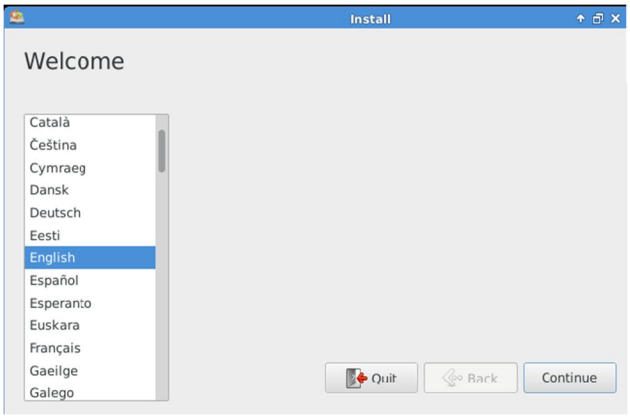
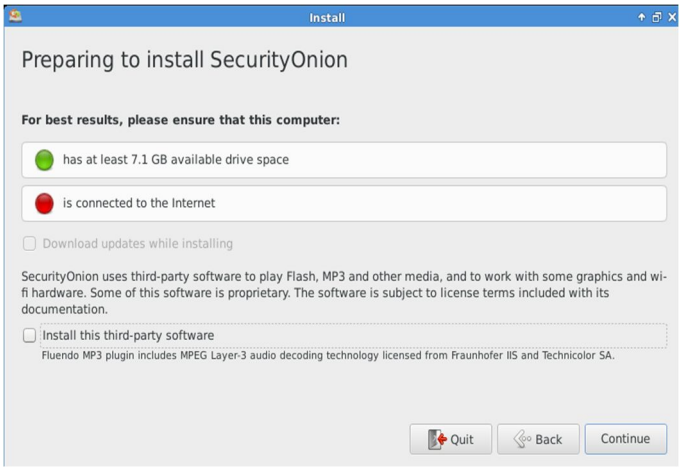
NSM(Network Security Monitoring) 설치

Part 1. 일반설정

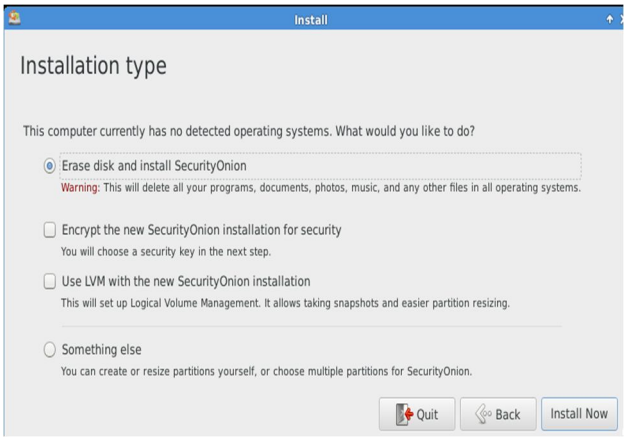
1. [Install-Install Security Onion 선택



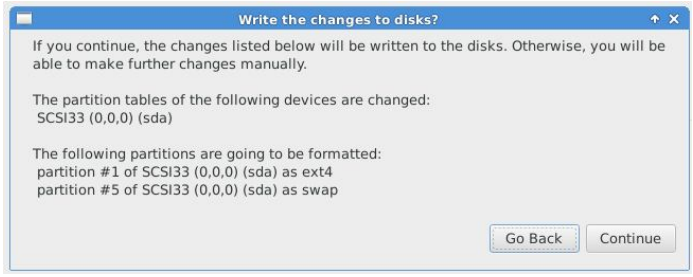
2. 대화상자 언어 선택 [영어 선택]



