사이버 훈련 환경을 위한 위협/방어 도구 다운로드 자동화 구조 설계

류한얼, 홍수연, 김동화*, 서성연*

LIG넥스원, *국방과학연구소

haneul.ryu@lignex1.com, suyoun.hong@lignex1.com, *donghwa.kim@add.re.kr, *syseo@add.re.kr

Structure Design of Automatic Download Threat and Defense Tools for Cyber Training Environment

Ryu Haneul, Hong Suyoun, Kim Dongwha*, Seo Seongyun*

LIG nex1, *Agency for Defense Development

요 약

사이버 훈련 환경은 공격의 위험성으로 인해 통상 인터넷에 연결되지 않은 독립된 네트워크 환경으로 구성된다. 이러한 환경에서 훈련에 필요한 위협/방어 도구를 관리하고 공급해 줄 수 있는 시스템이 필요하다. 본 연구에서는 가상 훈련환경 구성 시 동일한 훈련 세션을 동시에 여러개 운영할 수 있도록 시스템을 설계하고, 훈련 내/외부 네트워크를 분리하여 훈련 환경으로부터 발생될 수 있는 사이버 위협의 전파를 방지할 수 있도록 설계하였다. 또한 사이버 훈련에 필요한 위협/방어 도구를 관리하고, 훈련 환경과는 독립된 형태로 네트워크를 구성하여 훈련 트래픽에 영향을 받지 않으면서 필요한 도구를 훈련 대상 가상머신으로 자동으로 다운로드하도록 설계하였다.

Ⅰ. 서론

정보화 기술의 발전으로 다양한 기기들이 인터넷에 연결되고 기존에 오프라인에서 이루어지던 많은 영역이 온라인 환경으로 옮겨지고 있다. 네트워크를 기반으로 하는 환경이 발전하는 것에 비례하여 사이버 공격 또한 지속적으로 증가되고 있으며, 공격 대상과 파급력 또한 커지고 있다. 이러한 사이버 공간은 일상적인 생활의 영역을 넘어서 집단 간 혹은 국가 간의 대립이 이루어지는 장소이며, 사이버 공격으로부터 집단의 이익, 국가의 이익을 보호하기 위해 다양한 민간 및 군 기관에서 사이버 훈련을 위한 환경을 구축하고 기술 발전, 인력 양성을 위한 교육 및 훈련을 시행하고 있다[1][2][3].

사이버 훈련 환경은 사이버 공격의 위험성으로 인해 통상 인터넷에 연결되지 않은 독립된 네트워크 환경으로 구성하며, 환경 구성 및 운영의 편의성을 고려하여 하이퍼바이저를 기반으로 하는 가상환경으로 구축하여 사용되고 있다. 가상환경에서의 훈련을 위해서 사전에 훈련자에게 할당되는 가상머신에 훈련 간 필요한 환경 설정 및 도구가 설치된다. 하지만 훈련 중 필요한 도구를 다운받을 필요가 있고, 사용자가 필요한 도구를 찾고 선택하는 과정도 훈련의 한 부분이기 때문에 공격과 방어가 이루어지는 환경 외에도 훈련 도구를 제공하고 공급받는 환경이 구축되어야 한다. 훈련을 위한 독립된 네트워크 환경에서 훈련 도구를 제공하기 위해서 파일 서버 형태로 환경이 구축될 수 있지만, 훈련환경과 직접 연결된 네트워크로 구성될 경우 훈련에 의한 영향이 있을 수 있으며 두 개 이상의 훈련 세션이 운영될 경우 파일 서버를 통해 연결되어 독립된 네트워크 환경이라고 할 수 없다.

본 연구에서는 훈련 목적의 네트워크와 제어/관리 목적의 네트워크를 분리하여 가상 훈련 환경에서 발생할 수 있는 위험성을 차단하는 환경을 구축하고, 제어 네트워크를 통해 위협/방어 훈련 도구를 자동으로 다운로드하는 시스템의 구조를 설계하였다.

