STUDENT HANDOUT · WEEK 1

Course Orientation and Fundamental Security Concepts

SY0-701 objectives 1.2. Notes, exercises, review questions, and the lab.

Name	
Date	

THIS WEEK YOU WILL

1. Describe how the lessons, labs, quizzes, and the Lakeside Family Clinic project fit together.
2. Define confidentiality, integrity, and availability, and match a control to each.
3. Explain non-repudiation and why it depends on a digital signature or individual accounts.
4. Distinguish authentication, authorization, and accounting for both people and systems.
5. Outline a gap analysis and name the control plane and data plane parts of zero trust.
6. Select physical security and deception controls for a stated problem.

KEY IDEAS

Every week follows the same rhythm

1. Read	Read the lesson page before class
2. Lecture	Ninety minutes on one or two exam objectives
3. Exercises	Apply each idea to a short scenario in class
4. Lab	Hands-on work in your own isolated virtual lab
5. Project	Each lab adds a piece to the clinic's security plan
6. Quiz	Ten exam-style questions to check yourself

Four goals every control serves

Confidentiality	Only authorized people can read the data. (Encrypted patient records)
Integrity	Data is accurate and has not been changed without approval. (File hashes, change logs)
Availability	Systems and data are there when authorized users need them. (Backups, redundant power)
Non-repudiation	A person cannot credibly deny an action they took. (Digitally signed e-prescription)

Authentication, authorization, and accounting

Step	Question it answers	Clinic example
Identification	Who do you claim to be?	A nurse types her username, jlopez
Authentication	Can you prove it?	Password plus a code from a phone app
Authorization	What are you allowed to do?	She can open charts but not payroll
Accounting	What did you do, and when?	The EHR logs every chart she opens

People and systems both prove who they are

Authenticating people	Authenticating systems
Something you know: a password or PIN	A device certificate proves a laptop's identity
Something you have: a smart card or phone app	802.1X checks a device before the port opens
Something you are: a fingerprint or face	Services use their own accounts and keys
MFA combines two or more different factors	Mutual TLS: both ends present certificates

Gap analysis compares today with the target

1. Pick a target	Choose a framework such as the NIST CSF or CIS Controls
2. Assess today	Document the controls actually in place now
3. Find the gaps	List each requirement not met, or met only in part
4. Prioritize	Rank the gaps by risk, cost, and effort
5. Plan	Write a remediation plan with owners and dates

Zero trust splits decisions from enforcement

Control plane: decides	Data plane: enforces
Adaptive identity: context changes the checks	Subject or system: the user or device asking
Threat scope reduction: least access needed	Policy Enforcement Point allows or blocks
Policy-driven access control	Implicit trust zone: kept as small as possible
Policy Engine decides; Administrator applies it	Traffic reaches the resource only after a yes

Layers that keep people and vehicles out

Bollards	Posts that stop vehicles but let people walk past. (Clinic entrance)
Access vestibule	Two doors, one open at a time. Stops tailgating. (Data center entry)
Fencing	Marks the boundary and slows anyone on foot. (Generator yard)
Video surveillance	Cameras record events and deter attempts. (Lobby and back door)
Guards and badges	Guards use judgment; badges show who may enter. (Front desk check-in)
Lighting and sensors	Light deters; sensors detect motion or presence. (IR, pressure, microwave)

Deception tools turn attackers into alerts

Tool	What it is	Clinic example
Honeypot	A decoy system that looks real and valuable	A fake file server named BILLING-01
Honeynet	A network of honeypots that mimics a segment	A decoy subnet of servers and workstations
Honeyfile	A bait file that alerts when opened	passwords.xlsx on a share, with an alert
Honeytoken	Fake data or credentials that alert when used	A fake admin account no one should use

EXERCISE 1: WHICH GOAL OR FUNCTION DOES EACH CONTROL SERVE

8 MINUTES · PAIRS

For each item, name the CIA goal, non-repudiation, or the AAA function it mainly supports. Be ready to defend it.

#	Prompt	Your answer
1	Nightly backups copied to a second site	
2	A hash value posted next to a software download	
3	A badge and a PIN are required at the pharmacy door	
4	Front desk staff cannot open billing reports	
5	Every chart view is logged with the user and the time	
6	A doctor signs e-prescriptions with a private key	
7	Laptop drives are encrypted with BitLocker	
8	A second internet line from a different provider	
9	The VPN checks the laptop's device certificate	

EXERCISE 2: FIX THE GAPS AT LAKESIDE FAMILY CLINIC

10 MINUTES · SMALL GROUPS

For each finding, name the weakness, one control that fixes it, and the goal or function that control supports.

