# PEAS Report

# Basic information

```
OS: Darwin macs-MacBook-Pro.local 22.5.0 Darwin Kernel Version 22.5.0: Thu Jun 8
22:22:22 PDT 2023; root:xnu-8796.121.3~7/RELEASE_X86_64 x86_64
User & Groups: uid=0(root) gid=0(wheel) groups=0(wheel),1(daemon),2(kmem),3(sys),4(tt
y),5(operator),8(procview),9(procmod),12(everyone),20(staff),29(certusers),61(localac
counts),80(admin),701(com.apple.sharepoint.group.1),33(_appstore),98(_lpadmin),100(_l
poperator),204(_developer),250(_analyticsusers),395(com.apple.access_ftp),398(com.app
le.access_screensharing),399(com.apple.access_ssh),400(com.apple.access_remote_ae)
Hostname: macs-MacBook-Pro.local
Writable folder: /Applications
[+] /sbin/ping is available for network discovery (macpeas can discover hosts, learn
more with -h)
[+] /bin/bash is available for network discovery, port scanning and port forwarding
(macpeas can discover hosts, scan ports, and forward ports. Learn more with -h)
[+] /usr/bin/nc is available for network discovery & port scanning (macpeas can
discover hosts and scan ports, learn more with -h)
Caching directories DONE
```

# System Information

## Operative system

*https://book.hacktricks.xyz/linux-hardening/privilege-escalation#kernel-exploits*

```
Darwin macs-MacBook-Pro.local 22.5.0 Darwin Kernel Version 22.5.0: Thu Jun 8
22:22:22 PDT 2023; root:xnu-8796.121.3~7/RELEASE_X86_64 x86_64
lsb_release Not Found
Software:
System Software Overview:
System Version: macOS 13.4.1 (22F82)
Kernel Version: Darwin 22.5.0
Boot Volume: Untitled
Boot Mode: Normal
Computer Name: macs MacBook Pro
User Name: System Administrator (root)
Secure Virtual Memory: Enabled
System Integrity Protection: Enabled
Time since boot: 2 days, 13 hours, 48 minutes
```

## Date & uptime

```
Mon Jul 31 09:04:23 IST 2023
9:04 up 2 days, 13:48, 2 users, load averages: 3.71 3.63 2.31
```

## Any sd*/disk* disk in /dev? (limit 20)

```
disk0
disk0s1
disk0s2
disk1
disk1s1
disk1s2
disk1s3
disk1s4
disk1s4s1
disk1s5
disk1s6
disk2
disk2s1
disk2s2
sdt
```

### Mounted SMB Shares

```
================================================================================
================
SHARE ATTRIBUTE TYPE VALUE
================================================================================
================
--------------------------------------------------------------------------------
---------------
```

# Container

### Container details

```
Is this a container? ........... No
Any running containers? ........ No
```

# Cloud

```
Google Cloud Platform? ............... No
AWS ECS? ............................. No
AWS EC2? ............................. No
AWS EC2 Beanstalk? ................... No
AWS Lambda? .......................... No
AWS Codebuild? ....................... No
DO Droplet? .......................... No
IBM Cloud VM? ........................ No
Azure VM? ............................ No
Azure APP? ........................... No
```

# Network Information

### Hostname, hosts and DNS

```
127.0.0.1 localhost
255.255.255.255 broadcasthost
::1 localhost
dnsdomainname Not Found
```

### Interfaces

```
##
# Networks Database
##
loopback 127 loopback-net
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
```

```
inet 127.0.0.1 netmask 0xff000000
inet6 ::1 prefixlen 128
inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en5: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
ether ac:de:48:00:11:22
inet6 fe80::aede:48ff:fe00:1122%en5 prefixlen 64 scopeid 0x4
nd6 options=201<PERFORMNUD,DAD>
media: autoselect (100baseTX <full-duplex>)
status: active
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
options=460<TSO4,TSO6,CHANNEL_IO>
ether 82:99:21:a5:60:01
media: autoselect <full-duplex>
status: inactive
en3: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
options=460<TSO4,TSO6,CHANNEL_IO>
ether 82:99:21:a5:60:05
media: autoselect <full-duplex>
status: inactive
en4: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
options=460<TSO4,TSO6,CHANNEL_IO>
ether 82:99:21:a5:60:04
media: autoselect <full-duplex>
status: inactive
en2: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
options=460<TSO4,TSO6,CHANNEL_IO>
ether 82:99:21:a5:60:00
media: autoselect <full-duplex>
status: inactive
bridge0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=63<RXCSUM,TXCSUM,TSO4,TSO6>
ether 82:99:21:a5:60:01
Configuration:
id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
ipfilter disabled flags 0x0
member: en1 flags=3<LEARNING,DISCOVER>
ifmaxaddr 0 port 5 priority 0 path cost 0
member: en2 flags=3<LEARNING,DISCOVER>
ifmaxaddr 0 port 8 priority 0 path cost 0
member: en3 flags=3<LEARNING,DISCOVER>
ifmaxaddr 0 port 6 priority 0 path cost 0
member: en4 flags=3<LEARNING,DISCOVER>
ifmaxaddr 0 port 7 priority 0 path cost 0
nd6 options=201<PERFORMNUD,DAD>
media: <unknown type>
status: inactive
ap1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> mtu 1500
options=400<CHANNEL_IO>
ether a6:83:e7:af:8d:19
media: autoselect
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=6463<RXCSUM,TXCSUM,TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
ether a4:83:e7:af:8d:19
inet6 fe80::1c61:b842:ff8f:5feb%en0 prefixlen 64 secured scopeid 0xb
inet 169.254.153.73 netmask 0xffff0000 broadcast 169.254.255.255
nd6 options=201<PERFORMNUD,DAD>
media: autoselect (<unknown type>)
status: inactive
awdl0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=6463<RXCSUM,TXCSUM,TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
ether 7a:5e:49:e7:85:75
inet6 fe80::785e:49ff:fee7:8575%awdl0 prefixlen 64 scopeid 0xc
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: active
llw0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=400<CHANNEL_IO>
ether 7a:5e:49:e7:85:75
inet6 fe80::785e:49ff:fee7:8575%llw0 prefixlen 64 scopeid 0xd
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: inactive
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
```

```
inet6 fe80::8179:c93d:4c8c:8f52%utun0 prefixlen 64 scopeid 0xe
nd6 options=201<PERFORMNUD,DAD>
utun1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
inet6 fe80::c9dc:5b5a:497d:8baa%utun1 prefixlen 64 scopeid 0xf
nd6 options=201<PERFORMNUD,DAD>
utun2: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1000
inet6 fe80::ce81:b1c:bd2c:69e%utun2 prefixlen 64 scopeid 0x10
nd6 options=201<PERFORMNUD,DAD>
```

### Firewall status

```
Firewall:
Firewall Settings:
Mode: Allow all incoming connections
Firewall Logging: Yes
Stealth Mode: No
```

### Active Ports

*https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports*

```
tcp6 0 0 fe80::aede:48ff:.49164 *.* LISTEN 131072 131072 84 0 00180 00000006
0000000000000137 00000000 00000800 1 0 000001
tcp6 0 0 fe80::aede:48ff:.49163 *.* LISTEN 131072 131072 84 0 00180 00000006
0000000000000136 00000000 00000800 1 0 000001
tcp6 0 0 fe80::aede:48ff:.49162 *.* LISTEN 131072 131072 84 0 00180 00000006
0000000000000135 00000000 00000800 1 0 000001
tcp6 0 0 fe80::aede:48ff:.49161 *.* LISTEN 131072 131072 84 0 00180 00000006
0000000000000134 00000000 00000800 1 0 000001
tcp6 0 0 fe80::aede:48ff:.49160 *.* LISTEN 131072 131072 84 0 00180 00000006
0000000000000133 00000000 00000800 1 0 000001
tcp6 0 0 fe80::aede:48ff:.49159 *.* LISTEN 131072 131072 84 0 00180 00000006
0000000000000132 00000000 00000800 1 0 000001
tcp6 0 0 fe80::aede:48ff:.49158 *.* LISTEN 131072 131072 84 0 00180 00000006
0000000000000131 00000000 00000800 1 0 000001
tcp6 0 0 fe80::aede:48ff:.49157 *.* LISTEN 131072 131072 84 0 00180 00000006
0000000000000130 00000000 00000800 1 0 000001
tcp6 0 0 fe80::aede:48ff:.49156 *.* LISTEN 131072 131072 84 0 00180 00000006
000000000000012f 00000000 00000800 1 0 000001
tcp6 0 0 fe80::aede:48ff:.49155 *.* LISTEN 131072 131072 84 0 00180 00000006
000000000000012e 00000000 00000800 1 0 000001
tcp6 0 0 fe80::aede:48ff:.49154 *.* LISTEN 131072 131072 84 0 00180 00000006
000000000000012d 00000000 00000800 1 0 000001
eaa38b2f7dc65b23 stream 0 0 eaa38b211d151133 0 0 0 8192 8192 1 0
/private/tmp/com.apple.launchd.alq0HjhOwR/Listeners
```

### Can I sniff with tcpdump?

```
No
```

# Users Information

## Keychains

*https://book.hacktricks.xyz/macos/macos-security-and-privilege-escalation#chainbreaker*

```
"/Users/mac/Library/Keychains/login.keychain-db"
"/Library/Keychains/System.keychain"
```

## Do I have PGP keys?

```
gpg Not Found
netpgpkeys Not Found
netpgp Not Found
```

## Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d

*https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid*

```
/etc/sudoers:Defaults env_reset
/etc/sudoers:Defaults env_keep += "BLOCKSIZE"
/etc/sudoers:Defaults env_keep += "COLORFGBG COLORTERM"
/etc/sudoers:Defaults env_keep += "__CF_USER_TEXT_ENCODING"
/etc/sudoers:Defaults env_keep += "CHARSET LANG LANGUAGE LC_ALL LC_COLLATE
LC_CTYPE"
/etc/sudoers:Defaults env_keep += "LC_MESSAGES LC_MONETARY LC_NUMERIC LC_TIME"
/etc/sudoers:Defaults env_keep += "LINES COLUMNS"
/etc/sudoers:Defaults env_keep += "LSCOLORS"
/etc/sudoers:Defaults env_keep += "SSH_AUTH_SOCK"
/etc/sudoers:Defaults env_keep += "TZ"
/etc/sudoers:Defaults env_keep += "DISPLAY XAUTHORIZATION XAUTHORITY"
/etc/sudoers:Defaults env_keep += "EDITOR VISUAL"
/etc/sudoers:Defaults env_keep += "HOME MAIL"
/etc/sudoers:Defaults lecture_file = "/etc/sudo_lecture"
/etc/sudoers:root ALL = (ALL) ALL
/etc/sudoers:%admin ALL = (ALL) ALL
```

## Users with console

```
NFSHomeDirectory: /var/setup
Password: *
RealName:
Setup User
RecordName: _mbsetupuser
UserShell: /bin/bash
NFSHomeDirectory: /Users/mac
Password: ********
RealName: mac
RecordName: mac
UserShell: /bin/bash
NFSHomeDirectory: /var/root /private/var/root
Password: *
RealName:
System Administrator
RecordName:
root
BUILTIN\Local System
UserShell: /bin/sh
```

## All users & groups

```
uid=0(root) gid=0(wheel) groups=0(wheel),1(daemon),2(kmem),3(sys),4(tty),5(operato
r),8(procview),9(procmod),12(everyone),20(staff),29(certusers),61(localaccounts),8
0(admin),701(com.apple.sharepoint.group.1),33(_appstore),98(_lpadmin),100(_lpopera
tor),204(_developer),250(_analyticsusers),395(com.apple.access_ftp),398(com.apple.
access_screensharing),399(com.apple.access_ssh),400(com.apple.access_remote_ae)
uid=1(daemon) gid=1(daemon) groups=1(daemon),12(everyone),61(localaccounts),701(co
```

```
m.apple.sharepoint.group.1),100(_lpoperator)
uid=13(_taskgated) gid=13(_taskgated) groups=13(_taskgated),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=200(_softwareupdate) gid=200(_softwareupdate) groups=200(_softwareupdate),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=202(_coreaudiod) gid=202(_coreaudiod) groups=202(_coreaudiod),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=203(_screensaver) gid=203(_screensaver) groups=203(_screensaver),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=205(_locationd) gid=205(_locationd) groups=205(_locationd),12(everyone),61(localaccounts),207(_detachedsig),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=208(_trustevaluationagent) gid=208(_trustevaluationagent) groups=208(_trustevaluationagent),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=210(_timezone) gid=210(_timezone) groups=210(_timezone),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=211(_lda) gid=211(_lda) groups=211(_lda),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=212(_cvmsroot) gid=212(_cvms) groups=212(_cvms),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=213(_usbmuxd) gid=213(_usbmuxd) groups=213(_usbmuxd),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=214(_dovecot) gid=6(mail) groups=6(mail),12(everyone),29(certusers),61(localaccounts),701(com.apple.sharepoint.group.1),30(_keytabusers),100(_lpoperator)
uid=215(_dpaudio) gid=215 groups=215,12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=216(_postgres) gid=216(_postgres) groups=216(_postgres),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=217(_krbtgt) gid=4294967294(nobody) groups=4294967294(nobody),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=218(_kadmin_admin) gid=4294967294(nobody) groups=4294967294(nobody),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=219(_kadmin_changepw) gid=4294967294(nobody) groups=4294967294(nobody),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=220(_devicemgr) gid=220(_devicemgr) groups=220(_devicemgr),12(everyone),61(localaccounts),70(_www),94(_teamsserver),216(_postgres),221(_webauthserver),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=221(_webauthserver) gid=221(_webauthserver) groups=221(_webauthserver),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=222(_netbios) gid=222(_netbios) groups=222(_netbios),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=224(_warmd) gid=224(_warmd) groups=224(_warmd),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=227(_dovenull) gid=227(_dovenull) groups=227(_dovenull),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=228(_netstatistics) gid=228(_netstatistics) groups=228(_netstatistics),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=229(_avbdeviced) gid=4294967294(nobody) groups=4294967294(nobody),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=230(_krb_krbtgt) gid=4294967294(nobody) groups=4294967294(nobody),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=231(_krb_kadmin) gid=4294967294(nobody) groups=4294967294(nobody),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=232(_krb_changepw) gid=4294967294(nobody) groups=4294967294(nobody),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=233(_krb_kerberos) gid=4294967294(nobody) groups=4294967294(nobody),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=234(_krb_anonymous) gid=4294967294(nobody) groups=4294967294(nobody),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=235(_assetcache) gid=235(_assetcache) groups=235(_assetcache),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=236(_coremediaiod) gid=236(_coremediaiod) groups=236(_coremediaiod),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=239(_launchservicesd) gid=239(_launchservicesd) groups=239(_launchservicesd),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=24(_networkd) gid=24(_networkd) groups=24(_networkd),12(everyone),61(localaccounts),250(_analyticsusers),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=240(_iconservices) gid=240(_iconservices) groups=240(_iconservices),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=241(_distnote) gid=241(_distnote) groups=241(_distnote),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=242(_nsurlsessiond) gid=242(_nsurlsessiond) groups=242(_nsurlsessiond),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=243(_nsurlstoraged) gid=243(_nsurlstoraged) groups=243(_nsurlstoraged),12(everyone),20(staff),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=244(_displaypolicyd) gid=244(_displaypolicyd) groups=244(_displaypolicyd),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=245(_astris) gid=245(_astris) groups=245(_astris),12(everyone),61(localaccount
```

```
s),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=246(_krbfast) gid=4294967294(nobody) groups=4294967294(nobody),12(everyone),61
(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=247(_gamecontrollerd) gid=247(_gamecontrollerd) groups=247(_gamecontrollerd),1
2(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=248(_mbsetupuser) gid=248(_mbsetupuser) groups=248(_mbsetupuser),12(everyone),
61(localaccounts),250(_analyticsusers),701(com.apple.sharepoint.group.1),100(_lpop
erator)
uid=249(_ondemand) gid=249(_ondemand) groups=249(_ondemand),12(everyone),61(locala
ccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=25(_installassistant) gid=25(_installassistant) groups=25(_installassistant),1
2(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=251(_xserverdocs) gid=251(_xserverdocs) groups=251(_xserverdocs),12(everyone),
61(localaccounts),216(_postgres),701(com.apple.sharepoint.group.1),100(_lpoperator
)
uid=252(_wwwproxy) gid=252(_wwwproxy) groups=252(_wwwproxy),12(everyone),61(locala
ccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=253(_mobileasset) gid=253(_mobileasset) groups=253(_mobileasset),12(everyone),
61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=254(_findmydevice) gid=254(_findmydevice) groups=254(_findmydevice),12(everyon
e),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=257(_datadetectors) gid=257(_datadetectors) groups=257(_datadetectors),12(ever
yone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=258(_captiveagent) gid=258(_captiveagent) groups=258(_captiveagent),12(everyon
e),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=259(_ctkd) gid=259(_ctkd) groups=259(_ctkd),12(everyone),61(localaccounts),701
(com.apple.sharepoint.group.1),100(_lpoperator)
uid=26(_lp) gid=26(_lp) groups=26(_lp),12(everyone),61(localaccounts),701(com.appl
e.sharepoint.group.1),100(_lpoperator)
uid=260(_applepay) gid=260(_applepay) groups=260(_applepay),12(everyone),61(locala
ccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=261(_hidd) gid=261(_hidd) groups=261(_hidd),12(everyone),61(localaccounts),701
(com.apple.sharepoint.group.1),100(_lpoperator)
uid=262(_cmiodalassistants) gid=262(_cmiodalassistants) groups=262(_cmiodalassista
nts),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpopera
tor)
uid=263(_analyticsd) gid=263(_analyticsd) groups=263(_analyticsd),12(everyone),61(
localaccounts),250(_analyticsusers),701(com.apple.sharepoint.group.1),100(_lpopera
tor)
uid=265(_fpsd) gid=265(_fpsd) groups=265(_fpsd),12(everyone),61(localaccounts),701
(com.apple.sharepoint.group.1),100(_lpoperator)
uid=266(_timed) gid=266(_timed) groups=266(_timed),12(everyone),61(localaccounts),
250(_analyticsusers),281(_sntpd),701(com.apple.sharepoint.group.1),100(_lpoperator
)
uid=268(_nearbyd) gid=268(_nearbyd) groups=268(_nearbyd),12(everyone),61(localacco
unts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=269(_reportmemoryexception) gid=269(_reportmemoryexception) groups=269(_report
memoryexception),12(everyone),61(localaccounts),250(_analyticsusers),701(com.apple
.sharepoint.group.1),100(_lpoperator)
uid=27(_postfix) gid=27(_postfix) groups=27(_postfix),12(everyone),29(certusers),3
0(_keytabusers),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperato
r)
uid=270(_driverkit) gid=270(_driverkit) groups=270(_driverkit),12(everyone),61(loc
alaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=271(_diskimagesiod) gid=271(_diskimagesiod) groups=271(_diskimagesiod),12(ever
yone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=272(_logd) gid=272(_logd) groups=272(_logd),12(everyone),61(localaccounts),701
(com.apple.sharepoint.group.1),100(_lpoperator)
uid=273(_appinstalld) gid=273(_appinstalld) groups=273(_appinstalld),12(everyone),
61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=274(_installcoordinationd) gid=274(_installcoordinationd) groups=274(_installc
oordinationd),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100
(_lpoperator)
uid=275(_demod) gid=275(_demod) groups=275(_demod),12(everyone),61(localaccounts),
701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=277(_rmd) gid=277(_rmd) groups=277(_rmd),12(everyone),61(localaccounts),701(co
m.apple.sharepoint.group.1),100(_lpoperator)
uid=278(_accessoryupdater) gid=278(_accessoryupdater) groups=278(_accessoryupdater
),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator
)
uid=279(_knowledgegraphd) gid=279(_knowledgegraphd) groups=279(_knowledgegraphd),1
2(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=280(_coreml) gid=280(_coreml) groups=280(_coreml),12(everyone),61(localaccount
s),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=281(_sntpd) gid=281(_sntpd) groups=281(_sntpd),12(everyone),61(localaccounts),
701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=282(_trustd) gid=282(_trustd) groups=282(_trustd),12(everyone),61(localaccount
s),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=283(_mmaintenanced) gid=283(_mmaintenanced) groups=283(_mmaintenanced),12(ever
```

```
yone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=284(_darwindaemon) gid=284(_darwindaemon) groups=284(_darwindaemon),12(everyon
e),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=285(_notification_proxy) gid=285(_notification_proxy) groups=285(_notification
_proxy),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpop
erator)
uid=288(_avphidbridge) gid=288(_avphidbridge) groups=288(_avphidbridge),12(everyon
e),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=289(_biome) gid=289(_biome) groups=289(_biome),12(everyone),61(localaccounts),
701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=291(_backgroundassets) gid=291(_backgroundassets) groups=291(_backgroundassets
),12(everyone),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator
)
uid=31(_scsd) gid=31(_scsd) groups=31(_scsd),12(everyone),61(localaccounts),701(co
m.apple.sharepoint.group.1),100(_lpoperator)
uid=32(_ces) gid=32(_ces) groups=32(_ces),12(everyone),61(localaccounts),701(com.a
pple.sharepoint.group.1),100(_lpoperator)
uid=33(_appstore) gid=33(_appstore) groups=33(_appstore),12(everyone),61(localacco
unts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=4(_uucp) gid=4(tty) groups=4(tty),12(everyone),61(localaccounts),701(com.apple
.sharepoint.group.1),100(_lpoperator)
uid=4294967294(nobody) gid=4294967294(nobody) groups=4294967294(nobody),12(everyon
e),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=441(_oahd) gid=441(_oahd) groups=441(_oahd),12(everyone),61(localaccounts),701
(com.apple.sharepoint.group.1),100(_lpoperator)
uid=501(mac) gid=20(staff) groups=20(staff),12(everyone),61(localaccounts),79(_app
serverusr),80(admin),81(_appserveradm),98(_lpadmin),701(com.apple.sharepoint.group
.1),33(_appstore),100(_lpoperator),204(_developer),250(_analyticsusers),395(com.ap
ple.access_ftp),398(com.apple.access_screensharing),399(com.apple.access_ssh),400(
com.apple.access_remote_ae)
uid=54(_mcxalr) gid=54(_mcxalr) groups=54(_mcxalr),12(everyone),61(localaccounts),
701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=55(_appleevents) gid=55(_appleevents) groups=55(_appleevents),12(everyone),61(
localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=56(_geod) gid=56(_geod) groups=56(_geod),12(everyone),61(localaccounts),701(co
m.apple.sharepoint.group.1),100(_lpoperator)
uid=59(_devdocs) gid=59(_devdocs) groups=59(_devdocs),12(everyone),61(localaccount
s),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=60(_sandbox) gid=60(_sandbox) groups=60(_sandbox),12(everyone),61(localaccount
s),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=65(_mdnsresponder) gid=65(_mdnsresponder) groups=65(_mdnsresponder),12(everyon
e),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=67(_ard) gid=67(_ard) groups=67(_ard),12(everyone),61(localaccounts),701(com.a
pple.sharepoint.group.1),100(_lpoperator)
uid=70(_www) gid=70(_www) groups=70(_www),12(everyone),61(localaccounts),701(com.a
pple.sharepoint.group.1),100(_lpoperator)
uid=71(_eppc) gid=71(_eppc) groups=71(_eppc),12(everyone),61(localaccounts),701(co
m.apple.sharepoint.group.1),100(_lpoperator)
uid=72(_cvs) gid=72(_cvs) groups=72(_cvs),12(everyone),61(localaccounts),701(com.a
pple.sharepoint.group.1),100(_lpoperator)
uid=73(_svn) gid=73(_svn) groups=73(_svn),12(everyone),61(localaccounts),701(com.a
pple.sharepoint.group.1),100(_lpoperator)
uid=74(_mysql) gid=74(_mysql) groups=74(_mysql),12(everyone),61(localaccounts),701
(com.apple.sharepoint.group.1),100(_lpoperator)
uid=75(_sshd) gid=75(_sshd) groups=75(_sshd),12(everyone),61(localaccounts),701(co
m.apple.sharepoint.group.1),100(_lpoperator)
uid=76(_qtss) gid=76(_qtss) groups=76(_qtss),12(everyone),61(localaccounts),701(co
m.apple.sharepoint.group.1),100(_lpoperator)
uid=77(_cyrus) gid=6(mail) groups=6(mail),12(everyone),29(certusers),61(localaccou
nts),701(com.apple.sharepoint.group.1),30(_keytabusers),100(_lpoperator)
uid=78(_mailman) gid=78(_mailman) groups=78(_mailman),12(everyone),61(localaccount
s),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=79(_appserver) gid=79(_appserverusr) groups=79(_appserverusr),12(everyone),61(
localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=82(_clamav) gid=82(_clamav) groups=82(_clamav),12(everyone),61(localaccounts),
701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=83(_amavisd) gid=83(_amavisd) groups=83(_amavisd),12(everyone),61(localaccount
s),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=84(_jabber) gid=84(_jabber) groups=84(_jabber),12(everyone),29(certusers),30(_
keytabusers),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=87(_appowner) gid=87(_appowner) groups=87(_appowner),12(everyone),61(localacco
unts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=88(_windowserver) gid=88(_windowserver) groups=88(_windowserver),12(everyone),
61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=89(_spotlight) gid=89(_spotlight) groups=89(_spotlight),12(everyone),61(locala
ccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=91(_tokend) gid=91(_tokend) groups=91(_tokend),12(everyone),61(localaccounts),
701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=92(_securityagent) gid=92(_securityagent) groups=92(_securityagent),12(everyon
```

```
e),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=93(_calendar) gid=93(_calendar) groups=93(_calendar),12(everyone),29(certusers
),30(_keytabusers),61(localaccounts),216(_postgres),701(com.apple.sharepoint.group
.1),100(_lpoperator)
uid=94(_teamsserver) gid=94(_teamsserver) groups=94(_teamsserver),6(mail),12(every
one),61(localaccounts),70(_www),93(_calendar),209(_odchpass),216(_postgres),221(_w
ebauthserver),701(com.apple.sharepoint.group.1),30(_keytabusers),100(_lpoperator)
uid=95(_update_sharing) gid=4294967294(nobody) groups=4294967294(nobody),12(everyo
ne),61(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=96(_installer) gid=4294967294(nobody) groups=4294967294(nobody),12(everyone),6
1(localaccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=97(_atsserver) gid=97(_atsserver) groups=97(_atsserver),12(everyone),61(locala
ccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=98(_ftp) gid=4294967294(nobody) groups=4294967294(nobody),12(everyone),61(loca
laccounts),701(com.apple.sharepoint.group.1),100(_lpoperator)
uid=99(_unknown) gid=99(_unknown) groups=99(_unknown),12(everyone),61(localaccount
s),701(com.apple.sharepoint.group.1),100(_lpoperator)
```

