사물인터넷융복합논문지 Vol. 11, No. 2, pp. 179-184, 2025 https://doi.org/10.20465/KIOTS.2025.11.2.179

중소기업대상 자동화침투 테스트기반 보안취약점 분석 및 대응모델 설계
-Pentera Core 적용 사례를 중심으로-

이근호*
백석대학교 컴퓨터공학부 교수

Design of a Security Vulnerability Analysis and Response Model Based on Automated Penetration Testing for SMEs
-A Case Study Using Pentera Core-

Keun-Ho Lee*
Professor, Div. of Computer Engineering, BaekSeok University

요 약 중소기업은 보안 인력과 예산의 제약으로 인해 실효성 있는 보안 점검에 어려움을 겪고 있다. 본 연구는 자동화 침투 테스트 솔루션인 Pentera Core를 활용하여 중소기업의 실제 보안 취약점을 분석하였다. Black Box 기반 테스트를 통해 계정 탈취, 권한 상승, 랜섬웨어 시뮬레이션 등의 위협을 실시간으로 검증하였다. 테스트 결과, 대부분의 기업에서 암호 재사용, 패치 미적용 등 기본 보안 수칙이 미준수된 것이 확인되었다. 이에 따라 단계별 대응 프로세스를 설계하고, 위험 기반 우선순위 설정과 재점검 체계를 제안하고자 한다. 또한 PTaaS(Pentest as a Service) 형태로의 도입 가능성을 통해 현실적 보안 운영 방안을 제안하였다. 이 모델은 중소기업의 보안 수준 향상뿐 아니라 향후 공공·금융 분야로의 확장성도 갖춘다.

주제어 : 정보보호, 모의해킹, 취약점, 자동화, 대응방안

Abstract Small and medium-sized enterprises(SMEs) often face challenges in conducting effective security assessments due to limitations in security personnel and budget. This study analyzes real-world security vulnerabilities in SMEs using an automated penetration testing solution, Pentera Core. By employing Black Box-based testing, threats such as credential theft, privilege escalation, and ransomware simulation were validated in real time. The results revealed that most organizations failed to comply with basic security practices, such as avoiding password reuse and applying critical patches. Based on these findings, a step-by-step response framework was designed, including risk-based prioritization and revalidation processes. Furthermore, the study proposes a practical security operation model through the adoption of Pentest as a Service(PTaaS). This approach not only enhances the cybersecurity posture of SMEs, but also offers scalability for future adoption in public and financial sectors.

Key Words : Cybersecurity, Pentesting, Vulnerabilities, Automation, Mitigation

*이 논문은 2025학년도 백석대학교 학술연구비 지원을 받아 작성되었음
*교신저자 : 이근호(root1004@bu.ac.kr)
접수일: 2025년 03월 02일 수정일: 2025년 04월 12일 심사완료일: 2025년 04월 15일

1. 서론

디지털 전환이 가속화됨에 따라 정보보안의 중요성은 전 산업군에 걸쳐 크게 부각되고 있다. 특히 사이버 공격의 지능화와 자동화는 전통적인 보안 체계를 손쉽게 우회할 수 있게 되었으며, 이로 인해 조직의 규모와 관계없이 누구나 사이버 위협의 주요 대상이 될 수 있는 환경이 형성되고 있다. 이러한 환경 속에서 대기업이나 공공기관은 비교적 탄탄한 보안 인프라와 전문 인력을 바탕으로 위협에 대응할 수 있는 반면, 중소기업은 보안 전문 인력의 부재, 예산 제약, 체계적인 대응 프로세스 부족 등의 문제로 인해 더욱 취약한 상황에 놓여 있다.

중소기업의 이러한 보안 취약성은 실제 침해사고 통계와 피해 사례를 통해 확인되고 있으며, 이는 단순히 개별 기업의 손실에 그치지 않고 협력 생태계 전체의 위험 요소로 작용할 수 있다. 예컨대, 공급망 공격의 사례에서 보듯, 대기업이나 정부기관의 보안망이 우회되는 통로로 중소기업이 악용되는 경우가 빈번하다. 그러나 현실적으로 대부분의 중소기업은 보안 점검을 외부 컨설팅에 의존하고 있으며, 그마저도 연 1회 이내의 정기적 점검에 그치는 경우가 많다. 더욱이, 수동적 방식의 취약점 점검은 공격자의 실제 관점과 괴리가 있어 대응 효과에 한계가 있다.

