**HTB: Finding and Retrieving a Flag via rsync (Human-friendly Write-up)**

My approach (what I did, in plain language):

**1) Find open services with nmap**

I started with a fast port scan to see which services the target was running. The command I used scans common ports quickly:  
  
nmap --min-rate 4000 --top-ports 50000 10.129.99.30  
  
When the scan finished I noticed port 873 was open, which is the default port for an rsync daemon.

**2) Check rsync modules (look for anonymous access)**

Next I asked the rsync server what modules it exposes. This is a polite, non-destructive way to see if anything is publicly shareable:  
  
rsync rsync://10.129.99.30/  
  
This printed 'public' (anonymous), meaning I could read files from that module without credentials.

**3) Peek inside the public module (list-only)**

To avoid accidentally downloading anything, I listed the contents rather than copying them. The --list-only flag shows filenames, sizes and dates:  
  
rsync --list-only rsync://10.129.99.30/public/  
  
From this listing I saw a file named 'flag.txt' — exactly what I was after.

**4) Retrieve the flag and print it safely**

I wanted to print the flag to my terminal without leaving a permanent copy on disk. Rsync doesn’t stream to stdout, so I used a single command that downloads the file, prints it, and deletes it:  
  
rsync -av --progress rsync://10.129.99.30/public/flag.txt ./ && cat ./flag.txt && rm ./flag.txt  
  
This downloads flag.txt into the current directory, prints its contents with cat, and removes the file immediately afterwards.

**5) Optional: use RAM for zero-disk footprint**

If you prefer the file never touch disk, put it in /dev/shm (a RAM-backed filesystem) and then securely delete it:  
  
rsync -av --progress rsync://10.129.99.30/public/flag.txt /dev/shm/flag && cat /dev/shm/flag && shred -u /dev/shm/flag  
  
This keeps the file in memory and shreds it after printing.

**Short summary:** Scan for rsync, list modules, inspect public module with --list-only, and fetch the flag with rsync then print and remove it. Keep it ethical and redact sensitive data before publishing.