GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

GSEC Practical
Assignment 2.5b – option 1
Enoch Gamble I
Trapping A Monster: An Observation of Honeypots

Introduction

Lance Spitzner's brainstorm, the honeypot, has received great praise in the fight to defend information systems and networks from criminal hackers. Many believe that this is the answer to the challenges of capturing a monster, the professional hacker, who has pretty much exercised control over the cyber crime world until now. At the present revelation, the monster is leading in the Internet war. As the information system security fight rages on, expansion of honeypot technologies has brought about a new chapter in the cyber (internet) war story. Honeypots are not only being used in recording and revealing hacker activity, but now they have the potential of joining the fight in the pursuit and hopeful prosecution of hacker criminals. Though temporarily hindered while legal questions are being answered, they are by far a great step in the direction of the development of a more secure cyber world. Though not and end in themselves, fortunately, their use with other security measures have raised the score for the good guys. For them, capturing the monster is only one step. Once captured, a sound cage will be needed to keep the monster from escaping again and in a fit of rage and retaliation, causing Internet chaos.

As the complexity of the honeypot grows, so does the risk if control of it is lost to the wrong side. As if the risk was not high enough and with the good guys already playing "catch up" in the cyber war, the idea of using honeypots has been complicated further with newly raised issues of legality such as protecting the hackers from entrapment by law enforcers as well as the fear that cyber vigilantes are using "hack back" techniques to counter attacks and administer their own justice. At present the hacker threat is still a monster that cannot be stopped but hopefully can be brought under some degree of control. With these strikes by professional hackers, lack of legal guidelines and others already against those trying to keep the Internet safe from the monster, users of honeypot and similar technology must beware of trapping it in a cage that will not hold it. If the cage fails, the information system world is in grave danger.

Honeypots: Tools of Defensive or Offensive Pursuit?

In recent history, honeypots have had effective results in uncovering the formerly hidden formulas of exploits against information systems and networks. Though not a new idea, honeypots are still relatively new technology in their use in the cyber world. Despite the hurdles yet to jump in the information warfare battle, honeypots and similar tools are still a great idea that's gaining serious momentum. The idea of setting a trap for the attacker is a heroic effort of the selected victims-to-be to protect themselves from theft or destruction of property.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The honeypot could become not only the most attractive way to detect intruders, but also the way to monitor what they are actively doing and have done. The question of whether an exploit is taking place or not is seemingly nullified when a honeypot is involved. Lance Spitzner writes in an Internet article these words. "Any time a connection is sent to the honeypot, this is most likely a probe, scan, or even attack. Any time a connection is initiated from the honeypot, this most likely means the honeypot was compromised"[1]. With this in mind, they could be the ultimate alarm system that warns of hack attacks and the tool to use to develop a better defense. Since no legitimate users are found on it, all users that connect are "suspects". The near future looks promising, but before going any further in their use, the question probably should be addressed, "What exactly is a honeypot?"

A honeypot is a system (or software to create a virtual system that's not really there) that is placed along the network path with the purpose of being hacked. Hacking can come in the form of different attacks (viruses, worms, Trojans, etc.), unauthorized probes (to gather sensitive system and network information) or compromises (breaking in and gaining control of data, applications, systems, the network or more). The object is to let the attacker use his or her tools to breach the system's security and search around for important data and applications to exploit (steal, destroy, take control of, etc.). While the intruder is invading the system, their every move is recorded and watchful eyes (the good guys) monitor what they are actively doing and analyze to data collected after the crime is committed to learn the hacker's techniques and patterns. The information learned is to be used to fortify the systems and networks being attacked against new attempts to be exploited by the monster.

The interesting part about honeypots is that the intruder is kept unaware that they have attacked a system or network with data that is useless to their purpose. The information they observe is intended to deceive them into spending more time searching, collecting information and hopefully exhausting their arsenal of tools completely exposing themselves and their purpose. Hopefully the intruder will come and go without realizing that the evidence of their activity has just been captured. As they (and their friends) return from time to time, the evidence against them mounts and the pattern of their tactics are revealed. A variety of honeypot technology now awaits the cyber criminal. Honeypots can come in as many shapes, sizes and configuration setups as there are operating systems, applications, network components and the like. For now, the experts (specifically Lance Spitzner and those associated with the Honeynet Project team) have narrowed honeypots into two main categories.

