

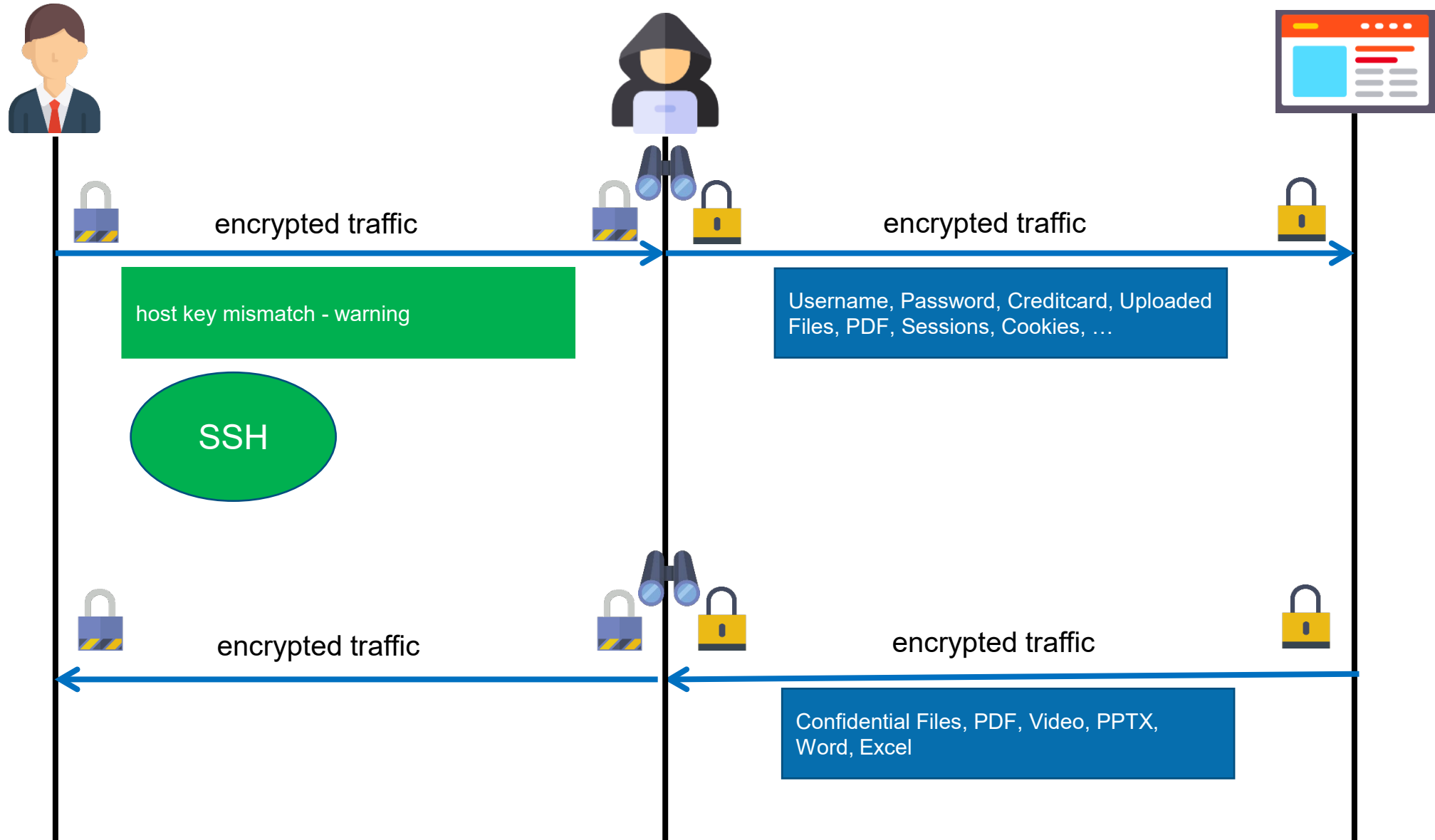


# Man in the Middle Attacks

## SSH

HS2024 Cyber Defense

# Man in the Middle – SSH Interception - Encrypted Traffic



# Man in the Middle – Intercepting - Encrypted Traffic

ssh mitm

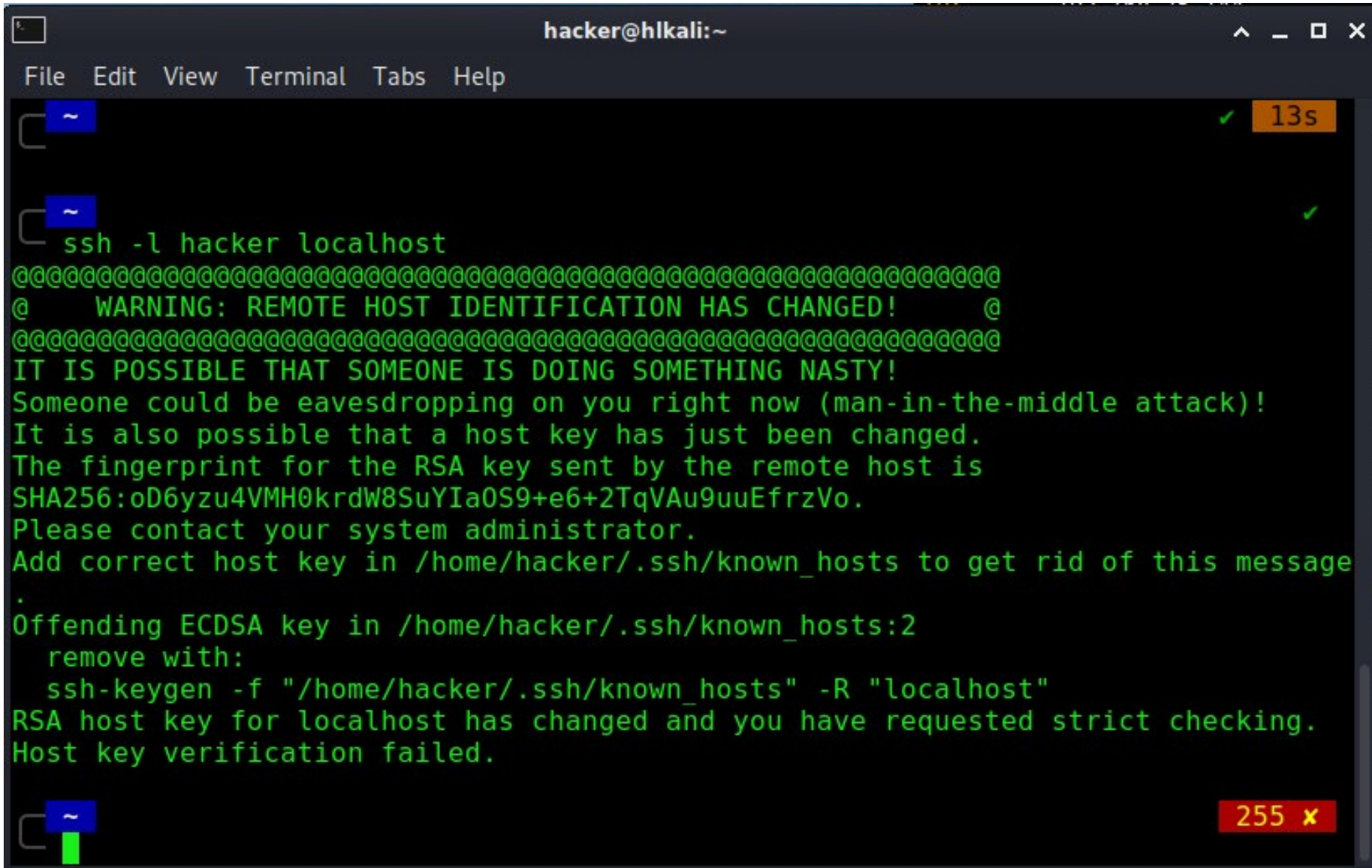


origin ssh server



```
ssh-mitm_1 | [CLIENT] * Wait for client shell
ssh-mitm_1 | [SERVER] * If the user has used up all attempts, or if he hasn't
ssh-mitm_1 | ticate in 60 seconds (n * 100ms), disconnect
ssh-mitm_1 | [CLIENT] > Try auth with Username:hacker and Password:compass
ssh-mitm_1 | [CLIENT] Authentication succeeded (password), user:hacker
ssh-mitm_1 | [SERVER] < channel 0: new [server-session]
ssh-mitm_1 | [CLIENT] > channel 0: new [client-session]
ssh-mitm_1 | [CLIENT] > channel 0: send open
ssh-mitm_1 | [CLIENT] Entering interactive session
ssh-mitm_1 | [*** SERVER EVENT LOOP ***]
ssh-mitm_1 | [CLIENT] > Request xterm 256color[CLIENT] error: Client send env LANG = en_US.UTF-8, but failed to send it to remote SERVER
```

