**OSINT Passive/Active**

1. To get background info using OSINT sources, run:-

* + ruffo.sh
  + ztr.sh
  + dns.sh

2. Look at website (if any) with Shodan browser plugin

3. Run:-

* + [netcraft.com](http://netcraft.com) to find technologies
  + [robtex.com](http://robtex.com) to find DNS info, rDNS, websites on same server
  + Maltego for detailed OSINT
  + Spiderfoot for detailed OSINT
  + theharvester to get emails
  + dnsrecon
  + dnsenum
  + dig
  + nslookup
  + host
  + fierce
  + netcat to grab banners
  + SimplyMail
  + finger to enum users (semi-active scan)
  + Discover scripts

4. recon-ng (recon modules) use hibp\_breach to find any dumped passwords fro given emails. Try other recong-ng modules, for example Social media searches. Also try Maryam which is a recong-ng clone.

5. Google operators such as site, inurl, filetype entitle e.g

site:target.com -site:www.target.com (find other domains)

intitle:”netbotz appliance” “OK” -filetype:pdf. (Webcams

6. Check usernames https://checkusernames.com and https://knowem.com

7. Track any found images using tineye.com

8. Scrape webpages for custom wordlist use smeeg and brutescrape scripts

9. Document all findings

10. Use screen shots whenever possible

11. Use Reaper for social networks search on keywords

12. Use knock.py for finding subdomains

13. Use gitrob to search Github for sensitive files related to target organisation

14. Use OSINT-master scripts to scan Amazon, Instagram and Shodan

15. Use OSINT-Spy to scan email/domain/ip\_address/organizations

16. Use security-scripts-master to deeper analysis of hosts (some active tests so are loud!)