Portable HoneyPot & HoneyNet: Within a Closed Network

Héctor D. Concepción Rivera
Master in Computer Science
Dr. Jeffrey Duffany
Electrical & Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

Abstract *— At any given time a business network could be or has been compromised by a hacker or its information been exposed or breach. This is why building a honeypot and understanding how to use it can help network security expert, avoid being hack in the first or try to mitigate those attacks and breach. It also shows that this tools can be used for research purpose in a local home network for test and research. This paper will explain what honeypots and honeynets are, and the help of building one in a Microsoft environment using low cost tools and hardware and being portable.*

Key Terms *— Hackers, Honeynets, Honeypots, Packets.*

INTRODUCTION

From looking to protect physical documents by creating physical filing system and locking them with key-code or any other physical measure, too little by little evolving to now days migrating and using all these files on a digital era. The rules for protecting and limiting access have change drastically over the course of the years. The ability to safeguard information has become of the highest importance and even an art form. Saying all this, as a computer security expert you have to be prepared to protect not only files and data but to keep the virtual network where the data would be share, stored and used safe. They are many measure and technique to make this happen, one of these techniques which this project focus in on the building and understanding of honeypots and honeynets. With the use of a honeypot or honeynet we can lure attackers to a fake environment and watch all theirs moves. This tool help any security expert to check new or old vulnerability in their systems, and even new trends of attacks.

This project attempts to explain what are honeypots and honeynet, and in which cases they should be used and their purpose. It will include on how to build a simple honeypot using now day tools in a Microsoft environment. It will show that it does not require much work and money to build one. Also some test conduct it inside closed network with the honeypot.

HONEYPOT & HONEYNETS

Let's not confused the term Honeypot with a real honeypot. The words come from a figure of speech which a honeypots contains bees and it also can be used to lure bees. In the technology space we called this machines or software honeypots, cause we will be luring attackers. So what is the meaning and use of a honeypot? Spitzner gives a brief definitions of what are honeypots. "Honeypots do not solve a specific problem. Instead, they are a highly flexible tool that has many applications to security" [1]. Honeypots are decoys or traps, set to deflect or capture attacks from unauthorized access mostly to a system or network. Some expert described honeypots as "highly flexible security tool with different applications for security". They can be used for many purpose such as to distract adversaries from more vulnerable machines or systems on a network. Could help proved early warning about new trends of attacks and exploitations trends. Also it gives a nice playground for a Forensic Analysis to investigate and gather the information it would need for future research references. A honeypot is a security resource in which values lies in the ability in which lies being probed, attack or compromised. There are two different kinds of honeypots. There are virtual honeypots and physical honeypots the author Niels Provos explains. "A physical honeypot is a real machine with its own IP address. A virtual honeypot is a simulated machine with modeled behaviors, one which is the ability to respond to

network traffic" [2]. They can be classified depending on the way they would be deploy.

- **Production Honeypot:** They are used by companies and corporations for the purpose of researching the motives of hackers as well as diverting and mitigating the risk of attacks on the overall network. This are put inside production networks with other productions servers by an organization to improve their state of security.
- **Research Honeypots:** This are used by nonprofit organizations and educational institution for the sole purpose of researching the motives and tactics of the hacker community to targeting different networks.
- **Pure Honeypot**: They are the one used by companies and corporations for the purpose of researching the motives of hackers as well as diverting and mitigating the risk of attacks on the overall network.
- **High-interaction Honeypot:** This are honeypots with high time consuming to design, manage and maintain. Multiple honeypots could be hosted virtually with many service and features for the hackers to used or physical machine for each one of them.
- **Low-interaction Honeypot**: This are easily installed on a system and configured. Mostly just running simple services not multiple ones.

Honeypots are in increasingly used in companies to provide a heads up and early warning of potential intrudes, hackers. To identify flaws in security strategies and improve the organization's overall security awareness. One important aspect of a honeypot is that it should not be used by no one. It should not see any activity or anyone interacting with the honeypot. Anything or anyone who interacts or alter a honeypot will be consider an anomaly. This means that the honeypot has capture it first bee (hacker).

MULTIPLE HONEYPOTS

Honeynets are advance and real complex. They are actually a collection of honeypots inside the same networks or system. Their main purpose is to capture extensive information on threats. The author Spitzner explains a honey like a fishbowl "honeynets is a specialized architecture that creates a fishbowl, you can place any targets of system you want within this fishbowl" [1].

