



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

**CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION**

IDS Performance in Constrained Environments

January 20, 2022

Shelton Wright

Topic Overview

Determine the performance of an intrusion detection system with limited hardware resources

- Single board computers
- Embedded systems
- Edge devices
- Etc.



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

HIDS

Host-based Intrusion Detection Systems (HIDS)

- Examine host-based actions such as applications, files, and logs
- Works even when device is offline
- Detects after system is already breached
- Analyze a single device or node



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

NIDS

Network-based Intrusion Detection Systems (NIDS)

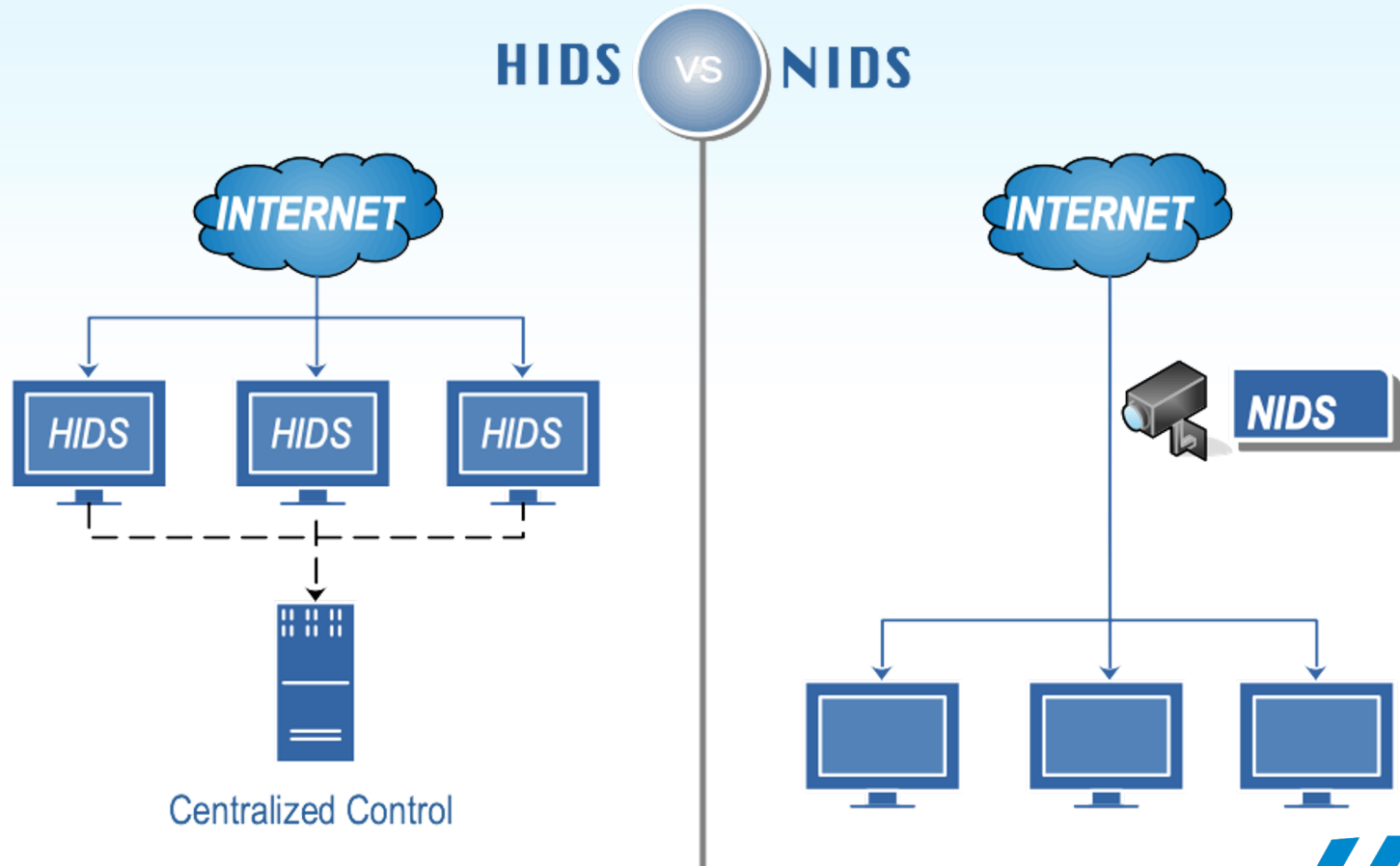
- Analyze network traffic
- Only works when on a network
- Detect before unauthorized access
- Typically a centralized inspection for multiple devices on a network



