Honeypots: Using Clones to take back from Hackers

Charles J. Guarino

Coastal Carolina University

Author Note:

Made for CSCI – 385 Introduction to Information Systems Security

Professor Corey Nance

Honeypots: Using Clones to take back from Hackers

Honeypots

In the infinite world of computer technology, threats are discovered every day and the patches that go along with them. As time goes on technology continues to grow. But with technology growing so does the danger and importance of computer security. At a time the only ways to decipher where and how an attacker got into a system was after the attack happened and reviewing the system for hours until stumbling across a way to get in yourself. Almost a generation later, we now have honeypots. When we hear the word honeypot we might refer to a beehive or maybe even [1]Whinnie the Pooh but in the computer world we have to think of a bear being lured in by honey. Honeypots are the defense systems that are made to either attract attackers by providing attractive and vulnerable resources or to divert their path from their attack target (Tiwari 2012). So why would a white hat hacker set a computer up with vulnerabilities on purpose? These systems are used in various ways and clone the real systems only with false information not only to mislead the hacker but also to learn from the hacker. Honeypots are used all the way from government hacking, to individual business hacking and even personal use. No matter who you are and what you do, a honeypot can prove to be useful to a person for many different reasons.

Honeypots were invented in 1999 by the Honeynet Project; a non-profit organization set up with the interest of monitoring and documenting attacks all over the world in order to benefit computer security (Shuja 2019). At that time, their honeypot wasn't seen as something that could be widely used by everyone and was only used to monitor the hacks of their choosing. As time

advanced, more and more companies gave in to the widespread use of honeypots. And although the honeypot is still in it's early years, they've become one of the most prominent ways for security analysts to learn about the new attacks hackers are coming up with. Many people ask the question if honeypots are just a learning tool or if they actually do keep a system safer. It is clear that there is no method honeypots use that can keep a hacker from breaking in to the actual system, but they can lure the attackers towards the fake, evidently drawing them away from the actual system.

Implementation

So far we learned what a honeypot is, but not exactly how to set one up. It's obvious that if you're skilled enough in the programming field, you could code and execute your own but it could be very costly and tedious. Thankfully, there are now many companies that allow you to download or purchase one on your own. And reluctantly, many of these companies are open source and allow their honeypots to be downloaded free of charge. Software such as Cowrie, Honeything, ElasticHoney, Thug and Honeydrive are all open-source honeypots available for various different platforms and software. Cowrie is a SSH honeypot that acts as a honeypot on a networking level, Honeything is a honeypot that deploys on the internet for website-level mimicking, ElasticHoney is used to mimic software at the database level, and HoneyDrive is a bundle that acts as an all in one for various different levels of security. (Ion 2012)

Since HoneyDrive is an all in one we're going to dissect what you can get for free with its package. To start, HoneyDrive comes with Dionea, which is an alternative to Cowrie, as well as Honeyd, Thug, Amun, and ElasticHoney. So you get all the needs for setting up the honeypot's network, systems, data and browsers all in one [2].OVA file. Now once you acquire these files, all you would have to do is set them up on your virtual machine then tweak the

machine to your personal, but fake standards and the different honeypots do the rest. You would set up the honeypots judging by what you think the hackers are trying to target. You then have a fake machine with vulnerabilities that can lure a hacker snooping around your systems. Since the machine is fake, it is considered a low-interaction honeypot. In general, there are two levels of honeypots: high and low. A low-interaction honeypot is what we see here; a honeypot that is run through a virtual machine and can only be faked to a certain extent. A high-interaction honeypot is a honeypot that isn't actually run on a machine at all because; well, it is the machine itself. These honeypots are typically used at the government or large business level for victims that may have very serious problems that can affect a lot of people or they are used for employee training. Though it is possible for a person to go out, personally buy a computer and download these packages, it does get costly and at some point useless to have if you aren't a large target at home.

Analyzing Honeypots

Although honeypots may lure hackers away from systems, the overall goal and point of them is not only to be able to learn the hackers methods, but their motives as well. Once a hacker gets in, they might tweak a few settings, manipulate a few files, or browse the web. From there we can learn their overall goal and see what it is they are looking for. This is the goal of most companies who want to know why they have hackers breaking into their systems in the first place.

