Hacked

Sunday, 3 April, 2022 1:20 PM

1. What is the system timezone?

```
maman@ubuntu:/mnt/case1$ cat etc/timezone
Europe/Brussels
maman@ubuntu:/mnt/case1$
```

2. Who was the last user to log in to the system? mail

```
maman@ubuntu:/mnt/case1/var/log$ utmpdump wtmp | tail -f
Utmp dump of wtmp
[6] [00995] [6   ] [LOGIN   ] [tty6        ] [                ] [0.0.0.0        ] [2019-10-05T09:41:55,000000+00:00]
[6] [01411] [1   ] [LOGIN   ] [tty1        ] [                ] [0.0.0.0        ] [2019-10-05T09:41:59,000000+00:00]
[7] [02624] [ts/1] [mail    ] [pts/1       ] [192.168.210.131 ] [192.168.210.131] [2019-10-05T11:13:53,375084+00:00]
[8] [02624] [    ] [        ] [pts/1       ] [                ] [0.0.0.0        ] [2019-10-05T11:18:48,043528+00:00]
[7] [02825] [ts/1] [mail    ] [pts/1       ] [192.168.210.131 ] [192.168.210.131] [2019-10-05T11:18:54,607606+00:00]
[8] [02825] [    ] [        ] [pts/1       ] [                ] [0.0.0.0        ] [2019-10-05T11:19:42,548402+00:00]
[7] [02999] [ts/1] [mail    ] [pts/1       ] [192.168.210.131 ] [192.168.210.131] [2019-10-05T11:21:04,107187+00:00]
[8] [02999] [    ] [        ] [pts/1       ] [                ] [0.0.0.0        ] [2019-10-05T11:21:45,539577+00:00]
[7] [03108] [ts/1] [mail    ] [pts/1       ] [192.168.210.131 ] [192.168.210.131] [2019-10-05T11:23:34,640343+00:00]
[8] [03108] [    ] [        ] [pts/1       ] [                ] [0.0.0.0        ] [2019-10-05T11:24:11,772124+00:00]
maman@ubuntu:/mnt/case1/var/log$
```

