사이버 공격 시뮬레이션 기술 동향

Technological Trends in Cyber Attack Simulations

이주영 (J.Y. Lee, joolee@etri.re.kr) 네트워크·시스템보안연구실 책임연구원
문대성 (D.S. Moon, daesung@etri.re.kr) 네트워크·시스템보안연구실 책임연구원/실장
김익균 (I.K. Kim, ikkim21@etri.re.kr) 정보보호연구본부 책임연구원/본부장

ABSTRACT

Currently, cybersecurity technologies are primarily focused on defenses that detect and prevent cyber-attacks. However, it is more important to regularly validate an organization's security posture in order to strengthen its cybersecurity defenses, as the IT environment becomes complex and dynamic. Cyber-attack simulation technologies not only enable the discovery of software vulnerabilities but also aid in conducting security assessments of the entire network. They can help defenders maintain a fundamental level of security assurance and gain control over their security posture. The technology is gradually shifting to intelligent and autonomous platforms. This paper examines the trends and prospects of cyberattack simulation technologies that are evolving according to these requirements.

KEYWORDS 사이버 공격, 시뮬레이션, 공격 그래프, Breach and Attack Simulation, 모의 해킹 기술

Ⅰ. 서론

세계 최초의 악성코드로 알려진 모리스 웜(Morris Worm, 1988년)이 인터넷에 연결된 6천여 대 이상의 컴퓨터 시스템들을 사용 불가 상태로 만든 사이버 보안사고 이후로 다양한 목적과 더욱 정교해진 방법을 통해 사이버 공격이 지속적으로 진행되고 있다. 이에 따라 사이버 공격에 대응하기 위한 방법도 발전해왔는데, 지금까지 주된 접근법은 공격이 진행되는 시점에 이를 탐지하고 차단하기 위한 방어 기술들을 개발하는 것이었다.

하지만 더욱 복잡해지고 동적으로 변화하는 IT 환경으로 인해 공격 노출면(Attack surface)이 확대되어 특정 지점에서 공격을 탐지하고 차단하는 방어 기술만으로는 정밀한 타겟 공격을 막기 어려워졌다. 또한 RSA 컨퍼런스에서 실시한 서베이[1]에 따르면 많은 보안 전문가가 보안 장비와 서비스를 현재 이용하고 있지만, 실제 이러한 장

* DOI: https://doi.org/10.22648/ETRI.2020.J.350104
* 이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임[No.2017-0-00213, 능동적 사전보안을 위한 사이버 자가변이 기술 개발].

비들이 의도대로 잘 작동하고 있는지, 구매한 보안 제품의 기능을 잘 활용하고 있는지에 대한 확신이 없다고 응답하였다. 더불어 보안 장비가 너무 복잡하고 설정하기 힘들며, 이를 잘 활용하고 판단할 전문가가 없어 보안 기능이 제대로 동작하고 있을 것으로 간주한다고 한다.

이러한 문제를 해결하기 위해서는 조직의 IT 환경에 어떤 보안 기능이 작동하고 있는지, 어느 부분을 보완해야 하는지, 네트워크와 장비 구성이 운영 시나리오에 맞게 적절하게 설정되어 있는지, 보안 기능들이 의도대로 작동하는지 등에 대한 정보가 필요하며, 이를 확인할 수 있도록 보안 상태에 대한 지속적이고 일관된 테스트가 요구된다.

그래서 최근에는 반복적인 보안성 평가를 통해 공격 노출면을 파악하고, 대응 전략을 수립해 전체적인 IT 환경의 보안을 강화하는 접근법에 대한 중요성이 강조되고 있다.

사이버 공격 시뮬레이션 기술은 조직에서 운용 중인 보안 정책 및 상태를 점검하기 위해 사용할 수 있는 기술로, 관리할 필요가 있는 공격 노출면을 미리 파악함으로써 보안 강화 전략을 수립할 수 있도록 한다. 사이버 공격 시뮬레이션 기술 분야는 침투 테스팅(Penetration testing) 기술, 공격 그래프 기술, BAS(Breach and Attack Simulation) 기술, 자율해킹기반 시뮬레이션 기술 등의 세부 기술들을 포함하며, 그림 1과 같이 자동화를 통해 조직에서 보안성 평가를 위해 반복적으로 사용할 수 있는 기술로 점차 발전하고 있다.

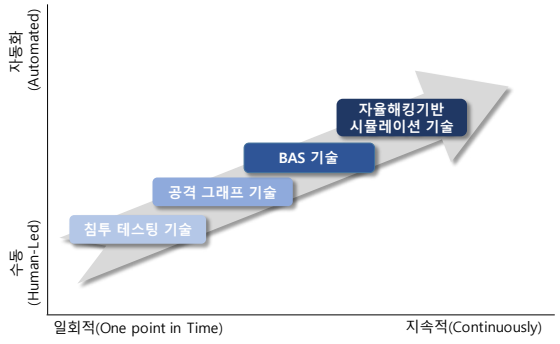


그림 1 사이버 공격 시뮬레이션 기술의 패러다임 변화

취약점 분석이나 모의 해킹을 위해 보편적으로 사용되고 있는 침투 테스팅 기술은 공격 단계에서 주로 수동으로 사용해야 하며 사용자의 전문성에 따라 활용 가치가 달라진다. 최근의 침투 테스팅 기술은 취약점을 찾아내기 위한 취약점 스캐닝 기능뿐만 아니라 실제 취약점에 대한 익스플로잇을 시도할 수 있는 기능을 함께 제공하는 추세이다.

공격 그래프 기술은 기존의 침투 테스팅 기술이 중점을 두었던 '포인트' 기반의 취약점 탐색 관점에서 한 걸음 더 나아가 포인트들 간의 연결성을 고려하여 공격에 이용 가능한 모든 경로를 식별하기 위한 기술이다. 이때 확률적으로 공격에 이용될 가능성이 높은 경로에 대한 우선순위를 결정하여 사용자에게 제시한다. 하지만 공격 그래프 기술을 이용해 찾아내는 모든 공격 경로들이 실제로 유효한지, 공격자가 해당 경로를 실제로 사용할지에 대해서는 보장하지 못한다.

그러한 측면에서 BAS 기술은 정적 분석에 의해 공격 경로를 식별하는 공격 그래프 기술과는 달리 공격 시나리오를 기반으로 모의 해킹을 시뮬레이션함으로써 유효한 공격에 의한 평가 결과를 얻을 수 있다. 대부분의 BAS 제품들이 기존 공격을 모델링한 시나리오를 제공할 뿐만 아니라 사용자가 직접 공격 시나리오를 정의할 수 있게 한다. 하지만 조직의 IT 인프라 환경을 잘 알고 있는 내부 인력이 정의하는 시나리오는 정형화될 수밖에 없고, 무엇보다 BAS 기술 또한 제로데이(Zero-day) 취약점을 이용한 공격에 대응하기 어렵다. 따라서 실제 해커의 창의성에 기반한 공격 전략을 모방할

수 있는 자율해킹기반 공격 시뮬레이션 기술이 필요하다.

