VPWEB.DEV · STUDY SCHEDULE

CompTIA Security+ — Weekly Plan

A 10-week daily study schedule · Exam SY0-701

A day-by-day plan that pairs Professor Messer's free course with a light Python thread, a home lab, and active recall. Weeks 1–2 are broad exposure; Weeks 3–8 are deep study and memorization, one focus area at a time; Weeks 9–10 are practice exams and the test itself. Check off each block as you go.

YOUR SETUP: 3+ hrs on weekdays · weekends light or off · watch videos at ·1.25×

COMPTIA SECURITY+ · WEEK 1

Foundations

Goal this week: Broad exposure, not memorization. Get through the first half of Messer's course (Domains 1–3), set up your lab + Python, and start light hands-on. If something doesn't fully stick now, that's by design.

Day 1 ~3 hrs — *Orientation + Domain 1*

- [ ] 0:45 Setup: download the official SY0-701 objectives PDF and skim it; watch Messer's intro + "how to study" videos; make a free TryHackMe account
- [ ] 1:45 Messer, Domain 1: General Security Concepts (the gentlest domain — easy momentum)
- [ ] 0:30 Active recall: write the day's key terms in your own words (CIA triad, control types)

Day 2 ~3 hrs — *Domain 2 (part 1) + Python kickoff*

- [ ] 2:00 Messer, Domain 2: Threats, Vulnerabilities & Mitigations (threat actors, attack types)
- [ ] 0:30 Active recall on today's videos
- [ ] 0:30 Python: install it, then write a ~12-line script that reads a text file and prints each line numbered

Day 3 ~3 hrs — *Domain 2 (part 2) + Lab setup*

- [ ] 1:30 Messer: finish Domain 2
- [ ] 1:00 Home lab: install VirtualBox and spin up one Linux VM (a one-time chore that powers later hands-on work)
- [ ] 0:30 Messer Pop Quiz / flashcards covering Domains 1–2

Day 4 ~3 hrs — *Domain 3 (part 1) + Python*

- [ ] 2:00 Messer, Domain 3: Security Architecture (most people's hardest domain — just expose yourself, no pressure to master)
- [ ] 0:30 Active recall
- [ ] 0:30 Python: extend your script to flag lines containing a keyword like "failed" or "error" (the seed of a log parser)

Day 5 ~3 hrs — *Finish Domain 3 + consolidate*

- [ ] 1:30 Messer: finish Domain 3
- [ ] 0:45 Active recall + a short Pop Quiz across Domains 1–3
- [ ] 0:45 Python: make your keyword-flagger count how often each keyword appears and print a small summary

Weekend — *light or off*

- [ ] Best case: one easy ~45–60 min session re-skimming your terms doc (passive, low effort)
- [ ] Otherwise: rest, and mean it — protecting energy in Week 1 is part of the plan
- [ ] Nothing new, no cramming

> **End-of-week checkpoint:** Domains 1–3 seen once · a running terms doc · a working VM · a Python script quietly turning into a log parser.

Next up — Week 2 — exposure to Domains 4 & 5. Domain 4 (Security Operations, 28% of the exam) is where your coding starts to pay off.

Keep Python sessions short — they complement the cert, they don't compete with it. If a day's video runs long, let it spill rather than skipping active recall; writing terms in your own words is what moves them into memory.

COMPTIA SECURITY+ · WEEK 2

Exposure — Domains 4 & 5

Goal this week: Finish the first watch-through of Messer (Domains 4 & 5) and keep growing the lab and the Python log parser. Still exposure, not mastery — Domain 4 is the largest (28%), so give it room.

Day 1 ~3 hrs — *Domain 4 (part 1)*

- [ ] 2:00 Messer, Domain 4: Security Operations (baselines, hardening, monitoring, SIEM)
- [ ] 0:30 Active recall
- [ ] 0:30 Python: read a sample auth log and print only the lines containing “Failed password”

Day 2 ~3 hrs — *Domain 4 (part 2) + Lab*

- [ ] 1:45 Messer: continue Domain 4 (IAM, MFA, SSO, incident response)
- [ ] 0:45 Lab: in your Linux VM, look at /var/log/auth.log and practice `grep "Failed"`
- [ ] 0:30 Active recall

