Honeypots: Using deception to strengthen Cyber Security

As many computer science majors are familiar with, “if you know the enemy and you know yourself, you need not fear the result of a hundred battles. If you know yourself, but not the enemy, for every victory gained you will also suffer a defeat.” (Sun Tzu "A Quote from The Art of War") Honeypots are a computer security resource that allow you to detect network intrusions and learn information about your enemy. Whether for professional or personal use, we all have digital devices and information and communication we want to secure and kept private. Securing information and communication has been a long sought-after struggle dating back to early civilizations. With technological advances into the digital age securing that information has become increasingly sophisticated as each means to protect it has been defeated. In the digital era most, digital devices are connected to a network and to the internet. Throughout my experience as a computer security major and my personal life, I have seen how important it is to protect and secure your data. I have also learned how important it is to know when your network has been intruded and knowing about your attacker. Honey pots allow us to detect an attacker in your network and give us a jump start on the road to response and recovery. To understand this topic, I will discuss the current relevance and status of the topic, background information and history of the topic, and future implications and relevance of the topic. To develop a strong understanding of what honeypots are it is best to look at the current relevance and status of this topic.

To learn more about honeypots and where they are used, we will look at where the technology is at presently. In his book, Intrusion Detection Honeypots, Chris Sanders defines Honeypots as “a security resource whose value lies in being probed, attacked, or compromised.” (Sanders, 21) In class, we defined Honeypots as “Decoy computer system for trapping hackers or tracking unconventional or new hacking methods” (1410_L41, 3) Honeypots are essentially

exactly as they sound; they are traps that disguise their true nature and with the intent of luring unsuspecting individuals in. There are two primary goals of honeypots which are to discover network intrusions and learn more about your attacker. The author discusses three main types of honey pots which are honey systems, honey services, and honey tokens. (Sanders, 22) These three different types of honey pots provide a large amount of versatility and customization in how you implement honeypots within your network ecosystem. The author talks about how, "A honey system mimics interaction of an operating system and the services it provides." (Sanders, 22) An example would be a honeypot system that emulates windows. On the other hand, "A honey service mimics the interaction of a specific software or protocol function." An example of a honey service is a honeypot that mirrors the SSH protocol. (Sanders, 22) Lastly, "A honey token mimics legitimate data." (Sanders, 22) Word documents are examples of honey tokens. Each of these styles of honeypots have different advantages and disadvantages which primarily take the form of interactivity and risk. More complex honeypots offer more complex interaction but present more overhead and greater risk for being turned against the defender. There are also a large variety of different free and open-source honeypot tools available to download and use on the internet. The author mentions, "As of this writing, I count over 80 different free honeypot tools focused across a broad spectrum of systems and services." (Sanders, 20) Some of the examples the author includes are Cowrie, Conpot, Dionaea, RDPy, Open Canary, Glastopf, and HoneyPress. (Sanders, 20) Now that we know the basics of what a honeypot is you might be wondering why we would want to use something like this.

In class we learned, "There is no absolute protection against cyber-attack. Not even separating yourself from the Internet." (0625_L18, 2) We also learned that "it is only a matter of "when", not "if" a cyber-attack will succeed." (0625_L18, 5) In his book, the author also

discusses this and mentions that “No matter how deliberate your efforts, an attacker who is relentlessly motivated or resourced will eventually gain access to a device on your network. Therefore, you should deploy detection mechanisms to aid in investigating and responding to attacks as quickly as possible” (Sanders, 4) As discussed previously, a Honeypot is a security resource that provides you a means of detecting an intruder within your network. It accomplishes this by mimicking a system, service, or data. Knowing when your network has been breached is an important step in computer security. In class we learned “There are only two types of systems: Those that have been hacked and those that don’t know they’ve been hacked.” (515_L15, 21) We also learned “That is why today the first and last line of cyber defense rests with system owners and operators” (515_L15, 15) This means it is on us to ensure our systems are secure and know when we have been a target of a cyber-attack. When it comes to learning about the attacker honeypots use logging to keep track of all commands that are used when an attacker accesses a honeypot. In many honeypots everything the attacker interacts with and sees is all fabricated by the defender and does not exist. Honeypots can log how an attacker interacts with it, then send that information to an offsite log aggregator. Another important topic to discuss regarding honeypots is the common misconceptions regarding this technology.

