BlackHack Academy

CompTIA Security+ SY0-701

Certification Preparation Course

Executive Summary & Table of Contents

465	10	3	10
Assessment Questions	Weekly Quizzes	Progressive Exams	Hands-On Labs

235 Pages | 23 Deliverables | 20+ Hours of Lab Work
Aligned to All 5 CompTIA SY0-701 Exam Domains

EXECUTIVE SUMMARY

BlackHack Academy's Security+ SY0-701 Certification Preparation Course is a complete, turnkey training program that takes professionals from zero to exam-ready across 10 structured weeks. Built by practitioners who live in the trenches of offensive and defensive security, this course develops professionals who can think critically, respond to real incidents, and defend enterprise environments from day one.

The program is purpose-built for organizations investing in workforce cybersecurity readiness -- whether upskilling IT teams, preparing staff for compliance mandates, or building internal security operations capability. Every assessment and lab maps directly to CompTIA's five exam domains, ensuring measurable alignment between training activity and certification outcomes.

Why This Program

- Practitioner-Built: Designed by active cybersecurity consultants with red team, blue team, and GRC experience -- not recycled textbook content.
- Progressive Difficulty: Assessments scale from foundational recall through exam-equivalent rigor to advanced scenarios harder than the actual SY0-701.
- Hands-On From Week One: Ten 2-hour labs using free, industry-standard tools (Kali, Wireshark, Suricata, Wazuh, Splunk, BloodHound, Autopsy).
- Full Domain Coverage: All five SY0-701 domains addressed with weighted question distribution matching the actual exam blueprint.
- Turnkey Delivery: 23 print-ready PDFs with branded covers, answer keys, detailed explanations, and submission checklists. LMS-ready.
- MITRE ATT&CK; Integration: Advanced assessments tag questions to MITRE ATT&CK; tactics and techniques, bridging certification prep to real-world threat intelligence.

Program Snapshot

Component	Details
Certification	CompTIA Security+ SY0-701 (current exam version)
Duration	10 weeks (flexible pacing available)
Assessments	13 total (10 quizzes + 3 exams) -- 465 questions with answer keys
Labs	10 guided labs, 2 hours each, 20+ hours of hands-on exercises
Lab Environment	Kali Linux + VirtualBox -- free, no licensing costs
Delivery	23 branded PDF documents, 235 pages total
Question Types	Multiple choice, scenario-based, and Performance-Based Questions (PBQs)

DOMAIN COVERAGE & ASSESSMENT MODEL

SY0-701 Exam Domains

Domain	Weight	Focus Areas	Weeks
1. General Security Concepts	12%	Controls, CIA Triad, Zero Trust, AAA, cryptography	1-2
2. Threats, Vulns & Mitigations	22%	Threat actors, social engineering, malware, hardening	3-5
3. Security Architecture	18%	Network defense, cloud, IDS/IPS, data protection, resilience	6-7
4. Security Operations	28%	SIEM, IAM, vulnerability mgmt, IR, forensics	8-9
5. Program Management	20%	GRC, risk assessment, compliance, third-party risk, audits	10

Progressive Assessment Ladder

Assessment	Qs	Time	Difficulty	Purpose
Weekly Quizzes (x10)	25 ea	30 min	Targeted	Reinforce weekly material, identify gaps early
Initial Mock Test	50	60 min	Below Exam	Baseline before deep study begins
Midterm Exam	75	75 min	Exam-Level	Mid-course checkpoint at real SY0-701 difficulty
Final Assessment	90	90 min	Above Exam	Capstone -- harder than the real exam

Performance-Based Questions (PBQs) are integrated into the Midterm (3 PBQs) and Final Assessment (5 PBQs), mirroring the actual SY0-701 format. Types include firewall ACL writing, ALE risk calculations, IR phase ordering, tool classification, and log analysis with MITRE ATT&CK; technique identification.

LAB PROGRAM

Each week includes a 2-hour guided lab using exclusively free, open-source tools. Labs provide step-by-step commands, expected outputs, reflection questions, SY0-701 exam objective mapping, and a submission checklist. No paid software licenses required.

#	Lab	Tools
01	Build Your Hacker Lab	VirtualBox, Kali Linux
02	Cryptography in Action	Hashcat, OpenSSL, CyberChef
03	OSINT & Reconnaissance	theHarvester, Shodan, MXToolbox
04	Malware Analysis & Vuln Scanning	Any.Run, Nmap, NVD
05	Web App Exploit & Hardening	DVWA, Docker, UFW, CIS
06	Firewall & IDS Configuration	UFW, Suricata, Wireshark
07	Cloud Security & Backup	ScoutSuite, rsync, GPG
08	SIEM, AD Attack & Defense	Wazuh, Splunk, BloodHound CE
09	IR Simulation & Forensics	Autopsy, MITRE ATT&CK; Navigator
10	Risk Assessment & Compliance	Lynis, LibreOffice, NIST RMF

TABLE OF CONTENTS

The following 23 documents comprise the complete assessment and lab package. All documents are branded, print-ready PDFs with answer keys and detailed explanations.

Weekly Quizzes (25 questions each, answer key included)

Examinations (progressive difficulty, PBQs included)

Lab Assignments (2 hours each, 6 pages each)

WHY BLACKHACK ACADEMY

BlackHack Academy is the training arm of BlackHack Society -- a practitioner-led cybersecurity organization founded on the principle that the best defenders think like attackers. Our instructors are active consultants, penetration testers, and security architects who bring real engagement experience into every module.

What Sets Us Apart

- Purple Team DNA: Every module teaches both the attack and the defense -- building professionals who understand the full picture.
- Real-World Case Studies: WannaCry, Colonial Pipeline, MOVEit, SolarWinds, Log4Shell -- learners study the incidents that shaped modern security.
- Zero Licensing Costs: All lab tools are free and open-source. No per-seat fees, no cloud credits, no vendor lock-in.
- Enterprise-Ready: Branded, professional PDFs that integrate into corporate LMS platforms, classrooms, or self-paced delivery without modification.
- Measurable Outcomes: Pre-assessment baselining, weekly checks, mid-course checkpoint, and a capstone exceeding exam difficulty -- giving managers clear visibility into readiness.

Ideal For

- IT teams transitioning into security roles
- SOC analysts and help desk professionals seeking certification
- Organizations meeting compliance mandates (CMMC, NIST, ISO 27001)
- MSSPs training staff at scale
- Career changers entering cybersecurity
- Government and defense contractors requiring security-cleared personnel

Ready to deploy Security+ training for your team?

Contact BlackHack Academy to discuss volume licensing, custom delivery, and instructor-led packages.

blackhacksociety.com