

kali linux on AWS serial console issue

date: March 23, 2024

author: Lynx(_lynx___@discord)

Summary

The kali Linux AMI ami-08ff8eb7758eb14ec, available on the AWS Marketplace, has a vulnerability that enables operation with root privileges without the need for authentication. With only limited IAM permissions, an attacker can access the kali root prompt. This vulnerability might enable users with minimal privileges on the operating system, like monitoring operators, to acquire root privileges via the serial console.

Steps for reproduce

1. CHOOSE THE FOLLOWING AMI FROM THE AWS MARKETPLACE AND LAUNCH AN INSTANCE AS VICTIM.

- Install all options with the default settings tailored to your environment.

AMI name: kali-last-snapshot-amd64-2023.4.0-804fcc46-63fc-4eb6-85a1-50e66d6c7215

AMI ID: ami-08ff8eb7758eb14ec

Kali Linux

By Kali

Version Kali Linux 2023.4

[17 AWS reviews](#) | [140 external reviews](#) Kali Linux (formerly known as BackTrack Linux) is an open-source, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. It does this by providing common tools, configurations, and automations which allows the user to focus on the task that needs to be...

2. GRANT PERMISSIONS TO IAM USERS.

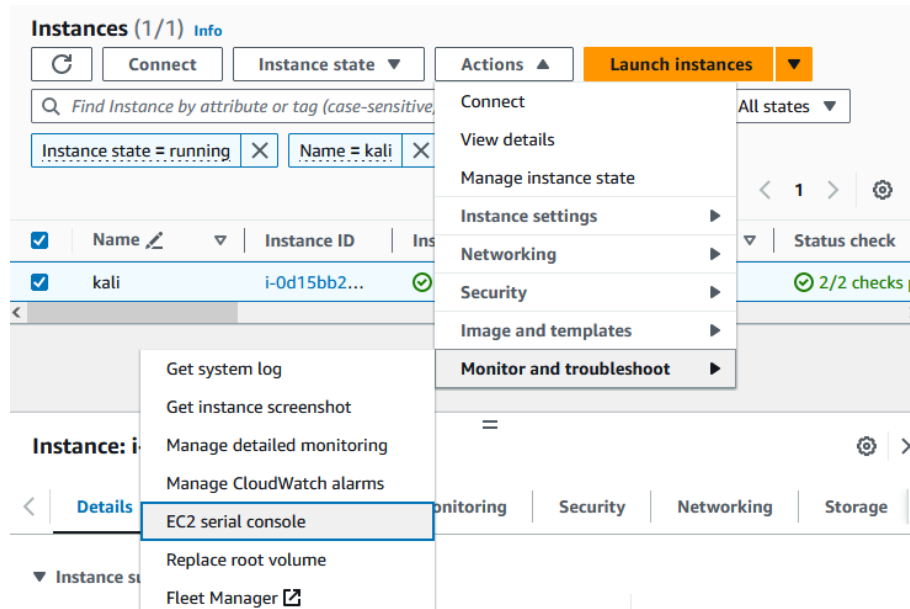
The IAM user who is performing the operation needs to have the permission to connect to the EC2 serial console. Please grant the following permissions.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowEC2SerialConsole",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:GetSerialConsoleAccessStatus",
        "ec2:EnableSerialConsoleAccess",
        "ec2:DisableSerialConsoleAccess",
        "ec2-instance-connect:SendSerialConsoleSSHPublicKey",
        "ec2-instance-connect:SendSSHPublicKey"
      ],
      "Resource": "*"
    }
  ]
}
```

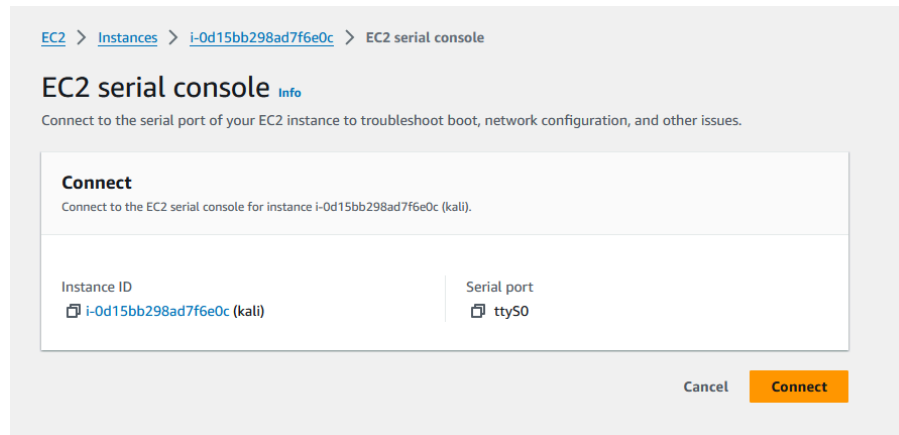
}

3. OPERATIONS IN THE AWS MANAGEMENT CONSOLE

- Choose the target instance.
- Navigate to [Actions] > [Monitor and troubleshoot] > [EC2 serial console]



- Click on "Connect" in the displayed screen to establish a connection to ttyS0.



- After the screen has loaded, press the Enter key. The root@kali: ~# prompt will be displayed.

