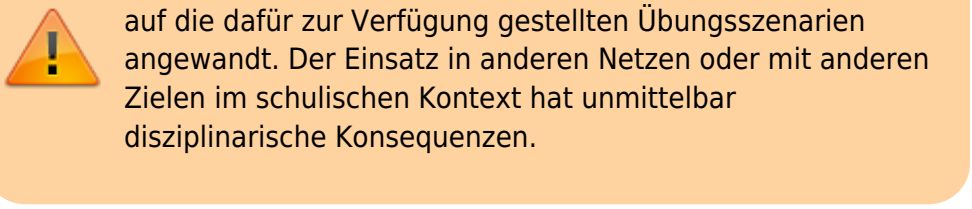
Rechtliches und Rahmenbedingungen

In Deutschland ist die Rechtslage für den Einsatz von Hacking-Werkzeugen aller Art für den Anwender stets risikobehaftet, der 202c des Strafgesetzbuchs ("Hackerparagraph") führt > dazu aus:

> §(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er
>
> 1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
> 2. 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.

(https://dejure.org/gesetze/StGB/202c.html)

Das bedeutet, dass bereits ein Netzwerkscan oder das Mitführen eines Rechners mit Kali-Linux unter ungünstigen Umständen gravierende Auswirkungen haben kann.



Ethisches Hacken

Ein "ethischer Hacker" ist ein Computer- und Netzwerk-Experte, der Sicherheitssysteme im Auftrag ihrer Eigentümer angreift, um Sicherheitsprobleme aufzudecken. Dabei sucht er nach Schwachstellen, die ein Angreifen mit mit bösartigen Absichten ebenfalls ausnutzen könnte.

Erkannte Probleme werden an an den Auftraggeber gemeldet und nicht zum eigenen Vorteil ausgenutzt. Manchmal spricht man bei einem ethischen Hacker auch von einem "White Hat" im Gegensatz zum "Black Hat" des bösartigen Angreifers.

Überprüft man Systeme ohne expliziten Auftrag des Betreibers, befindet man sich in Deutschland aufgrund des Hackerparagraphen tief im dunkelgrauen Bereich, besonders dann, wenn ins Netz offene IT-Systeme bereits ohne großen Aufwand Sicherhetslücken offenbar werden lassen. Hier muss man auch bei Meldung der Lücke an den Betreiber mit rechtlichen Konsequenzen rechnen, als Neuling bietet es sich an bei Experten Rat zu holen, z.B. bei Mitgliedern des CCC.

Für **Meldung von Sicherheitslücken** sollte generell das "Responsible Disclosure"-Vorgehen angewandt werden: Sicherheitslücken werden stets die Betreiber/Anbieter fehlerhafter Systeme informiert und es wird eine Frist vereinbart, in der die Lücke geschlossen werden kann (oder ein Patch zur Verfügung gestellt wird), bevor die Lücke öffentlich bekannt gegeben wird.