



SCHNITZELJAGD IM CYBERRAUM - EINFÜHRUNG IN CAPTURE THE FLAG (CTF) FOR TRAINING, FUN, PROFIT?

KNF-KONGRESS 2021

ROLAND WAGNER

ROLAND@DATEVNET.DE



Stopp, nicht nachmachen



Ja, bitte nachmachen

AUFGABEN WÄHREND DES WORKSHOPS

... und auch später

Download über:

<https://1drv.ms/f/s!Ar3PA4MVhZlAdh6PN-njPmD58bw>

<https://is.gd/EdAfL7>



CTF - ABGRENZUNG

The image features a dark blue background with white, stylized circuit board traces in the corners. These traces consist of straight lines and small circles, resembling electronic components or connections. The top-left and bottom-left corners have more complex, branching patterns, while the top-right and bottom-right corners have simpler, more linear traces.

CTF - ABGRENZUNG

live

CTF - ABGRENZUNG

live

Gelände
-spiel

CTF - ABGRENZUNG

live

Gelände
-spiel

Paintball

CTF - ABGRENZUNG

live

Gelände
-spiel

Lasertag

Paintball

CTF - ABGRENZUNG

live

virtuell

Gelände
-spiel

Lasertag

Paintball

CTF - ABGRENZUNG

live

virtuell

Gelände
-spiel

Lasertag

(Ego-)
Shooter

Paintball

CTF - ABGRENZUNG

live

virtuell

Gelände
-spiel

Lasertag

(Ego-)
Shooter

Paintball

Hacker-CTF

The image features a dark blue background with white, stylized circuit board traces in the corners. These traces consist of straight lines, right-angle turns, and small circles representing components or nodes. The patterns are located in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.

CTF - VARIANTEN

CTF - VARIANTEN

- Attack-Defense

CTF - VARIANTEN

- Attack-Defense
- King of the Hill

CTF - VARIANTEN

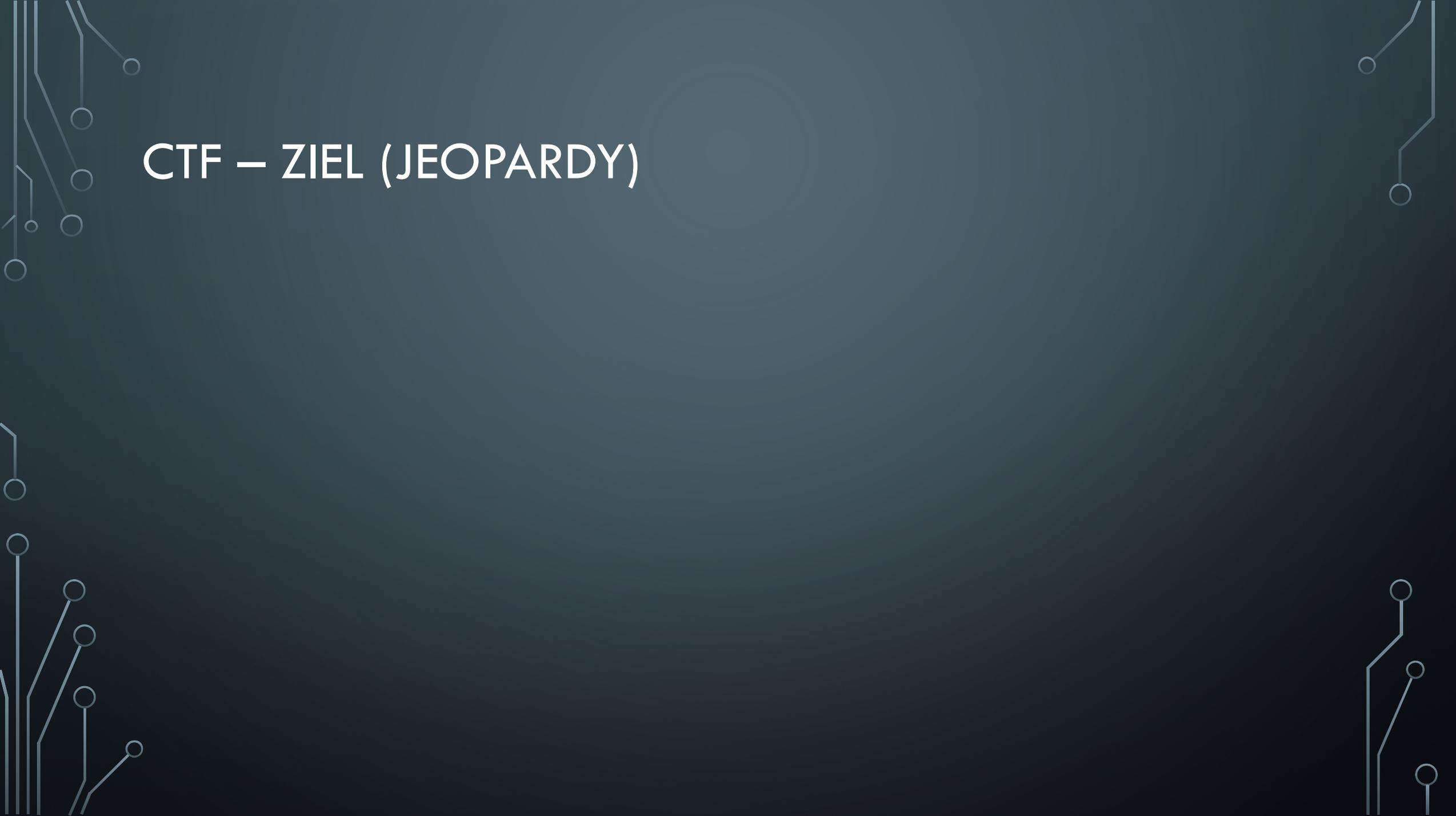
- Attack-Defense
- King of the Hill
- **Jeopardy**

