논문 19-44-09-16 The Journal of Korean Institute of Communications and Information Sciences '19-09 Vol.44 No.09
https://doi.org/10.7840/kics.2019.44.9.1723

사이버 공격예측 및 대응을 위한 유연적 시험환경 구축

류 한 얼•, 전 성 구*, 심 신 우*, 임 선 영*, 한 인 성**, 오 행 록**

Implementation of Flexible Test Bed for Cyber Attack Prediction and Countermeasure

Han-Eul Ryu•, Sung-Goo Jun*, Shin-Woo Shim*, Sun-Young Im*, In-Sung Han**, Haeng-Rok Oh**

요 약

최근 사이버 공격은 공격자 및 적용기술에 따라 다양한 전략·전술·절차적 특징을 갖고 있으며, 사이버 공격기술 또한 빠르게 변화하고 있다. 이와 같은 상황에서 사이버 공격 특징을 분석하고 공격을 예측하며, 각 공격 절차의 변화에 대응할 수 있는 시험환경 구축이 필요하다. 본 논문에서는 빠르게 변화하고 있는 사이버 공격을 분석·예측하고 검증할 수 있는 보다 유연한 시험환경을 제공하기 위해 테스트베드 상에서 모의공격자가 공격을 수행하는 방안, 테스트베드 상에서 모의공격자 대신 위협모의기를 통하여 공격을 수행하는 방안, 테스트베드 없이 수집된 정보와 에뮬레이션 SW를 활용하는 방안 등 세 가지 형태의 시험환경 구축 방안을 제시하였다. 시험 단계 및 환경에 따라 적합한 구성 방안을 선택하여 유연하게 시험에 적용할 수 있다.

Key Words : Cyber Attack, Test bed, Attack Reproduction, Attack Simulator, Emulation SW

ABSTRACT

Recently, cyber attacks have a variety of strategic, tactical and procedural features according to attacker or technology, and cyber attack techniques are changing rapidly. In this situation, it is necessary to construct a test bed that can analyze the features of cyber attacks, predict the attacks and respond to the changes in attacks. In this paper, we propose 3 types test bed configuration. Type 1 is method that configure test bed with an attacker, Type 2 is method that configure test bed with attack simulator instead of an attacker, Type 3 is method that configure collected files and emulation SW without test bed. Therefore it can be tested flexibly by choosing the configuration suitable for test phase and environment.

Ⅰ. 서 론

최근 발생하는 사이버 공격들은 공격자 및 적용기술에 따라 다양한 전략·전술·절차적 특징을 갖고 있으며, 공격에 사용되는 기술 또한 빠르게 변화하고 있다. 이와 같은 상황에서 사이버 공격 특징을 분석하고 공격을 예측하며, 각 공격 절차의 변화에 대응하여 보다 유연하게 시험할 수 있는 시험환경 구축이 필요하다.

미국 DARPA(Defense Advanced Research Projects Agency)에서 국가 사이버전 시험장(NCR, National Cyber Range)[1,2]을 개발하여 실제적인 네트워크 환경을 구성하고 사이버전 훈련 및 시험을 수행할 수 있도록 지원하고 있으며, 이스라엘에서도 이스라엘 전력(IEC)과 사이버보안 기업의 공동투자로 사

※ 본 연구는 국방과학연구소 연구 과제(시제 주관: LIG Nex1) "사이버 지휘통제 실시간 의사결정지원기술"의 일환으로 수행되었습니다.
• First and Corresponding Author : LIG nex1, haneul.ryu@lignex1.com, 정회원
* LIG nex1, {sunggoo.jun, shimshinwoo, sunyoung.im}@lignex1.com
** Agency for Defense Development, {insung.han, haengrok}@add.re.kr
논문번호 : 201903-484-B-RE, Received February 28, 2019; Revised July 2, 2019; Accepted July 9, 2019

이버짐(Cybergym)을 설립하여 주요 기반시설에 대한 침해사고와 대응 교육을 지원하고 있다.

국내의 경우 한국인터넷진흥원에서 사이버보안인재센터를 설립하여 K-Shield 과정 등 사이버 보안 인력의 훈련을 지원하고 있으며, 국방과학연구소 주관으로 사이버전 훈련, 기술검증, 전투실험 등에 필요한 테스트환경에 대한 연구개발[3-6]이 활발히 진행되고 있다.

