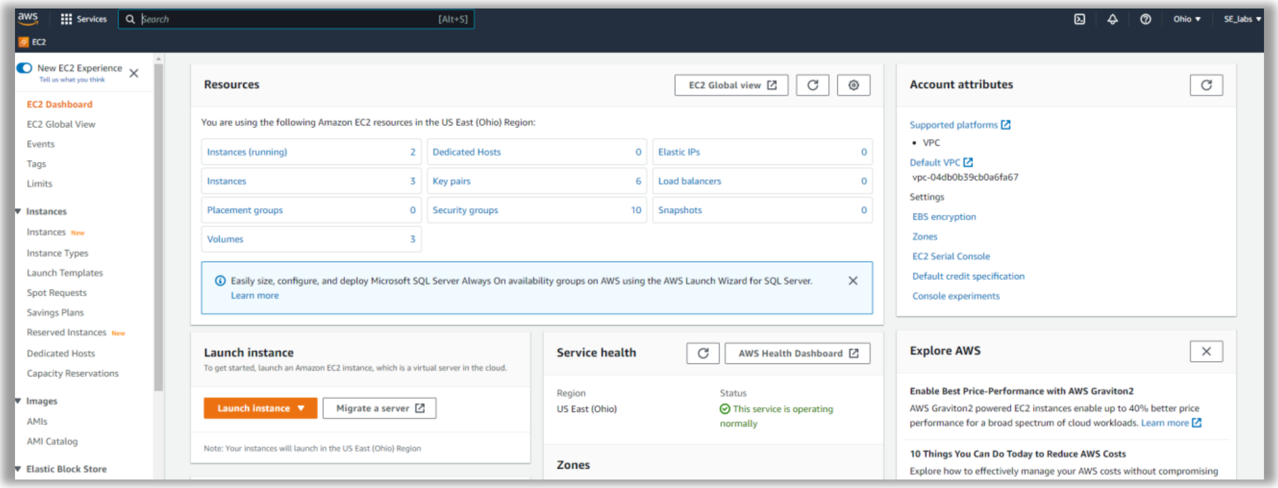
Follow the Below Steps to Configure Metasploitable in AWS

Note: Here we are using Metasploitable as our target machine to scan for vulnerabilities

1. After you login into AWS Console you should be able to see below screen. Then click or search for EC2 in search dialogue and **select Ohio Region** in top right corner



You are using the following Amazon EC2 resources in the US East (Ohio) Region:

Instances (running)	2	Dedicated Hosts	0	Elastic IPs	0
Instances	3	Key pairs	6	Load balancers	0
Placement groups	0	Security groups	10	Snapshots	0
Volumes	3				

Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more

- VPC

vpc-04db0b39cb0a6fa67

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Note: Your instances will launch in the US East (Ohio) Region

Region: US East (Ohio)

Status: This service is operating normally

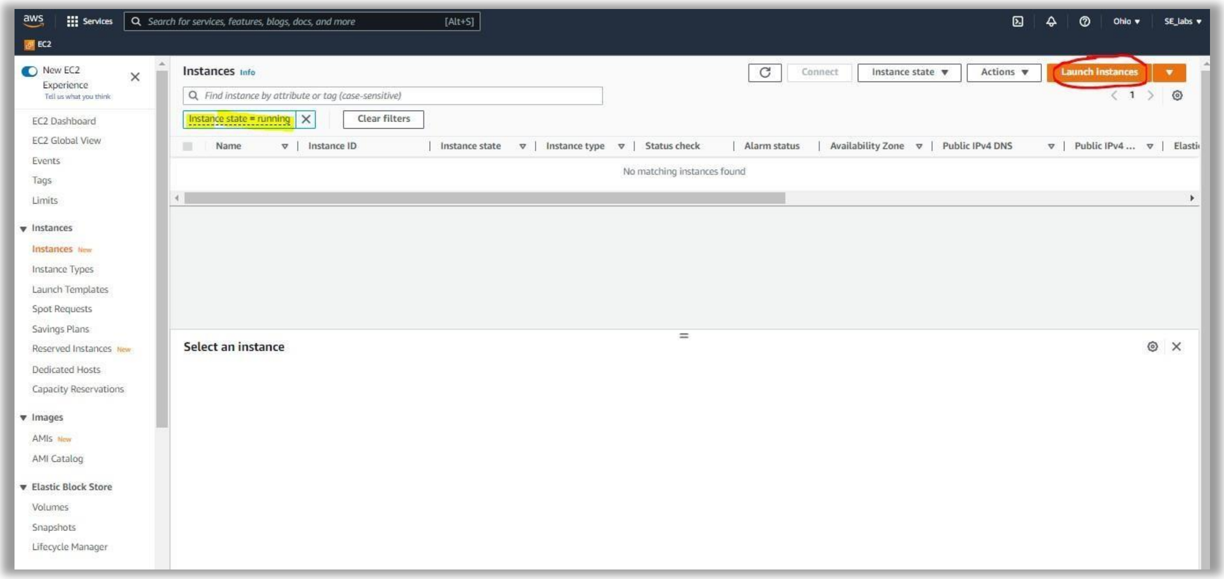
Enable Best Price-Performance with AWS Graviton2