Day 3 ~3 hrs — *Finish Domain 4 + Python*

- [ ] 1:30 Messer: finish Domain 4 (automation/orchestration, digital forensics)
- [ ] 0:30 Pop Quiz / flashcards on Domain 4
- [ ] 1:00 Python: count failed logins per user/IP and print the top offenders (a brute-force-detector seed)

Day 4 ~3 hrs — *Domain 5 (part 1)*

- [ ] 2:00 Messer, Domain 5: Security Program Management & Oversight (governance, risk)
- [ ] 0:30 Active recall
- [ ] 0:30 TryHackMe: one beginner-friendly room (intro to security)

Day 5 ~3 hrs — *Finish Domain 5 + consolidate*

- [ ] 1:15 Messer: finish Domain 5
- [ ] 0:45 Active recall + a Pop Quiz across Domains 4–5
- [ ] 1:00 Python: have your parser write its summary to a results file — your first real “report”

Weekend — *light or off*

- [ ] Best case: a light re-skim of your terms doc across all five domains
- [ ] Otherwise: rest
- [ ] No new material

End-of-week checkpoint: All five domains seen once · the lab can read logs · the Python parser flags and counts failed logins.

Next up — Week 3 — deep study begins. The second pass is where it sticks; start with Domain 1.

You’ve now seen the whole exam once. Resist feeling behind — exposure is supposed to feel shallow. Mastery comes next.

Deep study — Domain 1: General Security Concepts

Goal this week: Switch from exposure to mastery. Re-study Domain 1 deeply: control categories and types, the CIA/AAA foundations, zero trust, and change management. Memorization mode is on.

Day 1 ~3 hrs — *Control categories & types*

- [ ] 1:30 Re-study control categories (technical/managerial/operational/physical) and types (preventive/deterrent/detective/corrective/compensating/directive)
- [ ] 1:00 Build a control-types table from memory, then check it
- [ ] 0:30 Flashcards

Day 2 ~3 hrs — *CIA, AAA & core principles*

- [ ] 1:30 CIA triad, AAA, non-repudiation, authentication factors
- [ ] 1:00 Active recall: explain each principle in your own words with an example
- [ ] 0:30 Flashcards

Day 3 ~3 hrs — *Zero trust & change management*

- [ ] 1:30 Zero trust architecture, gap analysis, change-management process
- [ ] 1:00 Active recall + targeted practice questions
- [ ] 0:30 Python: use `hashlib` to SHA-256 a string and compare two hashes (warm-up for crypto week)

Day 4 ~3 hrs — *Physical security & deception*

- [ ] 1:30 Physical security controls; deception & disruption (honeypots, honeytokens)
- [ ] 1:00 Flashcards across all of Domain 1
- [ ] 0:30 TryHackMe: a beginner security-concepts room

Day 5 ~3 hrs — *Domain 1 mastery check*

- [ ] 1:15 Practice questions: Domain 1 only
- [ ] 0:45 Review every miss and fix the gap
- [ ] 1:00 Python: extend your hashing script to verify file integrity (hash a file, detect a change)

Weekend — *light or off*

- [ ] Best case: re-skim the control-types table and CIA/AAA; short flashcard session
- [ ] Otherwise: rest

End-of-week checkpoint: Domain 1 solid · control types memorized cold · Python doing hashing + integrity checks.

Next up — Week 4 — cryptography and PKI, the densest, highest-yield topic on the exam.

Control types come up everywhere. If you can rattle off all six types and four categories from memory, you've banked easy points across the whole exam.

COMPTIA SECURITY+ · WEEK 4

Deep study — Cryptography & PKI

Goal this week: Cryptography earns its own week because it's dense and heavily tested. Master symmetric vs asymmetric vs hashing, and the full PKI picture: certificates, signatures, and trust.

Day 1 ~3 hrs — *Symmetric vs asymmetric*

- [ ] 1:45 Symmetric (AES, ChaCha20) vs asymmetric (RSA, ECC, Diffie-Hellman) — strengths, uses, key exchange
- [ ] 0:45 Active recall: build a "which crypto when?" table
- [ ] 0:30 Flashcards

Day 2 ~3 hrs — *Hashing & integrity*

- [ ] 1:30 Hashing (SHA-2/3), salting, HMAC, where integrity matters; why MD5/SHA-1 are out
- [ ] 1:00 Active recall + practice questions
- [ ] 0:30 Python: have your integrity checker hash every file in a folder and flag any that changed

