STUDENT HANDOUT · WEEK 8

Review and Midterm: Weeks 1 to 7

SY0-701 objectives 1.1, 1.2, 1.3, 1.4, 2.1, 2.3, 2.4, 3.1, 5.2. Notes, exercises, review questions, and the lab.

Name	
Date	

THIS WEEK YOU WILL

1. Classify any control by category and type, and avoid the deterrent and compensating traps.
2. Calculate SLE, ALE, and a control's net benefit, and match RTO, RPO, MTTR, and MTBF to scenarios.
3. Explain CIA, non-repudiation, AAA, zero trust, and deception technology in plain terms.
4. Match a cryptographic tool to what it provides: confidentiality, integrity, or non-repudiation.
5. Identify the threat actor, vector, and vulnerability in a short scenario.
6. Connect an indicator of malicious activity to the mitigation that blunts it.
7. Compare the security implications of cloud, on-premises, IoT, ICS, and embedded architectures.

KEY IDEAS

One category, one or more types

Control	Category	Type
Firewall access control list	Technical	Preventive
Visible camera at a door	Physical	Detective and deterrent
Acceptable use policy	Managerial	Directive
Restore from backup	Technical	Corrective
Monitoring an unpatchable PC	Technical	Compensating
Awareness training	Operational	Preventive and directive

The ideas every control serves

CIA triad	Confidentiality, integrity, and availability. (Encryption, hashing, redundancy)
Non-repudiation	Proof a party acted, so they cannot deny it. (Digital signature)
AAA	Authenticate, authorize, and account for users. (RADIUS with logging)
Zero trust	No trust by location; verify every request. (Policy engine and PEP)
Physical security	Bollards, vestibules, guards, badges, sensors. (Access control vestibule)
Deception	Decoys that alert the moment anyone touches them. (Honeyfile on a file share)

Show every step of the risk math

$100,000	Asset value (AV)
30%	Exposure factor (EF)
$30,000	SLE = AV x EF
0.5	ARO, once in two years
$15,000	ALE = SLE x ARO
	A control is worth buying when the drop in ALE is larger than the control's yearly cost.

Every change follows the same path

1. Request	Owner submits purpose, scope, and timing.
2. Impact analysis	Name affected systems, dependencies, and downtime.
3. Approve	Change board or owner signs off; stakeholders agree.
4. Test	Prove the change in a test environment first.
5. Implement	Change in the maintenance window, backout plan ready.
6. Document	Update diagrams, policies, and version control.

Match each crypto tool to its job

Tool	Provides	Exam trap
Symmetric (AES)	Confidentiality, fast bulk encryption	Sharing the key safely is the hard part
Asymmetric (RSA, ECC)	Key exchange and signatures	Encrypt with the recipient's public key
Hashing (SHA-256)	Integrity	One way; hashing is not encryption

Tool	Provides	Exam trap
Salting	Unique hashes for equal passwords	Defeats rainbow tables, not weak passwords
Digital signature	Integrity, authentication, non-repudiation	Signed with the sender's private key
Certificates and PKI	Bind a public key to an identity	CRL and OCSP check revocation

Resources and motivation identify the actor

Actor	Resources	Typical motivation
Nation-state	Very high; long, stealthy campaigns	Espionage, war, disruption
Organized crime	High; run like a business	Financial gain
Hacktivist	Varies	Philosophical or political beliefs
Insider threat	Access already granted	Revenge, financial gain
Unskilled attacker	Low; uses other people's tools	Notoriety, disruption
Shadow IT	Internal and unsanctioned	Convenience, not malice

The path in versus the weakness used

Threat vectors (2.2)	**Vulnerabilities (2.3)**
Message-based: email, SMS, instant messaging	Memory injection, buffer overflow, race conditions
Unsecure networks: open Wi-Fi, Bluetooth, wired ports	Web: SQL injection and cross-site scripting
Supply chain: MSPs, vendors, suppliers	Misconfiguration and default settings
Human: phishing, vishing, pretexting, BEC	Hardware: firmware, end-of-life, legacy
Default credentials and open service ports	Zero-day: no patch exists yet

