Week 6 Security Foundations

Bridging Security Theory with Windows Server Practice

Class code

gxgxvq4

Course name: Server Management Course code:IT420

4th Year IT Department, Tishk International University
Lecturer: Mohammad Salim Al-Othman

Quick Glossary

Acronym	Expanded Term	One-Line Meaning
ABAC	**Attribute-Based Access Control**	Dynamic rights based on user & resource attributes
AD DS	Active Directory Domain Services	Directory service storing users, groups, and policies
CIA	**Confidentiality • Integrity • Availability**	Classic security objectives
JEA	**Just Enough Administration**	PowerShell endpoint with least-privilege cmdlets
Kerberos	–	Ticket-granting authentication protocol
PKI	**Public-Key Infrastructure**	Certificates; trust & encryption
RPO/RTO	Recovery Point / Time Objective	Acceptable data loss / downtime
STRIDE	Spoofing • Tampering • Repudiation • Info Disclosure • DoS • Elevation	Threat model mnemonic
TCB	**Trusted Computing Base**	Minimal code that must remain secure
Zero Trust	–	"Never trust, always verify"

RBAC (Role-Based Access Control)

TLS = Transport Layer Security
(It is the successor to **SSL** – Secure Sockets Layer.)

RAID (Redundant Array of Independent Disks)

WDAC (Windows Defender Application Control)

SMB (Server Message Block) is a **network file sharing protocol**

MFA (Multi-Factor Authentication)

Azure Active Directory (AAD)

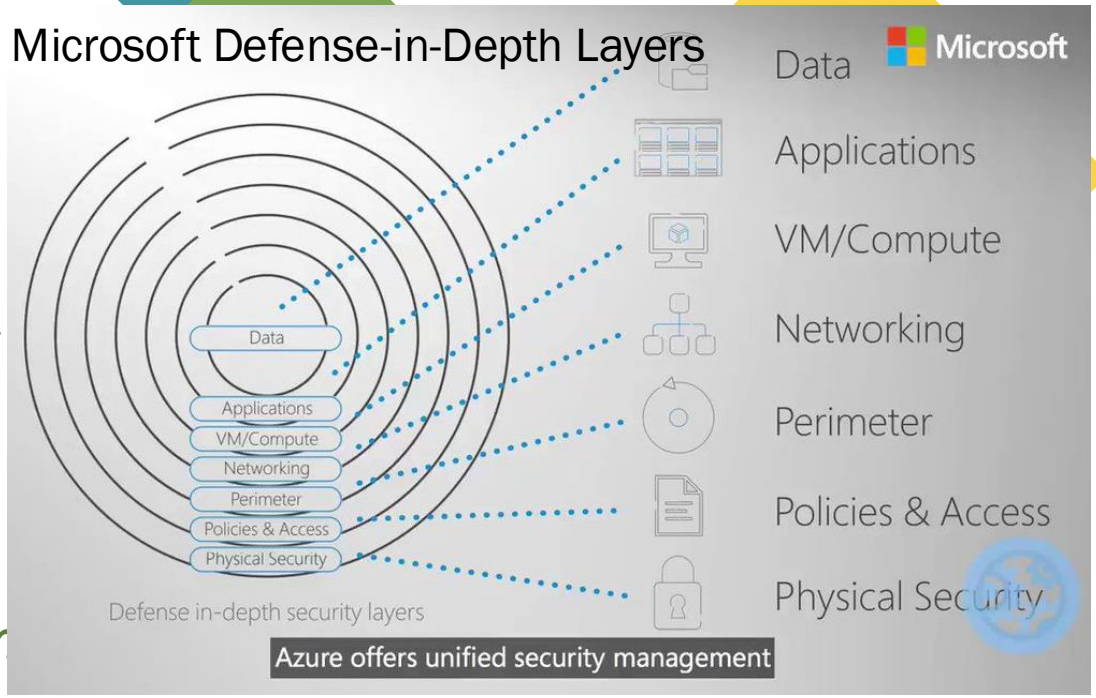
Lecture Road-Map

(how theory blocks map to labs)

1. Models & Frameworks → Hardening baseline lab- CIS Controls, NIST SP 800-53, and Zero Trust Architecture.
2. Identity / Access → AD DS & RBAC lab
3. Threat Modeling → STRIDE worksheet + attack-tree build
4. Design Principles → Server role install exercise
5. Policy Management → Group Policy baseline lab
6. Information Protection → BitLocker + TLS demo
7. Resilience & Recovery → Backup & restore lab
8. Monitoring & IR → Defender alert hunt lab

Security Models & Frameworks

- CIA Triad : foundation for every feature (e.g., BitLocker → RAID → *A*)
- Defense-in-Depth : layered firewall + WDAC + backups
- Least Privilege : built-in *Server Operators* vs *Domain Adm*
- Zero Trust: every SMB share now requires authenticated access, and encryption can be enforced per share or globally via Group Policy to prevent eavesdropping.