본 고에서는 이러한 필요성 및 방향성에 따라 발전하고 있는 사이버 공격 시뮬레이션 기술의 동향과 전망을 살펴보고자 한다.

Ⅱ. 침투 테스팅 기술

1. 기술 개요

사이버 공격에 이용될 수 있는 약점과 보안상의 결함을 찾아내기 위한 방법을 제공하는 침투 테스팅 기술은 사이버 공격을 실행하는 공격자뿐만 아니라 조직의 보안 상태를 점검하기 위한 목적의 모의 해킹을 수행하는 인력에 의해서도 보편적으로 사용되어 왔다.

침투 테스팅 기술은 앞서 언급한 다른 사이버 공격 시뮬레이션 기술과 달리 주로 네트워크 스캐닝을 통해 네트워크 호스트의 열린 포트를 탐색하고, 이 포트에서 실행 중인 서비스를 식별하여 이러한 서비스와 관련된 이용 가능한 취약성을 찾아내는 취약점 분석 기능에 더 집중한다. 또한 잘못된 파일 권한, 레지스트리 사용 권한 등의 소프트웨어 구성 오류를 비롯한 시스템 레벨의 취약점을 인식하고 대상 시스템이 보안 정책을 준수하는지를 파악할 수 있는 호스트기반 취약점 분석 기술도 제공되고 있다.

최근의 침투 테스팅 기술은 취약점 분석을 위한 기능과 더불어 발견된 취약점에 대해 익스플로잇 시도를 할 수 있는 기능을 포함하여 자동화하는 추세이다. 대부분은 알려진 취약점에 대한 정보를 기반으로 실제 공격을 수행할 수 있도록 지원하며, 주로 웹 서버나 웹 응용 프로그램을 주요 타겟으로 한다.

2. 기술 개발 현황

현재 침투 테스트를 지원하는 오픈소스 및 상용 도구들이 많이 존재한다. 이러한 도구들이 침투 테스트를 위해 필요한 기능들을 패키지화해서 지원하지만 대부분의 전문가들은 세부적인 공격 전술에 따라 특화된 기능을 이용하기 위해 하나 이상의 도구를 사용하거나 더 전문적인 해커들의 경우 모의 해킹 테스트를 위해 편의에 따라 자체적으로 도구를 제작 및 개선하여 사용하는 경우가 많다. 앞서 언급했듯이 최근의 침투 테스팅 기술은 취약점 분석 및 익스플로잇 단계를 자동화하는 추세이고, 본 고에서는 자동화된 침투 테스팅 기능을 제공하는 대표적인 도구에 대해 기술한다.

가. Burp

Portswigger Web Security[2]에서 제공하는 Burp는 웹 응용프로그램에 대한 보안 테스팅 소프트웨어로 침투 기능보다 스캐닝 기능에 더 강점이 있어 웹 취약점 스캐너로 많은 조직에서 사용한다. 상용 버전으로는 단순 테스터를 위한 Professional 버전, 확장성 보장 및 자동화 기능을 제공하면서 CI (Continuous Integration) 통합을 지원하는 Enterprise 버전이 있다. 무료로 제공되는 Community 버전은 자동화와 같은 기능 없이 필수적인 매뉴얼 툴만을 제공한다.

Community 버전에서는 Burp Proxy를 이용해 웹 트래픽을 인터셉트하고 내용을 분석, 조작할 수 있다. 시퀀서 도구를 이용해 세션 토큰에 대한 통계 분석을 할 수 있으며, 세션 단위의 조작을 가능하게 한다. 또한 Clickbandit 도구를 이용하여 취약 서비스에 대해 클릭 재킹 공격을 수행할 수 있는 기능을 제공한다.

나. Metasploit

Rapid7의 Metasploit[3]은 오픈소스 커뮤니티의 지원을 받는 침투 테스팅 프레임워크로 취약점에 대한 스캐닝과 침투 테스팅 기능을 제공한다. 오픈소스 프로젝트로 운영되는 Metasploit Framework와 상용버전 침투 테스팅 솔루션인 Metasploit Pro[4]가 있으며, InsightVM을 이용하여 취약점 관리와 네트워크에 대한 가시화를 제공한다.

Metasploit은 침투 테스트와 그 결과에 대한 분석 및 대응 방법을 제시하기 위해 150,000개 이상의 취약점과 4,000개 이상의 익스플로잇 모듈을 이용하고 있으며, 이 데이터베이스는 오픈소스 커뮤니티의 지원을 받아 지속적으로 업데이트되고 있다. InsightVM의 취약점 관리 기능을 위해서 이 취약점 데이터를 이용하고 있으며, Metasploit Framework에는 모든 익스플로잇 모듈이 포함되어 제공된다. 또한 Metasploit Pro는 취약점 관리 모듈과 연동하여 자동적으로 취약점과 익스플로잇을 연관시켜 사용자가 침투 테스트를 수행할 수 있도록 지원한다.

하지만 Enterprise 레벨의 확장성을 지원하지 못하고 초보자가 사용하기에는 너무 어렵다는 단점이 있다. 또한 Metasploit Pro를 사용해서 피봇(Pivot)을 할 수 있지만 사용자가 구성해야 하는 프록시나 VPN을 통해 가능하여 이를 위해 추가적인 오버헤드와 비용이 필요하다.

다. Canvas

Immunity의 Canvas[5,6]는 현재 800여 개의 익스플로잇을 기반으로 자동화된 익스플로잇 시스템과 익스플로잇 개발 프레임워크를 제공한다. 상용 도구로서 공격 프레임워크와 침투 테스팅 Suite로 구성되어 있다.

한 시스템뿐만 아니라 네트워크 범위 설정을 통해서 웹 응용프로그램에 대한 모의 공격을 수행할 수 있으며 필요에 따라 Canvas 엔진을 수정해 사용할 수 있게 한다. Canvas는 콜백(Callback) 호스트와 공격 타겟 호스트를 사용자가 정의하도록 하고 있으며, 콜백 기능은 공격 성공 후 타겟 호스트를 콜백 호스트로 연결한다. 호스트를 대상으로 실행할 수 있는 모듈들의 리스트를 제공하며, 이 모듈 중에서 선택한 익스플로잇을 타겟 호스트를 대상으로 수행하는데, 이때 Canvas가 자동으로 쉘코드를 작성한다. 이러한 일련의 절차를 사용자가 메뉴에 따라 선택함으로써 침투 테스트를 수행할 수 있도록 한다.

하지만 Canvas가 호스트를 대상으로 실행할 수 있는 모듈과 정보를 제공한다 할지라도 타겟 호스트에 대해 무엇을 해야 할지, 결과를 어떻게 분석하고 이용해야 할지 등에 대해 판단하기 위해서는 사용자가 해킹과 관련된 전문적인 지식을 갖추어야 하며, 이에 따라 모의 해킹 결과는 사용자의 전문성에 의존적일 수 있다.