## Login now

```
9:05 up 2 days, 13:49, 2 users, load averages: 3.06 3.48 2.31
USER TTY FROM LOGIN@ IDLE WHAT
mac console - Fri19 2days -
```

## Last logons

```
mac console Sun Jul 16 18:54 - 18:58 (00:04)
reboot ~ Thu Jul 13 20:49
shutdown ~ Thu Jul 13 20:36
mac console Thu Jul 13 17:17 - 20:36 (03:18)
reboot ~ Thu Jul 13 17:17
shutdown ~ Thu Jul 13 11:02
mac console Wed Jul 12 19:05 - 11:02 (15:57)
reboot ~ Wed Jul 12 19:30
wtmp begins Wed Jul 12 19:30
```

## Last time logon each user

```
Login: _mbsetupuser Name: Setup User
Directory: /var/setup Shell: /bin/bash
Never logged in.
No Mail.
No Plan.
Login: _appstore Name: Mac App Store Service
Directory: /var/db/appstore Shell: /usr/bin/false
Never logged in.
No Mail.
No Plan.
Login: mac Name: mac
Directory: /Users/mac Shell: /bin/bash
On since Fri Jul 28 19:32 (IST) on console, idle 2 days 13:32 (messages off)
On since Sat Jul 29 22:09 (IST) on ttys000, idle 1 day 0:13
On since Sun Jul 30 08:57 (IST) on ttys003, idle 23:45
No Mail.
No Plan.
Login: _cvmsroot Name: CVMS Root
Directory: /var/empty Shell: /usr/bin/false
Never logged in.
No Mail.
No Plan.
Login: root Name: System Administrator
Directory: /var/root Shell: /bin/sh
Never logged in.
No Mail.
No Plan.
```

# Software Information

## Useful software

```
/usr/bin/base64
/usr/bin/curl
/usr/bin/g++
/usr/bin/gcc
/usr/bin/make
/usr/bin/nc
/usr/bin/perl
/sbin/ping
/usr/local/bin/python3
/usr/bin/ruby
/usr/bin/sudo
```

## Installed Compilers

```
/usr/bin/gcc
/usr/bin/g++
```

## Writable Installed Applications

```
/Users/mac/Library/Application Scripts/group.is.workflow.my.app is writable
/Library/Image
Capture/Support/LegacyDeviceDiscoveryHelpers/AirScanLegacyDiscovery.app is writable
/Library/Application Support/Script Editor/Templates/Droplets/Recursive File
Processing Droplet.app is writable
/Library/Application Support/Script Editor/Templates/Droplets/Droplet with Settable
Properties.app is writable
/Library/Application Support/Script Editor/Templates/Droplets/Recursive Image File
Processing Droplet.app is writable
/Library/Application Support/Script Editor/Templates/Cocoa-AppleScript Applet.app
is writable
/Library/Image Capture/Devices/Canon IJScanner2.app is writable
/Library/Image Capture/Devices/Canon IJScanner4.app is writable
/Library/Image Capture/Devices/Canon IJScanner6.app is writable
/Library/Image Capture/Devices/EPSON Scanner.app is writable
/Library/Printers/EPSON/Fax/AutoSetupTool/EPFaxAutoSetupTool.app is writable
/Library/Printers/EPSON/Fax/FaxIOSupport/epsonfax.app is writable
/Library/Printers/EPSON/Fax/Filter/commandFilter.app is writable
/Library/Printers/EPSON/Fax/Filter/rastertoepfax.app is writable
/Library/Printers/EPSON/Fax/Utility/FAX Utility.app is writable
/Library/Printers/EPSON/Fax/Utility/Fax Receive Monitor.app is writable
/Applications/Google Chrome.app is writable
/Applications/Python 3.11/IDLE.app is writable
/Applications/Python 3.11/Python Launcher.app is writable
/Users/mac/Downloads/Visual Studio Code.app is writable
/Library/Frameworks/Python.framework/Versions/3.11/Resources/Python.app is writable
/Library/Developer/CommandLineTools/SDKs/MacOSX12.3.sdk/System/Library/Frameworks/
WebKit.framework/Versions/A/Frameworks/WebKitLegacy.framework/Versions/A/WebKitPlu
ginHost.app is writable
/Library/Developer/CommandLineTools/Library/Frameworks/Python3.framework/Versions/
3.9/Resources/Python.app is writable
/Library/Frameworks/CoreRepairKit.framework is writable
/Library/Frameworks/Python.framework is writable
/Library/Frameworks/CoreRepairCore.framework is writable
```

## Analyzing Http conf Files (limit 70)

```
-rw-r--r-- 1 root wheel 21648 Jun 15 15:38 /private/etc/apache2/httpd.conf
-rw-r--r-- 1 root wheel 21648 Jun 15 15:38 /private/etc/apache2/original/httpd.conf
```

## Searching ssl/ssh files

```
Searching inside /etc/ssh/ssh_config for interesting info
Include /etc/ssh/ssh_config.d/*
Host *
SendEnv LANG LC_*
```

## Searching kerberos conf files and tickets

*http://book.hacktricks.xyz/linux-hardening/privilege-escalation/linux-active-directory*

```
kadmin was found on /usr/sbin/kadmin
kadmin was found on /usr/bin/kinit
klist execution
ptrace protection is enabled (), you need to disable it to search for tickets
inside processes memory
keytab file found, you may be able to impersonate some kerberos principals and add
users or modify passwords
tickets kerberos Not Found
klist Not Found
```

## Searching uncommon passwd files (splunk)

```
passwd file: /private/etc/pam.d/passwd
passwd file: /private/etc/passwd
passwd file: /private/etc/uucp/passwd
```

## Analyzing Kubernetes Files (limit 70)

```
-rw------- 1 root wheel 272 Jun 15 15:38 /private/etc/racoon/psk.txt
# IPv4/v6 addresses
# 10.160.94.3 asecretkeygoeshere
# 172.16.1.133 asecretkeygoeshere
# 3ffe:501:410:ffff:200:86ff:fe05:80fa asecretkeygoeshere
# 3ffe:501:410:ffff:210:4bff:fea2:8baa asecretkeygoeshere
# USER_FQDN
# macuser@localhost somethingsecret
# FQDN
# kame hoge
```

## Analyzing SNMP Files (limit 70)

```
-rw-r--r-- 1 root wheel 16445 Jun 15 15:38 /private/etc/snmp/snmpd.conf
# rocommunity: a SNMPv1/SNMPv2c read-only access community name
rocommunity public default .1.3.6.1.2.1.1.4
# rwcommunity: a SNMPv1/SNMPv2c read-write access community name
#rwcommunity private
```

## Analyzing Postfix Files (limit 70)

```
drwxr-xr-x 23 root wheel 736 Jun 15 15:38 /private/etc/postfix
-rw-r--r-- 1 root wheel 7443 Jun 15 15:38 /private/etc/postfix/master.cf
# flags=DRhu user=vmail argv=/usr/local/bin/maildrop -d ${recipient}
# user=_cyrus argv=/usr/bin/cyrus/bin/deliver -e -r ${sender} -m ${extension}
${user}
# flags=R user=cyrus argv=/cyrus/bin/deliver -e -m ${extension} ${user}
flags=DRhu user=_dovecot:mail argv=/usr/libexec/dovecot/dovecot-lda -d ${user}
# flags=DRhu user=_dovecot:mail argv=/usr/libexec/dovecot/dovecot-lda -d ${user} -a
${recipient} -m ${extension}
user=nobody:mail argv=/usr/bin/perl /usr/libexec/postfix/greylist.pl
# flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail ($recipient)
# flags=F user=ftn argv=/usr/lib/ifmail/ifmail -r $nexthop ($recipient)
# flags=Fq. user=bsmtp argv=/usr/local/sbin/bsmtp -f $sender $nexthop $recipient
# flags=R user=scalemail argv=/usr/lib/scalemail/bin/scalemail-store
# flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py
drwx------ 2 _postfix wheel 64 Jun 15 15:38 /private/var/lib/postfix
drwxr-xr-x 16 root wheel 512 Jun 15 15:38 /private/var/spool/postfix
drwxr-xr-x 45 root wheel 1440 Jun 15 15:38 /usr/libexec/postfix
-rwxr-xr-x 1 root wheel 461616 Jun 15 15:38 /usr/sbin/postfix
drwxr-xr-x 60 root wheel 1920 Jun 15 15:38 /usr/share/doc/postfix
```

## Analyzing Env Files (limit 70)

```
-rw-r--r--@ 1 mac staff 24 Jul 29 10:21
/Users//mac/.vscode/extensions/ms-python.python-2023.12.0/pythonFiles/.env
PYTHONPATH=./lib/python
```

## Analyzing Racoon Files (limit 70)

```
-rw-r--r-- 1 root wheel 3587 Jun 15 15:38 /private/etc/racoon/racoon.conf
path include "/etc/racoon" ;
path pre_shared_key "/etc/racoon/psk.txt" ;
path certificate "/etc/cert" ;
padding
{
maximum_length 20; # maximum padding length.
randomize off; # enable randomize length.
strict_check off; # enable strict check.
exclusive_tail off; # extract last one octet.
}
listen
{
#isakmp ::1 [7000];
#isakmp 202.249.11.124 [500];
#admin [7002]; # administrative's port by kmpstat.
#strict_address; # required all addresses must be bound.
}
timer
{
# These value can be changed per remote node.
counter 10; # maximum trying count to send.
interval 3 sec; # interval to resend (retransmit)
persend 1; # the number of packets per a send.
# timer for waiting to complete each phase.
phase1 30 sec;
phase2 30 sec;
# Auto exit delay timer - for use when controlled by VPN socket
auto_exit_delay 3 sec;
}
remote ::1 [8000]
{
#exchange_mode main,aggressive;
exchange_mode aggressive,main;
doi ipsec_doi;
situation identity_only;
my_identifier user_fqdn "macuser@localhost";
```

```
peers_identifier user_fqdn "macuser@localhost";
#certificate_type x509 "mycert" "mypriv";
nonce_size 16;
lifetime time 1 min; # sec,min,hour
proposal {
encryption_algorithm 3des;
hash_algorithm sha1;
authentication_method pre_shared_key ;
dh_group 2 ;
}
}
sainfo address ::1 icmp6 address ::1 icmp6
{
pfs_group 1;
lifetime time 60 sec;
encryption_algorithm 3des, aes ;
authentication_algorithm hmac_sha1, hmac_md5 ;
compression_algorithm deflate ;
}
include "/var/run/racoon/*.conf" ;
-rw------- 1 root wheel 272 Jun 15 15:38 /private/etc/racoon/psk.txt
# IPv4/v6 addresses
# 10.160.94.3 asecretkeygoeshere
# 172.16.1.133 asecretkeygoeshere
# 3ffe:501:410:ffff:200:86ff:fe05:80fa asecretkeygoeshere
# 3ffe:501:410:ffff:210:4bff:fea2:8baa asecretkeygoeshere
# USER_FQDN
# macuser@localhost somethingsecret
# FQDN
# kame hoge
```

### Analyzing Other Interesting Files (limit 70)

```
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /private/etc/hosts.equiv
```

# Files with Interesting Permissions

### SUID - Check easy privesc, exploits and write perms

*https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid*

```
strace Not Found
-r-sr-xr-x 1 root wheel 267K Jun 15 15:38 /usr/bin/top
-r-sr-xr-x 1 root wheel 183K Jun 15 15:38 /usr/bin/atq
-rwsr-xr-x 1 root wheel 199K Jun 15 15:38 /usr/bin/crontab
-r-sr-xr-x 1 root wheel 183K Jun 15 15:38 /usr/bin/atrm
-r-sr-xr-x 1 root wheel 132K Jun 15 15:38 /usr/bin/newgrp ---> HP-UX_10.20
-rwsr-xr-x 1 root wheel 134K Jun 15 15:38 /usr/bin/su
-r-sr-xr-x 2 root wheel 183K Jun 15 15:38 /usr/bin/batch
-r-sr-xr-x 2 root wheel 183K Jun 15 15:38 /usr/bin/at --->
RTru64_UNIX_4.0g(CVE-2002-1614)
-r-sr-xr-x 1 root wheel 164K Jun 15 15:38 /usr/bin/quota
-r-s--x--x 1 root wheel 1.2M Jun 15 15:38 /usr/bin/sudo --->
check_if_the_sudo_version_is_vulnerable
-r-sr-xr-x 1 root wheel 168K Jun 15 15:38 /usr/bin/login --->
IBM_AIX_3.2.5/SGI_IRIX_6.4
-rws--x--x 1 root wheel 132K Jun 15 15:38 /usr/libexec/security_authtrampoline
-r-sr-xr-x 1 root wheel 132K Jun 15 15:38 /usr/libexec/authopen
-r-sr-xr-x 1 root wheel 166K Jun 15 15:38 /usr/sbin/traceroute6
-r-sr-xr-x 1 root wheel 183K Jun 15 15:38 /usr/sbin/traceroute --->
LBL_Traceroute_[2000-11-15]
-rwsr-xr-x 1 root wheel 199K Jun 15 15:38 /bin/ps (Unknown SUID binary!)
-rwsr-xr-x 1 root wheel 1.9M Jun 15 15:38
/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/MacOS/ARDAgent
(Unknown SUID binary!)
```

## SGID

*https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid*

```
-r-xr-sr-x 1 root tty 132K Jun 15 15:38 /usr/bin/write
-rwxr-sr-x 1 root _postdrop 588K Jun 15 15:38 /usr/sbin/postqueue
-rwxr-sr-x 1 root _postdrop 588K Jun 15 15:38 /usr/sbin/postdrop
```