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

HIDS vs NIDS



NIDS on the Edge

- SCADA, IoT, weapon system, OT, etc.
- Higher resource, centralized monitoring is not available
- Still want to monitor network traffic

Solution

- Place NIDS on individual, low-resource nodes
- Each node is responsible for itself



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

Goals

- 1) Determine the ability of Suricata to run on minimal hardware resources
- 2) Specify the minimum resources needed for a specific scenario

*Not an evaluation of Suricata's performance



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

Suricata Overview

- Network-based IDS
- Open-source threat detection engine
- Intrusion detection & prevention system
- Signature language to match known threats, policy violations, and malicious behavior
- Capable of using the Emerging Threats and VRT rulesets

<https://suricata.io/>



CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

Attack Framework

- Pytbull/Pytbull-NG
- Open-source IDS testing framework
- +300 individual test grouped into 11 modules
- Originally written in Python 2, updated for Python 3
- Updated many outdated tests

<https://github.com/netrunn3r/pytbull-ng>



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

Pytbull Modules

- Bad Traffic
- Brute Force
- Client Side Attacks
- Denial of Service
- Evasion Techniques
- Fragmented Packets
- IP Reputation
- Normal Usage
- ~~Peap Replay~~
- Shell Codes
- Test Rules

<https://github.com/netrunn3r/pytbull-ng>



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

Logged Metrics

- Event Count (Alerts)
- CPU % Usage
- Physical Memory Usage
- Swap Usage
- Disk Usage
- Packet Count
- Byte Count
- Kernel Packet Drops



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

Test Environments

- Virtual Machines (Vagrant/VirtualBox)
 - Easy to configure and deploy
 - Easy to revert back changes
- BeagleBone Black
 - Single board computer
 - Representative of a target system



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

Virtual Host Configuration

Hardware Configuration	
Parameter	Value
CPU	Intel Core i5-6200U 2.30GHz 2-core
Physical Memory Size	8 GB
Physical Memory Type	DDR3
Drive Size	128 GB
Drive Type	SSD
Host OS	Windows 10



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

Virtual Machine Configurations

Base Configuration

Configuration:	1
Virtualization Platform	Oracle VirtualBox
Guest OS	Centos 7
CPU Cores	1
Memory Size	512 MB
Disk Size	40 GB
Swapfile Size	512 MB

Configuration:	2
Virtualization Platform	Oracle VirtualBox
Guest OS	Centos 7
CPU Cores	1
Memory Size	1024 MB
Disk Size	40 GB
Swapfile Size	-0-

Initial Results

- Startup
 - Requires 1GB of total virtual memory
 - <1GB Service crashes without attack



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

Stress Test Results

Test	Config	Event Count (Alerts)	CPU % Usage	Total Usage (Mem + Swap)	Data Rate (MB/second)	Kernel Drops (1000 packet drops)
Denial of Service	1	Total: 572,417	Max: 95.7	Max: 831.55	Max: 2,997.6	Total: 1,110.4
Normal Usage	1	Total: 2,483	Highest Alerts & MEM		Max: 315e-3	N/A
IP Reputation	1	Total: 17	Max: 13.6	Max: 645.12	Max: 10e-3	N/A
Fragmented Packets	1	Total: 103	Highest CPU Usage		Max: 1e-3	N/A
Client Side Attacks	1	Total: 4	Max: 24.3	Max: 644.86	Max: 2.82e-3	N/A
Test Rules	1	Total: 767	Max: 98.0	Max: 722.98	Max: 4.5	Total: 874.84
Brute Force	1	Total: 73	Max: 9.0	Max: 645.17	Max: 2.22e-3	N/A
Bad Traffic	1	Total: 43	Max: 14.9	Max: 651.58	Max: 127e-3	N/A
Evasion Techniques	1	Total: 26,894	Max: 29.6	Max: 666.16	Max: 468e-3	Total: 1.3
Shell Codes	1	Total: 160	Max: 7.6	Max: 645.32	Max: 7.3e-3	N/A