라. Core Impact Pro

Core Impact Pro[7]는 Core Security에서 제공하는 침투 테스팅 솔루션으로 가장 많은 상용 등급의 익스플로잇을 제공한다. 매달 자체적으로 제작하는 40여 개의 익스플로잇 코드들과 함께 Metasploit에서 제공하는 익스플로잇 및 SCADA 익스플로잇 패키지를 통합해서 사용할 수 있게 한다. 특히 SCADA 익스플로잇 패키지는 SCADA와 ICS를 대상으로 하는 140개 이상의 익스플로잇을 제공한다. 또한 Metasploit이나 PowerShell Empire와 같은 다른 침투테스트 도구들과도 통합이 가능하다.

Metasploit과 비교하여 Core Impact는 인접 장치에 자동으로 피봇팅하고 익스플로잇할 수 있도록 하며, 이러한 피봇팅 플로우를 직관적으로 제시한다는 점에서 장점을 갖는다[8]. 또한 스텔스 모드로

동작할 수 있도록 WMI를 통해 에이전트 없는 쉘과의 지속성을 지원한다. 또한 단계별 침투 테스트 방법을 제공할 뿐만 아니라 사용자 취약성과 공격자에 의해 획득될 수 있는 자격증명(Credential)을 식별하고 사회공학적 접근법에 의한 취약성을 테스트할 수 있도록 이메일이나 가짜 URL과 같은 공격벡터를 이용한 캠페인을 수행할 수 있게 한다.

3. 침투 테스팅 기술의 한계

앞서 기술한 것 이외에도 침투 테스트를 수행하기 위한 도구들이 지속적으로 개발되고 있다. 이러한 도구들이 사용자 편의를 위해 많은 부분을 자동화하고 있다고 할지라도 기본적으로는 취약점 분석을 수행하고, 모의 해킹을 수행하는 데 있어 전문 지식을 갖춘 사용자의 개입이 반드시 필요하다[9].

표 1 사이버 공격 방어 관점에서의 공격 포인트 분석과 공격 노출면 분석 비교

비고	공격 포인트 분석	공격 노출면 분석
관점	취약점 혹은 호스트 단위로 보안 점검	독립적 보안이벤트가 다단계 공격시나리오에 의한 공격경로 구성 과정일 수 있음
탐지	OS, Service, SW의 취약점 탐지	개별 취약점의 연결기반 공격경로 식별 보안정책 및 네트워크 설정 오류 검출
대응	SW 최신버전 업데이트 등을 통한 취약점 제거	취약점 제거, 보안정책 오류 점검, 네트워크 동적 변경 등을 통한 보안 강도 향상
효과	취약점 수 감소에 의한 보안성 증가	비용대비 효과적인 보안 강화 전략 수립 가능
한계	공격 체인, 요소 간 연관성 정보 획득 불가	계산 비용 및 연관 분석의 복잡성 증가
예시	Apache Struts2 Arbitrary Command Execution 취약점(CVE-2017-5638)을 통한 웹서버 공격에 대응	PMS 서버의 신뢰관계를 통해 PMS로부터 업데이트 데이터를 받는 모든 클라이언트 시스템을 공격에 대응

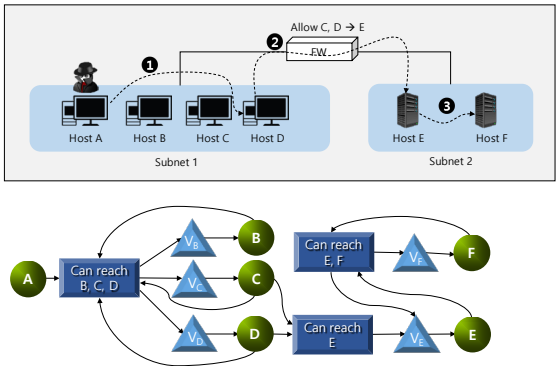
이는 근본적으로 기존의 침투 테스팅 기술이 하나의 공격 포인트인 취약점을 찾아내고 익스플로잇하는 것에 집중한다는 데 기인한다. 최근의 사이버 공격이 다단계의 공격 시나리오를 기반으로 진행된다는 것을 상기하면, 현재의 침투 테스팅 기술이 제공하지 못하는 각 포인트 간의 연결성 부분은 사용자의 전문성에 의한 판단으로 채워야 한다. 이러한 공격에 대한 방어 관점에서 공격 포인트 분석과 공격 노출면 분석에 따른 차이를 표 1에 비교 제시하였다.

또한 이렇게 인적 자원을 활용하는 방법은 많은 시간이 소요되고 고비용이기 때문에 일회성 평가에 그칠 뿐만 아니라 점검 및 평가 시점에 발견된 취약점만을 대상으로 얻은 단편적인 결과이기 때문에 새로운 장비나 소프트웨어가 도입되거나 설정이 변경되면 그 결과가 더 이상 유효하지 않다는 문제점이 있다.

III. 사이버 공격 그래프 기술

1. 공격 그래프 기술의 개요

공격 그래프는 공격자가 타겟 네트워크에 침입하는 데 사용할 수 있는 경로를 표현하기 위한 모델을 정의하고, 이 모델을 기반으로 공격자가 이용할 수 있는 모든 공격 경로를 찾아내기 위한 기술이다[10]. 생성된 공격 그래프는 보안 평가와 네트워크 보안 강화 전략 수립 등 많은 분야에서 활용될 수 있다. 예를 들면, PMS(Patch Management System) 시스템에 대한 공격에 성공함으로써 PMS과의 신뢰 관계에 있었던 조직 내의 모든 시스템들이 한 번에 공격을 당한 것과 같은 사례에 대해 공격 그래프 기술을 이용하면 취약점이 없어 보이는



출처 이주영, "공격 그래프에서의 위험도 결정과 시맨틱 검색 방법에 관한 연구," 忠南大學校 大學院 : 컴퓨터공학과 컴퓨터통신 및 보안 2019. 2.

그림 2 네트워크 환경과 공격 그래프 예시

시스템을 대상으로 하는 공격 경로를 찾아낼 수 있다. 이렇게 공격 그래프를 사용하면 네트워크 호스트에 한정된 로컬 취약점뿐만 아니라 호스트 간의 상호작용에 의해 발생할 수 있는 글로벌 취약점을 식별할 수 있다.

그림 2는 방화벽에 의해 접근제어가 이뤄지고 있는 두 개의 서브넷으로 구성된 네트워크 환경에서 생성될 수 있는 공격 그래프의 한 예시를 보여준다. 공격 그래프에서 Subnet1에 존재하는 호스트 A에 있는 공격자는 방화벽 규칙에 의해 Subnet2에 있는 호스트들로 접근이 불가능한 것처럼 보이지만 호스트 C와 D에 내재된 취약점 Vc와 Vd를 이용해 궁극적으로 호스트 F와 E를 공격할 수 있음을 확인할 수 있다.

