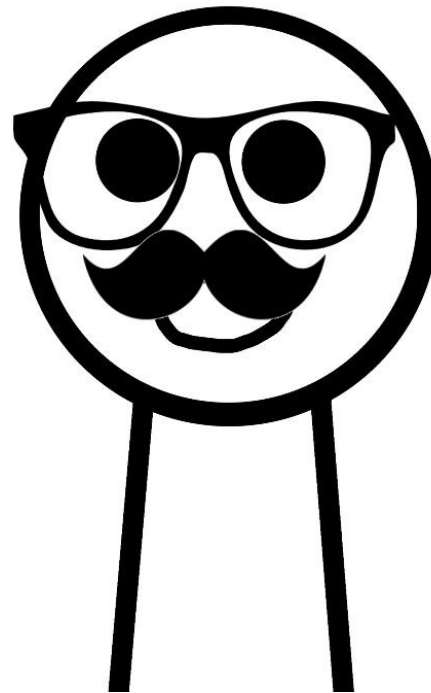
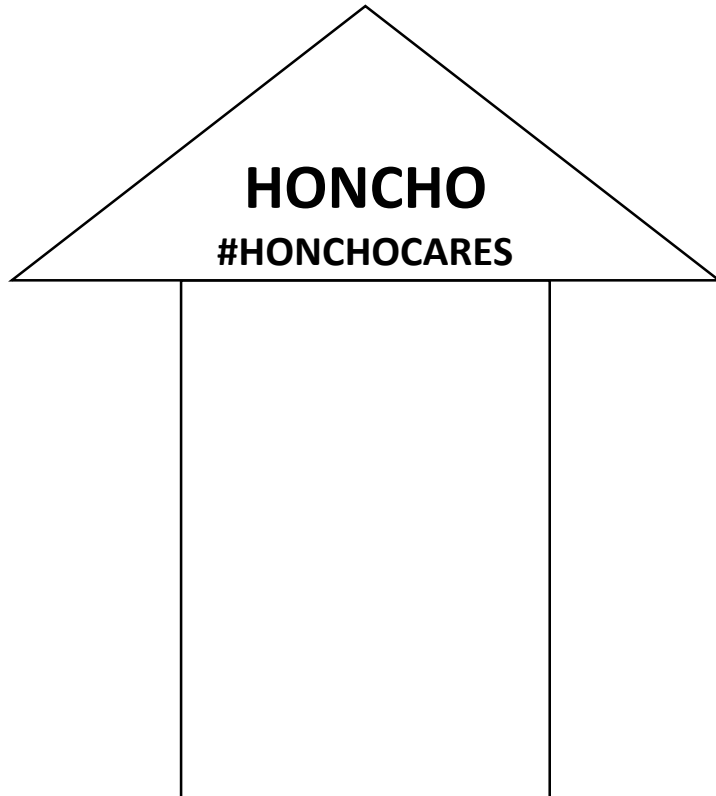


