Friedrich-Alexander-Universität
Technische Fakultät

FAU

Capture-the-flag-Wettbewerbe: Mit Praxiserfahrungen sicherer werden

$ whoami

$ > Immanuel Lautner immanuel.lautner@fau.de

M.Sc. Informatik:

- IT-Security
- Kryptographie
- Künstliche Intelligenz

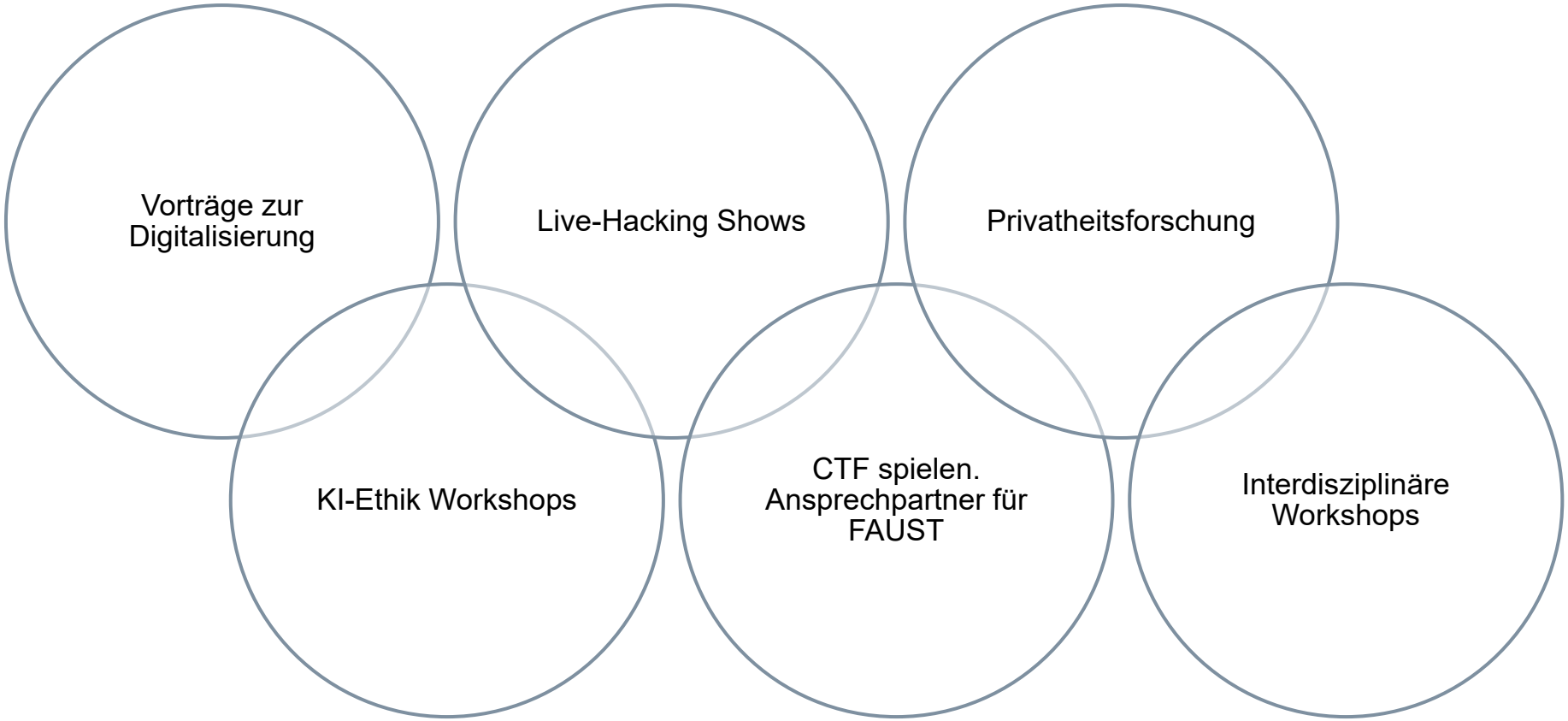
M.A. Ethik der Textkulturen:

- Staatsphilosophie
- Rechtsphilosophie
- Angewandte Ethik

Privatheit in der Arbeit von IT-Sachverständigen

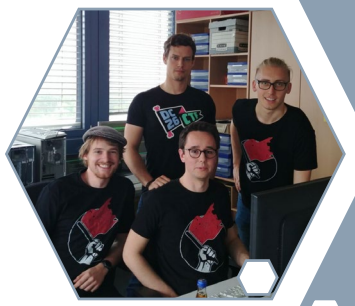
Und sonst so?

Ich versuche zu verstehen!



FAUST

FAU – Security Team



Gelerntes praktisch anwenden

Capture-The-Flag

Hacking for Fun and Profit (and Legal!)

Eigene (Hacking)-Skills erweitern

An (inter)-nationalen Wettbewerben teilnehmen (Las Vegas, Abu Dhabi, Mannheim, …)

Im Team an komplexen Aufgaben arbeiten

FAUST

FAU – Security Team

FAU

- Zwischen 10-20 aktive Mitglieder
- 2021: 2 in DE, 2022: 4 in DE
- Besteht seit 2010
- Seit 2015 eigener Wettbewerb(A&D)
- Wöchentliche Treffen

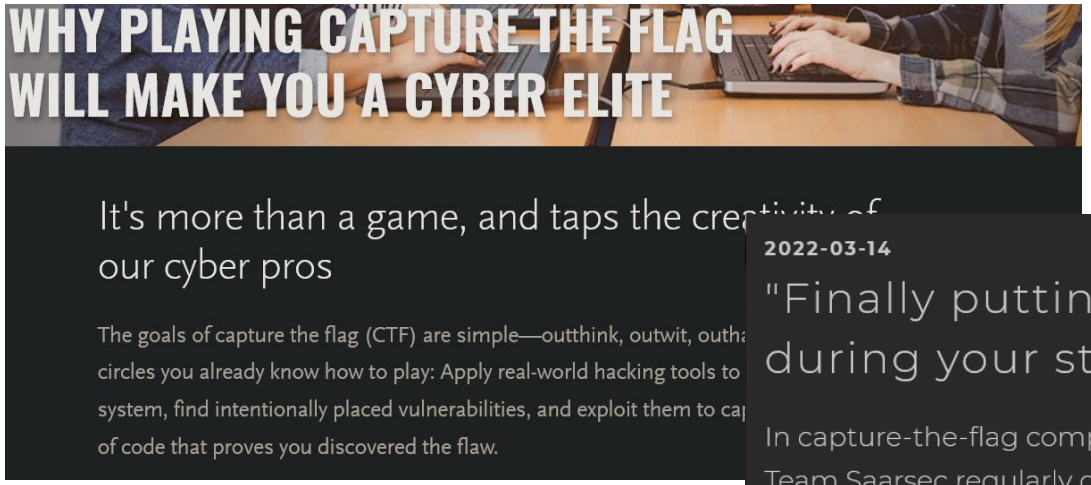
Was sind CTFs?

