기초 오펜시브 시큐리티 기법 실습을 위한 파이썬 기반 교보재 개발

이해영*, 김태형*, 임윤수*, 박도규*, 최승용*

*청주대학교 소프트웨어융합학부

Development of Python Based Training Aids for Basic Offensive Security Technique Exercises

Hae Young Lee*, Tae Hyeng Kim*, Yoonsu Lim*, Do Kyu Park*, Seongyong Choi*

*Division of Software Convergence, Cheongju University

요 약

본 논문은 대학 학부 과정에서 기초적인 오펜시브 시큐리티 기법을 실습할 수 있는 파이썬 기반 교보재를 설명한다. 학생이 주어진 파이썬 스니펫을 확장하여 직접 오펜시브 시큐리티 기법을 코드로 작성 및 실행하고, 공격에 대해 대응 기법을 실습할 수 있다. 필요한 경우 대상 체계를 취약하도록 만드는 설정 파일과, 수업 후 과제로 부여할 수 있는 예제도 제공한다. 이를 통해 학생의 체계에 대한 이해도 및 정보보호 교육 효과를 높일 수 있을 것으로 기대한다.

I. 서론

보안 교육에서 오펜시브 시큐리티 기법을 활용하여 실습을 수행하면, 대상 체계에 대한 이해를 향상시킬 수 있으며, 이에 따라 교육 효과의 향상도 기대할 수 있다[1]. 그러나 현재 오펜시브 시큐리티 기법 교육 대부분[1~3]이 단순 공격 도구를 활용하는 수준에 머물고 있다. 예를 들어, arpspoof 도구[4]로 ARP 스푸핑(ARP spoofing)을 수행하는 수준이다. 만약 학습자가 직접 오펜시브 시큐리티 기법을 코드로 작성하여 실습할 수 있다면, 체계에 대한 이해 및 교육 효과도록 보다 더 향상시킬 수 있을 것이다.

본 논문에서는 기초적인 오펜시브 시큐리티 기법을 실습하는데 활용할 수 있는 파이썬(Python) 기반 교보재를 설명한다. 교보재는 학부생 대상 교육을 가정하며, 실습 시간에 활용할 수 있는 오펜시브 기법 스니펫 모음(snippets), 필요한 경우 대상 호스트를 취약하게 만드는 설정 파일(setups), 그리고 실습 후 복습 및 심화 학습을 위한 과제 예제(assignments)로 구성된다.

II. 파이썬 기반 실습 교보재

본 절에서는 기초 오펜시브 시큐리티 기법 실습에서 활용할 수 있는 파이썬 스니펫에 대해 설명한다.

2.1 스니펫 모음

파이썬 스니펫 모음은 대학 학부 전공 과정에서 기초적인 보안 공격 기법을 실습할 때 교보재로 활용할 수 있도록 개발 중이며, 깃헙(GitHub)을 통해 제공[1]된다. 각 스니펫은 해당 보안 공격 기법 실습에 필요한 핵심적인 코드만을 포함한다. 학생은 실습 환경 및 주어진 정

1) https://github.com/haelee/allbypythonself

보에 맞춰 스니펫을 수정·보완하며 보안 공격 기법을 실습할 수 있으며, 이에 대한 대응 기법도 함께 실습할 수 있다.

<그림 1>의 텔넷 대상 사전 공격(dictionary attack) 스니펫(dictionary.py)으로, telnetlib을 사용하여 대상 호스트의 텔넷 서버와 연결하고, 로그인을 수행하는 코드만 포함한다. 학생은 스니펫을 주어진 계정 ID와 사전에 있는 단어를 반복적으로 입력하는 코드로 발전시키고, 이를 실행하여 대상 ID의 패스워드를 알아낸다. 학생은 대응으로 패스워드 복잡성 및 계정 잠금 임계값을 설정한다[5].

```
import os
import telnetlib

t = telnetlib . Telnet ("10.0.2.4")
t . read_until ("login: ")
t . write ("victim\n")
t . read_until ("Password": ")
t . write ("rockyou\n")
t . close ()
```

