AWS HONEYPOT CONFIGURATION LAB

By Brennen Tse

3/12/23

Purpose:

The purpose of this lab is to create a honeypot and observe and document the attacks and vulnerabilities that are exploited to try to gain access to the system. I will likely be running two AWS honeypots, one on the west coast and one on the east coast, both for a week and comparing the results.

Background:

Honeypots are a type of cybersecurity tool that is designed to detect and monitor unauthorized access to computer systems. They are essentially decoy systems that are intentionally left vulnerable to attract and distract attackers. By luring attackers to these systems, security professionals can gain valuable insight into their methods and motives, as well as behaviors.

Amazon Web Services (AWS) is a popular platform for hosting honeypots because it offers a high level of scalability, flexibility, and security. With AWS, security professionals can easily spin up and configure multiple honeypot instances across the country, and they can also take advantage of AWS's advanced security features, such as encryption and network isolation, ensuring that even if a honeypot is breached, that intrusion is contained and can be remediated.

One popular honeypot software that can be hosted on AWS is the T-Pot GitHub honeypot. T-Pot is an open-source tool that provides a fully functional honeypot environment, complete with a range of pre-installed services and tools, like honeypots resembling mail severs, shell environments, web servers, and much more. It is designed to be easy to deploy and configure, and it can be customized to suit the specific needs of individual users.

Overall, honeypots are an important tool in the fight against cyber threats, and AWS is a powerful platform for hosting and managing these tools. By using tools like T-Pot, security professionals can gain valuable insight into the tactics and techniques used by attackers, and they can use this information to better protect their systems and networks.

Resources/Prerequisites:

AWS Account

https://github.com/telekom-security/tpotce

PuTTY

Debian EC2 Instance

18 cents an hour

Lab Commands:

sudo apt install git: This command installs the Git version control system, ensuring Git is installed on the system and ready to use.

sudo apt update: “sudo apt update” updates the package lists on the Linux system from the repositories. It doesn’t install or upgrade packages but retrieves information about available updates and their dependencies.

sudo apt upgrade: “sudo apt upgrade” upgrades all installed packages to their latest versions.

git clone https://github.com/telekom-security/tpotce: This command copies the GitHub Telekom tpotce repository.

cd tpotce/iso/installer/: This command navigates to the directory the repository is stored in.

sudo ./install.sh –type=user: This command runs the script of install.sh with elevated privileges using “sudo” while the –type=user ensures the software is only installed for the specified user, rather than all users on the system.

Diagram of Network Topology:

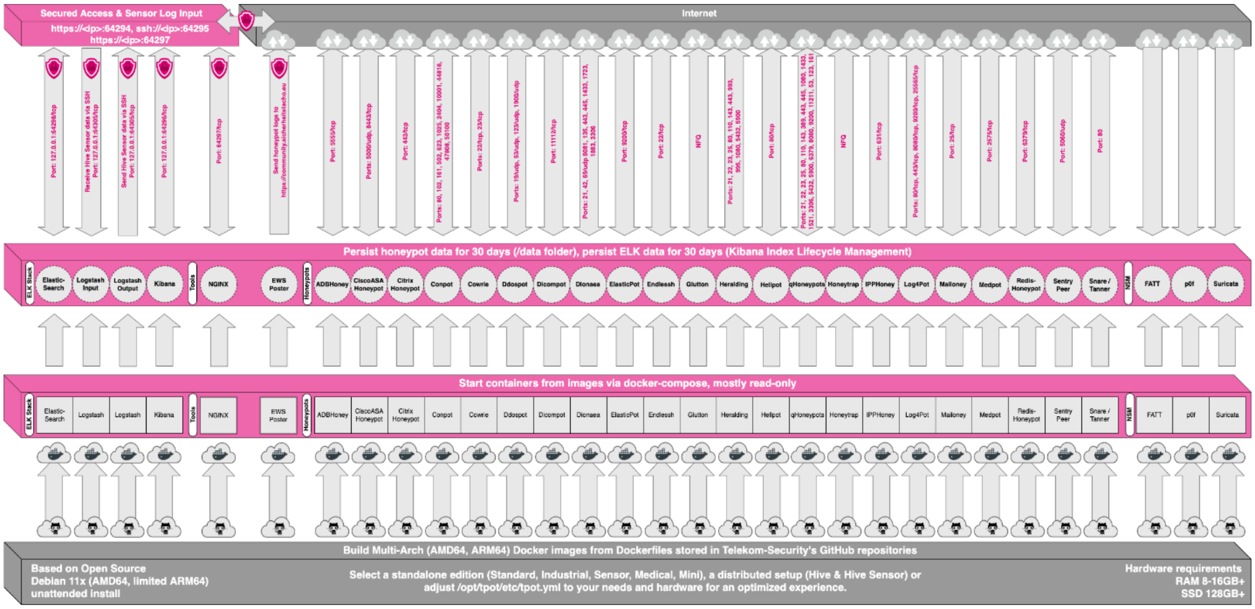
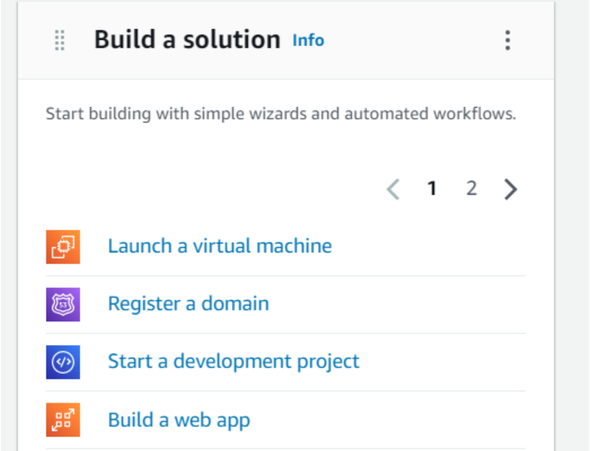
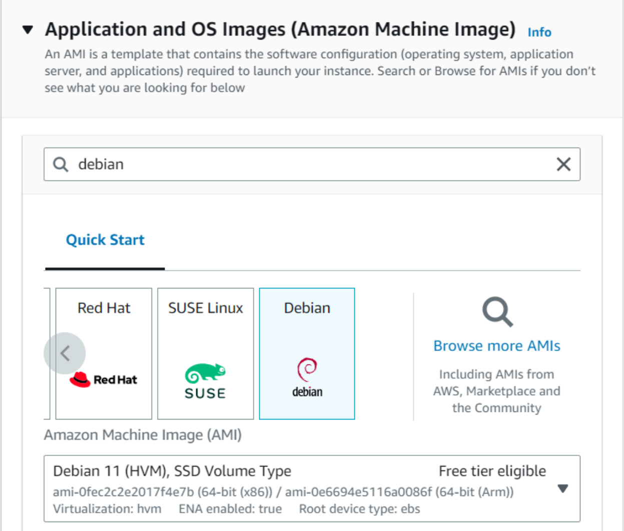
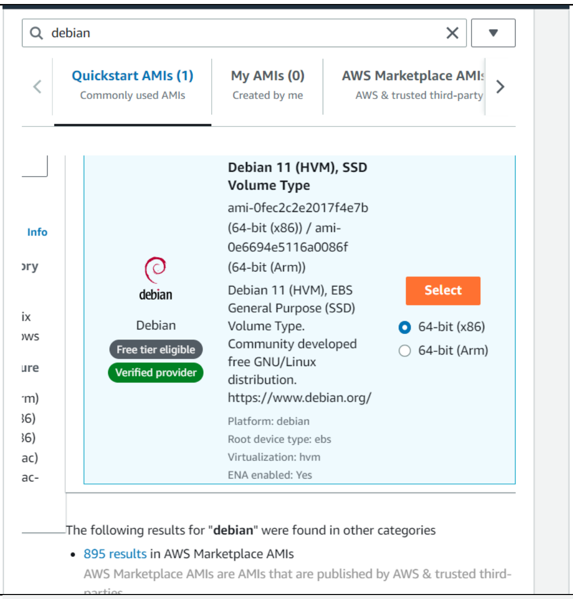

Secured Access & Sensor Log Input
https://<ip>:64294, ssh://<ip>:64295
https://<ip>:64297
Internet
Port: 127.0.0.1:64298/tcp
Receive Hive Sensor data via SSH Port: 127.0.0.1:64305/tcp
Send Hive Sensor data via SSH Port: 127.0.0.1:64305/tcp
Port: 127.0.0.1:64298/tcp
Port: 64297/tcp
Send honeypot logs to https://community.sicherheitstacho.eu
Port: 5555/tcp
Ports: 5000/udp, 8443/tcp
Port: 443/tcp
Ports: 80, 102, 161, 502, 623, 1025, 2404, 10001, 44818, 47808, 50100
Ports: 22/tcp, 23/tcp
Ports: 19/udp, 53/udp, 123/udp, 1900/udp
Port: 11112/tcp
Ports: 21, 42, 69/udp 8081, 135, 443, 445, 1433, 1723, 1883, 3306
Port: 9200/tcp
Port: 22/tcp
NFQ
Ports: 21, 22, 23, 25, 80, 110, 143, 443, 993, 995, 1080, 5432, 5900
Port: 80/tcp
Ports: 21, 22, 23, 25, 80, 110, 143, 389, 443, 445, 1080, 1433, 1521, 3306, 5432, 5900, 6379, 8080, 9200, 11211, 53, 123, 161
NFQ
Port: 631/tcp
Ports: 80/tcp, 443/tcp, 8080/tcp, 9200/tcp, 25565/tcp
Port: 25/tcp
Port: 2575/tcp
Port: 6379/tcp
Port: 5060/udp
Port: 80
Persist honeypot data for 30 days (/data folder), persist ELK data for 30 days (Kibana Index Lifecycle Management)
ELK Stack
Elastic-Search
Logstash Input
Logstash Output
Kibana
Tools
NGINX
EWS Poster
Honeypots
ADBHoney
CiscoASA Honeypot
Citrix Honeypot
Conpot
Cowrie
Ddospot
Dicompot
Dionaea
ElasticPot
Endlessh
Glutton
Heralding
Hellpot
qHoneypots
Honeytrap
IPPHoney
Log4Pot
Mailoney
Medpot
Redis-Honeypot
Sentry Peer
Snare / Tanner
NSM
FATT
p0f
Suricata
Start containers from images via docker-compose, mostly read-only
ELK Stack
Elastic-Search
Logstash
Logstash
Kibana
Tools
NGINX
EWS Poster
Honeypots
ADBHoney
CiscoASA Honeypot
Citrix Honeypot
Conpot
Cowrie
Ddospot
Dicompot
Dionaea
ElasticPot
Endlessh
Glutton
Heralding
Hellpot
qHoneypots
Honeytrap
IPPHoney
Log4Pot
Mailoney
Medpot
Redis-Honeypot
Sentry Peer
Snare / Tanner
NSM
FATT
p0f
Suricata
Build Multi-Arch (AMD64, ARM64) Docker images from Dockerfiles stored in Telekom-Security's GitHub repositories
Based on Open Source
Debian 11x (AMD64, limited ARM64)
unattended install
Select a standalone edition (Standard, Industrial, Sensor, Medical, Mini), a distributed setup (Hive & Hive Sensor) or adjust /opt/tpot/etc/tpot.yml to your needs and hardware for an optimized experience.
Hardware requirements
RAM 8-16GB+
SSD 128GB+

