The CyberStars Competition will test participants across a wide range of cyber security competences. Specifically, the competition will test candidates across a number of learning objectives. Learning objectives fall into the following main categories:

- K = Knowledge, assessed through theoretical questions
- C = Competence, assessed through practical questions

The following tables summarize the learning objective domains and the assessment method for each learning objective.

Ethical Hacking

LEARNING OBJECTIVE	K	C
LO 1 Ethical Hacking Methodology		
LO 1.1 Explain the Ethical Hacking Methodology	x	
LO 1.2 Identify examples of unethical conducts with regards to Ethical Hacking	x	
LO 2 Footprinting and Reconnaissance		
LO 2.1 Explain the Footprinting and Reconnaissance phase and identify relevant activities and tools	x	
LO 2.2 Select and use appropriate open-source tools to perform footprinting and reconnaissance activities		x
LO 2.3 Correctly interpret the results from WHOIS queries		x
LO 2.4 Correctly interpret the results from DNS interrogation tools	x	
LO 2.5 Perform Open-source intelligence (OSINT) using Web search engines and open-source tools		x
LO 3 Scanning Networks, Systems		
LO 3.1 Apply and evaluate the effectiveness of different techniques to perform host enumeration		x
LO 3.2 Apply and evaluate the effectiveness of different techniques to perform service enumeration		x
LO 3.3 Explain the difference between TCP and UDP service enumeration	x	
LO 3.4 Explain how it is possible to fingerprint Operating Systems and Services	x	

LEARNING OBJECTIVE	K	C
LO 3.5 Select and apply open-source tools to perform enumeration of networks and systems	x	x
LO 3.6 Explain the meaning and relationship between the terms vulnerability, exploit, threat and risk	x	
LO 3.7 Explain the difference between Network and System vulnerability scanners and Web Application Vulnerability scanners	x	
LO 3.8 Describe the difference between false positives, false negatives, true positives and true negatives	x	
LO 3.9 List and describe best practice initiatives for classifying and exchanging information on vulnerabilities such as CVE, CVSS etc.	x	
LO 3.10 Ability to interpret the results of vulnerability scanners		x
LO 3.11 Ability to identify false positives from Vulnerability Scans		x
LO 3.12 List and describe defences against Vulnerability Scanning	X	
LO 4 Password Attacks		
LO 4.1 Compare the strength of different Windows and Linux authentication schemes	x	
LO 4.2 List and describe different online and offline password cracking techniques	x	
LO 4.3 List and describe most commonly used hash algorithms	x	
LO 4.4 Ability to create effective password lists and user lists for dictionary attacks		x
LO 4.5 Ability to perform password attacks of online services and applications (SSH, FTP, SMTP, HTTP, etc.)		x
LO 4.6 Ability to perform offline password attacks		x
LO 4.7 Ability to capture passwords from compromised systems		x
LO 5 Hacking Web Applications		
LO 5.1 List and describe OWASP top 10 vulnerabilities	x	
LO 5.2 List tools and tool categories related to web application hacking	x	
LO 5.3 Ability to profile target Web servers and Web Applications		x
LO 5.4 Ability to identify false positives in the results of a Web vulnerability scanner		x
LO 5.5 Ability to use open-source tools to exploit OWASP Top 10 vulnerabilities	x	
LO 5.5 Ability to use open-source tools to exploit OWASP Top 10 vulnerabilities	x	
LO 5.6 Assess the existence of different types of SQL Injection vulnerabilities		x

