지능형 사이버 훈련장의 기술 동향

Technological Trends in Intelligent Cyber Range

유재학 (J.H. Yu, dbzzang@etri.re.kr) 네트워크·시스템보안연구실 선임연구원
구기종 (K.J. Koo, kjkoo@etri.re.kr) 네트워크·시스템보안연구실 책임연구원
김익균 (I.K. Kim, ikkim21@etri.re.kr) 정보보호연구본부 책임연구원/본부장
문대성 (D.S. Moon, daesung@etri.re.kr) 네트워크·시스템보안연구실 책임연구원/실장

ABSTRACT

As the interest in achieving an intelligent society grows with the fourth industrial revolution's development, information and communications technologies technologies like artificial intelligence (AI), Internet of Things, virtual reality, information security, and blockchain technology are being actively employed in different fields for achieving an intelligent society. With these modifications, the information security paradigm in industrial and public institutions, like personal sensitive data, is quickly changing, and it is exposed to different cyber threats and breaches. Furthermore, as the number of cyber threats and breaches grows, so does the need for rapid detection and response. This demand can be satisfied by establishing cyber training programs and fostering experts that can improve cyber security abilities. In this study, we explored the domestic and international technology trends in cyber security education and training facilities for developing experts in information security. Additionally, the AI technology application in the cyber training ground, which can be established to respond to and deter cyber threats that are becoming more intelligent, was examined.

KEYWORDS artificial intelligence, cyber attack, information security, intelligent cyber range, reinforcement learning

Ⅰ. 서론

최근 ICT 기술과 4차 산업혁명에 따른 초연결 인프라 구축으로 디지털 사회, 사이버 공간으로의 전환이 빠르게 진행되고 있다. 이러한 환경에서의 무분별한 데이터 활용과 정보 공개는 악의적인 해킹 및 위협 등의 사이버 공격에 쉽게 노출될 가능성이 크다. 사이버 공간에서는 보호 대상의 증가, 이전보다 자동화되고 신기술로 무장한 다양한 사이버 공격에 대응하기 위해 보안 패러다임도 빠르게 변화

* DOI: https://doi.org/10.22648/ETRI.2022.J.370405
* 이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임[No. 2022-0-00961, 자가진화형 AI 기반 사이버 공방 핵심원천기술 개발].

하고 있다[1-3]. 더욱이 COVID-19 시대를 거치며 물리 세계와 사이버 세계의 경계가 더욱 모호해지고 있으며, 사이버 환경에서의 위협이 물리 세계에까지 영향을 미치는 양상으로 발전하고 있다. 특히, 사이버 공간 확대로 개인·산업·국가시설 등에 사이버 공격 및 보안 위협이 폭넓게 증가하고, 국가 간의 사이버안보 위협에 대한 경쟁은 더욱 치열해질 것으로 전망된다. Statista 2022의 전 세계 사이버 보안 시장 규모 및 전망을 살펴보면, 2021년 2,179억 달러를 시작으로 2026년에는 3,454억 달러로 성장할 것으로 예상하였다[4]. 결과적으로 효율적인 사이버 보안 환경 구축 및 운영을 포함한 사이버 보안 시장은 높은 성장률을 지속할 것으로 보인다.

사이버 공간에서의 공격은 날로 고도화 및 대량화되고 있을 뿐만 아니라 새로운 기술로 무장한 공격 주기도 짧아지고 있어, 그 피해를 최소화하기 위한 방어전략 연구 및 전문인력 양성은 필수적이다[5,6]. 이러한 이유로 사이버 환경에서의 보안 역량을 강화할 수 있는 교육 프로그램 개발 및 전문인력 양성을 위한 사이버 훈련장(Cyber Range)에 대한 필요성이 증가하고 있다[5]. 현재까지의 사이버 훈련장은 전문가의 경험에 의존한 시나리오 기반의 문제풀이 방법이 일반적이다[5,6]. 특히, 일반인을 사이버 보안 전문가로 양성하기 위한 기존의 교육 프로그램들은 이기종 네트워크, 복잡한 보안체계 등을 고려한 훈련과는 거리가 멀었다. 즉 새로운 기술의 사이버 공격 도구, 고정된 훈련 시나리오, 복합적인 공격, 실제 환경을 고려한 공격 등에 대한 훈련과 대응이 어려운 실정이다. 무엇보다 실제로 운용되고 있는 환경이나 서비스를 대상으로 공격도구나 훈련 시나리오의 실행은 많은 제약사항 및 위험부담이 존재하기 때문에 실 환경에서 실행이 불가능하다.

