TEXAS A&M UNIVERSITY
Engineering

Booth Number: 333

Kubernetes Based Attacks

Thomas Gumienny, Patrick Churchill, Albert Ma

Faculty Mentor: Sandip Roy

THE TEXAS A&M Global Cyber Research Institute
endowed by Roy Rothrock '77 and Anthony Wood '87

Problem Definition

The US Navy is using Kubernetes, a container management platform, to manage software. However, as a relatively new cyberservice, Kubernetes has a variety of cybersecurity weaknesses.

Methodology

Develop a RKE2 Kubernetes testbed that can simulate and collect the data of common types of attacks, and can also serve as a way to run more attacks.

CLUSTER DEVELOPMENT

- Connect two computers in a Server Node/Agent Node setup and install a PHP Guestbook and a camera streaming deployment on the cluster to simulate a command and control setup.

IMAGE ATTACK

- Simulates a malicious docker image call that would install a cryptominer when the image is ran
- Consumes CPU on the server node using matrix multiplication to simulate cryptominer CPU usage.

NODE ATTACK

- Simulates a denial of service attack created by the server node sending 60 pods to the agent node.
- Each pod contains an infinite amount of small requests, causing the agent node's CPU to max out and inevitably crash the node.

POD ATTACK

- Creates spam containers for a pod based on a malicious image when executed.
- Consumes CPU and RAM and slows the system.

Cluster Diagram

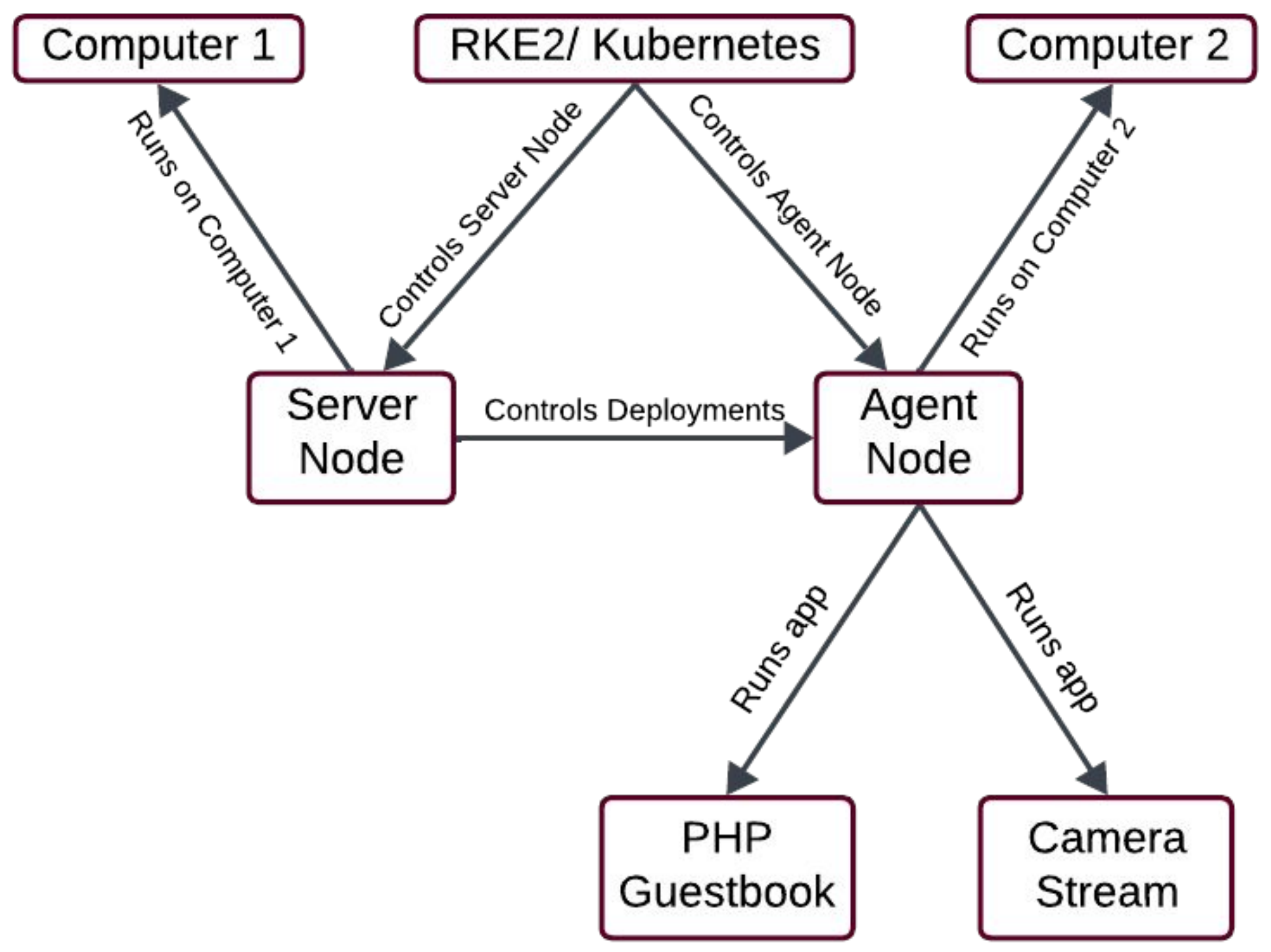


Figure 1. Diagram of cluster operation.