사이버 공격 및 방어 훈련을 위한 시험·훈련 환경은 실 시스템 혹은 가상 시스템을 기반으로 모의공격자가 공격을 직접 수행하거나 공격 스크립트를 활용하는 방식이 활용되고 있지만 대부분 특정 환경에 고정된 방식만을 사용하고 있다.

한편, 모의공격 및 침투테스트는 사이버 공격의 기술적 난이도로 인해 전문지식을 보유한 인원을 필요로 한다. 이에 따라 시간적 제약사항과 많은 비용이 발생되므로, 전문가의 지속적인 투입 없이도 다양하고 반복적이고 자동화된 시험을 수행할 수 있는 방안이 요구된다.

Ⅱ. 본 론

본 논문에서는 빠르게 변화하고 있는 사이버 공격을 분석·예측하고 검증할 수 있는 보다 유연한 시험환경을 제공하기 위해, 테스트베드 상에서 모의공격자가 공격을 수행하는 방안, 테스트베드 상에서 모의공격자 대신 위협모의기를 통하여 공격을 수행하는 방안, 테스트베드 없이 수집된 정보와 에뮬레이션 SW를 활용하는 방안을 제시하였다.

2.1 공격자 기반의 테스트베드 구성 방안

본 연구에서 제안하는 공격자 기반의 테스트베드 환경은 그림 1과 같이 크게 테스트 대상 시스템(SUT, System Under Test) 영역과 가상환경, 실환경, 모의공격환경으로 구성된다.

SUT 영역은 구성형태에 따라 달라질 수 있으며, 본 연구에서는 수집/통합 서버, 위협분석 서버, 공격예측 및 방어방책 서버, 통합DB 서버, 가시화 서버로 구성하였다. 본 연구에 적용된 SUT는 사이버 공격예측 및 대응을 지원하는 시스템으로 실환경으로 구성하였으며, 시험환경 구성 형태에 따라 테스트 대상을 가상환경으로 구성할 수도 있다.

가상환경 영역은 가상화서버 3대, 스토리지 그리고 가상화서버와 스토리지를 연결하기 위한 10G 스위치로 구성된다. 가상화서버는 VMware사의 vCenter,

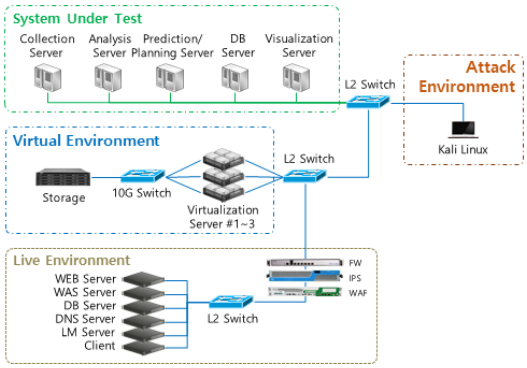


그림 1. 공격자 기반의 테스트베드 구성
Fig. 1. Test bed Configuration with an Attacker

vSphere, NSX를 활용하여 서버 3대를 통합한 하나의 가상환경을 제공하며, 가상환경 상에 생성되는 이미지들은 스토리지에 저장된다. 가상환경은 실환경 대비 저렴한 비용과 노력으로 시험환경을 구성하고 필요시 삭제 및 변경 등 유연한 환경구성이 가능하다는 장점이 있다.

실환경 영역은 WEB서버, WAS(Web Application Server)서버, DB(Data base)서버, DNS(Domain Name System)서버, LM(Log Management)서버, 운용단말 등의 실장비와 방화벽, IPS(Intrusion Prevention System), 웹방화벽 등의 보안장비로 구성된다. 실환경은 실제 운용되는 장비와 보안장비를 대상으로 직접 테스트할 수 있다는 장점이 있으며, 가상화를 지원하지 않는 시스템 및 보안장비는 실환경으로만 시험환경이 구성 가능하다.

모의공격환경은 Kali Linux 기반의 모의공격장비가 포함된다. 모의공격장비에는 공격자가 사용하는 공격도구 및 유틸리티가 설치되어 운용된다.

