# 실습 중심 보안 교육을 위한 실시간 패킷 시각화 및 코드 기반 플랫폼

임찬혁, 김상대

순천향대학교 의료IT공학과

ich053012@google.com, sdkim.mie@sch.ac.kr

# A Real-Time Packet Visualization and Code-Based Platform for Practice-Oriented Security Education

Chanhyeok Lim, Sangdae Kim

Dept. of Medical IT Engineering, Soonchunhyang University

요 약

본 논문은 보안 교육 현장에서의 이론 중심 교육과 코드-패킷 간 단절 문제를 해결하고자, 실시간 패킷 시각화 및 코드 기반 분석이 가능한 실습형 보안 교육 플랫폼을 제안한다. 제안된 플랫폼은 사용자가 직접 공격 시나리오(메시지 전송, DoS, 포트 스캔 등)를 실행하고, 그에 따른 패킷 흐름과 서버 측 방어 동작을 실시간으로 시각화하며, 동시에 관련된 코드까지 확인할 수 있어 코드 기반의 학습도 가능하다. 본 플랫폼은 보안 개념의 직관적인 이해를 지원하고, 향후 다양한 공격 시나리오 추가를 통해 실습 범위를 확대할 수 있는 확장성을 갖는다.

## Ⅰ. 서 론

최근 개인정보 유출, 랜섬웨어, 피싱 등 보안 사고가 잇따르면서 정보보안의 중요성이 그 어느 때보다 크게 부각되고 있다. 이에 따라 단순한 이론 중심 교육을 넘어, 실제 공격 시나리오를 체험하고 네트워크에서 오가는 패킷을 직접 분석하는 실습 중심의 보안 교육에 대한 수요가 급증하고 있다. 그러나 대부분의 교육은 코드 실행 과정과 네트워크 흐름을 분리해 다루는 경우가 많아, 보안 시스템의 동작 원리를 통합적으로 이해하는 데 한계가 있다. 이러한 배경에서, 공격·방어 코드의 실행 결과와 네트워크 패킷 흐름을 동시에 시각화하여 보여주는 '융합형 보안 해킹 교육 플랫폼'의 필요성이 점차 대두되고 있다.[1][2]

현재 네트워크 보안 교육에서는 다양한 플랫폼[3],[4]들이 활용되고 있지만 각기 특정 기능에 집중되어 있어 보안 시스템의 전체 동작을 통합적으로 이해하는데 한계가 있다. Wireshark는 수동적인 패킷분석에, TryHackMe는 해킹 시나리오 체험에 초점을 맞추고 있어, 코드 실행과 네트워크 흐름을 연계한 학습에는 부족함이 있다. 보안 개념을 깊이 있게 이해하려면 코드 실행과 패킷 전송 과정을 하나의 흐름으로 파악해야 하지만, 기존 플랫폼은 실시간 공격·방어 체험과 네트워크 기반 방어 학습을 효과적으로 지원하지 못하는 상황이다.

이러한 한계를 보완하고자, 본 연구에서는 사용자가 직접 공격 시나리오를 실행하고 그에 따른 패킷 흐름과 방어 로직의 작동 과정을 실시간으로 확인할 수 있는 '실시간 패킷 시각화 기반 보안 교육 플랫폼'을 개발하였다. 이 플랫폼은 코드 실행 결과와 네트워크 트래픽을 통합적으로 시각화함으로써, 보안 입문자들이 보다 직관적으로 공격과 방어의 원리를 이해할 수 있도록 설계되었다.

## Ⅱ. 플랫폼 구성 요소

본 연구의 플랫폼은 공격자 역할의 클라이언트 GUI와 패킷을 수신·분석하는 서버 웹 인터페이스로 구성된다. 사용자가 실행한 공격(메시지 전송, DoS, 포트 스캔 등)에 따라 패킷 로그가 실시간으로 수집·시각화되며, 임계치를 초과하면 방어 로직이 자동으로 작동한다.

공격 및 방어코드는 함께 시각화되어 코드 단위의 흐름 이해를 돕고, 웹 화면에서는 표, 그래프, 설명 메시지를 통해 전체 과정을 직관적으로 확인할 수 있다.

| 구성항목 | 내용/항목 설명 |
|---|---|
| 개발환경 | Visual Studio Code |
| 프로그래밍 언어 및 프레임워크 | Python(Flask, tkinter)<br>HTML, CSS, Java Script |
| 네트워크 관련 라이브러리 | socket, scapy |
| 시각화 도구 | Chart.js , Java Script |
| 시스템 구성 장치 | MacBook : 클라이언트(공격자)<br>Windows PC : 서버(피해자, 분석 및 시각화 담당) |

## Ⅲ. 플랫폼 동작 과정

### Ⅲ-1. 공격 화면 및 동작 과정 안내

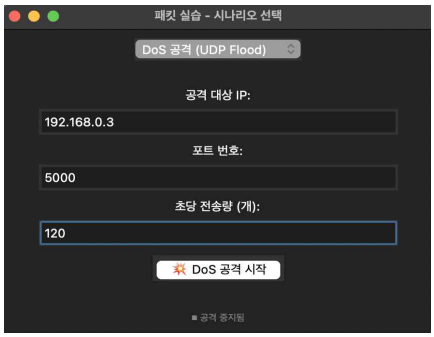


그림 1. 공격 예시 화면

[그림 1]은 사용자가 클라이언트 측 GUI에서 DoS 공격(UDP Flood) 시나리오를 선택하고, 공격 대상 IP, 포트 번호, 초당 전송량을 직접 입력한 후 공격을 실행하는 화면이다. 해당 GUI는 tkinter 기반으로 구현되었으며, 시나리오 실행 시 사용자의 설정에 따라 실시간으로 UDP 패킷을 생성하여 전송한다.

그림 2. 서버 측 웹 인터페이스 화면

### Ⅲ-2 서버 측 웹 인터페이스 동작 결과 설명

[그림 2]는 본 플랫폼의 서버 측 웹 인터페이스 구성으로, 실시간 패킷 수신 표, 초당 패킷 수 그래프, 설명 로그, 차단된 IP 목록의 네 가지 주요 요소로 이루어져 있다. 각 구성 요소의 기능은 다음과 같다. 먼저 [그림 2-1]은 시간, 출발지 IP, 목적지 IP, 프로토콜, 패킷 크기, 전송 상태(전송됨/차단됨), 전송된 데이터 크기 등의 정보를 실시간으로 표 형태로 보여주는 영역이다. 이 표는 출발지 및 목적지 IP 필터, 임계치 설정 드롭다운(예: DoS 100개/초), 보기 옵션(전체/정상/차단 패킷) 등을 제공하여, 사용자 맞춤형 필터링이 가능하다. [그림 2-2]는 초당 수신된 패킷 수를 시간 축 기준으로 시각화한 선형 그래프로, 실시간 갱신을 통해 특정 시점의 급격한 패킷 증가를 확인할 수 있어 DoS 공격과 같은 이상 트래픽 탐지에 효과적이다. [그림 2-3]은 탐지된 이벤트 정보를 요약한 설명 로그로, 공격 유형, 공격 IP, 시각, 패킷 수치, 임계치 초과 여부 등이 자동으로 기록된다. 또한, 임계치나 탐지 모드 변경과 같은 사용자 설정 이력도 함께 남아 분석 및 검토에 활용할 수 있다. 마지막으로, 그림 [2-4]는 임계치를 초과한 출발지 IP를 자동 탐지하여 실시간으로 차단 목록에 추가하는 기능을 제공하며, 사용자는 필요 시 해당 IP의 차단을 수동으로 해제할 수도 있다. 예시에서는 IP 192.168.0.230이 초당 101개의 UDP 패킷을 전송하여 DoS로 탐지되고 차단된 상태를 보여준다. 사용자는 차단된 IP를 확인하고 필요 시 수동으로 해제할 수도 있다. 이와 같이 본 인터페이스는 실시간 분석 결과를 시각적으로 제공함으로써, 사용자가 네트워크 패킷 흐름과 보안 탐지 결과를 보다 직관적으로 이해하고 판단할 수 있도록 설계되었다.

### Ⅲ-3 인터페이스 코드 추가 설명 화면

그림 3. 코드 추가 설명 화면

[그림 3]은 DoS 공격 시나리오에서 사용된 dos_attack 함수의 실행 코드를 시각화한 화면이다. Python으로 작성된 이 코드는 socket.sendto() 함수를 사용해 지정된 IP와 포트로 사용자가 설정한 속도(rate)만큼 UDP 패킷을 반복 전송하며, UDP Flood 공격을 수행한다. 이를 통해 사용자는 공격의 동작 원리를 코드 수준에서 직관적으로 파악할 수 있고, 같은 방식으로 방어 코드와 작동 조건도 확인할 수 있다.

이처럼 본 플랫폼은 GUI 기반 시나리오 실행, 실시간 패킷 분석, 코드 수준 확인까지 공격-분석-학습 전 과정을 연계함으로써 보안 교육의 직관성과 실습 효과를 동시에 높일 수 있다.

## Ⅳ. 결론

최근 실습 중심의 보안 교육에 대한 수요가 증가하고 있으나, 대부분의 교육 도구는 코드 실행과 네트워크 패킷 흐름을 별도로 다루어 보안 시스템의 동작 원리를 직관적으로 이해하기에 한계가 있었다. 이러한 문제를 보완하고자 본 연구에서는 공격·방어 코드와 실시간 패킷 흐름을 통합적으로 시각화할 수 있는 학습 플랫폼을 설계·구현하였다.

본 연구에서 제안한 플랫폼은 공격과 방어 과정을 코드와 패킷 흐름 차원에서 통합적으로 학습할 수 있는 환경을 제공함으로써, 보안 교육의 직관성과 실습 효과를 높일 수 있을 것으로 기대된다. 다만 현재는 DoS,포트 스캔 등 일부 기본 시나리오에 한정되어 있으며, 향후 다양한 유형의 공격 유형을 추가해 보다 현실적인 보안 교육으로 확장할 예정이다.

## ACKNOWLEDGMENT

"본 연구는 2025년 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학사업의 연구 결과로 수행되었음"(2021-0-01399)

## 참 고 문 헌

[1] 차상길. "해킹 교육을 해킹하라" 보안뉴스 2021.02 (https://m.boannews.com/html/detail.html?idx=94641)

[2] 문정후. "애플리케이션 보안, 강조만 하지 말고 교육부터 시작하라" 보안뉴스 2023.03.28. (https://www.boannews.com/media/view.asp?idx=115559)

[3] Wireshark Foundation, "Wireshark," (https://www.wireshark.org/)

[4] TryHackMe, "Learn Cyber Security," (https://tryhackme.com/)