FANSHAWE

INFO-6003

O/S & Application Security

Week 03

FANSHAWE

Agenda

- Test Week 6 and Week 10 in Class time
- Access Control Principles
- Steps to Harden the Operating System
- Patch Management
  - Sources
  - Challenges
- Lab 02 Details

FANSHAWE

Access Control Principles

FANSHAWE

Access Control Principles

RFC 4949 defines computer security as:

> "Measures that implement and assure security services in a computer system, particularly those that assure access control service."

FANSHAWE

Access Control Terminology

- Reliable Input
  - The access control system needs to be sure the information it is using to control access is accurate
  - If filtering is being done by IP, there need to be validation mechanisms in place to ensure the IP is accurate
- Fine and Course Specifications
  - At times controlling access to a system itself will be enough (course specification), but where applicable much more control (fine specifications) should be available
  - Read, Write, Execute on specific files for example

FANSHAWE

Access Control Terminology

- Principle of Least Privilege
  - By default users should be given the minimum privilege level required for them to complete their duties
  - If a users shouldn't be able to delete files in a shared folder, only give them read access
- Separation of Duties
  - When you are dealing with complex processes that require multiple steps to implement, you should separate the duties/steps between multiple users
  - No one user controls the entire process

FANSHAWE

Access Control Terminology

- Open and Closed Policies
  - Closed Policy
    - By default everything is denied
    - Access is only given as required
  - Open Policy
    - By default everything is allowed
    - Access is restricted as required
- Policy Combinations and Conflict resolution
  - What happens when multiple policies apply to a given resource
  - Ensuring you get the right outcome if there is a conflict

FANSHAWE

Access Control Terminology

- Administrative Policies
  - Controlling which users can add, delete, or modify the access controls you have in place
  - Making sure users can't bypass these administrative policies
  - Your controls are only good if you know they are being applied and administered properly

FANSHAWE

Access Control Policies

- An access control policy, which can be embodied in an authorization database, dictates what types of access are permitted, under what circumstances, and by whom

FANSHAWE

Access Control Policies

- Access control policies are generally grouped into the following categories:
  - Discretionary Access Control (DAC)
  - Mandatory Access Control (MAC)
  - Role-Based Access Control (RBAC)
  - Attribute-Based Access Control (ABAC)

FANSHAWE

Access Control Policies

- Discretionary Access Control (DAC)
  - Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do
  - This policy is termed discretionary because an entity might have access rights that permit the entity, by its own volition, to enable another entity to access some resource

FANSHAWE

Access Control Policies

- Mandatory access control (MAC)
  - Controls access based on comparing security labels (which indicate how sensitive or critical system resources are) with security clearances (which indicate system entities are eligible to access certain resources)
  - This policy is termed mandatory because an entity that has clearance to access a resource may not, just by its own volition, enable another entity to access that resource

FANSHAWE

Access Control Policies

- Role-based access control (RBAC)
  - Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles

FANSHAWE

Access Control Policies

- Attribute-based access control (ABAC)
  - Controls access based on attributes of the user, the resource to be accessed, and current environmental conditions

Subjects, Objects & Access Rights

Subject

An entity capable of accessing objects

Three classes
- Owner
- Group
- World

Object

A resource to which access is controlled

Entity used to contain and/or receive information

Access Rights

Describes the way in which a subject may access an object

Could include:
- Read
- Write
- Execute
- Delete
- Create
- Search

FANSHAWE

Access Control - Subjects

- A subject is typically held accountable for the actions they have initiated, and an audit trail may be used to record the association of a subject with security relevant actions performed on an object by the subject

FANSHAWE

Access Control - Subjects

- Basic access control systems typically define three classes of subject, with different access rights for each class
  - **Owner:** This may be the creator of a resource, such as a file. For system resources, ownership may belong to a system administrator. For project resources, a project administrator or leader may be assigned ownership

FANSHAWE

Access Control - Subjects

- **Group:** In addition to the privileges assigned to an owner, a named group of users may also be granted access rights, such that membership in the group is sufficient to exercise these access rights. In most schemes, a user may belong to multiple groups

