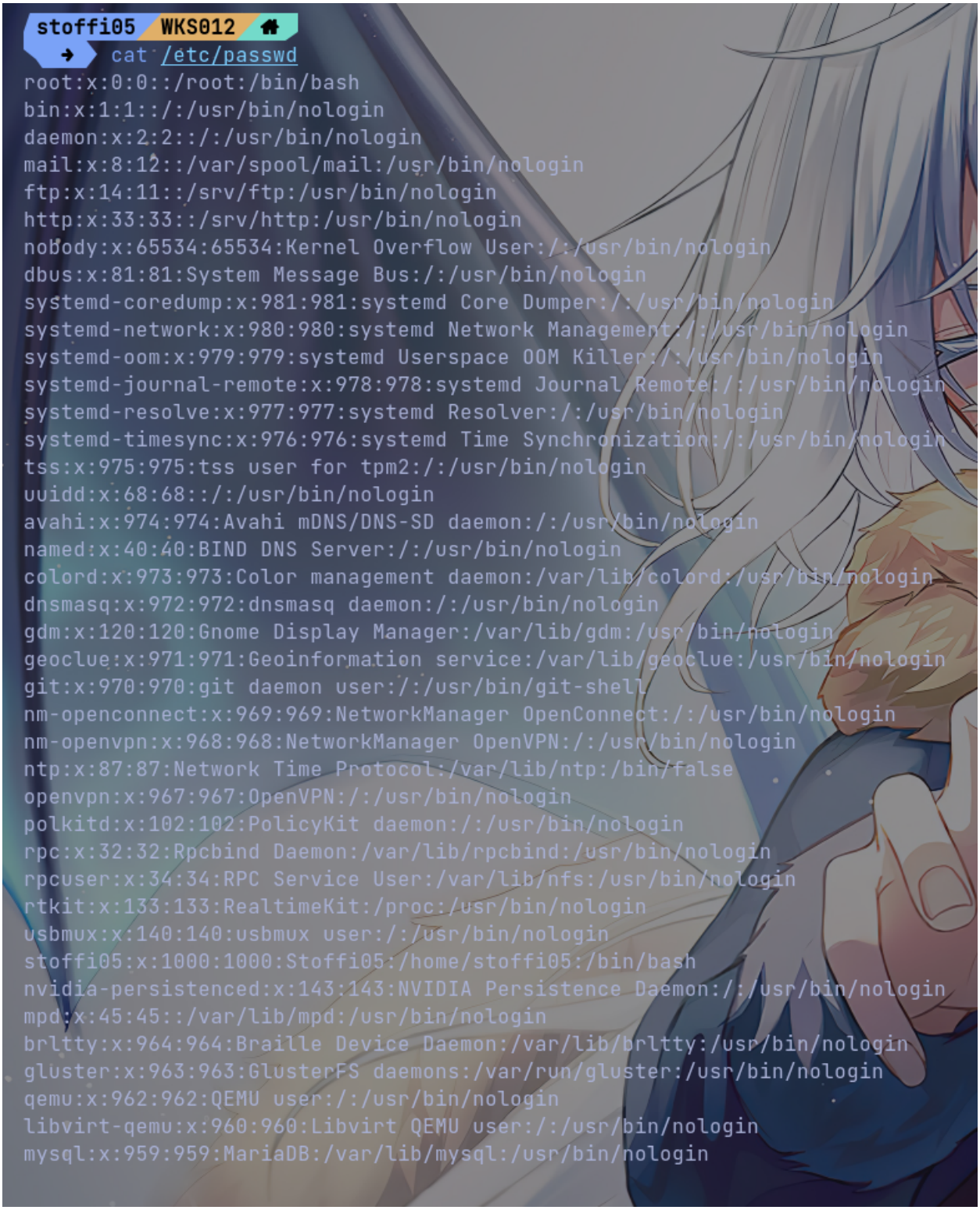
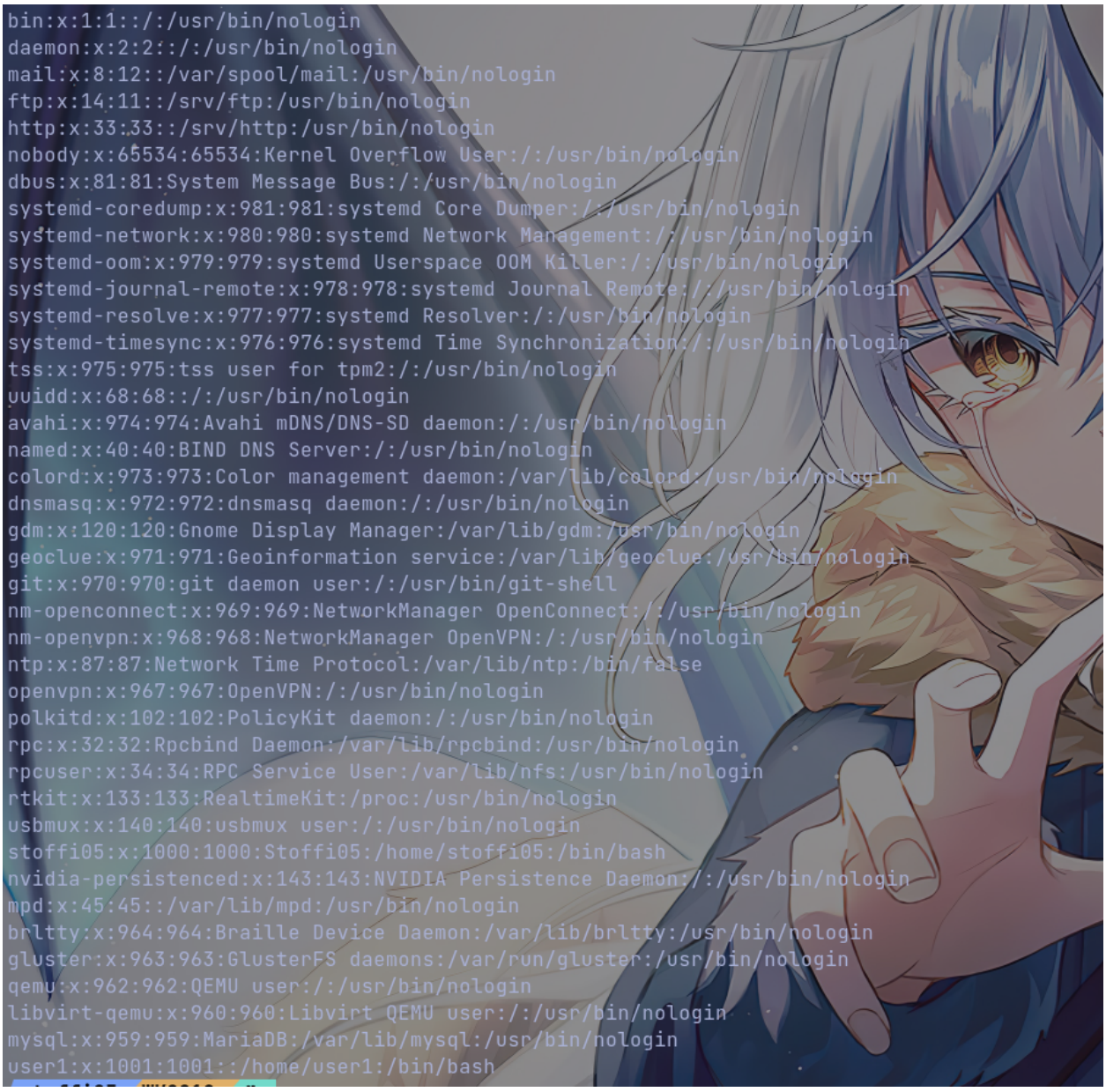
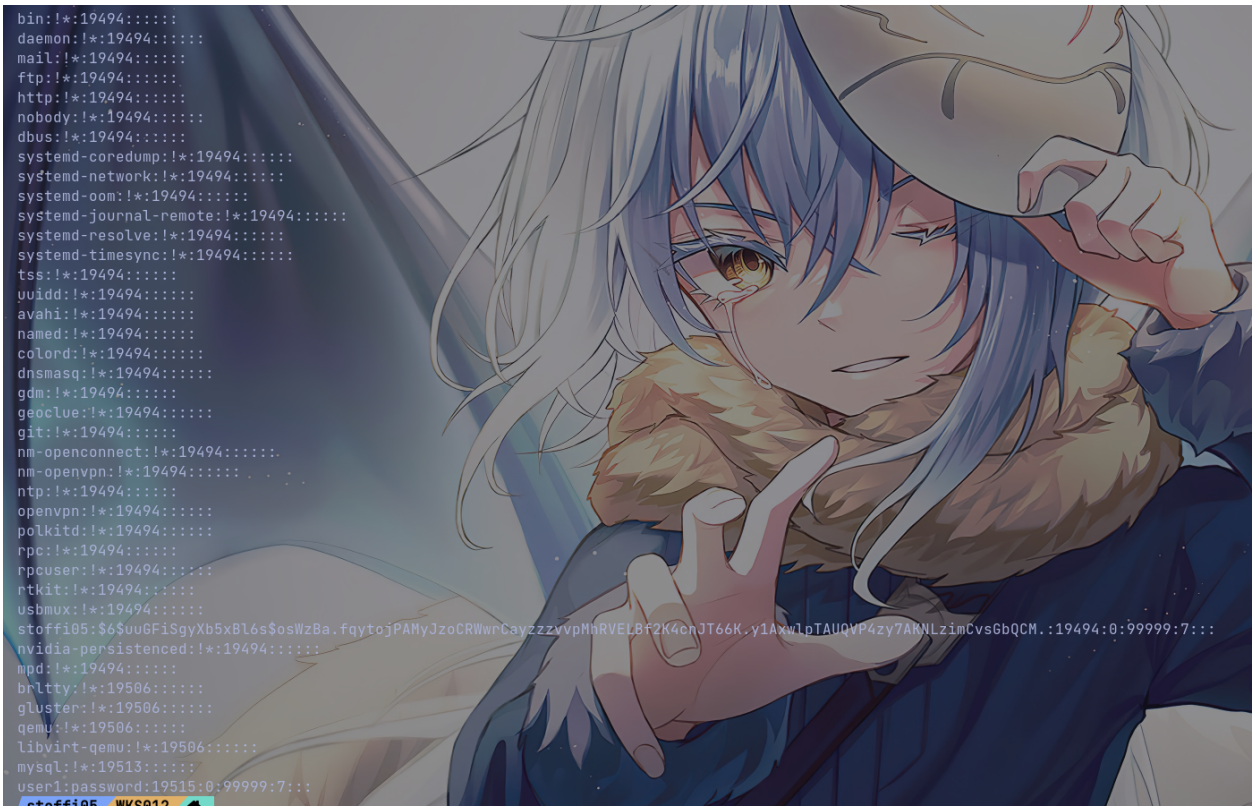
PASSWD

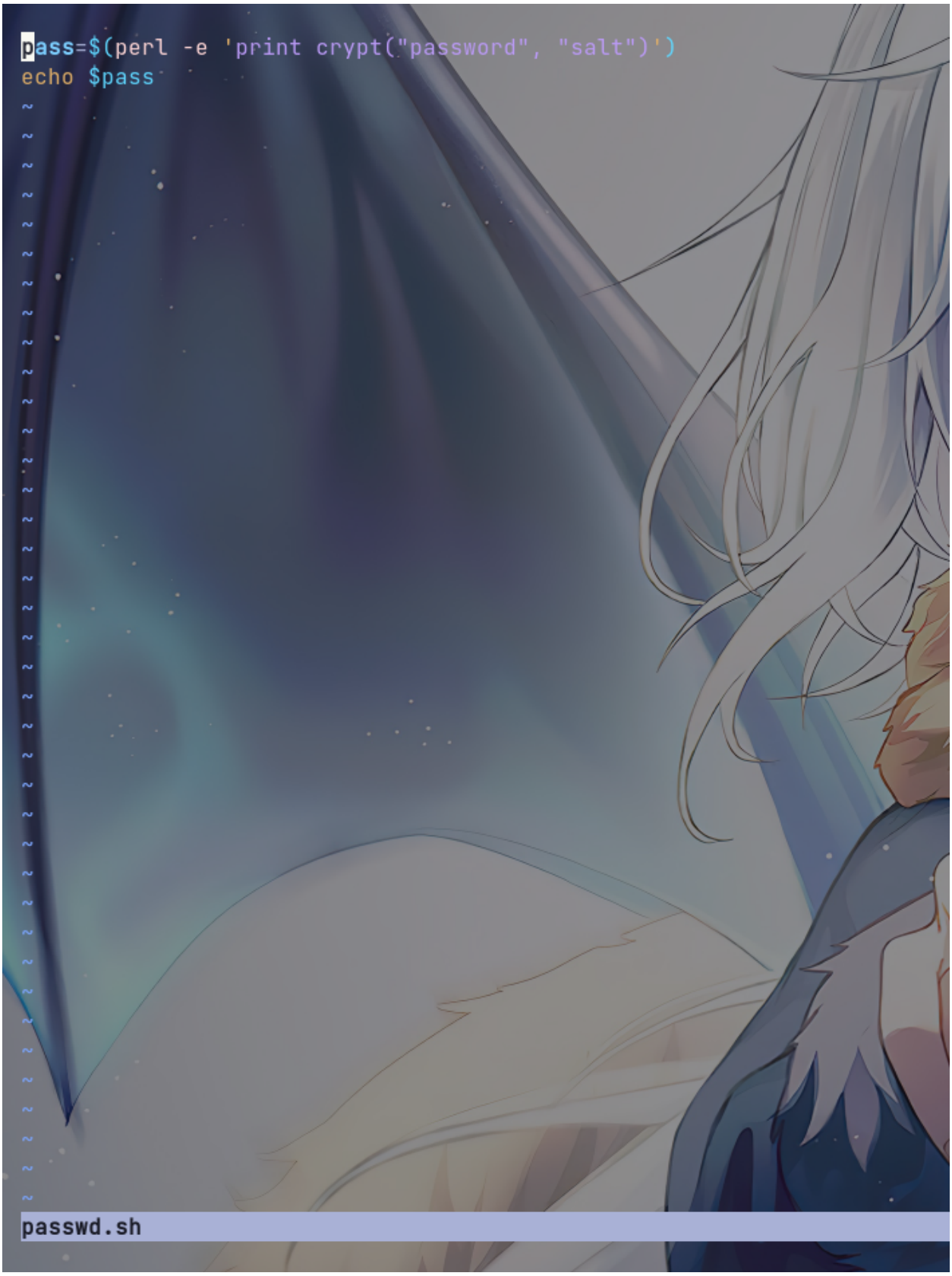
Christof Zlabinger


stoffi05 WKS012
cat /etc/passwd
root:x:0:0::/root:/bin/bash
bin:x:1:1::/:/usr/bin/nologin
daemon:x:2:2::/:/usr/bin/nologin
mail:x:8:12::/var/spool/mail:/usr/bin/nologin
ftp:x:14:11::/srv/ftp:/usr/bin/nologin
http:x:33:33::/srv/http:/usr/bin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/usr/bin/nologin
dbus:x:81:81:System Message Bus:/:/usr/bin/nologin
systemd-coredump:x:981:981:systemd Core Dumper:/:/usr/bin/nologin
systemd-network:x:980:980:systemd Network Management:/:/usr/bin/nologin
systemd-oom:x:979:979:systemd Userspace OOM Killer:/:/usr/bin/nologin
systemd-journal-remote:x:978:978:systemd Journal Remote:/:/usr/bin/nologin
systemd-resolve:x:977:977:systemd Resolver:/:/usr/bin/nologin
systemd-timesync:x:976:976:systemd Time Synchronization:/:/usr/bin/nologin
tss:x:975:975:tss user for tpm2:/:/usr/bin/nologin
uuidd:x:68:68::/:/usr/bin/nologin
avahi:x:974:974:Avahi mDNS/DNS-SD daemon:/:/usr/bin/nologin
named:x:40:40:BIND DNS Server:/:/usr/bin/nologin
colord:x:973:973:Color management daemon:/var/lib/colord:/usr/bin/nologin
