HackSimulator.nl

user@hacksimulator:~$

Je Eerste Pentest

Gratis Sample — Fase 0 & 1 uit het volledige Stap-voor-Stap Playbook

Versie 1.0 (sample) · april 2026

Over dit sample

Je hebt geleerd wat Nmap doet. Je weet dat SQL injection bestaat. Je hebt misschien zelfs een paar challenges in HackSimulator afgerond. Maar dan komt de grote vraag: **hoe voer je een echte pentest uit, van begin tot eind?**

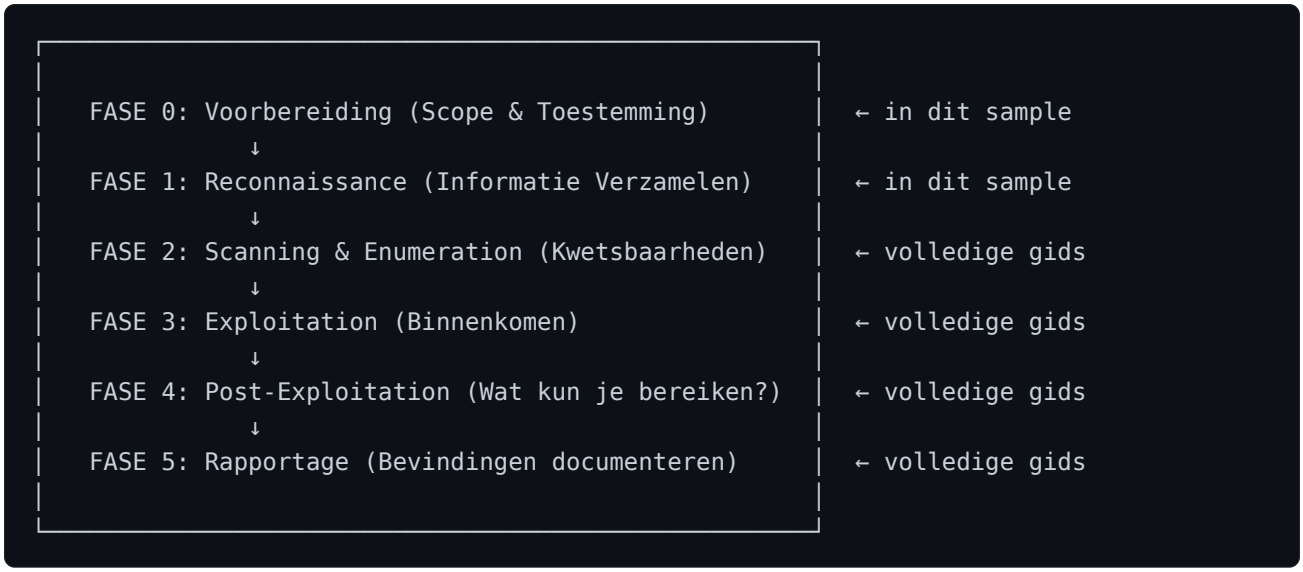
Dat is het verschil tussen tools kennen en een methodologie beheersen. Een timmerman die weet hoe een hamer werkt is nog geen huizenbouwer — daarvoor heb je een bouwplan nodig.

Dit **sample** geeft je de eerste twee fases van dat bouwplan: voorbereiding en reconnaissance. Dat is genoeg om te zien hoe de volledige gids werkt. De volledige versie bevat daarnaast ook scanning, exploitation, post-exploitation en rapportage — met template en voorbeelden.

> `[!]` Dit playbook is bedoeld voor gebruik op systemen waar je **schriftelijke toestemming** voor hebt. Zonder toestemming is elke techniek in dit boek illegaal. Zie de Juridische Gids van HackSimulator voor de volledige juridische achtergrond.

De 6 Fases van een Pentest

Elke professionele pentest volgt dezelfde structuur. Dit is geen willekeurige volgorde — elke fase bouwt voort op de vorige. Sla geen fases over.



