정보보안 전문가 과정

200106

박경덕

강사 소개 - 입상

대회	기간	성적	주최
HolyShield Hacking Contest	2013. 11	금상	카톨릭대학교
Hack in the Box	2016. 05	본선 진출	HITB
Hack in the Box	2017. 04	본선 진출	HITB
HUST Hacking Festival	2017. 05	1위	홍익대학교
Nuit du Hack	2017. 06	본선 5위	SYSDREAM
DEFCON CTF	2017. 07	본선 진출	DEFCON
사이버공격방어대회	2017. 11	1위	국정원&국보연
Codegate 국제해킹방어대회	2018. 04	대학부 3위	코드게이트
Ko-World 해킹방어대회	2018. 06	1위	한국폴리텍대학
DEFCON CTF	2018. 08	본선 진출	DEFCON
사이버공격방어대회	2018. 10	2위	국정원&국보연
PCTF	2019. 04	3위	PPP
DEFCON CTF	2019. 08	본선 진출	DEFCON
사이버공격방어대회	2019. 09	3위	국정원&국보연
SECCON CTF	2019. 10	본선 진출	SECCON

강사 소개 - 강의

	기관	주제
2017	국가보안기술연구소	시스템 취약점 분석 실무
	ETRI	리버스 엔지니어링
	국가보안기술연구소	시스템 취약점 분석 실무
2018	해양수산부	침해사고대응
	국토교통부	침해사고대응
	고용노동부	침해사고대응
	보건복지부	침해사고대응
	SK인포섹	시스템 취약점 분석 실무
	경찰청	리버스 엔지니어링
	한국전력공사	침해사고대응
	국방부	리버스 엔지니어링, 악성코드 분석
	KISA K-Shield	최신 해킹동향과 악성코드 탐지와 분석
	경찰청	침해사고대응
	국가보안기술연구소	리버스 엔지니어링
	금융보안원	침해사고대응 1차
	금융보안원	침해사고대응 2차

강사 소개 - 강의

	기관	주제
2019	한국수력원자력	침해사고대응
	공군	침해사고대응 및 취약점 분석
	KISA K-Shield	악성코드 탐지와 분석
	한림대학교	보안실무과정 특강
	한국전력	침해사고대응
	경찰청	침해사고대응
	건강보험심사평가원	침해사고대응
	KISA K-Shield	악성코드 탐지와 분석
	한림대학교	게임 핵과 보안 특강
	서부발전	2019 사이버공격방어대회 예선 분석
	한국전력	2019 사이버공격방어대회 예선 분석
	국방부	악성코드 분석
	금융보안원	악성코드 분석

