Cybersecurity Essentials

Module 7: The Windows Operating System

Lecture Notes with Lab Exercise Guidelines

Undergraduate Level — Washington Accord (Bloom C3 & C4)

Module Learning Objectives

After completing this module, students will be able to:

- Explain Windows architecture, processes, memory, and registry concepts.
- Apply Windows administrative tools to manage users and monitor system behavior (C3).
- Analyze system activity to identify abnormal or suspicious behavior (C4).
- Perform guided laboratory exercises using built-in Windows tools.

1 Windows Architecture and Operation

1.1 Hardware Abstraction Layer (HAL)

Windows runs on a wide variety of hardware. The Hardware Abstraction Layer (HAL) is a software layer that isolates the operating system kernel from hardware differences.

Why HAL is important:

- Allows Windows to run on different CPUs and devices
- Prevents applications from directly accessing hardware
- Improves stability and portability

1.2 User Mode and Kernel Mode

Windows uses two CPU execution modes:

- **User Mode**: Applications run with restricted access.
- **Kernel Mode**: OS components run with full hardware access.

This separation prevents user applications from crashing or corrupting the operating system.

Security implication (C4): If malware executes in kernel mode, it gains unrestricted access, making detection and removal very difficult.

2 Windows File Systems and Storage

2.1 NTFS Overview

NTFS is the default Windows file system due to:

- Support for large files and partitions
- File and folder permissions
- Journaling and recovery features

2.2 Alternate Data Streams (ADS)

NTFS allows files to contain multiple data streams:

```
example.txt:hidden
```

ADS can be abused by attackers to hide malicious content.

Analytical Insight (C4): ADS content is not visible in standard directory listings, making it useful for stealth persistence.

3 Windows Processes, Threads, and Handles

3.1 Processes and Threads

- A **process** is a running program.
- A **thread** is a unit of execution within a process.

Windows uses multithreading to improve performance and responsiveness.

3.2 Handles

Handles are references that allow user-mode processes to safely access kernel resources such as files, registry keys, or memory.

Security note: Excessive or unusual handle usage may indicate malicious behavior.

4 The Windows Registry

The Windows Registry is a hierarchical database storing configuration data.

4.1 Registry Structure

- HKEY_LOCAL_MACHINE (system-wide settings)
- HKEY_CURRENT_USER (current user settings)
- HKEY_USERS (all user profiles)

Warning: Improper registry modification can cause system instability or failure.

5 Windows User and Account Management

5.1 Least Privilege Principle

Users should operate with standard privileges and elevate permissions only when necessary.

Why this matters (C4):

- Limits malware damage
- Reduces accidental system changes

5.2 Users, Groups, and Domains

- Permissions are assigned to groups, not individuals.
- Domains centralize authentication and security policies.

6 Windows Administrative and Monitoring Tools

6.1 Task Manager

Task Manager provides real-time visibility into:

- Running processes
- CPU, memory, disk, and network usage

Sorting by memory or CPU usage helps identify abnormal behavior.

6.2 PowerShell

PowerShell is both a command-line interface and scripting language.

```
Get-Process
Get-ChildItem
```

PowerShell is widely used for automation and remote administration.

6.3 Netstat and Process Correlation

```
netstat -abno
```

This command links network connections to specific processes using Process IDs (PIDs).

7 Guided Laboratory Exercises

7.1 Lab 1: Exploring Processes and Threads

Objective: Understand parent-child processes and thread behavior.

Steps:

1. Launch a web browser and Command Prompt.
2. Open Task Manager and observe running processes.
3. Close Command Prompt and note which processes terminate.

Expected Outcome: Child processes terminate when their parent process ends.

7.2 Lab 2: Exploring the Windows Registry

Objective: Safely view registry keys.

Steps:

1. Open `regedit`.
2. Navigate to HKEY_CURRENT_USER.
3. Identify application-specific configuration entries.

Caution: Do not modify keys unless instructed.

7.3 Lab 3: Creating and Managing User Accounts

Objective: Apply least privilege.

Steps:

1. Create a new local user.
2. Verify file access permissions.
3. Temporarily assign and remove administrator privileges.

Reflection (C4): Why should administrative rights be temporary?

7.4 Lab 4: Monitoring System Resources

Objective: Identify performance issues.

Steps:

1. Open Task Manager and Performance Monitor.
2. Observe CPU and memory usage during application load.
3. Log memory usage over time.

Analysis (C4): Steady memory decline may indicate a memory leak or runaway process.

Conclusion

These lecture notes integrate Windows operating system theory with practical laboratory exercises. Students learn not only how Windows works, but how to apply administrative tools and analyze system behavior in a security context, fulfilling Washington Accord outcomes at Bloom's C3 and C4 levels.