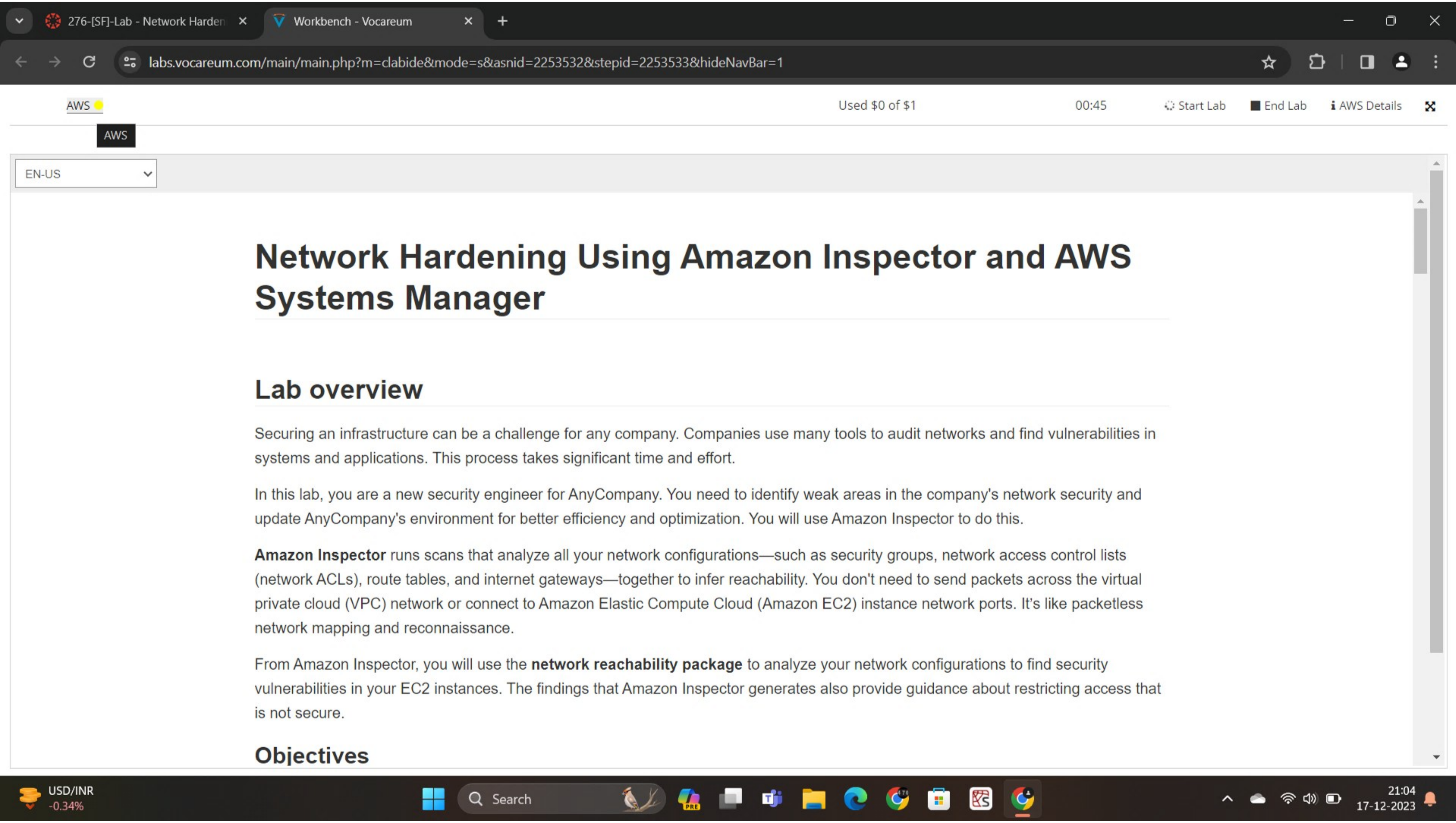

276-[SF]-Lab - Network Harden
Workbench - Vocareum
labs.vocareum.com/main/main.php?m=clabide&mode=s&asnid=2253532&stepid=2253533&hideNavBar=1
AWS
Used $0 of $1
00:45
Start Lab
End Lab
AWS Details
AWS
EN-US
USD/INR
-0.34%
Search
21:04
17-12-2023

Network Hardening Using Amazon Inspector and AWS Systems Manager

Lab overview

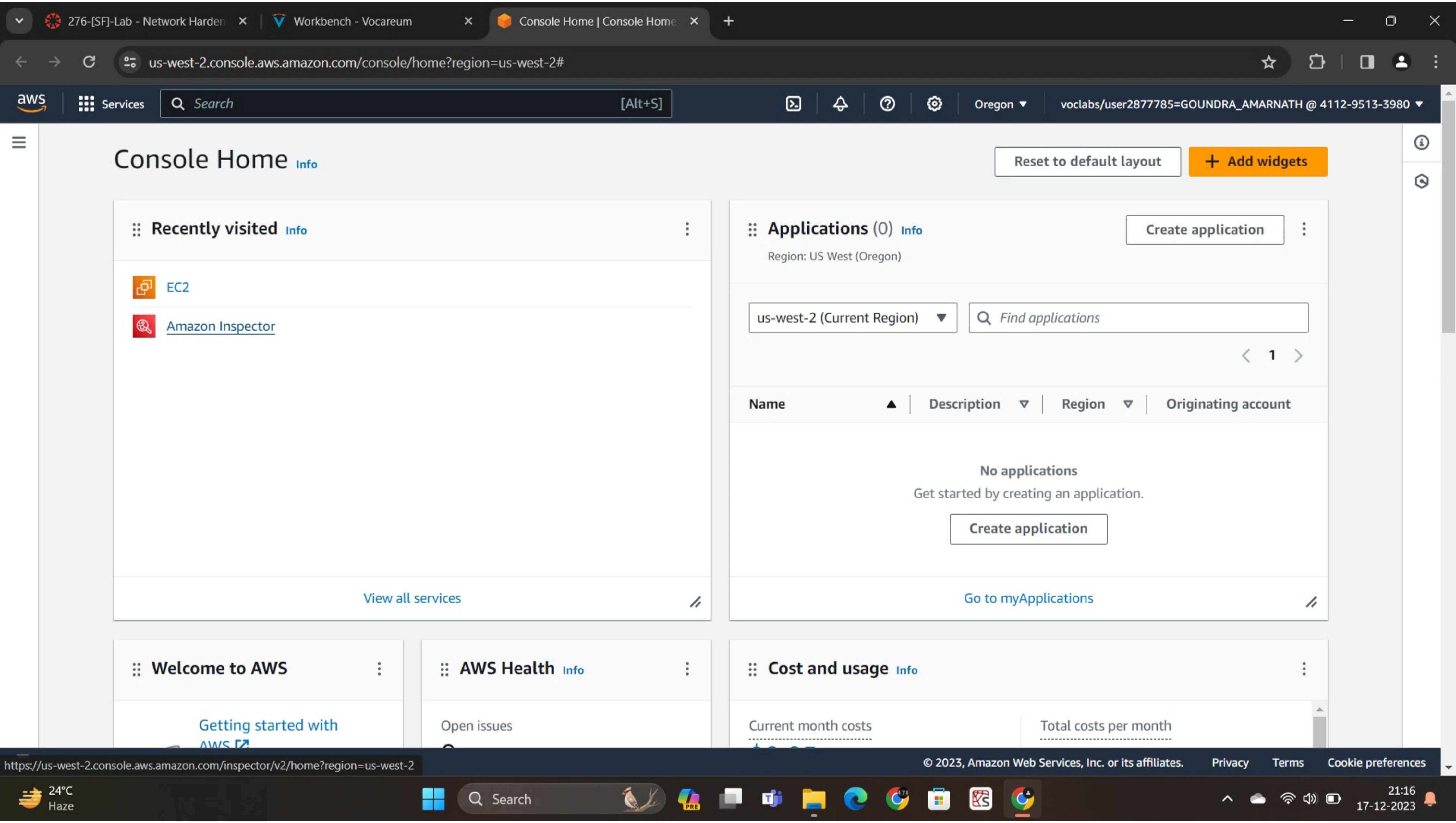
Securing an infrastructure can be a challenge for any company. Companies use many tools to audit networks and find vulnerabilities in systems and applications. This process takes significant time and effort.

