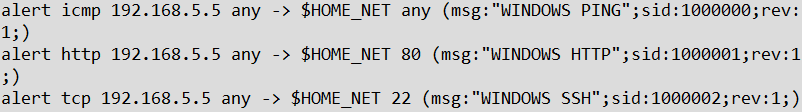
**- IDS 시스템의 정상적 운영 및 탐지 확인**

본인의 실습 환경에 따 3개의 임의의 룰을 작성하여 테스트하고 확인



Suricata rules

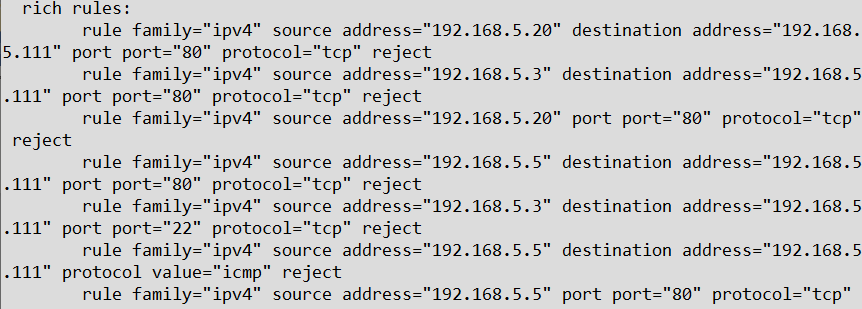




  
  
