Security+ Fun 30-Day Boot Camp Syllabus

Course Overview

The objective of this Security+ boot camp is to maintain an interactive, group-based, and peer-teaching approach to solidify mastery.

Class Format & Schedule

📅 **Dates:** August 1 – August 27, 2025
🕒 **Schedule:** Tues & Thurs (6–9 PM EST), Sat (9 AM–2 PM EST)
💻 **Delivery:** Live via Microsoft Teams (Replay access included)
⏱️ **Total Hours:** 40 hours instructor-led + optional self-study support

---

Domain 1: General Security Concepts

Day 1 (Aug 1, Thurs)

Topic: Information Security & CIA Triad

- **Define information security and its purpose**
- **Explain the CIA Triad: confidentiality, integrity, availability**
- **Describe non-repudiation with simple examples**
- **Group activity: Identify CIA failures in real-life news headlines**
- **Quick quiz: CIA triad and non-repudiation questions**

Day 2 (Aug 3, Sat)

Topic: Frameworks, Gap Analysis, and IAM

- **Describe what a cybersecurity framework is and why it's used**
- **Explain gap analysis and its benefits**
- **Define IAM (identification, authentication, authorization, accounting)**
- **Workshop: Map IAM functions to user scenarios**
- **Group debate: Are frameworks or policies more critical for security?**
- **Lab: Review of a sample gap analysis report and discuss missing controls**

Domain 2: Security Architecture

Day 3 (Aug 5, Tues)

Topic: Threat Actors and Their Motivations

- **Threat Actors & Motivations**
- **Group Activity: Role-play different threat actor profiles and their attack planning**

Day 4 (Aug 7, Thurs)

Topic: Attack Surfaces and Vectors

- **Attack Surfaces & Vectors (Software, Network, Supply Chain)**
- **Workshop: Map your home or workplace attack surface with group feedback**

Day 5 (Aug 9, Sat)

Topic: Social Engineering & Endpoint Security Hardening

- **Social Engineering, Phishing, and Endpoint Security Hardening**
- **Lab: Endpoint hardening baseline configuration walkthrough**
- **Group Debate: Best mitigation strategies for lure-based and supply chain attacks**

<u>Domain 3: Security Operations</u>

Topic: Enterprise Network Architecture and Segmentation

Day 6 (Aug 17, Sat)

Topic: Enterprise Network Architecture

- **Explain what network architecture is and why it matters**
- **Describe infrastructure, applications, and data assets in a network**
- **Discuss network segmentation and security zones**
- **Workshop – Design a secure email network architecture**
- **Quick quiz: Network architecture, segmentation, and security zones**

Day 7 (Aug 18, Sun)

Topic: Firewalls, Proxies, IDS & IPS

- **Compare stateless vs. stateful firewalls**
- **Differentiate Layer 4 vs. Layer 7 firewalls**
- **Explain forward and reverse proxies**

- Lab – Configure proxy settings and simulate firewall filtering

Day 8 (Aug 19, Mon)

Topic: Next-Gen Firewalls, Load Balancers & Secure Remote Connections

- Describe NGFWs and UTM devices
- Explain load balancers (Layer 4 vs. Layer 7) and session persistence
- Discuss VPN types and secure remote access methods
- Group activity – Design a secure remote access solution

Domain 4: Incident Response & Risk Management

Day 9 (Aug 20, Tue)

Topic: Identity and Access Management Fundamentals

- Explain the purpose of cryptographic hashes for passwords
- Describe authentication types in Windows systems
- Discuss federation in identity management
- Interactive Activity: Workshop – Configure user accounts and test authentication methods

Day 10 (Aug 23, Fri)

Topic: Single Sign-On (SSO) with Kerberos

- Explain the purpose of SSO and how it differs from federation
- Describe Kerberos components: Client, KDC, TGS, and Application Server
- Explain the Kerberos authentication and authorization process
- Discuss mutual authentication and its security benefits
- Quick quiz: SSO concepts and Kerberos workflow

Day 11 (Aug 25, Sun)

Topic: Federated Identity Management: SAML & OAuth

- Explain SAML and its role in federated identity
- Describe OAuth and its authorization flows
- Compare SAML vs. OAuth for enterprise and API access
- Discuss practical examples of SAML and OAuth implementations
- Quick quiz: SAML assertions and OAuth tokens

Domain 5: Final Review & Exam Prep

Day 11 (Aug 25, Sun)

Domain: Identity & Access Management
Topic: Federated Identity Management: SAML & OAuth
• Explain SAML and its role in federated identity
• Describe OAuth and its authorization flows
• Compare SAML vs. OAuth for enterprise and API access
• Discuss practical examples of SAML and OAuth implementations
• Quick quiz: SAML assertions and OAuth tokens

Day 12 (Aug 27, Tues)

Domain: Final Review & Exam Prep
Topic: Capstone Review and Graduation
• Targeted review of weak areas (peer coaching)
• Jeopardy-style full exam review
• Personal exam strategy planning
• Graduation & certificate presentation

Teaching Philosophy

✅ **Active Learning**
✅ **Peer Teaching**
✅ **Real-World Application**
✅ **Fun & Engaging Environment**

Materials Provided

- Digital slides & workbook
- Replay recordings
- Practice quizzes & full mock exam

- WhatsApp study group for accountability & Q&A