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.

Objectives



us-west-2.console.aws.amazon.com/console/home?region=us-west-2#

voclabs/user2877785=GOUNDRA_AMARNATH @ 4112-9513-3980

Console Home

Recently visited

- EC2
- Amazon Inspector

Applications (0)

Region: US West (Oregon)

us-west-2 (Current Region)

Find applications

1

Name	Description	Region	Originating account

No applications

Get started by creating an application.

Welcome to AWS

Getting started with AWS

AWS Health

Open issues

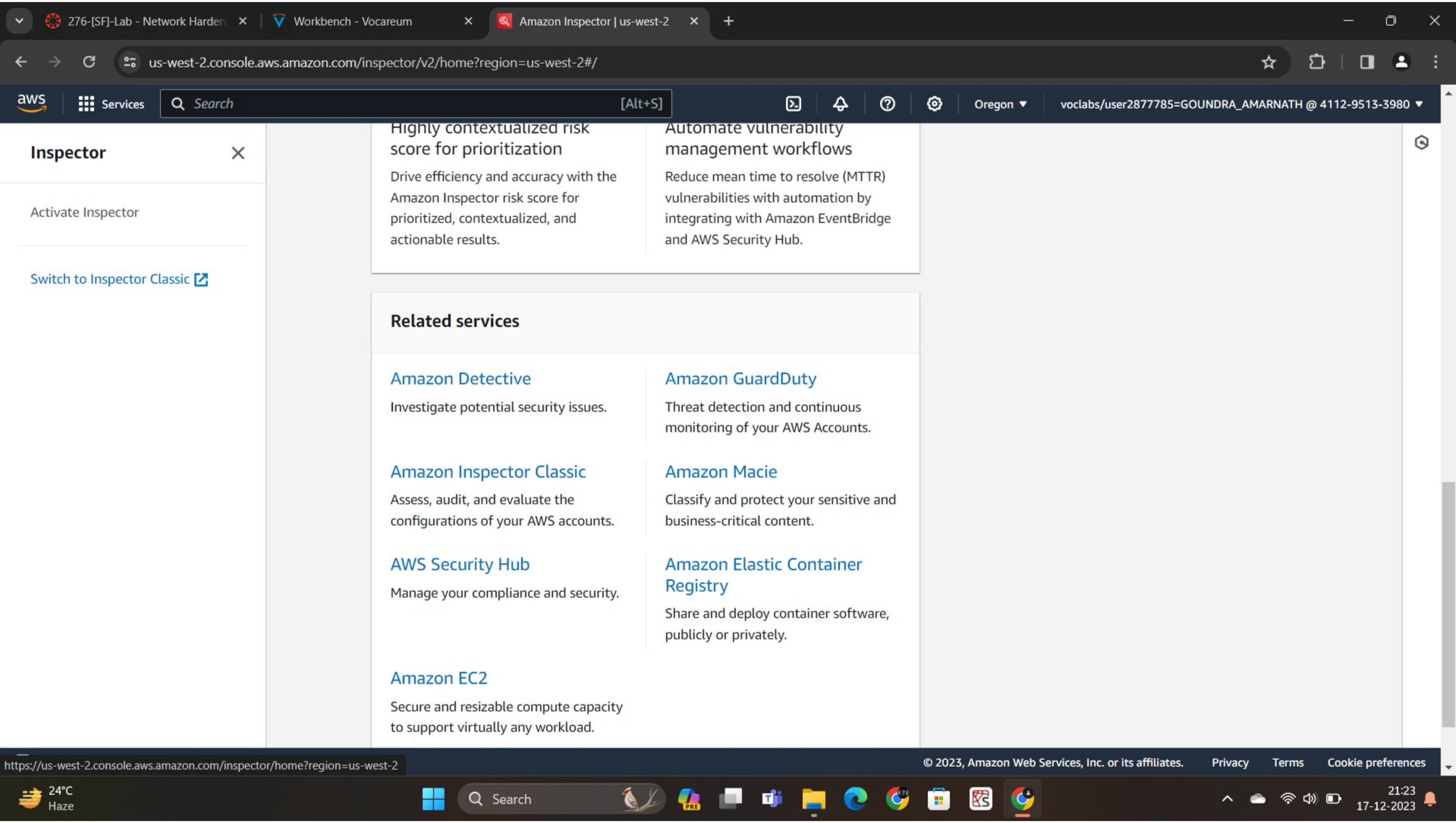
Cost and usage

Current month costs

Total costs per month

https://us-west-2.console.aws.amazon.com/inspector/v2/home?region=us-west-2

© 2023, Amazon Web Services, Inc. or its affiliates.



276-[SF]-Lab - Network Harden
Workbench - Vocareum
Amazon Inspector | us-west-2
us-west-2.console.aws.amazon.com/inspector/v2/home?region=us-west-2#/
aws
Services
Search
[Alt+S]
Oregon
voclabs/user2877785=GOUNDRA_AMARNATH @ 4112-9513-3980

Inspector

Activate Inspector

Switch to Inspector Classic

Highly contextualized risk score for prioritization

Drive efficiency and accuracy with the Amazon Inspector risk score for prioritized, contextualized, and actionable results.

Automate vulnerability management workflows

Reduce mean time to resolve (MTTR) vulnerabilities with automation by integrating with Amazon EventBridge and AWS Security Hub.

Related services

Amazon Detective

Investigate potential security issues.

Amazon GuardDuty

Threat detection and continuous monitoring of your AWS Accounts.

Amazon Inspector Classic

Assess, audit, and evaluate the configurations of your AWS accounts.

Amazon Macie

Classify and protect your sensitive and business-critical content.

AWS Security Hub

Manage your compliance and security.