AWS Graviton2 powered EC2 instances enable up to 40% better price performance for a broad spectrum of cloud workloads. Learn more

10 Things You Can Do Today to Reduce AWS Costs

Explore how to effectively manage your AWS costs without compromising

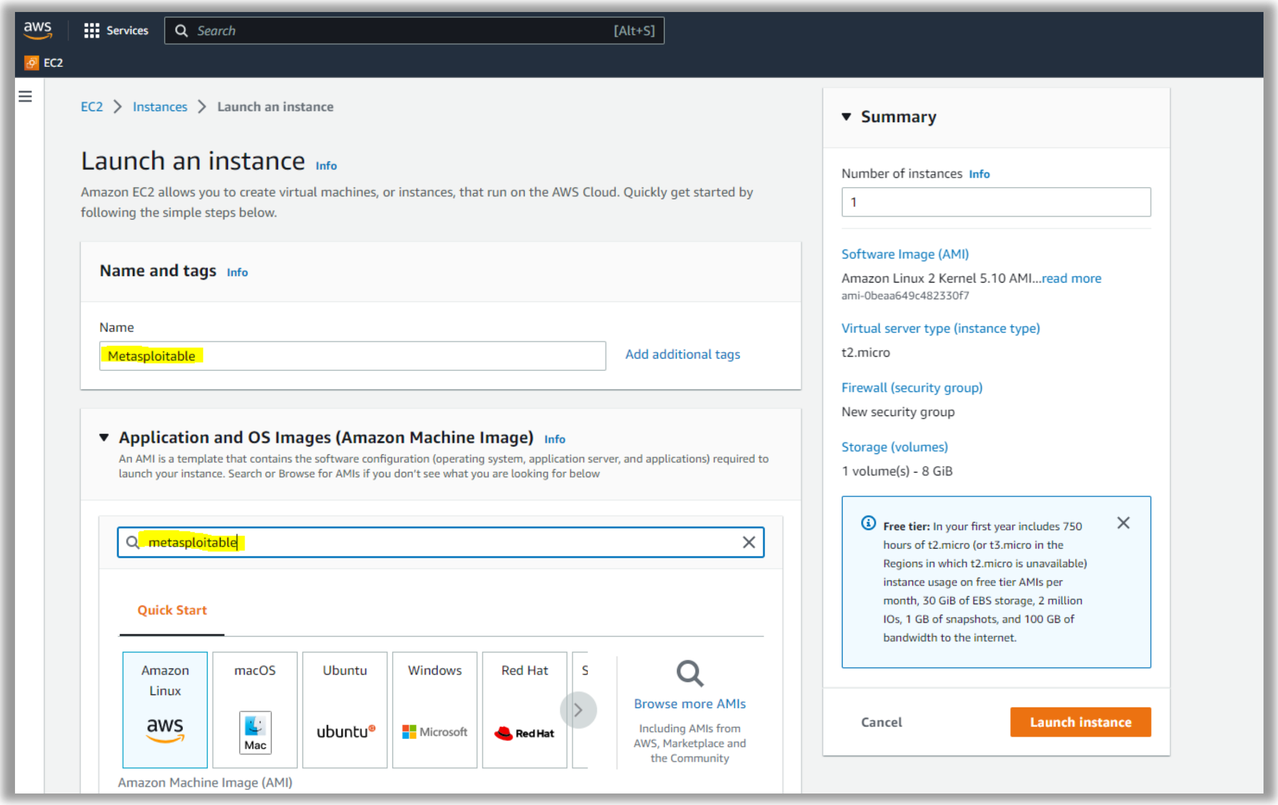
2. Click on Launch Instance tab on top right corner as marked in below image tospin up new server.



Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elasti

No matching instances found

3. To spin up Metasploitable Vulnerable Machine search for metasploitable in search box



EC2 > Instances > Launch an instance

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name: Metasploitable

Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search: metasploitable

Summary

Number of instances Info: 1

Software Image (AMI): Amazon Linux 2 Kernel 5.10 AMI...read more
ami-0beaa649c482330f7

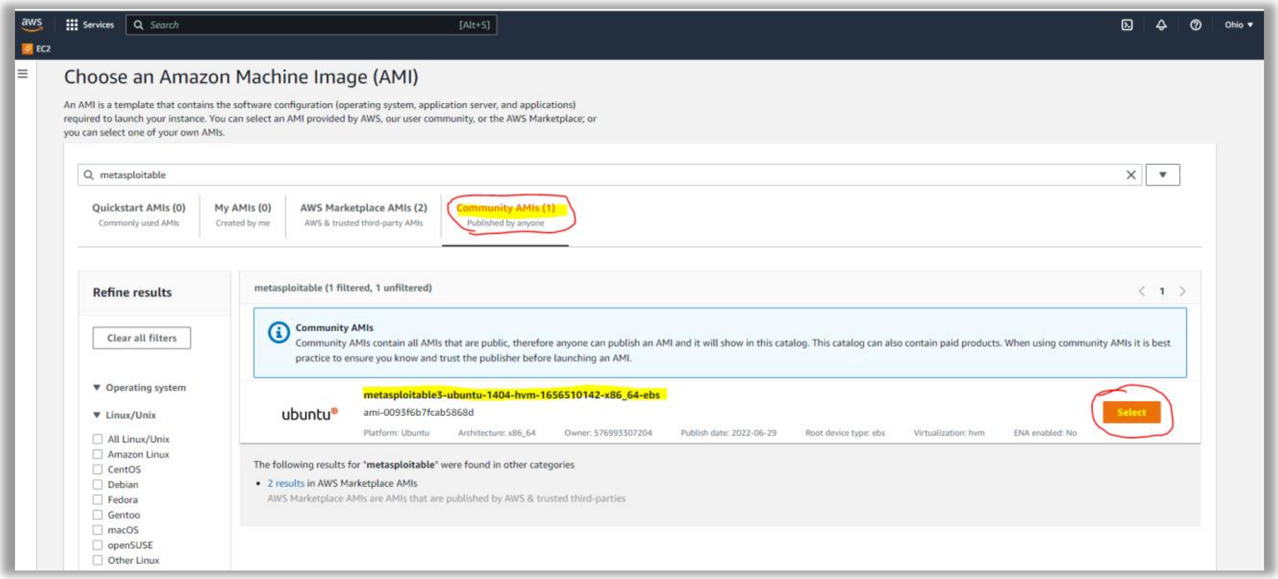
Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

4. Click on community AMI and then select metasploitable-ubuntu-1404 as shown in below image.



Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Search: metasploitable

- □ All Linux/Unix
- □ Amazon Linux
- □ CentOS
- □ Debian
- □ Fedora
- □ Gentoo
- □ macOS
- □ openSUSE
- □ Other Linux

metasploitable (1 filtered, 1 unfiltered)

