BASICS OF INFORMATION SYSTEM SECURITY

# User Authentication, Access Control, and Operating System



## **Video Summary**

- Operating System Strategy
- System Security Planning
- System Security Planning Process
- Operating System Hardening

#### **Strategies**

- The 2010 Australian Signals Directorate (ASD) lists the "Top 35 Mitigation Strategies"
- Over 85% of the targeted cyber intrusions investigated by ASD in 2009 could have been prevented
- The top four strategies for prevention are:
  - White-list approved applications
  - Patch third-party applications and operating system vulnerabilities
  - Restrict administrative privileges
  - Create a defense-in-depth system (layered defense mechanisms which increases the security of a system as a whole)

#### **Strategies**

 Since 2013 these top four strategies are mandatory for all Australian government agencies.

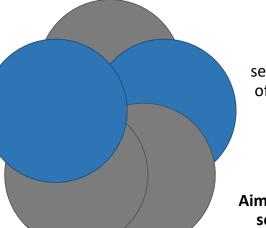
 These strategies largely align with those in the "20 Critical Controls" developed by DHS, NSA, the Department of Energy, SANS, and others in the United States

### **System Security Planning**

Plan needs to identify appropriate personnel and training to install and manage the system

Planning process needs to determine security requirements for the system, applications, data, and users

The first step in deploying a new system is planning



Planning should include a wide security assessment of the organization

Aim is to maximize security while minimizing costs

#### **System Security Planning Process**

The purpose of the system, Who will administer the the type of information Any additional security system, and how they will stored, the applications and measures required on the manage the system (via services provided, and their system, including the use of local or remote access) security requirements host firewalls, anti-virus or other malware protection mechanisms, and logging What access the system has The categories of users of to information stored on the system, the privileges other hosts, such as file or they have, and the types of database servers, and how information they can access this is managed How access to the

information stored on the

system is managed

How the users are

authenticated

### **Operating Systems Hardening**

- While the details of how to secure each specific operating system differ, the broad approach is similar.
- Appropriate security configuration guides and checklists exist for most common operating systems, and these should be consulted by the specific needs of each organization and their systems.

#### **Operating Systems Hardening**

- First critical step in securing a system is to secure the base operating system
- Basic steps
  - Install and patch the operating system
  - Harden and configure the operating system to adequately address the indentified security needs of the system by:
    - Removing unnecessary services, applications, and protocols
    - Configuring users, groups, and permissions
    - Configuring resource controls

#### **Operating Systems Hardening**

 Install and configure additional security controls, such as anti-virus, host-based firewalls, and intrusion detection system (IDS)

• Test the security of the basic operating system to ensure that the steps taken adequately address its security needs

## **Video Summary**

- Operating System Strategy
- System Security Planning
- System Security Planning Process
- Operating System Hardening