Amazon Elastic Container Registry

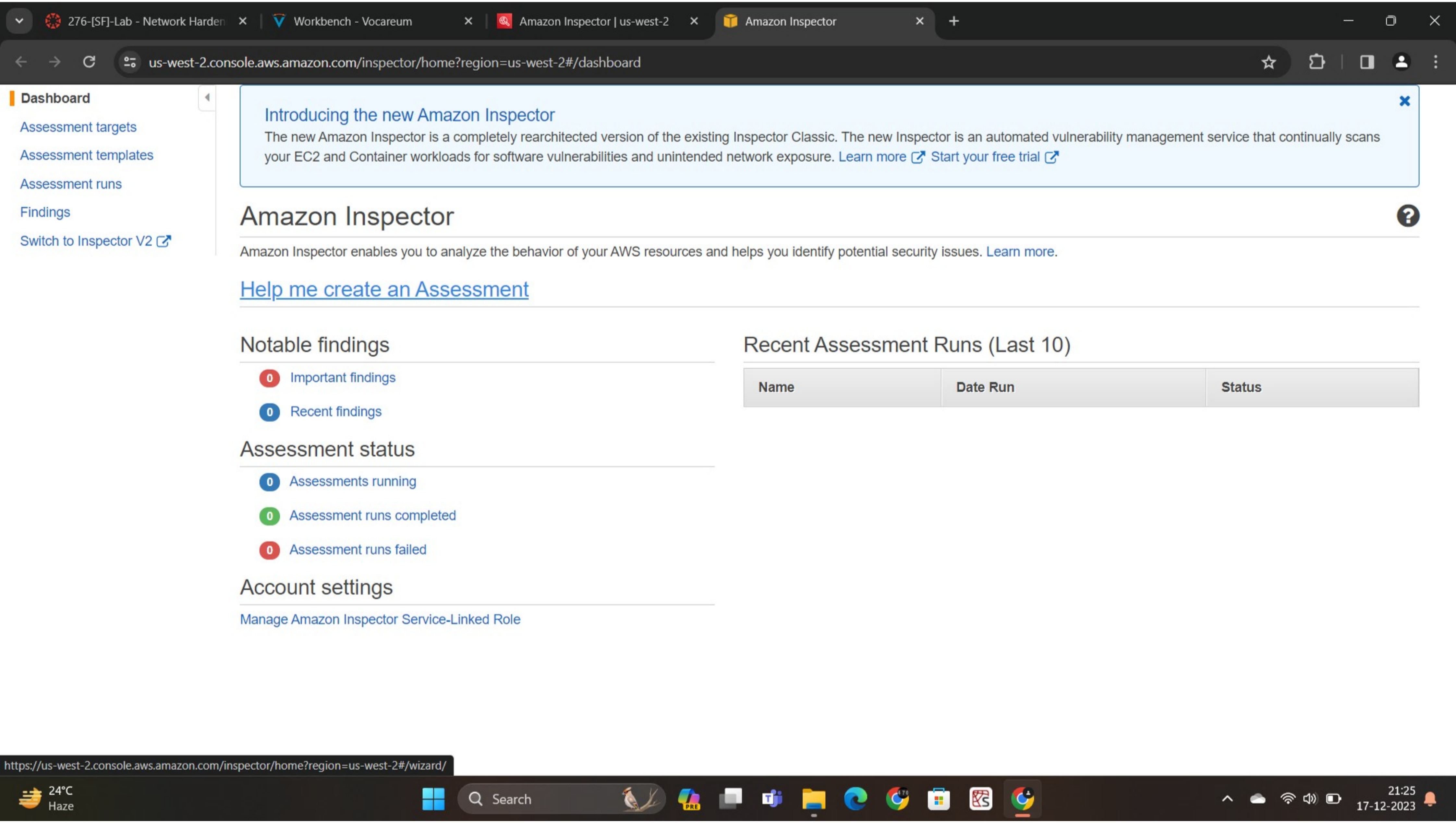
Share and deploy container software, publicly or privately.

Amazon EC2

Secure and resizable compute capacity to support virtually any workload.

https://us-west-2.console.aws.amazon.com/inspector/home?region=us-west-2

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



276-[SF]-Lab - Network Harden
Workbench - Vocareum
Amazon Inspector | us-west-2
Amazon Inspector
us-west-2.console.aws.amazon.com/inspector/home?region=us-west-2#/dashboard

Dashboard
Assessment targets
Assessment templates
Assessment runs
Findings
Switch to Inspector V2

Introducing the new Amazon Inspector

The new Amazon Inspector is a completely rearchitected version of the existing Inspector Classic. The new Inspector is an automated vulnerability management service that continually scans your EC2 and Container workloads for software vulnerabilities and unintended network exposure. Learn more Start your free trial

Amazon Inspector

Amazon Inspector enables you to analyze the behavior of your AWS resources and helps you identify potential security issues. Learn more.

Help me create an Assessment

Notable findings

- 0 Important findings
- 0 Recent findings

Assessment status

- 0 Assessments running
- 0 Assessment runs completed
- 0 Assessment runs failed

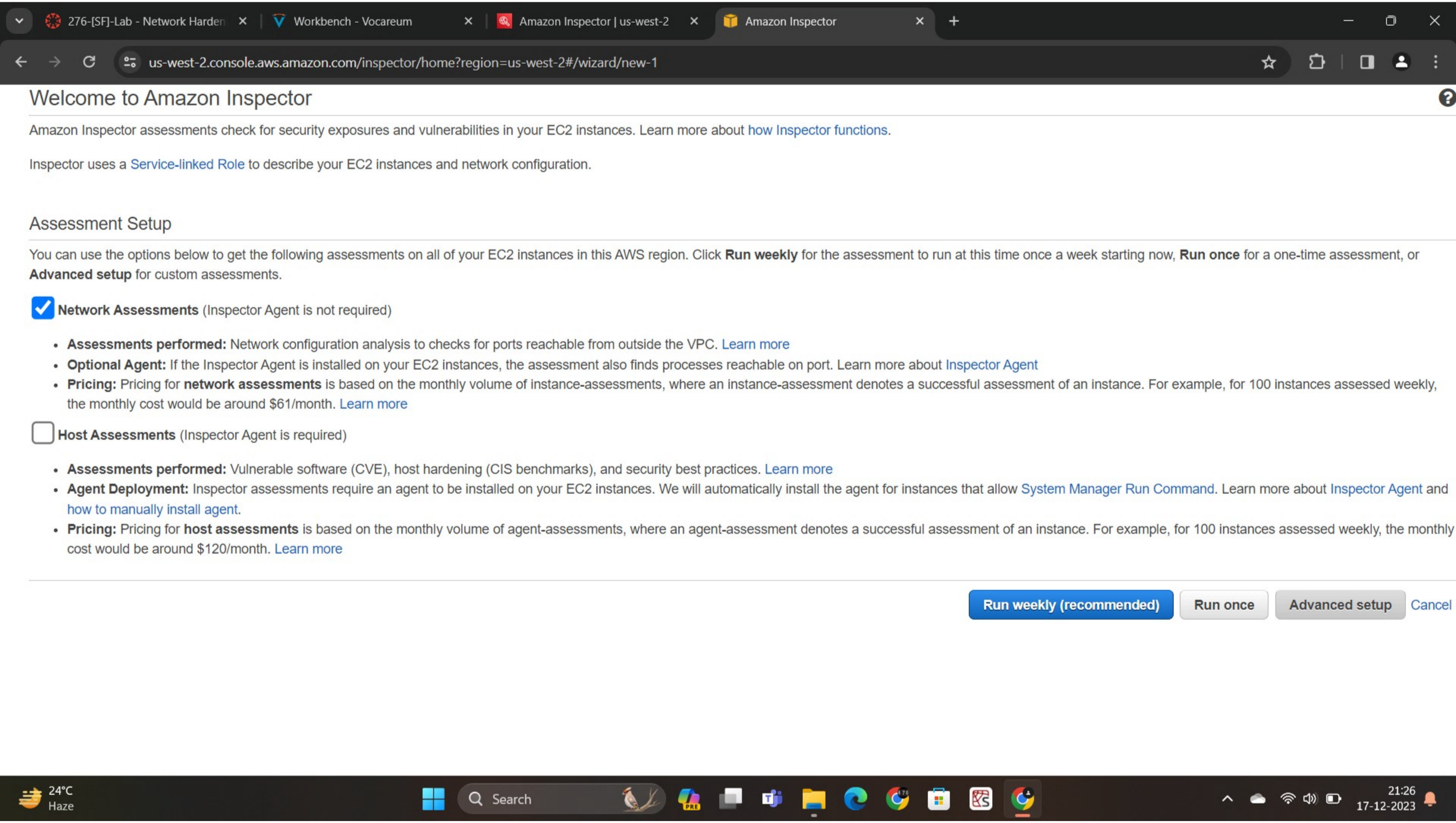
Account settings

Manage Amazon Inspector Service-Linked Role

Recent Assessment Runs (Last 10)

Name	Date Run	Status

https://us-west-2.console.aws.amazon.com/inspector/home?region=us-west-2#/wizard/
24°C
Haze
Search
21:25
17-12-2023


276-[SF]-Lab - Network Harden
Workbench - Vocareum
Amazon Inspector | us-west-2
Amazon Inspector
us-west-2.console.aws.amazon.com/inspector/home?region=us-west-2#/wizard/new-1
24°C
Haze
Search
21:26
17-12-2023

Welcome to Amazon Inspector

Amazon Inspector assessments check for security exposures and vulnerabilities in your EC2 instances. Learn more about how Inspector functions.

Inspector uses a Service-linked Role to describe your EC2 instances and network configuration.