CTF - VARIANTEN

- Attack-Defense
- King of the Hill
- **Jeopardy**
- Story Based

CTF - VARIANTEN

- Attack-Defense
- King of the Hill
- **Jeopardy**
- Story Based
- Scenario Driven

The image features a dark blue background with white, stylized circuit board traces in the corners. These traces consist of straight lines and right-angle turns, ending in small circles that represent components or connection points. The traces are located in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.

CTF – ZIEL (JEOPARDY)

CTF – ZIEL (JEOPARDY)

- Rätsel lösen

CTF – ZIEL (JEOPARDY)

- Rätsel lösen
- Flagge finden

Beispiel: FLAG{dasisteinflag}

CTF – ZIEL (JEOPARDY)

- Rätsel lösen
- Flagge finden

Beispiel: FLAG{dasisteinflag}

- Format der Flagge

CTF – ZIEL (JEOPARDY)

- Rätsel lösen
- Flagge finden

Beispiel: FLAG{dasisteinflag}

- Format der Flagge
- Punkte sammeln

CTF – ZIEL (JEOPARDY)

- Rätsel lösen
- Flagge finden
 - Beispiel: FLAG{dasisteinflag}
- Format der Flagge
- Punkte sammeln
- Hinweise: Achtung Punktabzug!

BEISPIEL 1

1.zip

Download über:

<https://1drv.ms/f/s!Ar3PA4MVhZlAdh6PN-njPmD58bw>

<https://is.gd/EdAfL7>



CTF - KATEGORIEN

CTF - KATEGORIEN

- OSINT

CTF - KATEGORIEN

- OSINT
- Web (online)

CTF - KATEGORIEN

- OSINT
- Web (online)
- Programmierung

CTF - KATEGORIEN

- OSINT
- Web (online)
- Programmierung
- Mobile (online)

CTF - KATEGORIEN

- OSINT
- Web (online)
- Programmierung
- Mobile (online)
- IoT / OT (online)

CTF - KATEGORIEN

- OSINT
- Web (online)
- Programmierung
- Mobile (online)
- IoT / OT (online)
- Exploitation

CTF - KATEGORIEN

- OSINT
- Web (online)
- Programmierung
- Mobile (online)
- IoT / OT (online)
- Exploitation
- Kryptografie

CTF - KATEGORIEN

- OSINT
- Web (online)
- Programmierung
- Mobile (online)
- IoT / OT (online)
- Exploitation
- Kryptografie
- IT-Forensik

CTF - KATEGORIEN

- OSINT
- Web (online)
- Programmierung
- Mobile (online)
- IoT / OT (online)
- Exploitation
- Kryptografie
- IT-Forensik
- Reverse Engineering

CTF - KATEGORIEN

- OSINT
- Web (online)
- Programmierung
- Mobile (online)
- IoT / OT (online)
- Exploitation
- Kryptografie
- IT-Forensik
- Reverse Engineering

