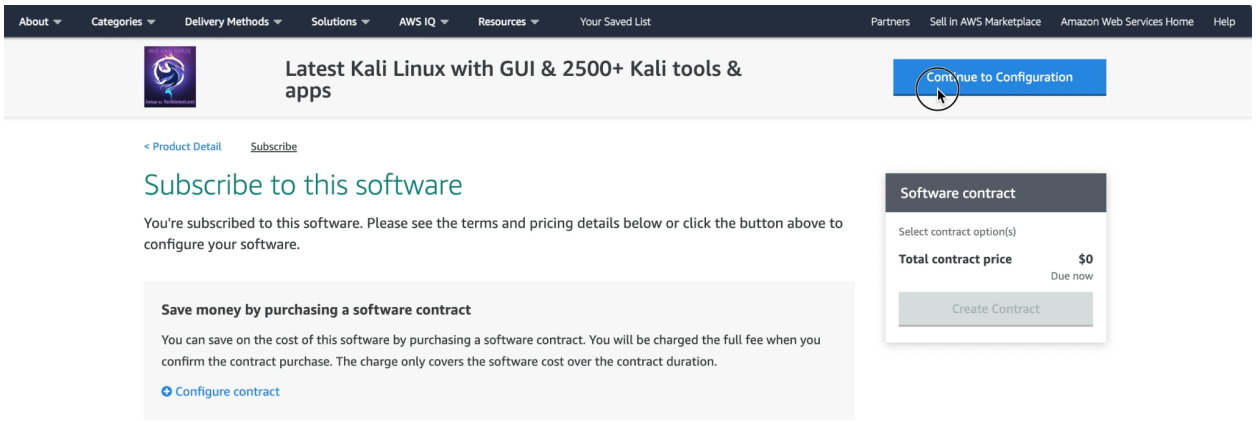
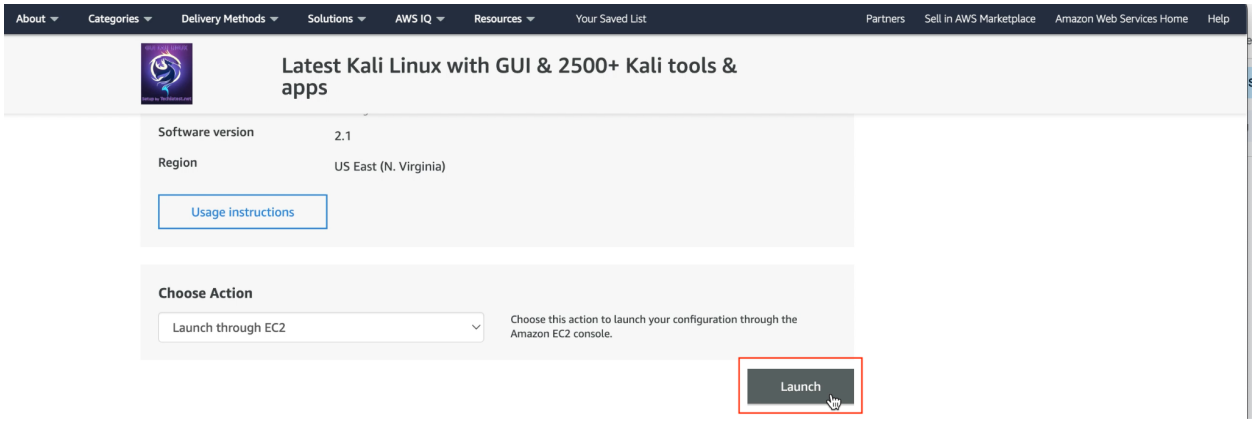
Using Kali Linux AMI EC2 to Install John the Ripper

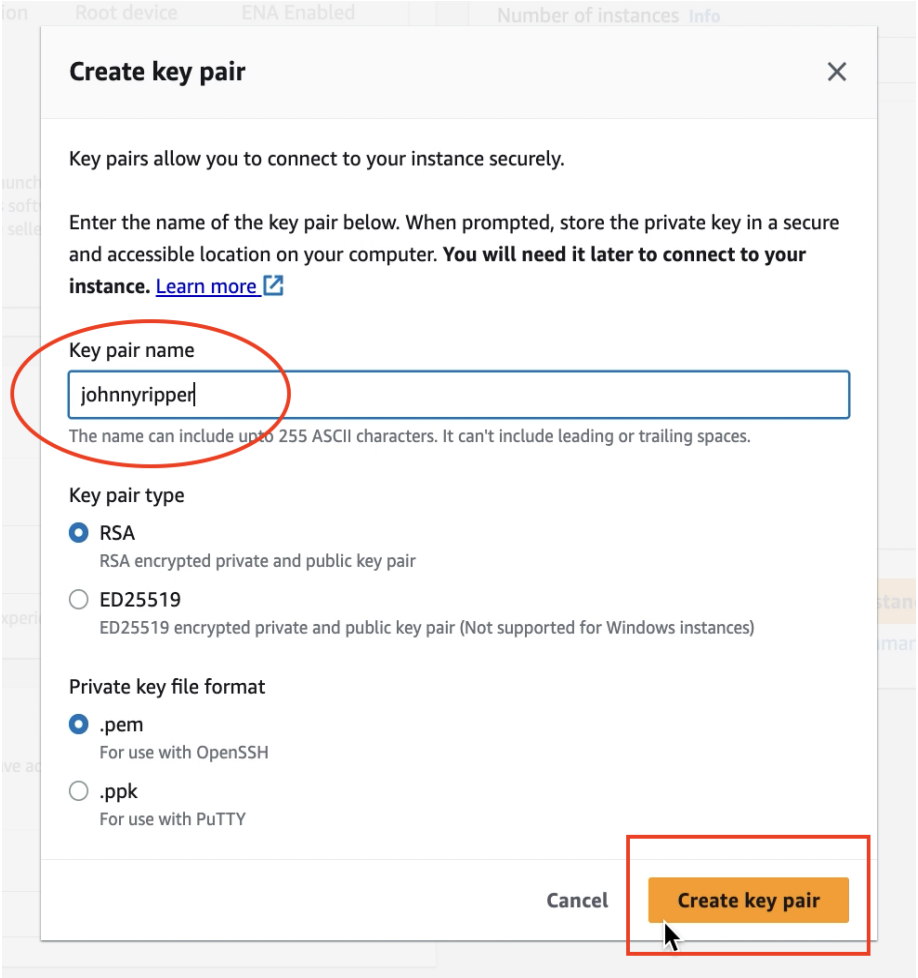
1. Sign into AWS and naviage to the following AMI website: https://aws.amazon.com/marketplace/pp/prodview-nll223ymffzm6?sr=0-2&ref_=beagle&applicationId=AWSMPContessa. Click “Subscribe” to this access AMI and press “Continue to Configure.” This will allow you to create the EC2 Instance using the Kali Linux AMI which has many of the tools already preinstalled.