dnsmasq:x:972:972:dnsmasq daemon:/:/usr/bin/nologin
gdm:x:120:120:Gnome Display Manager:/var/lib/gdm:/usr/bin/nologin
geoclue:x:971:971:Geoinformation service:/var/lib/geoclue:/usr/bin/nologin
git:x:970:970:git daemon user:/:/usr/bin/git-shell
nm-openconnect:x:969:969:NetworkManager OpenConnect:/:/usr/bin/nologin
nm-openvpn:x:968:968:NetworkManager OpenVPN:/:/usr/bin/nologin
ntp:x:87:87:Network Time Protocol:/var/lib/ntp:/bin/false
openvpn:x:967:967:OpenVPN:/:/usr/bin/nologin
polkitd:x:102:102:PolicyKit daemon:/:/usr/bin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/usr/bin/nologin
rpcuser:x:34:34:RPC Service User:/var/lib/nfs:/usr/bin/nologin
rtkit:x:133:133:RealtimeKit:/proc:/usr/bin/nologin
usbmux:x:140:140:usbmux user:/:/usr/bin/nologin
stoffi05:x:1000:1000:Stoffi05:/home/stoffi05:/bin/bash
nvidia-persistenced:x:143:143:NVIDIA Persistence Daemon:/:/usr/bin/nologin
mpd:x:45:45::/var/lib/mpd:/usr/bin/nologin
brltty:x:964:964:Braille Device Daemon:/var/lib/brltty:/usr/bin/nologin
gluster:x:963:963:GlusterFS daemons:/var/run/gluster:/usr/bin/nologin
qemu:x:962:962:QEMU user:/:/usr/bin/nologin
libvirt-qemu:x:960:960:Libvirt QEMU user:/:/usr/bin/nologin
