

Wahlpflicht Kurs

- Microcontrolling
- IT-Sicherheit mit Kali Linux

Microcontrolling

Material:

- 1x Arduino Nano
- 1x ESP8266
- 3x LED (Aktor)
- 1x BME680 (Sensor)
- 1x LCD 1602 Modul(Aktor)
- 2x Widerstände (220Ω & 470Ω)

Grobes Konzept:

Messung und Monitoring der Luftqualität und anderen Umgebungsdaten. Ausgabe der Messung wird auf einem LCD-Display ausgegeben. Sobald ein bestimmter Grenzwert über- oder unterschritten werden, leuchten eine oder mehr LEDs auf.

Zeitplan:

1. Doppelstunde: Brainstorming was wir machen wollen.

- Alarmanlage mit Bewegungssensor
- MQTT-Luftqualitätsmesser
- MQTT-Lichtsteuerung

2. Doppelstunde: Alle benötigten Materialien aufgezeichnet und rausgesucht. Begonnen die Dokumentation zu verfassen. Installieren der Arduino IDE.

Verbindung zwischen den beiden Arduino aufgebaut:

Serielle Kommunikation (UART):

1. **Hardware:** Die jeweiligen RX-Pins mit den TX-Pins des anderen Arduino verbunden.
2. **Gemeinsame Masse (GND):** Verbinde die GND-Pins beider Arduinos.
3. **Programmierung:**

- Verwenden der `Serial`-Bibliothek in der Arduino-IDE.
- Beispielcode (Sender):

```
void setup() {  
  Serial.begin(9600);  
}
```

```

void loop() {
  Serial.println("Hallo von Arduino 1");
  delay(1000);
}

```

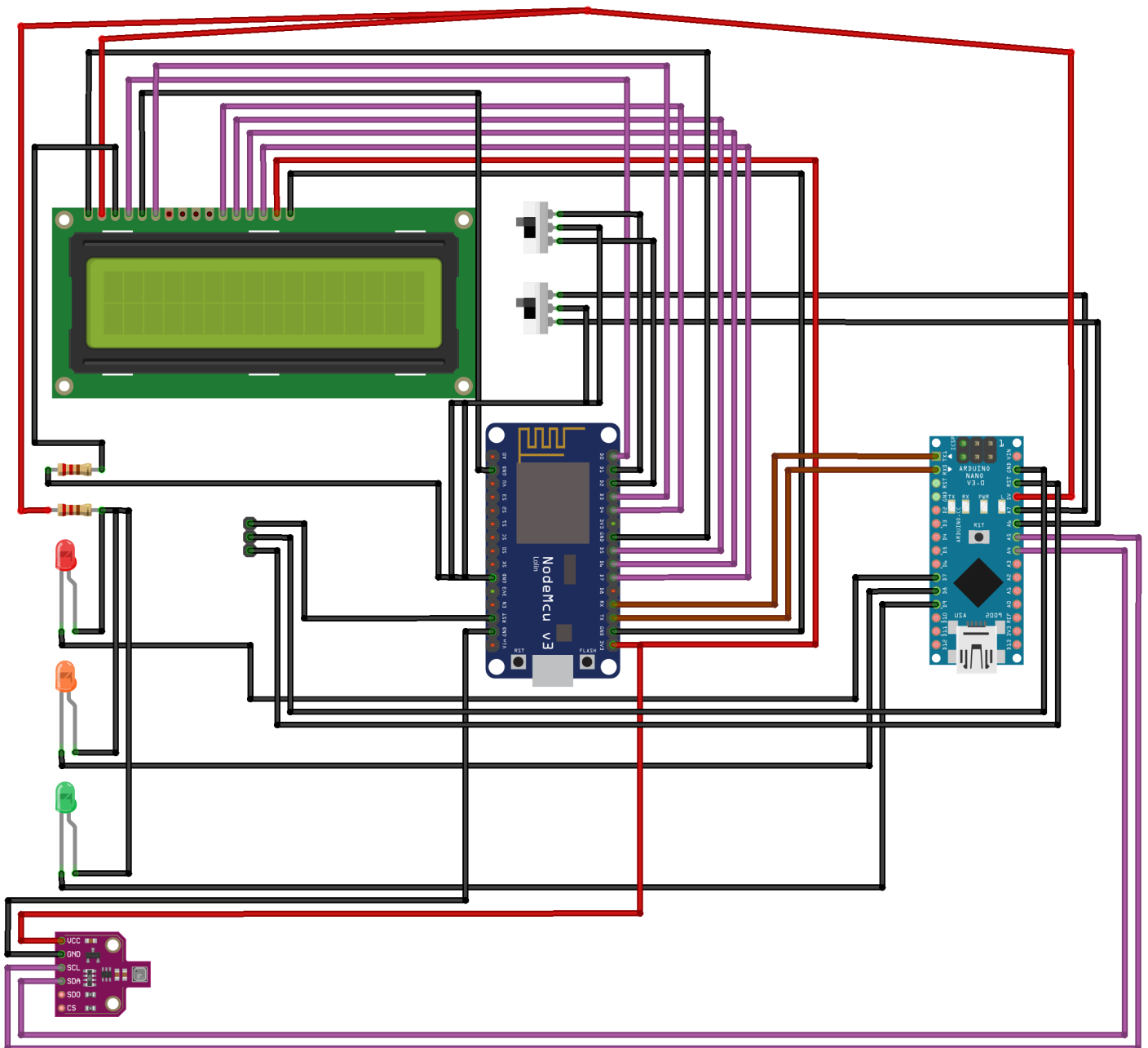
- Beispielcode (Empfänger):

```

void setup() {
  Serial.begin(9600);
}

void loop() {
  if (Serial.available() > 0) {
    String message = Serial.readString();
    Serial.println("Empfangene Nachricht: " + message);
  }
}