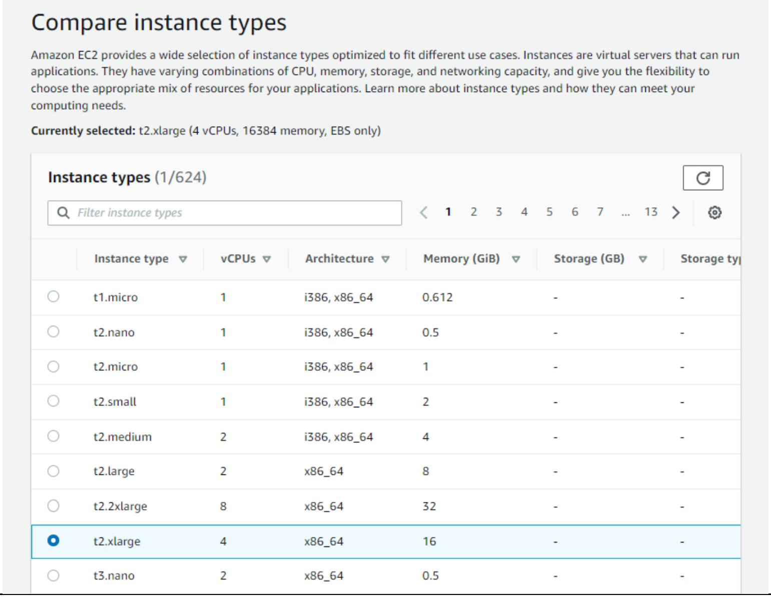
Table of Contents:

AWS Instance Creation

Sign into https://aws.amazon.com/ and log into AWS Management Console

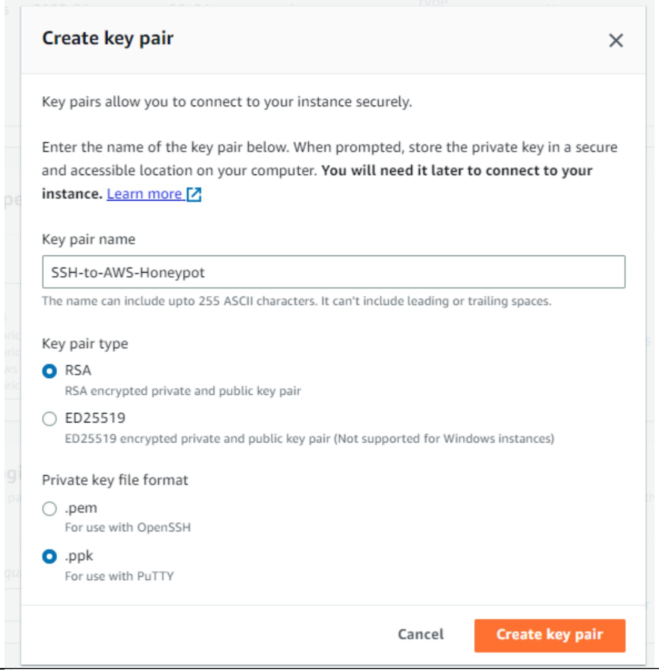
“Launch a virtual machine” or navigate to Services > EC2 > Instances, and click “Launch Instance”	 Build a solution Info Start building with simple wizards and automated workflows. 1 2 Launch a virtual machine Register a domain Start a development project Build a web app
	 Application and OS Images (Amazon 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 debian Quick Start Red Hat SUSE Linux Debian Browse more AMIs Including AMIs from AWS, Marketplace and the Community Amazon Machine Image (AMI) Debian 11 (HVM), SSD Volume Type Free tier eligible ami-0fec2c2e2017f4e7b (64-bit (x86)) / ami-0e6694e5116a0086f (64-bit (Arm)) Virtualization: hvm ENA enabled: true Root device type: ebs

<table>
<tr>
<td>You can choose different versions but I used the most recent, Debian 11. Select x86</td>
<td>


Debian
Free tier eligible
Verified provider
<b>Debian 11 (HVM), SSD Volume Type</b>
ami-0fec2c2e2017f4e7b (64-bit (x86)) / ami-0e6694e5116a0086f (64-bit (Arm))
Debian 11 (HVM), EBS General Purpose (SSD) Volume Type. Community developed free GNU/Linux distribution. https://www.debian.org/
Platform: debian
Root device type: ebs
Virtualization: hvm
ENA enabled: Yes
● 64-bit (x86)
○ 64-bit (Arm)
The following results for "<b>debian</b>" were found in other categories
• 895 results in AWS Marketplace AMIs
AWS Marketplace AMIs are AMIs that are published by AWS &amp; trusted third-parties
</td>
</tr>
<tr>
<td>Once you select Debian, you will be prompted to select the instance type. Click edit and navigate to t2.xlarge, giving us 4 CPUs and 16 GB of memory.</td>
<td>


Compare instance types
Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.
<b>Currently selected:</b> t2.xlarge (4 vCPUs, 16384 memory, EBS only)
<b>Instance types</b> (1/624)
<table>
<tr><th></th><th>Instance type</th><th>vCPUs</th><th>Architecture</th><th>Memory (GiB)</th><th>Storage (GB)</th><th>Storage ty</th></tr>
<tr><td>○</td><td>t1.micro</td><td>1</td><td>i386, x86_64</td><td>0.612</td><td>-</td><td>-</td></tr>
<tr><td>○</td><td>t2.nano</td><td>1</td><td>i386, x86_64</td><td>0.5</td><td>-</td><td>-</td></tr>
<tr><td>○</td><td>t2.micro</td><td>1</td><td>i386, x86_64</td><td>1</td><td>-</td><td>-</td></tr>
<tr><td>○</td><td>t2.small</td><td>1</td><td>i386, x86_64</td><td>2</td><td>-</td><td>-</td></tr>
<tr><td>○</td><td>t2.medium</td><td>2</td><td>i386, x86_64</td><td>4</td><td>-</td><td>-</td></tr>
<tr><td>○</td><td>t2.large</td><td>2</td><td>x86_64</td><td>8</td><td>-</td><td>-</td></tr>
<tr><td>○</td><td>t2.2xlarge</td><td>8</td><td>x86_64</td><td>32</td><td>-</td><td>-</td></tr>
<tr><td>●</td><td>t2.xlarge</td><td>4</td><td>x86_64</td><td>16</td><td>-</td><td>-</td></tr>
<tr><td>○</td><td>t3.nano</td><td>2</td><td>x86_64</td><td>0.5</td><td>-</td><td>-</td></tr>
</table>
</td>
</tr>
</table>

In order to access the AWS machine from Putty through an SSH session, we have to create a key pair. Choose the option to Create key pair. Make sure to create it as RSA and .ppk. It will automatically download once you click create. Save this in a safe place for later.



Create key pair

Key pairs allow you to connect to your instance securely.

Enter the name of the key pair below. When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** Learn more

Key pair name

SSH-to-AWS-Honeypot

The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

● RSA
RSA encrypted private and public key pair

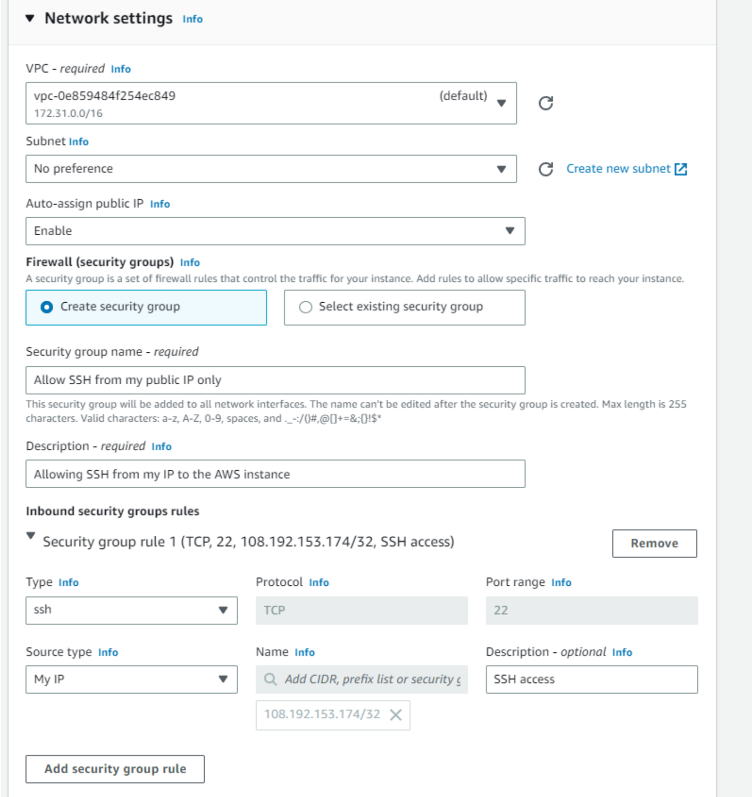
○ ED25519
ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format

○ .pem
For use with OpenSSH

● .ppk
For use with PuTTY

On the Configure Security Group page, click edit and create a new security group. Ensure the security group is type ssh, TCP 22, source is my IP. Add a description if you want to.



Network settings Info

VPC - *required* Info

vpc-0e859484f254ec849 (default)
172.31.0.0/16

Subnet Info

No preference

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

Security group name - *required*

Allow SSH from my public IP only

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* Info

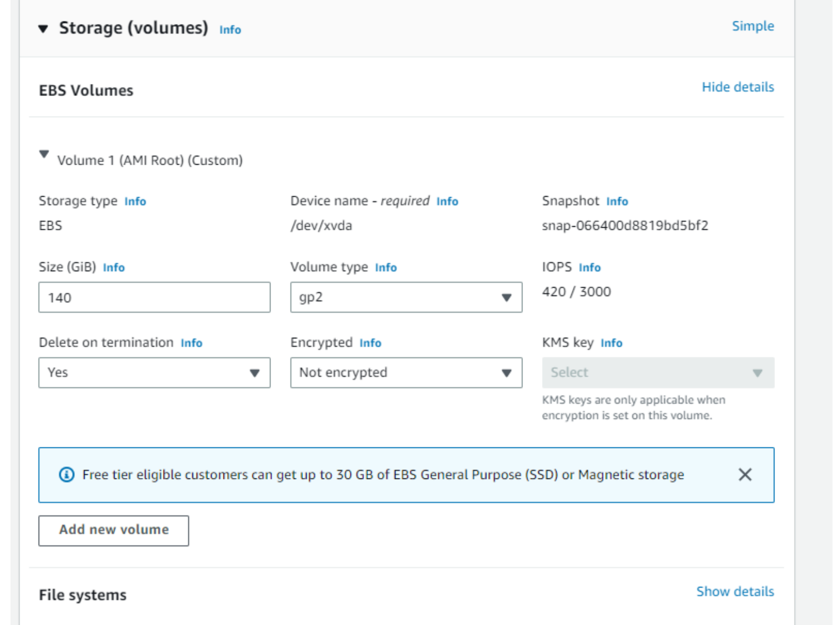
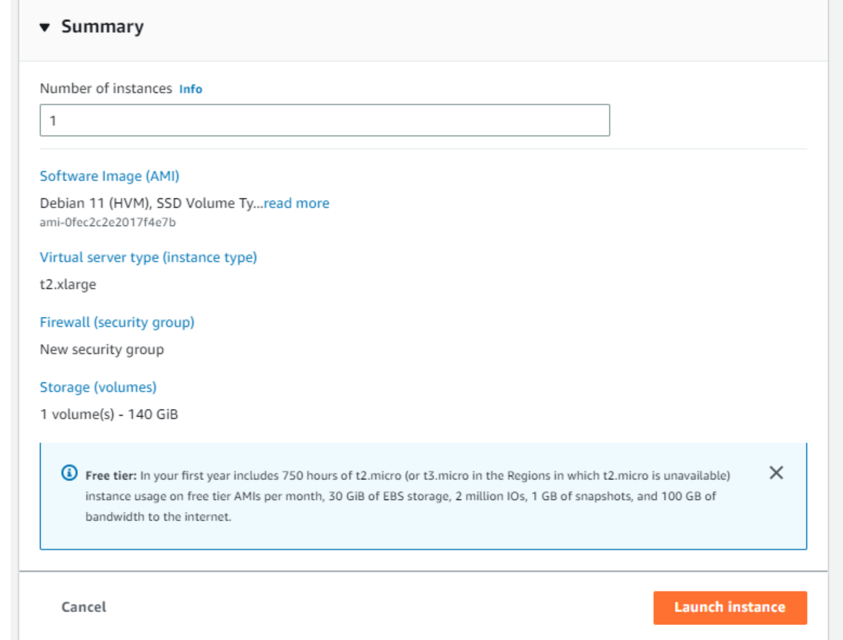
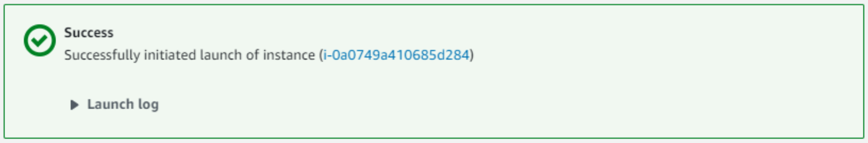
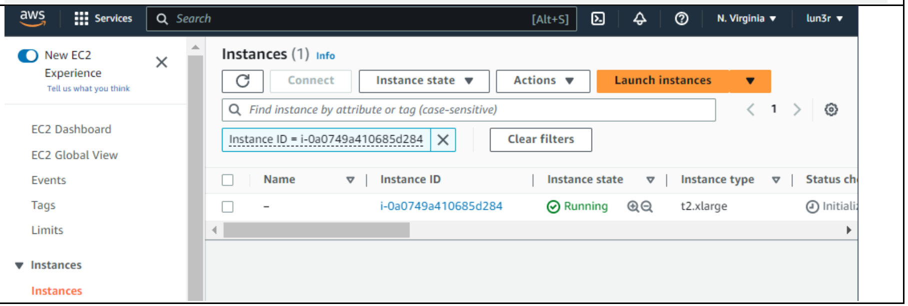
Allowing SSH from my IP to the AWS instance