## Capabilities

*https://book.hacktricks.xyz/linux-hardening/privilege-escalation#capabilities*

## Permissions in init, init.d, systemd, and rc.d

*https://book.hacktricks.xyz/linux-hardening/privilege-escalation#init-init-d-systemd-and-rc-d*

```
Hashes inside passwd file? ........... No
Writable passwd file? ................ /etc/passwd is writable
Credentials in fstab/mtab? ........... No
Can I read shadow files? ............. ##
# User Database
#
# Note that this file is consulted directly only when the system is running
# in single-user mode. At other times this information is provided by
# Open Directory.
#
# See the opendirectoryd(8) man page for additional information about
# Open Directory.
##
nobody:*:-2:-2::0:0:Unprivileged User:/var/empty:/usr/bin/false
root:*:0:0::0:0:System Administrator:/var/root:/bin/sh
daemon:*:1:1::0:0:System Services:/var/root:/usr/bin/false
_uucp:*:4:4::0:0:Unix to Unix Copy Protocol:/var/spool/uucp:/usr/sbin/uucico
_taskgated:*:13:13::0:0:Task Gate Daemon:/var/empty:/usr/bin/false
_networkd:*:24:24::0:0:Network Services:/var/networkd:/usr/bin/false
_installassistant:*:25:25::0:0:Install Assistant:/var/empty:/usr/bin/false
_lp:*:26:26::0:0:Printing Services:/var/spool/cups:/usr/bin/false
_postfix:*:27:27::0:0:Postfix Mail Server:/var/spool/postfix:/usr/bin/false
_scsd:*:31:31::0:0:Service Configuration Service:/var/empty:/usr/bin/false
_ces:*:32:32::0:0:Certificate Enrollment Service:/var/empty:/usr/bin/false
_appstore:*:33:33::0:0:Mac App Store Service:/var/db/appstore:/usr/bin/false
_mcxalr:*:54:54::0:0:MCX AppLaunch:/var/empty:/usr/bin/false
_appleevents:*:55:55::0:0:AppleEvents Daemon:/var/empty:/usr/bin/false
_geod:*:56:56::0:0:Geo Services Daemon:/var/db/geod:/usr/bin/false
_devdocs:*:59:59::0:0:Developer Documentation:/var/empty:/usr/bin/false
_sandbox:*:60:60::0:0:Seatbelt:/var/empty:/usr/bin/false
_mdnsresponder:*:65:65::0:0:mDNSResponder:/var/empty:/usr/bin/false
_ard:*:67:67::0:0:Apple Remote Desktop:/var/empty:/usr/bin/false
_www:*:70:70::0:0:World Wide Web Server:/Library/WebServer:/usr/bin/false
_eppc:*:71:71::0:0:Apple Events User:/var/empty:/usr/bin/false
_cvs:*:72:72::0:0:CVS Server:/var/empty:/usr/bin/false
_svn:*:73:73::0:0:SVN Server:/var/empty:/usr/bin/false
_mysql:*:74:74::0:0:MySQL Server:/var/empty:/usr/bin/false
_sshd:*:75:75::0:0:sshd Privilege separation:/var/empty:/usr/bin/false
_qtss:*:76:76::0:0:QuickTime Streaming Server:/var/empty:/usr/bin/false
_cyrus:*:77:6::0:0:Cyrus Administrator:/var/imap:/usr/bin/false
_mailman:*:78:78::0:0:Mailman List Server:/var/empty:/usr/bin/false
_appserver:*:79:79::0:0:Application Server:/var/empty:/usr/bin/false
_clamav:*:82:82::0:0:ClamAV Daemon:/var/virusmails:/usr/bin/false
_amavisd:*:83:83::0:0:AMaViS Daemon:/var/virusmails:/usr/bin/false
_jabber:*:84:84::0:0:Jabber XMPP Server:/var/empty:/usr/bin/false
_appowner:*:87:87::0:0:Application Owner:/var/empty:/usr/bin/false
_windowserver:*:88:88::0:0:WindowServer:/var/empty:/usr/bin/false
_spotlight:*:89:89::0:0:Spotlight:/var/empty:/usr/bin/false
_tokend:*:91:91::0:0:Token Daemon:/var/empty:/usr/bin/false
_securityagent:*:92:92::0:0:SecurityAgent:/var/db/securityagent:/usr/bin/false
```

```
_calendar:*:93:93::0:0:Calendar:/var/empty:/usr/bin/false
_teamsserver:*:94:94::0:0:TeamsServer:/var/teamsserver:/usr/bin/false
_update_sharing:*:95:-2::0:0:Update Sharing:/var/empty:/usr/bin/false
_installer:*:96:-2::0:0:Installer:/var/empty:/usr/bin/false
_atsserver:*:97:97::0:0:ATS Server:/var/empty:/usr/bin/false
_ftp:*:98:-2::0:0:FTP Daemon:/var/empty:/usr/bin/false
_unknown:*:99:99::0:0:Unknown User:/var/empty:/usr/bin/false
_softwareupdate:*:200:200::0:0:Software Update
Service:/var/db/softwareupdate:/usr/bin/false
_coreaudiod:*:202:202::0:0:Core Audio Daemon:/var/empty:/usr/bin/false
_screensaver:*:203:203::0:0:Screensaver:/var/empty:/usr/bin/false
_locationd:*:205:205::0:0:Location Daemon:/var/db/locationd:/usr/bin/false
_trustevaluationagent:*:208:208::0:0:Trust Evaluation
Agent:/var/empty:/usr/bin/false
_timezone:*:210:210::0:0:AutoTimeZoneDaemon:/var/empty:/usr/bin/false
_lda:*:211:211::0:0:Local Delivery Agent:/var/empty:/usr/bin/false
_cvmsroot:*:212:212::0:0:CVMS Root:/var/empty:/usr/bin/false
_usbmuxd:*:213:213::0:0:iPhone OS Device Helper:/var/db/lockdown:/usr/bin/false
_dovecot:*:214:6::0:0:Dovecot Administrator:/var/empty:/usr/bin/false
_dpaudio:*:215:215::0:0:DP Audio:/var/empty:/usr/bin/false
_postgres:*:216:216::0:0:PostgreSQL Server:/var/empty:/usr/bin/false
_krbtgt:*:217:-2::0:0:Kerberos Ticket Granting Ticket:/var/empty:/usr/bin/false
_kadmin_admin:*:218:-2::0:0:Kerberos Admin Service:/var/empty:/usr/bin/false
_kadmin_changepw:*:219:-2::0:0:Kerberos Change Password
Service:/var/empty:/usr/bin/false
_devicemgr:*:220:220::0:0:Device Management Server:/var/empty:/usr/bin/false
_webauthserver:*:221:221::0:0:Web Auth Server:/var/empty:/usr/bin/false
_netbios:*:222:222::0:0:NetBIOS:/var/empty:/usr/bin/false
_warmd:*:224:224::0:0:Warm Daemon:/var/empty:/usr/bin/false
_dovenull:*:227:227::0:0:Dovecot Authentication:/var/empty:/usr/bin/false
_netstatistics:*:228:228::0:0:Network Statistics Daemon:/var/empty:/usr/bin/false
_avbdeviced:*:229:-2::0:0:Ethernet AVB Device Daemon:/var/empty:/usr/bin/false
_krb_krbtgt:*:230:-2::0:0:Open Directory Kerberos Ticket Granting
Ticket:/var/empty:/usr/bin/false
_krb_kadmin:*:231:-2::0:0:Open Directory Kerberos Admin
Service:/var/empty:/usr/bin/false
_krb_changepw:*:232:-2::0:0:Open Directory Kerberos Change Password
Service:/var/empty:/usr/bin/false
_krb_kerberos:*:233:-2::0:0:Open Directory Kerberos:/var/empty:/usr/bin/false
_krb_anonymous:*:234:-2::0:0:Open Directory Kerberos
Anonymous:/var/empty:/usr/bin/false
_assetcache:*:235:235::0:0:Asset Cache Service:/var/empty:/usr/bin/false
_coremediaiod:*:236:236::0:0:Core Media IO Daemon:/var/empty:/usr/bin/false
_launchservicesd:*:239:239::0:0:_launchservicesd:/var/empty:/usr/bin/false
_iconservices:*:240:240::0:0:IconServices:/var/empty:/usr/bin/false
_distnote:*:241:241::0:0:DistNote:/var/empty:/usr/bin/false
_nsurlsessiond:*:242:242::0:0:NSURLSession
Daemon:/var/db/nsurlsessiond:/usr/bin/false
_displaypolicyd:*:244:244::0:0:Display Policy Daemon:/var/empty:/usr/bin/false
_astris:*:245:245::0:0:Astris Services:/var/db/astris:/usr/bin/false
_krbfast:*:246:-2::0:0:Kerberos FAST Account:/var/empty:/usr/bin/false
_gamecontrollerd:*:247:247::0:0:Game Controller Daemon:/var/empty:/usr/bin/false
_mbsetupuser:*:248:248::0:0:Setup User:/var/setup:/bin/bash
_ondemand:*:249:249::0:0:On Demand Resource Daemon:/var/db/ondemand:/usr/bin/false
_xserverdocs:*:251:251::0:0:macOS Server Documents
Service:/var/empty:/usr/bin/false
_wwwproxy:*:252:252::0:0:WWW Proxy:/var/empty:/usr/bin/false
_mobileasset:*:253:253::0:0:MobileAsset User:/var/ma:/usr/bin/false
_findmydevice:*:254:254::0:0:Find My Device
Daemon:/var/db/findmydevice:/usr/bin/false
_datadetectors:*:257:257::0:0:DataDetectors:/var/db/datadetectors:/usr/bin/false
_captiveagent:*:258:258::0:0:captiveagent:/var/empty:/usr/bin/false
_ctkd:*:259:259::0:0:ctkd Account:/var/empty:/usr/bin/false
_applepay:*:260:260::0:0:applepay Account:/var/db/applepay:/usr/bin/false
_hidd:*:261:261::0:0:HID Service User:/var/db/hidd:/usr/bin/false
_cmiodalassistants:*:262:262::0:0:CoreMedia IO Assistants
User:/var/db/cmiodalassistants:/usr/bin/false
_analyticsd:*:263:263::0:0:Analytics Daemon:/var/db/analyticsd:/usr/bin/false
_fpsd:*:265:265::0:0:FPS Daemon:/var/db/fpsd:/usr/bin/false
_timed:*:266:266::0:0:Time Sync Daemon:/var/db/timed:/usr/bin/false
_nearbyd:*:268:268::0:0:Proximity and Ranging Daemon:/var/db/nearbyd:/usr/bin/false
_reportmemoryexception:*:269:269::0:0:ReportMemoryException:/var/db/reportmemoryex
ception:/usr/bin/false
_driverkit:*:270:270::0:0:DriverKit:/var/empty:/usr/bin/false
_diskimagesiod:*:271:271::0:0:DiskImages IO
Daemon:/var/db/diskimagesiod:/usr/bin/false
_logd:*:272:272::0:0:Log Daemon:/var/db/diagnostics:/usr/bin/false
_appinstalld:*:273:273::0:0:App Install Daemon:/var/db/appinstalld:/usr/bin/false
```

```
_installcoordinationd:*:274:274::0:0:Install Coordination
Daemon:/var/db/installcoordinationd:/usr/bin/false
_demod:*:275:275::0:0:Demo Daemon:/var/empty:/usr/bin/false
_rmd:*:277:277::0:0:Remote Management Daemon:/var/db/rmd:/usr/bin/false
_accessoryupdater:*:278:278::0:0:Accessory Update
Daemon:/var/db/accessoryupdater:/usr/bin/false
_knowledgegraphd:*:279:279::0:0:Knowledge Graph
Daemon:/var/db/knowledgegraphd:/usr/bin/false
_coreml:*:280:280::0:0:CoreML Services:/var/db/coreml:/usr/bin/false
_sntpd:*:281:281::0:0:SNTP Server Daemon:/var/empty:/usr/bin/false
_trustd:*:282:282::0:0:trustd:/var/empty:/usr/bin/false
_mmaintenanced:*:283:283::0:0:mmaintenanced:/var/db/mmaintenanced:/usr/bin/false
_darwindaemon:*:284:284::0:0:Darwin Daemon:/var/db/darwindaemon:/usr/bin/false
_notification_proxy:*:285:285::0:0:Notification Proxy:/var/empty:/usr/bin/false
_avphidbridge:*:288:288::0:0:Apple Virtual Platform HID
Bridge:/var/empty:/usr/bin/false
_biome:*:289:289::0:0:Biome:/var/db/biome:/usr/bin/false
_backgroundassets:*:291:291::0:0:Background Assets
Service:/var/empty:/usr/bin/false
_oahd:*:441:441::0:0:OAH Daemon:/var/empty:/usr/bin/false
Can I read shadow plists? ............
/var/db/dslocal/nodes/Default/users/_accessoryupdater.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000116"
);
gid = (
278
);
home = (
"/var/db/accessoryupdater"
);
name = (
"_accessoryupdater"
);
passwd = (
"*"
);
realname = (
"Accessory Update Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
278
);
}
/var/db/dslocal/nodes/Default/users/_amavisd.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000053"
);
gid = (
83
);
home = (
"/var/virusmails"
);
name = (
"_amavisd",
amavisd
);
passwd = (
"*"
);
realname = (
"AMaViS Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
83
);
}
/var/db/dslocal/nodes/Default/users/_analyticsd.plist
{
```

```
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000107"
);
gid = (
263
);
home = (
"/var/db/analyticsd"
);
name = (
"_analyticsd"
);
passwd = (
"*"
);
realname = (
"Analytics Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
263
);
}
/var/db/dslocal/nodes/Default/users/_appinstalld.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000111"
);
gid = (
273
);
home = (
"/var/db/appinstalld"
);
name = (
"_appinstalld"
);
passwd = (
"*"
);
realname = (
"App Install Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
273
);
}
/var/db/dslocal/nodes/Default/users/_appleevents.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000037"
);
gid = (
55
);
home = (
"/var/empty"
);
name = (
"_appleevents"
);
passwd = (
"*"
);
realname = (
"AppleEvents Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
55
);
```

```
}
/var/db/dslocal/nodes/Default/users/_applepay.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000104"
);
gid = (
260
);
home = (
"/var/db/applepay"
);
name = (
"_applepay"
);
passwd = (
"*"
);
realname = (
"applepay Account"
);
shell = (
"/usr/bin/false"
);
uid = (
260
);
}
/var/db/dslocal/nodes/Default/users/_appowner.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000057"
);
gid = (
87
);
home = (
"/var/empty"
);
name = (
"_appowner",
appowner
);
passwd = (
"*"
);
realname = (
"Application Owner"
);
shell = (
"/usr/bin/false"
);
uid = (
87
);
}
/var/db/dslocal/nodes/Default/users/_appserver.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000004F"
);
gid = (
79
);
home = (
"/var/empty"
);
name = (
"_appserver",
appserver
);
passwd = (
"*"
);
realname = (
"Application Server"
);
shell = (
```

```
"/usr/bin/false"
);
uid = (
79
);
users = (
appserver
);
}
/var/db/dslocal/nodes/Default/users/_appstore.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000021"
);
gid = (
33
);
home = (
"/var/db/appstore"
);
name = (
"_appstore"
);
passwd = (
"*"
);
realname = (
"Mac App Store Service"
);
shell = (
"/usr/bin/false"
);
uid = (
33
);
}
/var/db/dslocal/nodes/Default/users/_ard.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000043"
);
gid = (
67
);
home = (
"/var/empty"
);
name = (
"_ard"
);
passwd = (
"*"
);
realname = (
"Apple Remote Desktop"
);
shell = (
"/usr/bin/false"
);
uid = (
67
);
}
/var/db/dslocal/nodes/Default/users/_assetcache.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000EB"
);
gid = (
235
);
home = (
"/var/empty"
);
name = (
"_assetcache"
);
passwd = (
```

```
"*"
);
realname = (
"Asset Cache Service"
);
shell = (
"/usr/bin/false"
);
uid = (
235
);
}
/var/db/dslocal/nodes/Default/users/_astris.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000F5"
);
gid = (
245
);
home = (
"/var/db/astris"
);
name = (
"_astris"
);
passwd = (
"*"
);
realname = (
"Astris Services"
);
shell = (
"/usr/bin/false"
);
uid = (
245
);
}
/var/db/dslocal/nodes/Default/users/_atsserver.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000061"
);
gid = (
97
);
home = (
"/var/empty"
);
name = (
"_atsserver",
atsserver
);
passwd = (
"*"
);
realname = (
"ATS Server"
);
shell = (
"/usr/bin/false"
);
uid = (
97
);
}
/var/db/dslocal/nodes/Default/users/_avbdeviced.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000E5"
);
gid = (
"-2"
);
home = (
"/var/empty"
);
```

```
name = (
"_avbdeviced"
);
passwd = (
"*"
);
realname = (
"Ethernet AVB Device Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
229
);
}
/var/db/dslocal/nodes/Default/users/_avphidbridge.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000120"
);
gid = (
288
);
home = (
"/var/empty"
);
name = (
"_avphidbridge"
);
passwd = (
"*"
);
realname = (
"Apple Virtual Platform HID Bridge"
);
shell = (
"/usr/bin/false"
);
uid = (
288
);
}
/var/db/dslocal/nodes/Default/users/_backgroundassets.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000123"
);
gid = (
291
);
home = (
"/var/empty"
);
name = (
"_backgroundassets"
);
passwd = (
"*"
);
realname = (
"Background Assets Service"
);
shell = (
"/usr/bin/false"
);
uid = (
291
);
}
/var/db/dslocal/nodes/Default/users/_biome.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000121"
);
gid = (
289
);
```

```
home = (
"/var/db/biome"
);
name = (
"_biome"
);
passwd = (
"*"
);
realname = (
Biome
);
shell = (
"/usr/bin/false"
);
uid = (
289
);
}
/var/db/dslocal/nodes/Default/users/_calendar.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000005D"
);
gid = (
93
);
home = (
"/var/empty"
);
name = (
"_calendar",
calendar
);
passwd = (
"*"
);
realname = (
Calendar
);
shell = (
"/usr/bin/false"
);
uid = (
93
);
}
/var/db/dslocal/nodes/Default/users/_captiveagent.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000102"
);
gid = (
258
);
home = (
"/var/empty"
);
name = (
"_captiveagent"
);
passwd = (
"*"
);
realname = (
captiveagent
);
shell = (
"/usr/bin/false"
);
uid = (
258
);
}
/var/db/dslocal/nodes/Default/users/_ces.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000020"
```

```
);
gid = (
32
);
home = (
"/var/empty"
);
name = (
"_ces"
);
passwd = (
"*"
);
realname = (
"Certificate Enrollment Service"
);
shell = (
"/usr/bin/false"
);
uid = (
32
);
}
/var/db/dslocal/nodes/Default/users/_clamav.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000052"
);
gid = (
82
);
home = (
"/var/virusmails"
);
name = (
"_clamav",
clamav
);
passwd = (
"*"
);
realname = (
"ClamAV Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
82
);
}
/var/db/dslocal/nodes/Default/users/_cmiodalassistants.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000106"
);
gid = (
262
);
home = (
"/var/db/cmiodalassistants"
);
name = (
"_cmiodalassistants"
);
passwd = (
"*"
);
realname = (
"CoreMedia IO Assistants User"
);
shell = (
"/usr/bin/false"
);
uid = (
262
);
}
```

```
/var/db/dslocal/nodes/Default/users/_coreaudiod.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000CA"
);
gid = (
202
);
home = (
"/var/empty"
);
name = (
"_coreaudiod"
);
passwd = (
"*"
);
realname = (
"Core Audio Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
202
);
}
/var/db/dslocal/nodes/Default/users/_coremediaiod.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000EC"
);
gid = (
236
);
home = (
"/var/empty"
);
name = (
"_coremediaiod"
);
passwd = (
"*"
);
realname = (
"Core Media IO Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
236
);
}
/var/db/dslocal/nodes/Default/users/_coreml.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000118"
);
gid = (
280
);
home = (
"/var/db/coreml"
);
name = (
"_coreml"
);
passwd = (
"*"
);
realname = (
"CoreML Services"
);
shell = (
"/usr/bin/false"
);
uid = (
```

```
280
);
}
/var/db/dslocal/nodes/Default/users/_ctkd.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000103"
);
gid = (
259
);
home = (
"/var/empty"
);
name = (
"_ctkd"
);
passwd = (
"*"
);
realname = (
"ctkd Account"
);
shell = (
"/usr/bin/false"
);
uid = (
259
);
}
/var/db/dslocal/nodes/Default/users/_cvmsroot.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000D4"
);
gid = (
212
);
home = (
"/var/empty"
);
name = (
"_cvmsroot"
);
passwd = (
"*"
);
realname = (
"CVMS Root"
);
shell = (
"/usr/bin/false"
);
uid = (
212
);
}
/var/db/dslocal/nodes/Default/users/_cvs.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000048"
);
gid = (
72
);
home = (
"/var/empty"
);
name = (
"_cvs"
);
passwd = (
"*"
);
realname = (
"CVS Server"
);
shell = (
```

```
"/usr/bin/false"
);
uid = (
72
);
}
/var/db/dslocal/nodes/Default/users/_cyrus.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000004D"
);
gid = (
6
);
home = (
"/var/imap"
);
name = (
"_cyrus",
cyrusimap
);
passwd = (
"*"
);
realname = (
"Cyrus Administrator"
);
shell = (
"/usr/bin/false"
);
uid = (
77
);
}
/var/db/dslocal/nodes/Default/users/_darwindaemon.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000011C"
);
gid = (
284
);
home = (
"/var/db/darwindaemon"
);
name = (
"_darwindaemon"
);
passwd = (
"*"
);
realname = (
"Darwin Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
284
);
}
/var/db/dslocal/nodes/Default/users/_datadetectors.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000101"
);
gid = (
257
);
home = (
"/var/db/datadetectors"
);
name = (
"_datadetectors"
);
passwd = (
"*"
);
```

```
realname = (
DataDetectors
);
shell = (
"/usr/bin/false"
);
uid = (
257
);
}
/var/db/dslocal/nodes/Default/users/_demod.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000113"
);
gid = (
275
);
home = (
"/var/empty"
);
name = (
"_demod"
);
passwd = (
"*"
);
realname = (
"Demo Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
275
);
}
/var/db/dslocal/nodes/Default/users/_devdocs.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000003B"
);
gid = (
59
);
home = (
"/var/empty"
);
name = (
"_devdocs",
devdocs
);
passwd = (
"*"
);
realname = (
"Developer Documentation"
);
shell = (
"/usr/bin/false"
);
uid = (
59
);
}
/var/db/dslocal/nodes/Default/users/_devicemgr.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000DC"
);
gid = (
220
);
home = (
"/var/empty"
);
name = (
"_devicemgr"
```

```
);
passwd = (
"*"
);
realname = (
"Device Management Server"
);
shell = (
"/usr/bin/false"
);
uid = (
220
);
}
/var/db/dslocal/nodes/Default/users/_diskimagesiod.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000010F"
);
gid = (
271
);
home = (
"/var/db/diskimagesiod"
);
name = (
"_diskimagesiod"
);
passwd = (
"*"
);
realname = (
"DiskImages IO Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
271
);
}
/var/db/dslocal/nodes/Default/users/_displaypolicyd.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000F4"
);
gid = (
244
);
home = (
"/var/empty"
);
name = (
"_displaypolicyd"
);
passwd = (
"*"
);
realname = (
"Display Policy Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
244
);
}
/var/db/dslocal/nodes/Default/users/_distnote.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000F1"
);
gid = (
241
);
home = (
"/var/empty"
```

```
);
name = (
"_distnote"
);
passwd = (
"*"
);
realname = (
DistNote
);
shell = (
"/usr/bin/false"
);
uid = (
241
);
}
/var/db/dslocal/nodes/Default/users/_dovecot.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000D6"
);
gid = (
6
);
home = (
"/var/empty"
);
name = (
"_dovecot"
);
passwd = (
"*"
);
realname = (
"Dovecot Administrator"
);
shell = (
"/usr/bin/false"
);
uid = (
214
);
}
/var/db/dslocal/nodes/Default/users/_dovenull.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000E3"
);
gid = (
227
);
home = (
"/var/empty"
);
name = (
"_dovenull"
);
passwd = (
"*"
);
realname = (
"Dovecot Authentication"
);
shell = (
"/usr/bin/false"
);
uid = (
227
);
}
/var/db/dslocal/nodes/Default/users/_dpaudio.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000D7"
);
gid = (
215
```

```
);
home = (
"/var/empty"
);
name = (
"_dpaudio"
);
passwd = (
"*"
);
realname = (
"DP Audio"
);
shell = (
"/usr/bin/false"
);
uid = (
215
);
}
/var/db/dslocal/nodes/Default/users/_driverkit.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000010E"
);
gid = (
270
);
home = (
"/var/empty"
);
name = (
"_driverkit"
);
passwd = (
"*"
);
realname = (
DriverKit
);
shell = (
"/usr/bin/false"
);
uid = (
270
);
}
/var/db/dslocal/nodes/Default/users/_eppc.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000047"
);
gid = (
71
);
home = (
"/var/empty"
);
name = (
"_eppc",
eppc
);
passwd = (
"*"
);
realname = (
"Apple Events User"
);
shell = (
"/usr/bin/false"
);
uid = (
71
);
}
/var/db/dslocal/nodes/Default/users/_findmydevice.plist
{
generateduid = (
```

```
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000FE"
);
gid = (
254
);
home = (
"/var/db/findmydevice"
);
name = (
"_findmydevice"
);
passwd = (
"*"
);
realname = (
"Find My Device Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
254
);
}
/var/db/dslocal/nodes/Default/users/_fpsd.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000109"
);
gid = (
265
);
home = (
"/var/db/fpsd"
);
name = (
"_fpsd"
);
passwd = (
"*"
);
realname = (
"FPS Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
265
);
}
/var/db/dslocal/nodes/Default/users/_ftp.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000062"
);
gid = (
"-2"
);
home = (
"/var/empty"
);
name = (
"_ftp",
ftp
);
passwd = (
"*"
);
realname = (
"FTP Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
98
);
```

```
}
/var/db/dslocal/nodes/Default/users/_gamecontrollerd.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000F7"
);
gid = (
247
);
home = (
"/var/empty"
);
name = (
"_gamecontrollerd"
);
passwd = (
"*"
);
realname = (
"Game Controller Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
247
);
}
/var/db/dslocal/nodes/Default/users/_geod.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000038"
);
gid = (
56
);
home = (
"/var/db/geod"
);
name = (
"_geod"
);
passwd = (
"*"
);
realname = (
"Geo Services Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
56
);
}
/var/db/dslocal/nodes/Default/users/_hidd.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000105"
);
gid = (
261
);
home = (
"/var/db/hidd"
);
name = (
"_hidd"
);
passwd = (
"*"
);
realname = (
"HID Service User"
);
shell = (
"/usr/bin/false"
);
```

```