WHO ARE THE BEES (HACKERS/INTRUDERS)

The main purpose of the honeypot it to be able to capture data. This data will be provided by intruders who try to enter this pot. We can call these intruder what everyone else calls them hackers. Hackers or intruders are people who might or not have a high skill on computer subject and matter. They will mostly use their skills to try penetrate or extract information from unauthorized systems. We can categorized hacker into some major groups.

- **White Hat:** Someone who tries to break into a security system and whatnot. But he has no malicious intent when he does this. Most of the time they do this for challenges or to satisfy them self. In many cases white hats can be call ethical hacker or security experts. Which they use their knowledge to penetrate security systems, to make them safer and inform the company of the vulnerability of such systems. A lot of company now day have these type of hacker in their IT Departments to keep track of vulnerability in their company.
- **Black Hat:** Someone who breaks into a system with malicious intent. Either been paid or just for the fun. Once he breaks the security he does malevolent acts, such as erasing data, stealing data, doing piracy acts. From here we get a lot of identity theft crime and credit card frauds. He also might spread worms and virus. They also may block access to websites and cause vandalism. If the vandalism or the website blocked, are related to political views or socials views will be label as a hacktivist. Try not to confuse the hacktivist with the black hat. The black hat does the hacking on doing damage no

matter the cause and the hacktivist has a social cause or political intent.

- **Grey Hat:** Someone who has a mix of traits from the black hat and white hat. Mostly a little moral ambiguous, these guys do penetrate security systems. Like a black hat they go where ever they want but with no malicious intent. They might spread the rumors of the exploit of the system to other hackers which he does not know with what intention they will use it. IN some time they call the attention of the owner so they know of the weakness in their systems. Sometime even ask to be paid to fix them. As different from the white hats that are mostly ethical hacker and security expert, grey hat don't ask for permission they just go.
- **Hacktivist:** Someone who uses the tools and techniques of hacking, but he focus only to disrupt services to bring the attention to a political or social cause. It's like vandalism but with a cause either social or political. These type of hacker can be very common when elections in certain country are about to start or social issue are occurring.
- **Scrip Kiddie:** These, on most term are not consider "real hackers". Most of the time they even lack the knowledge of programming or security skills. It's a non-expert hacker who breaks into computers systems without the knowledge in security and programming. They use prepackage automated scripts, tools and software. Which all of them are written by other people who know what they are doing. Most of the time they won't even know how the script or tool work. You could see this trend a lot in young people. They will mostly brag about how they are real hackers, this is a big sign telling you he is not really a one. Most real hacker don't even tell nobody about it

LEGAL ISSUES

Deploying a honeypot or honeynet without knowing the legal terms could get any one into legal problems. The author Spritzer describe three major issues that might be commonly discussed on the subject of honeypots. Since honeypots been around from the early 2000's it can be considered still a new emerging technology. These three issues Spitzner described are Entrapment, Privacy and Liability.

- **Entrapment:** Many people believe that if they deploy a honeypot, that they can be prosecuted for entrapping an attacker. This premise is completely false.
- **Privacy:** One of the most complex issues related to honeypots. The biggest problem is that there is no one statute covering privacy. Since the internet is a global, you can have the honeypot in one state, and the attacker coming from another state or country. The one law that might have the biggest effect on this issue is the Federal Wiretap Act.
- **Liability:** This one means that one can be sued if their honeypot is used to bring harm toward others. It's mostly consider more of a civil issue and not a criminal one. "The more flexibility you allow an attacker, the more risk you bring to your honeypot which means greater chance of liability problem."[3].

BUILDING AND CONFIGURING

Building a honeypot is not a very difficult task at all, but depending on the scale and type of honeypot it could be time consuming and in some cases could impact the budget of the company. These are one of the first thing to observer when building a honeypot. Check the necessity of the company and what would they like to accomplish once this honeypot is build and put into used. Setting up and operating a honeypot involves legal considerations as well as some expertise with networking tools and computer forensic analysis. Now days we have many ways on setting up a honeypot. Could be a real server hardware or it could be made with virtual machines to just used specific services which would be mimic in a fake environment. For this project we will use real

hardware for building, configuring and testing a honeypot and a honeynet.

For building a honeypot does not require really expensive hardware with a simple CPU and some ram it should be more than enough to emulate or run your pot. For purpose of this project it will be utilizing:

A laptop, which I could tell you it not recommended but since I did not have a steady laboratory this was the best option for the moment. It had a I7 processor with 8 cores, 6 GB RAM, 500 GB hard drive, 15 inch screen and a 10/100/1000 network card. That last component it's very important since you want connect the machine to a network. The advantage of being a laptop is that could be portable and connected to any networks or system, but it might lack the processing power.

