HONEYPOTS REVEALED

Prepared by:

Mohamed Noordin Yusuff

IT Security Officer

Specialist Dip. Info Security, MA. Internet Security Mgmt(Ongoing)

INTRODUCTION

IT Security instantly becomes an issue for anyone who connects their system to the Internet, either via a corporate network, an Internet Service Provider (ISP) from home or wireless device that can be used virtually anywhere when there are wireless access points. Security threats range from hacking intrusions, denial of service attacks to computer worms, viruses and more. We must understand that intrusion to a network or system can never be eliminated but however, can be reduced. Computer crimes are always increasing. Countermeasures are developed to detect or prevent attacks - most of these measures are based on known facts, known attack patterns – as in the military, it is important to know who your enemy is, what kind of strategy he uses, what tools he utilizes and what he is aiming for – by knowing attack strategies, countermeasures can be improved and vulnerabilities can be fixed.[1] Security activities range from keeping intruders out of the network or system, preventing the interception of information sent via the Internet to limiting the spread of and damage caused by computer viruses.

Most security professionals understand that the three concepts in IT Security are prevention, detection and respond whereby there is no end-to-end security equipment or solution that can cover two or all the concepts. For example, firewalls and anti-virus would fall under prevention, intrusion detection system and vulnerability scanners under detection and incident response teams would come under respond. Comprehensive security solutions include a mixture of software and hardware components. But however, honeypots fall under two main categories, Detection and Respond. Honeypots have a primary goal, which is to collect as much information as possible on the attack. The honeypot should operate in stealth mode so that the attacker would not know of its presence, as such, the information gathered would give the defenders a considerable advantage to protect and prevent attacks on the production systems.

DEFINITION OF HONEYPOTS AND HOW DOES IT WORK?

[1] Reto Baumann and Christian Plattner, “White Paper: Honeypots”, 26 February 2002, URL: http://www.inf.ethz.ch/~plattner/pdf/whitepaper.pdf

A honeypot is a security resource whose value lies in being probed, attacked, or compromised.[2] This means that whatever we designate as a honeypot, it is our expectation and goal to have the system probed, attacked, and potentially exploited.[3] In the earlier paragraph, I did mention that honeypot is a detection and response tool, rather than prevention which it has a little value in. Why did I say that? Because honeypots cannot prevent a particular intrusion or spread of virus or worm, it merely collect information and detect attack patterns. After doing so, the defenders can respond to this evidence by building better defences and countermeasures against future security threats. A honeypot is a tool to collect evidence or information, and to gain as much knowledge as possible especially on the attack patterns, hacker's purpose and motivations and the commonly used programs launched by them. From all the information received, we can even learn more about the hacker's ability especially their technical knowledge. I can say this is the main objective of a honeypot.

However, there are many uses of honeypots. Honeypots can also be used to catch hackers while they are in the network and to redirect hackers from the actual production systems to the honeypot system. The best personnel to manage the honeypot is one with extensive knowledge in three critical areas – Security, Systems, and Networks. In the right hands, a honeypot can be an effective tool for information gathering – In the wrong, inexperienced hands; a honeypot can become infiltrated machine and an instrument for the blackhat community.[4] But there are the needs to remind organizations that implement honeypots of one main thing – honeypots never assist to upgrade the network security of an organization, but it rather lures hackers into the network. Honeypots are security tools that have no real or production value. It should not be communicated by anyone. If there is an activity or traffic to the honeypot, this can be suspected as an intrusion, unauthorized access or a probing attempt. And rather, if there are any outgoing connections initiated by the honeypot, there is a high possibility that the honeypot has been compromised and taken over.

[2] Lance Spitzner, "Honeypots Tracking Hackers", 2003, Pearson Education, Inc

[3] Lance Spitzner, "Honeypots Definition and Value of Honeypots", 17 May, 2002, URL: http://www.enteract.com/~lspitz/honeypot.html

[4] Reto Baumann and Christian Plattner, "White Paper: Honeypots", 26 February 2002, URL: http://www.inf.ethz.ch/~plattner/pdf/whitepaper.pdf

Honeypots can be broken down into two general categories – *production honeypots* and *research honeypots*.[5] A production honeypot is used to assist an organization in protecting its internal IT infrastructure whereas a research honeypot is used to accumulate evidence and information in order to study hackers' or the blackhat criminal attack patterns and motives. But as mentioned in my earlier paragraphs, honeypots add very little value in prevention – They WILL NOT keeps the blackhat hackers out. The organization still need to depend on their security policies, procedures and best practices such as disabling unused services, patch management, implementing security mechanisms such as firewall, intrusion detection systems, anti-virus and secure authentication mechanisms to keep the blackhat community out of the organization's IT infrastructure. There is a need to ensure that the production honeypot is properly built, as if it is incorrectly implemented, the hacker can easily get into the honeypot. Production honeypots are valuable to the organization especially commercial, as it helps to reduce or mitigate risk that a specific organization faces. Production honeypots secure the organization by policing its IT environment to identify attacks. These production honeypots are useful in catching hackers with criminal intentions. The implementation and deployment of production honeypots are relatively easier than research honeypots. One of the reasons is that production honeypots have less purpose and require fewer functions. As a result, production honeypots also provide less evidence about hacker's attack patterns and motives. Using production honeypots, we may know the origin of the hackers such what kind of machine or operating system it uses, which country they are from, the kind of tools they used and the types of exploits the blackhat launches. But, how the hackers interact with each other and how they create their attack weapons might not be revealed from the production honeypot. Production honeypots have less risk. The concept of production honeypots is to let the blackhat community spend time and resource into attacking the honeypots rather than the organization's production systems. The attacker is tricked, deceived and mislead into attacking the honeypot, thus protecting the organization's production systems from the attack. But rather than using deception which also contributes little to prevention, organizations should use their time and resources into better securing their IT infrastructure with best security practices and

[5] As defined by Marty Roesch, creator of Snort

policies. Nowadays, attacks are becoming more automated and creative. Deception fails against two of the most common attack today; automated toolkits and worms – These automated tools will probe, attack, and exploit anything they can find vulnerable.[6] These tools will definitely be used to attack honeypots, and if you have a refrigerator with an IP address, it will be attack too!