# **System Security Life Cycle**

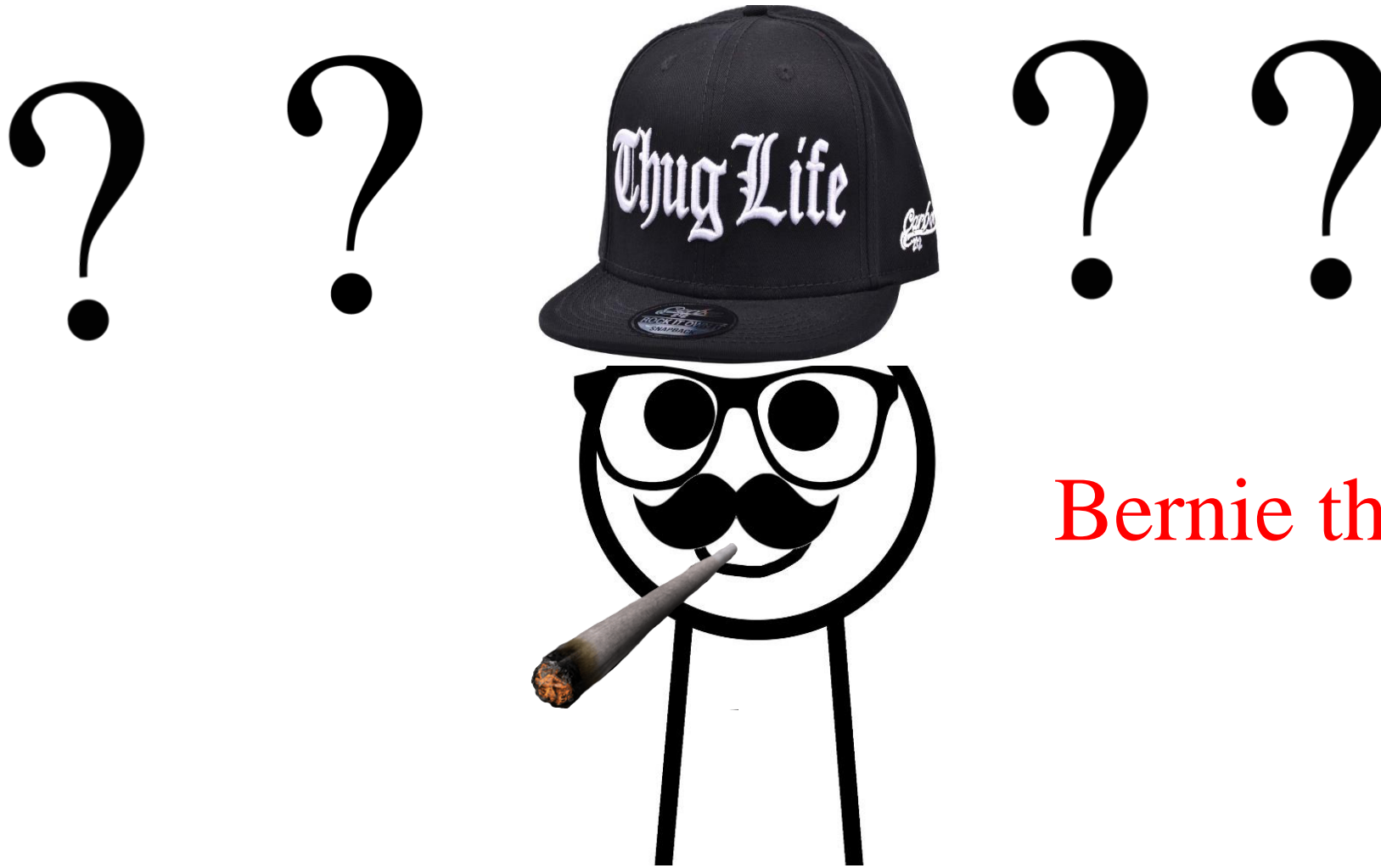
Landley Bernardo

February 17, 2018



Bernie the SeMan

System Security Life Cycle



Bernie the SeMan

*“To ensure that all systems and networks across the company are secure and remain secure.”*

*“To ensure that all systems and networks across the company are secure and remain secure.”*

## System Security Life Cycle



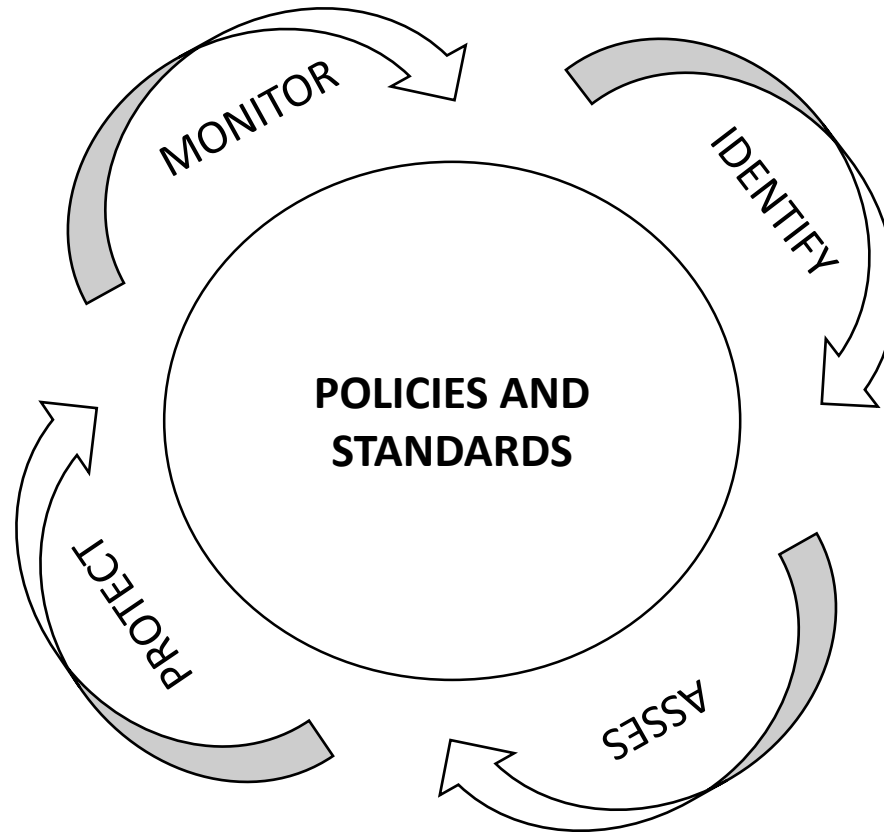
# System Security Life Cycle

# System Security Life Cycle

- Cycle that provides a continues monitoring and improvement of system security.
- The results of each phase feed into the next phase of a lifecycle.
- IDENTIFY-ASSES-PROTECT-MONITOR

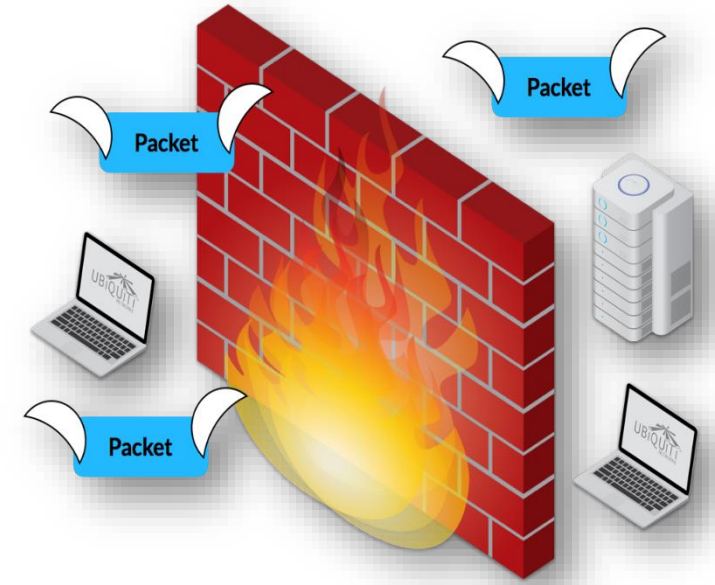


# System Security Life Cycle



# IDENTIFY

- Bernie has to have a good understanding of the resources that he is trying to protect.



# IDENTIFY

1. Where are the assets physically located? Are they in a secure data center or scattered about multiple office locations?
2. How many servers, firewalls, and routers does his company have?
3. What flavor of OS is running on each system?
4. What applications and services are running on each server?
5. Who is the customer for each system? (HR, Finance, Marketing, etc.)

