THE CYBERLAUNCH CTF

POWERED BY CYBER FLORIDA

CYBER LAUNCH

2025 CTF Instructor Playbook

By EC-Council

Attention Teachers and Faculty:

Thank you for registering your team(s) for this year's 2025 CyberLaunch Capture the Flag competition!

The purpose of this playbook is to share information on the following:

1. Capture the Flag Difficulty Level Overview
2. Capture the Flag Competition Rounds and Times
3. CTF Challenges (Total Points & Skills Coverage)
4. Access to the Scoreboard

1. Capture the Flag Difficulty Level Overview

- All levels have up to 4 players on a single team. Schools are limited to 12 players total.
- Each team will have 1 CTF access point to the range, while other players may have 1 single device (e.g. Laptop, or Tablet/Phone) to research or support topics.

BASIC Level => Access handed out in a GREEN folder (Example Username: CL-B-TEAM-001)

(E.g. Students that have not taken a cybersecurity course before)

Open Notes/Internet, With Step-By-Step Instructions

- 7 trivia questions, 1 max attempt/question
- Guided Instructions
- Up to 5 flag attempts

INTERMEDIATE Level => Access handed out in a BLUE folder (Example Username: CL-I-TEAM-001)

(E.g. Students that have taken a cybersecurity course before and have basic networking knowledge)

Open Notes/Internet, With Step-By-Step Instructions

- 5 trivia questions, 1 max attempt/question
- Guided Instructions
- Up to 5 flag attempts

ADVANCED Level => Access handed out in a BLACK folder **(Example Username: CL-A-TEAM-001)**

(E.g. Students that have taken one or more cybersecurity courses before, and have basic networking and information security knowledge)

Open Notes/Internet, With Step-By-Step Instructions

- No trivia question
- No Instructions
- Up to 5 flag attempts

2. Capture the Flag Competition Rounds and Times

- Round 1: 10:00 AM - 12:00 PM (Basic, Intermediate, and Advanced Teams compete)
- Round 2: 1:00 PM - 3:00 PM (Basic, Intermediate, and Advanced Teams compete)

Since there are 4 hours worth of CTFs, we will present 6 hours of challenges (e.g. 2 bonus challenges), including the following:

6 BASIC CTFs: 3 for Round 1 ; 3 for Round 2 (Note: Provided on a single CTF Token)

6 INTERMEDIATE CTFs: 3 for Round 1 ; 3 for Round 2 (Note: Provided on a single CTF Token)

6 ADVANCED CTFs: 3 for Round 1 ; 3 for Round 2 (Note: Provided on a single CTF Token)

3. CTF Challenges (Total Points & Skills Coverage)

Challenge	Rating	Primary Skills	Flags	Trivia	Points
Intro To The Cyber Range	Basic	Cyber Range Navigation and Virtual Machine Basics Capture the Flag Fundamentals Networking and System Interaction Troubleshooting and System Management Ethical Hacking Mindset and Best Practices	12	7	107
Qwertyuiop	Basic	Network Scanning with Nmap Web Application Enumeration Burp Suite Proxy Usage Command Injection Exploitation Base64 Encoding & Decoding SSH Key Exploitation Privilege Escalation Cryptographic Hash Analysis	7	7	107
Intruder	Basic	Packet Capture Analysis (PCAP Analysis) Wireshark Filtering & Protocol Analysis Wireless Network Investigation WPA2 Handshake Identification Password Cracking with Aircrack-ng Decryption of Network Traffic HTTP Traffic Analysis & Credential Extraction Cybersecurity Incident Investigation	10	7	107
Decepti0n.exe	Basic	Network Scanning & Service Enumeration Web Enumeration Directory Brute-Forcing Social Engineering Email Spoofing Phishing Attacks Reverse Shell Execution Netcat Usage Privilege Escalation Sudo Misconfiguration Exploitation Basic Linux Command-Line Navigation SMTP Interaction User Awareness and Defensive Security Concepts	11	7	107
Kernel	Basic	Reconnaissance & Scanning Vulnerability Research Remote Code Execution (RCE) Privilege Escalation SSH Key Cracking Reverse Shell Execution Post-Exploitation & System Navigation Exploit Compilation & Execution File Transfer & Web Hosting	12	7	107
Shark	Basic	Network Reconnaissance Traffic Analysis Service Enumeration Credential Harvesting Privilege Escalation Network Forensics Command Execution & System Enumeration	14	7	107

Challenge	Rating	Primary Skills	Flags	Trivia	Points
Arbfile	Intermediate	Network Scanning & Enumeration Web Application Exploitation Reverse Shell Execution Password Cracking & Credential Extraction Privilege Escalation Linux System Navigation	12	5	105
Mara	Intermediate	Network Scanning SMB Enumeration NetBIOS Information Extraction Traffic Analysis Credential Extraction Password Cracking Web Vulnerability Identification Remote Code Execution Privilege Escalation Post-Exploitation	13	5	105
Policy	Intermediate	Active Host Discovery Service Enumeration Web Application Exploitation Reverse Shell Deployment Custom Wordlist Generation Brute-Force Authentication Remote Command Execution Privilege Escalation Windows Task Analysis System Flag Extraction	15	5	105
Kerberoasted	Intermediate	Network Scanning & Enumeration Active Directory Enumeration Kerberos AS-REP Roasting Password Cracking Web Directory Bruteforcing File Upload Exploitation Remote Command Execution (RCE) Privilege Escalation Log Analysis & Detection Awareness	13	5	105
Corporate Breach	Intermediate	Network Scanning & Service Enumeration SMB Enumeration & Exploitation Packet Capture Analysis Data Decoding & Obfuscation Analysis Password Cracking & Brute-Forcing Windows Remote Exploitation Post-Exploitation & System Control	15	5	105
Hospital Hack 2.0	Intermediate	Network Scanning with Nmap Service Version Detection CVE Research & Exploit Validation SQL Injection Exploitation Metasploit Module Execution Apache Security Hardening Web Application Enumeration	10	5	105

Challenge	Rating	Primary Skills	Flags	Trivia	Points
Operation Entry Level	Advanced	Cryptanalysis Reverse Engineering Javascript Application Security Password Management	3	0	100
Operation Deobfuscate	Advanced	Reverse Engineering Javascript Application Security	3	0	100
Operation Windows	Advanced	Windows Internals Application Security Reverse Engineering	3	0	100
Operation Escalate	Advanced	Linux System Security Application Security Password Cracking Password Management	3	0	100
Operation Penguin	Advanced	Linux Internals Application Security Reverse Engineering	3	0	100
Operation Decipher	Advanced	Cryptanalysis Reverse Engineering Random Number Generation Algorithms	3	0	100

Access to the Scoreboard

Basic Capture the Flag

Intermediate Capture the Flag

Advanced Capture the Flag

THE CYBERLAUNCH CTF

POWERED BY CYBER FLORIDA

DID YOU KNOW?

This Capture the Flag competition is hosted by EC-Council,
the creators of Certified Ethical Hacker.

C|EH

Certified Ethical Hacker