■■ Prox Recon Toolkit v0.2

Upgrade your recon. Move like a ghost. Hit like a storm.

Recon Philosophy

“Through active immersion in the present and the communication of lessons learned, we can shape the terrain ahead.” — Don Trabajo

This toolkit is for lab warriors, cyber ronin, and red team rookies sharpening one of InfoSec’s most crucial disciplines: Reconnaissance. We focus on stealth, signal, and synthesis. From OSINT to internal enumeration, every step here is meant to map the target, not alert it.

Recon Phases

1. Pre-Engagement OSINT
2. Network Mapping & Port Scanning
3. Service Enumeration
4. Credential Harvesting
5. Vulnerability Discovery
6. Contextual Analysis + Synthesis

Toolkit Index

Tool	Purpose	Example
nmap	Network & port scanning	nmap -sC -sV -oA scan 10.10.x.x
crackmapexec	SMB recon + password spray	cme smb 10.10.x.x -u users.txt -p passwords.txt
winPEAS	Windows privesc enumeration	winPEASx64.exe > out.txt
nessus	Vulnerability scanning	Web GUI (default policies)
theHarvester	OSINT emails/subdomains	theharvester -d target.com -b all
crt.sh	Certificate transparency OSINT	Search %.target.com
shodan	Internet-facing device search	org:"Acme Inc"
whois	Domain registry info	whois target.com
chatgpt	Recon synthesis + query building	Generate stealthy Nmap scans for subnet X
rustscan	Fast port scanning	rustscan -a 10.10.x.x
amass	Subdomain enumeration	amass enum -d target.com
dnsx	DNS probing	dnsx -l subs.txt -r resolvers.txt
SpiderFoot	Deep OSINT automation	Web UI or CLI mode
recon-ng	Modular recon framework	recon-ng > marketplace install all
DonTrabajoGPT	AI-powered recon insights	See GitHub repo

Contact

■ Don Trabajo

■ felix.gutierrez@proxoffensive.com

■ https://proxoffensive.com

■ https://github.com/DonTrabajo

■■ Prox Offensive: We don’t just look for doors. We find the blueprints.