Subjects and Keywords	Bk	Page #	Definition
ACME and Lets Encrypt	1	51	Lets Encrypt is a free CA that implements the ACME protocol standard
Amazon ARN	2	35	Amazons own Resource Name format -- arn:paritition:service:region:account-id:resource_type/resource-id
Amazon IAM	2	39	Responsible for Authentication, Authorization, and Accounting (AAA) RBAC system - versioning permission policies, permission boundaries, access though api keys, permission groups, federation // by default DENY model
Amazon KMS	3	55	Amazon Key Management Service provides the end-user, or developer, the ability to manage cryptographic keys. KMS validates that the user has appropriate IAM role
Appendix basic info Kubernetes	1	124	Service orchestration tool for containers
Application deployment strategy	N/A	N/A	canary deployment where new version is released to subset of users, then full rollout //big bang deployment update large part of app at one time //Rolling deployment - new version is rolled out over time slowly replacing the old version //Blue\Green - new version is released alongside the old version and traffic is switched to new version
Attacker Path Utilizing Ec2	3	43	Several possible attacks are possible in Ec2
Attacker View of Kubernetes	5	11	Kubernetes API should never be exposed on the internet, older versions are not protected by RBAC, if not many RBAC suffer from insufficient privs
Attacker view of URI and RFC3986	2	33	the format followed scheme://Authority:8080/Path/query? =thisIsQuery
Attackers View of Azure AD connector	2	78	transports users and even passwords to Azure AD, this service is what is required to take an on prem AD user to exist in Azure AD
Attackers View of Identity Services in Azure	2	77	
Attackers View of Windows Functions	4	63	entire system has write access to disk on os , all functions are in D:\home\site\wwwroot\<name> , secrets are at D:\Home\data\Functions\secrets
Attacking Infrastructure as a Service	1	29	Least restrictive
Attacking Ci/CD	4	23	There are many steps The CI/CD must build an artifact and then take this artifact and do something with it. This means it must have access to repositories you may find keys for. Make sure to check environment variables - Drone directory is where drone continuous integration platform stores its configuration
Attacking Platform as a Service	1	28	Focus on the application, stop at container escapes, customer owns the app layer, almost none of the other layers.
Attacking Software as a Service	1	27	One of the most restrictive tests, goal is to gain access to admin/user accounts -- data is the main goal
Attribute-Based Access control	2	48	ABAC can provide conditional access based on tags or attributes

Subjects and Keywords	Bk	Page #	Definition
Authentication and Key Material	2	14	AWS CLI stores its creds in $HOME/.aws/credentials , AZURE is stored in $HOME/.azure
AWS Access and Restrictions	1	31	
AWS and Azure service name comparison	2	67	
AWS CLI	2	23	
AWS Compute	3	41	Ec2 the original environment with the most functionality, LightSail: a light weight environment ,less functionality than EC2, EBS - Elastic bean stalk for Ec2 and S3 deployments, this is an older technology
AWS Instance Metadata Service & Session token	3	26	Sometimes you may find exposed creds in the metadata service - with this you can create a session token, to take over with the same permission of the service
AWS Instance Metadata V2	3	28	Changes in V2. Token requests are done with a 1MS ttl, token inserted into the request in header , to obtain a token you must first request one with PUT method and ask for range of lifetime most is 6 hours,
AWS ROOT account	2	40	When you first create an Amazon Web Services (AWS) account, you begin with one identity that has complete access to all AWS services and resources account
Azure Access and Restrictions	1	33	
Azure Active Directory	2	74	Azure AD is NOT the Microsoft Active Directory system implemented in Azure. Azure AD is OAuth2 IdP with SAML support, and it is integral in providing RBAC
Azure Active Directory Domain Service	2	76	Service in which the classic AD system is delivered as a "service"
Azure Active Directory Roles	2	75	
Azure AD Administrator Roles	2	81	Global Admin starts out with access to other services, but is the highest role one can be
Azure AD Privilege Escalation	2	85	Azure AD will require that global administrators grant themselves access to azure resources, by default they do not have access
Azure AD RBAC roles	2	80	There are over 70 predefined AD RBAC roles
Azure AD Scope	2	82	If you place a user in a management group, it can manage a subscription that manages a resource group or individual resource
Azure CLI	2	50	
Azure Files	2	61	Two type of storage accounts, General and blobs. //table- NoSQL like storage, Blobs- unstructured objects of data,queus-FIFO message parsing, file storage- SMB file sharing
Azure RBAC VS Azure AD Admin	2	84	Azure RBAC roles: Manage resources like VM, Serverless functions, SQL service; while Azure AD Administrator Roles manage Azure AD services itself; it does not manage the Azure resources but can provide access to those resources

Subjects and Keywords	Bk	Page #	Definition
Azure serverless Functions	4	62	Azure functions run inside of Windows, support .NET , ship with public gateway functions and private function by default, this is different than AWS that requires setup
Azure VMs	3	71	Loosely based on Hyper-V , VMs have similar properties to AWS EC2 machines, primary management tool is RDP and PowerShell
Backdooring containers	5	27	Con: your payload can be found if the container is found - Pro:Most containers are dynamically built and destroyed, destroying evidence
Beacon Based C2	5	52	
Bearer Authentication	2	101	While JWT may push information into the browser, bearer tokens are used as leys into the system in HTTP Header - Authorization: Bearer <token>
Cloud Native Applications	4	12	CNFA have several properties - Container managed, Continuously Integrated/Continuously Tested CICD, Orchestrated and defined, Microservices Oriented (architected) , Measurable/Moveable
Code Execution on Azure - CSE	3	79	Custom Script Extension or CSE allows to run code on a remote host in Azure/// runcommand executes PowerShell// Hybrid workers automation that run PowerShell // Hybrid workers watchers using watcher task you can restore a backdoor // WinRM PowerShell remoting
Command Line Execution in a Web App	4	45	PHP-FPM, Python WSGI and .NET ASPI are interfaces allowing native execution of operating system commands
Container Architecture - Linux	4	101	
Container Architecture - Windows	4	102	
containerd	1	126	can spawn and manage containers, a daemon that manages Docker container runtime
Containers and Micro Services	4	98	
Data Pivoting Options	5	66	There are multiple ways to move data within the cloud, to you own controlled instance - AWS-Cross Account copies, IAM permissions, exfil between buckets, Azure cross account copies, smuggling with enterprise tools, OneDrive
Deployment Pipelines and Attacks	4	18	Developers can now deploy to production multiple times a day
Detecting CI/CD tools	4	22	look within some directories to find which build environment is in use - Jenkins, Travis, circleci, drone
DNS	N/A	N/A	CNAME record - used to hid a service name by making a hostname with another hostname. // A record - stores a hostname with an IPV4 address.
docker	1	127	Container management system
Dockerfile	4	104	
Domain and Host Discovery	1	49	passive techniques - cert transparency report, google cache; active techniques - Bruteforce, shuffling wordlists through dns engines
Domain Fronting	5	97	Abuse the SNI field in TLS to obfuscate the destination of your connection

Subjects and Keywords	Bk	Page #	Definition
Ec2 User Data	3	50	Ec2 can boot and automatically execute scripts //sounds like services -- PowerShell and batch, runs at boot time so can avoid AV
Exploiting Command Injections	4	47	Double encoding bypasses front end server being affected by command injection but not backend
Exposed Databased	4	68	Shodan is a tool that helps you find exposed services. There are many that have no auth on the internet
Flow Types	2	93	Oauthv1 had 3 flows, OauthV2 has 8 flow types (Authentication Code Grant - Code flow, Implicit Flow, Resource Owner pass creds, client creds, revocation flow)
Golden SAML	2	107	Allows users to create their own signed SAML authentication assertions without speaking to an IDP, in this case Active Directory
GRPc	4	16	How Native cloud applications talk - GRPC
IAM and Privilege Escalation	3	20	
IAM and User Versioning	3	24	User with the IAM:SetDefault policy set would be able to load old version of their policy and potentially priv esc that way
IAM policy example	2	43	
IAM:Passrole	3	25	If a user has this permission and they can attach a role policy to a service, they may be able to use it as a pivot to their target
Identity types on AWS - POLICIES	2	42	Several IAM policies that can be leveraged in AWS -- Identity policies, Resource policies, IAM permission boundary, service control, access control, session policy
Identity vs Resource Policy	2	45	IAM has the ability to provide access to a user, group , or role (identity) and the resource can also provide access
Implanting an EC2 environment	3	49	add user data to make a reverse shell from the bastion host to your external C2. //needed permission ec2:stopInstances, ec2:startInstances, ec2:ModifyUserData
IP Addressing and Hosts	1	66	IP addressing is not useless in cloud; can look at PRT records to get hostname; some resources may not be available unless you are coming from a specific IP
JMESPATH Queries	2	53	A specification that allows for the querying of JSON objects , different from jq as it is NOT a command line tool
JSON Web Token (JWT)	2	99	Attacking JWT in the wild, normally means using a weak password so an attacker can brute force it, using public key to sign a new JWT and switch algorithm
Kubernetes	5	5	Open source system for automating deployment of containers -> Kubernetes Cluster -> worker ode -> pods -> container lives in pods, kublet an agent that runs on each node in the cluster
Kubernetes and Meterpreter	5	36	1. create an evil payload 2. create a docker file that runs the payload 3.push this container into a repository

Subjects and Keywords	Bk	Page #	Definition
Kubernetes components	N/A	N/A	kubelet - agent that takes in items from the Kubernetes API that works on the nodes. //kube-proxy - designed to move traffic from one container to another without using worker nodes directly // kubeadm- main administrative tool that control the cluster //kubectl - control software that can copy files, execute binary, on containers action and service mesh
Kubernetes Control Planes	5	13	
Kubernetes RBAC	5	18	
Kubernetes Types of Deployments	5	12	Several deployment options exist for Kubernetes - Completely cloud managed, cloud turn key, on prem, and custom
lab 2.2 Using AWS CLI	6	81	the aws access key ID is like a username, the aws secret key access is like password.
lab 2.3 Using Azure CLI	6	87	
lab 2.4 looking for unauth file shares	6	98	You can use a tool called storage Explorer to mount shares in Azure
lab 2.5 HTTP and Postman Tour	6	101	
Lab 3.1 Microsoft Graph API	6	110	An API that allows programmatic access to Microsoft cloud services- in lab we used it to fetch emails and found ssh key
lab 3.2 socat	6	119	
lab 3.3 Ec2 Attack Setup	6	128	steps- 1.Find keys in source / 2.Use keys to enumerate AWS /3.List permissions /4.RunInstance w/ permissions for S3
lab 3.4 Attacking with EC2	6	138	use another token to decrypt KMS , steal more keys and login as a new user with more access
lab 3.5 pacu lab	6	146	Pacu will automate the enumeration, exploitation, and discovery of services in Amazon Web Services (AWS), we will weaponize the keys we found
lab 3.6 Azure VMs	6	162	Shows how storage and backup operations can be abused to gain unauthorized access to a system
lab 3.7 running commands in Azure VM	6	177	run-command, and multiple az commands
lab 4.1 backdoor CI/CD Pipelines	6	185	
lab 4.2 SSRF Attack Lab	6	197	
lab 4.3 command injection lab	6	203	
lab 4.4 serverless labs	6	215	upload a NodeJS function that will give us a full file shell
lab 4.5 Databases and Exposed Ports	6	221	
lab 4.6 SQL injection in RDS	6	231	
lab 5.1 Kubernetes and Peirates	6	239	

Subjects and Keywords	Bk	Page #	Definition
lab 5.2 backdooring containers	6	250	
lab 5.3 Heavy and light web shells	6	265	
lab 5.4 Credential Stuffing	6	279	cred stuffing is using creds exposed in a data breach
lab 5.5 domain fronting	6	286	Domain Fronting is a cloud c2 detection avoidance technique that utilizes the SNI header
Mapping URLs	1	84	AWS naming convention for URLs protocol://service-code. Region-code.amazonaws.com. ; AZURE keyword.file.core.windows.net
Mapping Workflow/tips	2	8	Consider connecting to the *aaS vendor and using APIs to pull down all assets than an org has
Metadata V2 Token Protections	4	40	Create a put request to obtain a TOKEN value can have a TTL 21600 seconds or 6 hours -- before using the GET statement, request TTL of 1ms, must have a token in the header
Microsoft Active Directory Federation Service	2	73	Requires access to DC designed for DMZ Microsoft AD Federation Service allowed third part users the ability to authenticate and authorize what resources they should have access to
Microsoft Graph API	3	11	Microsoft Graph provides users of Microsoft services a singular API to talk to
Microsoft Identity Services	2	70	Microsoft Identity services- Microsoft Active Directory, Microsoft Active Directory Federation Services, Azure Active Directory, Azure Active Directory Domain Services
MongoDB cheat sheet	4	79	Uses BSON syntax to query - Amazon DocumentDB is a fork of it
NodeJS Lambda	4	57	
NoSQL	4	72	
Oauth and Bearer authentication	2	90	Provides access to systems on the web without asking for a username and password
Obfuscation of C2 Infrastructure	5	93	Using CDN network to hide traffic, using well known sites to disguise attacks, Using cloud proxies and load balancers
Open ID Connect	2	96	
Open Source Databases	1	54	Tools like Shodan, DNSdb, Intelx, Security trails, Project Sonar can be used for Passive host discovery
Pass the PRT Attacks	3	9	Similar to PTH attack, if an attacker can construct a request to the CloudAP service, then a JWT will be returned
Passive Technique - Cert Transparency	1	50	list of every TLS certificate created to be used to validate certificates in browsers - pay attention to Subject Alternative Name or SAN it has CN of other hosts
Password Attack Types and Methodology	5	79	Bruteforce, Dictionary attack, password spraying, Credential stuffing (needs target org user and pass)
Password Attacks	5	74	example attacks - use token to bypass authentication such as caputring certs api tokens, attempt to logon to live system, crack hashes, MitM
Payloads and Payload Selection	5	48	
Pivoting with HTTP	5	102	place a php file on DMZ, victim and threat actor both connect to the PHP file