룰에 따른 PING, HTTP(80), SSH(22) 감지 확인

**- Firewalld or IPTables 룰 작성 및 테스트**

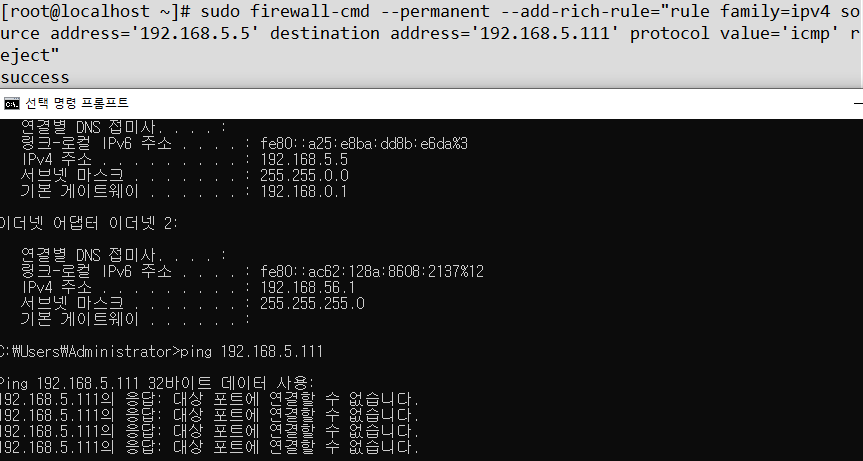
본인의 실습 환경에 따라 3개의 임의의 룰을 작성하여 테스트하고 확인



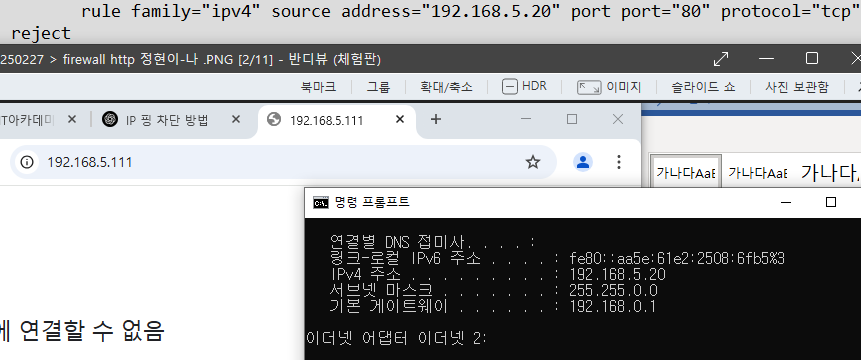
여러 룰 추가



WINDOWS(.5)에서 오는 HTTP(.111) 접속 접속 차단

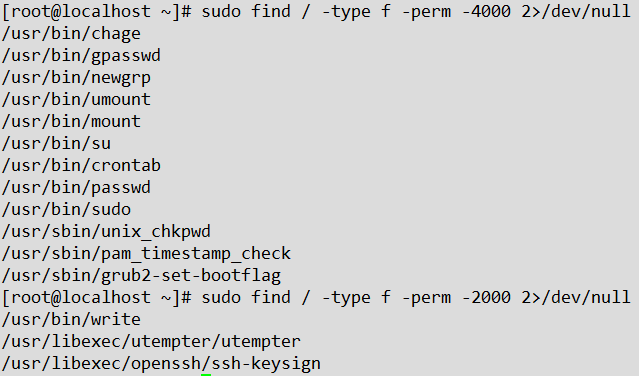


WINDOWS(.5)에서 오는 PING(.111) 차단

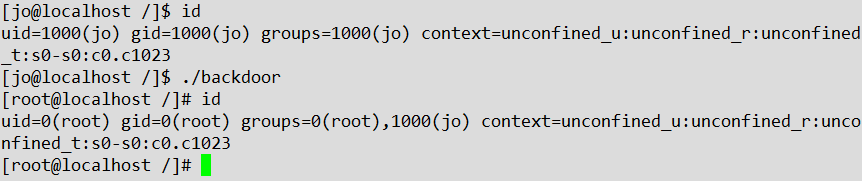


타 컴퓨터(정현 .20)에서 오는 HTTP(.111) 접속 차단

**- 시스템에서 suid / sgid 파일을 find 명령어를 통해 확인하고 권한 상승 테스트를 진행**

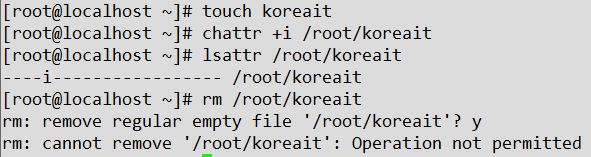


find 명령어를 통해 suid/sgid 파일을 확인



사용자 jo를 추가하고 backdoor를 만들어 실행해 권한이 상승한 결과

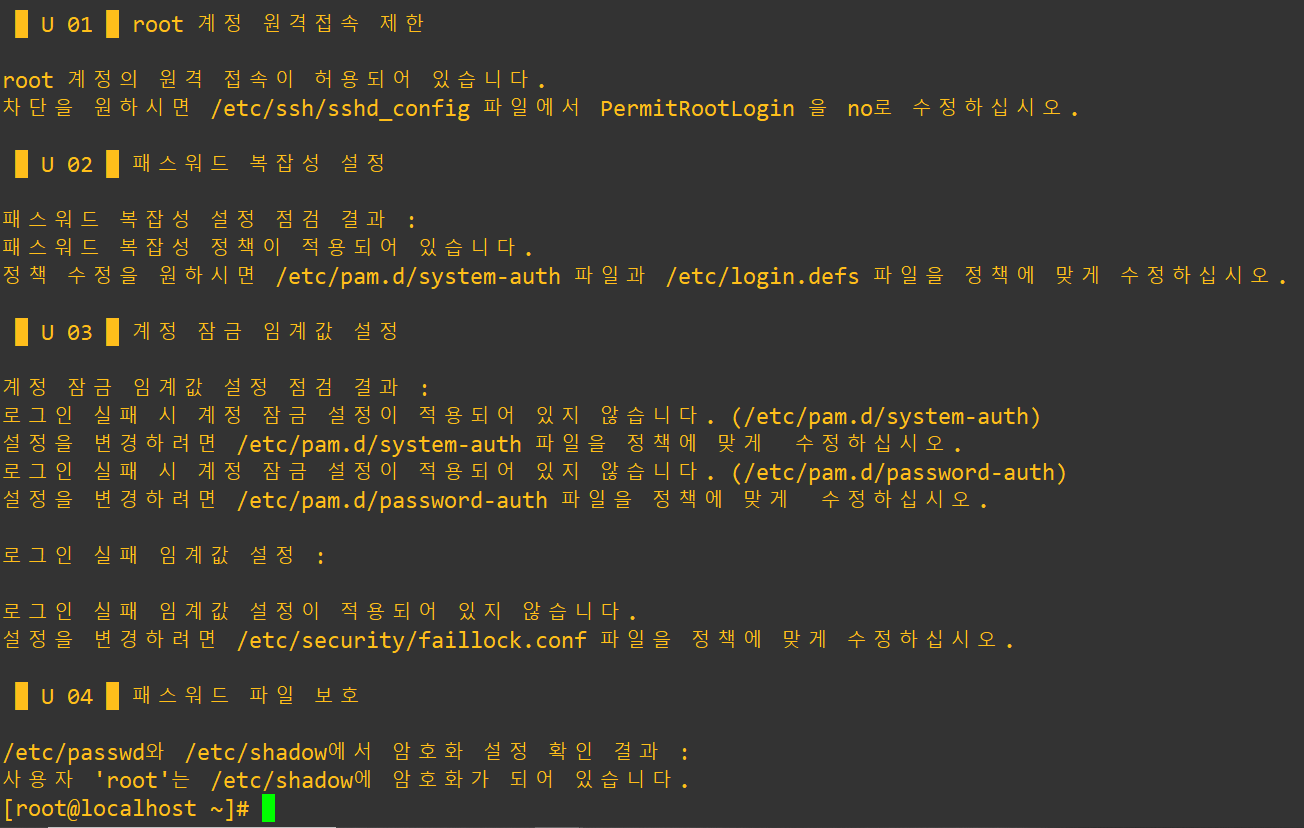
**- /root/koreait 파일 생성 후 rm koreait 명령어 실행 시 삭제가 되지 않도록 파일의 속성을 변경하고 확인**