Day 3 ~3 hrs — *PKI & certificates*

- [ ] 1:45 PKI: certificate authorities, chains of trust, CSRs, OCSP/CRL, key escrow
- [ ] 0:45 Active recall
- [ ] 0:30 Lab: inspect a real website's certificate in your browser — issuer, validity, chain

Day 4 ~3 hrs — *Digital signatures & TLS*

- [ ] 1:30 Digital signatures, non-repudiation, how TLS uses both asymmetric and symmetric crypto
- [ ] 1:00 Flashcards across all of cryptography
- [ ] 0:30 Python: encrypt and decrypt a message with a symmetric library (e.g. `cryptography` / Fernet)

Day 5 ~3 hrs — *Cryptography mastery check*

- [ ] 1:15 Practice questions: cryptography across Domains 1 & 3
- [ ] 0:45 Review misses
- [ ] 1:00 TryHackMe: a cryptography/hashing room

Weekend — *light or off*

- [ ] Best case: re-skim your crypto table and PKI flow; flashcards
- [ ] Otherwise: rest

End-of-week checkpoint: Crypto and PKI memorized · you can explain TLS's hybrid approach · Python doing real symmetric encryption.

Next up — Week 5 — Domain 2: threats, vulnerabilities, and mitigations.

Don't just memorize algorithm names — know what each is FOR (bulk data, key exchange, integrity, signing). The exam tests application, not trivia.

Deep study — Domain 2: Threats & Vulnerabilities

Goal this week: Master who attacks, how, and what to do about it. Threat actors, attack vectors, vulnerability classes, indicators of compromise, and mitigation techniques.

Day 1 ~3 hrs — *Threat actors & motivations*

- [ ] 1:30 Threat actors (nation-state, insider, hacktivist, organized crime, script kiddie) and motivations
- [ ] 1:00 Build an actor/motivation table
- [ ] 0:30 Flashcards

Day 2 ~3 hrs — *Attack types*

- [ ] 1:45 Attacks: phishing/social engineering, malware types, DoS, on-path, password, injection (SQLi/XSS)
- [ ] 0:45 Build an attack-types table from memory
- [ ] 0:30 Python: parse a log for several keywords (failed, error, denied) and tally each

Day 3 ~3 hrs — *Vulnerabilities & attack surfaces*

- [ ] 1:30 Vulnerability classes (application, web, OS, cloud, supply chain) and attack surfaces
- [ ] 1:00 Active recall + practice questions
- [ ] 0:30 TryHackMe: an attacks/vulnerabilities room

Day 4 ~3 hrs — *Indicators & mitigations*

- [ ] 1:45 Indicators of compromise; mitigation techniques (segmentation, hardening, patching, least privilege)
- [ ] 0:45 Active recall
- [ ] 0:30 Flashcards

Day 5 ~3 hrs — *Domain 2 mastery check*

- [ ] 1:15 Practice questions: Domain 2
- [ ] 0:45 Review misses, fix gaps
- [ ] 1:00 Python: group your log tallies by type and print a tidy summary table

Weekend — *light or off*

- [ ] Best case: re-skim the attack-types and actor tables; flashcards
- [ ] Otherwise: rest

End-of-week checkpoint: Domain 2 solid · attack types and IoCs memorized · Python summarizing log events by type.

Next up — Week 6 — Domain 3: security architecture and data protection.

*Attack types are prime PBQ and scenario material. Knowing the *indicators* of each is what lets you pick the right answer under pressure.*

Deep study — Domain 3: Security Architecture

Goal this week: Master secure design across environments and how to protect data. This is many people's hardest domain — focus on the "why," not just definitions.

Day 1 ~3 hrs — *Architecture models*

- [ ] 1:45 Cloud, serverless, microservices, IaC, on-prem, virtualization, IoT/ICS/SCADA — security trade-offs of each
- [ ] 0:45 Active recall
- [ ] 0:30 Flashcards

Day 2 ~3 hrs — *Enterprise infrastructure security*

- [ ] 1:30 Secure network design: device placement, firewalls, IDS/IPS, proxies, segmentation, zero-trust zones
- [ ] 1:00 Active recall + practice questions
- [ ] 0:30 Flashcards

Day 3 ~3 hrs — *Data protection*

- [ ] 1:45 Data classification, states (at rest / in transit / in use), encryption, DLP, tokenization, masking
- [ ] 0:45 Active recall
- [ ] 0:30 Python: have your toolkit timestamp and save its reports (a data-handling exercise)