<그림 1> 사전 공격 실습용 스니펫

<표 1> 파이썬 스니펫 목록

분야	스니펫	기법
암호 및 시스템	crack.py	패스워드 크래킹
	dictionary.py	사전 공격
네트워크	arpspoof.py	ARP 스푸핑
	icmpredirect.py	ICMP 리다이렉트 공격
	portscan.py	SYN 스캐닝
	smurf.py	스머프 공격
	synflood.py	SYN 플러딩
	tcpreset.py	TCP 리셋 공격

<표 1>은 2019년 10월 1일 현재 제공되는 파이썬 스니펫 목록이다. 네트워크 분야 실습용 스니펫은 데이터 링크 수준에서 패킷을 조작할 수 있는 Scapy 프로그램[6]을 사용한다. 시스템 분야 실습용 스니펫 중, 패스워드 크래킹 스니펫은 리눅스 crypt 루틴과의 인터페이스를 구현한 crypt 모듈을, 사전 공격 스니펫은 텔넷 클라이언트를 구현한 telnetlib 모듈을 사용한다.

2.2 설정 파일

제공 스니펫 중 일부는 대상 호스트에 취약점이 존재해야 실습이 가능하다. 예를 들어, 스머프 공격(Smurf attack)은 로컬 네트워크 내의 모든 호스트에서 net.ipv4.icmp_echo_ignore_broadcasts를 0으로 설정해야 공격이 가능하다. 설정 파일은 이와 같은 설정을 수행하는 스크립트 모음이다. 학생은 공격 기법 실습 전 대상 호스트에서 해당 설정 파일을 실행한다.

2.2 과제 예제

실습수업 후 학생에게 스니펫을 보다 발전시키도록 과제를 부여할 수 있다. 예를 들어, 패스워드 크래킹 스니펫은 실습에서 하드 코딩된 해시 값을 사용자로부터 입력받거나 /etc/shadow 파일에서 읽어오도록 수정할 수 있다. 사전 공격 스니펫의 경우, 스레드를 사용하여 보다 효율을 높일 수도 있다. 과제 예제는 이러한 과제의 예로, 현재 학부 1~2학년 수준으로 제공한다.

III. 결론 및 향후 연구

본 논문은 학부 교과에서 보안 공격·방어 메커니즘에 대한 이해를 돕기 위한 파이썬 기반의 실습 교보재를 소개하였다. 실습 교보재는 스니펫, 설정 파일, 과제 예제로 구성되며, 스니펫을 활용한 보안 공격 코드 작성, 설정 파일을 사용한 취약점 설정, 보안 공격·방어 수행, 공격 코드 보완하는 형태로 실습 및 과제를 진행할 수 있다.

파이썬 기반 실습 교보재를 네트워크 보안, 암호학, 운영체제 관련 학부 교과 및 동아리 비교과 프로그램에서 활용하였다. 정식으로 설문을 실시하지는 않았으나, 학생의 피드백(강의평가 등)을 볼 때 공격·방어 메커니즘 이해에 많

은 도움이 된 것으로 평가된다.

향후에는 보다 다양한 오펜시브 시큐리티 기법 실습을 위한 교보재를 제공할 계획이다. 우선적으로 DNS 캐시 오염, DNS 증폭 공격 등이 추가될 예정이다. 또한, 정규 교과 활용 결과를 조사할 계획이다.

[참고문헌]

[1] B. Wilson, "eaching security defense through web-based hacking at the undergraduate level," *Journal of Computing Science in Colleges*, 2017.

[2] M. Timchenko, D. Starobinski, "A Simple Laboratory Environment for Real-World Offensive Security Education," *Proc. of ACM SIGCSE*, 2015.

[3] W. Du, "The SEED Project: Providing Hands-on Lab Exercises for Computer Security Education," *IEEE Security and Privacy Magazine*, 2011.

[4] arpspoof. https://su2.info/doc/arpspoof.php

[5] 한국인터넷진흥원, 주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세가이드, 2017.12.

[6] Scapy. https://scapy.net