3. What was the source port the user 'mail' connected from? 57708

```
maman@ubuntu:/mnt/case1/var/log$ grep mail auth.log
Oct  5 13:08:31 VulnOSv2 chsh[2536]: changed user 'mail' shell to '/bin/bash'
Oct  5 13:09:03 VulnOSv2 chpasswd[2558]: pam_smbpass(chpasswd:chauthtok): Failed to find entry for user mail.
Oct  5 13:09:03 VulnOSv2 chpasswd[2558]: pam_unix(chpasswd:chauthtok): password changed for mail
Oct  5 13:09:03 VulnOSv2 chpasswd[2558]: pam_smbpass(chpasswd:chauthtok): Failed to find entry for user mail.
Oct  5 13:09:18 VulnOSv2 usermod[2561]: add 'mail' to group 'sudo'
Oct  5 13:09:18 VulnOSv2 usermod[2561]: add 'mail' to shadow group 'sudo'
Oct  5 13:13:53 VulnOSv2 sshd[2624]: Accepted password for mail from 192.168.210.131 port 57686 ssh2
Oct  5 13:13:53 VulnOSv2 sshd[2624]: pam_unix(sshd:session): session opened for user mail by (uid=0)
Oct  5 13:14:04 VulnOSv2 sudo:     mail : TTY=pts/1 ; PWD=/var/mail ; USER=root ; COMMAND=/bin/su -
Oct  5 13:14:04 VulnOSv2 sudo: pam_unix(sudo:session): session opened for user root by mail(uid=0)
Oct  5 13:14:04 VulnOSv2 su[2721]: pam_unix(su:session): session opened for user root by mail(uid=0)
Oct  5 13:18:48 VulnOSv2 sshd[2624]: pam_unix(sshd:session): session closed for user mail
Oct  5 13:18:54 VulnOSv2 sshd[2825]: Accepted password for mail from 192.168.210.131 port 57704 ssh2
Oct  5 13:18:54 VulnOSv2 sshd[2825]: pam_unix(sshd:session): session opened for user mail by (uid=0)
Oct  5 13:19:21 VulnOSv2 sudo:     mail : TTY=pts/1 ; PWD=/var/mail ; USER=root ; COMMAND=/bin/su -
Oct  5 13:19:21 VulnOSv2 sudo: pam_unix(sudo:session): session opened for user root by mail(uid=0)
Oct  5 13:19:21 VulnOSv2 su[2804]: pam_unix(su:session): session opened for user root by mail(uid=0)
Oct  5 13:19:42 VulnOSv2 sshd[2825]: pam_unix(sshd:session): session closed for user mail
Oct  5 13:20:57 VulnOSv2 sshd[2999]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131  user=mail
Oct  5 13:20:59 VulnOSv2 sshd[2999]: Failed password for mail from 192.168.210.131 port 57706 ssh2
Oct  5 13:21:03 VulnOSv2 sshd[2999]: Accepted password for mail from 192.168.210.131 port 57706 ssh2
Oct  5 13:21:03 VulnOSv2 sshd[2999]: pam_unix(sshd:session): session opened for user mail by (uid=0)
Oct  5 13:21:11 VulnOSv2 sudo:     mail : TTY=pts/1 ; PWD=/var/mail ; USER=root ; COMMAND=/bin/su -
Oct  5 13:21:11 VulnOSv2 sudo: pam_unix(sudo:session): session opened for user root by mail(uid=0)
Oct  5 13:21:11 VulnOSv2 su[3055]: pam_unix(su:session): session opened for user root by mail(uid=0)
Oct  5 13:21:30 VulnOSv2 sudo:     mail : TTY=pts/1 ; PWD=/var/mail ; USER=root ; COMMAND=/bin/su -
Oct  5 13:21:30 VulnOSv2 sudo: pam_unix(sudo:session): session opened for user root by mail(uid=0)
Oct  5 13:21:30 VulnOSv2 su[3082]: pam_unix(su:session): session opened for user root by mail(uid=0)
Oct  5 13:21:45 VulnOSv2 sshd[2999]: pam_unix(sshd:session): session closed for user mail
Oct  5 13:23:34 VulnOSv2 sshd[3108]: Accepted password for mail from 192.168.210.131 port 57708 ssh2
Oct  5 13:23:34 VulnOSv2 sshd[3108]: pam_unix(sshd:session): session opened for user mail by (uid=0)
Oct  5 13:23:39 VulnOSv2 sudo:     mail : TTY=pts/1 ; PWD=/var/mail ; USER=root ; COMMAND=/bin/su -
Oct  5 13:23:39 VulnOSv2 sudo: pam_unix(sudo:session): session opened for user root by mail(uid=0)
Oct  5 13:23:39 VulnOSv2 su[3164]: pam_unix(su:session): session opened for user root by mail(uid=0)
Oct  5 13:24:11 VulnOSv2 sshd[3108]: pam_unix(sshd:session): session closed for user mail
maman@ubuntu:/mnt/case1/var/log$
```

4. How long was the last session for user 'mail'? (Minutes only)

5. Which server service did the last user use to log in to the system?] sshd

```
Oct  5 13:21:45 VulnOSv2 sshd[2999]: pam_unix(sshd:session): session closed for user mail
Oct  5 13:23:34 VulnOSv2 sshd[3108]: Accepted password for mail from 192.168.210.131 port 57708 ssh2
Oct  5 13:23:34 VulnOSv2 sshd[3108]: pam_unix(sshd:session): session opened for user mail by (uid=0)
```

