

보안관제센터 기초

LogOn 김승수, 김태우, 박준호, 이가은
가천대학교 정보보안동아리 Pay1oad



CONTENTS

- 01 프로젝트 소개
- 02 학습 자료
- 03 참고 자료



01

프로젝트 소개



○ 01. 프로젝트 소개 - 개요

본 자료는 2025-2 Pay1oad LogOn팀 프로젝트의 일환으로 제작된 결과물입니다.

1주차부터 7주차까지의 스터디 내용을 기반으로 하며, 각 주차별 핵심 개념 정리와 직접 따라해볼 수 있는 실습 문제를 포함하고 있습니다.

본 자료는 여러 주제를 폭넓게 다루며 전체적인 SOC의 흐름을 빠르게 파악하는 데 중점을 두고 있습니다.

따라서 세부적인 기술이나 개념의 깊은 설명보다는 개요와 실습 위주로 구성되어 있으며, 보다 전문적인 내용은 참고 자료를 통해 보완해주시기 바랍니다.

제작 목표는 다음과 같습니다 :

- 보안 관제의 핵심 개념 정리
- 실제 업무에 사용되는 툴 실습을 통한 실무 능력 향상
- 스터디 및 교육에 사용할 수 있는 자료와 커리큘럼 제공

○ 01. 프로젝트 소개 - 저자

1. 김승수

- 커리큘럼 제작
- 1, 4, 6, 7주차 학습/실습 자료 제작
- 이메일: 0101087ssk@gmail.com
- 깃헙: <https://github.com/DeceptiveRat>

2. 김태우

- 5주차 학습/실습 자료 제작
- 이메일: kr27890@gachon.ac.kr
- 깃헙: <https://github.com/DuJoGaks>

3. 박준호

- 3주차 학습/실습 자료 제작
- 이메일: junpumpk1@gachon.ac.kr
- 깃헙: <https://github.com/ParkJunho01>

4. 이가은

- 2주차 학습/실습 자료 제작
- 이메일: Igeun0905@gachon.ac.kr
- 깃헙: <https://github.com/alslmini>

02

학습 자료



○ 02. 학습 자료 - (1주차 학습) 보안 관제 센터 (1)

1. 보안 관제 센터(Security Operating Center, SOC)란?

이상 현상(Anomaly)과 위협 탐지를 위해 IT 인프라를 관제하는 팀을 가리킨다. 주요 업무는 위협 감지 및 대응, 그리고 방지 등이 있다. 맡은 역할에 따라 티어1 분석가, 티어2 분석가, 티어3 분석가, 그리고 매니저로 나뉜다.

티어 1 분석가는 관제를 하며 거짓 양성(false positive)과 실제 양성(true positive)을 구별해서 필요시 티어 2 분석가에게 알리는 역할을 한다.

티어 2 분석가는 로그 분석과 디지털 포렌식을 통해 공격의 범위(scope)와 영향 받은 시스템을 파악한 후 확산 방지(containment), 무력화(neutralize), 그리고 복원(remediation)을 한다.

티어 3 분석가는 가장 높은 수준의 경험과 지식이 요구되며 선제적(proactive) 위협 사냥(threat hunting)등의 업무를 맡는다.

SOC 매니저는 분석가들을 관리하고 총괄하는 역할을 한다.

○ 02. 학습 자료 - (1주차 학습) 보안 관제 센터 (2)

2. 보안 관제 센터에서 사용하는 툴

- **Security Information and Event Management (SIEM)**: 로그를 종합해서 보기 쉽게 시각화하는데 사용된다.
- **Intrusion Detection and Prevention System (IDS/IPS)**: 침입(intrusion)을 탐지 및 차단하는 툴이다. 침입이 감지될 시 알림(alert)를 생성하고 침입을 차단한다.
- **Endpoint Detection and Response (EDR)**: 실시간으로 노트북, 서버, IoT 등 단말기(endpoint)를 관제한다. 사건 발생 시 조사(incident investigation)에도 사용된다.
- **방화벽 (firewall)**
- **포렌식 툴**: 공격이 발생했을 때 사건 경위를 조사하기 위해 사용된다. 메모리, 레지스트리, 네트워크 등 여러 종류가 있다.
- **악성코드 분석(malware analysis) 툴**: 사건 조사 중 발견된 악성코드를 분석하는데 사용된다.

1. MITRE ATT&CK 프레임워크란 ?

사이버 보안 위협 모델링을 위한 지식 베이스(knowledge base)이다. 사이버 공격의 단계에 따라 전술(tactics), 기법(technique), 절차(procedure)를 분류(catalog)하는데 사용한다.

전술은 공격자가 달성하고자 하는 목표이다. 정찰(reconnaissance), 초기 액세스(initial access), 실행(execution), 지속성(persistence), 권한 상승(privilege escalation), 탐지 회피(defense evasion) 등이 여기 포함된다.

기법은 목표를 달성하기 위해 사용하는 방법이다. 예를 들면 초기 액세스 전술을 위한 피싱 기법, 탐지 회피 전술의 파일리스 악성코드(fileless malware) 등이 있다.

절차는 기법의 자세한 구현(implementation)이다. 예를 들어 기법에서 사용된 파워쉘 스크립트나 커맨드 등이 절차에 포함된다.

2. MITRE ATT&CK 프레임워크의 필요성

MITRE ATT&CK 프레임워크는 발생한 공격을 문서화할 때 사용할 수 있는 표준화 된 언어를 제공한다. 이를 통해 서로 다른 조직이나 보안 제품(solution)이 소통할 수 있도록 해주며 보고하는 과정에서 일관성을 유지할 수 있게 해준다. 이외에도 ATT&CK 매트릭스를 통해 어느 기법에 취약한지 찾을 수 있게 해주는 등의 역할도 한다.

3. MITRE ATT&CK 매트릭스

- **기업 매트릭스 (Enterprise Matrix):** 기업 인프라 공격에 사용되는 기법들이 포함돼있다. 네트워크 인프라, Windows, Linux 플랫폼 등에 대한 하위 매트릭스를 포함한다.
- **모바일 매트릭스 (Mobile Matrix):** 모바일 디바이스에 대한 공격과 네트워크 기반 모바일 공격에 대한 기법들이 포함돼있다. iOS와 Android 플랫폼 하위 매트릭스가 여기 속한다.
- **ICS 매트릭스:** 산업 제어 시스템 공격에 사용되는 기법들이 포함돼있다.

○ 02. 학습 자료 - (1주차 학습) 피싱 이메일 (1)



1. 피싱 기법

피싱 기법에는 크게 3가지가 있다: 사칭(impersonation), URL 조작(URL manipulation), 악성 첨부파일.

사칭은 말 그대로 자신이 아닌 사람인척하는 것이며 스퓌핑(spoofing)을 통해 신뢰성을 높일 수도 있다.

URL 조작에는 bitly등의 사이트를 통해 URL 줄이기(shortening), 서브도메인을 통해 다른 도메인을 사칭하는 서브도메인 스퓌핑(1), 비슷하게 생긴 문자로 다른 도메인을 사칭하는 호모그래프(homograph) 공격(2), 오타 스쿼팅(typo squatting)(3) 등 여러 방식이 있다.

(1)서브도메인 스퓌핑

원본
amazon.com
google.com

서브도메인
amazon.malicious.com
google.com.malicious.com

(2)호모그래프 공격

원본
amazon.com

호모그래프
amazOn.com
amazon.com
àmazon.com

(3)오타 squatting

원본
amazon.com
google.com

오타
amazon.co
gogle.com

○ 02. 학습 자료 - (1주차 학습) 피싱 이메일 (2)

2. 이메일 분석 - 헤더

쉽게 gmail 등 메일 프로그램에서 헤더를 분석할 수도 있지만 볼 수 있는 정보가 제한돼있기 때문에 [분석 사이트](#)를 사용하는 것을 추천한다. 중요한 헤더는 다음과 같다:

- **date**: 이메일간 상관관계 파악 (**correlate**)하는데 사용된다.
- **from**: 보낸 사람을 파악할 수 있다. 그러나 스퓌핑이 가능하기 때문에 완전히 신뢰할 수는 없다.
- **subject**: 비슷한 이메일을 찾는데 사용한다.
- **message-id**: ID가 만들어진 도메인의 이름을 포함한다.
- **received**: 지나간 MTA 하나 당 하나씩 추가된다. 스퓌핑할 수 있으니 밀을 수 있는 도메인의 메일 서버에 도착하기 전에는 완전히 신뢰할 수 없다.

from: [REDACTED]
to: 0101087ssk@gmail.com
date: Nov 17, 2025, 7:20 AM
subject: [REDACTED]
mailed-by: [REDACTED]
signed-by: [REDACTED]
security: Standard encryption (TLS) [Learn more](#)