mysql:x:959:959:MariaDB:/var/lib/mysql:/usr/bin/nologin


bin:x:1:1::/:/usr/bin/nologin
daemon:x:2:2::/:/usr/bin/nologin
mail:x:8:12::/var/spool/mail:/usr/bin/nologin
ftp:x:14:11::/srv/ftp:/usr/bin/nologin
http:x:33:33::/srv/http:/usr/bin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/usr/bin/nologin
dbus:x:81:81:System Message Bus:/:/usr/bin/nologin
systemd-coredump:x:981:981:systemd Core Dumper:/:/usr/bin/nologin
systemd-network:x:980:980:systemd Network Management:/:/usr/bin/nologin
systemd-oom:x:979:979:systemd Userspace OOM Killer:/:/usr/bin/nologin
systemd-journal-remote:x:978:978:systemd Journal Remote:/:/usr/bin/nologin
systemd-resolve:x:977:977:systemd Resolver:/:/usr/bin/nologin
systemd-timesync:x:976:976:systemd Time Synchronization:/:/usr/bin/nologin
tss:x:975:975:tss user for tpm2:/:/usr/bin/nologin
uuidd:x:68:68::/:/usr/bin/nologin
avahi:x:974:974:Avahi mDNS/DNS-SD daemon:/:/usr/bin/nologin
named:x:40:40:BIND DNS Server:/:/usr/bin/nologin
colord:x:973:973:Color management daemon:/var/lib/colord:/usr/bin/nologin
dnsmasq:x:972:972:dnsmasq daemon:/:/usr/bin/nologin
gdm:x:120:120:Gnome Display Manager:/var/lib/gdm:/usr/bin/nologin
geoclue:x:971:971:Geoinformation service:/var/lib/geoclue:/usr/bin/nologin
