CTFs und Ethical Hacking

Falls ihr bemerkt, das etwas falsch ist oder es gibt etwas, woran ihr euch stört, gebt mir bitte Bescheid.

1. CTFs?
2. Recht und Ethik
3. Methodik
4. Hands-on: OWASP Juice Shop
5. Abschluss und Ressourcen

CTFs?

Capture **T**he **F**lag

- sind Wettbewerbe, bei denen Teilnehmende Schwachstellen suchen, finden und ausnutzen, um versteckte Informationen ➜ Flags zu finden
- `Flag{w3lc0m3_t0_th3_w0rld_0f_h4ck1ng}`

Links

- Try Hack me: https://tryhackme.com/de
- Hack the box: https://www.hackthebox.com/
- OverTheWire: https://overthewire.org/wargames/

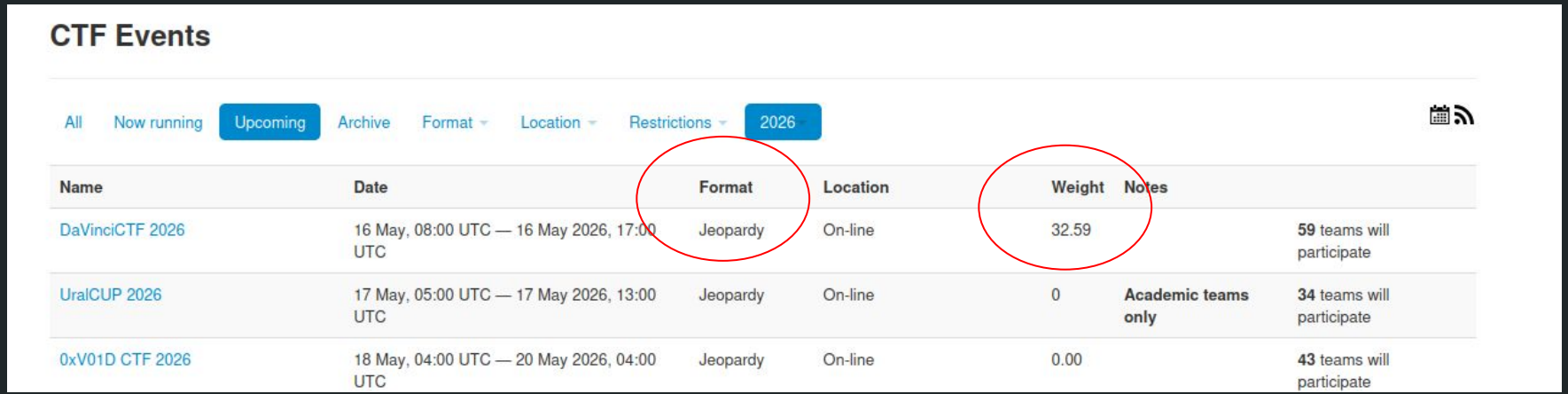
Windows und AD:

- GOAD: https://github.com/Orange-Cyberdefense/GOAD

Links

Upcoming Events:

- https://ctftime.org/event/list/upcoming



CTF Events

All | Now running | Upcoming | Archive | Format | Location | Restrictions | 2026

Name	Date	Format	Location	Weight	Notes	
DaVinciCTF 2026	16 May, 08:00 UTC — 16 May 2026, 17:00 UTC	Jeopardy	On-line	32.59		**59** teams will participate
UralCUP 2026	17 May, 05:00 UTC — 17 May 2026, 13:00 UTC	Jeopardy	On-line	0	**Academic teams only**	**34** teams will participate
0xV01D CTF 2026	18 May, 04:00 UTC — 20 May 2026, 04:00 UTC	Jeopardy	On-line	0.00		**43** teams will participate

CTFs?

Spielmodi:

- **Jeopardy:** Teilnehmende wählen aus verschiedenen Kategorien (Web-Sicherheit, Kryptografie) Aufgaben mit unterschiedlichen Schwierigkeitsgraden aus. Jede gelöste Aufgabe bringt Punkte.
- **Attack/Defense:** Teams treten direkt gegeneinander an. Jedes Team hat ein eigenes Netzwerk/Server mit Schwachstellen, das es gegen Angriffe verteidigen muss. Gleichzeitig soll das gegnerische Team angegriffen werden.
- **King of the Hill:** Teams müssen den Hill einnehmen und gegen andere Teams verteidigen

CTFs?