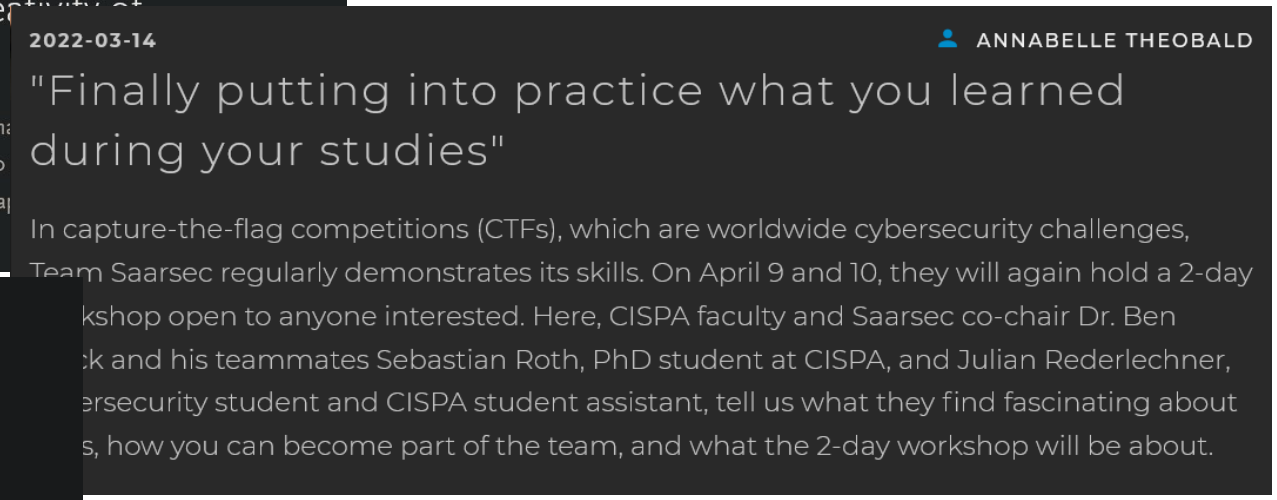
Was ist CTF?

Capture the Flag

Was ist CTF?

Capture the Flag



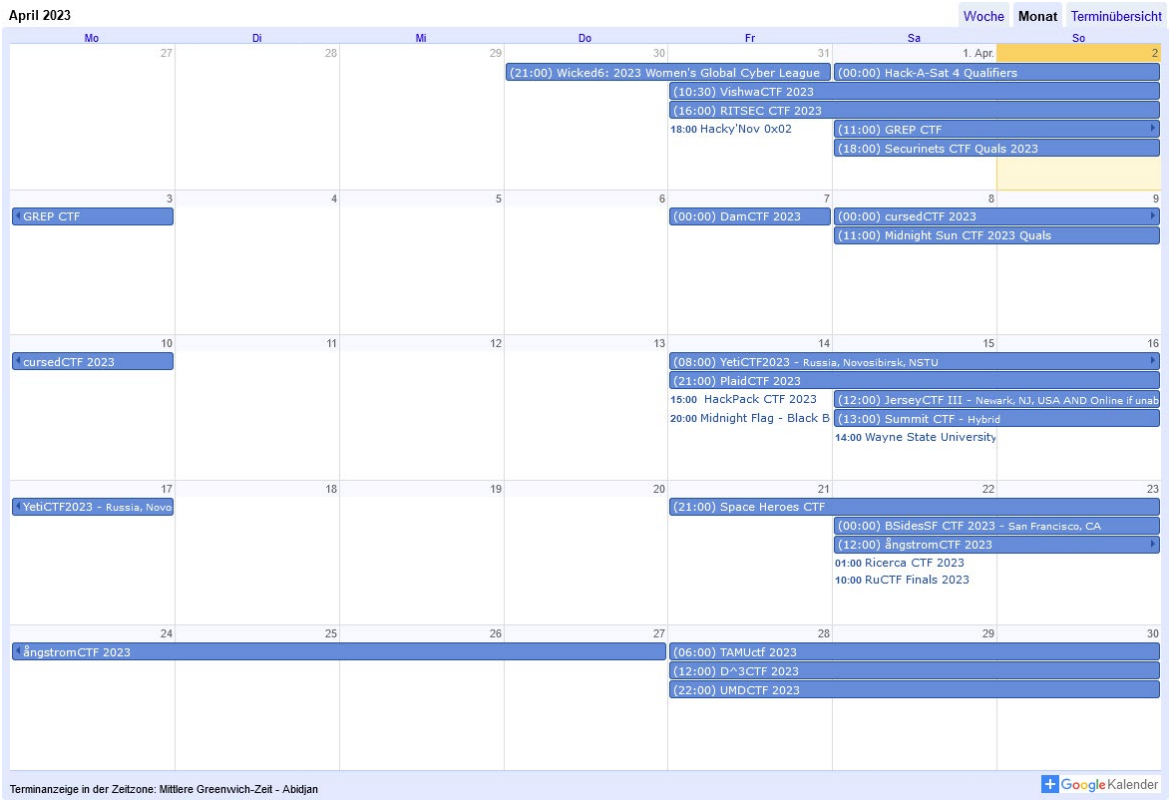


Was ist CTF?

