Red Team – Initial Foothold Checklist (Fillable)

Tick the boxes directly in this PDF to track progress.

OSINT & Recon

- [ ] Google Dorking
- [ ] Login portal through Google Dorking
- [ ] Credential harvesting through Intelx
- [ ] Web.archieve
- [ ] Github Dorking
- [ ] Shodan Enumeration
- [ ] FOFA enumeration
- [ ] DNSdumpster
- [ ] Cencys
- [ ] hunter.how
- [ ] SecurityTrails
- [ ] RapidDNS.io
- [ ] CentralOps.net
- [ ] mxToolbox
- [ ] crt.sh
- [ ] whois
- [ ] IP details of web app
- [ ] Cloudflare bypass

Scanning / Enumeration

- [ ] Nuclei Scan
- [ ] Nikto Scan
- [ ] WpScan Scan
- [ ] Gobuster/FFUF Scan

Vulnerability Validation

- [ ] BurpSuite Pro Scan for File upload/SQLi

Automation

- [ ] Automation through subfinder+httpx+katana+dalfox+SQLMap