VOID WALKER

RUNE OPERATOR LAB

Ethical recon · network mapping · OSINT on systems YOU own

WHAT THIS BOOK IS

Fun, practical tools inside Rune Term: nmap, dig, whois, traceroute, curl, python scripts, IP intel, and home-lab mapping.

Written for lifetime holders who want the cyberdeck side of Void Walker. Not a crime guide. Not for attacking random people or networks.

GOLDEN RULE

Only scan, probe, and track systems you own or have written permission to test.

Your home lab. Your VPS. Your employer's approved scope. Nobody else's Wi■Fi.

Christ is King. Operate clean.

Rules of engagement

break these and tools become weapons — we teach defense, not harm

LAW & ETHICS — READ THIS

DO: map your own LAN, harden your own servers, practice on lab VMs you spun up.
DO: use public IP intel on your own domains / your own public endpoints.
DO NOT: scan strangers, schools, workplaces (unless written pen-test scope), or neighbors.
DO NOT: use tracking to stalk, harass, or dox. That is illegal and against our terms.
DO NOT: run exploits, password spraying, or malware. This manual does not cover that.
Support: admin@alphaomegatech.net — we will not help with illegal use.

Good targets for practice

- Your home router's LAN side (192.168.x.x / 10.x.x.x) — carefully; don't DoS it.
- A spare Raspberry Pi, old laptop, or free lab VM you control.
- Your own public website / VPS (rate-limit friendly scans only).
- Intentionally vulnerable lab images (e.g. local DVWA / Metasploitable you install).

Mindset

You are learning how attackers think so you can defend family devices, small business gear, and your own lab. Curiosity is good. Permission is mandatory. Slow scans beat loud ones. If a tool feels sketchy for the target — stop.

VOID WALKER STACK REMINDER

Rune = cockpit shell on the phone (no root).
Heavy attack platforms (if any) belong on a PC you own — not forced onto the phone.
Armor / Shield / Call Gate still protect the phone while you learn.
Public guide: voidwalker.app · Rune quick ref: voidwalker.app/downloads/Rune-Quick-Reference.pdf

Open Rune · install the lab

one-time package kit for recon tools

Open Void Walker → bottom tab Rune Term. Wait for the rune$ prompt. Prefer one session (S1). Type one command, press Enter / Send, wait for output before the next.

STEP 1 — HEALTH + UPDATE MIRRORS

```
vw doctor
pkg update -y
pkg upgrade -y
```

STEP 2 — ETHICAL RECON KIT (COPY ONE LINE AT A TIME IF NEEDED)

```
pkg install -y nmap nmap-ncat
pkg install -y dnsutils traceroute whois
pkg install -y curl wget openssl openssh
pkg install -y git python python-pip
pkg install -y net-tools iproute2
pkg install -y jq nano tmux
```

STEP 3 — PROVE TOOLS INSTALLED

```
nmap --version
dig -v
whois --version || which whois
python3 --version
git --version
ssh -V
```

If pkg fails mid-way: run pkg update again, then reinstall only the missing package. Family builds include pkg self-heal — open a fresh Rune session (New) after big installs.

TYPING TIP

One command per Enter. Soft-wrap can break long URLs — paste carefully.
Do not glue rm + git clone + ls on one line.
Paste button pastes clipboard into the draft line.

Know your own IP footprint

IP intel · “tracker” style lookups · only on your identity / lab

“IP tracker” in operator speak means: what is this address, where does DNS point, what ASN owns it, what ports answer on MY host. It does not mean following people around the internet.

PUBLIC EGRESS IP (YOU / YOUR CELL / YOUR WIFI)

```
# Your phone's view of the path out
curl -s https://ifconfig.me ; echo
curl -s https://ipinfo.io/json | python3 -m json.tool
curl -s https://ipapi.co/json/ | python3 -m json.tool
```

DNS + WHOIS (REPLACE example.com WITH YOUR DOMAIN)

```
# DNS facts for a domain YOU own
dig example.com ANY +noall +answer
dig example.com A +short
dig example.com MX +short
dig example.com NS +short
dig example.com TXT +short
whois example.com | head -n 40
```

PATH + OWNERSHIP INTEL

```
# Reverse look at an IP YOU control (VPS / home public IP)
dig -x 203.0.113.10 +short
whois 203.0.113.10 | head -n 50
traceroute -n 1.1.1.1
```

- ipinfo / ipapi return city-level geo estimates — often wrong by miles. Treat as hints.
- Never paste someone else’s personal IP into public pastes with intent to harass.
- For continuous monitoring of your own site, prefer uptime tools on a PC later.

nmap — map what you own

discover hosts · open ports · service banners · slow & polite

nmap is the classic network mapper. On a phone, keep scans small. Start with your LAN. Do not nmap the entire internet. Do not nmap corporate networks without a signed scope.

STEP A — KNOW YOUR NETWORK

```
# Find your LAN interface / gateway (names vary)
ip route
ip -brief addr
# Example private ranges: 192.168.1.0/24  192.168.0.0/24  10.0.0.0/24
```

STEP B — DISCOVERY + PORTS

```
# Ping sweep YOUR /24 only (swap the subnet)
nmap -sn 192.168.1.0/24

# Top common ports on one host YOU own
nmap -F 192.168.1.10

# Service/version guess (noisier — lab only)
nmap -sV -F 192.168.1.10
```

STEP C — RECORD EVIDENCE (YOUR LAB NOTES)

```
# Save results for study
mkdir -p ~/lab-scans
nmap -sn 192.168.1.0/24 -oN ~/lab-scans/lan-hosts.txt
nmap -sV -F 192.168.1.10 -oN ~/lab-scans/host-10.txt
ls -la ~/lab-scans
```

OPERATOR NOTES

Avoid: nmap -A -p- on production gear during family movie night (can stress devices).
Avoid: aggressive UDP floods. Prefer -T3 or slower if things get flaky.
Router admin pages / cameras: patch them; don't leave default passwords after you find them.