Inbound security groups rules

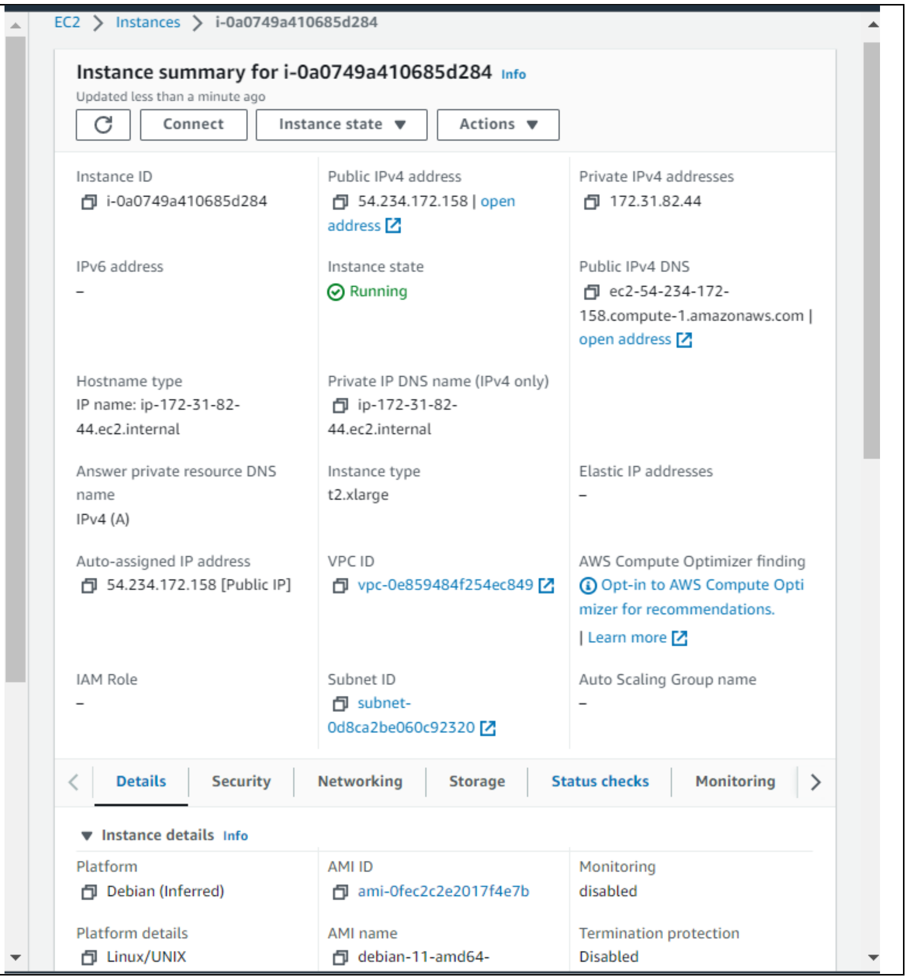
Security group rule 1 (TCP, 22, 108.192.153.174/32, SSH access)

Type Info	Protocol Info	Port range Info
ssh	TCP	22

Source type Info	Name Info	Description - *optional* Info
My IP	Add CIDR, prefix list or security g 108.192.153.174/32	SSH access

Finally add the storage, and adjust the storage size from 8 to 140GB. Keep the other default settings.	 Storage (volumes) Info — Simple EBS Volumes — Hide details Volume 1 (AMI Root) (Custom) Storage type Info: EBS Device name - *required* Info: /dev/xvda Snapshot Info: snap-066400d8819bd5bf2 Size (GiB) Info: 140 Volume type Info: gp2 IOPS Info: 420 / 3000 Delete on termination Info: Yes Encrypted Info: Not encrypted KMS key Info: Select KMS keys are only applicable when encryption is set on this volume. Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage Add new volume File systems — Show details
Check all your settings are correct and click Launch instance.	 Summary Number of instances Info: 1 Software Image (AMI) Debian 11 (HVM), SSD Volume Ty...read more ami-0fec2c2e2017f4e7b Virtual server type (instance type) t2.xlarge Firewall (security group) New security group Storage (volumes) 1 volume(s) - 140 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. Cancel — Launch instance
Click the instance ID to navigate to the Instance.	 Success Successfully initiated launch of instance (i-0a0749a410685d284) Launch log
Here you can see details about the instance, such as it's state, type, and status checks. Click into the instance ID again to get more details.	 aws Services Search [Alt+S] N. Virginia lun3r New EC2 Experience — Tell us what you think EC2 Dashboard EC2 Global View Events Tags Limits Instances Instances Instances (1) Info Connect — Instance state — Actions — Launch instances Find instance by attribute or tag (case-sensitive) Instance ID = i-0a0749a410685d284 — Clear filters Name | Instance ID | Instance state | Instance type | Status ch – | i-0a0749a410685d284 | Running | t2.xlarge | Initiali

Here we can see the IP address of 54.234.172.158. The private IP address, DNS, subnet, and other useful details. If you haven’t already also download Putty, but if not here’s a guide.



EC2 > Instances > i-0a0749a410685d284

Instance summary for i-0a0749a410685d284 Info

Updated less than a minute ago

Instance ID
i-0a0749a410685d284

Public IPv4 address
54.234.172.158 | open address

Private IPv4 addresses
172.31.82.44

IPv6 address
–

Instance state
Running

Public IPv4 DNS
ec2-54-234-172-158.compute-1.amazonaws.com | open address

Hostname type
IP name: ip-172-31-82-44.ec2.internal

Private IP DNS name (IPv4 only)
ip-172-31-82-44.ec2.internal

Answer private resource DNS name
IPv4 (A)

Instance type
t2.xlarge

Elastic IP addresses
–

Auto-assigned IP address
54.234.172.158 [Public IP]

VPC ID
vpc-0e859484f254ec849

AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations.
| Learn more

IAM Role
–

Subnet ID
subnet-0d8ca2be060c92320

Auto Scaling Group name
–

▼ Instance details Info

Platform
Debian (Inferred)

AMI ID
ami-0fec2c2e2017f4e7b

Monitoring
disabled

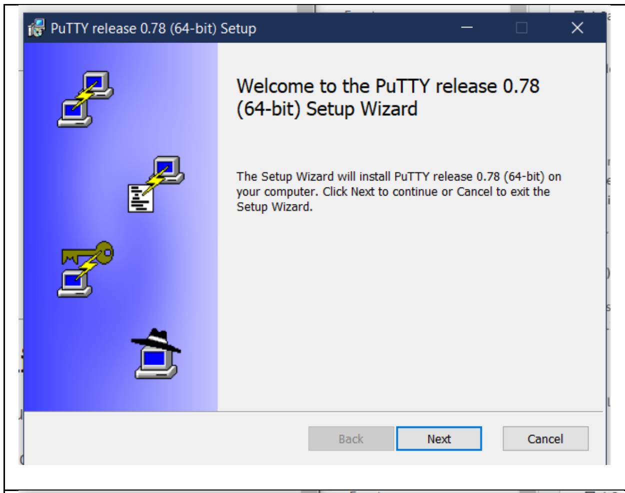
Platform details
Linux/UNIX

AMI name
debian-11-amd64-

Termination protection
Disabled

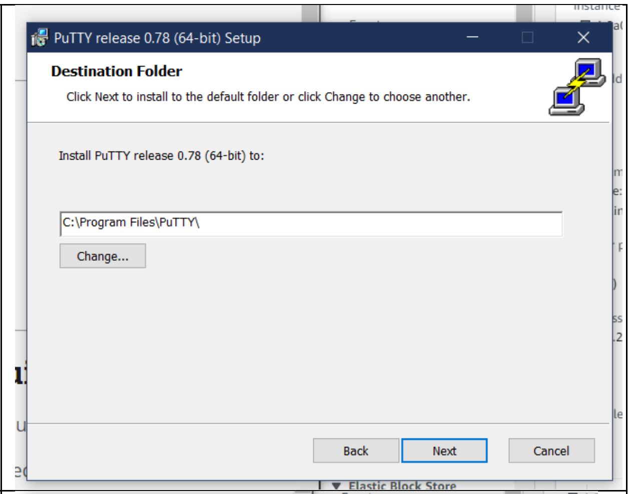
Downloading Putty:

Download from this link -> https://www.puttygen.com/download-putty



Welcome to the PuTTY release 0.78 (64-bit) Setup Wizard

The Setup Wizard will install PuTTY release 0.78 (64-bit) on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

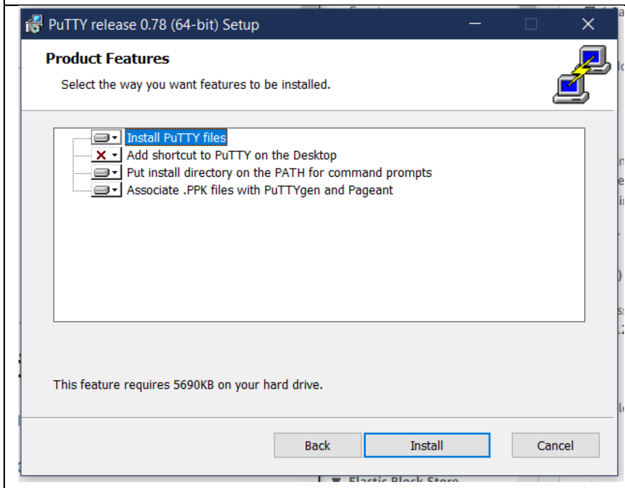


Destination Folder

Click Next to install to the default folder or click Change to choose another.