이러한 테스트베드 구성 방식은 가상환경 및 실환경으로 구성된 환경 하에서 모의공격자가 공격을 수행하는 기본적인 시험환경 구성 방안으로, 공격자가 개입되어 공격 반복 효율성이 낮지만 공격자의 역량에 따라 다양한 기법을 활용하여 변경된 공격을 수행할 수 있다.

2.2 위협모의기를 통한 모의공격 재현 방안

위협모의기를 포함하는 테스트베드 구성은 앞서 구성한 공격자 기반의 테스트베드 구성에 위협모의기가 추가된 형태이다(그림 2 참조).

위협모의기는 공격자의 모든 공격 행위를 캡처하고 재현하는 기능을 하며, 본 연구에서는 Spirent사의 iTest를 활용하였다. iTest는 테스트 작성 및 실행 통

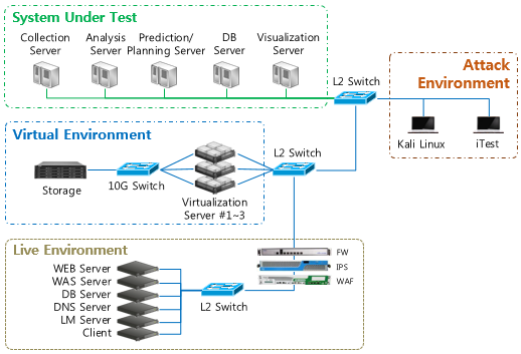


그림 2. 위협모의기를 포함한 테스트베드 구성
Fig. 2. Test bed Configuration with Attack Simulator

합 솔루션으로, 다양한 시험환경과 여러 종류의 테스트를 쉽게 다룰 수 있도록 도와주고 자동화된 테스트로 생산성을 높인다. 본 연구에서는 모의공격 수행 과정을 iTest 기반으로 진행하고 이를 관리함으로써 반복적인 공격뿐만 아니라 공격 과정을 변경하거나 적용된 공격 기술을 변경하여 시험을 수행한다. 위협모의기를 활용한 모의공격 재현 절차는 다음과 같다.

2.2.1 모의공격 수행 및 캡처

모의공격자는 iTest 화면 상에서 Telnet 세션, Web 세션, VNC(Virtual Network Computing) 세션 등을 기반으로 모의공격장비를 활용한 모의공격을 진행하며, 이 과정에서 iTest는 사용자 행위를 캡처하여 모든 행위 과정을 스크립트로 자동 생성한다.

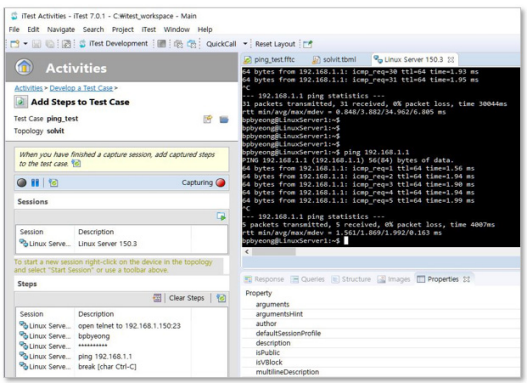


그림 3. 위협모의기를 활용한 모의공격 수행 및 캡처 단계
Fig. 3. Attack & Capture Phase with Attack Simulator

2.2.2 시나리오 생성

앞 순서에서 생성된 스크립트를 공격 시나리오에 따라 조건 및 분기문을 추가하여 Test Case를 생성한다. 이 과정에서 특정 행위를 반복적으로 수행하거나

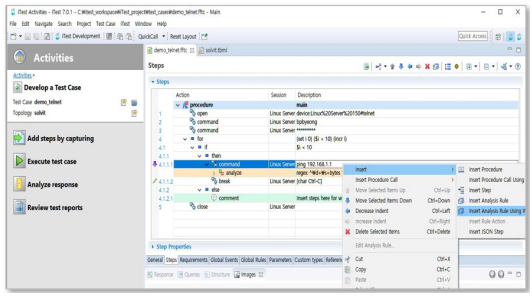


그림 4. 위협모의기를 활용한 시나리오 생성 단계
Fig. 4. Scenario Development Phase with Attack Simulator