First comes the installation of Windows 2012 Server on the computer, this process was fairly easy and straightforward. This server was going to be the main host of the honeynet we are building. After this is done we configure the active directory domain services. What this would do is transform our server as a domain and create its active directory of user who could log in into the server. We would need here to configure a static IP address to be able to make it a domain. The IP used was 192.168.1.15 with tis default gateway 192.168.1.1. This IP address are very important cause later on they would need to be configure into the router to host the host computer.

Once the AD (Active Directory) is set and the domain is created its time to create the accounts for our users. First creating the administrator account and later creating different type of user account. This is done to recreate an ambient of at least a small company with 20-40 employees. Giving the impression the server are real and live. Remember part of building honeypot is making it as real possible so it lures intruders.

Hyper-V will be installed to virtualize other servers or computers. Add a windows server 2012 as a SQL server and another one for n exchange server and document management system. As Hyper-V we can also use any other software to virtualize machines.

Once configure and set, it would be uploaded to the DMZ inside the router. That way its exposed to the public. If not uploaded to the DMZ I could do local test sniffing ports and messing around with the honeypot utilizing another computer with in the network. Once on the DMZ and the router configure to lower it security it can be compromised by an intruder. Just to tell that there are a lot of other tools and other ways to build honeypots.

For testing purpose I use two options. Use another computer within the network to conduct the investigation and attacks. Utilized a virtual machine with in inside the machine hosting the honeypot to conduct the investigation and attacks. At first I ask people to attack me but I wasn't able to capture any activity. There when I decided to take the approach to test it by myself and inside a private network.

AREAS WHERE HONEYPOT COULD BE LOCATED

One of the best place to host the honeypot it's in the DMZ area. This is a safe zone for it since they would need to infiltrate your firewall but it's in an isolated zone from all the servers and users. If a honeypot it's located within the internal network it will automatically become a "canary". The term comes from when miners where working they would bring a bird in a cage. IF the bird would die they would know some gas had been exposed and they would need to evacuate immediately. In this case if the "canary" gets infected, the network administrator should know an intrusion is inside the intranet.

For this investigation it was first set on the DMZ, but I had 0 activity recorder and I wasn't been able to analyze anything. I decided to move it inside the main network and create a virtual network to conduct myself all the test requires. The project became building a honeypot for testing purpose on a closed or private network.

TOOLS AND SOFTWARES

Here we would mentions a list of tools and software utilized during this investigation.

HoneyBot

To be able to monitor traffic and to easily configure a honeypot we can rely on tools to make these task a little more easily and even automated alerts. One of these tools used and install on the honeypot we are building it's called HoneyBot. This tools will allow you to easily configure your computer ports. This software could be downloaded for free from http://www.atomicsoftwaresolutions.com/. It also has a listener to every port you list, which means it will notify you and log when an intrusion is made or the port is called. This way you can later analysis the data to know if was an attacked.

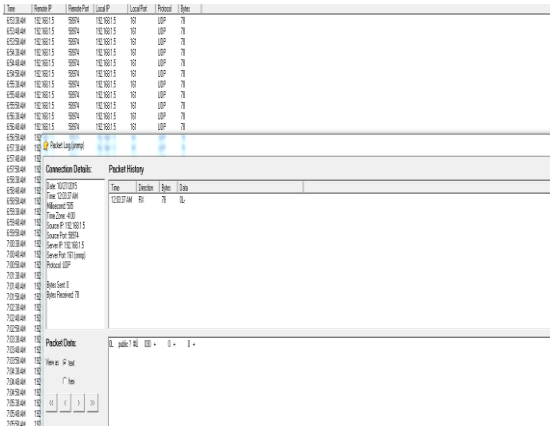

Figure 2
Example of HoneyBot

This is a print screen of HoneyBot in used. The main screen is a virtual log of the activity inside your machines ports. It keeps a track of the intruders or service IP-Address, which port was used for the attack, which protocol and the time it occurred. Each log this tool tracks, keeps a log of all the activity that occur during the attack.

Wireshark

"Wireshark is the world's foremost network protocol; analyzer."[4] This is tool for analyzing and monitoring network packets. It can be downloaded from https://www.wireshark.org/. It will display all the network activity in its GUI interface. From there packets can be analyze to try to determine what type of traffic is going through your network. Has lot of option of configuration and a big community which can give tips or help on how to use.