Typische Kategorien:

Recht und Ethik

Es gilt:

Jeder Zugriff auf fremde IT-Systeme ohne ausdrückliche Erlaubnis ist grundsätzlich rechtswidrig.

Das bedeutet:

- Pentesting ist **nur mit Autorisierung (schriftlich!) legal**
- Red Teaming benötigt klare vertragliche Freigaben
- Schon Scan-Aktivitäten können problematisch sein

Recht und Ethik

- stiftungdatenschutz.org/veroeffentlichungen/datenschutz-im-fokus/datenschutz-im-fokus-detailansicht/ethical-hacking-bleibt-riskant-636
- https://www.heise.de/news/Bundesverfassungsgericht-lehnt-Beschwerde-im-Fall-Modern-Solution-ab-10663649.html

Recht und Ethik - Paragraphen

- **§ 202a StGB – Ausspähen von Daten:**
  - unbefugtes beschaffen von gesicherten Daten
  - Beispiele:
    - Passwortgeschützte Systeme
    - interne Netzwerke
    - Datenbanken

- **§ 202b StGB – Abfangen von Daten:**
  - Mitschneiden fremder Kommunikation
  - Sniffing
  - MITM ohne Berechtigung
  - Beispiele:
    - Wireshark in fremdem Netz
    - Session-Capturing

Recht und Ethik - Paragraphen

- **§ 202c StGB – „Hackerparagraph“:**
  - Strafbar kann sein:
    - Herstellen
    - Beschaffen
    - Verkaufen
    - Verbreiten

    von Werkzeugen, deren Zweck Straftaten nach §202a/b ist.

Recht und Ethik - Paragraphen

- **§ 303b StGB – Computersabotage**

  Sehr wichtig für Red Teams.

  - Verboten:
    - Systeme stören
    - lahmlegen
    - DoS verursachen

Zum nachlesen:

Link: https://www.bundestag.de/resource/blob/1005444/ed435cb1a5311bb688385a81f295c8a3/WD-7-104-23-pdf.pdf

Recht und Ethik

Immer für Pentesting und Red-Teaming

- **Schriftliche Beauftragung**
- **Scope Definition**
- **Rules of Engagement**
- **Haftungsregelungen**
- **Datenschutzvereinbarung**

CTFs-Methoden

Wie beginnen?

- Reconnaissance (Informationsgewinnung)
  - DNS-, OSINT-Recherche
  - Port-Scan mit dem Tool Nmap
  - Banner Grabbing
- Enumeration
  - detaillierte Analyse gefundener Dienste z.B. mit SMB Enumeration (Windows-Freigaben)
  - oder Web Enumeration: Verzeichnisse und APIs untersuchen -> Tools: Gobuster, Dirb, Dirbuster
    - z.Bsp. gobuster dir -u http://target -w wordlist.txt
  - Userlisten auslesen
- Quellcodeanalyse

CTFs-Methoden

Was mit den gefundenen Informationen anfangen?

- Vulnerability Analysis
- Exploitation
- Privilege Escalation
- Lateral Movement

Hands-on: OWASP Juice Shop

- Docker: https://github.com/juice-shop/juice-shop

Docker Container

docker pulls 86M docker stars 227

1. Install Docker
2. Run `docker pull bkimminich/juice-shop`
3. Run `docker run --rm -p 127.0.0.1:3000:3000 bkimminich/juice-shop`
4. Browse to http://localhost:3000 (on macOS and Windows browse to http://192.168.99.100:3000 if you are using docker-machine instead of the native docker installation)

- Herokuapp: http://juice-shop.herokuapp.com/#/

Hands-on: OWASP Juice Shop

Challenges zum Einsteigen:

1. Finden der Seite mit allen Challenges
2. Sensitive Data Exposure -> Meta Geo Stalking

Most important part:

FUN