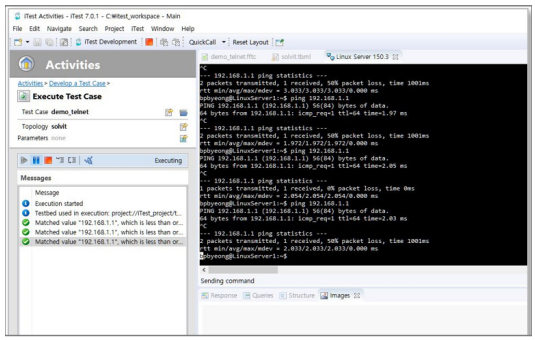


그림 5. 위협모의기를 활용한 모의공격 재현 단계
Fig. 5. Attack Replay Phase with Attack Simulator

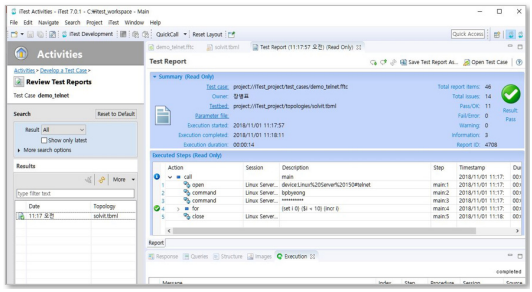


그림 6. 위협모의기를 활용한 결과분석 및 환경 복구 단계
Fig. 6. Review & Recovery Phase with Attack Simulator

여러 공격기술을 적용하여 다양한 공격 시나리오를 생성할 수 있다.

2.2.3 모의공격 재현

스크립트 수정/보완을 통해 생성된 공격 시나리오를 순차적으로 재현한다. 이 과정에서는 공격자의 개입 없이 모의공격 수행 단계에서 수행했던 공격 행위를 그대로 재현하거나, 일부 기술 및 절차를 변경하여 수행 가능하다.

2.2.4 결과분석 및 환경 복구

모의공격 과정이 모두 종료되면 공격 과정을 리뷰하고 결과를 분석한다. 향후 시험을 위해 시험환경을 최초 상태로 복구하며, 가상머신의 Snapshot 복구 기능 및 실환경의 복구 프로그램을 활용한다.

이와 같이 위협모의기를 통한 모의공격 재현 및 반복 시 모의공격자의 추가 투입 없이도 특정 공격과정을 반복하거나 여러 기술을 변경·적용하여 테스트할 수 있으며, 이러한 반복 시험을 통해 지능형 분석에 활용하기 위한 학습 실험데이터 생성이 가능하다.

2.3 에뮬레이션 SW를 통한 모의공격 재현 방안

모의공격을 재현하기 위한 또 다른 방안으로 그림 7과 같이 에뮬레이션 SW를 활용하여 모의공격 과정에서 생성되는 정보를 재현할 수 있다. 사이버 공격을 예측하고 대응하기 위한 본 과제에서는 모의공격 시 탐지장비에 의해 위협이벤트 정보가 생성되며 해당 파일이 수집/통합서버로 수집된다. 이 과정에서 에뮬레이션 SW를 통해 정보수집 단계와 실행 단계를 거쳐 모의공격을 재현할 수 있다.

2.3.1 공격정보 수집 단계

1) 운영자는 공격에 대한 이벤트 정보 수집을 위해 에뮬레이션SW의 위협이벤트 정보 수집 명령을 실행한다.
2) 에뮬레이션SW는 수집된 정보를 정규화하고 분석하는 수집통합SW 처리기(Processor)를 중지한다.
3) 공격자는 모의공격을 수행하고, 탐지장비에 의해 발생된 위협이벤트는 Agent를 통해 Collector로 전달하여 파일이 생성된다. 이때 수집통합SW의 처리기가 비활성화 상태이므로 파일이 처리되지 않고 누적된다.
4) 에뮬레이션SW는 누적된 위협 이벤트 정보 파일을 복사하여 저장한다.