Research honeypots are complex. They are designed to collect as much information as possible about hackers' and their activities. Research honeypots are not specifically valuable to an organization. Their primary mission is to research the threats organization may face, such as who the attackers are, how they are organized, what kind of tools they use to attack other systems, and where they obtained those tools.[7] While production honeypots are like the police, research honeypots act as their intelligence counterpart and their mission – To collect information about the blackhat community. From the information gathered by research honeypots, it will help the organization to better understand on the hackers' attack patterns, motives and how they function. With all these knowledge about potential threats in grasp, the organization can better prepare to arm itself with the necessary defence mechanisms and processes. Research honeypots are also an excellent tool to capture automated attacks as mentioned in the above paragraphs, such as auto-rooters or worms. From research honeypots, organizations can better understand the three important concepts in Security; Prevention, Detection and Respond. But for the organization to better secure its security infrastructure, they should use production honeypots as it is easier to implement and manage. An example of research honeypot is *honeynet*. To better utilize research honeypots, organization need to provide the blackhat community with real operating systems, protocols and applications for them to communicate with. But, with added role, research honeypots become a disadvantage as it is difficult and complex to implement, higher risk and require skilled personnel with time and effort to manage the honeypot.

In this paragraph, the difference between a production honeypot and research honeypot has been distinctly distinguished. It all depends on the objective of an organization on what they actually wants from a honeypot, either for production or

[6] Lance Spitzner, "Honeypots Definition and Value of Honeypots", 17 May, 2002, URL: http://www.enteract.com/~lspitz/honeypot.html

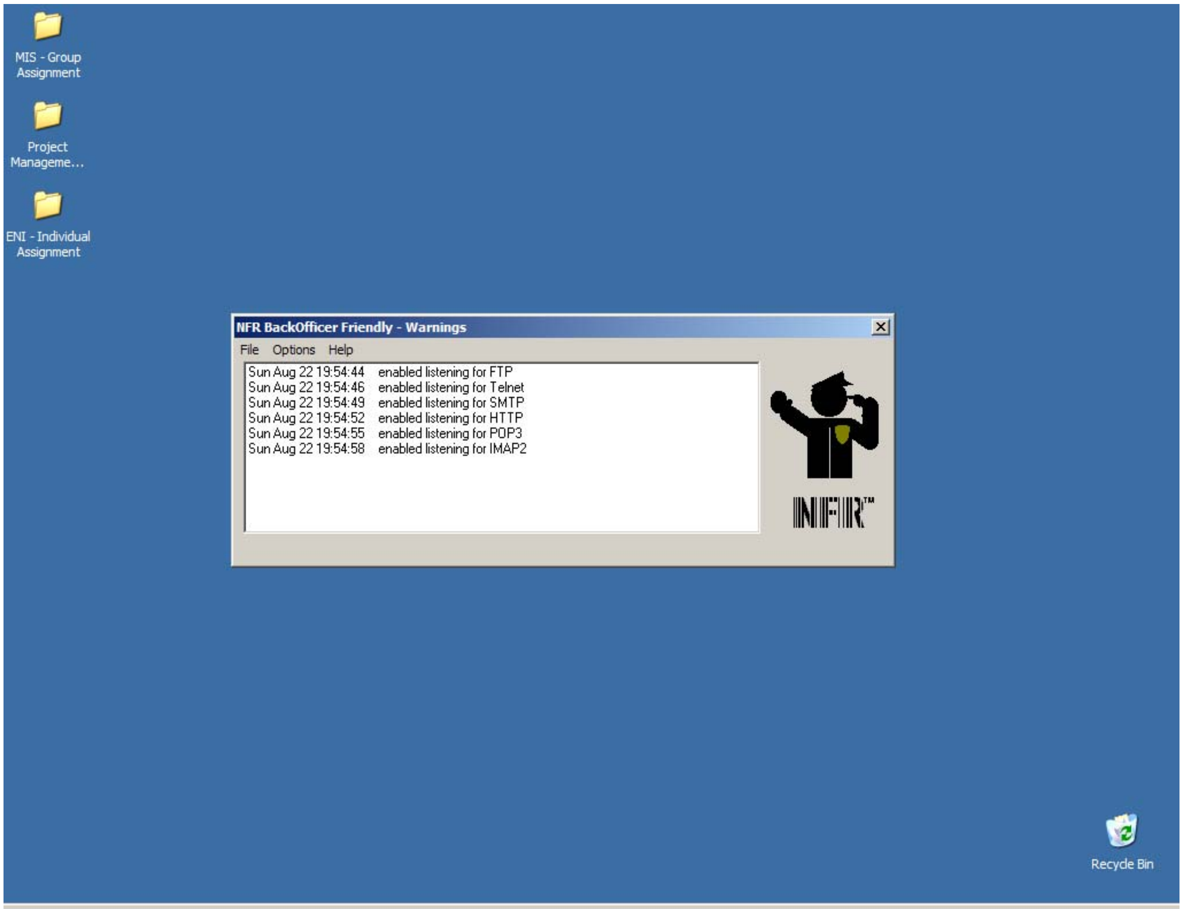
[7] Lance Spitzner, "Honeypots Tracking Hackers", 2003, Pearson Education, Inc

research. In short, if an organization wants to protect its IT environment and production systems by detecting and blocking the attacker, and to prosecute the attacker in court later, they should use a production honeypot. But, if the organization just wants to strengthen the security of its IT infrastructure by learning the hackers' attack techniques, the origin of attack, the kinds of tools and exploits used and his activities on the compromised honeypot, they should use a honeypot with a research touch.