One common misconception that the author discusses is we do not loose once an attacker gains access to our network. The book mentions, “You don’t lose when one of your users clicks a link in a phishing e-mail or when an attacker harvests VPN credentials with drive-by malware. You lose when an attacker exfiltrates intellectual property or scrapes thousands of credit card numbers form memory or point-of-sale terminals.” (Sanders, 4) Despite that there is no perfect defense, and a determined attacker will gain access to a network, all hope is not lost. The defender only loses when the attacker accomplishes one or more of their objectives. Which

means after initial detection there is still a chance to respond and recover. This is like a topic we covered in class which is that “measures taken to identify, protect, detect, and respond to cyber-attack can only ever be partially effective. On the hand, the mans for recovery are completely within your control.” (0625_L18, 9) However, if we can detect an intrusion than we can start the road towards response and recovery. In his book the author mentions, “Attackers have objectives, and defenders typically don’t lose until an attacker accomplishes one or more of them… It’s in that particular space between initial access and completed objectives where you have the most significant opportunity for detection and response before the attacker causes substantial damage.” (Sanders, 4) One other concern that many bring up regarding honeypots is what if the attacker determines it is a honeypot. The author diffuses this by mentioning, “By the time the attacker discovers they’re interacting with a honeypot, you are already hot on their trail. If you’re able to provide more layers of deception and interaction to learn about the attacker’s tradecraft, that’s a positive. But it’s certainly not required to achieve the primary benefit of detection honeypots.” (Sanders, 39-40) This concept again comes back to the idea that detection gives the defender the ability to prevent significant damage or losses from occurring. Another common concern about honeypots is that they can be turned against the defender and require to much maintenance. However, there are a variety of honeypots that meet different uses. This gives system administrators the ability to find a honeypot that fits their needs and is maintainable given their constraints. Using honeypots with less interactivity still provides the benefits of the technology while also requiring less maintenance and concern for potential issues arising. The next step toward understanding this topic is moving to the history of how this technology arose.

Now that we understand basics of what a honeypot is and the current state of them, we can investigate the history of honeypots to gain a better understanding of this topic. One of the

first ever recorded implementations of a honeypot was by an astronomer named Cliff Stoll at the Lawrence Berkeley Laboratory in California. (Sanders, 10) Cliff had noticed 75 cents worth of computer time was missing but could not attribute it to one specific user. (Sanders, 10) He then observed the type of data the attacker had been searching for and created a fake missile defense project named SDINET and painstakingly drafted a trove of false documents to make it look like the real deal. (Sanders, 11) The author then continued to talk about how the attacker found the documents and spend hours accessing the files which allowed them to trace the source of the attacker. (Sanders, 11) This is a great example because it shows how the defender was able to create fake data and use that to lure the attacker to stay on the network. This bought the defender time and allowed him take steps towards determining his identity. Another early use of a honeypot was in 1991 when a technical staff member at AT&T's Bell Labs set up a series of custom-built fake service honeypots on their outward-facing internet gateway. (Sanders, 12) This individual was able to redirect the attacker into a carefully constructed "jailed" environment where they could execute a limited number of commands while not causing any immediate harm. (Sanders, 12) The defender, Bill, was then able to monitor the attacker for a while and learn about their tactics and what vulnerabilities they went after. (Sanders, 12) This example shows how the defender was able to learn about the tactics and methods of the attacker. It also shows how the defender was able to deceive the attacker and lure him into a digital space where he could do no harm. Another important part to investigate regarding the history of honeypots is early honeypot tools.