강사 소개 – 지금 하는 일

- 해킹팀 SED 활동
  - 국내/외 해킹대회 참가
  - 모의해킹 프로젝트 수행

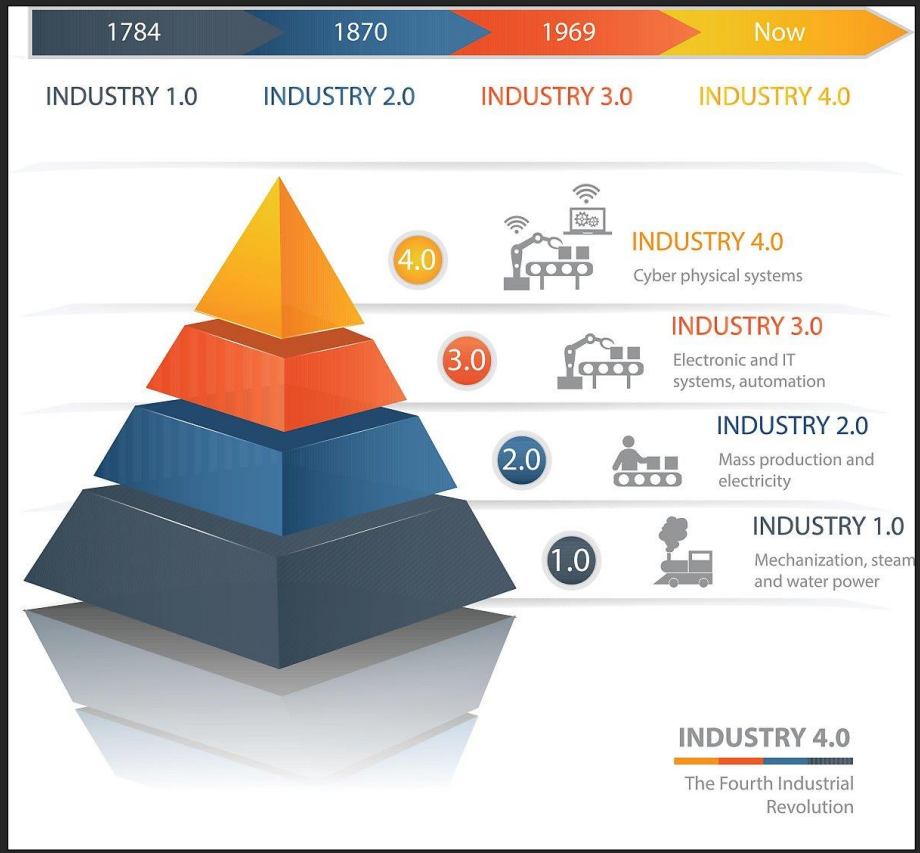
- 보안 교육 강의
  - 공공기관
  - 연구소
  - 공기업

- PUBG Anti-Cheat팀 엔지니어
  - 배틀그라운드 자체 방어 솔루션 개발
  - 게임 핵 탐지 및 차단 기술 연구개발

PUBG
SEOUL
KRAFTON GAME UNION

개요

- 보안 실무
  - 4차 산업혁명 시대를 맞아 보안과 해킹에 대한 관심/위협 증가
    - 빅데이터
    - 인공지능
    - 사물인터넷(IoT)
    - 보안이 필요 없는 분야?
  - 보안에 대한 정확한 지식과 실무적 능력 필요
    - 학교에서 배우는 보안 vs 현장에서 필요한 보안



1차 ~ 4차 산업혁명 (출처: 게티이미지 코리아)

