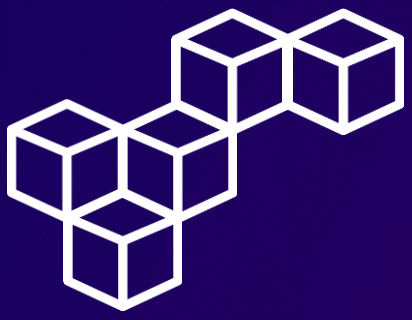
AWS re:Start LAB

Network Hardening

WEEK 4

aws re/start



Overview

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 AnyCompany. You need to identify weak areas in the company's network security and update AnyCompany'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 packetless network mapping and reconnaissance.

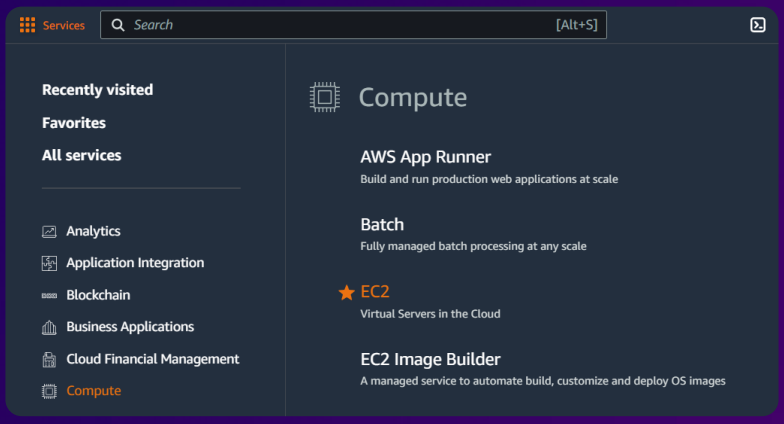
From Amazon Inspector, you will use the **network reachability package** to analyze your network configurations to find security vulnerabilities in your EC2 instances. The findings that Amazon Inspector generates also provide guidance about restricting access that is not secure.

Task 1

View EC2 instances and add tags

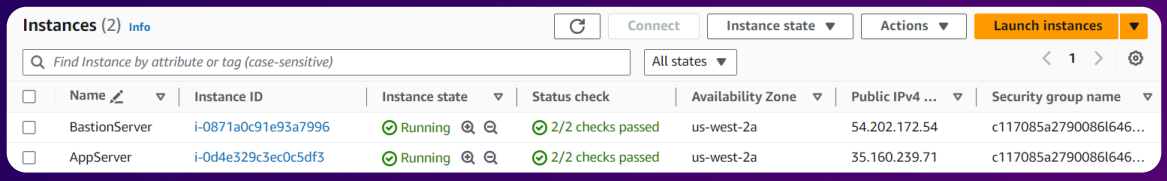
Step 1: Access the EC2 Management Console

Open the AWS Management Console, and select EC2.



Step 2: Review running instances

Navigate to the **Instances** section. The running BastionServer and AppServer EC2 instances are listed.