Subjects and Keywords	Bk	Page #	Definition
Pods and Podsec	5	14	Smallest workload unit in a Kubernetes clusters, composed of a single or multiple container, PODSEC contains information on how to run a pod
Policy Boundary	2	46	These are permissions that can NOT be overridden at all, no matter how much power the account has
Policy for services	2	47	IAM also restricts what services can call on what other services
Red Team and Exploitation	5	43	Cloud can help us scale our RT operations, also it is difficult to block cloud service providers
Red Team Ops in the Cloud	5	63	
Redis labs	4	71	
Redis-CLI	4	73	set <hash> superuser - change the key value to superuser
runc	1	125	a lightweight container runtime that talks directly to the kernel
SAML	2	102	Identifying SAML Protocols utilized for authentication //Name Identifier Protocol - Artifact Resolution Protocol etc.
SANs Cloud Penetration Testing Methodology	1	21	More steps than the traditional methodology. Recon/Data collect, Data analysis, Scanning, Vuln Discovery, Exploitation, post ex recon, persist/pivot, Lesson learned
Serverless Function Attacks with Lambda	4	54	It is possible to get command injection in Lambda, these are basically functions that run on a per cost basic, they normally spin down after 15 minutes
Shared Responsibility and Pen Testing	1	26	Identifies what is owned by the customer and what is owned by the service provider
SQL Injection	4	86	
SQL injection defenses	4	95	Use an ORM if that is not an options use prepared statements - ORM can be slow and inefficient. ORM do not tie the entire system to a single DB structure, dev can move from 1 db to another without rewriting queries, safe way of handling strings
SQL vs MongoDB primer	4	77	SQL uses Select From Where, Mongo DB uses a JSON array like structure -> class, location, Method, Filter
SSRF	4	36	SSRF are very popular in cloud applications because resources are normally hosted in other remote locations
Statically complied binary	5	49	
Subset of useful strings to look for	2	18	YAML format and .env/TOML format
Terms of Service and Demarcation Points	1	25	What is in scope and out of scope in cloud tests
Types of Clouds	1	24	Software as a Service - You can access the software through proper channels ; Platform a s Service - Restriction on escaping the environment; Infra as service-Least restrictive

Subjects and Keywords	Bk	Page #	Definition
URI components	N/A	N/A	scheme: the service can be http:// or other // Authority: domain or location where resource is being identified // Path: these. route or path where resource are found //Query: typically a key value pair in which the component is a sink that we can manipulate. // Fragment: typically only used on application that are heavily client focused
URI URL AND URNS	2	34	
Useful commands for injection	4	50	set command will list Azure Functions environment -- & means run command at same time - &&means run second command after first command successfully runs
Username harvesting in the Cloud	2	56	We get different error messages depending on error, this allows the attacker ability to get valid username// i.e. different error message for wrong user or domain
Using Port proxies with built in tools	3	35	Linux- Iptables, nftables and Nat functionality // Windows - netsh and port proxy // cross platform-Apache, nginx, pther web server
Web shells	5	54	There are heavy web shells that entire functionality lives on the web server - There are Light web shells that the whole shell is sent each time
Working with Disks in Azure	3	73	Azure RBAC may restrict an attacker from interacting with a VM directly; attack can directly interact with it's disk witch in turn interacts with the VM