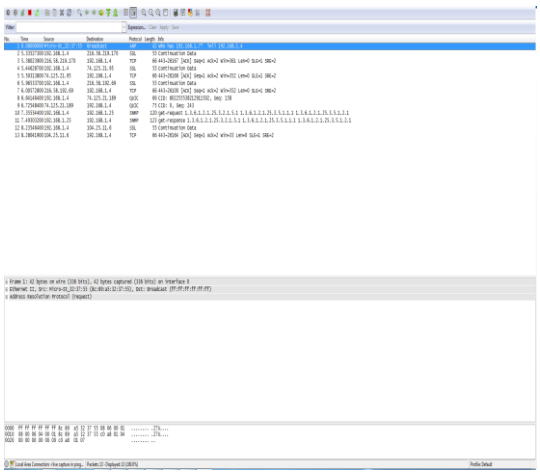

Figure 2
Wireshark Example

Kali Linux

It's a free open source Operating system from the Linux family which its focus on security/forensic, for computer security expert. This O/S comes ready for the purpose for doing security related task or hacking. It is easy to install and there's a lot of tutorials and guides on how to use most of its tools. It could be downloaded from: https://www.kali.org/. Before it was known as Backtrack 5.

INVESTIGATION AND ATTACKS

Since getting a honeypot attack can take time and even sometimes it never gets attack since it's not luring enough for intruder. It can be used as a playground for testing attacks and analyzing the data from those attack. Like mentioned before honeypots are very useful for investigation purpose. Here it will be use as a investigation tools to gather the behavior of packets in the network when getting attack. See the use of the portable Honeypot called honeybot and use Wireshark to monitor the network while doing some intrusion test. This way documenting the behaviors of packages during an

attack or during normal activity. In this test our victim will be the computer with IP-Address 192.168.1.15 and the attacks will be conducted from the computer with IP-Address 192.168.1.3. Also to mention inside 192.168.1.15 we got two additional virtual machines which can be tested.

The best way to use Wireshark is trying to keep your network as quiet as possible. The quieter your network the more easily is to analyze package. But we learned here that even on a home network the computer, router and switches are constantly broadcasting message from within the network and to outside the network. Here is an example with Wireshark of normal traffic on the host computer with idle activity.

Once everything is set we will proceed to do a raw nmap scan from Kali Linux to the server which is hosting HoneyBot inside. First we will open on the command prompt the application nmap. Once loaded we will input the command:

root@kali# nmap –v 192.168.1.15

This command will sniff and check for possible open port on the computer been scanned. Here we are scanning the Server 2013 which has HoneyBot hosted on it. TO make this work the firewall should be disable. On occasion if the firewall is on it will detect the sniff as an attack and it will block the ports and we will get negative results. When everything is set correctly the nmap will give back the discovery of every single port which can be access on the host computer. It would look like this:

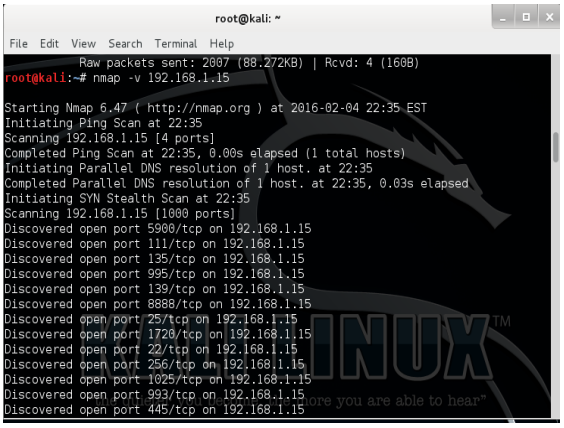

Figure 3
Nmap Scan on Linux

HONEYBOT REACTION

Once the scan complete you will get a complete list of open ports, this could be used for advantage of making and attack or entering the host machine without the user noticing. On the host machine we can detect the intrusion attack with HoneyBot. Most the port nmap showed are fake ports hosted by the HoneyBot utility. This is good cause you could capture hacker activity in a safe environment without actual equipment been compromised. Herse how HoneyBot reacted once this command was executed in the host machine.