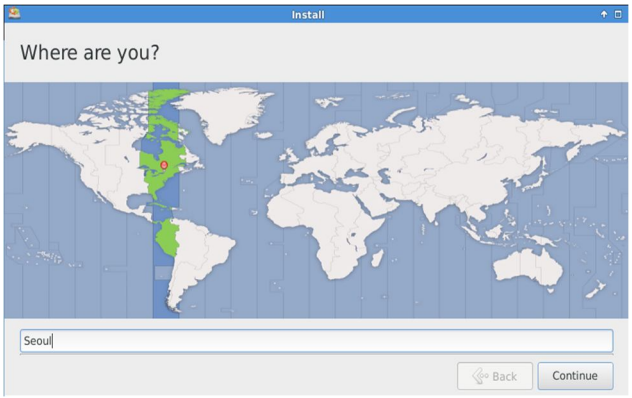
3. 디스크 공간과 인터넷 연결 상태 확인 [Continue] 클릭



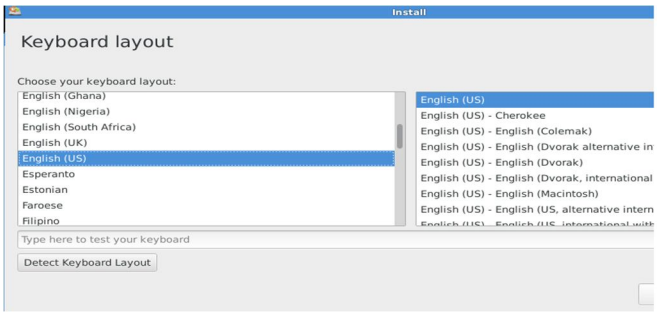
4. 설치 종류를 선택 [Erase disk and Install Security Onion]



5. 설치될 파티션 정보와 포맷 상황 보고 메시지 [Continue] 클릭



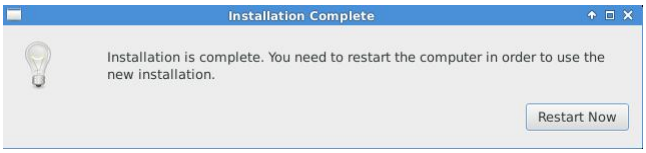
6. 사용자의 위치 설정 [Seoul]입력



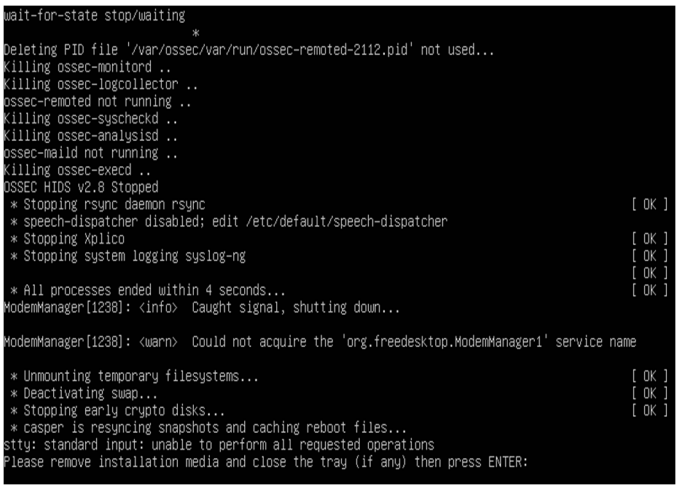
7. 키보드설정 [English(US)] 클릭

8. 사용자 아이디와 비밀번호 설정 (ID: boan PW : 1234)

Part 2. 네트워크 설정



9. 설치가 완료되면 재부팅

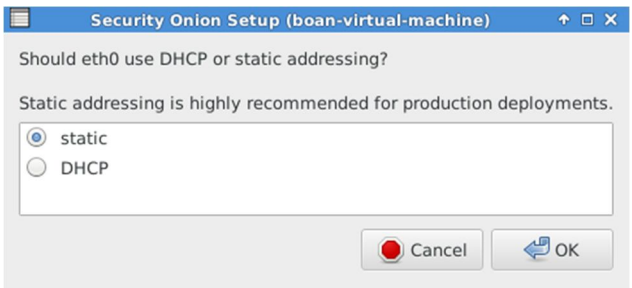


10. 재부팅 후 [enter]를 입력하여 정상적으로 부팅

11. 부팅 후 바탕 화면의 [Setup 아이콘] 클릭

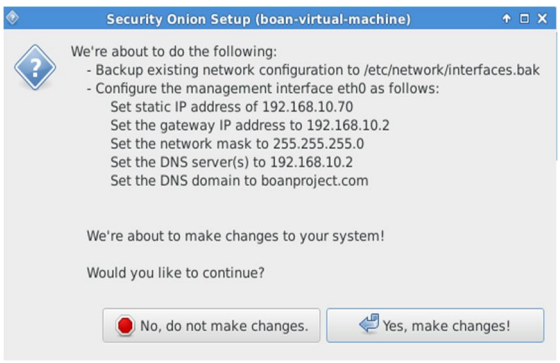
12. Onion 설정의 지속 설치 여부 확인 [Yes, Continue]클릭