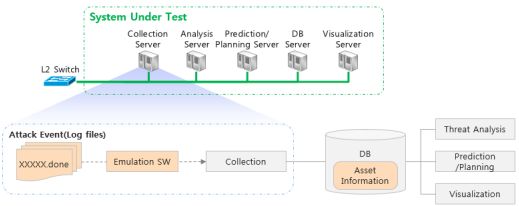


그림 7. 에뮬레이션SW를 활용한 테스트베드 구성
Fig. 7. Test bed Configuration with Emulation SW

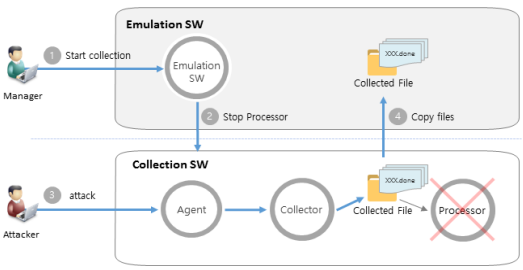


그림 8. 에뮬레이션 SW를 활용한 공격정보 수집 단계
Fig. 8. Attack Event Collection Phase with Emulation SW

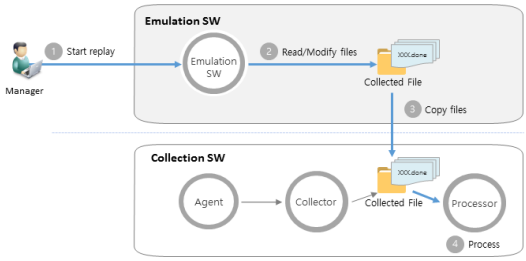


그림 9. 에뮬레이션 SW를 활용한 공격 재현 단계
Fig. 9. Attack Replay Phase with Emulation SW

2.3.2 공격 재현 단계

1) 운영자는 모의공격 재현을 위해 에뮬레이션SW의 재현 명령을 실행한다.
2) 에뮬레이션SW는 파일을 읽은 후 파일 내용 중 이벤트 발생 시간을 현재 시간으로 수정한다.
3) 에뮬레이션SW는 수정된 파일을 수집통합SW의 처리기가 참조하는 위치로 이동시킨다.
4) 수집통합SW의 처리기가 입력된 파일을 처리한다.

본 방식은 시험환경에서 산출된 위협 이벤트 정보 파일을 기반으로 시험을 수행하는 방안으로, 모의공격 과정을 통해 생성된 파일이 필요하며 파일을 에뮬레이션하는 SW가 필요하다. 기 생성된 이벤트 정보 파일을 활용하므로 변경된 형태의 공격은 어렵지만 시험 대상 장비의 시험을 위해 반복적인 수행이 용이하다. 또한 테스트베드 없이 시험 대상 장비만으로 독립적 구성이 가능하므로 휴대성이 높아 시연 등에도 활용될 수 있다.

Ⅲ. 사례 연구

본 연구에서 제안한 세 가지 시험환경 구성방안을 기반으로 그림 10과 같이 가상환경 및 실환경의 테스트베드 상에 150여개의 노드로 구성된 전장망을 구축하고 그림 11의 시나리오로 모의공격을 수행하여 시

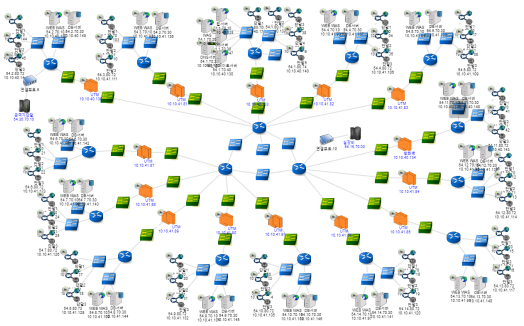


그림 10. 테스트베드 상에 구축된 전장망 환경
Fig. 10. Battlefield Network Environment Configurated in Test Bed

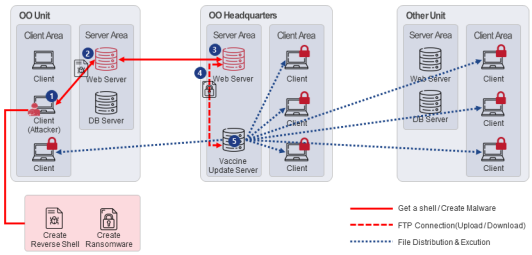


그림 11. 정보유출 및 랜섬웨어 모의공격 시나리오
Fig. 11. Information Leakage and Ransomware Penentration Scenario

험에 활용하였다. 본 연구에 활용된 네트워크 구성은 가상의 데이터를 활용하였으며, 단말들의 백신 업데이트는 OO사령부의 백신 업데이트 서버에서 패치파일을 배포 받아 자동으로 실행되는 것으로 가정한다.