According to Marty Roesch, the creator of Snort (a popular Unix based intrusion detection system), there are basically two types of honeypots currently in use. First, production honeypots that help reduce risk and enhances an organizations security posture. They can be "thought of as 'law enforcement', whose job is to detect and deal with bad guys". These are considered the starting range of

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

which Mr. Roesch, along with colleagues Lance Spitzner and David Dittrich define as “low interaction honeypots”. At the “low interaction” level are production honeypots being “simple and easy to install because they emulate only a few services and the information collected is limited.” Virtual honeypots fall into this category since they are programs that can emulate different types of systems on a virtual network that doesn’t really exist. When compromised, the hacker has “little to exploit” or take control of and use to their advantage making the risk level low. The monster has been limited in its ability to attack.

Secondly, there are research honeypots with the purpose of "gaining information on the blackhat (bad guys) community by researching threats organizations have to face". Think of these types as "counter-intelligence". Labeled as “high interaction” honeypots, these are not programs to create virtual systems but “actual systems” placed in a honeypot or honeynet (a more advanced network of systems in a honeypot). A lot more information can be captured and more lessons learned with research honeypots but extra caution must be taken due to the risk being much higher. If these systems fall into the intruders control, having real systems and applications at their command can give them more power to exploit the victim and other systems. Instead of controlling the monster, it is fed, strengthened and has increased its power to destroy.

Honeypots can just as effectively be used as a weapon of offense as it is a tool of defense. Marcus J. Ranum speaks out to this effect. “Traditionally, security has been purely defensive. There has been little an organization could do to take the initiative and challenge the bad guys. Honeypots change the rules. They are a technology that allows organizations to take the offensive.”[2]

The offensive approach does not mean hacking back at the unlawful hacker community. Retaliation will never fit as a lawful way of protecting against an attack due to its suggestion of revenge. Even when attacked, getting revenge is not the answer to the crime – getting justice is. Justice administered by law officials has the task of stopping the criminal and set the precedence for others who commit the same crimes. The perception seems to be that honeypots can be used in the offensive against cyber criminals only by law enforcement to collect forensic data to be used in a court of law. Data lawfully collected and properly protected (not contaminated) by civilian organizations via honeypots can be turned over to the Internet police to retrieve evidence used for prosecution. Organizations need to be informed as to how to handle these types of systems and data since special handling is required. In some occurrences, the offender can be identified, trapped and apprehended, but still set free or given a lesser sentence. Why? The data evidence had been rendered inadmissible because the court was convinced that it was possibly tampered with or there was a failure to properly secure it. It’s simple, no evidence, no case.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Some questions surface when the use of honeypots as an offensive tool for civilians or as a weapon by the law are addressed. Can the responsibility of offensive use be passed to certified information security professionals with the ability to perform forensic data collection or is it reserved to just the formally trained government security analyst. Currently, law enforcers as well as laws for cyber crimes are too few for a reasonable amount of control. Most governmental law agencies have neither the trained personnel nor the budget to tackle the cyber crime world since such activity is mounting beyond detection and still too new to be properly handled by the justice system. While waiting for lawmakers to act, honeypots are moving forward in popularity, research and use. With such technology beginning to flood networks, some may reason that the offensive use of honeypots as a license for hacker counterstrikes. But a rational view, even without concrete laws in place yet, teach us that the monster won't be legally trapped by applying exploit for exploit. The potential legal setbacks in such cases could cripple the fight to protect cyberspace. With such an excellent tool at the disposal of the security community and the possible results honeypots can produce, maintaining lawful application is the favorable avenue.

Are Honeypots The Answer To Hacker Protection?