TYPES OF HONEYPOTS – *Advantages and Disadvantages*

As mentioned in the earlier paragraphs, there are two main categories of honeypots – *production honeypots* and *research honeypots*, but what matters most is the kind of involvement and interaction of these honeypots with the attackers. It actually depends on what the organization wants to achieve when they choose the level of interaction for a honeypot. Honeypots can be classified into three different levels; *Low-Interaction Honeypots*, *Medium-Interaction Honeypots* and *High-Interaction Honeypots*.[8] In terms of installation, configuration, deployment and maintenance, the low-interaction honeypots are the easiest to implement. Basic services such as Telnet and FTP are emulated on low-interaction honeypots. It limits the hacker to interact with only these few pre-configured services. For example, a honeypot could emulate a Windows 2000 server running with several services such as Telnet and FTP. A hacker could first telnet to the honeypot to get a banner which would indicate what operating system the honeypot is running on. The hacker will then be brought to a login screen. The hacker have two options to gain access to the honeypot; either by brute force or password guessing. The honeypot would capture and collect all the hacker's attempts to the honeypot. But remember, there is no real or legitimate operating system for the hacker to interact with, but instead the hacker's involvements and interactions are limited to only login attempts. The main objective of low-interaction honeypot is only to detect, such as unauthorized probes or login attempts. To emulate a low-interaction honeypot, simple programs such as *BackOfficer Friendly* can be used.

[8] Lance Spitzner, "Honeypots Tracking Hackers", 2003, Pearson Education, Inc



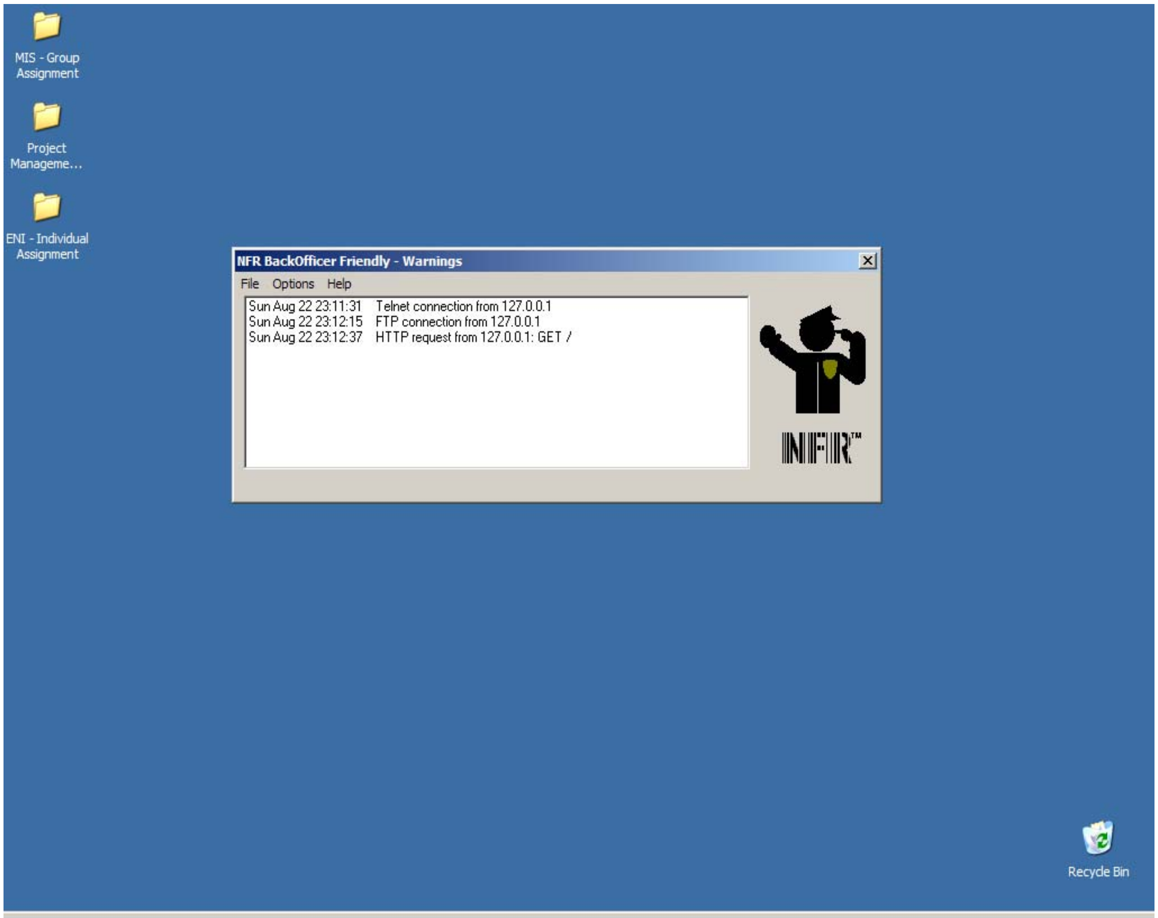
```
Sun Aug 22 19:54:44   enabled listening for FTP
Sun Aug 22 19:54:46   enabled listening for Telnet
Sun Aug 22 19:54:49   enabled listening for SMTP
Sun Aug 22 19:54:52   enabled listening for HTTP
Sun Aug 22 19:54:55   enabled listening for POP3
Sun Aug 22 19:54:58   enabled listening for IMAP2
```