최근 연구문헌 및 기술 동향에 의하면, 국방·산업·스마트시티 등의 다양한 분야에서 보안 위협이 증가하고 있다[1,6]. 특히, 인공지능 기술을 활용한 복잡하고 다양한 공격 시나리오 및 도구를 생성한 공격이 활발한 상황이다. 하지만, 이에 적합한 방어전략을 수립하고 실행하기 위한 전문가의 분석과 비용적인 측면에서 한계에 다다르고 있다. 무엇보다 공격 대상이 되는 ICT 인프라의 복잡한 환경정보와 네트워크 토폴로지 등을 반영한 가상의 훈련장 생성에 많은 어려움을 겪고 있다. 따라서, 사이버 훈련장에서는 훈련 목적에 따른 도메인 환경 적용 및 공격 시나리오의 자율적인 생성, 선제적 조치와 방어 훈련을 수행함으로써 보안 역량을 제고할 수 있어야 한다. 또한, 방어전략 수립 및 훈련에서는 공격을 탐지·분석·대응·예방 등이 순환적으로 실행하고 재훈련할 수 있는 일련의 과정을 포함해야 한다[7].

본고의 Ⅱ장에서는 정보보안 분야에서의 전문인력 교육 및 양성을 위한 사이버 훈련장의 국내·외 동향을 살펴본다. Ⅲ장에서는 인공지능 기반의 사이버 훈련장 적용 사례 및 요소기술들을 설명하고, 마지막으로 Ⅳ장에서 본고의 결론을 제시한다.

Ⅱ. 사이버 훈련장 국내·외 기술 동향

가까운 미래에 4차 산업혁명 시대 진입으로 일상생활을 비롯한 사회 및 경제 전반에서 빠르게 변화하는 융합의 시대가 도래할 것이다. 무엇보다 사이버 환경에서 생활하는 패러다임으로 전환되고 있어, 불법적인 정보유출과 위협으로부터의 대응 및 예방은 필수적인 기술로 큰 관심을 받고 있다. 따라서, 사이버 환경에서의 위협으로부터 안전을 보장할 수 있는 보안 역량 강화와 전문인력 양성을 위한 사이버 훈련장 및 교육 프로그램 개발이 절실히 요구되고 있다. 이 장에서는 국내·외 사이버 훈련장에 대한 동향을 살펴보고자 한다.

1. 국내 사이버 훈련장 기술 동향

가. 한국인터넷진흥원(KISA)의 시큐리티짐

한국인터넷진흥원(KISA)은 'K-사이버 방역' 추진 전략을 통해 정보보호 산업 육성과 인력을 양성해 오고 있다[8-10]. 경기도 성남시 판교에 위치한 사이버 보안 인재 센터에서는 정보보호 산업현장 및 서비스에 즉시 투입 가능한 인력양성을 목표로 다양한 사이버 침해사고 및 위협사례를 활용한 시큐리티짐(Security-Gym) 사이버 훈련장을 운영 중이다. 이러한 시큐리티짐은 미국의 NCR(National Cyber Range)과 이스라엘의 사이버짐(CyberGym) 등을 벤치마킹하여 구축한 것으로, 실제와 유사한 가상 사이버 환경을 만들어 실 환경에 버금가는 사이버 대응 훈련을 실시하고 있다. 실전형 사이버 훈련장인 시큐리티짐은 공공 및 민간, 군인, 학생 등 다양한 인력을 대상으로 보안기술 훈련 프로그램, 초급부터 고급 역량을 키울 수 있는 양방향의 실전 공격과 방어 훈련, 단방향의 훈련 등 다양한 수준에 맞춰 프로그램을 운영 중이다. 그림 1은 KSIA 관계자가 사이버 공격 및 방어 훈련이 가능한 실전형 사이버 훈련장인 시큐리티짐 보안 교육을 실시하는 모습이다[9].

출처 Reprinted with permission from [9], 공공누리 1유형.

그림 1 KISA의 시큐리티짐에서 오프라인 보안 교육을 실시하는 모습

출처 Reprinted with permission from KISA [10].

그림 2 KISA에서 스타트업을 선발하고 트레이닝을 진행하는 모습

시큐리티짐의 훈련 프로그램은 해킹공격 발생 즉시 탐지 및 대응이 가능한 시나리오 기반의 단방향 침해사고 대응, 양방향 실전 공방훈련이 가능하다. 최근 'K-사이버 방역' 추진 전략에 의하면, 2023년까지 현장 실무형 디지털 보안 전문인력을 3,000명 이상 양성하는 것을 목표로 하고 있다. 또한, 정보보호특성화대학 및 융합보안대학원 등의 과정을 통해 전문인력을 양성 중이며, KISA의 케이실드(K-Shield)와 가명처리 전문인력 양성 과정도 추진하고 있다. 마지막으로, COVID-19로 인하여 비대면 교육을 위한 온라인 교육 플랫폼을 구축했으며, 365일 24시간 가상 및 실습 위주의 교육 콘텐츠도 제공 중이다. 그림 2는 KSIA에서 정보보호 기업 육성 사업을 통해 스타트업을 선발한 뒤 트레이닝하고 비대면 설명회를 진행하는 모습이다[10].