```
kali login: root (automatic login)

Linux kali 6.5.0-kali3-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) x86_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Mar 23 01:38:04 UTC 2024 on ttyS0
■(Message from Kali developers)
■
■ This is a minimal installation of Kali Linux, you likely
■ want to install supplementary tools. Learn how:
■ https://www.kali.org/docs/troubleshooting/common-minimum-setup/
■
■ This is a cloud installation of Kali Linux. Learn more about
■ the specificities of the various cloud images:
■ https://www.kali.org/docs/troubleshooting/common-cloud-setup/
■
■(
■(root@kali)~#
```

Root cause analysis

The following entry is located in `/etc/systemd/system/serial-getty@.service.d/autologin.conf`.

```
[Service]
ExecStart=
ExecStart=-/sbin/agetty -autologin root -o '-p -f - \\u' -keep-baud 115200,38400,9600
```

Recommendation

I recommend modifying `/etc/systemd/system/serial-getty@.service.d/autologin.conf` as follows:

```
[Service]
ExecStart=
ExecStart=-/sbin/agetty -o '-p - \\u' -keep-baud 115200,38400,9600 -noclear %I $TERM
```

Additional recommendations

- A similar entry is found in `/etc/systemd/system/getty@tty1.service.d/autologin.conf`. It is advisable to make corrections here too.
- In the `/etc/sudoers.d/90-cloud-init-users` file, the entry is set to `kali ALL=(ALL:ALL) NOPASSWD:ALL`, which may indicate the file was unintentionally left behind. This configuration allows sudo commands to execute without a password. If the file's presence is intentional, changing the entry to `kali ALL=(ALL:ALL) ALL` would enhance security.