Zahlen und Fakten

FAU

- 11841 Teams laut CTFTime
- 924 Teams in Deutschland
- „Erfindung“ 1993 auf der DefCon
- Def Con CTF immer noch die Weltmeisterschaft
- Deutsches „Über“-Team Namens Sauercrowd
- Meisten Teams sind akademisch
- Aber auch Teams wie ALLES,C4ButS4D
- Preisgelder gehen in den 5-stelligen Raum



Warum gibt es CTFs?

Capture the Flag als Lernmethode

Hacken:

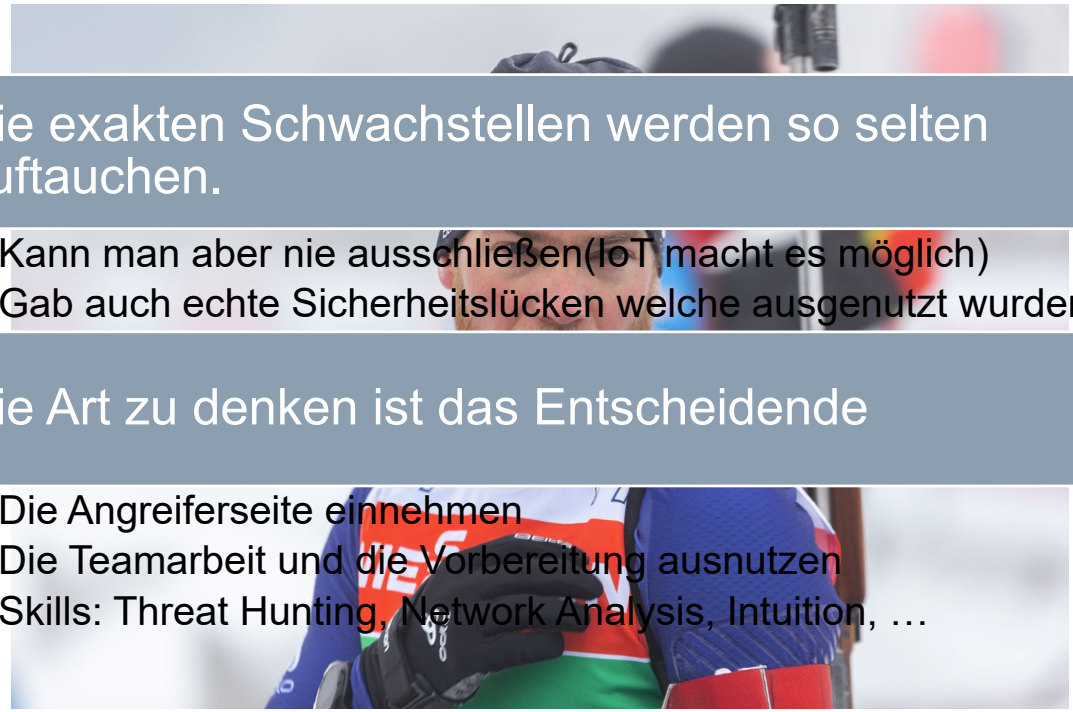
- Für IT-Security Experten ist es wichtig die Angreiferperspektive einzunehmen
- Lernen wie der “Feind” denkt
- Die eigenen Fähigkeiten verbessern
- Es macht Spaß

➔ Aber es ist illegal!