git:x:970:970:git daemon user:/:/usr/bin/git-shell
nm-openconnect:x:969:969:NetworkManager OpenConnect:/:/usr/bin/nologin
nm-openvpn:x:968:968:NetworkManager OpenVPN:/:/usr/bin/nologin
ntp:x:87:87:Network Time Protocol:/var/lib/ntp:/bin/false
openvpn:x:967:967:OpenVPN:/:/usr/bin/nologin
polkitd:x:102:102:PolicyKit daemon:/:/usr/bin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/usr/bin/nologin
rpcuser:x:34:34:RPC Service User:/var/lib/nfs:/usr/bin/nologin
rtkit:x:133:133:RealtimeKit:/proc:/usr/bin/nologin
usbmux:x:140:140:usbmux user:/:/usr/bin/nologin
stoffi05:x:1000:1000:Stoffi05:/home/stoffi05:/bin/bash
nvidia-persistenced:x:143:143:NVIDIA Persistence Daemon:/:/usr/bin/nologin
mpd:x:45:45::/var/lib/mpd:/usr/bin/nologin
brltty:x:964:964:Braille Device Daemon:/var/lib/brltty:/usr/bin/nologin
gluster:x:963:963:GlusterFS daemons:/var/run/gluster:/usr/bin/nologin
qemu:x:962:962:QEMU user:/:/usr/bin/nologin
libvirt-qemu:x:960:960:Libvirt QEMU user:/:/usr/bin/nologin
mysql:x:959:959:MariaDB:/var/lib/mysql:/usr/bin/nologin
user1:x:1001:1001::/home/user1:/bin/bash

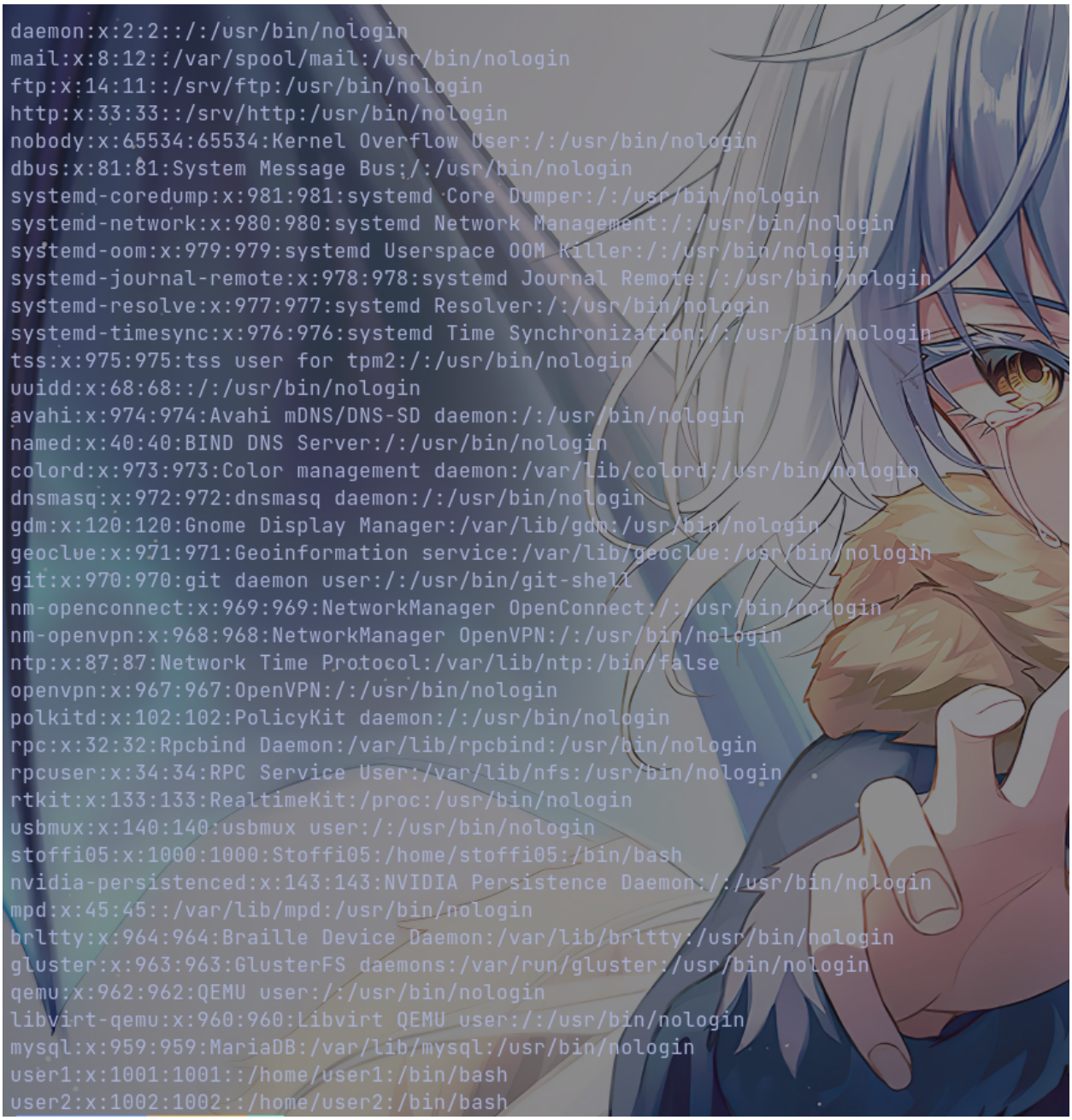


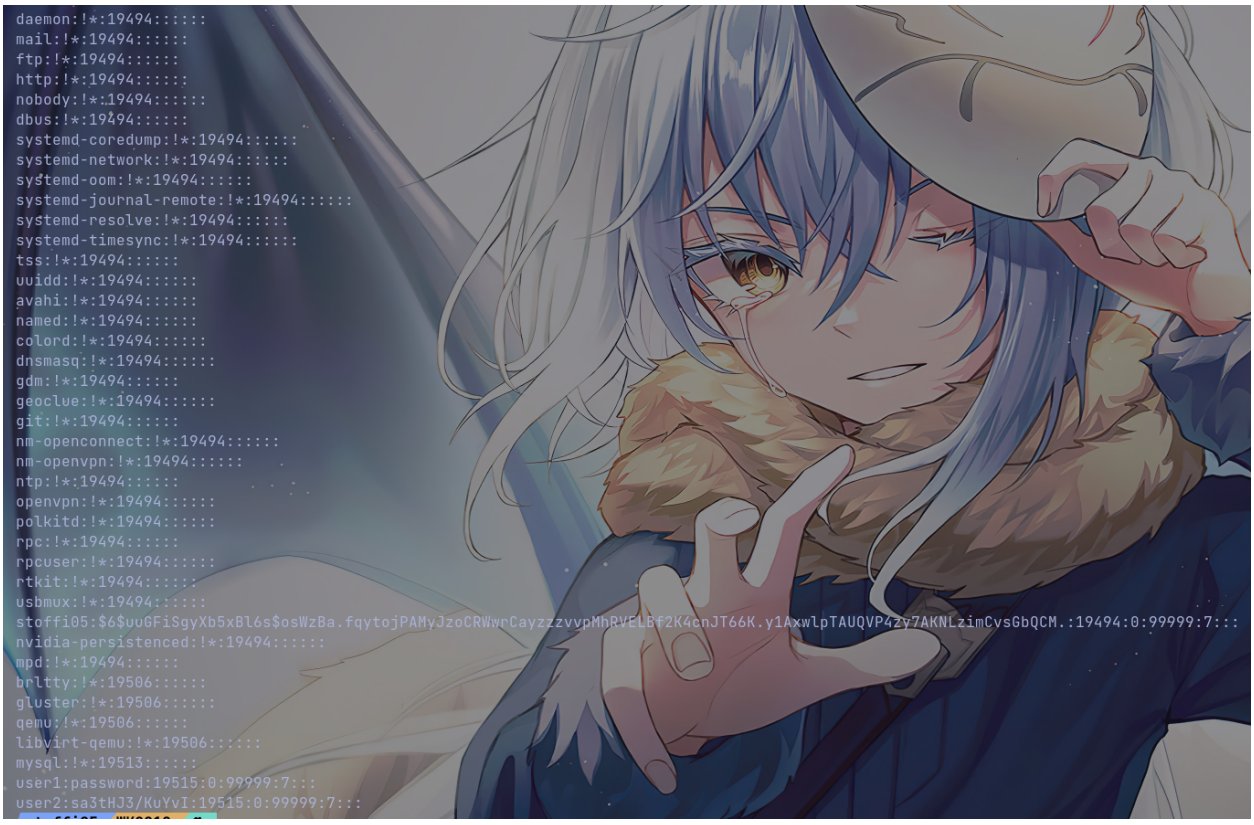

```
➜ perl -e 'print crypt("password","sa")'
sa3tHJ3/KuYvI↵
```

