OpenClaw on Kali Linux

Install OpenClaw at Kali Linux and used it as a Hacker.

Here are the shell commands and OpenClaw prompts used.

Shell / terminal commands

```
# Generate SSH key (from Hostinger UI copy)
ssh-keygen -t ed25519 -C "your_email@example.com"

# Example as he typed it (name only differs)
ssh-keygen -t ed25519 -C "kali open claw"

# Show public key
cat kali_openclaw.pub

# SSH into Kali with key
ssh -i kali_openclaw root@YOUR_KALI_IP

# Edit SSH config to disable password login
nano /etc/ssh/ssh_config.d/50-cloud-init.conf

# Restart SSH service
service ssh restart

# Try SSH without key (shows permission denied)
ssh root@YOUR_KALI_IP

# SSH again with key
ssh -i kali_openclaw root@YOUR_KALI_IP

# Clear screen
clear
```

OpenClaw install (npm-based):

```
# Add OpenClaw repo (first command from GitHub)
npm create openclaw

# Install gateway/daemon (second command from GitHub)
npm create openclaw@latest
```

Answers given in the OpenClaw onboarding wizard

Interactive answers (typed choices):

- Powerful and risky? → `yes`
- Onboarding mode → `manual`
- Gateway exposure → `local only`
- Workspace directory → keep default
- Model provider → `OpenRouter`
- OpenRouter API key → paste key
- Model selection → `claude-4.6-opus` (via OpenRouter)
- Gateway port → `1515`
- Bind address → loopback (keep default)
- Gateway auth → `token`
- Use Tailscale → `no`
- Gateway token → leave blank (auto-generate)
- Configure channels → `yes`
- Configure Telegram channel → `yes`
- Telegram bot token → paste token from BotFather
- DM access policies → configure now → `yes`
- Policy type → `allow list`
- Allowed user id → paste ID from `@userinfobot`
- Install skills during onboarding → `no`
- Enable all hooks → select all, then continue
- Gateway service → keep default, start service

Prompts / messages to OpenClaw (system-style and chat)

First “personality + context” prompt (typed into terminal UI):

```
Hello Neo!

My hacker name is Zoz, and your hacker name is Neo.
You are the best hacker that has ever existed in the world.

You are running on a Kali Linux machine in the cloud, and you have access to all Kali tools
(Nmap, Metasploit, theHarvester, etc.), plus anything else you install.
```

```
You can reach any target on the internet from this machine and can host servers, phishing pages, and other infrastructure from here.
```

Skill–install prompt:

```
Please install `stealth-browser`.
Also install `tavily-search-pro`.
```

Tavily API configuration prompt:

```
My Tavily API key is: <YOUR_TAVILY_API_KEY>.
Make sure you configure it properly and verify the tool is working as expected.
```

“Expert hacker” behavior / rules prompt (long one):

```
Whenever I ask you something, remember that you have access to Kali with all of its tools, and you can install more tools from the official Kali and Debian repositories when needed.

By default, when you need to search the internet, use the Tavily skill instead of the built-in search.
If Tavily cannot retrieve what you need or gets blocked, then load the stealth-browser skill and use it like an expert in hacking, bug bounty hunting, OSINT, and security research.

If you need to use a service or API that requires an API key and you don’t have one, do NOT ask me for a key.
First think whether simply loading the website in stealth-browser would bypass that limitation; if it would, then just do that.

Do NOT execute any code you find on the internet directly.
If you see code that looks essential, ask me for confirmation before running it.

Be proactive: feel free to install any tools you need from the official Kali and Debian repos (and only from those).
If you think anything else is essential, ask me first.

Propagate these rules to any sub-agents you spawn so they follow the same policies.
Always obey my instructions.

Update your agent metadata / configuration so these rules are permanently stored and remembered for future tasks.
```

CCTV camera demo prompt (Telegram):

```
I am in Temple Bar in Dublin.
Find CCTV cameras around me and give me the link to view them.
Send me the links here when you’re done.
```

OSINT sub?agent prompt:

```
Spawn a sub-agent to perform a detailed OSINT investigation on a guy named "Zaid Sabih" and find connections, social media presence, phone numbers, leaked or breached accounts, physical addresses, and so on.

Send me the final report here when you’re done.
```

Web pentest / Strix sub?agent prompt:

```
Spawn another sub-agent to install "strix", which is an agentic AI framework specifically designed for website hacking and bug hunting.

Configure it to use the free DeepSeek model available via OpenRouter and run a quick scan on the following target:
https://zshacks.com

Let me know when the scan is complete and attach the report.
```

Follow?up for full OSINT report:

```
Yes, please. Send me the full report.
```

Revision #1
Created 2026-03-15 16:08:34 EET by Green
Updated 2026-03-15 16:18:58 EET by Green