Research Proposal Form

Name and Surname:

Ryan Cortis

MCAST Email:

ryan.cortis.b42697@mcast.edu.mt

Group:

6.1A

Research Title:

Honeypot Driven Access Control Rules: A Proof of Concept

Hypothesis and/or Research Questions:

Research Question:

Are honeypots an effective security solution for enterprises?
Are honeypots tricky to implement?

Hypothesis:

It is hypothesised that honeypots are an effective security tool. As they are highly monitored computer systems designed to deceive attackers and are used to learn, how and what types of attacks where attempted on the system. They also waste an attacker's time by having to go around the honeypot instead of going after systems which have real data, ultimately deterring attackers and giving system administrators time to act and put in place necessary measurements to counteract any future security breaches.

Honeypots are also tricky to implement because they are designed to mimic a real system as much as possible therefore implementing a honeypot will be very time consuming to both implement and maintain.

Outline of Key Literature:

A honeypot is a security tool setup on a computer system which is used to mimic a real system and used to detect attacks and log them or deflect them from a legitimate target. Its value lies in the unauthorised use of the system and any interaction with the honeypot is considered to be malicious intent. While honeypots do not solve a security problem, they can still be helpful as information captured from the honeypot can be used to help a system administrator to enhance the security of their systems and networks. (Anon, 2018)

Various configurations of honeypots exist but these can be classified into two main types: Production and Research.

Production honeypots are typically low interaction honeypots which have little to no interaction with attackers and mostly serve as an early warning system. These types of honeypots are of little purpose, apart from capturing data. Which in essence makes them a basic event log system that can't be interacted with but are easy to deploy and maintain across different segments of the network. (Tsikerdekis, 2018)

Research honeypots are deployed by security researchers and their goal is to learn tactics, tools and techniques of the hackers exploiting the network and its computer systems. This type of honeypot is a step ahead of production honeypots and give complete freedom to the attacker and is designed to detect and log information without letting the attacker figure out that it's a honeypot. Researchers then share the findings with network and system administrators, anti-virus vendors and system programmers in order for them to patch or update their systems against any security risks. This is effective at acting as an early warning system for 0-day exploits. (Lakhani, n.d.)

Overview of Methodology:

For the purpose of answering the research questions and proving my hypothesis two types of honeypots will be deployed and tested upon in order to gather information regarding on how each type of honeypot functions. A Production Honeypot (Low Interaction Honeypot) and a Research Honeypot (High Interaction honeypot) which both can be found distributed on the internet by vendors as open source software.

First, a low interaction honeypot will be deployed. This type of honeypot will be easy to deploy and maintain but has limited interaction capabilities. As such it will be setup for the simple purpose of listening in on a specific port in order to detect any unauthorised intrusions on the port. Such intrusions will then be logged and analysed in order to get an insight on what is happening from both the attacker and the system administrators' side.

A high interaction honeypot will also be deployed. This type of honeypot is generally designed to mimic a real system as much as possible in order to give freedom to the attacker to explore the system whilst hiding the fact that it is a honeypot. Therefore, this setup will be more time consuming as all actions taken by the attacker will need to be logged into greater detail.

For the purpose of testing, both honeypots will be deployed on virtual machines which will be running either a Linux or a windows server operating system and have network monitoring software to log steps taken by the attacker.

The use of the aforementioned implementations will help provide the means of evaluating and proving the hypothesis. As through the setup and implementation stage of the honeypots, it will be determined whether honeypots are tricky to implement. After, the honeypots have been setup and implemented. Through logging and testing the honeypots in various ways that an attacker might go about traversing the honeypot, will help determine whether honeypots are an effective security solution for enterprises.

Ethical Considerations:

In order to test, virtual machines will be used. Using virtual machines will cause no harm to any other system or network as they will be completely walled off and all tests will be simulations of how an attacker could potentially traverse the system.

No confidential data will be used for the tests and all tests attempted on the system will be planned and logged.

References:

Anon., 2018. *Analysis of Honeynets and Honeypots for Security.* [online]. Available at: <https://www.ukdiss.com/examples/honeynet.php?vref=1> [Accessed 12 March 2020].

Tsikerdekis, M., 2018. *Approaches For Preventing Honeypot Detection And Compromise*. [online] Research Gate. Available at:

<https://www.researchgate.net/publication/328430317_Approaches_for_Preventing_Honeypot_Detection_and_Compromise> [Accessed 13 March 2020].

Lakhani, A., n.d. *Deception Techniques Using Honeypots*. [online] Isg.rhul.ac.uk. Available at: <https://www.isg.rhul.ac.uk/~pnai166/thesis.pdf> [Accessed 13 March 2020].