Enumeration

2021年7月29日 0:06

1: Use autorecon to enumerate its services, **21, 80, 135, 139, 445, 9998,17001** are open
2: FTP does support **anonymous** login, however, it does not contains some interesting files
3: And I don't have access to SMB service
4: Http service running on port 80 does not have any content, and Http service running on port **9998** has a **login portal**. It requires **email account** to login, since I do not know target's **domain name**, **hostname**, or one of its **username**, it is hard for me to guess
5: Meanwhile, I know the management is **SmarterMai**l. It has a **RCE** exploit (https://www.exploit-db.com/exploits/49216), however, I am not sure about its version. So **further enumeration** is needed
5: Enumerate its directory, it does have many webpages and directories, however, most of them are **decoys**.
6: Look back to scanning result, I start to look into the service running on port **17001**. Search for its exploit, and I find previous exploit again. That means Port 17001 communicates/ **works with** port 9998 together.

Foothold

2021年7月29日 0:06

1: Even though I still not sure about its version, but I have a try
2: Edit the exploit, and then execute **python3 poc.py**
3: Get a system shell!

Privilege Escalation

2021年7月29日 0:06

1: It is already a system shell

Review

2021年7月29日 0:06

1: Target **HTTP** and **Remoting** services
2: **Eliminate decoys**, combine pieces together: **SmarterMai**l works with .**NET Remoting Service**
3: Edit exploit and get the shell