SSH Permission denied on Correct Password Authentication

I could successfully SSH into my machine yesterday with the exact same credentials I am using today. The machine is running **Centos 6.3**. But now for some reason it is giving me permission denied. Here is my `-v` print out, sshd_config, and ssh_config files.

```
$ ssh -vg -L 3333:localhost:6666 misfitred@devilsmilk
OpenSSH_6.1p1, OpenSSL 1.0.1c 10 May 2012
debug1: Reading configuration data /etc/ssh_config
debug1: Connecting to devilsmilk [10.0.10.113] port 22.
debug1: Connection established.
debug1: identity file /home/kgraves/.ssh/id_rsa type -1
debug1: identity file /home/kgraves/.ssh/id_rsa-cert type -1
debug1: identity file /home/kgraves/.ssh/id_dsa type -1
debug1: identity file /home/kgraves/.ssh/id_dsa-cert type -1
debug1: identity file /home/kgraves/.ssh/id_ecdsa type -1
debug1: identity file /home/kgraves/.ssh/id_ecdsa-cert type -1
debug1: Remote protocol version 2.0, remote software version OpenSSH_6.1
debug1: match: OpenSSH_6.1 pat OpenSSH*
debug1: Enabling compatibility mode for protocol 2.0
debug1: Local version string SSH-2.0-OpenSSH_6.1
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: server->client aes128-ctr hmac-md5 none
debug1: kex: client->server aes128-ctr hmac-md5 none
debug1: sending SSH2_MSG_KEX_ECDH_INIT
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
debug1: Server host key: ECDSA de:1c:37:d7:84:0b:f8:f9:5e:da:11:49:57:4f:b8:f1
debug1: Host 'devilsmilk' is known and matches the ECDSA host key.
debug1: Found key in /home/kgraves/.ssh/known_hosts:1
debug1: ssh_ecdsa_verify: signature correct
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug1: SSH2_MSG_NEWKEYS received
debug1: Roaming not allowed by server
debug1: SSH2_MSG_SERVICE_REQUEST sent
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug1: Authentications that can continue: publickey,password,keyboard-interacti
ve
debug1: Next authentication method: publickey
debug1: Trying private key: /home/kgraves/.ssh/id_rsa
debug1: Trying private key: /home/kgraves/.ssh/id_dsa
debug1: Trying private key: /home/kgraves/.ssh/id_ecdsa
debug1: Next authentication method: keyboard-interactive
debug1: Authentications that can continue: publickey,password,keyboard-interacti
ve
debug1: Next authentication method: password
misfitred@devilsmilk's password:
debug1: Authentications that can continue: publickey,password,keyboard-interacti
ve
Permission denied, please try again.
misfitred@devilsmilk's password:
debug1: Authentications that can continue: publickey,password,keyboard-interacti
ve
Permission denied, please try again.
misfitred@devilsmilk's password:
debug1: Authentications that can continue: publickey,password,keyboard-interactive
debug1: No more authentication methods to try.
Permission denied (publickey,password,keyboard-interactive).
```

Here is my sshd_config file on devilsmilk:

```
#   $OpenBSD: sshd_config,v 1.80 2008/07/02 02:24:18 djm Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options change a
# default value.

Port 22
#AddressFamily any
```

```
#ListenAddress 0.0.0.0
#ListenAddress ::

# Disable legacy (protocol version 1) support in the server for new
# installations. In future the default will change to require explicit
# activation of protocol 1
#Protocol 2

# HostKey for protocol version 1
# HostKey /etc/ssh/ssh_host_key
# HostKeys for protocol version 2
# HostKey /etc/ssh/ssh_host_rsa_key
# HostKey /etc/ssh/ssh_host_dsa_key

# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 1h
#ServerKeyBits 1024

# Logging
# obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
StrictModes no
#MaxAuthTries 6
#MaxSessions 10

#RSAAuthentication yes
#PubkeyAuthentication yes
#AuthorizedKeysFile .ssh/authorized_keys
#AuthorizedKeysCommand none
#AuthorizedKeysCommandRunAs nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#RhostsRSAAuthentication no
# similar for protocol version 2
#HostbasedAuthentication yes
# Change to yes if you don't trust ~/.ssh/known_hosts for
# RhostsRSAAuthentication and HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
#KerberosUseKuserok yes

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPIAuthentication yes
#GSSAPICleanupCredentials yes
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
#UsePAM no

# Accept locale-related environment variables
#AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES
#AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
#AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
#AcceptEnv XMODIFIERS

#AllowAgentForwarding yes
AllowTcpForwarding yes
GatewayPorts yes
#X11Forwarding no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PrintMotd yes
#PrintLastLog yes
TCPKeepAlive yes
#UseLogin no
#UsePrivilegeSeparation yes
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#ShowPatchLevel no
#UseDNS yes
```

```
#PidFile /var/run/sshd.pid
#MaxStartups 10
#PermitTunnel no
#ChrootDirectory none

# no default banner path
#Banner none

# override default of no subsystems
Subsystem   sftp    /usr/libexec/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#   X11Forwarding no
#   AllowTcpForwarding no
#   ForceCommand cvs server
```