- **World:** The least amount of access is granted to users who are able to access the system but are not included in the categories owner and group for this resource

FANSHAWE

Access Control - Objects

- An object is a resource to which access is controlled
- In general, an object is an entity used to contain and/or receive information
- Examples include:
  - Records
  - Pages
  - Files
  - Directories
  - Programs
- Some access control systems also encompass, bits, bytes, words, processors, communication ports, clocks, and network nodes

FANSHAWE

Access Control - Objects

- The number and types of objects to be protected by an access control system depends on the environment in which access control operates and the desired tradeoff between security on the one hand and complexity, processing burden, and ease of use on the other hand

FANSHAWE

Access Control – Access Rights

- An access right describes the way in which a subject may access an object
- Access rights could include the following:
  - **Read**: User may view information in a system resource (e.g., a file, selected records in a file, selected fields within a record, or some combination)
  - Read access includes the ability to copy or print

FANSHAWE

Access Control – Access Rights

- **Write:** User may add, modify, or delete data in system resource (e.g., files, records, programs). Write access includes read access.
- **Execute**: User may execute specified programs.
- **Delete**: User may delete certain system resources, such as files or records.
- **Create**: User may create new files, records, or fields.
- **Search**: User may list the files in a directory or otherwise search the directory

FANSHAWE

Hardening the O/S

FANSHAWE

Access Control Terminology

- Securing the operating systems and applications on a system is also referred to as Hardening the system / OS
- Hardening the system has 3 main steps
  - Restrict and Control access
  - Remove Unused Services
  - Install Updates and Patches

FANSHAWE

Restrict & Control Access

FANSHAWE

Restrict & Control Access

- Follow the Principle of Least Privilege
- Create strong password policies
- Restrict permissions to system files
- Remove unused user accounts
  - Terminated employees
  - Temporary Contract Workers
- Disable Guest accounts
- Use Local Authentication or AAA servers

Remove Unused Services

FANSHAWE

Remove Unused Services

- Remove or disable services, applications, programs and utilities not being used on the system
- Many services run automatically at start up as part of the default installation
  - Disable all services that are not required for the programs running on the client or server

FANSHAWE

Remove Unused Services

- Determine which services are active on the server
  - Process Explorer, Task Manager, etc.
- Evaluate every service for need and risks
  - Operating system vendors install many services by default
  - Easier for users if the service or application was required in the future
  - Attackers have found flaws in many of these default services

Patch Management

FANSHAWE

Patches & Updates

- Keeping track of latest security updates
- Some applications have automatic notifications for registered users
- Others require the user to check a website for announcements
- Vendor websites
  - Mozilla Firefox
    - www.mozilla.org/security
  - Adobe
    - www.adobe.com/support/security
  - Apache
    - http://httpd.apache.org/security_report.html

FANSHAWE

Patch Management

- Patches are software updates that fall into 3 general categories
  - Security updates
    - Generally given High Priority
    - (in terms of implementation)
  - Program reliability improvements
    - Generally given Medium Priority
  - Program performance improvements
    - Generally given Medium to Low Priority
- Goal of patch management
  - Install updates in a reasonable time frame with minimal impact on the business

FANSHAWE

Vulnerability Scanners

- Vulnerability Scanners can assist with patch management
- There are many commercial vulnerability scanners available on the market
  - Tripwire
  - McAfee
  - Rapid7
  - Tenable
- We will use some open source scanners next semester in INFO-6065 and INFO-6009

FANSHAWE

Patch Management

- 4 phases of patch management
  - 1 – Assess
  - 2 – Identify
  - 3 – Evaluate & Plan
  - 4 – Deploy

Phase 1 - Assess

FANSHAWE

Patch Management - Assess

- The Assess phase deals with auditing the software & hardware in your production environment, evaluating potential security threats and vulnerabilities, and assessing your update management infrastructure.