Lösung: In dezidierten Netzwerken gegen/zeitgleich mit anderen an vorbereiteten Schwachstellen hacken.

Klappt das?

Die kritische Nachfrage



Die exakten Schwachstellen werden so selten auftauchen.

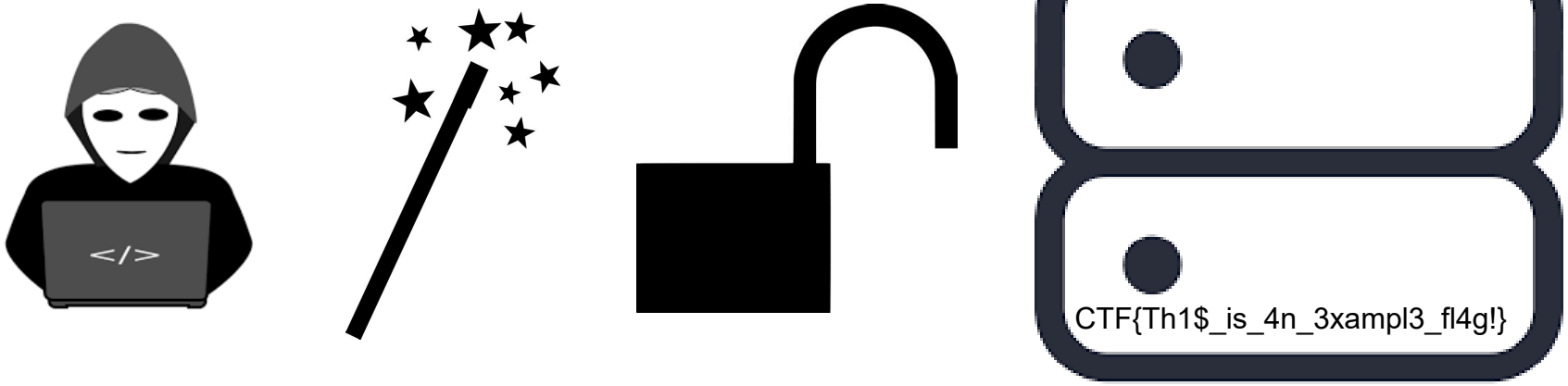
- Kann man aber nie ausschließen(IoT macht es möglich)
- Gab auch echte Sicherheitslücken welche ausgenutzt wurden

Die Art zu denken ist das Entscheidende

- Die Angreiferseite einnehmen
- Die Teamarbeit und die Vorbereitung ausnutzen
- Skills: Threat Hunting, Network Analysis, Intuition, …

Generelles Konstrukt

Generelles Konstrukt



Jeopardy CTF

Der Klassiker

FAU

Nach dem klassischen Jeopardy-Spiel benannt:

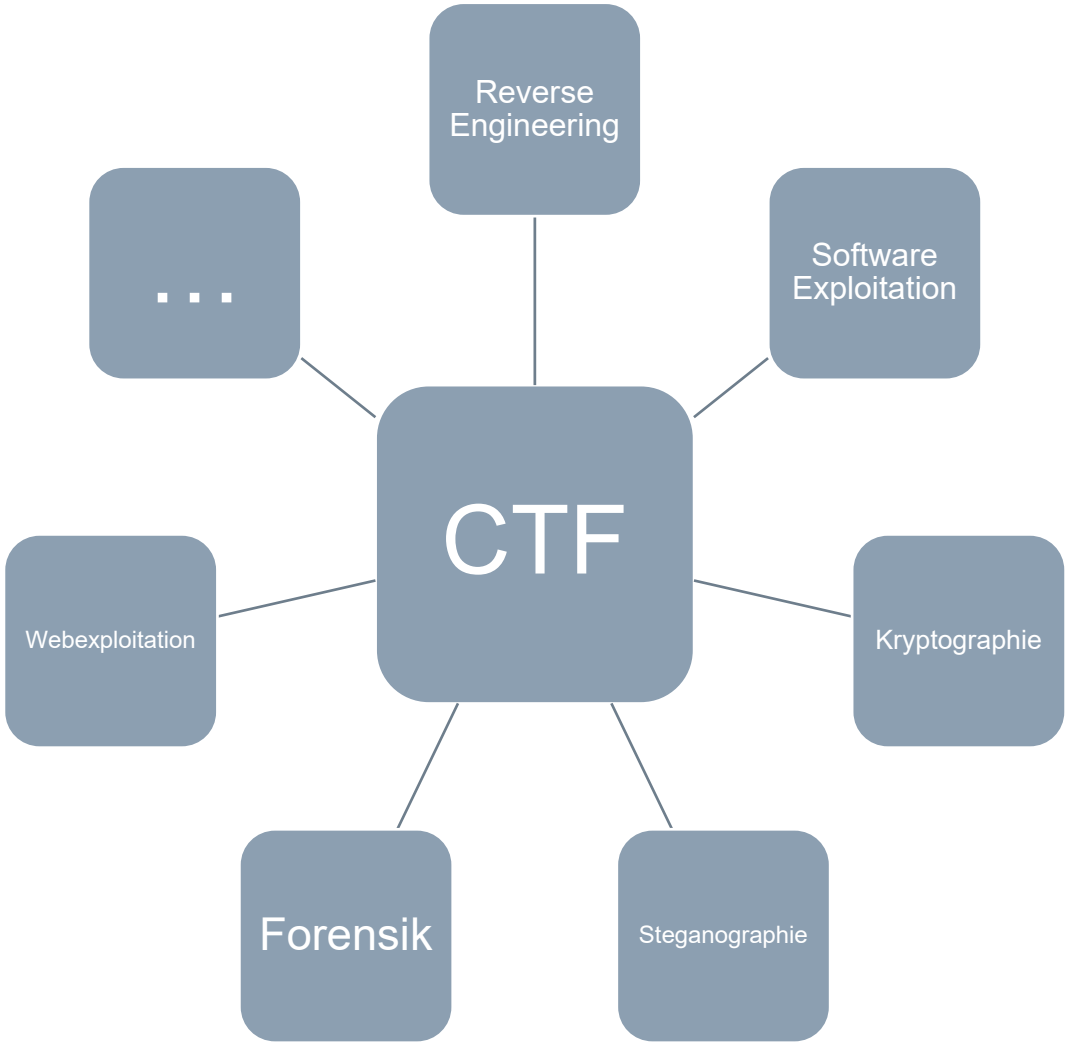
- Funktioniert asynchron
- Meistens über 48h lang
- Es gibt unterschiedlichsten Kategorien
- Teamgrößen: 1-X
- Häufig auch leichtere Aufgaben

Web	Crypto	Forensics	Reverse	Misc
1	165	100	50	50
150	150	150	100	100
204	150	150	150	165
203	200	200	200	150

[1] https://www.cyber.nj.gov/cyber-blog/ctf-competitions-why-you-should-play-how-to-win

Aufgabentypen

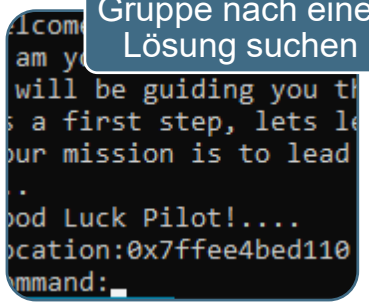
Einschub



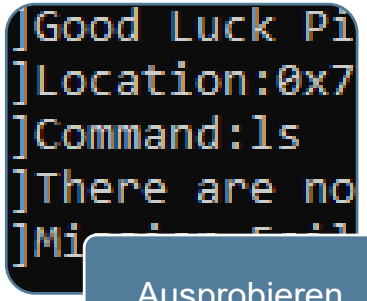
Jeopardy CTF

Der Klassiker

Aufgabe aufrufen und verstehen

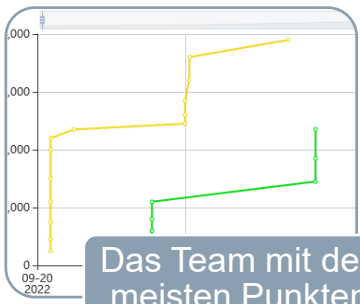


Alleine oder in der Gruppe nach einer Lösung suchen



Ausprobieren

Flagge abholen



Das Team mit den meisten Punkten gewinnt!

