HI

Anything suspicious in the authorized_keys file?

root@ubuntu:~/.ssh# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDLbNC7I0IRcYcpjDMgfBYTMQw0g+LAFkwxF5eChdpZ6×19zILTPeznJmw6fOK4U+CEBchqzDrOG13O
root@ubuntu
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCkUZTf50C1vmy840PrY7NtIvJMQWDsXKZ7mhIVg1W/claHflDcH6Ig6bjFzVeqdOVaO5a8vV0JPTyIeKIc
root@ubuntu
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC375t+XyYfjIbnAeKPmXLVEQILlvTw/a/zoyzKTZKmQChfH9FnpwI58cDrMHHmTPrPTSLIZC18yDVN1cv7UPxqI
root@ubuntu
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCRME8Dd8P9MLcL2gmsoJ/reQqrUojIQcJNmQZPXDQeRBH9S7M7sy+1dEPomqImMZ5pZmLEC3iqZWi3dyBN
root@ubuntu
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCSnopCZEN9H+tvlennkHqKg2SdYAfAhmGiEeTA2GCgELuU+dulITb59UUMi8jzT4nupHEgdj8VA7TY/

GPT

There is a suspicious entry in the authorized_keys file:

`ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCSnopCZEN9H+tvlennkHqKg2SdYAfAhmGiEeTA2GCgELuU+
dulITb59UUMi8jzT4nupHEgdj8VA7TY/7GgIkM+PBfKXCAPD3dqVtjtRcrbdjp/yYc3usWakuqCEM
+NObnkC29OrT9CPEfcGyD2L95315×3ZtH2JxVZOjAyuDJT9uIFdNfQuDpEyhCEtXZH/iMovRksl5/
1D7HYChaOaKiMnZ/WjbsJyuVZAINWH2KEdAnPUo843xRa5rGVij9F4Z7aUjlzR+sRZno2OuZrOd/8
QDmu6fowDuqsCMwvQCSeEy9m2gkvHycyRNqfsFsRG1S8RVEN/KPxZ6bKNO3GMVAvkAUqYnkZtDGOZ
D+eLdXNIbSUsUlhTomqzK7RxKMRrIZPZSLe3/nhfgRCklJfd14iPlC2H2VnOFoM77PfrpEEqJqkEz
Gkr+wiOr3/r/L3oP+Arc750YMeuYeF4RD+1bObZ55yIy69FP3D/Ht9WLVsvmccRTB2T+X27sO98tl
AcMU= hacker`

The username "hacker" at the end of the key indicates that it might belong to someone with malicious intent. You should remove this entry from the authorized_keys file and investigate any unauthorized access to the system. Also, consider changing passwords and reviewing security measures to prevent future unauthorized access.

HI

What does "hacker" after the key mean?

GPT

The "hacker" text after the key is a comment associated with that specific key. Comments in SSH keys can serve as a way to help identify the key's owner, purpose, or any other relevant information. In this case, the comment "hacker" may suggest that the key could belong to someone with malicious intent or was added without proper authorization.

While the comment itself does not impact the functionality of the key, it is essential to investigate the origin of the key and verify whether it should have access to the system. If it's found to be unauthorized, remove the key from the authorized_keys file and take necessary security precautions, such as changing passwords and reviewing security measures.