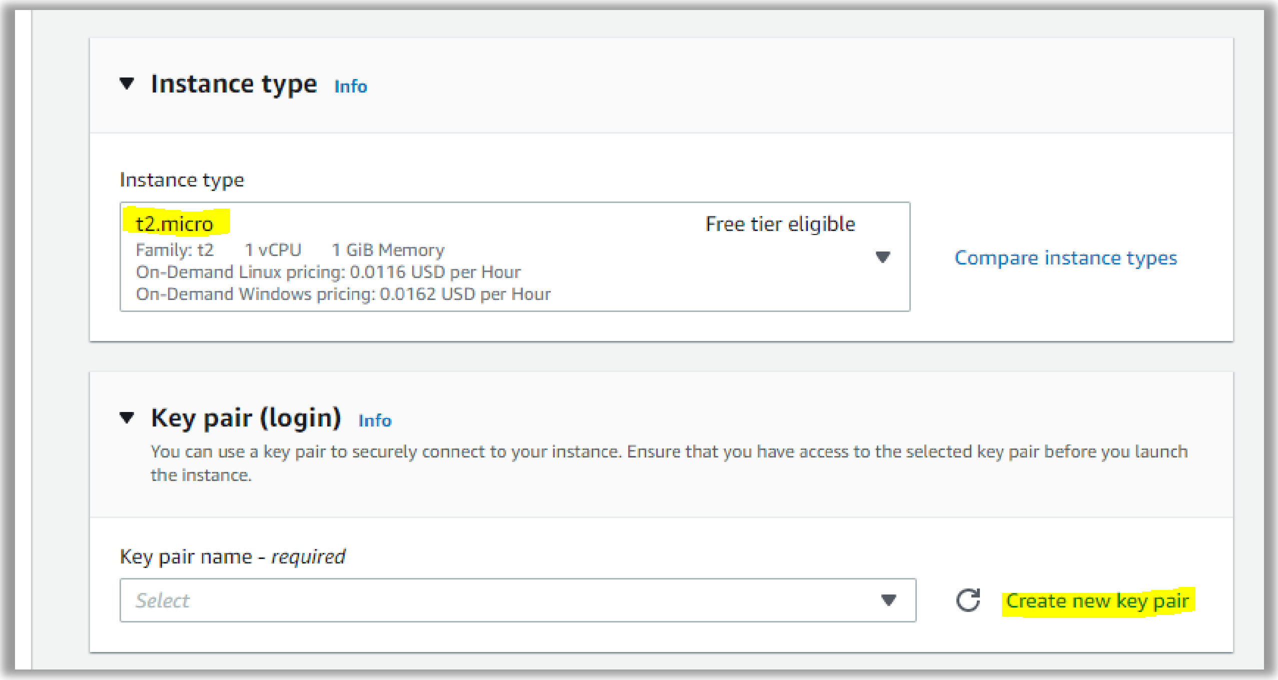
Community AMIs
Community AMIs contain all AMIs that are public, therefore anyone can publish an AMI and it will show in this catalog. This catalog can also contain paid products. When using community AMIs it is best practice to ensure you know and trust the publisher before launching an AMI.

metasploitable3-ubuntu-1404-hvm-1656510142-x86_64-ebs
ami-0093f6b7fcab5868d
Platform: Ubuntu Architecture: x86_64 Owner: 576993307204 Publish date: 2022-06-29 Root device type: ebs Virtualization: hvm ENA enabled: No

The following results for "metasploitable" were found in other categories

- 2 results in AWS Marketplace AMIs
  AWS Marketplace AMIs are AMIs that are published by AWS & trusted third-parties

5. Select t2.micro as the Instance Type and Give the name as metasploitable and click on create new key pair a file gets automatically downloaded.



▼ Instance type Info

Instance type

t2.micro — Free tier eligible
Family: t2 1 vCPU 1 GiB Memory
On-Demand Linux pricing: 0.0116 USD per Hour
On-Demand Windows pricing: 0.0162 USD per Hour