Test Rules

- 6 Tests
 - Nmap scans
 - Netcat reverse shell
 - Nikto scan

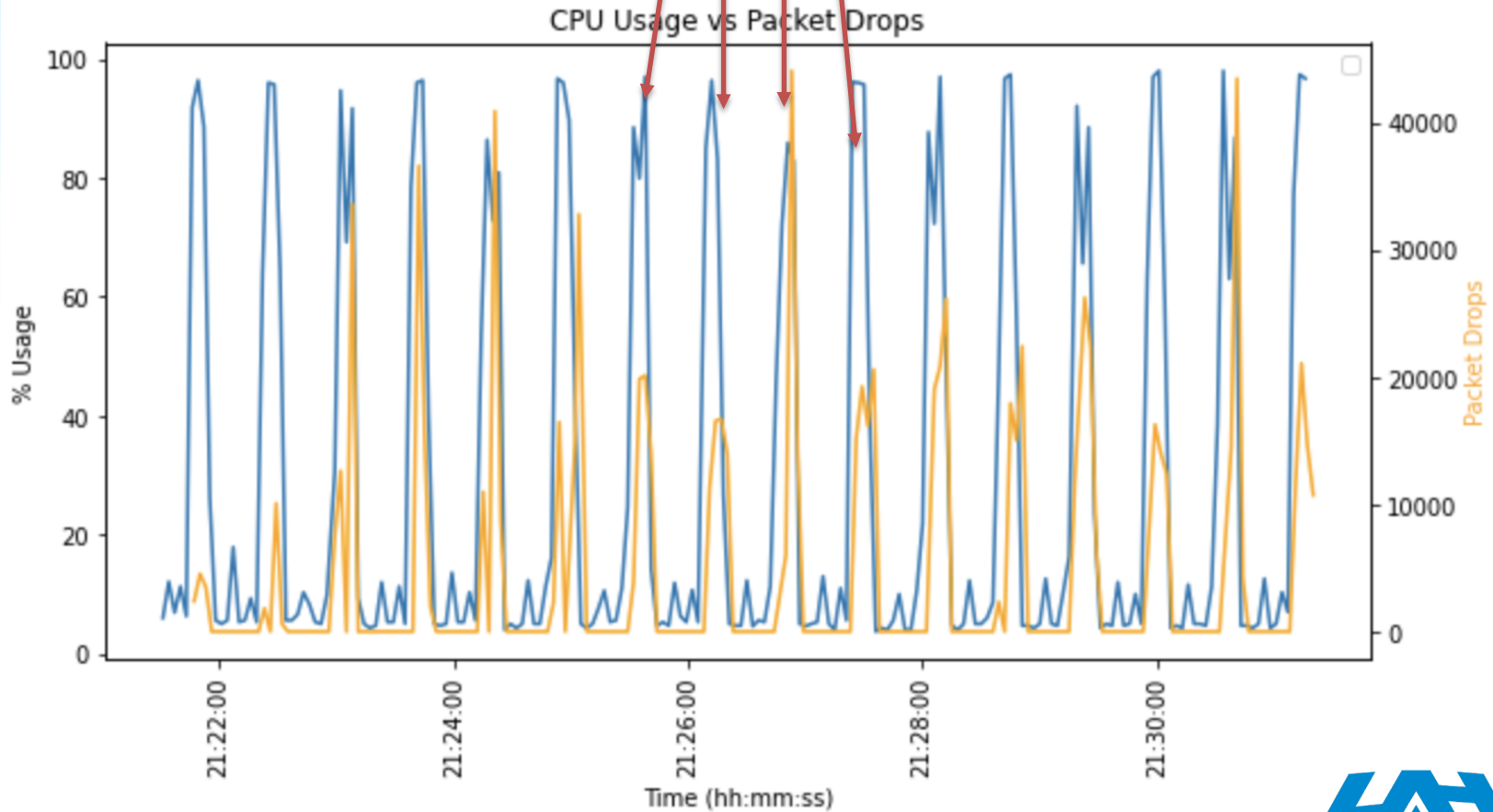


THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

Test Rules