# Man in the Middle – Intercepting - Encrypted Traffic



A screenshot of a terminal window titled "hacker@hlkali:~". The window has a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". The terminal shows a session where a user has run the command `ssh -l hacker localhost`. The output displays a warning message from SSH: "WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY! Someone could be eavesdropping on you right now (man-in-the-middle attack)! It is also possible that a host key has just been changed. The fingerprint for the RSA key sent by the remote host is SHA256:oD6yzu4VMH0krdW8SuYIa0S9+e6+2TqVAu9uuEfrzVo. Please contact your system administrator. Add correct host key in /home/hacker/.ssh/known\_hosts to get rid of this message". Below the warning, it shows the removal of an offending ECDSA key from the known\_hosts file and the execution of `ssh-keygen -f "/home/hacker/.ssh/known_hosts" -R "localhost"`. The final output is "RSA host key for localhost has changed and you have requested strict checking. Host key verification failed." The terminal interface includes a scrollbar on the right and a status bar at the bottom right showing "255 x".

```
hacker@hlkali:~  
File Edit View Terminal Tabs Help  
~  
~  
ssh -l hacker localhost  
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@  
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!    @  
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@  
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!  
Someone could be eavesdropping on you right now (man-in-the-middle attack)!  
It is also possible that a host key has just been changed.  
The fingerprint for the RSA key sent by the remote host is  
SHA256:oD6yzu4VMH0krdW8SuYIa0S9+e6+2TqVAu9uuEfrzVo.  
Please contact your system administrator.  
Add correct host key in /home/hacker/.ssh/known_hosts to get rid of this message  
.  
Offending ECDSA key in /home/hacker/.ssh/known_hosts:2  
  remove with:  
    ssh-keygen -f "/home/hacker/.ssh/known_hosts" -R "localhost"  
RSA host key for localhost has changed and you have requested strict checking.  
Host key verification failed.  
~
```