13. 네트워크 설정 유무 확인
[Yes, Configure /etc/network/interfaces] 클릭



14. IP 설정 환경 지정 [Static] 클릭

15. 네트워크 설정 값 연속 지정
IP address : 192.168.10.10
Subnetmask : 255.255.255.0
Gateway IP address : 192.168.10.2
DNS Server IP address : 192.168.10.2
Domain name : boanproject.com

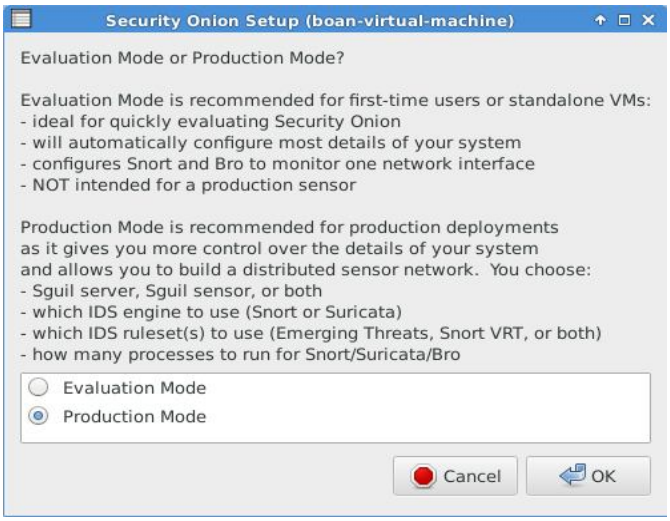


16. 설정 확인 후 [Yes, make changes] 클릭

17. 시스템 재부팅 [Yes, reboot]

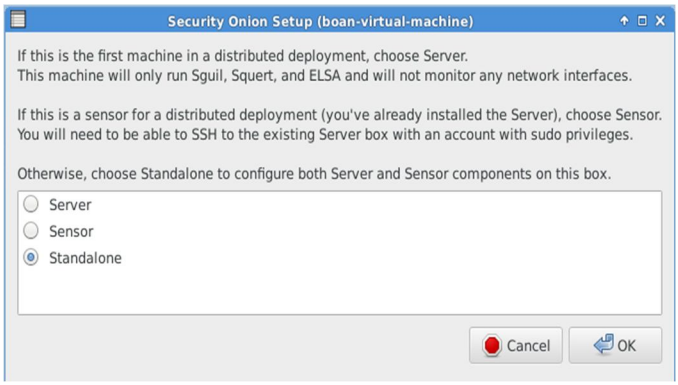
18. 재부팅 후 바탕 화면 [Setup] 아이콘 실행 후
[Yes, skip network configuration] 선택

