The Security+ Bootcamp is a fast-paced, highly condensed, "11th hour" crash course for those students who are getting ready to take the Security+ exam in the next few weeks. It is also an excellent course for those who want to discover the depth and breadth of the exam and build their security knowledge foundation for the real world. The course will cover the high-points and more difficult topics of all Security+ domains as well as examine the special question types that test-takers will encounter on the exam.

The instructor for this bootcamp will be Michael J Shannon. Mr. Shannon began his IT career when he transitioned from recording studio engineer to network technician for a major telecommunications company in the early 1990's. He soon began to focus on security and was one of the first 10 people to attain the HIPAA Certified Security Specialist. Throughout his 30 years in IT he has worked as an employee, contractor, and consultant for several companies including Platinum Technologies, Fujitsu, IBM, State Farm, MindSharp, Thomson, Pearson, and Skillsoft among others. Mr. Shannon has authored several books, training manuals, blog articles, and CBT modules over the years as well. He has attained the CISSP, Security+, CCNP Security, Palo Alto PCNSE7, ITIL 4 Managing Professional, and OpenFAIR security-related certifications, as well as other various cloud- based certifications.

Course Syllabus

Session 1

- **Threats, Attacks and Vulnerabilities**
  - Threat actor types and attributes
  - Indicators of compromise and determine the type of malware
  - Types of attacks and exploits
  - Impact associated with types of vulnerabilities
  - Types of malware
- **Social Engineering**
  - Phishing and variants
  - Tailgating and piggybacking
  - Hoaxing and impersonation
  - Shoulder surfing and dumpster diving
- **Application and Service Attacks**
  - DoS, DDoS, and Botnets
  - Man-in-the-middle and spoofing
  - Buffer overflow attacks
  - Injection attacks
  - Poisoning, reflection, and amplification
  - Browser attacks
  - Cryptographic attacks
- **Cryptography and PKI**
  - Basic concepts of cryptography
  - Cryptographic algorithms and their basic characteristics
  - Implement public key infrastructure

Session 2

- **Vulnerability Assessment, Testing, and Scanning**
  - Identifying and assessing vulnerability
  - Identifying misconfigurations
  - System and account vulnerability
  - Vulnerable users and business processes
  - System sprawl and undocumented assets
  - Architecture and design vulnerabilities
  - Improper certificate and key management
  - Vulnerability scanning and testing tools
- **Penetration Testing**
  - Pentesting vs. vulnerability scanning
  - Penetration testing techniques and process
  - White, black, and gray box testing
  - Tools and exploitation kits
- **Infrastructure Devices**
  - Firewalls and access control lists
  - IDS and IPS
  - Secure routers, VPN gateways, switches, and WAPs
  - Proxies and load balancers
  - SIEM and DLP systems
  - Specialty gateway appliances
  - Tools for data sanitization, steganography, and backups
- **Wireless Attacks and Security**
  - Survey of wireless attack types
  - WPA and WPA2
  - Protected Management Frames (PMF)
- **Enterprise Mobility Management (EMM)**
  - Survey of connection methods
  - Mobile deployment models
  - Mobile device management
  - Mobile application and content management
  - Common mobility security issues and enforcement

Session 3

- **Survey of secure protocols**
  - DNSSEC
  - SSH
  - S/MIME
  - SRTP
  - FTPS and SFTP
  - SNMPv3
  - HTTPS-SSL/TLS

    - POP3S and IMAP4
- **Security Standards**
    - Industry standards
    - Frameworks and architectures
    - Benchmarks
    - Compliance and configuration guides
    - Principles of secure design
- **Secure Network Architecture**
    - Zones and topologies
    - Segregation, Segmentation, and Isolation
    - Software Defined Networking (SDN)
    - Hardware root of trust
    - Trusted computing and secure computing
    - Operating system security
    - Securing peripherals
- **Secure Development Concepts**
    - Sandboxing environments
    - Secure baselines
    - SCADA, IoT, and HVAC
    - SoC and RTOS
    - Development lifecycles
    - Security automation and infrastructure-as-code
    - Secure coding principles
- **Virtualization and Cloud Computing**
    - Hypervisors
    - VM security
    - Cloud computing types
    - Cloud deployment models
    - Virtual desktop security
    - Cloud value added services
- **Physical Security**
    - Physical security threats
    - Lighting and cameras
    - Signage, barriers, and security guards
    - Motion detection and alarms
    - Secure enclosures and locks
    - Biometrics, tokens, and cards
    - Environmental controls

Session 4

- **Identity and Access Management**
    - Identity and access management concepts
    - Install and configure identity and access services
    - Implement identity and access management controls

    - Differentiate common account management practices
- **Security Operations**
    - Categories and types of security controls
    - Change and configuration management
    - Data handling, labeling, and classification
    - Data owners, stewards, and custodians
    - Data disposition
    - Account management
    - Auditing and review of operational policies
- **Security Policy**
    - Security awareness and training
    - Acceptable Use Policy (AUP)
    - Written security policies
    - Business agreements
    - Employee onboarding and investigations
    - Exit interviews
- **Risk Management**
    - Defining risk and vulnerability
    - Threat and risk assessment
    - Risk register or ledger
    - Qualitative risk analysis
    - Semi-quantitative risk analysis
    - Quantitative risk management
- **Incident response and forensics**
    - Incident response plans
    - Incident response teams
    - IR process and lifecycle
    - After action and lessons learned
- **Business Continuity Planning**
    - Business and continuity of operations
    - Business Impact Analysis (BIA)
    - Disaster recovery planning
    - Backup and restoration