나. 사이버작전사령부의 사이버 훈련장

국방부에서는 미래의 사이버 전쟁을 대비 및 시행하기 위한 최일선 부대로 사이버작전사령부를 운용해오고 있다[11]. 사이버작전사령부는 현재와 미

래의 사이버 전쟁 대비를 위한 실전 교육과 훈련을 실시하고 있다. 이러한 사이버 훈련은 2019년 '사이버 공방 훈련장 구축 사업'을 통해 군에서의 사이버전 대응능력 향상과 전문인력을 육성할 수 있도록 시작되었다. 본 훈련장에서는 사이버 방어 훈련(Cyber Defense Exercise)을 실시간으로 수행함으로써 보안 역량을 향상시키고자 노력하고 있다. 훈련 참가자는 역할에 따라 그린팀(Green Team)에서 사이버 훈련장 환경을 구축하고, 방어를 수행하는 블루팀(Blue Team)을 대상으로 레드팀(Red Team)이 사이버 공격을 실행하는 과정으로 구성된다. 사이버 공방전의 방어에는 탐지·대응·분석·예방 등이 순환적으로 수행하는 일련의 과정으로 사이버 훈련장은 이들 과정을 종합적으로 포함하고 있다. 국방 분야의 사이버 훈련장은 보안상 대외비 내용으로 현황을 알기가 어려운 측면이 있으나, 군의 네트워크와 장비 등 특수환경을 반영한 실전 대응훈련을 겸하고 있는 것으로 파악된다.

다. 사이버안전훈련센터의 사이버 훈련장

2012년 7월에 개원한 국가정보보안교육원의 사이버안전훈련센터는 사이버 훈련장의 보안 훈련 프로그램을 통해 매년 1,000~2,000명이 넘는 정보보안 핵심인력을 배출하고 있다[12]. 주로 정부부처 및 공공기관의 보안교육을 담당하고 있으며, 웹서버에서의 침해사고 분석, 기반시설의 제어시스템 보안, 업무 PC 침해사고, 보안관제 및 사고대응, 국가중요시설의 사이버 공격 대응 프로그램 등을 운영하고 있다. 사이버안전훈련센터의 방어 훈련에서는 최신의 사이버 공격기법 및 위협사례를 고려하고 있으며, 실제 환경을 모사하여 대응 방법 등을 훈련하고 있어 그 효과가 크게 반영된다고 한다. 본 사이버 훈련장에서는 기존 침해사고 등의 위협사례를 시나리오로 정의하고 학습하는 방식으로 운영되고 있다. 또한, 사이버 위기 경보 단계를 기준으로 순차적인 경보 단계별 정의와 예방, 실시간 대응, 사후대응을 통해 사이버 회복력의 요소를 훈련하고 있다. 최근에는 기존의 훈련뿐만 아니라 빅데이터·클라우드·IoT 기술을 활용한 로봇 및 스마트카 등의 미래 첨단기술 대상의 사이버 공격에 대응하기 위한 새로운 훈련 콘텐츠 개발에 심혈을 기울이고 있다.

2. 국외 사이버 훈련장 기술 동향

미국과 이스라엘을 중심으로 2000년대부터 사이버 보안 훈련장을 구축하였으며, 정부 및 산업체 교육 등에 적극적으로 활용하고 있다. 이 절에서는 미국을 비롯한 주요 선진국에서의 사이버 훈련장 기술 동향을 살펴보고자 한다.

가. 사이버짐(이스라엘)

2013년 설립된 이스라엘의 사이버 시큐리티 기업인 사이버짐(CyberGym)은 유럽과 호주를 비롯한 전 세계에 지사를 두고 있으며, 맞춤형 사이버 교육 솔루션을 제공하고 있다[13]. 사이버짐은 입소한 고객이 실제 기업 환경처럼 꾸며진 환경에서 사이버 공격을 방어하는 블루팀, 공격 담당은 이스라엘 방위군(IDF) 조직인 '유닛8200'이나 정보기관에서 훈련받은 해커로 구성된 레드팀, 사이버 훈련을 감독하고 공격과 방어를 모니터링하는 화이트팀으로 구성된다. 레드팀은 제로데이(Zero-Day) 취약점, 산업제어시스템(ICS) 가동 중지, 데이터 유출, 랜섬웨어 유포 등 최신 기법으로 블루팀을 공격한다. 사이버짐을 통한 공격과 방어 테스트가 끝나면, 화이트팀은 전 과정에서 수집한 데이터를 검토 및 분석하여 그동안 발견되지 않았던 취약점 등을 보완하는 과정을 거친다. 예를 들어 훈련이 끝난 후 어떤 공격을 통해 데이터가 유출되었는지 설명하고, 블루팀에서

