Scalable Campus Networks Training
April 13 - 17 2015

Cyber Security

Ronald Osure, CEH

Agenda

- Introduction to security
- Attacks and Threats
- Host, Application and Data Security
- Vulnerability Assessment and Mitigating attacks

The CIA Triad

Confidentiality

Integrity

Availability

Fundamental principles of Security

- Availability
  - Reliable and timely access to data and resources to authorized individuals
- Integrity
  - This is upheld when the assurance of the accuracy and reliability of information and systems is provided and any unauthorized modification is prevented
- Confidentiality
  - Ensuring that the necessary level of secrecy is enforced at each junction of data processing and prevents unauthorized disclosure.

Key Terminologies

- **Vulnerability** Weakness or a lack of a countermeasure.
- **Threat agent** Entity that can exploit a vulnerability.
- **Threat** The danger of a threat agent exploiting a vulnerability.
- **Risk** The probability of a threat agent exploiting a vulnerability and the associated impact.
- **Control** Safeguard that is put in place to reduce a risk, also called a countermeasure.
- **Exposure** Presence of a vulnerability, which exposes the organization to a threat.

Attack Motivation

- Nations State want SECRETS
- Organized criminals want MONEY
- Protesters or activists want ATTENTION
- Hackers and researchers want KNOWLEDGE

Types of attacks

- Passive
- Active
- Distributed
- Insider
- Close in e.g social engineering
- Phishing
- Hijack
- Spoofing
- Buffer overflow

Host and Application Security

- System hardening
- Application firewalls and OS firewalls

Causes of attacks

- A look at the causes of attacks
  - Protocol error
  - Software bugs
  - Active attacks
  - Configuration mistakes

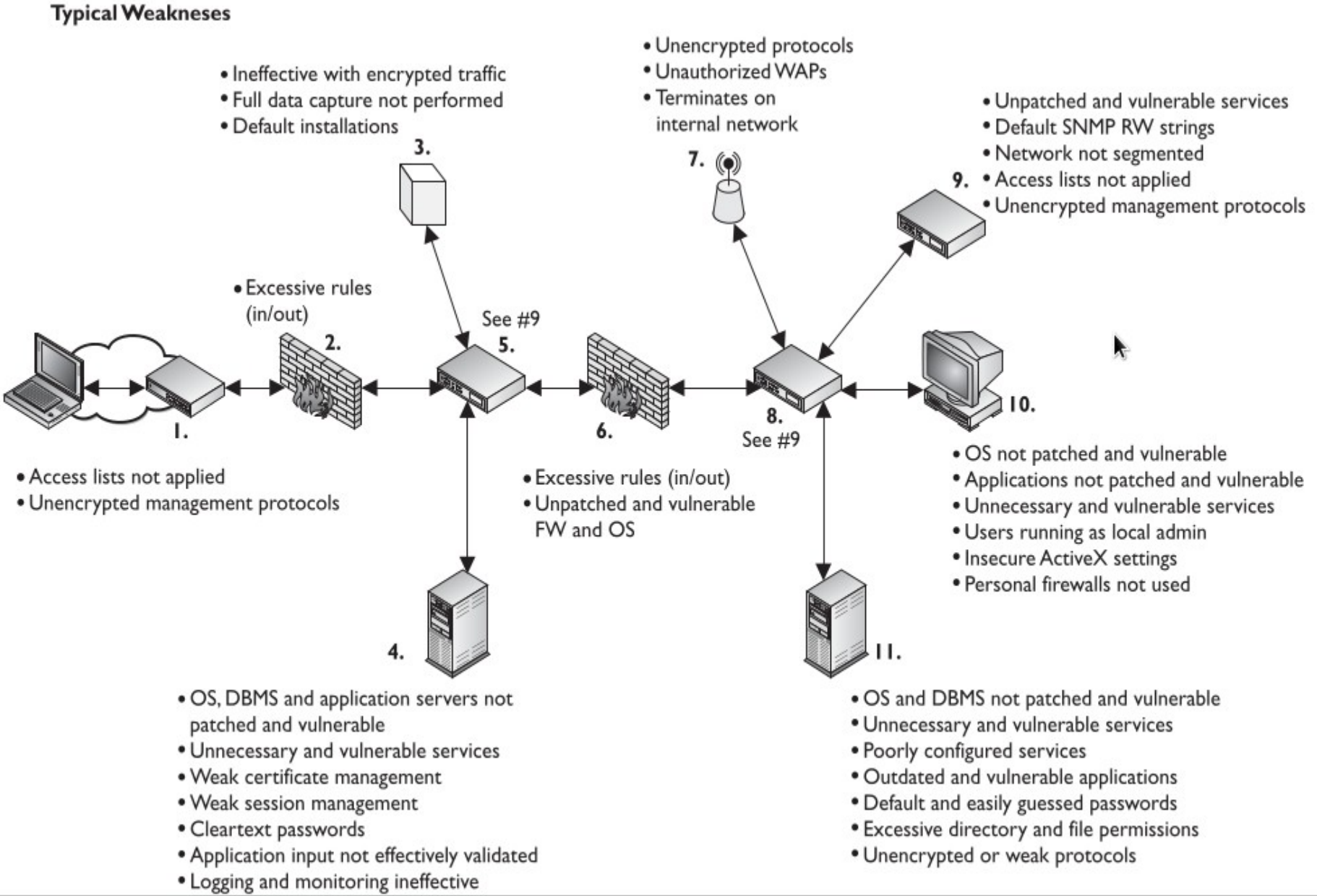
Mitigating Attacks

- Application whitelisting
- Patching applications
- **Patching operating systems**
- Minimize administration privileges

Vulnerability Testing

- Running a series of tests to establish exposure, security posture etc
- Goals of vulnerability Assessment
- Evaluate true security posture
- Identify as many vulnerabilities as possible
-

Typical weaknesses



Penetration Testing

Excuse me. Could you please attack me?
Response: I would love to!

Penetration Testing

Penetration testing is the process of simulating attacks on a network and its systems at the request of the owner, senior management

A penetration test emulates the same methods attackers would use.

References

- Shon Harris, CISSP 6th edition
- Educause

QUESTIONS?

rosure@kenet.or.ke