Gmail에서 본 헤더

#	Header	Value
1	Delivered-To	0101087ssk@gmail.com
2	X-Google-Smtp-Source	AGHT+IfyIdM86DnP
3	X-Received	by 2002:ad2:4eac:0:t
4	ARC-Seal	i=1; a=rsa-sha256; t=1638400000; YyAgOnXg9gDEATJN8
5	ARC-Message-Signature	i=1; a=rsa-sha256; c=BFMt2cBfIHyEd+d-X
6	ARC-Authentication-Results	i=1; mx.google.com: d=NONE; h=NTINE dts=NONE; he
7	Return-Path	<bounce+746a7e.074@bounces.gserviceaccount.com>
8	Received-SPF	pass (google.com: do
10	DKIM-Signature	a=rsa-sha256; v=1; i=3ApPi2PmEtL6Yv
11	DKIM-Signature	a=rsa-sha256; v=1; dtkIOcfH+4PLiEg
12	List-Unsubscribe-Post	List-Unsubscribe=O
13	List-Unsubscribe	[REDACTED]
14	X-Feedback-Id	[REDACTED]
15	Sender	[REDACTED]
16	Mime-Version	1.0
17	Feedback-Id	unifiedDigestEmail:[REDACTED]
18	Content-Type	text/html; charset="n

헤더 분석 사이트에서 본 헤더

○ 02. 학습 자료 - (1주차 학습) 피싱 이메일 (3)

3. 이메일 분석 - SPF, DKIM, DMARC

Sender Policy Framework (SPF)는 도메인 관리자들이 어느 메일 서버가 그 도메인을 대신해서 메일을 보낼 수 있는지 명시할 수 있게 해준다. 각 도메인의 SPF 기록은 nslookup이나 dig 등의 커맨드로 확인할 수 있다.

```
$ nslookup -type=txt naver.com | grep -i spf
naver.com      text = "v=spf1 ip4:111.91.135.0/27 ip4:125.209.208.0/20
ip4:125.209.224.0/19 ip4:210.89.163.112 ip4:210.89.173.104/29 ip4:114.11
1.35.0/24 ip4:61.247.196.0/24 ip4:61.247.197.0/24 ~all"
```

Domain Keys Identified Mail (DKIM)은 암호화를 통해 인증(authentication)과 무결성(integrity)를 확인할 수 있도록 해준다.

Domain-based Message Authentication, Reporting, and Conformance (DMARC)는 이메일을 보내는 도메인 관리자들이 이메일이 SPF나 DKIM 체크에 실패했을 때 어떻게 행동할지 명시할 수 있게 해준다.

6	ARC- Authentication- Results	i=1; mx.google.com; dkim=pass header.i=@[REDACTED] header.s=pic header.b=ScaBkvIw; dkim=pass header.i=[REDACTED] header.s=mg header.b=mLtwEcj4; spf=pass (google.com: domain of [REDACTED] designates 1 [REDACTED].29 as permitted sender) smtp.mailfrom=[REDACTED]; dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=[REDACTED]
---	------------------------------------	--

이메일 헤더에 자동으로 인증결과들이 나온다

○ 02. 학습 자료 - (1주차 학습) 피싱 이메일 (4)



4. URL 분석

`https://docs.google.com/presentation/d/`

- **https:** 프로토콜
- **docs:** 서브 도메인
- **google:** 도메인
- **com:** 최상위 도메인 (Top Level Domain, TLD)
- **presentation/d/:** 경로

URL을 분석할 때 도메인 + TLD는 스퓌핑할 수 있으니 반드시 유의해서 봐야한다.

○ 02. 학습 자료 - (1주차 실습) 피싱 이메일 분석 (1)

링크에서 sample-1.eml, sample-2.eml, sample-5.eml, sample-7.eml, sample-8.eml 분석

도움말 :

- 위험한 파일과 URL을 다룰 때는 반드시 가상머신을 사용해야 한다
- 수상한 URL을 기재할 때 실수로 링크로 들어가지 않도록 defang을 해야 한다 (링크)



- IP 주소 블랙리스트 확인 사이트 : [whatismyip](http://whatismyip.org)
- URL unshorten 사이트 : [unshorten](http://unshorten.it)
- URL/첨부파일 분석 사이트 : [바이러스 토탈](http://virustotal.com), [urlscan](http://urlscan.io)

○ 02. 학습 자료 - (1주차 실습) 피싱 이메일 분석 (2)



이메일 분석 체크리스트 :

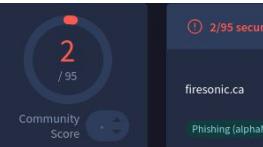
- from, return, received 헤더 확인: 수상한 도메인이 있거나 from 헤더와 received 헤더의 도메인이 일치하는가?
- authentication 헤더 확인: 인증이 성공했는가?
- 전송한 IP 주소 조사: whois, dig 커맨드 및 블랙리스트 사이트 확인
- 내용 확인: 문법, 스펠링 에러 혹은 오타가 있는가? 내용에 있는 도메인이 from 헤더의 도메인과 일치하는가? 수상한 링크나 파일은 없는가?

○ 02. 학습 자료 - (1주차 실습) 피싱 이메일 분석 예시

사용 샘플: sample-9.eml

1. From 헤더의 도메인이 coinbase가 아님 `From` Coinbase <noreply@firesonic.ca>

사용된 도메인 바이러스 토탈 (VT)에서 확인



2. To 헤더를 보면 동시에 여러 명한테 보냄

3. 수상한 링크 사용 - coinbase 도메인이 아님

`hxps[://]www[.]bing[.]com/ck/a?!&&p=8cc5352d816ad678JmltdHM9MTY5NDA0NDgwMCZpZ3VpZD0xNTM1ZDczZS1IMDk0LTy2N2ltMmU0YS1jNDIzZTFjMjY3OGQmaW5zaWQ9NTE3Nw&ptn=3&hsh=3&fclid=1535d73e-e094-667b-2e4a-c423e1c2678d&psq=firesonic[.]ca&u=a1aHR0cHM6Ly9maXJlc29uaWMuY2Ev&ntb=1`

○ 02. 학습 자료 - (2주차 학습) 네트워크 프로토콜 기초



1. 네트워크 프로토콜이란 ?

: 서로 다른 장치(컴퓨터, 스마트폰, 서버 등)들이 네트워크를 통해 데이터를 교환할 때 사용되는 공식적인 규칙, 약속, 또는 표준 => 네트워크 통신을 위한 약속과 규칙

2. 필요성

- 호환성 보장

데이터를 주고 받는 형식과 절차에 대해 미리 합의된 규칙이 필요하며 프로토콜은 이러한 이기종 장치 간의 호환성을 보장해 줌 ex) 삼성 스마트폰과 맥 노트북 간의 데이터를 주고받음

- 질서 있는 통신

데이터가 언제 출발하고, 도착하며, 만약 오류가 발생했을 경우 어떻게 처리해야 하는지에 대한 모든 절차를 프로토콜을 통해 정의 -> 인터넷 통신이 혼란 없이 질서 정연하게 이루어지도록 함

3. 주요 역할

- 데이터 형식: 데이터는 어떤 모양으로 포장되어야 하는가? (데이터 구조)
- 주소 지정: 데이터를 누가, 어디로 보내야 하는가? (IP 주소, MAC 주소)
- 흐름 제어: 데이터를 얼마나 빨리 보낼 것인가? (수신자가 감당할 수 있도록 속도 조절)
- 오류 제어: 데이터가 잘못되거나 유실되면 어떻게 재전송 요청을 할 것인가?

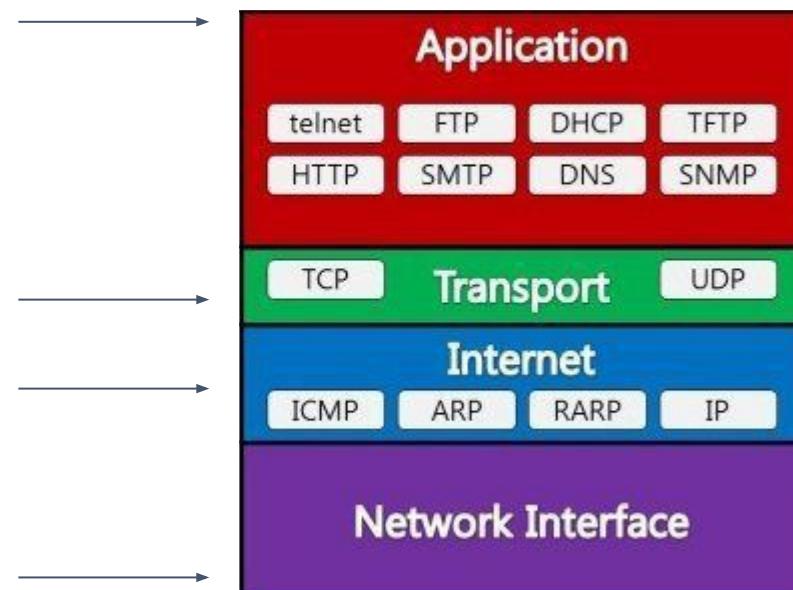
○ 02. 학습 자료 - (2주차 학습) 네트워크 프로토콜 기초

네트워크 계층 구조

우리가 다루는 프로토콜들이 어떤 위치에서 작동하는가 ? TCP/IP 4계층 모델

계층? 그게 뭔가요? 네트워크 7계층

L7	응용 계층
L6	표현 계층
L5	세션 계층
L4	전송 계층
L3	네트워크 계층
L2	데이터 링크 계층
L1	물리 계층



HTTP, HTTPS : 응용계층
사용자에게 서비스를 제공
(웹 브라우징, 이메일 등)

