사이버전 훈련을 위한 트래픽 발생 시나리오 정책 저작 방안

임선영, 김용현*, 홍수연, 장우현
LIG넥스원, *국방과학연구소
sunyoung.im@lignex1.com, yonghyunkim@add.re.kr, {suyoun.hong, woohyun.jang}@lignex1.com

A Policy Authoring Method for Traffic Generation Scenario in Cyber Warfare Training

Sun-young Im, Yonghyun Kim*, Su-Youn Hong, Woo-hyun Jang
LIG Nex1, *Agency of Defense Development

요 약

사이버 공격이 증가함에 따라 사이버전에 대비하여 실제와 같이 훈련할 수 있는 사이버전 모의전투 기술이 필요하다. 사이버전 모의전투 기술에는 실제 트래픽이 유통되는 네트워크 환경을 모사하기 위해 트래픽 발생 시나리오 저작이 필요하다. 본 논문에서는 트래픽 발생 시나리오를 저작하기 위해 공통으로 사용될 수 있는 정책 저작 방법을 제안하였다.

Ⅰ. 서 론

사이버 공격은 갈수록 증가하고 있다. 이는 일반 기업 대상뿐만 아니라 국가를 대상으로도 마찬가지이다. 그 이유는 네트워크에 연결된 자산들이 증가하고 자산들이 가지고 있는 정보들이 방대해 지면서 정보가 전쟁을 좌지우지 할 수 있게 되었기 때문이다. 사이버전에 대비하기 위해서는 전투원의 역량을 향상 시켜야 하며, 이를 위해서 실제와 같이 훈련할 수 있는 사이버전 모의전투 기술이 필요하다.

사이버전 모의전투 기술은 전투 환경구성, 시나리오 저작, 모니터링, 사후평가로 구분 된다 [1]. 시나리오 저작은 훈련 관리 시나리오, 네트워크 맵 시나리오, 트래픽 발생 시나리오, 위협/방어 행위 시나리오의 네 가지 항목으로 구성 되며, 트래픽 발생 시나리오는 트래픽 소스(상용 트래픽 발생 장치, 트래픽 에이전트 등)를 활용해 트래픽을 발생 시킬 수 있어야 한다 [2]. 기존에는 훈련 관리자가 네트워크 환경만 다르고 비슷한 훈련을 진행할 때 마다 새 네트워크 환경에 맞게 트래픽 발생 시나리오에 대한 모든 정보를 저작해야 하는 번거로움이 있었다. 본 논문에서는 트래픽 발생 시나리오를 저작하기 위해 공통으로 사용될 수 있는 트래픽 발생 시나리오 정책 저작 방법을 제안하였다.

Ⅱ. 트래픽 발생 시나리오 정책 저작

트래픽 발생 시나리오 정책은 사용자 행위, PCAP replay, ATCIS(Amry Tactical Command Infomation System, 육군전술지휘정보체계) 모의를 통해 네트워크 상 일반 사용자들과 군 사용자들의 행위를 모의하기 위해 공통으로 사용할 수 있는 정책을 저작한다.

1. 사용자 행위 정책

사용자 행위 정책에서는 네트워크 상 일반 사용자들의 행위를 모의하기 위한 정책을 저작한다. 사용자 행위는 웹 행위, 메일 행위, 자료 연동 행위로 분류하였다.

1.1 웹 행위 정책

웹 행위 정책에는 웹서핑을 모의하기 위한 정보를 입력한다. 웹 행위 정책은 기본 정보, 웹 분포 설정, 탑 레벨 페이지 리스트로 구성된다.

기본 정보에는 행위명, 행위 설명을 입력한다. 웹 분포 설정에는 뒤로 가기 확률, 탑 레벨 웹 페이지 분포, 탑 레벨 간 시간간격, 부속 페이지 탐색 횟수, 사용자 분포 여부를 입력한다. 탑 레벨 페이지 리스트에는 웹 서핑 대상 URL을 입력한다. 그림 1은 웹 행위 정책 저작 화면을 나타낸다.

그림 1. 웹 행위 정책 저작 화면

1.2 메일 행위 정책

메일 행위 정책에는 메일 송수신을 모의하기 위한 정보를 입력한다. 메일 행위 정책은 기본 정보, 메일 발송 분포 설정, 메일 수신 분포 설정, 메일 내용, 메일 수신자 설정, 첨부파일 설정으로 구성된다.

기본 정보에는 행위명, 행위 설명을 입력한다. 메일 발송 분포 설정에는 파일첨부 확률, 메일 전송 시간 간격, 첨부파일 선정 확률을 입력한다. 메일 수신 분포 설정에는 IMAP/POP3, 답장률, 체크주기, 첨부파일 실행 종료시간, 첨부파일 실행률을 입력한다. 메일 내용에는 메일 제목과 메일 내용을 입력한다. 메일 수신자 설정에는 이름과 메일 주소를 입력한다. 첨부파일 설정에는 첨부파일을 업로드 한다.