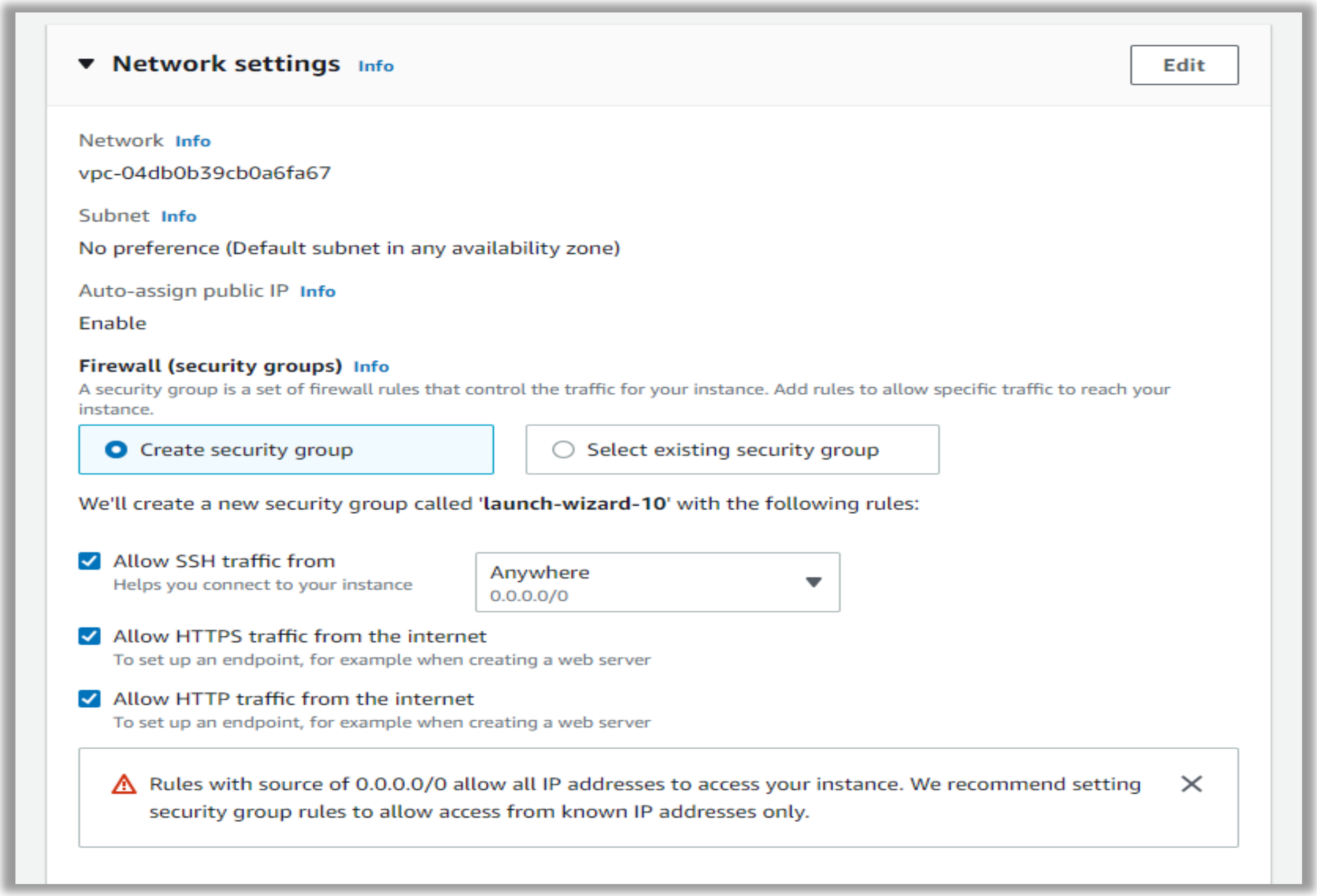
▼ Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Select

6. Make sure the below settings are reflected in your Instance



▼ Network settings Info

Network Info
vpc-04db0b39cb0a6fa67

Subnet Info
No preference (Default subnet in any availability zone)

Auto-assign public IP Info
Enable

Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

We'll create a new security group called '**launch-wizard-10**' with the following rules:

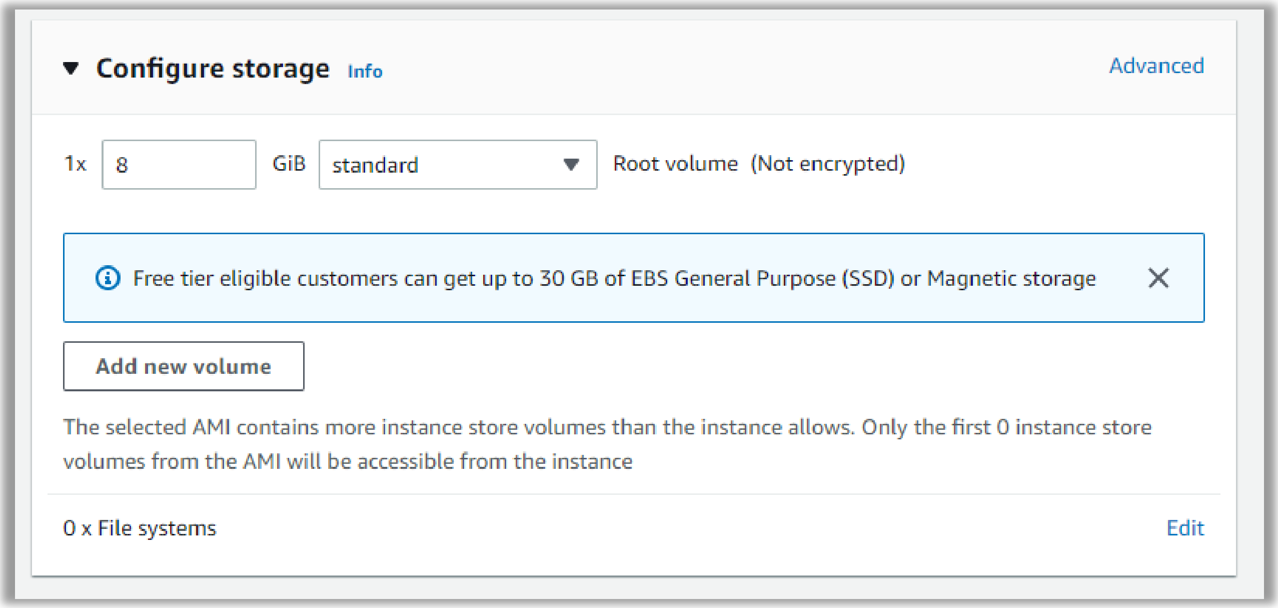
☑ Allow SSH traffic from — Anywhere 0.0.0.0/0
Helps you connect to your instance