Figure 1: Services Running on NFR BackOfficer Friendly

BackOfficer Friendly or BOF is a simple to install, easy to configure, and low maintenance free honeypot solution developed by Marcus Ranum and the folks at Network Flight Recorder – It was designed to run on almost any Windows operating system.[9] BOF could emulate several services limited to FTP, Telnet, SMTP, HTTP, POP3 and IMAP2. This low-interaction honeypots can be easily installed on the system and configured to any of the services specified above. With BOF, this low-interaction honeypot is both easy to deploy and maintain. But to prevent the system from being fully exploited by hackers, the administrator needs to ensure patch management on the host system and to conscientiously monitor the alert mechanisms on BOF. Low-interaction honeypots have the lowest level of risk. The honeypot cannot be used as a launch pad to

[9] Lance Spitzner, “Honeypots Tracking Hackers”, 2003, Pearson Education, Inc

attack other systems as there is no legitimate operating system for the hacker to interact with.



```
Sun Aug 22 23:11:31   Telnet connection from 127.0.0.1
Sun Aug 22 23:12:15   FTP connection from 127.0.0.1
Sun Aug 22 23:12:37   HTTP request from 127.0.0.1: GET /
```

Figure 2: Unauthorized connection attempts detected on NFR BackOfficer Friendly

But, we must understand that limited information can be obtained about the attacker from low-interaction honeypots. For low-interaction honeypots such as BackOfficer Friendly, we can obtain information such as date and time of attack, protocol used, source IP address and destination IP address as shown in Figure 2. If hackers' involvement is allowed on the emulated services for further interaction, we may know what the hackers' motives and intentions are via their activities. But it still depends on the emulation of the low-interaction honeypot to determine the amount of evidence collection during an intrusion or unauthorized connection attempt. How the low-interaction honeypot acts or respond to the hacker has already been pre-defined as shown in Figure 1.

In another words, the low-interaction honeypot is only good at capturing known attack patterns, but is worthless at interacting or discovering unknown attack signatures. I believe a low-interaction honeypot is a good start to those who are new and just beginning to understand the concepts of honeypots. Some other examples of low-interaction honeypots would be Specter[10] and Honeyd[11].

Another type of honeypot is the *Medium-Interaction Honeypots*. In terms of interaction, this is a little more advanced than low-interaction honeypots, but a little less advanced than high-interaction honeypots. Medium-Interaction honeypots still do not have a real operating system, but the bogus services provided are more sophisticated technically. As mentioned in the earlier paragraphs, as the levels of honeypots get complicated, the risk also increases especially with regards to vulnerability. Medium-interaction honeypots will give a certain feedback when it is queried upon. For example, the attacker might design a virus or worm scanning for SQL vulnerabilities on SQL servers. In this case, such a malware would be the SLAMMER worm. Thus, the honeypot would need to emulate a SQL server, and it have to be customized in order to accommodate what the worm is searching for, function or protocol wise. Whenever a connection attempt on TCP 1434 (in this case, SLAMMER) was made to the honeypot, it would respond as a SQL server, tricking the attacker that it has SQL functionality in the server. On the defence side, the intention would be to capture the worm payload for investigation and forensic analysis. But remember, like it was said earlier, the attacker (in

[10] Specter is a low-interaction honeypot developed and sold by NetSec.

[11] Honeyd is an OpenSource low-interaction honeypot developed by Niels Provos

this case, worm) was not given any operating system to interact with; it is still an emulated application. This medium-interaction honeypot, though more advanced than the low interaction honeypot comes with itself certain higher risks. It is more complex, time consuming and requires huge effort to build such a honeypot. The personnel who would build this honeypot need to have very good knowledge in protocols and application services. Customization and a significant level of development are required to build such this honeypot as you are actually creating a virtual environment to act as a real operating system. Not only that, the knowledge of security or securing this honeypot by covering up all the security loopholes and vulnerabilities are required. But, we must remember that, as security vulnerabilities, exploits especially zero-day exploit are increasing rapidly in the wild, attackers may still have access to the real operating system, though their access is restricted. Though the risks keep on increasing as the level of honeypots increase, the rewards are bountiful of evidence and information for you to analyse. Homemade honeypots can be classified as a medium-interaction honeypots as they are created by organizations and individuals to accommodate a certain needs. Thus, they are normally built either for production or research purpose.

The final and most advanced of honeypots are the *high-interaction honeypots*. As mentioned earlier, it has been clearly enunciated that as the level of interaction of honeypots increases, the risks and complexity increases, but the rewards also increases. These kinds of honeypots are really time consuming to design, manage and maintain. Among the three types of honeypots, this honeypot possess a huge risk. BUT, the information and evidence gathered for analysis are bountiful. The goal of a high-interaction honeypot is to give the attacker access to a real operating system where nothing is emulated or restricted.[12] In another words, the organization or individual who build this honeypot wants the attacker to gain root or super user access to the machine. This honeypot are normally connected to the Internet round the clock. With this kind oh honeypot, we can learn what are the kind of tools hackers' use, which country does the hacker normally comes from, what kind of exploits they use, what kind of vulnerabilities they normally look for, their knowledge in hacking and surfing their way through operating systems and how or what the hackers interact about. As the hacker needs to

[12] Lance Spitzner, "Honeypots Tracking Hackers", 2003, Pearson Education, Inc

compromise the honeypot to gain root access, and thus have the ability to move his way around the operating system or do whatever he wishes on the machine, this system is NOT SECURE. As a result, this system must be constantly monitored. We must remember that this honeypot have no production value, only research and the value is that it has to be scanned, probed, attacked and compromised. As the level of risks increases, we must ensure that these risks are reduced and mitigated. How? There is a need to place a firewall before the high-interaction honeypot. Because, when the hacker has gained control over that machine, he have exclusive rights to the machine including using that machine to compromise other systems or launch Distributed Denial of Service (DDoS)[13] attacks against other systems. In order to prevent that, rules must be configured on the firewall to allow the attacker to come into the honeypot environment (Allow Incoming Traffic) but block the attacker from going out of the honeypot (Deny Outgoing Traffic). As such designing this architecture and configuring firewall rules require a significant amount of work, time and expertise. Honeynets[14] are an example of high-interaction honeypots.

