CSSIA CompTIA Security+® Supported Labs - V1

Lab	Title	CSSIA CompTIA Security+®Domain	Tasks Included
1	Network Devices and Technologies - Capturing Network Traffic	Network Security	• Using tcpdump to Capture Network Traffic • Capturing and Analyzing Traffic with Wireshark • Capturing and Analyzing Traffic with Network Miner
2	Secure Network Administration Principles - Log Analysis	Network Security	• Log Analysis in Linux Using Grep • Log Analysis in Linux Using Gawk • Log Analysis in Windows Using Find
3	Protocols and Default Network Ports - Transferring Data Using TCP/IP	Network Security	• Using Hyper Text Transfer Protocol (HTTP) to Transfer Files • Using Fire Transfer Protocol (FTP) to Transfer Files • Transferring Files Securely Using SCP
4	Protocols and Default Network Ports - Connecting to a Remote System	Network Security	• Connecting to a Windows system Through the Command Line • Connecting to a Linux System Through the Command Line • Analyzing Remote Connections in Network Traffic
5	Secure Implementation of Wireless Networking	Network Security	• Examining Plain Text Traffic • Cracking and Examining WEP Traffic

Lab	Title	CSSIA CompTIA Security+®Domain	Tasks Included
			• Cracking and Examining WPA Traffic
6	Incident Response Procedures	Compliance and Operational Security	• Using db_autopwn to Attack a Remote System • Collecting Volatile Data • Viewing Network Logs
7	Analyze and Differentiate Types of Malware	Threats and Vulnerabilities	• Using Netcat to Send a Reverse Shell • Using Ncat to Send a Reverse Shell • Sending a Bash Shell to a Windows Machine using NetCat
8	Analyze and Differentiate Types of Attacks Using Window Commands	Threats and Vulnerabilities	• Viewing Network Resources • Using PSEXEC to Connect to a Remote System • Stopping, Starting, and Removing Services
9	Analyze and Differentiate Types of Application Attacks	Threats and Vulnerabilities	• Scanning the Network for Vulnerable Systems • Introduction to Metasploit, a Framework for Exploitation • Attacking a Remote System Utilizing Armitage • Post Exploitation of the Remote System
10	Mitigation and Deterrent Techniques - Anti Forensic	Threats and Vulnerabilities	• The Windows Event Viewer • Enabling Auditing • Clearing the Event Logs
11	Mitigation and Deterrent Techniques - Password Cracking	Threats and Vulnerabilities	• Cracking Linux Passwords

Lab	Title	CSSIA CompTIA Security+®Domain	Tasks Included
			• Cracking Windows Passwords • Cracking Windows Passwords with Cain
12	Discovering Security Threats and Vulnerabilities	Threats and Vulnerabilities	• Scanning the Network for Vulnerable Systems • Using Nessus • Introduction to Metasploit, a Framework for Exploration
13	Importance of Data Security - Data Theft	Application, Data and Host Security	• Using Metasploit to Attack a Remote System • Stealing Data using FTP and HTTP • Stealing Data using Meterpreter
14	Importance of Data Security - Securing Data Using Encryption Software	Application, Data and Host Security	• Installing TrueCrypt • Creating a TrueCrypt Container • Opening and Viewing Data within a TrueCrypt Container
15	Authentication, Authorization and Access Control	Access Control and Identity Management	• Adding Users, Groups, and Passwords • Symbolic Permissions • Absolute Permissions
16	General Cryptography Concepts	Cryptography	• Hiding a Picture within a Picture Using S-Tools • Hiding a Media File within a Picture Using S-Tools • Revealing Hidden Data Using S-Tools

