Enumeration

2021年7月29日 0:06

1: Use autorecon to enumerate its services, **22, 23, 80, 3306** are open
2: Access **HTTP** service, use dirb to enumerate its directories
3: A hidden directory **/test** is presented, and use gobuster to continue to enumerate its sub-directory
4: Finally, I find **ZenPhoto** is installed. **Default login** does not work, and I also try dictionary attack, fail. It means, it is not the right way
5: Search for **ZenPhoto's exploit**, and this one looks like the right one: https://www.exploit-db.com/exploits/18083

Foothold

2021年7月30日 11:48

1: Execute script, **php poc.php 192.168.61.41 /test**
2: Get a shell, upload nc, make it more stable
3: There is **no standard user** (except root) on this server

Privilege Escalation

2021年7月30日 11:48

1: Its kernel version is **2.6.32**, could be exploited by **Dirty Cow 2**
2: Download the exploit and compile it (https://www.exploit-db.com/exploits/40839), run it. A **new root user** added to the target
3: **ssh newuser@192.168.61.41**, with password
4: Get the root shell

Review

2021年7月30日 11:48

1: Target **HTTP** service
2: Find the **hidden directory**
3: Brute force login is not the right way, because exploit does not require **authentication**
4: Use a **kernel exploit**
5: SSH to target with new **added credential**