Part 3. NSM 구성



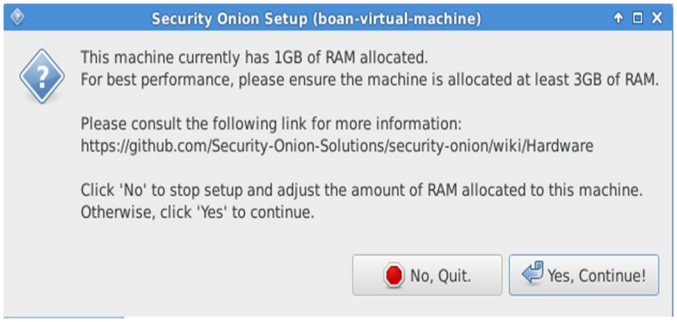
19. 도구 설치 방법 지정 [production mode] 선택

Evaluation	사용자 시스템에 맞게 자동으로 설정 처음 설정시 권고
production	시스템을 조정 하면서 NSM 설치

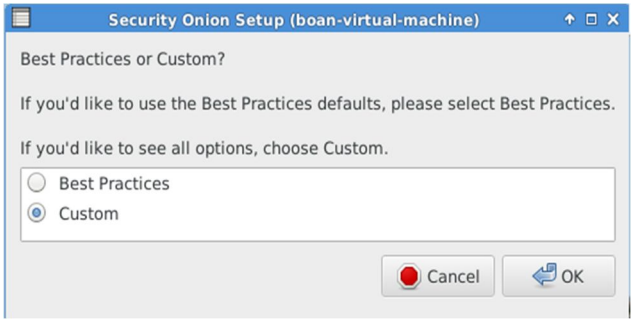


20. 시스템 환경 설정 [Standalone] 선택

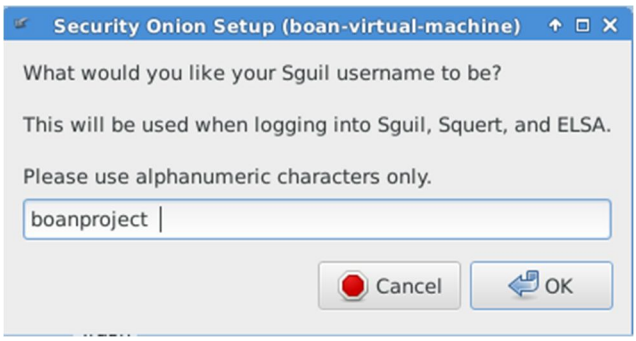
server	분산시스템 구축 시 사용 이벤트 분석용으로 사용시 선택
sensor	분산시스템 구축 시 사용 정보 수집과 침입탐지 수행 탐지된 이벤트가 서버로 전송
Standalone	Server와 Sensor를 모두 구성 수집, 침입탐지, 분석을 한 장비에서 처리



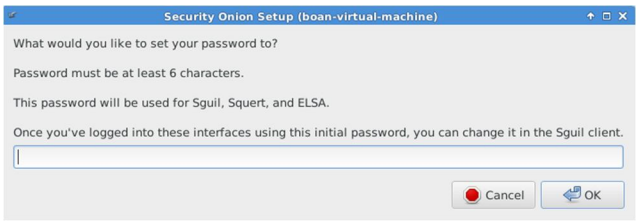
21. 메모리 부족 (최소 3-4GB) 시 시스템 운영의 어려움을 알리는 공고 메시지 [Yes, Continue] 클릭



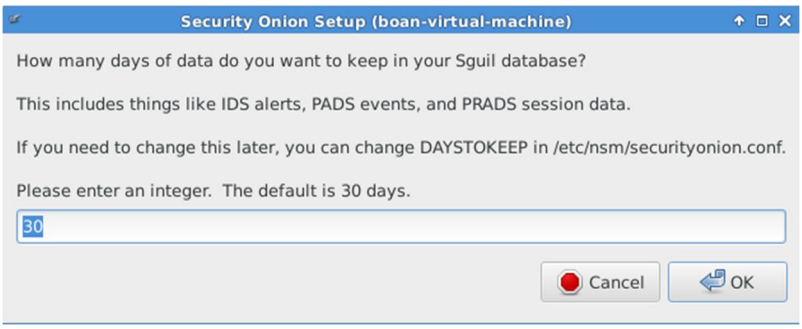
22. 설정값을 기본값 또는 사용자 지정으로 할것인지 선택 [Custom] 선택



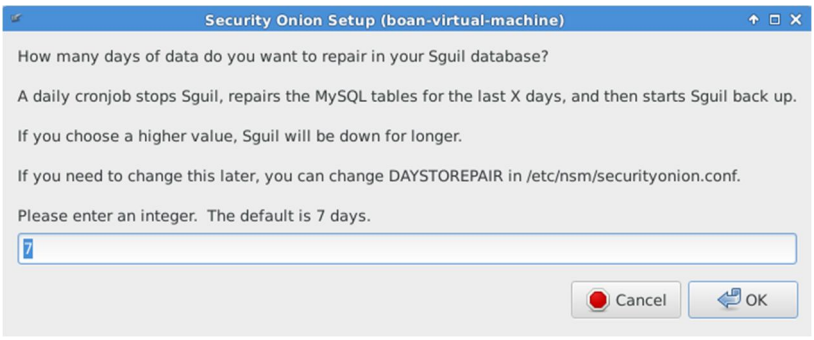
23. 스구일, 스쿼트, 엘사에서 사용될 사용자 이름 지정 [boan] 또는 [boanproject] 입력