☑ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

☑ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

7. Add storage as shown in below Image.



▼ Configure storage Info

Advanced

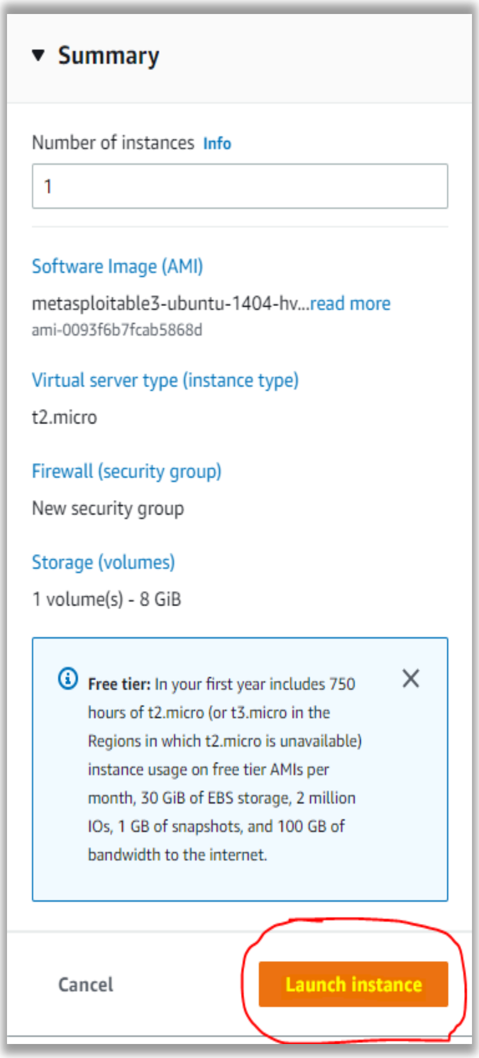
1x 8 GiB standard ▼ Root volume (Not encrypted)

ⓘ Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage ✕

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

0 x File systems

8. Review your Instance settings and then click on Launch Instances.



▼ Summary

Number of instances Info

1

Software Image (AMI)

metasploitable3-ubuntu-1404-hv...read more
ami-0093f6b7fcab5868d

Virtual server type (instance type)

t2.micro

Firewall (security group)