이에 따라 최근 보안 분야에서는 자동화된 침투 테스트를 기반으로 한 능동적 위협 진단 기법이 주목받고 있다. 이 방식은 실제 공격자와 유사한 방식으로 시스템을 점검함으로써, 단순한 취약점 나열이 아닌 '실제 침투 가능한 경로'를 도출해내는 데 초점을 둔다. 본 연구는 이러한 관점에서, Pentera Core라는 자동화 침투 테스트 솔루션을 활용하여 국내 중소기업의 실제 운영 환경에서 나타나는 보안 취약점을 분석하고, 이를 기반으로 단계적 대응 프로세스 및 적용 가능한 대응모델을 설계하고자 한다.

Pentera Core는 비인가 접근, 권한 상승, 정보 유출, 랜섬웨어 감염 등 다양한 공격 시나리오를 자동으로 시뮬레이션할 수 있으며, 테스트 결과를 기술 및 경영 관점으로 구분된 보고서 형태로 제공하는 기능을 갖추고 있다. 본 연구에서는 이 도구를 실환경에 적용하여 보안 실태를 계량화하고, 발견된 위협요소에 기반한 우선순위 대응 체계를 설계함으로써, 중소기업의 정보보호 수준을 실질적으로 향상시킬 수 있는 방안을 제시하고자 한다.

또한 본 연구는 Pentera 기반 위협 진단의 결과를 서비스형 침투 테스트(Pentest as a Service, PTaaS) 형태로 확장하는 방안까지를 아우르며, 자원이 제한된 조직이 정기적이고 효율적인 방식으로 보안 점검과 대응을 이어갈 수 있는 실용적인 모델을 제안한다. 이를 통해 본 논문은 중소기업의 보안 리스크를 실질적으로 줄이고, 나아가 공공 및 금융 등 다른 산업 영역으로의 확산 가능성을 함께 제시하는 데 그 목적이 있다.

2. 관련 연구

2.1 중소기업 보안 환경의 한계와 과제

중소기업은 대기업에 비해 보안 인프라와 인력, 예산이 현저히 부족한 현실에 놓여 있다. 실제로 정보보안 전담 인력이 없는 중소기업의 비율은 국내에서 70%를 상회하며, 보안 투자는 대부분 외부 컨설팅이나 간헐적 취약점 진단에 의존하는 구조를 보이고 있다[1,6]. 이에 따라 해킹, 악성코드 감염, 랜섬웨어 등 사이버 위협에 대한 대응이 사후적인 수준에 머무는 경우가 많고, 침해사고가 발생해도 원인 분석이나 개선 조치가 체계적으로 이루어지지 못하는 한계가 있다[1,8]. 이러한 상황에서 중소기업의 보안 수준을 객관적으로 진단하고, 실제 위협에 기반한 능동적 보안 대응 체계 마련의 필요성이 제기되고 있다[3,10]. 최근 정부 주도하에 정보보호 컨설팅이나 보안 솔루션 지원 사업이 활성화되고 있으나, 단발성에 그치는 경우가 많아 실질적인 보안 역량 제고에는 한계가 있다[6].

2.2 침투 테스트 및 자동화 보안 진단 기술

전통적인 침투 테스트는 숙련된 보안 전문가가 수작업으로 시스템의 취약점을 탐지하고, 이를 기반으로 공격 시나리오를 구성해 실제 침입 가능성을 검증하는 방식이다[2,11]. 이러한 방법은 높은 정확성과 맞춤형 분석이 가능하다는 장점이 있지만, 비용과 시간이 많이 소요되고 반복 수행이 어렵다는 단점도 존재한다. 또한 보안 인력이 부족한 중소기업에서는 이러한 고도화된 서비스를 지속적으로 운영하기 어렵다는 현실적인 문제가 있다[4,6]. 이와 같은 한계를 보완하기 위해 등장한 것이 자동화 침투 테스트 기술이다. 이 기술은 공격자 관점의 위협 시나리오를 자동으로 실행하고, 침투 성공 여부를 기반으로 실제적인 보안 취약성을 도출하는 방식이다[2,13,15]. 자동화 도구들은 반복 수행이 가능하고, 광범위한 자산에 대한 점검을 단시간 내 수행할 수 있어 중소기업 환경에 적합한 기술로 평가받고 있다[3,5]. 대표적

인 예로 Pentera, Cymulate, AttackIQ 등의 상용 솔루션이 있으며, MITRE ATT&CK, NIST SP 800-115 같은 글로벌 프레임워크에서도 자동화 기반 검증을 점차 강조하고 있다[2,12].

