Enumeration

2021年7月14日 12:40

1: Use autorecon to enumerate its services, **22, 25, 80, 139, 199, 445, 60000 (ssh)** are open
2: SMTP's version is **Sendmail 8.13.4**, it could be exploited by a public exploit (https://www.exploit-db.com/exploits/2051). However it fails, it could relate to server's configuration of SMTP
3: There is plenty info can be captured by enumerating SMB service, however, SMB itself it is not vulnerable to some vulnerabilities
4: Check HTTP service, meanwhile run nikto and dirb. However, HTTP is not the intended target
5: Use searchsploit to search SMTP related vulnerabilities again, aside from the exploit mentioned in step2, there is **another exploit** catches my eyes
6: It is **Sendmail with clamav-milter < 0.91.2-RCE**. Though it does not specify Sendmail's version, but I don't mind having a try
7: No need to modify the exploit, execute **perl 4761.pl 192.168.217.42**

Foothold

2021年7月14日 12:40

1: Read exploit code, after executing it a **new port** will be opened, use nc to connect to this port: **nc -nv 192.168.217.42 31337**
2: Get a shell after connection

Privilege Escalation

2021年7月14日 12:40

1: It is already a root shell
2: cat /root/proof.txt

Review

2021年7月14日 12:40

1: Target **SMTP** service
2: Identify **SendMail**'s vulnerability and find a proper exploit. **If the version is not specified, do not mind having a try!**
3: Apache's version, and SMB's version distract me for some time
4: **Box's name** could be helpful, however, we will not always know box's name, this is a trick which I **cannot rely on**