TCP, UDP : 전송 계층
데이터 전송 방식을 결정함
(신뢰성 VS 속도)

Ethernet, Wi-Fi : 네트워크
접근 계층
물리적 데이터 전송

전송계층 프로토콜

: 데이터를 '어떻게' 보낼지 결정하는 계층으로 속도를 중요시할지, 아니면 데이터의 정확성을 중요시할지에 따라 TCP와 UDP를 선택함

TCP (Transmission Control Protocol)

: 신뢰성을 최우선으로 하는 프로토콜 (보낸 사람이 받는 사람에게 확실히 받았는지 확인)

- 연결 지향: 통신을 시작하기 전에 반드시 연결을 설정 (3-way Handshake)
- 신뢰성 보장: 데이터를 전송했는지 확인(AKC)하고, 유실 시 재전송함
- 흐름 제어: 수신자가 처리할 수 있는 속도로 데이터를 보냄
- 순서 보장: 데이터 패킷에 번호를 붙여 순서대로 조립

3-way HandShake (연결 설정 과정)

1. SYN (Synchronize): 클라이언트가 서버에게 "나 연결하고 싶어" 요청.
2. SYN-ACK (Synchronize-Acknowledge): 서버가 클라이언트에게 "응, 알았어. 너도 준비됐니?" 회신.
3. ACK (Acknowledge): 클라이언트가 서버에게 "응, 준비됐어. 이제 통신 시작하자" 최종 확인.

UDP (User Datagram Protocol)

: 속도를 최우선으로 하는 프로토콜 (데이터가 유실되어도 신경 쓰지 않음)

- 비연결형: 연결 설정 과정이 없음, 데이터를 바로 전송
- 신뢰성 보장 X: 데이터 유실이나 순서 변경이 발생
- 오버헤드 최소: 헤더 정보가 매우 간단하여 속도는 빠름

TCP VS UDP 비교
->

구분	TCP	UDP
신뢰성	높음 (재전송, 순서 보장)	낮음
속도	느림 (Handshake)	빠름
연결 방식	연결 지향	비 연결형
오버 헤드	높음 (헤더 정보 많음)	IP datagram 그대로 전송
응용 서비스	HTTP, FTP, SMTP, SSH	DNS, DHCP, TFTP
사용 예시	웹, 파일 전송, 이메일 등	실시간 스트리밍, 온라인 게임

응용계층 프로토콜

: 사용자의 요청과 서버의 응답을 처리하는데 사용되는 웹 통신의 기본 규칙

HTTP (HyperText Transfer Protocol)

: WWW에서 정보를 주고받는 가장 기본적인 프로토콜

- **기능**

클라이언트(웹 브라우저)가 서버에게 데이터를 요청하고, 서버가 그에 대한 응답(HTML, 이미지 등)을 보낼 때 사용

- **문제점**

HTTP 통신은 암호화되지 않은 평문으로 이루어져 중간에 누군가 데이터를 가로채면 내용이 그대로 노출됨

-> 보안 위협에 취약

HTTPS (HyperText Transfer Protocol Secure)

: HTTP에 보안 계층 (Secure Socket Layer, SSL 또는 Transfer Layer Security, TLS)을 추가한 프로토콜

- 보안

SSL/TLS를 사용하여 클라이언트와 서버 사이의 모든 통신 내용을 암호함

- 인증

서버가 신뢰할 수 있는 기관(CA)으로부터 발급받은 인증서를 통해 자신이 진짜 서버임을 증명함

- 작동 방식

TCP 포트 443번을 주로 사용하며, 통신을 시작하기 전에 TLS Handshake를 통해 암호화 키를 교환

! 웹 브라우저 주소창에 자물쇠 모양이 있다면 HTTPS가 적용되었다는 뜻



정리 비교표

구분	TCP	UDP	HTTP	HTTPS
연결 방식	연결 지향	비연결	TCP 기반	TCP + SSL/TLS
신뢰성	높음	낮음	요청/응답	요청/응답 + 암호화
속도	상대적으로 느림	빠름	중간	중간 (암호화 오버헤드)
사용 예시	웹, 이메일	게임, 스트리밍	웹 페이지	보안 웹 페이지

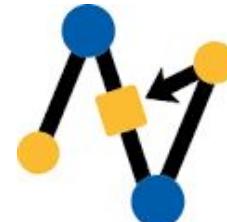
패킷 분석기

: 네트워크 인터페이스 카드 (NIC)를 통해 송수신되는 모든 데이터를 패킷 형태로 캡처하고, 그 내용을 상세하게 분석하여 보여주는 도구

- 프로토콜 학습: TCP 3-Way HandShake가 실제로 어떻게 일어나는지, HTTP 요청이 어떤 구조를 갖는지 확인할 수 있음
- 문제 해결: 네트워크 지연, 연결 오류, 설정 오류 등의 원인을 찾아냄
- 보안 분석: 악의적인 트래픽이나 비정상적인 통신을 감지



TCPDUMP



NetMiner

○ 02. 학습 자료 - (2주차 학습) 패킷 분석 방법 학습



Wireshark

: 가장 널리 사용되는 도구로 GUI를 제공하여 사용자가 시각적으로 네트워크 패킷을 파악하기 쉬운 도구

특징

- 시각화: 캡처된 패킷을 색으로 구분하고 계층별로 구조화하여 표시
- 심층 분석: 패킷 내부의 모든 계층 정보 (MAC, IP, TCP/UDP, 응용 계층)를 상세하게 표시
- 강력한 필터링: `ip.addr == 192.168.28.128`, `http.request`와 같은 복잡한 필터를 사용하여 원하는 패킷만 걸러냄
- 스트림 재구성: TCP 통신처럼 여러 패킷에 걸쳐 전송된 데이터를 합쳐서 사용자 눈에 보이도록 재구성

학습 포인트

- 패킷 목록 창: 캡처된 모든 패킷의 요약 정보 (시간, 소스, 목적지, 프로토콜)가 나열
- 패킷 상세 정보 창: 선택된 패킷의 모든 프로토콜 계층 정보가 트리 구조로 표시
- 16진수 데이터 창: 실제 패킷 데이터가 16진수나 ASCII 코드로 표시됨

TCPdump

: 리눅스나 유닉스 기반 시스템에서 작동하는 CLI 기반 패킷 분석 도구

특징

- 경량성: 시스템 자원을 매우 적게 사용
- 원격 사용: SSH로 접속한 서버에서도 즉시 실행하여 실시간 트래픽 확인 가능
- 스크립팅 용이: 웹 스크립트에 포함하여 자동화된 캡처 및 모니터링 작업을 수행하기 좋음
- Bpf 필터링: 캡처 시작 단계에서부터 특정 트래픽만 걸러낼 수 있는 필터링 문법을 사용

사용 예시

```
# 80번 포트로 오가는 트래픽만 캡처하여 화면에 출력
$ sudo tcpdump -i eth0 port 80
```

```
# 특정 IP 주소(192.168.1.100)로 가는 트래픽 캡처
$ sudo tcpdump host 192.168.1.100
```

○ 02. 학습 자료 - (2주차 학습) 패킷 분석 방법 학습

Wireshark VS TCPDump 활용 시나리오 비교

두 분석도구의 세세한 기능은 직접 실습을 해보면서 익히는 것을 추천

구분	Wireshark	TCPDump
인터페이스	GUI	CLI
주요 장점	상세 분석, 시각화, 사용자 친화적	빠름, 경량, 원격 서버 작업에 최적
시스템 자원	비교적 많이 사용	매우 적게 사용
이상적인 상황	로컬 PC에서 캡처, 복잡한 프로토콜 구조 파악	원격 서버에서 간단한 트래픽 확인, 대규모 트래픽 확인
활용 예시	TCP 3-Way HandShake 과정을 흐름으로 분석	웹 서버에서 특정 공격 IP의 유입 여부를 실시간으로 확인

○ 02. 학습 자료 - (2주차 실습) 패킷 분석 실습



실습 시 주의 사항

1. 악성코드가 함유되어 있으므로 가상 머신 사용 추천
2. zip 파일 비밀번호는 “infected_yyyymmdd” 예) infected_19720614
3. 실습 준비: Wireshark 설치

1. 25.01.22 실습 데이터 확인

다중 프로토콜 활용, Powershell 분석, 다중 IOC 식별, TLS C2 이해

2. 목표

피해 호스트 식별: [피해 호스트 식별 과정 참고 링크](#)

피싱 및 감염 경로 분석: [감염 경로 과정 참고 링크](#)

C2 서버 식별 및 악성 코드 추출: [C2 서버 식별 과정 참고 링크](#)

3. 정답 및 전체 과정 확인: [실습 문제 1번 정답](#)