# IDENTIFY

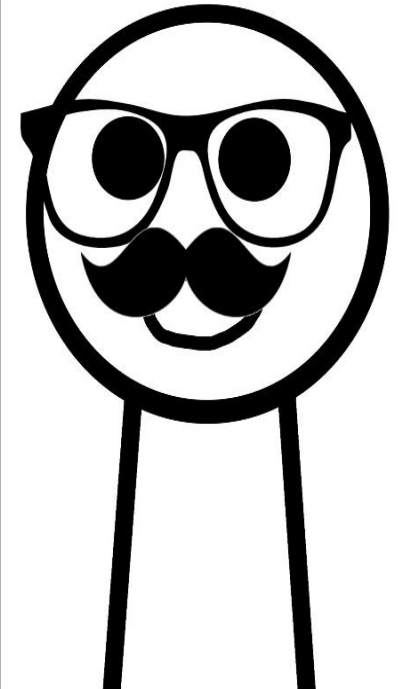
1. Where are the assets physically located? Are they in a secure data center or scattered about multiple office locations?
2. How many servers, firewalls, and routers does his company have?
3. What flavor of OS is running on each system?
4. What applications and services are running on each server?
5. Who is the customer for each system? (HR, Finance, Marketing, etc.)

# IDENTIFY

Conducting interview

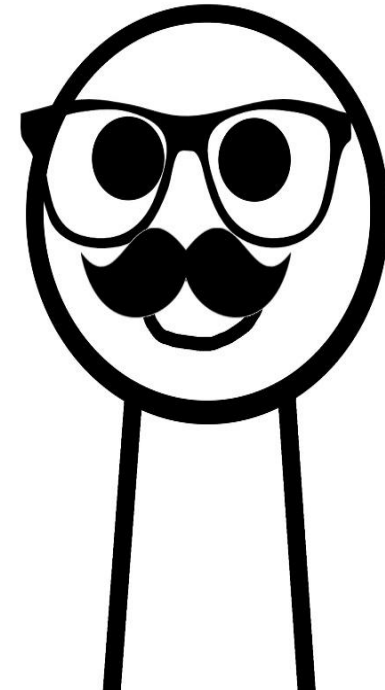
Utilize applications

- NMAP
- SuperScan
- NetScan Tools Pro (\$200)



# IDENTIFY

Store all the collected information to a secure place.



# ASSESS

- Examine and evaluate all the assets that were gathered during identification phase.
- **PRIORITIZE! BERNIE! PRIORITIZE!**