Day 4 ~3 hrs — *Resilience & recovery*

- [ ] 1:30 Backups, redundancy, high availability, capacity planning, recovery testing
- [ ] 1:00 Build a resilience/recovery table
- [ ] 0:30 Flashcards

Day 5 ~3 hrs — *Domain 3 mastery check*

- [ ] 1:15 Practice questions: Domain 3
- [ ] 0:45 Review misses
- [ ] 1:00 TryHackMe: a network/architecture-flavored room

Weekend — *light or off*

- [ ] Best case: re-skim data states and resilience concepts; flashcards
- [ ] Otherwise: rest

End-of-week checkpoint: Domain 3 solid · architecture trade-offs clear · data states memorized.

Next up — Week 7 — Domain 4 (Security Operations), part 1: hardening, monitoring, and identity.

*For every architecture choice, ask "what threat does this reduce?" Answering the *why* turns memorization into understanding the exam rewards.*

Deep study — Domain 4 (part 1): Hardening, Monitoring & Identity

Goal this week: Begin the largest domain (28%). Master secure baselines and hardening, monitoring and SIEM, and identity & access management. Your Python work mirrors this directly.

Day 1 ~3 hrs — *Baselines & hardening*

- [ ] 1:45 Secure baselines and hardening across servers, endpoints, mobile, cloud, and apps
- [ ] 0:45 Active recall
- [ ] 0:30 Lab: harden your VM — disable an unused service, set a firewall rule

Day 2 ~3 hrs — *Monitoring & SIEM*

- [ ] 1:30 Monitoring, alerting, log aggregation, SIEM, SNMP, NetFlow
- [ ] 1:00 Active recall + practice questions
- [ ] 0:30 Python: turn your log parser into a mini-SIEM — alert when failed logins exceed a threshold

Day 3 ~3 hrs — *Identity & access management*

- [ ] 1:45 IAM: provisioning/deprovisioning, MFA, SSO, federation, privileged access management
- [ ] 0:45 Build an IAM concepts table
- [ ] 0:30 Flashcards

Day 4 ~3 hrs — *Enterprise security capabilities*

- [ ] 1:30 Firewalls, IDS/IPS, web/DNS filtering, email security, EDR
- [ ] 1:00 Active recall + practice questions
- [ ] 0:30 Flashcards

Day 5 ~3 hrs — *Consolidate Domain 4 (part 1)*

- [ ] 1:15 Practice questions across the week's topics
- [ ] 0:45 Review misses
- [ ] 1:00 Python: add timestamps to your SIEM alerts and write them to an alerts log

Weekend — *light or off*

- [ ] Best case: re-skim IAM and monitoring concepts; flashcards
- [ ] Otherwise: rest

End-of-week checkpoint: Hardening, monitoring, and IAM solid · Python mini-SIEM raising threshold alerts.

Next up — Week 8 — Domain 4 (part 2): incident response & automation, plus Domain 5.

Domain 4 is over a quarter of the exam. If any week needs more of your time, it's these two.

Deep study — Domain 4 (part 2) + Domain 5

Goal this week: Finish Security Operations — incident response, forensics, and automation — and master Domain 5: governance, risk, and compliance. After this week, every domain is deeply studied.

Day 1 ~3 hrs — *Incident response*

- [ ] 1:45 The incident-response lifecycle (prepare → detect → contain → eradicate → recover → lessons learned)
- [ ] 0:45 Active recall: the IR steps in order, with what happens in each
- [ ] 0:30 TryHackMe: an incident-response / SOC room

Day 2 ~3 hrs — *Forensics & automation*

- [ ] 1:30 Digital forensics, chain of custody, evidence handling; automation & orchestration (SOAR)
- [ ] 1:00 Active recall + practice questions
- [ ] 0:30 Python: finalize your toolkit (parser + integrity + alerts) and write a short README

Day 3 ~3 hrs — *Governance & policies*

- [ ] 1:45 Domain 5: governance, policies/standards/procedures, roles, regulatory frameworks
- [ ] 0:45 Active recall
- [ ] 0:30 Flashcards

Day 4 ~3 hrs — *Risk management*

- [ ] 1:45 Risk identification & assessment (qualitative/quantitative), appetite/tolerance, treatment, vendor risk
- [ ] 0:45 Build a risk-management table
- [ ] 0:30 Flashcards

Day 5 ~3 hrs — *Compliance + Domains 4–5 check*

- [ ] 1:00 Compliance & privacy (GDPR, PCI DSS), audits, attestations, security awareness
- [ ] 1:15 Practice questions: Domains 4 & 5
- [ ] 0:45 Review misses

Weekend — *light or off*

- [ ] Best case: re-skim the IR lifecycle and risk concepts; flashcards across all five domains
- [ ] Otherwise: rest

End-of-week checkpoint: All five domains deeply studied · IR & risk memorized · Python toolkit finished and documented.