공격 그래프는 그림 3에 도식화된 데이터 수집, 도달가능성 분석, 공격 그래프 모델링, 공격 그래프 생성 및 공격 그래프의 적용 단계에 따라 생성될 수 있다. 공격 그래프 생성에 대한 많은 연구에서 데이터 수집 단계는 Nessus 취약성 스캐너와 같은 오픈소스 도구를 사용하여 데이터를 수집하거나 사전 처리된 데이터를 사용하는 것을 가정하고 있다.

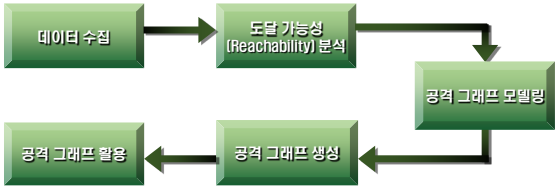


그림 3 공격 그래프 생성 절차

도달가능성(Reachability)에 대한 분석 단계에서는 주로 한 호스트에서 다른 호스트의 사용 권한을 획득해서 해당 호스트의 자원에 대한 접근이 가능한지에 대한 조건을 고려한다. 전체 네트워크의 도달가능성은 두 호스트 간의 도달가능성을 기반으로 확장해 판단할 수 있다. 도달가능성을 계산하기 위해 방화벽 같은 네트워크 보안 장비에서 정의한 접근제어 규칙은 물론 호스트 또는 서비스 간의 신뢰 관계를 모델링해 사용할 수 있다.

공격 그래프 모델링 단계는 개별적인 공격 템플릿과 공격 그래프에서 표현하고자 하는 구조를 모델링하는 과정이다. 공격 그래프 모델은 노드가 그래프에서 무엇을 나타내고자 하는지에 따라 다양하게 설계될 수 있다. 개념적으로 공격 그래프에서 노드는 관심 대상 개체(예를 들면, 호스트, 취약점, 소프트웨어 등)를 표현한다. 노드 사이의 연결선은 공격자가 다음 노드에 도달 가능하여 공격자가 해당 노드에 대한 권한을 획득할 수 있음을 내포한다.

2. 기술 개발 현황

공격 그래프 기술에 대한 연구는 2000년대 초에 시작하여 지금까지 지속적으로 진행되어 왔다. K. Kaynar는 공격 그래프에 대한 서베이 논문[11]에서 기존의 연구들을 분석해 공격 그래프 모델에 따른 분류 체계를 소개하였다. 하지만 기존의 연구들이

특정 공격 모델에 효과적인 새로운 공격 그래프 모델을 제안하고 공격 시나리오를 제시함으로써 검증 결과를 제시해왔기 때문에 수많은 공격 그래프 모델을 논문에서 제안한 것과 같은 체계로 명확하게 분류하는 것이 어렵고, 공격 그래프 모델 간의 장단점에 대한 비교가 어렵다.

가. Dependency 공격 그래프

공격 그래프 생성 분야에 있어서 대표적인 연구는 George Mason 대학의 S. Jajodia와 S. Noel에 의한 것이다. 그들은 연구 논문[12]에서 Dependency 공격 그래프를 제안하고, 공격 그래프를 생성하기 위해 TVA(Topological Vulnerability Analysis) 엔진과 Cauldron 시스템을 개발하였다.

Dependency 공격 그래프는 공격에 필요한 사전조건, 익스플로잇, 공격 성공에 따른 사후조건 간의 의존성을 모델링하여 생성되는 그래프이다. 취약성을 나타내는 시큐리티 조건들 간의 전이 규칙을 가장 작은 단위의 공격 익스플로잇으로 정의하는데, 즉 한 익스플로잇의 성공을 하나 이상의 시큐리티 조건을 만족시키는 것으로 모델링한다. 이 모델에 따라 공격 경로는 이러한 익스플로잇들의 시퀀스로 표현된다. 시큐리티 조건은 전문가가 수작업 분석을 통해 생성한다.

Dependency 공격 그래프는 다이렉트 그래프 형태로 그래프의 노드는 익스플로잇과 조건을 표현하고, 연결선은 익스플로잇, 사전조건 및 사후조건 간의 의존성을 나타내며, 연결선에 대한 레이블은 정의되지 않는다. Dependency 그래프의 생성은 초기 익스플로잇에서 시작해서 익스플로잇의 사후조건과 일치하는 사전조건을 갖는 익스플로잇을 검색하고, 검색된 익스플로잇에 대해 해당 과정을 반복한다. 그 결과 최소 크기의 공격 그래프를 획득할 수 있으며, 이는 공격 경로를 얻는 데 활용될 수 있다.

공격 경로의 생성은 Dependency 그래프에서 최종 타겟에 도달하도록 하는 단계별 타겟 목표, 즉 단계별 익스플로잇에 대한 사전조건의 집합으로 표현할 수 있고, 이를 통해 각 사전조건이 사후조건에 해당하는 익스플로잇들의 집합으로 대체될 수 있다. 전체 그래프에 대해 BFS 탐색으로 이 과정을 수행하면 최종적인 공격 경로를 결정할 수 있게 된다. 이때 대체 가능한 익스플로잇이 하나 이상이면 경로를 분리한다. 이러한 과정을 통해서 결과적으로 최종 타겟에 이르는 모든 가능한 경로를 획득할 수 있게 된다.

나. MP 공격 그래프

MIT 링컨 랩의 K. Ingols와 R. Lippman은 수 만 개의 호스트를 가진 대규모 네트워크를 대상으로 공격그래프를 생성할 때 확장성을 제공하기 위한 연구를 수행했다. 참고문헌 [13,14]에서는 전형적인 네트워크의 크기가 증가함에 따라 공격 그래프의 생성 시간이 거의 선형으로 증가하는 MP(Multiple Prerequisite) 공격 그래프 모델과 NetSPA 프로토타입 시스템을 제안하였다.

MP 공격 그래프에서 노드는 세 가지 타입으로 State 노드는 특정 호스트와 접근 레벨을, Prerequisite 노드는 도달가능성 그룹 혹은 자격증명을, Vulnerability 노드는 취약성을 표현한다. 이 모델을 기반으로 State 노드는 공격자에게 자격증명 등의 Prerequisite 노드를 제공할 수 있으며, 공격자는 획득된 자격증명을 통해 이용 가능한 Vulnerability 노드에 접근할 수 있게 되고, 취약점을 익스플로잇함으로써 새로운 State에 도달할 수 있게 된다. 따라서 MP 그래프의 연결선은 공격 시나리오를 표현하기 위한 이들 노드 간의 순서 관계를 표시하게 된다.

