**PENETRATION TESTING**

**Recon**

* Sublist3r : sublist3r –d domain.com (sub domains)
* theHarvester (emails)
* wappalizer (browser, acts like builtwith)
* whatweb url (same as above)
* social media
* burpsuite (called web proxy)
* crt.sh (web)
* amass
* httprobe

**Scanning**

* arp-scan -l
* netdiscover –I eth0
* netdiscover –r IP/24
* nmap –T4 –A –p- IP

**Exploitation**

* wpscan –url <https://10.0.2.4> –u username –p usr/share/wordlists/…
* smbclient –L [\\\\IP\\](file:///\\\\IP\\)
* hydra –l root –P /usr/share/wordlists/… ssh://IP –t4 –V
* {if SSH is open, use metasploit to scan}
* ssh IP {add the key from the web}
* **To check if a machine has been patched: python <vuln\_checker.py from online> IP**