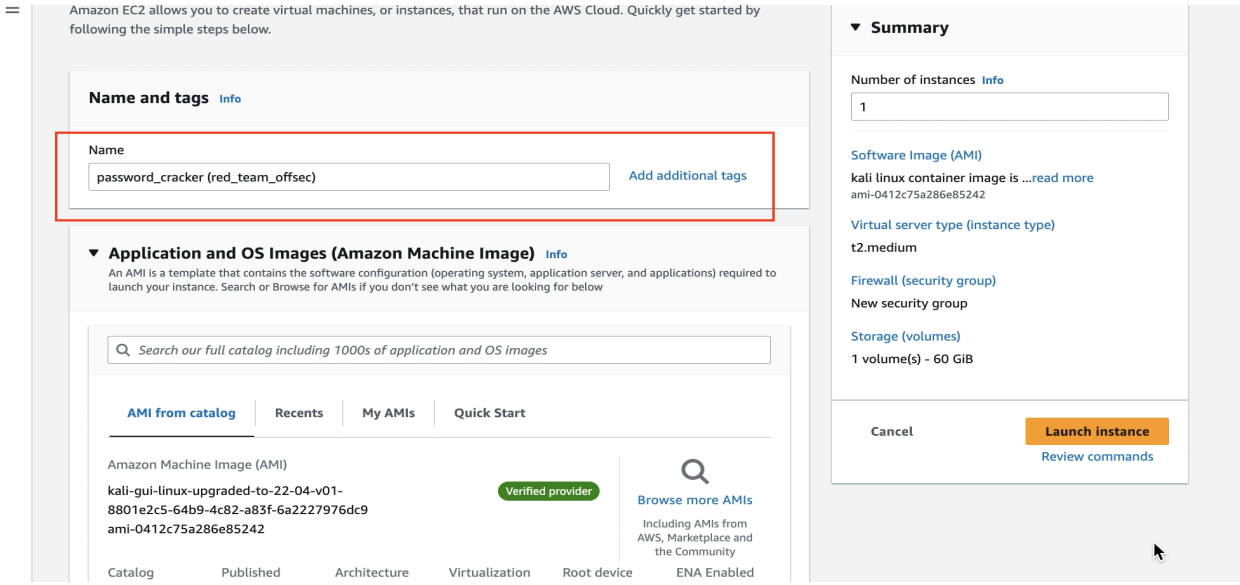
2. In “Choose Action” make sure that “Launch through EC2” is selected and click “Launch.”