# Users not aware of the warning

```
ssh-keygen -f "/home/hacker/.ssh/known_hosts" -R "localhost"
```

```
~ ssh-keygen -f "/home/hacker/.ssh/known_hosts" -R "localhost"
# Host localhost found: line 2
/home/hacker/.ssh/known_hosts updated.
Original contents retained as /home/hacker/.ssh/known_hosts.old
```



```
~ ssh -l hacker localhost
The authenticity of host 'localhost (:::1)' can't be established.
RSA key fingerprint is SHA256:oD6yzu4VMH0krdW8SuYIa0S9+e6+2TqVAu9uuEfrzVo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (RSA) to the list of known hosts.
hacker@localhost's password:
Welcome to Alpine!

The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See <http://wiki.alpinelinux.org/>.

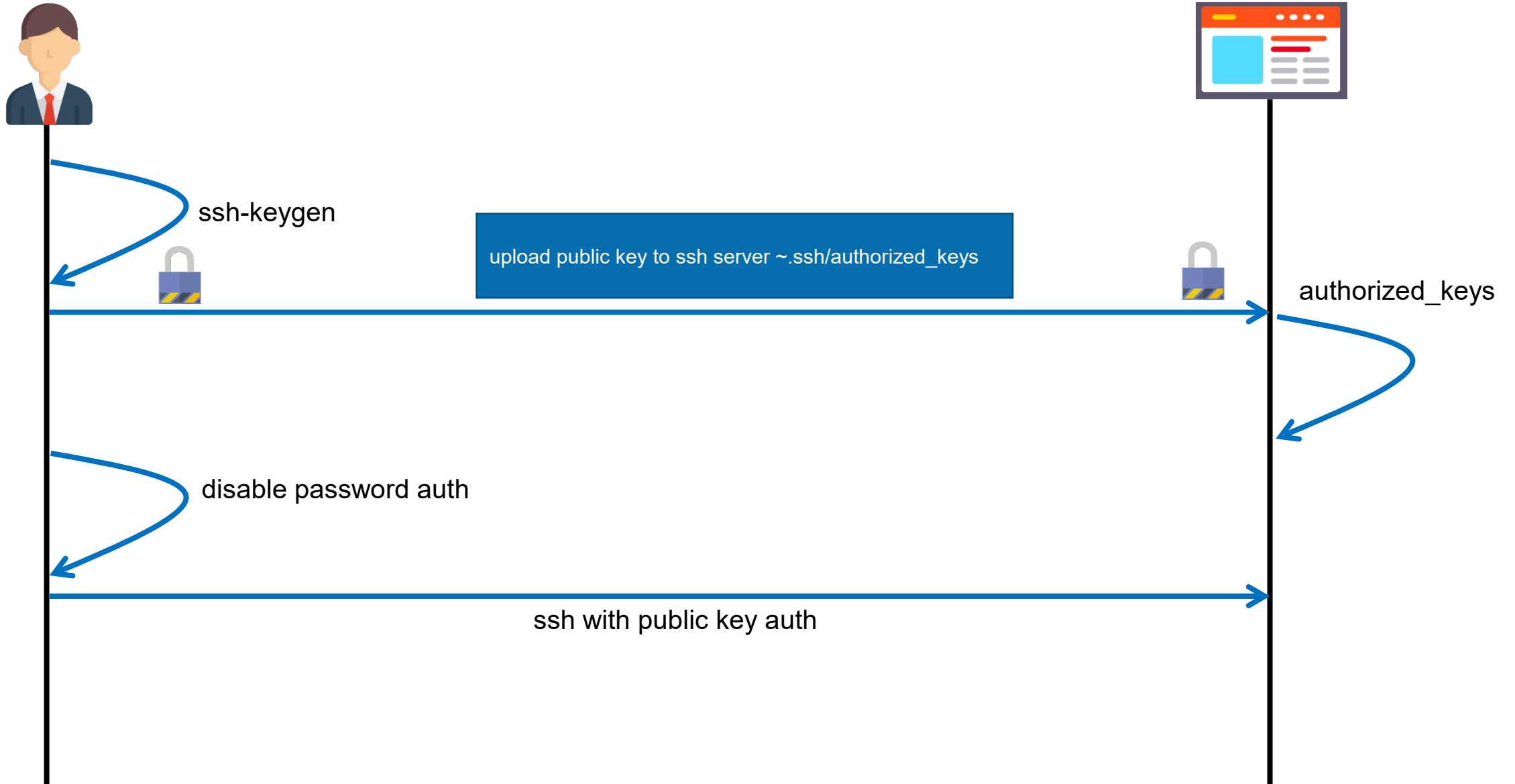
You can setup the system with the command: setup-alpine

You may change this message by editing /etc/motd.

dd5a35db37f3:~$
```

