**Anonymity Tools**

**Kalitorify**

**Proxy chain**

**VPN (Public ip )**

**Tor borowser (Private ip)**

**OSINT Tools**

**Maltego**

**The Harvester ( to check the domain details from different browser)**

**Sherlock ( username registered social medias)**

**Osint framework ( all type of osint in web format)**

**Google docking (indepth google searching)**

**Wigle.net ( find the bsssid location)**

**Exif tool ( document osint)**

**Shodan**

**Subdomain finder (**[**https://subdomainfinder.c99.nl/**](https://subdomainfinder.c99.nl/)**)**

**MXtoolbox (get website records and owner name)**

**Wayback machine(get website old state )**

**SCANNING**

**Nmap –sn (host up)**

**Nmap –O (os)**

**Namp –F (quick scan**

**Nmap –sV (version scan)**

**Nmap –v <Targetip> -S <sourceip> -e eth0 –Pn –f –data-length 64**

**Sparta (Gui scanning)**

**VULNARABILITY ASSESMENT**

**Nikto ( for webserver vulnerability)**

**Arachini ( scanning web application with GUI)**

**Vulscan ( nmap –sV –p- --script=vlun\* <ip>)**

**Vulners (nmap –sV –p- –script vulners <ip>)**

**Open vas tool**

**PASSWORD CRACKING**

**John the ripper**

**Hydra**

**Hashcat**

**Hash-identifier**

**Crunch (wordlist making)**

**Dirsearch (directory search and url)**

**Forexbuster (directory search)**

**Nc –lvnp (portno) (it used to listen particular port)**

**Nc –v (ip) (port) (command used to establish connection)**

**Python3 http.server 8000 (local server)**

**Linpeas (linux privilege escalation)**

**Winpeas (windows privilege escalation)**

**Wget (download the folder from remote)**

**Curl (for http request)**

**Env ( for getting all environment variable in system)**