Next up — Week 9 — consolidation: full practice exams and PBQ drills across everything.

You now know the whole exam. From here it's about retrieval speed and accuracy — shift from learning to testing yourself.

Consolidation & practice exams

Goal this week: Stop learning new material; start proving you know it. Full-length practice exams, ruthless review of misses, and PBQ-style drills. Climb toward a steady 90%.

Day 1 ~3 hrs — *First full practice exam*

- [ ] 1:30 Take a full-length, timed practice exam (Dion or Messer)
- [ ] 1:00 Review every miss and note its domain
- [ ] 0:30 Flashcards on the weak areas

Day 2 ~3 hrs — *Weakest-domain review*

- [ ] 2:00 Re-study the two weakest domains from yesterday's exam
- [ ] 0:30 Targeted practice questions there
- [ ] 0:30 Active recall

Day 3 ~3 hrs — *PBQ drills*

- [ ] 1:30 Performance-based question practice (configure / sort / scenario)
- [ ] 1:00 Review and note patterns
- [ ] 0:30 Python: map each part of your toolkit to the Security+ concept it demonstrates (interview prep)

Day 4 ~3 hrs — *Second full practice exam*

- [ ] 1:30 Another full practice exam (a fresh question set)
- [ ] 1:00 Review misses
- [ ] 0:30 Flashcards

Day 5 ~3 hrs — *Mixed review*

- [ ] 1:30 Mixed practice questions across all domains
- [ ] 0:45 Review
- [ ] 0:45 Re-skim acronyms + key ports

Weekend — *light or off*

- [ ] Best case: one short mixed quiz
- [ ] Otherwise: rest before the final week

End-of-week checkpoint: Scoring in the 80s and climbing · weak domains shored up · comfortable with PBQs.

Next up — Week 10 — final review, reach 90%, and pass the exam.

*Your practice-exam *review* matters more than the score — every miss is a gap you can close before exam day. Always read why the right answer is right.*

Final review & exam

Goal this week: Reach a consistent 90%+ on fresh practice exams, do a light final review, handle logistics, and pass SY0-701. Taper toward the end — rested beats crammed.

Day 1 ~3 hrs

Practice exam + review

- [ ] 1:30 A fresh full-length practice exam
- [ ] 1:00 Review misses
- [ ] 0:30 Flashcards

Day 2 ~3 hrs

Final weak-spot pass

- [ ] 1:45 A last deep review of any lingering weak topics
- [ ] 0:45 Targeted questions
- [ ] 0:30 Re-skim crypto + control types (highest-yield)

Day 3 ~3 hrs

The 90% gate + logistics

- [ ] 1:30 Final full practice exam — you want a confident 90%+
- [ ] 1:00 Review
- [ ] 0:30 Logistics: register the exam and test your online-proctoring setup (or locate the test center)

Day 4 ~1.5 hrs

Light review (then stop)

- [ ] 1:00 Re-skim your terms doc + acronyms
- [ ] 0:30 A few easy questions for confidence — then stop early and rest

Day 5 exam day

Sit and pass

- [ ] – Light: re-read the exam-day strategy, eat well, arrive calm
- [ ] – Sit and pass SY0-701. Flag-and-move on hard PBQs, bank the multiple-choice, then circle back

Weekend

light or off

- [ ] Celebrate — you earned it
- [ ] Start renewing your A+/Network+ CEs if you hold them (Security+ renews them too)

End-of-week checkpoint: 90%+ on fresh exams · logistics handled · certified.

Next up — Security+ done. Consider a SOC analyst role, or stack toward CySA+ or a cloud cert — and bring your Python toolkit to interviews as a real talking point.

On exam day the PBQs come first and weigh the most — if one stalls you, flag it and move on, then return with the time you banked. Trust your prep.