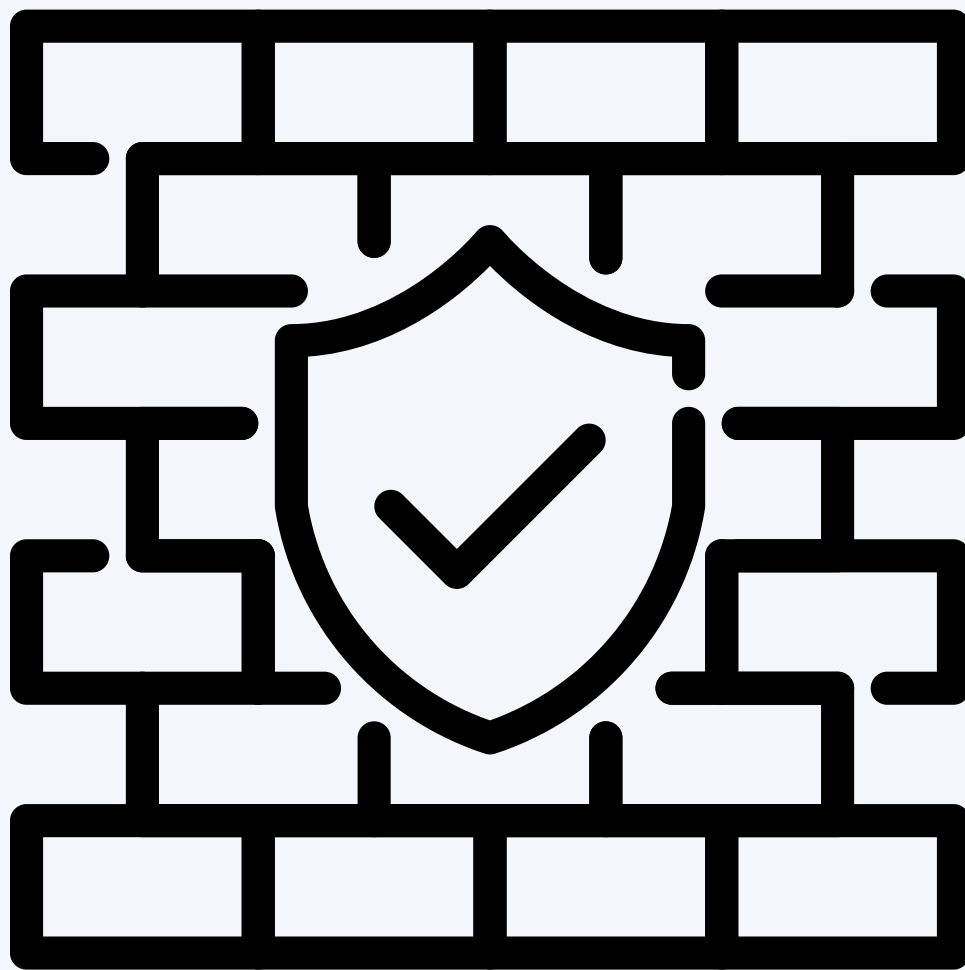




23°

Lab - AWS re/Start

Endurecimiento de red





Protegiendo redes con Amazon Inspector y Systems Manager

A continuación, se muestra los objetivos del laboratorio:

- Configurar Amazon Inspector
- Ejecutar una auditoría de red sin agente.
- Investigar los resultados del análisis
- Actualizar grupos de seguridad
- Inicie sesión en una instancia del servidor de aplicación usando AWS Systems Manager Session Manager

Nota. Utilizamos Amazon Inspector para analizar todas las configuraciones de red como grupos de seguridad, listas de control de acceso de red, tablas de enrutamiento, puertas de enlace de internet, pero sin la necesidad de enviar paquetes a través de la red de la VPC o conectarse a los puertos de la instancia de EC2.

Tarea 01



En el entorno del lab tenemos dos instancias EC2: *BastionServer* (subred pública) y *AppServer* (subred privada). Para que Amazon Inspector pueda evaluar las instancias EC2, lo primero que debes hacer es *tagear* a aquellas que quieres como *target*.

EC2 > Instances > i-01a70cdf441432c60 > Manage tags

Manage tags [Info](#)

A tag is a custom label that you assign to an AWS resource. You can use tags to help organize and identify your instances.

Key	Value - optional	
<input type="text" value="Name"/>	<input type="text" value="BastionServer"/>	<button>Remove</button>
<input type="text" value="SecurityScan"/>	<input type="text" value="true"/>	<button>Remove</button>

Add new tag

You can add up to 48 more tags.

Después de esto, procedemos a configurar Amazon Inspector. Empezamos definiendo el *target de evaluación*, en este caso la instancia EC2 *BastionServer*. Esto debido a que tiene el tag *SecurityScan* en *true*.

