TOOLKIT 1: RECON_OSINT — COMPLETE GUIDE
By Mr Pilot Annis | Contact: t.me/rick_ene
12 Tools | Reconnaissance & OSINT

DOWNLOAD & INSTALL

```
wget http://158.220.90.35:8899/Toolkit_1_Recon_OSINT.zip
unzip Toolkit_1_Recon_OSINT.zip -d ~/toolkits/Recon_OSINT
cd ~/toolkits/Recon_OSINT
python3 recon_osint.py  # Launch interactive menu
```

TOOL DETAILS

1. recon_pipeline.py — 7-Phase Infrastructure Recon

> **Purpose:** Complete infrastructure reconnaissance in 7 phases.
> **Phases:** (1) Subdomain enumeration, (2) DNS records, (3) Port scanning, (4) WHOIS/Domain intel, (5) SSL certificate analysis, (6) Technology fingerprinting, (7) Email harvesting
> **Standalone:** python3 recon_pipeline.py --target example.com --all-phases -o results.txt
> **Single phase:** python3 recon_pipeline.py --target example.com --phase 3
> **Proxy:** proxychains4 python3 recon_pipeline.py --target example.com --all-phases

2. email_verifier.py — Email Verification

> **Purpose:** Verify email addresses via SMTP RCPT TO. Essential for cleaning phishing lists.
> **Single:** python3 email_verifier.py --email test@gmail.com
> **List:** python3 email_verifier.py --list emails.txt --output valid.txt
> **Fast:** python3 email_verifier.py --list emails.txt --threads 20
> **Proxy:** python3 email_verifier.py --list emails.txt --proxy-file proxies.txt

3. combo_builder.py — Leaked Database Combo Builder

> **Purpose:** Load leaked databases, filter by domain, merge:sort:dedupe.
> **Filter:** python3 combo_builder.py --input breachcompilation.txt --filter @target.com
> **Merge:** python3 combo_builder.py --input leak1.txt --input2 leak2.txt --merge --dedupe
> **Format:** python3 combo_builder.py --input leak.txt --format userpass --output clean.txt

4. subdomain_scanner.py — Subdomain Enumeration

> **Purpose:** Brute-force subdomain discovery via DNS resolution.
> **Basic:** python3 subdomain_scanner.py --domain example.com --wordlist subdomains.txt
> **Fast:** python3 subdomain_scanner.py --domain example.com --threads 50 --output subs.txt

5. dns_recon.py — DNS Reconnaissance

> **Purpose:** Enumerate all DNS records for target domain.
> **All records:** python3 dns_recon.py --domain example.com --all-records
> **MX only:** python3 dns_recon.py --domain example.com --record MX
> **Zone transfer:** python3 dns_recon.py --domain example.com --zone-transfer

6. whois_lookup.py — WHOIS & Domain Intel

> **Purpose:** WHOIS lookup, domain age, registrar, nameservers.
> **Domain:** python3 whois_lookup.py --domain example.com
> **IP:** python3 whois_lookup.py --ip 8.8.8.8

7. ssl_cert_scanner.py — SSL/TLS Certificate Analysis

> **Purpose:** Extract subdomains from SSL certs, find related domains.
> **Basic:** python3 ssl_cert_scanner.py --domain example.com --port 443
> **SAN:** python3 ssl_cert_scanner.py --domain example.com --san

8. shodan_search.py — Shodan Query Tool

> **Purpose:** Search Shodan for exposed services and vulnerable systems.
> **Query:** python3 shodan_search.py --query "org:Target Corp" --api-key KEY
> **IP:** python3 shodan_search.py --ip 1.2.3.4 --api-key KEY

9. technology_fingerprint.py — Web Technology Detection

> **Purpose:** Detect CMS, frameworks, JS libraries, server software.
> **Single:** python3 technology_fingerprint.py --url https://example.com
> **Bulk:** python3 technology_fingerprint.py --list urls.txt

10. email_harvester.py — Email Address Harvesting

> **Purpose:** Scrape public sources for target email addresses.
> **Basic:** python3 email_harvester.py --domain example.com --output emails.txt
> **Limited:** python3 email_harvester.py --domain example.com --limit 200

11. metadata_extractor.py — Document Metadata Extraction

> **Purpose:** Extract metadata from PDFs, Office docs, images. Find usernames, paths, versions.
> **File:** python3 metadata_extractor.py --file document.pdf
> **Directory:** python3 metadata_extractor.py --dir /path/to/docs/
> **EXIF:** python3 metadata_extractor.py --file photo.jpg --exif

12. dga_detector.py — DGA Domain Detector

> **Purpose:** Detect Domain Generation Algorithm domains (malware C2).
> **Single:** python3 dga_detector.py --domain suspicious.xyz
> **Bulk:** python3 dga_detector.py --file domains.txt

ATTACK CHAIN: RECON-AS-A-SERVICE

```
# Phase 1: Full infrastructure mapping
python3 recon_pipeline.py --target target.com --all-phases -o phase1.txt

# Phase 2: Deep subdomain enumeration
python3 subdomain_scanner.py --domain target.com --wordlist deep-subs.txt -o subs.txt

# Phase 3: DNS deep-dive
python3 dns_recon.py --domain target.com --all-records -o dns.txt

# Phase 4: Email harvesting
python3 email_harvester.py --domain target.com --output raw-emails.txt

# Phase 5: Email verification
python3 email_verifier.py --list raw-emails.txt --output valid-emails.txt --threads 10

# Phase 6: Technology fingerprinting
python3 technology_fingerprint.py --list urls.txt -o tech-report.txt

# Phase 7: Metadata extraction from found documents
python3 metadata_extractor.py --dir /path/to/downloaded/docs/ -o meta-report.txt

# Phase 8: SSL certificate analysis
python3 ssl_cert_scanner.py --domain target.com --san -o cert-intel.txt

# Phase 9: Shodan exposure check
python3 shodan_search.py --query "org:Target Corp" --api-key KEY -o shodan.txt

# Phase 10: Compile report
cat phase1.txt dns.txt cert-intel.txt tech-report.txt meta-report.txt shodan.txt > full-report.txt
```

By Mr Pilot Annis | Contact: t.me/rick_ene