LEARNING OBJECTIVE	K	C
LO 5.7 Ability to exploit SQL injection vulnerabilities to gather database information		x
LO 5.8 Assess the existence of different types of XSS vulnerabilities		x
LO 5.9 Compare different types of attacks to HTTP session management	x	
LO 5.10 Identify weaknesses in a given HTTP session management implementation		x
LO 6 Exploiting Systems		
LO 6.1 List and describe the different techniques for identifying software vulnerabilities	x	
LO 6.2 Explain Common software vulnerabilities	x	
LO 6.3 Describe the architectural components of the Metasploit Framework Architecture		x
LO 6.4 Select and use exploits and payload from the Metasploit Framework to exploit a given vulnerability		x
LO 6.5 List and describe different post-exploitation activities	x	
LO 6.6 Ability to gather information from compromised systems		x
LO 6.7 Ability to upload/download files and tools from the compromised system		x
LO 7 Hacking Wireless Networks		
LO 7.1 Compare different Wireless Standards	x	
LO 7.2 Compare different types of antennas, cards and wireless equipment	x	
LO 7.3 Describe the difference between monitor, master, ad hoc and promiscuous modes	x	
LO 7.4 Use different techniques and tools to identify available wireless networks and extract relevant information		x
LO 7.5 Assess the strength of WEP and WPA/WPA2 implementation		x
LO 7.6 List and describe different types of wireless client attacks	x	
LO 7.7 Ability to identify Rogue Access Points using Kismet	x	
LO 8 Maintaining Access		
LO 8.1 List and describe common techniques used for maintaining access in systems	x	
LO 8.2 Describe the difference between various types of malware	x	
LO 8.3 Ability to establish a backdoor connection to a compromised system using native or basic operating system tools and commands such as ssh and netcat		x

LEARNING OBJECTIVE	K	C
LO 9 Data Exfiltration		
LO 9.1 Describe the terms covert channel and data exfiltration	x	
LO 9.2 List and describe different types of covert channels	x	
LO 9.3 Describe different ways data can be exfiltrated from a company		x
LO 9.4 Ability to use SSH as a covert channel		x
LO 10 Covering Tracks		
LO 10.1 Describe different techniques used to hide information on systems	x	
LO 10.2 List common logs used by operating systems and applications	x	
LO 10.3 Describe different techniques used to alter system and application logs	x	
LO 10.4 Describe different techniques used to hide command line history on systems	x	

Intrusion Detection and Security Monitoring

LEARNING OBJECTIVE	K
LO 1 TCP/IP Protocols	
LO 1.1 List and describe Common networking protocols (e.g. DHCP, ARP, TCP,UDP, IP, ICMP, IPsec)	x
LO 1.2 List and describe Common application protocols (e.g. HTTP, SMTP, FTP, DNS)	x
LO 1.3 Describe the IP fragmentation process and the IP header fields used	x
LO 2 Cyber Threats and Attacks	
LO 2.1 List and describe common types of malware	
LO 2.2 List and describe common network and systems attack patterns	x
LO 2.3 List and describe different types of covert channels	x
LO 3 Network traffic and protocol analysis	
LO 3.1 List and describe bets practice tools to carry out network and protocol analysis	x
LO 3.2 Ability to capture network traffic and to analyse traffic, both live and from traffic capture files using opensource tools	

LEARNING OBJECTIVE	K
LO 3.3 Ability to analyse crafted packets and abnormal behaviour of IP, TCP, UDP protocols	
LO 4 Security Monitoring and Prevention Controls	x
LO 4.1 Define the common features of Network, Host and Wireless IDS/IPS	x
LO 4.2 Explain the difference between and IDS and IPS and related common usage scenarios	x
LO 4.3 List and define different Intrusion Detection Methodologies (e.g. anomaly detection, behavioural analysis, signature based etc.)	x
LO 4.4 List and define best practice network security controls and IDS/IPS Components (e.g. Sensors, Network Taps, Load Balancers, Reverse Proxy etc.)	x
LO 4.5 Compare different deployment architectures of IDS/IPS	x
LO 4.6 Explain the terms False positives, false negatives and Severity of attacks	x
LO 5 Network Intrusion Detection and Prevention Systems	
LO 5.1 List key open source and commercial network IDS/IPS solutions	
LO 5.2 Describe Snort architectural components and different Deployment Options	
LO 5.3 Ability to install, configure and use Snort according to given requirements	
LO 5.4 Ability to run Snort in different modes	
LO 5.5 Describe Snort Rules Structure	x
LO 5.6 Ability to customize and write Snort rules to detect specific attack signatures and to perform specific actions	
LO 5.7 Ability to analyse Snort events both manually and using GUI-applications	
LO 5.8 Ability to managing Snort rules	
LO 5.9 Compare Snort with Suricata	x
LO 5.10 Describe Bro IDS features and in comparison to signature-based IDS	x
LO 5.12 Ability to install, configure and use Ourmon according to given requirements	
LO 5.13 Describe techniques that can be used test the performance of network IDS/IPS	x
LO 5.14 Ability to use opensource tools to test network IDS/IPS performance and effectiveness	
LO 6 Web Application Firewalls (WAF)	
LO 6.1 Explain each of the OWASP Top 10 Vulnerabilities	x