Kombinationen

BEISPIEL 5

5.zip

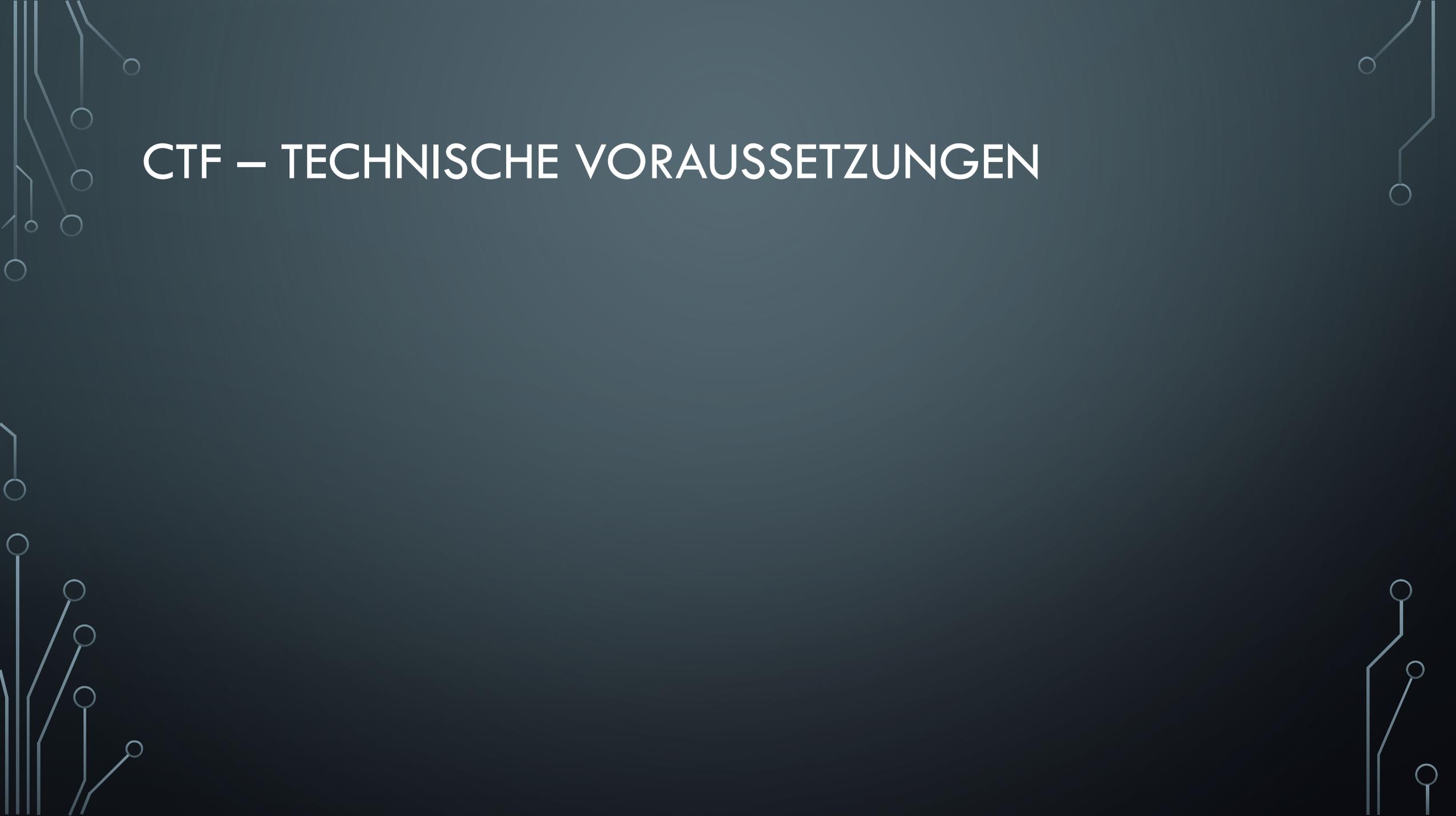
Download über:

<https://1drv.ms/f/s!Ar3PA4MVhZlAdh6PN-njPmD58bw>

<https://is.gd/EdAfL7>



CTF – TECHNISCHE VORAUSSETZUNGEN

The image features a dark blue background with white decorative elements resembling circuit board traces and nodes. These elements are located in the four corners of the frame, creating a technical and digital aesthetic. The central text is rendered in a clean, white, sans-serif font.