CSSIA CompTIA Security+® Supported Labs - v2

Lab	Title	CSSIA CompTIA Security+®Domain	Tasks Included
1	Network Devices and Technologies - Capturing Network Traffic	Network Security	• Using tcpdump to Capture Network Traffic • Capturing and Analyzing Traffic with Wireshark • Capturing and Analyzing Traffic with Network Miner
2	Secure Network Administration Principles - Log Analysis	Network Security	• Log Analysis in Linux Using Grep • Log Analysis in Linux Using Gawk • Log Analysis in Windows Using Find
3	Protocols and Default Network Ports - Transferring Data Using TCP/IP	Network Security	• Using Hyper Text Transfer Protocol (HTTP) to Transfer Files • Using Fire Transfer Protocol (FTP) to Transfer Files • Transferring Files Securely Using SCP
4	Protocols and Default Network Ports - Connecting to a Remote System	Network Security	• Connecting to a Windows system Through the Command Line • Connecting to a Linux System Through the Command Line • Analyzing Remote Connections in Network Traffic
5	Secure Implementation of Wireless Networking	Network Security	• Examining Plain Text Traffic • Cracking and Examining WEP Traffic

Lab	**Title**	**CSSIA CompTIA Security+®Domain**	**Tasks Included**
			• Cracking and Examining WPA Traffic
6	Incident Response Procedures	Compliance and Operational Security	• Using db_autopwn to Attack a Remote System • Collecting Volatile Data • Viewing Network Logs
7	Configuring the pfSense Firewall - **NEW**	Network Security	• Configuring ICMP on the Firewall • Redirecting Traffic to Internal Hosts on the Network • Setting up a Virtual Private Network
8	Configuring Backups - **NEW**	Compliance and Operational Security	• Backing Up Files to a Network Drive • Backing Up Files to an FTP Server • Backing Up Files using SCP
9	Analyze and Differentiate Types of Malware	Threats and Vulnerabilities	• Using Netcat to Send a Reverse Shell • Using Ncat to Send a Reverse Shell • Sending a Bash Shell to a Windows Machine using NetCat
10	Analyze and Differentiate Types of Attacks Using Window Commands	Threats and Vulnerabilities	• Viewing Network Resources • Using PSEXEC to Connect to a Remote System • Stopping, Starting, and Removing Services
11	Analyze and Differentiate Types of Application Attacks	Threats and Vulnerabilities	• Scanning the Network for Vulnerable Systems

Lab	Title	CSSIA CompTIA Security+®Domain	Tasks Included
			• Introduction to Metasploit, a Framework for Exploitation • Attacking a Remote System Utilizing Armitage • Post Exploitation of the Remote System
12	Mitigation and Deterrent Techniques - Anti Forensic	Threats and Vulnerabilities	• The Windows Event Viewer • Enabling Auditing • Clearing the Event Logs
13	Mitigation and Deterrent Techniques - Password Cracking	Threats and Vulnerabilities	• Cracking Linux Passwords • Cracking Windows Passwords • Cracking Windows Passwords with Cain
14	Discovering Security Threats and Vulnerabilities	Threats and Vulnerabilities	• Scanning the Network for Vulnerable Systems • Using Nessus • Introduction to Metasploit, a Framework for Exploration
15	Importance of Data Security - Data Theft	Application, Data and Host Security	• Using Metasploit to Attack a Remote System • Stealing Data using FTP and HTTP • Stealing Data using Meterpreter
16	Importance of Data Security - Securing Data Using Encryption Software	Application, Data and Host Security	• Installing TrueCrypt • Creating a TrueCrypt Container • Opening and Viewing Data within a TrueCrypt Container

Lab	**Title**	**CSSIA CompTIA Security+$^{®}$Domain**	**Tasks Included**
17	Authentication, Authorization and Access Control	Access Control and Identity Management	• Adding Users, Groups, and Passwords • Symbolic Permissions • Absolute Permissions
18	Access Controls - **NEW**	Access Control and Identity Management	• Configuring ICMP on the Firewall • Configuring Auditing for Object Access • Viewing the Security Log to Determine Security Incidents
19	General Cryptography Concepts	Cryptography	• Hiding a Picture within a Picture Using S-Tools • Hiding a Media File within a Picture Using S-Tools • Revealing Hidden Data Using S-Tools
20	Cryptography - **NEW**	Cryptography	• Encryption with the Encrypted File System • Backing up Encrypted File System Keys • Encrypted File System File Recovery