uid = (
261
);
}
/var/db/dslocal/nodes/Default/users/_iconservices.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000F0"
);
gid = (
240
);
home = (
"/var/empty"
);
name = (
"_iconservices"
);
passwd = (
"*"
);
realname = (
IconServices
);
shell = (
"/usr/bin/false"
);
uid = (
240
);
}
/var/db/dslocal/nodes/Default/users/_installassistant.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000019"
);
gid = (
25
);
home = (
"/var/empty"
);
name = (
"_installassistant"
);
passwd = (
"*"
);
realname = (
"Install Assistant"
);
shell = (
"/usr/bin/false"
);
uid = (
25
);
}
/var/db/dslocal/nodes/Default/users/_installcoordinationd.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000112"
);
gid = (
274
);
home = (
"/var/db/installcoordinationd"
);
name = (
"_installcoordinationd"
);
passwd = (
"*"
);
realname = (
"Install Coordination Daemon"
);
```

```
shell = (
"/usr/bin/false"
);
uid = (
274
);
}
/var/db/dslocal/nodes/Default/users/_installer.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000060"
);
gid = (
"-2"
);
home = (
"/var/empty"
);
name = (
"_installer"
);
passwd = (
"*"
);
realname = (
Installer
);
shell = (
"/usr/bin/false"
);
uid = (
96
);
}
/var/db/dslocal/nodes/Default/users/_jabber.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000054"
);
gid = (
84
);
home = (
"/var/empty"
);
name = (
"_jabber",
jabber
);
passwd = (
"*"
);
realname = (
"Jabber XMPP Server"
);
shell = (
"/usr/bin/false"
);
uid = (
84
);
}
/var/db/dslocal/nodes/Default/users/_kadmin_admin.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000DA"
);
gid = (
"-2"
);
home = (
"/var/empty"
);
name = (
"_kadmin_admin"
);
passwd = (
"*"
```

```
);
realname = (
"Kerberos Admin Service"
);
shell = (
"/usr/bin/false"
);
uid = (
218
);
}
/var/db/dslocal/nodes/Default/users/_kadmin_changepw.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000DB"
);
gid = (
"-2"
);
home = (
"/var/empty"
);
name = (
"_kadmin_changepw"
);
passwd = (
"*"
);
realname = (
"Kerberos Change Password Service"
);
shell = (
"/usr/bin/false"
);
uid = (
219
);
}
/var/db/dslocal/nodes/Default/users/_knowledgegraphd.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000117"
);
gid = (
279
);
home = (
"/var/db/knowledgegraphd"
);
name = (
"_knowledgegraphd"
);
passwd = (
"*"
);
realname = (
"Knowledge Graph Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
279
);
}
/var/db/dslocal/nodes/Default/users/_krb_anonymous.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000EA"
);
gid = (
"-2"
);
home = (
"/var/empty"
);
name = (
"_krb_anonymous"
```

```
);
passwd = (
"*"
);
realname = (
"Open Directory Kerberos Anonymous"
);
shell = (
"/usr/bin/false"
);
uid = (
234
);
}
/var/db/dslocal/nodes/Default/users/_krb_changepw.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000E8"
);
gid = (
"-2"
);
home = (
"/var/empty"
);
name = (
"_krb_changepw"
);
passwd = (
"*"
);
realname = (
"Open Directory Kerberos Change Password Service"
);
shell = (
"/usr/bin/false"
);
uid = (
232
);
}
/var/db/dslocal/nodes/Default/users/_krb_kadmin.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000E7"
);
gid = (
"-2"
);
home = (
"/var/empty"
);
name = (
"_krb_kadmin"
);
passwd = (
"*"
);
realname = (
"Open Directory Kerberos Admin Service"
);
shell = (
"/usr/bin/false"
);
uid = (
231
);
}
/var/db/dslocal/nodes/Default/users/_krb_kerberos.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000E9"
);
gid = (
"-2"
);
home = (
"/var/empty"
```

```
);
name = (
"_krb_kerberos"
);
passwd = (
"*"
);
realname = (
"Open Directory Kerberos"
);
shell = (
"/usr/bin/false"
);
uid = (
233
);
}
/var/db/dslocal/nodes/Default/users/_krb_krbtgt.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000E6"
);
gid = (
"-2"
);
home = (
"/var/empty"
);
name = (
"_krb_krbtgt"
);
passwd = (
"*"
);
realname = (
"Open Directory Kerberos Ticket Granting Ticket"
);
shell = (
"/usr/bin/false"
);
uid = (
230
);
}
/var/db/dslocal/nodes/Default/users/_krbfast.plist
{
KerberosFlags = (
110
);
KerberosKeys = (
{length = 128, bytes = 0x307ea103 020101a0 77307530 2da12b30 ... ef751519 4589e615
}
);
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000F6"
);
gid = (
"-2"
);
home = (
"/var/empty"
);
name = (
"_krbfast"
);
passwd = (
"*"
);
realname = (
"Kerberos FAST Account"
);
"record_daemon_version" = (
8780000
);
shell = (
"/usr/bin/false"
);
uid = (
```

```
246
);
}
/var/db/dslocal/nodes/Default/users/_krbtgt.plist
{
KerberosFlags = (
110
);
KerberosKeys = (
{length = 128, bytes = 0x307ea103 020101a0 77307530 2da12b30 ... 707940df 623261d5
}
);
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000D9"
);
gid = (
"-2"
);
home = (
"/var/empty"
);
name = (
"_krbtgt"
);
passwd = (
"*"
);
realname = (
"Kerberos Ticket Granting Ticket"
);
"record_daemon_version" = (
8780000
);
shell = (
"/usr/bin/false"
);
uid = (
217
);
}
/var/db/dslocal/nodes/Default/users/_launchservicesd.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000EF"
);
gid = (
239
);
home = (
"/var/empty"
);
name = (
"_launchservicesd"
);
passwd = (
"*"
);
realname = (
"_launchservicesd"
);
shell = (
"/usr/bin/false"
);
uid = (
239
);
}
/var/db/dslocal/nodes/Default/users/_lda.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000D3"
);
gid = (
211
);
home = (
"/var/empty"
);
```

```
name = (
"_lda"
);
passwd = (
"*"
);
realname = (
"Local Delivery Agent"
);
shell = (
"/usr/bin/false"
);
uid = (
211
);
}
/var/db/dslocal/nodes/Default/users/_locationd.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000CD"
);
gid = (
205
);
home = (
"/var/db/locationd"
);
name = (
"_locationd"
);
passwd = (
"*"
);
realname = (
"Location Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
205
);
}
/var/db/dslocal/nodes/Default/users/_logd.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000110"
);
gid = (
272
);
home = (
"/var/db/diagnostics"
);
name = (
"_logd"
);
passwd = (
"*"
);
realname = (
"Log Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
272
);
}
/var/db/dslocal/nodes/Default/users/_lp.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000001A"
);
gid = (
26
);
```

```
home = (
"/var/spool/cups"
);
name = (
"_lp",
lp
);
passwd = (
"*"
);
realname = (
"Printing Services"
);
shell = (
"/usr/bin/false"
);
uid = (
26
);
}
/var/db/dslocal/nodes/Default/users/_mailman.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000004E"
);
gid = (
78
);
home = (
"/var/empty"
);
name = (
"_mailman",
mailman
);
passwd = (
"*"
);
realname = (
"Mailman List Server"
);
shell = (
"/usr/bin/false"
);
uid = (
78
);
}
/var/db/dslocal/nodes/Default/users/_mbsetupuser.plist
{
IsHidden = (
YES
);
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000F8"
);
gid = (
248
);
home = (
"/var/setup"
);
name = (
"_mbsetupuser"
);
passwd = (
"*"
);
realname = (
"Setup User"
);
shell = (
"/bin/bash"
);
uid = (
248
);
}
```

```
/var/db/dslocal/nodes/Default/users/_mcxalr.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000036"
);
gid = (
54
);
home = (
"/var/empty"
);
name = (
"_mcxalr",
mcxalr
);
passwd = (
"*"
);
realname = (
"MCX AppLaunch"
);
shell = (
"/usr/bin/false"
);
uid = (
54
);
}
/var/db/dslocal/nodes/Default/users/_mdnsresponder.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000041"
);
gid = (
65
);
home = (
"/var/empty"
);
name = (
"_mdnsresponder"
);
passwd = (
"*"
);
realname = (
mDNSResponder
);
shell = (
"/usr/bin/false"
);
uid = (
65
);
}
/var/db/dslocal/nodes/Default/users/_mmaintenanced.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000011B"
);
gid = (
283
);
home = (
"/var/db/mmaintenanced"
);
name = (
"_mmaintenanced"
);
passwd = (
"*"
);
realname = (
mmaintenanced
);
shell = (
"/usr/bin/false"
);
```

```
uid = (
283
);
}
/var/db/dslocal/nodes/Default/users/_mobileasset.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000FD"
);
gid = (
253
);
home = (
"/var/ma"
);
name = (
"_mobileasset"
);
passwd = (
"*"
);
realname = (
"MobileAsset User"
);
shell = (
"/usr/bin/false"
);
uid = (
253
);
}
/var/db/dslocal/nodes/Default/users/_mysql.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000004A"
);
gid = (
74
);
home = (
"/var/empty"
);
name = (
"_mysql",
mysql
);
passwd = (
"*"
);
realname = (
"MySQL Server"
);
shell = (
"/usr/bin/false"
);
uid = (
74
);
}
/var/db/dslocal/nodes/Default/users/_nearbyd.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000010C"
);
gid = (
268
);
home = (
"/var/db/nearbyd"
);
name = (
"_nearbyd"
);
passwd = (
"*"
);
realname = (
"Proximity and Ranging Daemon"
```

```
);
shell = (
"/usr/bin/false"
);
uid = (
268
);
}
/var/db/dslocal/nodes/Default/users/_netbios.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000DE"
);
gid = (
222
);
home = (
"/var/empty"
);
name = (
"_netbios"
);
passwd = (
"*"
);
realname = (
NetBIOS
);
shell = (
"/usr/bin/false"
);
uid = (
222
);
}
/var/db/dslocal/nodes/Default/users/_netstatistics.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000E4"
);
gid = (
228
);
home = (
"/var/empty"
);
name = (
"_netstatistics"
);
passwd = (
"*"
);
realname = (
"Network Statistics Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
228
);
}
/var/db/dslocal/nodes/Default/users/_networkd.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000018"
);
gid = (
24
);
home = (
"/var/networkd"
);
name = (
"_networkd"
);
passwd = (
"*"
```

```
);
realname = (
"Network Services"
);
shell = (
"/usr/bin/false"
);
uid = (
24
);
}
/var/db/dslocal/nodes/Default/users/_notification_proxy.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000011D"
);
gid = (
285
);
home = (
"/var/empty"
);
name = (
"_notification_proxy"
);
passwd = (
"*"
);
realname = (
"Notification Proxy"
);
shell = (
"/usr/bin/false"
);
uid = (
285
);
}
/var/db/dslocal/nodes/Default/users/_nsurlsessiond.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000F2"
);
gid = (
242
);
home = (
"/var/db/nsurlsessiond"
);
name = (
"_nsurlsessiond"
);
passwd = (
"*"
);
realname = (
"NSURLSession Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
242
);
}
/var/db/dslocal/nodes/Default/users/_nsurlstoraged.plist
{
accountPolicyData = (
{length = 245, bytes = 0x3c3f786d 6c207665 7273696f 6e3d2231 ... 2f706c69 73743e0a
}
);
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000F3"
);
gid = (
243
);
home = (
```

```
"/var/db/nsurlstoraged"
);
name = (
"_nsurlstoraged"
);
passwd = (
"*"
);
realname = (
"_nsurlstoraged"
);
shell = (
"/usr/bin/false"
);
uid = (
243
);
}
/var/db/dslocal/nodes/Default/users/_oahd.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000001B9"
);
gid = (
441
);
home = (
"/var/empty"
);
name = (
"_oahd"
);
passwd = (
"*"
);
realname = (
"OAH Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
441
);
}
/var/db/dslocal/nodes/Default/users/_ondemand.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000F9"
);
gid = (
249
);
home = (
"/var/db/ondemand"
);
name = (
"_ondemand"
);
passwd = (
"*"
);
realname = (
"On Demand Resource Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
249
);
}
/var/db/dslocal/nodes/Default/users/_postfix.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000001B"
);
gid = (
```

```
27
);
home = (
"/var/spool/postfix"
);
name = (
"_postfix",
postfix
);
passwd = (
"*"
);
realname = (
"Postfix Mail Server"
);
shell = (
"/usr/bin/false"
);
uid = (
27
);
}
/var/db/dslocal/nodes/Default/users/_postgres.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000D8"
);
gid = (
216
);
home = (
"/var/empty"
);
name = (
"_postgres"
);
passwd = (
"*"
);
realname = (
"PostgreSQL Server"
);
shell = (
"/usr/bin/false"
);
uid = (
216
);
}
/var/db/dslocal/nodes/Default/users/_qtss.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000004C"
);
gid = (
76
);
home = (
"/var/empty"
);
name = (
"_qtss",
qtss
);
passwd = (
"*"
);
realname = (
"QuickTime Streaming Server"
);
shell = (
"/usr/bin/false"
);
uid = (
76
);
}
/var/db/dslocal/nodes/Default/users/_reportmemoryexception.plist
```

```
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000010D"
);
gid = (
269
);
home = (
"/var/db/reportmemoryexception"
);
name = (
"_reportmemoryexception"
);
passwd = (
"*"
);
realname = (
ReportMemoryException
);
shell = (
"/usr/bin/false"
);
uid = (
269
);
}
/var/db/dslocal/nodes/Default/users/_rmd.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000115"
);
gid = (
277
);
home = (
"/var/db/rmd"
);
name = (
"_rmd"
);
passwd = (
"*"
);
realname = (
"Remote Management Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
277
);
}
/var/db/dslocal/nodes/Default/users/_sandbox.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000003C"
);
gid = (
60
);
home = (
"/var/empty"
);
name = (
"_sandbox",
sandbox
);
passwd = (
"*"
);
realname = (
Seatbelt
);
shell = (
"/usr/bin/false"
);
uid = (
```

```
60
);
}
/var/db/dslocal/nodes/Default/users/_screensaver.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000CB"
);
gid = (
203
);
home = (
"/var/empty"
);
name = (
"_screensaver"
);
passwd = (
"*"
);
realname = (
Screensaver
);
shell = (
"/usr/bin/false"
);
uid = (
203
);
}
/var/db/dslocal/nodes/Default/users/_scsd.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000001F"
);
gid = (
31
);
home = (
"/var/empty"
);
name = (
"_scsd"
);
passwd = (
"*"
);
realname = (
"Service Configuration Service"
);
shell = (
"/usr/bin/false"
);
uid = (
31
);
}
/var/db/dslocal/nodes/Default/users/_securityagent.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000005C"
);
gid = (
92
);
home = (
"/var/db/securityagent"
);
name = (
"_securityagent",
securityagent
);
passwd = (
"*"
);
realname = (
SecurityAgent
);
```

```
shell = (
"/usr/bin/false"
);
uid = (
92
);
}
/var/db/dslocal/nodes/Default/users/_sntpd.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000119"
);
gid = (
281
);
home = (
"/var/empty"
);
name = (
"_sntpd"
);
passwd = (
"*"
);
realname = (
"SNTP Server Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
281
);
}
/var/db/dslocal/nodes/Default/users/_softwareupdate.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000C8"
);
gid = (
200
);
home = (
"/var/db/softwareupdate"
);
name = (
"_softwareupdate"
);
passwd = (
"*"
);
realname = (
"Software Update Service"
);
shell = (
"/usr/bin/false"
);
uid = (
200
);
}
/var/db/dslocal/nodes/Default/users/_spotlight.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000059"
);
gid = (
89
);
home = (
"/var/empty"
);
name = (
"_spotlight",
spotlight
);
passwd = (
"*"
```

```
);
realname = (
Spotlight
);
shell = (
"/usr/bin/false"
);
uid = (
89
);
}
/var/db/dslocal/nodes/Default/users/_sshd.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000004B"
);
gid = (
75
);
home = (
"/var/empty"
);
name = (
"_sshd",
sshd
);
passwd = (
"*"
);
realname = (
"sshd Privilege separation"
);
shell = (
"/usr/bin/false"
);
uid = (
75
);
}
/var/db/dslocal/nodes/Default/users/_svn.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000049"
);
gid = (
73
);
home = (
"/var/empty"
);
name = (
"_svn"
);
passwd = (
"*"
);
realname = (
"SVN Server"
);
shell = (
"/usr/bin/false"
);
uid = (
73
);
}
/var/db/dslocal/nodes/Default/users/_taskgated.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000000D"
);
gid = (
13
);
home = (
"/var/empty"
);
name = (
```

```
"_taskgated"
);
passwd = (
"*"
);
realname = (
"Task Gate Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
13
);
}
/var/db/dslocal/nodes/Default/users/_teamsserver.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000005E"
);
gid = (
94
);
home = (
"/var/teamsserver"
);
name = (
"_teamsserver",
teamsserver
);
passwd = (
"*"
);
realname = (
TeamsServer
);
shell = (
"/usr/bin/false"
);
uid = (
94
);
}
/var/db/dslocal/nodes/Default/users/_timed.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000010A"
);
gid = (
266
);
home = (
"/var/db/timed"
);
name = (
"_timed"
);
passwd = (
"*"
);
realname = (
"Time Sync Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
266
);
}
/var/db/dslocal/nodes/Default/users/_timezone.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000D2"
);
gid = (
210
);
```

```
home = (
"/var/empty"
);
name = (
"_timezone"
);
passwd = (
"*"
);
realname = (
AutoTimeZoneDaemon
);
shell = (
"/usr/bin/false"
);
uid = (
210
);
}
/var/db/dslocal/nodes/Default/users/_tokend.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000005B"
);
gid = (
91
);
home = (
"/var/empty"
);
name = (
"_tokend",
tokend
);
passwd = (
"*"
);
realname = (
"Token Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
91
);
}
/var/db/dslocal/nodes/Default/users/_trustd.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000011A"
);
gid = (
282
);
home = (
"/var/empty"
);
name = (
"_trustd"
);
passwd = (
"*"
);
realname = (
trustd
);
shell = (
"/usr/bin/false"
);
uid = (
282
);
}
/var/db/dslocal/nodes/Default/users/_trustevaluationagent.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000D0"
```

```
);
gid = (
208
);
home = (
"/var/empty"
);
name = (
"_trustevaluationagent"
);
passwd = (
"*"
);
realname = (
"Trust Evaluation Agent"
);
shell = (
"/usr/bin/false"
);
uid = (
208
);
}
/var/db/dslocal/nodes/Default/users/_unknown.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000063"
);
gid = (
99
);
home = (
"/var/empty"
);
name = (
"_unknown",
unknown
);
passwd = (
"*"
);
realname = (
"Unknown User"
);
shell = (
"/usr/bin/false"
);
uid = (
99
);
}
/var/db/dslocal/nodes/Default/users/_update_sharing.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA0000005F"
);
gid = (
"-2"
);
home = (
"/var/empty"
);
name = (
"_update_sharing"
);
passwd = (
"*"
);
realname = (
"Update Sharing"
);
shell = (
"/usr/bin/false"
);
uid = (
95
);
}
```

```
/var/db/dslocal/nodes/Default/users/_usbmuxd.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000D5"
);
gid = (
213
);
home = (
"/var/db/lockdown"
);
name = (
"_usbmuxd"
);
passwd = (
"*"
);
realname = (
"iPhone OS Device Helper"
);
shell = (
"/usr/bin/false"
);
uid = (
213
);
}
/var/db/dslocal/nodes/Default/users/_uucp.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000004"
);
gid = (
4
);
home = (
"/var/spool/uucp"
);
name = (
"_uucp"
);
passwd = (
"*"
);
realname = (
"Unix to Unix Copy Protocol"
);
shell = (
"/usr/sbin/uucico"
);
uid = (
4
);
}
/var/db/dslocal/nodes/Default/users/_warmd.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000E0"
);
gid = (
224
);
home = (
"/var/empty"
);
name = (
"_warmd"
);
passwd = (
"*"
);
realname = (
"Warm Daemon"
);
shell = (
"/usr/bin/false"
);
uid = (
```

```
224
);
}
/var/db/dslocal/nodes/Default/users/_webauthserver.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000DD"
);
gid = (
221
);
home = (
"/var/empty"
);
name = (
"_webauthserver"
);
passwd = (
"*"
);
realname = (
"Web Auth Server"
);
shell = (
"/usr/bin/false"
);
uid = (
221
);
}
/var/db/dslocal/nodes/Default/users/_windowserver.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000058"
);
gid = (
88
);
home = (
"/var/empty"
);
name = (
"_windowserver",
windowserver
);
passwd = (
"*"
);
realname = (
WindowServer
);
shell = (
"/usr/bin/false"
);
uid = (
88
);
}
/var/db/dslocal/nodes/Default/users/_www.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000046"
);
gid = (
70
);
home = (
"/Library/WebServer"
);
name = (
"_www",
www
);
passwd = (
"*"
);
realname = (
"World Wide Web Server"
```

```
);
shell = (
"/usr/bin/false"
);
uid = (
70
);
}
/var/db/dslocal/nodes/Default/users/_wwwproxy.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000FC"
);
gid = (
252
);
home = (
"/var/empty"
);
name = (
"_wwwproxy"
);
passwd = (
"*"
);
realname = (
"WWW Proxy"
);
shell = (
"/usr/bin/false"
);
uid = (
252
);
}
/var/db/dslocal/nodes/Default/users/_xserverdocs.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000FB"
);
gid = (
251
);
home = (
"/var/empty"
);
name = (
"_xserverdocs"
);
passwd = (
"*"
);
realname = (
"macOS Server Documents Service"
);
shell = (
"/usr/bin/false"
);
uid = (
251
);
}
/var/db/dslocal/nodes/Default/users/daemon.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000001"
);
gid = (
1
);
home = (
"/var/root"
);
name = (
daemon
);
passwd = (
"*"
```

```
);
realname = (
"System Services"
);
shell = (
"/usr/bin/false"
);
uid = (
1
);
}
/var/db/dslocal/nodes/Default/users/mac.plist
{
AvatarRepresentation = (
""
);
HeimdalSRPKey = (
{length = 559, bytes = 0x3082022b a0820204 04820200 5b19cb03 ... 45b6a204 02020fa0
}
);
KerberosKeys = (
{length = 332, bytes = 0x30820148 a1030201 02a08201 3f308201 ... 34464334 336d6163
}
);
ShadowHashData = (
{length = 905, bytes = 0x62706c69 73743030 d2010203 0a5f101e ... 00000000 0000034b
}
);
"_writers_AvatarRepresentation" = (
mac
);
"_writers_UserCertificate" = (
mac
);
"_writers_hint" = (
mac
);
"_writers_inputSources" = (
mac
);
"_writers_jpegphoto" = (
mac
);
"_writers_passwd" = (
mac
);
"_writers_picture" = (
mac
);
"_writers_unlockOptions" = (
mac
);
accountPolicyData = (
{length = 416, bytes = 0x3c3f786d 6c207665 7273696f 6e3d2231 ... 2f706c69 73743e0a
}
);
"authentication_authority" = (
";ShadowHash;HASHLIST:<SALTED-SHA512-PBKDF2,SRP-RFC5054-4096-SHA512-PBKDF2>",
";Kerberosv5;;mac@LKDC:SHA1.F312D61EEEE71F3601ECB73194A304E204E4FC43;LKDC:SHA1.F31
2D61EEEE71F3601ECB73194A304E204E4FC43;",
";SecureToken;"
);
generateduid = (
"18A223F3-2113-4303-B270-D719FB6AA686"
);
gid = (
20
);
home = (
"/Users/mac"
);
inputSources = (
"<?xml version=\\"1.0\\" encoding=\\"UTF-8\\"?>\\n<!DOCTYPE plist PUBLIC
\\"-//Apple//DTD PLIST 1.0//EN\\"
\\"http://www.apple.com/DTDs/PropertyList-1.0.dtd\\">\\n<plist version=\\"1.0\\">\
\n<array>\\n\\t<dict>\\n\\t\\t<key>InputSourceKind</key>\\n\\t\\t<string>Keyboard
Layout</string>\\n\\t\\t<key>KeyboardLayout
ID</key>\\n\\t\\t<integer>252</integer>\\n\\t\\t<key>KeyboardLayout
```

```
Name</key>\\n\\t\\t<string>ABC</string>\\n\\t</dict>\\n</array>\\n</plist>\\n"
);
jpegphoto = (
{length = 789838, bytes = 0x4d4d002a 000c0008 eaeaeae5 e5e5eded ... fe4bfedc
ff6dffff }
);
name = (
mac
);
passwd = (
"********"
);
picture = (
"/Library/User Pictures/Flowers/Dahlia.tif"
);
realname = (
mac
);
"record_daemon_version" = (
4855000
);
shell = (
"/bin/bash"
);
uid = (
501
);
unlockOptions = (
0
);
}
/var/db/dslocal/nodes/Default/users/nobody.plist
{
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAAFFFFFFFE"
);
gid = (
"-2"
);
home = (
"/var/empty"
);
name = (
nobody
);
passwd = (
"*"
);
realname = (
"Unprivileged User"
);
shell = (
"/usr/bin/false"
);
"smb_rid" = (
501
);
uid = (
"-2"
);
}
/var/db/dslocal/nodes/Default/users/root.plist
{
accountPolicyData = (
{length = 245, bytes = 0x3c3f786d 6c207665 7273696f 6e3d2231 ... 2f706c69 73743e0a
}
);
generateduid = (
"FFFFEEEE-DDDD-CCCC-BBBB-AAAA00000000"
);
gid = (
0
);
home = (
"/var/root",
"/private/var/root"
);
name = (
root,
```

```
"BUILTIN\\\\Local System"
);
passwd = (
"*"
);
realname = (
"System Administrator"
);
"record_daemon_version" = (
4855000
);
shell = (
"/bin/sh"
);
"smb_sid" = (
"S-1-5-18"
);
uid = (
0
);
}
Can I write shadow plists? ........... No
Can I read opasswd file? ............. No
Can I write in network-scripts? ...... No
Can I read root folder? .............. No
```

