

PASSWD

Christof Zlabinger

```
cat /etc/passwd
root:x:0:0::/root:/usr/bin/zsh
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
uidd: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
dnsmasq:x:973:973:dnsmasq daemon::/usr/bin/nologin
git:x:972:972:git daemon user::/usr/bin/git-shell
nm-openconnect:x:971:971:NetworkManager OpenConnect::/usr/bin/nologin
nm-openvpn:x:970:970:NetworkManager OpenVPN::/usr/bin/nologin
ntp:x:87:87:Network Time Protocol:/var/lib/ntp:/bin/false
openvpn:x:969:969: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
sddm:x:968:968:Simple Desktop Display Manager:/var/lib/sddm:/usr/bin/nologin
usbmux:x:140:140:usbmux user::/usr/bin/nologin
stoffi05:x:1000:1000:stoffi05:/home/stoffi05:/usr/bin/zsh
nvidia-persistenced:x:143:143:NVIDIA Persistence Daemon::/usr/bin/nologin
geoclue:x:966:966:Geoinformation service:/var/lib/geoclue:/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
```

```
cat /etc/passwd
root:x:0:0::/root:/usr/bin/zsh
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
uidd: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
dnsmasq:x:973:973:dnsmasq daemon:/:usr/bin/nologin
git:x:972:972:git daemon user:/:usr/bin/git-shell
nm-openconnect:x:971:971:NetworkManager OpenConnect:/:usr/bin/nologin
nm-openvpn:x:970:970:NetworkManager OpenVPN:/:usr/bin/nologin
ntp:x:87:87:Network Time Protocol:/var/lib/ntp:/bin/false
openvpn:x:969:969: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
sddm:x:968:968:Simple Desktop Display Manager:/var/lib/sddm:/usr/bin/nologin
usbmux:x:140:140:usbmux user:/:usr/bin/nologin
stoffi05:x:1000:1000:stoffi05:/home/stoffi05:/usr/bin/zsh
nvidia-persistenced:x:143:143:NVIDIA Persistence Daemon:/:usr/bin/nologin
geoclue:x:966:966:Geoinformation service:/var/lib/geoclue:/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
user1:x:1001:1001:/:home/user1:/bin/bash

```

```

~ sudo cat /etc/shadow
root:$6$P68wLC.scJIXap0y$ZPF8nNwBMh19SUxdpbh34Tn1MmWh3qfgX7bCAo1nPg9Vuh8Wzcr9xMDBxWOLjN/IdzGhhBYEGPalFdtNeDn...19421:0:0:0:
bin:!*:19421:0:0:0:
daemon:!*:19421:0:0:0:
mail:!*:19421:0:0:0:
ftp:!*:19421:0:0:0:
http:!*:19421:0:0:0:
nobody:!*:19421:0:0:0:
dbus:!*:19421:0:0:0:
systemd-coredump:!*:19421:0:0:0:
systemd-network:!*:19421:0:0:0:
systemd-oom:!*:19421:0:0:0:
systemd-journal-remote:!*:19421:0:0:0:
systemd-resolve:!*:19421:0:0:0:
systemd-timesync:!*:19421:0:0:0:
tss:!*:19421:0:0:0:
uidd:!*:19421:0:0:0:
avahi:!*:19421:0:0:0:
named:!*:19421:0:0:0:
dnsmasq:!*:19421:0:0:0:
git:!*:19421:0:0:0:
nm-openconnect:!*:19421:0:0:0:
nm-openvpn:!*:19421:0:0:0:
ntp:!*:19421:0:0:0:
openvpn:!*:19421:0:0:0:
polkitd:!*:19421:0:0:0:
rpc:!*:19421:0:0:0:
rpcuser:!*:19421:0:0:0:
rtkit:!*:19421:0:0:0:
sddm:!*:19421:0:0:0:
usbmux:!*:19421:0:0:0:
stoffi05:$6$q0cFR7tzS.FVDKPk$ht6EwDF3mKzG7XvRUUX036L3P.ukYiyHMyZZHp1JiEW9ZkW6ID6RPwKJnqM1FBFS.SB0yFA4pKF/FkNNw/wX1:19421:0:99999:7::
nvidia-persistenced:!*:19421:0:0:0:
geoclue:!*:19422:0:0:0:
brltty:!*:19424:0:0:0:
gluster:!*:19424:0:0:0:
qemu:!*:19424:0:0:0:
libvirt-qemu:!*:19425:0:0:0:
user1:test:19426:0:99999:7::