Nmap Full SYN Scan



Denial of Service

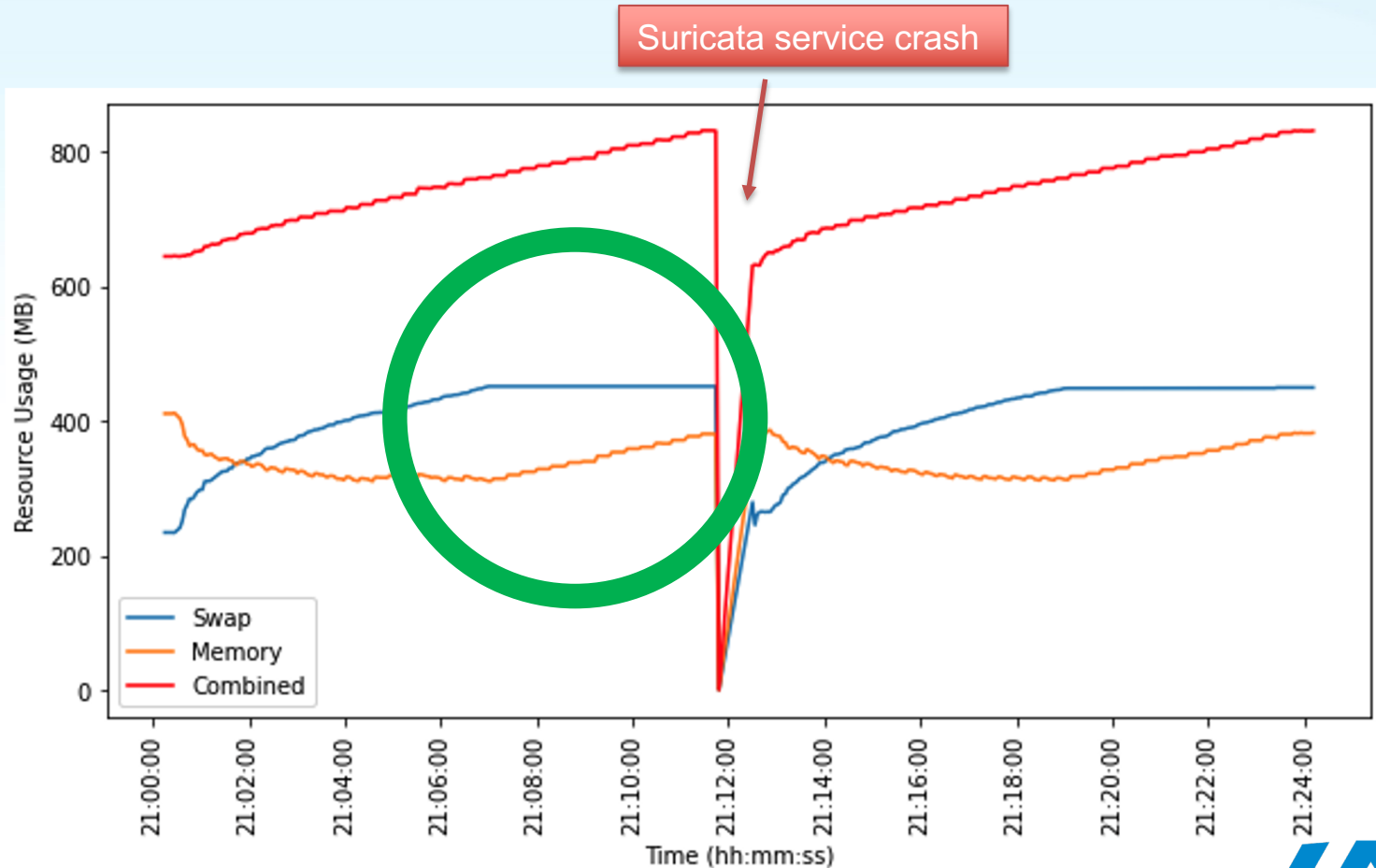
- 2 Tests
 - Apache Bench
 - hping3



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