개요

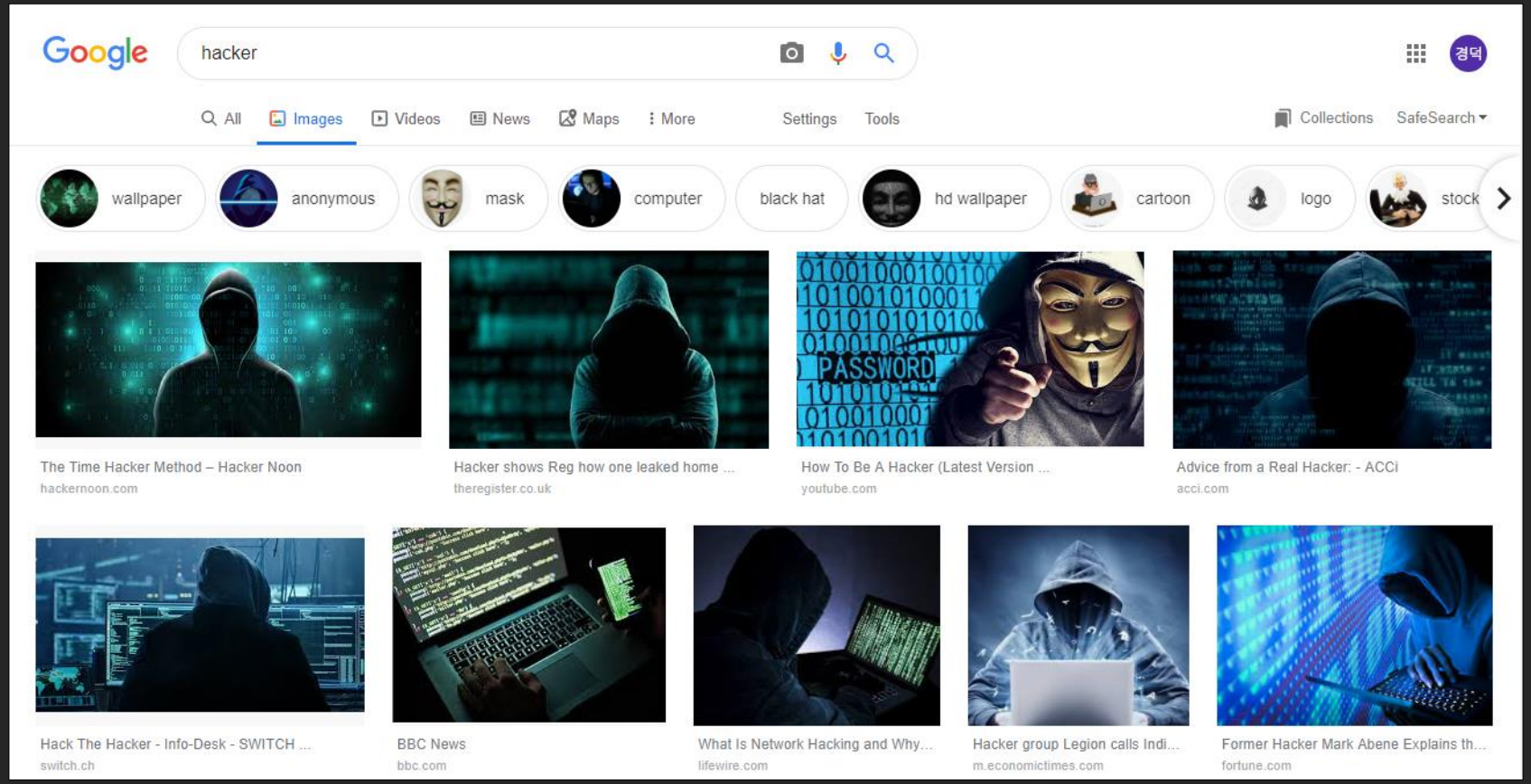
- 학습 내용
  - Yara, Snort 개념 및 사용법 실습
  - 여러 해킹 시도에 대한 탐지 및 분석 실습
  - 팀 프로젝트 수행을 통한 보안 실무 간접 경험

개요

- 강의계획
  - 1주차: 오리엔테이션: Yara, Snort 세팅 및 기본 사용법
  - 2주차: 악성코드 탐지 및 분석 실습
  - 3주차: 익스플로잇 탐지 및 분석 실습
  - 4주차: 웹 해킹 탐지 및 분석 실습
  - 5주차: 팀 프로젝트 진행 및 발표
- 강의 진행 방식
  - 2명의 강사가 진행
    - 박경덕 – 오늘, 3주차, 마지막 날
    - 정찬혁 – 그 외
  - 강의 중간중간 질문 대환영

해커와 해킹

- 해커
  - 떠오르는 이미지?



해커와 해킹

- 해커
  - 보안 전문가
  - 끊임없이 공부와 연구를 해야 함
  - 컴퓨터의 모든 분야에 대해 알아야 함
  - 나쁜 사람일까?

해커와 해킹

- 해킹
  - 불법? 합법?
    - 화이트: 합법
    - 블랙: 불법
    - 그 중간은?
  - (불법적으로) 무엇을 하는가?
    - 사이버 공격(?)
  - (합법적으로) 무엇을 하는가?
    - Offensive
    - Defensive
  - 어떻게?
    - …