And here is my ssh_config file:

```
#   $OpenBSD: ssh_config,v 1.25 2009/02/17 01:28:32 djm Exp $

# This is the ssh client system-wide configuration file.  See
# ssh_config(5) for more information.  This file provides defaults for
# users, and the values can be changed in per-user configuration files
# or on the command line.

# Configuration data is parsed as follows:
#  1. command line options
#  2. user-specific file
#  3. system-wide file
# Any configuration value is only changed the first time it is set.
# Thus, host-specific definitions should be at the beginning of the
# configuration file, and defaults at the end.

# Site-wide defaults for some commonly used options.  For a comprehensive
# list of available options, their meanings and defaults, please see the
# ssh_config(5) man page.

# Host *
#   ForwardAgent no
#   ForwardX11 no
#   RhostsRSAAuthentication no
#   RSAAuthentication yes
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
#   GSSAPIKeyExchange no
#   GSSAPITrustDNS no
#   BatchMode no
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/identity
#   IdentityFile ~/.ssh/id_rsa
#   IdentityFile ~/.ssh/id_dsa
#   Port 22
#   Protocol 2,1
#   Cipher 3des
#   Ciphers aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc
#   MACs hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160
#   EscapeChar ~
#   Tunnel no
#   TunnelDevice any:any
#   PermitLocalCommand no
#   VisualHostKey no
#Host *
# GSSAPIAuthentication yes
# If this option is set to yes then remote X11 clients will have full access
# to the original X11 display. As virtually no X11 client supports the untrusted
# mode correctly we set this to yes.
    ForwardX11Trusted yes
# Send locale-related environment variables
    SendEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES
    SendEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
    SendEnv LC_IDENTIFICATION LC_ALL LANGUAGE
    SendEnv XMODIFIERS
```

