Evaluating the Observability of Network Security Monitoring Strategies With TOMATO

Zachary Werle, William Heinecke, James Halvorsen, and Assefaw Gebremedhin

INTRODUCTION

- In order to deal with an attack on a network, the attack must first be detected. Therefore, we need to place sensors around our network to collect data that could signal a potential attack.
- However, how do we know where to place the sensors to maximize detection? Additionally, is the data we are collecting even relevant and accurate? If we collect all data, the chance for false positives increases.
- The measurement of how a network's monitoring strategies effectively address the above issues is called **observability.** In order to calculate observability, James Halvorsen, Jesse Waite, and Adam Hahn developed a tool called TOMATO.
- They already conducted research into the effectiveness of TOMATO, so our project is an extension of their previous work.
- We use a new SIEM/data aggregation tool called Wazuh which aggregates data from Suricata, Sysmon, and Windows Event Channels.
- The previous experiment used the ELK Stack (Elasticsearch, Logstash, and Kibana) to aggregate data from Sysmon, Windows Logs, and Netflows.
- As a result, our project seeks to test TOMATO on measuring the observability of more SIEM/data aggregation tools.
- We are also looking into the possibility of expanding the previous experiment by using new tactics.

MITRE ATT&CK FRAMEWORK

- A database of tactics and techniques that adversaries use against computer systems. It's based on real-world observations.
- It was developed by the MITRE corporation.

TOMATO

- A tool made by James Halvorsen to measure the observability of a network's security monitoring strategies.
- Requires a graphical model of a network, a set of known attack tactics and techniques, and a real-time dataset.
- Using the real-time data, a conditional probability distribution is generated with respect to the techniques of the tactics we are observing. This distribution is used to get the local probability of observing features associated with the technique on a host and connection between hosts.
- Furthermore, a frequency matrix of the tactics used on the system is produced by generating sequences of attacks and simulating them on the graphical representation of our network.
- By combining the matrix of local probabilities of observing tactics with the frequency matrix of the tactics, TOMATO outputs a metric for each host in the network to help understand the effectiveness of sensor placement and quality of the overall data.

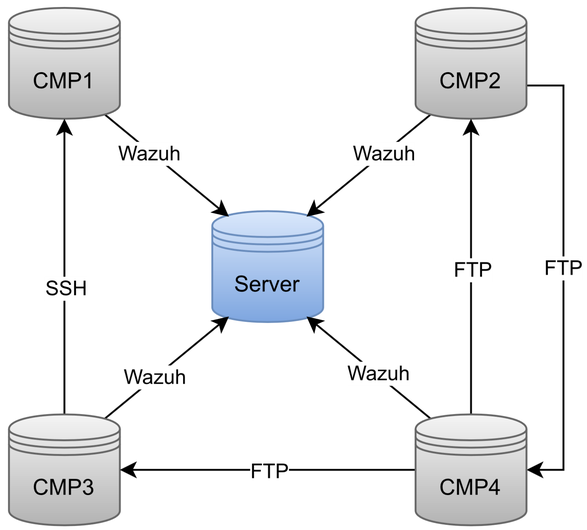

Figure 2: Graphic depicting the experimental setup.

EXPERIMENTAL SETUP

- Our experiment consists of five computers. Four are Windows 10 machines that generate network traffic between each other. The fifth is an Ubuntu Linux machine that hosts the Wazuh server.
- On all of the Windows 10 Machines, we use Wazuh agents to collect data from Sysmon, Windows Event Channels, and Suricata.
- This information gets stored in the Wazuh server and can be processed using the ELK Stack.
- **Sysmon**: A Windows system service that collects system information and logs it in the Windows Event log. We use it to log process creation events.
- **Windows Event Channels**: These channels store information on events that correspond to applications, security, and the system of a windows machine.
- **Suricata**: A network intrusion detection system that stores information on network events into and out of a host.

TACTICS

- **Discovery** - Discovery is when an attacker has gained access to an environment, which they then use to gain knowledge about the system and internal network. This process allows the adversary to examine the environment and determine their next course of action. Discovery is often a precursor to other attacks.
- **Execution** - Execution is often a remote attack where the attacker tries to run malicious code on a system. Execution is often paired with other techniques to achieve broader goals.
- **Lateral Movement** - Lateral movement is when an attacker gains control of one part of a network, which is then used to move further within the system. The adversary moves through the environment using different tactics, compromising systems and accounts in the process.
- **Privilege Escalation** – Privilege Escalation is when an attacker uses techniques to grant themselves elevated permissions to perform actions they were not previously authorized to. Sometimes an attacker needs to have more privileges to carry out their goals such as having access to the root of a machine.

RESULTS

Host	Observability	Efficiency
Server	0.0	0.0
CMP1	569.1233	0.006224
CMP2	716.6818	0.06231
CMP3	755.4637	0.06371
CMP4	819.7784	0.06499

Table 1: Shows the observability and efficiency scores of each host for a full stats run with Sysmon and Windows Security Event Channel events. Total Efficiency is 0.02247.

Host	Type	Observability	Efficiency
Server	Source	109.413	0.005302
Server	Destination	37.0	0.005302
CMP1	Source	616.3609	0.005382
CMP1	Destination	654.2583	0.005382
CMP2	Source	765.3321	0.05732
CMP2	Destination	756.8345	0.05732
CMP3	Source	830.6766	0.05946
CMP3	Destination	778.2159	0.05946
CMP4	Source	842.1131	0.01585
CMP4	Destination	937.5869	0.01585

Table 2: Shows the observability and efficiency scores of each host for a full stats run with Sysmon, Windows Security E.C, and Suricata events. Total Efficiency is 0.01468.

REFERENCES

J. Halvorsen, J. Waite and A. Hahn, "Evaluating the Observability of Network Security Monitoring Strategies With TOMATO," in *IEEE Access*, vol. 7, pp. 108304-108315, 2019, doi: 10.1109/ACCESS.2019.2933415.

ACKNOWLEGEMENTS AND FUNDING

The authors are grateful for funding from the Griffiss Institute under contract No. SA10012021MM0336.