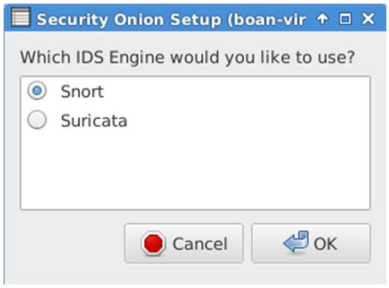
24. 비밀번호 지정, 최소 6글자 [123456]입력



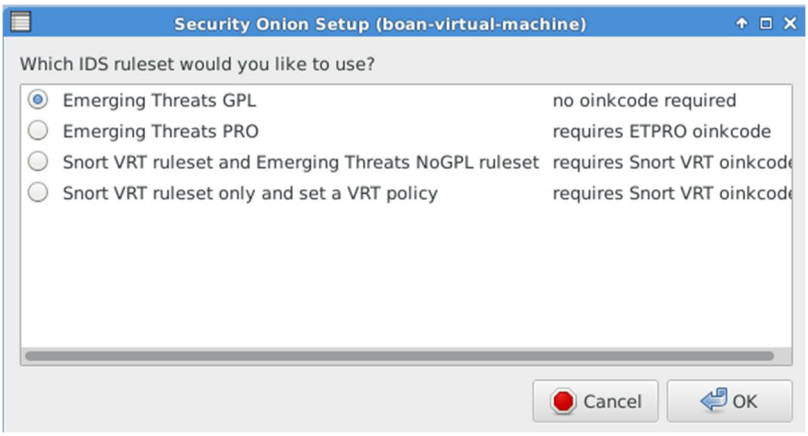
25. IDS 경고, PADS 이벤트 값들을 몇일 동안 보관할 것인지 설정 [30] 입력



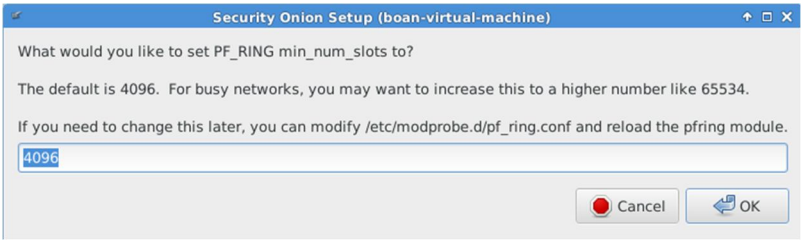
26. 스구일 데이터베이스 자료의 수정 기간 지정 [7] 입력



27. IDS 엔진 선택 [Snort] 선택

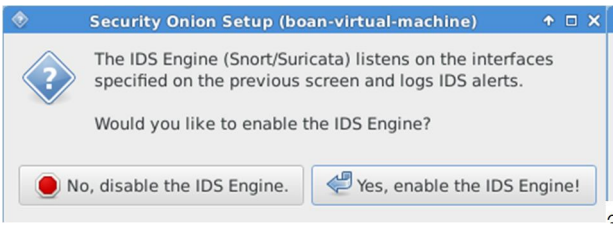


28. IDS 룰셋 선택 [Emerging Threats GPL] 선택

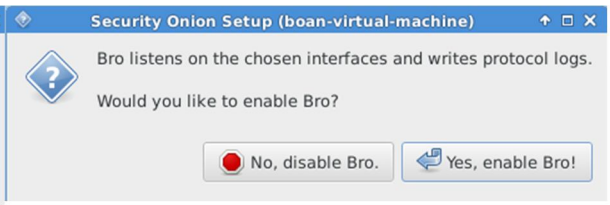


29. PF_RING 의 슬롯 수 지정 [4096] 입력

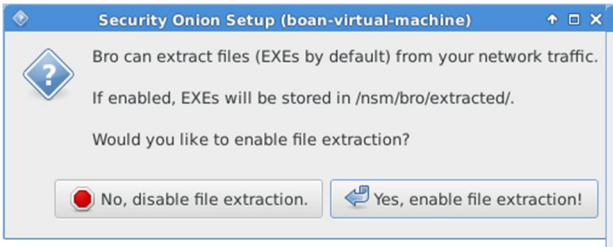
PF_RING : 수신받은 패킷을 사용자 영역으로 전달 할 수 있는 패킷 캡처를 위한 소켓 트래픽이 많으면 65534와 같은 큰값지정



