

A Hacker's Guide to Computer Network Defense

Who Am I?

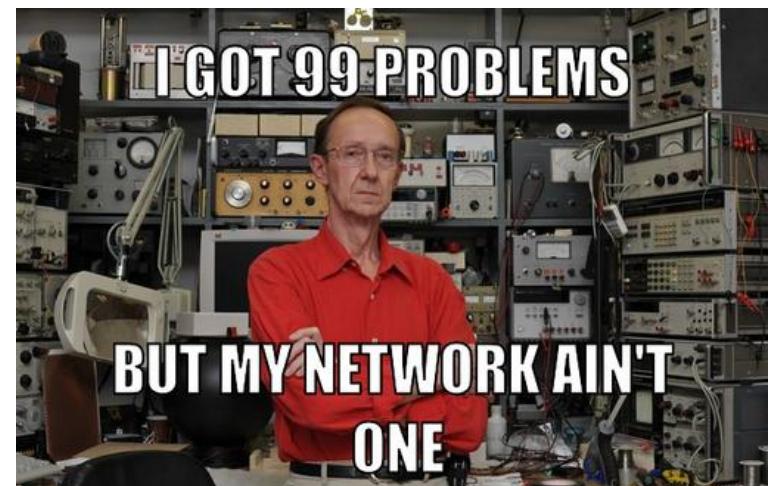
- Trevon (blackmanta)
- Random graduate student
- Linux Junky
- Computer Enthusiast



What even is a Network?

- A collection of connect computers
- A bus that provides access to resources

The New Boston: [Computer Networking](#) (Video)



Defending Computers

- How even does that work?
- Who manages that?

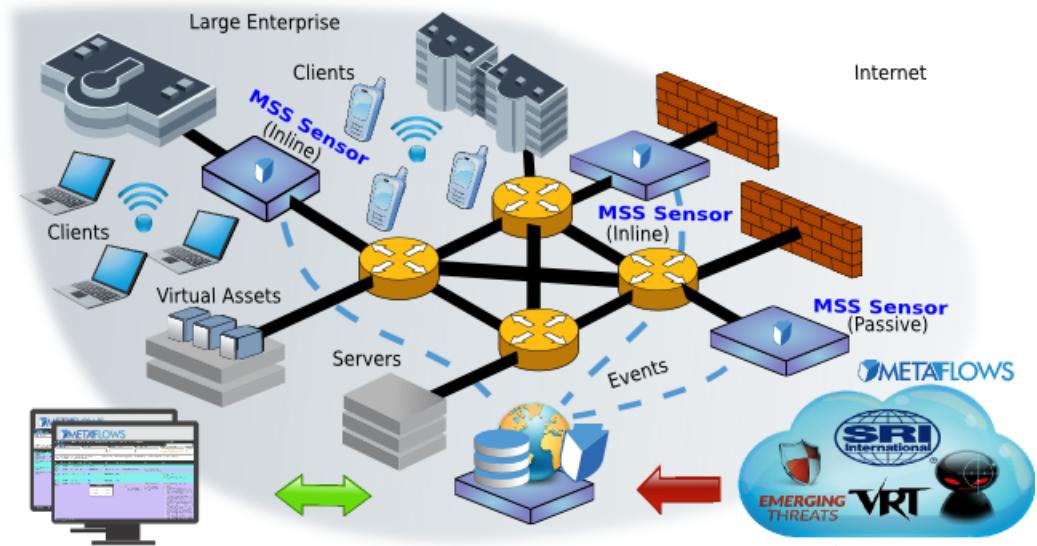
[Network Security](#) (Video)



