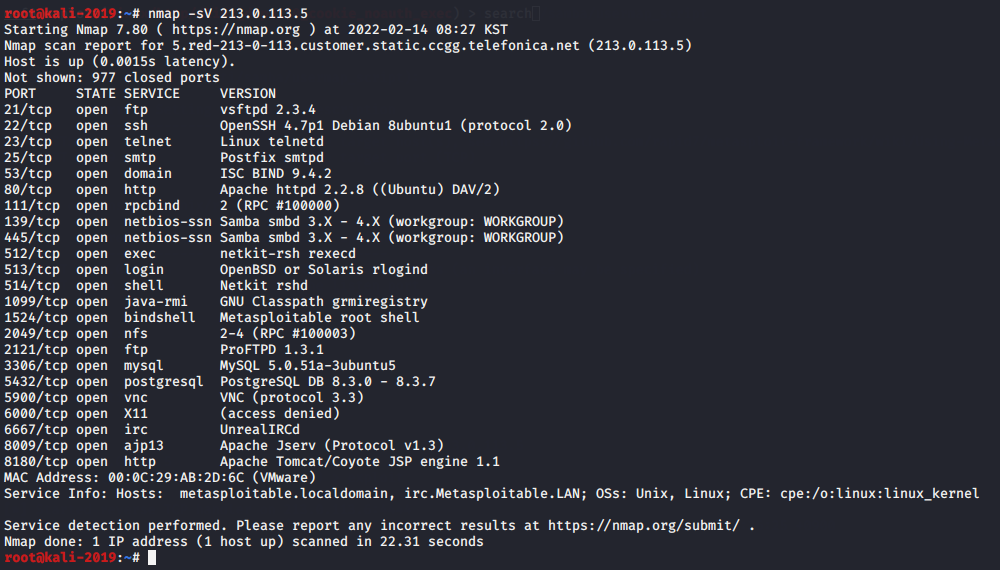
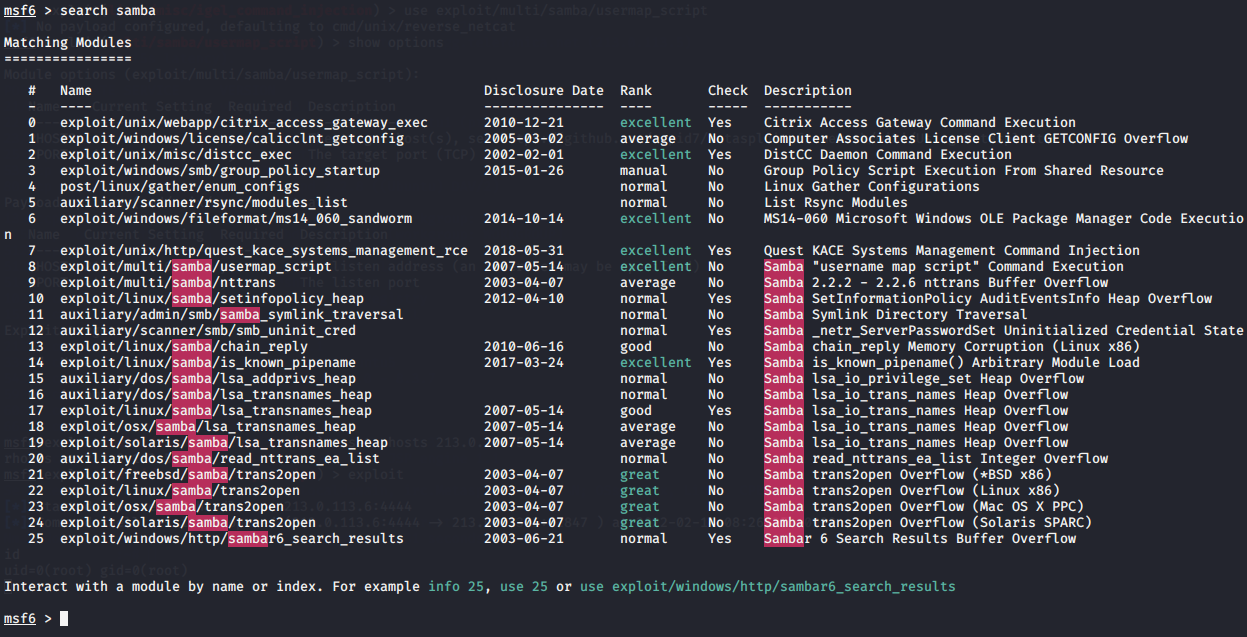
**취약점 분석**