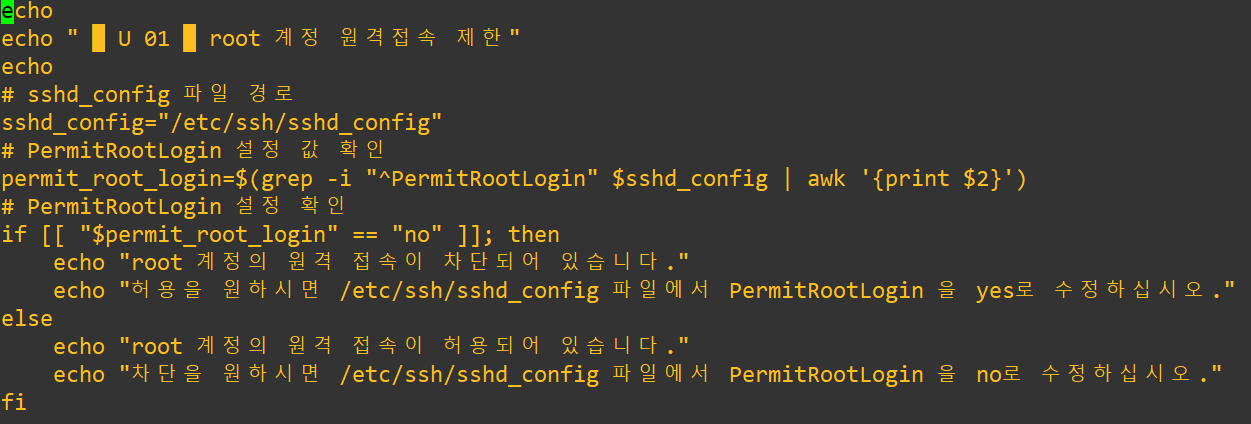
Immutable 명령어를 사용하여 속성의 변경을 확인하고 삭제가 되는지 확인한 결과 삭제가 되지 않는다