Pillar	1-line definition
Confidentiality (C)	Keep data secret from the wrong eyes
Integrity (I)	Ensure data and code aren't tampered with
Availability (A)	Keep services up and data accessible

https://azure.microsoft.com/en-us/blog/microsoft-azures-defense-in-depth-approach-to-cloud-vulnerabilities/

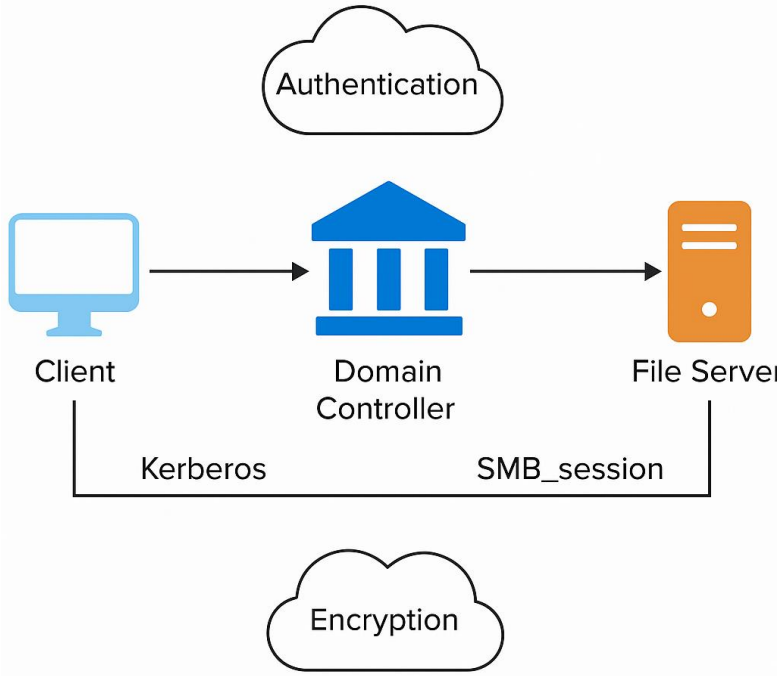
MSFT diagram of layered defenses.

Microsoft "Defense-in-Depth" concentric-ring model

The official Azure SQL security page illustrates Microsoft's standard layered-defense concept: seven security rings that wrap ever-tighter protections around your data.

Ring	What's protected	Typical Microsoft controls & examples
Physical Security	Datacenter buildings, power, HVAC, hardware	Multi-factor badge gates, perimeter fencing, CCTV, hardware root-of-trust chips Microsoft Learn
Identity & Access	People & services that request resources	Entra ID MFA, Conditional Access, PIM, RBAC
Perimeter	Internet edge & DDoS mitigation	Azure DDoS Network Protection, Azure Firewall, WAF on Front Door
Network	East-west traffic inside your virtual networks	NSGs, Private Link/Endpoints, Micro-segmentation, VPN/ExpressRoute Microsoft Learn
Compute	VMs, containers, serverless runtimes	Secure Boot, Azure Disk Encryption, Defender for Cloud endpoint protection
Application	Code & runtime components you deploy	Key Vault for secrets, App Gateway WAF, DevSecOps pipelines
Data	SQL, Storage, blobs, secrets	TDE, Azure Backup, Purview sensitivity labels, Customer-managed keys

SMB



- 💡 **SMB = Server Message Block**
  Windows protocol for sharing files, folders, printers across the network.
- **Used in: \\ServerName\Share, File Explorer, network drives, etc.**
- SMB is what powers \\fileserver\students — if you've ever opened a shared folder, you've used SMB.
- SMB is how Windows lets one computer read or write files on another over the network — just like opening \\Server\HR from your PC. Behind the scenes, SMB does login checks, checks permissions, and (in modern versions) encrypts everything.

