Week 4 Foundation

Week 4 Module: Operating System and Network Security in Pract

Primary textbook focus: Chapter 5 advanced concepts and Chapter 6 network defenses

Theme: keep systems trustworthy when endpoints and networks are under active pressure

Deliverables: quick lab, in-class reading response, and operational decision making

Week 4 Foundation

How Week 4 Builds on Week 3

Week 3 covered programming flaws, web attacks, and operating-system fundamentals

Week 4 extends to hardening, monitoring, containment, and recovery workflows

Main shift: from naming vulnerabilities to prioritizing controls and ownership

Week 4 Foundation

Learning Objectives

Explain how host-level controls enforce trust at runtime

Analyze network attack paths and map layered defenses

Prioritize containment actions using impact and feasibility

Evaluate privacy and ethics tradeoffs in security monitoring

Produce concise, professional security analysis artifacts

Essential Questions

What makes a host control trustworthy in adversarial conditions?

Why do network attacks often succeed despite multiple tools?

How should teams prioritize containment in the first 30 minutes?

When does security monitoring become a privacy risk?

Chapter 5 Advanced Focus: Host Trust Under Attack

Operating system controls are foundational to all upper-layer security

Host compromise can neutralize detections, logs, and policy enforcement

Design goal: preserve mediation, visibility, and recovery options

Privilege Escalation Mechanics

Escalation converts limited footholds into broad control

Common paths include weak service permissions and token abuse

Least privilege and separation of duties reduce blast radius

Host Hardening Baseline

Patch discipline, service minimization, and secure configuration baselines

Application allowlisting and execution policy constraints

Administrative access controls with strong authentication

Documented exceptions with expiration and review

Endpoint Telemetry: Logging, Alerts, and Signal Quality

Collect process, authentication, integrity, and network telemetry

Prioritize high-confidence alerts to reduce fatigue

Preserve forensic value through integrity and retention controls

In-Class Reading Response (10-12 Minutes)

Read the provided excerpt on zero trust and monitoring ethics

Write a 250-300 word response using claim, evidence, and counterargument

Connect one technical control choice to one ethical principle

Chapter 6 Focus: Network Security as Systemic Resilience

Networks carry both business value and attack opportunity

Remote attacks can scale faster than host-local attacks

Design objective: preserve service, trust, and detection visibility

Network Model and Trust Boundaries

Data flows through layered protocols with different control responsibilities

Every boundary crossing needs identity, integrity, and policy checks

Routing and addressing decisions influence exposure paths

Threat Class 1: Interception and Eavesdropping

Attackers capture traffic to extract credentials or sensitive data

Insecure links and weak encryption increase interception risk

Mitigations include strong transport encryption and key hygiene

Threat Class 2: Modification and Fabrication

Adversaries alter packets, commands, or responses in transit

Forgery can produce unauthorized actions while appearing legitimate

Integrity controls and authentication reduce manipulation risk

Threat Class 3: Interruption and Denial of Service

Goal is to degrade or stop service delivery

DoS and DDoS exploit capacity limits and dependency fragility

Resilience requires architecture, not only edge filtering

Reconnaissance: Port Scanning and Service Discovery

Scanning maps reachable hosts, services, and likely weaknesses

Unnecessary exposed services increase attack options

Rate limits, segmentation, and monitoring reduce reconnaissance value

Segmentation and Network Access Control

Segment by business function and sensitivity, not just by convenience

Use least-privilege connectivity between zones

NAC policies can enforce device and identity posture before access

Cryptographic Protection for Network Traffic

Use modern TLS configurations for in-transit confidentiality and integrity

Use VPN or tunnel protections where network trust is low

Certificate lifecycle and key management are critical dependencies

Zero Trust Network Access (ZTNA)

Never assume trust based only on network location

Continuously verify identity, device posture, and request context

Limit access to specific resources rather than broad network segments

DDoS Readiness Strategy

Plan capacity, upstream support, and traffic filtering before incidents

Define critical services and graceful-degradation priorities

Practice communication and escalation for fast coordinated response

Network Management and Change Governance

Maintain accurate inventories for assets, dependencies, and routes

Review security impact for every meaningful network change

Use post-change validation to confirm policy behavior

Privacy and Ethics in Network Monitoring

Monitoring improves detection but can over-collect user data

Data minimization and purpose limitation reduce privacy harm

Transparent policy and access controls preserve institutional trust

Applied Walkthrough

Applied Incident Walkthrough: Campus Service Disruption

Incident issue: likely credential theft enabled unauthorized privileged access
Observed behavior: unsigned process execution on ADV-WS-14 and 7x outbound HTTPS spike
Operational impact: campus portal latency increased 48% with failed student transactions
Decision challenge: contain fast while preserving critical service continuity and evidence

Applied Walkthrough

Incident Timeline

T0: unusual authentication pattern appears on one privileged account

T+20: endpoint telemetry shows suspicious process behavior

T+45: network congestion and failed transactions increase rapidly

T+70: team initiates containment and communication protocol

Applied Walkthrough

Detection Quality Review

High-confidence signals should trigger immediate analyst review

Weakly tuned alerts can hide important patterns

Correlation across host and network data improves confidence

Applied Walkthrough

Containment Decision Matrix

Option A: isolate affected endpoints immediately

Option B: block suspicious network paths while preserving core services

Option C: rotate credentials and force reauthentication quickly

Best practice: combine options based on evidence and service criticality

Applied Walkthrough

Recovery and Post-Incident Governance

- Validate system integrity before full service restoration
- Document root cause and control gaps with accountable owners
- Update policies, playbooks, and training based on lessons learned
- Communicate clearly with affected users and stakeholders

Quick Lab

Quick Lab: Overview

Task: classify evidence, map CIA impact, and prioritize controls

Output: one-page mitigation brief with named owners