Tools and Commands	Bk	Page #	Definition
Awk	6	29	flags -F is delimiter
AWS CLI	2	23	
az	6	88	Azure command line and commands - regards to AD
az run-commands	6	177	
Azure CLI	2	50	Azure command line and commands
buckets.grayhatwarfare.com	2	12	to look for publically exposed buckets
censys.io	1	53	Search engine for Certificate Transparency logs for host discovery
certbot	5	100	a python tool that helps us get a valid cert via lets encrypt
CEWL	5	77	Custom Wordlist Generator tool, creates wordlists
chmod	N/A	N/A	execute 1 - write 2 - read 4 --- Order of permission left to right -> USER, GROUP, Others
CommonSpeak2 Queries	1	95	Wordlist construction tool
Credential stuffing tools	5	86	Hydra, pastor, burp suite, Custom scripts
DISM	3	73	able to modify a live image and inject items, insert files, extract data, and more (backdoor)
dnsrecon.py	1	59	python based dns recon tool created by carlos Perez
dnsrecon.py	6	27	a subdomain enumeration tool
Docker Commands	4	104	expose 443 is a valid command
domainhunter.py	5	95	allows user to search for expired domains that are of neutral or good reputation
Eyewitness	1	105	captures screenshot of web apps and puts it in report
flippa	5	96	Website that allows people to build, sell, and buy web properties
git	4	19	
git utility	6	70	critical issue with git utility , deleting an incorrectly committed file is not enough to wipe the memory
GoBuster	1	87	bruteforcing tool, designed to be multi-threaded
inetdata	1	55	HD Moore repo for enumerating domain names and IP addresses
Intrigue	1	110	designed for mass collection- finding assets, Fingerprinting tools ,Screenshot and code capture - can be called through docker to fingerprint assets
Iptables	3	36	
John	6	173	tool to crack hashes
jq	2	27	A grep like tool for json, the default output of AWS CLI
Kubeadm	5	13	main admin tool that will control the cluster and allow and admin to connect to kubernetes environment

Tools and Commands	Bk	Page #	Definition
Kubectl	5	13	Control software that can perform actions on containers such as copy files, execute binaries, and other misc. network items
Kubelet	5	13	The agent that takes in items from the kubernetes API that works on the nodes.
Masscan	1	71	Port scanning at scale, can scan the internet in 5 minutes -- if you want tcp banner you need spoof source IP
Meterpreter	5	31	We can use meterpreter to backdoor containers
Mimikatz	3	6	Reads into the LSASS process, has many uses
Ngrok	1	38	Netcat as a service, used for tunneling like proxy chains
NMAP	1	77	
nmap	6	38	
PACU	3	59	Rhino Security created an open-source AWS Exploitation tool, operates Amazon API
Peirates	5	22	Compromise of a kubernetes environment can be better accomplished with an attack tool
Postman	2	113	Postman acts as your interface to APIs that you point it to and allows you to interact in a programmatic way
Proxycannon-NG	5	65	creates a network of compute hosts in Amazon and uses each host to route traffic to the internet if at any point a host is shunned, a new one will replace it with a new IP address.
Pw-Inspector	5	89	allows you to take a typical wordlist of any type and manipulate it
SecretsDump.py	6	170	From Impacket and extracts SAM DB, registries, ntds.dit
SHIMIT	2	109	Golden SAML creation tool
shuffledns	6	31	a wrapper for massdns
Socat	3	30	A traffic pivot tool
SQL Map	4	91	Automatic sql injection tool // --crawl-forms might not be used, so might need to sue --forms and a special header , for attacking cloud Native applications and API calls
storageExplorer	6	98	Used to mount shares in Azure
THC hydra	5	87	command line password cracking tool
Travis	4	24	Commonly used tool for deployments, can run commands before, during , or after builds