Assessment Methodologies

Information Gathering - Passive

Tool / Command	Result
host {CMD}	IPv4 + IPv6 + Mail Server
WebsiteURL/robots.txt {URL}	Unindexed Folders / Files
WebsiteURL/sitemap.xml {URL}	Website Mapping
Wappalyzer {Browser Add-On}	Technology stack of the website
whatweb {CMD}	Technology stack of the website
httrack {CMD}	Website source code analysis
whois {CMD}	Internet resource's registration info
netcraft.com {Website}	Site report {All in 1}
dnsdumpster.com {Website}	DNS Records, *but better*
sublist3r {CMD}	Subdomain enumeration
Google Dorks {Search Engine}	General info gathering + Accidental leaks
Google Hacking DB {Website}	General info gathering + Accidental leaks
theHarvester {CMD}	Email Harvesting
haveibeenpwned {Website}	Email leak DB

Information Gathering - Active

Tool / Command	Result
wafw00f {CMD}	WAF Fingerprinting
dnsenum {CMD}	DNS Zone Transfer / Bruteforce
dnsrecon {CMD}	DNS Records
nmap {CMD}	Network Mapper
netdiscover {CMD}	ARP Host Discovery
ping/fping {CMD}	ICMP Host Discovery
arp-scan {CMD}	ARP Host Discovery
route -n {CMD}	Routing Table