UPDATE REQUEST 1: /var/log/secure

```
Jan 29 12:26:26 localhost sshd[2317]: Server listening on 0.0.0.0 port 22.
Jan 29 12:26:26 localhost sshd[2317]: Server listening on :: port 22.
Jan 29 12:26:34 localhost polkitd(authority=local): Registered Authentication Agent for
session /org/freedesktop/ConsoleKit/Session1 (system bus name :1.29 [/usr/libexec/polkit-
gnome-authentication-agent-1], object path /org/gnome/PolicyKit1/AuthenticationAgent,
locale en_US.UTF-8)
Jan 29 12:36:09 localhost pam: gdm-password[3029]: pam_unix(gdm-password:session): session
opened for user misfitred by (uid=0)
Jan 29 12:36:09 localhost polkitd(authority=local): Unregistered Authentication Agent for
session /org/freedesktop/ConsoleKit/Session1 (system bus name :1.29, object path
/org/gnome/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Jan 29 12:36:11 localhost polkitd(authority=local): Registered Authentication Agent for
session /org/freedesktop/ConsoleKit/Session2 (system bus name :1.45 [/usr/libexec/polkit-
gnome-authentication-agent-1], object path /org/gnome/PolicyKit1/AuthenticationAgent,
locale en_US.UTF-8)
Jan 29 12:53:39 localhost polkitd(authority=local): Operator of unix-
session:/org/freedesktop/ConsoleKit/Session2 successfully authenticated as unix-user:root
to gain TEMPORARY authorization for action org.freedesktop.packagekit.system-update for
system-bus-name::1.64 [gpk-update-viewer] (owned by unix-user:misfitred)
Jan 29 12:54:02 localhost su: pam_unix(su:session): session opened for user root by
misfitred(uid=501)
Jan 29 12:54:06 localhost sshd[2317]: Received signal 15; terminating.
```

```
Jan 29 12:54:06 localhost sshd[3948]: Server listening on 0.0.0.0 port 22.
Jan 29 12:54:06 localhost sshd[3948]: Server listening on :: port 22.
Jan 29 12:55:46 localhost su: pam_unix(su:session): session closed for user root
Jan 29 12:55:56 localhost pam: gdm-password[3029]: pam_unix(gdm-password:session): session
closed for user misfitred
Jan 29 12:55:56 localhost polkitd(authority=local): Unregistered Authentication Agent for
session /org/freedesktop/ConsoleKit/Session2 (system bus name :1.45, object path
/org/gnome/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Jan 29 12:55:58 localhost polkitd(authority=local): Registered Authentication Agent for
session /org/freedesktop/ConsoleKit/Session3 (system bus name :1.78 [/usr/libexec/polkit-
gnome-authentication-agent-1], object path /org/gnome/PolicyKit1/AuthenticationAgent,
locale en_US.UTF-8)
Jan 29 12:56:29 localhost pam: gdm-password[4044]: pam_unix(gdm-password:auth):
conversation failed
Jan 29 12:56:29 localhost pam: gdm-password[4044]: pam_unix(gdm-password:auth): auth could
not identify password for [misfitred]
Jan 29 12:56:29 localhost pam: gdm-password[4044]: gkr-pam: no password is available for
user
Jan 29 12:57:11 localhost pam: gdm-password[4051]: pam_selinux_permit(gdm-password:auth):
Cannot determine the user's name
Jan 29 12:57:11 localhost pam: gdm-password[4051]: pam_succeed_if(gdm-password:auth):
error retrieving user name: Conversation error
Jan 29 12:57:11 localhost pam: gdm-password[4051]: gkr-pam: couldn't get the user name:
Conversation error
Jan 29 12:57:17 localhost pam: gdm-password[4053]: pam_unix(gdm-password:session): session
opened for user misfitred by (uid=0)
Jan 29 12:57:17 localhost polkitd(authority=local): Unregistered Authentication Agent for
session /org/freedesktop/ConsoleKit/Session3 (system bus name :1.78, object path
/org/gnome/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Jan 29 12:57:17 localhost polkitd(authority=local): Registered Authentication Agent for
session /org/freedesktop/ConsoleKit/Session4 (system bus name :1.93 [/usr/libexec/polkit-
gnome-authentication-agent-1], object path /org/gnome/PolicyKit1/AuthenticationAgent,
locale en_US.UTF-8)
Jan 29 12:57:49 localhost unix_chkpwd[4495]: password check failed for user (root)
Jan 29 12:57:49 localhost su: pam_unix(su:auth): authentication failure; logname=misfitred
uid=501 euid=0 tty=pts/0 ruser=misfitred rhost=  user=root
Jan 29 12:58:04 localhost su: pam_unix(su:session): session opened for user root by
misfitred(uid=501)
Jan 29 13:16:16 localhost su: pam_unix(su:session): session closed for user root
Jan 29 13:18:05 localhost su: pam_unix(su:session): session opened for user root by
misfitred(uid=501)
Jan 29 13:21:14 localhost su: pam_unix(su:session): session closed for user root
Jan 29 13:21:40 localhost su: pam_unix(su:session): session opened for user root by
misfitred(uid=501)