**- ‘주요정보통신기반시설\_기술적\_취약점\_분석\_평가\_방법\_상세가이드‘에 따라**

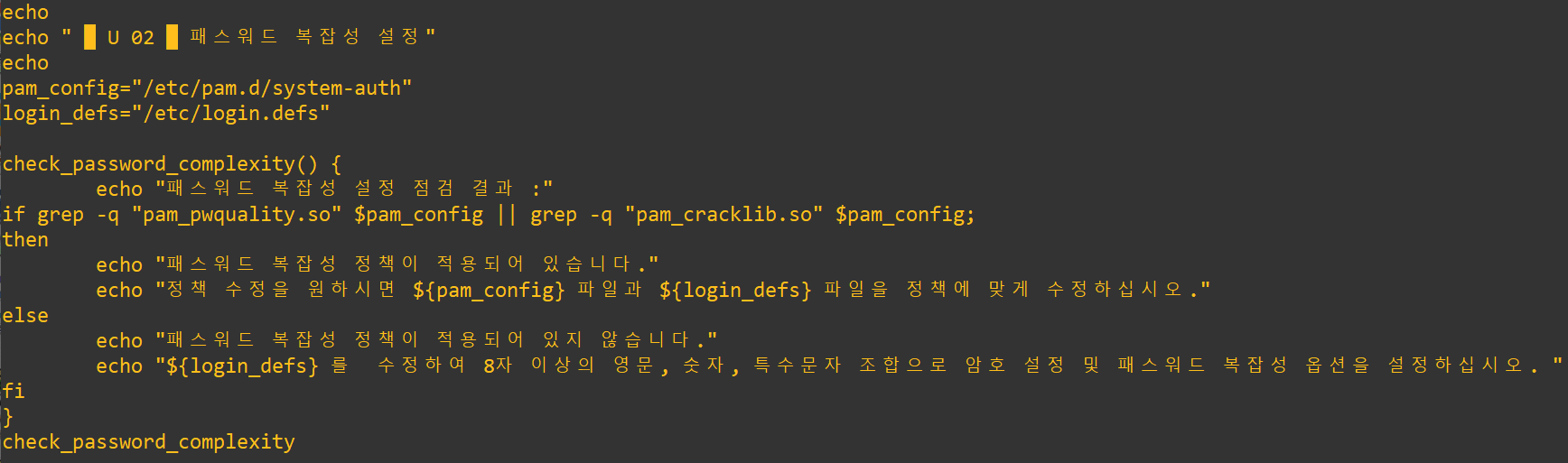
**U01 ~ U04까지의 계정관리 취약점을 점검할 수 있는 보안 점검 쉘 스크립트를 작성**