Assessment Setup

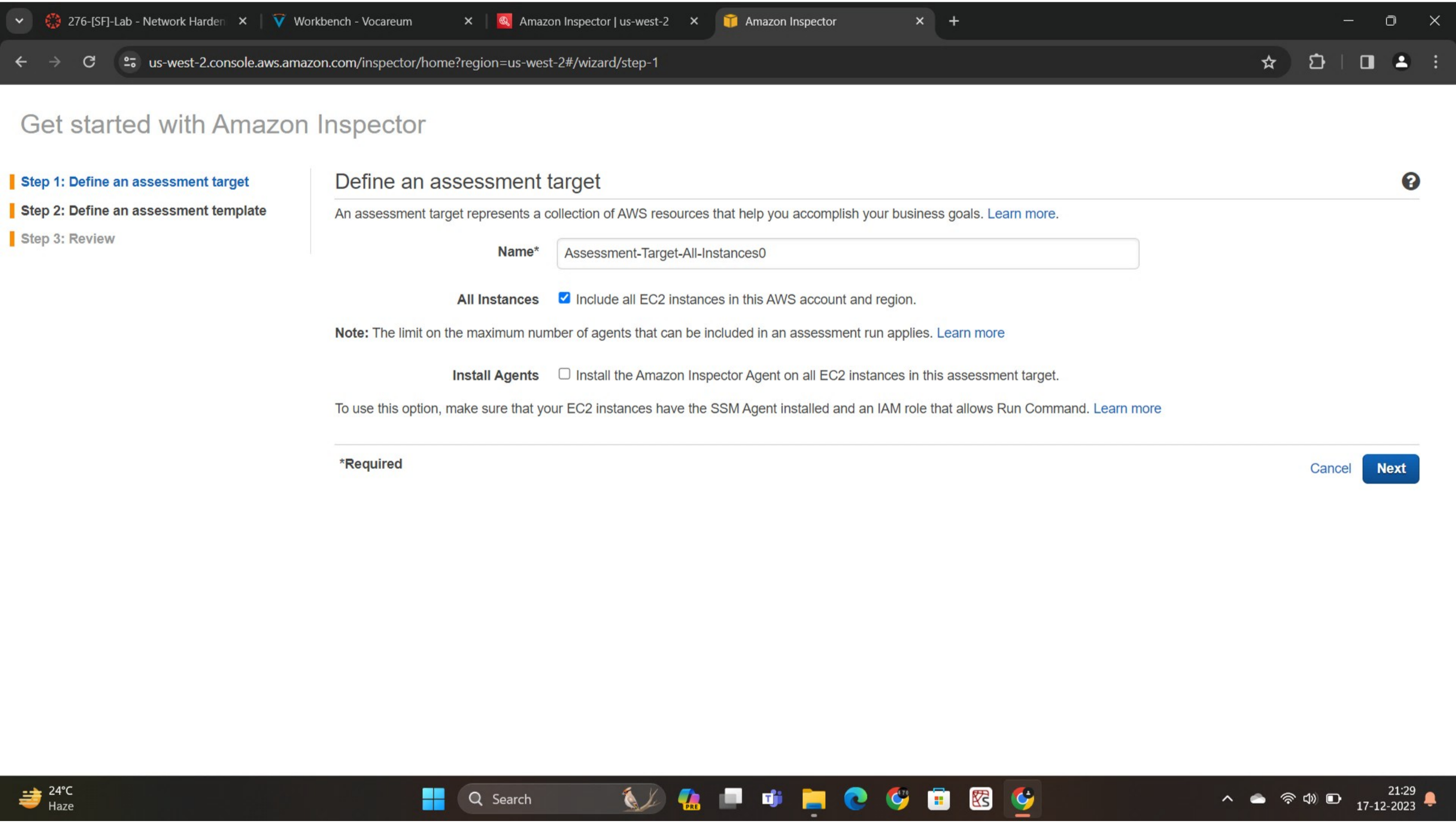
You can use the options below to get the following assessments on all of your EC2 instances in this AWS region. Click **Run weekly** for the assessment to run at this time once a week starting now, **Run once** for a one-time assessment, or **Advanced setup** for custom assessments.

☑ **Network Assessments** (Inspector Agent is not required)

- **Assessments performed:** Network configuration analysis to checks for ports reachable from outside the VPC. Learn more
- **Optional Agent:** If the Inspector Agent is installed on your EC2 instances, the assessment also finds processes reachable on port. Learn more about Inspector Agent
- **Pricing:** Pricing for **network assessments** is based on the monthly volume of instance-assessments, where an instance-assessment denotes a successful assessment of an instance. For example, for 100 instances assessed weekly, the monthly cost would be around $61/month. Learn more

☐ **Host Assessments** (Inspector Agent is required)

- **Assessments performed:** Vulnerable software (CVE), host hardening (CIS benchmarks), and security best practices. Learn more
- **Agent Deployment:** Inspector assessments require an agent to be installed on your EC2 instances. We will automatically install the agent for instances that allow System Manager Run Command. Learn more about Inspector Agent and how to manually install agent.
- **Pricing:** Pricing for **host assessments** is based on the monthly volume of agent-assessments, where an agent-assessment denotes a successful assessment of an instance. For example, for 100 instances assessed weekly, the monthly cost would be around $120/month. Learn more



276-[SF]-Lab - Network Harden
Workbench - Vocareum
Amazon Inspector | us-west-2
Amazon Inspector
us-west-2.console.aws.amazon.com/inspector/home?region=us-west-2#/wizard/step-1

Get started with Amazon Inspector

Step 1: Define an assessment target

Step 2: Define an assessment template

Step 3: Review

Define an assessment target

An assessment target represents a collection of AWS resources that help you accomplish your business goals. Learn more.

Name* Assessment-Target-All-Instances0

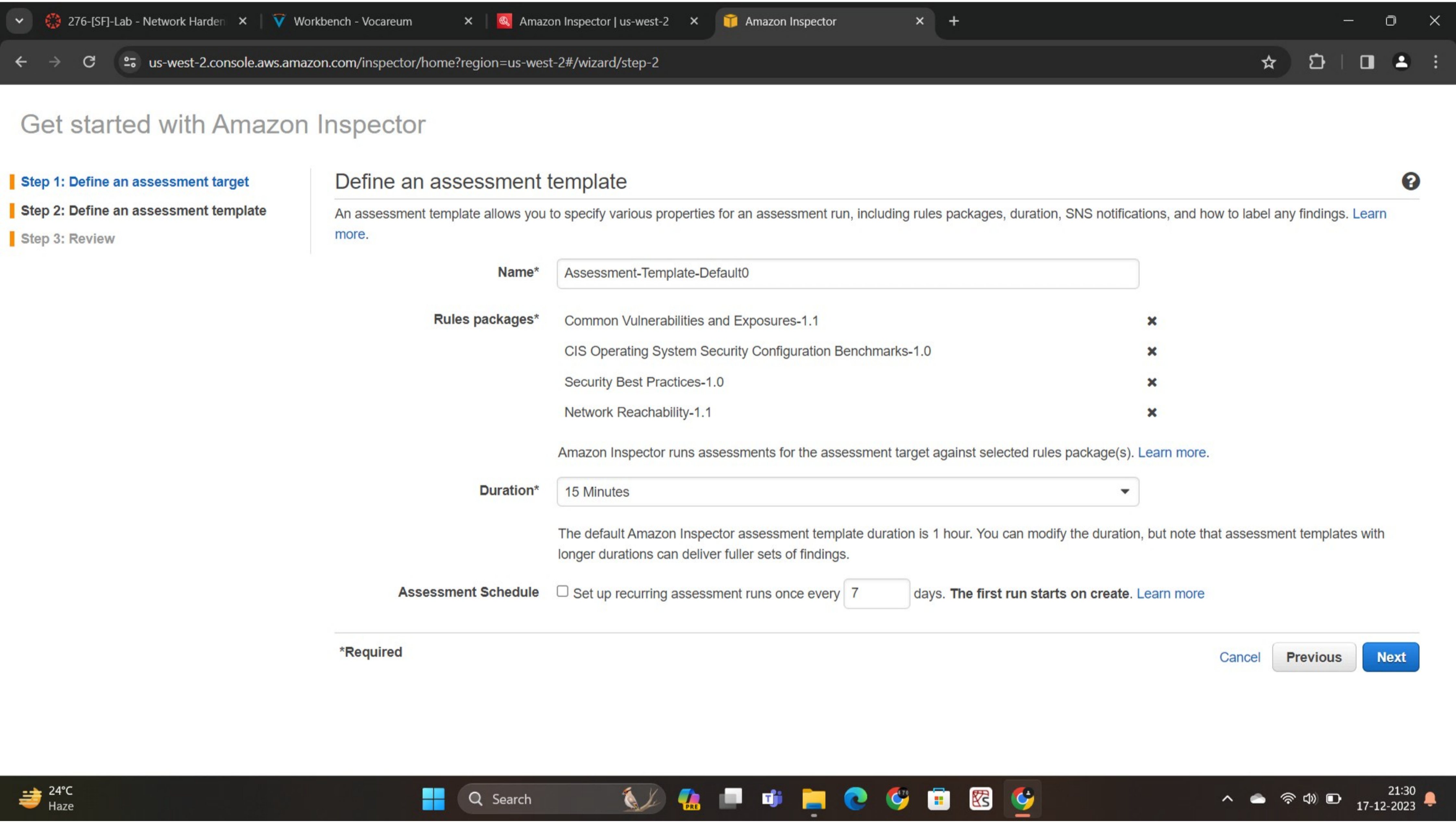
All Instances ☑ Include all EC2 instances in this AWS account and region.