Engineering Analysis

As a way to run each of our attacks with minimal effort and enable data collection, we created a GUI that can do the following:

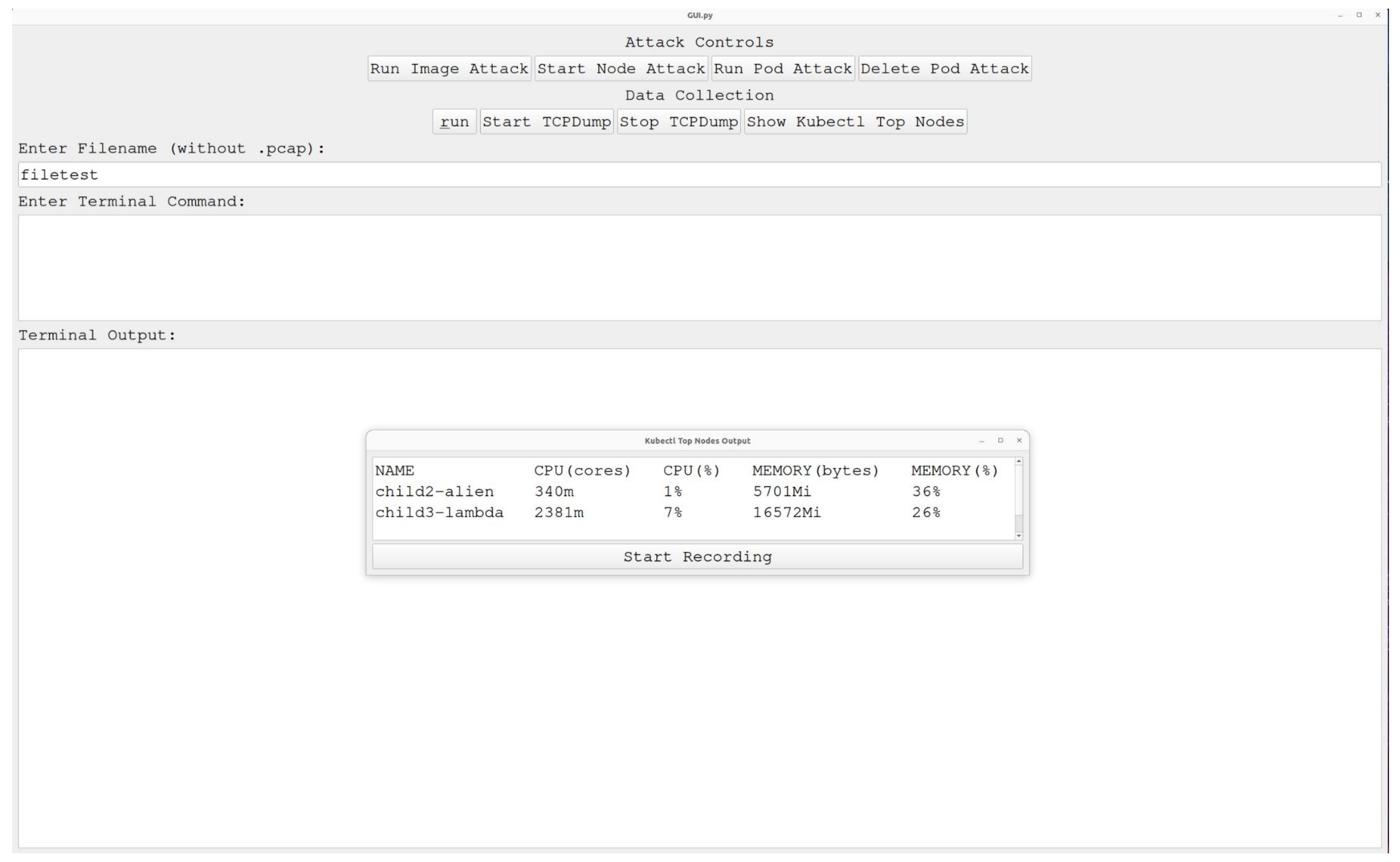
A. The GUI can run each attack.

