# Enumeration

2021年7月13日 12:28

1: Use autorecon to enumerate its services, **80, 135, 139, 445, 3573**, and msrpc are open.
2: Check **smb** vulnerability, it seems to be vulnerable to **ms17-010**. After verification, it does not. SMB service could be a **rabbit hole**
3: **3573** is an unknown service, few documents about it.
4: Access its HTTP service, use default credential **admin:admin** to log in, meanwhile run nikto and dirb
5: It is a **HP-Power-Manager**, its version is vulnerable to a **buffer-overflow vulnerability**. The public exploit can be found here (https://github.com/Muhammd/HP-Power-Manager/blob/master/hpm_exploit.py)

# Foothold

2021年7月13日 12:29

1: Execute **python hpm.py 192.168.161.45**, and after about 30 seconds, I get a shell

# Privilege Escalation

2021年7月13日 12:29

1: It is already a privileged shell

# Review

2021年7月13日 12:29

1: Target **HTTP** service
2: The **buffer-overflow** is quite simple, no need to modify anything