Surely honeypots represent the cutting edge in the fight to find, track and apprehend hacker criminals. Though not a new idea, they've arisen to the forefront in the list of tools to be used to gain knowledge of how the protect against cyber attacks today. So far, no other tools have enjoyed the success honeypots have had in revealing, recording and now actively tracking the stealthy (masked) activities of the Internet underworld. Are there other tools that will allow the information network protectors to identify, track and record forensic data (proof of criminal activity and intent for prosecution) of an intruder even while they are actively compromising a system or network? If allowed to continue even to the point of pursuit (legal guidelines pending), honeypots could be the answer to help bridge the gap in the race against criminal control of cyberspace. Real world hacks can be found in a "step by step" format showing detailed data of an intruder's activities and exploits used. This is key information that can be used (and hopefully is being used) in the initial professional training of information systems security analysts and in the awareness training of system and network personnel. One such Internet article written by Toby Miller reveals what he describes as the …"attacker's recon, the attack, the attempted cover-up, and the reason for the attack on the honeypot" [3]. He describes in what appears to be in just enough detail (not to technical the for good guy beginners) one example of a simple honeypot setup and record of an attack. Following the proper procedure of securing the network first before implementing the honeypot, (an important part for legal defense if ever needed) the following guidelines can be simply outlined and used for training.

- Hiding a honeypot among production systems.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Ensuring it is behind a router for protection of the network (all traffic in but controlled traffic out in case intruder gains control).
- Ensuring the integrity of logs by setting up a remote log server out of the honeypot's reach.
- Some simple log analysis to gain information on the intruder and follow his/her activity from the initial scan, to system access, exploitation and final exit after removing evidence of their presence.

With this depth of information placed in the hands of the protectors and effectively taught to the security community, a definite edge can be gained on behalf of the defenders in the many battles of the information systems security war. It's encouraging to know that even as this paper is being written, decisions are being drafted and hopefully soon implemented to continue the honeypot avenue of detect and pursue. If honeypots are not used to answer the information security threat, what tool can replace them? This fresh tactic could bring the answer to help close in and trap the monster.

Criminal Hackers Have More Network Control

It is still painfully obvious that cyber criminals are ahead in the Internet war while law enforcement races in the attempt to even the odds. Many hackers operate at an advanced level of knowledge and experience and can determine the presence of a honeypot or other potential trap. Once aware that they have been had, the monster can retaliate and make the hunters pay seriously for attempting to expose their presence, nullify their exploits or stop their advance. Others can take control of the honeypot, assume the compromised system's identity, then use it to attack new victims to leave the true owner of the system with the blame for the attack. They can find many places to hide or stealth their intrusions in the complicated web of hardware, operating systems and applications of a network. The hacker threat is continually the un-caged monster that can avoid capture by the cyber patrol and randomly attack new victims.

Whether blackhats (the criminals), whitehats (the cops) or greyhats (the undecided), professional hackers can avoid detection and take control of systems. From this point, criminal hackers will be referred to as blackhats, the cyber cops as the whitehats, while the undecided will not be categorized until they make up their mind whose side they are on.

Blackhats, in most cases, are too smart to break into a system and allow themselves to become "trapped" without either retaliating with a crippling backlash or slipping through a stealthy escape route. Though very good at what they do, even the best can slip up and make mistakes. Whitehats and blackhats (the primary opponents) are counting on each other to make these mistakes to give the other an advantage. Unlike the script kiddie (Blackhat wanna-be firing off canned scripts randomly), those who are actually being trained in Blackhat technology (next generation cyber criminals) and of course, the certificate

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

seeking security analyst (would be cyber warrior), professional hackers know and have usually carefully planned their activity to include a built in avenue of evasion and escape. They're not the average cyber criminal that attack systems and networks and then flee at the first sign of possible exposure or capture. They demand respect. Some have even attained enough knowledge of systems and exploits that when discovered, attempting to capture them is futile. The worst type, as revealed by Bruce Schneier in his book, "Secrets and Lies", are the Blackhats that break in undetected with ease but if discovered and hindered in their goal can angrily strike back with a vengeance. They not only easily escape capture, but they also retaliate (hack back) and leave the would-be apprehenders broken and discouraged.[4]

Initially, the Whitehat trap setter cannot know the expertise level of the Blackhat that may get caught in their honeypot and could painfully discover that they are in a losing battle with a more advanced and more powerful opponent. It would be awful to finally trap the monster and then find out that the "cage" is not strong enough or has been weakened and will not hold together. In such a case, retaliation by the monster is a very probable option.