MP 공격 그래프를 이용해 공격 그래프를 생

성하는 NETSPA 시스템은 Nessus 취약점 스캐너, Sidewinder와 Checkpoint 방화벽, CVE 딕셔너리와 NVD 취약점 데이터베이스로부터 입력 데이터를 획득한다. 하지만 자격증명 데이터는 획득하는 방법이 응용프로그램이나 플랫폼에 의존적이어서 일반화해서 사용하는 것이 불가능할 수 있기 때문에 자격증명을 모델링하기 위한 데이터를 자동 수집하거나 임포트하는 모듈을 제공하지 않았다. 또한 그래프 생성의 확장성을 검증하기 위한 방법으로 필드 테스트와 시뮬레이션 테스트를 수행하여 네트워크의 호스트 수 증가에 대해 거의 선형적인 확장성을 제공함을 보였으며, 도달가능성에 대한 판단을 위해서 도달가능성 매트릭스를 생성하고 이를 기반으로 도달가능성 그룹을 판별하는 방법과 각 노드들을 조합해 그래프를 간단히 표현하는 방안을 제시하는 방식으로 대규모의 그래프의 처리 및 가시화에 대한 이슈를 고려하였다.

다. 시나리오 및 논리 기반 공격 그래프

SPIIRAS의 I. Kotenko 등이 제안한 시나리오 기반 그래프[15]는 공격을 위한 악의적인 행위들을 시뮬레이션하고 이를 이용해 공격 그래프를 생성하였다. 공격 행위를 모델링하기 위해 다단계 공격 모델을 반영하는 공격 시나리오를 채택했으며 공격자가 있을 수 있는 다양한 위치를 고려하여 공격 그래프에 적용하였다.

또한, X. Ou는 공격 그래프에 논리적 관계를 반영하기 위해서 자동 논리 추론을 통해 생성하는 공격 그래프[16]를 제안했으며, 제안된 논리 기반 공격 그래프 생성기는 대부분의 구성 정보를 데이터로그(Datalog) 튜플로 나타내며, 이를 위해 MALVAL[17] 추론 엔진을 개발하였다. 논리 기반 공격 그래프에서 그래프 연결선은 시스템 구성 정보와 공격자의 잠재적 권한 간의 인과 관계를 지정하기 때문에 이 공격 그래프는 공격이 진행되는 논리적 관계를 명확하게 보여줄 수 있다. 그들의 연구는 이전 연구와 비교하여 확장성이 향상되었으며 주기적 규칙에서 발생하는 공격 그래프 루프 문제에 대해서도 논의하였다. 그러나 쓸모없는 엣지 제거 및 그래프 루프 문제에 대한 개선 방법에 대해서는 향후 과제로 남겨두었다.

라. 시맨틱 공격 그래프

기존의 공격 그래프 기술은 그 결과로 사용자에게 그래프로 표현된 데이터만 제시하기 때문에 대규모의 그래프가 생성되면 이해가 어렵다는 문제점이 있다. 이러한 문제를 해결하기 위한 방법 중 하나로 ETRI에서는 시맨틱 공격 그래프 모델을 제안하였다[18]. 그림 4에는 시맨틱 공격 그래프 생성을 위한 접근 방법이 나타나 있다.

시맨틱 온톨로지는 특정 분야의 지식 표현을 위한 데이터 모델로 그 분야에 속한 개념과 개념 사이의 관계를 기술하는 정형 어휘의 집합이다. 컴퓨터는 온톨로지로 표현된 개념을 이해하고 지식처리를 할 수 있게 되는데, 온톨로지를 통해 구축된 지식 그래프를 이용하면 올바른 검색 결과를 찾거나 더 심층적이고 확장된 결과를 얻을 수 있다. ETRI에서 제안한 시맨틱 공격 그래프는 사이버 공격과 관련된 시맨틱 온톨로지를 구축하고 이를 기

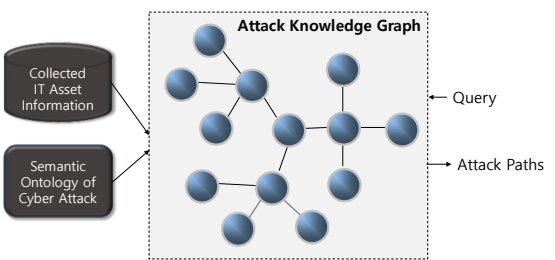


그림 4 시맨틱 온톨로지 구축을 통한 공격 그래프 생성 접근 방법

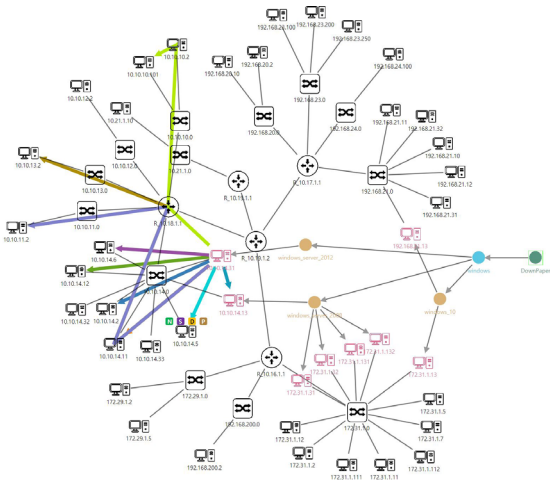


그림 5 시맨틱 공격 그래프에서 멀웨어 정보(DownPaper)를 이용한 공격 경로 검색

반으로 수집 자산 정보에 대한 지식 그래프를 생성하여 그래프 엔터티 간의 의미 관계를 추론함으로써 공격 경로를 제시한다.

이렇게 생성된 시맨틱 공격 그래프를 이용하면 다양한 공격 벡터 정보를 이용해 공격 경로를 검색할 수 있다. 그림 5는 시맨틱 공격 그래프에서 멀웨어 정보를 이용한 공격 경로를 검색한 결과의 예시를 보여준다. 공격자가 Windows 플랫폼을 대상으로 하는 멀웨어인 DownPaper를 이용하면 네트워크에서 운영체제로 Windows Server 2008, 2012와 Windows 10을 사용하는 호스트들을 공격할 수 있다. 또한 공격에 성공한 특정 호스트에서 다시 취약한 주변 호스트를 대상으로 내부전파가 이루지는 과정을 직관적으로 확인하는 것이 가능하다.

현재 사이버 공격과 관련해 산재한 정보들이 많이 존재한다. 이 정보들을 시맨틱 온톨로지로 확장함으로써 시맨틱 공격 그래프 모델은 더 의미 있고 유용한 결과를 제공할 수 있으며, 이를 기반으로 추론에 기반한 지능화된 사이버 공격 시뮬레이션 기술로 발전해 갈 수 있다.

3. 공격 그래프 기술의 한계

공격 그래프 기술이 취약성을 가진 독립적인 호스트 간의 연결성을 반영함으로써 다단계 공격 시나리오에 따른 공격 경로를 식별하는 데 도움을 줄 수 있을지라도 공격 그래프는 공격자가 개별 취약성을 실제 익스플로잇할 수 있는지, 익스플로잇을 통해 실제 호스트에 대해 어떤 권한을 획득할 수 있는지에 대한 판단은 고려하지 않는다. 다시 말하면 공격자의 능력을 배제한 채로 모든 공격 경로를 식별하고 방어적인 관점에서 이에 대한 보안 강화 정책을 취하도록 정보를 제공한다.