	Low	Medium	High
Degree of Involvement	Low	Mid	High
Real Operating System	No	No	Yes
Risk	Low	Mid	High
Information Gathering	Connections	Requests	All
Compromised Wished	No	No	Yes
Knowledge to Run	Low	Low	High
Knowledge to Develop	Low	High	Mid-High
Maintenance Time	Low	Low	Very High

Figure 3: Overview of Advantages and Disadvantages of each level of involvement[15]

[13] In DDoS, computers are compromised called zombies. These zombies are used to send huge packets of traffic to targets, thus crashing their servers or PCs, or flooding their bandwidth, denying service.

[14] Honeynets are variety of standard systems deployed in controlled environments specifically research purpose.

[15] Reto Baumann and Christian Plattner, "White Paper: Honeypots", 26 February 2002, URL: http://www.inf.ethz.ch/~plattner/pdf/whitepaper.pdf

DEPLOYING HONEYPOTS IN AN ENTERPRISE ENVIRONMENT

Before deploying honeypots, there is a need to analyse the purpose of implementing the honeypot. Do we want to use it as production honeypots or research honeypots? In another word, do we want to protect our environment by diverting hackers away from our production environment, or do we want to strengthen the security of our IT infrastructure by studying the activities of the blackhat communities in terms of hacking techniques, the kind of tools and exploits used and their activities. Organizations should not adopt honeypot as a security equipment that can replace their firewall, anti-virus or intrusion detection systems. Furthermore, organizations need to understand the value they want to achieve by implementing the honeypot. If you are looking to deceive attackers, potentially confusing them or slowing them down, then you want a honeypot for prevention – If you are hoping to detect attacks, identifying blackhats that penetrated your firewall or networks – then you want a honeypot for detection – If you are hoping to improve your reaction to system compromises, then you want a honeypot for incident response – that is, reaction.[16] It would be best that organizations make their intentions, specifications and purpose of implementing honeypots as clear and specific as possible. If for example, the organization wants to adopt a research honeypot to learn hackers' *modus operandi.* Protocols such as telnet and ftp to production servers are strictly disallowed in accordance to the organization's security policy. The organization wants to ensure that there are no violations of the security policy, and also wants to detect and track down any individuals, either internal or external, who may have penetrated the organization's firewall by using commands such as telnet and ftp. But what does the organization wants to track down? Is it the source IP address? Is it the frequency of protocol used? Is it the frequency of dropped or accepted traffic by the firewall, or does the organization wants to capture the attack in real-time? The more precise the specifications and purpose of a honeypot, the more beneficial it will be to the organization. Like in the sayings of Sun Tzu, a Chinese general in circa 500 B.C, quoted *"if you know your enemy as much as you know yourself, you will never suffer defeat"*.

[16] Lance Spitzner, "Honeypots Tracking Hackers", 2003, Pearson Education, Inc

Depending on the organization's requirements, there are several different types of honeypot solutions to choose from.

- Preventing attacks through deception or deterrence – for example, Specter's ability to emulate vulnerabilities or give warning messages.
- Detecting attacks, acting as a burglar alarm. Almost all of the honeypots excel at this.
- Responding to attacks, collecting data and evidence of an attacker's activities. ManTrap is an excellent way for your organization to figure out how an attacker broke in.
- Researching attackers' tools, tactics and motives – for example, capturing payloads of worms, new exploits or covert communication methods. Homemade honeypots, ManTrap, and Honeynets are valuable in these areas.[17]

As mentioned in the paragraphs above, determining the interaction level of a honeypot is very important. The higher the involvement and interaction from the honeypot, the more information and evidence can be studied and learned. But we must remember; the higher the interaction and complexity of the honeypot, the greater the risk is. Apart from determining the interaction level, the organization has to figure out whether to purchase a commercial honeypot or develop it in house. For commercial honeypots, it will be much easier to install, configure, deploy, manage and maintain, but commercial honeypots are normally very expensive. Commercial honeypots are normally managed by administrators with less skills and knowledge, and possibly via the administrative graphical user interface (GUI). Commercial honeypots come with many different functions and utilities. Some of them could be viewing of logs and executive or management reports, monitor attacks in "real-time", pager and hand phone alerts. For honeypots developed in-house or homemade honeypots, the one thing that an organization really saves is cost. It is really a lot cheaper to build a honeypot in-house rather than purchasing a commercial honeypot. One disadvantage on homemade honeypots is that it requires a considerable amount of effort and time to implement it.

[17] Lance Spitzner, "Honeypots Tracking Hackers", 2003, Pearson Education, Inc

Another disadvantage is that a honeypot built in-house requires one with good skill and knowledge to manage it. But what really makes a homemade really beneficial is that it is not limited to customization and configuration. The organization can tailor the honeypot to whatever configuration they want and comfortable with. For example, a commercial honeypot could only listen to default ports such as FTP, HTTP, SMTP and TELNET, but an organization or enterprise could configure or customize the honeypot to listen to all the above-mentioned ports, high ports, and even emulate any vulnerabilities that they feel required. Lastly, we need to determine what kind of operating system the honeypot should run on, either Windows or Unix. This actually depends on the capability of the organization, whether they are more comfortable technically with Windows or Unix. This reason prevents any accidental misconfiguration on the honeypot or operating system. The organization must take into consideration that Windows-based honeypots are easier to manage and maintain rather than a Unix-based honeypots. Thus, basically it is really up to the discretion of an organization on what kind of operating system or honeypots they should use how they should implement and who to manage it.

