Bottlenose Labs

Bottlenose Lab: Linux Security Overview

1a. Firstly, create a new Linux user account named "demo" for your EC2 instance "Server". Please save the command that you ran for this task to "/tmp/answer1a.txt" file.

sudo useradd demo

1b. Now, assign a password to the "demo" user. And, save the command that you ran for this task to "/tmp/answer1b.txt" file.

sudo passwd demo

1c. Finally, check if the user has been added to user list. And, save the command that you ran for this task to "/tmp/answer1c.txt" file.

sudo cat /etc/passwd | grep demo

Find out if the user created in above step has a password assigned or not. And, save the command that you ran for this task to "/tmp/answer2.txt" file.

sudo cat /etc/shadow | grep demo

Create a new group called "devgroup" and then assign the user "demo" to this group.

sudo groupadd devgroup
gpasswd -M demo devgroup

Create a shared group directory called "devdirectory" in /usr directory.

sudo mkdir /usr/devdirectory

5a. Find out the ownership of the "devdirectory" created in the previous step. Please save the command that you ran for this task to "/tmp/answer5a.txt" file.

ls -l /usr | grep devdirectory

5b. Now, change the ownership of this directory to "devgroup". Please save the command that you ran for this task to "/tmp/answer5b.txt" file.

sudo chown :devgroup /usr/devdirectory

Add write permissions for the group to the "devdirectory" and also verify the directory permissions. After that, please the command that you ran for assigning write permissions to the group ("devgroup") to the "devdirectory" to "/tmp/answer6.txt" file.

sudo chmod g+w /usr/devdirectory/ && ls -l /usr/ | grep devdirectory

Find out and remove the **other** users read and execute privileges from the directory "devdirectory". And, please save the command used for removing the "rx" permissions of other users on the devdirectory to "/tmp/answer7.txt" file.

sudo chmod u-rx /usr/devdirectory/
sudo chmod o-rx /usr/devdirectory/

Bottlenose Lab: Managing Linux Services, Processes and Jobs

1. What command can list CPU usage, Memory usage, as well as all the processes.
    a. `top`
    b. echo "top" > ans1.txt
2. What other command can also list all processes?
    a. `ps aux`
    b. echo “ps aux” > ans1.txt
3. Command to launch the vim process in the background with a nice value of 19
    a. `nice -n 19 vim &`
4. Command to filter the ps command to just output the vim process?
    a. `ps aux | grep vim`
5. A command that will get **just** the PID of the vim process you just launched using the processes name (vim)
    a. `pgrep vim`
    b. pidof vim
6. What command and signal would you use to stop the vim process **immediately** with no graceful exit
    a. `pkill -9 vim`
7. What command would you use to create a cron job?
    a. `crontab -e`
8. What command would you run to send one refresh of the output of top to a file called top.txt?
    a. `top -b -n 1 > top.txt`
9. What command would you run to check if the 'cloud-init.service' service is configured to start at boot?
    a. `systemctl is-enabled cloud-init.service`

Bottlenose Lab: Linux Filesystems and Filesystem Hierarchy Standard

1. Check the current EBS volume’s size attached to your EC2 instance using an appropriate command. And, please just save the volume’s size (in GB) returned as the output of the command used by you to “/tmp/answer1.txt” file.
    a. `sudo lsblk`
2. Check the current file system's usage. And, save the command that you ran for this task to "/tmp/answer2.txt" file. Please ensure that you save the exact command without any quotes or extra unnecessary spaces.
    a. `sudo df -h`
3. As part of the lab, we have already created an EBS Volume named "NewVolume" of 8Gib size. Please attach this new volume to your EC2 instance "Server" to "/dev/sdf" device.
    a. attach EBS

4. Create an "ext4" filesystem on the newly created/attached EBS volume.
    a. `sudo mkfs -t ext4 /dev/sdf`
5. Run a filesystem check on the new 'ext4' file system. And, save the command that you ran for this task to "/tmp/answer3.txt" file. Please ensure that you save the exact command without any quotes or extra unnecessary spaces.
    a. `sudo fsck /dev/sdf`
6. Assign the label "SECONDARY" to the new 'ext4' filesystem.
    a. `sudo e2label /dev/xvdf SECONDARY`
7. Mount the 'ext4' filesystem using its label "SECONDARY" to the "/mnt" mountpoint. Please save the command that you ran for mounting to "/tmp/answer4.txt" file. Please ensure that you save the exact command without any quotes or extra unnecessary spaces.
    a. `sudo mount LABEL=SECONDARY /mnt`
8. Permanently mount the 'ext4' filesystem using its Label "SECONDARY" to the "/mnt" mountpoint. Do save the line you would you would add to /etc/fstab to mount the filesytem permanently using it's label, into the"/tmp/answer5.txt" text file. Please ensure that you save the exact fstab line used without any quotes or extra unnecessary spaces.
    a. `LABEL=SECONDARY /mnt ext4 defaults 0 2`

