Week1. OT

강사. 유효곤

(ugonfor@gmail.com)

whoami

유효곤 (ugonfor)

Department of Cyber Defense,
Korea University

ugonfor@gmail.com

blog.ugonfor.kr

github.com/ugonfor

Education

- 고려대학교 사이버국방학과 19학번 (2019.03~)
- KAIST부설 한국과학영재학교 (2016.02~2019.02)

Works

- 차세대 보안리더 양성프로그램 Best of the Best 취약점 분석 트랙 9기 (2020.07~2021.03)
- 고려대학교 정보보호대학원 보안공학 연구실(김승주 교수님) 인턴(2020.05~2020.08)
- 고려대학교 정보보호대학원 인공지능 연구실(이상근 교수님) 인턴(2021.01~)
- 해킹동아리 CyKor 회원 (2019.09~, 2021년도 부회장)

AWARD (CTF)

- DEFCON 28 CTF Finalist
- 코드게이트 CTF 2020 대학부 6위
- WCTF 2020 Belluminar China 8위
- zer0pts CTF 2021 2위
- LINE CTF 2021 13위
- SSTF Hacker's Playground 5위
- ...

AWARD (AI Competition)

- CLOVA AI RUSH Round1 (Abuse Detection from time series) 2nd
- CLOVA AI RUSH Round2 (eXtreme Multi-label Classification) 4th

Interested in..

- 정보보호
  - 리버스 엔지니어링
  - 악성코드 분석 (Windows/ APK)
  - 네트워크 보안
- 인공지능
  - 인공지능 보안
  - 자연어 처리
  - 딥러닝

커리큘럼 1

1주차	IDA Pro Fundamental	IDA Pro의 사용법을 배우고, IDA Python을 통하여 바이너리 분석 자동화를 해본다.
2주차	Anti-Reversing Technique 1	SEH, ptrace, oLLVM, Hot patching 등 Anti-reversing 기법들을 배운다.
3주차	Anti-Reversing Technique 2	Virtual Machine을 구현하여 동작하는 바이너리를 분석해본다.
4주차	Hooking and Frida	Hooking에 대해서 배우고, Frida를 통해 상용 채팅 프로그램의 챗봇을 만들어본다.
5차시	Android Application	안드로이드 어플리케이션 대상 취약점 분석 및 악성코드 분석
6차시	Network Hacking	네트워크 해킹기법에 대해 배우고, 패킷 스니핑 툴을 직접 만들어 본다.
7차시	CTF	1~6차시동안 배운 내용을 토대로 CTF를 진행한다.

커리큘럼 2

1차시	Linux Basic, IDA Pro Fundamental	리눅스의 명령어들을 배우고, 배운 명령어를 활용해본다. IDA Pro의 사용법을 배우고, IDA Python을 통하여 바이너리 분석 자동화를 해본다.
2차시	Linux Fundamental	ls 명령어를 직접 구현해보며, 리눅스 파일 구조에 대해 깊이 이해한다.
3차시	Reversing Fundamental	PE 파일 구조에 대해 배우고, PE 헤더 파서를 직접 작성해본다.
4차시	Reversing Advanced	API 후킹과 키로거에 대해 배운다. 직접 계산기를 한글로 출력시켜본다.
5차시	Malware Analysis	실제 악성코드를 분석해본다.
6차시	Network Fundamental	네트워크 모델 및 TCP/IP Layer에 대해 배운다. 패킷 스니핑 툴을 직접 만들어본다.
7차시	Network Security	대표적인 네트워크 공격 중 하나인 ARP-spoofing에 대해 배우고 실습을 해본다.

Q&A

- 수업은 실습 위주로 진행할 것.
- Ubuntu나 Kali 가상머신 설치할 것. + WSL
- 과제 제출은 github.com의 git repository로 제출할 것.
- 수업자료는 https://github.com/ugonfor/Cyber-Guardians-Lecture-Note
- C랑 파이썬은 다 알고 있다고 가정하고 수업 할 것.