이러한 접근 방법은 실제 공격자가 사용할 경로를 예측하는 데 있어 재현율을 높일 수 있지만 정확도가 떨어질 수밖에 없다는 한계가 있다. 가장 이상적인 방법은 발견된 수많은 공격 가능 경로를 모두 제거하는 것이지만 현실적으로는 비용이 많이 소요될 뿐만 아니라 서비스 운용상의 문제로 불가능할 수도 있다. 이러한 문제에 대한 일반적인 해결방법 중 하나로 공격 경로의 우선순위를 제시하는데, 이 또한 제공하는 공격 경로의 우선순위가 실제 공격자가 사용할 가능성이 가장 높은 것이라는 것을 보장할 수 없다. 따라서 제시되는 우선순위를 방어 목적으로 활용하고, 효과적으로 보안성을 높일 수 있는 메트릭을 적용하여 우선순위를 산정할 필요가 있다. 또한, 사회공학적인 접근 방법에 의해 두 공격 경로가 연결되는 경우에 대해서도 솔루션을 제공하지는 못한다.

IV. BAS 기술

1. BAS 기술의 개요

BAS 기술은 다단계의 사이버 공격 시나리오를 자동화된 방법으로 시뮬레이션할 수 있게 한다. 이

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
11 items	34 items	62 items	32 items	69 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting
	Local Job Scheduling	Create Account		DCShadow	Keychain
				Deobfuscate/Decode Files or Information	

Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
23 items	18 items	13 items	22 items	9 items	16 items
Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
Security Software Discovery					System Shutdown/Reboot
Software Discovery					Transmitted Data Manipulation

출처 © 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation

그림 6 ATT&CK™의 Enterprise Matrix

를 위해서 실제 공격자들이 IT 환경을 공격하기 위해 사용할 것 같은 공격 체인을 모델링한다. BAS 기술이 이전 시뮬레이션 기술과 차이점을 갖는 주된 특징은 사용자가 선택한 공격 시나리오를 자동화해 수행할 수 있다는 점과 이를 위해 타겟 시스템에 설치된 에이전트를 기반으로 실제로 익스플로잇을 수행해 공격을 시도한다는 점이다.

BAS 기술은 기존 자산이나 서비스에 영향을 주지 않는지에 대한 안전성과 공격 시뮬레이션 결과에 대한 정확성 및 제품의 배치부터 공격 실행, 결과 보고까지 시뮬레이션 전 과정에 소요되는 시간과 성능 등이 주요 성능 지표로 검토될 수 있다. 이러한 접근법의 핵심은 얼마나 많은 공격 시나리오를 지속적으로 지원할 수 있는지 여부이고, 오픈 플랫폼으로서 해당 분야의 전문가들의 활발한 참여를 전제로 한다.

일반적으로 사이버 공격을 위해 해커들은 정찰, 무기화, 전달, 익스플로잇, 설치, C&C, 행동 개시 단계로 구성되는 사이버 킬체인을 동적으로 수행한다. 이를 위해 공격을 수행하기에 앞서 자신에 능력에 맞는 다양한 공격 전술과 기술을 이용한 공격 시나리오를 명시적 혹은 암묵적으로 계획하는

것처럼 BAS 기술도 사이버 공격을 시뮬레이션하기 위해서 공격 시나리오를 구성해야 하는데, 이때 활용하는 데이터 중 하나가 MITRE에서 제공하는 ATT&CK™[19] 프레임워크이다. ATT&CK™은 실제 발생한 사이버 공격 사례를 기반으로 공격자의 전술과 공격 기술에 관한 정보를 구축해 놓은 지식 베이스로 무료로 오픈되어 있다. 공격자가 목표하는 섹터별로 PRE-ATTACK, Enterprise, Mobile로 구분하고 있으며, 각 섹터에서 공격자가 주로 활용하는 공격 전술과 기술에 대한 정보를 제공한다. 그림 6은 ATT&CK™의 Enterprise Matrix의 일부를 보여준다.

이러한 데이터를 기반으로 BAS 기술은 각 단계별로 이용 가능한 TTP(Tactics, Techniques, Procedures)를 다양하게 조합하여 공격 시나리오를 구성할 수 있게 하며, 각 전술을 가능하게 하는 공격 기술 및 세부 공격 도구들을 선택하여 에이전트가 이를 실행하는 형태로 진행된다.

2. 기술 개발 현황

BAS 기술 카테고리는 2017년 처음으로 Gartner의 하이프 사이클(Hype cycle)에 등장하였다. Gartner는 Threat-Facing Technologies에 대한 하이프 사이클에서 BAS 기술을 혁신 촉발(Innovation Trigger) 단계에 배치하고 향후 5~10년 이내에 생산성 안정 단계(Plateau)에 도달할 것으로 예측하고 있다[20]. 이에 따라 현재는 해당 분야의 선도 기업들이 솔루션을 개발하여 시장을 구축하고 있는 상황이다.

가. AttackIQ

AttackIQ[21]의 FireDrill 플랫폼은 지속적으로 조직의 보안 프로그램의 효과를 검증하고 보안 제품 및 서비스가 시뮬레이션된 공격 시나리오에 잘 대응하는지를 평가하기 위한 플랫폼으로 1,500개 이상의 개별적인 공격에 대한 라이브러리를 구축하고 있다. 보안 담당자가 시나리오를 생성하거나 제공하는 공격 시나리오 라이브러리를 이용하여 자동으로 보안 평가를 수행할 수 있는 기능을 제공한다.

AttackIQ 제품은 클라우드, 가상 환경, 온프레미스에 설치 가능한 관리 콘솔과 에이전트로 구성되며 에이전트가 AttackIQ 플랫폼의 센서로서 선택된 시나리오를 받아서 익스플로잇을 실행하는 역할을 담당한다.

이러한 시나리오 기반의 공격 시뮬레이션 기능을 제공하기 위해서는 공격 시나리오를 구현 가능하게 하는 라이브러리를 지속적으로 제공할 수 있는 커뮤니티의 지원이 필요한데, 이러한 부분이 시나리오 기반 시뮬레이션 기술이 채택되는데 있어 어려운 점으로 꼽힌다.

나. SafeBreach

SafeBreach[22]는 인프라의 보안 상태를 테스트하기 위해서 시뮬레이션된 자산과 실제 공격 기술을 이용하는 시뮬레이션 플랫폼을 제공한다. 선택된 세그먼트들에 실제 자산들을 시뮬레이션하는 페이크 자산들을 배치하고 이 시뮬레이터들 간에 공격 시나리오를 실행하며, 클라우드, 네트워크 및 엔드포인트 시뮬레이터를 조합할 수 있도록 한다. 또한 신용 카드, 개인 식별 정보, 소스 코드 등 공격할 데이터 타입도 선택할 수 있게 한다.