모의공격 시나리오는 OO부대 웹 서버 및 OO사령부 웹 서버를 탈취하여 시스템 정보 및 문서 자료를 수집하고, OO사령부 백신 업데이트 서버를 이용한 랜섬웨어 배포 및 사용자 단말 내 문서 자료를 암호화하는 절차로 구성한다. 침투 경로 및 세부 절차는 다음과 같다.

1) OO부대 웹 서버 정찰 및 스캔
   (1) 포트 스캔
   (2) 웹 취약점 스캔
2) OO부대 웹 서버 탈취 및 정찰
   (1) PHPMYADMIN 브루트포스
   (2) 리버스 쉘 제작 및 업로드
   (3) 리버스 쉘 획득
   (4) 시스템 및 네트워크 정보 탈취 및 분석
   (5) 키로깅 실행 및 계정 획득
3) OO사령부 웹 서버 탈취 및 정찰
   (1) SSH 로그인
   (2) 시스템 및 네트워크 정보 탈취 및 분석
   (3) 백신 업데이트 서버 관련 정보 획득 (계정, 배포 방법)
4) 업데이트 서버에 랜섬웨어 업로드
   (1) 업데이트 서버 FTP 로그인
   (2) 랜섬웨어 파일 업로드
5) 사용자 단말 랜섬웨어 감염
   (1) 업데이트 서버에서 랜섬웨어 자동으로 다운로드/실행
   (2) 랜섬웨어 감염에 의한 문서 자료 암호화

본 연구에 적용된 기술 및 도구는 공개된 CVE 및 도구를 활용하였다. 주요 도구로는 정찰 단계에서 Nmap, Skipfish를 활용하였고, 침투 및 익스플로잇 과정에서는 DIRB, Hydra, MSFVENOM, METASPLOIT을 활용하였다.

주요 기술로는 Dirtyc0w(CVE-2016-5195) 취약점을 이용한 관리자 권한 획득 기술을 활용하였으며, root 권한의 Meterpreter를 획득하여 In-Memory 라이브러리 인젝션을 통해 명령 제어 및 Fileless 공격이 적용되었다.

이와 같이 구성된 모의공격 시나리오를 본 연구에서 제안한 세 가지 시험환경으로 구축하여 시험에 활용하였다. 실환경 및 가상환경으로 구성된 테스트베드 상에서 모의공격자가 직접 공격을 수행하는 과정을 통해 정찰, 침투, 익스플로잇 및 목표 달성이 이루어지는 것을 확인하였으며, Command - Line 기준 200여개의 세부 절차로 이루어진 모의공격 시나리오 수행에 약 1시간이 소요되었다.

또한 위협모의기를 포함한 테스트베드 구성 방안을 적용한 경우 모의공격자가 수행한 공격 과정을 Command -Line 기반으로 동일하게 수행하고, 필요에 따라 명령 옵션 값을 수정하거나 프로그래밍적인 요소를 적용하여 목적지 IP, 절차 간 시간 간격 등을 변수화하여 효율적으로 활용하였다. 이 경우 사용자에 의한 시간 지연이 최소화되어 동일한 모의공격 시나리오 수행에 약 30분이 소요됨을 확인하였다.

마지막으로 에뮬레이션 SW를 활용하여 앞선 과정에서 발생되는 위협 이벤트 정보를 수집하고 재현하는 방안에서는 동일한 모의공격 과정을 재현 시간 설정에 따라 10분 혹은 5분만에도 수행 가능함을 확인하였다. 수집된 파일을 재활용하기 때문에 세부 내용 변경은 제한되지만 특정 시험 과정에 반복적인 공격이 필요한 경우 효과적으로 활용할 수 있다.

Ⅳ. 결 론

본 논문에서는 다양한 공격 기술에 대응하여, 보다 유연하게 시험을 수행하기 위한 세 가지 형태의 시험 환경 구성 방안을 제시하였다. 가상환경 및 실환경으로 통합된 환경에서 모의공격자가 직접 공격을 수행하는 방안을 통해 다양한 기법을 활용하여 변경된 공격을 수행할 수 있으며, 위협모의기를 포함한 테스트베드 구성 방안 활용하여 모의공격자 투입 없이 공격과정을 재현하여 효율적인 시험환경을 제공할 수 있다. 또한 에뮬레이션 SW를 활용하여 위협 이벤트 정보를 수집 및 재현하는 구성 방안을 통해 테스트베드 없이 시험 대상 장비만으로 반복적인 시험 수행이 가능하다.