```



Code für den ESP8266:

```
#include <ArduinoMqttClient.h>
#include <Adafruit_NeoPixel.h>

#include <ESP8266WiFi.h>
#include <Wire.h>
#include <LiquidCrystal.h>

#define wifi_ssid "Bunker"
#define wifi_password "DasIstNichtDasPasswort"

WiFiClient espClient;
MqttClient mqttClient(espClient);

const char broker[] = "nioy.de";
int port = 1883;
const char willTopic[] = "arduino/error";

#define MQTT_Topic_Status "JJ-Test/Wetterstation/ESP8266_Status"
#define MQTT_Topic_LCD "JJ-Lab/Wetterstation/LCD"

const long interval = 2000;
unsigned long previousMillis = 0;

bool debug = false;

unsigned long delayTime = 20;
unsigned long lastHeapCheck = 0;
const unsigned long heapCheckInterval = 60000;

unsigned long lastMessageTime = 0;
const unsigned long timeout = 10000;

int cnt=129600;

const int rs = 16, en = 0, d4 = 2, d5 = 14, d6 = 12, d7 = 13;
LiquidCrystal lcd(rs, en, d4, d5, d6, d7);

void setup() {
  lcd.begin(16, 2);
  lcd.print("Starte nun...");
  Serial.begin(9600);
  pinMode(LED_BUILTIN, OUTPUT);
  digitalWrite(LED_BUILTIN, HIGH);
  delay(60);

  Serial.println(" ");
  Serial.println("Moin Moin ....");
  Serial.println("Der Arduino Startet nun //JJ");

  lcd.setCursor(0, 0);
  lcd.print("Attempting to");
```

```

lcd.setCursor(0, 1);
lcd.print("connect to WPA");

Serial.print("Attempting to connect to WPA SSID: ");
Serial.println(wifi_ssid);
while (WiFi.begin(wifi_ssid, wifi_password) != WL_CONNECTED) {
  Serial.print(".");
  delay(5000);
}

digitalWrite(LED_BUILTIN, LOW);

Serial.print("Ich habe die IP Adresse : ");
Serial.print(WiFi.localIP());
lcd.begin(0, 2);
lcd.print(WiFi.localIP());
delay(60);

Serial.println("You're connected to the network");
Serial.println();
/*
String willPayload = "oh no!";
bool willRetain = true;
int willQos = 1;

mqttClient.beginWill(willTopic, willPayload.length(), willRetain, willQos);
mqttClient.print(willPayload);
mqttClient.endWill();
*/

Serial.print("Attempting to connect to the MQTT broker: ");
Serial.println(broker);

if (!mqttClient.connect(broker, port)) {
  Serial.print("MQTT connection failed! Error code = ");
  Serial.println(mqttClient.connectError());

  while (1);
}

Serial.println("You're connected to the MQTT broker!");
Serial.println();

mqttClient.onMessage(onMqttMessage);

Serial.print("Subscribing to topic: ");
Serial.println(MQTT_Topic_LCD);

int subscribeQos = 1;
mqttClient.subscribe(MQTT_Topic_LCD, subscribeQos);

// topics can be unsubscribed using:
// mqttClient.unsubscribe(MQTT_Topic_LED);

Serial.print("Waiting for messages on topic: ");

