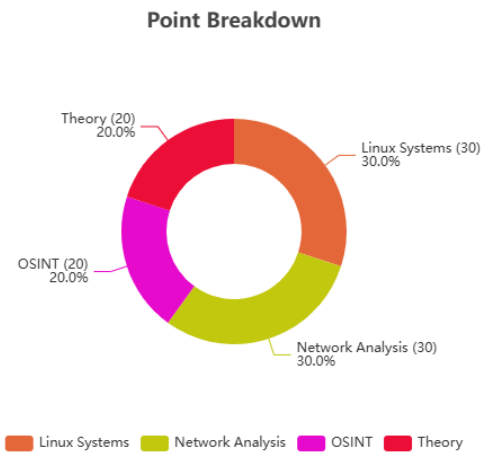
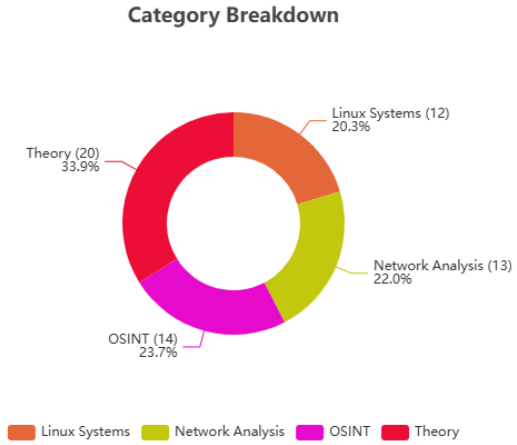
World Skills Pre-Competition Notes:

This pre-competition stage is divided into four parts:

1. **OSINT (Open Source Intelligence):** Participants will demonstrate their ability to gather and analyse publicly available information to uncover valuable insights.
2. **Network Analysis:** Competitors will be tasked with examining network traffic and identifying potential security threats and vulnerabilities.
3. **Theory Questions:** A series of theoretical questions will test participants' knowledge of cybersecurity principles, best practices, and current trends.
4. **Linux Reconnaissance:** This segment will challenge contestants to use their Linux skills to perform reconnaissance and gather critical information from systems.

The breakdown of the competition is as follows: 4 section totalling 100 points.





Theory

The theory section consists of the following Questions:

name	description	Answer	value	category
Theory 1	What is the term for malicious software designed to disrupt, damage, or gain unauthorised access to computer systems? (Single Word Answer)	Malware	1	Theory
Theory 2	What do you call an attack where a person is tricked into revealing sensitive information through deception?(Single Word Answer)	Phishing	1	Theory
Theory 3	What is the name of the practice of protecting sensitive data by converting it into an unreadable format?(Single Word Answer)	Encryption	1	Theory
Theory 4	What is the standard protocol used to secure communications over the internet?(Single Word Answer)	HTTPS	1	Theory
Theory 5	What is the common term for a program that replicates itself and spreads to other devices?(Single Word Answer)	Worm	1	Theory
Theory 6	What is the primary goal of a firewall in a network?(Single Word Answer)	Protection	1	Theory
Theory 7	What is the process of verifying the identity of a user or device before granting access?(Single Word Answer)	Authentication	1	Theory
Theory 8	What is the term for a weakness or flaw in a system that can be exploited by an attacker?(Single Word Answer)	Vulnerability	1	Theory
Theory 9	What type of attack involves overwhelming a system with a flood of traffic to make it unavailable?(Single Word Answer)	DDoS	1	Theory
Theory 10	What do you call a device that monitors and filters incoming and outgoing network traffic to ensure security?(Single Word Answer)	Firewall	1	Theory
Theory 11	Which browser feature allows anyone to view front-end JavaScript and source files? HINT: _ _ _ _ _ _ _ _ _ _ _ _ _ _	Developer tools	1	Theory
Theory 12	What SQL clause can be used to retrieve data from multiple tables? HINT: _ _ _ _ _	union	1	Theory
Theory 13	What insecure coding practice allows SQL to be injected by mixing user input into queries? HINT: _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _	Input Concatenation	1	Theory

Theory 14	What principle states users should only have minimum necessary permissions? HINT: _	Least Privilege Principle	1	Theory
Theory 15	"What term describes an attack where malicious input is stored first and triggers later when the server uses it in a query?	Second-Order SQL injection	1	Theory
Theory 16	HINT: _ _ _ _ _ _ - _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _	script	1	Theory
Theory 17	"	Obfuscation	1	Theory
Theory 18	What HTML tag is most commonly blocked to prevent basic cross-site script injection? HINT: < _ _ _ _ _ _ >	Steganography	1	Theory
Theory 19	What is the term for intentionally making code harder to read to conceal its purpose? HINT: _ _ _ _ _ _ _ _ _ _ _	Parameterised query	1	Theory
Theory 20	"What is the name of the technique where information is hidden inside image, audio, or other media?	Cookie	1	Theory