Install PuTTY release 0.78 (64-bit) to:

C:\Program Files\PuTTY\

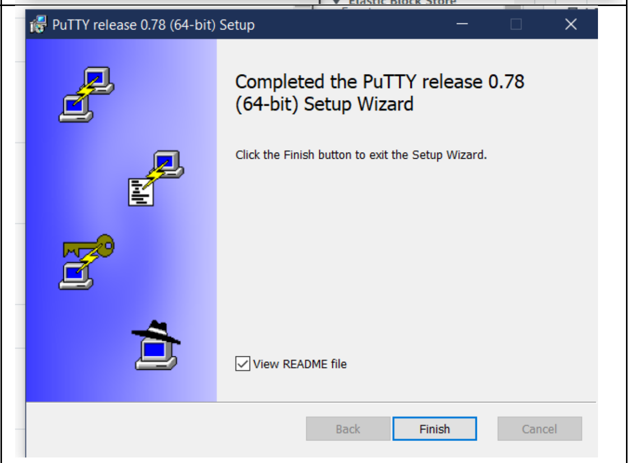


Product Features

Select the way you want features to be installed.

- Install PuTTY files
- Add shortcut to PuTTY on the Desktop
- Put install directory on the PATH for command prompts
- Associate .PPK files with PuTTYgen and Pageant

This feature requires 5690KB on your hard drive.



Completed the PuTTY release 0.78 (64-bit) Setup Wizard

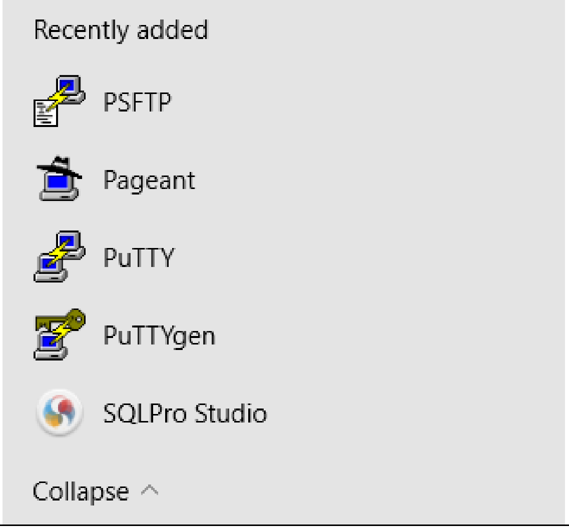
Click the Finish button to exit the Setup Wizard.

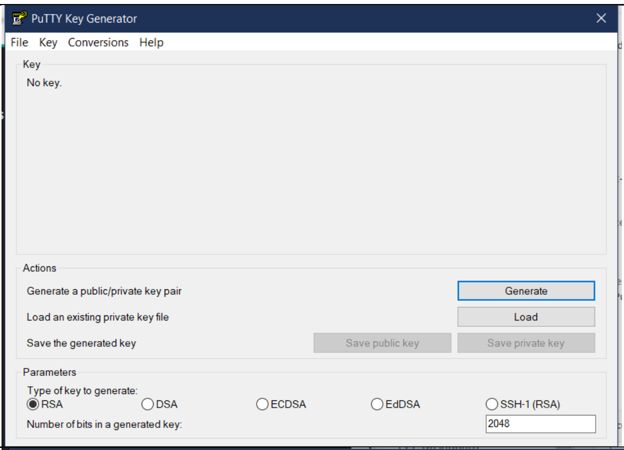
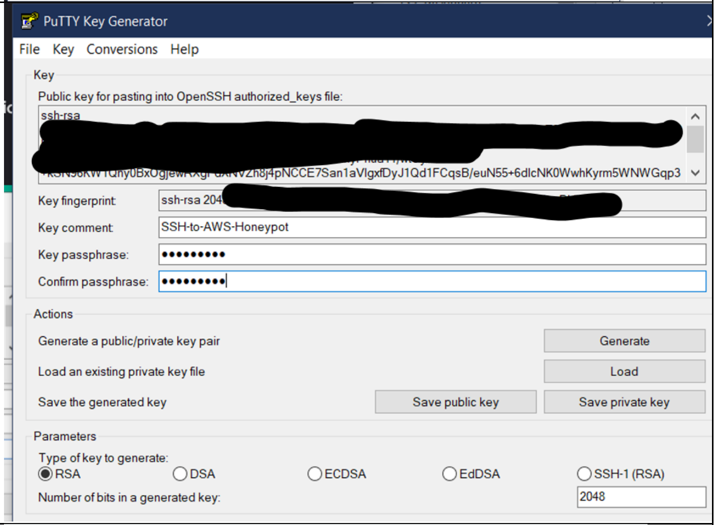
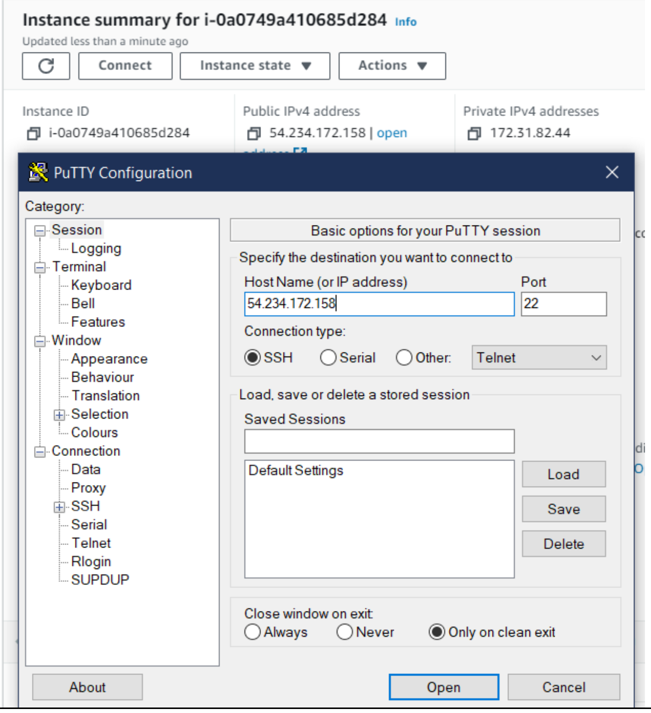
☑ View README file

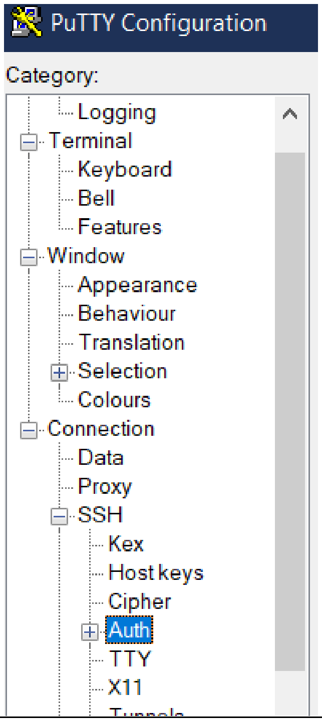
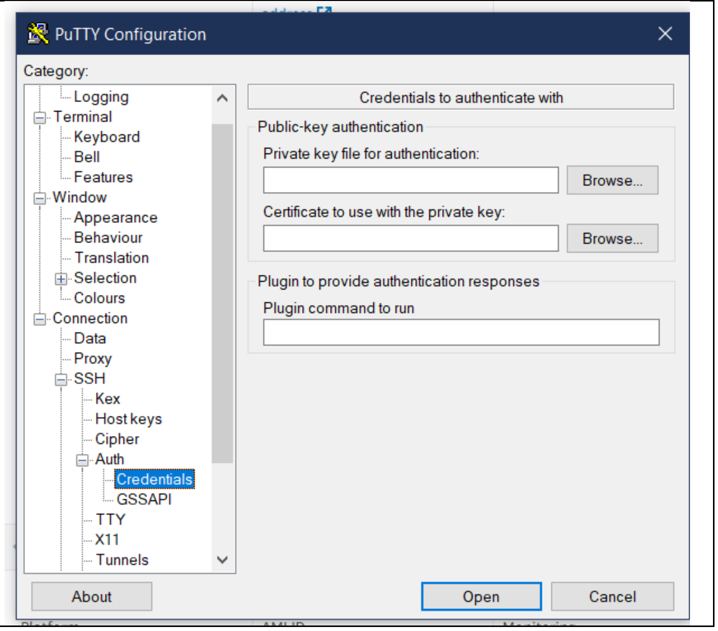
Now you have installed PuTTY

AWS Machine Logon

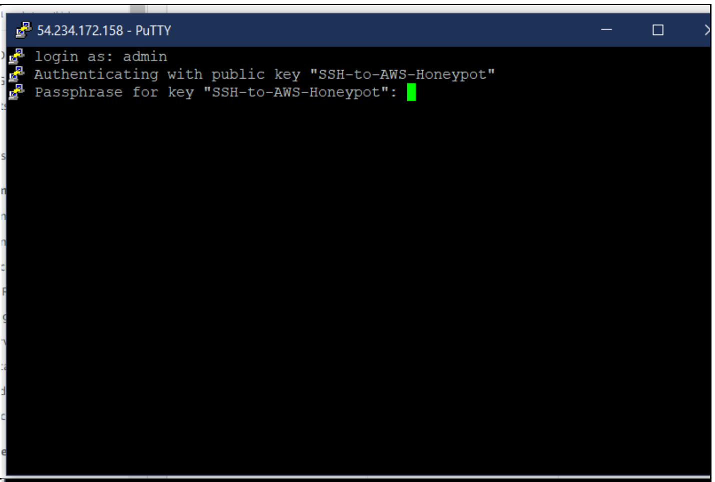
In the recently added section, you should find software called PuTTYgen. This will help us convert the key pair we downloaded earlier into a private key for PuTTY.