SafeBreach 플랫폼은 시뮬레이션 된 환경을 대상으로 공격을 수행함으로써 실제 자산 및 서비스에 영향을 미치지 않고 안전하게 공격을 테스트해 볼 수 있도록 하고 있다. 공격 결과에 따라 어느 부분을 교정해야 할지를 쉽게 식별하기 위해 킬체인을

통해 결과를 가시화하여 제공한다.

SafeBreach와 같이 시뮬레이션 환경을 대상으로 공격을 수행하는 접근법에서는 시뮬레이션 된 자산과 실제 IT 환경이 동일한지에 대한 정확성을 확인할 수 있는 방법이 필요할 뿐만 아니라 지속적으로 동일한 환경을 유지 관리하는 방안을 제공하는 것이 운영의 효율성을 높이기 위한 핵심이 될 수 있다.

다. Cymulate

Cymulate[23]는 실제 보안 침해 위험 없이 실제 자산에 대한 실제 공격을 사용하여 기업의 보안 아키텍처 및 운영을 평가하는 자동화된 솔루션을 제공하는 것을 특징으로 한다.

Cymulate의 BAS 플랫폼은 실제 자산에 배포된 Cymulate의 Hopper 모듈이라 불리는 소프트웨어 에이전트 간 또는 소프트웨어 에이전트와 Cymulate의 클라우드 간에 실행된다. 타겟 시스템에 소프트웨어 에이전트를 설치하고 SaaS 솔루션으로부터 실제 멀웨어를 다운받아서 하나의 공격 벡터를 대상으로 시작하여 추가적으로 공격 벡터를 확장하면서 평가를 수행한다.

위협 벡터는 이메일이나 웹 브라우징, 기업의 웹 어플리케이션에 대한 공격, 측면 이동 등으로 모든 위협 벡터들은 타겟 시스템상에서 하나의 에이전트를 이용해 수행되거나 다른 설정의 자산에 새로운 소프트웨어 에이전트를 추가해서 수행될 수 있다.

Cymulate BAS 플랫폼처럼 실제 환경에 적용하는 접근법은 네트워크나 시스템의 성능을 저하시키거나 심지어 크래시를 발생시켜 중요 서비스를 제공하는 데 문제가 있을 수 있다. 따라서 이러한 접근법을 사용하기 위해서는 사전에 정의된 실행 및 조치 방법을 계획하는 것이 필요하다.

3. BAS 기술의 한계

BAS 기술이 해커들이 수행하던 것과 유사한 방법으로 다단계의 사이버 공격 시나리오를 자동화해 시뮬레이션할 수 있게 한다는 점에서 이전 시뮬레이션 기술들보다 장점을 가진다.

하지만 BAS 기술에서 제공하는 공격 시나리오는 정형적인 모델이기 때문에 조직의 보호 대상 자산들의 특성을 파악하고 이에 따라 구축한 보안 전략이 제대로 작동하는지에 대한 판단을 할 수 있는 전문가가 공격 시뮬레이션을 위한 공격 시나리오를 강화하거나 변경할 필요가 있다. 또한 이에 따라 수행된 시뮬레이션 결과를 정확히 해석하고 판단하는 것도 사용자의 역할로 남아 있다.

BAS 기술 등의 자동화된 시스템은 알려진 취약점, 위협, 공격 기법을 대상으로 시뮬레이션을 수행하기 때문에 제로데이 혹은 알려지지 않은 취약점을 이용한 공격을 시도해 보기 어렵고, 실제 공격자가 창의적으로 수행하는 새로운 공격 방식을 시도해 볼 수 없다는 단점이 있다. 추가적으로 사이버 공격 시뮬레이션 기술이 시스템이 갖는 취약점을 식별하는 것을 넘어서 시스템 운용 및 업무 프로세스상에서 발생하는 약점을 발견하기 위해서 다양한 사회공학적인 요소를 반영할 수 있도록 발전할 필요가 있다.

V. 자율해킹기반 시뮬레이션 기술

자율해킹을 기반으로 하는 사이버 공격 시뮬레이션 기술은 자동적인 취약점 발견, 해당 취약점에 대한 익스플로잇 코드 자동 생성, 취약점에 대한 자동 패치 등의 핵심 요소 기술들의 개발을 필요로 하며, 아직까지 이 기술 분야는 태동기에 있다. 이 중 제한된 환경을 타겟으로 취약점을 찾아내고 이

를 익스플로잇하는 자동화된 혹은 자율해킹 솔루션을 위한 연구가 부분적으로 진행되고 있다.

카네기멜론에서 개발한 Mayhem은 2015년도에는 취약점을 찾고 이에 대한 패치 성능에 따라 점수를 얻는 해킹대회인 DARPA의 CGC(Cyber Grand Challenge)에서 우승을, 2016년에 열린 Defcon CTF (Catch The Flag) 24에서 15개의 참가자 중 14위를 거둔 바 있다.

Mayhem은 실행코드 변환 도구, 공격 도구, 패치 도구, 코디네이션 도구 등으로 구성되어 있으며, 심볼릭 실행을 통한 소프트웨어 프로그램 분석과 퍼징(Fuzzing) 기법을 통해 취약점이나 결함을 찾아내는 방법을 사용하였다. Mayhem의 해킹은 사람이 할 수 있는 것보다 훨씬 더 빠른 연산력을 통해 성취된 것으로 핵심 기술과 더불어 자율적인 추론 시스템을 기반으로 사람의 개입 없이 해킹을 수행할 수 있었다[24].

Mayhem 개발연구팀이 설립한 ForAllSecure는 현재 미국 정부와 첨단 기술 및 항공 우주 산업 기업 등 얼리어답터를 대상으로 머신 스케일과 속도로 자동적으로 취약점을 찾아내는 퍼징 솔루션으로서 Mayhem의 초기 버전을 판매하고 있다[25].

자동화된 해킹을 위해 AI 기술을 이용한 접근법 중 하나로서 GAN(Generative Adversarial Network)을 이용한 멀웨어 생성 알고리즘인 MalGAN이 제안되었다[26].

MalGAN은 머신러닝 기반의 멀웨어 탐지 시스템에 블랙박스 공격을 수행하는 것을 목표로 하며, 이 논문에서 MalGAN은 블랙박스인 멀웨어 탐지 시스템을 대체하기 위한 탐지기를 사용하고 회귀 생성을 담당하는 Generator에 의해 생성된 샘플 멀웨어가 대체 탐지기에 의해 탐지(예측)되는 확률을 최소화할 수 있도록 학습된다. 이 연구 결과를 통해 MalGAN을 통해 생성된 샘플 멀웨어들이 블랙박스 멀웨어 탐지기를 효과적으로 우회할 수 있음을 보였다.