1. 24.11.26 실습 데이터 확인

실습 준비

- 네트워크 대역: 10.11.26.0/24
- AD 환경 호스트 식별, 악성 코드 통신 분석

2. 목표

피해 호스트 식별: [피해 호스트 식별 과정 참고 링크](#)

감염 경로 및 IOC 추출: [감염 경로 과정 참고 링크](#)

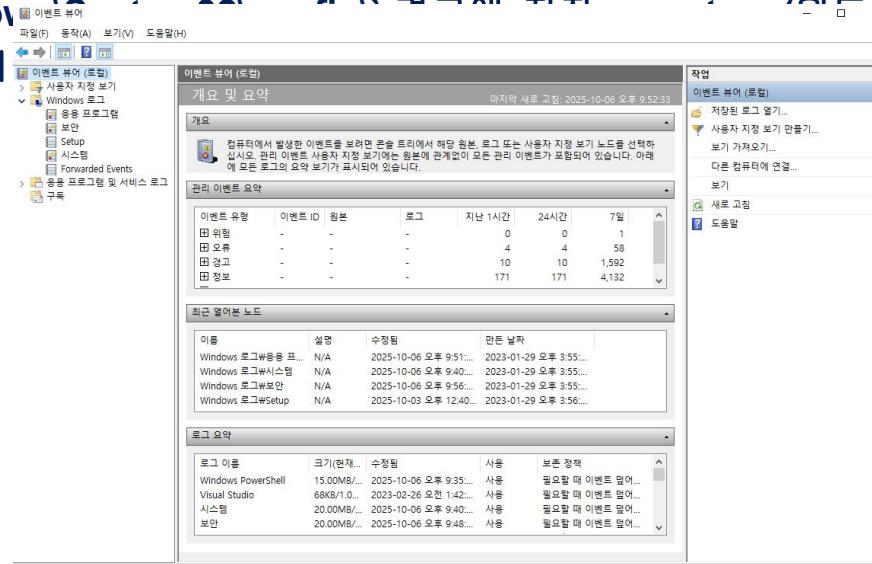
3. 정답 및 전체 과정 확인: [실습 문제 2번 정답](#)

정답 출처: 김태우 학우

○ 02. 학습 자료 - (3주차 학습) 윈도우 이벤트 로그 (1)

1. 개념

- 윈도우 운영체제가 시스템 내부에서 발생한 사건(애플리케이션, 보안, 시스템 등)을 기록한 데이터베이스
- 누가 언제 로그인했는지, 어떤 프로그램이 실행되었는지, 시스템오류, 보안정책 변경이 있었는지 등을 기록
- 일반적으로 `C:\Windows` 이벤트 뷰어 (Windows Event Viewer) 등으로 확인
- 윈도우 “시스템의 일기”



○ 02. 학습 자료 - (3주차 학습) 윈도우 이벤트 로그 (2)

2. 구성 요소

- 윈도우 이벤트 로그는 하드웨어·소프트웨어에서 발생한 모든 사건의 정보를 저장하여, 관리자가 잠재적 위협이나 성능 저하 요인을 추적할 수 있게 해줌
- 각 이벤트는 표준화된 형식으로 저장되어 있으며, 주요 요소는 아래와 같음

로그 이름(name)	로그가 기록될 범주 (System, Security, Application 등)
로그된 날짜(Date)	이벤트가 발생한 날짜와 시간
작업 범주(category)	이벤트의 세부 유형 (개발자가 직접 정의할 수도 있음)
이벤트 ID(Event_id)	이벤트를 고유하게 식별하는 번호
원본(Source)	이벤트를 발생시킨 프로그램 또는 서비스 이름
수준(Level)	이벤트의 심각도 수준 (Information, Warning, Error 등)
사용자(User)	이벤트 발생 시 로그인한 사용자 이름
컴퓨터(Computer)	이벤트가 발생한 컴퓨터 이름

○ 02. 학습 자료 - (3주차 학습) 윈도우 이벤트 로그 (3)

3. 이벤트 심각도(레벨)

- a. 정보(Information) : 문제 없이 발생한 정상 이벤트
- b. 자세한 정보 표시(verbose) : 특정 이벤트의 진행 또는 성공 메시지
- c. 경고(Warning) : 잠재적 문제에 대한 경고
- d. 오류(error) : 즉시 해결은 필요하지 않지만 시스템 오류 발생
- e. 위험(critical) : 즉각적인 조치가 필요한 심각한 문제

로그 이름(M):	응용 프로그램	로그된 날짜(D):	2025-10-07 오전 1:11:10
원본(S):	Security-SPP	작업 범주(Y):	없음
이벤트 ID(E):	1034	키워드(K):	클래식
수준(L):	정보	컴퓨터(R):	Laptop-JH
사용자(U):	해당 없음	Opcode(O):	정보

○ 02. 학습 자료 - (3주차 학습) 윈도우 이벤트 로그 (4)

4. 종류(로그 이름)

- 윈도우는 이벤트를 발생한 카테고리별로 나눠서 저장, 그 종류는 아래와 같음
- 그 중 보안(Security) 로그는 SOC, 포렌식 분야에서 중요하게 사용 됨

로그 이름	설명
시스템 (System)	운영체제(OS) 자체 동작 관련 이벤트 (예: 드라이버 오류)
응용 프로그램 (Application)	설치된 소프트웨어의 오류나 작동 이벤트 (예: PowerPoint 실행 오류)
보안 (Security)	로그인 성공/실패, 파일 삭제 등 보안 관련 활동
Setup	윈도우 설치나 업데이트 관련 이벤트
Forwarded Events	다른 컴퓨터에서 전달된 로그 (중앙 로그 서버용)

○ 02. 학습 자료 - (3주차 학습) 윈도우 보안 로그 (1)

1. 보안 감사 정책

- 보안 로그는 일반적으로 보안 감사 정책에서 설정한 항목에 대해서만 남음
- 현재 활성화된 보안 감사 정책은 관리자 권한의 **powershell**에서 아래 명령어를 통해 확인 가능

> **auditpol /get /category:***



```
관리자: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

새로운 크로스 플랫폼 PowerShell 사용 https://aka.ms/pscore6

PS C:\Windows\system32> auditpol /get /category:*
시스템 감사 정책
범주/하위 범주          설정
시스템
    보안 시스템 확장          감사 없음
    시스템 투명성          성공 및 실패
    IPsec 드라이버          감사 없음
    기타 시스템 이벤트          성공 및 실패
    보안 상태 변경          성공
로그온/로그오프
    로그온          성공 및 실패
    로그오프          성공
    계정 잠금          성공
    IPsec 주 모드          감사 없음
    IPsec 빠른 모드          감사 없음
    IPsec 확장 모드          감사 없음
    특수 로그온          성공
    기타 로그온/로그오프 이벤트          감사 없음
네트워크 정책 서버          성공 및 실패
사용자/작업 클레임          감사 없음
그리고 구독          감사 없음
```

○ 02. 학습 자료 - (3주차 학습) 윈도우 보안 로그 (2)

2. 주요 역할

- 로그인 추적 : 사용자 로그인 성공/실패 기록 (ID 4624, 4625)
- 권한 변경 감시 : 관리자 권한 획득, 그룹 정책 변경 (4672, 4728 등)
- 파일/객체 접근 감시 : 특정 파일이나 폴더 접근 시도 (4663 등)
- 시스템 감사 : 보안 정책, 사용자 계정 변경, 감사 설정 수정 등 기록

3. 주요 이벤트

- 윈도우에서 제공하는 모니터링 할 이벤트는 해당 사이트에서 전체 확인 가능

<https://learn.microsoft.com/ko-kr/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor>

이벤트 ID	이벤트 이름	의미/사용 예시
4624	로그인 성공 (Logon Success)	계정이 정상 로그인됨
4625	로그인 실패 (Logon Failure)	잘못된 암호, 계정 잠금 등
4672	특수 권한 부여된 로그온	관리자 등 높은 권한 부여 시
1102	보안 로그가 지워짐	누군가 Security 로그 삭제 시

○ 02. 학습 자료 - (3주차 학습) 윈도우 보안 로그 (3)

4. 활용 예시

탐지 목적	참조 이벤트	분석 포인트
무차별 로그인 시도 탐지	4625 (로그인 실패)	동일한 IP에서 반복 실패 발생 여부
권한 상승 감시	4672	관리자 권한이 부여된 사용자 확인
새 사용자 생성 탐지	4720	비정상 계정 생성 여부
로그 삭제 흔적 탐지	1102	로그 삭제 시도 = 흔적 은폐 가능성
원격 접속(RDP) 감시	4624 + LogonType 10	원격 로그인 흔적 확인

5. 보안적 의미

- 침해사고 후 포렌식의 핵심 근거 (누가 언제 침입했는지, 어떤 계정이 사용되었는지)
- SIEM 탐지 룰 작성의 근간 데이터 (Splunk, ELK, Wazuh 등에서 이벤트 기반 탐지 규칙 구성)
- 내부자 모니터링 (권한 변경, 로그 삭제 등 이상 행위 탐지)