6. What type of authentication attack was performed against the target machine? Bruteforce

```
maman@ubuntu:/mnt/case1/var/log$ grep Failed auth.log
Apr 20 19:22:04 VulnOSv2 sshd[1243]: Failed password for vulnosadmin from 192.168.56.101 port 35584 ssh2
May  2 18:50:32 VulnOSv2 sshd[1393]: Failed password for vulnosadmin from 192.168.56.103 port 57208 ssh2
May  2 18:54:02 VulnOSv2 passwd[1501]: pam_smbpass(passwd:chauthtok): Failed to find entry for user root.
May  2 18:54:20 VulnOSv2 passwd[1501]: pam_smbpass(passwd:chauthtok): Failed to find entry for user root.
Oct  5 12:39:27 VulnOSv2 sshd[1822]: Failed password for root from 192.168.210.131 port 57190 ssh2
Oct  5 12:39:33 VulnOSv2 sshd[1822]: Failed password for root from 192.168.210.131 port 57190 ssh2
Oct  5 12:42:35 VulnOSv2 sshd[1838]: Failed password for root from 192.168.210.131 port 57200 ssh2
Oct  5 12:42:35 VulnOSv2 sshd[1836]: Failed password for root from 192.168.210.131 port 57196 ssh2
Oct  5 12:42:40 VulnOSv2 sshd[1842]: Failed password for root from 192.168.210.131 port 57208 ssh2
Oct  5 12:42:40 VulnOSv2 sshd[1837]: Failed password for root from 192.168.210.131 port 57198 ssh2
Oct  5 12:42:40 VulnOSv2 sshd[1839]: Failed password for root from 192.168.210.131 port 57202 ssh2
Oct  5 12:42:40 VulnOSv2 sshd[1840]: Failed password for root from 192.168.210.131 port 57204 ssh2
Oct  5 12:42:40 VulnOSv2 sshd[1841]: Failed password for root from 192.168.210.131 port 57206 ssh2
Oct  5 12:42:45 VulnOSv2 sshd[1836]: message repeated 5 times: [ Failed password for root from 192.168.210.131 port 57196 ssh2]
Oct  5 12:42:45 VulnOSv2 sshd[1838]: message repeated 5 times: [ Failed password for root from 192.168.210.131 port 57200 ssh2]
Oct  5 12:42:45 VulnOSv2 sshd[1843]: Failed password for root from 192.168.210.131 port 57210 ssh2
Oct  5 12:42:46 VulnOSv2 sshd[1835]: Failed password for root from 192.168.210.131 port 57194 ssh2
Oct  5 12:42:46 VulnOSv2 sshd[1851]: Failed password for root from 192.168.210.131 port 57220 ssh2
Oct  5 12:42:46 VulnOSv2 sshd[1850]: Failed password for root from 192.168.210.131 port 57218 ssh2
Oct  5 12:42:46 VulnOSv2 sshd[1844]: Failed password for root from 192.168.210.131 port 57212 ssh2
Oct  5 12:42:46 VulnOSv2 sshd[1848]: Failed password for root from 192.168.210.131 port 57214 ssh2
Oct  5 12:42:46 VulnOSv2 sshd[1858]: Failed password for root from 192.168.210.131 port 57228 ssh2
Oct  5 12:42:46 VulnOSv2 sshd[1849]: Failed password for root from 192.168.210.131 port 57216 ssh2
Oct  5 12:42:46 VulnOSv2 sshd[1857]: Failed password for root from 192.168.210.131 port 57226 ssh2
Oct  5 12:42:50 VulnOSv2 sshd[1842]: message repeated 5 times: [ Failed password for root from 192.168.210.131 port 57208 ssh2]
Oct  5 12:42:50 VulnOSv2 sshd[1837]: message repeated 5 times: [ Failed password for root from 192.168.210.131 port 57198 ssh2]
Oct  5 12:42:51 VulnOSv2 sshd[1841]: message repeated 5 times: [ Failed password for root from 192.168.210.131 port 57206 ssh2]
Oct  5 12:42:51 VulnOSv2 sshd[1839]: message repeated 5 times: [ Failed password for root from 192.168.210.131 port 57202 ssh2]
Oct  5 12:42:51 VulnOSv2 sshd[1840]: message repeated 5 times: [ Failed password for root from 192.168.210.131 port 57204 ssh2]
Oct  5 12:42:55 VulnOSv2 sshd[1843]: message repeated 5 times: [ Failed password for root from 192.168.210.131 port 57210 ssh2]
Oct  5 12:42:56 VulnOSv2 sshd[1857]: message repeated 5 times: [ Failed password for root from 192.168.210.131 port 57226 ssh2]
Oct  5 12:42:56 VulnOSv2 sshd[1835]: message repeated 5 times: [ Failed password for root from 192.168.210.131 port 57194 ssh2]
Oct  5 12:42:56 VulnOSv2 sshd[1850]: message repeated 5 times: [ Failed password for root from 192.168.210.131 port 57218 ssh2]
Oct  5 12:42:56 VulnOSv2 sshd[1851]: message repeated 5 times: [ Failed password for root from 192.168.210.131 port 57220 ssh2]
Oct  5 12:42:56 VulnOSv2 sshd[1858]: message repeated 5 times: [ Failed password for root from 192.168.210.131 port 57228 ssh2]
Oct  5 12:42:56 VulnOSv2 sshd[1848]: message repeated 5 times: [ Failed password for root from 192.168.210.131 port 57214 ssh2]
Oct  5 12:42:56 VulnOSv2 sshd[1844]: message repeated 5 times: [ Failed password for root from 192.168.210.131 port 57212 ssh2]
Oct  5 12:42:56 VulnOSv2 sshd[1849]: message repeated 5 times: [ Failed password for root from 192.168.210.131 port 57216 ssh2]
Oct  5 12:43:17 VulnOSv2 sshd[1869]: Failed password for root from 192.168.210.131 port 57230 ssh2
```