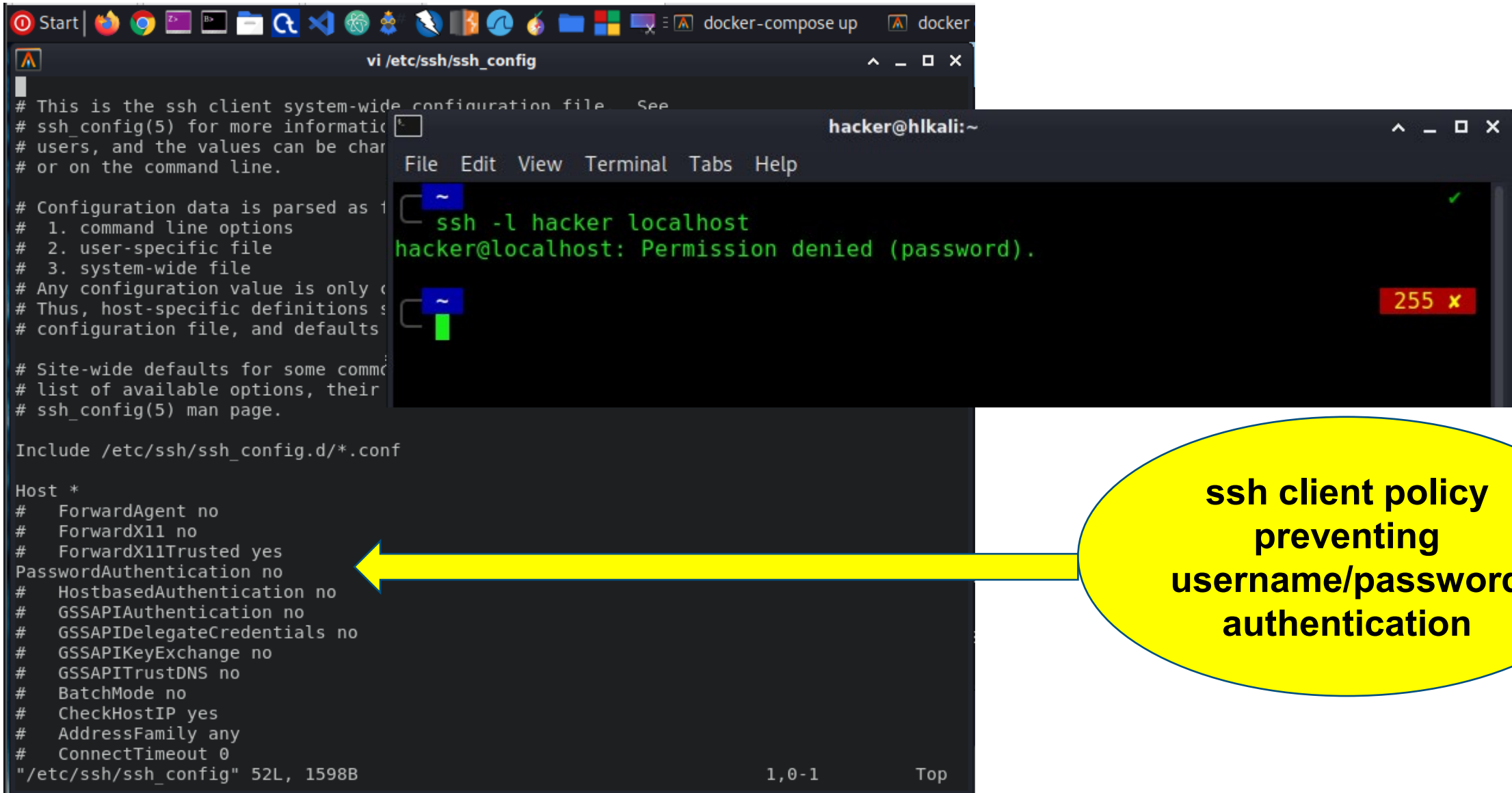
# SSH Public Key Authentication

# SSH Public Key Authentication





# SSH Public Key Authentication



The screenshot shows a terminal window with a dark background. The top bar displays the title 'vi /etc/ssh/ssh\_config' and window controls. The main content is the SSH configuration file, which includes comments about system-wide configuration and a list of options for the 'Host \*' section. A yellow arrow points from a yellow oval on the right to the 'PasswordAuthentication no' line. Overlaid on the terminal is a smaller window titled 'hacker@hlkali:~' showing the command 'ssh -l hacker localhost' and the output 'hacker@localhost: Permission denied (password)'. A red box with '255 x' is in the bottom right of this window.

```
# This is the ssh client system-wide configuration file. See
# ssh_config(5) for more information.
# users, and the values can be changed 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 if it exists in a
# configuration file, and defaults to the system-wide file.

# Site-wide defaults for some common options.
# list of available options, their defaults, and the man page.

Include /etc/ssh/ssh_config.d/*.conf

Host *
# ForwardAgent no
# ForwardX11 no
# ForwardX11Trusted yes
PasswordAuthentication no
# HostbasedAuthentication no
# GSSAPIAuthentication no
# GSSAPIDelegateCredentials no
# GSSAPIKeyExchange no
# GSSAPITrustDNS no
# BatchMode no
# CheckHostIP yes
# AddressFamily any
# ConnectTimeout 0
"/etc/ssh/ssh_config" 52L, 1598B
```

hacker@hlkali:~

```
ssh -l hacker localhost
hacker@localhost: Permission denied (password).
```