Define an assessment target

An assessment target represents a collection of AWS resources that help you accomplish your business goals. [Learn more.](#)

Name*

All Instances ☐ Include all EC2 instances in this AWS account and region.

Note: The limit on the maximum number of agents that can be included in an assessment run applies. [Learn more](#)

Tags*

Key	Value	
<input type="text" value="SecurityScan"/>	<input type="text" value="true"/>	<button>✕</button>
<input type="text" value="Add a new key"/>		

Install Agents ☐ Install the Amazon Inspector Agent on all EC2 instances in this assessment target.

To use this option, make sure that your EC2 instances have the SSM Agent installed and an IAM role that allows Run Command. [Learn more](#)

Tarea 01



Ahora, procedemos a definir la *Plantilla de evaluación*. En este caso solo nos concentraremos en el análisis del acceso a la red: *Network Reachability-1.1*

Define an assessment template ?

An assessment template allows you to specify various properties for an assessment run, including rules packages, duration, SNS notifications, and how to label any findings. [Learn more.](#)

Name*

Rules packages* ×

Amazon Inspector runs assessments for the assessment target against selected rules package(s). [Learn more.](#)

Duration*

The default Amazon Inspector assessment template duration is 1 hour. You can modify the duration, but note that assessment templates with longer durations can deliver fuller sets of findings.

Assessment Schedule ☐ Set up recurring assessment runs once every days. **The first run starts on create.** [Learn more](#)

Así quedaría la configuración del análisis con Inspector:

Review ?

Review the details of your target and template, and then choose **Create**.

Define an assessment target Edit

Name Network-Audit

Tags

Key	Value
<input type="text" value="SecurityScan"/>	<input type="text" value="true"/>

Install Agents ☐ Install the Amazon Inspector Agent on all EC2 instances in this assessment target.

To use this option, make sure that your EC2 instances have the SSM Agent installed and an IAM role that allows Run Command. [Learn more](#)

Define an assessment template Edit

Name Assessment-Template-Network

Rules packages [Network Reachability-1.1](#)

An assessment run requires the AWS agent to run on all EC2 instances that comprise your assessment target. If you have not yet deployed the AWS agent, you can create the assessment template, but remember to [install AWS agents](#) before you run the assessment.

[Cancel](#) [Preview](#) [Previous](#) [Create](#)

Tarea 01



Después de que el análisis ha sido completado, podemos ver los *resultados(findings)*. A continuación, se muestran los resultados de *severidad alta (High Severity)*

Finding for assessment target 'Network-Audit' and template 'Assessment-Template-Network'	
ARN	arn:aws:inspector:us-west-2:252526466788:target/0-bmjxAaNq/template/0-kGgPs5ad/run/0-uQjbMGza/finding/0-iAmrizLX
Run name	Run - Assessment-Template-Network - 2024-01-30T05:33:40.090Z
Target name	Network-Audit
Template name	Assessment-Template-Network
Start	Today at 12:33 AM (GMT-5) (7 minutes ago)
End	Today at 12:34 AM (GMT-5) (6 minutes ago)
Status	Analysis complete
Rules package	Network Reachability-1.1
AWS agent ID	i-01a70cdf441432c60
Finding	On instance i-01a70cdf441432c60 , TCP port 23 which is associated with 'Telnet' is reachable from the internet
Severity	High ⓘ
Description	On this instance, TCP port 23, which is associated with Telnet, is reachable from the internet. You can install the Inspector agent on this instance and re-run the assessment to check for any process listening on this port. The instance i-01a70cdf441432c60 is located in VPC vpc-09674d9f767dfd16c and has an attached ENI eni-008c7c6941b6a33f0 which uses network ACL acl-0f035762742c3181f . The port is reachable from the internet through Security Group sg-0c8cf9a42fcae9257 and IGW igw-038f0a0c68036d31d
Recommendation	You can edit the Security Group sg-0c8cf9a42fcae9257 to remove access from the internet on port 23

Y el de *severidad media*:

Finding for assessment target 'Network-Audit' and template 'Assessment-Template-Network'	
ARN	arn:aws:inspector:us-west-2:252526466788:target/0-bmjxAaNq/template/0-kGgPs5ad/run/0-uQjbMGza/finding/0-KQ9xUhj5
Run name	Run - Assessment-Template-Network - 2024-01-30T05:33:40.090Z
Target name	Network-Audit
Template name	Assessment-Template-Network
Start	Today at 12:33 AM (GMT-5) (8 minutes ago)
End	Today at 12:34 AM (GMT-5) (7 minutes ago)
Status	Analysis complete
Rules package	Network Reachability-1.1
AWS agent ID	i-01a70cdf441432c60
Finding	On instance i-01a70cdf441432c60 , TCP port 22 which is associated with 'SSH' is reachable from the internet
Severity	Medium ⓘ
Description	On this instance, TCP port 22, which is associated with SSH, is reachable from the internet. You can install the Inspector agent on this instance and re-run the assessment to check for any process listening on this port. The instance i-01a70cdf441432c60 is located in VPC vpc-09674d9f767dfd16c and has an attached ENI eni-008c7c6941b6a33f0 which uses network ACL acl-0f035762742c3181f . The port is reachable from the internet through Security Group sg-0c8cf9a42fcae9257 and IGW igw-038f0a0c68036d31d
Recommendation	You can edit the Security Group sg-0c8cf9a42fcae9257 to remove access from the internet on port 22



Tarea 01



Vamos a hacer las respectivas correcciones en las reglas de entrada en los puertos 22 y 23 del grupo de seguridad de la instancia. Esto debido a que *Telnet* es vulnerable a ataques de seguridad y el hecho de cualquier dirección IP pueda conectarse a nuestra instancia EC2 via el puerto 22 es inseguro, por lo que solo permitiremos la conexión a nuestra instancia si es que el origen es nuestra dirección IP.

EC2 > Security Groups > sg-0c8cf9a42fcae9257 - LabStack-783c9c4b-e126-4728-9951-0a7c5c23e5f5-8tPfwWg62884nYPaMVsURv-0-BastionSG-11931A6C2SXSO > Edit inbound rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules [Info](#)

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
sgr-0f9aca90709afa45f	SSH	TCP	22	My IP		Delete
				38.250.129.130/32		

Add rule

Esto hace que el resultado de severidad alta sea superado, sin embargo, el de severidad media persiste puesto que el puerto 22 está técnicamente abierto al internet fuera de la VPC.

Amazon Inspector - Findings ?

Findings are potential security issues discovered after Amazon Inspector runs an assessment against a specified assessment target. [Learn more.](#)

Add/Edit attributes

Last updated on January 30, 2024 12:53:07 AM (2m ago) ↺ ⬇ ⚙

Filter

Viewing 1-5 of 5

<input type="checkbox"/>	Severity 📢	Date	Finding	Target	Template	Rules Package
<input type="checkbox"/>	Medium	Today at 12:51 AM (GMT-5) (4...	On instance i-01a70cdf441432c60, TCP port 22 wh...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Informational	Today at 12:34 AM (GMT-5) (2...	Aggregate network exposure: On instance i-01a70...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Informational	Today at 12:51 AM (GMT-5) (4...	Aggregate network exposure: On instance i-01a70...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Medium	Today at 12:34 AM (GMT-5) (2...	On instance i-01a70cdf441432c60, TCP port 22 wh...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	High	Today at 12:34 AM (GMT-5) (2...	On instance i-01a70cdf441432c60, TCP port 23 wh...	Network-Audit	Assessment-Temp...	Network Reachability-1.1

Tarea 01



Ahora, procedemos a reemplazar nuestra instancia *BastionServer*, que es utilizada para conectarse a la instancia *AppServer* que se encuentra dentro de una subred privada, por **Systems Manager**. El cual es una solución de administración integral segura para entornos de nube híbrida.

Con **Sessions Manager**, podemos conectarnos de manera segura y rápida a nuestras instancias EC2, sin la necesidad de abrir puertos de entrada o administrar claves SSH.

The screenshot shows the AWS Systems Manager console interface for starting a session. The breadcrumb navigation at the top reads 'AWS Systems Manager > Session Manager > Start a session'. On the left, a sidebar lists three steps: 'Step 1: Specify target', 'Step 2 - optional: Specify session document', and 'Step 3: Review and launch'. The main area is titled 'Review and launch' and contains a 'Session details' table. The table has four columns: 'Session reason' (value: None), 'Instance name' (value: AppServer), 'Instance ID' (value: i-0f260bfb7139197f7), and 'Document name' (value: No document selected (use default settings)). At the bottom right of the table are three buttons: 'Cancel', 'Previous', and 'Start session' (highlighted in orange).

Session details			
Session reason	Instance name	Instance ID	Document name
None	AppServer	i-0f260bfb7139197f7	No document selected (use default settings)

Notamos que la conexión fue exitosa:

The screenshot shows a terminal window with a black background and white text. The text displays the commands and output of an SSH session: 'sh-4.2\$ cd', 'sh-4.2\$ pwd', and the resulting path '/home/ssm-user'. The prompt 'sh-4.2\$' is shown again at the end. Above the terminal, the browser address bar shows the URL 'us-west-2.console.aws.amazon.com/systems-manager/session-manager/i-0f260bfb7139197f7?region=us-west-2'. Below the URL, the session ID '783c9c4b-e126-4728-9951-0a7c5c23e5f5-024880303881d81ab' and instance ID 'i-0f260bfb7139197f7' are displayed. A 'Terminate' button is visible in the top right corner of the terminal area.

```
sh-4.2$ cd
sh-4.2$ pwd
/home/ssm-user
sh-4.2$
```