Organization also should use their discretion on how many honeypots they wish to deploy. If an organization has a large-scale IT infrastructure with segregated networks, they may want to consider having more than one honeypot. Because, if an organization uses production honeypots for their network, they would need different honeypots to protect their segregated networks. Another discretionary move an organization should consider before deploying honeypots is cost. Having more honeypots would require more budgets and more time to build them. The organization should also think of resources to manage these honeypots because too many honeypots may engulf them with a lot of information and very little time to manage the honeypots. The organization need to be very specific on their goals in implementing the honeypot. But for research purpose, it would be recommended that the organization deploy one or two honeypots as contrary to production honeypots, research honeypots have very little value. Besides, similar information can be gathered from either of the research honeypots.

With regards to the placement of honeypots, it must be deployed in an ideal location. If the organization wants to detect hackers entering their private network, they may like to place the honeypot in their intranet environment. But if they are more concern with attacks coming from the Internet, they should deploy their honeypot before their firewall, demilitarized zone or behind their second layer firewall. But there is a need to take extra precautions on the honeypot in front of the firewall, as it may be subjected to compromise. The honeypot in front of the firewall will generate numerous traffic such as port scans, exploits and unauthorized attempts. For honeypots that are placed before the firewall, it will pose an increase risk to the organization as attackers would attempt to attack and interact with this honeypot. By placing the honeypots before the firewall, there are two sides of a coin with this. Firstly, it will increase the publicity of your organization to hackers, thus bringing in more attackers to compromise the honeypot. Secondly, when attackers especially script-kiddies who do not know how to spoof their originating IP address realized that they are attacking a honeypot, they might be frightened off. But, this honeypot would also receive a lot of false positives from the wild and it would definitely overwhelm administrators who are taking care of this honeypot. Placing the honeypot in the DMZ seems to be a good idea because not all traffic is allowed to pass through the firewall. But, there is also need to ensure that all of the other systems in the DMZ are hardened and secured. Placing honeypots at the DMZ would be a good idea as DMZ is a network that has one of the greatest risk to be attacked. By placing the honeypot behind the second layer firewall, organization will see less traffic. Only legitimate traffic are allowed to pass through the second layer firewall but if there are traffic attacking or use unauthorized protocols such as TELNET and FTP to the honeypot, then something is suspicious and obviously not right there. But this is for traffic coming from the Internet. The main purpose of placing a firewall behind the second layer firewall is to detect and capture internal attacks.

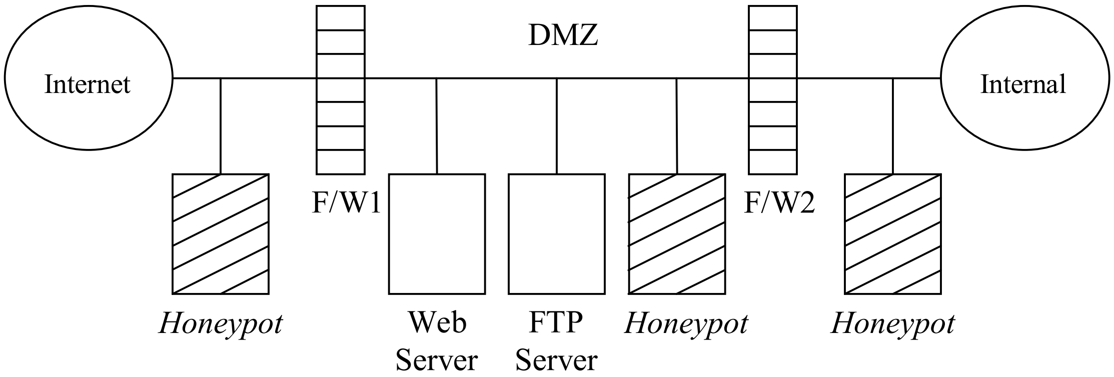


Figure 4: Typical network diagram of honeypot before F/W1, DMZ and after F/W2

The honeypot should be installed with VMWARE Workstation. VMWARE allows the honeypot to run multiple operating system such as Windows 2000, Unix and Linux. By doing this, the organization is actually building a honeynet-type honeypot. Honeynets are one of the high-involvement honeypots. By having different systems with different applications, the organization can learn different tools and tactics used by hackers. The organization is able to accurately profile specific blackhat trends and signature. All systems placed within the honeynets are standard production systems. These are real systems and applications. Nothing is emulated nor is nothing done to make the system less secure. The risks and vulnerabilities discovered within a honeynet is the same that exist in many organizations today. The primary aim of a honeynet is to gather information about threats that exist. New tools can be discovered, attack patterns can be determined and attacker motivations are studied. In a honeynet, it is good to place a firewall such as Checkpoint NG before the honeypot for access control; to allow only legitimate traffic into the honeynet so as not to overwhelm the honeypot. Apart from VMWARE, the honeypot could also be installed with tools such as SPECTER, BackOfficer Friendly or Mantrap. Furthermore, by configuring the firewall to prevent outgoing traffic, the attacker will get trapped in the honeynet once they managed to penetrate into the internal network. The honeypots in the honeynet are meant to be probed and attacked. By doing so, it could be used to gather information on the proceedings of attackers who are attacking the internal network of systems and their deployed tools. Once attacked, and if gathering information is the primary objective, no other security mechanism is comparable to a honeypot. The honeypots in the honeynet will definitely collect high volume of data, showing network activity and what the hacker do once they are inside the system.