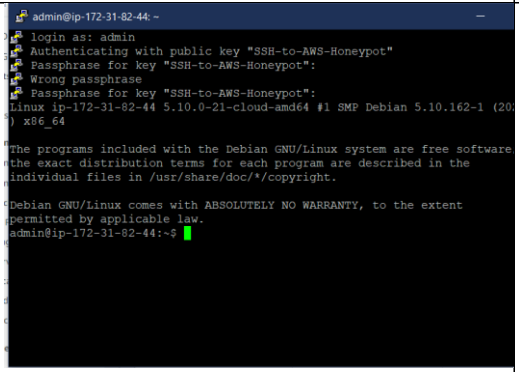
Click Load, and navigate to where you downloaded the key pair.	 PuTTY Key Generator Key: No key. Actions Generate a public/private key pair — Generate Load an existing private key file — Load Save the generated key — Save public key, Save private key Parameters Type of key to generate: ● RSA ○ DSA ○ ECDSA ○ EdDSA ○ SSH-1 (RSA) Number of bits in a generated key: 2048
Once loaded, give the key a passphrase, this will be how you log into the AWS machine. Save it as a private key, and rename it something different then the AWS key pair you downloaded earlier to reduce confusion. Keep this in a safe space too.	 PuTTY Key Generator Key Public key for pasting into OpenSSH authorized_keys file: ssh-rsa [redacted] Key fingerprint: ssh-rsa 204[redacted] Key comment: SSH-to-AWS-Honeypot Key passphrase: ••••••••• Confirm passphrase: ••••••••• Actions Generate a public/private key pair — Generate Load an existing private key file — Load Save the generated key — Save public key, Save private key Parameters Type of key to generate: ● RSA ○ DSA ○ ECDSA ○ EdDSA ○ SSH-1 (RSA) Number of bits in a generated key: 2048
Reopen PuTTY and enter in the public IP address or the public DNS of the AWS machine and port 22 for SSH. On the lefthand side navigate to	 Instance summary for i-0a0749a410685d284 Info Updated less than a minute ago Instance ID: i-0a0749a410685d284 Public IPv4 address: 54.234.172.158 | open Private IPv4 addresses: 172.31.82.44 PuTTY Configuration Basic options for your PuTTY session Specify the destination you want to connect to Host Name (or IP address): 54.234.172.158 Port: 22 Connection type: ● SSH ○ Serial ○ Other: Telnet Load, save or delete a stored session Saved Sessions: Default Settings Close window on exit: ○ Always ○ Never ● Only on clean exit

Connection>SSH>Auth>Credentials  PuTTY Configuration Category: Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy SSH Kex Host keys Cipher Auth TTY X11 Tunnels	
In the credentials section, use the private key you just created with PuTTYgen. Finally click Open to connect to the Debian 11 vm on AWS.	 PuTTY Configuration Category: Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy SSH Kex Host keys Cipher Auth Credentials GSSAPI TTY X11 Tunnels Credentials to authenticate with Public-key authentication Private key file for authentication: Browse... Certificate to use with the private key: Browse... Plugin to provide authentication responses Plugin command to run About Open Cancel

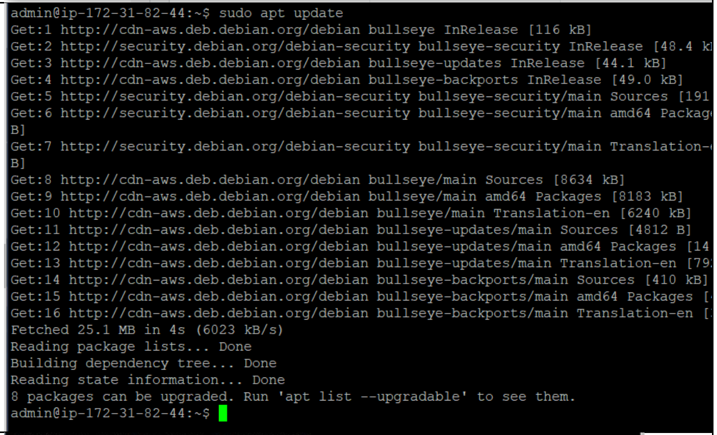
When you connect, click accept on the prompt for unknown key and proceed. The username should be admin, and the password is the key you assigned when converting the private key.



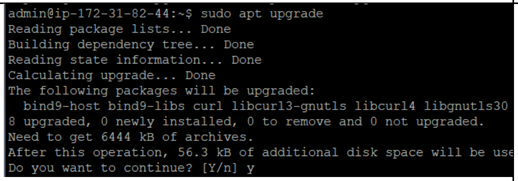
```
login as: admin
Authenticating with public key "SSH-to-AWS-Honeypot"
Passphrase for key "SSH-to-AWS-Honeypot":
```



```
login as: admin
Authenticating with public key "SSH-to-AWS-Honeypot"
Passphrase for key "SSH-to-AWS-Honeypot":
Wrong passphrase
Passphrase for key "SSH-to-AWS-Honeypot":
Linux ip-172-31-82-44 5.10.0-21-cloud-amd64 #1 SMP Debian 5.10.162-1 (20
) x86_64

The programs included with the Debian GNU/Linux system are free software
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
admin@ip-172-31-82-44:~$
```

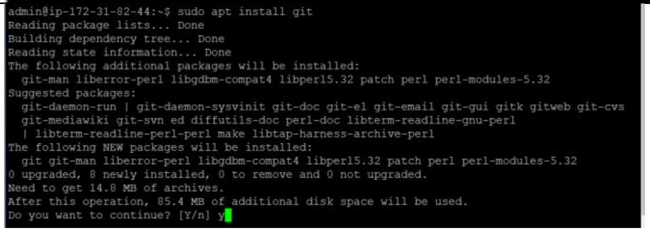


```
admin@ip-172-31-82-44:~$ sudo apt update
Get:1 http://cdn-aws.deb.debian.org/debian bullseye InRelease [116 kB]
Get:2 http://security.debian.org/debian-security bullseye-security InRelease [48.4 k
Get:3 http://cdn-aws.deb.debian.org/debian bullseye-updates InRelease [44.1 kB]
Get:4 http://cdn-aws.deb.debian.org/debian bullseye-backports InRelease [49.0 kB]
Get:5 http://security.debian.org/debian-security bullseye-security/main Sources [191
Get:6 http://security.debian.org/debian-security bullseye-security/main amd64 Packag
B]
Get:7 http://security.debian.org/debian-security bullseye-security/main Translation-
B]
Get:8 http://cdn-aws.deb.debian.org/debian bullseye/main Sources [8634 kB]
Get:9 http://cdn-aws.deb.debian.org/debian bullseye/main amd64 Packages [8183 kB]
Get:10 http://cdn-aws.deb.debian.org/debian bullseye/main Translation-en [6240 kB]
Get:11 http://cdn-aws.deb.debian.org/debian bullseye-updates/main Sources [4812 B]
Get:12 http://cdn-aws.deb.debian.org/debian bullseye-updates/main amd64 Packages [14
Get:13 http://cdn-aws.deb.debian.org/debian bullseye-updates/main Translation-en [79
Get:14 http://cdn-aws.deb.debian.org/debian bullseye-backports/main Sources [410 kB]
Get:15 http://cdn-aws.deb.debian.org/debian bullseye-backports/main amd64 Packages [
Get:16 http://cdn-aws.deb.debian.org/debian bullseye-backports/main Translation-en [
Fetched 25.1 MB in 4s (6023 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
8 packages can be upgraded. Run 'apt list --upgradable' to see them.
admin@ip-172-31-82-44:~$
```



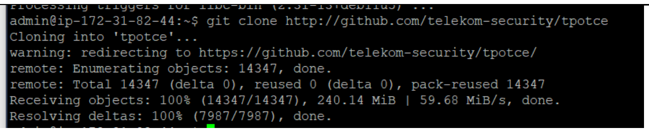
```
admin@ip-172-31-82-44:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages will be upgraded:
  bind9-host bind9-libs curl libcurl3-gnutls libcurl4 libgnutls30
8 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 6444 kB of archives.
After this operation, 56.3 kB of additional disk space will be use
Do you want to continue? [Y/n] y
```

Run *sudo apt update, sudo apt upgrade, and sudo apt install git* to install all relevant packages and updates.



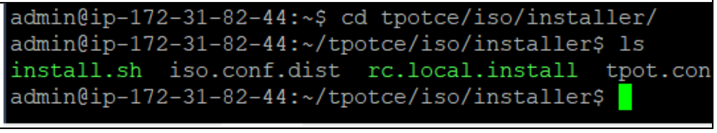
```
admin@ip-172-31-82-44:~$ sudo apt install git
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  git-man liberror-perl libgdbm-compat4 libperl5.32 patch perl perl-modules-5.32
Suggested packages:
  git-daemon-run | git-daemon-sysvinit git-doc git-el git-email git-gui gitk gitweb git-cvs
  git-mediawiki git-svn ed diffutils-doc perl-doc libterm-readline-gnu-perl
  | libterm-readline-perl-perl make libtap-harness-archive-perl
The following NEW packages will be installed:
  git git-man liberror-perl libgdbm-compat4 libperl5.32 patch perl perl-modules-5.32
0 upgraded, 8 newly installed, 0 to remove and 0 not upgraded.
Need to get 14.8 MB of archives.
After this operation, 85.4 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Clone the GitHub repository of T-Pot using git clone *http://github.com/telekom-security/tpotce*



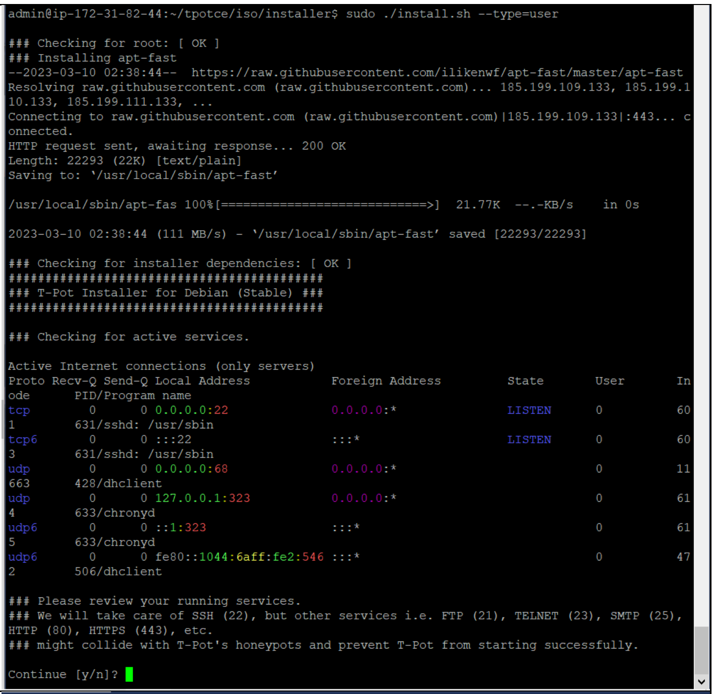
```
Processing triggers for libc-bin (2.31-13+deb11u5) ...
admin@ip-172-31-82-44:~$ git clone http://github.com/telekom-security/tpotce
Cloning into 'tpotce'...
warning: redirecting to https://github.com/telekom-security/tpotce/
remote: Enumerating objects: 14347, done.
remote: Total 14347 (delta 0), reused 0 (delta 0), pack-reused 14347
Receiving objects: 100% (14347/14347), 240.14 MiB | 59.68 MiB/s, done.
Resolving deltas: 100% (7987/7987), done.
```

Navigate to the relevant working directory using cd tpotce/iso/installer/



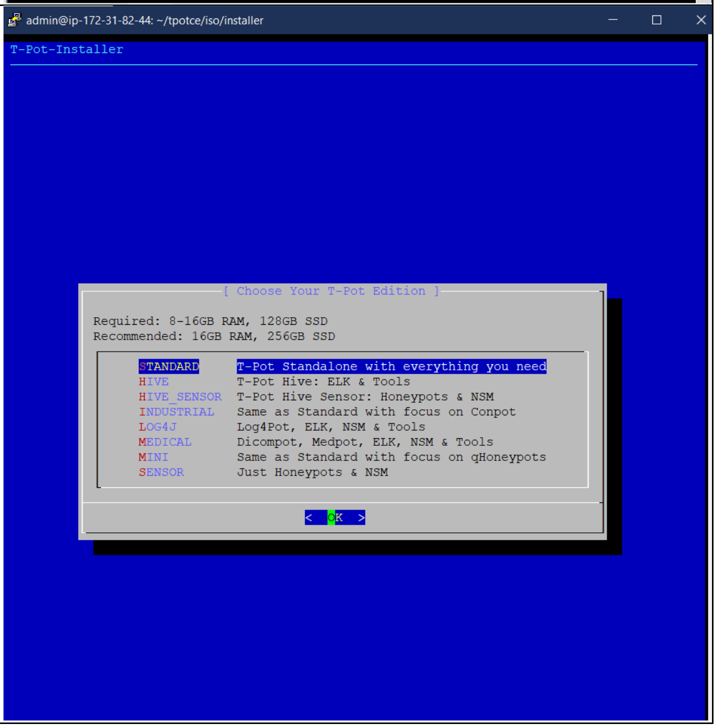
```
admin@ip-172-31-82-44:~$ cd tpotce/iso/installer/
admin@ip-172-31-82-44:~/tpotce/iso/installer$ ls
install.sh  iso.conf.dist  rc.local.install  tpot.con
admin@ip-172-31-82-44:~/tpotce/iso/installer$
```

Finally use the command sudo ./install.sh –type=user to install T-Pot on the vm.

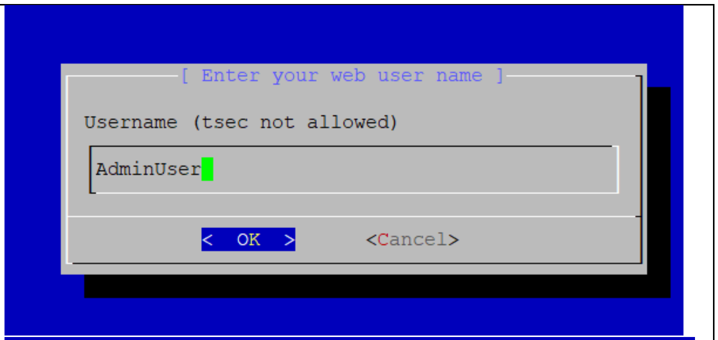
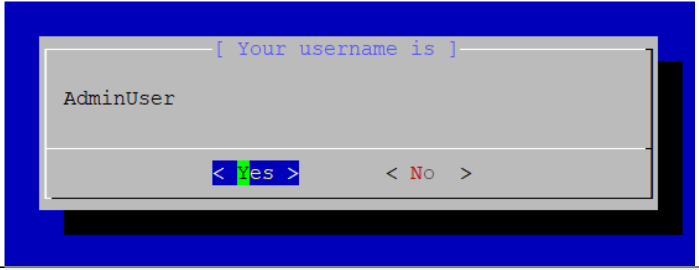
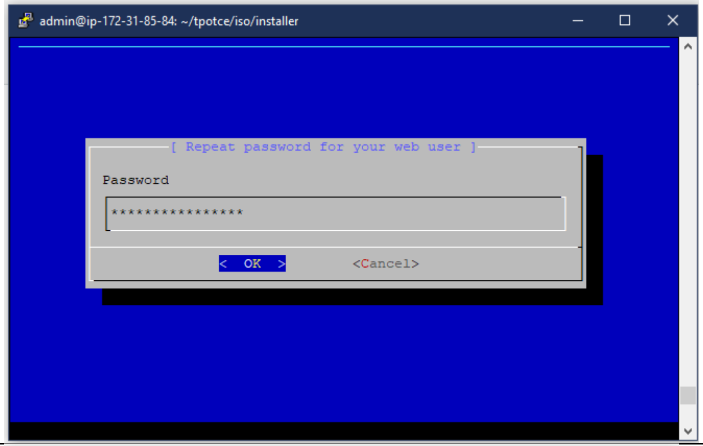
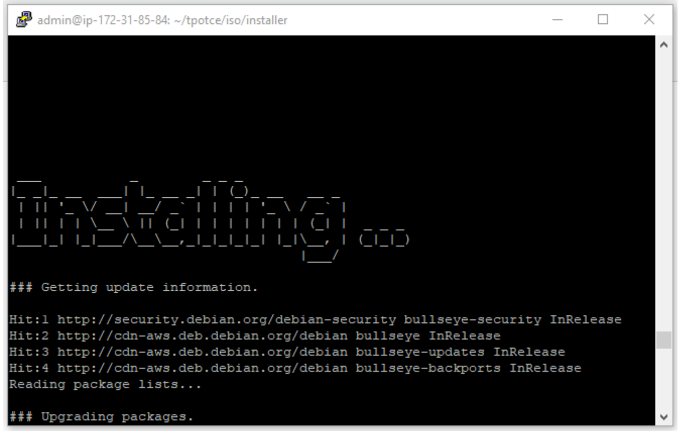