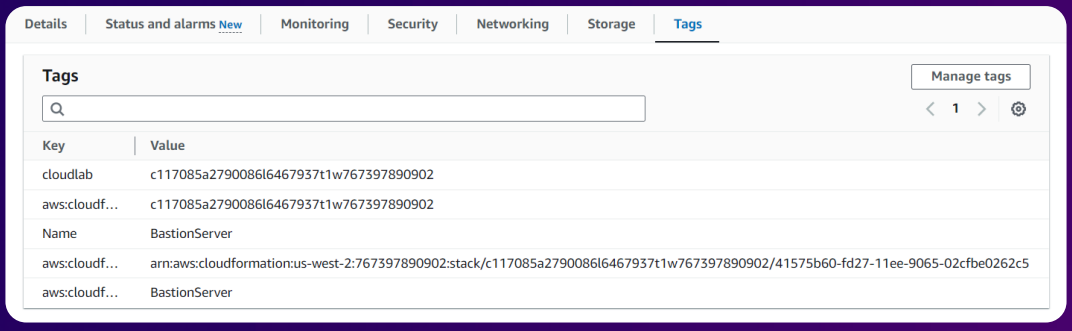
aws re/start

Task 1

View EC2 instances and add tags

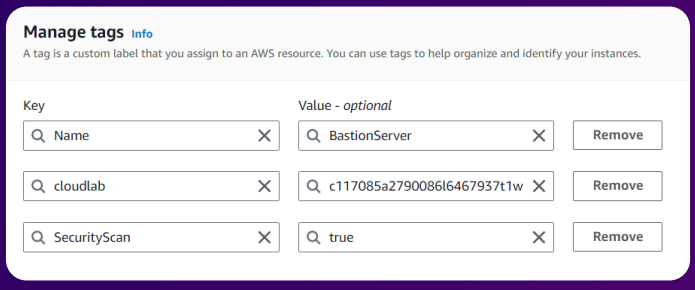
Step 3: Manage instance tags

Select the BastionServer instance and go to the **Tags** tab, then select Manage tags.



Step 4: Add a tag to an instance

Add a new tag with the key SecurityScan and the value true.



aws re/start

Task 2

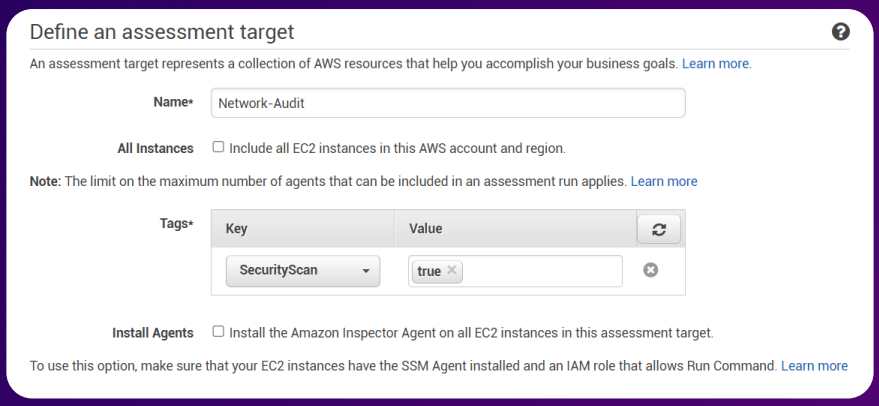
Configure and run Amazon Inspector

Step 1: Access Amazon Inspector Classic

On the AWS Management Console, navigate to the **Amazon Inspector** service, choose Switch to Inspector Classic, click on Get started and select Advanced setup.

Step 2: Define an assesment target

In the **Define an assessment target** section, configure the following options.