B. The GUI can display the attack's effect as it is being executed.

C. The GUI can record relevant data while the attack is being executed.

D. New attacks can be added to the testbed.

The cluster and GUI setup process is fully documented on Github, for both Navy and future senior design project use. The documentation includes a guide on using the GUI and adding new attacks.



```
Enter Filename (without .pcap):
filetest
Enter Terminal Command:

Terminal Output:
```

```
NAME           CPU(cores)   CPU(%)   MEMORY(bytes)   MEMORY(%)
child2-alien   340m         1%       5701Mi          36%
child3-lambda  2381m        7%       16572Mi         26%
```

Figure 2. Screenshot of GUI

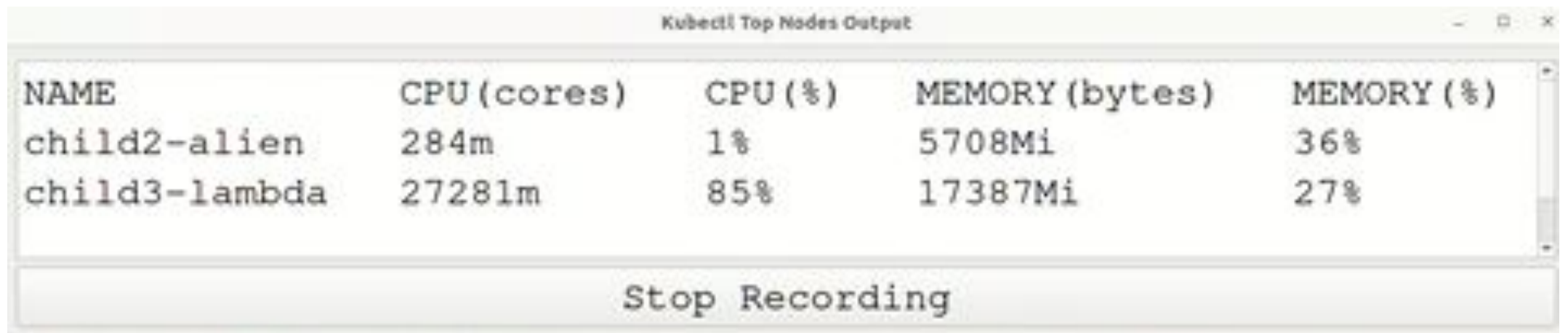
Outcomes

TESTBED FUNCTIONALITY

- The GUI can run each attack vector successfully. The GUI can record the CPU usage and packet capture data to record the attacks.

IMAGE ATTACK

- When the attack is run, the GUI first calls a non-existant image, then runs the attack image to simulate a real-world image attack. When run, the docker image consumes up to 85% of the CPU.

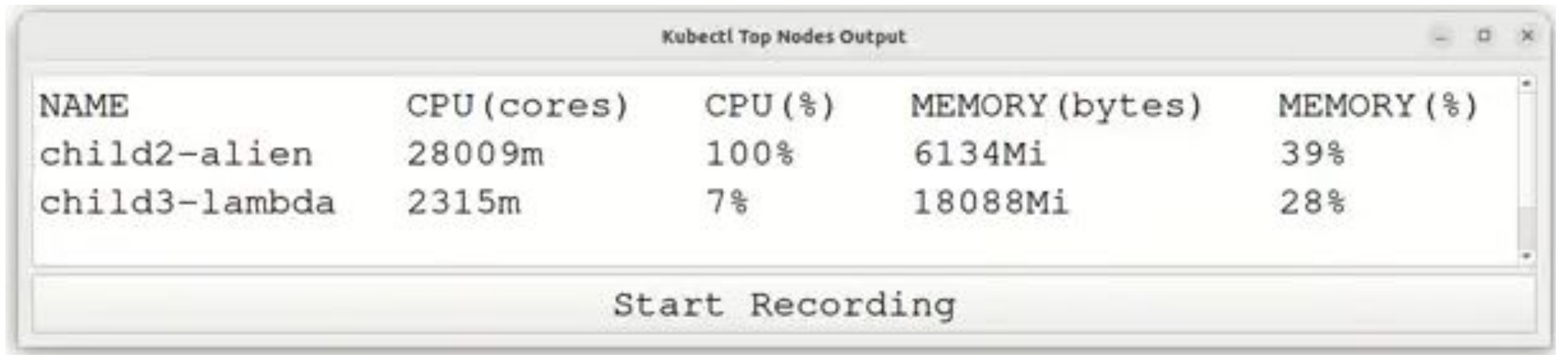


```
NAME           CPU(cores)   CPU(%)   MEMORY(bytes)   MEMORY(%)
child2-alien   284m         1%       5708Mi          36%
child3-lambda  27281m       85%      17387Mi         27%
```

Figure 4. CPU usage display during image attack.