255 x

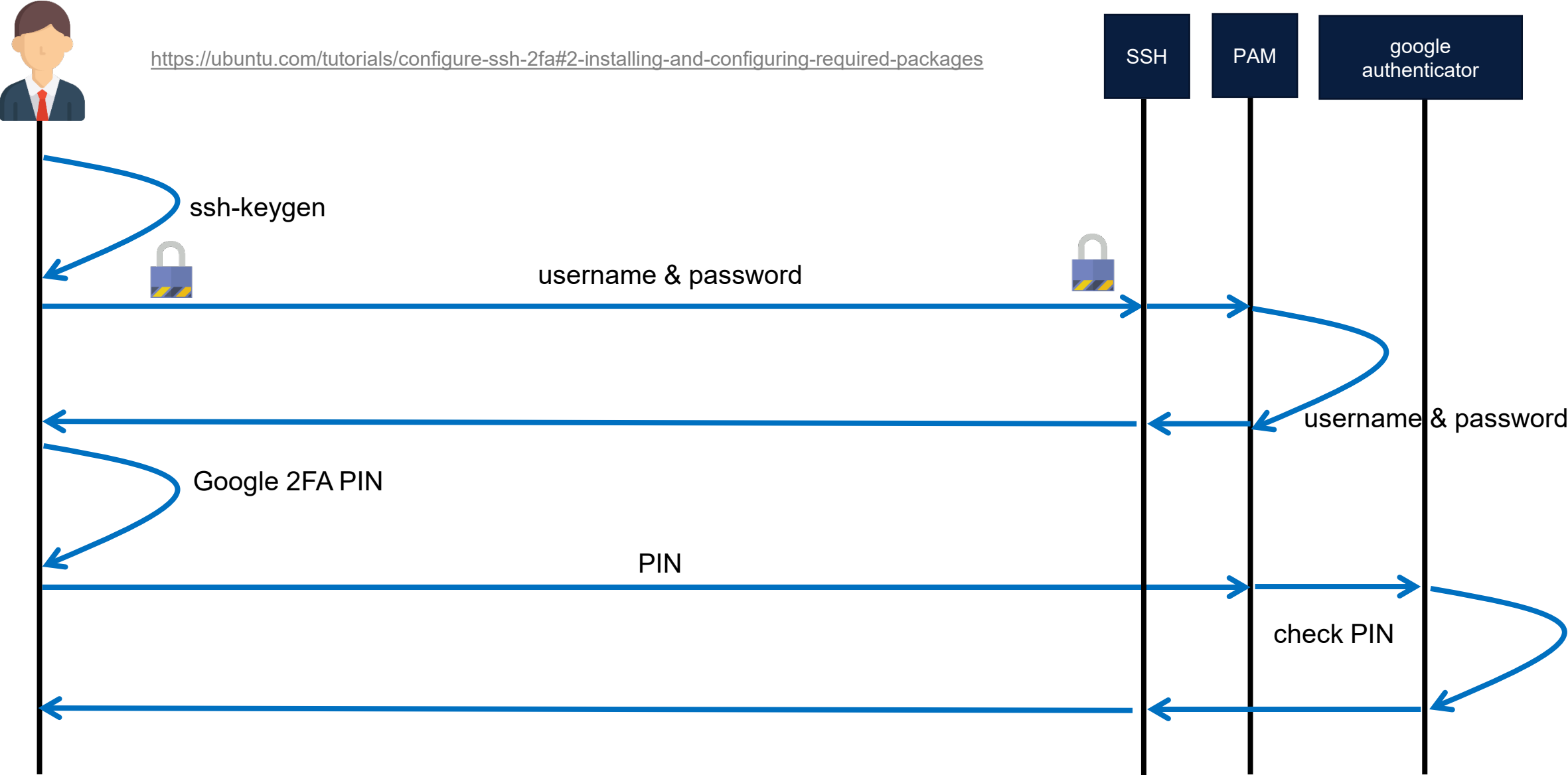
**ssh client policy  
preventing  
username/password  
authentication**