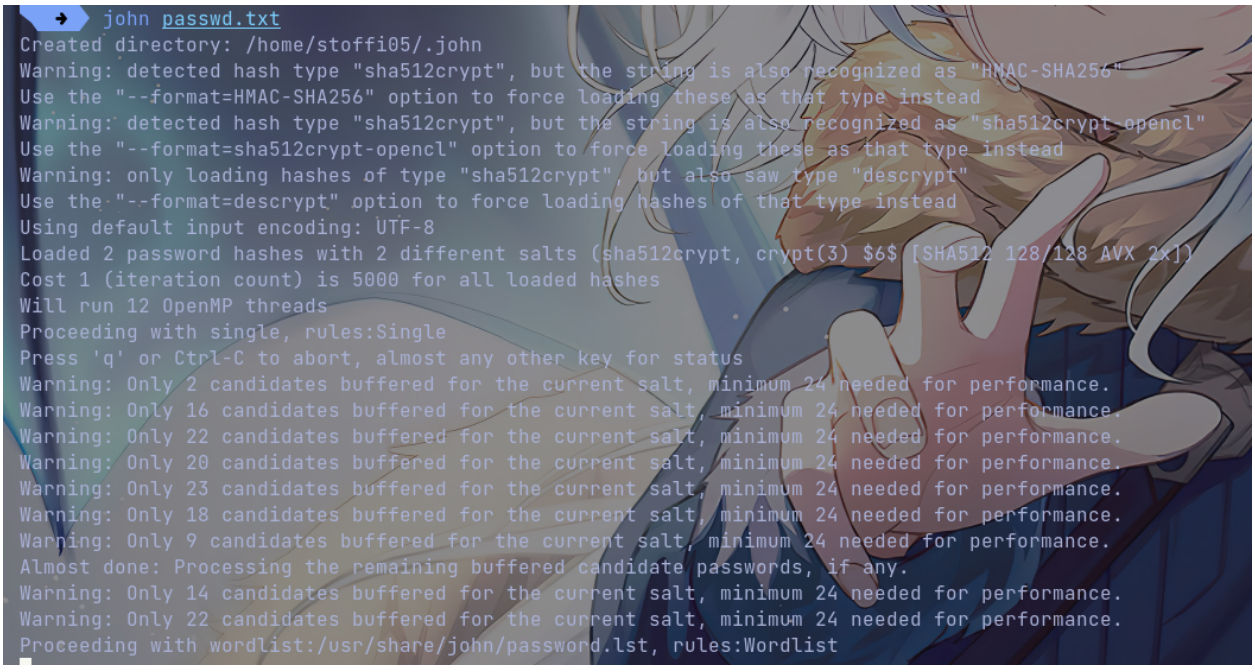

pass=$(perl -e 'print crypt("password", "salt")')
echo $pass
passwd.sh

```
stoffi05 WKS012
➜ sh passwd.sh
sa3tHJ3/KuYvI
```

```
pass=$(perl -e 'print crypt("password", "salt")')
echo $pass
useradd -p $pass user2
```


daemon:x:2:2::/:/usr/bin/nologin
mail:x:8:12::/var/spool/mail:/usr/bin/nologin
ftp:x:14:11::/srv/ftp:/usr/bin/nologin
http:x:33:33::/srv/http:/usr/bin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/usr/bin/nologin
dbus:x:81:81:System Message Bus:/:/usr/bin/nologin
systemd-coredump:x:981:981:systemd Core Dumper:/:/usr/bin/nologin
systemd-network:x:980:980:systemd Network Management:/:/usr/bin/nologin
systemd-oom:x:979:979:systemd Userspace OOM Killer:/:/usr/bin/nologin
systemd-journal-remote:x:978:978:systemd Journal Remote:/:/usr/bin/nologin
systemd-resolve:x:977:977:systemd Resolver:/:/usr/bin/nologin
systemd-timesync:x:976:976:systemd Time Synchronization:/:/usr/bin/nologin
tss:x:975:975:tss user for tpm2:/:/usr/bin/nologin
uuidd:x:68:68::/:/usr/bin/nologin
avahi:x:974:974:Avahi mDNS/DNS-SD daemon:/:/usr/bin/nologin
named:x:40:40:BIND DNS Server:/:/usr/bin/nologin
colord:x:973:973:Color management daemon:/var/lib/colord:/usr/bin/nologin
