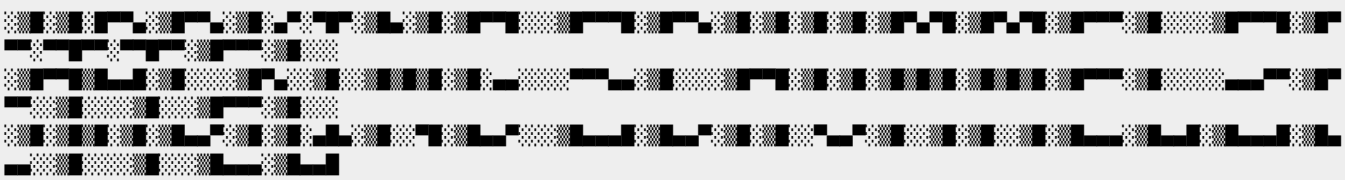
file, hetti, hacking, schummelzettel

Hettis Hacking Schummelzettel



Matrix: @Hetti:matrix.org
Mastodon: @Hetti@chaos.social

```
#########################
#    ACHTUNG - WICHTIG!
#########################
```

- Greift ausschließlich Systeme an für die ihr eine Berechtigung habt (schriftlich!) bzw. für Lernzwecke freigegeben sind (Lernplattformen wie z.B. THM/HTB)
- Angriff auf fremde Systeme ist **illegal** und kann im schlimmsten Fall zu Gefängnisstrafen führen.

```
############################
#    Seite für Challenge Boxen
############################
```

- TryHackMe (THM): https://tryhackme.com (meine Empfehlung um in die IT Security Materie reinzukommen, man wird bei den Basics an der Hand genommen beim Lernen und Üben!)
- HackTheBox (HTB): https://www.hackthebox.com

```
#########################
#   TryHackMe OpenVPN Guide
#########################
```

IP rausfinden nach OpenVPN Verbindung:

Nach folgender Zeile im Verbindungslog suchen welche net_addr_v4_add beinhaltet: `2022-12-29 06:17:28 net_addr_v4_add: 13.37.40.4/16 dev tun0`

Die IP Adresse vor dem /16 ist eure zugewiesene IP Adresse im Netzwerk von THM. Also in dem Fall –> 13.37.40.4

Alternativ: Wieder auf die Access Seite gehen nachdem ihr Verbunden seid (https://tryhackme.com/access), dort steht beim Feld “Internal Virtual IP Address” eure zugewiesene interne IP Adresse.

Auch möglich: Ihr könnt den TryHackme OpenVPN Raum nutzen, um die IP rauszufinden: https://tryhackme.com/room/openvpn

```
#########################
#   Callenge Box Empfehlung
#########################
```

- https://tryhackme.com/room/basicpentestingjt → Empfehlung für begleites Hacken für Anfänger*innen

```
#########################
#    Webseiten Empfehlungen
```

```
##########################
```

- CyberChef: https://gchq.github.io/CyberChef/
- Hacktricks: https://book.hacktricks.xyz/welcome/readme
- OWASP Cheat Sheet Series: https://cheatsheetseries.owasp.org/index.html
- GTFO Bins: https://gtfobins.github.io/

```
######################
#    Tool Empfehlungen
######################
```

- Burp Suite Community Edition: https://portswigger.net/burp/communitydownload
    - Üblicherweise über euren Packetmanager auf Linux installierbar
    - Ist in Kali Linux auch dabei.
- man - Man Pages - Sammlung von Hilfs und Dokumentationsseiten; Aufruf: man <programmname>
    - Beispiel: man nmap
- nmap - Port Scanning Tool mit vielen Funktionalitäten
- ffuf (in Kali integriert) - Fuzzing/Bruteforcing Tool: https://github.com/ffuf/ffuf
- SecLists - nützliche Listen: https://github.com/danielmiessler/SecLists
- Scripte für automatisierte Reconnaissance am System (Hacktricks Mensch): https://github.com/carlospolop/PEASS-ng

```
################################
#    Methoden Empfehlungen für Linux
################################
```

Übliche Dinge die man auch schnell manuell prüfen kann (Linux):

- Dateien im Home Verzeichnis
- Bash History
- Berechtigungen im Home Verzeichnis
- Cronjobs inkl. der Berechtigungen für die Dateien
- Binaries mit SUID Bit gesetzt (Siehe GTFO Bins)

SUID Binaries suchen mittels find: `find <VERZEICHNIS> -perm -4000`

Beispiel:

```
find /bin -perm -4000
```

Siehe auch: https://linux-audit.com/finding-setuid-binaries-on-linux-and-bsd/