#	Prompt	Your answer
1	Staff share one admin login on the front desk PC	
2	The server closet opens with a key kept on a hook beside it	
3	No log shows who opened which patient chart	
4	A laptop on the guest Wi-Fi can reach the file server	
5	The back door to the parking lot is propped open at lunch	
6	Nobody would notice someone browsing the file shares at night	
7	The parking lot is dark after evening clinic hours	

REVIEW QUESTIONS

1. A user hashes a downloaded installer and compares it to the vendor's posted hash. Which CIA goal does this check?

2. A logged-in nurse is blocked from opening payroll records. Which AAA function blocked her?

3. A login asks for a password and a code from an authenticator app. Is this MFA, and why?

4. In zero trust, which component makes the access decision, and which enforces it?

5. A fake administrator account exists only to raise an alert if someone uses it. What is it called?

KEY TAKEAWAYS

- **CIA plus non-repudiation.** Every control protects secrecy, accuracy, uptime, or proof of who acted.
- **AAA needs one account each.** Shared logins break authentication, accounting, and non-repudiation.
- **Zero trust checks every request.** The control plane decides; the Policy Enforcement Point enforces.
- **Layer physical and deception.** Fences, doors, cameras, and decoys catch what technical controls miss.

LAB 1: BUILD THE COURSE LAB

60 MINUTES

You need a computer with at least 16 GB of RAM (8 GB works if you run one VM at a time; for the ping test in step 7, which needs both running, lower each VM to 3 GB first), 100 GB of free disk space, and hardware virtualization turned on, plus Oracle VirtualBox, which is free. Both VMs go on a host-only network so nothing you run in later labs can reach the campus network or the internet.

Steps

1. Confirm virtualization is on. In Windows, open Task Manager, then Performance, then CPU, and check that Virtualization says Enabled. If it does not, turn on Intel VT-x or AMD-V in your computer's firmware settings.
2. Install VirtualBox from virtualbox.org. Download an Ubuntu Desktop 24.04 LTS ISO from ubuntu.com and a Windows evaluation ISO (Windows 11 Enterprise or Windows Server 2022) from the Microsoft Evaluation Center.
3. Create the isolated network. In VirtualBox, open the Network Manager, choose Host-only Networks, and create one (VirtualBox usually offers 192.168.56.0/24). Turn its DHCP server on.
4. Create the Linux VM (2 CPUs, 4 GB RAM, 40 GB disk) with its default NAT adapter so it can download updates. Install Ubuntu, then run sudo apt update && sudo apt upgrade -y.
5. Create the Windows VM (2 CPUs, 4 GB RAM, 60 GB disk) and install from the evaluation ISO, also on NAT for now. Install the VirtualBox Guest Additions on both VMs and run Windows Update once.
6. Isolate the lab. Power off both VMs, set Adapter 1 on each to Host-only Adapter on your new network, and disable any other adapters. Start them and find each address with ip a on Linux and ipconfig on Windows.
7. Test the network. In an administrator PowerShell on Windows, allow ping with New-NetFirewallRule -DisplayName "Lab ICMPv4" -Protocol ICMPv4 -IcmpType 8 -Direction Inbound -Action Allow. From Linux, ping the Windows address; it should answer. Then ping 8.8.8.8 from both VMs; it should fail, which proves the lab is isolated.
8. Take a snapshot of each VM named clean-baseline. Then create a file on each desktop, restore the snapshot, and confirm the file is gone.
9. Record a lab inventory: VM names, operating system versions, IP addresses, and snapshot names. Keep the VM passwords in a password manager, not in your report.

Hand in

A one-page lab report with your lab inventory table and four screenshots: the host-only network settings, a successful ping between the VMs, a failed ping to 8.8.8.8, and the snapshot list for each VM.

Questions to answer in your report

1. Why does the lab use a host-only network rather than a bridged adapter? What could go wrong in later labs with a bridged adapter?
2. Which CIA goal do snapshots mainly support? Give one reason a snapshot kept on the same disk as the VM is not a real backup.
3. The firewall rule you added is a control. Name its category and type, and say what risk you accepted by adding it.
4. Your lab has no AAA server. How do the two VMs currently authenticate users, and what would accounting look like on each?