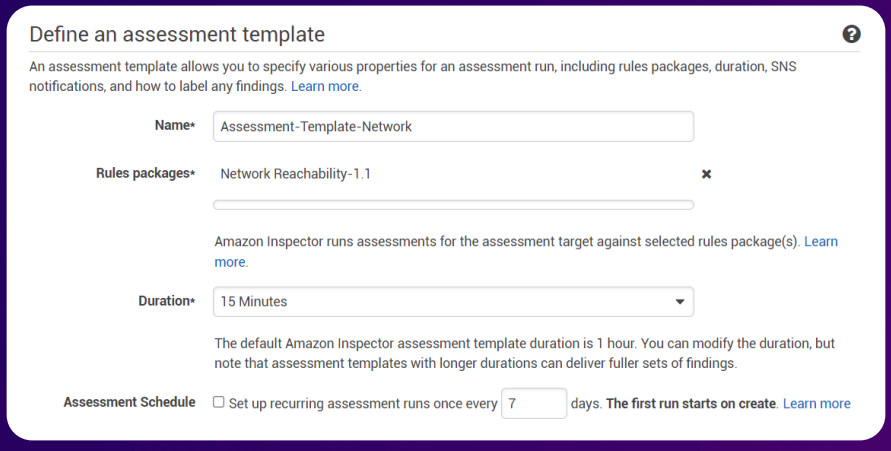
aws re/start

Task 2

Configure and run Amazon Inspector

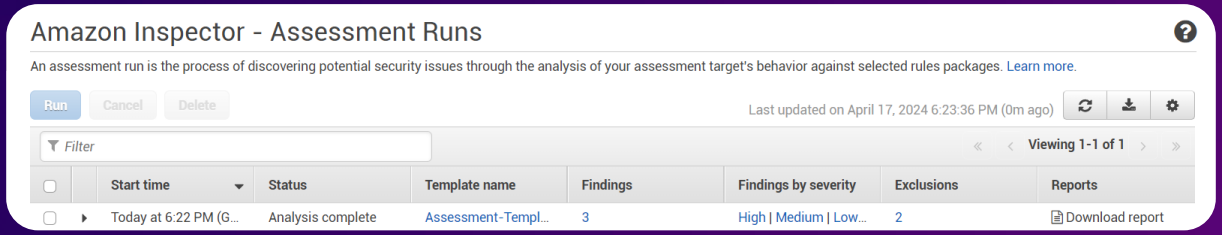
Step 3: Define an assessment template

In the **Define an assessment template** section, configure the following options.



Step 4: Create the assesment

Review the setup and choose Create. Once the Assessment Run status changes to Analysis complete, go to **Findings**.



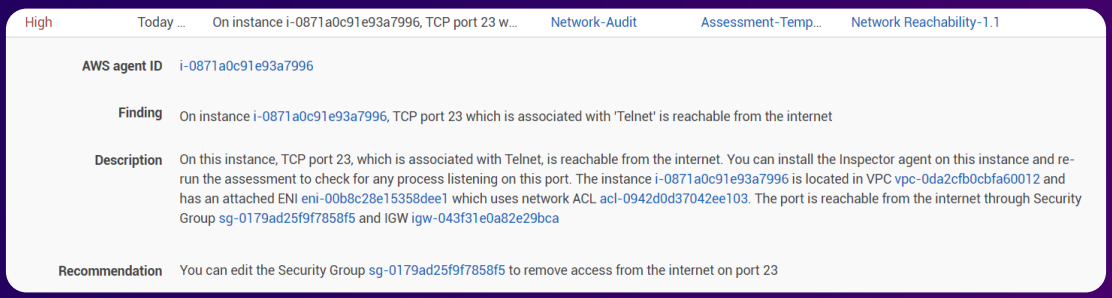
aws re/start

Task 3

Analyze Amazon Inspector findings

Review the high-severity finding

Expand the high-severity finding and review key details.



Review the medium-severity finding

Expand the medium-severity finding and review key details.