는 어떻게 대응했는지 분석하고 개선점 등을 교육한다. 현재 글로벌 사이버 훈련장 시장에서 가장 선두인 사이버짐은 정부, 산업, 금융, 교통, 에너지 분야 등에 특화된 훈련 시나리오를 400여 개 이상 보유하고 있으며, 매년 8만 명 이상의 훈련자를 배출하고 있다.

사이버짐은 가상 클라우드 아레나(Virtual Cloud Arena)를 통해 전 세계 기업들과 기관에서 전문 교육을 받을 수 있도록 원격 학습 환경에 맞춰 프로그램을 운영하고 있다. 최근 가상 클라우드 아레나에서의 훈련생은 마이크로소프트 애저(Microsoft Azure)를 사용해 보안 연결을 생성하고 사무실, 집, 전 세계 어디서나 교육에 참여할 수 있도록 서비스를 시작하였다. 훈련생은 레드팀의 실제 시나리오 기반 작업 환경, 인프라 및 기술 맞춤형으로 다양한 사이버 공격으로부터 시스템을 방어하는 실습 및 피드백을 지원받을 수 있다.

나. Raytheon Technologies(미국)

레이시온(Raytheon) Technologies는 소프트웨어, 하드웨어, 네트워크 등에 대한 공격·방어 임무에 맞춰 사이버 훈련을 수행할 수 있는 기술을 제공하고 있다[14]. 레이시온의 사이버 훈련장은 사이버 공격·방어에 대한 유연성(Flexibility)과 확장성(Scalability) 등의 핵심기술 회복력(Resilience)을 테스트할 수 있도록 지원하고 있다. 특히, 레이시온 코드 센터(Raytheon Code Center)에서는 훈련 참가자의 기관 및 시설의 네트워크와 유사한 환경을 고려하고, 최신의 사이버 공격·방어에 대한 도구를 사용하여 기술 테스트와 훈련을 실행할 수 있다. 또한, 코드 센터에서는 사이버 방어 기술향상과 전문가의 노하우 습득을 위한 테스트 및 반복적인 훈련 수행, CODE(Raytheon Cyber Operations, Development and Evaluation)와 연계하고 참가자의 소속 기관 환경을 복제하여 사이버 훈련을 실시하고 있다. 최근에 공개한 코드 센터 자료에 의하면, 며칠 또는 수 시간 안에 항공 및 교통관제, 급수시설, 전력망 등의 다양한 네트워크 에뮬레이션과 대규모 사이버 공격에 대한 영향 평가를 위한 환경까지 생성하고 제공할 수 있다고 설명하였다.

다. NCR(미국 국방부)

미국 국방부(DoD: Department of Defense) 산하의 NCR(National Cyber Range)은 방위고등연구계획국(DARPA: Defense Advanced Research Project Agency)에서 인터넷과 동일한 가상의 사이버 환경을 구축하고 CMF(Cyber Mission Force) 지원, 다양한 공격의 대응 방법 실험을 위해 개발된 폐쇄 루프 시스템(Closed-Loop System) 구조의 사이버 훈련장을 개발하였다[15]. 국방훈련뿐만 아니라 민간과 관공서 등의 사이버 훈련장을 통합한 광대한 개념으로 대학 및 연구소에서 개발한 보안기술 실험, 상용제품 시험 등에도 활용되고 있다. 이러한 NCR은 안전한 보안 시설 안에서 최신의 취약점, 다양한 공격기법, 대응방안 등을 수용함과 동시에 재현 가능한 프로세스를 제공하고 있다. 활용사례를 살펴보면, 미국 국방부는 사이버 작전 테스트, 훈련 및 임무 리허설 등을 위한 사이버 공간 및 환경정보를 반영한 훈련장으로 활용 중이다. 또한, 미군의 요구사항을 고려한 맞춤형 시나리오와 군의 현실적 상황을 반영한 사이버 공간, 데이터 설계와 구현 및 분석까지 전 주기적인 사이버 훈련장 제공을 목표로 하고 있다.