1. 모니터링의 쓰임

- 시스템 오류, 무단 접근, 외부 공격, 시스템 장애 등을 즉시 감지
- 이벤트의 소스, 사용자, 컴퓨터, 유형, 심각도를 통해 문제의 원인 파악
- 과거 데이터를 분석해 미래의 문제를 예측

2. 자동화 이용 방식

- 웹 콘솔을 통한 필터링 및 시각적 확인
- SNMP 트랩 및 Syslog 메시지와 통합 분석
- 규제 준수를 위한 로그 자동 보관/정리
- 이벤트의 시간, 유형, 소스 기반 실시간 알림(Alerts) 설정 가능

○ 02. 학습 자료 - (3주차 실습) 윈도우 이벤트 로그 분석툴



윈도우 이벤트 로그 분석 툴들을 직접 사용해보자

1. 각 툴의 개념
2. 실행 및 사용 방법
3. 활용 예시
4. 장점 등 특징

사용 분석툴

1. 윈도우 이벤트 뷰어
2. Sysmon
3. Get-WinEvent

참고 자료 : https://stone-hallway-ce8.notion.site/2841c677b79980fbba8ffde732f73e8f?source=copy_link

1. SIEM (Security Information and Event Management)이란?

여러 로그를 통합하고 분석하여 보안 위협 탐지에 도움을 주는 툴이다. 주요 기능으로는 로그 수집 및 저장, 로그 분석, 로그 시각화, 규정 준수(regulatory compliance) 및 보고 등이 있다. 통합 보안 관제 솔루션이라고도 불린다.

2. SIEM 장점

- 실시간 로그 분석을 통한 빠른 조치가 가능
- 로그 시각화를 통해 데이터 분석이 편리
- 차세대 SIEM은 인공지능 모델을 통한 자동화 가능
- 모든 로그가 모여있기 때문에 포렌식 작업이 쉬워짐
- PCI-DSS와 같은 규정 준수와 보고가 편리해짐

○ 02. 학습 자료 - (4주차 학습) ELK stack (1)

1. ELK stack이란?

Elasticsearch, Logstash, 그리고 Kibana를 통합한 소프트웨어 스택이며 가장 사용자가 많은 SIEM 중 하나이다.

Elasticsearch는 ELK stack의 탐색(search) 및 해석(analytics) 엔진이다. 데이터의 인덱싱, 저장, 그리고 쿼리를 담당한다.

Logstash는 로그를 모아서 Elasticsearch로 보내는 역할을 한다. 필요한 경우에 데이터 향상(enrichment)을 하기도 한다.

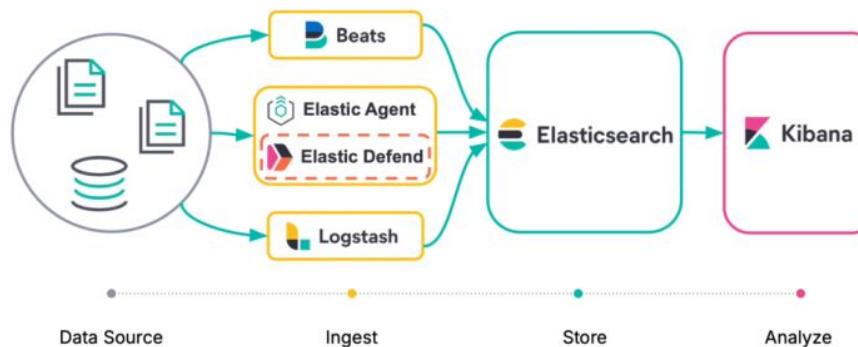
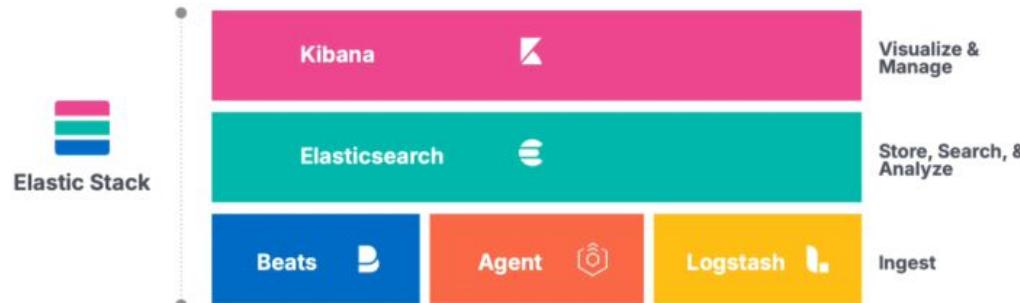
Kibana는 ELK stack의 인터페이스이다. 사용자와 ELK stack의 모든 상호작용은 Kibana를 통해서 이루어진다. 인터페이스의 역할 이외에도 데이터를 시각화해서 대시보드를 생성하는 역할도 한다.

Beats는 단말(endpoint)에서 로그 데이터를 Elasticsearch 혹은 Logstash로 전달한다. Filebeat, Metricbeat, Packetbeat 등 로그 종류에 따라 여러 종류가 있다. Logstash에 비해 가볍지만 기능이 부족하다는 단점이 있다.

Agents는 beats에서 진화했으며 로그나 다른 호스트 정보를 모니터링할 수 있는 통합된 방식을 제공한다.

○ 02. 학습 자료 - (4주차 학습) ELK stack (2)

2. ELK stack 구성



Elastic Stack에서 데이터의 흐름을 나타낸
그림이다.

3. Kibana Query Language

Lucene과 함께 Kibana에서 데이터를 필터링할 때 사용하는 언어이다. 단순히 필터링만 하기 때문에 데이터 집합(aggregation), 변형(transformation)은 불가능하다. 특징은 다음과 같다:

- 필드와 값 쌍으로 이루어져 있다. e.g. event.code:4625
- 문자열로 검색을 할 수도 있다. e.g. 4625
- 와일드카드를 사용할 수 있다. e.g. http.response.status_code: 4*
- 논리 연산과 비교 연산이 가능하다. e.g. http.response.bytes < 1000 AND http.response.bytes > 200
- 문자열이 **text**와 **keyword** 타입 두 가지로 나뉜다. **text** 타입은 각 단어가 토큰화 돼서 단어를 매칭할 수 있고 **keyword** 타입은 문자열로 저장되기 때문에 문자열 전체를 매칭할 수 있다. ([자세한 설명 링크](#))

○ 02. 학습 자료 - (4주차 실습) ELK stack 설치

ELK stack을 설치하고 세팅해보는 것이 구성과 사용법을 익히는데 중요하다고 생각하기 때문에 설치 방법을 보지 않고 생성형 AI의 도움을 받아서라도 직접 해보는 것을 추천한다.

[설치 방법 링크](#)

○ 02. 학습 자료 - (4주차 실습) ELK stack 실습

링크의 아파치 로그를 분석하여 다음을 구하시오:

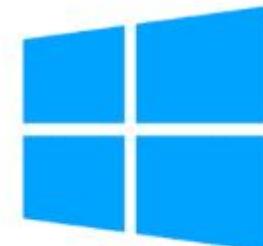
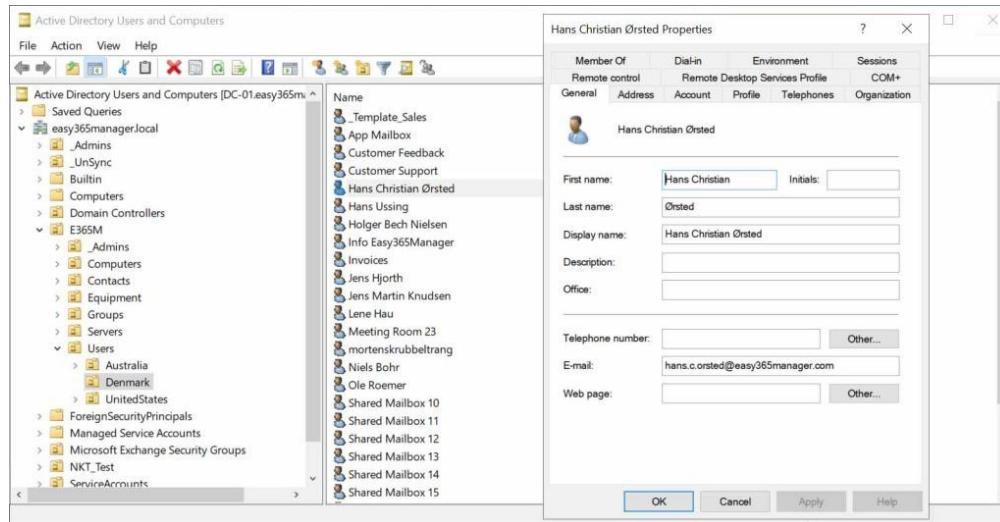
- 가장 많은 이벤트를 생성한 source IP 5개
- 5[.]9[.]143[.]150의 접속 횟수
- 130[.]88[.]99[.]231이 접속할 때 사용한 http method
- user agent가 Windows 7인 이벤트의 수
- http method가 POST 혹은 HEAD인 이벤트 개수
- http method는 POST이고 response status code는 200이 아닌 이벤트 개수는?
- (고난이도) 한 시간 동안 가장 많은 고유한 source IP의 접속이 있는 시간은 어느 날의 몇 시이며 고유한 source IP의 수는 몇 개인지 구하시오 (e.g. 20xx년 xx월 xx일 xx시에 xx개의 고유한 source IP의 접속이 있었다)
- (고난이도) http method GET, HEAD, 그리고 POST 각각 어느 도시로부터 request를 가장 많이 받았고 그게 몇 개인지 구하시오 (e.g. GET은 서울에서 10개의 request, HEAD는 뉴욕에서 12개의 request, POST는 런던에서 8개의 request를 받았다)

정답 링크

○ 02. 학습 자료 - (5주차 학습) Active Directory

- Active Directory

- Microsoft가 개발한 중앙 집중 디렉터리 서비스(디렉터리 = 리소스, 파일구조가 아니다)
- 네트워크 안의 유저, 컴퓨터, 서버, 프린터, 정책, 권한... 등을 중앙에서 통합 관리
- 관리하기 위한 중앙 데이터베이스가 있음.
- 여기서 사용하는 프로토콜이 LDAP, Kerberos.. 등임.