아직까지 이러한 연구들은 초창기에 있으며, 취약점에 대한 자동화된 공격 해킹 방법을 제안하는 데 초점이 맞춰져 있다. 기계 연산력의 강점이나 발전하고 있는 AI 기술에 기반하여 지능화된 해킹을 시도하고 있지만 아직까지 자율해킹에 의해 다단계 공격을 시뮬레이션하기 위한 솔루션으로는 부족하다. 또한 보안성을 강화하기 위한 목적을 갖는 자율해킹을 위해서는 취약점에 대한 자동 패치 기술에 대한 연구 개발이 진행될 필요가 있다.

VI. 결론

사이버 공격에 대한 선제적 대응 방법으로써 보안성 평가를 위한 사이버 공격 시뮬레이션 기술의 동향에 대해 기술하였다. 사이버 공격 시뮬레이션 기술은 실제 공격에 대비하기 위해 가상의 공격을 수행할 수 있는 기능을 지원하며, 현재 보편적으로 사용되는 침투 테스팅 기술로부터 공격 그래프 기술, BAS 기술 등이 많은 관심을 받고 있다.

사이버 공격 시뮬레이션 기술은 사용자의 능력에 의존적인 기존의 수동 분석 기술에서 점차 자동화된 분석 기술로 발전하는 단계에 있다. 이러한 변화의 이면에는 고비용의 수동 분석에 의한 일회성 평가가 빠르게 동적으로 변화하는 IT 환경에 존재할 수밖에 없는 버그와 보안 결함 등을 신속하게 파악하고 진단하는 데 한계가 있다는 점에 기인한다.

따라서 특정 시점만이 아닌 반복적이고 지속적인 수행을 통해 보안성 판단할 수 있으며, 전문가가 아닌 사용자가 보안 상태를 파악하는 데 도움을 줄 수 있는 기술이 필요하다. 이러한 요구사항에 따라 사이버 공격 시뮬레이션 기술은 더욱 자동화,

지능화, 자율화되는 방향으로 발전될 것으로 여겨진다. 하지만 여전히 사이버 공격 시뮬레이션에 의한 보안 평가의 가치와 정확성을 입증하는 것은 어려우며, 사회공학적인 기법과 직관적인 판단을 함께 사용하는 지능적인 휴먼 해커의 수준에 도달하는 것은 도전적인 과제이다.

용어해설

공격 노출면(Attack Surface) 공격 표면, 공격 접점이라고도 하며 하드웨어, 소프트웨어, 펌웨어 구성 요소, 네트워크 등의 IT 자산에서 사이버 공격에 취약하게 만드는 약점(weakness)이나 결함(deficiencies)들의 집합

제로데이(Zero-day) 공격 보안 취약점이 발견되었을 때 그 문제의 존재 자체가 널리 공표되기도 전에 해당 취약점을 악용하여 이루어지는 보안 공격

약어 정리

BAS	Breach and Attack Simulation
CI	Continuous Integration
CVE	Common Vulnerabilities and Exposures
GAN	Generative Adversarial Network
ICS	Industrial Control System
PMS	Patch Management System
SCADA	Supervisory Control And Data Acquisition
TTP	Tactics, Techniques, Procedures
WMI	Windows Management Instrumentation

참고문헌

[1] ISACA/RSA Conference survey, Survey: 82% of Boards Are Concerned about Cybersecurity, https://www.rsaconference.com/about/press-releases/survey-82-of-boards-are-concerned-about

[2] PortSwigger, Burp, https://portswigger.net/burp

[3] Rapid7, Metasploit, https://www.metasploit.com/

[4] Rapid7, "Put Your Defenses to the Test," https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-product-brief-metasploit.pdf

[5] Immunity, CANVAS, https://www.immunityinc.com/products/canvas/

[6] Immunity, Tutorial: CANVAS 101 Part 1, https://www.immunityinc.com/downloads/documentation/tutorials/canvas101-part1.pdf

[7] Core Security, Core impact, https://www.coresecurity.com/core-impact

[8] Core Impact 2017 versus Metasploit: the Shootout Comparison, https://www.programmableweb.com/news/core-impact-2017-versus-metasploit-shootout-comparison/sponsored-content/2017/11/02

[9] Paul Rubens, Penetration Testing: DIY or Hire a Pen Tester?, https://www.esecurityplanet.com/network-security/penetration-testing.html (April 2017)

[10] 이주영, "공격 그래프에서의 위험도 결정과 시맨틱 검색 방법에 관한 연구," 忠南大學校 大學院: 컴퓨터공학과 컴퓨터통신 및 보안 2019. 2.

[11] K. Kaynar, "A taxonomy for attack graph generation and usage in network security," *J. Inf. Security Applicat.*, vol. 29, 2016, pp. 27-56.

[12] S. Jajodia, S.Noel, and B. O'berry, "Topological analysis of network attack vulnerability," *Managing Cyber Threats,* Springer, Boston, MA, 2005. pp. 247-266.

[13] K. Ingols, R. Lippmann, and K. Piwowarski, "Practical attack graph generation for network defense," in *Proc. Annu. Comput. Security Applicat. Conf.,* Miami Beach, FL, USA, Dec. 2006, doi: 10.1109/ACSAC.2006.39

[14] R. Lippmann, "Validating and restoring defense in depth using attack graphs," in Proc. MILCOM 2006-2006 IEEE Military Commun. Conf., Washington, DC, USA, Oct. 2006, doi: 10.1109/MILCOM.2006.302434.

[15] Kotenko, Igor, and Mikhail Stepashkin, "Attack graph based evaluation of network security," in Proc. IFIP Int. Conf. Commun. Multimedia Security, Crete, Greece, Oct. 2006, pp. 216-227, doi: 10.1007/11909033_20

[16] X. Ou, W.F. Boyer, and M.A. McQueen, "A scalable approach to attack graph generation," in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 336-345, doi: 10.1145/1180405.1180446.

[17] X. Ou, S. Govindavajhala, and A.W. Appel, "MulVAL: A Logic-based Network Security Analyzer," USENIX Security Symposium. Vol. 8. 2005.

[18] J. Lee et al., "A semantic approach to improving machine readability of a large-scale attack graph," J. Supercomput., vol. 75, no. 6, 2019, pp. 3028-3045.

[19] MITRE, ATT&CK, https://attack.mitre.org/

[20] Gartner, Hype Cycle for Threat-Facing Technologies, 2019, July 2018.

[21] AttackIQ, https://attackiq.com/

[22] SafeBreach, https://safebreach.com/

[23] Cymulate, https://cymulate.com/

[24] D. Brumley, “Mayhem, the Machine That Finds Software Vulnerabilities, Then Patches Them,” (2019), https://spectrum.ieee.org/computing/software/mayhem-the-machine-that-finds-software-vulnerabilities-then-patches-them

[25] ForAllSecure, https://forallsecure.com/

[26] W. Hu and Y. Tan, “Generating adversarial malware examples for black-box attacks based on GAN,” arXiv preprint arXiv:1702.05983, 2017.