2.3 Pentera Core의 기술 특성

Pentera Core는 전 세계 600개 이상의 기업에 도입된 자동화 침투 테스트 솔루션으로, 내부망 환경에서 발생할 수 있는 실질적인 보안 위협을 공격자 시각에서 실시간으로 시뮬레이션하는 기능을 제공한다[5,13]. Black Box, Credential Attack, Lateral Movement, Ransomware Simulation 등 다양한 시나리오를 지원하며, [Fig 1]은 공격 경로를 시각화한 'Attack Map'을 통해 침해 흐름을 직관적으로 파악할 수 있는 것이 특징이다[13,14].

또한 Pentera는 관리자 계정 탈취, 권한 상승, 비인가 공유폴더 접근, AD 정보 수집 등 실제 침해 사례에 기반한 테스트 항목을 자동으로 수행하고, 테스트 결과를 기술자용과 경영진용 보고서로 분리하여 제공한다[5,13,15]. 이러한 특성은 단순한 취약점 나열을 넘어 위협 기반의 실제 대응 전략 수립을 가능하게 한다. 해외에서는 이미 금융, 제조, 의료, 공공기관 등 다양한 산업군에서 Pentera를 도입해 정보보호 수준 향상과 ISMS, ISO27001, NIST CSF 등 인증 대응에 활용하고 있으며[3,5,13], 국내에서도 일부 대기업과 보안 서비스 기업을 중심으로 도입이 확산되고 있다. 그러나 중소기업 차원에서 이를 체계적으로 적용한 국내 연구는 드물며, 본 연구는 실제 중소기업을 대상으로 Pentera Core를 활용한 적용 사례를 분석하고, 이를 기반으로 보안 대응 모델을 제시한다는 점에서 의의가 있다.

3. 연구방법론

3.1 연구 설계 및 대상 기업 선정

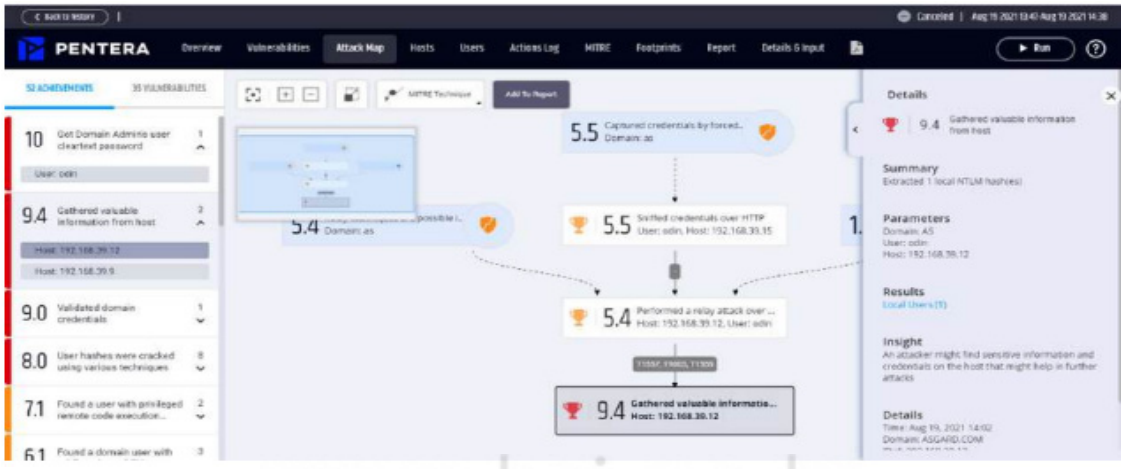
본 연구는 국내 중소기업을 대상으로 Pentera Core 기반의 자동화 침투 테스트를 적용하고, 실제로 식별된 보안 취약점을 분석하여 이를 바탕으로 위협 대응 중심의 보안 모델을 설계하는 것을 목적으로 한다. 연구 설계는 다음과 같은 절차에 따라 수행되었다.

- 대상 기업 선정

수도권과 충청권에 위치한 제조, 유통, IT서비스 중소기업 5개사를 선정하였다. 기업당 평균 임직원 수는 50인 이하로, 독립된 네트워크 및 Windows 기반 내부망, Active Directory(AD) 기반 사용자 관리 체계를 갖추고 있었다.

