The table below lists the domain areas measured by the CompTIA Security+™ examination and the approximate extent to which they are represented in the exam:

CompTIA Security+™ Domain	% of Examination
1.0 Network Security	21%
2.0 Compliance and Operational Security	18%
3.0 Threats and Vulnerabilities	21%
4.0 Application, Data and Host Security	16%
5.0 Access Control and Identity Management	13%
6.0 Cryptography	11%
Total	**100%**

The lab exercises listed as follows are mapped to the appropriate CompTIA Security+™ domain and performance-based exam objective:

- **1.0 Network Security**:
  - Objective 1.2: Apply and implement secure network administration principles:
    - **Lab Exercise 1**: *Network Devices and Technologies - Capturing Network Traffic*
    - **Lab Exercise 2**: *Secure Network Administration Principles - Log Analysis*
  - Objective 1.4: Implement and use common protocols:
    - **Lab Exercise 3**: *Protocols and Default Network Ports - Transferring Data Using TCP/IP*
    - **Lab Exercise 4**: *Protocols and Default Network Ports - Connecting to a Remote System*
  - Objective 1.6: Implement wireless network in a secure manner:
    - **Lab Exercise 5**: *Secure Implementation of Wireless Networking*
- **2.0 Compliance and Operational Security**:
  - Objective 2.3: Execute appropriate incident response procedures:
    - **Lab Exercise 6**: *Incident Response Procedures*

- **3.0 Threats and Vulnerabilities**:

- Objective 3.1: Analyze and differentiate among types of malware
  - **Lab Exercise 7**: *Analyze and Differentiate Types of Malware*
- Objective 3.2: Analyze and differentiate among types of attacks:
  - **Lab Exercise 8**: *Analyze and Differentiate Types of Attacks Using Window Commands*
- Objective 3.5: Analyze and differentiate among types of application attacks:
  - **Lab Exercise 9**: *Analyze and Differentiate Types of Application Attacks*
- Objective 3.6: Analyze and differentiate among types of mitigation and deterrent techniques:
  - **Lab Exercise 10**: *Mitigation and Deterrent Techniques - Anti Forensic*
  - **Lab Exercise 11**: *Mitigation and Deterrent Techniques - Password Cracking*
- Objective 3.7: Implement assessment tools and techniques to discover security threats and vulnerabilities:
  - **Lab Exercise 12**: *Discovering Security Threats and Vulnerabilities*

- **4.0 Application, Data and Host Security**:
  - Objective 4.2: Carry out appropriate procedures to establish host security:
    - **Lab Exercise 13**: *Importance of Data Security - Data Theft*
    - **Lab Exercise 14**: *Importance of Data Security - Securing Data Using Encryption Software*

- **5.0 Access Control and Identity Management**:
  - Objective 5.3: Implement appropriate security controls when performing account management:
    - **Lab Exercise 15**: *Authentication, Authorization and Access Control*

- **6.0 Cryptography**:
  - Objective 6.2: Use and apply appropriate cryptographic tools and products:
    - **Lab Exercise 14**: *Importance of Data Security - Securing Data Using Encryption Software*
    - **Lab Exercise 16**: *General Cryptography Concepts*