Identity & Access Control Theory

- Authentication vs Authorization : Kerberos handles *auth*; group membership handles *authz*
- Kerberos Flow(Kerberos Ticket-Granting Ticket (TGT)) : Client →KDC ↔ Service Ticket
- RBAC : *Backup Operators* group limited to ntbackup.exe
- ABAC: Dynamic Access Control: file read if Department=Finance & Sensitivity<Secret
- PKI: Smart-card logon → cert mapped to AD user

Threat Modeling (STRIDE)

STRIDE	Example on Windows Server
Spoofing(pretending to be someone else)	Pass-the-Hash to impersonate admin
Tampering (altering data/code)	Registry key edit to alter service binary
Repudiation (denying an action)	Clear Event Logs to deny action
Info Disclosure (data leak)	SMB share with world-readable finance.xlsx
DoS Denial of Service (blocking service)	Flood SMB 445; exhaust worker threads
Elevation of Privilege (gaining higher rights)	Token impersonation via insecure service perms

What are attack trees ?

Attack trees are conceptual diagrams that show the variety of ways in which something can go wrong, and the reason why they might go wrong. In cyber security, you can investigate the different ways that a system might be attacked, or how an attacker might achieve a specific objective.

Security Design Principles

- Secure by Default : Windows blocks all inbound traffic by default using the firewall — nothing listens unless you open it.
- Secure by Design : Code signed drivers enforced by WDAC(Windows Defender Application Control)
- Security-through-Obscurity ≠ Security : Renaming Administrator account ≠ sufficient
- Trusted Computing Base (TCB) : Core system parts like the kernel and Hyper-V hypervisor — must stay secure, as everything depends on them.
- Attack Surface Reduction : (e.g., IIS, FTP) with Remove-WindowsFeature — fewer services = fewer ways to get hacked.

Policy-Based Security Management

- Policy Hierarchy: Org-wide (Governance) → Technical (GPO) → Enforcement (WDAC)
- Management vs Technical Policy: “Require MFA” doc vs actual AAD rule
- Lifecycle: Create → Approve → Implement → Monitor → Retire(when outdated)
- Conflict Resolution: GPO precedence (L-S-D-O-U) beats overlapping Intune policy

“Local → Site → Domain → OU — then the specific Unit you’re in.”

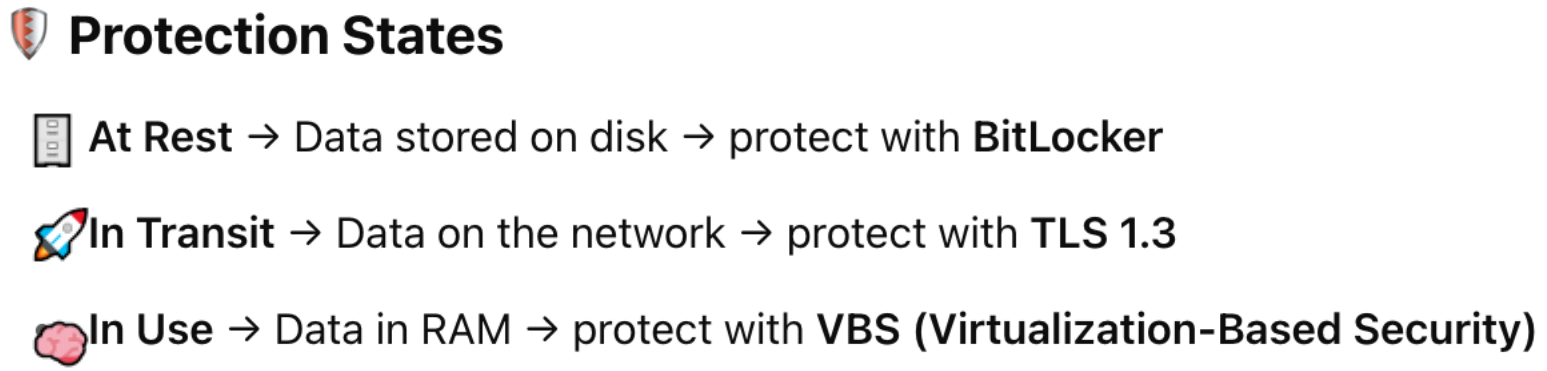
🧠 “Governance sets the rules, GPO applies them, and WDAC enforces them.”