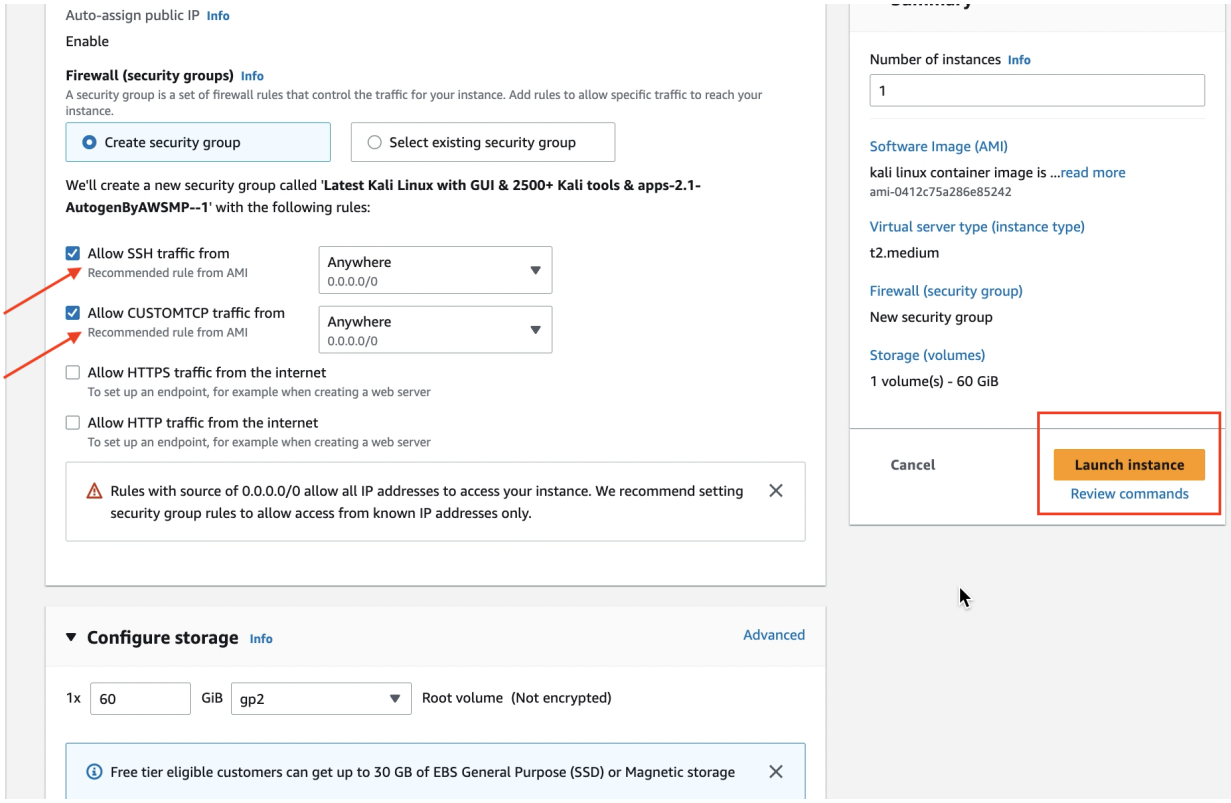


3. Choose a new keypair name. It will be used in Steps _____ to SSH into this EC2 instance.

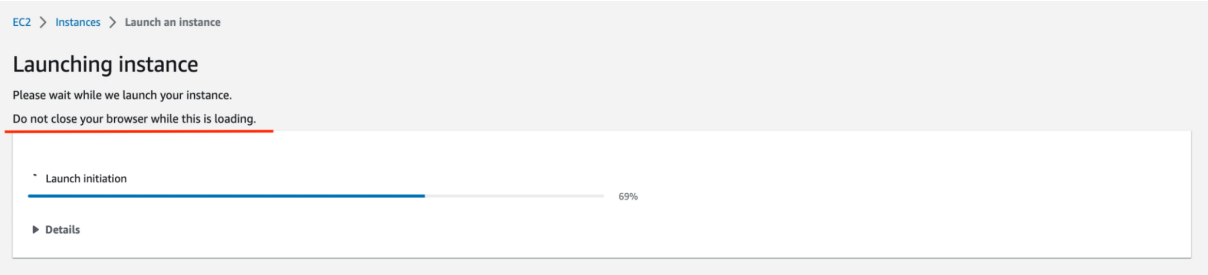


4. Here you can check your Instance options and include a name or additional security rules. Click Launch Instance.

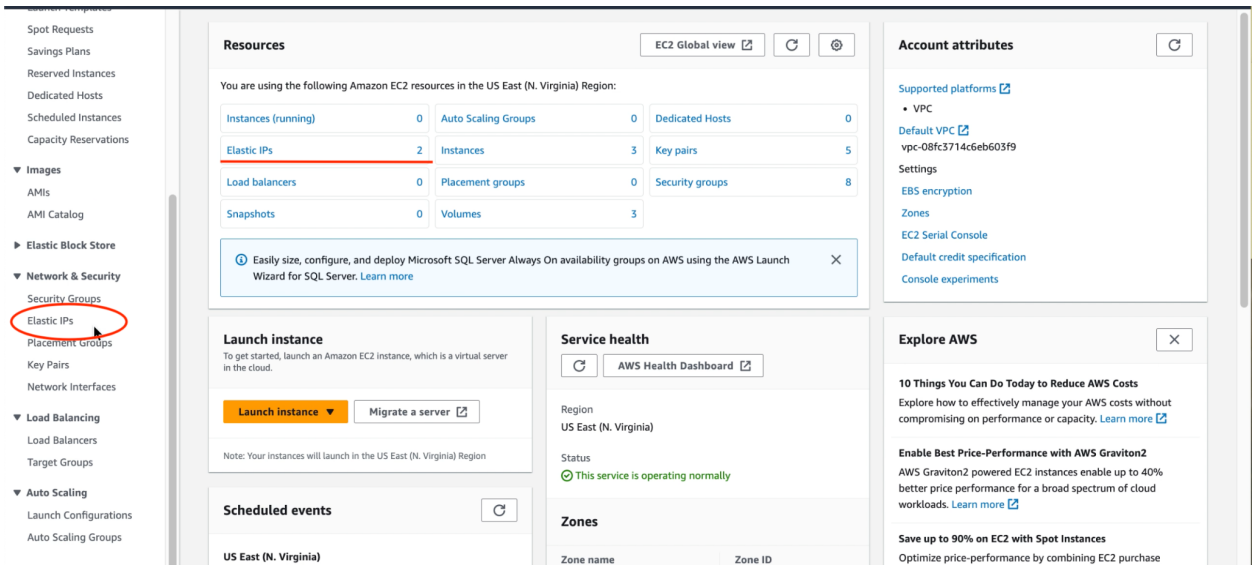




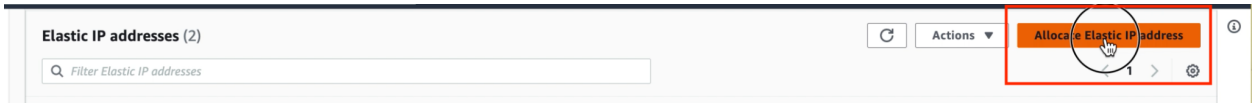
5. Wait for your Instance to Launch. Do not close the window while it's launching.