One of the earliest honeypot technologies was Fred Cohen's Deception Toolkit (DTK). (Sanders, 16) The benefit of this toolkit is that "DTK could be installed on a system and configured to make the system appear as though it was vulnerable to one or more attacks."

(Sanders, 16) The author further explains that “An attacker then probes the system, discovers the vulnerabilities, and attempts to attack it. DTK doesn’t allow the attack to succeed, but it logs the attempt along with the source and payload of the attack.” (Sanders, 16) This was a great tool for determining how an attacker would approach a vulnerability. Another early honeypot tool was CyberCop sting which was developed by Network Associates and released in 1999. (Sanders, 17) “CyberCop sting ran on Windows NT server and could simulate an entire network segment, including routers and hosts running various platforms and services.” (Sanders, 17) Another important early honeypot software was Honeyd, which was created by Neil Provos in 2003 as a free and open-source honeypot Swiss Army knife. (Sanders, 18) “It was a self-contained package that ran on Windows and Unix-based systems that was easy to use and incredibly flexible…” (Sanders, 18) The author discussed how “One particularly useful feature of Honeyd was its ability to mirror specific operating system versions…” (Sanders, 19) This means you could use Honeyd mimic a Linux or windows system and make it appear to be a real system. One of the reasons this software was so popular is because “it was so flexible that it allowed users to deploy honeypots within minutes, bringing theoretical honeypots into immediate reality.” (Sanders, 19) Scalability is an important factor for companies and helps to make this technology more accessible. To understand how we can move forward with honeypots, we must look at the future implications and relevance of this topic.

Now that we understand the past and the current use of honeypots, we will look at the future potential for this technology. There are three main uses for honeypots that make this a valuable technology. These uses are intrusion detection, technique and proliferation research, and resource exhaustion. (Sanders, 31) Intrusion detection honeypots are situated within your network and are used for detection to determine if an attacker has compromised the network.

These types of honeypots can take the form of a system, service or data, but one that is more closely observed than others. (Sanders, 32) The book talks about how, “While it isn’t feasible to alert on every access to a legitimate production server due to the volume of connections, alerting on any interaction with a honeypot is perfectly manageable. There shouldn’t be anything else happening there.” (Sander, 33) This is important because it makes network intrusion honeypots more reliable and more feasible. The overhead and maintenance of alerting on every server is not reasonable but detecting accesses on a honeypot is. The second type of honey pots are proliferation research honeypots. These honeypots are not used for network defense and are instead are used for learning about methods of attackers. These types of honeypots are placed outside of the network. “If a research honeypot is successful at eliciting attacks, you’ll be rewarded with examples of tools and techniques used to exploit the services you’ve exposed.” (Sanders, 35) These are used by the government and research organizations to gather data on attackers. An example is a company would like to know what kind of people go after their intellectual property and the methods the attacker uses to accomplish that. The third type of honeypots are resource exhaustion honeypots which essentially are focused on slowing down the attacker. “The goal is for these honeypots to waste as much of the attacker’s time as possible by deploying a large number of honeypots that allow enough interaction to appear real and keep the bad guys interested” (Sanders, 37) Another added benefit, “It can also buy time for defenders to identify, contain, and eradicate the attacker before they do more damage.” (Sanders, 38) These types of honeypots are a great way to slow the attacker down to buy the defender more time to respond and recover from network intrusions. Resource Exhaustion honeypots also allow network defenders to waste the attackers time which in some cases can deter and discourage an attacker. One might ask with how useful this technology is, why is it not used more?