In dit sample werk je Fase 0 en Fase 1 volledig door. Dat is bewust — de eerste twee fases bepalen of je pentest legaal en gestructureerd is. Zonder die basis is de rest zinloos.

Fase 0: Voorbereiding — Voordat Je Begint

Dit is de fase die beginners overslaan en professionals nooit vergeten. Zonder goede voorbereiding heb je geen bewijs van toestemming, geen duidelijke scope, en geen plan.

Het toestemmingsdocument

Voordat je ook maar één command typt, moet je dit op papier hebben:

Onderdeel	Wat erin staat	Voorbeeld
Wie	Opdrachtgever + tester	“SecureCorp BV, pentest door [jouw naam]”
Wat	Welke systemen (scope)	“Webapplicatie op app.securecorp.nl + API”
Wat NIET	Expliciet buiten scope	“Productiedatabase mag niet gewijzigd worden”
Wanneer	Start- en einddatum	“1-15 april 2026, werkdagen 09:00-18:00”
Hoe	Toegestane technieken	“Port scanning, web app testing, brute force op test-accounts”
Contact	Wie bel je bij problemen?	“Jan de Vries, CISO, 06-12345678”
Data	Wat doe je met gevonden gegevens?	“Versleuteld opgeslagen, na rapport verwijderd”

> [!] Geen document = geen pentest. “Ze zeiden dat het mocht” is geen bewijs. Schriftelijk, ondertekend, bewaard.

Je testomgeving

Zorg dat je het volgende hebt:
- [ ] Eigen laptop/VM (niet het netwerk van je werkgever of school)
- [ ] VPN-verbinding als je op afstand test
- [ ] Logging aan — alles wat je doet wordt vastgelegd (beschermt jou)
- [ ] Screenshot-tool klaar (bewijs van bevindingen)
- [ ] Notitieboek/document open voor aantekeningen
- [ ] Contactgegevens van opdrachtgever bij de hand

Mentale checklist

Stel jezelf drie vragen:
1. **Heb ik toestemming voor wat ik ga doen?** → Zo niet: stop.
2. **Weet ik wat de scope is?** → Zo niet: vraag verduidelijking.

3. **Weet ik wie ik moet bellen als er iets misgaat?** → Zo niet: regel het eerst.

Fase 1: Reconnaissance — Het Doelwit Verkennen

Doel: Zoveel mogelijk informatie verzamelen ZONDER het doelwit direct aan te raken.

Reconnaissance is de fase die het verschil maakt tussen een amateur en een professional. Hoe meer je weet voordat je begint met scannen, hoe gerichter (en stiller) je kunt werken.

Passieve reconnaissance (geen direct contact)

Dit zijn technieken waarbij het doelwit niet merkt dat je bezig bent.

WHOIS — Wie is de eigenaar?

```
whois securecorp.nl
```

Wat je zoekt:
- Registrant naam en organisatie → wie beheert het domein?
- Nameservers → welke DNS provider? (bijv. Cloudflare = extra beveiliging)
- Aanmaakdatum → oud domein = meer historie om te onderzoeken
- E-mailadressen → bruikbaar voor social engineering of als login-naam

DNS records — Welke systemen bestaan er?

```
dig securecorp.nl ANY
```

> **[LET OP]** `dig` is een standaard Linux-tool voor DNS-lookups. Dit command is niet beschikbaar in HackSimulator, maar wel op elk Linux-systeem en in TryHackMe-omgevingen.

Wat je zoekt:
- A-records → IP-adressen van servers
- MX-records → mailservers (vaak andere leverancier)
- TXT-records → SPF/DKIM configuratie, soms interne info
- Subdomains → dev.securecorp.nl, staging.securecorp.nl

Openbare bronnen:
- Google dorking: `site:securecorp.nl filetype:pdf` → openbare documenten
- LinkedIn: welke technologieën gebruiken hun developers? (vacatures zijn goudmijnen)
- GitHub: heeft het bedrijf openbare repositories? Staan er secrets in commits?
- Shodan.io: welke services zijn publiek zichtbaar?

