HackSimulator.nl

user@hacksimulator:~$

Ethisch Hacken & de Nederlandse Wet

Gratis Sample — De wet en 'wat mag wél' uit de volledige Juridische Gids

Versie 1.0 (sample) · augustus 2026

Over dit sample

Je wilt ethisch hacken leren. Misschien heb je al wat commands uitgeprobeerd in HackSimulator, of je bent net begonnen met je eerste Nmap scan. En dan komt de vraag die alles bepaalt: *mag dit eigenlijk wel?*

Het korte antwoord: **hacken is niet per definitie illegaal — ongeautoriseerd hacken is dat wél.** Het verschil zit in toestemming, proportionaliteit en hoe je ermee omgaat.

Dit **sample** geeft je de twee hoofdstukken die je het hardst nodig hebt voordat je iets aanraakt wat niet van jou is: wat de wet precies verbiedt, en onder welke voorwaarden hacken juist wél mag. Dat is genoeg om veilig te beginnen.

De volledige gids gaat daarna verder met echte Nederlandse rechtszaken (inclusief ECLI-nummers), de AVG bij pentesting, bug bounty-programma's, het Hack_Right-programma van het OM en een checklist die je vóór elke opdracht afloopt.

> **[LET OP]** Deze gids is informatief en vervangt geen juridisch advies. Bij twijfel: raadpleeg een advocaat gespecialiseerd in cybercrime.

De Wet — Wat Zegt de Nederlandse Wet Over Hacken?

Artikel 138ab Sr — Computervredebreuk

De kern van de Nederlandse hackwetgeving is **artikel 138ab van het Wetboek van Strafrecht**. Dit artikel stelt "computervredebreuk" strafbaar: het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk (computer, server, netwerk, database, IoT-apparaat — elk digitaal systeem).

De drie leden van art. 138ab Sr

Lid	Wat is strafbaar?	Maximale straf
Lid 1 — Basis	Opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk	**2 jaar cel** of geldboete vierde categorie (max. €27.500 per 2026)
Lid 2 — Met datadiefstal	Binnendringen + vervolgens gegevens overnemen, aftappen of opnemen	**4 jaar cel** of geldboete vierde categorie
Lid 3 — Via telecomnetwerk	Binnendringen via openbaar telecomnetwerk + verwerkingscapaciteit misbruiken of als springplank naar andere systemen	**4 jaar cel** of geldboete vierde categorie

Wat telt als "binnendringen"? De wet noemt expliciet:

- Doorbreken van een beveiliging (wachtwoord kraken, firewall omzeilen)
- Technische ingreep (exploit gebruiken, buffer overflow)
- Valse signalen of een valse sleutel (gestolen credentials, session hijacking)
- Aannemen van een valse hoedanigheid (social engineering, phishing)

> `[!]` Sinds de Wet Computercriminaliteit III (2019) hoeft er **geen beveiliging doorbroken** te zijn. Ook een onbeveiligd systeem binnendringen zonder toestemming is strafbaar.

Bron: Art. 138ab Wetboek van Strafrecht — inwerkingtreding 20 april 2016, gewijzigd bij Wet Computercriminaliteit III (2019)

Wat Mag Wél — Wanneer is Hacken Niet Strafbaar?

De Gouden Regel: Toestemming

De eenvoudigste manier om legaal te hacken: **vraag toestemming.** Schriftelijk. Vooraf. Concreet.

Situatie	Legaal?	Waarom?
Je werkgever vraagt je hun systeem te testen	Ja	Schriftelijke opdracht = toestemming
Je scant je eigen thuisnetwerk met Nmap	Ja	Eigen systeem = eigen toestemming
Je scant het wifi-netwerk van je buurman “uit nieuwsgierigheid”	Nee	Geen toestemming, geen reden
Je vindt per ongeluk een open database en downloadt alles	Nee	Geen toestemming + disproportioneel
Bug bounty programma van een bedrijf	Ja	Bug bounty = expliciete uitnodiging

Coordinated Vulnerability Disclosure (CVD)

Wat als je per toeval een kwetsbaarheid vindt? Nederland heeft hiervoor een internationaal geprezen systeem: **Coordinated Vulnerability Disclosure** (CVD), voorheen “Responsible Disclosure” genoemd.