```

```

Serial.println(MQTT_Topic_LCD);
Serial.println();

mqttClient.beginMessage(MQTT_Topic_Status);
mqttClient.print("Ready");
mqttClient.endMessage();

/*
if ( hello_start )
{
}
*/
ESP.wdtEnable(WDTO_8S);
}

void loop() {
  Serial.println(cnt);
  if(cnt==20){
    mqttClient.beginMessage(MQTT_Topic_Status);
    mqttClient.print("Reset ESP8266 equal");
    mqttClient.endMessage();
    delay(120);
  }
  if(cnt==0){
    Serial.println("Reset..");
    mqttClient.beginMessage(MQTT_Topic_Status);
    mqttClient.print("Reset ESP8266 now....");
    mqttClient.endMessage();
    delay(120);
    ESP.restart();
  }
  cnt--;
  delay(50);

  ESP.wdtFeed();
  mqttClient.poll();

  unsigned long currentMillis = millis();

  if (currentMillis - lastHeapCheck >= heapCheckInterval) {
    lastHeapCheck = currentMillis;
    Serial.print("Free Heap: ");
    Serial.println(ESP.getFreeHeap());

    mqttClient.beginMessage(MQTT_Topic_Status);
    mqttClient.print(ESP.getFreeHeap());
    mqttClient.endMessage();
  }

  if (currentMillis - previousMillis >= interval) {
    previousMillis = currentMillis;

    bool retained = false;
    int qos = 1;
    bool dup = false;

```

```

    mqttClient.beginMessage(MQTT_Topic_Status);
    mqttClient.print("Online");
    mqttClient.endMessage();
}
mqttClient.poll();

if (currentMillis - previousMillis >= interval) {
    previousMillis = currentMillis;

    bool retained = false;
    int qos = 1;
    bool dup = false;

    mqttClient.beginMessage(MQTT_Topic_Status);
    mqttClient.print("Online");
    mqttClient.endMessage();
}
mqttClient.poll();
}

void onMqttMessage(int messageSize) {
    if (debug) {
        Serial.print("Received a message with topic ");
        Serial.print(mqttClient.messageTopic());
        Serial.print(", duplicate = ");
        Serial.print(mqttClient.messageDup() ? "true" : "false");
        Serial.print(", QoS = ");
        Serial.print(mqttClient.messageQoS());
        Serial.print(", retained = ");
        Serial.print(mqttClient.messageRetain() ? "true" : "false");
        Serial.print(", length ");
        Serial.print(messageSize);
        Serial.println(" bytes:");
    }

    if (strcmp(mqttClient.messageTopic().c_str(), MQTT_Topic_LCD) == 0)
    {
        lastMessageTime = millis();
        Serial.println("Neue Nachricht empfangen:");
        Serial.println("Topic: " + mqttClient.messageTopic());
        Serial.print("Payload: ");

        // Konvertiere das Payload-Array in einen String
        String payloadString;
        for (int i = 0; i < messageSize; i++) {
            payloadString += (char)mqttClient.read();
        }
        Serial.println(payloadString);

        int maxLineLength = 16;
        String line1 = payloadString.substring(0, maxLineLength);
        String line2 = payloadString.length() > maxLineLength ? payloadString.substring(maxLineLength) : "";
        lcd.setCursor(0, 0);
        lcd.print(line1);

        lcd.setCursor(0, 1);

```

```
lcd.print(line2);  
}  
}
```


IT-Sicherheit mit Kali Linux

1. Gesetzliche Rahmenbedingungen

Nicht autorisiertes Hacking ist strafbar!