A quick note on the script kiddies is in order here. Though ridiculed as infant cyber adolescents and portrayed as more of a nuisance than a threat, they are responsible for the mass volume of probes and attacks on the Internet. They may not have a clue as to the cyber traffic accidents caused across systems and networks worldwide due to their activity but they are a force to be reckoned with and their skills are growing. Also seemingly growing is their attitude of oppression by the law as they follow the teachings of their leaders. One individual identified only as “Mentor” expresses…

“Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.” [5]

He invites what appears as the world of authority that is around him that has neither reason nor care of fair treatment to “enter my world”. The writing is a portrayal of a hacker’s serious view and vow to continue the perceived fight against the law at all costs. He ends the message with a prideful assurance that the fight will rage on even if he gets stopped.

Honeypots may sound like an easy catch for the monster, but there are many cyber villains who can figure out the trap, destroy its purpose or even turn its use against its owners as well as attack other victims. The user of honeypot technology should be keenly aware of the risks involved before implementing it. If a capable foe, the captured individual will not give up without a fight when he/she realizes they’ve been caged. William W. Martin echoes in his System

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Administration and Network Security (SANS) paper these familiar words from the security wise.

"Be ready to pull-the-plug, especially after all has been learned within reason. The goal is to learn how intruders' compromise a system, not to let the intruder use the Honey Pot as his/her tool and cause further damage." [6]

It's a humbling thought to realize that the Blackhats have the upper hand but as the Whitehats gain ground (as with honeypots), they cannot boast of any great victories. The battle for Internet security will be around for a long time with both sides using whatever tool or technology that arises to attempt to maintain a step ahead in the arms race. Even if captured, the monster will escape and again the cyber cops start another leg of the race to catch up with it. To some, this is very frustrating.

Cyber Vigilantes

Some defenders give up on the law. Personal justice becomes attractive to them. Others feel that the legal system cannot handle the threat and see their personal exploits against the enemy as assisting the law. As the Blackhats continually slip through snares, stings and stake outs, some feel that their destruction is more rewarding than their capture. Destruction comes in the form of hack backs to give them a taste of what it feels like to be the victim. CNN.com painted this picture in an old article, which reads…

"If vendor tools are any indication, fighting back may indeed be gathering acceptance in the IT community. Intrusion detection tools, for example, can be configured to reverse attacks. New reactive tools are also popping up in the marketplace, and freeware attack-reversing tools abound on the Web". [7]

At what point does protecting my organizational network against attacks become too aggressive. Since laws are not yet specific and in some cases non-existent, can and should cyber vigilantes be prosecuted? Will the Blackhat (which in this case could be either) expose their activity by suing against a hack back that shut them down? The CNN article mentions only Denial of Services as the return attack, what about viruses, Trojans, worms or probes from the supposedly victim to the attacker. Where does it stop? Another observation is if a return hack was successful but the initial hack was not (just detected), who is the identified victim. The initial attack becomes an attempt or reportable incident that caused no harm due to failure. The return attack becomes an intrusion violating the targeted system or network. While we are tackling these issues, the monster continues its rampage.

It doesn't take much to figure out that administering a personal version of the law will not be justified. There are too many guidelines already in place (laws protecting privacy and liability, regulations for the government, policies of

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

organizations for its personnel and systems) that assist the internet community in finding the line that should not be crossed. Any individual or organization that is willing to put themselves in a strike back position could still be held accountable under law even if the victim does not press any charges. The Internet community frowns on retaliation in any form but frustration is running higher. Corporations lose billions of dollars every year. Security defenders are in some cases stretched to the limit just to keep pace with the cyber threat. Though the pressure is on, taking the matter out of the hands of law enforcement has serious repercussions. The vigilante is not a hero at all. They've taken an easier way out than just abiding in the law. What will happen, if when retaliated against, the attacker is able to escape and inflict greater harm? It would not be very wise to forget that the Blackhats are leading while the rest follow. The great goal of the protector is to defeat the monster, not become one also.