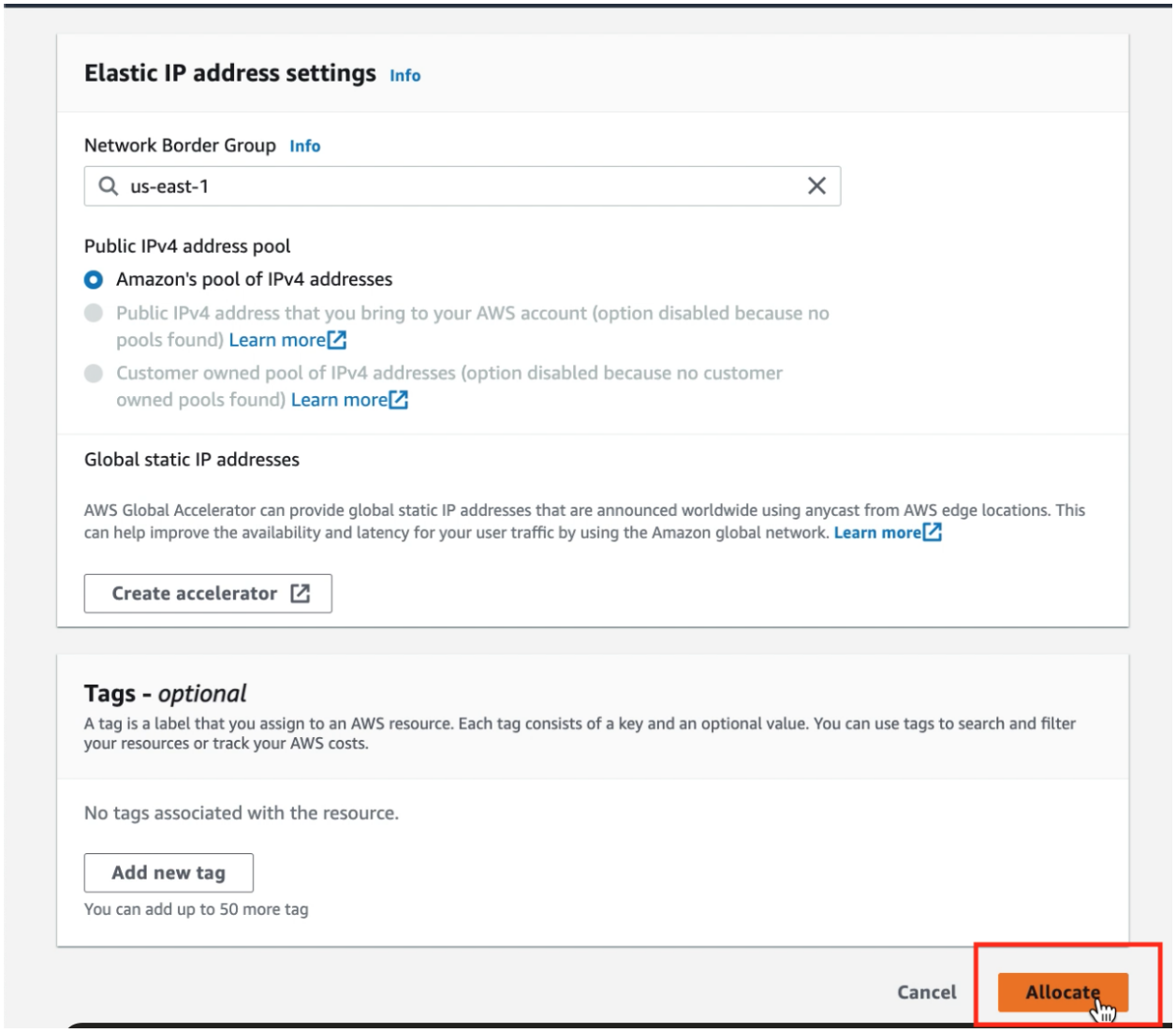
6. There are many ways to connect to your EC2 Instance. One way to do this is to SSH into the EC2 instance. There are also multiple ways to SSH into an EC2 Instance. One such way is to allocate and attach an Elastic IP. In order to do this, return to the EC2 Dashboard and select Elastic IP.