## Searching root files in home dirs (limit 30)

```
/home/
/Users/
/Users//.localized
/Users//Shared
/Users//Shared/.localized
/Users//mac/Library/Containers/com.apple.UsageTrackingAgent/Data/Library/Applicati
on
/Users//mac/Library/Application
/var/root
/var/root/.CFUserTextEncoding
/var/root/Library
/var/root/Library/Application Support
/var/root/Library/Application Support/DiskImages
/var/root/Library/Application Support/DiskImages/com.apple.diskimages.fsck
/var/root/Library/Application Support/dmd
/var/root/Library/Application Support/com.apple.sharedfilelist
/var/root/Library/Application Support/com.apple.sharedfilelist/com.apple.LSSharedF
ileList.ApplicationRecentDocuments
/var/root/Library/Application
Support/com.apple.sharedfilelist/com.apple.LSSharedFileList.FavoriteVolumes.sfl2
/var/root/Library/Application Support/com.apple.avfoundation
/var/root/Library/Application Support/com.apple.avfoundation/Frecents
/var/root/Library/Application
Support/com.apple.avfoundation/Frecents/com.apple.avfoundation.frecents.plist
/var/root/Library/Saved Application State
/var/root/Library/Saved Application
State/com.apple.SoftwareUpdateLauncher.savedState
/var/root/Library/Saved Application
State/com.apple.SoftwareUpdateLauncher.savedState/window_1.data
/var/root/Library/Saved Application
State/com.apple.SoftwareUpdateLauncher.savedState/windows.plist
/var/root/Library/Saved Application
State/com.apple.SoftwareUpdateLauncher.savedState/data.data
/var/root/Library/MediaRemote
/var/root/Library/MediaRemote/DeviceInfo.plist
/var/root/Library/MediaRemote/MediaRemoteTelevisionDeviceInfoIdentifier.plist
/var/root/Library/Preferences
/var/root/Library/Preferences/com.apple.duetactivityscheduler.plist
```

# Other Interesting Files

## Unexpected in root

```
/.file
/etc
/var
/.VolumeIcon.icns
/tmp
```

## Modified interesting files in the last 5mins (limit 100)

```
/Library/Application Support/CrashReporter/DiagnosticMessagesHistory.plist
/Library/Preferences/com.apple.networkextension.uuidcache.plist
/Library/Preferences/com.apple.powerlogd.plist
/Library/Logs/DiagnosticReports/awdd_2023-07-31-090429_macs-MacBook-Pro.awd
/Library/Logs/DiagnosticReports/awdd_2023-07-31-090429-1_macs-MacBook-Pro.awd
/System/Library/AssetsV2/analytics/com.apple.mobileassetd.Download.Attempt_7B178C9
D-FCD0-4371-955F-BCF3EAC71A00.MADAnalytics
/System/Library/AssetsV2/analytics/com.apple.mobileassetd.Query.Attempt_89624201-8
E1D-4441-A02D-C87A4B1EED48.MADAnalytics
/System/Library/AssetsV2/analytics/com.apple.mobileassetd.Query.Attempt_405AA33D-4
BC6-438A-B1F4-D92BC6B667D1.MADAnalytics
/System/Library/AssetsV2/analytics/com.apple.mobileassetd.Query.Attempt_02852432-A
FD1-4DCD-9171-E6E1BD8DDBA1.MADAnalytics
/System/Library/AssetsV2/analytics/com.apple.mobileassetd.Query.Attempt_F1EA5D3F-6
E65-4E32-97BE-F6ADCF6CD2BB.MADAnalytics
/System/Library/AssetsV2/analytics/com.apple.mobileassetd.Query.Attempt_8B2659CF-B
4E6-4413-BBD2-DD802757FD98.MADAnalytics
/System/Volumes/Data/Library/Application
Support/CrashReporter/DiagnosticMessagesHistory.plist
/System/Volumes/Data/Library/Preferences/com.apple.networkextension.uuidcache.plis
t
/System/Volumes/Data/Library/Preferences/com.apple.powerlogd.plist
/System/Volumes/Data/Library/Logs/DiagnosticReports/awdd_2023-07-31-090429_macs-Ma
cBook-Pro.awd
/System/Volumes/Data/Library/Logs/DiagnosticReports/awdd_2023-07-31-090429-1_macs-
MacBook-Pro.awd
/System/Volumes/Data/System/Library/AssetsV2/analytics/com.apple.mobileassetd.Down
load.Attempt_7B178C9D-FCD0-4371-955F-BCF3EAC71A00.MADAnalytics
/System/Volumes/Data/System/Library/AssetsV2/analytics/com.apple.mobileassetd.Quer
y.Attempt_89624201-8E1D-4441-A02D-C87A4B1EED48.MADAnalytics
/System/Volumes/Data/System/Library/AssetsV2/analytics/com.apple.mobileassetd.Quer
y.Attempt_405AA33D-4BC6-438A-B1F4-D92BC6B667D1.MADAnalytics
/System/Volumes/Data/System/Library/AssetsV2/analytics/com.apple.mobileassetd.Quer
y.Attempt_02852432-AFD1-4DCD-9171-E6E1BD8DDBA1.MADAnalytics
/System/Volumes/Data/System/Library/AssetsV2/analytics/com.apple.mobileassetd.Quer
y.Attempt_F1EA5D3F-6E65-4E32-97BE-F6ADCF6CD2BB.MADAnalytics
/System/Volumes/Data/System/Library/AssetsV2/analytics/com.apple.mobileassetd.Quer
y.Attempt_8B2659CF-B4E6-4413-BBD2-DD802757FD98.MADAnalytics
/System/Volumes/Data/private/var/vm/sleepimage
/System/Volumes/Data/private/var/logs/keybagd.log.0
/System/Volumes/Data/private/var/audit/20230728134559.not_terminated
/System/Volumes/Data/private/var/root/Library/Preferences/com.apple.powerdatad.pli
st
/System/Volumes/Data/private/var/root/Library/Preferences/com.apple.xpc.activity2.
plist
/System/Volumes/Data/private/var/root/Library/Preferences/com.apple.CoreBrightness
.plist
/System/Volumes/Data/private/var/root/Library/Preferences/com.apple.awdd.persisten
t.plist
/System/Volumes/Data/private/var/root/Library/Logs/Bluetooth/bluetoothd-hci-latest
.pklg
/System/Volumes/Data/private/var/root/Library/TRM/analytics2
/System/Volumes/Data/private/var/root/Library/TRM/policy
/System/Volumes/Data/private/var/root/Library/Caches/com.apple.rtcreporting/eventc
ache/cache.db-wal
/System/Volumes/Data/private/var/root/Library/Caches/com.apple.countryd/countryCod
eCache.plist
/System/Volumes/Data/private/var/db/locationd/clients.plist
```

```
/System/Volumes/Data/private/var/db/powerlog/Library/BatteryLife/CurrentPowerlog.P
LSQL
/System/Volumes/Data/private/var/db/powerlog/Library/BatteryLife/CurrentPowerlog.P
LSQL-wal
/System/Volumes/Data/private/var/db/analyticsd/Library/Preferences/analyticsd.plis
t
/System/Volumes/Data/private/var/db/analyticsd/state.sqlite-wal
/System/Volumes/Data/private/var/db/awdd/staging/awdd-anonymous-28-fragment-3.metr
iclog
/System/Volumes/Data/private/var/db/awdd/staging/awdd-primary-27-fragment-1.metric
log
/System/Volumes/Data/private/var/db/awdd/staging/awdd-anonymous-28-fragment-4.metr
iclog
/System/Volumes/Data/private/var/db/awdd/staging/awdd-primary-27-fragment-2.metric
log
/System/Volumes/Data/private/var/db/awdd/staging/awdd-anonymous-28-fragment-6.metr
iclog
/System/Volumes/Data/private/var/db/awdd/staging/awdd-primary-27-fragment-5.metric
log
/System/Volumes/Data/private/var/db/com.apple.xpc.launchd/disabled.501.plist
/System/Volumes/Data/private/var/db/diagnostics/Special/000000000000001c.tracev3
/System/Volumes/Data/private/var/db/diagnostics/timesync/0000000000000003.timesync
/System/Volumes/Data/private/var/db/diagnostics/Persist/0000000000000024.tracev3
/System/Volumes/Data/private/var/db/diagnostics/logdata.statistics.0.txt
/System/Volumes/Data/private/var/db/sudo/ts/mac
/System/Volumes/Data/private/var/db/timed/com.apple.timed.plist
/System/Volumes/Data/private/var/db/com.apple.countryd/countryCodeCache.plist
/System/Volumes/Data/private/var/db/systemstats/0EF79A57-643D-4D9C-8937-CA8074DC5E
0A.coalitions.XXXXXX.stats
/System/Volumes/Data/private/var/db/systemstats/0EF79A57-643D-4D9C-8937-CA8074DC5E
0A.batched_events.XXXXXX.stats
/System/Volumes/Data/private/var/db/systemstats/0EF79A57-643D-4D9C-8937-CA8074DC5E
0A.pkg_energy.XXXXXX.stats
/System/Volumes/Data/private/var/db/systemstats/0EF79A57-643D-4D9C-8937-CA8074DC5E
0A.ioreporting.XXXXXX.stats
/System/Volumes/Data/private/var/db/systemstats/0EF79A57-643D-4D9C-8937-CA8074DC5E
0A.battery_charge.XXXXXX.stats
/System/Volumes/Data/private/var/db/systemstats/0EF79A57-643D-4D9C-8937-CA8074DC5E
0A.system_events.XXXXXX.stats
/System/Volumes/Data/private/var/db/systemstats/0EF79A57-643D-4D9C-8937-CA8074DC5E
0A.coalitions_private.XXXXXX.stats
/System/Volumes/Data/private/var/db/systemstats/0EF79A57-643D-4D9C-8937-CA8074DC5E
0A.coalitions_memory.XXXXXX.stats
/System/Volumes/Data/private/var/db/systemstats/0EF79A57-643D-4D9C-8937-CA8074DC5E
0A.devices.XXXXXX.stats
/System/Volumes/Data/private/var/log/displaypolicy/displaypolicyd.0:2:0.log
/System/Volumes/Data/private/var/log/powermanagement/2023.07.31.asl
/System/Volumes/Data/private/var/log/powermanagement/StoreData
/System/Volumes/Data/private/var/log/asl/AUX.2023.07.31/559
/System/Volumes/Data/private/var/log/asl/AUX.2023.07.31/557
/System/Volumes/Data/private/var/log/asl/2023.07.31.G80.asl
/System/Volumes/Data/private/var/log/asl/StoreData
/System/Volumes/Data/private/var/log/DiagnosticMessages/2023.07.31.asl
/System/Volumes/Data/private/var/log/DiagnosticMessages/StoreData
/System/Volumes/Data/private/var/log/com.apple.xpc.launchd/launchd.log
/System/Volumes/Data/private/var/log/system.log
/System/Volumes/Data/private/var/log/wifi.log
/System/Volumes/Data/private/var/log/install.log
/System/Volumes/Data/private/var/folders/32/j27ws12d1h7clhtwczptn6hr0000gn/C/mds/m
dsDirectory.db
/System/Volumes/Data/private/var/folders/32/j27ws12d1h7clhtwczptn6hr0000gn/C/mds/m
dsObject.db
/System/Volumes/Data/private/var/folders/32/j27ws12d1h7clhtwczptn6hr0000gn/C/com.a
pple.sharingd/mds/mdsDirectory.db
/System/Volumes/Data/private/var/folders/32/j27ws12d1h7clhtwczptn6hr0000gn/C/com.a
pple.sharingd/mds/mdsObject.db
/System/Volumes/Data/private/var/folders/zz/zyxvpxvq6csfxvn_n00000y800007k/T/com.a
pple.nsurlsessiond/CFNetworkDownload_MjHf7p.tmp
/System/Volumes/Data/private/var/protected/sfanalytics/18A223F3-2113-4303-B270-D71
9FB6AA686/trust_analytics.db-wal
/System/Volumes/Data/private/var/protected/sfanalytics/18A223F3-2113-4303-B270-D71
9FB6AA686/ckks_analytics.db-wal
/System/Volumes/Data/private/var/protected/sfanalytics/FFFFEEEE-DDDD-CCCC-BBBB-AAA
A0000011A/trust_analytics.db-wal
/System/Volumes/Data/Users/mac/Desktop/Kavach/MacPEASjson.json
/System/Volumes/Data/Users/mac/Library/Application
Support/Google/Chrome/GrShaderCache/data_1
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
```

```
1/GPUCache/data_1
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/WebStorage/QuotaManager-journal
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/WebStorage/QuotaManager
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/DIPS
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Extension State/000003.log
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Network Persistent State
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Secure Preferences
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Local Extension Settings/gighmmpiobklfepjocnamgkkbiglidom/000003.log
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Local Extension Settings/kbfnbcaeplbcioakkpcpgfkobkghlhen/000003.log
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/DIPS-journal
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Local Storage/leveldb/000011.log
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Cookies
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/DawnCache/data_1
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Cookies-journal
/System/Volumes/Data/Users/mac/Library/Application
Support/Google/Chrome/ShaderCache/data_1
```