CTF – TECHNISCHE VORAUSSETZUNGEN

- Linux

CTF – TECHNISCHE VORAUSSETZUNGEN

- Linux
- Windows / Mac

CTF – TECHNISCHE VORAUSSETZUNGEN

- Linux
- Windows / Mac
- Infrastruktur

CTF – TECHNISCHE VORAUSSETZUNGEN

- Linux
- Windows / Mac
- Infrastruktur
- Netzwerk

CTF – TECHNISCHE VORAUSSETZUNGEN

- Linux
- Windows / Mac
- Infrastruktur
- Netzwerk
- Software / Scripting

CTF – TECHNISCHE VORAUSSETZUNGEN

- Linux
- Windows / Mac
- Infrastruktur
- Netzwerk
- Software / Scripting
- Web

BEISPIEL 7B

enc01.zip

Download über:

<https://1drv.ms/f/s!Ar3PA4MVhZlAdh6PN-njPmD58bw>

<https://is.gd/EdAfL7>



CTF - WEAPONISATION

CTF - WEAPONISATION

Voraussetzung:

CTF - WEAPONISATION

Voraussetzung:

- Englische Sprache

CTF - WEAPONISATION

Voraussetzung:

- Englische Sprache

Minimum:

- unzip
- netcat
- F12 (Web-entwickler)
- Hexeditor
- Ver- /Entschlüsselung (CyberChef)
- Bildbearbeitung (GIMP)

CTF - WEAPONISATION

Voraussetzung:

- Englische Sprache

(später bei Kryptographie:
Häufigkeitsanalyse)

Minimum:

- unzip
- netcat
- F12 (Web-entwickler)
- Hexeditor
- Ver- /Entschlüsselung (CyberChef)
- Bildbearbeitung (GIMP)

BEISPIEL 7C

enc02.zip

Download über:

<https://1drv.ms/f/s!Ar3PA4MVhZlAdh6PN-njPmD58bw>

<https://is.gd/EdAfL7>



CTF – NICHTTECHNISCHE VORAUSSETZUNGEN

CTF – NICHTTECHNISCHE VORAUSSETZUNGEN

- Kreativität

CTF – NICHTTECHNISCHE VORAUSSETZUNGEN

- Kreativität
- Detailverliebtheit

CTF – NICHTTECHNISCHE VORAUSSETZUNGEN

- Kreativität
- Detailverliebtheit
- Beharrlichkeit

CTF – NICHTTECHNISCHE VORAUSSETZUNGEN

- Kreativität
- Detailverliebtheit
- Beharrlichkeit
- Resilienz

CTF – NICHTTECHNISCHE VORAUSSETZUNGEN

- Kreativität
- Detailverliebtheit
- Beharrlichkeit
- Resilienz
- (Teamfähigkeit)

CTF – NICHTTECHNISCHE VORAUSSETZUNGEN

- Kreativität
- Detailverliebtheit
- Beharrlichkeit
- Resilienz
- (Teamfähigkeit)
- Übung, Übung, Übung, ...

BEISPIEL 6

6.zip

Download über:

<https://1drv.ms/f/s!Ar3PA4MVhZlAdh6PN-njPmD58bw>

<https://is.gd/EdAfL7>



CTF – REGELN (JEOPARDY)

CTF – REGELN (JEOPARDY)

- Kein Angriff auf CTF-Server

CTF – REGELN (JEOPARDY)

- Kein Angriff auf CTF-Server
- Kein (D)DoS

CTF – REGELN (JEOPARDY)

- Kein Angriff auf CTF-Server
- Kein (D)DoS
- Kein Angriff auf andere Spieler

CTF – REGELN (JEOPARDY)

- Kein Angriff auf CTF-Server
- Kein (D)DoS
- Kein Angriff auf andere Spieler
- Alle Aufgaben verfügbar vs. Freischaltung der Aufgaben

CTF – REGELN (JEOPARDY)

- Kein Angriff auf CTF-Server
- Kein (D)DoS
- Kein Angriff auf andere Spieler
- Alle Aufgaben verfügbar vs. Freischaltung der Aufgaben
- Zeitlimit

BEISPIEL 3

be01.zip

Download über:

<https://1drv.ms/f/s!Ar3PA4MVhZlAdh6PN-njPmD58bw>

<https://is.gd/EdAfL7>



The image features a dark blue background with white, stylized circuit board traces in the corners. These traces consist of straight lines and small circles, resembling electronic components or connections. The traces are located in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.

CTF – FUN? TRAINING? PROFIT?

CTF – FUN? TRAINING? PROFIT?

- Profit
 - Dienstleistung muss bezahlt werden
 - Teilnahme teilweise kostenlos
 - „Gewinn“ – nur geringe Preise

CTF – FUN? TRAINING? PROFIT?