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

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

*Required



276-[SF]-Lab - Network Harden
Workbench - Vocareum
Amazon Inspector | us-west-2
Amazon Inspector
us-west-2.console.aws.amazon.com/inspector/home?region=us-west-2#/wizard/step-2

Get started with Amazon Inspector

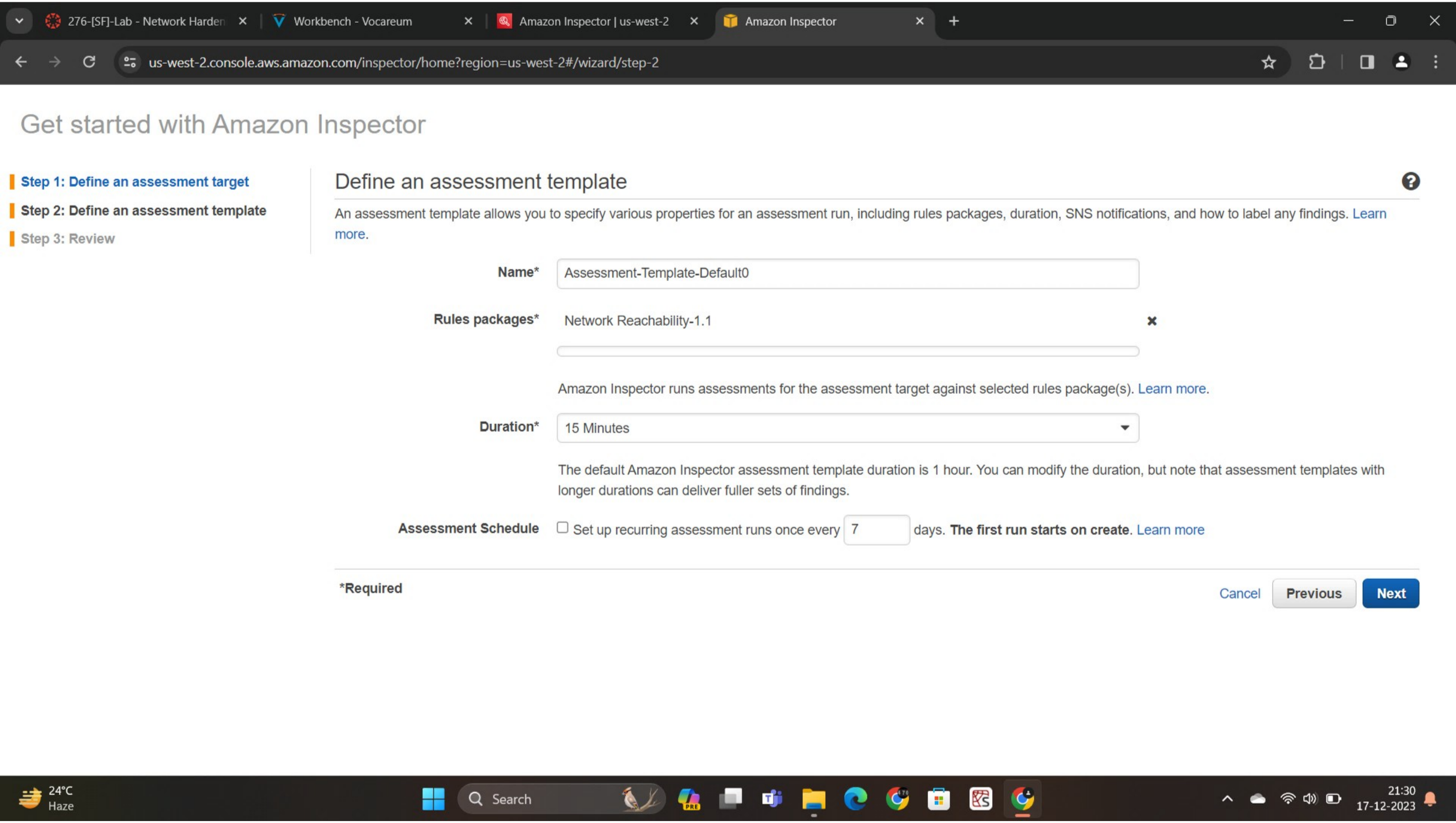
- Step 1: Define an assessment target
- Step 2: Define an assessment template
- Step 3: Review

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*	Assessment-Template-Default0
Rules packages*	Common Vulnerabilities and Exposures-1.1 ✖ CIS Operating System Security Configuration Benchmarks-1.0 ✖ Security Best Practices-1.0 ✖ Network Reachability-1.1 ✖
	Amazon Inspector runs assessments for the assessment target against selected rules package(s). Learn more.
Duration*	15 Minutes
	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 7 days. **The first run starts on create.** Learn more

*Required



276-[SF]-Lab - Network Harden
Workbench - Vocareum
Amazon Inspector | us-west-2
Amazon Inspector
us-west-2.console.aws.amazon.com/inspector/home?region=us-west-2#/wizard/step-2

Get started with Amazon Inspector

- Step 1: Define an assessment target
- Step 2: Define an assessment template
- Step 3: Review

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*	Assessment-Template-Default0
Rules packages*	Network Reachability-1.1 ✖