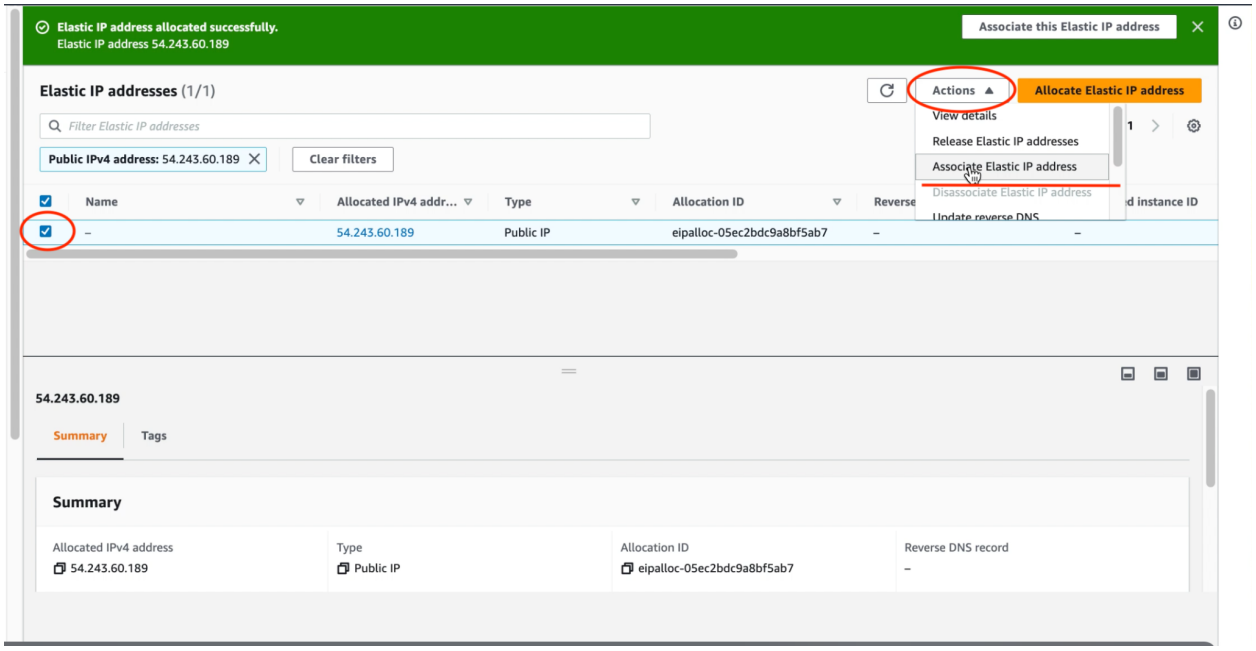
7. Select "Allocate Elastic IP Address"



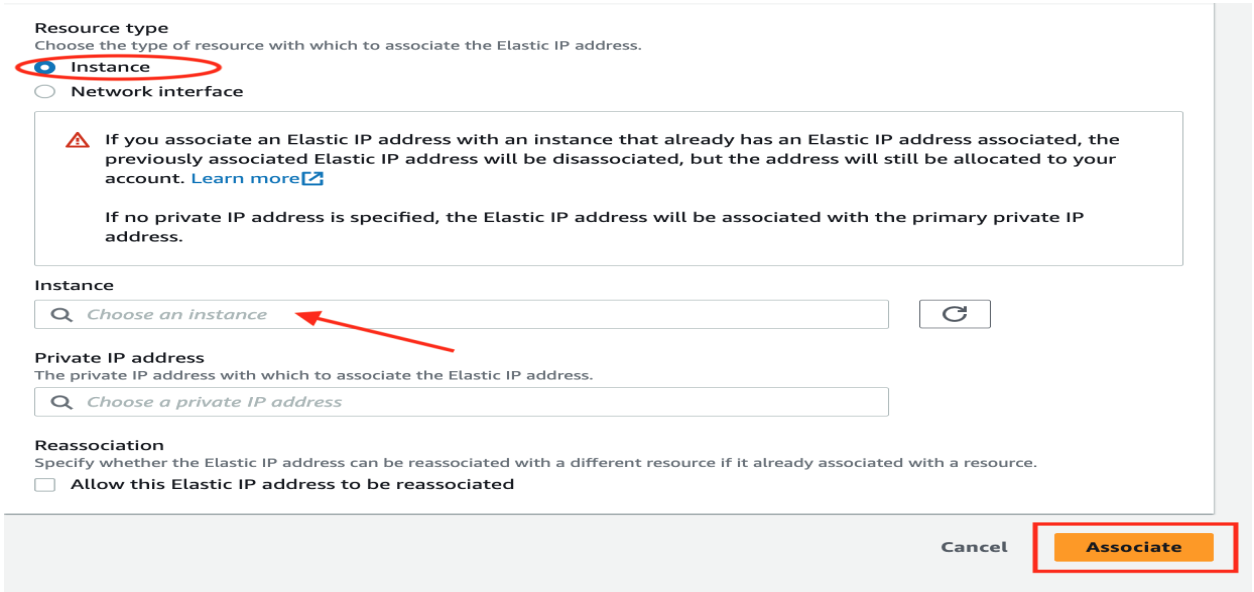
8. Under "Elastic IP address settings" choose your Network Border Group, Public IPv4 option and Tags. Click "Allocate."