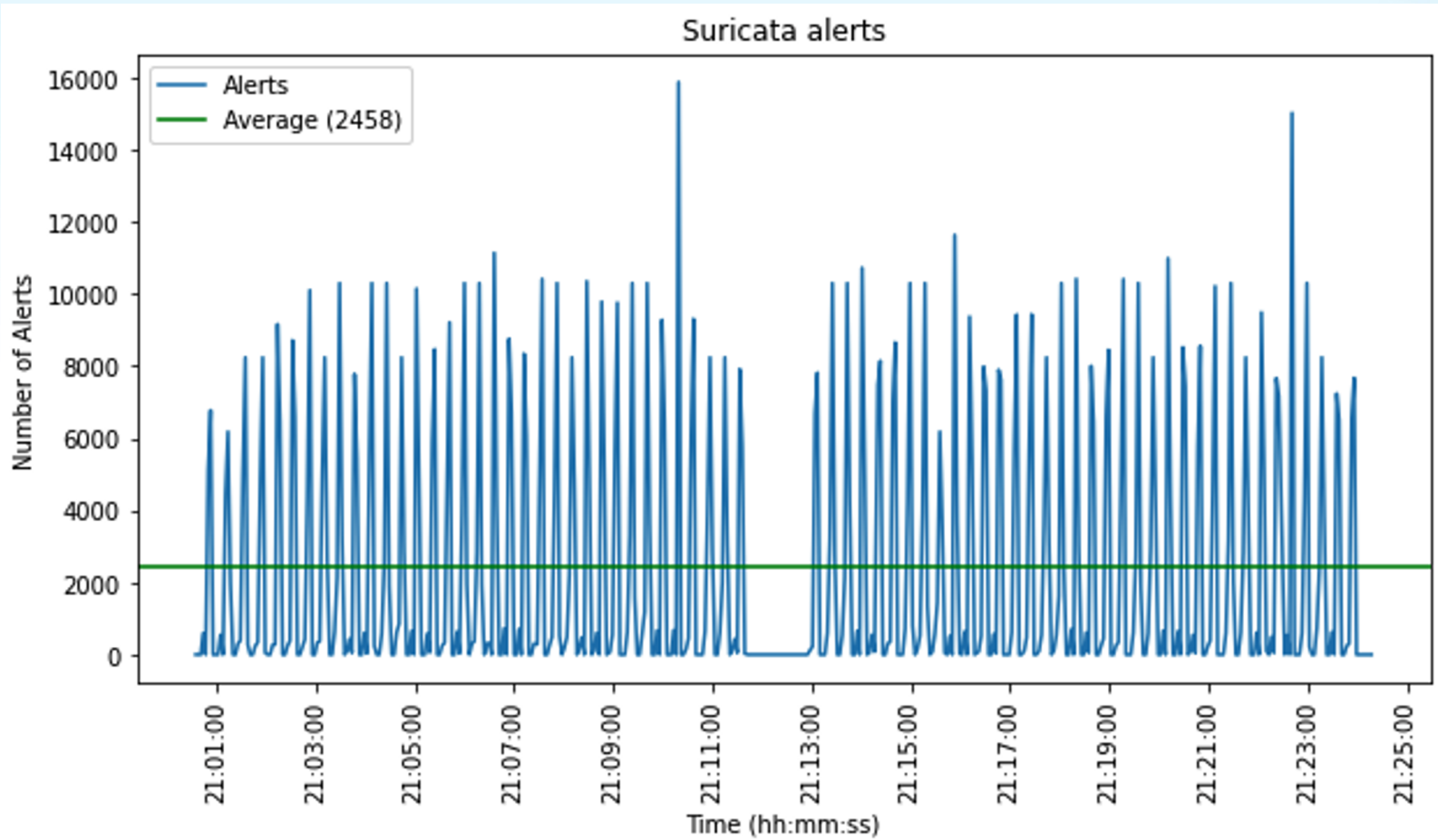
Default DOS



CPU: 95.7%

Combined: 831.55 MB

Default DOS



Suricata Service Crash

- Suricata service crashes when combined memory and swapfile ~830MB
