ScoutSuite AWS Security Assessment Summary

# EC2

* \*\*Findings:\*\*
* - EBS Volume Not Encrypted
* - Security Group Opens All Ports to All
* - Security Group Opens SSH Port to All
* - EBS Encryption By Default Is Disabled
* - Non-empty Rulesets for Default Security Groups
* - Security Group Opens All Ports
* - Unrestricted Network Traffic within Security Group
* - Default Security Groups in Use
* - Potential Secret in Instance User Data
* - Security Group Allows ICMP Traffic to All
* - Security Group Opens DNS Port to All
* - Security Group Opens FTP Port
* - Security Group Opens MongoDB Port to All
* - Security Group Opens MsSQL Port to All
* - Security Group Opens MySQL Port to All
* - Security Group Opens NFS Port to All
* - Security Group Opens Oracle DB Port to All
* - Security Group Opens PostgreSQL Port to All
* - Security Group Opens RDP Port to All
* - Security Group Opens SMTP Port to All
* - Security Group Opens TCP Port to All
* - Security Group Opens Telnet Port
* - Security Group Opens UDP Port to All
* - Security Group Uses Port Range
* - Security Group Whitelists AWS CIDRs
* - Unused Security Group
* - EBS Snapshot Not Encrypted
* - Public EBS Snapshot
* - Publicly Accessible AMI
* \*\*Recommendation:\*\*
* Restrict security groups to only required ports and IPs. Enable encryption for all EBS volumes and snapshots. Avoid public AMIs and secrets in user data.

# IAM

* \*\*Findings:\*\*
* - Managed Policy Allows All Actions
* - Minimum Password Length Too Short
* - Password Expiration Disabled
* - Password Policy Allows the Reuse of Passwords
* - Passwords Expire after 90 Days
* - Root Account Used Recently
* - Root Account without Hardware MFA
* - Root Account without MFA
* - AssumeRole Policy Allows All Principals
* - Credentials Unused for 90 Days or Greater Are Not Disabled
* - Cross-Account AssumeRole Policy Lacks External ID and MFA
* - Lack of Key Rotation for 90 Days (Key Status: Active)
* - Lack of Key Rotation for 90 Days (Key Status: Inactive)
* - Managed Policy Allows 'iam:PassRole' For All Resources
* - Managed Policy Allows 'NotActions'
* - Managed Policy Allows 'sts:AssumeRole' For All Resources
* - Managed Policy Not Attached to Any Entity
* - Policy with Denied User Actions for Group Objects
* - Role with Inline Policies
* - Root Account Has Active Keys
* - Root Account Has Active X.509 Certs
* - User with inline Policies
* - User with Multiple API Keys
* - User with Password and Keys Enabled
* - User without MFA
* - Group with Inline Policies
* - Group with No Users
* - Inline group Policy Allows 'iam:PassRole' For All Resources
* - Inline group Policy Allows 'NotActions'
* - Inline group Policy Allows 'sts:AssumeRole' For All Resources
* - Inline role Policy Allows 'iam:PassRole' For All Resources
* - Inline role Policy Allows 'NotActions'
* - Inline role Policy Allows 'sts:AssumeRole' For All Resources
* - Inline user Policy Allows 'iam:PassRole' For All Resources
* - Inline user Policy Allows 'NotActions'
* - Inline user Policy Allows 'sts:AssumeRole' For All Resources
* - Unused Role for EC2 Service
* \*\*Recommendation:\*\*
* Enforce strong password policies, enable MFA for all users, rotate keys regularly, and avoid overly permissive policies.

# VPC

* \*\*Findings:\*\*
* - Network ACLs Allow All egress Traffic (default)
* - Network ACLs Allow All ingress Traffic (default)
* - Subnet with 'Allow All' egress NACLs
* - Subnet with 'Allow All' ingress NACLs
* - Subnet without a Flow Log
* - Network ACLs Allow All egress Traffic (custom)
* - Network ACLs Allow All ingress Traffic (custom)
* - Unused Network ACLs
* - Routing Table with VPC Peering
* \*\*Recommendation:\*\*
* Tighten NACL rules to least privilege, enable VPC flow logs, and review routing configurations and unused resources.

# Config

* \*\*Findings:\*\*
* - AWS Config Not Enabled
* \*\*Recommendation:\*\*
* Enable AWS Config to continuously monitor and record AWS resource configurations.

# CloudTrail

* \*\*Findings:\*\*
* - CloudTrail Service Not Configured
* \*\*Recommendation:\*\*
* Enable CloudTrail in all regions to track and log account activity.