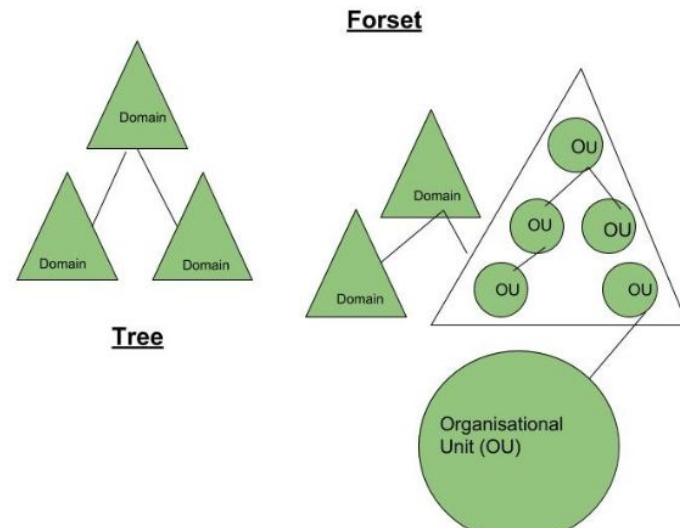


Active Directory

○ 02. 학습 자료 - (5주차 학습) Active Directory

- 구성요소

- Object : AD에서 관리되는 모든 항목들을 Object라고 부름
- Domain : ad의 기본 단위로, 사용자/컴퓨터/그룹 등의 객체를 묶음.
- OU : Organizational Unit, 도메인 내의 하위 그룹. 회사라면, 부서별/역할별로 나눌 수 있음.
- Tree : 도메인이 상하관계로 연결된 구조
- Forest : 여러 트리가 연결된 가장 큰 ad 구조 단위. 조직 전체를 나타냄.



○ 02. 학습 자료 - (5주차 학습) Active Directory



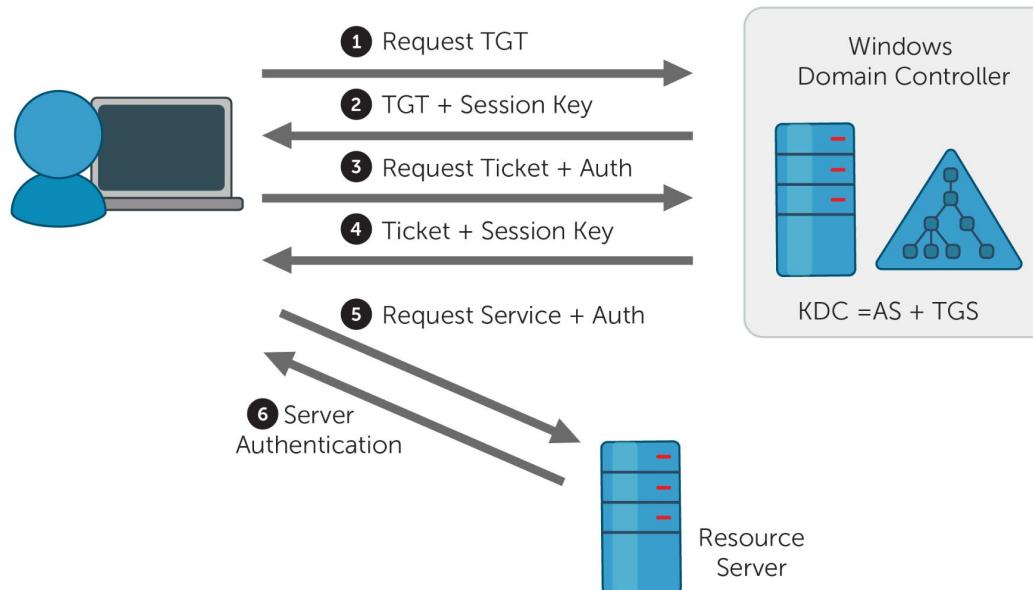
- 기능
 - 인증 (Authentication)
 - Kerberos 등을 활용하여 사용자 인증을 처리합니다.
 - 사용자 로그인 요청 시, 티켓(TGT/TGS) 기반으로 사용자의 신원을 확인합니다.(다음 페이지에서 설명)
 - 신원 확인 후, TGT(Ticket Granting Ticket)를 발급하여 클라이언트가 로컬에 보관합니다.
 - 클라이언트가 특정 서비스에 접근하려면 TGT를 전송하고, TGS(Ticket granting service)에서 티켓을 검증하여 서비스 티켓을 발급합니다.
 - 클라이언트가 이 서비스 티켓을 서비스에 제시하여 접근합니다.
 - 디렉터리 접근
 - LDAP 등을 활용하여 디렉터리에 접근합니다.
 - 여기서 디렉터리는 파일이 아닌, 네트워크 상의 자원(웹 서버, 프린터 등)을 의미합니다.
 - 그룹 정책
 - 구성 요소에 맞게 Object를 그룹화합니다.
 - DNS와 통합하여 활용 가능

개념

- 티켓 기반의 네트워크 인증 프로토콜입니다.
- 티켓에는 다음 정보가 서버 비밀 키로 암호화되어 있습니다.
 - 사용자 ID (User ID)
 - 사용자 호스트 IP 주소 (User host IP addr)
 - 타임스탬프 (timestamp)
 - 티켓 유효 기간 (Ticket TTL)
 - 세션 키 (Session Key)
- Active Directory (AD)의 인증 기능이 이 프로토콜을 사용합니다.
- KDC (Key Distribution Center) : 중앙 인증 서버로서, TGT(Ticket Granting Ticket)를 발급하는 AS(Authentication Server)와 서비스 티켓을 발급하는 TGS(Ticket Granting Server)로 구성됩니다.
- TGT (Ticket Granting Ticket) : 사용자가 KDC로부터 발급받는 증명서입니다. (장시간 유효)
- 서비스 티켓 (Service ticket) : 클라이언트가 서비스를 이용하고자 할 때 해당 서비스에 제시하는 티켓입니다.

○ 02. 학습 자료 - (5주차 학습) Kerberos Protocol

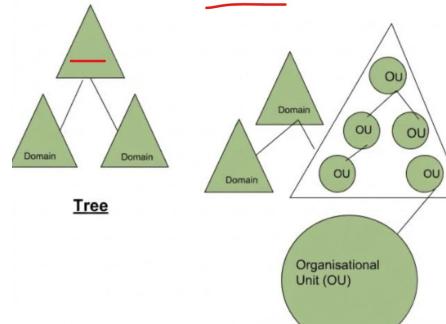
실제 진행 흐름



- 클라이언트 → KDC(AS)에 TGT요청 (AS_REQ)
- KDC → 클라이언트에 암호화된 TGT/세션 키 제공 (AS REP)
- 클라이언트 → KDC(TGS)에 특정 서비스의 티켓 요청 (TGS_REQ)
 - 이때, 클라이언트는 TGT와 서비스 식별자를 함께 보냄
- KDC → 클라이언트 서비스 티켓과 세션키 제공 (TGS REP)
- 클라이언트 → 서비스에 서비스 티켓 제시 (AP REQ)

○ 02. 학습 자료 - (5주차 실습) 개념 확인 문제

1. 이 트리에서, 비워진 빨간 부분에 들어갈 단어를 작성하세요 .