본 연구에서 제안한 방안들은 시험 단계 및 환경을 고려하여 적합한 구성을 선택하여 유기적으로 활용 가능하므로 향후 다양한 사이버공격의 전략·전술·절차적 특징을 분석하여 공격을 예측하고 대응하는 연구에 활용될 것으로 기대한다.

References

[1] R. Hollister, P. Lardieri, and L. Pridmore, "National cyber range(NCR) automated test tools: implications and application to network-centric support tools," *IEEE AUTOTESTCON Conf.,* pp. 1-4, Sep. 2010.

[2] B. Ferguson, A. Tall, and D. Olsen, "National cyber range overview," *IEEE Military Commun. Conf.*, pp. 123-128, Baltimore, MD, USA, Oct. 2014.

[3] M. K. Ahn and Y. H. Kim. "Research on system architecture and simulation environment for cyber warrior training," *J. KIISC*, vol. 26, no. 2, pp. 533-540, Apr. 2016.

[4] H. Yun, H. Jang, S. Kim, J. Park, and C. Kim, "CyberSecurity virtual network modeling and simulation," in *Proc. KCC KIISE*, pp. 253-255, Yongpyong, Korea, Jun. 2006.

[5] K. Kim, S.-Y. Hong, T. Kim, D. Kim, and Y.-H. Kim, "Applying a hidden router to provide test traffics into training environment for cyber threat," in *Proc. Symp. KICS*, pp. 1372-1373, Jeju Island, Korea, Jun. 2018.

[6] H. J. Kim, D. Lee, M. K. Ahn, Y.-H. Kim, K.-S. Noh, "Measuring technical effectiveness in cyber warfare," in *Proc. KCC KIISE*, pp. 143-145, Jeju Island, Korea, Jun. 2015.

류 한 얼 (Han-Eul Ryu)

2009년 2월 : 한국항공대학교 컴퓨터공학 학사

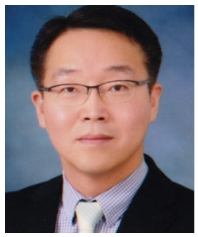
2011년 2월 : 한국항공대학교 컴퓨터공학 석사

2011년 1월~현재 : LIG넥스원 선임연구원

<관심분야> 사이버 보안, 사이버 훈련체계, 시스템 및 네트워크 가상화

[ORCID:0000-0003-2236-1766]

전 성 구 (Sung-Goo Jun)



1998년 2월 : 육군3사관학교 전산정보학 학사

2012년 2월 : 연세대학교 전산정보학 석사

2017년 2월~현재 : LIG넥스원 수석연구원

<관심분야> 사이버전, 사이버 훈련체계, 사이버 지휘통제

심 신 우 (Shin-Woo Shim)

2007년 2월 : 포항공과대학교 컴퓨터공학 학사

2019년 2월 : 고려대학교 정보보호학 석사

2007년 1월~현재 : LIG넥스원 선임연구원

<관심분야> 정보보호, 사이버 지휘통제

[ORCID:0000-0003-0959-9200]

임 선 영 (Sun-Young Im)

2015년 2월 : 아주대학교 컴퓨터공학과 학사
2017년 2월 : 아주대학교 컴퓨터공학과 석사
2017년 1월~현재 : LIG넥스원 선임연구원

<관심분야> 사이버전, 사이버 위협 피해평가
[ORCID:0000-0003-4385-173X]

한 인 성 (In-Sung Han)

2004년 2월 : 광운대학교 컴퓨터과학 석사
2009년 2월 : 광운대학교 컴퓨터과학 박사
2010년~2012년 : 한국정보인증 R&D
2012년~현재 : 국방과학연구소 선임연구원

<관심분야> 센서/애드혹 네트워크보안, 네트워크포렌식, 사이버 위협분석, 사이버 지휘통제

오 행 록 (Haeng-Rok Oh)

1987년 2월 : 인하대학교 전산학과 학사
1989년 2월 : 인하대학교 전산학과 석사
2004년 2월 : 고려대학교 컴퓨터학과 박사수료
1989년 1월~현재 : 국방과학연구소 수석연구원

<관심분야> 사이버 보안, 사이버 지휘통제