사이버 공격(?) 개요

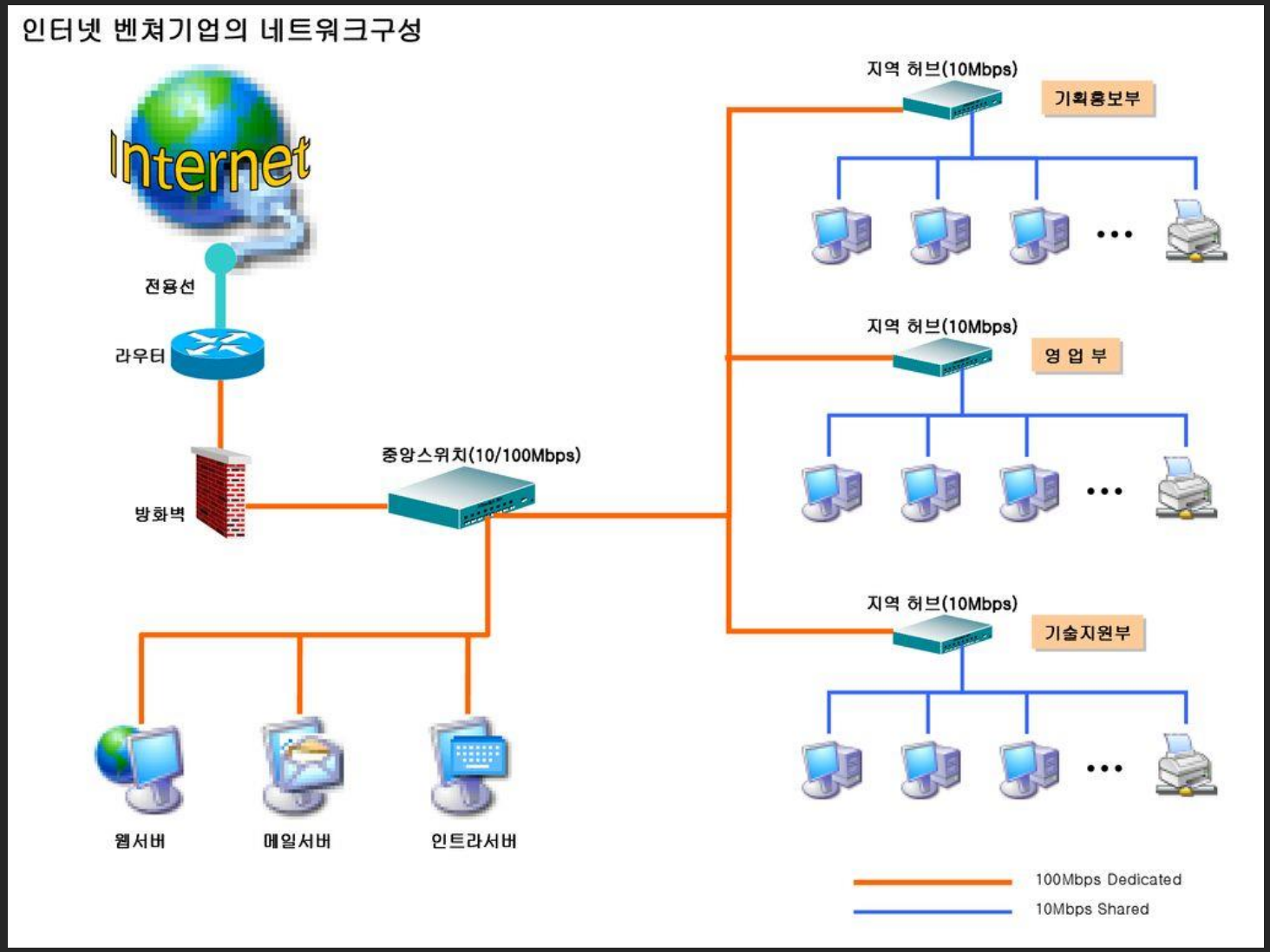
- 주 타겟: 기업 vs 개인
- 준비 유형: 즉흥적 vs 계획적
- 공격 방법
  - 웹 해킹
  - 사회공학적 해킹
  - 취약점 (제로데이?)
  - ...
- 공격 피해
  - 개인 정보 유출
  - 기업 기밀 유출
  - 시스템 파괴
  - 좀비화

