from cybercriminal device to gain unauthorized access to Kippo Honeypot.

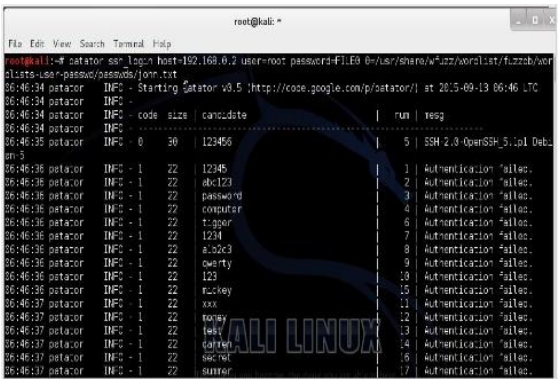

Figure 6
Cybercriminal Running a Bruteforce SSH Login Attack against the Honeypot

In figure 7 you see Honeypot detecting the IP address of cybercriminal device.

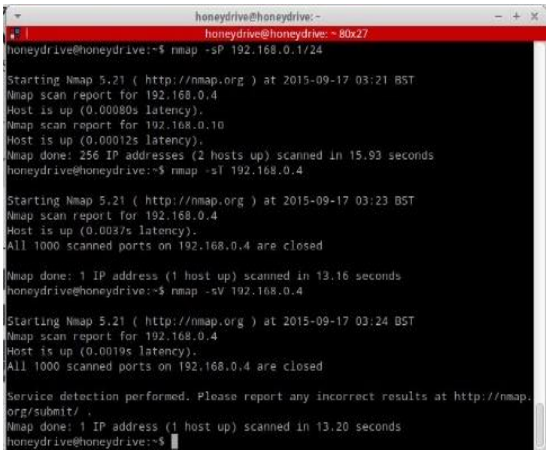

Figure 7
Honeypot Detect Cybercriminal IP Address

If attacker get access to the Honeypot then all activity and commands executed in the Honeypot and all information about the device that gain access to it is stored in Kippo Honeypot. In figure 8 failed login attempts executed in cybercriminal device. In figure 9 an activity log created by Kippo Honeypot after cybercriminal success login.

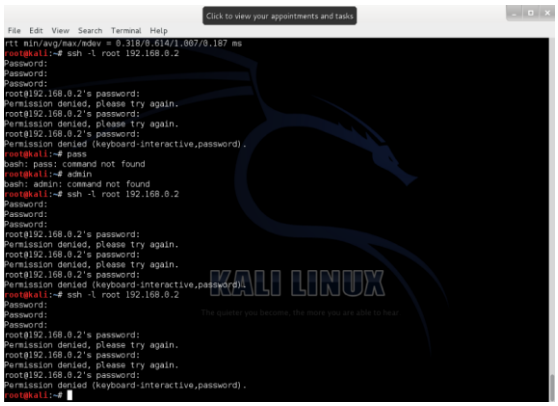

Figure 8
Cybercriminal Failed Login Attempts

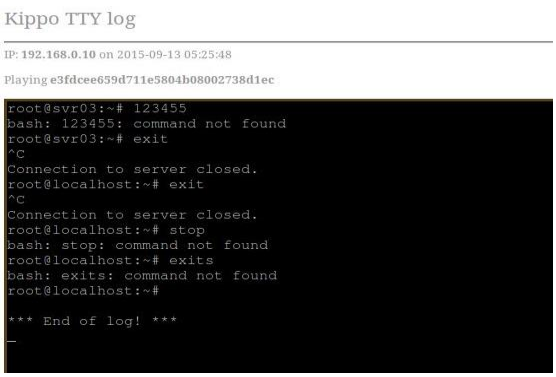

Figure 9
Kippo Honeypot log

Future Work Related to Honeypots

The implementation of future Honeypots will depend on special needs, objectives and the cybercrime. It's necessary to understand its components and functionality in order to make a correct implementation that permits gathering all possible information of the cybercriminal without fake system is discovered. Special knowledge is necessary for Computer Forensics Analysts, detective and law enforcement personnel in order to take advance of Honeypots. All necessary updates always will be recommended to improve the functionality of the Honeypot. Other apps or tools could be installed or implemented together with Honeypot in order to complete a security system. Maybe in the future some actual laws will be modified in order to implement Honeypots and other Computer Forensics tools. I expect in near future local law enforcement agencies add Honeypots as a Computer Forensics tool. This because in future majority of crimes will be cybercrimes.

CONCLUSION

The technology and Internet arrived to change human's life. Electronic devices like smartphone, tablets usually use Internet daily to connect to the World Wide Web and do many things unfortunately also used to commit cybercrimes. In other words, technology and Internet is changing people life, education, commerce, communication and almost everything that is actually been realized. More often crimes involve technology, smart devices and networks. People including criminals have easy access to technology. For that reason there are no doubt that cybercrimes will increase with the time. Are necessary more tools to resolve and reduce cybercrimes. Thanks to Computer Forensics it's possible to look for traces about Internet negative uses like bank fraud, identity theft or child pornography download. When people use the Internet they use an Internet Service Provider, the device have a MAC address, and IP address, there are a date and time of access, Web Browser History, e-mail service provide like Gmail or Hotmail and other services where they will leave traces. So negative use of the Internet not always could be hidden and Forensic Examiner could look and found these traces of cybercriminals.