- Inventory of existing computing assets. (initial audit)
  - Hardware types and versions
  - Operating systems and versions
  - Applications
  - How inventory items are being used
  - What data needs to be protected

FANSHAWE

Patch Management - Assess

- Assess security threats and vulnerabilities
  - Identifying security standards and policies
  - Determining how security policies and standards are to be enforced
  - Analyzing system vulnerabilities
- Determine the best source for information about new software updates
  - What is the best source of information for updates
    - E-mail notifications, Web Sites, etc.

FANSHAWE

Patch Management - Assess

- Assess the existing software distribution infrastructure
  - Is there a mechanism in place to deploy updates
    - WSUS for example
      - Windows Server Update Services
- Assess operational effectiveness
  - Do you have enough trained employees
  - Do you have a change management process in place
  - Are you doing continuous auditing

Phase 2 - Identify

FANSHAWE

Patch Management - Identify

The Identify phase deals with the reliable discovery of new software updates, whether new updates are relevant to your production environment, and whether an update represents a normal or emergency change.

- Discover new software updates
  - Setting up notifications
  - Reading security bulletins for sites you found in the Assess phase

FANSHAWE

Patch Management - Identify

- Determine whether new updates are required in your environment.
  - Does the specific update or patch apply to your setup
    - Whether you need to patch Server 2008R2, for example, may depend on whether you have certain roles and feature enabled
- Obtain software update source files and confirm that they are safe and will install successfully.
  - Ensure you are getting files from an authorized source
  - The hardware manufacturers site, not drivers-r-us.com

FANSHAWE

Patch Management - Identify

- Determine whether the software update should be considered a normal change or an emergency

Phase 3 – Evaluate & Plan

Patch Management – Evaluate & Plan

The Evaluate and Plan phase deals with deciding whether to deploy an update, determining what is needed to deploy it, and testing the software update in a production-like environment to confirm that it does not compromise business-critical systems and applications.

- Determine the appropriate response
  - Deploying update, Applying countermeasures, or Both

FANSHAWE

Patch Management – Evaluate & Plan

- Plan the release of the software update
  - What actually needs to be updated
  - What are the issues and constraints associated with the release
- Build the release
  - What procedures will be used to deploy the release
    - Scripts, tools, etc.
- Conduct acceptance testing of the release
  - Make sure the update works in your environment
  - Test on a small group of users
  - Simulates a production environment

Phase 4 - Deploy

Patch Management – Deploy

The Deploy phase deals with the successful rollout of approved software updates within the production environment

- Prepare for deployment
  - Communicate timeframe to affected staff
  - Stage deployment in WSUS or relevant management system

FANSHAWE

Patch Management – Deploy

- Deploy a software update to targeted computers.
  - Letting staff know the update/patch is about to install
  - Monitoring the deployment
  - Handling failures
- Review the deployment, post-implementation.
  - What can you learn from the deployment
  - Improvements for the future

FANSHAWE

Patch Management Sources

FANSHAWE

Patch Management – Sources

- Microsoft Technical Security Notifications
  - E-mail or RSS feeds
  - https://technet.microsoft.com/en-us/security/bulletins.aspx
- Microsoft Security Resource Centre Blog
  - Blog can be fast method to alert of security vulnerability
  - http://blogs.technet.com/msrc
- US-CERT
  - US Computer Emergency Readiness Team
  - www.us-cert.gov

FANSHAWE

Patch Management – Sources

- SANS Internet Storm Center
  - Storm Center diary is filled out by SANs incident handlers
  - http://isc.sans.org
- National Vulnerability Database
  - https://nvd.nist.gov

FANSHAWE

Patch Management – Sources

- Full Disclosure Mailing List
  - Discusses security vulnerabilities on a wide range of products
  - Software vulnerability could be placed on the list before vendor has a patch to fix the problem
    - You should know what the bad guys know
- All major software vendors have web site that notify when a patch is available
  - Adobe, Oracle, Apache, Sun Microsystems, Mozilla Firefox