1.3 자료 연동 행위 정책

자료 연동 행위 정책에는 자료 연동 체계를 이용한 파일 전송을 모의하기 위한 정보를 입력한다.

자료 연동 행위 정책은 기본 정보, 자료 연동 행위 분포 설정, 첨부파일을 입력한다. 기본 정보에는 행위명, 행위 설명을 입력한다. 자료 연동 행위 분포 설정에는 첨부파일 실행률, 첨부파일 실행 종료시간, 업로드 주기, 다운로드 주기, 첨부파일 선정 확률을 입력한다. 첨부파일에는 첨부할 파일들을 업로드 한다.

2. PCAP Replay 정책

PCAP Replay 정책에는 군 내부에서 정상 데이터셋 구축 도구를 통해 수집 및 데이터셋으로 구축된 PCAP(Packet CAPture, 패킷 캡처) 파일을 업로드하여 해당 PCAP에 있는 패킷들을 모의하기 위한 정보를 입력한다.

PCAP Replay 정책은 기본 정보, PCAP 파일 등록으로 구성된다. 기본정보에는 PCAP명, PCAP 설명, 첫 번째 IP, 첫 번째 IP 설명, 두 번째 IP, 두 번째 IP 설명을 입력한다. PCAP 파일 등록에는 사용할 PCAP 파일을 업로드한다. 그림 2는 PCAP Replay 정책 저작 화면을 나타낸다.

그림 2. PCAP Replay 정책 저작 화면

3. ATCIS 모의 정책

ATCIS 모의 정책은 전장망 환경 제공을 위한 정책으로 ATCIS 전문 모의 정책과 ATCIS 서버 모의 정책으로 구성된다.

3.1 ATCIS 전문 모의 정책

ATCIS 전문 모의 정책에는 ATCIS 무기체계 전문을 모의하기 위한 정보를 입력한다. ATCIS 전문 모의 정책은 기본 정보, 메시지 전송 분포 설정, 전문으로 구성된다. 기본 정보에는 모의명, 모의 설명을 입력한다. 메시지 전송 분포 설정에는 반복 횟수 및 메시지 전송 시간 간격을 입력한다. 전문은 무기체계 별로 입력하는 내용이 다르며 BTCS (Battalion Tactical Command System, 포병대대 전술 통제기)의 경우 헤더와 전문 내용으로 구성된다. 헤더에는 수신자 주소, 암호, 송신자 주소가 있으며, 전문 내용에는 표적규모와 좌표 등을 입력한다. 그림 3은 ATCIS 전문 모의 정책 화면을 나타낸다.

그림 3. ATCIS 전문 모의 정책 화면

3.2 ATCIS 서버 모의 정책

ATCIS 서버 모의 정책에는 ATCIS 무기체계 하달 전문을 모의하기 위한 정보를 입력한다. ATCIS 서버 모의 정책은 기본 정보, 메시지 수신 분포 설정, 전문으로 구성된다. 기본 정보에는 모의명, 모의 설명을 입력한다. 메시지 수신 분포 설정에는 서버 응답률과 체크 주기를 입력한다. 전문 내용은 무기체계 별로 입력하는 내용이 다르며 BTCS의 경우 표적 번호와 표적 규모 등을 입력한다.

Ⅲ. 결론

본 논문에서는 사이버전 훈련을 위한 트래픽 발생 시나리오 정책 저작 방안에 대하여 제안하였다. 제안한 방법을 통해 트래픽 발생 시나리오 저작 시 공통으로 사용될 수 있는 부분을 정형화하였다. 이를 통해 훈련 관리자가 시나리오 저작 시 네트워크 환경만 다르고 비슷한 훈련을 진행할 때 공통적으로 사용될 수 있는 부분도 매번 새 네트워크 환경에 맞게 트래픽 발생 시나리오를 저작하는 번거로움을 줄일 수 있을 것으로 기대한다.

ACKNOWLEDGMENT

이 논문은 국방과학연구소의 지원으로 수행된 연구임(UC180003ED)

참 고 문 헌

[1] 임선영, 박아란, 전성구, 김태규, “사이버전 모의전투 결과 분석 방법,” 한국통신학회 학술대회논문집, pp.1449-1450, 2018.

[2] 송의현, 조완수, 이창원, 안명길, “통합 DB를 이용한 사이버전 훈련 시나리오 저작 방안,” 한국군사과학기술학회 종합학술대회, pp.1322-1323, 2019.