- Still default configuration of 500MB memory and 500MB swapfile

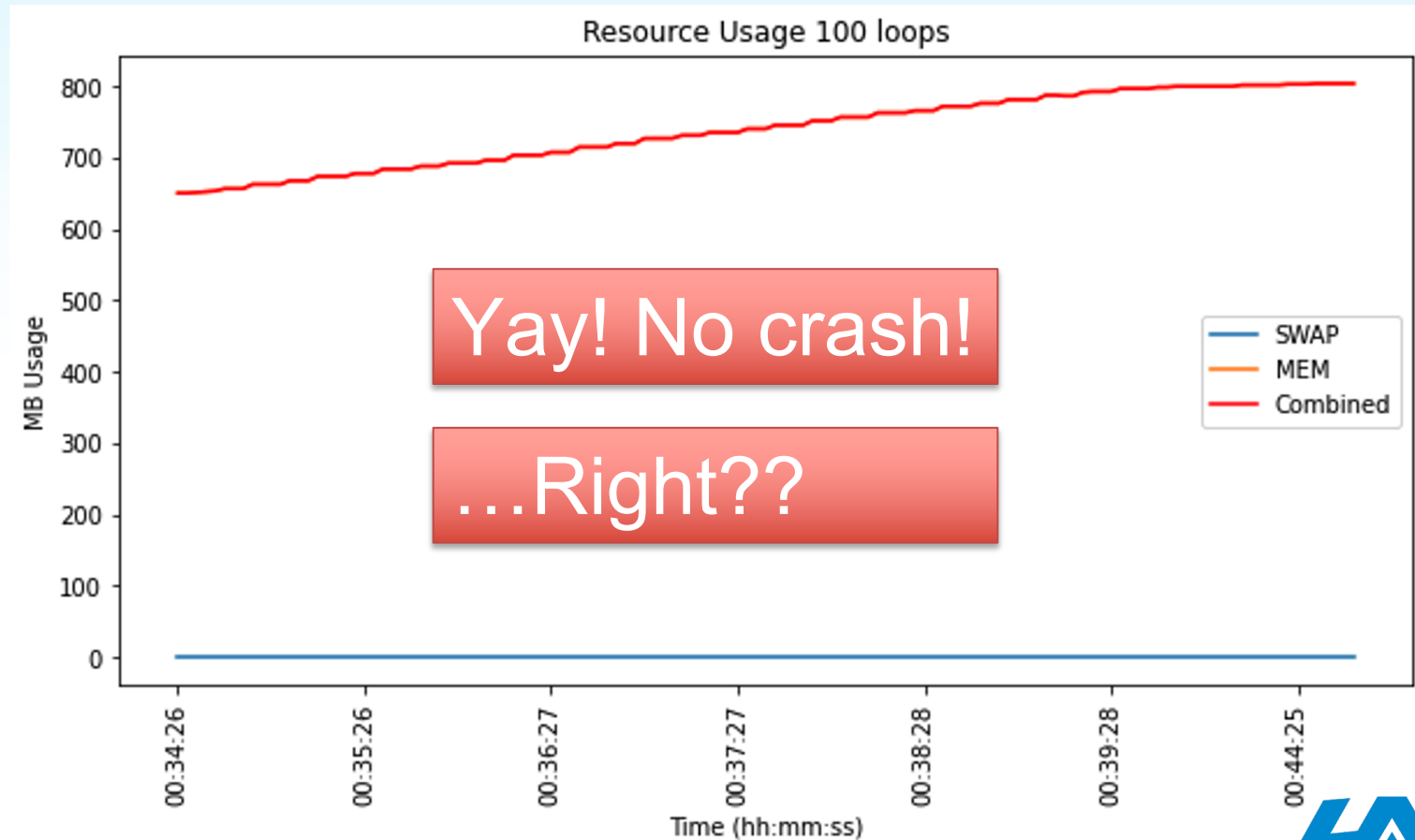
What if we increase memory and get rid of swap?
1GB memory and no swapfile