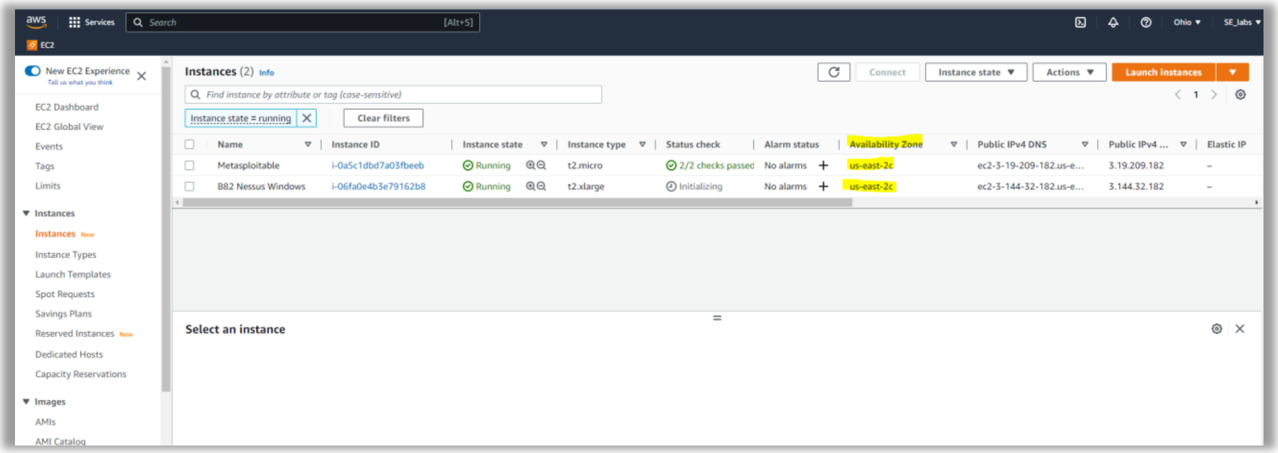
New security group

Storage (volumes)

1 volume(s) - 8 GiB

ⓘ **Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet. ✕

9. Make sure that both the Instances are working in same subnet, same subnet is mandatory to establish a bridge between both the Instances



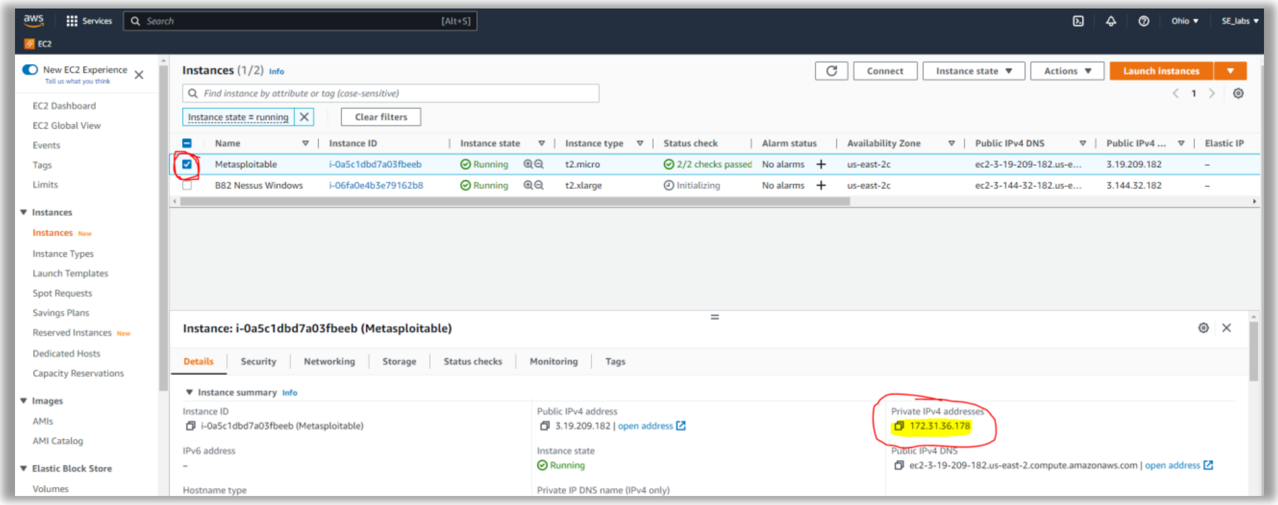
Instances (2) Info

Instance state = running

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
Metasploitable	i-0a5c1dbd7a03fbeeb	Running	t2.micro	2/2 checks passed	No alarms	us-east-2c	ec2-3-19-209-182.us-e...	3.19.209.182	–
B82 Nessus Windows	i-06fa0e4b3e79162b8	Running	t2.xlarge	Initializing	No alarms	us-east-2c	ec2-3-144-32-182.us-e...	3.144.32.182	–

Select an instance

10. Then select your Metasploitable Machine copy the Private IP as shown in below Image which acts as Target IP for your Tenable Nessus.