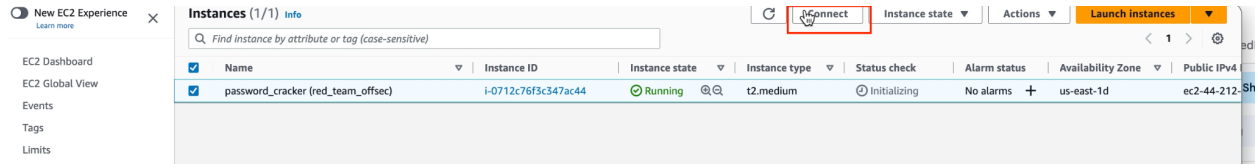
9. Usually, you will be redirected to Elastic IP menu, however, if you are not, you can return to the EC2 Dashboard. Here, you will attach the Elastic IP address to the EC2 Instance you have just created. First, make sure that you have the correct newly allocated Elastic IP selected with its checkbox marked. Then, click on the “Actions” button and select “Associate Elastic IP address.”



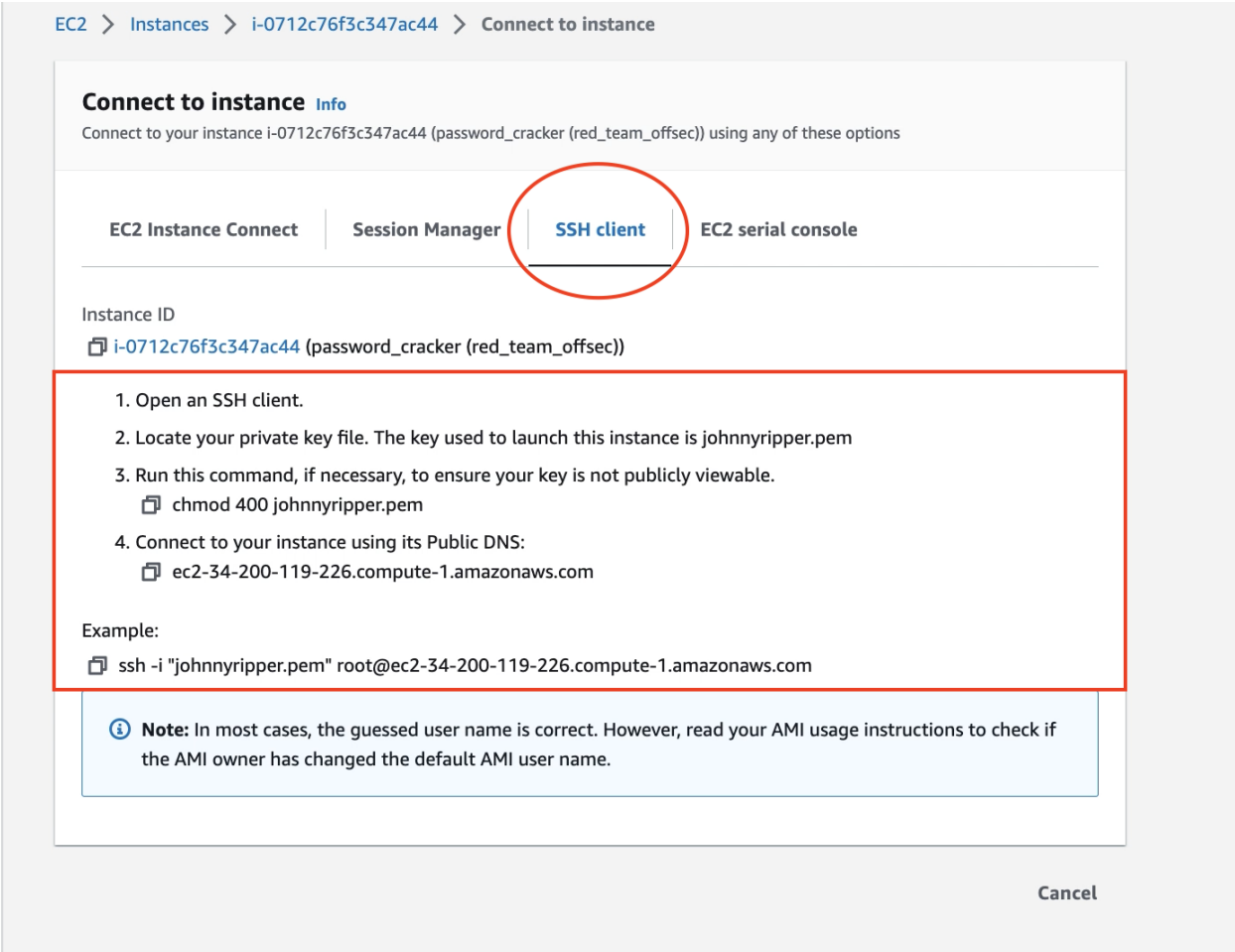
10. Within “Associate Elastic IP address” options, under “Resource type” select “Instance.” Click under “Instance” and a drop menu showing your EC2 Instances will appear. Select the instance you want to associate the Elastic IP address with. You also have the option of associating an Elastic IP address with a Private IP and whether to allow this Elastic IP address to be reassociated. Review your selections and click “Associate” to attach the Elastic IP to your EC2 Instance.