Information Protection Concepts

- Data Classification : Public • Internal • Confidential • Secret
- Crypto Foundations : AES (symmetric) vs RSA (asymmetric)
- Protection States : At Rest (BitLocker), In Transit (TLS 1.3), In Use (VBS-shielded)
- Data Loss Prevention : DLP rules block Outlook attachment > 1 GB classified “Secret”

“We classify data, encrypt it at every stage, and use DLP to stop leaks.”

Quick Quiz: *SMB - Server Message Block (SMB) signing—rest or transit?*



Resilience & Recovery Theory

⏱️ RPO vs RTO

- **RPO** (Recovery Point Objective) = How much data you can lose → *15 mins*
- **RTO** (Recovery Time Objective) = How fast to recover → *4 hours*

💾 Backup Strategies

- **Full** = complete backup every Sunday
- **Differential** = changes since last full (Mon–Thu)
- **Incremental** = changes since last backup (Fri–Sat)

ACLs = Access Control Lists

They are **lists of permissions** attached to files, folders, or objects that **define who can do what.**

🧠 "We plan backups and failover based on how much data loss and downtime we can tolerate."

🧨 Attack Kill Chain

The 7 steps of a cyberattack:

Recon → Weaponize → Deliver → Exploit → Install → Command & Control (C2) → Action

> Helps defenders break the chain early (e.g., block delivery or exploit).

🔁 OODA Loop

Observe → Orient → Decide → Act

> A decision-making model used in **SOC playbooks** to **respond fast and adapt** to threats.

real-world threats: “Phishing alert detected ⟶ isolate user ⟶ reset credentials”

📉 Signal-to-Noise

Out of **100,000 daily logs**, maybe **500 matter** — tools and analysts must filter **the real threats**.

🕵️ Root Cause Analysis (RCA)

Use **5 Whys** to dig deep:

> “Why did the patch fail?” → leads to **true cause** of the breach.

Tishk International University

Security Monitoring & Incident Response

Understand how attacks happen, respond smartly, focus on real threats, and fix the root, not the symptom.

SOC playbooks are **step-by-step guides** that security analysts follow in a **Security Operations Center (SOC)** to detect, investigate, and respond to cyber threats.

ⓘ Reference: *“Backup and Disaster Recovery for Your Data and Applications in Azure”* (Microsoft white-paper, PDF).
https://download.microsoft.com/download/8/6/7/8676f96b-5802-4cfd-8bda-ec6ae73d27dc/BCDR_AAC_Part1_Strategic.pdf
download.microsoft.com

Roles and Responsibilities

- 🔵 Blue team- SOC Analysts: Monitor logs, classify threats (STRIDE), suggest alerts or responses
- 🟢 Green team- Server Admins: Find misconfigs, harden AD/SMB, apply GPO/WDAC
- 🔴 Red team- Red Team: Think like attackers, propose realistic exploits
- 🟡 Golden team- Incident Manager (Optional): Balance lockdown vs. availability, track RTO/RPO

Check Your Understanding

1. Match each STRIDE element to a Windows Server example.
2. Define RBAC vs ABAC in one sentence each.
3. Which CIA Triad pillar is impacted first by a ransomware attack?

Conclusion

- Key Takeaways
  - CIA Triad underpins every Windows-Server control.
  - Defense-in-Depth & Zero Trust call for *layered* and *continuous* verification.
  - Policy hierarchy links governance → GPO/Intune → enforcement (WDAC, ASR).
  - Resilience is security's safety net: backups, RPO/RTO, fault tolerance.
- From Theory to Practice
  - Map each concept to its matching Windows feature (e.g., ABAC → Dynamic Access Control).
  - Use threat-model outputs (attack trees) to prioritize hardening tasks.
  - Validate with monitoring & incident-response playbooks.
- What's Next
  - Hands-on labs begin next session (baseline import, AD DS hardening).
  - Suggested reading: MS SDL whitepaper, NIST SP 800-53 Rev 5 mappings.

Thank you

Mohammad Salim-

IT Dept- Applied Science Faculty- TIU University

mohammad.salim@tiu.edu.iq

Class code

gxgxvq4

“Security is not a product, but a process.” – Bruce Schneier