## 信息收集

cmd中查询

**C:\Users\lenovo>nslookup localhost:9997  
1.11.111.in-addr.arpa nameserver = bdns.he.chinamobile.com  
1.11.111.in-addr.arpa nameserver = dns.he.chinamobile.com  
dns.he.chinamobile.com internet address = 111.11.1.2  
bdns.he.chinamobile.com internet address = 111.11.11.2  
服务器: UnKnown  
Address: 111.11.1.1**

**nslookup bluecms  
1.11.111.in-addr.arpa nameserver = dns.he.chinamobile.com  
1.11.111.in-addr.arpa nameserver = bdns.he.chinamobile.com  
dns.he.chinamobile.com internet address = 111.11.1.2  
bdns.he.chinamobile.com internet address = 111.11.11.2  
服务器: UnKnown  
Address: 111.11.1.1  
  
非权威应答:  
名称: bluecms.edu2act.org  
Address: 111.63.112.254**

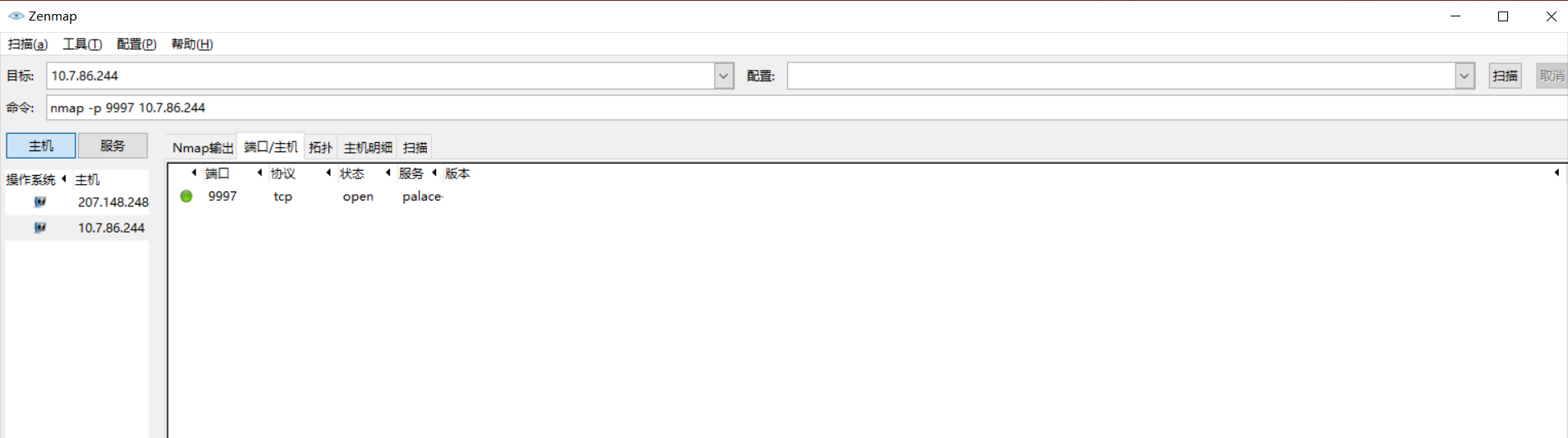


查询注册人信息





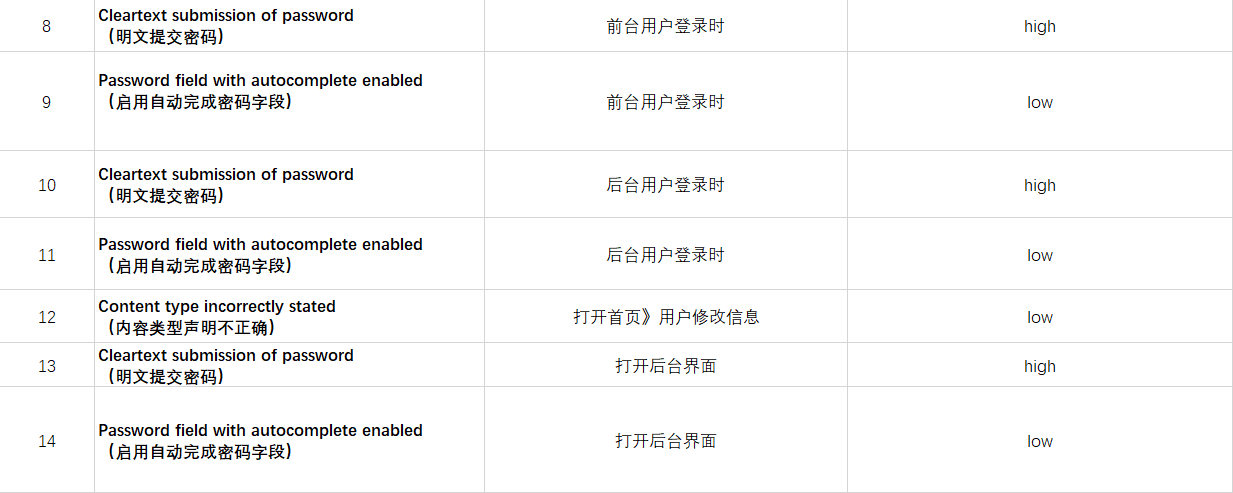
nmap扫描



旁站c端



## burp suite 扫描



## 手工渗透测试





## 手工界面测试

