Enumeration

2021年7月16日 20:03

1: Use autorecon to enumerate its services, **22, 80, 110, 139, 143, 445, 993, 995** are open
2: Check **HTTP** service, use dirb and nikto to enumerate
3: **/admin.php** is found, access it. It requires credential to sign in, use default credential **admin:admin**, and it works.
4: Click **Upgrade center** in **ADMINISTRATION** section, the version info is revealed. It is **CSCART 1.3.3**, which has a **RCE** vulnerability. The public exploit can be found here: https://www.exploit-db.com/exploits/48891
5: Click Template editor, an **upload entry** is found!
6: Upload a php reverse shell (Change **.php** to .phtml to bypass **file extension filter**)

Foothold

2021年7月16日 20:04

1: Set up a netcat listener
2: Access http://192.168.250.39/skins/tmp.phtml, get a reverse shell!
3: cat /home/patrick/local.txt

Privilege Escalation

2021年7月16日 20:04

1: Download linenum.sh and linpeas.sh from Kali Box
2: Mysql is running **locally**, however, it is **not run by root privilege**
3: Kernel and some other binaries appears to have vulnerability, however, I cannot run **compiled binary** exploit with **bash** shell
4: Scripts show that user **patrick** has **admin privilege**, therefore, it is a good way to switch to user patrick
5: Use hydra to brute patrick's password**, hydra -l patrick -P dict/rockyou.txt 192.168.250.39 -t 4 ssh**, and it succeeds. Its password is **patrick**, too
6: Switch to **patrick** or ssh to patrick
7: sudo su
8: chmod 777 proof.txt, cat proof.txt

Review

2021年7月16日 20:04

1: Target **HTTP** service
2: Get **CSCART**'s version info and then find the upload entry
3: Change shell's file extension to **phtml** to pbypass **file extension blacklist**
4: Notice user **patrick's privilege**
5: There are some **rabbit holes** during PE. Such as **readable root folder**, **locally running mysql**, **vulnerable service/binary version**, etc. They **appears to be exploitable**, however, it is **not the case**!