Instances (1/2) Info

Instance state = running

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
☑	Metasploitable	i-0a5c1dbd7a03fbeeb	Running	t2.micro	2/2 checks passed	No alarms	us-east-2c	ec2-3-19-209-182.us-e...	3.19.209.182	–
□	B82 Nessus Windows	i-06fa0e4b3e79162b8	Running	t2.xlarge	Initializing	No alarms	us-east-2c	ec2-3-144-32-182.us-e...	3.144.32.182	–

Instance: i-0a5c1dbd7a03fbeeb (Metasploitable)

Instance summary Info

Instance ID: i-0a5c1dbd7a03fbeeb (Metasploitable)

Public IPv4 address: 3.19.209.182 | open address

Private IPv4 addresses: 172.31.36.178

IPv6 address: –

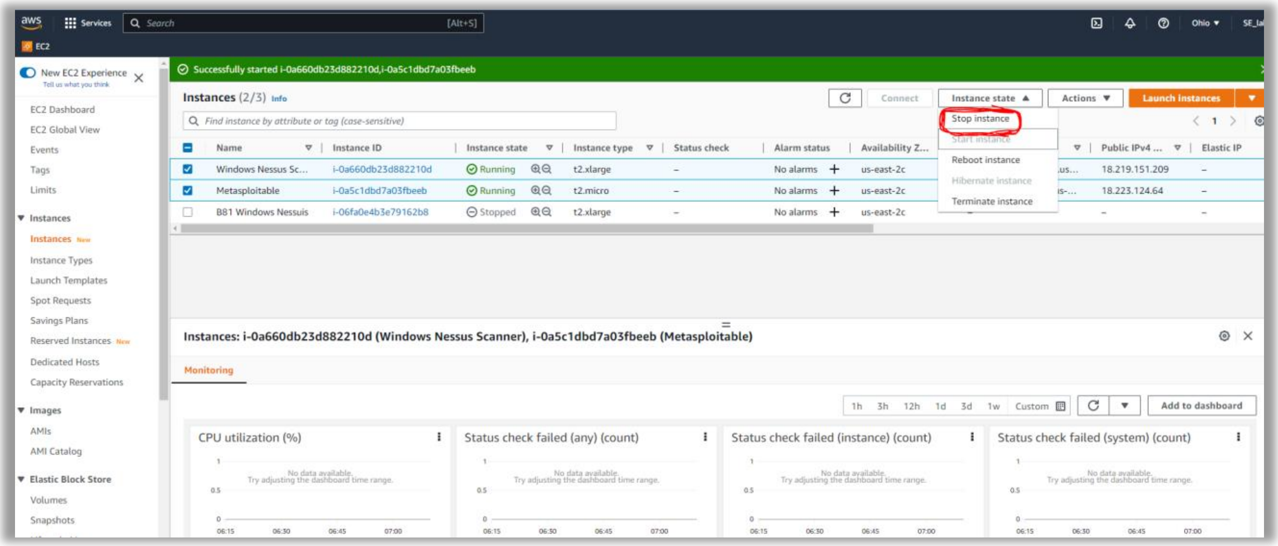
Instance state: Running

Public IPv4 DNS: ec2-3-19-209-182.us-east-2.compute.amazonaws.com | open address

Hostname type

Private IP DNS name (IPv4 only)

11. In the end make sure that you are stopping the Instances without fail to avoid getting charged.



Successfully started i-0a660db23d882210d,i-0a5c1dbd7a03fbeeb

Instances (2/3) Info

Instance state: Stop instance / Start instance / Reboot instance / Hibernate instance / Terminate instance

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Z...	Public IPv4 ...	Elastic IP
☑	Windows Nessus Sc...	i-0a660db23d882210d	Running	t2.xlarge	–	No alarms	us-east-2c	18.219.151.209	–
☑	Metasploitable	i-0a5c1dbd7a03fbeeb	Running	t2.micro	–	No alarms	us-east-2c	18.223.124.64	–
□	B81 Windows Nessuis	i-06fa0e4b3e79162b8	Stopped	t2.xlarge	–	No alarms	us-east-2c	–	–

Instances: i-0a660db23d882210d (Windows Nessus Scanner), i-0a5c1dbd7a03fbeeb (Metasploitable)

Monitoring

CPU utilization (%) · Status check failed (any) (count) · Status check failed (instance) (count) · Status check failed (system) (count)

No data available. Try adjusting the dashboard time range.

Congratulations you have successfully Completed Tenable Nessus Lab Installation and your First Vulnerable Report should be ready.