

Cyber Security Training

This is a curated list of interactive platforms, games, CTFs, open-source intelligence tools, and educational resources for anyone interested in cybersecurity, threat hunting, or ethical hacking.

Source:

https://www.linkedin.com/posts/mohessa511_cybersecurity-incidentresponse-playgames-activity-7132644163556114432-xC67?utm_source=share&utm_medium=member_desktop&rcm=ACoAAB4yqIYBh8d6l6lWTW6bdVPynH4m3OpMRZI

And own additions

📁 Learning Platforms

- [INE](#) – Free cybersecurity and networking courses.
 - [Immersive Labs](#) – Advanced interactive cybersecurity labs.
 - [RangeForce](#) – Interactive and scalable cyber training.
 - [Pluralsight](#) – Developer & security skill-building platform.
 - [Haiku, Inc](#) – Platform for hosting cybersecurity ranges and challenges.
 - [Pentest Cheat Sheets](#) – Collection of red team tactics and commands.
 - [Darkstar7471](#) – Blog of a TryHackMe admin with various security insights.
 - [Gian's GitHub Page](#) – Personal write-ups and insights from a LinkedIn security expert.
-

📁 Learning Platforms & CTFs

- [Hacksplaining](#)
Interactive lessons explaining common web vulnerabilities and their mitigations.
- [picoCTF](#)
Beginner-friendly CTF (Capture The Flag) competition platform created by cybersecurity experts at Carnegie Mellon.

- [**Let's Defend**](#)
Blue team-focused simulation platform with SOC analyst tasks.
 - [**OverTheWire**](#)
Classic wargames to learn Linux security, shell scripting, and exploitation.
 - [**HackerOne CTF**](#)
A hacking playground hosted by HackerOne for web vulnerability training.
 - [**Splunk Boss of the SOC**](#)
Realistic SOC analyst challenges using Splunk data.
 - [**CyberDefenders**](#)
Blue team-oriented challenges and training platform.
 - [**CyberDefenders Blue Team CTFs**](#)
Archive of practical detection and analysis challenges.
 - [**EchoCTF**](#)
Competitive red/blue team CTF environment.
 - [**Exploitation Education**](#)
Linux-based exploitation challenges covering stack overflows, heap, and format strings.
 - [**Google CTF**](#)
Official Google-hosted cybersecurity CTFs.
 - [**W3Challs**](#)
Various hacking challenges: web, forensics, and crypto.
 - [**WeChall**](#)
Meta-CTF aggregator that tracks your challenge progress across sites.
 - [**Webgoat**](#)
OWASP's deliberately insecure web app for learning web vulnerabilities.
 - [**CMD Challenge**](#)
Solve problems using only Linux command line knowledge.
 - [**CryptoHack**](#)
Learn cryptography by solving Python-based challenges.
 - [**CTFtime**](#)
CTF competition calendar and team ranking tracker.
 - [**Vulnmachines**](#)
Vulnerable machines and labs to practice penetration testing.
 - [**Alert to Win**](#)
Fun JavaScript-based hacking challenge.
 - [**TCM Security Academy**](#)
Practical cybersecurity courses including ethical hacking and OSINT.
-

☐☐ Hacking-Themed Games

- [**Duskers**](#)
Sci-fi tactical game using command-line-like interface.
 - [**TIS-100**](#)
Assembly language puzzle game that simulates reverse engineering.
 - [**ThreatGen Red vs. Blue**](#)
Turn-based strategy game teaching cyber offensive/defensive skills.
 - [**Spudnet Board Game**](#)
Fun family board game teaching cybersecurity concepts.
 - [**Nite Team 4**](#)
A tactical hacking simulation game with real-world inspired missions.
 - [**Hacknet**](#)
Terminal-based hacking simulation game.
-

☐☐ Reports & Insights

- [**2024 State of the Security Team - TrendMicro**](#)
Research report on challenges faced by security teams.
 - [**Backdoors & Breaches Card Game**](#)
A fun tabletop game to simulate incident response and detection.
-

Revision #3

Created 9 July 2022 12:27:52 by Togoboi

Updated 2 July 2025 21:14:57 by Togoboi