The main reason Honeypots are not as common as you would think they would be despite the capabilities of this technology is because there is not much public information about the topic. The author sheds some lite on this subject, “I believe the inherent deception honeypots rely on has also hampered their adoption, simply because there aren’t many public stories about how people use them successfully on their networks, particularly for detection purposes.” (Sanders, 15) He also mentions that “Alas, my research suggests that some, particularly those who excel at secrecy, have continually used detection honeypots for quite some time.” (Sanders, 15) Some examples the author gives is the us government, foreign government, and corporations. He also mentions that “The secrecy surrounding honeypot operations ensures we’ll likely never hear the specific success stories of how practitioners used honeypot technology in some environments. But like many other facets of cyber security, the ideas that spawned them eventually matriculate out into the public domain.” (Sanders, 15) This suggests that honeypots will become more popular over time as more success stories and public information is released regarding the topic. Another issue is many people may not want to openly admit the use honeypots for network defense. For example, for obvious safety and security reasons the government is not going to reveal its tactics to the public for cyber security. Chances are an organization would not either. However, as we have discussed, this does not mean this tool is not useful nor does it not mean it is not being used already.

It is likely Honeypot technology will continue to expand and evolve as time progresses. By being early adopters, we can utilize this technology to strengthen our network defense and security. We can also learn more about hacking and tactics used to exploit vulnerabilities. Honey pots have a wide variety of use for security purposes. It gives us the ability to detect network intrusions with minimal overhead, learn more about who will go after online resources and

common types and techniques used in cyber-attacks, as well as implement means of slowing attackers down in accomplishing their goals. The foreknowledge of attacks allows system administrators to respond and recover from attacks quicker and before significant damage is done. Regarding the detection tool kit previously mentioned, the author talks about how the creator believed using this software could make the internet safer. He wrote, “If one person uses, DTK, they can see attacks coming well ahead of time. If a few others start using it, we will probably exhaust the attackers and they will go somewhere else to run their attacks. If a lot of people use DTK, the attackers will find that they need to spend 100 times the effort to break into systems and that they have a high risk of detection well before their attempts succeed. If enough people adopt DTK and work together to keep it’s [sic] deceptions up to date, we will eliminate all but the most sophisticated attackers, and all the copy-cat attacks will be detected soon after they are released to the wide hacking community.” (Sanders 15-16) The reason this quote is so powerful is because it shows how using just one tool could make an impact for every person who uses it and what the potential outcome could be. I share the belief that adopting honeypots is one small step we can take to make our networks safer, deter cybercrime, and make the internet safer.

Throughout this paper I discussed the current relevance and status of the topic, background information and history of the topic, and future implications and relevance of the topic. Whether it be private, commercial, government, or a cooperate network, honeypots can be used to detect and learn more about your enemy. We have learned that we cannot get over the cyber security issue nor can we mount a perfect defense against cyber-attacks. Our only choice is to continue to innovate and do what we can to respond and recover to cyber-attacks. Being a part of the Bachelors of Innovation has shown me the impact of innovative ideas, which made this subject interesting for me. I also find that mounting an active defense is an intriguing and

appealing concept in cyber security. New ideas are one of the best ways we can improve security. With the internet being a critical infrastructure itself, we know that cybersecurity plays a large part in Homeland Security as well. Many critical infrastructures also rely on internet connectivity and computer systems which also make them vulnerable to attacks. The great thing about honeypots is they can be deployed in virtually any network and are scalable and customizable to fit the needs of any company or organization. Honeypots can be used to defend networks and therefore protect our critical infrastructure. By implementing innovative ideas and technologies such as these, perhaps one day we can make the internet safer for everyone and end the growth industry of cybercrime.

Works Cited

"A Quote from The Art of War." *Goodreads*, Goodreads, www.goodreads.com/quotes/17976-if-you-know-the-enemy-and-know-yourself-you-need.

"Online Lectures 15, 18, 41." Homeland Security & Cyber Security. Homeland Security & Cyber Security, 2020, Colorado Springs, University of Colorado Colorado Springs.

Sanders, Chris. *Intrusion Detection Honeypots: Detection through Deception*. Chris Sanders, 2020.