Defending that Network.. thing

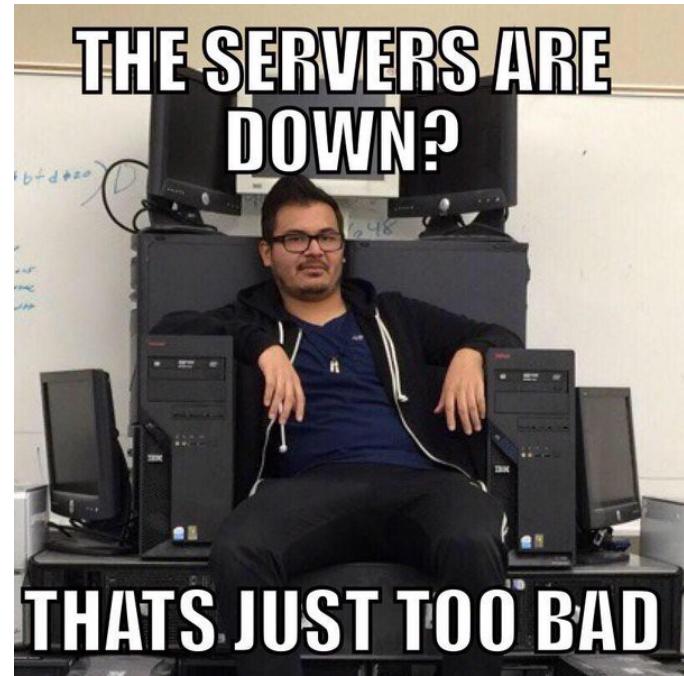
- How might one defend a Network?

MITRE ATT&CK Framework (Website)



So Computers...

- Why are computers an important?
- Host services
- Play... Video Games



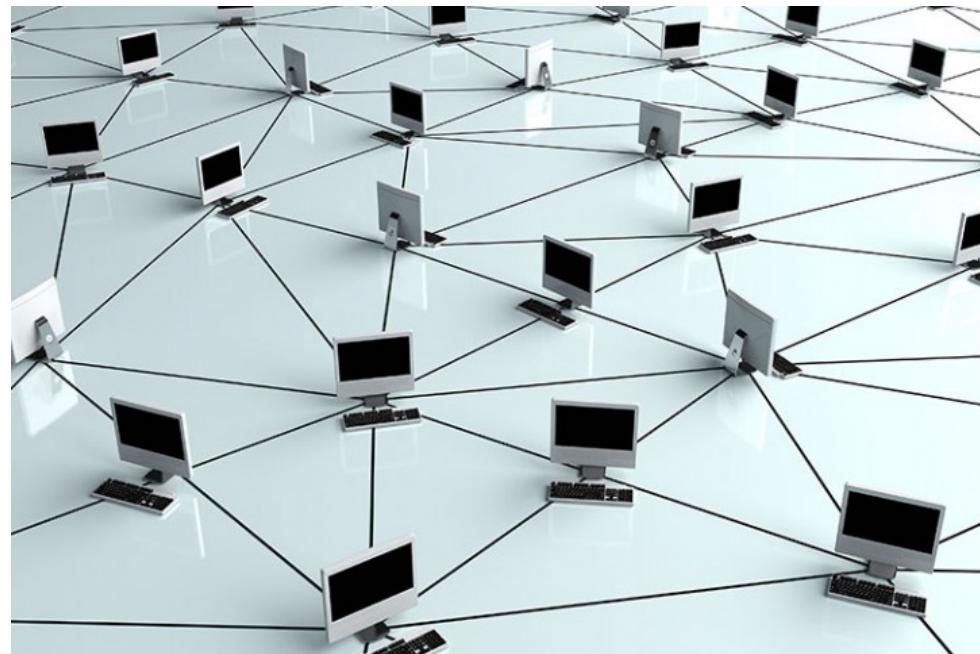
Many Layers of Defense...

cough defense in depth

- Intrusion Detection System
- Antivirus and local firewall
- Access Control



Connect all the things



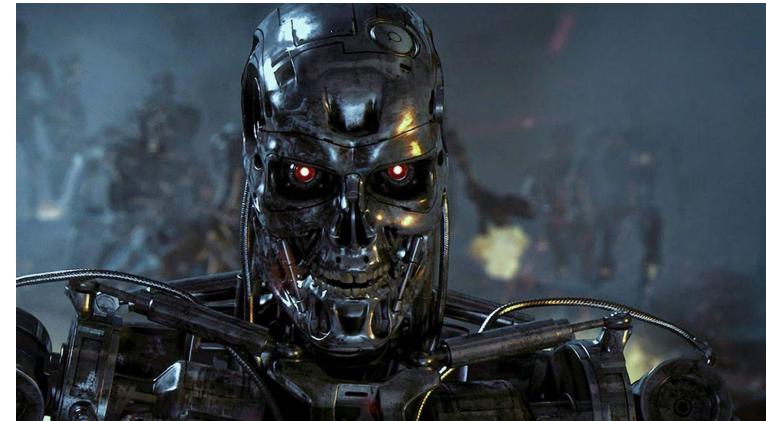
What about those fancy tools...