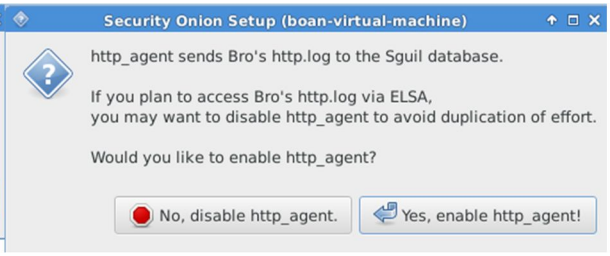
30. IDS 엔진이 사용을 결정
[Yes, enable the IDS Engine] 선택



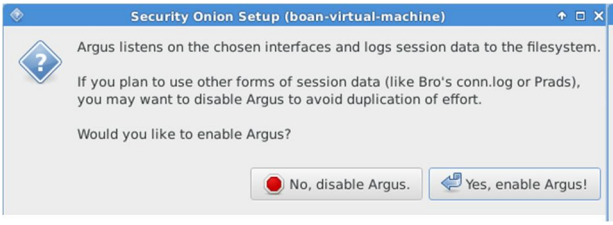
31. 인터페이스에서 bro 활성화 여부 결정
[Yes, enable Bro]



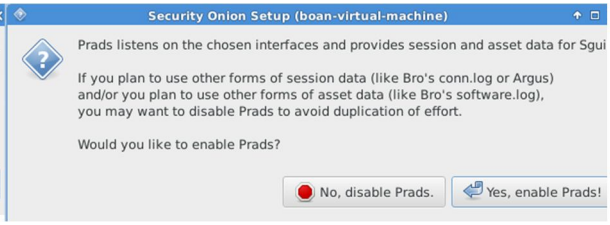
32. 파일 추출 활성화 결정
[No, disable file extraction] 선택



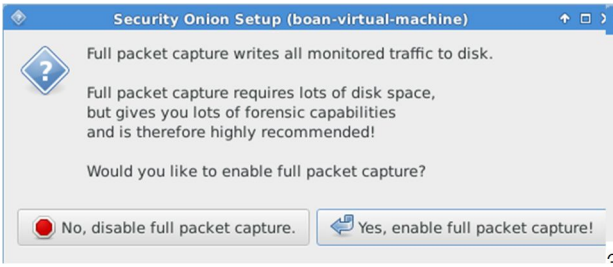
33. http_agent 활성화 결정
[No, disable http_agent] 선택



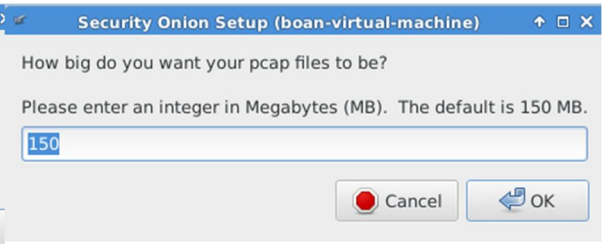
34. 아르고스 활성화 결정 [No, disable Argus]



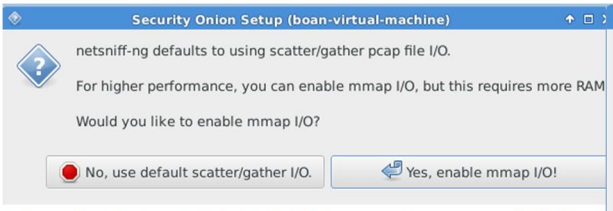
35. Prads 활성화 결정 [No, disable Prads]



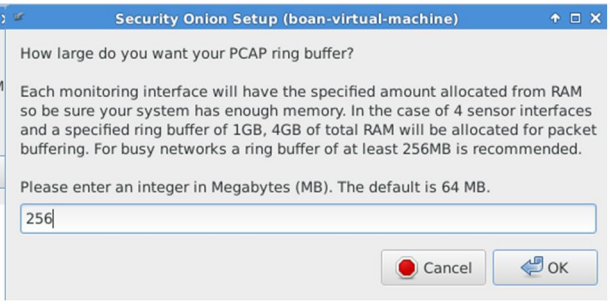
36. 패킷 전체의 캡쳐 기능 사용 결정
[No, disable full packet capture]