11. Return to the EC2 Dashboard. Click on the checkbox next to your EC2 Instance name and click “Connect.”

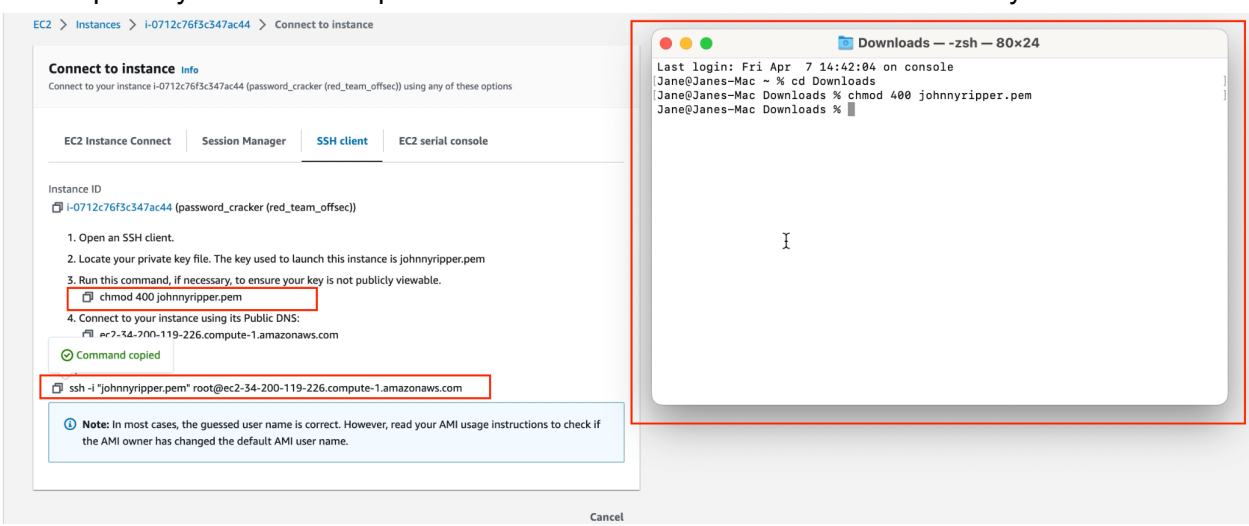


12. Under “Connect to instance,” click on “SSH client” tab for instructions on how to SSH into the EC2 Instance.

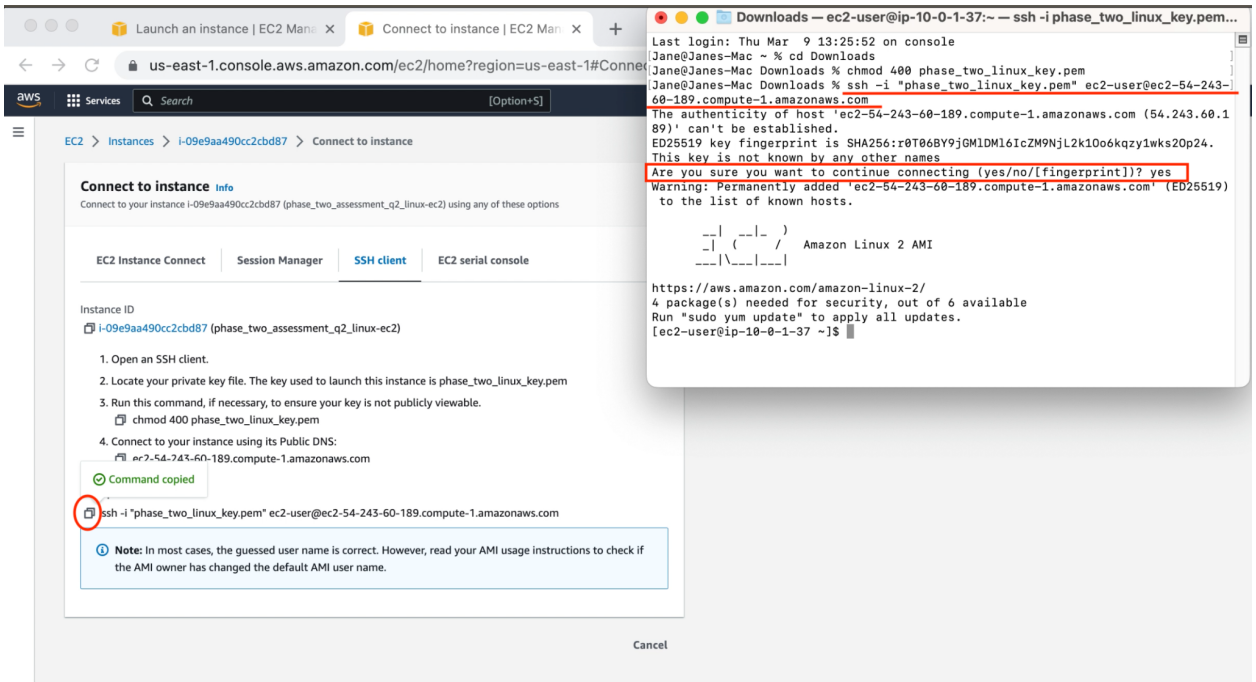


13. Open the application that will allow you to SSH into the EC2 Instance, in this case, it is a Mac terminal. Use the “`cd ..`” (without the quotation marks) command to move from directory to directory until you are in your Downloads folder.

14. From the “SSH client” tab, copy the command that will ensure your key pair is not publicly viewable and paste it into the terminal CLI. Press the Enter key.



15. From the “SSH client” tab, copy the command under “Example” that will allow you to securely connect to and SSH into the EC2 Instance with your key pair and paste it into the terminal CLI. Press the Enter key.