LEARNING OBJECTIVE	K
LO 6.2 List and describe the functionalities of a Web Application Firewall	x
LO 6.3 List key open source and commercial network WAF solutions	x
LO 6.4 Describe ModSecurity Architecture and modes of operation	x
LO 6.5 Ability to install, configure and use ModSecurity according to given requirements	
LO 6.6 Describe ModSecurity rules structure	x
LO 6.7 Ability to customize and write ModSecurity rules to detect and mitigate specific attack signatures and to perform specific actions	
LO 6.8 Ability to write rules using Regular Expressions	
LO 6.9 Ability to Analyze Modsecurity logs both manually and using GUI-applications	
LO 7 Host-Based Intrusion Detection and Prevention Systems (HIDS/HIPS)	
LO 7.1 List and describe the functionalities of Host-Based Intrusion Detection and Prevention Systems	x
LO 7.2 List key open source and commercial HIDS/HIPS	x
LO 7.3 Describe OSSEC Architecture and modes of operation	x
LO 7.4 Ability to install, configure and use OSSEC according to given requirements	
LO 7.5 Describe OSSEC rules structure	x
LO 7.6 Ability to customize and write OSSEC rules to detect and mitigate specific attack signatures and to perform specific actions	
LO 7.7 Ability to analyse OSSEC events both manually and using GUI-applications	
LO 7.4 Use different techniques and tools to identify available wireless networks and extract relevant information	
LO 8 Security Events Analysis	
LO 8.1 List common security events to analyse with regards to network, systems and applications	x
LO 8.2 List and describe common Unix/Linux tools that can be used to parse data (e.g. grep, cut, sed, uniq, awk etc.)	x
LO 8.3 Ability to use common Unix/Linux commands for the purposed of events analysis and other tasks of a security analyst	
LO 8.4 Ability to write Unix/Linux shell scripts to analyse logs from IDS/IPS and other security monitoring and protection systems	
LO 9 Regular Expressions	
LO 9.1 Describe regular expressions (regex) and common use cases	x

LEARNING OBJECTIVE	K
LO 9.2 List and describe different standards of regex	x
LO 9.3 Ability to write regex expression and use them within the context of intrusion detection signatures and events analysis	
LO 10 Security Monitoring Processes	
LO 10.1 List and describe best practice security monitoring processes and protection controls within an organization	x
LO 10.3 List and describe key events to monitor across different applications, systems and networking elements of an ICT infrastructure.	x
LO 10 Covering Tracks	
LO 10.1 Describe different techniques used to hide information on systems	x
LO 10.2 List and describe the key responsibilities of a security analyst	x
LO 10.3 List and describe key events to monitor across different applications, systems and networking elements of an ICT infrastructure.	x
LO 10.4 List and describe best practice reports and deliverables to be produced within an organization.	x