Lets revert back to HoneyDrive again to see what tools they have to offer for analyzing these honeypots for educational purposes. On [3]SourceForge.com they list the analyzing tools in their software features by stating: "HoneyDrive comes equipped with A full suite of security, forensics and anti-malware tools for network monitoring, malicious shellcode and PDF analysis,

such as ntop, p0f, EtherApe, nmap, DFF, Wireshark, Recon-ng, ClamAV, ettercap, MASTIFF, Automater, UPX, pdftk, Flasm, Yara, Viper, pdf-parser, Pyew, Radare2, dex2jar and more" (Ikoniaris 2014). To dive in a little deeper, ntop is software that monitors your network just like a task manager monitors your processes. Similarly, p0f is a network monitor and TCP/IP stack-fingerprinting tool specifically for virtual machines. EtherApe maps network traffic in order to see where the most traffic is entering and leaving from and WireShark is an all-in-one for network traffic. Recon-ng is a web reconnaissance tool used on the Internet and Ettercap is used specifically for man-in-the-middle attacks. Radare2 is a command line utility used for analyzing binaries and dex2jar is a tool for analyzing java files. Lastly, ClamAV, MASTIFF, Vipre, Pyew and Yara are general protection softwares for identifying and tracking malware depending on what attacks are being used.

On top of all these tools running at the same time, it is not difficult to record a virtual machine when the system is running. From there you can see what the attacker is physically doing on your desktop, on the web, or with your files without risking anything valuable. This information gets poured out to the host computer and you are then able to further defend your real systems from that specific hacker and the penetrations they carried out.

Hacking Origin

It's always a question why and how there are constantly so many hackers trying to get into different sites. How would they ever know when a new honeypot is even deployed? How do these hackers find all these vulnerable sites? They must have knowledge that they are vulnerable in order to be "attracted" to them in the first place. John P. John, Security Analyst at The University of Washington describes how attackers find vulnerable servers in his WWW Conference article by stating:

> "Attackers often use two methods to find vulnerable Web servers. The first is to perform brute-force port scanning on the Internet, and the second is to make use of Internet search engines. It is reported that vulnerable Web servers are compromised immediately after a Web search reveals their underlying software. For example, a query phpiz- abi v0.848b c1 hfp1 to a search engine will return to the attacker a list of Web sites that have a known [4]PHP vulnerability. Because of the convenience of this approach, many attackers adopt it, and our system is designed to attract such attackers." (John 2011).

Furthermore, the security team at UW teamed up with Microsoft Security Technicians to create their honeypot. Although they knew a state university network would be a haven for hackers, they were shocked when they realized they had over 6,000 different machines attempting hacks:

> **"**We implement and deploy our heat-seeking honeypot under a personal home page at the University of Washington. Despite its relatively obscure location, during the three months of operation it attracted more than 31,000 attacker visits from 6,000 distinct IP address. In comparison to a setup where real vulnerable applications are installed, our honeypot pages get a similar amount of traffic, albeit at a much lower setup cost. We observe a wide variety of attacks including password guesses, software installation attempts, SQL-injection attacks, remote file inclusion attacks, and cross-site scripting (XSS) attacks." (John 2011).

Knowing how many hackers attempted to get into a university network can turn the eye of a lot of security analysts because it is a scary thought knowing how many people could potentially want to cause harm to a university. Without these honeypots, the UW would have no idea what the motives of all these hackers was and from that they can see how they can limit the amount of intrusions and make a safer environment for their students.