Zo werkt CVD:

1. Je vindt een kwetsbaarheid
2. Je meldt het **direct** aan de eigenaar van het systeem (of aan het NCSC)
3. Je houdt de kwetsbaarheid **geheim** totdat deze is opgelost
4. Je gaat **niet verder dan nodig** om het probleem aan te tonen
5. De eigenaar lost het op, en je krijgt (eventueel) erkenning

NCSC-tijdlijnen bij melding:

Stap	Termijn
Bevestiging ontvangst	1 werkdag
Eerste beoordeling	3 werkdagen
Oplossing door organisatie	Richt op 60 dagen

Wat je NIET mag doen bij CVD:

- Malware plaatsen
- Gegevens kopiëren of downloaden (meer dan strikt nodig als bewijs)
- Brute force aanvallen uitvoeren
- DDoS-aanvallen uitvoeren
- Social engineering toepassen
- Wijzigingen aanbrengen in het systeem

Bron: NCSC — Kwetsbaarheid melden

De Drie Juridische Voorwaarden

Het Openbaar Ministerie (OM) erkent dat ethisch hacken onder bepaalde omstandigheden niet wederrechtelijk is. Maar je moet aan **drie voorwaarden** voldoen:

1. Zwaarwegend maatschappelijk belang

Je hack moet een echt maatschappelijk doel dienen — niet je nieuwsgierigheid bevredigen of indruk maken op vrienden.

2. Proportionaliteit

Je mag niet verder gaan dan nodig om de kwetsbaarheid aan te tonen. Eén bestand downloaden als bewijs? Mogelijk acceptabel. Een hele database kopiëren? Nooit.

3. Subsidiariteit

Was er een minder ingrijpende manier om hetzelfde doel te bereiken? Had je het bedrijf eerst kunnen mailen? Dan had je dat moeten doen.

> **[LET OP]** Zelfs als je aan alle drie voorwaarden voldoet, biedt dit **geen garantie** op strafrechtelijke immuniteit. Het OM kan altijd besluiten om te vervolgen. CVD is een richtlijn, geen vrijbrief.

Hoe nu verder?

Wat je nu al kunt

Met alleen dit sample kun je veilig oefenen. De drie regels die je overhoudt:

1. **Oefen op wat van jou is** — je eigen netwerk, een eigen VM, of een simulator zoals HackSimulator.
2. **Vraag toestemming schriftelijk en vooraf** — mondeling is geen bewijs.
3. **Vind je per ongeluk iets? Stop, documenteer, meld** — ga niet verder kijken “om het zeker te weten”. Juist dat doorzoeken kost mensen hun zaak.

De volledige gids

Ethisch Hacken & de Nederlandse Wet — de complete juridische gids voor (aankomende) ethische hackers in Nederland. Naast de twee hoofdstukken hierboven bevat de volledige versie:

- **Echte Nederlandse rechtszaken** met ECLI-nummers — wat er precies misging en waar de grens lag
- **De AVG bij pentesting** — wanneer je een verwerkersovereenkomst nodig hebt, en wat er in je toestemmingsdocument moet staan
- **Bug bounty in Nederland** — welke organisaties een CVD-beleid hebben en hoe je je eerste melding aanpakt
- **Hack_Right** — het programma van het OM voor jonge hackers, en waarom dat voor jou relevant is
- **De 10-punten veiligheidscheck** — de checklist die je vóór elke opdracht afloopt

Download de volledige gids

hacksimulator.gumroad.com/l/yzdtfx

Vanaf €5 (pay-what-you-want) · Direct download · PDF

Of bekijk alle gidsen op hacksimulator.nl/gidsen.html — daar vind je ook het Pentest Playbook en het Leerplan.

Dit sample is gemaakt voor HackSimulator.nl — de gratis browser-based terminal simulator voor ethisch hacken.
Sample versie 1.0 · Hoofdstuk 1 & 2 van volledige Juridische Gids v1.1 · augustus 2026