보안 실무

- Offensive
  - 모의 해킹
  - 취약점 연구개발
- Defensive
  - 네트워크 보안
    - 보안 관제
    - 비정상 트래픽 탐지 및 차단
  - 취약점 분석
    - 악성코드 분석
  - 보안 개발
    - 보안 솔루션 개발
    - 제품 취약점 방지
  - 사후 대처
    - 로그 분석
    - 침해사고대응
  - 행정 관련
    - 보안 정책 수립
- 실제 현업에서는 Defensive 업무가 절대다수

보안 실무 – 네트워크 보안

- 조직의 네트워크에 대한 보안
- 대부분 기업 보안팀의 업무
- 기술적 보안
  - 망 분리
  - 보안 장비 구성
- 정책적 보안
  - 권한 분리
  - 보안 정책 수립
- 여러 솔루션 및 장비를 활용
  - Firewall
  - IDS
  - IPS
  - Yara
  - Snort
  - 등등

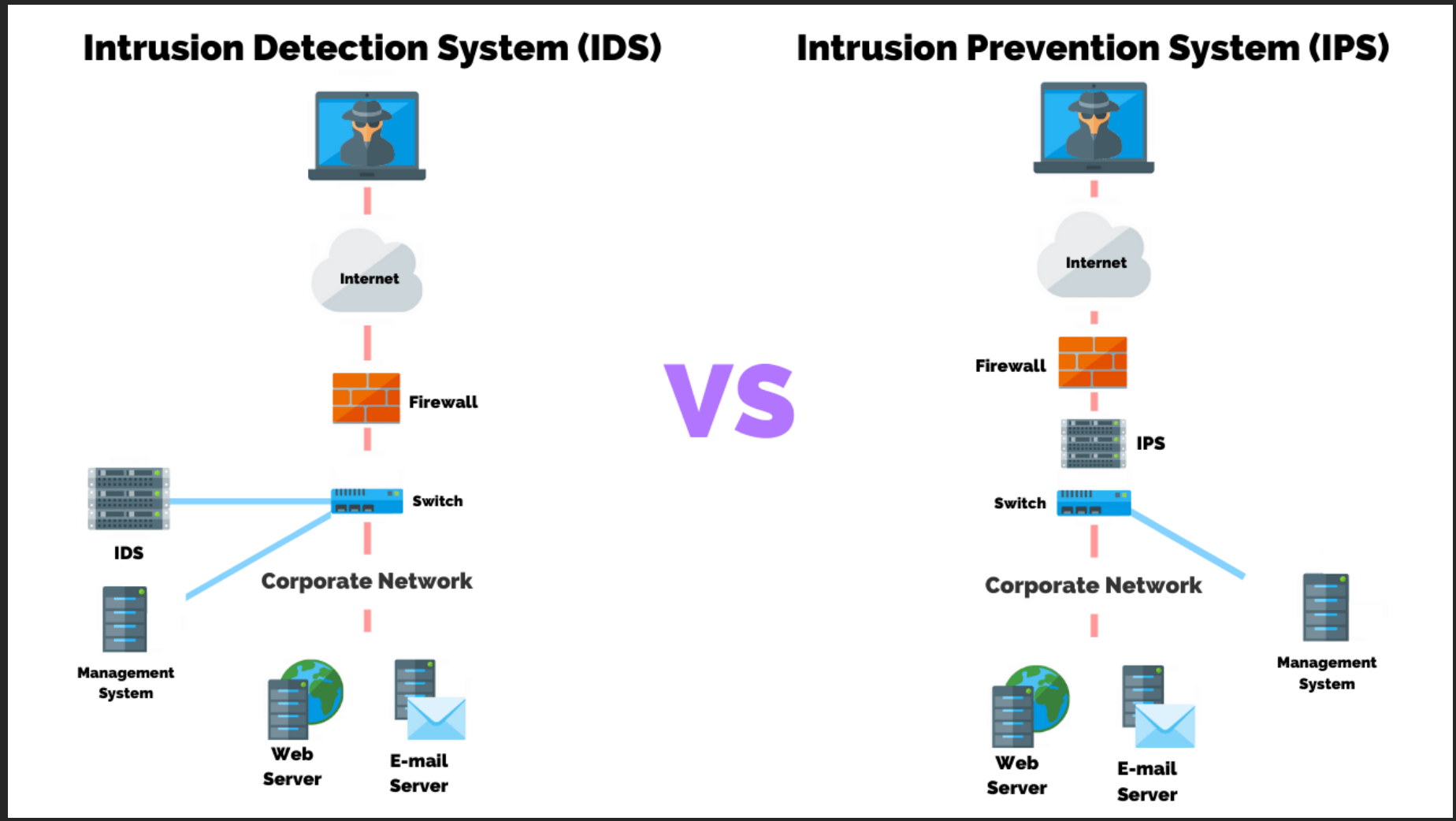


보안 실무 – 네트워크 보안

- Firewall
  - 가장 앞 단에 두는 보안 장비
  - IP 주소, 포트, 프로토콜만을 이용하여 트래픽 필터링
  - Ex) http, https 포트 외의 접근은 모두 차단
- Intrusion Detection System (IDS)
  - 네트워크를 감시하여 위협이 의심되는 트래픽에 대해 보고
  - Signature 비교 탐지
  - Anomaly 탐지
- Intrusion Prevention System (IPS)
  - 네트워크를 감시하여 위협이 의심되는 트래픽 차단
  - Rule 기반 차단