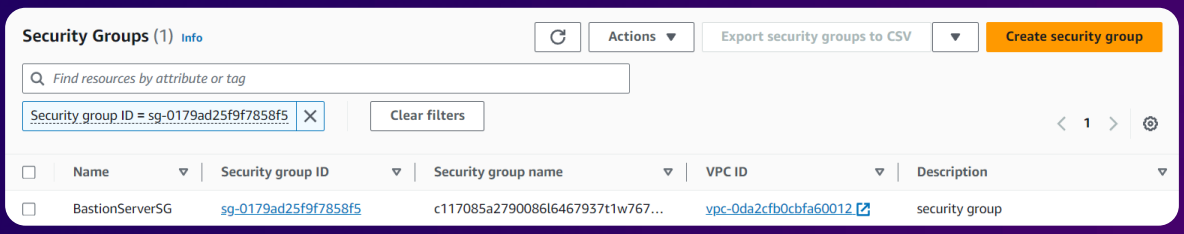
aws re/start

Task 4

Update security groups

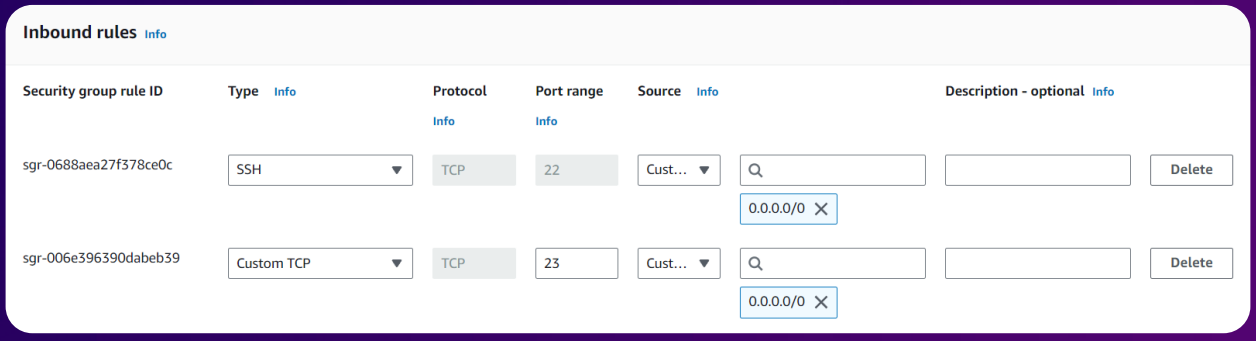
Step 1: Follow the Recommendation link

On the high-severity finding, follow the Recommendation link to the security group attached to the BastionServer instance.



Step 2: Check current inbound rules

Select the **Inbound rules** tab of the BastionServerSG security group and click on Edit inbound rules.



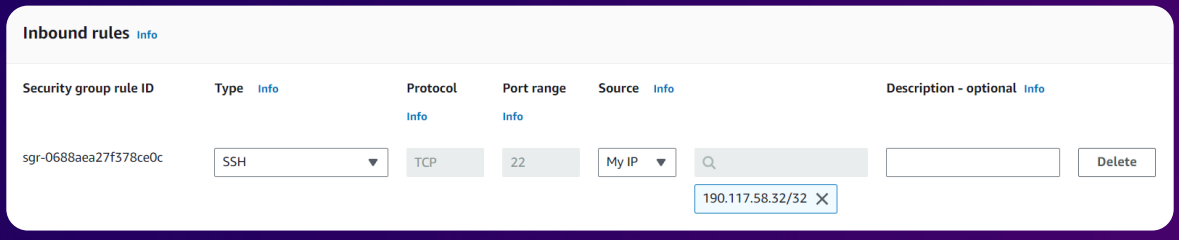
aws re/start

Task 4

Update security groups

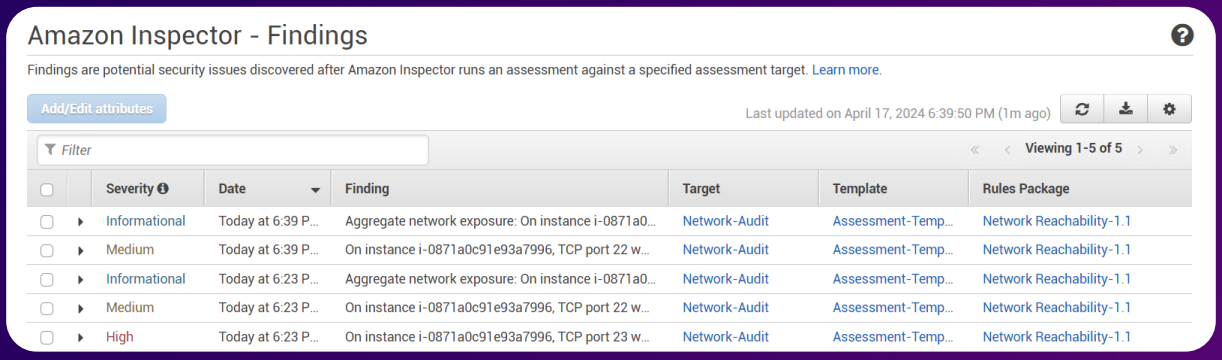
Step 3: Edit inbound rules

Delete the inbound rule associated with port range 23 and change the Source of the SSH rule to My IP.



Step 4: Re-scan the environment

Re-run the assessment and go to **Findings**. The high-severity finding is now gone, but the medium-severity finding remains.