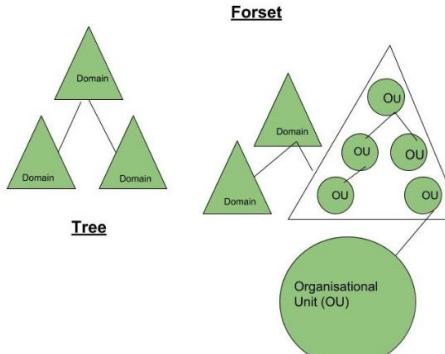


2. O/X류 문제

- a. Kerberos(커버로스)는 패스워드 자체를 네트워크로 전송하여 인증하는 프로토콜이다. (O / X)
- b. KDC(Key Distribution Center)는 인증 서버인 AS와 티켓 발급 서버인 TGS 두 가지로 구성된다. (O / X)
- c. Active Directory의 구성 요소 중 'Forest(포리스트)'는 여러 개의 Tree가 연결된 가장 큰 AD 구조 단위이다. (O / X)
- d. Active Directory에서 'OU(Organizational Unit)'는 도메인 내의 하위 그룹으로, 회사라면 부서별이나 역할별로 나눌 때 사용한다. (O / X)
- e. Active Directory에서 말하는 '디렉터리'는 단순히 파일 시스템의 폴더를 의미한다. (O / X)
- f. TGT(Ticket Granting Ticket)는 한 번 발급받으면 영구적으로 사용할 수 있다. (O / X)

○ 02. 학습 자료 - (5주차 실습) 개념 확인 문제

1. 이 트리에서, 비워진 빨간 부분에 들어갈 단어를 작성하세요



2. O/X류 문제

- a. X, Kerberos는 티켓 기반의 네트워크 인증 프로토콜입니다.
- b. O, KDC는 AS(Authentication Server)와 TGS(Ticket Granting Server)로 구성됩니다.
- c. O, Active Directory의 구성 요소 중 'Forest(포리스트)'는 여러 개의 Tree가 연결된 가장 큰 AD 구조 단위가 맞습니다.
- d. O, Active Directory에서 OU는 "**Organizational Unit**, 도메인 내의 하위 그룹"이며 부서별/역할별로 나눌 수 있습니다.
- e. X, Active Directory에서 말하는 '디렉터리'는 파일이 아닌, 네트워크 상의 자원(웹 서버, 프린터 등)을 의미합니다
- f. X, TGT(Ticket Granting Ticket)는 장시간 유효하나, TTL이 포함되어 유효기간이 있습니다.

○ 02. 학습 자료 - (6주차 학습) IDS/IPS (1)

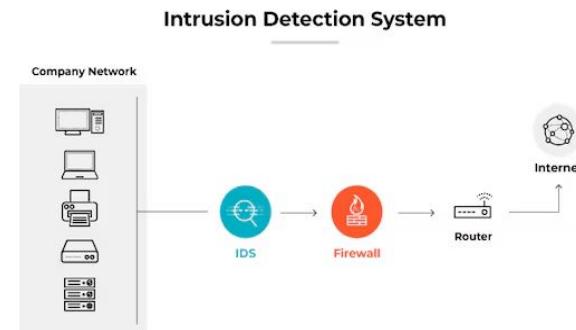
1. 침입 탐지 시스템 (Intrusion Detection System, IDS)란?

네트워크 트래픽과 디바이스에서 위협이나 의심스러운 활동이 있는지 탐지하는 툴이다. 침입 방지 시스템(IPS)과 통합되어 사용되는 경우가 많다. 위협을 탐지하는 방식에는 시그니처 기반, 이상징후(anomaly) 기반, 등이 있다.

시그니처 기반 탐지는 네트워크 트래픽을 알려진 공격 패턴과 대조해서 위협을 탐지하는 방식이다. 공격 패턴들을 담고 있는 데이터베이스를 유지하고 관리하는 것이 필요하다. 알려지지 않은 새로운 위협에 약하다는 단점이 있다.

이상징후 기반 탐지는 머신러닝을 통해 평상시의 트래픽 상태를 모델링하고 여기서 벗어난 활동을 탐지하는 방식이다. 새로운 공격 유형도 탐지할 수 있지만 거짓 양성(false positive)가 빈번하게 발생한다.

이외에도 악의적인 도메인과 연관돼있는 IP주소는 차단하는 평판 기반(reputation based) 탐지, 프로토콜 동작에 중점을 둔 스테이트풀 프로토콜(stateful protocol) 탐지 등이 있다.



2. 침입 탐지 시스템 유형

- 네트워크 침입 탐지 시스템(**NIDS**)는 네트워크 상 중요한 위치에 설치돼 네트워크 상의 트래픽을 모니터링한다. 외부에서 들어오는 공격을 탐지할 수도 있고 내부자 위협(**insider threat**) 혹은 공격자에게 넘어간(**compromised**) 내부 계정의 이상 활동을 탐지할 수도 있다. 탐지하는 것이 역할이기 때문에 트래픽을 방해하지 않도록 대역외(**out-of-band, OOB**)에 설치된다. 즉 네트워크 패킷들의 복사본을 분석한다.
- 호스트 침입 탐지 시스템(**HIDS**)는 단말(**endpoint**)에 설치하여 디바이스의 트래픽과 활동을 모니터링한다. 주기적으로 운영체제 파일 등의 스냅샷을 찍어 변경사항을 탐지한다.
- 프로토콜 기반 침입 탐지 시스템(**PIIDS**)는 서버와 디바이스 사이의 연결 프로토콜을 모니터링한다. 대체로 웹 서버에 설치하여 **HTTP** 커넥션을 모니터링한다.
- 애플리케이션 프로토콜 기반 **IDS(APIDS)**는 애플리케이션 층 프로토콜을 모니터링한다. 주로 **SQL** 인젝션을 탐지하기 위해 웹서버와 **SQL** 데이터베이스 사이에 설치한다.

3. 침입 방지 시스템 (Intrusion Prevention System, IPS)란?

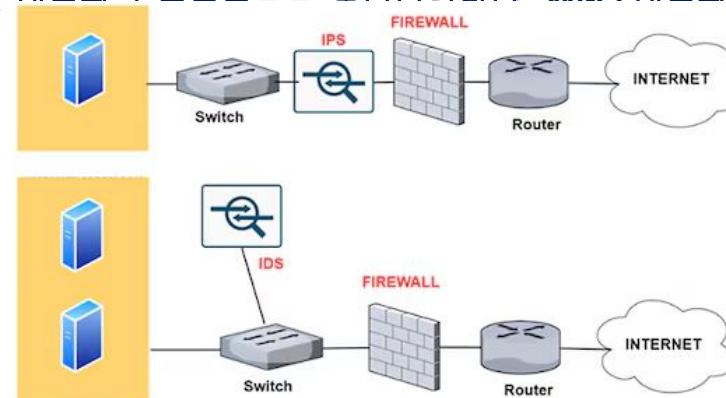
침입 탐지 시스템에서 발전했다. 탐지와 보고뿐만 아니 방지 기능도 지닌다. 위협 탐지 방식에는 침입 탐지 시스템과 마찬가지로 시그니처 기반, 이상 징후 기반 두 가지와 추가로 정책 기반 등이 있다.

정책 기반 탐지는 보안 팀이 설정한 정책을 기반으로 한다. 필요에 따라 쉽게 추가하고 삭제할 수 있다는 장점이 있지만 그만큼 정책을 설정하는데 시간과 자원이 필요하다.

침입 탐지 시스템과 침입 방지 시스템이 통합되어 사용하는 경우가 많으므로 합쳐서 IDS/IPS 혹은 IDPS라고 칭한다.

4. 침입 방지 시스템 유형

- 네트워크 기반 침입 방지 시스템(NIPS)는 대역외에 설치하는 침입 탐지 시스템과 달리 위협을 차단하기 위해서 대역내(inline)에 설치한다.
- 호스트 기반 침입 방지 시스템(HIPS)
- 네트워크 행동 분석(Network Behavior Analysis, NBA)는 네트워크의 흐름을 모니터링한다. IP주소와 포트 번호 같은 상위 층(higher level) 정보를 중점적으로 분석한다. 이상 징후 기반 탐지 방식을 사용하여 이상 징후가 발생하면 차단한다.
- 무선 침입 방지 시스템(WIPS)은 무선 네트워크 프로토콜을 미니미화한 WiFi 네트워크 상 승인되지 않은 장치 등 의심스러운 활동을 탐지할 수 있다.



IDS와 IPS 설치 방식 차이 (out of band vs inline)

○ 02. 학습 자료 - (6주차 학습) Suricata 기초



1. Suricata란?

Open Information Security Foundation (OISF)가 개발하는 오픈 소스 IDS/IPS이다. 탐지룰(detection rule)를 통해 탐지 및 차단을 할 수 있다. 무료이며 유저 친화적인 인터페이스를 가지기 때문에 실습해보기 좋은 툴이다.

2. Suricata 탐지룰

탐지룰은 **action**, **header**, **rule option** 순으로 구성돼있다. **action**은 룰이 일치할 때 할 행동을 나타내고 **header**는 프로토콜과 IP주소, 포트 등을 나타낸다. 마지막으로 **rule option**은 룰의 자세한 옵션을 나타낸다.