Bottlenose Lab: Linux Network Troubleshooting

1. Which command will you use to find out if the instance has internet connectivity ? Please execute the command on your EC2 instance "Server". If you get the desired output using that command then please just save the command without any arguments to "/tmp/answer1.txt" file.
    a. `ping`
2.
    a. 2a. Which command is used to check the network interfaces attached to an instance? Please save the command that you ran for this task to "/tmp/answer2a.txt" file.
        i. `ip link show`
    b. 2b. Now, what is the name of the network interface? Please just save the name of the network interface to "/tmp/answer2b.txt" file.
        i. `ip -br link show | awk '{print $1}'`
3. Find out if the httpd service is listening on port 80. And, save the command that you ran for this task to "/tmp/answer3.txt" file.
    a. sudo netstat -tunlp l grep :80
    b. `sudo netstat -tulnp | grep httpd`
4. Which command is used to display the routes on OS Level ? Please execute the command on your EC2 instance. If you get the desired output using that command then please save the command to "/tmp/answer4.txt" file.
    a. `route`
5. Find out A records for "amazon.com" ? And, then please save the command that you ran for this task to "/tmp/answer5.txt" file.
    a. `dig amazon.com A`

6.
    a. 6a. Install iptables-services on your instance and save the command used for installing to "/tmp/answer6a.txt" file.
        i. `sudo yum install iptables-services`
    b. 6b. Then, enable iptables-service and save the command used for enabling to "/tmp/answer6b.txt" file.
        i. `sudo systemctl enable iptables`
    c. 6c. Next, start the iptables-service on the instance and save the command used for starting to "/tmp/answer6c.txt" file.
        i. `sudo systemctl start iptables`
    d. 6d. Finally, check if iptables-service is running on the instance and save the save the command used for checking the status to "/tmp/answer6d.txt" file.
        i. `sudo systemctl status iptables`
7.
    a. 7a. Once that is done, please check what is the name of the secondary network interface by executing an appropriate command on your EC2 instance? And, please just save the name of the secondary network interface to "/tmp/answer7a.txt" file.
        i. `ip link show | grep eth1`
    b. 7b. Now, which command will you have to run to bring the secondary interface down. Please save the command to /tmp/answer7b.txt" file.
        i. `sudo ip link set eth1 down`

Bottlenose Lab: System Libraries and Package Management Basics

1. Which command will you use to show all the shared libraries along with their versions? Please execute the command on your EC2 instance "Server". If you get the desired output using that command then please save the command to "/tmp/answer1.txt" file.
    a. `sudo ldconfig -v`
2. Please install the "httpd" package on the EC2 instance using "yum" and save the command that you ran for this task to "/tmp/answer2.txt" file.
    a. `sudo yum install -y httpd`
3. List the dependencies that are required by the "httpd" package. And, save the command that you ran for this task to "/tmp/answer3.txt" file.
    a. `yum deplist httpd`
    b. `rpm -qR htppd`
4. Which command can be used to see information on previously installed packages such as seeing the start time when the "httpd" package was installed? ? Please execute the command on your EC2 instance. If you get the desired output using that command then please save the command to "/tmp/answer4.txt" file.
    a. `sudo yum history info httpd`
5. Show the command that can be used for enabling the epel repository on the instance. Please use the command to install the said repo and save the command to "/tmp/answer5.txt" file.
    a. `sudo yum install epel-release`
6. Remove the httpd package from your instance and save the command that you ran for this task to "/tmp/answer6.txt" file.

a. `sudo yum remove -y httpd`

EC2 INSTANCE FAILING INSTANCE STATUS CHECKS

Bottlenose Lab: IAM AssumeRole Issue

,

"arn:aws:iam::646005135696:root"

User: arn:aws:iam::460360857379:user/myuser is not authorized to perform: access-analyzer:ListPolicyGenerations on resource: arn:aws:access-analyzer:us-east-1:460360857379:*

Bottlenose Lab: Commands to gather OS level Info and perform some Tasks

Description

You are provided with a new EC2 instance public IP and private ssh key. Connect to the EC2 instance using the provide key and IP.