**고해준**

1. 취약점 알아내기 – DVWA, METASPLOITABLE2, CENTOS7

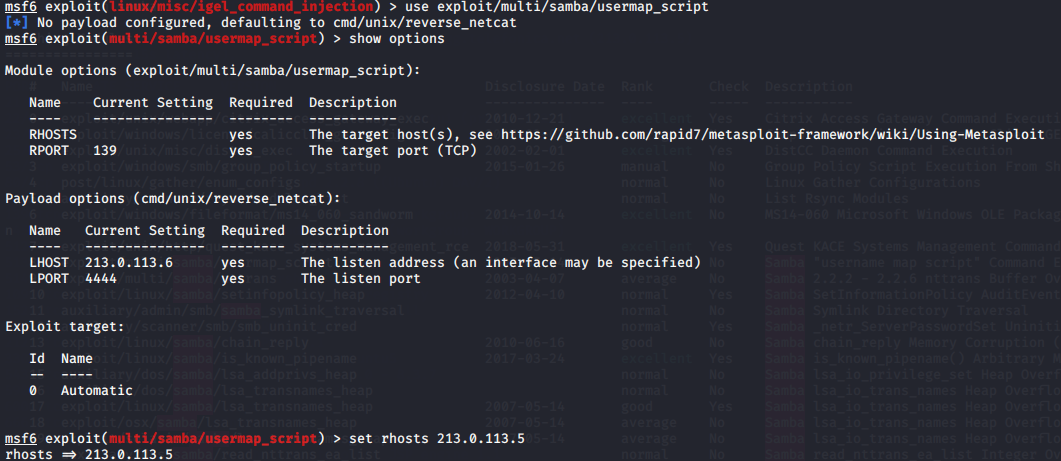


Nmap으로 213.0.113.5의 취약점 스캔 결과 samba 취약점 발견



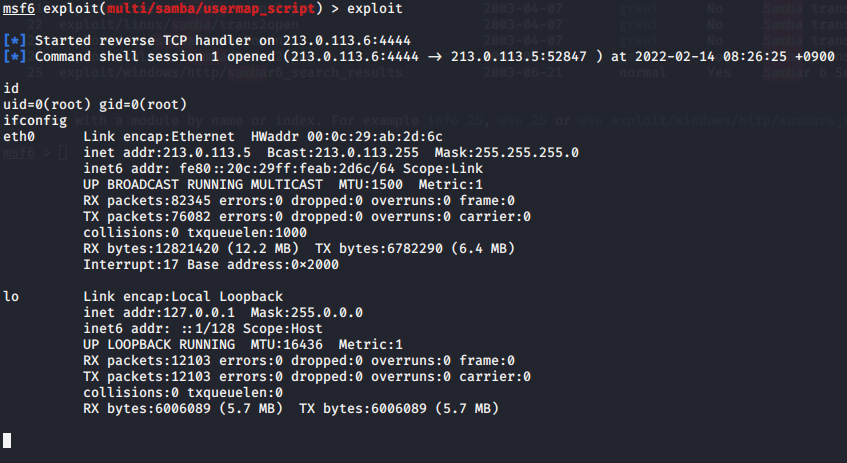
Search 후 8번 취약점으로 선택

1. 취약점 공격 – Metasploit 이용 가능, 다른 방법

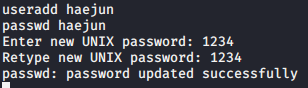


필요한 정보 확인 후 RHOSTS 설정

1. 성공(root, or user shell) – nc 이용 백도어 생성/기타 서버 정보 변경 등



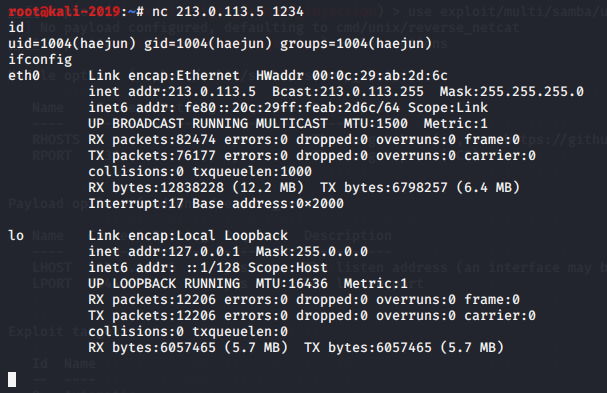
213.0.113.5의 Root 권한을 획득한 것을 확인



213.0.113.5에 계정 생성



213.0.113.5의 1234 포트로 백도어 생성



Kali에서 1234번 포트로 nc 접속 후 확인

1. 취약점 해결 방법

Samba 3.0.0 ~ 3.0.25rc3 버전에 해당하는 취약점이므로 업데이트를 한다.