- Orchestration and automation's?
- Next Generation Firewalls
- Sooo... deploy to the cloud!!!
- No really... the cloud



Autonomic Systems

- Cognitive Systems
- IBM and DARPA 2001
- Inspired by Autonomic Nervous System



Virtualization Technologies

- Docker
- Linux Containers
- Qemu/KVM
- ESXI

[What is virtualization](#) (website)

Software Defined Networking

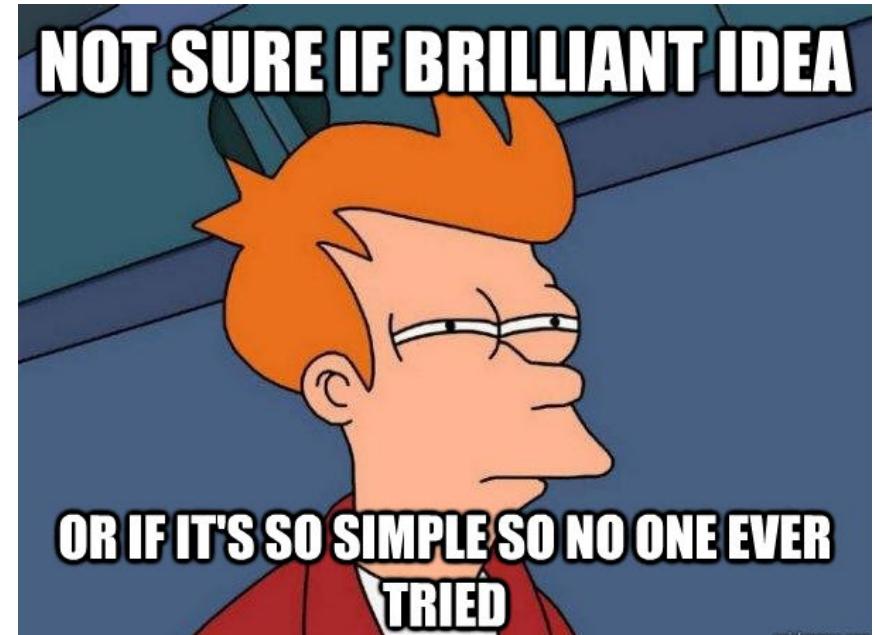
I AM NO EXPERT

- Programmable
- Firewalls
- Management, Data/Forwarding and Control plane

Good read: [Software Defined Networking \(SDN\): Anatomy of OpenFlow](#)

Easy Solution...

- Dude, so use Machine Learning
- Deep learning?



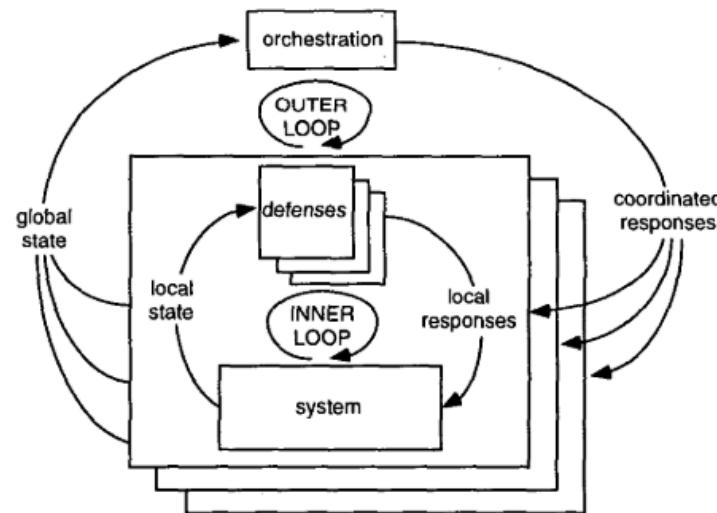
My Research

- Build off previous ideas
- Autonomic Systems
- So really?



SARA Framework

- DARPA Framework (2001) *cough MIT Lincoln Lab*



:)

Your PC haven't ran in to a problem it couldn't handle, and it does not need to restart.

You dont need to search online for error

It'll restart when you want to

Thanks for Listening

(References)

- Autonomic Networking
- SARA: Survivable Autonomic Response Architecture
- Learn Terraform
- Learn SaltStack
- LXD