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

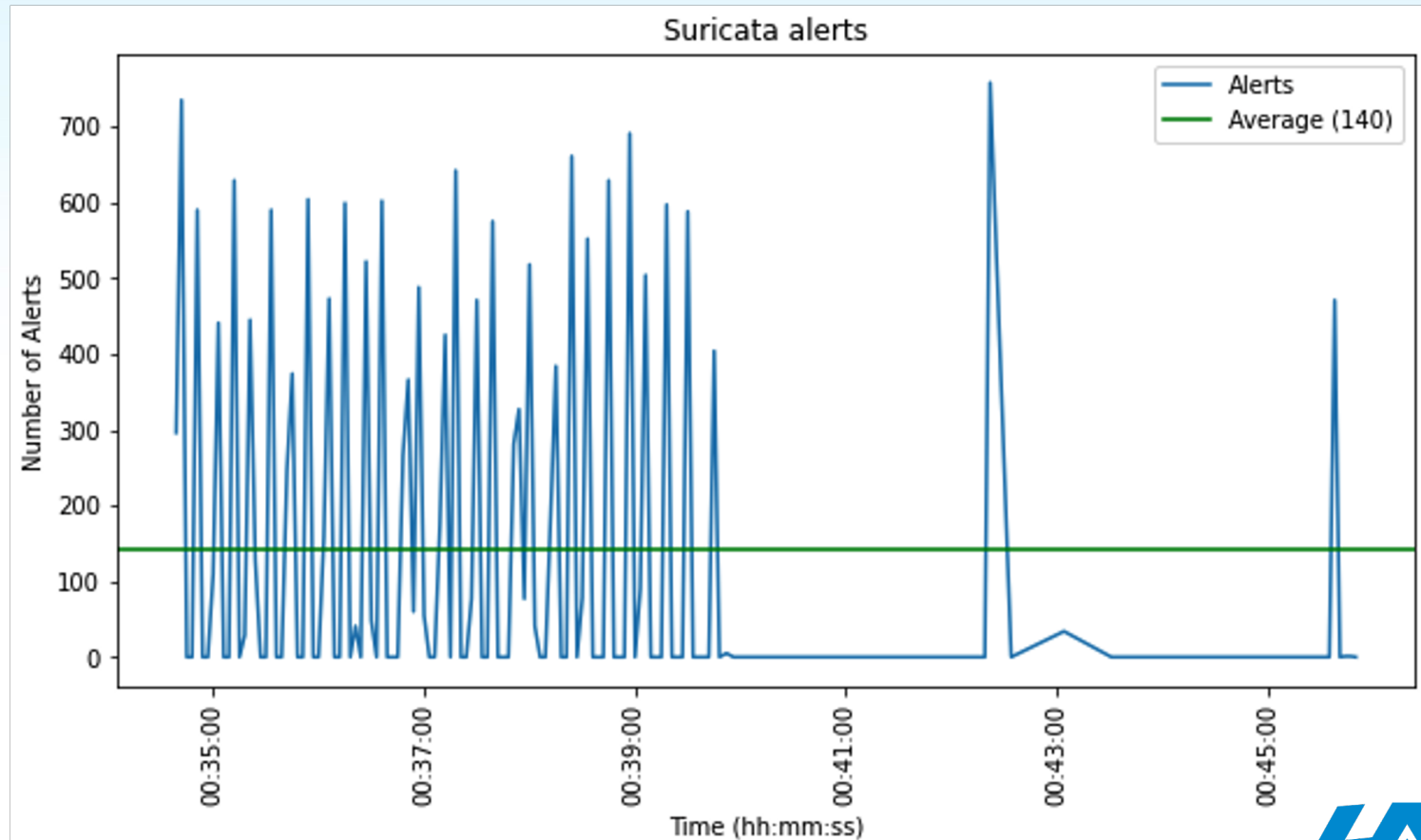
CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