- 환경 사전 점검

각 기업의 정보보호 관리자 또는 시스템 담당자와의 인터뷰를 통해 현재 운영 중인 보안 솔루션, 네트워크 구성, 서버 및 사용자 수 등을 파악하였다. 사전 점검 결과, 대부분의 기업은 방화벽, 백신 외에 추가적인 위협 탐지 시스템이 없었으며, 취약점 점검은 연 1회 수준으로 외부 업체에 의존하고 있는 상황이었다.



[Fig. 1] Attack Map Tab(Kill Chain)

〈Table 1〉 Overview of Key Features and Expected Outcomes of Pentera Core Attack Scenarios

Item	Function Description	Expected Outcome
Attack Map	Visualization based on attack kill chain	Analysis of intrusion paths and visualized response plan
Credential Exposure	Password cracking and reused credential identification	Guidance for improving account and password policies
Lateral Movement	Simulation of lateral movement between internal users and systems	Review and improvement of network segmentation policies
Shadow Admin Detection	Detection of unauthorized administrator privileges	Measures to prevent privilege escalation
Ransomware Simulation	Execution of scenarios targeting file encryption and backup disruption	Simulation-based preparedness against ransomware attacks
Reporting Module	Automatic generation of technical and executive-level reports	Simplified internal reporting and communication process

- 테스트 목적 정의

단순한 취약점 스캐닝을 넘어, 실제 침투 경로를 자동화된 방식으로 검증함으로써 "공격자의 입장에서 어떤 행위가 가능한가"를 중심으로 테스트 목적을 설정하였다. 따라서 보안 수준의 정량적 평가 외에도 시나리오 기반 위협 인지 및 대응 전략 수립을 목적으로 하였다.

3.2 Pentera Core 기반 자동화 침투 테스트 구성

본 테스트는 Black Box 방식으로 진행되었으며, 이는 인증 정보 없이 외부 침입자의 관점에서 공격을 시작하는 시나리오를 의미한다. 공격자의 위치는 내부망 내 노드로 설정하여, 실제 조직 내에서 발생할 수 있는 내부 위협 중심의 상황을 재현하도록 구성하였다. 또한 테스트 과정에서는 Silent Mode를 적용하여, SIEM(Security Information and Event Management), EDR(Endpoint Detection and Response) 등 기존 보안 장비의 탐지 및 운영에 영향을 주지 않는 범위 내에서 비가시성 테스트를 수행하였다.

〈Table 1〉은 주요 테스트 기능에 대한 내용을 보여주고 있다. 테스트는 초기 환경 설정 및 대상 자산 탐지부터 시작하여, 취약점 자동 탐색과 익스플로잇 시도, 공격 경로 시뮬레이션 및 영향도 분석을 거쳐 테스트를 종료하고 자동 보고서를 생성한 뒤, 각 기업별 설명회 및 결과 브리핑을 통해 최종 피드백을 제공하는 절차로 진행되었다.

3.3 데이터 분석 및 대응모델 도출 절차

테스트 수행 이후, 도출된 결과를 바탕으로 보안 취약점 유형을 분류하고, 이에 대응하는 보안 대응 모델을 제안하였다. 본 테스트를 통해 기업당 평균 34건의 취약점이 도출되었으며, 주요 유형은 패치 미적용(34%), 취약한 암호 정책 및 계정 재사용(28%), SMB 및 RDP 등 비암호화 서비스 노출(19%), 비인가 권한 보유 사용자(11%), 불완전한 네트워크 분리(8%)로 나타났고, 기업 유형별로는 제조업체에서 공유폴더 권한 설정 오류가 빈번했으며, IT서비스 기업에서는 암호 정책 미비와 사내 개발용 테스트 계정 방치가 주요 취약점으로 확인되었다. 위협 기반 대응모델 설계로 도출된 분석 결과를 기반으로 〈Table 2〉와 같은 단계별 대응 프로세스를 설계하였다. PTaaS 기반 운영 방안은 Pentera 테스트 결과와 분석 보고서는 PTaaS 형태로 정기적(분기별) 점검 모델에 따라 1회차 전체 자산 기반 공격 경로 점검, 2회차 개선 여부 확인 및 특정 영역 집중 점검, 3회차 신규 위협 및 정책 위반 점검의 순환 구조로 제공 가능하며, 이는 ISMS-P 인증 대응에도 활용할 수 있도록 설계되었다.