dnsmasq:x:972:972:dnsmasq daemon:/:/usr/bin/nologin
gdm:x:120:120:Gnome Display Manager:/var/lib/gdm:/usr/bin/nologin
geoclue:x:971:971:Geoinformation service:/var/lib/geoclue:/usr/bin/nologin
git:x:970:970:git daemon user:/:/usr/bin/git-shell
nm-openconnect:x:969:969:NetworkManager OpenConnect:/:/usr/bin/nologin
nm-openvpn:x:968:968:NetworkManager OpenVPN:/:/usr/bin/nologin
ntp:x:87:87:Network Time Protocol:/var/lib/ntp:/bin/false
openvpn:x:967:967:OpenVPN:/:/usr/bin/nologin
polkitd:x:102:102:PolicyKit daemon:/:/usr/bin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/usr/bin/nologin
rpcuser:x:34:34:RPC Service User:/var/lib/nfs:/usr/bin/nologin
rtkit:x:133:133:RealtimeKit:/proc:/usr/bin/nologin
usbmux:x:140:140:usbmux user:/:/usr/bin/nologin
stoffi05:x:1000:1000:Stoffi05:/home/stoffi05:/bin/bash
nvidia-persistenced:x:143:143:NVIDIA Persistence Daemon:/:/usr/bin/nologin
mpd:x:45:45::/var/lib/mpd:/usr/bin/nologin
brltty:x:964:964:Braille Device Daemon:/var/lib/brltty:/usr/bin/nologin
gluster:x:963:963:GlusterFS daemons:/var/run/gluster:/usr/bin/nologin
qemu:x:962:962:QEMU user:/:/usr/bin/nologin
libvirt-qemu:x:960:960:Libvirt QEMU user:/:/usr/bin/nologin
mysql:x:959:959:MariaDB:/var/lib/mysql:/usr/bin/nologin