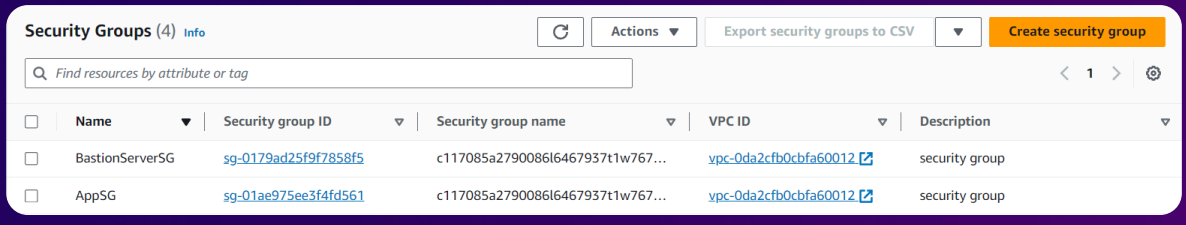
aws re/start

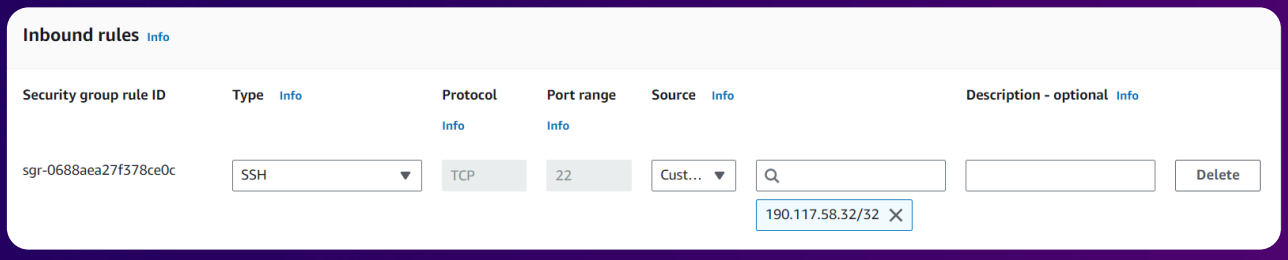
Task 5

Replace BastionServer with Systems Manager

Step 1: Edit inbound rules

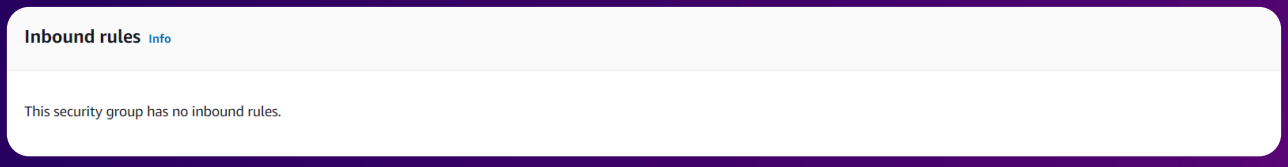
In the EC2 dashboard, go to **Security Groups**. Select the BastionServerSG security group and choose Edit inbound rules.





Step 2: Remove the SSH inbound rule

Delete the SSH rule of the BastionServerSG security group.



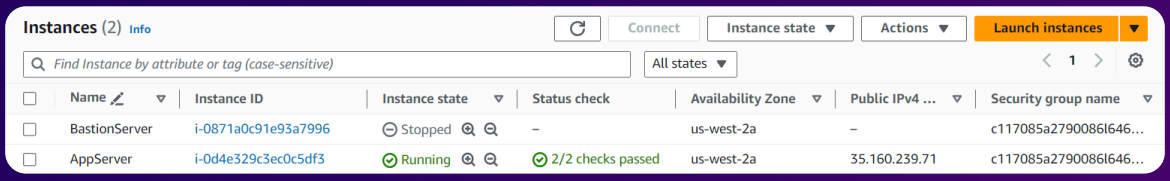
aws re/start

Task 5

Replace BastionServer with Systems Manager

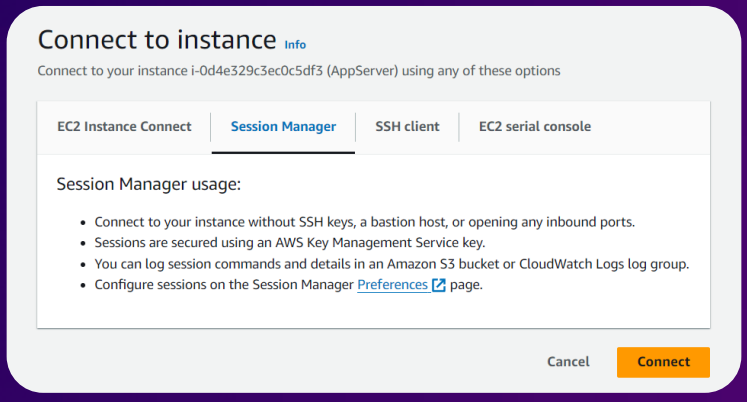
Step 3: Stop the BastionServer instance

Go to the **Instances** section and stop the BastionServer instance.