라. Airbus(EU)

EU에서의 Airbus 사이버 훈련장에서는 수백 대 이상으로 구성된 IT/OT(Operational Technology) 시스템을 쉽게 모델링하고, 실제 사이버 공격을 포함한 다양한 시나리오를 시뮬레이션할 수 있는 솔루션이

다[16]. Airbus 사이버 훈련장에서는 관리자, 통합자, 테스터, 트레이너 등이 가상화 또는 하이브리드 네트워크 환경을 설계하고, 단말 간의 통신과 같은 단위 활동을 에뮬레이션하거나 실제로 이루어지는 사이버 공격에 대한 실행 및 분석정보 등을 제공한다. 모바일 박스(Mobile Box)로 명명된 사이버 레인지 플랫폼은 베이(Bay) 또는 클라우드(Cloud)에서 접근하여 시뮬레이션할 수 있는 추가적인 장점을 가지고 있다. 이러한 Airbus 사이버 레인지는 1,200여 개의 VM과 40,000여 개의 도커(Docker)를 지원하는 대규모 시스템이다. 또한, 복잡한 실제 환경의 제약을 충족하기 위해 산업 제어시스템, 하드웨어 트래픽 생성기, 물리/가상 시스템과 같은 외부 장비와 인터페이스가 가능하도록 지원하고 있다.

Ⅲ. 인공지능 기반의 사이버 훈련장 동향

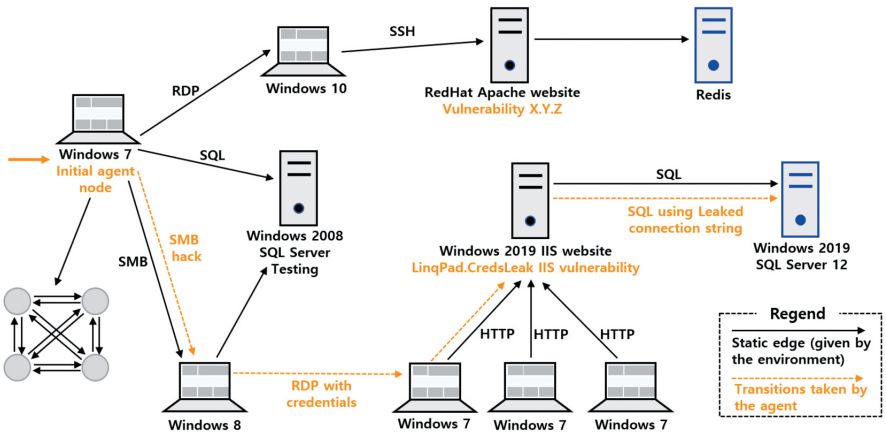
최근 ICT 기술을 활용한 사이버 보안 분야의 공격기술은 더욱 정교하고 다양해지고 있으며, 이전에 관측되지 않았던 새로운 공격의 출현 빈도가 짧아지고 있다. 따라서, 이를 대비하기 위한 대응기술 습득 및 인력양성을 위한 테스트베드로써의 사이버 훈련장은 날로 중요해지고 있다. 이 장에서는 새로운 패턴의 사이버 공격에 대한 탐지, 방어, 예방 등을 위한 인공지능(AI) 및 기계학습(Machine Learning) 기반 사이버 훈련장의 연구사례들을 살펴보고자 한다.

1. CyberBattleSim(마이크로소프트)

마이크로소프트(Microsoft)의 365 Defender Research 연구팀에서 개발한 CyberBattleSim은 사이버 공격에 대비할 수 있는 교육 시뮬레이션 모델로, AI와 기계학습을 활용해 보안 문제를 해결하고자 연구 및 개발된 시스템이다[17,18]. CyberBattleSim은 시뮬레이션된 엔터프라이즈 네트워크에서 특정한 지식이나 매개변수를 사용하여 자율 에이전트가 환경 내부에서 상호작용하는 방식으로 보안기술의 교육 및 개선을 목적으로 하고 있다. 이러한 CyberBattleSim 시뮬레이션은 추상화된 네트워크 환경과 사이버보안 개념을 제공하며, 파이썬 기반의 OpenAI Sim 인터페이스를 사용하여 강화학습 알고리즘으로 자동화된 에이전트 학습을 실행한다. 또한, 강화학습 알고리즘으로 보안을 개선하고, 방어자를 위한 자동화 및 플레이어 에이전트의 승리를 보상으로 전략을 학습한다. 이러한 과정을 거쳐 공격자가 네트워크를 통해 확산을 시도할 때, 강화학습의 방어 에이전트는 네트워크 상태를 감지하거나 공격을 자동으로 차단 또는 완화할 수 있는 기능을 포함하고 있다. 최근에는 허니팟(Honeypot) 등을 시스템에 통합하여 기만적인 방어 요소를 시뮬레이션된 엔터프라이즈 환경에서 공격과 방어 알고리즘 학습 및 재현이 가능한 수준으로 발전시켰다. 그림 3은 CyberBattleSim에서 다양한 운영체제 및 소프트웨어를 포함한 네트워크에서 각 시스템이 갖는 속성, 사전 할당된 취약점 집합이 있음을 나타내고 있다. 여기에서 시뮬레이션은 측면(Lateral) 이동의 시각적 표현 예제이고, 검은색 선은 노트 간에 실행되는 트래픽으로 통신 프로토콜에 의해 레이블이 지정됨을 의미한다.

