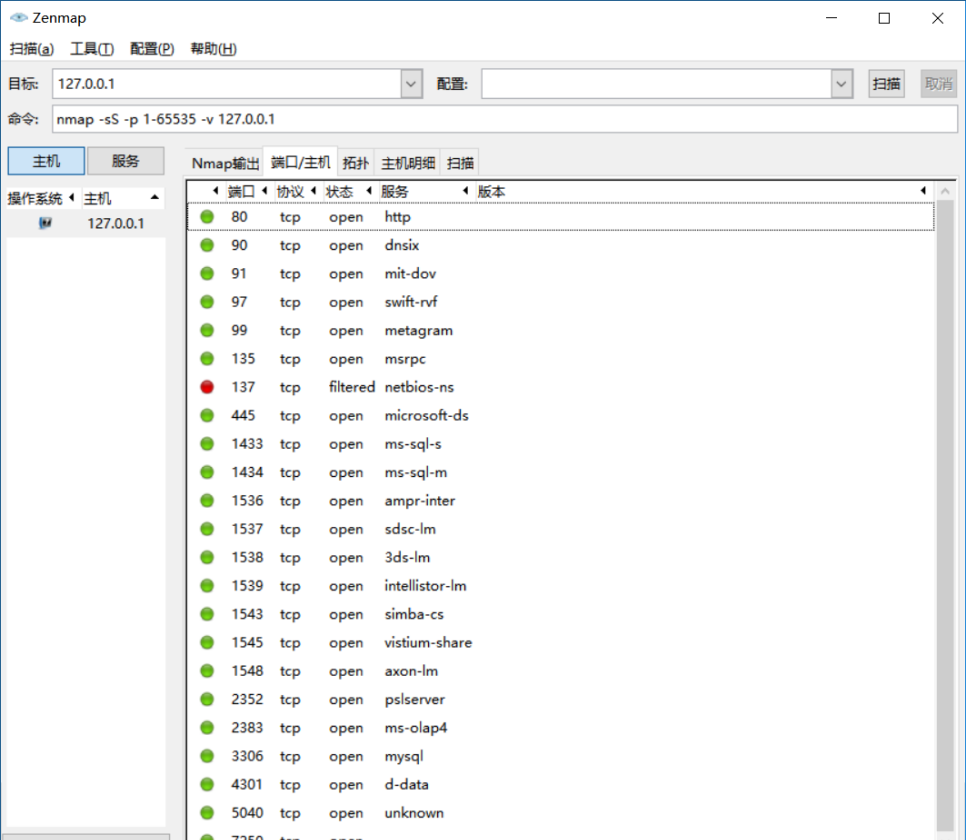
渗透测试-曾钰

1. 信息收集

扫描端口

使用Zenmap扫描端口

扫描1-65535所有端口



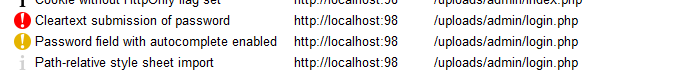
1. 漏洞扫描

利用burpsuit进行漏洞扫描

1. 打开burpsuit，进行设置后访问http://bluecms:8888/uploads/，拦截后扫描
2. 发现漏洞

Cleartex submission of password

Password field with automplete enabled



1. 爬取网站

对bluecms:8888进行爬取