16. After displaying a message regarding the security of the host, you will be prompted to answer the question, “Are you sure you want to continue connecting (yes/no/[fingerprint])?” Type `yes` as your answer and press the Enter key.

```
Downloads — fish /home/ubuntu — ssh -i johnnyripper.pem ubuntu@ec2-...
* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

  System information as of Fri 07 Apr 2023 06:59:05 PM UTC

  System load:  1.93                Processes:               149
  Usage of /:   39.3% of 58.09GB    Users logged in:         0
  Memory usage: 9%                  IPv4 address for docker0: 172.17.0.1
  Swap usage:   0%                  IPv4 address for eth0:    172.31.81.194

  Get cloud support with Ubuntu Advantage Cloud Guest:
    http://www.ubuntu.com/business/services/cloud

86 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Fri Mar  3 18:56:47 2023 from 183.82.205.194
Welcome to fish, the friendly interactive shell
ubuntu@ip-172-31-81-194 ~>
```

17. After successfully SSH-ing into the EC2 instance, run the following command: `sudo apt update`. This will ensure your Kali Linux EC2 is up to date before installing John the Ripper

```
Downloads — sudo /home/ubuntu — ssh -i johnnyripper.pem ubuntu@ec2...
  Usage of /:   39.3% of 58.09GB    Users logged in:         0
  Memory usage: 9%                  IPv4 address for docker0: 172.17.0.1
  Swap usage:   0%                  IPv4 address for eth0:    172.31.81.194

  Get cloud support with Ubuntu Advantage Cloud Guest:
    http://www.ubuntu.com/business/services/cloud

86 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Fri Mar  3 18:56:47 2023 from 183.82.205.194
Welcome to fish, the friendly interactive shell
ubuntu@ip-172-31-81-194 ~> sudo apt update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-updates InRelease [11
4 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-backports InRelease [
108 kB]
Get:4 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
0% [Working]
```

18. Once the update is complete, type the following command to begin downloading John the Ripper: `sudo snap install john-the-ripper  # version roll+15b3b7c`. This will download John-the-Ripper onto the Kali Linux EC2.

```
Downloads — sudo /home/ubuntu — ssh -i johnnyripper.pem ubuntu@ec2...
[165 kB]
Get:28 http://security.ubuntu.com/ubuntu focal-security/universe amd64 c-n-f Met
adata [17.6 kB]
Get:29 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 Package
s [22.9 kB]
Get:30 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 c-n-f M
etadata [516 B]
Fetched 11.9 MB in 3s (4,341 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
125 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ip-172-31-81-194 ~> john

Command 'john' not found, but can be installed with:

sudo snap install john-the-ripper  # version roll+15b3b7c, or
sudo apt  install john             # version 1.8.0-2build1

See 'snap info john-the-ripper' for additional versions.

ubuntu@ip-172-31-81-194 ~ [127]>
sudo snap install john-the-ripper  # version roll+15b3b7c
Download snap "john-the-ripper" (581) from channel "stable"  100% 17.9MB/s 0.0ns
```

19. Once the download is complete, run the following command to install John-the-Ripper: `sudo apt install john`

```
Downloads — sudo /home/ubuntu — ssh -i johnnyripper.pem ubuntu@ec2...
Created directory: /home/ubuntu/snap/john-the-ripper/581/.john/opencl
Unknown option: "--version"
ubuntu@ip-172-31-81-194 ~ [1]> sudo apt install john
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libfwupdplugin1 libllvm11 linux-aws-headers-5.4.0-1041
  linux-headers-5.4.0-1041-aws linux-image-5.4.0-1041-aws
  linux-modules-5.4.0-1041-aws xbase-clients
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  john-data
The following NEW packages will be installed:
  john john-data
0 upgraded, 2 newly installed, 0 to remove and 125 not upgraded.
Need to get 4,466 kB of archives.
After this operation, 7,875 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal/main amd64 john-data
all 1.8.0-2build1 [4,276 kB]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal/main amd64 john amd64
 1.8.0-2build1 [189 kB]
87% [2 john 8,289 B/189 kB 4%]
```

20. To double check that John-the-Ripper is now a tool available within your instance, run the following command: `john`

Downloads — fish /home/ubuntu — ssh -i johnnyripper.pem ubuntu@ec2-...

```
Usage: john [OPTIONS] [PASSWORD-FILES]
--single                  "single crack" mode
--wordlist=FILE --stdin   wordlist mode, read words from FILE or stdin
--rules                   enable word mangling rules for wordlist mode
--incremental[=MODE]      "incremental" mode [using section MODE]
--external=MODE           external mode or word filter
--stdout[=LENGTH]         just output candidate passwords [cut at LENGTH]
--restore[=NAME]          restore an interrupted session [called NAME]
--session=NAME            give a new session the NAME
--status[=NAME]           print status of a session [called NAME]
--make-charset=FILE       make a charset, FILE will be overwritten
--show                    show cracked passwords
--test[=TIME]             run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..] [do not] load this (these) user(s) only
--groups=[-]GID[,..]      load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..]    load users with[out] this (these) shell(s) only
--salts=[-]N              load salts with[out] at least N passwords only
--save-memory=LEVEL       enable memory saving, at LEVEL 1..3
--node=MIN[-MAX]/TOTAL    this node's number range out of TOTAL count
--fork=N                  fork N processes
--format=NAME             force hash type NAME: descrypt/bsdicrypt/md5crypt/
                          bcrypt/LM/AFS/tripcode/dummy/crypt
ubuntu@ip-172-31-81-194 ~>
```