# Enumeration

2021年7月13日 14:22

1: Use autorecon to enumerate its services, **53, 135, 139, 445, 3389, 5357**, and msrpc are open.
2: Among these services, SMB can be exploited by **Eternal Blue** exploit

# Foothold

2021年7月13日 14:22

1: Execute **python send_and_execute.py 192.168.217.40 ms17–010.exe**
2: Get a **privileged** shell

# Privilege Escalation

2021年7月13日 14:22

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

# Review

2021年7月13日 14:22

1: Target **SMB**
2: Identify **eternal blue** exploit