FANSHAWE

Microsoft Security Bulletins

- Review these bulletins for critical and important vulnerabilities
- Bulletins are given a rating of
  - Critical, Important or Moderate
  - Will list the operating system version and service pack affected
  - Will list the software program affected

FANSHAWE

Microsoft Security Bulletins

- Each bulletin is linked to a page with an
  - Executive summary
  - A list of operating systems and versions affected
    - Windows Server R2 x64 Service Pack 1
    - Windows 7 for 32 bit systems
    - etc.
  - A vulnerability section that gives a more detailed description and links to related CVE bulletin

CVE

- CVE - Common Vulnerabilities & Exposures
- cve.mitre.org
- Information on publicly known vulnerabilities
- Reported by public
- Over 64,000 CVEs
- Mitre board reviews and determines if the vulnerability should be listed
  - Candidate vulnerabilities receive a number but are still under review

SANS Top 20

- First list complied in year 2000 and listed top 10 vulnerabilities
- In 2001 it was expanded to 20 vulnerabilities in 3 categories
  - General vulnerabilities
  - Windows vulnerabilities
  - Unix vulnerabilities
- In 2002 the list comprised the top 10 Windows & top 10 Unix vulnerabilities

FANSHAWE

SANS Top 20

- In 2005 the top 20 was changed to add categories for
  - cross platform applications
  - Networking products
- In 2007 the format was changed again to identify
  - Client side vulnerabilities
  - Server side vulnerabilities
  - Application abuse
  - Security Policy & Personnel
  - Network devices
  - Zero day attacks

FANSHAWE

SANS Top 20

- Today the list has been renamed:
  - The Top Cyber Security Risks
  - http://www.sans.org/top-cyber-security-risks/?ref=top20
- The Top Cyber Security Risks now takes the form of a report on the state of security

Patch Management Challenges

FANSHAWE

Patch Management Challenges

- Patches are Often Not Applied
- Companies get overwhelmed by the number of patches
  - May use many software products
  - Vendors release many patches per product
  - Might simply lack the resources to apply all patches
    - People and time
  - May lack off hours windows for deployment

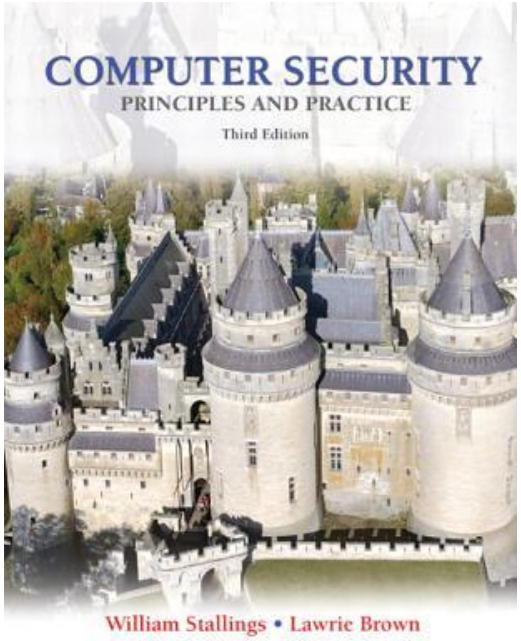
FANSHAWE

Patch Management Challenges

- Risks of Patch installation
  - Could result in reduced functionality
  - Sometimes there is no uninstall possible
    - Special problem for mission-critical production systems that must work
- Deployment issues
  - Group policies that block software installation
  - Disk space required for update (SANs)
  - Down time for high availability servers

Homework

- Finish Reading Chapter 4 Sections
  - 4.7 – Identity, Credential, and Access Management
- Read Chapter 12 Sections
  - 12.1 – Introduction to Operating System Security
  - 12.2 – System Security Planning
  - 12.3 – Operating System Hardening



FANSHAWE

Lab 02 – Gathering Information

FANSHAWE

Lab 02 Details

- You don’t need VM-Workstation this week
- You are going to be exploring the various resources we have at our disposal as IT administrators to keep ourselves informed
- You need to have MS Word installed for this lab
  - You get a free copy through the FSU