****

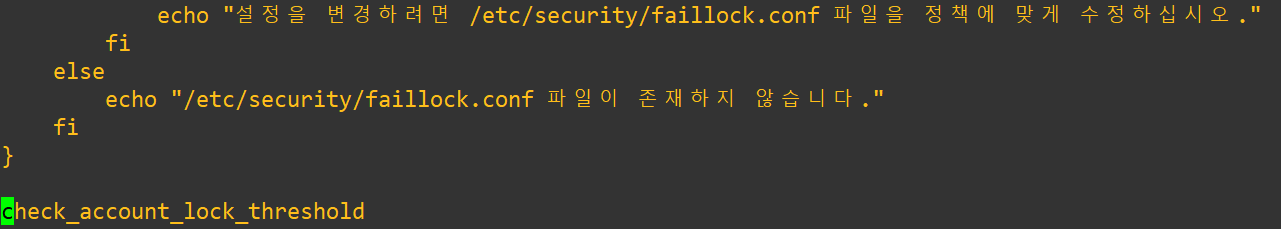
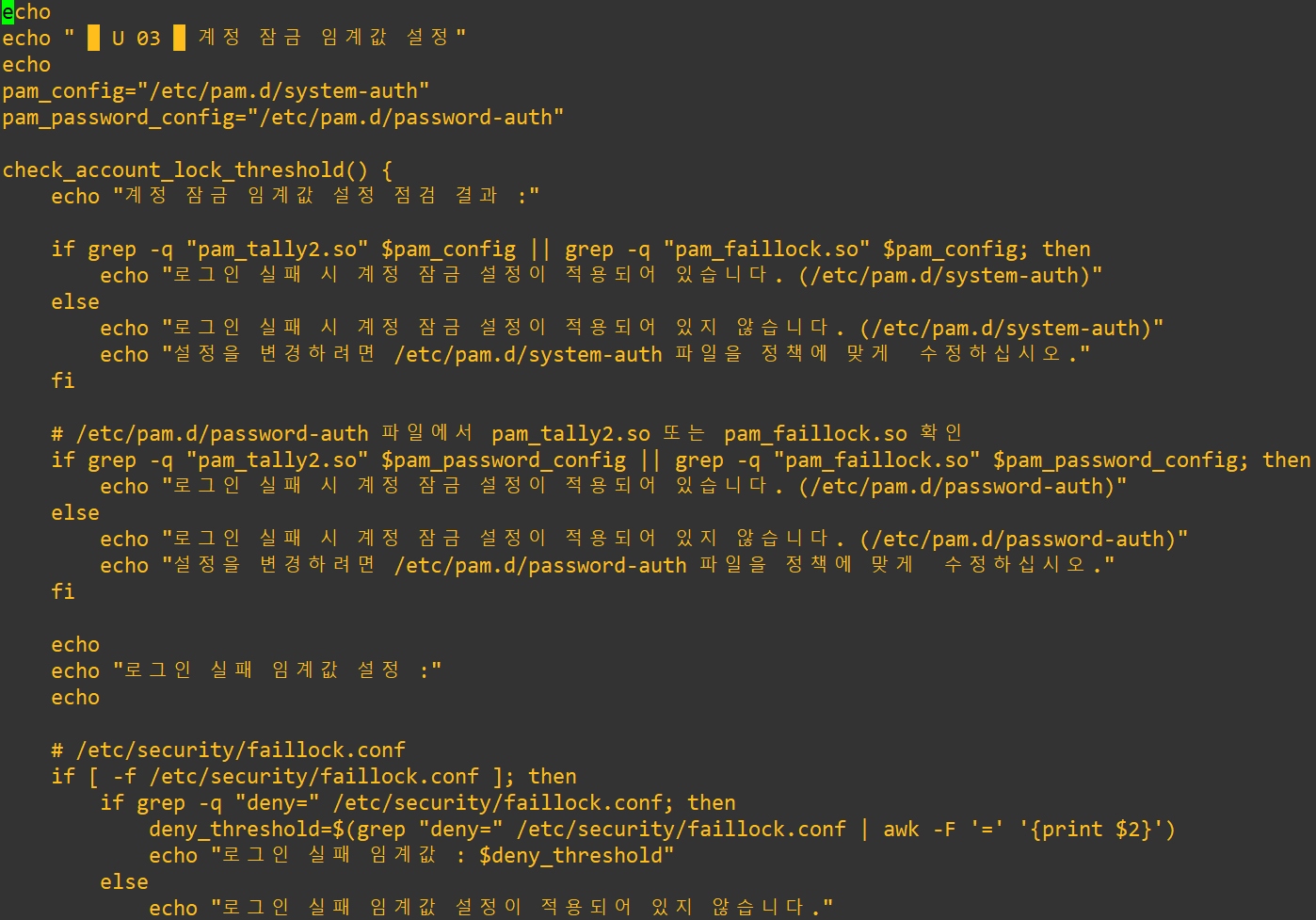
U 01~04 스크립트 실행 결과



