2019 한국정보보호학회 동계학술대회
CISC-W'19
Conference on Information Security and Cryptography-Winter 2019

기초 오펜시브 시큐리티 기법 실습을 위한 파이썬 기반 교보재 개발

이해영, 김태형, 임윤수, 박도규, 최승용
청주대학교 SW융합학부 디지털보안전공
whichmeans@gmail.com

청주대학교

서론

XenServer 같은 거? 누가 관리? 누가 계정 생성?

- 학부 정보보호 교육에서 오펜시브 시큐리티 실습 필요 ➔ 대상 체계 이해 및 교육 효과 향상
- 대부분의 학과는 **돈**도 없고, 관리 **인력**도 없음 ➔ VMware vSphere 기반 체계 도입은 어려움
- 매 학기 실습실 데스크톱에 가상환경 설치하는 **노가다**를 줄일 수 없을까? 실습에서 취약 환경 설정하는 **단순반복**을 줄일 수 없을까?
- **공짜** SW 기반의 실습 환경 구축
  - ABP : 실습 콘텐츠
  - opbp4p : 실습 환경 제어

서버는 구매해도 결국 **방치**되는 것이 현실

ABP

- Practice basic offensive security techniques *all-by-Pythonself*.
- 실습 콘텐츠
- 구성요소
  - Snippets : 실습용 코드 조각
  - Assignments : 과제용 참고 코드
  - Setups: 시스템을 취약하게 만듦
  - Checks: 공격 성공 여부를 확인
  - 향후 자동 공격 및 대응 확인 모듈도 추가(대응 실습)

파이썬을 포기하면 Metasploit 모듈(루비)로 작성하는 형태도 가능

청주대학교

ABP (계속)

- 콘텐츠
  - 패스워드 크래킹(/etc/passwd)
  - 사전 공격(Telnet)
  - ARP 스푸핑
  - ICMP 리다이렉트 공격
  - SYN 스캔
  - 스머프 공격
  - SYN 플러딩
  - TCP 리셋 공격
  - …

ABP (계속)

- Snippet 예제

실습 환경에 맞춰
학생이 수정해야 함

```
from scapy . all import *

p = Ether (dst = "08:00:27:95:1f:5a", src = "08:00:27:ad:c2:d3") / ARP
(op = 2, hwsrc = "08:00:27:ad:c2:d3", psrc = "10.0.2.1", hwdst =
"08:00:27:95:1f:5a", pdst = "10.0.2.4")

sendp (p)
```

실제 공격 수준이 될 수
있도록 학생이 수정해야 함

- Setup 예제(자동 실행)

```
import os

os . system ("sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=0")
```

opbp4p

- Cyber hands-on labs *of the Python people, by the Python people, for the Python people*
- 실습 환경 제어
- 구성요소
  - VM 제어(Oracle VM VirtualBox)
  - 실습 중앙 통제
  - 콘텐츠 탑재(Setups, Snippets)
  - 실습 결과 확인(Checks)

청주대학교

결론 및 향후과제

- Python과 Oracle VM VirtualBox 기반
- 가난한 학교 및 학과를 위한 실습 환경 및 콘텐츠 개발
- 깃 클론으로 간단히 설치되도록 개발
  - 설정은 교수자만 간단히
- 중앙 통제 가능한 opbp4p 개발
  - 교수자가 실습 콘텐츠를 선택하면 모든 학생 VM에 자동 탑재 ➔ 결과 확인 및 집계 역시 교수자가 중앙에서 수행