## Files inside /Users/mac (limit 20)

```
total 40
drwxr-xr-x+ 16 mac staff 512 Jul 29 22:03 .
drwxr-xr-x 5 root admin 160 Jul 12 19:29 ..
-r-------- 1 mac staff 7 Jun 17 18:16 .CFUserTextEncoding
-rw-r--r--@ 1 mac staff 10244 Jul 30 17:25 .DS_Store
drwx------+ 2 mac staff 64 Jul 13 10:50 .Trash
-rw-------@ 1 mac staff 132 Jul 30 09:41 .bash_history
drwx------ 16 mac staff 512 Jul 30 08:57 .bash_sessions
drwxr-xr-x@ 5 mac staff 160 Jul 29 10:20 .vscode
drwx------+ 5 mac staff 160 Jul 29 10:24 Desktop
drwx------+ 3 mac staff 96 Jun 17 18:16 Documents
drwx------+ 10 mac staff 320 Jul 30 08:49 Downloads
drwx------@ 89 mac staff 2848 Jul 30 09:19 Library
drwx------+ 4 mac staff 128 Jul 28 19:35 Movies
drwx------+ 4 mac staff 128 Jul 28 19:35 Music
drwx------+ 5 mac staff 160 Jul 28 12:46 Pictures
drwxr-xr-x+ 4 mac staff 128 Jun 17 18:16 Public
```

## Files inside others home (limit 20)

```
/Users//.localized
/Users//Shared/.localized
/Users//Shared/.betamigrated
/Users//mac/Music/Music/Media.localized/.Media Preferences.plist
/Users//mac/Music/Music/Media.localized/.localized/id.strings
/Users//mac/Music/Music/Media.localized/.localized/es.strings
/Users//mac/Music/Music/Media.localized/.localized/no.strings
/Users//mac/Music/Music/Media.localized/.localized/zh_TW.strings
/Users//mac/Music/Music/Media.localized/.localized/fi.strings
/Users//mac/Music/Music/Media.localized/.localized/ru.strings
/Users//mac/Music/Music/Media.localized/.localized/en.strings
/Users//mac/Music/Music/Media.localized/.localized/es_419.strings
/Users//mac/Music/Music/Media.localized/.localized/he.strings
/Users//mac/Music/Music/Media.localized/.localized/uk.strings
/Users//mac/Music/Music/Media.localized/.localized/fr_CA.strings
/Users//mac/Music/Music/Media.localized/.localized/nl.strings
/Users//mac/Music/Music/Media.localized/.localized/de.strings
/Users//mac/Music/Music/Media.localized/.localized/ja.strings
```

```
/Users//mac/Music/Music/Media.localized/.localized/sk.strings
/Users//mac/Music/Music/Media.localized/.localized/hr.strings
```

## Searching installed mail applications

```
postfix
sendmail
```

## Backup files (limited 100)

```
-rw-r--r-- 1 root wheel 394 Jun 15 15:38 /usr/share/man/man8/backupd-helper.8
-rw-r--r-- 1 root wheel 455 Jun 15 15:38 /usr/share/man/man8/backupd.8
-rw-r--r-- 1 root wheel 6896 Jun 15 15:38 /usr/share/man/man1/profiles.old.1
-rw-r--r-- 1 root wheel 394 Mar 7 10:52 /Library/Developer/CommandLineTools/SDKs/M
acOSX13.3.sdk/usr/share/man/man8/backupd-helper.8
-rw-r--r-- 1 root wheel 455 Mar 7 11:00 /Library/Developer/CommandLineTools/SDKs/M
acOSX13.3.sdk/usr/share/man/man8/backupd.8
-rw-r--r-- 1 root wheel 6896 Mar 5 04:38 /Library/Developer/CommandLineTools/SDKs/
MacOSX13.3.sdk/usr/share/man/man1/profiles.old.1
-rw-r--r-- 1 root wheel 320 Mar 5 03:59 /Library/Developer/CommandLineTools/SDKs/M
acOSX13.3.sdk/System/Library/Frameworks/Ruby.framework/Versions/2.6/usr/lib/ruby/g
ems/2.6.0/gems/sqlite3-1.3.13/ext/sqlite3/backup.h
-rw-r--r-- 1 root wheel 4474 Mar 5 03:58 /Library/Developer/CommandLineTools/SDKs/
MacOSX13.3.sdk/System/Library/Frameworks/Ruby.framework/Versions/2.6/usr/lib/ruby/
gems/2.6.0/gems/sqlite3-1.3.13/ext/sqlite3/backup.c
-rw-r--r-- 1 root wheel 394 Nov 11 2022 /Library/Developer/CommandLineTools/SDKs/M
acOSX13.1.sdk/usr/share/man/man8/backupd-helper.8
-rw-r--r-- 1 root wheel 455 Nov 11 2022 /Library/Developer/CommandLineTools/SDKs/M
acOSX13.1.sdk/usr/share/man/man8/backupd.8
-rw-r--r-- 1 root wheel 6896 Nov 5 2022 /Library/Developer/CommandLineTools/SDKs/M
acOSX13.1.sdk/usr/share/man/man1/profiles.old.1
-rw-r--r-- 1 root wheel 320 Nov 6 2022 /Library/Developer/CommandLineTools/SDKs/Ma
cOSX13.1.sdk/System/Library/Frameworks/Ruby.framework/Versions/2.6/usr/lib/ruby/ge
ms/2.6.0/gems/sqlite3-1.3.13/ext/sqlite3/backup.h
-rw-r--r-- 1 root wheel 4474 Nov 6 2022 /Library/Developer/CommandLineTools/SDKs/M
acOSX13.1.sdk/System/Library/Frameworks/Ruby.framework/Versions/2.6/usr/lib/ruby/g
ems/2.6.0/gems/sqlite3-1.3.13/ext/sqlite3/backup.c
-rw-r--r-- 1 root wheel 394 Feb 22 2022 /Library/Developer/CommandLineTools/SDKs/M
acOSX12.3.sdk/usr/share/man/man8/backupd-helper.8
-rw-r--r-- 1 root wheel 455 Feb 22 2022 /Library/Developer/CommandLineTools/SDKs/M
acOSX12.3.sdk/usr/share/man/man8/backupd.8
-rw-r--r-- 1 root wheel 6896 Feb 12 2022 /Library/Developer/CommandLineTools/SDKs/
MacOSX12.3.sdk/usr/share/man/man1/profiles.old.1
-rw-r--r-- 1 root wheel 320 Feb 12 2022 /Library/Developer/CommandLineTools/SDKs/M
acOSX12.3.sdk/System/Library/Frameworks/Ruby.framework/Versions/2.6/usr/lib/ruby/g
ems/2.6.0/gems/sqlite3-1.3.13/ext/sqlite3/backup.h
-rw-r--r-- 1 root wheel 4474 Feb 12 2022 /Library/Developer/CommandLineTools/SDKs/
MacOSX12.3.sdk/System/Library/Frameworks/Ruby.framework/Versions/2.6/usr/lib/ruby/
gems/2.6.0/gems/sqlite3-1.3.13/ext/sqlite3/backup.c
-rw-r--r-- 1 root wheel 5917 May 8 12:06 /Library/Developer/CommandLineTools/Libra
ry/Frameworks/Python3.framework/Versions/3.9/lib/python3.9/sqlite3/test/backup.py
-rw-r--r-- 1 root wheel 3483 Jul 12 19:05 /Library/Preferences/SystemConfiguration
/com.apple.airport.preferences.plist.backup
-rw-rw-r-- 1 root admin 16710 Jul 29 10:15 /Library/Frameworks/Python.framework/Ve
rsions/3.11/lib/python3.11/test/test_sqlite3/__pycache__/test_backup.cpython-311.o
pt-1.pyc
-rw-rw-r-- 1 root admin 16710 Jul 29 10:15 /Library/Frameworks/Python.framework/Ve
rsions/3.11/lib/python3.11/test/test_sqlite3/__pycache__/test_backup.cpython-311.p
yc
-rw-rw-r-- 1 root admin 5767 Jun 7 04:53 /Library/Frameworks/Python.framework/Vers
ions/3.11/lib/python3.11/test/test_sqlite3/test_backup.py
-rw-r--r-- 1 root wheel 142 Jun 15 15:38 /System/Library/Preferences/ProtectedClou
dStorage/Identities/com.apple.pcs.backup.plist
-rwxr-xr-x 1 root wheel 4381808 Jun 15 15:38
/System/Library/CoreServices/backupd.bundle/Contents/Resources/backupd
-rwxr-xr-x 1 root wheel 517360 Jun 15 15:38
/System/Library/CoreServices/backupd.bundle/Contents/Resources/backupd-helper
-rw-r--r-- 1 root wheel 4474 Jun 15 15:38 /System/Library/Frameworks/Ruby.framewor
k/Versions/2.6/usr/lib/ruby/gems/2.6.0/gems/sqlite3-1.3.13/ext/sqlite3/backup.c
```

```
-rw-r--r-- 1 root wheel 338 Jun 15 15:38 /System/Library/Frameworks/Ruby.framework
/Versions/2.6/usr/share/ri/2.6.0/system/Bundler/EnvironmentPreserver/backup-i.ri
-rw-r--r-- 1 root wheel 2980 Jun 15 15:38
/System/Library/LaunchDaemons/com.apple.backupd-helper.plist
-rw-r--r-- 1 root wheel 1261 Jun 15 15:38
/System/Library/LaunchDaemons/com.apple.backupd.plist
-rw-r--r-- 1 root wheel 394 Mar 7 10:52 /System/Volumes/Data/Library/Developer/Com
mandLineTools/SDKs/MacOSX13.3.sdk/usr/share/man/man8/backupd-helper.8
-rw-r--r-- 1 root wheel 455 Mar 7 11:00 /System/Volumes/Data/Library/Developer/Com
mandLineTools/SDKs/MacOSX13.3.sdk/usr/share/man/man8/backupd.8
-rw-r--r-- 1 root wheel 6896 Mar 5 04:38 /System/Volumes/Data/Library/Developer/Co
mmandLineTools/SDKs/MacOSX13.3.sdk/usr/share/man/man1/profiles.old.1
-rw-r--r-- 1 root wheel 320 Mar 5 03:59 /System/Volumes/Data/Library/Developer/Com
mandLineTools/SDKs/MacOSX13.3.sdk/System/Library/Frameworks/Ruby.framework/Version
s/2.6/usr/lib/ruby/gems/2.6.0/gems/sqlite3-1.3.13/ext/sqlite3/backup.h
-rw-r--r-- 1 root wheel 4474 Mar 5 03:58 /System/Volumes/Data/Library/Developer/Co
mmandLineTools/SDKs/MacOSX13.3.sdk/System/Library/Frameworks/Ruby.framework/Versio
ns/2.6/usr/lib/ruby/gems/2.6.0/gems/sqlite3-1.3.13/ext/sqlite3/backup.c
-rw-r--r-- 1 root wheel 394 Nov 11 2022 /System/Volumes/Data/Library/Developer/Com
mandLineTools/SDKs/MacOSX13.1.sdk/usr/share/man/man8/backupd-helper.8
-rw-r--r-- 1 root wheel 455 Nov 11 2022 /System/Volumes/Data/Library/Developer/Com
mandLineTools/SDKs/MacOSX13.1.sdk/usr/share/man/man8/backupd.8
-rw-r--r-- 1 root wheel 6896 Nov 5 2022 /System/Volumes/Data/Library/Developer/Com
mandLineTools/SDKs/MacOSX13.1.sdk/usr/share/man/man1/profiles.old.1
-rw-r--r-- 1 root wheel 320 Nov 6 2022 /System/Volumes/Data/Library/Developer/Comm
andLineTools/SDKs/MacOSX13.1.sdk/System/Library/Frameworks/Ruby.framework/Versions
/2.6/usr/lib/ruby/gems/2.6.0/gems/sqlite3-1.3.13/ext/sqlite3/backup.h
-rw-r--r-- 1 root wheel 4474 Nov 6 2022 /System/Volumes/Data/Library/Developer/Com
mandLineTools/SDKs/MacOSX13.1.sdk/System/Library/Frameworks/Ruby.framework/Version
s/2.6/usr/lib/ruby/gems/2.6.0/gems/sqlite3-1.3.13/ext/sqlite3/backup.c
-rw-r--r-- 1 root wheel 394 Feb 22 2022 /System/Volumes/Data/Library/Developer/Com
mandLineTools/SDKs/MacOSX12.3.sdk/usr/share/man/man8/backupd-helper.8
-rw-r--r-- 1 root wheel 455 Feb 22 2022 /System/Volumes/Data/Library/Developer/Com
mandLineTools/SDKs/MacOSX12.3.sdk/usr/share/man/man8/backupd.8
-rw-r--r-- 1 root wheel 6896 Feb 12 2022 /System/Volumes/Data/Library/Developer/Co
mmandLineTools/SDKs/MacOSX12.3.sdk/usr/share/man/man1/profiles.old.1
-rw-r--r-- 1 root wheel 320 Feb 12 2022 /System/Volumes/Data/Library/Developer/Com
mandLineTools/SDKs/MacOSX12.3.sdk/System/Library/Frameworks/Ruby.framework/Version
s/2.6/usr/lib/ruby/gems/2.6.0/gems/sqlite3-1.3.13/ext/sqlite3/backup.h
-rw-r--r-- 1 root wheel 4474 Feb 12 2022 /System/Volumes/Data/Library/Developer/Co
mmandLineTools/SDKs/MacOSX12.3.sdk/System/Library/Frameworks/Ruby.framework/Versio
ns/2.6/usr/lib/ruby/gems/2.6.0/gems/sqlite3-1.3.13/ext/sqlite3/backup.c
-rw-r--r-- 1 root wheel 5917 May 8 12:06 /System/Volumes/Data/Library/Developer/Co
mmandLineTools/Library/Frameworks/Python3.framework/Versions/3.9/lib/python3.9/sql
ite3/test/backup.py
-rw-r--r-- 1 root wheel 3483 Jul 12 19:05 /System/Volumes/Data/Library/Preferences
/SystemConfiguration/com.apple.airport.preferences.plist.backup
-rw-rw-r-- 1 root admin 16710 Jul 29 10:15 /System/Volumes/Data/Library/Frameworks
/Python.framework/Versions/3.11/lib/python3.11/test/test_sqlite3/__pycache__/test_
backup.cpython-311.opt-1.pyc
-rw-rw-r-- 1 root admin 16710 Jul 29 10:15 /System/Volumes/Data/Library/Frameworks
/Python.framework/Versions/3.11/lib/python3.11/test/test_sqlite3/__pycache__/test_
backup.cpython-311.pyc
-rw-rw-r-- 1 root admin 5767 Jun 7 04:53 /System/Volumes/Data/Library/Frameworks/P
ython.framework/Versions/3.11/lib/python3.11/test/test_sqlite3/test_backup.py
-rw------- 1 root wheel 492 Jul 8 04:12
/System/Volumes/Data/private/var/db/dslocal-backup.xar
-rw-------@ 1 mac staff 283 Jul 29 10:07
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Session Storage/LOG.old
-rw-------@ 1 mac staff 355 Jul 29 10:13
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/IndexedDB/https_www.youtube.com_0.indexeddb.leveldb/LOG.old
-rw-------@ 1 mac staff 411 Jul 29 10:08
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile 1
/IndexedDB/chrome-extension_gighmmpiobklfepjocnamgkkbiglidom_0.indexeddb.leveldb/L
OG.old
-rw-------@ 1 mac staff 293 Jul 29 10:07
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/GCM Store/Encryption/LOG.old
-rw-------@ 1 mac staff 271 Jul 29 10:07
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/GCM Store/LOG.old
-rw-------@ 1 mac staff 0 Jul 29 10:07
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/AutofillStrikeDatabase/LOG.old
-rw-------@ 1 mac staff 311 Jul 29 10:07
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
```

```
1/Site Characteristics Database/LOG.old
-rw-------@ 1 mac staff 371 Jul 29 10:08
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Managed Extension Settings/gighmmpiobklfepjocnamgkkbiglidom/LOG.old
-rw-------@ 1 mac staff 371 Jul 29 10:08
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Managed Extension Settings/kbfnbcaeplbcioakkpcpgfkobkghlhen/LOG.old
-rw-------@ 1 mac staff 0 Jul 29 10:07
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/coupon_db/LOG.old
-rw-------@ 1 mac staff 365 Jul 29 10:08
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Sync Extension Settings/oehoffnnkgcdacmbkhmlbjedinpampak/LOG.old
-rw-------@ 1 mac staff 0 Jul 29 10:07
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Download Service/EntryDB/LOG.old
-rw-------@ 1 mac staff 299 Jul 29 10:08
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Service Worker/Database/LOG.old
-rw-------@ 1 mac staff 291 Jul 29 10:25
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/File System/Origins/LOG.old
-rw-------@ 1 mac staff 0 Jul 29 10:07
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Feature Engagement Tracker/EventDB/LOG.old
-rw-------@ 1 mac staff 0 Jul 29 10:07
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Feature Engagement Tracker/AvailabilityDB/LOG.old
-rw-------@ 1 mac staff 283 Jul 29 10:07
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Extension State/LOG.old
-rw-------@ 1 mac staff 0 Jul 29 10:07
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/commerce_subscription_db/LOG.old
-rw-------@ 1 mac staff 0 Jul 29 10:07
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/BudgetDatabase/LOG.old
-rw-------@ 1 mac staff 0 Jul 29 10:07
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/optimization_guide_hint_cache_store/LOG.old
-rw-------@ 1 mac staff 283 Jul 29 10:07
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/shared_proto_db/LOG.old
-rw-------@ 1 mac staff 301 Jul 29 10:07
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/shared_proto_db/metadata/LOG.old
-rw-------@ 1 mac staff 0 Jul 29 10:07
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/optimization_guide_model_metadata_store/LOG.old
-rw-------@ 1 mac staff 367 Jul 29 10:08
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Local Extension Settings/gighmmpiobklfepjocnamgkkbiglidom/LOG.old
-rw-------@ 1 mac staff 367 Jul 29 10:08
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Local Extension Settings/kbfnbcaeplbcioakkpcpgfkobkghlhen/LOG.old
-rw-------@ 1 mac staff 9818 Jul 30 08:47
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Bookmarks.bak
-rw-------@ 1 mac staff 451 Jul 29 10:39
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Sync Data/LevelDB/LOG.old
-rw-------@ 1 mac staff 0 Jul 29 10:07
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/LOG.old
-rw-------@ 1 mac staff 786 Jul 29 10:43
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Local Storage/leveldb/LOG.old
-rw-------@ 1 mac staff 0 Jul 29 10:07
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Segmentation Platform/SegmentInfoDB/LOG.old
-rw-------@ 1 mac staff 0 Jul 29 10:07
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Segmentation Platform/SignalStorageConfigDB/LOG.old
-rw-------@ 1 mac staff 0 Jul 29 10:07
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Profile
1/Segmentation Platform/SignalDB/LOG.old
-rw-------@ 1 mac staff 320 Jul 29 10:09
/System/Volumes/Data/Users/mac/Library/Application
Support/Google/Chrome/Default/Session Storage/LOG.old
```

```
-rw-------@ 1 mac staff 448 Jul 29 10:09
/System/Volumes/Data/Users/mac/Library/Application Support/Google/Chrome/Default/I
ndexedDB/chrome-extension_cfhdojbkjhnklbpkdaibdccddilifddb_0.indexeddb.leveldb/LOG
.old
-rw-------@ 1 mac staff 330 Jul 29 10:09
/System/Volumes/Data/Users/mac/Library/Application
Support/Google/Chrome/Default/GCM Store/Encryption/LOG.old
-rw-------@ 1 mac staff 308 Jul 29 10:09
/System/Volumes/Data/Users/mac/Library/Application
Support/Google/Chrome/Default/GCM Store/LOG.old
```