```
admin@ip-172-31-82-44:~/tpotce/iso/installer$ sudo ./install.sh --type=user

### Checking for root: [ OK ]
### Installing apt-fast
--2023-03-10 02:38:44--  https://raw.githubusercontent.com/ilikenwf/apt-fast/master/apt-fast
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.109.133, 185.199.1
10.133, 185.199.111.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.109.133|:443... c
onnected.
HTTP request sent, awaiting response... 200 OK
Length: 22293 (22K) [text/plain]
Saving to: '/usr/local/sbin/apt-fast'

/usr/local/sbin/apt-fas 100%[============================>]  21.77K  --.-KB/s    in 0s

2023-03-10 02:38:44 (111 MB/s) - '/usr/local/sbin/apt-fast' saved [22293/22293]

### Checking for installer dependencies: [ OK ]
###########################################
### T-Pot Installer for Debian (Stable) ###
###########################################

### Checking for active services.

Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       User       In
ode       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      0          60
1         631/sshd: /usr/sbin
tcp6       0      0 :::22                   :::*                    LISTEN      0          60
3         631/sshd: /usr/sbin
udp        0      0 0.0.0.0:68              0.0.0.0:*                           0          11
663       428/dhclient
udp        0      0 127.0.0.1:323           0.0.0.0:*                           0          61
4         633/chronyd
udp6       0      0 ::1:323                 :::*                                0          61
5         633/chronyd
udp6       0      0 fe80::1044:6aff:fe2:546 :::*                                0          47
2         506/dhclient

### Please review your running services.
### We will take care of SSH (22), but other services i.e. FTP (21), TELNET (23), SMTP (25),
HTTP (80), HTTPS (443), etc.
### might collide with T-Pot's honeypots and prevent T-Pot from starting successfully.

Continue [y/n]?
```

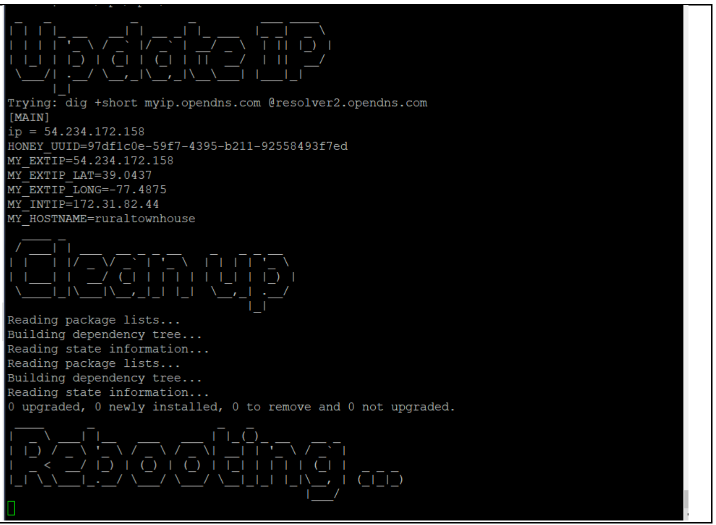
This will take a while, but after a bit you should see a blue window prompting you to choose an edition. Choose STANDARD and hit Enter.



```
T-Pot-Installer

[ Choose Your T-Pot Edition ]

Required: 8-16GB RAM, 128GB SSD
Recommended: 16GB RAM, 256GB SSD

      STANDARD      T-Pot Standalone with everything you need
      HIVE          T-Pot Hive: ELK & Tools
      HIVE_SENSOR   T-Pot Hive Sensor: Honeypots & NSM
      INDUSTRIAL    Same as Standard with focus on Conpot
      LOG4J         Log4Pot, ELK, NSM & Tools
      MEDICAL       Dicompot, Medpot, ELK, NSM & Tools
      MINI          Same as Standard with focus on qHoneypots
      SENSOR        Just Honeypots & NSM

                          < OK >
```

Select a username and select Enter. Write this and the password down because it’ll be what you’re using to log into the T-Pot dashboard later. Confirm the username then proceed.	 [Enter your web user name] Username (tsec not allowed) AdminUser < OK > <Cancel>  [Your username is] AdminUser < Yes > < No >
Configure the password and hit Enter.	 admin@ip-172-31-85-84: ~/tpotce/iso/installer [Repeat password for your web user] Password **************** < OK > <Cancel>
Click Y to proceed and the installation will begin.	 admin@ip-172-31-85-84: ~/tpotce/iso/installer Installing ... ### Getting update information. Hit:1 http://security.debian.org/debian-security bullseye-security InRelease Hit:2 http://cdn-aws.deb.debian.org/debian bullseye InRelease Hit:3 http://cdn-aws.deb.debian.org/debian bullseye-updates InRelease Hit:4 http://cdn-aws.deb.debian.org/debian bullseye-backports InRelease Reading package lists... ### Upgrading packages.

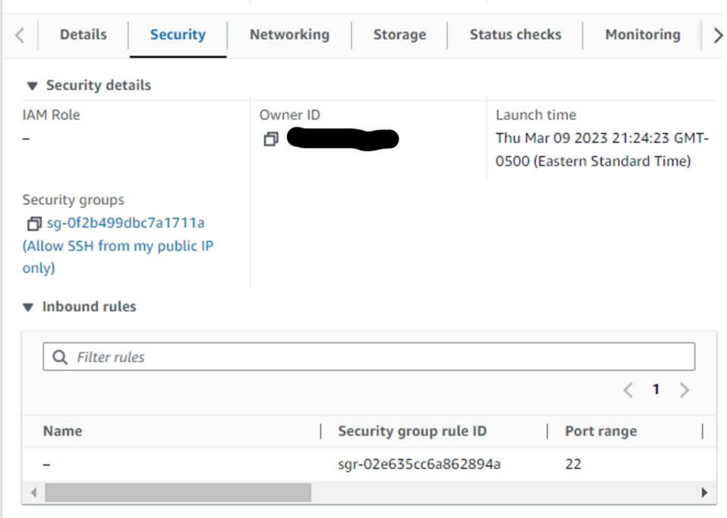
After installation, the AWS machine will reboot and you’ll not be able to access the command line anymore except through the web interface.