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"HTTP GET Request  
Containing Rule in URI"; flow:established,to_server; http.method;  
content:"GET"; http.uri; content:"rule"; fast_pattern; classtype:bad-  
unknown; sid:123; rev:1;)
```

탐지룰에 관한 자세한 내용은 [링크](#)를 통해 확인할 수 있다.

○ 02. 학습 자료 - (6주차 실습) Suricata 실습

사용할 pcap 파일 링크

반드시 가상 머신 사용!

상단의 pcap파일을 사용하여 다음을 구하시오 :

1-1. ".com"이 들어있는 dns 쿼리들을 찾는 룰은?

1-2. jq를 사용해서 rrname를 중복 없이 순서대로 나열했을 때 10번째 URL은?

2-1. 200 ok로 응답이 된 http GET 요청들을 찾는 룰은?

2-2. jq를 사용해서 요청된 URL 중복없이 순서대로 나열

3. Suricata를 IPS 모드로 실행, http 요청들을 무시하는 룰 작성 후 테스트

정답 링크

1. 네트워크 트래픽 분석(Network Traffic Analysis, NTA)란?

네트워크에서 데이터를 수집하고 분석하는 과정이다. 네트워크 성능을 개선, 위협 탐지, 네트워크 문제 해결 등에 사용된다.

2. 분석 과정

- 데이터 수집: 네트워크 상의 데이터를 수집하는 단계다. 네트워크 분석기, 패킷 스니퍼(packet sniffer), IDS 등 특수한 툴을 사용한다.
- 데이터 처리: 원본(raw) 데이터를 사용할 수 있는 데이터로 바꾸는 단계다. 성능 최적화를 위해 필수적이다.
- 데이터 분석: 처리한 데이터를 분석하는 단계다. (1) 기본(baseline) 모델과 현재 트래픽을 대조하는 행동(behavioral) 분석, (2) 프로토콜 분석, (3) 통계적 분석, (4) 애플리케이션 층을 면밀히 살피는 내용(payload) 분석, (5) 흐름(flow) 분석 5개의 세부 단계로 나뉜다.
- 데이터 시각화: 표, 그래프, 대시보드를 활용하여 데이터를 한 눈에 볼 수 있게 시각화하는 단계다.

3. NTA 장점

- 트래픽 패턴을 파악함으로써 네트워크 성능 최적화, 병목현상(bottleneck) 식별, 그리고 위협 탐지에 도움을 준다.
- AI/ML을 통해 이상 현상 탐지를 자동화해서 SOC팀의 시간과 자원을 절약한다.
- 네트워크의 부하(load)를 실시간으로 보여줘서 로드 밸런싱에 필요한 정보를 제공한다.
- SIEM과 같은 다른 도구와 통합해서 효율적인 사용이 가능하다.

4. NTA vs IDS/IPS

- IDS/IPS는 보안에 중점을 두는 반면 NTA는 보안뿐만 아니라 네트워크 성능, 부하 등 여러 내용을 종합적으로 분석한다.
- NTA는 이상이 탐지 되더라도 보고만하고 다른 행동을 취하지 않는데 IDS/IPS는 보고뿐만 아니라 차단, 방지 등의 역할도 수행한다.
- NTA는 네트워크 데이터 수집을 위해 곳곳에 설치하지만 IDS/IPS는 방화벽 바로 뒤 등 전략적인 위치에 설치한다.

○ 02. 학습 자료 - (7주차 학습) Zeek (1)

1. Zeek란

스크립트를 사용할 수 있는 무료 오픈소스 네트워크 분석 툴이다. 전통적 IDS인 Suricata, Snort와 달리 Zeek는 문맥이 풍부한 (context rich) 로그를 제공하여 포렌식, 위협 사냥(threat hunting), 네트워크 보안 모니터링 (Network Security Monitoring, NSM)에 특화돼있다.

구조는 크게 이벤트 엔진과 스크립트 인터프리터 (interpreter)로 나뉜다. 이벤트 엔진은 네트워크 패킷을 분석하고 HTTP GET 요청 탐지 등의 이벤트를 제기(raise)한다. 스크립트 인터프리터는 커스텀 스크립트를 통해 이벤트가 발생했을 때 어떤 행동을 취할지 정할 수 있다. 이러한 구조는 관제와 방침 시행(policy enforcement)을 분리함으로써 상황에 따라 유연한 사용이 가능하도록 한다.

2. Zeek 주요 프레임워크

Zeek는 기능을 확장하기 위해 다양한 프레임워크 모듈을 사용한다. 주요 프레임워크는 다음과 같다:

- 파일 분석: 네트워크에서 파일과 해시를 추출한다.
- 시그니처 프레임워크: 패킷을 알려진 패턴과 대조한다.
- 정보 프레임워크: 위협 인텔리전스 (threat intelligence) 피드를 통합(integrate)한다.
- 로깅 프레임워크: conn.log, dns.log, http.log 등의 로그를 생성한다.
- 통지(notice) 프레임워크: 수상한 활동이 발생하면 경고를 생성해서 notice.log에 저장한다.

○ 02. 학습 자료 - (7주차 실습) Filebeat 세팅

Filebeat가 Zeek 로그를 사용할 수 있도록 설정하시오

[정답 링크](#) (ELK stack과 Zeek 설치 방법에 따라 세부 내용은 다를 수 있다. 결과적으로 Zeek로그를 Kibana에서 볼 수 있기만 하면 된다.)

○ 02. 학습 자료 - (7주차 실습) Zeek 실습



사용할 pcap 파일 링크

반드시 가상 머신 사용!

상단의 pcap파일에 대해 zeek 로그를 생성하고 ELK stack을 사용하여 다음을 구하시오 :

1. 가장 많은 양의 데이터를 주고 받은 프로토콜을 찾고 싶을 때 사용하는 로그는?
2. conn.log를 사용해서 10[.]1[.]17[.]215와 5[.]252[.]153[.]241가 주고 받은 패킷의 수를 구하시오
3. http.log를 사용해서 10[.]1[.]17[.]215가 5[.]252[.]153[.]241에 보낸 GET 요청의 수와 그 중 응답 코드가 200인 이벤트의 수를 구하시오
4. 가장 많은 수의 파일을 주고 받은 세션의 source ip, destination ip, 요청한 URL을 구하시오 (힌트: file.log, http.log를 둘 다 사용)

정답 링크

03

참고 자료



○ 03. 참고 자료 - 1주차

- [1] <https://www.ibm.com/kr-ko/think/topics/mitre-attack>
- [2] <https://www.ibm.com/think/topics/mitre-attack>
- [3] <https://www.ibm.com/think/topics/security-operations-center>
- [4] <https://radianitsecurity.ai/learn/soc-tier-1-vs-tier-2-vs-tier-3/>
- [5] <https://youtu.be/56NDgBOSpUg?feature=shared>

○ 03. 참고 자료 - 2주차

- [1] 데이터 통신 학습 자료 - 이병문 교수님 제공
- [2] <https://share.google/DMvXoaGqgda3a5444>
- [3] <https://share.google/abToVn1uGFmotVsE8>

o 03. 참고 자료 - 3주차

- [1] <https://learn.microsoft.com/ko-kr/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor>
- [2] <https://learn.microsoft.com/ko-kr/sysinternals/downloads/sysmon>
- [3] <https://learn.microsoft.com/ko-kr/sysinternals/downloads/sysmon#event-filtering-entries>

o 03. 참고 자료 - 4주차

- [1] <https://www.ibm.com/think/topics/siem>
- [2] <https://m.blog.naver.com/withnetworks/222004949824>
- [3] <https://learn.elastic.co/learn/courses/569/elastic-security-for-siem-on-demand>
- [4] <https://logstail.com/blog/what-is-filebeat-and-why-is-it-important/>

○ 03. 참고 자료 - 5주차

- [1] <https://co-no.tistory.com/entry/Windows-ADActive-Directory%EC%9D%98-%EA%B0%9C%EB%85%90-%EB%B0%8F-%ED%99%9C%EC%9A%A9>
- [2] <https://ossian.tistory.com/47?category=757844>
- [3] <https://aahc.tistory.com/16>

○ 03. 참고 자료 - 6주차

- [1] <https://www.ibm.com/kr-ko/think/topics/intrusion-detection-system>
- [2] <https://www.ibm.com/kr-ko/think/topics/intrusion-prevention-system>
- [3] <https://www.paloaltonetworks.co.kr/cyberpedia/firewall-vs-ids-vs-ips>
- [4] <https://www.paloaltonetworks.co.kr/cyberpedia/what-is-an-intrusion-detection-system-ids>
- [5] [https://en.wikipedia.org/wiki/Suricata_\(software\)](https://en.wikipedia.org/wiki/Suricata_(software))
- [6] <https://clearnetwork.com/top-intrusion-detection-and-prevention-systems/>

o 03. 참고 자료 - 7주차

- [1] <https://www.ibm.com/kr-ko/think/topics/network-traffic-analysis>
- [2] <https://sentinel-overwatch.com/what-are-the-differences-between-network-traffic-analysis-and-intrusion-detection/>
- [3] <https://medium.com/@ashutoshthakurofficial/deep-dive-into-zeek-a-powerful-network-security-monitoring-tool-f52ff3485035>

Thank You