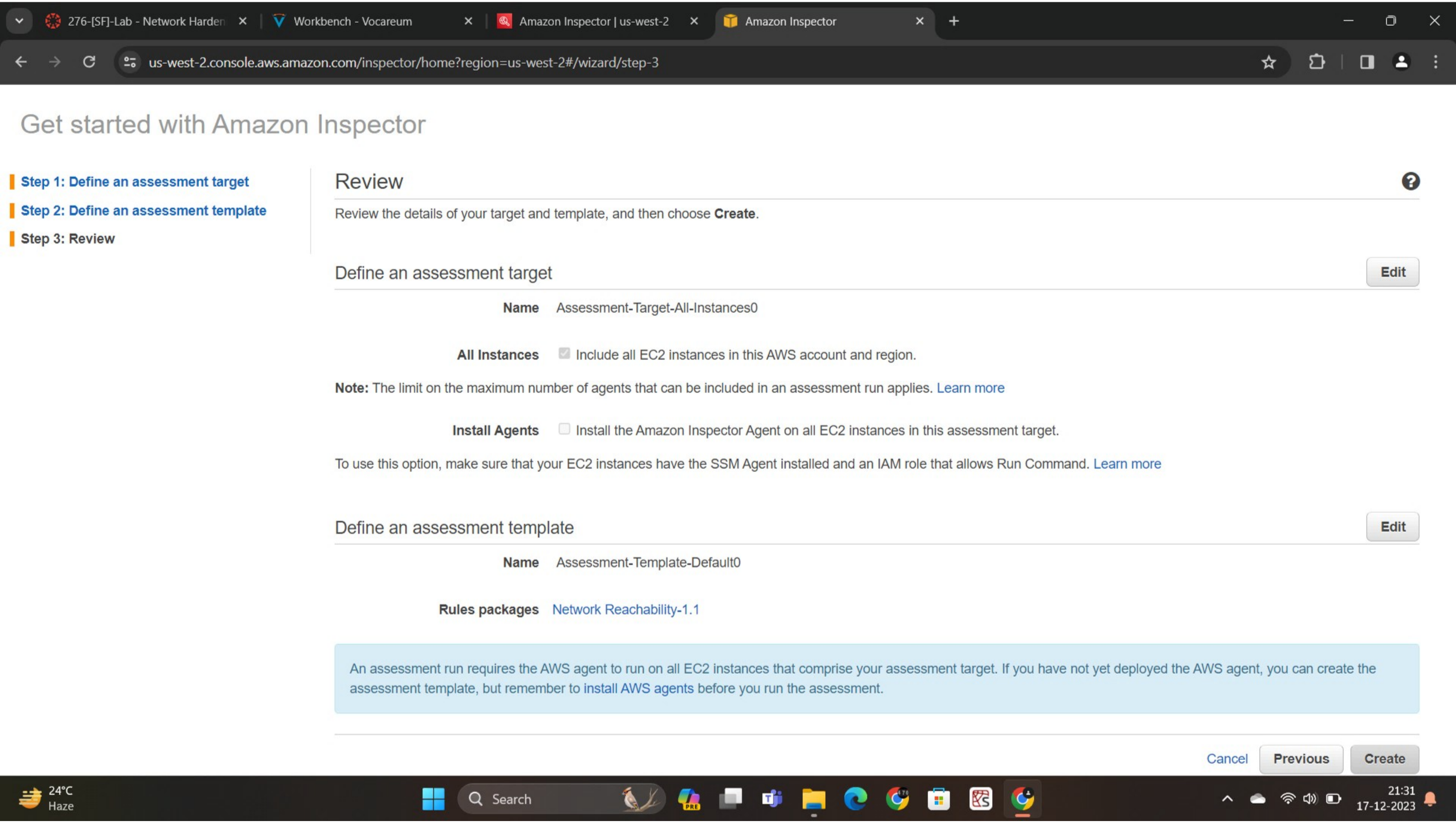
Amazon Inspector runs assessments for the assessment target against selected rules package(s). Learn more.

Duration*	15 Minutes ▾

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 7 days. **The first run starts on create**. Learn more

*Required



276-[SF]-Lab - Network Harden
Workbench - Vocareum
Amazon Inspector | us-west-2
Amazon Inspector
us-west-2.console.aws.amazon.com/inspector/home?region=us-west-2#/wizard/step-3

Get started with Amazon Inspector

- Step 1: Define an assessment target
- Step 2: Define an assessment template
- Step 3: Review

Review

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

Define an assessment target

Name Assessment-Target-All-Instances0

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

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

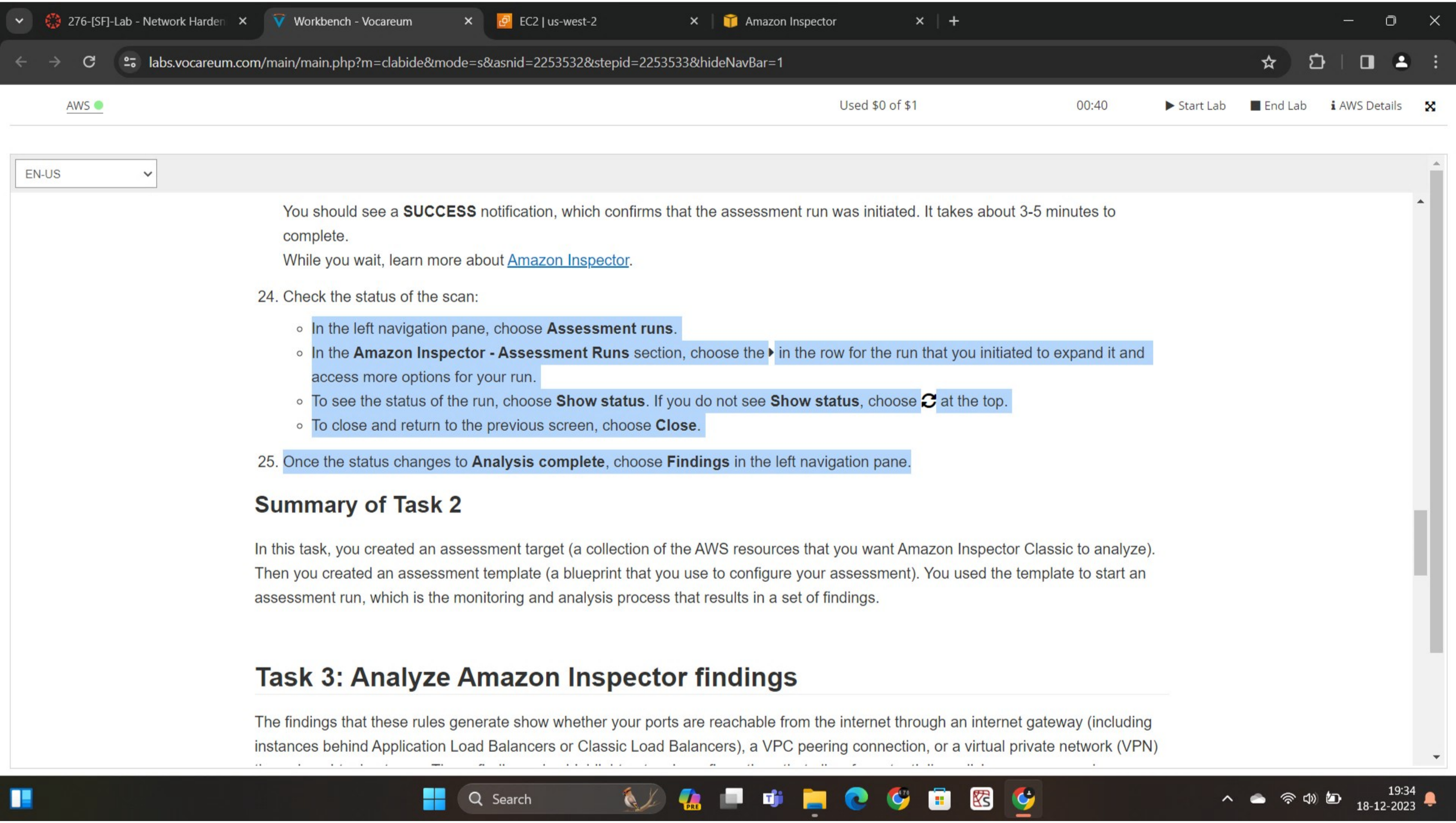
To use this option, make sure that your EC2 instances have the SSM Agent installed and an IAM role that allows Run Command. Learn more

Define an assessment template

Name Assessment-Template-Default0

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.



You should see a **SUCCESS** notification, which confirms that the assessment run was initiated. It takes about 3-5 minutes to complete.
While you wait, learn more about Amazon Inspector.