7. How many IP addresses are listed in the '/var/log/lastlog' file? 2

```
maman@ubuntu:/mnt/case1/var/log$ strings lastlog
'3*Wtty1
]pts/1
192.168.210.131
2*Wpts/0
192.168.56.101
)Wtty1
maman@ubuntu:/mnt/case1/var/log$
```

8. How many users have a login shell?

```
root@ubuntu:/mnt/case1# cat etc/passwd | grep "/bin/bash"
root:x:0:0:root:/root:/bin/bash
mail:x:8:8:mail:/var/mail:/bin/bash
php:x:999:999::/usr/php:/bin/bash
vulnosadmin:x:1000:1000:vulnosadmin,,,:/home/vulnosadmin:/bin/bash
postgres:x:107:116:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
root@ubuntu:/mnt/case1#
```

9. What is the password of the mail user?

10. Which user account was created by the attacker? Php account

```
Oct  5 12:52:38 VulnOSv2 sshd[2367]: Failed password for root from 192.168.210.131 port 57672 ssh2
Oct  5 12:52:38 VulnOSv2 sshd[2365]: Connection closed by 192.168.210.131 [preauth]
Oct  5 12:52:38 VulnOSv2 sshd[2367]: Connection closed by 192.168.210.131 [preauth]
Oct  5 12:52:50 VulnOSv2 sshd[2372]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131  user=root
Oct  5 12:52:50 VulnOSv2 sshd[2370]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131  user=root
Oct  5 12:52:52 VulnOSv2 sshd[2372]: Failed password for root from 192.168.210.131 port 57676 ssh2
Oct  5 12:52:52 VulnOSv2 sshd[2370]: Failed password for root from 192.168.210.131 port 57674 ssh2
Oct  5 12:52:52 VulnOSv2 sshd[2370]: Connection closed by 192.168.210.131 [preauth]
Oct  5 12:52:52 VulnOSv2 sshd[2372]: Connection closed by 192.168.210.131 [preauth]
Oct  5 13:00:01 VulnOSv2 CRON[2438]: pam_unix(cron:session): session opened for user www-data by (uid=0)
Oct  5 13:00:01 VulnOSv2 CRON[2438]: pam_unix(cron:session): session closed for user www-data
Oct  5 13:06:38 VulnOSv2 sudo:     root : TTY=pts/0 ; PWD=/tmp ; USER=root ; COMMAND=/usr/sbin/useradd -d /usr/php -m --system --shell /bin/bash --skel /etc/skel -G sudo php
Oct  5 13:06:38 VulnOSv2 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Oct  5 13:06:38 VulnOSv2 useradd[2525]: new group: name=php, GID=999
Oct  5 13:06:38 VulnOSv2 useradd[2525]: new user: name=php, UID=999, GID=999, home=/usr/php, shell=/bin/bash
Oct  5 13:06:38 VulnOSv2 useradd[2525]: add 'php' to group 'sudo'
Oct  5 13:06:38 VulnOSv2 useradd[2525]: add 'php' to shadow group 'sudo'
```

11. How many user groups exist on the machine? 58

```
root@ubuntu:/mnt/case1# wc -l etc/group
58 etc/group
root@ubuntu:/mnt/case1#
```

12. How many users have sudo access?

```
maman@ubuntu:/mnt/case1$ sudo cat etc/group | grep "mail\|php"
mail:x:8:
sudo:x:27:php,mail
php:x:999:
maman@ubuntu:/mnt/case1$
```

13. What is the home directory of the PHP user?

```
Oct  5 13:06:38 VulnOSv2 sudo:     root : TTY=pts/0 ; PWD=/tmp ; USER=root ; COMMAND=/usr/sbin/useradd -d /usr/php -m --system --shell /bin/bash --skel /etc/skel -G sudo php
Oct  5 13:06:38 VulnOSv2 useradd[2525]: new group: name=php, GID=999
Oct  5 13:06:38 VulnOSv2 useradd[2525]: new user: name=php, UID=999, GID=999, home=/usr/php, shell=/bin/bash
Oct  5 13:06:38 VulnOSv2 useradd[2525]: add 'php' to group 'sudo'
Oct  5 13:06:38 VulnOSv2 useradd[2525]: add 'php' to shadow group 'sudo'
Oct  5 13:21:24 VulnOSv2 passwd[3080]: passwd: can't view or modify password information for php
```