user1:x:1001:1001::/home/user1:/bin/bash
user2:x:1002:1002::/home/user2:/bin/bash


daemon:!*:19494:::::
mail:!*:19494:::::
ftp:!*:19494:::::
http:!*:19494:::::
nobody:!*:19494:::::
dbus:!*:19494:::::
systemd-coredump:!*:19494:::::
systemd-network:!*:19494:::::
systemd-oom:!*:19494:::::
systemd-journal-remote:!*:19494:::::
systemd-resolve:!*:19494:::::
systemd-timesync:!*:19494:::::
tss:!*:19494:::::
uuidd:!*:19494:::::
avahi:!*:19494:::::
named:!*:19494:::::
colord:!*:19494:::::
dnsmasq:!*:19494:::::
gdm:!*:19494:::::
geoclue:!*:19494:::::
git:!*:19494:::::
nm-openconnect:!*:19494:::::
nm-openvpn:!*:19494:::::
ntp:!*:19494:::::
openvpn:!*:19494:::::
polkitd:!*:19494:::::
rpc:!*:19494:::::
rpcuser:!*:19494:::::
rtkit:!*:19494:::::
usbmux:!*:19494:::::
stoffi05:6uuGFiSgyXb5xBl6s$osWzBa.fqytojPAMyJzoCRWwrCayzzzvvpMhRVELBf2K4cnJT66K.y1AxwlpTAUQVP4zy7AKNLzimCvsGbQCM.:19494:0:99999:7:::
nvidia-persistenced:!*:19494:::::
mpd:!*:19494:::::
brltty:!*:19506:::::
gluster:!*:19506:::::
qemu:!*:19506:::::
libvirt-qemu:!*:19506:::::
mysql:!*:19513:::::
user1:password:19515:0:99999:7:::
user2:sa3tHJ3/KuYvI:19515:0:99999:7:::


john passwd.txt
Created directory: /home/stoffi05/.john
Warning: detected hash type "sha512crypt", but the string is also recognized as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type instead
Warning: detected hash type "sha512crypt", but the string is also recognized as "sha512crypt-opencl"
Use the "--format=sha512crypt-opencl" option to force loading these as that type instead
Warning: only loading hashes of type "sha512crypt", but also saw type "descrypt"
Use the "--format=descrypt" option to force loading hashes of that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) 6 [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 12 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 16 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 22 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 20 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 23 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 18 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 9 candidates buffered for the current salt, minimum 24 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 14 candidates buffered for the current salt, minimum 24 needed for performance.
Warning: Only 22 candidates buffered for the current salt, minimum 24 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist