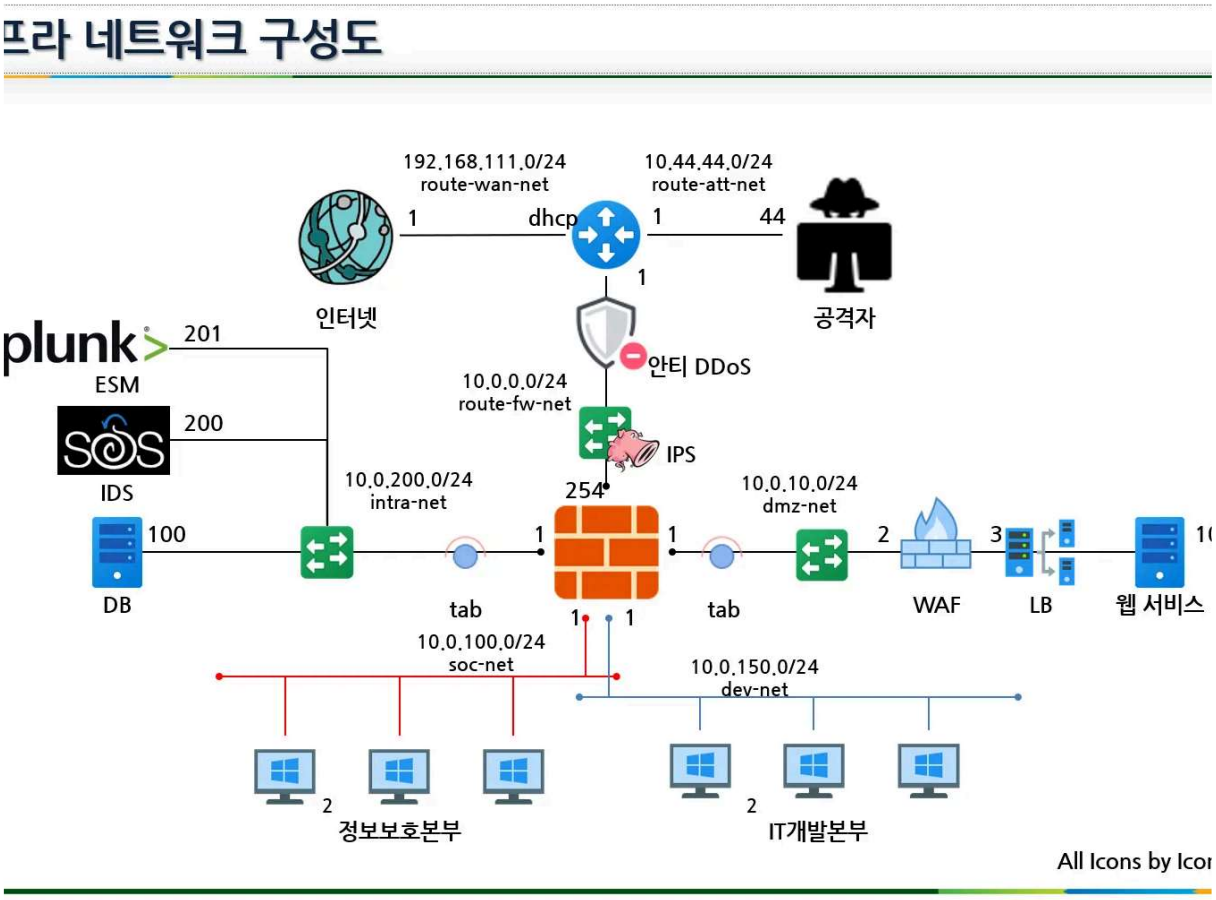
모의해킹 업무 이해



모의해킹 업무 이해

모의해킹 개념

- **모의해킹(Penetration Testing)**은 **해커와 동일한 환경과 조건**, 기술을 가지고 시스템, 네트워크, 애플리케이션 등의 보안 취약점을 식별하고, 그 취약점을 실제로 악용할 수 있는지를 검증하는 과정을 의미

- 보안 전문가가 공격자의 관점에서 시스템을 평가함으로써, 잠재적인 보안 위협을 사전에 발견하고 해결하기 위해 수행
- **Penetration**: 침투, 침입, 침해 + **TEST**: 테스트, 합쳐서 **Pentest**라고도 함

모의해킹 대상

- 모의해킹은 다양한 시스템과 기기를 대상으로 수행
  - **웹 사이트**: 웹 애플리케이션 및 서버의 보안 취약점 점검.
  - **IoT 기기**: 사물인터넷 기기의 보안 취약점 분석. → **자동차(자율주행?)!!!**
  - **모바일 앱**: 안드로이드 및 iOS 애플리케이션의 보안 점검.
  - **정맥인식기**: 바이오메트릭 장치의 보안 검증.
  - **지문인식기**: 지문 인식 시스템의 보안 점검.
  - 기타 다양한 정보 시스템 및 장치.
  - **리버싱 분석 (역공학분석)**
  - **소스코드진단(시큐어진단 - S/W보안 진단원)**

모의해커와 크래커(범죄자) 구분

- 모의해킹과 범죄적으로 사용되는 해킹(크래킹)의 구분은 해당 활동이 합법적인지 여부가 중요
- 모의해킹은 조직과 '계약'을 맺고 허락하에 진행되며, 보안 강화와 취약점 개선을 목표
- 반면, 크래킹은 승인 없이 시스템을 침해하고 악의적인 목적으로 취약점을 악용하는 행위

구분	모의해커	범죄자
합법적 여부	계약 후 진행	합의 없이 진행
공격 항목	네트워크 장애를 유발하는 DDoS, BOF 공격 제외	마음대로
공격 시간	정해진 날짜와 시간	시간 제한 없음
공격 포인트	웹 서비스, 모바일 서비스, IoT 기기	웹 서비스, 모바일 서비스, 개인 컴퓨터 (악성코드 감염)
목적	보안 강화 및 취약점 개선	데이터 탈취, 금전적 이익, 시스템 손상 등
활동 후 결과	보고서 작성 및 보안 권고 제공	피해 및 법적

모의해킹을 하는 이유(법률 명시)

제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2004. 1. 29., 2007. 1. 26., 2007. 12. 21., 2008. 6. 13., 2010. 3. 22.> 7. “침해사고”란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다. ...(중략)...

정보통신망 이용촉진 및 정보보호 등에 관한 법률 | 국가법령정보센터 | 법령 > 본문

https://www.law.go.kr/lsInfoP.do?lsiSeq=111970#0000

제45조의3(정보보호 최고책임자의 지정 등) ① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 기준에 해당하는 임직원을 정보보호 최고책임자로 지정하고 과학기술정보통신부장관에게 신고하여야 한다. 다만, 자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 신고하지 아니할 수 있다. [개정 2014.5.28, 2017.7.26 제14839호(정부조직법), 2018.6.12, 2021.6.8] [[시행일 2021.12.9]] ② 제1항에 따른 신고의 방법 및 절차 등에 대해서는 대통령령으로 정한다. [신설 2014.5.28] [[시행일 2014.11.29]] ③ 제1항 본문에 따라 지정 및 신고된 정보보호 최고책임자(자산총액, 매출액 등 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우로 한정한다)는 제4항의 업무 외의 다른 업무를 겸직할 수 없다. [신설 2018.6.12] [[시행일 2019.6.13]] ④ 정보보호 최고책임자의 업무는 다음 각 호와 같다. [개정 2021.6.8] [[시행일 2021.12.9]] 1. 정보보호 최고책임자는 다음 각 목의 업무를 총괄한다. 가. 정보보호 계획의 수립·시행 및 개선 나. 정보보호 실태와 관행의 정기적인 감사 및 개선 다. 정보보호 위험의 식별 평가 및 정보보호 대책 마련 라. 정보보호 교육과 모의 훈련 계획의 수립 및 시행

국가법령정보센터 | 오류페이지

정확한 한글 주소명인지 확인해 주시기 바랍니다. 자세한 한글주소명 사용법[한글 법령주소]을 확인해 주시기 바랍니다. 동일한 문제가 지속될 경우 아래 번호로 문의해주시기 바랍니다.

https://www.law.go.kr/법령/정보통신망

/IS인증 의무대상자(정보통신망법 제47조 2항)

무대상자는 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용
공하거나 정보의 제공을 매개하는 자로서 표에서 기술한 의무대상자 기준에 하나라도 해당되는 자이다.

구분	의무대상자 기준
ISP	「전기통신사업법」 제6조제1항에 따른 허가를 받은 자로서 서울특별시 및 모든 광역시에서 정보통신망서비스를 제공하는
IDC	정보통신망법 제46조에 따른 집적정보통신시설 사업자
음의 조건 중 나도 해당하는 자	연간 매출액 또는 세입이 1,500억원 이상인 자 중에서 다음에 해당되는 경우 - 「의료법」 제3조의4에 따른 상급종합병원 - 직전연도 12월 31일 기준으로 재학생 수가 1만명 이상인 「고등교육법」 제2조에 따른 학교
	정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자
	전년도 직전 3개월간 정보통신서비스 일일평균 이용자 수가 100만명 이상인 자

KISA 정보보호 및 개인정보보호관리체계 인증 ISMS-P 인증대상

의무대상자 기준에 해당하지 않으나 자발적으로 정보보호 및 개인정보보호 관리체계를 구축·운영하는 기업·기관은 임의신청자로 분류되며, 임의신청자가 인증 취득을 희망할 경우 자율적으로 신청하여 인증심사를 받

https://isms.kisa.or.kr/main/ispims/target/

모의해킹 업무 절차

- 일반적인 모의해킹 업무 절차

절차	설명
사전협의단계	담당고객(관리실무자)와 프로젝트 진행 범위 결정
정보수집단계	점검할 대상에 대해 어떤 서비스인지, 외부에 노출되어 있는 정보들이 어떤 것인지 모든 정보 수집
위협모델링단계	수집된 정보 중에서 서비스와 비교를 하여 보안적인 문제가 발생할 수 있는 부분 분류
취약점 분석 단계	진단 항목에 맞게 어떤 취약점들이 도출될 수 있는지 확인
침투단계	시나리오 기반으로 각 진단 항목을 서비스에 대입하여 침투 여부 확인
내부침투단계	1차 침투가 완료된 후에 2차, 3차로 내부 시스템 침투 여부 확인
보고서 작성	도출된 취약점 위협평가, 영향도를 반영하여 결과 보고 작성

Penetration Testing Execution Standard

- **PTES**는 침투 테스트를 수행하는 데 있어 체계적이고 표준화된 접근 방식을 제공하기 위한 프레임워크