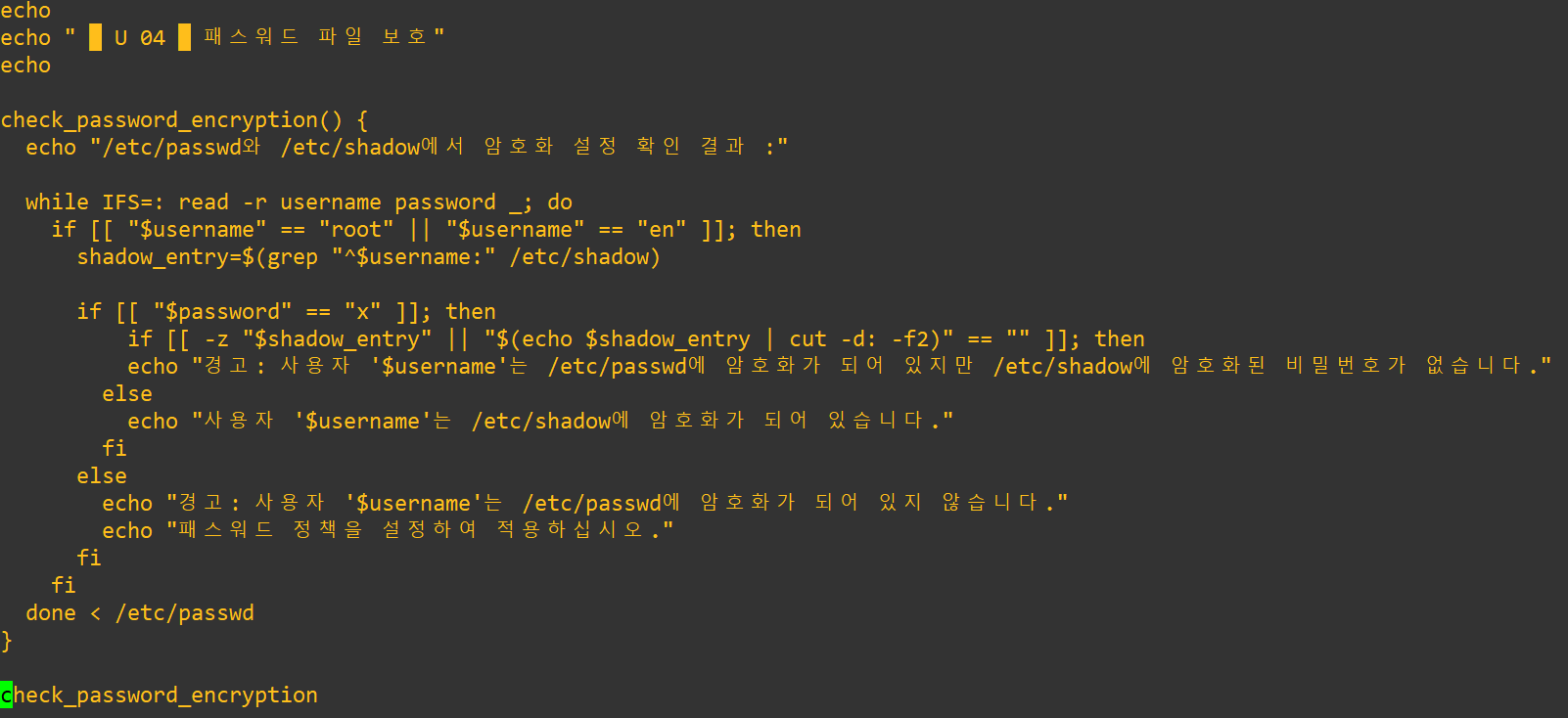
U 01 코드



U 02 코드

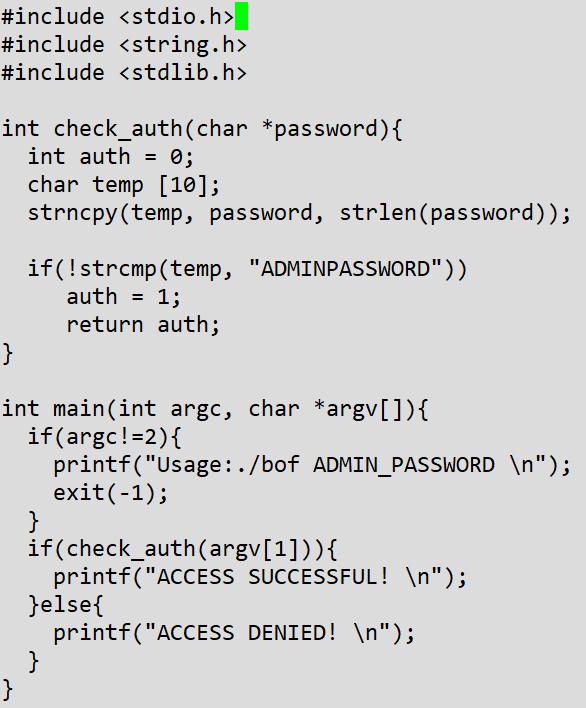


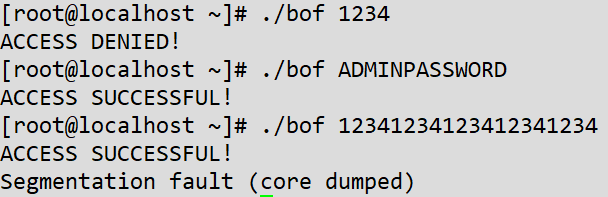
U 03 코드



u 04 코드

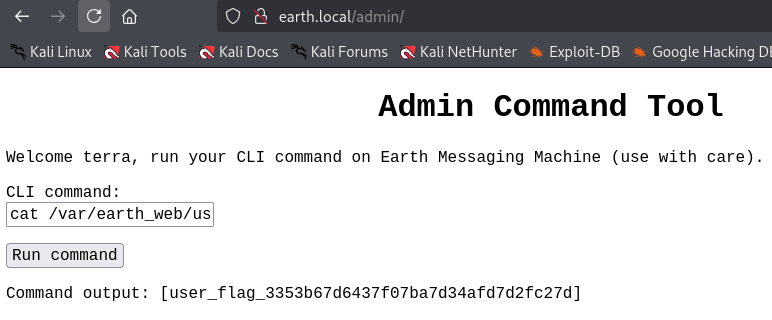
**- BoF 공격에 대해 간략히 서술하고 코드를 작성하여 테스트를 진행하여 확인**

BoF란 Buffer overflow로 버퍼의 크기를 초과하여 데이터를 쓸 때 다른 메모리영역에 덮어씌우기가 되는데, 덮어씌워지기가 되면서 악성코드가 삽입, 예기치 않은 동작을 하게 되는 등 오류가 일어나는 현상을 말한다.  
  


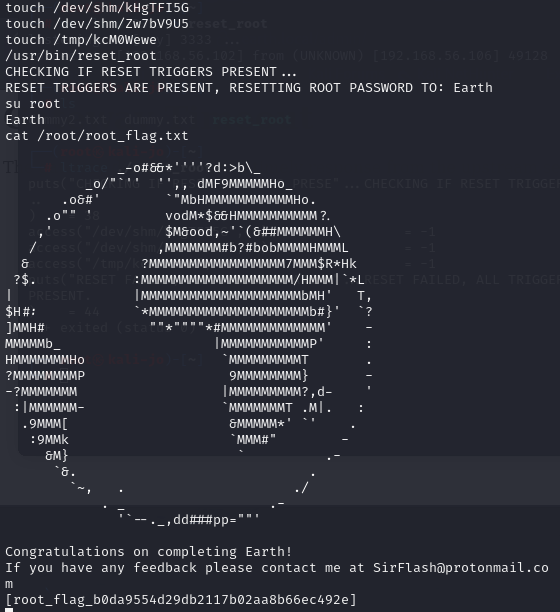


BoF 코드와 테스트 결과 (오버플로우 발생으로 엑세스가 성공함)

**- CTF VM를 해킹하여 user\_flag 및 root\_flag를 획득**



Nmap, netdiscover, dirb 명령어를 통해 http://earth.local, terratest.earth.local의 도메인을 찾아 등록하고 주소 탐색을 통해 robots.txt와 testdata.txt 파일을 찾았다. 파일 안에서 admin 계정과 암호화 된 비밀번호를 찾아 해석하여 <http://earth.local/admin>에 로그인 하여 user\_flag를 찾아냈다.



