AWS re:Start

LAB

Network Hardening

Securing an infrastructure can be a challenge for any company. Companies use many tools to audit networks and find vulnerabilities in systems and applications. This process takes significant time and effort.

In this lab, you are a new security engineer for Any Company. You need to identify weak areas in the company's network security and update Any Company’s environment for better efficiency and optimization. You will use Amazon Inspector to do this.

Amazon Inspector runs scans that analyze all your network configurations—such as security groups, network access control lists (network ACLs), route tables, and internet gateways—together to infer reachability. You don't need to send packets across the virtual private cloud (VPC) network or connect to Amazon Elastic Compute Cloud (Amazon EC2) instance network ports. It’s like pocketless network mapping and reconnaissance.

From Amazon Inspector, you will use the network reachability package to analyze your network configurations to find security vulnerabilities in your EC2 instances. The findings that Amazon Inspector generates also provide guidance about restricting access that is not secure.

aws re/start