Apache Bench Run 2



Mem Max: 803.84 MB
1GB Memory & no swap

Apache Bench Run 2



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

To Swap or Not

What's better: memory or a swapfile?

Time for service to restart after crash:

46 seconds

Time application is not processing:

147 seconds ... PLUS 120 seconds

Total: 267 seconds!



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

Disk Usage

Test Module	Avg Alert Size (KB)
DOS	0.506
ET	0.691
TR	0.718
CSA	1.142

Eve.JSON Event Type	Event Size (KB)	Logging Interval (Sec)	Approx. Size in 10 minutes (KB)
Stats	5.3	3	1,060
		5	636
		10	318



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

Virtual Machines v BeagleBone

- How do the Virtual Machines compare to actual hardware?
- All test run with a single run of attack module

Configuration	Virtual Machines	BeagleBone Black
CPU	Intel Core i5 2.30GHz	ARM® Cortex-A8 1GHz
CPU Cores	1	1
Memory Size	512 MB	512 MB
Memory Type	DDR3	DDR3
Swapfile Size	512 MB	512 MB



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

Alerts Comparison

Alerts			
Module	Virtual Machine	BeagleBone	Difference
Test Rules	22	15	-32%
Denial of Service	19790	24276	23%
Evasion Techniques	3966	3990	1%
Normal Usage	33	25	-24%
IP Reputation	16	14	-13%
Fragmented Packets	4	5	25%
Client Side Attacks	22	16	-27%
Brute Force	42	48	14%
Bad Traffic	15	12	-20%
Shell Codes	7	11	57%



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

Coefficients of Variance

Module	Virtual Machine	BeagleBone
Test Rules	8.11%	10.81%
Denial of Service	9.64%	0.19%
Evasion Techniques	3.75%	0.53%
Normal Usage	0.00%	10.58%
IP Reputation	0.00%	29.57%
Fragmented Packets	0.00%	0.00%
Client Side Attacks	4.14%	0.00%
Brute Force	1.06%	2.42%
Bad Traffic	6.13%	0.96%
Shell Codes	0.00%	5.41%



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

CPU Usage

Max CPU %			
Module	Virtual Machine	BeagleBone	Difference
Test Rules	87%	76%	-13%
Denial of Service	66%	92%	39%
Evasion Techniques	17%	86%	406%
Normal Usage	12%	28%	133%
IP Reputation	10%	25%	150%
Fragmented Packets	5%	26%	420%
Client Side Attacks	21%	82%	290%
Brute Force	10%	25%	150%
Bad Traffic	11%	38%	245%
Shell Codes	8%	27%	238%



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

Kernel Packet Drops

Drops Data Rate (kB/s)	
Virtual Machines	230
BeagleBone	43

- Slow down hping3 DOS attack until no drops
- Drops are directly correlated to CPU %
- BeagleBone has a slower CPU
 - 1 GHz v 2.3 GHz

Results Summary

- Minimum memory resources: 1GB
- CPU and memory usage depend on attack type
- Restarting Suricata service is quicker than waiting for new memory allocation
- Are VMs suitable for testing?



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

Conclusion

Two Approaches

- 1) Have the hardware defined and test what it can handle
- 2) Have attack data defined (data rates, types of attacks, etc.) and test minimum hardware requirements



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

Questions?

Shelton Wright

shelton.wright@uah.edu

O: 256.824.4789



THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION