- Filename: eccouncil-ceh31250-v11-19-3-1-hacking-cloud-services.md
- Show Name: CEHv11 (312-50)
- Topic Name: Cloud Computing - Cloud Computing
- Episode Name: Hacking Cloud Services
===

Hacking Cloud Services

Objectives:

- Cloud Vulnerability Scan

    - Trivy
    - Clair
    - Dadga
    - Twistlock
    - Kubernetes

        - Sysdig
        - etcd process enumeration

            - key storage
            - API objects
            - Config files
            - Open ports

- S3 Discovery and Enumeration

    - Check source code for S3
    - Brute-Force

        - Attack proxy
        - BucketKicker

            - https://github.com/craighays/bucketkicker

        - s3scanner

            - https://pypi.org/project/S3Scanner/

    - S3 Inspector

        - https://github.com/clario-tech/s3-inspector
        - Enumerates

            - Bucket permissions
            - Public/Private status

- AWS enumeration

    - Account IDs

        - Github
        - AWS Error messages
        - Public AMIs
        - People posting on social or in help forums

    - IAM Roles and Creds

        - Find Keys here

            - Git Repo
            - Social Engineering

- Password Reuse
    - Login to AWS and download keys
- Vulnerable App hosted in AWS
    - SSRF
- 3rd-Party cloud management app
- Insider Threat
- IAM Role Misconfiguration
    - PACU (Rhino Security Labs)
        - https://rhinosecuritylabs.com/aws/pacu-open-source-aws-exploitation-framework/
    - CloudGOAT 2
        - https://rhinosecuritylabs.com/aws/introducing-cloudgoat-2/
  - AWS-Pwn
    - https://github.com/dagrz/aws_pwn
- AWS IAM Priv Esc Techniques
  - Create an EC2 instance with existing EC2 profile
    - Needs access to
      - `iam:PassRole`
      - `ec2:RunInstances`
    - Attacker then accesses the OS and looks for AWS keys in metadata
  - Create a new policy version
    - Set custom permissions
    - `--set-as-default` flag
  - Add user to group
    - `iam:AddUserToGroup` permission
      - Add account to existing group
        - User inherits group permissions