Step 4: Connect to the AppServer instance

Connect to the AppServer instance using Session Manager.



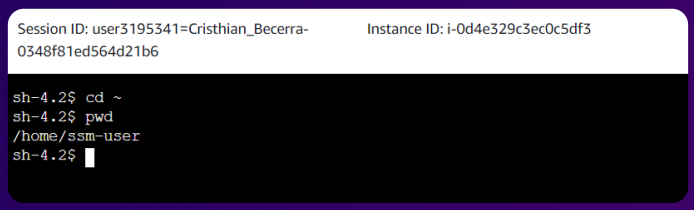
aws re/start

Task 5

Replace BastionServer with Systems Manager

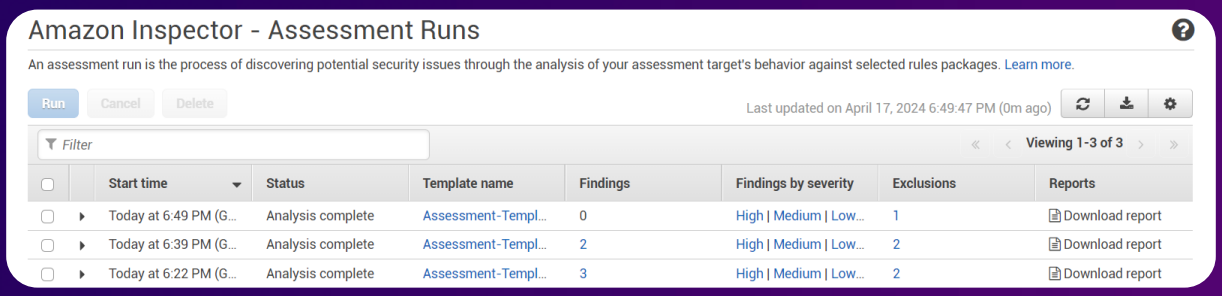
Step 5: Run commands in the Session Manager

Enter the commands cd ~ and pwd to change the directory and to view the current working directory of the AppServer.

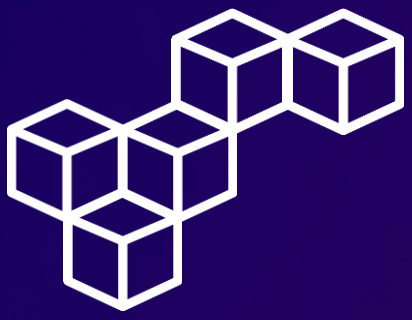


Step 6: Final scan of the environment

Re-run the assessment and verify that there are zero Findings.



aws re/start



Conclusions

Network Hardening
Network hardening enhances security by implementing robust measures like firewall rules and access controls.

Amazon Inspector
Amazon Inspector automates security assessments to identify vulnerabilities and compliance issues within AWS resources.

Amazon Inspector Classic
Amazon Inspector Classic focuses on security assessments for EC2 instances and applications, offering a detailed analysis of vulnerabilities and compliance issues within AWS environments.

Amazon Inspector Assessments
Amazon Inspector assessments provide actionable insights to improve security posture and meet regulatory requirements.

Amazon Inspector Findings
Amazon Inspector findings highlight specific security issues, enabling targeted remediation efforts.

Connecting to instances using Session Manager
Connecting to instances using Session Manager enhances security by providing secure, auditable access without the need for direct SSH access.

aws re/start

Cristhian Becerra

cristhian-becerra-espinoza

+51 951 634 354

cristhianbecerra99@gmail.com

Lima, Peru