Honeypot

av

Pål

IKT 207

Cybersikkerhet

Veiledet av

Sigurd Kristian Brinch

Fakultet for teknologi og realfag

Universitetet i Agder

Grimstad, September 2020

What is a honyepot? When i hear the word honeypot the first thing that comes to mind is Winnie the pooh. Since this is a computer class i guess Winnie has nothing to do with it. Therefor we will take a deeper look at honeypot. What is it? What is it used for?

Honeypot comes from espionage, where a spy lure their target in a honeytrap whether that is through romance or compromising information and then uses that to blackmail them for all the informastion they have. In computer security it works similarly. You lure a hacker with a sacrificial system that will mimic a target hackers often try to access. When the hacker try to penetrat this honeypot, it will start to collect informastion about him/her.[3]

On the outside a honeypot looks like your private/company network. which in turn you will monitor all traffic in that system, and by doing so you will learn where the hackers are comming from, how they operate, and what they want. You can also view if your security measures are actaully working and which one needs improvment. [4] The reason you will monitor this netwok is because it's a isolated netwok and there is no reason to access it, therefore all access to this netwok should be viewed as a hostil intruder.[5]

There is to main type of honeypots: Reaserch and produtcion. Reaserch honeypot is created to preform a close analysis off hackers activity and is intended to learn how hackers develop and progress so they can find a better way to protect system against them.

Production honeypots are inside a production network alongside production servers. This honeypot appears real and it will contain information so it can attract and occupy attackers, so the administrator have time to discover and close possible weaknesses in their system.[5]

There are also several different way to implement a honeypot: Email traps, Decoy database, Malware honeypot and Spider honeypot.[3]

We also got three levels off honeypots based on theire credibility, intelligent and purpous: pure, low- and high interaction honeypots.

- Pure honeypots: Is a full production system where the entire system is a honeypot, which are connected to the rest of the network. This is the most authentic honeypot, but carries the most risk. [1]
- Low interaction honeypots: are very basic and will imitate system that is frequently attacked. They will give an oppertunity to collect data from blind attack such as botnet and worms. [2]
- High interaction honeypots: This is a complex honeypot that act like a real system. The purpose with this honeypot is to occupy as much of the hackers time and resources, which in turn give you plenty of information about them and their intention. [3]

Although honeypot has alot of pros, there is also some huge cons about them. They only will be able to collect information when someone try or already have accessed them. So even if a company have a honeypot/honeynet implemented in their system, they can never really trust that no one have accessed their system. Another problem is that the most believable honeypots is that they are hard to implement and resource heavy. Becaus of that pure honeypot might not be wise if you don't have the right expertise, if they are incorrectly configure they can act as a gateway to other systems or networks. Even tho you have a belivable honeypot more experienced hacker will be able to find out about the honeypot and may turn their sight to another area on the network. [5]

References

[1] Emily Green. *What is a honeypot?* Oct 01, 2019. URL: `https://nordvpn.com/no/blog/what-is-a-honeypot/`.

[2] Imperva. *Honeypot.* read 04.09.2020. URL: `https://www.imperva.com/learn/application-security/honeypot-honeynet/`.

[3] kaspersky. *What is a honeypot?* read 04.09.2020. URL: `https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot`.

[4] Written by a NortonLifeLock employee. *What is a honeypot? How it can lure cyberattackers.* read 04.09.2020. URL: `https://us.norton.com/internetsecurity-iot-what-is-a-honeypot.html`.

[5] Margaret Rouse. *honeypot (computing)*. October 2018. URL: https://searchsecurity.techtarget.com/definition/honey-pot.