Jan 29 13:24:17 localhost su: pam_unix(su:session): session opened for user misfitred by
misfitred(uid=0)
Jan 29 13:27:10 localhost su: pam_unix(su:session): session opened for user root by
misfitred(uid=501)
Jan 29 13:28:55 localhost su: pam_unix(su:session): session closed for user root
Jan 29 13:28:55 localhost su: pam_unix(su:session): session closed for user misfitred
Jan 29 13:28:55 localhost su: pam_unix(su:session): session closed for user root
Jan 29 13:29:00 localhost su: pam_unix(su:session): session opened for user root by
misfitred(uid=501)
Jan 29 13:31:48 localhost sshd[3948]: Received signal 15; terminating.
Jan 29 13:31:48 localhost sshd[5498]: Server listening on 0.0.0.0 port 22.
Jan 29 13:31:48 localhost sshd[5498]: Server listening on :: port 22.
Jan 29 13:44:58 localhost sshd[5498]: Received signal 15; terminating.
Jan 29 13:44:58 localhost sshd[5711]: Server listening on 0.0.0.0 port 22.
Jan 29 13:44:58 localhost sshd[5711]: Server listening on :: port 22.
Jan 29 14:00:19 localhost sshd[5711]: Received signal 15; terminating.
Jan 29 14:00:19 localhost sshd[5956]: Server listening on 0.0.0.0 port 22.
Jan 29 14:00:19 localhost sshd[5956]: Server listening on :: port 22.
Jan 29 15:03:00 localhost sshd[5956]: Received signal 15; terminating.
Jan 29 15:10:23 localhost su: pam_unix(su:session): session closed for user root
Jan 29 15:10:38 localhost pam: gdm-password[4053]: pam_unix(gdm-password:session): session
closed for user misfitred
Jan 29 15:10:38 localhost polkitd(authority=local): Unregistered Authentication Agent for
session /org/freedesktop/ConsoleKit/Session4 (system bus name :1.93, object path
/org/gnome/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Jan 29 15:11:21 localhost polkitd(authority=local): Registered Authentication Agent for
session /org/freedesktop/ConsoleKit/Session1 (system bus name :1.29 [/usr/libexec/polkit-
gnome-authentication-agent-1], object path /org/gnome/PolicyKit1/AuthenticationAgent,
locale en_US.UTF-8)
Jan 29 15:11:32 localhost pam: gdm-password[2919]: pam_unix(gdm-password:session): session
opened for user misfitred by (uid=0)
Jan 29 15:11:32 localhost polkitd(authority=local): Unregistered Authentication Agent for
session /org/freedesktop/ConsoleKit/Session1 (system bus name :1.29, object path
/org/gnome/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Jan 29 15:11:33 localhost polkitd(authority=local): Registered Authentication Agent for
session /org/freedesktop/ConsoleKit/Session2 (system bus name :1.45 [/usr/libexec/polkit-
gnome-authentication-agent-1], object path /org/gnome/PolicyKit1/AuthenticationAgent,
locale en_US.UTF-8)
Jan 29 15:15:10 localhost su: pam_unix(su:session): session opened for user root by
misfitred(uid=501)
Jan 29 15:30:24 localhost userhelper[3700]: running '/usr/share/system-config-
users/system-config-users ' with root privileges on behalf of 'root'
Jan 29 15:32:00 localhost su: pam_unix(su:session): session opened for user misfitred by
misfitred(uid=0)
Jan 29 15:32:23 localhost passwd: gkr-pam: changed password for 'login' keyring
Jan 29 15:32:39 localhost passwd: pam_unix(passwd:chauthtok): password changed for
misfitred
Jan 29 15:32:39 localhost passwd: gkr-pam: couldn't change password for 'login' keyring: 1
Jan 29 15:33:06 localhost passwd: pam_unix(passwd:chauthtok): password changed for
misfitred
Jan 29 15:33:06 localhost passwd: gkr-pam: changed password for 'login' keyring
Jan 29 15:37:08 localhost su: pam_unix(su:session): session opened for user root by
misfitred(uid=501)
Jan 29 15:38:16 localhost su: pam_unix(su:session): session closed for user root
Jan 29 15:38:16 localhost su: pam_unix(su:session): session closed for user misfitred
Jan 29 15:38:16 localhost su: pam_unix(su:session): session closed for user root
Jan 29 15:38:25 localhost su: pam_unix(su:session): session opened for user root by
misfitred(uid=501)
Jan 29 15:42:47 localhost su: pam_unix(su:session): session closed for user root
Jan 29 15:47:13 localhost sshd[4111]: pam_unix(sshd:session): session opened for user
```

```
misfitred by (uid=0)
Jan 29 16:49:40 localhost su: pam_unix(su:session): session opened for user root by
misfitred(uid=501)
Jan 29 16:55:19 localhost su: pam_unix(su:session): session opened for user root by
misfitred(uid=501)
Jan 30 08:34:57 localhost sshd[4111]: pam_unix(sshd:session): session closed for user
misfitred
Jan 30 08:34:57 localhost su: pam_unix(su:session): session closed for user root
Jan 30 08:35:24 localhost su: pam_unix(su:session): session opened for user root by
misfitred(uid=501)
```