〈Table 2〉 Step-by-Step Threat-Based Security Response Model Using Pentera

Step	Description	Key Tool/Method
Step 1	Automated assessment using Pentera	Auto Pentesting Scenario
Step 2	Classification of vulnerabilities and risk rating	CVSS, Pentera Score
Step 3	Establishment of response measures and guidelines	Remediation sheet by vulnerability
Step 4	Reassessment after remediation	Effectiveness verification via retest
Step 5	Documentation and reporting	Dual reports for executives and staff

4. 분석결과

본 연구에서 수행한 Pentera Core 기반의 자동화 침투 테스트를 통해 도출된 보안 진단 결과를 종합한 결과, 기업당 평균 38건의 취약점이 발견되었으며, 그 중 약 70%는 보안 패치 미적용 또는 Credential Reuse(계정 재사용)에 관련된 항목으로 나타났다. 이는 대부분의 기업이 기본적인 보안 유지 관리에 있어 체계적인 정책을 수립하지 못하고 있음을 시사한다.

특히 Ransomware Simulation 항목에서는 5개 기업 중 3개 기업에서 Admin 권한 탈취가 가능한 상태로 확인되었다. 해당 기업들은 공격 시나리오 실행 후 파일 시스템 내 중요한 자료 암호화 가능 여부까지 확인되었으며, 백업 서버의 네트워크 접근 통제 미흡도 함께 드러났다. 이는 실제 침해사고 발생 시, 피해 확산 가능성이 매우 높다는 점을 반영한다.

또한 Credential Exposure 항목 분석 결과, 외부에서 유출된 과거 계정 목록과 현재 Active Directory 내 존재하는 계정 간의 문자열 유사도를 비교한 결과, 약 80% 이상의 유사도를 보이는 경우가 다수 발견되었다. 이는 동일한 ID/PW 조합의 반복 사용 또는 약간의 변형을 통한 계정 사용이 보편화되어 있으며, 이로 인해 계정 기반 공격에 매우 취약한 구조를 가지고 있음을 의미한다.

이러한 결과는 단순한 취약점 탐색을 넘어, 공격자가 실제로 내부 시스템을 어떻게 장악할 수 있는지를 명확히 시각화함으로써, 중소기업이 반드시 대응 체계를 강화해야 하는 보안 리스크의 실체를 구체적으로 보여준다.

5. 대응 모델 설계

5.1 위협 기반 보안 점검 프로세스

분석 결과를 바탕으로, 본 연구에서는 위협 중심의 보안 점검 및 대응 프로세스를 4단계로 설계하였다. 첫째, Pentera Core의 자동화 시나리오를 활용하여 실제 공격 경로 기반의 테스트를 수행한다. 둘째, 발견된 취약점에 대해 CVSS 점수 및 Pentera 내부 스코어를 기준으로 위험도를 산정하고 우선순위를 도출한다. 셋째, 각 취약점별로 맞춤형 대응 가이드를 제공하고, 조직 내 기술 인력 또는 외부 보안 컨설턴트를 통해 조치 이행을 유도한다. 마지막으로, 대응 조치 이후 재테스트를 통해 위험 해소 여부를 검증하고, 해당 내용을 기반으로 리스크 리포트를 정리한다. 이 프로세스는 기존의 취약점 진단이 '리스트 나열'에 그치는 한계를 극복하고, 공격자의 실제 행위 흐름에 기반한 대응 중심의 평가체계로 진화할 수 있는 기반을 제공한다.

5.2 중소기업 맞춤형 도입 전략

중소기업의 보안 자원 및 운영 여건을 고려할 때, 본 연구에서 제안하는 대응 모델은 SaaS 기반의 PTaaS 형태로 운용하는 것이 가장 현실적인 방식으로 판단된다. 이 서비스는 분기별 1회 Pentera 기반 자동화 테스트를 수행한 후, 분석 결과에 따른 취약점 요약 리포트 및 대응 가이던스를 제공하는 구조로 운영된다. 해당 모델은 단순한 테스트 결과 제공에 그치지 않고, 보안 자문을 포함한 사후관리 프로세스를 포함할 수 있으며, 또한 ISMS-P 인증 대응체계와도 연계될 수 있어 실무 적용성과 제도적 활용 가능성 모두를 확보할 수 있다. 궁극적으로는 중소기업이 자체적으로 관리하기 어려운 보안 점검과 리스크 대응을 전문가와 자동화 시스템이 분담하여 수행하는 하이브리드 보안 운영 모델로 확장될 수 있다.

6. 결론

본 연구는 보안 인력과 예산의 제약으로 인해 실효성 있는 보안 점검이 어려운 중소기업 환경에서, Pentera Core를 활용한 자동화 침투 테스트가 얼마나 효과적으로 위협을 식별하고 대응 체계를 설계할 수 있는지를 실증적으로 분석하였다. 테스트 결과를 통해 중소기업 내부에는 실제 침해로 이어질 수 있는 구조적 위험 요소가 다수 존재함을 확인하였고, 이를 기반으로 한 위협 기반 대응모델은 실질적 보안 개선 효과뿐만 아니라 재테스트를 통한 검증 가능성까지 포함하고 있어 지속 가능한 보안 운영 체계로의 전환 가능성을 보여주었다. 또한 본 연구는 해당 모델을 PTaaS 서비스 형태로 발전시킴으로써, 단발성 진단을 넘어서 분기별 주기적 보안 점검과 컨설팅이 결합된 선순환 보안 프레임워크를 제시하였다. 이는 향후 국내 환경에 맞춘 보안 자동화 도입 전략의 기반이 될 수 있으며, 공공기관이나 금융기관 등 보다 높은 보안 수준이 요구되는 분야로도 확장 적용할 수 있는 실용적 가능성을 제시한 점에서 의미가 있다.

REFERENCES

[1] S.H.Park and H.J.Ryu, "A Practical Approach to Cybersecurity Risk Assessment in Korean SMEs," Asia-Pacific Journal of Information Security, Vol.12, No.1, pp.25-42, 2021.

[2] R.Zhang, "Automated Penetration Testing Tools and Their Role in Security Validation," Cybersecurity Engineering Review, Vol.9, No.3, pp.150-164, 2020.

[3] M.Alqahtani and Y.Alotaibi, "Threat Modeling and Vulnerability Prioritization for Small Enterprises," International Journal of Cyber Risk Management, Vol.6, No.4, pp.215-229, 2022.

[4] H.J.Kang, "Implementation Challenges of Pentesting-as-a-Service (PTaaS) for SMEs," Korean Journal of Information Assurance, Vol.18, No.2, pp.98-115, 2021.

[5] E.Laurent, "Red Team Automation: A Next-Generation Approach to Continuous Security Testing," Journal of Offensive Security Research, Vol.5, No.1, pp.41-59, 2020.

[6] N.S.Choi and J.H.Park, "Case-Based Security Consulting Model for Small Businesses in Korea," Journal of Industrial Information Systems, Vol.11, No.3, pp.67-84, 2019.

[7] T.Mitchell and A.Flores, "Real-Time Vulnerability Simulation Using Pentera-Like Systems," Computational Security Studies, Vol.7, No.4, pp.110-128, 2022.

[8] B.R.Lee, "Developing a Security Maturity Model for Small-Scale Enterprises," Journal of Korean Information Systems, Vol.23, No.1, pp.55-73, 2020.

[9] S.Roy and M.Thomas, "AI-Augmented Threat Discovery in Hybrid Enterprise Environments," Information Systems Security Review, Vol.16, No.2, pp.133-149, 2021.

[10] Y.Nakamoto, "Quantitative Cyber Risk Analysis for SMEs Using Dynamic Threat Modeling," International Journal of SME IT Governance, Vol.8, No.3, pp.92-110, 2022.

[11] D.Martinez, "Evaluating Endpoint Security Solutions for Small Businesses," International Journal of Cybersecurity, Vol.15, No.4, pp.220-234, 2022.

[12] K.Tran, J.Lin, and M.Russo, "Deep Hierarchical Reinforcement Agents for Automated Penetration Testing," arXiv preprint, arXiv:2109.06449, 2021.

[13] C.Skandylas and M.Asplund, "Automated Penetration Testing: Formalization and Realization," IEEE Symposium on Security and Privacy, pp.112-129, 2024.

[14] M.C.Ghanem, A.Azzouni, and F.Lecroq, "ESASCF: Optimized Automation of Network Security Compliance," arXiv preprint, arXiv:2307.10967, 2023.

[15] Y.Akhurayyif and Y.S.Almarshdy, "Adopting Automated Penetration Testing Tools in Small Organizations," International Journal of Cybersecurity, Vol.12, No.3, pp.45-62, 2024.

이 근 호(Keun Ho Lee) [종신회원]

- 2006년 8월 : 고려대학교 컴퓨터학과(이학박사)
- 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
- 2010년 3월 ~ 현재 : 백석대학교 컴퓨터공학부 교수

〈관심분야〉
침해사고대응, 융합보안, 개인정보보호, 블록체인, 산업보안, 취약점분석, 모의해킹 등