Ⅱ. 본론

2.1 사이버 훈련 환경 네트워크 구성

사이버 훈련 환경의 네트워크는 훈련 세션 간 서로 영향을 받지 않도록 독립된 네트워크 환경으로 구성되어야 한다. 또한 사이버 위협 및 방어 훈련이 전개되는 내부 가상환경에서 발생할 수 있는 악성코드 등의 위협이 외부로 전파되지 않도록 차단되어야 한다. 이를 위해 그림 1과 같은 사이버 훈련 환경의 네트워크를 설계하였다. 구성도에 포함된 모든 모듈은 가상 환경 상에서 가상머신, 가상라우터 또는 가상스위치로 구성된다. 네트워크를 크게 세 부분으로 나누어, 독립된 훈련 환경을 구성하기 위한 훈련 네트워크(Training Network)와 훈련 외적인 부분을 처리하는 제어 네트워크(Control Network), 훈련환경 외부에서 전반적인 관리를 수행하는 관리 네트워크(Management network)로 구분하였다.

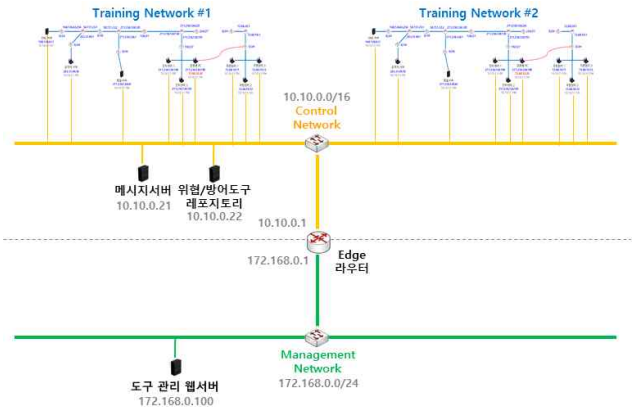

그림 1 사이버 훈련 환경 네트워크 구성도

2.1.1 훈련 네트워크

훈련 네트워크는 훈련 환경 구성에 따라 다양한 IP 대역을 가질 수 있으며, 가상 스위치 및 가상 라우터를 포함한 형태의 네트워크로 구성될 수 있다. 인터넷에 연결되지 않는 독립된 환경이므로 공인 IP 대역을 모의하여 훈련 대상이 되는 네트워크 대역을 그대로 가상환경에 구축할 수 있다. 또한 오버레이 네트워크 기술인 VXLAN(Virtual Extensible Local Area Network)을 활용하여 하나의 환경에 동일한 IP를 사용하는 훈련 환경을 동시에 독립된 환경으로 구축하여 운영하도록 구성하였다.

2.1.2 제어 네트워크

제어 네트워크는 제어 네트워크 스위치(그림 1에서 10.10.0.0/16 대역의 IP로 설정함)를 기반으로 훈련 환경의 서버 및 단말과 연결되며, 위협/방어 도구 레포지토리 및 메시지 서버 등 제어 인프라 노드와도 연결된다. 훈련 네트워크 환경에 포함되는 서버 및 단말 등의 노드는 훈련 네트워크 대역에 연결됨과 동시에 훈련 데이터 수집, 에이전트 제어, 훈련 도구 제공을 위한 제어 네트워크에 연결된다. 이는 훈련 외적인 부분으로 훈련자가 활용하고 접근하는 대상에서는 제외된다.

2.1.3 관리 네트워크

관리 네트워크는 훈련 환경의 외부에 위치하며 관리 네트워크 스위치(그림 1에서 172.168.0.0/24 대역의 IP로 설정함)를 기반으로 도구 관리 웹서버 등 훈련 환경을 전반적으로 관리하기 위한 시스템이 연결된다.

