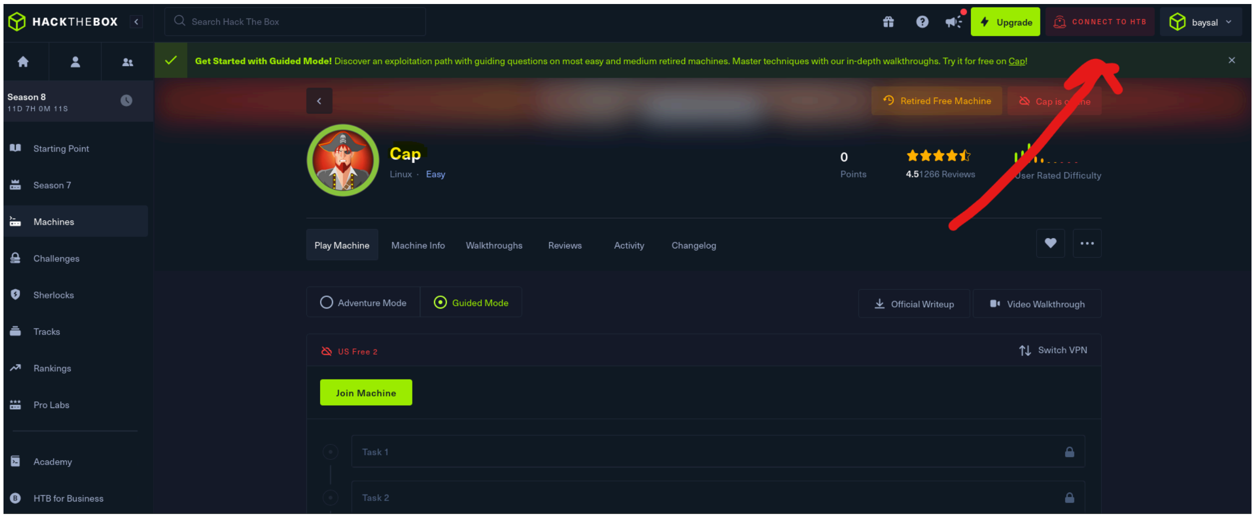
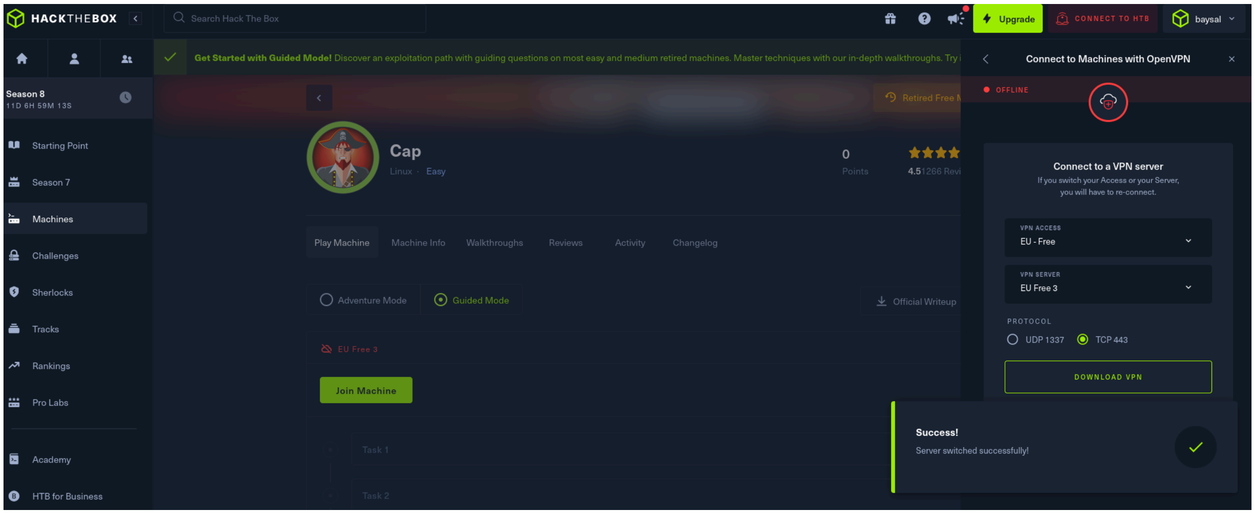
Yapay Zeka Destekli Sızma Testi

> Hack the Box üzerinden “Cap” adlı program kullanılmıştır.