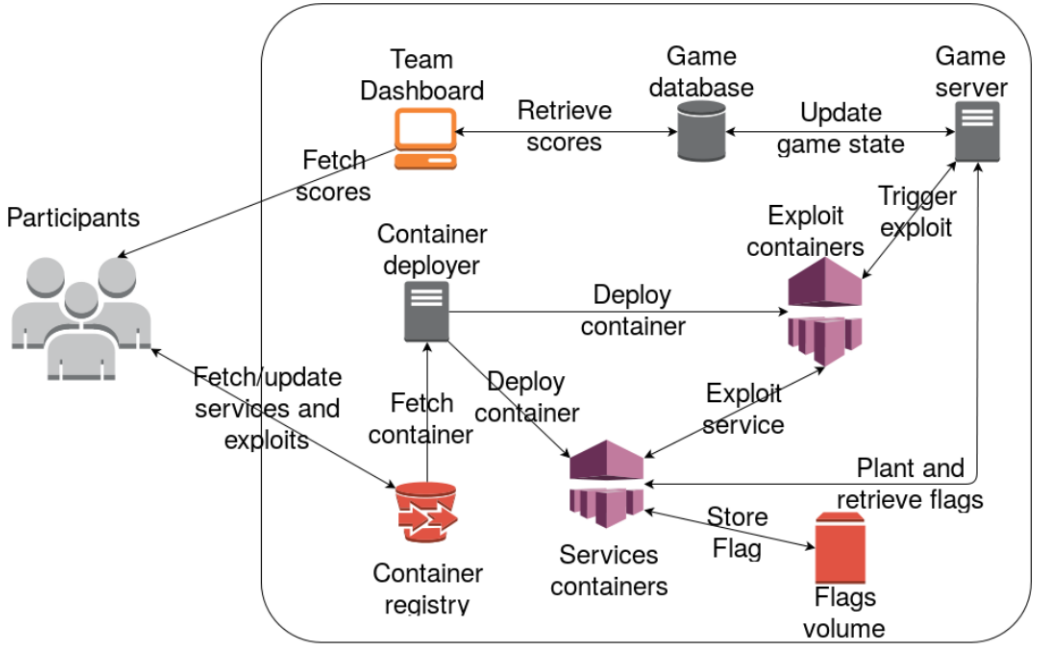
Attack-Defense CTF

Blue- und Red-Teaming

FAU

Team-basierte Wettbewerb:

- Funktioniert synchron
- Meistens um die 8h lang
- Begrenzte Anzahl an Aufgaben
- Teamgrößen: ~4-X
- Komplexeres Setup mit meist schwierigeren Aufgaben
- Fokus kann je nach Wettbewerb schwanken



[2] Raj, A. S., Alangot, B., Prabhu, S., & Achuthan, K. (2016, August). Scalable and Lightweight CTF Infrastructures Using Application Containers. In ASE@ USENIX Security Symposium.

Attack-Defense CTF

Koordination ist gefragt

FAU

Teams bekommen einen Server mit vulnerablen Anwendungen

Eine Stunde Zeit die Anwendungen zu verstehen (Grace Period)

Das Netzwerk wird live-geschaltet

Gleichzeitig:

Nach Schwachstellen suchen	Schwachstellen bei Gegnern ausnutzen	Eigene Schwachstellen fixen	Das Netzwerk überwachen

Team mit den meisten Punkten gewinnt!