Honeypot could be used as an additional Computer Forensics tool for various purposes. My proposition is to use them to acquire potential evidence while cybercrime happens and store this data in it to analyze this potential evidence while or after the crime happens in order to catch the cybercriminal and avoid more victims suffer the consequences. So Honeypots could be considered as a kind of Cybercrime Prevention System. In the other side while Honeypot is an additional Computer Forensics tool they serve to complement the security of a system and protect the real assets and information stored in it when it is used in combination with and IDS and IPS. Honeypots are not a magic formula to resolve all cybercrimes in the future but I'm really sure that could be a reliable additional Computer Forensics tool to help in the acquisition of evidence process and success of a cybercrime case. Honeypots are not necessary expensive, does not necessarily required physical devices restrictions because it could be a virtual machine and not necessarily is difficult to implement. But the success could depend on the implementation in order to take the attention of the cybercriminal but maintain the controlled environment while potential evidence is been acquired.

There are many challenges in Computer Forensics field. The born of new technology used in mobile device create the need of new and more effective tools to recover potential evidence from them. The speed of change is a big vulnerability that affect various disciplines and fields especially technology related fields. Sometime available technologies grow up or are upgraded faster than the time necessary to acquire enough knowledge to understand and manage them. The watch continues running too fast and new technology arrives too soon. Computer Forensics personnel and law enforcement people need to deal with that in order to improve efficiency of the field and the use of this

discipline as a tool to resolve any crime that involves the use of technology.

When years pass more criminals will use an electronic device even before, during or after a crime was realized. For that reason more importance should be taken on Computer Forensics in order to resolve crimes, proof innocence or guilty of a person. Computer Forensics need to incorporate to the field new tools to acquire potential evidence faster and resolver cybercrimes faster. Honeypots should be considered one of these new forensics tools. Actually, Computer Forensics is used in civil litigation especially during dollar litigation. In the future Computer Forensics should be necessary to resolve cybercrimes. Always a crime involves data storage on electronic devices; they need professionals with advanced skills on Computer Forensics and new tools to acquire the potential evidence they need to found traces that help resolve it. That's the future crimes, cybercrimes and the future evidence in court, electronic evidence and future tools for law enforcement agencies: Computer Forensics and its tools.

REFERENCES

[1] Interpol. (2015). *Cybercrime* [Online]. Available: http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime. [Accessed: 18-Aug-2015].

[2] C. Pfleeger and S. Lawrence, "Security Blanket or Security Theater?" in *Analyzing Computer Security*, M. Lou, 1st ed. Upper Saddle River, New Jersey: Pearson Education, 2012, pp. 22.

[3] Cbprdigital. (2012, April). Bills aim to plug cybercrime in PR. *Caribbean Business* [Online]. Available: http://www.caribbeanbusinesspr.com/news03.php?nt_id=70306&ct_id=1. [Accessed: 19-Aug-2015].

[4] Symantec. (2015). *Cybercrime* [Online]. Available: http://us.norton.com/cybercrime-definition. [Accessed: 10-May-2015].

[5] J. Sammons, "Preface", in *The Basic of Digital Forensics*, J. Rajewski, 1st ed. Waltman, MA: Elsevier, 2012, pp. xv.

[6] M. Rouse. (2007, May 7). *Honeypot Definition* [Online]. Available: http://searchsecurity.techtarget.com/definition/honey-pot. [Accessed: 10-May-2015].

[7] A. Sternstein. (2014, December). Should agencies ever let hackers rummage through Government networks? *NextGov* [Online]. Available: http://www.nextgov.com/cybersecurity/2014/12/when-should-agencies-let-hackers-rummage-through-government-networks/101322/. [Accessed: 26-May-2015].

[8] Techopedia. (2015). *Honeynet* [Online]. Available: https://www.techopedia.com/definition/16103/honeynet. [Accessed: 19-May-2015].

[9] J. McMillan. (2009, November). *Intrusion Detection FAQ: What is the difference between an IPS and a Web Application Firewall?* [Online]. Available: https://www.sans.org/security-resources/idfaq/ips-web-app-firewall.php. [Accessed: 29-Aug-2015].

[10] Cornell University Law School. (2015). *Fourth Amendment* [Online]. Available: https://www.law.cornell.edu/constitution/fourth_amendment. [Accessed: 29-May-2015].

[11] E. Grabianowski. (2007, July 6). *How the Patriot Act Works* [Online]. Available: http://people.howstuffworks.com/patriot-act.htm. [Accessed: 29-May-2015].

[12] FRCP.info. (2007). *Federal Rules for Court Procedures* [Online]. Available: http://www.federalrulesofcivilprocedure.info/frcp/. [Accessed: 20-Aug-2015].