```
 _   _           _       _         ___ ____
| | | |_ __   __| | __ _| |_ ___  |_ _|  _ \
| | | | '_ \ / _` |/ _` | __/ _ \  | || |_) |
| |_| | |_) | (_| | (_| | ||  __/  | ||  __/
 \___/| .__/ \__,_|\__,_|\__\___| |___|_|
      |_|
Trying: dig +short myip.opendns.com @resolver2.opendns.com
[MAIN]
ip = 54.234.172.158
HONEY_UUID=97df1c0e-59f7-4395-b211-92558493f7ed
MY_EXTIP=54.234.172.158
MY_EXTIP_LAT=39.0437
MY_EXTIP_LONG=-77.4875
MY_INTIP=172.31.82.44
MY_HOSTNAME=ruraltownhouse
  ____ _
 / ___| | ___  __ _ _ __    _   _ _ __
| |   | |/ _ \/ _` | '_ \  | | | | '_ \
| |___| |  __/ (_| | | | | | |_| | |_) |
 \____|_|\___|\__,_|_| |_|  \__,_| .__/
                                 |_|
Reading package lists...
Building dependency tree...
Reading state information...
Reading package lists...
Building dependency tree...
Reading state information...
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
 ____      _                 _   _
|  _ \ ___| |__   ___   ___ | |_(_)_ __   __ _
| |_) / _ \ '_ \ / _ \ / _ \| __| | '_ \ / _` |
|  _ <  __/ |_) | (_) | (_) | |_| | | | | (_| |_ _ _
|_| \_\___|_.__/ \___/ \___/ \__|_|_| |_|\__, (_|_|_)
                                         |___/
```

Security Group Configuration

Close the PuTTY window, but navigate back to your AWS Instance page and to the Security Section. Then click the Security groups link.



▼ Security details

IAM Role: –

Owner ID: [redacted]

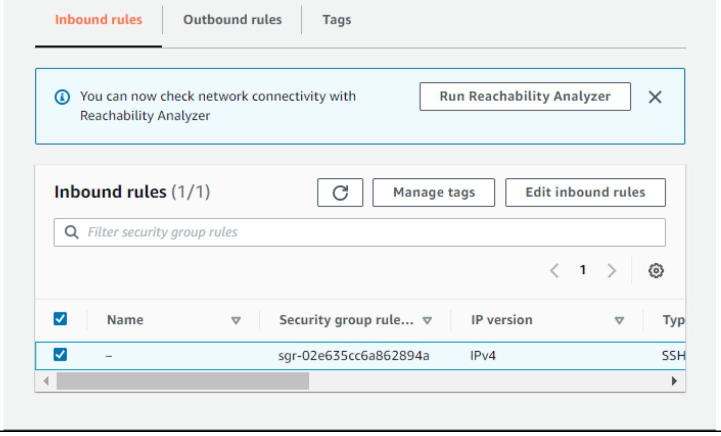
Launch time: Thu Mar 09 2023 21:24:23 GMT-0500 (Eastern Standard Time)

Security groups: sg-0f2b499dbc7a1711a (Allow SSH from my public IP only)

▼ Inbound rules

Name	Security group rule ID	Port range
–	sgr-02e635cc6a862894a	22

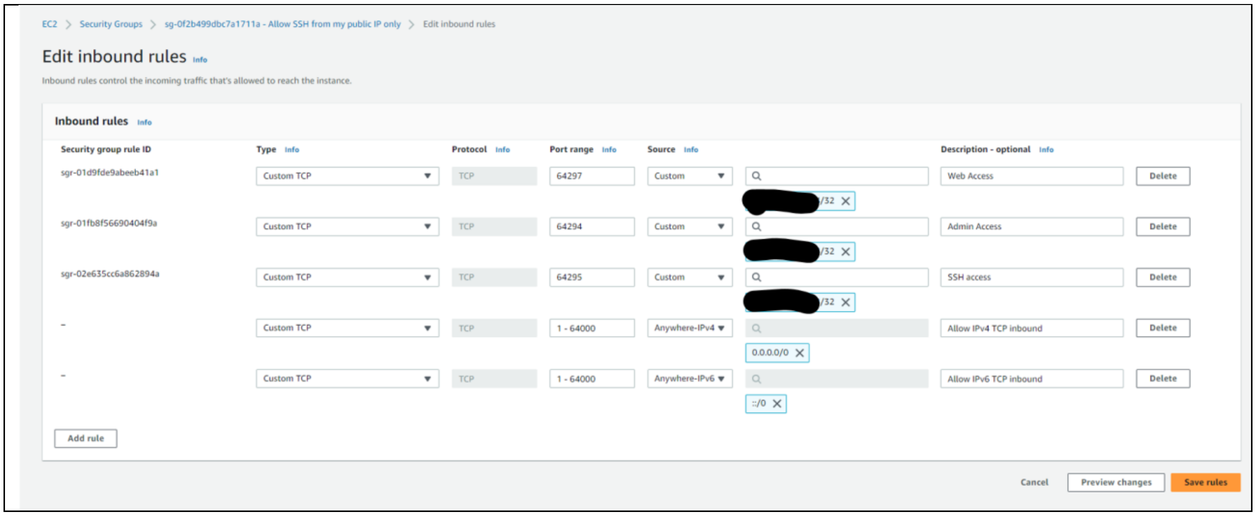
On the Security Group page, click Edit inbound rules.



You can now check network connectivity with Reachability Analyzer

Inbound rules (1/1)

☑	Name	Security group rule...	IP version	Typ
☑	–	sgr-02e635cc6a862894a	IPv4	SSH



EC2 > Security Groups > sg-0f2b499dbc7a1711a - Allow SSH from my public IP only > Edit inbound rules

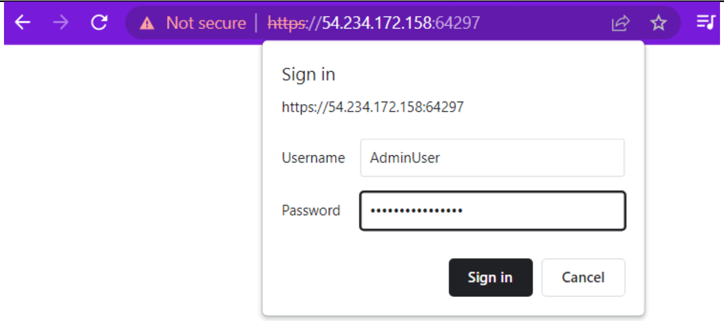
Edit inbound rules Info

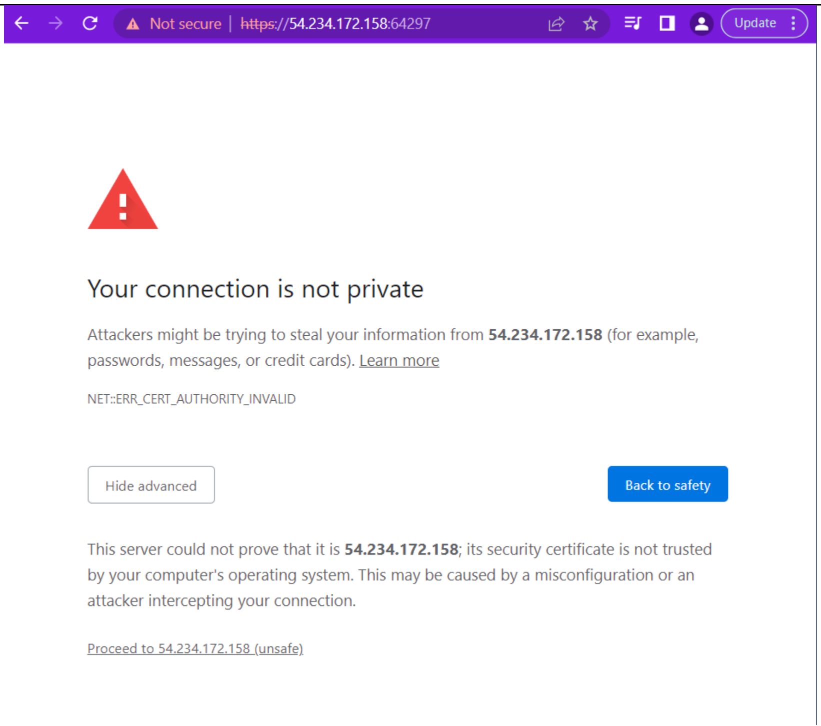
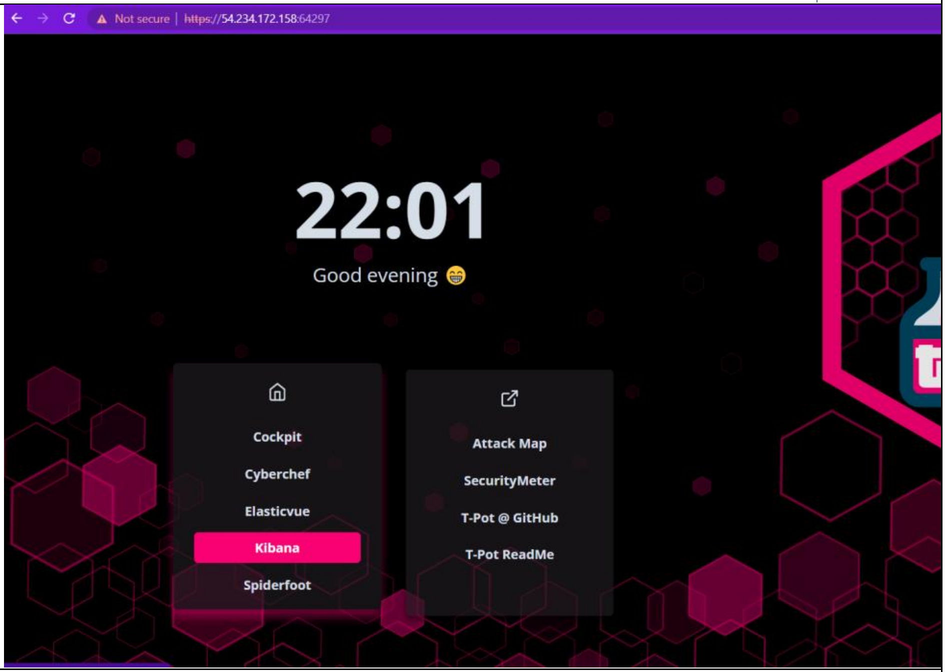
Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
sgr-01d9fde9abeeb41a1	Custom TCP	TCP	64297	Custom	[redacted]/32	Web Access	Delete
sgr-01fb8f56690404f9a	Custom TCP	TCP	64294	Custom	[redacted]/32	Admin Access	Delete
sgr-02e635cc6a862894a	Custom TCP	TCP	64295	Custom	[redacted]/32	SSH access	Delete
-	Custom TCP	TCP	1 - 64000	Anywhere-IPv4	0.0.0.0/0	Allow IPv4 TCP inbound	Delete
-	Custom TCP	TCP	1 - 64000	Anywhere-IPv6	::/0	Allow IPv6 TCP inbound	Delete

Kibana Dashboard Logon

<table>
<tr><td colspan="2">Adjust the security rules to the following requirements:
Ensure you restrict TCP port 64294 to allow Admin access only from your source IP address.
Ensure you restrict TCP port 64295 to allow SSH access only from your source IP address.
Ensure you restrict TCP port 64297 to allow the web interface access only from your source IP address.
Configure TCP ports 1 – 64000 on IPv4 and IPv6 to allow everything else from the internet.</td></tr>
<tr><td>Next, open your web browser and go https://###.###.###.###:64297 and log-in with the user account, you will be redirected to the following dashboard, simply click on Kibana:</td><td>
Not secure | ~~https~~://54.234.172.158:64297
Sign in
https://54.234.172.158:64297
Username AdminUser
Password ••••••••••••••••
Sign in Cancel</td></tr>
</table>

Proceed	 Your connection is not private Attackers might be trying to steal your information from **54.234.172.158** (for example, passwords, messages, or credit cards). Learn more NET::ERR_CERT_AUTHORITY_INVALID Hide advanced Back to safety This server could not prove that it is **54.234.172.158**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection. Proceed to 54.234.172.158 (unsafe)
Click on Kibana to access the Dashboards. You could also explore the other options like:	 Not secure | ~~https~~://54.234.172.158:64297 22:01 Good evening 😁 Cockpit Cyberchef Elasticvue Kibana Spiderfoot Attack Map SecurityMeter T-Pot @ GitHub T-Pot ReadMe

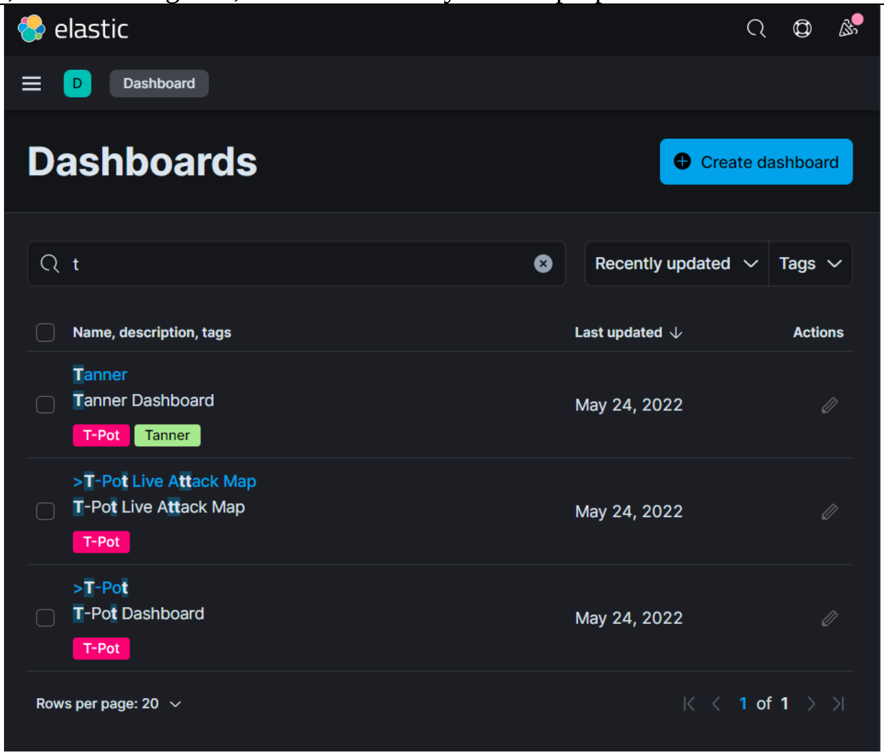
Cockpit: Cockpit is a web-based GUI that allows system administrators to manage various aspects of their Linux servers. It provides a dashboard for monitoring system performance, managing services and applications, and configuring settings. Cockpit is often used to manage server clusters, allowing administrators to monitor multiple servers from a single dashboard.

CyberChef: CyberChef is a powerful, web-based tool for decoding, encoding, analyzing, and manipulating data. It supports a wide range of data formats and provides a user-friendly interface for performing complex operations on data. CyberChef is often used by security professionals and researchers to analyze malware and extract information from various types of data.

ElasticVue: ElasticVue is a web-based GUI tool that allows users to interact with Elasticsearch data. Elasticsearch is a popular search engine and analytics platform used for indexing and searching large volumes of data. ElasticVue provides a user-friendly interface for querying and visualizing Elasticsearch data, making it easier for non-technical users to interact with the platform.

SpiderFoot: SpiderFoot is an open-source reconnaissance tool that automates the process of gathering information about a target. It can be used to perform footprinting, reconnaissance, and OSINT (Open-Source Intelligence) gathering on various targets, including websites, networks, and social media accounts. SpiderFoot is often used by security professionals and researchers to gather intelligence for vulnerability assessments, threat intelligence, and other security-related purposes.

Navigate to the T-Pot dashboard. You can also check out some of the other dashboards for individual honeypots like *Cowrie*, *Dionaea* or *Heralding*.



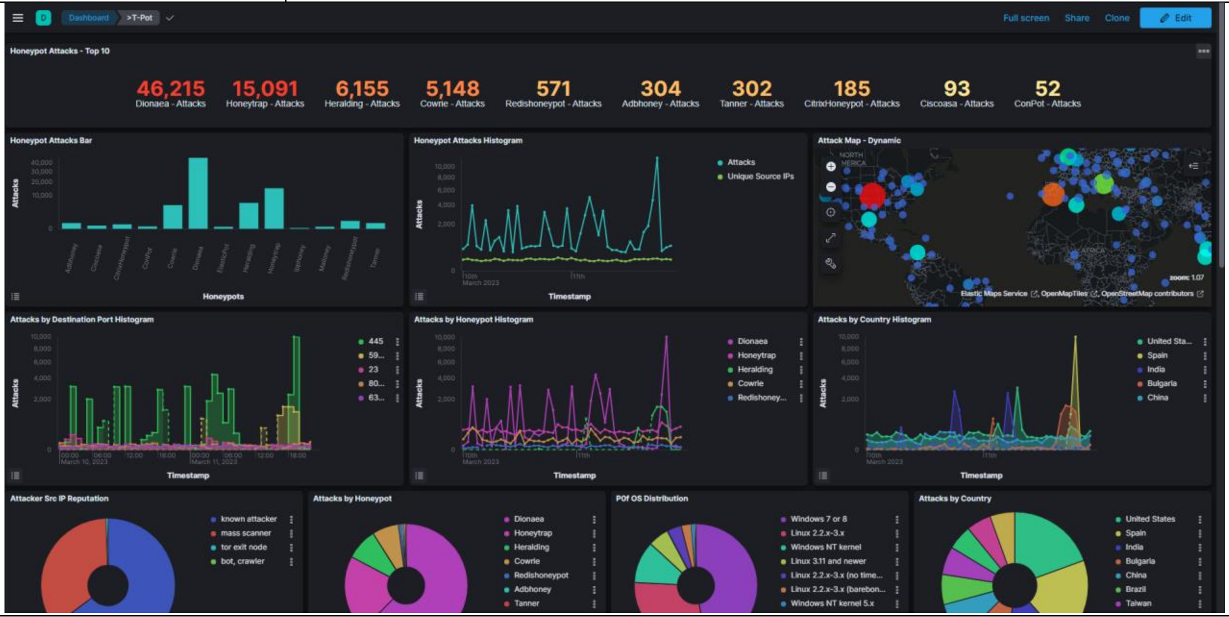
Dashboards

t

□	Name, description, tags	Last updated ↓	Actions
□	Tanner Tanner Dashboard T-Pot Tanner	May 24, 2022	✎
□	>T-Pot Live Attack Map T-Pot Live Attack Map T-Pot	May 24, 2022	✎
□	>T-Pot T-Pot Dashboard T-Pot	May 24, 2022	✎

Rows per page: 20

1 of 1

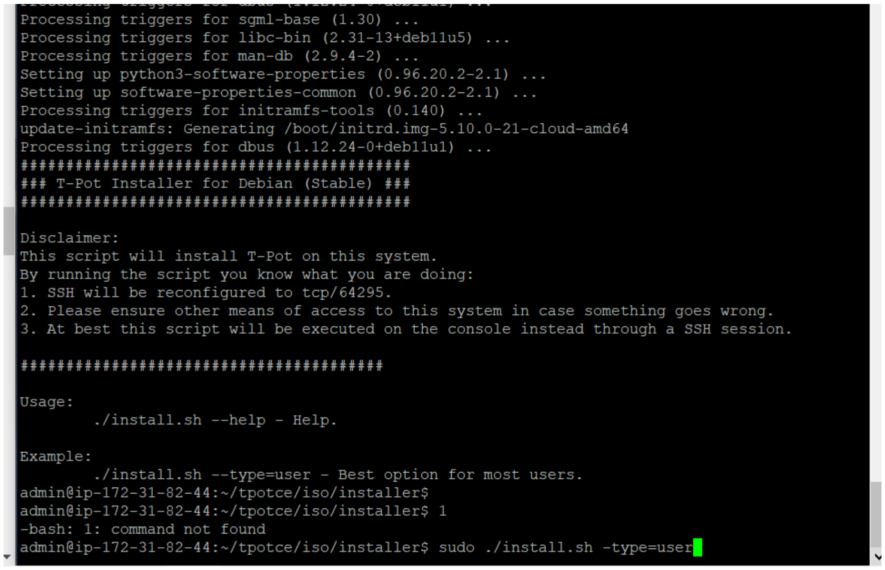


The following shows all attacks and threats occurring on our honeypot. If you leave the honeypot running for an extended period on the internet, it will accumulate more data and possibly be more useful/insightful. However, it's important to keep in mind that the virtual machine on AWS incurs charges based on usage. Therefore, it's advisable to stop or terminate any unused services on AWS to avoid unnecessary charges to your credit card. 1 week vs 1 day. It’s approximately 4$ a day to run this process.

Problems and Troubleshooting:

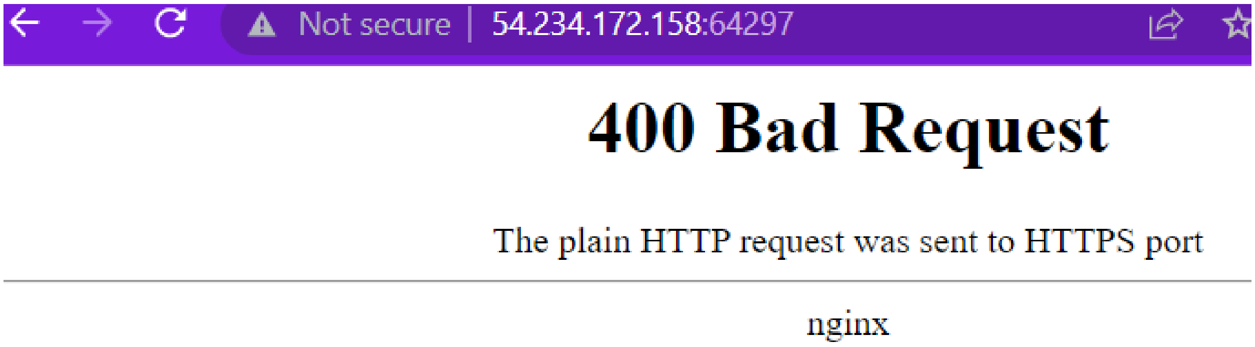
For the most part the installation ran smoothly, however I did encounter a few issues, but they were minor typecast errors. For example, you must use two dashes when installing sh –type=user instead of -type=user(figure 1). Also when connecting to the dashboard, you must use https, not http, or you will get a 400 bad request message(figure 2). Also if you want to make the T-Pot more accurate, you may want to remove your home IP address from the data through using NOT scr_ip.keyword: IP ADDRESS. For example I ran a few nmap scans on my AWS machine and that greatly skewed the data by thousands of attacks, so removing your IP address from the dataset generally a good idea.

Figure 1:



```
Processing triggers for dbus (1.12.24-0+deb11u1) ...
Processing triggers for sgml-base (1.30) ...
Processing triggers for libc-bin (2.31-13+deb11u5) ...
Processing triggers for man-db (2.9.4-2) ...
Setting up python3-software-properties (0.96.20.2-2.1) ...
Setting up software-properties-common (0.96.20.2-2.1) ...
Processing triggers for initramfs-tools (0.140) ...
update-initramfs: Generating /boot/initrd.img-5.10.0-21-cloud-amd64
Processing triggers for dbus (1.12.24-0+deb11u1) ...
###########################################
### T-Pot Installer for Debian (Stable) ###
###########################################

Disclaimer:
This script will install T-Pot on this system.
By running the script you know what you are doing:
1. SSH will be reconfigured to tcp/64295.
2. Please ensure other means of access to this system in case something goes wrong.
3. At best this script will be executed on the console instead through a SSH session.

########################################

Usage:
        ./install.sh --help - Help.

Example:
        ./install.sh --type=user - Best option for most users.
admin@ip-172-31-82-44:~/tpotce/iso/installer$
admin@ip-172-31-82-44:~/tpotce/iso/installer$ 1
-bash: 1: command not found
admin@ip-172-31-82-44:~/tpotce/iso/installer$ sudo ./install.sh -type=user
```

Figure 2:



400 Bad Request

The plain HTTP request was sent to HTTPS port

nginx

Conclusion

Overall, in this lab we set up an AWS instance, installed T-Pot onto it, and sucessfully started running the honeypot. Now all we have to do is wait and see what happens. T-Pot is a valuable open-source honeypot software that can be easily deployed and customized to suit the specific needs of individual users. As a fully functional honeypot environment, it offers a range of pre-installed services and tools that can help security professionals gain valuable insights into attacker behavior and tactics. Over the next week I will be documenting everything that happens every 24 hours, including number of attacks, their origins, commands ran, and a lot more.