2.1.4 사이버 위협 차단을 위한 네트워크 설정

사이버 훈련 환경 내부와 외부 환경의 경계를 구분하는 지점인 Edge 라우터에 네트워크 주소 변환(NAT, Network Address Translation) 기능을 적용하였다. NAT는 IP 패킷의 TCP/UDP 포트 번호와 소스 및 목적지의 IP 주소를 변경하여 라우터를 통해 네트워크 트래픽을 주고 받는 기술로, 주로 인터넷과 사설 네트워크 사이에서 사설 네트워크에 속한 여러 개의 호스트가 하나의 공인 IP 주소를 사용하여 인터넷에 접속하기 위한 용도로 사용된다. 사설 네트워크에서 외부의 인터넷에 위치한 공인 IP로 접근 시 Source IP 변경이 이루어지므로 외부에서는 사설 네트워크에 위치한 노드의 IP를 알 수 없으며 이는 사이버 공격이 난무하는 인터넷으로부터 사설 네트워크의 자산을 보호하는 효과가 있다. 본 연구에서는 사이버 위협/방어 훈련이 시행되는 훈련 환경이 위험성이 높으며, 이로부터 훈련 환경 외부에 위치한 관리 네트워크 자산을 보호하기 위해 NAT 설정을 적용하였다. 관리 네트워크에서 제어 네트워크로 접근 시 Source NAT를 적용하여 Source IP인 관리 네트워크 IP를 제어 네트워크의 Gateway IP로 변경한다. 이를 통해 훈련 환경에서 악성 코드 등이 제어 네트워크로 전파된다고 하더라도 Edge 라우터에 적용된 NAT로 인해 훈련 환경 외부에 위치한 관리 네트워크 자산을 보호할 수 있다.

2.2 위협/방어 도구 다운로드 자동화 구조 설계

독립된 사이버 훈련 환경 상에서 훈련에 필요한 위협/방어 도구를 가상머신에 다운받기 위해서는 도구를 제공해주는 별도의 파일서버가 필요하며, 훈련 세션의 독립성을 유지한 상태에서 도구가 제공되어야 한다. 훈련 네트워크에 직접 파일서버를 연결할 경우 훈련 세션 별로 파일서버를 제공해야 하는데, 파일서버의 규모가 커지고 훈련 세션이 많아질 경우 이러한 형태로 서버를 운영하기에는 스토리지 용량 문제와 유지 관리에 어려움이 있다. 이를 위해 본 연구에서는 앞서 설계한 제어 네트워크를 이용하여 도구를 다운받을 수 있도록 도구 관리 웹서버, 메시지 서버, 위협/방어 도구 레포지토리로 구성된 시스템을 설계하였고, 훈련자가 도구 다운로드를 요청할 경우 다운로드 대상 가상머신을 지정하여 해당 가상머신으로 자동 다운로드 되도록 설계하였다.

도구 관리 웹서버는 훈련 관리자가 웹 인터페이스를 통해 위협/방어 도구 레포지토리에 구축된 도구들의 목록을 확인하고 추가, 수정, 삭제할 수 있도록 관리 기능을 제공한다. 훈련 관리자는 인터넷에서 확보 가능한 도구들을 비롯하여 훈련에 필요한 위협/방어 도구를 도구 관리 웹서버를 통해 구축하고 관리한다. 훈련자는 도구 관리 웹서버에서 제공하는 키워드 검색 기능을 이용해 다양한 훈련 도구를 찾아서 본인에게 할당된 훈련 가상머신을 선택하고 다운로드를 요청할 수 있다. 훈련자가 다운로드를 요청하면 도구 관리 웹서버는 메시지 서버에 접속하여 다운로드 대상 도구의 파일 경로와 다운로드 대상 가상머신 정보를 기반으로 메시지를 생성하고 메시지 서버로 메시지를 Publish한다.

메시지서버는 Publish - Subscribe 모델을 기반으로 메시지를 처리하는 서버이다. 훈련자가 훈련 도구 다운로드를 요청하는 메시지를 Publish하면 해당 메시지가 메시지 서버에 저장되고 훈련 환경에 도구 다운로드 에이전트를 구축하여 메시지 서버로부터 다운로드 요청 메시지를 Subscribe하도록 설계하였다.

훈련 환경의 각 가상머신에 위치한 에이전트는 그림 2와 같은 순서로 동작한다. 에이전트 초기화 시 메시지 서버에 접속하여 자신이 Subscribe할 메시지를 등록한다. 그리고 주기적인 메시지 서버 조회를 통해 자신에게 할당된 메시지가 있을 경우 메시지 서버로부터 이를 Subscribe하여 다운로드할 도구의 경로를 획득하고, 위협/방어 도구 레포지토리로부터 FTP 프로토콜을 통해 해당 경로에 위치한 도구를 자동으로 다운로드한다.

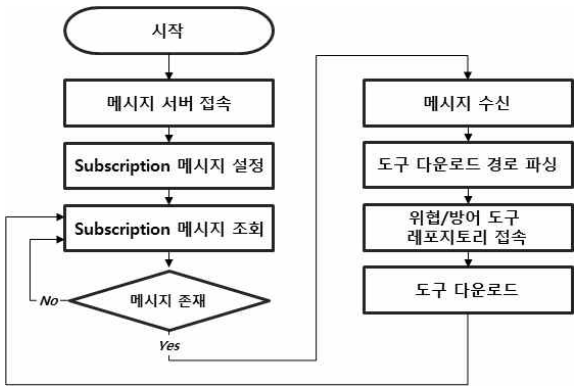

그림 2 도구 다운로드 에이전트 동작 순서도

위협/방어 도구 레포지토리는 훈련에 필요한 위협 및 방어 도구를 파일서버 형태로 구축한 노드이다. 훈련자가 특정 경로에 위치한 도구를 다운로드 요청할 경우 훈련 환경에 위치한 에이전트가 FTP 프로토콜을 통해 해당 파일을 다운로드할 수 있도록 설계하였다. 에이전트를 통해 위협/방어 도구를 자동으로 다운로드할 경우 훈련자는 가상머신의 OS 및 파일 전송 방식을 신경쓰지 않고 윈도우 가상머신은 물론 리눅스 및 유닉스 가상머신에도 용이하게 도구를 다운로드할 수 있다.

Ⅲ. 결론

본 연구에서는 가상 훈련환경 구성 시 VXLAN을 기반으로 훈련 네트워크 환경을 구성하여 동일한 훈련 세션을 동시에 여러개 운영할 수 있으며, Edge 라우터에 NAT를 적용하여 훈련 환경으로부터 발생될 수 있는 사이버 위협의 전파를 방지할 수 있도록 설계하였다.

또한 위협/방어 도구 다운로드 자동화 구조 설계를 통해 사이버 훈련에 필요한 위협/방어 도구를 관리하고, 훈련 환경과는 독립된 형태로 네트워크를 구성하여 훈련 트래픽에 영향을 받지 않으면서 필요한 도구를 훈련 대상 가상머신으로 다운로드할 수 있다. 훈련자가 가상머신의 플랫폼에 관계없이 도구 관리 웹서버로부터 다운로드 요청을 하면, 에이전트를 통해 윈도우, 리눅스, 유닉스 등 다양한 가상머신에서 해당 도구를 자동으로 다운로드하는 편의성을 제공한다.

ACKNOWLEDGMENT

이 논문은 국방과학연구소의 지원으로 수행된 연구임(UC180003ED)

참 고 문 헌

[1] B. Ferguson, A. Tall, and D. Olsen, “National cyber range overview,” IEEE Military Communications Conference, pp.123-128, Oct. 2014

[2] 안명길, 김용현, “사이버전사의 훈련을 위한 시스템 구축 방안 연구”, 정보보호학회논문지 26(2), pp.533-540, Apr. 2016

[3] 김광수, 홍수연, 김태규, 김동화, 김용현, “사이버 훈련 환경에 시험트래픽 공급을 위한 Hidden Router 개념”, 한국통신학회 학술대회논문집, pp.1372-1373, Jun. 2018