Name	B#	P#	L#
ACME , certbot	1	50	
AD RBAC Roles	2	80-85	
AD Services and Connector Attacker view	2	78	
Advance C2 architecture	5	53	
Amazon KMS	3	54	Lab3.4
amazon lambda	4	109	
amazon pentest permission	1	29	
Asset collection Frameworks	1	107	
Asset discovery pipeline	1	44	
attack methods for passwords	5	75	
Attacking Platform as service	1	26	
Attacking With EC2	3	52	Lab3.3
AutoSSH	5	28	
AWS CLI, jq	2	26,27	
AWS Compute	3	40	Lab3.2
AWS IAM Priv Escalation IAM Passrole -25 AWS Session Tokens27	3	19	Lab3.1
AWS IAM, Access Control	2	40-48	
AWS key format	2	14	
AWS Lambda Constraints	4	56	
AWS vs Azure	2	67	
Azure cross account copies	5	70	
Azure Files (General Storage, Blob Storage), Tables,Blobgs,Q,File	2	61	
Azure Identify Services (MS AD, MS ADFS, Azure AD, Azure AD DS)	2	70	
azure pentest scope	1	32	
Azure Storage Explorer and DISM	3	74	
azure urls	1	84	

Azure VM Commands	3	84	Lab3.7
C2 (Command and Control)	5	93	
c2 architecture (Redirection Nodes, File Servers, API Gate	5	53	
Certbot	5	100	
CEWL and Custom wordlists	5	77	
cgroups			
CICD	4	22	
Cloud Native Applications	4	11	
Cloud Pentest Methodology	1	20	
Cloud Properties	1	15	
CNCF	4	12	
Code Execution on Azure VMs	3	77	Lab3.6
commonspeak2	1	93	
Compute Attack Scenarios	3	46	Lab3.3
Container Architecutre	4	101	
Containers and Microservices	4	98	
Cred Stuff Attack Tools (Hydra, Patator, Burp Suite)	5	86	
Deployment pipelines and Attacks	4	17	
dism			
dnsrecon.py	1	57	
docker swarm			
DomainFronting	5	97	
domainhunter	5	94	
Eyewitness	1	103	
GIT	4	19	
Gobuster	1	85	
Golden SAML	2	107	
GRAPH API for Search	3	15	
hydra	5	86	

inetdata	1	53	
Intrigue	1	108	
intrigue-collections	1	110	
intrigue-core			
intrigue-Ident (asset fingerprinting)	1	111	
JWT (begins with ey)	2	99	
Kube master components & architecture Kube controller manager (Node, Replication, Endpoints and token controller), Cloud controller manager, kube API server, Etcd , Kube-Scheduler, Kube Nodes (kubelet, kube-proxy, containers)	5	6	
kube-hunter -21 Peirates -22	5	21	
Kubeadm , Kubectl, Kubelet (kube control panel)	5	13	
Kuberneters and the payload	5	38	
Kubernetest types of deployments	5	12	
Lab-Azure VM's	3	75	Lab3.5
Lab-EC2 Attack Setup	3	44	Lab3.3
Lab-Microsoft Graph API	3	17	Lab3.1
Lab-PACU (Azure VMs)	3	68	Lab3.5
Lab-Socat	3	38	Lab3.2
maasscan			
Mapping in AWS and AZURE	2	11	
masscan	1	68	
Metasploit Meterpreter	5	30	
Microsoft Graph	3	10	
Mimikatz and PRT	3	5	
Mimikatz Modules- Sekurlsa, lasdump,dpapi	3	8	
msfvenom	5	35	
ngrok	1	36	
nmap	1	75	

OAuth (Scope, Auth token and Access Token)	2	89-95	
OAuth v1 vs v2	2	127	
OpenID	2	96	
PACU	3	58	Lab3.4
Passive DNS (shodan, DNSdb, InetX,Security Trails, Sonar)	1	52	
Pod.. and Privileged pods PodSec contains: container name to pull, container to various, any mounts that may exist	5	14	
Postman	2	113	
ProxyCannon-NG	5	65	
PW-Inspector	5	89	
PWD attack type (Pwd spraying vs cred stuffing acct)	5	79	
RBAC	5	18	
SAML	2	102	
Secretes format openssh	2	16	
Serverless Functions Attacks with Azure functions	4	61	
Serverless Functions Attacks with Lambda	4	53	
shimt	2	109	
socat	3	29	commands - 33
sqlmap	4	92	
SSRF	4	35	
Staged (meterpreter/reverse_http) and Stageless (meterpreter_everse_http) payload	5	33	
THC-HYDRA	5	87	
Traditional payload challenges	5	48	
url arn	2	34-35	
Web Application Injections	4	32	
web shells	5	54	
WinRM	3	83	