## Searching tables inside readable .db/.sql/.sqlite files (limit 100)

```
Found /Users//mac/Library/Application Support/Animoji/CoreDataBackend/avatars.db:
SQLite 3.x database, last written using SQLite version 3039005, writer version 2,
read version 2, file counter 3, database pages 17, cookie 0xf, schema 4, largest
root page 17, UTF-8, vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Application Support/Code/databases/Databases.db: SQLite
3.x database, last written using SQLite version 3039004, file counter 1, database
pages 7, cookie 0x4, schema 4, UTF-8, version-valid-for 1
Found /Users//mac/Library/Application Support/Dock/desktoppicture.db: SQLite 3.x
database, last written using SQLite version 3024000, file counter 19, database
pages 13, cookie 0x10, schema 4, UTF-8, version-valid-for 19
Found /Users//mac/Library/Application
Support/Google/Chrome/Default/databases/Databases.db: SQLite 3.x database, last
written using SQLite version 3041002, file counter 1, database pages 7, cookie 0x4,
schema 4, UTF-8, version-valid-for 1
Found /Users//mac/Library/Application
Support/Google/Chrome/Default/heavy_ad_intervention_opt_out.db: SQLite 3.x
database, last written using SQLite version 3041002, file counter 2, database pages
4, cookie 0x2, schema 4, UTF-8, version-valid-for 2
Found /Users//mac/Library/Application Support/Google/Chrome/Profile
1/databases/Databases.db: SQLite 3.x database, last written using SQLite version
3041002, file counter 1, database pages 7, cookie 0x4, schema 4, UTF-8,
version-valid-for 1
Found /Users//mac/Library/Application Support/Google/Chrome/Profile
1/heavy_ad_intervention_opt_out.db: SQLite 3.x database, last written using SQLite
version 3041002, file counter 2, database pages 4, cookie 0x2, schema 4, UTF-8,
version-valid-for 2
Found /Users//mac/Library/Application Support/com.apple.ProtectedCloudStorage/Keys
SyncingVersion3-(null)-ProtectedCloudStorage.db: SQLite 3.x database, last written
using SQLite version 3024000, writer version 2, read version 2, file counter 2,
database pages 13, cookie 0x8, schema 4, UTF-8, version-valid-for 2
Found /Users//mac/Library/Application
Support/com.apple.ProtectedCloudStorage/PCSAnalytics.db: SQLite 3.x database, last
written using SQLite version 3024000, writer version 2, read version 2, file
counter 1, database pages 1, cookie 0, schema 0, unknown 0 encoding,
version-valid-for 1
Found /Users//mac/Library/Application
Support/com.apple.RemoteManagementAgent/Database/RemoteManagement.sqlite: SQLite
3.x database, last written using SQLite version 3039005, writer version 2, read
version 2, file counter 3, database pages 88, cookie 0x4d, schema 4, largest root
page 80, UTF-8, vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Application
Support/com.apple.transparencyd/TransparencyModel.sqlite: SQLite 3.x database, last
written using SQLite version 3039005, writer version 2, read version 2, file
counter 3, database pages 80, cookie 0x45, schema 4, largest root page 71, UTF-8,
vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Assistant/SiriAnalytics.db: SQLite 3.x database, last
written using SQLite version 3039005, writer version 2, read version 2, file
counter 65, database pages 212, 1st free page 44, free pages 4, cookie 0xf, schema
4, UTF-8, version-valid-for 65
Found /Users//mac/Library/Assistant/SiriReferenceResolution/rr.sqlite3: SQLite 3.x
database, user version 6, last written using SQLite version 3039005, file counter
3, database pages 3, cookie 0x1, schema 4, UTF-8, version-valid-for 3
Found /Users//mac/Library/Caches/GameKit/Data/com.apple.gamecenter/en-GB-global.gc
data/database.sqlite3: SQLite 3.x database, last written using SQLite version
3039005, writer version 2, read version 2, file counter 3, database pages 237,
cookie 0xcb, schema 4, largest root page 208, UTF-8, vacuum mode 1,
version-valid-for 3
Found /Users//mac/Library/Caches/GeoServices/ReqCount.db: SQLite 3.x database, last
```

```
written using SQLite version 3039005, writer version 2, read version 2, file
counter 2, database pages 1, cookie 0, schema 0, largest root page 1, unknown 0
encoding, version-valid-for 2
Found /Users//mac/Library/Caches/askpermissiond/Cache.db: SQLite 3.x database, user
version 203, last written using SQLite version 3039005, writer version 2, read
version 2, file counter 3, database pages 12, cookie 0x7, schema 4, largest root
page 12, UTF-8, vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Caches/com.apple.AppleMediaServices/Engagement/analytics
/app.db: SQLite 3.x database, user version 5, last written using SQLite version
3039005, writer version 2, read version 2, file counter 6, database pages 11,
cookie 0x7, schema 4, UTF-8, version-valid-for 6
Found /Users//mac/Library/Caches/com.apple.AppleMediaServices/Engagement/internal/
app.db: SQLite 3.x database, user version 5, last written using SQLite version
3039005, writer version 2, read version 2, file counter 7, database pages 16,
cookie 0x7, schema 4, UTF-8, version-valid-for 7
Found /Users//mac/Library/Caches/com.apple.AppleMediaServices/Engagement/journeys/
app.db: SQLite 3.x database, user version 5, last written using SQLite version
3039005, writer version 2, read version 2, file counter 11, database pages 101, 1st
free page 44, free pages 23, cookie 0x7, schema 4, UTF-8, version-valid-for 11
Found /Users//mac/Library/Caches/com.apple.AppleMediaServices/Engagement/recommend
ations/app.db: SQLite 3.x database, user version 5, last written using SQLite
version 3039005, writer version 2, read version 2, file counter 2, database pages
8, cookie 0x7, schema 4, UTF-8, version-valid-for 2
Found /Users//mac/Library/Caches/com.apple.InstallAssistant.macOSVentura/Cache.db:
SQLite 3.x database, last written using SQLite version 3024000, writer version 2,
read version 2, file counter 3, database pages 13, cookie 0x8, schema 4, largest
root page 13, UTF-8, vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Caches/com.apple.Music/Cache.db: SQLite 3.x database,
user version 203, last written using SQLite version 3039005, writer version 2, read
version 2, file counter 3, database pages 12, cookie 0x7, schema 4, largest root
page 12, UTF-8, vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Caches/com.apple.NewDeviceOutreach/Cache.db: SQLite 3.x
database, user version 203, last written using SQLite version 3039005, writer
version 2, read version 2, file counter 3, database pages 12, cookie 0x7, schema 4,
largest root page 12, UTF-8, vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Caches/com.apple.Spotlight/Cache.db: SQLite 3.x database,
user version 203, last written using SQLite version 3039005, writer version 2, read
version 2, file counter 4, database pages 13, 1st free page 13, free pages 1,
cookie 0x13, schema 4, largest root page 12, UTF-8, vacuum mode 1,
version-valid-for 4
Found /Users//mac/Library/Caches/com.apple.SystemProfiler/Cache.db: SQLite 3.x
database, user version 203, last written using SQLite version 3039005, writer
version 2, read version 2, file counter 4, database pages 13, 1st free page 13,
free pages 1, cookie 0x13, schema 4, largest root page 12, UTF-8, vacuum mode 1,
version-valid-for 4
Found /Users//mac/Library/Caches/com.apple.TV/Cache.db: SQLite 3.x database, user
version 203, last written using SQLite version 3039005, writer version 2, read
version 2, file counter 3, database pages 12, cookie 0x7, schema 4, largest root
page 12, UTF-8, vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Caches/com.apple.WalletSettingsExtension/Cache.db: SQLite
3.x database, user version 203, last written using SQLite version 3039005, writer
version 2, read version 2, file counter 3, database pages 12, cookie 0x7, schema 4,
largest root page 12, UTF-8, vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Caches/com.apple.akd/Cache.db: SQLite 3.x database, last
written using SQLite version 3039005, writer version 2, read version 2, file
counter 2, database pages 1, cookie 0, schema 0, largest root page 1, unknown 0
encoding, vacuum mode 1, version-valid-for 2
Found /Users//mac/Library/Caches/com.apple.amsaccountsd/Cache.db: SQLite 3.x
database, user version 203, last written using SQLite version 3039005, writer
version 2, read version 2, file counter 3, database pages 12, cookie 0x7, schema 4,
largest root page 12, UTF-8, vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Caches/com.apple.appstore/CommerceRequestCache/Cache.db:
SQLite 3.x database, last written using SQLite version 3024000, writer version 2,
read version 2, file counter 11, database pages 19, 1st free page 19, free pages 2,
cookie 0x8, schema 4, largest root page 13, UTF-8, vacuum mode 1, version-valid-for
11
Found /Users//mac/Library/Caches/com.apple.appstoreagent/Cache.db: SQLite 3.x
database, user version 203, last written using SQLite version 3039005, writer
version 2, read version 2, file counter 7, database pages 15, 1st free page 15,
free pages 3, cookie 0x13, schema 4, largest root page 12, UTF-8, vacuum mode 1,
version-valid-for 7
Found /Users//mac/Library/Caches/com.apple.appstoreagent/storeSystem.db: SQLite 3.x
database, last written using SQLite version 3039005, writer version 2, read version
2, file counter 1, database pages 1, cookie 0, schema 0, unknown 0 encoding,
version-valid-for 1
Found /Users//mac/Library/Caches/com.apple.appstoreagent/storeUser.db: data
Found /Users//mac/Library/Caches/com.apple.assistant_service/Cache.db: SQLite 3.x
database, user version 203, last written using SQLite version 3039005, writer
version 2, read version 2, file counter 3, database pages 12, cookie 0x7, schema 4,
```

```
largest root page 12, UTF-8, vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Caches/com.apple.dataaccess.dataaccessd/Cache.db: SQLite
3.x database, last written using SQLite version 3039005, writer version 2, read
version 2, file counter 2, database pages 1, cookie 0, schema 0, largest root page
1, unknown 0 encoding, vacuum mode 1, version-valid-for 2
Found /Users//mac/Library/Caches/com.apple.feedbacklogger/com.apple.assistantd/dat
a.sqlite: SQLite 3.x database, user version 6, last written using SQLite version
3039005, writer version 2, read version 2, file counter 36, database pages 30,
cookie 0x3, schema 4, UTF-8, version-valid-for 36
Found /Users//mac/Library/Caches/com.apple.feedbacklogger/com.apple.proactive.even
ttracker/data.sqlite: SQLite 3.x database, user version 6, last written using
SQLite version 3039005, writer version 2, read version 2, file counter 3, database
pages 9, 1st free page 8, free pages 3, cookie 0x3, schema 4, UTF-8,
version-valid-for 3
Found /Users//mac/Library/Caches/com.apple.helpd/Cache.db: SQLite 3.x database,
user version 203, last written using SQLite version 3039005, writer version 2, read
version 2, file counter 6, database pages 133, cookie 0x13, schema 4, largest root
page 12, UTF-8, vacuum mode 1, version-valid-for 6
Found /Users//mac/Library/Caches/com.apple.helpd/index.spotlightV3/.store.db: data
Found /Users//mac/Library/Caches/com.apple.helpd/index.spotlightV3/store.db: data
Found /Users//mac/Library/Caches/com.apple.iCloudHelper/Cache.db: SQLite 3.x
database, last written using SQLite version 3024000, writer version 2, read version
2, file counter 3, database pages 13, cookie 0x8, schema 4, largest root page 13,
UTF-8, vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Caches/com.apple.iCloudNotificationAgent/Cache.db: SQLite
3.x database, user version 203, last written using SQLite version 3039005, writer
version 2, read version 2, file counter 3, database pages 12, cookie 0x7, schema 4,
largest root page 12, UTF-8, vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Caches/com.apple.iTunes/CommerceRequestCache/Cache.db:
SQLite 3.x database, user version 203, last written using SQLite version 3039005,
writer version 2, read version 2, file counter 3, database pages 12, cookie 0x7,
schema 4, largest root page 12, UTF-8, vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Caches/com.apple.icloud.fmfd/Cache.db: SQLite 3.x
database, last written using SQLite version 3039005, writer version 2, read version
2, file counter 2, database pages 1, cookie 0, schema 0, largest root page 1,
unknown 0 encoding, vacuum mode 1, version-valid-for 2
Found /Users//mac/Library/Caches/com.apple.imfoundation.IMRemoteURLConnectionAgent
/Cache.db: SQLite 3.x database, last written using SQLite version 3024000, writer
version 2, read version 2, file counter 3, database pages 13, cookie 0x8, schema 4,
largest root page 13, UTF-8, vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Caches/com.apple.installer.osinstallersetupd/Cache.db:
SQLite 3.x database, last written using SQLite version 3024000, writer version 2,
read version 2, file counter 5, database pages 1139, cookie 0x8, schema 4, largest
root page 13, UTF-8, vacuum mode 1, version-valid-for 5
Found /Users//mac/Library/Caches/com.apple.itunescloudd/Cache.db: SQLite 3.x
database, user version 203, last written using SQLite version 3039005, writer
version 2, read version 2, file counter 3, database pages 12, cookie 0x7, schema 4,
largest root page 12, UTF-8, vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Caches/com.apple.keyboardservicesd/Cache.db: SQLite 3.x
database, last written using SQLite version 3024000, writer version 2, read version
2, file counter 3, database pages 13, cookie 0x8, schema 4, largest root page 13,
UTF-8, vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Caches/com.apple.nbagent/Cache.db: SQLite 3.x database,
user version 203, last written using SQLite version 3039005, writer version 2, read
version 2, file counter 5, database pages 17, 1st free page 13, free pages 5,
cookie 0x13, schema 4, largest root page 12, UTF-8, vacuum mode 1,
version-valid-for 5
Found /Users//mac/Library/Caches/com.apple.parsecd/Cohorts/cohorts.sqlite: SQLite
3.x database, last written using SQLite version 3039005, writer version 2, read
version 2, file counter 10, database pages 12, cookie 0x16, schema 4, largest root
page 11, UTF-8, vacuum mode 1, version-valid-for 10
Found /Users//mac/Library/Caches/com.apple.parsecd/EngagedCompletions/Cache.db:
SQLite 3.x database, last written using SQLite version 3039005, file counter 8,
database pages 6, cookie 0xa, schema 4, largest root page 6, UTF-8, vacuum mode 1,
version-valid-for 8
Found /Users//mac/Library/Caches/com.apple.passd/Cache.db: SQLite 3.x database,
user version 203, last written using SQLite version 3039005, writer version 2, read
version 2, file counter 4, database pages 13, 1st free page 13, free pages 1,
cookie 0x13, schema 4, largest root page 12, UTF-8, vacuum mode 1,
version-valid-for 4
Found /Users//mac/Library/Caches/com.apple.remindd/Cache.db: SQLite 3.x database,
last written using SQLite version 3039005, writer version 2, read version 2, file
counter 2, database pages 1, cookie 0, schema 0, largest root page 1, unknown 0
encoding, vacuum mode 1, version-valid-for 2
Found /Users//mac/Library/Caches/com.apple.tipsd/Cache.db: SQLite 3.x database,
user version 203, last written using SQLite version 3039005, writer version 2, read
version 2, file counter 3, database pages 12, cookie 0x7, schema 4, largest root
page 12, UTF-8, vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Caches/com.apple.touristd/Cache.db: SQLite 3.x database,
```

```
last written using SQLite version 3024000, writer version 2, read version 2, file
counter 4, database pages 26, cookie 0x8, schema 4, largest root page 13, UTF-8,
vacuum mode 1, version-valid-for 4
Found /Users//mac/Library/Caches/com.apple.translationd/Cache.db: SQLite 3.x
database, user version 203, last written using SQLite version 3039005, writer
version 2, read version 2, file counter 4, database pages 14, cookie 0x7, schema 4,
largest root page 12, UTF-8, vacuum mode 1, version-valid-for 4
Found /Users//mac/Library/Caches/com.google.Keystone/Cache.db: SQLite 3.x database,
user version 203, last written using SQLite version 3039005, writer version 2, read
version 2, file counter 3, database pages 12, cookie 0x7, schema 4, largest root
page 12, UTF-8, vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Caches/com.microsoft.VSCode/Cache.db: SQLite 3.x
database, user version 203, last written using SQLite version 3039005, writer
version 2, read version 2, file counter 3, database pages 12, cookie 0x7, schema 4,
largest root page 12, UTF-8, vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Caches/familycircled/Cache.db: SQLite 3.x database, user
version 203, last written using SQLite version 3039005, writer version 2, read
version 2, file counter 3, database pages 12, cookie 0x7, schema 4, largest root
page 12, UTF-8, vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Caches/storeassetd/Cache.db: SQLite 3.x database, last
written using SQLite version 3024000, writer version 2, read version 2, file
counter 7, database pages 15, 1st free page 14, free pages 1, cookie 0x8, schema 4,
largest root page 13, UTF-8, vacuum mode 1, version-valid-for 7
Found /Users//mac/Library/Caches/storedownloadd/Cache.db: SQLite 3.x database, last
written using SQLite version 3024000, writer version 2, read version 2, file
counter 3, database pages 13, cookie 0x8, schema 4, largest root page 13, UTF-8,
vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Containers/com.apple.AMPArtworkAgent/Data/Documents/artw
orkd.sqlite: SQLite 3.x database, last written using SQLite version 3039005, writer
version 2, read version 2, file counter 3, database pages 23, cookie 0x14, schema
4, largest root page 22, UTF-8, vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Containers/com.apple.AppStore/Data/Library/Caches/com.ap
ple.AppStore/Cache.db: SQLite 3.x database, user version 203, last written using
SQLite version 3039005, writer version 2, read version 2, file counter 4, database
pages 70, cookie 0x7, schema 4, largest root page 12, UTF-8, vacuum mode 1,
version-valid-for 4
Found /Users//mac/Library/Containers/com.apple.AppStore/Data/Library/HTTPStorages/
com.apple.AppStore/httpstorages.sqlite: SQLite 3.x database, last written using
SQLite version 3039005, writer version 2, read version 2, file counter 3, database
pages 4, cookie 0x1, schema 4, largest root page 4, UTF-8, vacuum mode 1,
version-valid-for 3
Found /Users//mac/Library/Containers/com.apple.FaceTime/Data/Library/Caches/com.ap
ple.FaceTime/Cache.db: SQLite 3.x database, last written using SQLite version
3024000, writer version 2, read version 2, file counter 3, database pages 13,
cookie 0x8, schema 4, largest root page 13, UTF-8, vacuum mode 1, version-valid-for
3
Found /Users//mac/Library/Containers/com.apple.Notes.IntentsExtension/Data/Library
/Caches/com.apple.Notes.IntentsExtension/Cache.db: SQLite 3.x database, user
version 203, last written using SQLite version 3039005, writer version 2, read
version 2, file counter 3, database pages 12, cookie 0x7, schema 4, largest root
page 12, UTF-8, vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Containers/com.apple.Notes.IntentsExtension/Data/Library
/HTTPStorages/com.apple.Notes.IntentsExtension/httpstorages.sqlite: SQLite 3.x
database, last written using SQLite version 3039005, writer version 2, read version
2, file counter 2, database pages 1, cookie 0, schema 0, largest root page 1,
unknown 0 encoding, vacuum mode 1, version-valid-for 2
Found /Users//mac/Library/Containers/com.apple.UsageTrackingAgent/Data/Library/App
lication Support/UsageTrackingAgent/UsageTracking.sqlite: SQLite 3.x database, last
written using SQLite version 3039005, writer version 2, read version 2, file
counter 4, database pages 33, cookie 0x1c, schema 4, largest root page 30, UTF-8,
vacuum mode 1, version-valid-for 4
Found /Users//mac/Library/Containers/com.apple.findmy.FindMyWidgetIntentsPeople/Da
ta/Library/HTTPStorages/com.apple.findmy.FindMyWidgetIntentsPeople/httpstorages.sq
lite: SQLite 3.x database, last written using SQLite version 3039005, writer
version 2, read version 2, file counter 3, database pages 4, cookie 0x1, schema 4,
largest root page 4, UTF-8, vacuum mode 1, version-valid-for 3
Found /Users//mac/Library/Containers/com.apple.freeform/Data/Library/Caches/com.ap
ple.freeform/Cache.db: SQLite 3.x database, user version 203, last written using
SQLite version 3039005, writer version 2, read version 2, file counter 3, database
pages 12, cookie 0x7, schema 4, largest root page 12, UTF-8, vacuum mode 1,
version-valid-for 3
-> Extracting tables from /Users//mac/Library/Assistant/SiriAnalytics.db (limit 20)
-> Extracting tables from
/Users//mac/Library/Assistant/SiriReferenceResolution/rr.sqlite3 (limit 20)
-> Extracting tables from /Users//mac/Library/Caches/GameKit/Data/com.apple.gamece
nter/en-GB-global.gcdata/database.sqlite3 (limit 20)
-> Extracting tables from /Users//mac/Library/Caches/askpermissiond/Cache.db (limit
20)
-> Extracting tables from /Users//mac/Library/Caches/com.apple.AppleMediaServices/
```

```
Engagement/analytics/app.db (limit 20)
-> Extracting tables from
/Users//mac/Library/Caches/com.apple.AppleMediaServices/Engagement/internal/app.db
(limit 20)
-> Extracting tables from
/Users//mac/Library/Caches/com.apple.AppleMediaServices/Engagement/journeys/app.db
(limit 20)
-> Extracting tables from /Users//mac/Library/Caches/com.apple.AppleMediaServices/
Engagement/recommendations/app.db (limit 20)
-> Extracting tables from
/Users//mac/Library/Caches/com.apple.InstallAssistant.macOSVentura/Cache.db (limit
20)
-> Extracting tables from /Users//mac/Library/Caches/com.apple.Music/Cache.db
(limit 20)
-> Extracting tables from
/Users//mac/Library/Caches/com.apple.NewDeviceOutreach/Cache.db (limit 20)
-> Extracting tables from /Users//mac/Library/Caches/com.apple.Spotlight/Cache.db
(limit 20)
-> Extracting tables from
/Users//mac/Library/Caches/com.apple.SystemProfiler/Cache.db (limit 20)
-> Extracting tables from /Users//mac/Library/Caches/com.apple.TV/Cache.db (limit
20)
-> Extracting tables from
/Users//mac/Library/Caches/com.apple.WalletSettingsExtension/Cache.db (limit 20)
-> Extracting tables from /Users//mac/Library/Caches/com.apple.akd/Cache.db (limit
20)
-> Extracting tables from
/Users//mac/Library/Caches/com.apple.amsaccountsd/Cache.db (limit 20)
-> Extracting tables from
/Users//mac/Library/Caches/com.apple.appstore/CommerceRequestCache/Cache.db (limit
20)
-> Extracting tables from
/Users//mac/Library/Caches/com.apple.appstoreagent/Cache.db (limit 20)
-> Extracting tables from
/Users//mac/Library/Caches/com.apple.appstoreagent/storeSystem.db (limit 20)
-> Extracting tables from
/Users//mac/Library/Caches/com.apple.assistant_service/Cache.db (limit 20)
-> Extracting tables from
/Users//mac/Library/Caches/com.apple.dataaccess.dataaccessd/Cache.db (limit 20)
-> Extracting tables from /Users//mac/Library/Caches/com.apple.feedbacklogger/com.
apple.assistantd/data.sqlite (limit 20)
-> Extracting tables from /Users//mac/Library/Caches/com.apple.feedbacklogger/com.
apple.proactive.eventtracker/data.sqlite (limit 20)
-> Extracting tables from /Users//mac/Library/Caches/com.apple.helpd/Cache.db
(limit 20)
-> Extracting tables from
/Users//mac/Library/Caches/com.apple.iCloudHelper/Cache.db (limit 20)
-> Extracting tables from
/Users//mac/Library/Caches/com.apple.iCloudNotificationAgent/Cache.db (limit 20)
-> Extracting tables from
/Users//mac/Library/Caches/com.apple.iTunes/CommerceRequestCache/Cache.db (limit
20)
-> Extracting tables from /Users//mac/Library/Caches/com.apple.icloud.fmfd/Cache.db
(limit 20)
-> Extracting tables from /Users//mac/Library/Caches/com.apple.imfoundation.IMRemo
teURLConnectionAgent/Cache.db (limit 20)
-> Extracting tables from
/Users//mac/Library/Caches/com.apple.installer.osinstallersetupd/Cache.db (limit
20)
-> Extracting tables from
/Users//mac/Library/Caches/com.apple.itunescloudd/Cache.db (limit 20)
-> Extracting tables from
/Users//mac/Library/Caches/com.apple.keyboardservicesd/Cache.db (limit 20)
-> Extracting tables from /Users//mac/Library/Caches/com.apple.nbagent/Cache.db
(limit 20)
-> Extracting tables from
/Users//mac/Library/Caches/com.apple.parsecd/Cohorts/cohorts.sqlite (limit 20)
-> Extracting tables from
/Users//mac/Library/Caches/com.apple.parsecd/EngagedCompletions/Cache.db (limit 20)
-> Extracting tables from /Users//mac/Library/Caches/com.apple.passd/Cache.db
(limit 20)
-> Extracting tables from /Users//mac/Library/Caches/com.apple.remindd/Cache.db
(limit 20)
-> Extracting tables from /Users//mac/Library/Caches/com.apple.tipsd/Cache.db
(limit 20)
-> Extracting tables from /Users//mac/Library/Caches/com.apple.touristd/Cache.db
(limit 20)
-> Extracting tables from
/Users//mac/Library/Caches/com.apple.translationd/Cache.db (limit 20)
```

```
-> Extracting tables from /Users//mac/Library/Caches/com.google.Keystone/Cache.db
(limit 20)
-> Extracting tables from /Users//mac/Library/Caches/com.microsoft.VSCode/Cache.db
(limit 20)
-> Extracting tables from /Users//mac/Library/Caches/familycircled/Cache.db (limit
20)
-> Extracting tables from /Users//mac/Library/Caches/storeassetd/Cache.db (limit
20)
-> Extracting tables from /Users//mac/Library/Caches/storedownloadd/Cache.db (limit
20)
-> Extracting tables from /Users//mac/Library/Containers/com.apple.AMPArtworkAgent
/Data/Documents/artworkd.sqlite (limit 20)
-> Extracting tables from /Users//mac/Library/Containers/com.apple.AppStore/Data/L
ibrary/Caches/com.apple.AppStore/Cache.db (limit 20)
-> Extracting tables from /Users//mac/Library/Containers/com.apple.AppStore/Data/L
ibrary/HTTPStorages/com.apple.AppStore/httpstorages.sqlite (limit 20)
-> Extracting tables from /Users//mac/Library/Containers/com.apple.FaceTime/Data/L
ibrary/Caches/com.apple.FaceTime/Cache.db (limit 20)
-> Extracting tables from /Users//mac/Library/Containers/com.apple.Notes.IntentsEx
tension/Data/Library/Caches/com.apple.Notes.IntentsExtension/Cache.db (limit 20)
-> Extracting tables from /Users//mac/Library/Containers/com.apple.Notes.IntentsEx
tension/Data/Library/HTTPStorages/com.apple.Notes.IntentsExtension/httpstorages.sq
lite (limit 20)
-> Extracting tables from /Users//mac/Library/Containers/com.apple.findmy.FindMyWi
dgetIntentsPeople/Data/Library/HTTPStorages/com.apple.findmy.FindMyWidgetIntentsPe
ople/httpstorages.sqlite (limit 20)
-> Extracting tables from /Users//mac/Library/Containers/com.apple.freeform/Data/L
ibrary/Caches/com.apple.freeform/Cache.db (limit 20)
```