ssh | permissions | centos | user-accounts | openssh

edited Jan 30 '13 at 13:40

asked Jan 29 '13 at 20:24

Kentgrav
718 1 9 16

1 Have you tried another user? Or changing the password for this one? – fboaventura Jan 29 '13 at 20:46

1 I agree with fboaventura; The configs look fine; try changing the password for your user to what you think it should be, also check that it isn't expired/account locked. And try another user just in case. Also, are you able to log in locally as that user? i.e. is the error specific to SSH or is it having an error via other auth mechs. – Justin Jan 29 '13 at 22:56

1 (1) caplock? (2) From server, post related error in `/var/log/secure` – John Siu Jan 29 '13 at 23:18

@ fboaventura & Justin I did try another user and I also changed the password and tried it again with no success. I can login locally just fine and I can also SSH to localhost just fine. – Kentgrav Jan 30 '13 at 13:33

@ John Siu I added the /var/log/secure and I attempted the SSH right before I copied it. And nothing was added to it. Hope it helps. – Kentgrav Jan 30 '13 at 13:41

3 Answers

server's `/etc/ssh/sshd_config` :

1. To enable password authentication, uncomment

```
#PasswordAuthentication yes
```

2. To enable root login, uncomment

```
#PermitRootLogin yes
```

3. To enable ssh key login, uncomment

```
#PubkeyAuthentication yes
#AuthorizedKeysFile .ssh/authorized_keys
```

I believe (1) is what you're looking for.

edited Jul 10 '16 at 11:54

The Sexiest Man in Jamaica
113 6

answered Jan 30 '13 at 14:02

John Siu
4,522 1 10 20

Yeah I did this already I actually figured out what the problem was. And as I thought...it was the one thing that should have been blatantly obvious. – Kentgrav Jan 30 '13 at 16:08

2 For anyone else who is wondering you can find it sshd_config here: /etc/ssh/sshd_config – Oliver Dixon Aug 21 '15 at 9:20

The problem with this answer is that the defaults are commented out by default as the comments in the file explain. It doesn't matter if (1) is commented or not because the default is "yes". The correct answer is below. It's probably a DNS problem and can easily test by using the IP address instead of the domain name. – Colin Keenan Sep 18 '15 at 4:41

I figured it out. As a last ditch effort I was going to attempt to ssh into the server via the IP address instead of the domain name. When I did an `ifconfig` on the server to get the IP I realized it was different than it was yesterday.

Turns out I forgot to set a static IP address on the server when I created it and trying to ssh to `devilsmilk` was still mapped to the old IP address on the DNS server. So I set a static IP address on the server and updated the A record with the new IP address and it works fine.

Thanks everyone for your help.

answered Jan 30 '13 at 16:12

Kentgrav
718 1 9 16

5 The SSH client would have warned you quite loudly that the host key has changed in this case. – BatchyX Jan 30 '13 at 16:44

Yeah it did but I was also messing around with ssh-keygen on all my servers and trying to figure out how to get the machines to authenticate without using username/password and RSA Pub keys only so after I scrubbed all the Known_hosts files, recreated all the Pub keys and copied them into the Authorized_keys files and it STILL was saying that, it kinda tipped me off. – Kentgrav Jan 30 '13 at 21:08

Try restarting the sshd service: `service --full-restart sshd`

edited Dec 16 '15 at 18:13
BowlesCR
2,411 6 17

answered Dec 16 '15 at 15:25
jojomannoh
9

protected by JakeGould Dec 17 '15 at 5:07

Thank you for your interest in this question. Because it has attracted low-quality or spam answers that had to be removed, posting an answer now requires 10 reputation on this site (the association bonus does not count).

Would you like to answer one of these unanswered questions instead?