Ein Vergleich

Pros and Cons

Jeopardy		Attack/Defense
Aufwand Einfach loslegen, alles andere ergibt sich!	01	**Aufwand** Erfordert Vorbereitung und einen festen Termin.
Lernkurve Gibt häufig anfängerfreundliche CTFs.	02	**Lernkurve** Im Zweifelsfall sehr steil!
Organisation Es gibt bestehende Frameworks, man muss “nur” die Aufgaben bereitstellen.	03	**Organistion** Frameworks müssen up-to-date sein. Man muss aktiv gegen “Cheater” vorgehen.
Teamgefühl Man fühlt sich häufig eher alleine.	04	**Teamgefühl** Man muss sich auf sein Team verlassen, Koordination ist die halbe Miete!

Wo finden CTFs aktuell statt

- Aktuell (leider) eher im akademischen Umfeld
- Es gibt Firmen die eigene CTFs anbieten
- Einige freie Teams
- Online oder vor Ort
- Weltweites Phänomen

IT-Security in (deutschen) Unternehmen

IT-Security und deutsche Unternehmen

Koordination ist immer noch gefragt

- Deutsche Unternehmen sind suboptimal vorbereitet, nur 11 Prozent sind optimal vorbereitet.
- Größte Schwachstelle bleibt die Vorbereitung der Mitarbeiter → Phishing bleibt größtes Problem
- Viele setzen auf interne Teams
- Nur 19 Prozent halten ihr IT-Security Team für kompetent
- Es gibt aber weder genug externe Berater, noch genügend interne IT-Security Experten
- Tatsächliches Monitoring findet selten statt
- Kontinuierliches Erhöhen des Budgets
- Hoffnung liegt bei Queereinsteigern

[3] Cisco Cybersecurity Readiness Index 2023
[4] CyberCompare Whitepaper 2023
[5] State of Security Preparedness 2023

Was können CTFs helfen

Zwei Arten

FAU

Als Werbestrategie	Zur Schulung der eigenen Mitarbeiter
• Ausrichten eigener Wettbewerbe • Sponsoring von Wettbewerben oder Teams	• Teilnehmen an Wettbewerben • Für das Thema begeistern

Wie können hier CTFs helfen

Zwei Arten

FAU

Als Werbestrategie

- Ausrichten eigener Wettbewerbe
- Sponsoring von Wettbewerben oder Teams

Zur Schulung der eigenen Mitarbeiter

- Teilnehmen an Wettbewerben
- Für das Thema begeistern

Was können CTFs helfen

Zwei Arten

FAU

Interner CTF

- Ein CTF wird (vor Ort) in der Firma ausgerichtet
- Mitarbeiter treten in Teams an
- Schafft Awareness
- Schwierigkeit kann angepasst werden
- Vorhandene Tools nutzen
- Es gibt Ressourcen auf die man zugreifen kann

An einem externen CTF teilnehmen

- Ein einem oder mehreren Teams an einem externen Wettbewerb teilnehmen
- Weniger Aufwand
- Für kleinere Firmen/IT-Teams machbarer

Ressourcen

ctftime.org	• Hauptplattform • Alle Teams und Competitions
hackthebox.com	• Upskilling Plattform • Sehr kleinteilige Aufgabenfelder
tryhackme.com	• Unterschiedliche Arten und Basics
picoCTF	• Anfänger freundlicher CTF
GoogleCTF	• Hat einen zusätzlichen Anfänger freundlichen CTF

Fazit

- CTF Wettbewerbe sind ein adäquates Mittel die eigenen Fähigkeiten zu verbessern
- CTF Wettbewerbe bieten ein viele unterschiedliche Aufgaben
- Als Trainingsmethode bereits sehr anerkannt
- Können auch in Firmenumfeld sinnvoll eingesetzt werden
- Trainieren Hard- und Softskills
- Verknüpfungsmöglichkeit mit anderen Teams

Save the Date: 23.10.2023 FAUST CTF

Vielen Dank
für Ihre Aufmerksamkeit!