Governments and Big Business

Despite the fact that a University can be targeted heavily, overall it still cannot cause physical harm to anyone. However there are many ways hackers can get into much more serious systems and recently we've been seeing that throughout the world. Just recently there were several attacks on U.S. electric, oil and gas sites. These may seem like no physical harm at first but think about colder places in the U.S. not having power or heat. Furthermore, nuclear control

stations, air traffic control centers, and military bases are all susceptible to these same attacks. Just last year the FBI, Department of Homeland Security and the [5]NCSC deployed a honeypot through [6]Cybereason for a major electrical company. They had hackers from all nations hop onto the clone and showcase their skills. They learned that one specific hacker had taken the honeypot and sold it on the [7]dark web with the honeypots network identifiers stating that it could control that companies industrial control systems. Although it was a honeypot and the control systems didn't actually control anything at all, Cybereason stated that the hackers seemed familiar with the control systems by moving quickly through the software. The Department of Homeland Security noted that with the information these hackers knew, had they gotten into the real system they could have control the operational technology where they could actually control who gets gas, electricity and even water (O'Flaherty 2018).

In big business such as social media, thousands of attacks happen every day on the larger companies because of how valuable their assets are despite not having as crucial of security resources as a government does. A company called [8]ZeroFox launched a [9]Honeynet on social media sites to catch hackers in social engineering reconnaissance attacks. With these attacks, they actually aren't hacks at all. Because large social media sites have now become a platform for jobs, they've seen many company impersonators rise to try to obtain information from potential employees and charge them an application fee. ZeroFox created the accounts in a honeypot to ensure their systems safety, then interacted with the impersonators. From there they examined the goal of their attacks, compared them and then put together the motive resulting in the social media companies banning these accounts (Francis 2017).

The Future

As honeypot technology continues to grow, so will the hackers who see them as vulnerable. But the more honeypots get implemented throughout the world, the less likely hackers will care to break into these systems. Judging by the scenario with Cybereason, someone broke in and sold what they thought was ICS controlling software on the dark web when the software actually was a honeypot. If every business had these honeypots set up, there would be false alarms everywhere and hackers would never know whether they have broken into real or fake systems. With that being said, honeypots are still in its early years and some honeypots may be easily noticeable. And if a hacker recognizes a system as a honeypot, they would be able to mislead the security analysts in the wrong direction. The tradeoffs can go on forever but as far as technology appears today, Honeypots have done nothing but good for the people who care about the virtual security of our everyday lives.

References

Francis, Ryan. 2017. Honeypot Catches Social Engineering Scams on Social Media. CSO. https://www.csoonline.com/article/3177458/honeypot-catches-social-engineering-scams-on-social-media.html

HoneyPotsRUs. 2012. Chinese Hacker Caught in a Honeypot. https://www.youtube.com/watch?v=gsytGk9kqbQ.

Ikoniaris. 2014. HoneyDrive. Source Forge. https://sourceforge.net/projects/honeydrive/.

Ion. 2012. HoneyDrive. Brute Force Labs. https://bruteforcelab.com/honeydrive.

John, John. 2011. Heat-seeking Honeypots: Design and Experience. WWW '11. ACM Digital Library.

Mohammadzadeh. Hamid. 2013. Evolution of Fingerprinting Techniques and a Windows-based Dynamic Honeypot. AISCII. ACM Digital Library.

Mokube. Iyatiti. 2007. Honeypots: Concepts, Approaches, and Challenges. ACM. ACM Digital Library.

O'Flaherty, Kate. 2018. This is what wappened when Security Researchers Placed a CNI-Based Honeypot on the Dark Web. Forbes. https://www.forbes.com/sites/kateoflahertyuk/2018/09/06/this-is-what-happened-when-security-researchers-placed-a-cni-based-honeypot-on-the-dark-web/#4dd390792312

Shuja, Faiz. 2019. About The HoneyNet Project. The HoneyNet Project. https://www.honeynet.org/about

Tiwari, Ritu. 2012. Improving Network Security and Design Using Honeypots. CUBE '12. ACM Digital Library.

Footnotes

[1] Whinnie The Pooh: Fictional Disney character that loves honey.
[2] .OVA file: Virtual Machine File.
[3] SourceForge.com: Website for various downloads.
[4] PHP: Hypertext Pre-Processor Language
[5] NCSC: National Cyber Security Centre
[6] Cybereason: Security Company Specializing in endpoint detection.
[7] Dark Web: Portion of the internet that requires specific software for access.
[8] ZeroFox: Cybersecurity company specializing in cloud based security for social medias.
[9] Honeynet: Group of multiple honeypots working together