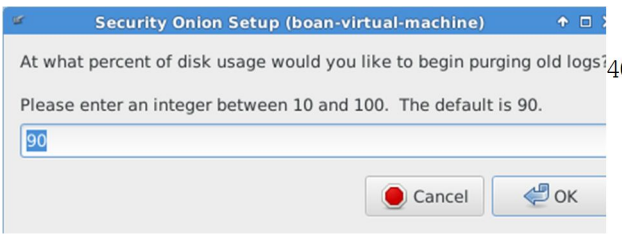
37. pcap 파일의 용량 지정, [150] MB 입력



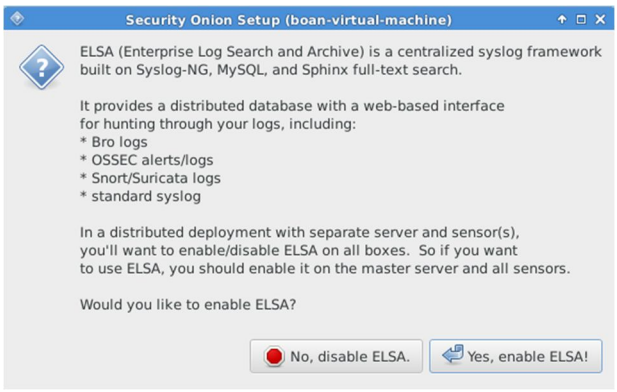
38. netsniffing 종류 결정 [Yes, enable mmap]선택



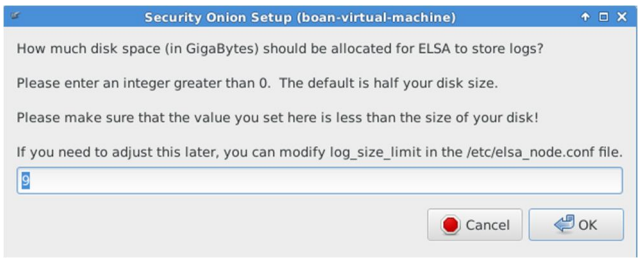
39. PCAP ring 버퍼 크기 지정 [256] 입력



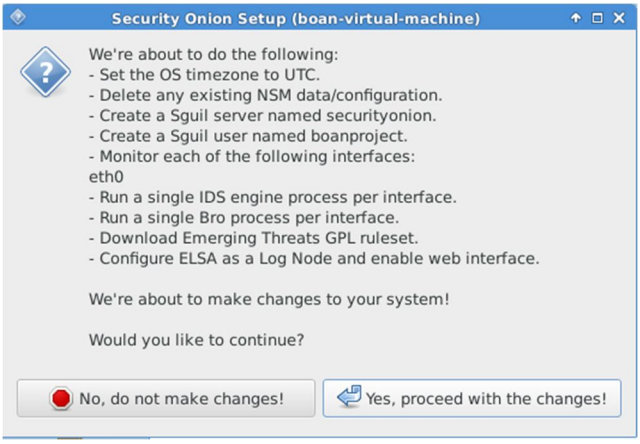
40. 로그 삭제율 지정, [90] 입력
디스크 용량의 90%이상일 때 자동 로그 삭제



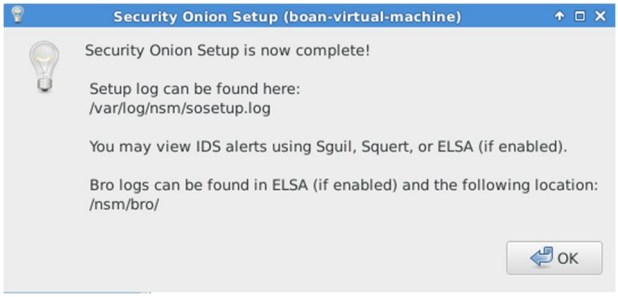
41. 엘사 사용 여부 결정 [Yes, enable ELSA] 선택



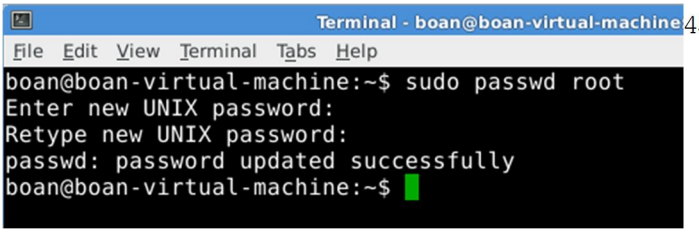
42. 엘사에 사용할 디스크 공간 설정
    - 설정값은 0보다 켜야 함



43. 엘사 설정확인
    [Yes, procced with the changes] 클릭



44. 설정된 모든 도구가 바탕화면에 설치



45. 관리자 패스워드 지정
    sudo passwd root
    1234