이후 root flag를 이용해 earth와 kali를 연결하여 reset\_root를 실행하기 위한 트리거를 만들었다. 결국 root계정의 비밀번호를 Earth로 초기화하고 계정에 접속해 root flag를 찾았다.

**- IDS 시스템의 업데이트와 리눅스의 커널 업데이트에 대해 서술하시오**

IDS(침입탐지시스템)는 네트워크, 시스템에 발생하는 침입, 공격을 실시간으로 감지하는 시스템으로 주요 요소로는 시그니처 업데이트, 기능업데이트 등이 있다.

시그니처 업데이트는 이미 알려진 공격의 패턴을 저장, 참고하여 네트워크 트래픽을 분석하여 침입을 식별한다. 이 업데이트는 새로운 유형의 공격을 탐지할 수 있게 해 준다. 기능 업데이트는 IDS 시스템이 공격 대상이 될 경우가 있기 때문에 IDS시스템의 보안 취약점을 수정하고 패치하는 것이다.

리눅스 커널은 하드웨어와 상위 소프트웨어 간의 상호작용을 관리한다. 커널 업데이트는 시스템의 성능, 보안, 기능 향상을 돕고 보안패치, 기능 개선 등이 있다.

커널에 보안 취약점이 발견되면 해커들이 악용할 우려가 있기 때문에 즉시 수정하여 업데이트 하하는 것 중요하다. 커널 버전을 최신으로 업데이트하여 시스템 성능 향상, 새로운 하드웨어 지원을 받으면 좋다.