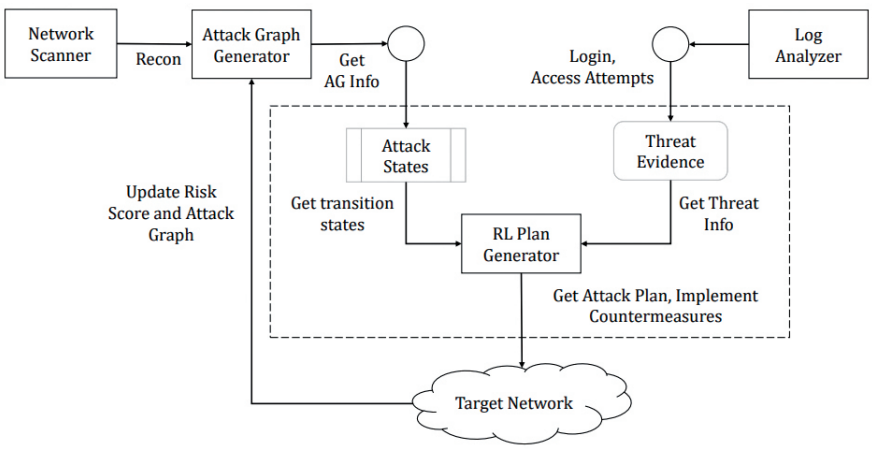
2. 애리조나 대학(ASAP)

미국 애리조나 주립대에서는 인공지능 기반 보안분석 및 침투 테스팅 프레임워크(ASAP: Autonomous Security Analysis and Penetration Testing Framework) 연구결과를 제안했다[16]. ASAP는 취약점 스캐닝 도구(Nessus, OpenVAS)를 이용하여 타겟 시스템의 취약점을 찾고, 스캔 결과를 바탕으로 취약점 분석 도구



출처 Reproduced with permission from [18].

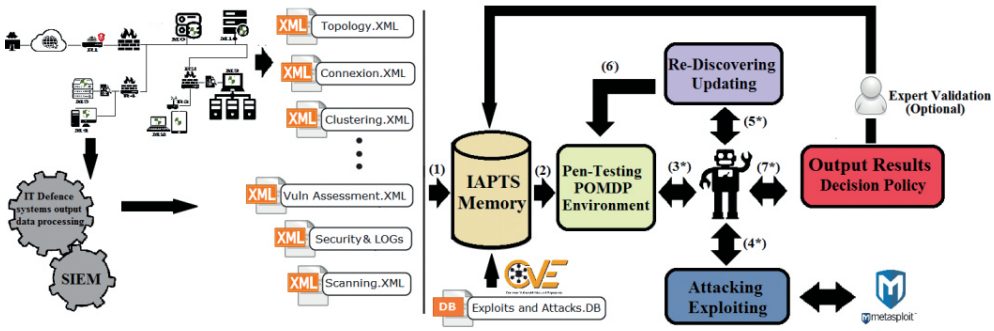
그림 3 CyberBattleSim에서 공격 후의 네트워크 측면 이동에 대한 시각적 표현 예제



출처 Reprinted with permission from [19].

그림 4 ASAP 아키텍처와 모듈 간의 데이터 흐름도

인 MulVAL을 이용하여 공격 그래프(Attack Graph)를 생성한다. ASAP는 보안 취약점의 중요성과 취약점 익스플로잇의 난이도를 반영하기 위해 도메인별 전이 매트릭스(Transition Matrix)와 보상(Reward)을 모델링한 DQN(Deep Q-Network) 기반의 강화학습 알고리즘을 사용하여 최적의 공격 경로를 찾는다. ASAP는 AI 기반의 공격 계획을 생성하고 실제 네트워크에 기능 검증을 수행하여 AI 기반 침투 테스팅 기술의 실현 가능성을 보여준다. 하지만, APT(Advanced Persistent Threat) 공격 및 제로데이 취약점 공격을 포함한 다양한 공격 시나리오에 대한 ASAP의 기능 검증이 필요하다. 또한, AI 기반의 레드팀과 블루팀을 포함하는 사이버 공방 훈련에 대한 추가 연구가 요구된다. 그림 4[19]에서는 취약점 스캐닝을 통해 취



출처 Reprinted from [20], CC BY 4.0.