- Profit
 - Dienstleistung muss bezahlt werden
 - Teilnahme teilweise kostenlos
 - „Gewinn“ – nur geringe Preise
- Training
 - Ausbildung im Bereich Cyber Security

CTF – FUN? TRAINING? PROFIT?

- Profit
 - Dienstleistung muss bezahlt werden
 - Teilnahme teilweise kostenlos
 - „Gewinn“ – nur geringe Preise
- Training
 - Ausbildung im Bereich Cyber Security
- Fun

CTF – FUN? TRAINING? PROFIT?

- Profit
 - Dienstleistung muss bezahlt werden
 - Teilnahme teilweise kostenlos
 - „Gewinn“ – nur geringe Preise
- Training
 - Ausbildung im Bereich Cyber Security
- Fun

<https://ctftime.org/calendar/>

BEISPIEL 2

2.zip

Download über:

<https://1drv.ms/f/s!Ar3PA4MVhZlAdh6PN-njPmD58bw>

<https://is.gd/EdAfL7>



The image features a dark blue background with white, stylized circuit board traces in the corners. These traces consist of straight lines and small circles, resembling electronic components or connections. The traces are located in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.

FÄHIGKEITEN („... THIS IS THE END MY FRIEND ...“)

FÄHIGKEITEN („... THIS IS THE END MY FRIEND ...“)

- Kenntnisse aus verschiedenen Bereichen
 - Dateiaufbau (Magic Bytes aber auch visuelle Erkennung, z.B. Base64)
 - Browser – Webserver: Aufbau, Protokolle, JSON, ...
 - Debugger
 - Verschiedene Bereiche der Cyber Security (Attack + Defense + Forensik + Kryptologie + ..)
 - Scripting! (Bash, Python, Perl)
 - ...

FÄHIGKEITEN („... THIS IS THE END MY FRIEND ...“)

- Kenntnisse aus verschiedenen Bereichen
 - Dateiaufbau (Magic Bytes aber auch visuelle Erkennung, z.B. Base64)
 - Browser – Webserver: Aufbau, Protokolle, JSON, ...
 - Debugger
 - Verschiedene Bereiche der Cyber Security (Attack + Defense + Forensik + Kryptologie + ..)
 - Scripting! (Bash, Python, Perl)
 - ...
- „Wo steht der Feind?“ -> Problem erkennen

The image features a dark blue background with white, stylized circuit board traces in the corners. These traces consist of straight lines and right-angle turns, ending in small circles that represent solder pads or vias. The traces are located in the top-left, top-right, bottom-left, and bottom-right corners, framing the central text.

DAS WICHTIGSTE ...

DAS WICHTIGSTE ...

Have Fun!!!





„... THIS IS **NOT** THE END MY FRIEND ...“

Weitere CTFs im Anschluss ...

... Fragen ?



„... THIS IS **NOT** THE END MY FRIEND ...“

Weitere CTFs im Anschluss ...

... Fragen ?

<https://ctftime.org/calendar/>

BEISPIEL 3B

3b.zip

Download über:

<https://1drv.ms/f/s!Ar3PA4MVhZlAdh6PN-njPmD58bw>

<https://is.gd/EdAfL7>



BEISPIEL 8

enc04.zip

Download über:

<https://1drv.ms/f/s!Ar3PA4MVhZlAdh6PN-njPmD58bw>

<https://is.gd/EdAfL7>



BEISPIEL 4

4.zip

Download über:

<https://1drv.ms/f/s!Ar3PA4MVhZlAdh6PN-njPmD58bw>

<https://is.gd/EdAfL7>



BEISPIEL 7D

enc03.zip

Download über:

<https://1drv.ms/f/s!Ar3PA4MVhZlAdh6PN-njPmD58bw>

<https://is.gd/EdAfL7>



BEISPIEL 9

9.zip

Download über:

<https://1drv.ms/f/s!Ar3PA4MVhZlAdh6PN-njPmD58bw>

<https://is.gd/EdAfL7>



BEISPIEL 10: MEDIUM : BM01.ZIP

bm01.zip

Download über:

<https://1drv.ms/f/s!Ar3PA4MVhZlAdh6PN-njPmD58bw>

<https://is.gd/EdAfL7>



BEISPIEL 11: HARD !

fh01.zip

Download über:

<https://1drv.ms/f/s!Ar3PA4MVhZlAdh6PN-njPmD58bw>

<https://is.gd/EdAfL7>