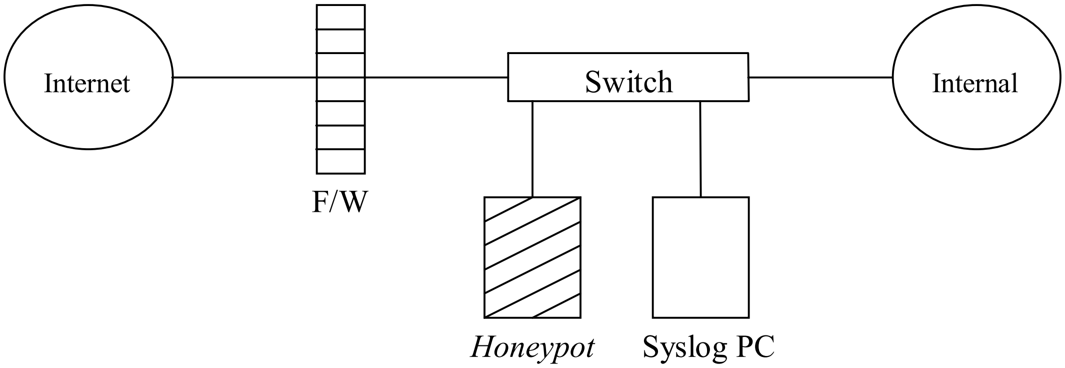


Figure 5: Typical network diagram of a Honeynet

The above diagram consists of a honeynet being deployed in an enterprise environment. There is a firewall to capture incoming and outgoing traffic which also provides Network Address Translation or NAT. The syslog PC would gather information for incoming traffic and commands executed by the hacker who is entering into the network. The PC which contains the honeypot would have honeypot software such as BackOfficer Friendly, Mantrap or Specter to gather all necessary information with regards to the hackers' motives. The honeypot would be installed with VMWARE Workstation which would then be able to run multiple operating systems such as Windows 2000, Linux and Unix. This typical network diagram of a honeynet will be very useful if deployed in an enterprise environment.

VALUE OF HONEYPOTS

As mentioned and explained in the above paragraphs, honeypots have many different values especially when defining between production and research honeypots for prevention, detection and response. As mentioned, production honeypots are used to help reduce risk and diverting hackers from attacking the production systems whereas a research honeypot is used to collect as much information and evidence as possible about the blackhat community. The latter may not bring any value on security to the organization but it sure helps an organization to understand the hacking techniques and tools used by hackers, attack patterns, how the blackhat community communicate with each other, etc. This will later help the organization to build stronger defences for their internal IT infrastructure in their fight against hackers. Organizations have to deem all traffic to the honeypot as suspicious activity because there should not be any illegitimate traffic such as FTP and TELNET to and from this part of the network. Data that is collected from the honeypot is of high value and can definitely lead to clearer comprehension to increase the security of an organization's IT environment. Depending on where the honeypot is placed, it will either collect vast amount of information that can be overwhelming, but most of it will be redundant and useless to the organization, and on the other hand, it collects very little data, but can be of very high value. Any data collected can be a scan, probe or attack which are useful information to the organization. Sometimes, the probability of finding a honeypot in the network can be quite low as it does not have any production activity, thus does not generate high noise level.

Depending on the honeypot tools used, useful information can be understood by the administrator from the easy-to-use graphical user interface. Data, especially those of malicious activity, can be used for statistical modelling, trend analysis, detecting attacks, or even researching attackers.[18] Depending on the placement of the honeypot, and if they collect little data and monitor little activity, they will not have problems of resource exhaustion. Organization must understand that honeypots do not collect all data and monitor all traffic flowing to and from a particular network instead it just collects data and monitor activity targeted at the honeypot itself. Unlike firewalls and intrusion detection systems, there is not a need to use expensive and sophisticated hardware to build a honeypot; an unused computer or laptop will do. Again, unlike firewalls which need to configure rule bases and anti-virus or intrusion detection systems which need to manage signature databases, there is no need to do all that on a honeypot. Just place it in the network, sit back and wait.

Does honeypot provide any "Return on Investment to the organization? As stated in above paragraphs that a honeypot is meant to be scan, probed or attacked. But what if there is none of the above and the honeypot was installed in the organization's network for a few years already? Management will definitely question the return on investment for the honeypot. Management must understand that honeypot is not a security equipment.

[18] Lance Spitzner, "Honeypots Tracking Hackers", 2003, Pearson Education, Inc

The reason why the organization’s honeypot was never compromised before and malicious activity had never been captured is because of the investments the organization made in ensuring the latest security technologies such as encryption, access controls, authentication had been in place.

Honeypots also have their disadvantages. Honeypots only capture and detect attacks targeted at itself only. If an attacker penetrates into the organization and attacks other production systems, the honeypot will not pick up any activity. Especially, if the attacker has identified the honeypot, he or she can avoid that system, penetrate the organization’s network and attack other innocent production systems. In worst case scenario, the attacker can even spoof the other production systems in the network and use them to attack the honeypot. Organization need to ensure that they do not reveal the true identity of the honeypot. Because once known, the attacker can easily avoid the honeypot. For example, if the honeypot is meant to emulate a Windows server, but instead it contains characteristics and behaviours of a Unix server, the attacker would suspect this misconfiguration to be a honeypot. Organization must ensure that the honeypot is correctly implemented as wrongly-implemented honeypots can pose a high security risk. Especially, if the honeypot is attacked or silently compromised, it can be used to harm other systems in the organization, or worst, systems in other organizations. For example, the attacker can make use the systems including the honeypot in Organization A to launch a Distributed Denial of Service attack to systems in Organization B. Organization must never replace any security equipment for a honeypot, but instead honeypots work hand-in-hand with security equipments.

LEGAL ASPECTS OF HONEYPOTS

Different countries may have different laws and regulations against honeypot technology. Even, there might be laws that limit certain honeypot implementations. Depending on the purpose and objectives of the honeypot, they might infringe certain legal rights. For example, is the honeypot meant to detect and prevent hackers, or are you trying to gather information on certain hackers’ terrorists groups and sell this information to a third party? This may be a bogus assumption but where law is concern, it may have certain impact on bilateral relations between countries. Another example, if a honeypot gets compromised and was used to launch a Distributed Denial of Service attack to another organization, who shall be at fault? The organization or the hacker? Or is there a hacker, and not a worm or an unauthorized script activated by an inside? This is another area to consider which may pose legal complications. Apart from governments' regulations, there must be some sort of an acceptable use policy clearly stated in an organization's privacy and security policy on honeypot implementations and usage. Another example will be recording of keystrokes and communications. Does the organization's user privacy and security policy allow the recording of users' keystrokes and communications, including that of outsiders entering the organization's network? This breach may cost an organization tons of money during a civil suit. Before an organization implement and deploy a honeypot in their organization, they should seek professional legal advice from their lawyers on the matter to prevent any unnecessary future legal claims.