```

```
~ sudo cat /etc/shadow
root:$6$Pg8w1C.scJIxap0y$ZPF8nNwBMh19SUxdpbh34Tn1MmWh3qfgX7bCAo1nPg9Vuh8wVzcr9xMDBxWOLjN/IdzGhhBYEGPa1FdtNeDn...:19421:::::::
bin:!:19421:::::::
daemon:!:19421:::::::
mail:!:19421:::::::
ftp:!:19421:::::::
http:!:19421:::::::
nobody:!:19421:::::::
dbus:!:19421:::::::
systemd-coredump:!:19421:::::::
systemd-network:!:19421:::::::
systemd-oom:!:19421:::::::
systemd-journal-remote:!:19421:::::::
systemd-resolve:!:19421:::::::
systemd-timesync:!:19421:::::::
tss:!:19421:::::::
uuid:!:19421:::::::
avahi:!:19421:::::::
named:!:19421:::::::
dnsmasq:!:19421:::::::
git:!:19421:::::::
nm-openconnect:!:19421:::::::
nm-openvpn:!:19421:::::::
ntp:!:19421:::::::
openvpn:!:19421:::::::
polkitd:!:19421:::::::
rpc:!:19421:::::::
rpcuser:!:19421:::::::
rtkit:!:19421:::::::
sddm:!:19421:::::::
usbmux:!:19421:::::::
stoeffi05:$6$q0cFR7tzS.FVDKPk$ht6EwDF3mKzG7XvRUUX036lL3P.ukYiyHMyZZHp1JiEW9ZkW6ID6RPwKJnqM1FBFS.SB0yFA4pKF/FkNNw/wX1:19421:0:99999:7:::
nvidia-persistenced:!:19421:::::::
geoclue:!:19422:::::::
brltty:!:19424:::::::
gluster:!:19424:::::::
qemu:!:19424:::::::
libvirt-qemu:!:19425:::::::
user1:test:19426:0:99999:7:::
```

```
pass=$(perl -e 'print crypt("password", "sa*")')
2 echo $pas
```

```
1 pass=$(perl -e 'print crypt("password", "sa")')
2 echo $pas
```

NORMAL myAddUser.sh

stoeffi05 Bot

```
root:x:0:0::/root:/usr/bin/zsh
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
uidd: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
dnsmasq:x:973:973:dnsmasq daemon:/usr/bin/nologin
git:x:972:972:git daemon user:/usr/bin/git-shell
nm-openconnect:x:971:971:NetworkManager OpenConnect:/usr/bin/nologin
nm-openvpn:x:970:970:NetworkManager OpenVPN:/usr/bin/nologin
ntp:x:87:87:Network Time Protocol:/var/lib/ntp:/bin/false
openvpn:x:969:969: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
sddm:x:968:968:Simple Desktop Display Manager:/var/lib/sddm:/usr/bin/nologin
usbmux:x:140:140:usbmux user:/usr/bin/nologin
stoffi05:x:1000:1000:stoffi05:/home/stoffi05:/usr/bin/zsh
nvidia-persistenced:x:143:143:NVIDIA Persistence Daemon:/usr/bin/nologin
geoclue:x:966:966:Geoinformation service:/var/lib/geoclue:/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
user1:x:1001:1001::/home/user1:/bin/bash
user2:x:1002:1002::/home/user2:/bin/bash
```



```

root:$6$P68w1C.scJIXap0y$ZPF8nNwBMh19SUXdpbh34Tn1MmWh3qfgX7bCAo1nPg9Vuh8wVzcr9xMDBxWOLjN/IdzGhhBYEGPa1FdtNeDn...:19421:19421:19421:
bin:!:19421:19421:19421:
daemon:!:19421:19421:19421:
mail:!:19421:19421:19421:
ftp:!:19421:19421:19421:
http:!:19421:19421:19421:
nobody:!:19421:19421:19421:
dbus:!:19421:19421:19421:
systemd-coredump:!:19421:19421:19421:
systemd-network:!:19421:19421:19421:
systemd-oom:!:19421:19421:19421:
systemd-journal-remote:!:19421:19421:19421:
systemd-resolve:!:19421:19421:19421:
systemd-timesync:!:19421:19421:19421:
tss:!:19421:19421:19421:
uuuid:!:19421:19421:19421:
avahi:!:19421:19421:19421:
named:!:19421:19421:19421:
dnsmasq:!:19421:19421:19421:
git:!:19421:19421:19421:
nm-openconnect:!:19421:19421:19421:
nm-openvpn:!:19421:19421:19421:
ntp:!:19421:19421:19421:
openvpn:!:19421:19421:19421:
polkitd:!:19421:19421:19421:
rpc:!:19421:19421:19421:
rpcuser:!:19421:19421:19421:
rtkit:!:19421:19421:19421:
sddm:!:19421:19421:19421:
usbmux:!:19421:19421:19421:
stoffi05:$6$q0cFR7tzS.FVDKPk$ht6EwDF3mKzG7XvRUUX0361L3P.ukYiyHMyZZHp1JiEW9Zk6ID6RPwKJnqM1FBFS.SB0yFA4pKF/FkNNw/wX1:19421:0:99999:7::
nvidia-persistenced:!:19421:19421:19421:
geoclue:!:19422:19422:19422:
brlty:!:19424:19424:19424:
gluster:!:19424:19424:19424:
qemu:!:19424:19424:19424:
libvirt-qemu:!:19425:19425:19425:
user1:test:19426:0:99999:7::
user2:sa3tHJ3/KuYvI:19426:0:99999:7::

```

```

~ /usr/bin/john mypassword.txt
Created directory: /home/stoffi05/.john
Warning: detected hash type "sha512crypt", but the string is also recognized as "sha512crypt-openc1"
Use the "--format=sha512crypt-openc1" 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
Proceeding with incremental:ASCII
0g 0:00:05:56 3/3 0g/s 1658p/s 3308c/s 3308C/s abboyy..arack7
0g 0:00:05:57 3/3 0g/s 1658p/s 3309c/s 3309C/s admj02..bonare
0g 0:00:08:02 3/3 0g/s 1656p/s 3305c/s 3305C/s 139941..samukk
0g 0:00:08:03 3/3 0g/s 1657p/s 3306c/s 3306C/s shoero..seliul
0q 0:00:08:26 3/3 0q/s 1662p/s 3318c/s 3318C/s 17/dy..myhjd

```