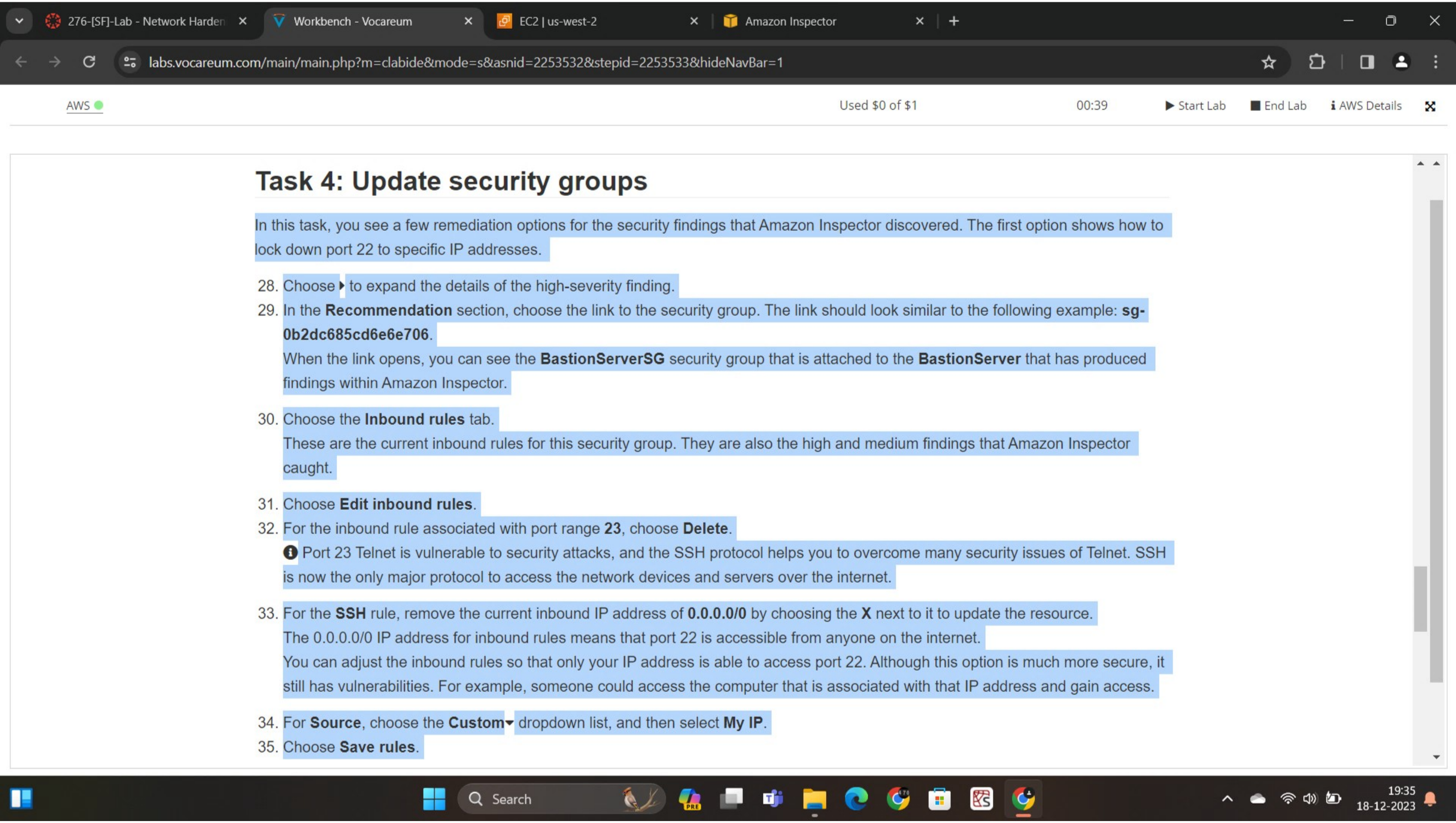
24. Check the status of the scan:
    - In the left navigation pane, choose **Assessment runs**.
    - In the **Amazon Inspector - Assessment Runs** section, choose the ▸ in the row for the run that you initiated to expand it and access more options for your run.
    - To see the status of the run, choose **Show status**. If you do not see **Show status**, choose ↻ at the top.
    - To close and return to the previous screen, choose **Close**.
25. Once the status changes to **Analysis complete**, choose **Findings** in the left navigation pane.

Summary of Task 2

In this task, you created an assessment target (a collection of the AWS resources that you want Amazon Inspector Classic to analyze). Then you created an assessment template (a blueprint that you use to configure your assessment). You used the template to start an assessment run, which is the monitoring and analysis process that results in a set of findings.

Task 3: Analyze Amazon Inspector findings

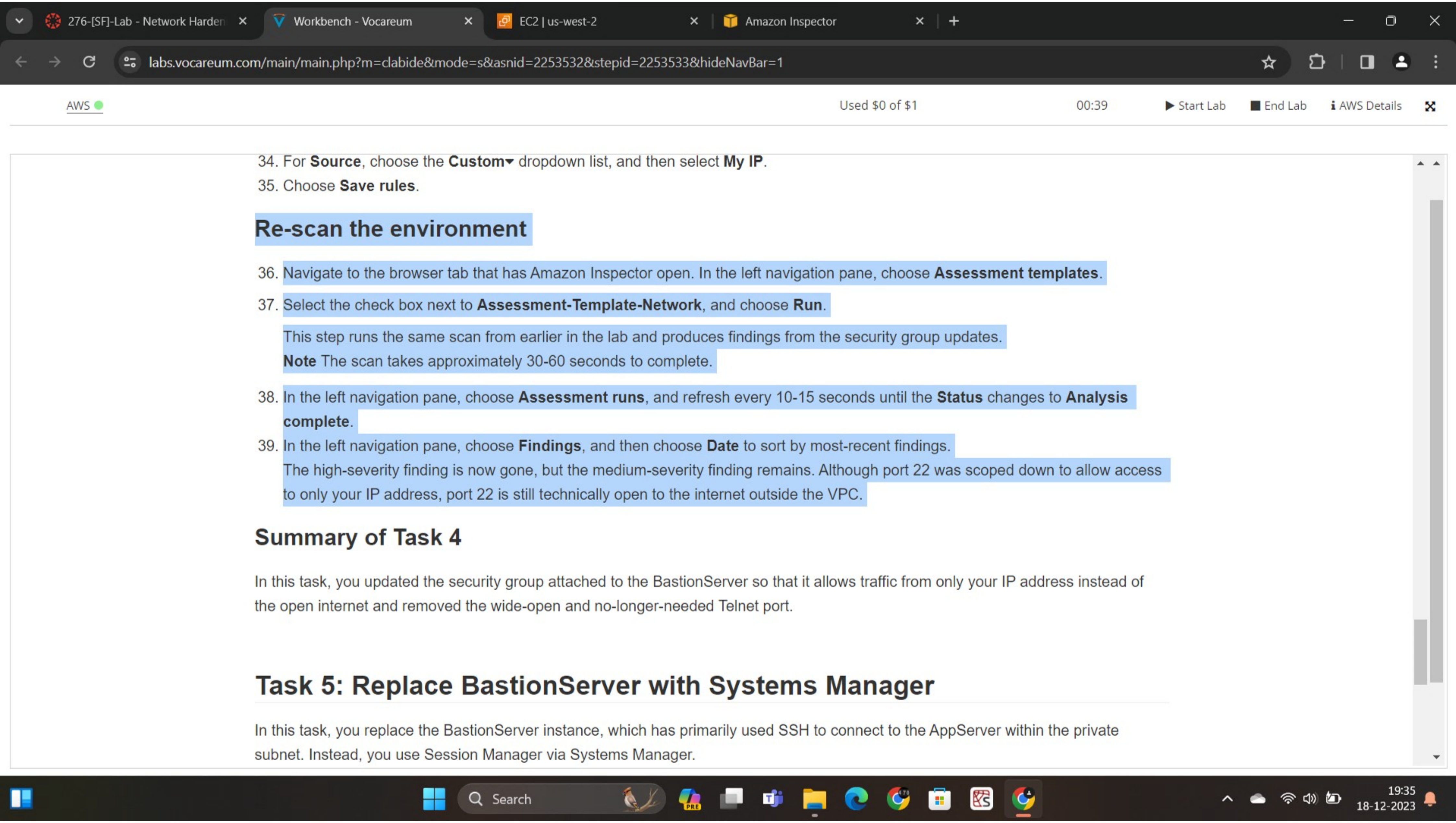
The findings that these rules generate show whether your ports are reachable from the internet through an internet gateway (including instances behind Application Load Balancers or Classic Load Balancers), a VPC peering connection, or a virtual private network (VPN)



Task 4: Update security groups

In this task, you see a few remediation options for the security findings that Amazon Inspector discovered. The first option shows how to lock down port 22 to specific IP addresses.

28. Choose ▸ to expand the details of the high-severity finding.
29. In the **Recommendation** section, choose the link to the security group. The link should look similar to the following example: **sg-0b2dc685cd6e6e706**.
    When the link opens, you can see the **BastionServerSG** security group that is attached to the **BastionServer** that has produced findings within Amazon Inspector.
30. Choose the **Inbound rules** tab.
    These are the current inbound rules for this security group. They are also the high and medium findings that Amazon Inspector caught.
31. Choose **Edit inbound rules**.
32. For the inbound rule associated with port range **23**, choose **Delete**.
    ℹ Port 23 Telnet is vulnerable to security attacks, and the SSH protocol helps you to overcome many security issues of Telnet. SSH is now the only major protocol to access the network devices and servers over the internet.
33. For the **SSH** rule, remove the current inbound IP address of **0.0.0.0/0** by choosing the **X** next to it to update the resource.
    The 0.0.0.0/0 IP address for inbound rules means that port 22 is accessible from anyone on the internet.
    You can adjust the inbound rules so that only your IP address is able to access port 22. Although this option is much more secure, it still has vulnerabilities. For example, someone could access the computer that is associated with that IP address and gain access.
34. For **Source**, choose the **Custom**▾ dropdown list, and then select **My IP**.
35. Choose **Save rules**.



34. For **Source**, choose the **Custom▾** dropdown list, and then select **My IP**.
35. Choose **Save rules**.

Re-scan the environment

36. Navigate to the browser tab that has Amazon Inspector open. In the left navigation pane, choose **Assessment templates**.
37. Select the check box next to **Assessment-Template-Network**, and choose **Run**.

    This step runs the same scan from earlier in the lab and produces findings from the security group updates.
    Note The scan takes approximately 30-60 seconds to complete.

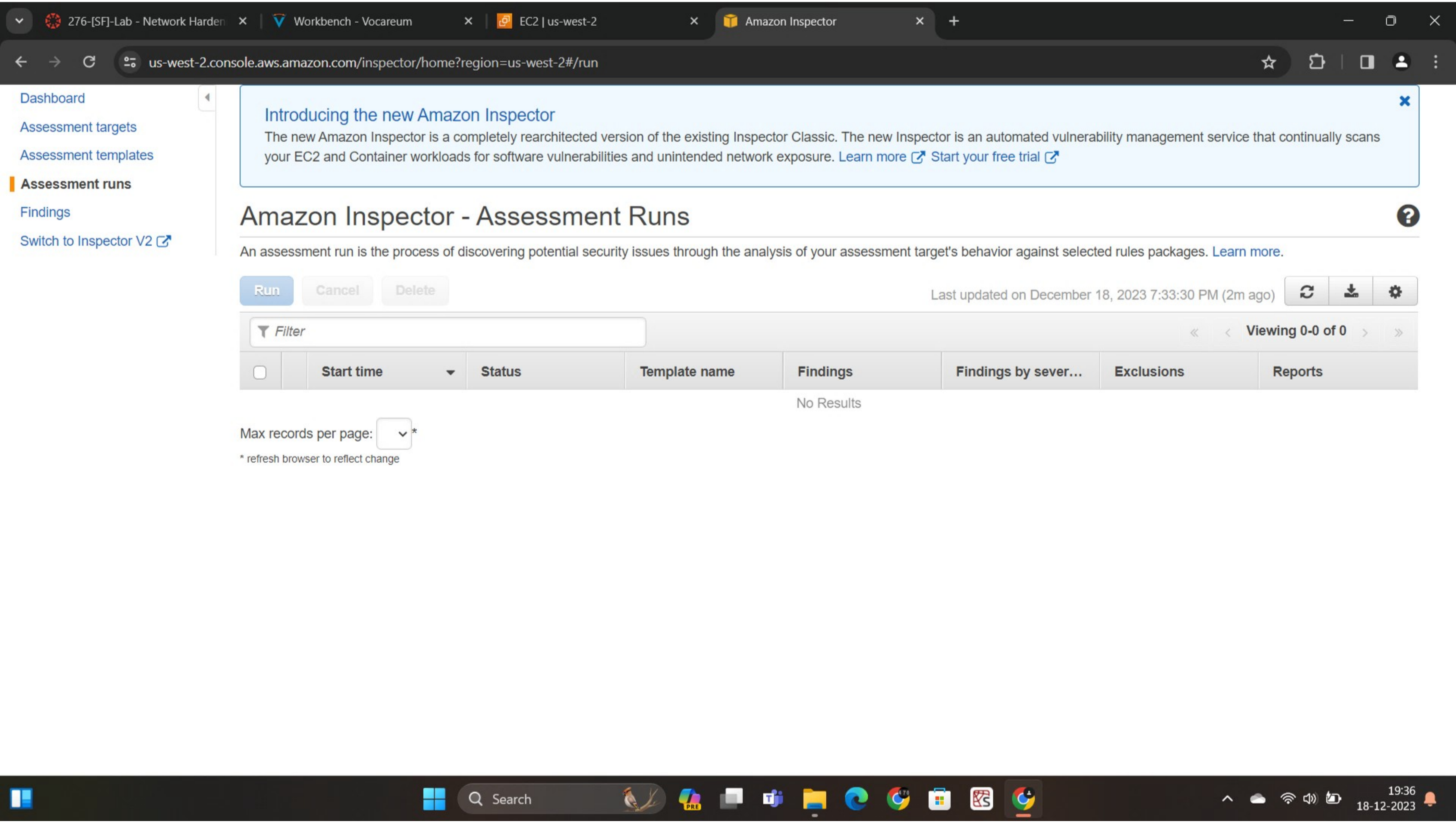
38. In the left navigation pane, choose **Assessment runs**, and refresh every 10-15 seconds until the **Status** changes to **Analysis complete**.
39. In the left navigation pane, choose **Findings**, and then choose **Date** to sort by most-recent findings.
    The high-severity finding is now gone, but the medium-severity finding remains. Although port 22 was scoped down to allow access to only your IP address, port 22 is still technically open to the internet outside the VPC.

Summary of Task 4

In this task, you updated the security group attached to the BastionServer so that it allows traffic from only your IP address instead of the open internet and removed the wide-open and no-longer-needed Telnet port.

Task 5: Replace BastionServer with Systems Manager

In this task, you replace the BastionServer instance, which has primarily used SSH to connect to the AppServer within the private subnet. Instead, you use Session Manager via Systems Manager.



Introducing the new Amazon Inspector

The new Amazon Inspector is a completely rearchitected version of the existing Inspector Classic. The new Inspector is an automated vulnerability management service that continually scans your EC2 and Container workloads for software vulnerabilities and unintended network exposure. Learn more Start your free trial

Amazon Inspector - Assessment Runs

An assessment run is the process of discovering potential security issues through the analysis of your assessment target's behavior against selected rules packages. Learn more.

Last updated on December 18, 2023 7:33:30 PM (2m ago)

Filter

Viewing 0-0 of 0

□	Start time	Status	Template name	Findings	Findings by sever...	Exclusions	Reports

No Results

Max records per page: *

* refresh browser to reflect change