    - Firewall과는 다른 개념의 차단
  - Ex) DDoS 차단 시스템
- IDS/IPS는 일반적으로 물리적 장비

보안 실무 – 네트워크 보안

- IDS와 IPS 비교



보안 실무 – Snort

- 오픈소스 IDS/IPS 소프트웨어
- 네트워크의 패킷을 감시
- 자체 규칙을 이용하여 특정 패킷 로깅 및 차단
  - <Action> <Protocol> <Source> <Direction> <Destination> <Rule>
  - Ex) alert tcp 192.168.10.1 any -> 192.168.10.2 80 (msg: "web access")
  - Ex) log tcp any any -> 192.168.10.0/24 any (msg: "every access")
- Windows에서의 Snort 세팅
  - https://koromoon.blogspot.com/2018/06/windows-ids-snort-base-apm_74.html

보안 실무 – 취약점 분석

- 취약점 공격에 사용된 악성코드 분석
- 여러 툴 활용
  - 백신
  - 샌드박스
  - YARA

보안 실무 – 취약점 분석

- 백신
  - 악성코드를 탐지할 수 있는 소프트웨어의 총칭
  - 전 세계적으로 수 많은 브랜드 존재 (~~V3~~)
- 샌드박스
  - 악성코드를 실행시킬 수 있는 독립된 환경
  - 일종의 VM
  - 악성코드를 실행시킨 후 자동으로 리포트 작성
  - Ex) Cuckoo Sandbox
- YARA
  - 미리 작성한 규칙을 이용하여 빠르게 악성코드를 탐지할 수 있는 프로그램
  - 파일 내부의 문자열을 매칭시켜 탐지