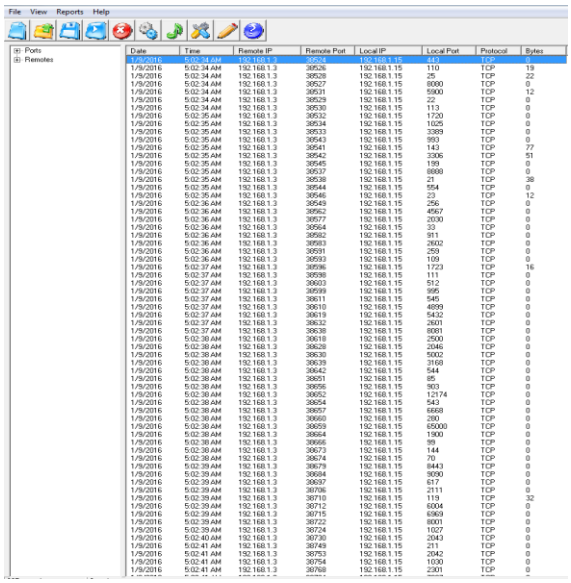

Figure 4
HoneyBot Reaction to Sniff

ANALYZING WIRESHARK

When the command nmap is executed we are using on the host machine Wireshark to monitor the activity in the network card. Once nmap is execute for 192.168.1.15 Wireshark start logging all the packages send to the network card.

When the command nmap is executed we are using on the host machine Wireshark to monitor the activity in the network card. Once nmap is execute for 192.168.1.15 Analyzing this traffic we found out that the nmap utility cause a lot of noise in the network when being use a scanner tool for open ports. Wireshark could be configure to generate warning and alarms when this type of activity is

captured. We can see in this picture that the computer 192.168.1.3 it's constantly asking for port request to the host 192.168.1.15. This teach us on how to detect a port scanning attack on a system. By this the network administrator could alert that their server might be getting attack or that a hacker is looking for a way to penetrated.

Wireshark also captured the protocol which the packet is transmitted. The next intrusion tested was trying to access via command prompt to the host computer. Once we gain access trying to guess the username and password of the server 192.168.1.15 to enter and browse the directory. Here we capture the how the attack or request is seen on Wireshark. The request was forcing a command prompt entry using invalid credentials.

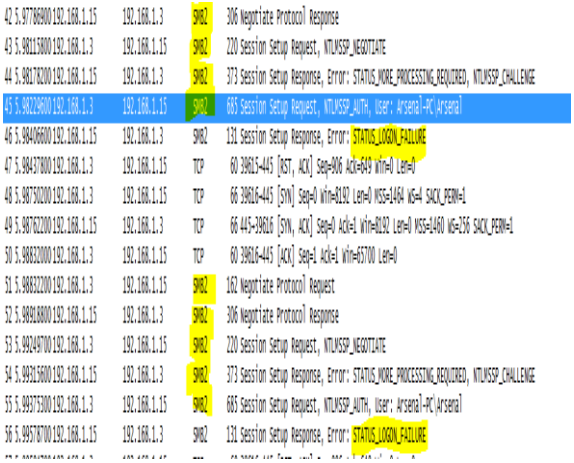

Figure 5
Packets in Wireshark

Analyzing these packaged we noticed the protocol change to SMB2. The SMB2 is a new version of the old Windows file sharing protocol SMB. This is use for file sharing purpose on modern and future windows host. Wireshark capture when the session was open, it even show the actual name of the computer which is in 192.168.1.3 (Arsenal). It show how many times it tried to do a file sharing session and that it failed on the logon twice. The other image will show getting access and creating a file directly inside the host computer.

CONCLUSION & FINDINGS

Honeypots have a big potential for investigation purpose as it was shown. It's a great tool to teach new or even pro-security experts on how to utilize different types of tools for intrusion detection or penetration purposes. They are easy to build, depending on the scale the person is willing to go and in some situation expend. For a simple honeypot it's only needed a computer and either install virtual machine in it or utilize plug in which simulate honeypots. Since trying to do pen testing or other type of security test without permission on other networks it consider illegal. Honeypots come to great used for this type of scenario.

Network are highly noise overall and to study packet could be hard. On a close environment like these, it would be easier to simulated different types of scenario to be analyze. Once this is done, it can be migrate to a real live world scenario and put it on practice. It can also be used to try deploy new malware and do forensic analysis on it. From how it was made on how it spread and which type of damage can cause.

REFERENCES

[1] L. Spitzner, "*Honeypots: Catching the Insider Threat*" unpublished.

[2] N. Provos, "*A virtual Honeypot Framework*", unpublished.

[3] L. Spitzner (2003). *Honeypots: Are They Illegal?* [Online]. Available:http://www.symantec.com/connect/article/honeypots-are-they-illegal.

[4] J. L. Davis, "*Using Wireshark to Create Network-Usage Baselines*". Georgia Tech Research Institute. Atlanta, GA, June. 10, 2007.