Consideration

- Installing kali linux on Hyper-V with `kali-linux-2023.4-installer-amd64.iso` did not result in any files containing the `autologin root` directive under `/etc/systemd/system/`. Furthermore, automatic login was not executed at startup (see Appendix 3). This issue does not stem from the installation media but is likely a flaw in the AWS AMI creation process.
- Automatic login through the EC2 serial console was not permitted for both Ubuntu 22.04.4 LTS and Amazon Linux 2023 (see Appendix 1 and Appendix 2). This phenomenon appears to be specific to the kali linux AMI offered on AWS.

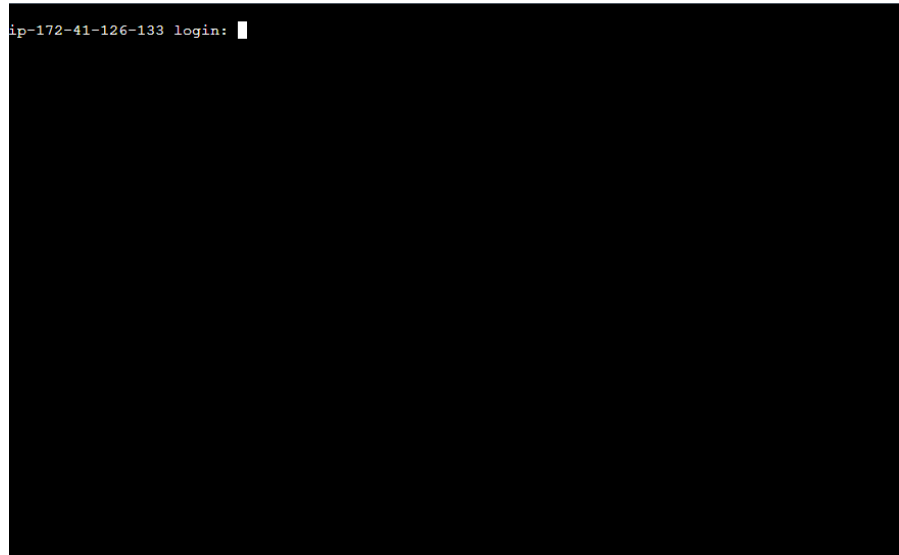
Conclusion

This report has outlined a method for invoking the root prompt in kali linux on AWS without the need for root privileges. Security is our top priority, and I earnestly hope for a resolution to this issue.

Appendix

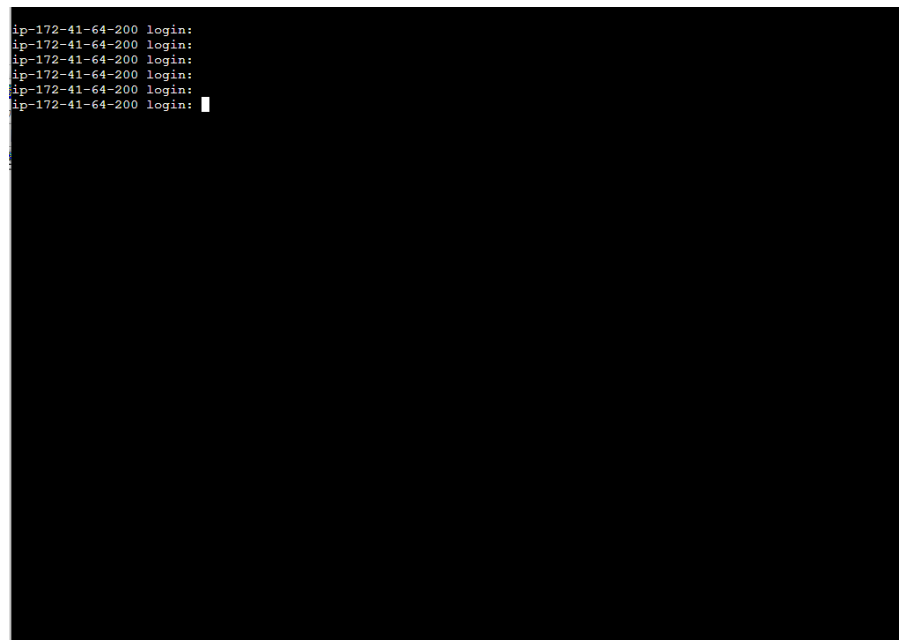
APPENDIX 1. SERIAL CONSOLE FOR UBUNTU 22.04.4 LTS

```
ip-172-41-126-133 login: █
```



APPENDIX 2. SERIAL CONSOLE FOR AMAZON LINUX 2023

```
ip-172-41-64-200 login:
ip-172-41-64-200 login:
ip-172-41-64-200 login:
ip-172-41-64-200 login:
ip-172-41-64-200 login:
ip-172-41-64-200 login:
ip-172-41-64-200 login:
ip-172-41-64-200 login: █
```



APPENDIX 3. HYPER-V CONSOLE FOR KALI LINUX MINIMAL INSTALLATION

kali GNU/Linux Rolling kali tty1

kali login: _