Auch wenn die exakten Formulierungen variieren, ist Hacking ohne Erlaubnis in den meisten Ländern strafbar. In Deutschland gilt der (umgangssprachlich) sogenannte *Hackerparagraph*, § 202c des deutschen Strafgesetzbuches:

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten

Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. (2) §149 Abs. 2 und 3 gilt entsprechend.

Dabei behandeln die § 202a oder § 202b weitere Aspekte der IT-Sicherheit, nämlich das Ausspähens und Abfangen von Daten. In § 149 geht es um die Fälschung von Geld und Wertzeichen. Wie Sie in der Wikipedia nachlesen können, war und ist § 202c keineswegs unumstritten, was an seiner Gültigkeit aber nichts ändert:

https://de.wikipedia.org/wiki/Vorbereiten_des_Ausp%C3%A4hens_und_Abfangens_von_Daten

Ein simpler Port-Scan (nmap) kann gemäß § 202c also bereits als Vorbereitung einer Straftat gewertet werden. Das scheint auf den ersten Blick absurd zu sein: Derartige Scans sind allgegenwärtig, und es gibt keine vernünftige Handhabe dagegen. Wenn das Sicherheitssystem bzw. die Firewall Ihrer Firma einen derartigen Scan feststellt und Sie die zugrundeliegende IP-Adresse beispielsweise in die Ukraine zurückverfolgen können - was wollen Sie als Sicherheitsverantwortlicher der Firma dann tun?

Natürlich können Sie versuchen herauszufinden, wem die IP-Adresse gehört, von welchem Internetprovider der Scan ursprünglich ausging. Selbst wenn das gelingt, kann es gut sein, dass Sie letztlich nur auf Rechner stoßen, die selbst kompromittiert sind und vom Angreifer aus einem ganz anderen Ort ferngesteuert werden. Also, kurzgefasst: Auch wenn Sie wissen, dass andere Hacker aus dem Ausland ununterbrochen Port-Scans durchführen, dürfen Sie selbst dennoch keinen Port-Scan auf einen fremdem Rechner starten.

Obwohl das Gesetz nicht explizit ausspricht und nicht zwischen White und Black Hats differenziert, wird der "gutwillige" Umgang mit Hacking-Tools, z. B. im Rahmen eines Pen-Tests, in der Regel

akzeptiert. Es ist Ihnen sicher dennoch klar, dass der Einsatz von Hacking-Programme außerhalb von Testsystemen unbedingt einer schriftlichen Erlaubnis bedarf!

Bedenken Sie auch, dass Hacking oft nationale Grenzen überschreitet: Auch wenn der Firmensitz in Deutschland ist, kann der eine oder andere Server durchaus in Irland oder in den USA stehen. Das macht die juristische Bewertung noch komplizierter.

Aufgabe:

1. Erläutern Sie folgende Arten von Hackers:

White Hats - , Gray Hats - und Black Hats - Hackers.

2. Welcher Art von Hacker könnte die Hackerin aus folgendem Beispiel (siehe Artikel) zugewiesen werden?

Link zum Artikel:

<https://www.ccc.de/en/updates/2021/ccc-meldet-keine-sicherheitslücken-mehr-an-cdu>

3. Beschreiben Sie die Situationen in denen Sie in einem Netzwerk Hacking-Tools verwenden können, ohne sich strafbar zu machen.

Quellen:

Hacking und Security, Michael Kofler et al. (Rheinwerk Computing)

1.
 - White Hats sind ethische Hacker, die ihre Fähigkeiten dazu nutzen, um Sicherheitslücken im System zu finden und zu beheben.
 - Gray Hats sind zwischen den White Hats und den Black Hats, dadurch sind die Handlungen sowohl ethisch als auch fragwürdig. Sie finden und legen Sicherheitslücken offen, ohne eine Erlaubnis dafür zu haben.
 - Black Hats sind böswillige Hacker, die ihre Fähigkeiten nutzen, um in Systeme einzudringen, Schaden anrichten oder persönliche Vorteile zu erlangen
2.