Three main legal issues of concern with respect to honeypots are privacy, entrapment, and liability.[19] For privacy, there is a need to pinpoint if the use of the honeypot invades users' privacy including those attackers that hacked the honeypot. And, if so, how much information can or cannot be captured? As stated in above paragraphs, does the organization have the right to capture keystrokes and record users' communication? Dependant on the interaction level of a honeypot, they record different amount of activities. A low-interaction honeypot mainly captures small amount of information such as source and type of attack whereas a high-interaction honeypot capture attacker's communications such as chat programs or emails. Ultimately, it becomes a question on how can all these amount of information be captures without infringing any legal statutes? Secondly, there is a need to know how entrapment applies to honeypot technology? Organizations and individuals feel that honeypots should never be deployed due to implications on entrapment. Entrapment only applies if a law enforcement officer or government agency induces a person to commit a criminal act for the purpose of subsequent criminal prosecution. But if the honeypot is operated by a private or commercial organization, this law is void. For liability, there is also a need to know if the organization that deploy the honeypot will be held liable if the honeypot was

[19] Lance Spitzner, "Honeypots Tracking Hackers", 2003, Pearson Education, Inc

used to conduct attacks to other organizations, storing and distributing illegal materials. Although the harm was performed by the attacker rather than the honeypot operator, it would not have been successful if the honeypot had been more secure. In another words, the organization who implement and deploy the honeypot fail to practise due care and diligence. The risk of the honeypot being compromised can be reduced if the honeypot administrator ensures that the honeypot is secure and make it as difficult as possible for an attacker to use it in order to harm other systems. This activity will include system patching, updating of anti-virus signatures. Also, deploying updated versions of honeypot with up-to-date patches, effective access and data control mechanisms are some of the security measures that can be put in place when implementing and deploying honeypots. Lastly, honeypot administrators need to be proactive in closely monitoring the contents in the honeypot PC to ensure that hackers do not store and distribute illegal contrabands from the honeypot which may result to legal implications on the organization. By understanding the legal issues surrounding honeypot technology, organizations can better prepare to face problems and pitfalls that may arise.

CONCLUSIONS

In this growing IT arena, there is also a need to strengthen its security. Preventive, Detective and Responsive measures have to be undertaken in order to improve IT Security. To improve our Security and to fight the enemy, we must know them, befriend them and learn from them. Hackers can find our computers in just 30mins. Malicious attackers are constantly scanning our network looking for vulnerable loopholes and open ports. But without the knowledge of the enemy, how can we defend ourselves? We have to think like a hacker in order to stop a hacker. To many, honeypot is a new form of security technology. But actually, honeypot is just common sense. As in the sayings of Sun Tzu, a Chinese general in circa 500 B.C quoted *"if you know your enemy better than you know yourself, you will never suffer defeat"*. There is a lot of research and discussions about honeypots going on all around the world. Commercial products exist. There are many low to high-interaction honeypots available in the market nowadays. For freedom of use and flexibility, homemade honeypots are built. Honeypot is definitely a valuable asset to an organization who constantly gets hacked. To understand hackers' attack patterns and techniques, the tools they used, how they interact with one another, organizations should deploy honeypots. By doing so and from the information collected, they can better build stronger defences to protect their IT infrastructure. However, organization need to ask for professional advice first from their legal counsel on the implementation of honeypots whether they will breach any laws and regulations. Organization must never treat honeypots as a "*plug-n-play*" product, meaning just buy and deploy in their IT network. Instead, they should take note of the risk involves in implementing and deploying honeypots. Proper security measures such as buying honeypot with latest patches, system patching of the underlying operating system, proper access and data control mechanisms, and adhering to best security practices have to be in place. I believe honeypots are still in their infancy and new developments will occur over time. Because, as hackers get smarter with their attacks, honeypots have to be more advanced to complement these attacks.

REFERENCES

Lance Spitzner, "Honeypots Tracking Hackers", 2003, Pearson Education, Inc

Reto Baumann and Christian Plattner, "White Paper: Honeypots", 26 February 2002 URL: http://www.inf.ethz.ch/~plattner/pdf/whitepaper.pdf

Lance Spitzner, "Honeypots Definition and Value of Honeypots", 17 May, 2002, URL: http://www.enteract.com/~lspitz/honeypot.html

Kurt Seifried, "Honeypotting with VMWARE – basics", 15 February 2002, URL: http://www.seifried.org/security/ids/20020107-honeypot-vmware-basics.html

Honeynet Project, "Know Your Enemy: Defining Virtual Honeynets, Different types of Virtual Honeynets", 18 August 2002, URL: http://www.honeynet.org/papers/virtual/

Michael Clark, “Honeynets”, 7 November 2001, URL: http://online.securityfocus.com/infocus/1506/

Telecommunication Network Group, Prof. Adam Wolisz, “Network Security Lab”, 24 April 2002, URL: http://www-tkn.ee.tu-berlin.de/research/SecurityLab/

Honeynet Project, “Know Your Enemy: The Tools and Methodologies of the Script Kiddie”, 21 July 2002, URL: http://www.honeynet.org/papers/enemy/

Honeynet Project, “Know Your Enemy: Honeynets, What a Honeynet is, its value, how it works, and risk/issues involved”, 15 August 2002, URL: http://www.honeynet.org/papers/honeynet/