**Prioritize:**

determining what is really  
important and making it a  
priority

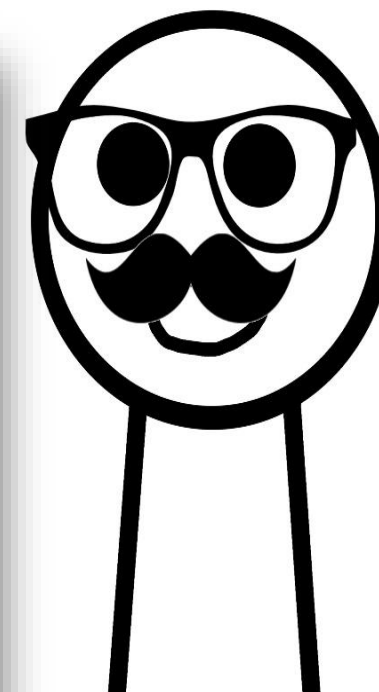
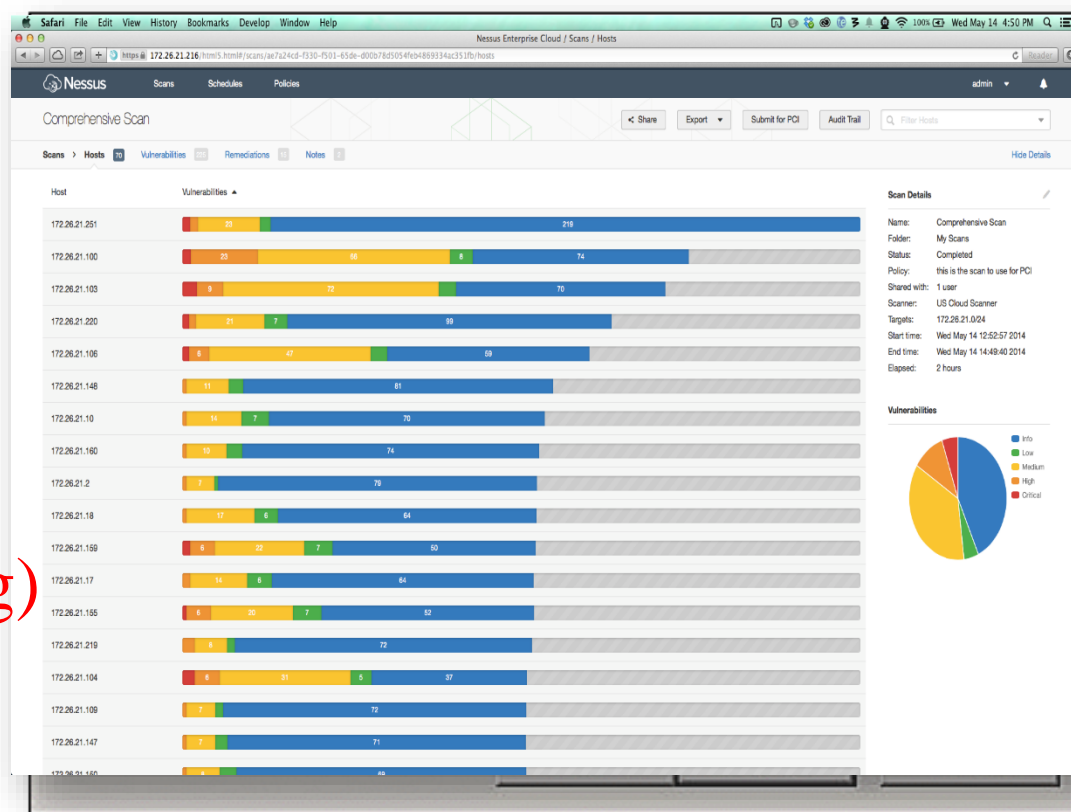
# ASSESS

Conducting interview

Utilize applications

- SuperScan
- BlackWidow
- Nessus

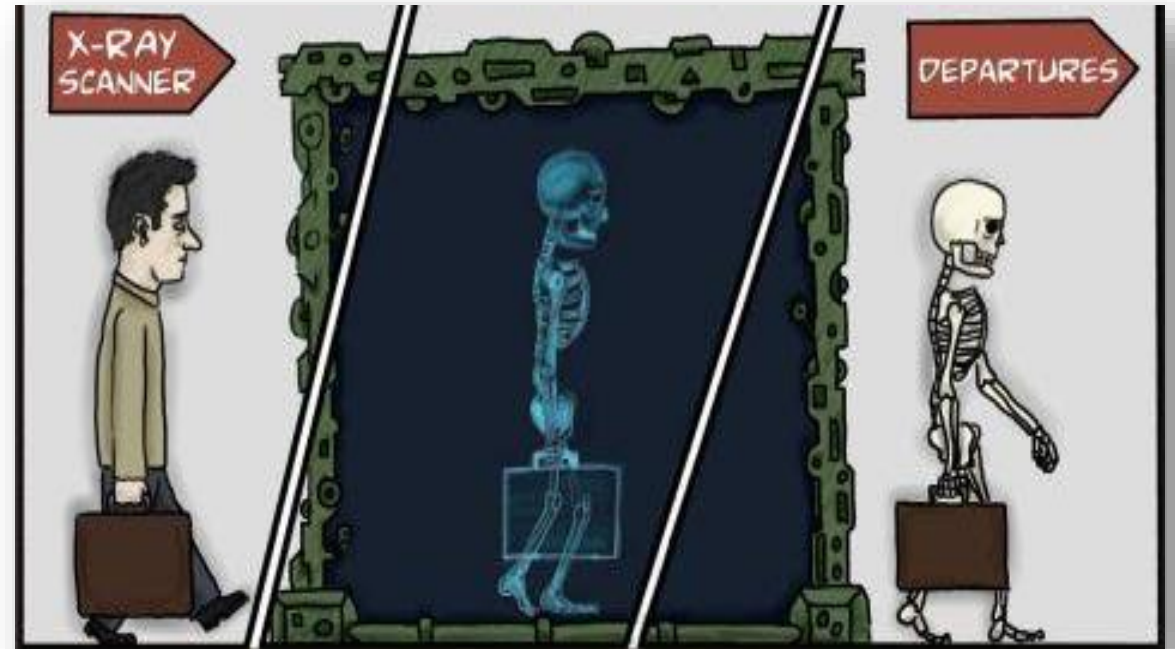
Center for internet  
security ([cisecurity.org](http://cisecurity.org))