그림 5 IAPTS의 기능 다이어그램

약점을 찾고 분석한 후, 공격 그래프를 생성하고, 강화학습 알고리즘을 통해 최적의 공격 경로를 추정하는 ASAP의 기능 구성과 처리 과정을 보여주고 있다.

3. 런던 대학(IAPTS)

영국의 런던 대학에서는 복잡한 네트워크 환경에서 효율적인 침투 시나리오를 생성하고 재현할 수 있는 인공지능 기반의 시스템인 IAPTS(Intelligent Automated Penetration Testing System)를 제안하였다[20]. IAPTS는 산업용 침투 테스트(PT: Penetration Test) 프레임워크와 통합되어 정보를 수집하고 경험을 통해 학습한 후 유사한 테스트 사례에서 테스트를 재현할 수 있는 기능으로 구성되어 있다. IAPTS는 시간 소모, 신뢰성 및 테스트 빈도 측면에서 향상된 결과 생성과 인적 자원 절약을 목표로 하며, 부분적으로 관찰된 마르코프 의사 결정 프로세스(POMDP: Partially Observed Markov Decision Process) 문제로 침투 테스트 환경 및 작업을 모델링한다. 실험 결과는 소비된 시간, 포함된 공격 벡터, 공격 결과의 정확도 및 신뢰성 측면에서 강화학습 모델이 인간 침투 테스트 전문가의 능력을 뛰어넘어 침투 테스트 시스템의 성능을 향상시킬 수 있음을 보여준다. 또한, 본 연구는 IAPTS의 학습 모듈이 인간 침투 테스트 전문가가 배우는 것과 유사한 방식으로 침투 테스트 정책을 저장하고 재사용할 수 있도록 함으로써 전문 지식 획득 및 재사용의 복잡한 문제를 해결하면서도 효율적인 방법을 제안한다. 하지만, IAPTS는 초기 학습 단계에서 강화학습 에이전트 행동에 대한 보상 제공자 역할이 필요하며 양질의 교육을 보장하기 위해 IAPTS와 함께 침투 테스트를 수행하고 학습 및 시스템 출력을 조정할 수 있는 높은 수준의 인간 전문가 감독을 필요로 하는 제약이 있다. 그림 5에서는 IAPTS의 기능 다이어그램을 상세히 설명하고 있다.

Ⅳ. 결론 및 시사점

본고에서는 ICT 기술과 4차 산업혁명 발전으로 디지털 사회로 전환하는 과정에서 정보보안 패러다임도 빠르게 변화하고 있음을 주목하였다. 이러한 디지털 사회에서는 이전보다 자동화되고 다양한 사이버 위협이 속속 등장하기 때문에, 이에 대한 빠른

탐지, 대응, 예방 등을 실행할 수 있는 기술이 크게 이슈화되고 있다. 특히, 사이버 공격은 인공지능 기술과 융합을 통해 더욱 지능화되고 있으며, 복잡한 실제 환경까지 고려하고 있어 그 피해는 더욱 커질 것으로 예상된다. 본고에서는 이러한 사이버 환경에서의 해킹 및 다양한 위협으로부터 안전을 보장할 수 있는 보안 역량 확보와 전문인력 양성을 위한 보안 교육 및 훈련장에 대한 국내·외 동향을 자세히 살펴보았다.

최근 인공지능 및 기계학습을 접목한 사이버 공격은 더욱 정교해진 공격기법과 자동화 도구 등에도 활용되고 있으며, 산업분야뿐만 아니라 국가안보 및 국민생명을 위협하는 수준까지 발전하고 있다. 하지만, 현재의 사이버 훈련장에서 공격과 방어 시나리오는 대부분 전문해커에 의해 수동으로 생성 및 활용되기 때문에 전문가의 기술 수준에 의존적이었다. 또한, 기존 사이버 훈련장은 훈련의 목적, 훈련을 받는 자의 수준, 적용 도메인에 따른 다양한 환경 가상화와 시나리오 생성에 한계가 있었다. 향후 사이버 훈련장은 다양한 환경 및 도메인 특성을 반영한 인공지능 기반의 공격 시나리오 생성, 최적의 방어전략 수립을 위한 멀티 에이전트 학습을 적용한 시스템으로 발전할 것으로 예상된다.

