r/linuxadmin • 5 yr. ago
martin_81

Passwordless SSH and Sudo

I inherited an environment where admins login to servers with a shared account using a username and password, I'm looking at switching this over to using named accounts using public/private keys for authentication, the private keys will be additionally protected with a passphrase. Ideally I'd like there to be no password configured on the named accounts so that access is only possible with authorized private key as that seems to be the most secure way. The only thing I'm struggling with is sudo access as you would typically be required to enter your password for sudo access but you obviously can't do that if no password is set on the account. I've tested the NOPASSWD option in suoders which works fine, but is it a good idea?

It seems to me setting a password on an account purely to require it to be entered for sudo access would actually weaken the security of an account as it creates attack vector that doesn't exist when no password is set. Am I missing anything? I'd be interested to know how others have handled this.

Join the conversation

Sort by: Best Search Comments

[deleted] • 5y ago

[deleted] • 5y ago

goat_on_a_float • 5y ago • Edited 5y ago

"PasswordAuthentication no".) This will not allow people to ssh using a password, but it will allow them to set a password, which they will be prompted for when they try to use sudo.

The sudo 'NOPASSWD' option is also probably fine, as long as your admins don't leave their terminals unattended.

18 Reply ...

[deleted] • 5y ago

pam_ssh_agent_auth

11 Reply ...

6 more replies

donnaber06 • 5y ago

> It seems to me setting a password on an account purely to require it to be entered for sudo access would actually weaken the security of an account as it creates attack vector that doesn't exist when no password is set. Am I missing anything? I'd be interested to know how others have handled this.

If you do not allow password access via ssh the the password is useless for anyone except the person who has a key and access. :-)

20 Reply ...

6 more replies

mstroeder • 5y ago

You could of course configure sshd to require *publickey* authentication and refuse *password* authentication.

Whether using sudo with *NOPASSWD* is a good idea depends on how many users can even login or whether a session can be used by an attacker.

Another option is to use pam_ssh or pam_ussh to use SSH publickey authentication also for sudo. But this requires SSH key agent forwarding, something I'd not do. YMMV.

4 Reply ...

[deleted] • 5y ago

for all of our servers in under a week. We added a script into our developer repo to make it easy for them to onboard into the system and it's been pretty seamless since.

I previously used my own CA for this and (temporarily) the BLESS project by Netflix. Unfortunately BLESS documentation isn't the best and the clients are a pain in the ass (IMO).

3 Reply ···

d00ber • 5y ago

I might be understanding the question (I am very tired as I write this..) but I use FreeIPA to manage this at a larger scale. You add hosts/users to HBAC/sudoer groups and rules and assign these things.

2 Reply ···

2 more replies

[deleted] • 5y ago

If you can only login via key there isn't much reason for sudo password. Azure does this by default. If you create a VM and set the user to have an ssh key when the VM spins up then it automatically sets your user to have password less sudo. It's just an extra pointless layer. If they have logged in they already have your ssh key. You can password protect the ssh key so if it gets found by someone then they need a password. That makes More dense then using a password on the user for sudo

2 Reply ···

1 more reply

[deleted] • 5y ago

`NOPASSWD` on sudo isn't allowed in our environment. Logging in with a password is also not allowed.

We do that by having `PasswordAuthentication No` in our `/etc/ssh/sshd.conf`

3 Reply ···

1 more reply

r/linuxadmin • 11 days ago

Password Manager for SSH (for su or escalating privileges, not logging in)

19 upvotes · 39 comments

27 upvotes · 18 comments

r/devops • 3 yr. ago

Sudo rules when using SSH certificates

17 upvotes · 18 comments

r/linuxquestions • 2 yr. ago

SSH connection without asking for password

3 upvotes · 26 comments

1 upvote

r/linuxquestions • 1 yr. ago

Using ssh with sudo without ssh key password

3 upvotes · 17 comments

r/linuxquestions • 3 yr. ago

Any passwordless authentication technology for remote sudo, like SSH/XRDP?

3 upvotes · 7 comments

r/shortcuts • 3 yr. ago

How do I pass sudo password to script to run over SSH?

4 upvotes · 6 comments

r/linux4noobs • 11 yr. ago

sudo without password from ssh?

5 upvotes · 16 comments

r/linuxquestions • 9 yr. ago

SSH key for sudo authentication? [x-post /r/linux]

9 upvotes · 6 comments

r/linuxquestions • 4 yr. ago

r/linuxadmin • 3 yr. ago

Where does passwordless sudo fit in to industry standards and security best practice?

2 upvotes · 10 comments

r/linuxquestions • 6 mo. ago

Why is passwordless sudo (for Ansible) popular?

30 upvotes · 18 comments

r/linuxadmin • 3 mo. ago

SSH Keys Between Windows 10 and Linux

1 upvote · 24 comments

r/linuxadmin • 1 mo. ago

OpenSSH 10 relies on standards for quantum-safe key exchange

64 upvotes · 6 comments

r/ShittySysadmin • 7 mo. ago

Third party vendor, “never trained on ssh…”

455 upvotes · 54 comments

r/dumbclub • 25 days ago

What happen to all the SSH*** websites? Seems no more services.**

5 upvotes · 8 comments

r/homelab • 1 yr. ago

A reminder: check and update your OpenSSH server RIGHT NOW

332 upvotes · 142 comments

r/cybersecurity • 10 mo. ago

Why not enable SSH?

179 upvotes · 135 comments

r/linuxquestions • 1 yr. ago

How exactly is SSH safe?

Log In

PoWeRsHeLl ScRiPts every windows user NEEDS

133 upvotes · 55 comments

r/embedded • 10 mo. ago

Lesson learned with systemd.

55 upvotes · 42 comments

r/ShittySysadmin • 2 mo. ago

If server is running, who cares if newer protocols aren't supported, riiight?

27 upvotes · 17 comments

r/linuxadmin • 14 days ago

Aren't all users (including root) running in userspace and do systemcalls that the kernel handles in kernel space?

37 upvotes · 17 comments

r/ShittySysadmin • 2 mo. ago

HELP - ran an unknown script on my pc, is it malware??

86 upvotes · 14 comments

TOP POSTS

Reddit

reReddit: Top posts of July 13, 2020

Reddit

reReddit: Top posts of July 2020

Reddit

reReddit: Top posts of 2020