## All relevant hidden files (not in /sys/ or the ones listed in the previous check) (limit 70)

```
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /usr/standalone/firmware/.tempfile
---------- 1 root admin 0 Jun 15 15:38 /.file
-rw-r--r-- 1 root wheel 276 Jul 12 19:31
/Library/Preferences/.GlobalPreferences.plist
-r--r--r-- 1 root wheel 0 Jun 17 18:08 /Library/Keychains/.fl947E1BDB
-r--r--r--@ 1 root wheel 0 Jun 17 18:08 /Library/Keychains/.fl043D1EDD
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/.localized
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/Compositions/.localized
-rwxr-xr-x 1 root wheel 2 Jun 15 15:38 /Library/KernelCollections/.file
-rw-r--r-- 1 root wheel 3 Jun 15 15:38 /Library/User
Template/he.lproj/.CFUserTextEncoding
-rw-r--r-- 1 root wheel 360 Jun 15 15:38 /Library/User
Template/he.lproj/Library/Preferences/.GlobalPreferences.plist
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/he.lproj/Library/.localized
-rw-r--r-- 1 root wheel 4 Jun 15 15:38 /Library/User
Template/en_AU.lproj/.CFUserTextEncoding
-rw-r--r-- 1 root wheel 320 Jun 15 15:38 /Library/User
Template/en_AU.lproj/Library/Preferences/.GlobalPreferences.plist
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/en_AU.lproj/Library/.localized
-rw-r--r-- 1 root wheel 3 Jun 15 15:38 /Library/User
Template/ar.lproj/.CFUserTextEncoding
-rw-r--r-- 1 root wheel 462 Jun 15 15:38 /Library/User
Template/ar.lproj/Library/Preferences/.GlobalPreferences.plist
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/ar.lproj/Library/.localized
-rw-r--r-- 1 root wheel 3 Jun 15 15:38 /Library/User
Template/el.lproj/.CFUserTextEncoding
-rw-r--r-- 1 root wheel 317 Jun 15 15:38 /Library/User
Template/el.lproj/Library/Preferences/.GlobalPreferences.plist
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/el.lproj/Library/.localized
-rw-r--r-- 1 root wheel 4 Jun 15 15:38 /Library/User
Template/uk.lproj/.CFUserTextEncoding
-rw-r--r-- 1 root wheel 317 Jun 15 15:38 /Library/User
Template/uk.lproj/Library/Preferences/.GlobalPreferences.plist
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/uk.lproj/Library/.localized
-rw-r--r-- 1 root wheel 3 Jun 15 15:38 /Library/User
```

```
Template/English.lproj/.CFUserTextEncoding
-rw-r--r-- 1 root wheel 249 Jun 15 15:38 /Library/User
Template/English.lproj/Library/Preferences/.GlobalPreferences.plist
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/English.lproj/Library/.localized
-rw-r--r-- 1 root wheel 4 Jun 15 15:38 /Library/User
Template/es_419.lproj/.CFUserTextEncoding
-rw-r--r-- 1 root wheel 321 Jun 15 15:38 /Library/User
Template/es_419.lproj/Library/Preferences/.GlobalPreferences.plist
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/es_419.lproj/Library/.localized
-rw-r--r-- 1 root wheel 5 Jun 15 15:38 /Library/User
Template/zh_CN.lproj/.CFUserTextEncoding
-rw-r--r-- 1 root wheel 322 Jun 15 15:38 /Library/User
Template/zh_CN.lproj/Library/Preferences/.GlobalPreferences.plist
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/zh_CN.lproj/Library/.localized
-rw-r--r-- 1 root wheel 3 Jun 15 15:38 /Library/User
Template/Dutch.lproj/.CFUserTextEncoding
-rw-r--r-- 1 root wheel 249 Jun 15 15:38 /Library/User
Template/Dutch.lproj/Library/Preferences/.GlobalPreferences.plist
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/Dutch.lproj/Library/.localized
-rw-r--r-- 1 root wheel 4 Jun 15 15:38 /Library/User
Template/da.lproj/.CFUserTextEncoding
-rw-r--r-- 1 root wheel 317 Jun 15 15:38 /Library/User
Template/da.lproj/Library/Preferences/.GlobalPreferences.plist
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/da.lproj/Library/.localized
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/Non_localized/Music/.localized
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/Non_localized/Pictures/.localized
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/Non_localized/Desktop/.localized
-rw-r--r-- 1 root wheel 79 Jun 15 15:38 /Library/User
Template/Non_localized/Library/Preferences/.GlobalPreferences.plist
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/Non_localized/Library/Compositions/.localized
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/Non_localized/Library/Favorites/.localized
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/Non_localized/Library/Input Methods/.localized
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/Non_localized/Public/.localized
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/Non_localized/Public/Drop Box/.localized
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/Non_localized/Movies/.localized
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/Non_localized/Documents/.localized
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/Non_localized/Downloads/.localized
-rw-r--r-- 1 root wheel 5 Jun 15 15:38 /Library/User
Template/sk.lproj/.CFUserTextEncoding
-rw-r--r-- 1 root wheel 317 Jun 15 15:38 /Library/User
Template/sk.lproj/Library/Preferences/.GlobalPreferences.plist
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/sk.lproj/Library/.localized
-rw-r--r-- 1 root wheel 4 Jun 15 15:38 /Library/User
Template/pt_PT.lproj/.CFUserTextEncoding
-rw-r--r-- 1 root wheel 320 Jun 15 15:38 /Library/User
Template/pt_PT.lproj/Library/Preferences/.GlobalPreferences.plist
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/pt_PT.lproj/Library/.localized
-rw-r--r-- 1 root wheel 3 Jun 15 15:38 /Library/User
Template/German.lproj/.CFUserTextEncoding
-rw-r--r-- 1 root wheel 317 Jun 15 15:38 /Library/User
Template/German.lproj/Library/Preferences/.GlobalPreferences.plist
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/German.lproj/Library/.localized
-rw-r--r-- 1 root wheel 3 Jun 15 15:38 /Library/User
Template/ms.lproj/.CFUserTextEncoding
-rw-r--r-- 1 root wheel 317 Jun 15 15:38 /Library/User
Template/ms.lproj/Library/Preferences/.GlobalPreferences.plist
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/ms.lproj/Library/.localized
-rw-r--r-- 1 root wheel 4 Jun 15 15:38 /Library/User
Template/sv.lproj/.CFUserTextEncoding
```

```
-rw-r--r-- 1 root wheel 317 Jun 15 15:38 /Library/User
Template/sv.lproj/Library/Preferences/.GlobalPreferences.plist
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/sv.lproj/Library/.localized
-rw-r--r-- 1 root wheel 5 Jun 15 15:38 /Library/User
Template/cs.lproj/.CFUserTextEncoding
-rw-r--r-- 1 root wheel 317 Jun 15 15:38 /Library/User
Template/cs.lproj/Library/Preferences/.GlobalPreferences.plist
-rw-r--r-- 1 root wheel 0 Jun 15 15:38 /Library/User
Template/cs.lproj/Library/.localized
-rw-r--r-- 1 root wheel 4 Jun 15 15:38 /Library/User
Template/ko.lproj/.CFUserTextEncoding
-rw-r--r-- 1 root wheel 317 Jun 15 15:38 /Library/User
Template/ko.lproj/Library/Preferences/.GlobalPreferences.plist
```

## Readable files inside /tmp, /var/tmp, /private/tmp, /private/var/at/tmp, /private/var/tmp, and backup folders (limit 70)

```
-rw-r--r-- 1 mac wheel 13 Jul 30 17:32 /var/tmp/siriBC
-rw-r--r--@ 1 mac wheel 0 Jul 29 10:04
/private/tmp/com.google.Keystone/.keystone_system_install_lock
-rw-rw-rw-@ 1 mac wheel 0 Jul 29 10:04
/private/tmp/com.google.Keystone/.keystone_install_lock
-rw-r--r-- 1 mac wheel 0 Jul 29 10:21
/private/tmp/.com.apple.dt.CommandLineTools.installondemand.in-progress
-rw-r--r--@ 1 mac wheel 3717357 Jul 29 10:05
/private/tmp/KSDownloadAction.EY52FfyjgL/com.google.Keystone.dmg
-rw-r--r-- 1 mac wheel 13 Jul 30 17:32 /private/var/tmp/siriBC
```

## Searching passwords in history files

```
Binary file /usr/bin/malloc_history matches
'\" Generated from file '/AppleInternal/Library/BuildRoots/c2cb9645-dafc-11ed-aa26
-6ec1e3b3f7b3/Library/Caches/com.apple.xbs/Sources/tcl/tcl_ext/tklib/tklib/modules
/history/tklib_history.man' by tcllib/doctools with format 'nroff'
'\" RCS: @(#) $Id: man.macros,v 1.1 2009/01/30 04:56:47 andreas_kupries Exp $
SUFFIX="$SUFFIX$ISUFFIX"
_history_complete_word "$@"
"r:root - strip suffix"
```

## Searching *password* or *credential* files in home (limit 70)

```
/Users//mac/.vscode/extensions/ms-python.python-2023.12.0/pythonFiles/lib/jedilsp/
jedi/third_party/django-stubs/django-stubs/contrib/auth/management/commands/change
password.pyi
/Users//mac/.vscode/extensions/ms-python.python-2023.12.0/pythonFiles/lib/jedilsp/
jedi/third_party/django-stubs/django-stubs/contrib/auth/password_validation.pyi
/Users//mac/.vscode/extensions/ms-python.vscode-pylance-2023.7.40/dist/bundled/stu
bs/django-stubs/contrib/auth/management/commands/changepassword.pyi
/Users//mac/.vscode/extensions/ms-python.vscode-pylance-2023.7.40/dist/bundled/stu
bs/django-stubs/contrib/auth/password_validation.pyi
/Users//mac/.vscode/extensions/ms-python.vscode-pylance-2023.7.40/dist/typeshed-fa
llback/stubs/braintree/braintree/credentials_parser.pyi
/Users//mac/.vscode/extensions/ms-python.vscode-pylance-2023.7.40/dist/typeshed-fa
llback/stubs/braintree/braintree/oauth_credentials.pyi
/Users//mac/.vscode/extensions/ms-python.vscode-pylance-2023.7.40/dist/typeshed-fa
llback/stubs/influxdb-client/influxdb_client/domain/password_reset_body.pyi
/Users//mac/.vscode/extensions/ms-python.vscode-pylance-2023.7.40/dist/typeshed-fa
llback/stubs/oauthlib/oauthlib/oauth2/rfc6749/grant_types/client_credentials.pyi
/Users//mac/.vscode/extensions/ms-python.vscode-pylance-2023.7.40/dist/typeshed-fa
llback/stubs/oauthlib/oauthlib/oauth2/rfc6749/grant_types/resource_owner_password_
```

```
credentials.pyi
/Users//mac/.vscode/extensions/ms-python.vscode-pylance-2023.7.40/dist/typeshed-fa
llback/stubs/pika/pika/credentials.pyi
/Users//mac/.vscode/extensions/ms-python.vscode-pylance-2023.7.40/dist/typeshed-fa
llback/stubs/redis/redis/credentials.pyi
/Users//mac/Library/Application Support/Google/Chrome/ZxcvbnData/3/passwords.txt
/private/var/db/heim-credential-store.archive
/usr/libexec/postfix/set_credentials.sh
/usr/sbin/unsetpassword
/usr/share/cups/ipptool/print-job-password.test
/usr/standalone/i386/EfiLoginUI/disk_passwordUI.efires
```

### Searching passwords inside logs (limit 70)

```
/private/var/log/asl/AUX.2023.07.30/500: autoFillInteractionType:
EDITED_TEXT_IN_PASSWORD_FIELD
/private/var/log/asl/AUX.2023.07.30/500: safariParticipatedInPasswordAutoFill {
/private/var/log/com.apple.xpc.launchd/launchd.log.2:2023-07-29 09:58:21.690637
(pid/799 [PasswordBreachA]) <Notice>: uncorking exec source upfront
/private/var/log/com.apple.xpc.launchd/launchd.log.2:2023-07-29 09:58:21.690667
(pid/799 [PasswordBreachA]) <Notice>: created
/private/var/log/install.log: "dsAttrTypeNative:_writers_passwd" = (
/private/var/log/install.log: "dsAttrTypeStandard:Password" = (
/private/var/log/install.log:2023-06-17 12:22:53+00 MacBook-Pro
InstallAssistant[612]: Env: PWD=/
/private/var/log/install.log:Jul 12 13:05:20 MacBook-Pro OSInstaller[604]: Env:
PWD=/
/private/var/log/install.log:Jun 17 12:29:39 MacBook-Pro OSInstaller[601]: Env:
PWD=/
/var/log//asl/AUX.2023.07.30/500: autoFillInteractionType:
EDITED_TEXT_IN_PASSWORD_FIELD
/var/log//asl/AUX.2023.07.30/500: safariParticipatedInPasswordAutoFill {
/var/log//com.apple.xpc.launchd/launchd.log.2:2023-07-29 09:58:21.690637 (pid/799
[PasswordBreachA]) <Notice>: uncorking exec source upfront
/var/log//com.apple.xpc.launchd/launchd.log.2:2023-07-29 09:58:21.690667 (pid/799
[PasswordBreachA]) <Notice>: created
/var/log//install.log: "dsAttrTypeNative:_writers_passwd" = (
/var/log//install.log: "dsAttrTypeStandard:Password" = (
/var/log//install.log:2023-06-17 12:22:53+00 MacBook-Pro InstallAssistant[612]:
Env: PWD=/
/var/log//install.log:Jul 12 13:05:20 MacBook-Pro OSInstaller[604]: Env: PWD=/
/var/log//install.log:Jul 12 13:59:55 MacBook-Pro opendirectoryd[64]: [default] Set
passwd in users/<private> (18A223F3-2113-4303-B270-D719FB6AA686)
/var/log//install.log:Jul 12 13:59:56 MacBook-Pro opendirectoryd[64]: [default] Set
passwd in users/<private> (FFFFEEEE-DDDD-CCCC-BBBB-AAAA000000F3)
/var/log//install.log:Jul 12 14:00:05 MacBook-Pro opendirectoryd[64]: [default] Set
passwd in groups/<private> (ABCDEFAB-CDEF-ABCD-EFAB-CDEF000000F3)
/var/log//install.log:Jun 17 12:29:39 MacBook-Pro OSInstaller[601]: Env: PWD=/
```

# API Keys Regex

```
Regexes to search for API keys aren't activated, use param '-r'
```