용어해설

제로데이(Zero-Day) 취약점 컴퓨터 SW의 취약점을 공격하는 기술적 위협으로, 취약점에 대한 패치가 나오지 않은 시점 및 그 문제가 알려지기 전에 이루어지는 보안 공격

허니팟(Honeypot) 비정상적 접근을 탐지 및 방어하기 위해 의도적으로 시스템에 중요한 정보가 있는 것처럼 꾸며 공격자의 해당 시스템 접근을 탐지

약어 정리

APT	Advanced Persistent Threat
ASAP	Autonomous Security Analysis and Penetration Testing Framework
CMF	Cyber Mission Force
CODE	Cyber Operations, Development and Evaluation
DoD	Department of Defense
DQN	Deep Q-Network
IAPTS	Intelligent Automated Penetration Testing System
ICS	Industrial Control System
NCR	National Cyber Range
OT	Operational Technology
PT	Penetration Testing

참고문헌

[1] 강용구 외, “공격 기법 모델링을 통한 사이버 공격 시뮬레이터 설계 및 구현,” 한국컴퓨터정보학회논문지, 제25권 제3호, 2020. 3, pp. 65-72.

[2] European Union Agency For Cybersecurity, “Cyber Europe 2022,” June 2022, https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme/cyber-europe-2022/

[3] 이주영, 문대성, 김익균, “사이버 공격 시뮬레이션 기술 동향,” 전자통신동향분석, 제35권 제1호, 2020. 2, pp. 34-48.

[4] Statista 2022, “Size of the cybersecurity market worldwide from 2021 to 2026,” June 2022, https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/

[5] H. Jiang, T. Choi, and R.K.L. Ko, “Pandora: A cyber range environment for the safe testing and deployment of autonomous cyber attack tools,” in Security in Computing and Communications, vol. 1364, 2020, pp. 1-20.

[6] 김대식, 김용현, “사이버 레인지 운용 방안 연구,” 인터넷정보학회논문지, 제18권 제5호, 2017. 10, pp. 9-15.

[7] 최영한 외, “사이버위기 경보 기반 사이버 방어 훈련장 설계 및 구축 연구,” 정보보호학회, 제30권 제5호, 2020. 10, pp. 805-821.

[8] 한국인터넷진흥원(KISA), Security-Gym, June 2022, https://www.kisa.or.kr/

[9] 과학기술정통부 보도자료, “사이버 침해대응 보안전문가 교육 수강생 모집,” 2022. 4. 13, https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=112&pageIndex=1&bbsSeqNo=94&nttSeqNo=3181618&searchOpt=ALL&searchTxt=%EA%B5%90%EC%9C%A1

[10] 전자신문, “[K-사이버방역 시대]〈하〉보안 기업 키우고 인력 늘리고…생태계 만든다,” 2021. 4. 19, https://m.etnews.com/20210419000178?obj=Tzo4OiJzdGRDbGFzcyI6Mjp7c

zo3OiJyZWZlcmVyIjtOO3M6NzoiZm9yd2FyZCI7czoxMzoid2ViIHRvIG1vYmlsZSI7fQ%3D%3D

[11] 사이버작전사령부, 사이버작전사령부령, 2022. 6, https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%82%AC%EC%9D%B4%EB%B2%84%EC%9E%91%EC%A0%84%EC%82%AC%EB%A0%B9%EB%B6%80%EB%A0%B9

[12] 사이버안전훈련센터, 2022. 6, https://www.cstec.kr/cstec/kor/html/sub01/sub0101.html

[13] CyberGym, Israel, June 2022, https://www.cybergym.com/#section_1

[14] Raytheon Code Center, Raytheon Technologies, USA, June 2022, https://www.raytheon.com/cyber/capabilities/range

[15] National Cyber Range(NCR), USA, June 2022, https://www.peostri.army.mil/national-cyber-range-ncr

[16] CyberRange-Airbus CyberSecurity, EU, June 2022, https://airbus-cyber-security.com/products-and-services/prevent/cyberrange/

[17] CyberBattleSim, Microsoft, USA, June 2022, https://www.microsoft.com/en-us/research/project/cyberbattlesim/

[18] CyberBattleSim, github, June 2022, https://github.com/microsoft/CyberBattleSim/blob/main/docs/quickintro.md

[19] A. Chowdhary et al., "Autonomous security analysis and penetration testing," in Proc. Int. Conf. Mobility, Sens. Netw. (MSN), (Tokyo, Japan), Dec. 2020, pp. 1-8.

[20] M.C. Ghanem and T.M. Chen, "Reinforcement learning for efficient network penetration testing," Information, vol. 11, no. 1, 2020, pp. 1-21.