보안 실무 – YARA

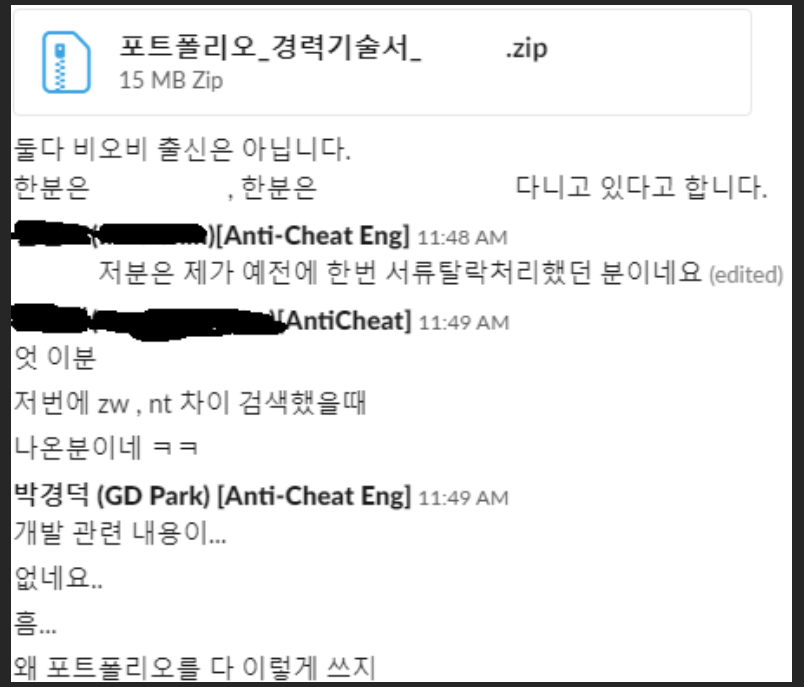
- VirusTotal에서 개발한 오픈소스 악성코드 탐지 및 분류도구
- https://github.com/VirusTotal/yara
- String 매칭 기반 탐지
- 자체적으로 정의한 문법에 맞게 규칙을 정의하여 사용
  - 특정 문자열(바이너리 포함)이 매칭되는 경우 탐지
  - Ex) 파일에 "DEL a.bat" 이란 문자열이 포함되어 있는 경우 탐지
  - Ex) 파일의 특정 오프셋에 "E8 00 00 00 00" 이란 5바이트가 있는 경우 탐지
  - 정규식을 이용하여 더욱 세밀한 규칙 정의 가능

보안 실무 – 업계 현실

- 대부분 기업의 주요 업무가 아님
  - 솔직히 인정받기가 쉽지 않음
- 기업의 주 서비스보다 우선수위가 낮음
  - 보안이 서비스를 방해할 수 없음
  - 훌륭한 보안보다 안정적인 서비스가 우선
    - Ex) 게임 핵을 99% 막을 수 있지만 5% 크래시가 발생한다면?
- 100%의 방어가 요구됨
  - Defensive: 99번 막았는데 1번 뚫린다면?
  - Offensive: 99번 막혔는데 1번 뚫는다면?
- 그럼에도 결코 빠질 수도 없고 빠져서도 안 되는 분야

보안 실무 – 무엇을 준비하면 좋을까

- 개발, 개발, 개발
  - 개발을 할 줄 모르는 해커는 없다
  - 어떤 분야를 가던 개발 능력은 필수
  - C/C++, Golang, Rust 등 시스템 프로그래밍 언어 최소한 하나는 반드시 익힐 것
  - Python 등의 스크립트 언어는 부가적으로 알고 있으면 좋음
  - Coder(X) → Architect(O)
  - 설마 Github 계정이 없는 사람이?
- 내 적성
  - Offensive or Defensive
  - 취약점을 찾는 업무 vs 취약점을 분석하는 업무
  - 해당 분야에서 필요한 기술 공부 (최신 기술까지 전부)
    - 악성코드 분석 → 리버싱
    - 모의해킹 → 웹 해킹
    - 침해사고대응 → 포렌식



보안 실무 – 팀 프로젝트 (초안)

- YARA를 이용한 악성코드 리그전
- 3인 1팀으로 진행
- 프로젝트 진행 방식
  1. 각 팀에 샘플 전달 (악성, 정상)
  2. 전달받은 샘플을 각자 분석하여 이를 탐지할 수 있는 YARA 룰 작성
  3. 전달받은 샘플은 수정 가능
  4. 최종적으로 작성된 YARA 룰과 수정한 샘플을 취합
  5. 취합한 샘플과 YARA 룰을 이용하여 탐지 성능 테스트
  6. 테스트 결과 평가
- 평가 기준
  - 수정한 악성 샘플이 얼마나 탐지되지 않는가 – 공격력
  - 작성한 YARA 룰의 탐지 성능 – 방어력
  - 탐지 성능
    - 정탐: 악성 샘플을 탐지 AND 정상 샘플은 미탐지
    - 오탐: 정상 샘플을 탐지
    - 미탐: 악성 샘플을 미탐지
    - 정확도: 정탐 / 전체

QnA