Virtual Machine Introspection Based SSH Honeypot

Stewart Sentanoe Benjamin Taubmann Hans P. Reiser

Universität Passau

sentanoe@fim.uni-passau.de, {bt,hr}@sec.uni-passau.de

1. Problem statement

Many companies implement intrusion detection systems (IDS) to get alerts whenever malicious activities occur. An IDS is relying either on anomaly detection based on dynamically learning user's activities or uses a database of known attacks. To enhance this database, we need to be able to learn more about new kind of malicious activities. To achieve that, we can use a honeypot system.

The problem with current SSH honeypot implementations is that they can be detected easily by an adversary because they support only a limited set of functionality. Thus, attackers can stop further steps in order to prevent the analysis. Cowrie for example is a SSH honeypot which emulates a Linux system. It does not provide access to a real system but it only behaves like normal system with a limited set of commands [3].

2. Goals

Our goal is to make a SSH honeypot with the following properties. First of all, an attacker should not be able to detect that he is interacting with a honeypot. This means that our honeypot provides the same functionality as a regular Linux server. Additionally, we want to separate the part of the honeypot which is tracing the activities of an attack by using virtualization. This helps to increase the stealthiness of the monitoring and also to improves the integrity of the extracted traces because an attacker is not able to attack it directly. Finally, we want to trace all activities in the honeypot in order to have a detailed view on the actions taken by an attacker.

3. Architecture and data extraction

To achieve these goals, we use virtual machine introspection (VMI) based system call tracing from a separate monitoring virtual machine. VMI is the process of monitoring a virtual machine from outside and extract information of it. It has been shown that VMI is a valuable approach for intrusion detection and honeypots [1, 2].

Our VMI-based SSH honeypot architecture is composed of three components: a sandbox VM (the honeypot), an introspection VM and a database. The execution trace from the honeypot is extracted by the introspection virtual machine, which sends it to the database.

To trace the activities of an attacker we use system call tracing which allows us to reconstruct SSH sessions and logs all the important operations of an attack to a database. Afterwards, this data can be used by a human investigator to analyze the attacks.

4. Conclusion

Compared with other SSH honeypots our approach is stealthy due to the usage of VMI. With our proof-of-concept implementation we were able to extract useful information such as user's credentials and keystrokes to reconstruct SSH sessions. The system is also able to detect post activities of an attack such as the communication of a backdoor which helps to investigate attacks in more detail. Furthermore, we plan to support the monitoring of other SSH features such as copying files and port forwarding. The presented approach is a very generic approach which can also be applied for other services besides SSH.

Acknowledgments

The research leading to these results was supported by the "Bavarian State Ministry of Education, Science and the Arts" as part of the FORSEC research association.

References

[1] X. Jiang, X. Wang, and D. Xu. Stealthy malware detection and monitoring through vmm-based "out-of-the-box" semantic view reconstruction. *ACM Transactions on Information and System Security (TISSEC)*, 13(2):12, 2010.

[2] T. K. Lengyel, J. Neumann, S. Maresca, B. D. Payne, and A. Kiayias. Virtual machine introspection in a hybrid honeypot architecture. In *Cyber Security Experiment and Test (CSET)*, 2012.

[3] Michel Oosterhof. Cowrie. https://github.com/micheloosterhof/cowrie. last-checked: 2017-03-17.

Virtual Machine Introspection Based SSH Honeypot

Stewart Sentanoe, Benjamin Taubmann, Hans P. Reiser
University of Passau
sentanoe@fim.uni-passau.de, {bt,hr}@sec.uni-passau.de

Motivation

SSH service is **attacked frequently**

An emulated honeypot **can be detected easily** by an adversary

Bash commands availability depends on the implementation

Emulated honeypot **can not give full pictures** of all activities inside the host machine since not all malware activities are executed and logged

A SSH Honeypot helps to **capture and analyze** novel attacks

Goals

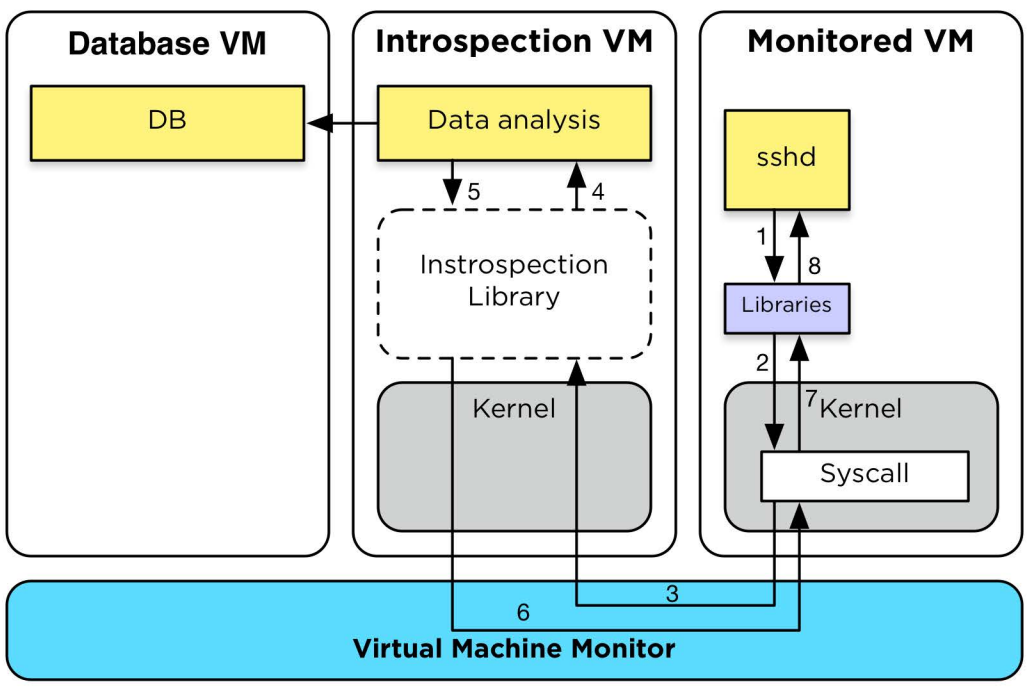
Implementation of a **VMI-based honeypot** with full system functionality

Hard to detect by an adversary that he is connected to a honeypot

Isolation between honeypot and Introspection framework

Full log of all activities inside the host

Architecture of System Call Tracing



1 - The SSHD in the honeypot VM calls library functions to read from and write to file descriptors.
2- The library function will then execute the proper system call.
3 - Each system call will be intercepted.
4,5 - The extracted parameters are sent to the data analysis and stored in the database.
6 - The introspection library resumes the execution of the virtual machine.
7,8 - When the invocation continues, process can proceed to the next step.

Evaluation

Overhead Calculation - Authentication Phase

Type	Total	Username and Password	%
sys_read	410.5	8	1.95%
sys_write	100.13	9	8.99%

The percentage of the system calls that contain username and password information compared to the total of system calls that invoked during authentication phase

cd00r Detection

Steps	VMI-Based Approach	Emulation	MiTM
Download the cd00r	✔	✔	✔
Installation of cd00r	✔	✗	✔
Connection via backdoor	✔	✗	✗

Real world scenario where an adversary performs the following steps: (1) download a rootkit from external sources, (2) compile the rootkit, (3) execute the rootkit and (4) use the rootkit to connect to a backdoor.

UNIVERSITÄT PASSAU

The research leading to these results was supported by the "Bavarian State Ministry of Education, Science and the Arts" as part of the FORSEC research association.

FORSEC Sicherheit hochgradig vernetzter IT-Systeme

Stewart Sentanoe
Universität Passau