# ASSESS

- The goal is to examine the resources at all levels.



# PROTECT

- Bring the system in-line with corporate security **POLICY AND STANDARDS**.
- aka **MITIGATION** phase.

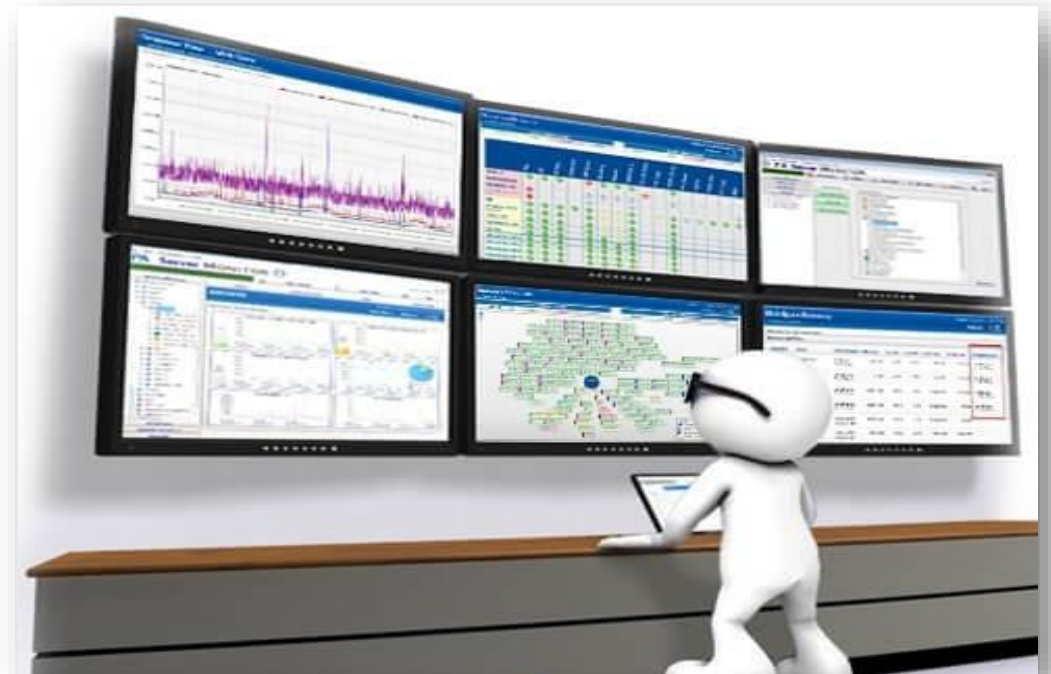
# PROTECT

- Fix the small things first.
- Coordinate with the key personnel.
- The goal is to bring systems and networks in line with corporate standards and policy and eliminating vulnerabilities.



# MONITOR

- Last phase aims to ensure that the security is maintain.
- Security compliance and verification.



# MONITOR

- Is the system secure? How do you know?
- Tripwire, Enterprise Security Manager, Routing Auditing Tool (RAT)



# MONITOR

- Monitoring report has to be submitted to senior management.
- Provide overall metric of the systems and networks.
- Measure the performance.



# MONITOR

- Monitoring report has to be submitted to senior management.
- Provide overall metric of the systems and networks.
- Measure the performance.



# CONCLUSION

- System Security Life Cycle is a continuous that needs to monitored during the course of time.



THE END!