Once you are logged in, you are required to complete some tasks using the commands you have learned so far. To receive credit for completing each task, you must save the command you used in a text file named "ans<task_number>.txt" in the default directory, which is "/home/ec2-user/" after you SSH. For example, if you are completing task 1, save the command you used in a file called "ans1.txt".

1. Find kernel release information. Please save the command used to perform this operation in a file named ‘ans1.txt’.
    a. uname -r
2. Find the operating system version. Please save the command used to perform this operation in a file named ‘ans2.txt’.
    a. cat /etc/os-release
3. List the currently installed kernel versions. Please save the command used to perform this operation in a file named ‘ans3.txt’.
    a. rpm -qa l grep kernel
4. Find name of the network interface. Please save the command used to perform this operation in a file named ‘ans4.txt’.
    a. ip link show
5. Find name of shell. Please save the command used to perform this operation in a file named ‘ans5.txt’.
    a. echo $SHELL
    b. echo \$SHELL

6. Change bash prompt to "linux-guru: " Please save the command used to perform this operation in a file named ‘ans6.txt’.
    a. PS1="linux-guru: "
7. Install apache (httpd) and enable apache to start across reboots. Note: No need of saving the commands here i.e. just install apache https server in such a way that it is running and can also survive restarts.
    a. Update the package list:
        i. sudo yum update -y
    b. Install Apache:
        i. sudo yum install httpd -y
    c. Start Apache:
        i. sudo systemctl start httpd
    d. Enable Apache to start on boot:
        i. sudo systemctl enable httpd

Bottlenose Lab: Network connectivity issue from EC2 to RDS

Bottlenose Lab: Ensure high availability of EC2 WIN instances using ALB

1. NACL - inbound adding HTTP
2. SG - ALB - inbound adding HTTP anywhere
3. SG - ALB - outbound change CIDR
4. SG - instance - inbound adding SG - ALB

Customer is getting 403 for the objects which are not present in S3 instead of HTTP 404 Not Found Error.

1. Allow public access
2. change policy

```
{
"Version": "2012-10-17",
"Id": "MyPolicy",
```

```
"Statement": [
{
"Sid": "PublicReadForGetBucketObjects",
"Effect": "Allow",
"Principal": "*",
"Action": "s3:GetObject",
"Resource": "arn:aws:s3:::bottlenose-a-3e592a2-s3bucket-jypvlujvzsdi/*"
}
]
}
```

S3 403 GetObject error

1. KMS - Allow
2. S3 - public access
3. policy bucket - allow

Basic Linux commands

1. Find the default file permissions for new files created by root in the /home/ec2-user directory, and save them in octal format (like “777”) in "/tmp/q1.txt" file.
    a.
2. Find the default directory permissions for new directories created by root in the /home/ec2-user directory, and save them in “/tmp/q2.txt” file in octal format (like “777”)
    a. umask l awk '{printf "%04o\n", 0777-$1}' > /tmp/q2.txt
3. Create an empty file "/tmp/q3.txt". Set the default permission of this file to 622 and the "/tmp/" directory to 733.
    a.
4. Find the available free space in xvda1 in MB and save the value in "/tmp/q4.txt" file
    a. df -h /dev/xvda1
    b. df -BM /dev/xvda1 l awk '/xvda1/ {print $4}'
5. Find the disk usage (in KB) of "/home/ec2-user/compressed.tar" file and save that number value in "/tmp/q5.txt".
    a. du -h /home/ec2-user/compressed.tar
6. Extract the "/home/ec2-user/compressed.tar" and list the file names in space separated format in "/tmp/q6.txt". For example "p1.txt p2.txt p3.txt".
    a. tar -xvf /home/ec2-user/compressed.tar

Bottlenose Lab: EC2 instance failing Instance Status Checks

sudo mount -t xfs -o nouuid /dev/sdf1 /mnt/test
sudo vim /mnt/test/etc/fstab
sudo umount /mnt/test

Fix the connection to the Website

1. change NACL allow all traffic to all - INO
2. check SG
3. SSH into isntance
    a. systemctl status httpd
    b. systemctl start httpd
    c. systemctl status firewalld

```
sudo yum install firewalld
sudo systemctl start firewalld
sudo systemctl enable firewalld
```

    a. firewall-cmd --list-all
        i. firewall-cmd --add-port=80/tcp --permanent
    b. firewall-cmd --reload