Read the sign, then pick the fix

Attack	Indicator	Mitigation
Ransomware	Mass file renames, a ransom note	Offline backups, EDR, patching
Password spraying	Few failures each across many accounts	MFA, lockout and conditional access
SQL injection	Quotes and UNION in web server logs	Input validation, parameterized queries
DDoS	Traffic spike, resource exhaustion	Upstream filtering, rate limits, CDN

Attack	Indicator	Mitigation
Credential theft	Impossible travel, concurrent sessions	MFA, session revocation
Privilege escalation	New admin accounts, odd group changes	Least privilege, monitoring

Each architecture moves the risk

Cloud	Shared responsibility splits duties with the provider. (IaaS, PaaS, SaaS)
Infrastructure as code	Templates build identical systems; drift shows. (Terraform, CloudFormation)
Containers, serverless	Small units, but images and code still need scans. (Docker, cloud functions)
ICS and SCADA	Availability first; hard to patch, so segment them. (Water plant PLCs)
IoT and embedded	Weak defaults, rare updates, long service lives. (Infusion pump, RTOS)
On-premises	Full control and full responsibility for the stack. (Clinic file server)

EXERCISE 1: NAME THE OBJECTIVE, THE TERM, AND THE FIX

12 MINUTES · SMALL GROUPS

For each scenario, name the objective, the key term it tests, and the best control or answer. Be ready to defend it.

#	Prompt	Your answer
1	A clerk's PC shows hundreds of files renamed with a .lock extension	
2	A former admin logs in a week after leaving the company	
3	A $40,000 server loses half its value per event, twice a year	
4	A vendor's monitoring software update ships with a backdoor	
5	A water plant PLC runs firmware the maker no longer supports	
6	Two users share a password, yet their stored hashes differ	
7	A patch goes in at noon with no ticket and breaks billing	
8	A file named passwords.xlsx alerts the SOC when it is opened	

REVIEW QUESTIONS

1. A visible camera covers the server room door. What are its category and type?

2. Asset value $50,000, exposure factor 40%, ARO 0.5. What are the SLE and ALE?

3. Which key creates a digital signature, and why?

4. A phishing email steals a password for webmail that has no MFA. Name the vector and the vulnerability.

5. In IaaS, who patches the guest operating system?

KEY TAKEAWAYS

- **Name category and type.** A control has one category and can serve more than one type.
- **Write the risk math out.** SLE = AV x EF, ALE = SLE x ARO. Show every step.
- **Match crypto to its job.** Encryption hides, hashing proves integrity, signatures prove origin.
- **Path, weakness, sign, fix.** Read scenarios as vector, vulnerability, indicator, and mitigation.

LAB 8: MIDTERM PREPARATION, A STUDY PLAN AND A SELF-CHECK

60 MINUTES

You need your scored practice midterm, your notes from weeks 1 to 7, and a copy of the CompTIA SY0-701 exam objectives. No lab VMs are needed this week.

Steps

1. Take the 25-question practice midterm in one timed sitting of 25 minutes, with no notes, and score it.
2. Make a table with columns: question, objective, my answer, correct answer, why I missed it. Fill one row for every miss.
3. Label each miss as one of three causes: did not know the term, knew it but misread the question, or narrowed to two and picked the wrong one.
4. Open the exam objectives and mark each sub-bullet for 1.1 to 1.4, 2.1 to 2.5, 3.1, and the risk analysis items in 5.2 as green (can explain it), yellow (shaky), or red (cannot define it).
5. Write a one-line definition and one example from Lakeside Family Clinic for every red and yellow item.
6. Rework the risk math by hand: invent two risks for Lakeside, compute SLE, ALE, and the net benefit of one control for each, and check your arithmetic twice.
7. Build a study calendar for the days before the graded midterm: at least three sessions of 30 minutes, each assigned to specific objectives, reds first.
8. Self-check: without notes, explain to a classmate or out loud the difference between a vector and a vulnerability, a hash and a signature, and RTO and RPO. Note anything you could not explain clearly and add it to the calendar.

Hand in

Your miss table, the color-coded objectives checklist, the definitions for red and yellow items, the worked risk math, and the study calendar, as one document.

Questions to answer in your report

1. Which domain produced most of your misses, and what pattern do you see in the causes?
2. Which two objectives will you study first, and why those two?
3. For one question you narrowed to two answers, what made the correct option better than the one you picked?
4. What will you do differently on the graded midterm to avoid misreading questions?