Der Artikel beschreibt eine White Hackerin
3.
 - Penetrationstest: Unternehmen beauftragen oft Sicherheitsfachleute, Penetrationstests durchzuführen, um Schwachstellen in ihren Netzwerken zu identifizieren.
 - Forensische Untersuchungen: Im Falle eines Sicherheitsvorfalls oder einer vermuteten Verletzung können forensische Ermittler Hacking-Tools verwenden, um die Ursache des

2. IT-Kurs: Übersicht und Ziele



Der Wahlpflichtkurs **IT-Sicherheit** fokussiert sich auf folgende **Inhalte**:

- Kennenlernen unterschiedlicher "Hacking-Tools" auf Kali Linux
- Konkretisieren des Sicherheit-Themas "Passwörter"

Ziel des Kurses ist:

- Security Training zu machen: sei es als Vorbereitung für Pentesting oder um zu verstehen welchen Gefahren die IT-Systeme und IT-Netzwerke ausgesetzt werden.

Lernumgebung:

- Kali Linux in VirtualBox
- Metasploitable 2 in VirtualBox

Kali Linux

- Bei Kali Linux handelt es sich um eine Linux-Distribution, die auf Sicherheits- und Penetrationstests von IT-Systemen spezialisiert ist.
- Kali Linux beinhaltet bereits eine große Menge an Sicherheits- und Hacker-tools.

Metasploitable 2

Viele von Ihnen haben wahrscheinlich vom Hacking-Tool Metasploitable gehört. Hier der Unterschied zwischen Metasploit und Metasploitable:

- Metasploit ist ein Framework, das sich auf Kali Linux befindet. Es beinhaltet eine Sammlung an Exploits, mit der sich die Sicherheit von Computersystemen testen lässt. Metasploit lässt sich auch missbräuchlich als Tool für Hacker verwenden.
 - Metasploitable ist ein verwundbares System, das als Ziel für Angriffe und Sicherheitstests verwendet werden kann.
-

3. Kali Linux

Kali Linux ist eine Linux-Distribution, die eine beinahe endlose Sammlung von Hacking-Werkzeuge in sich vereint. Natürlich können Sie die meisten Tools auch in anderen Linux-Distributionen installieren. Von einigen Hacking-Werkzeugen gibt es sogar Windows-Versionen. Aber Kali Linux hat den Vorteil, dass die Distribution viele wichtige Kommandos zum Penetration-Testing und für verwandte Aufgaben über ein zentrales Menü komfortabel zugänglich macht. Es entfällt der Zeitaufwand, die Kommandos zu suchen, zu installieren bzw. ggf. selbst zu kompilieren.

