Cloud Security Cheatsheet (CEH v13)

# 1. Reconnaissance & Enumeration (Cloud-Specific)

• CloudEnum → Finds valid cloud storage accounts (AWS, Azure, GCP).

python3 cloud\_enum.py -k <keyword>

• S3Scanner → Detects open/accessible AWS S3 buckets.

s3scanner.py buckets.txt

• GCPBucketBrute → Brute-forces Google Cloud Storage buckets.

python gcpbucketbrute.py -k <keyword>

# 2. Cloud Vulnerability Scanning

• ScoutSuite → Multi-cloud security auditing (AWS, Azure, GCP).

scout aws --report-dir scoutsuite-report

• Prowler → AWS security best practices & CIS benchmark checks.

./prowler -M csv,json

• CloudSploit → Security scanning for misconfigurations.

./cloudsploit scan --config aws.json

# 3. Cloud Exploitation & Attack Simulation

• Pacu (AWS Exploitation Framework) → Post-exploitation framework for AWS.

pacu  
run ec2\_\_enum  
run iam\_\_privesc\_scan

• CSRF & Token Hijacking (Burp Suite) → Stealing session tokens from misconfigured cloud apps.

Manual via Burp Suite

• Man-in-the-Cloud (MitC) Attack → Abuse of cloud sync tokens (Dropbox, Google Drive, OneDrive).

MitC attack toolkit

# 4. Cloud Security Controls & Defense Tools

• AWS CLI → Manage AWS resources & IAM securely.

aws iam list-users  
aws s3 ls  
aws configure

• Azure CLI → Manage Azure resources.

az account list  
az storage blob list --container-name <container>

• GCP CLI → Manage Google Cloud resources.

gcloud projects list  
gcloud storage buckets list

# 5. Monitoring & Logging

• AWS CloudTrail / GuardDuty → Activity logging & threat detection.

• Azure Monitor / Security Center → Event collection & alerts.

• GCP Security Command Center → Threat insights for cloud resources.

# 6. Cloud Best Practices (Quick Recall)

• Enable MFA → Always enable MFA on IAM users.

• Encrypt Data → Encrypt data (S3, EBS, RDS, GCP buckets, Azure blobs).

• Security Controls → Use security groups, firewalls, WAF.

• Key Rotation → Rotate keys & avoid embedding them in code.

• Monitoring → Enable monitoring (CloudTrail, GuardDuty, SIEM).

• Backup & Recovery → Backup & disaster recovery tested regularly.