NODE ATTACK

- While the attack is run, the child3-lambda node will send 50 pods that each infinitely send requests to the child2-alien node, causing its CPU to max at 100% and crash the child2-alien node.

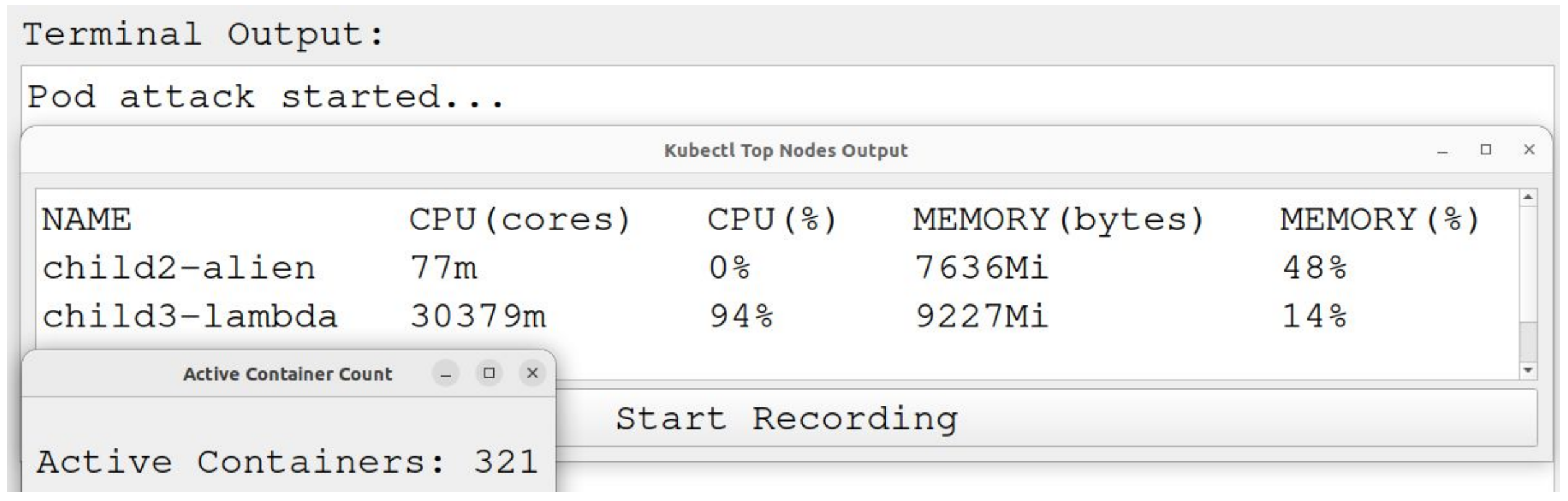


```
NAME           CPU(cores)   CPU(%)   MEMORY(bytes)   MEMORY(%)
child2-alien   28009m       100%     6134Mi          39%
child3-lambda  2315m        7%       18088Mi         28%
```

Figure 5. CPU usage display during node attack.

POD ATTACK

- During the attack, the GUI creates a large number of containers (which pods hold) based on a spam image.
- As more active containers are created, it consumes memory and up to 95% CPU, causing it to slow down and eventually crash.



```
Terminal Output:
Pod attack started...

NAME           CPU(cores)   CPU(%)   MEMORY(bytes)   MEMORY(%)
child2-alien   77m          0%       7636Mi          48%
child3-lambda  30379m       94%      9227Mi          14%

Active Containers: 321
```

Figure 6. CPU usage display during pod attack.

Impact

The testbed is a fully functional Kubernetes-based attack simulation platform. It will be used by the navy and future capstone teams for the following purposes:

- **Attack Simulation:** The GUI allows running a variety of attack simulations from a single interface.
- **Data Recording:** The testbed can display relevant real time attack data, and record that data for future viewing and analytics.
- **Defense Simulation:** Future capstone teams and graduate students will use the testbed to implement more types of attack, as well as use the testbed to figure out defense methods against cyberattacks.

References

1. Weizman, Yossi. "Threat Matrix for Kubernetes." Microsoft Security Blog, 2 Apr. 2020, www.microsoft.com/en-us/security/blog/2020/04/02/attack-matrix-kubernetes/.

2.Chierici, Stefano, and Stefano Chierici. "Analysis on Docker Hub Malicious Images: Attacks through Public Container Images." Sysdig, 23 Nov. 2022, sysdig.com/blog/analysis-of-supply-chain-attacks-through-public-docker-images/.

Acknowledgements

Dr. Sandip Roy, Dr. Jaewon Kim, Grace Harris, Nicholas Heinrich-Barna