14. What command did the attacker use to gain root privilege? (Answer contains two spaces).sudo su –

```
maman@ubuntu:/mnt/case1/var/mail$ sudo cat .bash_history
sudo su -
w
ll
ls -l
ls -la
pwd
logout
w
last
sudo su -
logout
sudo su -
passwd php
sudo su -
logout
sudo su -
logout
maman@ubuntu:/mnt/case1/var/mail$
```

15. Which file did the user 'root' delete?

```
root@ubuntu:/mnt/case1# cat root/.bash_history
poweroff
whoami
id
pwd
```

```
root@ubuntu:/mnt/case1# cat root/.bash_history
poweroff
whoami
id
pwd
vim /etc/passwd
ll
vim flag.txt
cat .psql_history
cd /var/www/html/
ll
cd jabc
ll
cat .htaccess
ll
vim scripts/update.php
ls -lh scripts/
w
logout
vim /var/log/lastlog
logout
passwd php
logout
cd /tmp/
ll
rm 37292.c
cd
ls -lha
ls .cache/
cat .cache/motd.legal-displayed
logout
```

16. Recover the deleted file, open it and extract the exploit author name.

```
root@ubuntu:/mnt/output1/tmp# file *
libssl1.0.0.config.T9bOfC:  C source, ASCII text, with very long lines, with CRLF line terminators
resolvconf.config.LHjPM6:   empty
resolvconf.template.9u3iwR: empty
sh-thd-2797907191:          C source, ASCII text, with very long lines, with CRLF line terminators
tmp.S692hUwVC8:             empty
root@ubuntu:/mnt/output1/tmp# cat sh-thd-2797907191
/*
# Exploit Title: ofs.c - overlayfs local root in ubuntu
# Date: 2015-06-15
# Exploit Author: rebel
# Version: Ubuntu 12.04, 14.04, 14.10, 15.04 (Kernels before 2015-06-15)
# Tested on: Ubuntu 12.04, 14.04, 14.10, 15.04
# CVE : CVE-2015-1328     (http://people.canonical.com/~ubuntu-security/cve/2015/CVE-2015-1328.html)

*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*=*
CVE-2015-1328 / ofs.c
overlayfs incorrect permission handling + FS_USERNS_MOUNT

user@ubuntu-server-1504:~$ uname -a
Linux ubuntu-server-1504 3.19.0-18-generic #18-Ubuntu SMP Tue May 19 18:31:35 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
user@ubuntu-server-1504:~$ gcc ofs.c -o ofs
user@ubuntu-server-1504:~$ id
uid=1000(user) gid=1000(user) groups=1000(user),24(cdrom),30(dip),46(plugdev)
user@ubuntu-server-1504:~$ ./ofs
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),24(cdrom),30(dip),46(plugdev),1000(user)
```

17. What is the content management system (CMS) installed on the machine?

```
root@ubuntu:/mnt/case1/var/www/html/jabc# cat index.php
<?php

/**
 * @file
 * The PHP page that serves all page requests on a Drupal installation.
 *
 * The routines here dispatch control to the appropriate handler, which then
 * prints the appropriate page.
 *
 * All Drupal code is released under the GNU General Public License.
 * See COPYRIGHT.txt and LICENSE.txt.
 */

/**
 * Root directory of Drupal installation.
 */
define('DRUPAL_ROOT', getcwd());

require_once DRUPAL_ROOT . '/includes/bootstrap.inc';
drupal_bootstrap(DRUPAL_BOOTSTRAP_FULL);
menu_execute_active_handler();
root@ubuntu:/mnt/case1/var/www/html/jabc#
```

18. What is the version of the CMS installed on the machine?

```
root@ubuntu:/mnt/case1/var/www/html/jabc/includes# cat bootstrap.inc | grep VERSION
define('VERSION', '7.26');
      $has_openssl = version_compare(PHP_VERSION, '5.3.4', '>=') && function_exists('openssl_random_pseudo_bytes');
root@ubuntu:/mnt/case1/var/www/html/jabc/includes#
```

19. Which port was listening to receive the attacker's reverse shell? 4444