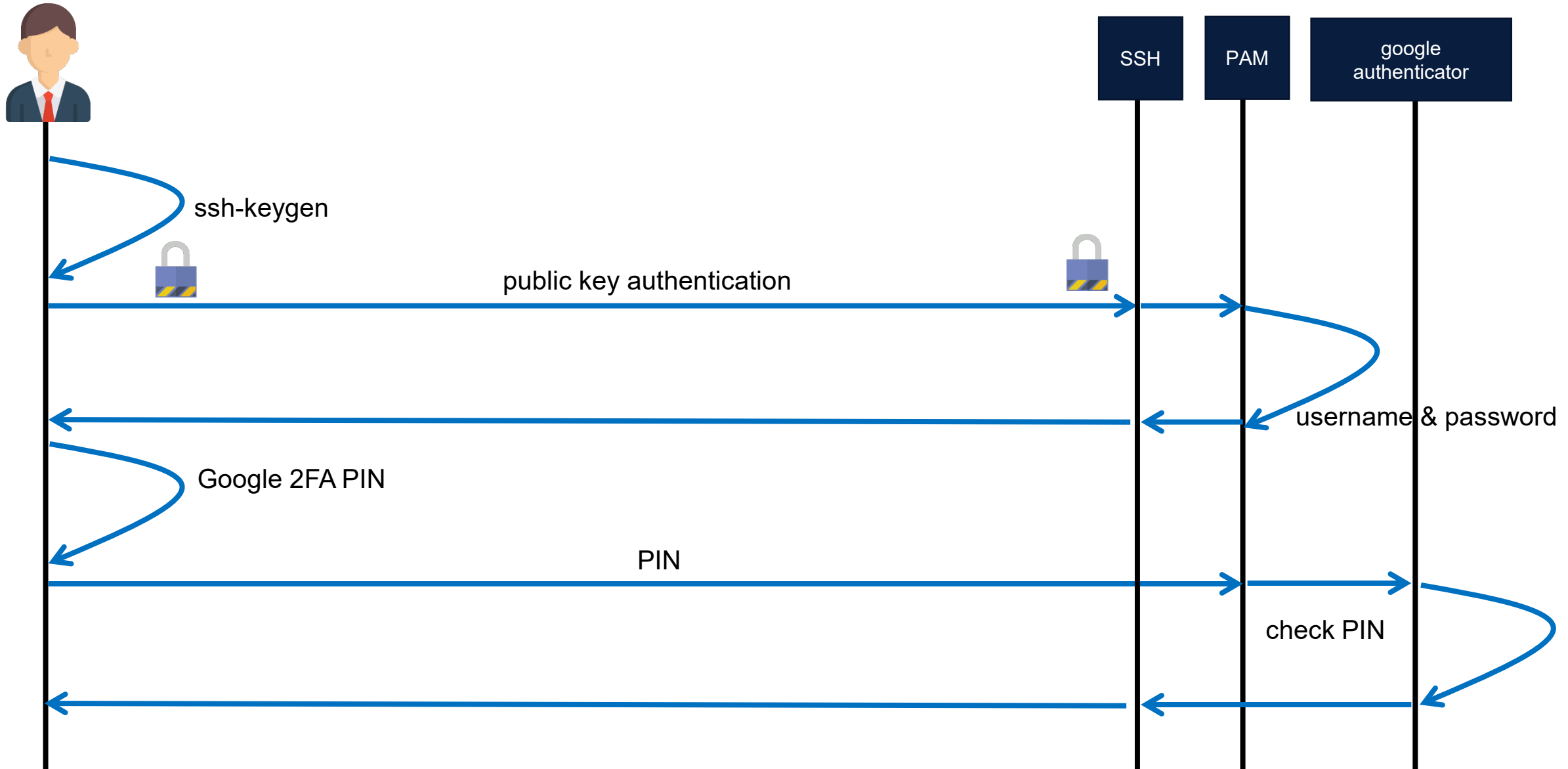
# SSH 2FA (Google Authenticator)



# SSH Username/Password Auth with 2FA using Google Authenticator



# SSH PubKey Auth with 2FA using Google Authenticator



# **Is Google 2FA preventing MitM?**

# Does SSH 2FA prevent MitM?

NO!!!! not at all

Only mutual authentication == public/private key auth is preventing SSH MitM

# Recommendation

# Use SSH Client config in ~/.ssh/config

```
Host *
    AddKeysToAgent yes
    IdentityFile ~/.ssh/id_dsa

Host nessus
    HostName nessus.ost.ch
    User ibuetler

Host gvm
    HostName 10.15.12.33
    Port 2222
    User ibuetler

Host jumphost
    HostName jumphost.ost.ch
    LocalForward 2222 192.168.99.100:22
    LocalForward 7026 80.32.130.139:22
    LocalForward 7027 80.32.140.131:22
    User jumpuser
```

Host *	default, applies to all
HostName	IP or DNS
User	what user ssh client shall use
LocalForward	ssh port forwarding