Makineye bağlanma



Get Started with Guided Mode! Discover an exploitation path with guiding questions on most easy and medium retired machines. Master techniques with our in-depth walkthroughs. Try it for free on Cap!



Get Started with Guided Mode! Discover an exploitation path with guiding questions on most easy and medium retired machines. Master techniques with our in-depth walkthroughs. Try i

○ Adventure Mode ● Guided Mode

EU Free 3

Connect to a VPN server

If you switch your Access or your Server, you will have to re-connect.

VPN ACCESS: EU - Free

VPN SERVER: EU Free 3

PROTOCOL: ○ UDP 1337 ● TCP 443

Success!

Server switched successfully!

- Machines>OpenVPN>Sunucuları seç>TCP>İndir
- Terminalden dosyanın indirildiği klasöre gidilir.
- `openvpn lab_dosya.ovpn` komutuyla diyerek vpn çalıştırılır.
- Ardından sitedeki **join machine** kısmından da makineye bağlanılır.

ChatGPT kullanarak pentesting

> **i am solving a ctf.i want to pentest a machine.what should be my first step?ip adress of machine is 10.10.10.245** gibi bir promptla yardım alınarak başlanabilir.

🔍 Step 1: Network Scanning with Nmap

Run an Nmap scan to discover open ports, services, and versions on the target:

Basic scan:

```
nmap -sC -sV -oN initial_scan.txt 10.10.10.245
```

- `sC` : Run default scripts
- `sV` : Detect service versions
- `oN` : Output to a file (`initial_scan.txt`)

This will give you:

- Open ports (e.g., SSH, HTTP, SMB)
- Running services and versions (e.g., Apache 2.4.41)
- Potential attack surfaces

🧠 Next Steps Based on Results:

- **Web server found (e.g., port 80/443)?** → Run `whatweb`, `gobuster`, or `dirsearch`.
- **SSH found (port 22)?** → Look for default creds, bruteforce (if allowed), or version-specific exploits.
- **SMB (port 445)?** → Try `enum4linux` or `smbclient`.
- **FTP (port 21)?** → Check for anonymous login.
- **RDP (3389)?** → Check for weak creds or vulnerable versions.

> Buradaki adımlar kullanılabilir.

- Sitede yer alan **guided mod** kısmındaki sorulara cevaplar verilebilir.
- İlk soru cevaplanır ve çıkan diğer soruya göre yine gpt'ye soru sorulur.

❓

> **open ports:80,21,22.what should i do next?** tarzı bir soruyla ikinci aşamaya geçilebilir.

🔎 1. Enumerate Port 21 (FTP) — High Value Early Target

FTP is often misconfigured or allows **anonymous login**, which can leak files or credentials.

✅ Check for anonymous access:

```
ftp 10.10.10.245
```

- Username: `anonymous`
- Password: (just press Enter)

If you log in:

- Use `ls` , `get filename` to explore/download files.
- Look for `usernames` , `passwords` , `web files` , or `.txt` notes.

🌐 2. Enumerate Port 80 (HTTP) — Likely to Have Hidden Info

Check the website in a browser:

```
http://10.10.10.245
```

Use `whatweb` to fingerprint the site:

```
whatweb http://10.10.10.245
```

Use `gobuster` or `dirsearch` to brute-force hidden directories:

```
gobuster dir -u http://10.10.10.245 -w /usr/share/wordlists/dirb/common.txt -t 30
```

Look for:

- Admin panels (`/admin` , `/login`)
- File leaks (`.bak` , `.zip` , `.php`)

- CMS systems (WordPress, Joomla)

🔐 3. Enumerate Port 22 (SSH) — Usually Later Stage

SSH often comes into play **after** you gain credentials from FTP or web.

But you can:

- Check banner: `nmap -p22 --script ssh2-enum-algos 10.10.10.245`
- Save any usernames you find — useful for bruteforce *if allowed* in your CTF rules.

🚀 Recommendation:

Start with **FTP** → then **Web (Port 80)** → use findings for **SSH access**.

- Sonrasında sorulara cevap verilir.

🖊️***Ömer Faruk Baysal***