Honeypot Legal Issues

It would seem that no one could argue that it is the right of the owner to safeguard what they own and have worked hard to build or attain. Of course the requirement of the owner would be to use lawful means to protect themselves. As far as honeypots, this is the big question in the legal arena. Are people using honeypots for protection breaking the law? Since this subject is reserved for the court system, by no means can this paper answer such a question. Research shows that before implementing a honeypot or similar tool on any system or network, it would be wise to seek legal counsel first.

Some areas of concern that have arisen with setting a trap for the hacker is that the legal system have not yet defined all the necessary details of the law concerning hacker criminals, hacker vigilantes or the confusing issue of hacker entrapment. Though all categories are considered unlawful activity, laws are still being written to deal with them.

With such a powerful tool (or weapon), why shouldn't cyber law enforcers us honeypots to catch the criminals? Responses in support of and against this question flow as the legal system ponders an answer. Lance Spitzner quiets some of the commotion with a recent article, "Honeypots: Are They Illegal?" The article points out three areas of legal concern as quoted. "Without cases directly on point, we are left trying to predict, based on cases in other contexts, how courts will treat honeypots. Until a judge gives a court order, we will really never know. With honeypots, there are three main issues that are commonly discussed: entrapment, privacy, and liability" [8]. He sums up the article with some suggestions and opinions concerning the legality of honeypots and defends their use. His defense is that honeypots are not tools for Internet criminal entrapment, but instruments for organizational protection against the threat of the monster as well as against legal liability if systems are compromised and misused.

Summary

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

This paper is an observation of the honeypot, its effect (and potential future effect against the Blackhat community. Honeypot use has expanded from a defensive network protection tool to an offensive weapon to track and apprehend Blackhats. Considered a breakthrough in Internet control technology, the honeypot could be the long awaited answer to gaining ground against attacks. Styled as a monster, the Blackhats are leading the way, while the Whitehats struggle to keep up in the race. Behind in the struggle, some defenders have taken matters into their own hands. Like cyber vigilantes, they go after the Blackhats themselves apart from the law. Though holding ground for now, the justice system must make some adjustments to cover the arena of cyber crime. Laws will have to be written and rewritten to ensure that the line between what is lawful and what is not is kept clear.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References:

1) Lance Spitzner, Marty Roesch and David Dittrich "Honeypots: Definition and Value of Honeypots"
URL: http://www.tracking-hackers.com/papers/honeypots.html
Last Accessed July 4, 2003

2) Marcus J. Ranum, “Forward: Giving The Hackers A Kick Where It Hurts”
"Honeypots: Tracking Hackers"
URL: http://www.tracking-hackers.com/book/forward.pdf
Last Accessed July 4, 2003

3) Toby Miller, “Intelligence Gathering: Watching a Honeypot At Work”
URL: http://securityfocus.com/infocus/1656
Last Accessed July 4, 2003

4) Bruce Schneier book, "Secrets and Lies"

5) Mentor, "The Conscience of a Hacker"
URL: http://www.geocities.com/carail666
Last Accessed July 4, 2003

6) William W. Martin, "Honeypots and Honeynets: Security Through Deception"
CISSP, SANS Practical Exam Paper
URL: http://www.sans.org/rr/papers/4/41.pdf
Last Accessed July 4, 2003

7) Lance Spitzner, “Honeypots: Are They Legal?”
URL: http://www.securityfocus.com/infocus/1703
Last Accessed July 4, 2003

8) CNN.com article, “Can You Hack Back?”
URL: http://www.cnn.com/2000/TECH/computing/06/01/hack.back.idg
Last Accessed July 4, 2003

© SANS Institute 2003, Author retains full rights.