3.1. Virtualisierung-Kurze Theorie

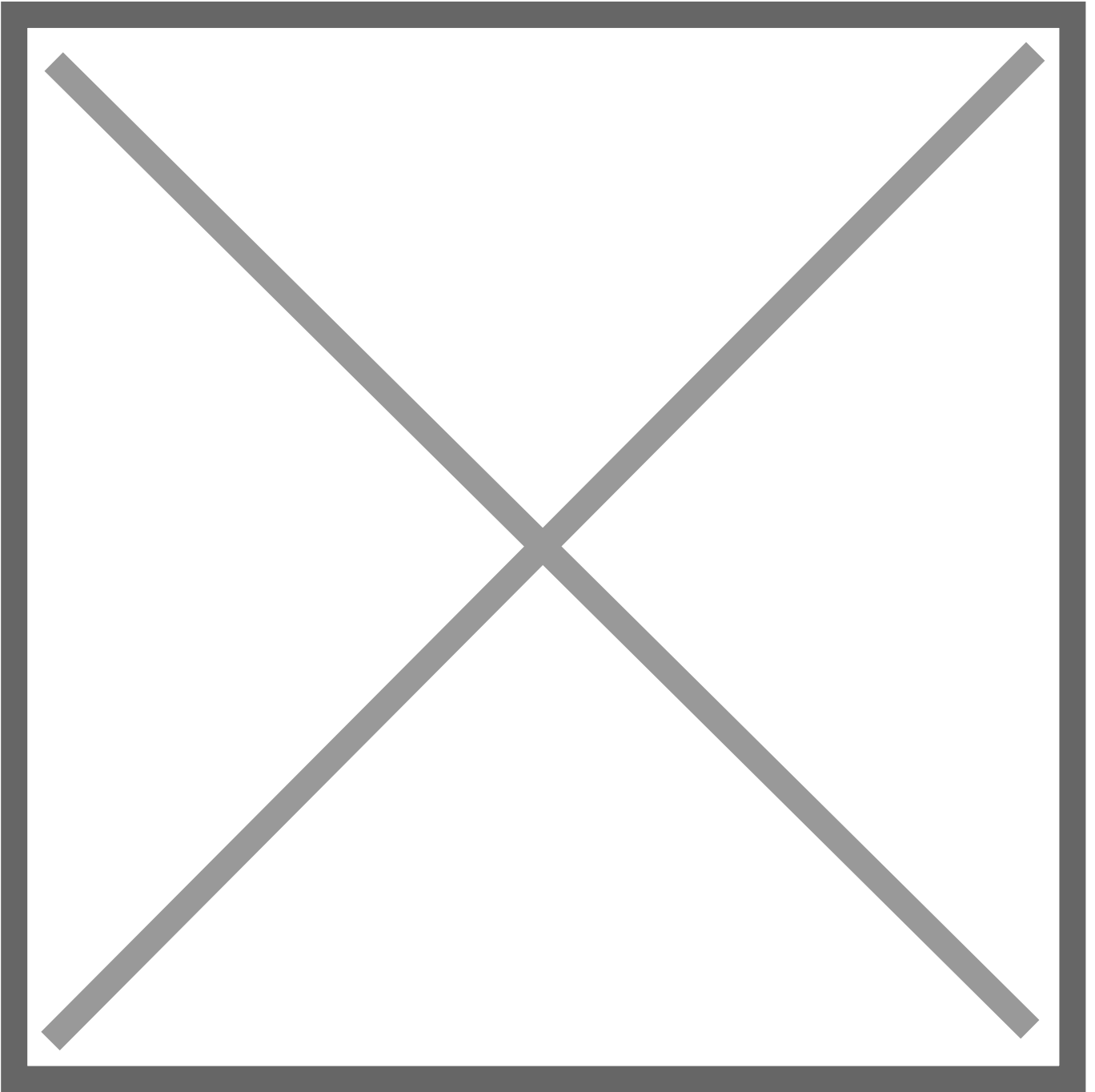
Virtualisierte Umgebung

Eine virtuelle Maschine ist ein Softwarecomputer, auf dem Betriebssystem und Anwendungen wie auf einem physischen Computer ausgeführt werden. Festplatte, Speicher oder CPU werden ihr mittels Softwareemulation bereitgestellt.

Hinweis: Wenn Sie auf Virtualisierung klicken, werden Sie an den WP-Kurs Virtualisierung weitergeleitet. Das ist an dieser Stelle nicht sinnvoll, allerdings gibt es auf Moodle nur die Allgemeine Einstellung Autoverlinkung zuzulassen oder nicht. Und weil alle WP-Kurse innerhalb des gleichen Moodle-Kurses sind, kann ich es nicht für meinen WP-Kurs individuell anpassen.

Gründe für den Einsatz von Virtualisierung:

- Konsolidierung von Hardware: Serverhardware ist sehr leistungsfähig und für einzelne Hardwarelösungen oversized. Die Konsolidierung der Funktionsserver als VM auf wenige Virtualisierungsknoten spart Geld, Strom und Platz.
- Virtualisierung spart Zeit: Virtuelle Maschinen können mit einem Mausklick schnell erstellt oder gelöscht werden.
- Erhöhung der Verfügbarkeit: In einem Clusterverbund können VMs zwischen den Virtualisierungsknoten verschoben werden und es gibt keine Abhängigkeit der Systeme zu bestehender physikalischer Hardware.

**Aufgabe:**

Wie Sie es aus *Kapitel 2. IT-Kurs: Übersicht und Ziele* erfahren haben, werden wir in diesem Kurs in einer virtualisierten Umgebung arbeiten.

Tauschen Sie sich darüber mit Ihrem Sitzpartner aus und entscheiden Sie gemeinsam, warum es sinnvoll ist in der Schule die Hacking-Tools in einer virtualisierten Umgebung auszuprobieren.

Beschreiben Sie die Gründe für die Nutzung von Kali Linux und Metasploitable 2 in einer virtualisierten Umgebung.