Computer Forensics

LEARNING OBJECTIVE	K
LO 1 Computer Forensics Methodology	
LO 1.1 List and describe the different characteristics of digital evidence	x
LO 1.2 List and describe different types of computer forensics evidence	x
LO 1.3 Describe the evidence collection and management process including the chain of custody	x
LO 1.4 Describe the Role of a computer forensics investigator	
LO 1.5 List and describe Legal and regulatory requirements that apply to apply a computer forensics investigation	x
LO 2 Incident Response	
LO 2.1 List and describe the best practice activities of the incident management process	x
LO 2.2 Describe the difference between a dead and a live system	x
LO 2.3 Explain the Lochard principle	x
LO 2.4 Describe the response processes involving a live system and a dead system	x

LEARNING OBJECTIVE	K
LO 3 Live Media collection and Analysis	
LO 3.1 List and describe different memory storage types and the related order of volatility	x
LO 3.2 List and describe the type of information that can be collected from different types of volatile memory storage systems	x
LO 3.3 List and describe different opensource tools for the collection of volatile data	x
LO 3.4 Ability to collect volatile data using opensource tools across Windows, Unix/Linux and Apple operating systems	
LO 3.5 Ability to analyse volatile data	
LO 4 Physical Media Data Collection and Analysis	
LO 4.1 Describe the difference between physical and logical acquisition	x
LO 4.2 List and describe different approaches for hard disk drive imaging	x
LO 4.3 Ability to perform hard drive and media imaging	
LO 4.4 Ability to analyse data from persistent storage media	
LO 4.5 Describe the structure and key elements of the Windows registry	x
LO 4.6 Ability to analyse the Windows Registry using opensource tools	
LO 4.7 Ability to create a computer forensics timeline	
LO 4.8 Ability to recover deleted evidence	
LO 5 File Systems	
LO 5.1 Describe the difference and relationship between the physical, filesystem, data, metadata and filename layers	x
LO 5.2 Ability to analyse information about physical, filesystem, data, metadata and filename layers using opensource tools	
LO 5.3 List and describe common filesystem layers (e.g. Microsoft, Unix/Linux and MacOS)	x
LO 6.1 List and describe key artifacts related to common Internet Browsers (e.g. Chrome, Firefox, Safari and IE	x
LO 6.2 Ability to collect and analyse internet browsers artifacts using opensource tools	
LO 7 Social Media Forensics and Artifacts	
LLO 7.1 List common opensource tools that can be used to carry out social media forensics	x
LO 7.2 Ability to extract and analyse key artifacts related to standard social media	

LEARNING OBJECTIVE	K
LO 8 File Forensics	
LO 8.1 List and describe the type of information that can be extracted from file	x
LO 8.2 List common opensource tools that can be used to carry out file forensics	x
LO 8.3 Ability to extract and analyse metadata from files	
LO 9 Network Forensics	
LO 9.1 Define Network Forensics and the related activities	
LO 9.2 List and describe different examples of network-based evidence	x
LO 9.3 List and describe different wiretapping strategies	x
LO 9.4 Ability to collect and analyse network-based evidence using opensource tools	
LO 10 Reporting	
LO 10.1 List and describe key elements of a computer forensics report	x
LO 10.2 List and describe common factors affecting Presentation of findings	x
LO 8.3 Ability to use common Unix/Linux commands for the purposed of events analysis and other tasks of a security analyst	
LO 8.4 Ability to write Unix/Linux shell scripts to analyse logs from IDS/IPS and other security monitoring and protection systems	
LO 9.1 Describe regular expressions (regex) and common use cases	x
LO 9.2 List and describe different standards of regex	x
LO 9.3 Ability to write regex expression and use them within the context of intrusion detection signatures and events analysis	
LO 10 Security Monitoring Processes	
LO 10.1 List and describe best practice security monitoring processes and protection controls within an organization	x
LO 10.3 List and describe key events to monitor across different applications, systems and networking elements of an ICT infrastructure.	x
LO 10 Covering Tracks	
LO 10.1 Describe different techniques used to hide information on systems	x
LO 10.2 List and describe the key responsibilities of a security analyst	x