Fun lab recipes

safe mini-projects that feel like “hacking class”

1) “Who is on my Wi■Fi?”

```
nmap -sn 192.168.1.0/24
# List live hosts → match MACs in router admin if available
# Unexpected device? Change Wi■Fi password + use Void Shield later
```

2) “Is my home server exposing junk?”

```
nmap -sV -p 22,80,443,8080,8443 YOUR.SERVER.IP
# Close ports you don’t need on the firewall / router
```

3) “HTTP headers of my site”

```
curl -sI https://your-domain.example
curl -sI https://your-domain.example | grep -i strict
```

4) “TLS certificate peek”

```
echo | openssl s_client -connect your-domain.example:443 -servername your-domain.example 2>/dev
```

5) “Local listening check via SSH on YOUR PC”

```
ssh you@your-pc
# then on the PC (Windows/Linux varies):
#   netstat -an | findstr LISTEN
#   ss -tulpn
```

GitHub · Python · custom tools

clone public tools · run scripts · stay in legal daylight

Git works over HTTPS in Rune. Clone educational repos, your own projects, or well-known security learning kits. Do not clone malware “for fun.” Read licenses. Prefer tools with clear docs and active maintainers.

GIT HTTPS SMOKE

```
mkdir -p ~/src && cd ~/src
# Smoke test clone (tiny public repo)
git clone --depth 1 https://github.com/git/git.git ~/src/git-smoke
ls ~/src/git-smoke | head
```

YOUR CODEBASE ON THE PHONE

```
# Example: clone YOUR repo (replace URL)
git clone https://github.com/YOURUSER/YOURREPO.git ~/src/YOURREPO
cd ~/src/YOURREPO
ls
```

PYTHON ONE-SHOT

```
# Tiny IP intel script you can edit (legal: your IP only)
python3 - <<'PY'
import json,urllib.request
u='https://ipinfo.io/json'
print(json.dumps(json.load(urllib.request.urlopen(u)), indent=2))
PY
```

PIP (LIGHT USE)

```
pip install --user requests  # if needed for scripts
# Prefer venv on a PC for heavy projects; phone is cockpit
```

- GitHub CLI (gh) may not always install cleanly on every Android ABI — git + HTTPS is enough.
- For passworded git over HTTPS, use a personal access token (never paste tokens into public chats).
- Big compile jobs → SSH to your PC and build there (phone stays the remote control).

SSH cockpit · files · mesh

use the phone to drive your real lab PC

The fun multiplies when Rune is the remote: run nmap on a Pi, keep notes on a desktop, pull results back to the phone. Set this up on gear you own.

SSH TO YOUR MACHINE

```
pkg install -y openssh   # if not already
bash ~/rune-ssh-connect.sh
# or:  ssh YOURUSER@YOUR-PC-LAN-IP
# optional passwordless:  bash ~/rune-ssh-setup.sh
# then add printed pubkey to PC authorized_keys
```

VW HELPERS (WHEN PROFILES ARE SET)

```
vw doctor
vw hosts
vw ssh <alias>
vw put ./lab-scans/host-10.txt pc:Desktop/
vw get pc:Desktop/notes.txt .
vw mesh list
```

MESH PATH (ANYWHERE)

```
# Work from anywhere (overview)
# 1) Tailscale on phone + PC (same account)
# 2) OpenSSH server on PC, PC left on
# 3) ssh you@magicdns-name from cellular
# Full steps: voidwalker.app  →  #mesh-anywhere
```

- Sessions: New = extra tab (max 6). Daily use: one session is enough.
- Shade notification can keep sessions alive; Exit kills when you are done.
- If commercial VPN fights Tailscale, turn one off while testing mesh.

Command sheet · support

tear-off cheats · keep it ethical

COPY/PASTE STARTER SHEET

```
pkg update -y && pkg upgrade -y
pkg install -y nmap dnsutils traceroute whois curl git python openssh
curl -s https://ipinfo.io/json | python3 -m json.tool
dig yourdomain.com A +short
whois yourdomain.com | head
nmap -sn 192.168.1.0/24
nmap -sV -F 192.168.1.10 -oN ~/lab-scans/host.txt
traceroute -n 1.1.1.1
git clone --depth 1 https://github.com/YOU/REPO.git ~/src/REPO
ssh you@your-pc
vw doctor ; vw status ; vw shield status
```

FINAL HARD LINE

If you are unsure whether a target is in scope — it is not.
Unauthorized scanning can violate computer crime laws where you live.
We will not provide exploit chains, credential stuffing, or malware help.

SUPPORT

Email: admin@alphaomegatech.net (Void Walker Support)
Site: https://voidwalker.app
What's new: https://voidwalker.app/whats-new
Rune quick ref: https://voidwalker.app/downloads/Rune-Quick-Reference.pdf
Field Manual (beginner): sent earlier in this thread
Include: what you typed, what you saw, Android version — no secrets/tokens.

Learn loud. Attack never — unless it's your lab.

Christ is King. — Alpha Omega / Void Walker