Actieve reconnaissance (direct contact)

Nu ga je het doelwit wél aanraken. Vanaf hier moet je toestemming hebben.

Ping — Is het doelwit bereikbaar?

```
ping 192.168.1.100
```

> **[TIP]** Geen ping-antwoord betekent niet altijd “offline.” Veel firewalls blokkeren ICMP. Gebruik nmap met de `-Pn` flag om toch te scannen.

Traceroute — Hoe ziet het netwerk eruit?

```
traceroute 192.168.1.100
```

Wat je zoekt:

- Aantal hops → hoe ver weg is het doelwit?
- Timeouts (* * *) → mogelijk een firewall die verkeer filtert
- Onverwachte tussenstops → proxy’s, load balancers

Wat je nu moet hebben

Na Fase 1 heb je een “target profile”:

```
┌─ TARGET PROFILE ──────────────────────────┐
│ Domein: securecorp.nl                     │
│ IP: 192.168.1.100                         │
│ Online: Ja (ping bevestigd)               │
│ DNS: Cloudflare (DDoS protection)         │
│ Subdomains: app., api., dev., staging.    │
│ Tech stack: nginx, mogelijk PHP/Node.js   │
│ Mail: Google Workspace (MX records)       │
│ Contactpersonen: 3 developers op LinkedIn │
└───────────────────────────────────────────┘
```

Einde Sample — Wat Zit er in de Volledige Gids?

Dit sample heeft je door Fase 0 (voorbereiding) en Fase 1 (reconnaissance) geleid. De volgende fases — waar het echte werk gebeurt — zitten in de volledige Pentest Playbook.

Wat je nog niet hebt gezien

```
FASE 2: Scanning & Enumeration
  → Port scanning met Nmap (beslisboom per poort)
  → Web vulnerability scanning met Nikto (ernst-tabel)
  → SQL injection testen met SQLmap (proportionaliteit)
  → Vulnerability map template

FASE 3: Exploitation
  → Brute force met Hydra (wanneer wel/niet)
  → Exploitation met Metasploit (CVE-tabel met echte voorbeelden:
    EternalBlue, Log4Shell, BlueKeep)

FASE 4: Post-Exploitation
  → Systeem verkennen (/etc/passwd, netstat)
  → Gevoelige data zoeken (config files, bash history)
  → Password cracking met Hashcat (hash-type tabel)

FASE 5: Rapportage
  → Rapport-structuur (6 secties)
  → CVSS-gebaseerde ernst-classificatie
  → Finding-template (kopieerbaar)
  → Management samenvatting schrijven

BONUS: Snelreferentie met ALLE commands + veelvoorkomende poorten
```

Waarom Fase 2-5 het verschil maken

Fase 0 en 1 leren je **structuur**. Fase 2 t/m 5 leren je **uitvoeren en rapporteren**. Een pentest zonder goed rapport is waardeloos — de opdrachtgever moet je bevindingen kunnen begrijpen én fixen. De volledige gids geeft je een template dat je direct kunt gebruiken.

> **[TIP]** Gebruikers die de volledige gids doorwerken hebben een concreet startpunt: een rapport-template dat ze kunnen invullen bij hun eerste échte opdracht of TryHackMe-walkthrough.

De volledige gids

Je Eerste Pentest: Stap-voor-Stap Playbook — complete methodologie voor beginnende ethische hackers. Fase 0 t/m 5, alle commands, rapport-template.

Download de volledige gids

hacksimulator.gumroad.com/l/wmvpx

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

Of bekijk alle gidsen op hacksimulator.nl/gidsen — daar vind je ook de Juridische Gids en het Leerplan.

Dit sample is gemaakt voor HackSimulator.nl — de gratis browser-based terminal simulator voor ethisch hacken.
Sample versie 1.0 · Fase 0 & 1 van volledige Playbook v1.0 · april 2026