OSINT

The OSINT section consists of the following Questions:

name	description	Answer	value	category
OSINT 1	Which Google operator restricts results to a specific domain?	site	1	OSINT
OSINT 2	What type of metadata often contains location data in photos?	GPS	1	OSINT
OSINT 3	Which service is commonly used to check domain registration details?	whois	1	OSINT
OSINT 4	Which platform shows historical versions of websites?	wayback	1	OSINT
OSINT 5	Which DNS record identifies mail servers for a domain?	mx	1	OSINT
OSINT 6	What year was the domain facebook.com first registered?	1997	1	OSINT
OSINT 7	Which company is the registrar for facebook.com?	RegistarSafe	1	OSINT
OSINT 8	What is the primary authoritative nameserver beginning with the letter “a” for facebook.com?a.ns.facebook.com	a.ns.facebook.com	1	OSINT
OSINT 9	What year was the domain meta.com created	1991	2	OSINT
OSINT 10	What is the MX mail host (hostname only) for facebook.com according to DNS lookup	smtpin.vvv.facebook.com	2	OSINT
OSINT 11	At which university did Mark Zuckerberg begin developing Facebook?	Harvard	2	OSINT

OSINT 12	What programming language was the earliest version of Facebook primarily written in?	PHP	2	OSINT
OSINT 13	What month was Mark Zuckerberg born in?	May	2	OSINT
OSINT 14	What is the top-level domain of the original Facebook domain name used at Harvard?	edu	2	OSINT

Network Analysis

The Network Analysis section consists of the following Questions each question will require the analysis of the file provided, competitors will need access to software or a site that can parse pcap files:

name	description	Answer	value	category
NA 1	> The file attached to this challenge is to be used for all challenges in the Network Analysis Section. [WorldSkills2025-Entry.pcap](/files/57a376d989a74bd820a6a4394ee02395/WorldSkills2025-Entry.pcap) What is the source IPv4 Address	192.168.1.101	2	Network Analysis
NA 2	IPv4 Address of DNS server	192.168.1.1	2	Network Analysis
NA 3	IPv6 Link-Local Address of the Default Gateway	fe80::a00:27ff:fe45:1e6c	2	Network Analysis
NA 4	Default Gateway MAC Address (use format of xx:xx:xx:xx:xx:xx)	08:00:27:45:1e:6c	2	Network Analysis
NA 5	Transport layer protocol type of 1st Packet	UDP	2	Network Analysis
NA 6	1st Packet Domain Name query URL	httpbin.org	2	Network Analysis
NA 7	IPv4 Address Answer from Domain Query	54.196.242.26	2	Network Analysis
NA 8	Source Port number used in 3-Way Handshake	35114	2	Network Analysis
NA 9	Destination Port number used in 3-Way Handshake	80	2	Network Analysis

NA 10	Using Unix time, input the time last packet was recorded on the packet capture	1738667254	3	Network Analysis
NA 11	User-Agent of source PC	Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0\r\n	3	Network Analysis
NA 12	Username input on login prompt	WorldSkills	3	Network Analysis
NA 13	Password input on Login prompt	LetM31n	3	Network Analysis

Linux Reconnaissance

The Linux Reconnaissance section is done in a more traditional CTF where the competitor is to explore a system and collect “flags” therefore there are no questions as such, just flags that they must discover, these will be found on a hosted website that we will provide access to on the day of the pre-competition activity:

Linux 1	Through the system you will be looking for certain tokens, this particular one starts with **wsentry-1{**	wsentry-1{GYSHAXYZRFN0B5Z1MFQRKI33122FVFX6}	1	Linux
Linux 2	Through the system you will be looking for certain tokens, this particular one starts with **wsentry-2{**	wsentry-2{FM4JESOKM50QHKHJG52W2G4JT63SL2IB}	1	Linux
Linux 3	Through the system you will be looking for certain tokens, this particular one starts with **wsentry-3{**	wsentry-3{5NUBC0WGY8IYHN689RC5MD1IVZYWW4S4}	1	Linux
Linux 4	Through the system you will be looking for certain tokens, this particular one starts with **wsentry-4{**	wsentry-4{LPJYHL9U53H6P05US28TULAZJS707XXZ}	3	Linux
Linux 5	Through the system you will be looking for certain tokens, this particular one starts with **wsentry-5{**	wsentry-5{VGMP99EKBQIQBU073KN6U8JE75VSYYS3}	3	Linux
Linux 6	Through the system you will be looking for certain tokens, this particular one starts with **wsentry-6{**	wsentry-6{G555HBDQGYY6ZGDAA9EEJY23DW45KM6D}	3	Linux
Linux 7	Through the system you will be looking for certain tokens, this particular one starts with **wsentry-7{**	wsentry-7{EP325PL1IN6JTHUCHJ2KGEZON77UQ505}	1	Linux
Linux 8	Through the system you will be looking for certain tokens, this particular one starts with **wsentry-8{**	wsentry-8{7SDZSB579NJWD7RLFVY2Q74LD5N529RD}	3	Linux
Linux 9	Through the system you will be looking for certain tokens, this particular one starts with **wsentry-9{**	wsentry-9{4AG2SAUGMENCEWQV54UAIXB9THFH2ZSV}	3	Linux
Linux 10	Through the system you will be looking for certain tokens, this particular one starts with **wsentry-10{**	wsentry-10{LKHP7UD9FVL3SLC0ZNOWYA9JBDN2P6CV}	3	Linux
Linux 11	Through the system you will be looking for certain tokens, this particular one starts with **wsentry-11{**	wsentry-11{37A8NNECCXBXS8V3GZ4VD5XHCZZDAEE6}	4	Linux
Linux 12	Through the system you will be looking for certain tokens, this particular one starts with **wsentry-12{**	wsentry-12{CR5Q1RHFPVB0O1XYE5Z7BT5RKRBETEUL}	4	Linux