Scalable Campus Networks Training
April 13 - 17 2015

Cyber Security

Ronald Osure, CEH

Agenda

- Configuration Management
- Access Control and Physical Security
- End user information security awareness to students and staff
- Defense in depth

The only constant thing is change

Configuration Management

- Growing demand for it in the security world
- Configuration management means many things
- Configuration management drives information security and information assurance

Change control process

1. Request for a change to take place
2. Approval of the change
3. Documentation of the change
4. Tested and presented
5. Implementation
6. Report change to management

Configuration management at campus level

- How are you managing configuration right now?
- Tools
  - Rancid
  - Chef
  - Ansible

Configuration management at campus level

- How are you managing configuration right now?
- Tools
  - Rancid
  - Chef
  - Ansible
  - ...

End user info-sec awareness

- Do you understand your end users?
- Information Security Awareness
- The 90-10 rule

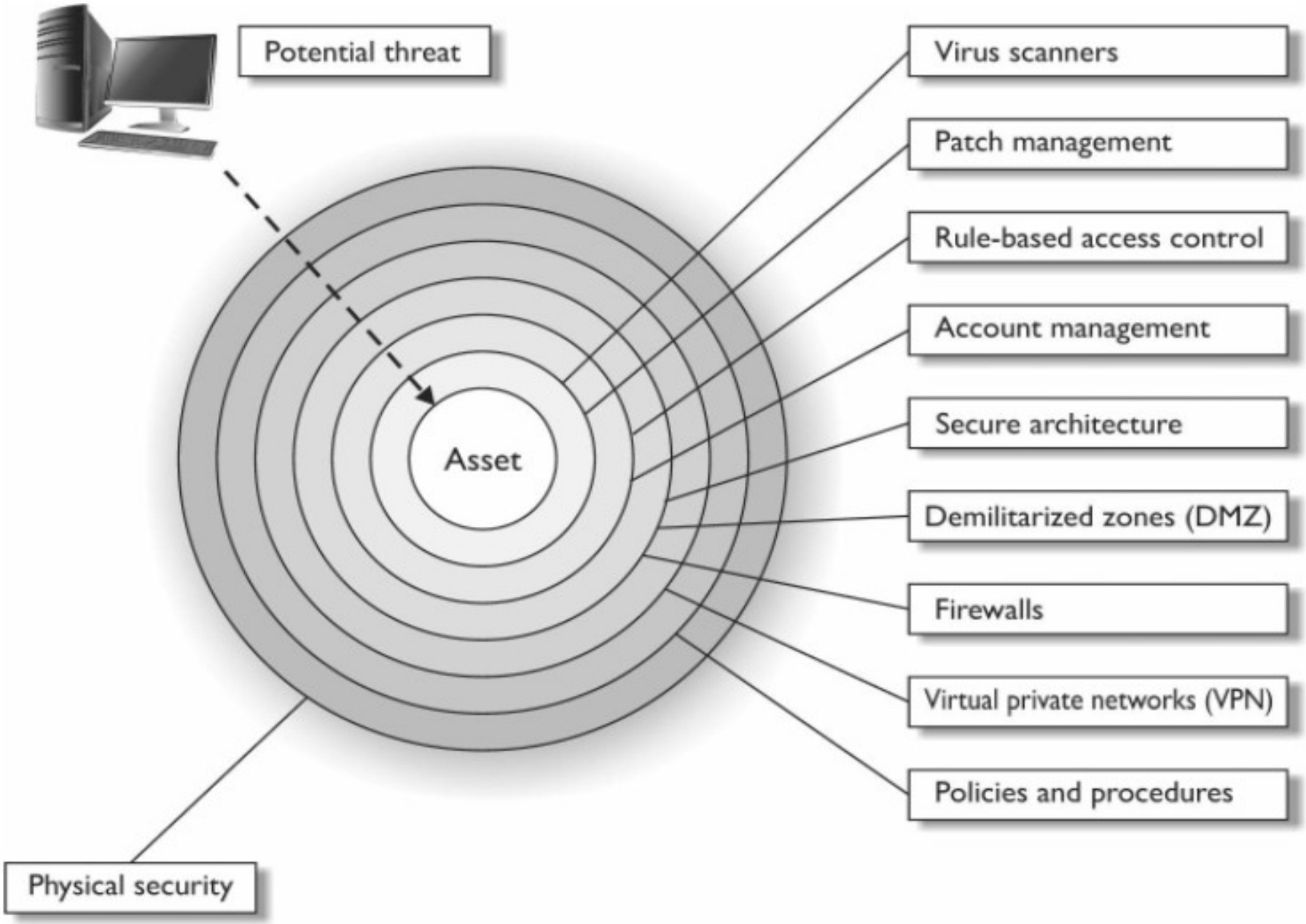
5 ways to keep end users safe

- Security awareness training
- Lock down the browser
- Automatically block access to malicious sites
- Keep up with workstation security patches
- Upgrade your anti-virus software

Creating engaging info-sec content

- Training every user is expensive
- Online Portal
  - Tutorials for staff and students
  - University ICT policy
- Handbooks

Defense in depth



Defense in depth

- Redundancy and resiliency
- Network segmentation
- Principle of least privilege
- Monitoring
- Security

Crime prevention through environmental design (CPTED)

- Discipline that outlines how proper design can reduce crime by directly affecting human behaviour
- CPTED strategies
  1. Natural access control
  2. Natural surveillance
  3. Natural territorial reinforcement

Designing a physical security program

Our security guards should wear pink uniforms and throw water balloons at intruders.

Designing a physical security program

- Facility
- Construction
- Entry points
- Computer and Equipment rooms

References

- Shon Harris, CISSP 6th edition
- Educause

QUESTIONS?

rosure@kenet.or.ke